User Guide

NTC-400 Series

Important Notice

This device, like any wireless device, operates using radio signals which cannot guarantee the transmission and reception of data in all conditions. While the delay or loss of signal is rare, you should not rely solely on any wireless device for emergency communications or otherwise use the device in situations where the interruption of data connectivity could lead to death, personal injury, property damage, data loss, or other loss. NetComm Wireless accepts no responsibility for any loss or damage resulting from errors or delays in transmission or reception, or the failure of the NetComm Wireless NTC-400 Series Router to transmit or receive such data.

Safety and Hazards

Warning – Do not connect or disconnect cables or devices to or from the USB port, SIM card tray, Ethernet port or the terminals of the Molex power connector in hazardous locations such as those in which flammable gases or vapours may be present, but normally are confined within closed systems; are prevented from accumulating by adequate ventilation; or the location is adjacent to a location from which ignitable concentrations might occasionally be communicated.

Copyright

NetComm Wireless Limited was acquired by Casa Systems, Inc. a Delaware company on 1 July 2019. The information contained herein is proprietary to Casa Systems, Inc. No part of this document may be translated, transcribed, reproduced, in any form, or by any means without prior written consent of Casa Systems, Inc.

Trademarks and registered trademarks are the property of NetComm Wireless Limited or their respective owners. Specifications are subject to change without notice. Images shown may vary slightly from the actual product.

Note – This document is subject to change without notice.

Save our environment

When this equipment has reached the end of its useful life, it must be taken to a recycling centre and processed separately from domestic waste.

The cardboard box, the plastic contained in the packaging, and the parts that make up this device can be recycled in accordance with regionally established regulations. Never dispose of this electronic equipment along with domestic waste. You may be subject to penalties or sanctions under the law. Instead, ask for disposal instructions from your municipal government.

Please be responsible and protect our environment.

Document history

This guide covers the following product models:

- NTC-402-01
- NTC-402-02

Ver.	Document description	Date
v1.0	Initial document release	1 November 2017
v1.1	Correction to paragraph numbering	16 January 2018
v1.2	Miscellaneous changes, additions, corrections, etc.	13 March 2018
v1.3	Added RF exposure/min separation warning	3 May 2018
v1.4	Corrected section *1.4 Logging on to the web interface*	10 October 2018
v1.5	Removed Band selection from section *3.1.2.7 Configure SIM-A / SIM-B Card*	13 December 2018
v1.6	Updated section *1.3.2.3 Insert the SIM card*	18 January 2019
v1.7	Updated the description of the 8GB embedded storage functionality	28 February 2020

Table i. - Document revision history

Contents

Overview

Introduction

This document provides you all the information you need to set up, configure and use the NetComm Wireless NTC-400 Series Router.

Target audience

This document is intended for system integrators or experienced hardware installers who understand telecommunications terminology and concepts.

Prerequisites

Before continuing with the installation of your NTC-400 Series Router, please confirm that you have the following:

An electronic computing device with a working Ethernet network adapter and a web browser such as Internet Explorer®, Mozilla Firefox® or Google Chrome™.

Notation

The following symbols are used in this user guide:

ℹ **Note** – The following note provides useful information.

⚠ **Important** – The following note requires attention.

⚡ **Warning** – The following note provides a warning.

1 Product introduction

1.1 Package contents

- 1 x NTC-400 Series Router
- 2 x 2.4GHz/5GHz Wi-Fi antennas
- 1 x 8-way terminal connector
- 2 x Mounting brackets
- 4 x Mounting bracket screws
- 1 x Quick start guide

1.2 Device overview

1.2.1 Interfaces

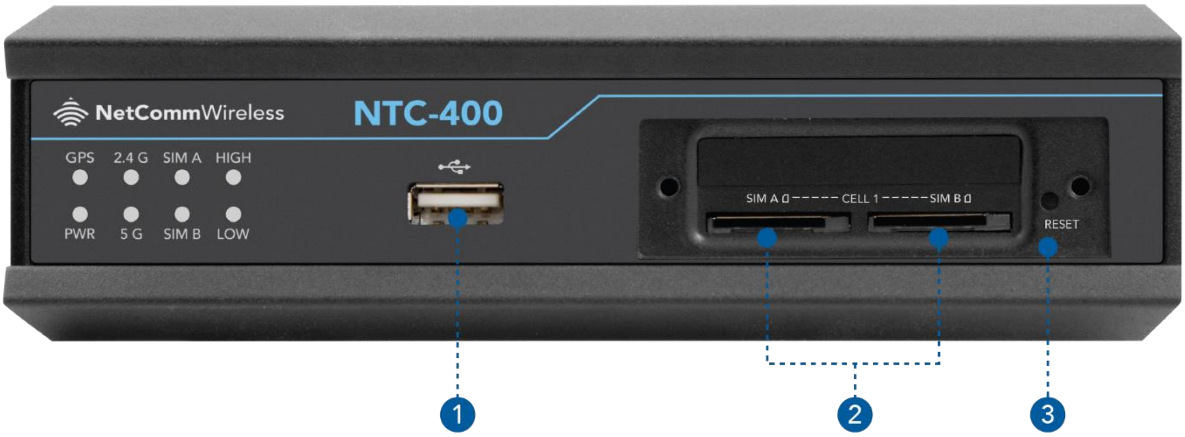


Figure 1 – Interfaces (Front)

No.	Description	Notes
1	USB Type A port	Connect a USB storage device.
2	SIM A and SIM B slots	Insert SIM cards into the SIM slots to use a cellular network. When two SIM cards are inserted, you can configure one to operate as primary and the other as a backup (failover).
3	Reset button	Used to reset the device to factory default settings. Hold the reset button down for 6 seconds, then release it to reboot the device with the factory default settings.

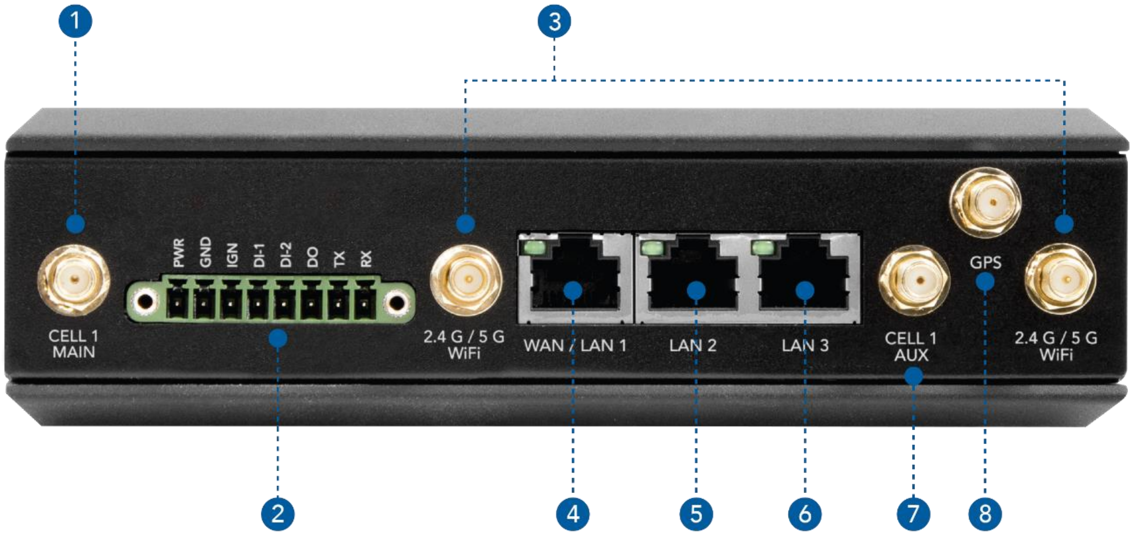


Figure 2 – Interfaces (Rear)

No.	Description	Notes
1	CELL1 Main Socket	Connect one of the 3G/LTE Antennas here. If only using a single antenna, ensure that it is connected to this port.
2	Power Terminal Block	The Power Terminal Block provides the following ports: • PWR (Power) – Supports 9V – 36V DC power input. • GND (Ground) – Terminal for ground wire connection. • IGN (Ignition) – Terminal used to connect to the ignition sense wire of a vehicle. • DI-1 (Digital Input 1) ○ Trigger voltage (high) – 5V - 30V ○ Trigger voltage (low) – 0V - 2.0V • DI-2 (Digital Input 2) ○ Trigger voltage (high) – 5V - 30V ○ Trigger voltage (low) – 0V - 2.0V • DO (Digital Output) ○ Voltage (Relay mode) – Depends on external device, maximum voltage is 30V. ○ Maximum current – 1A. • TX (Transmit) – Provides serial (RS-232) connectivity. • RX (Receive) - Provides serial (RS-232) connectivity.
3	2.4GHz/5GHz Wi-Fi Antenna Socket	Connect the Wi-Fi Antennas here.
4	WAN/LAN1 Port	Auto MDI/MDIX RJ45 Port to connect local devices or an upstream network when the port is set to WAN mode.
5	LAN2 Port	Auto MDI/MDIX RJ45 Port to connect local devices.
6	LAN3 Port	Auto MDI/MDIX RJ45 Port to connect local devices.

No.	Description	Notes
7	CELL1 AUX Socket	Connect one of the 3G/LTE Antennas here.
8	GPS Antenna Socket	Connect the included GPS antenna to this socket.

Table 1 – Interfaces (Rear)

1.2.2 LED indicators

LED Icon	Status	Description
GPS	Off	GNSS function is disabled.
	On	Location is fixed.
	Flashing	Fixing location.
PWR	Off	Device is powered off or is in standby mode.
	On	Device is powered on.
	Flashing one per second	Device is in “Delay off” mode.
	Fast flashing	Firmware upgrade in process or device is in recovery mode.
2.4G	Off	2.4GHz Wi-Fi is disabled.
	On	2.4GHz Wi-Fi is enabled.
	Fast flashing	Data is being transmitted via the 2.4GHz Wi-Fi network.
5G	Off	5GHz Wi-Fi is disabled.
	On	5GHz Wi-Fi is enabled.
	Fast flashing	Data is being transmitted via the 5GHz Wi-Fi network.
SIM A	Off	No SIM inserted or the SIM slot is not being used for a 3G/4G connection.
	On	SIM card is inserted and being used for a 3G/4G connection.
SIM B	Off	No SIM inserted or the SIM slot is not being used for a 3G/4G connection.
	On	SIM card is inserted and being used for a 3G/4G connection.
HIGH	On	3G/4G signal strength is at a high level.
LOW	On	3G/4G signal strength is at a low level.
WAN/ LAN1-3	On	Ethernet connection established on the corresponding LAN/WAN port.
	Flashing	Data is being transmitted or received on the port.

Table 2 – LED indicators

1.3 Installation

1.3.1 System requirements

Before beginning with the installation of your router, please ensure that you have the following:

- An RJ45 Ethernet cable
- An active 3G/4G SIM card (two SIM cards if you plan to use the SIM failover feature)
- An IEEE 802.11b/g/n/ac wireless client
- A computer with a:
  - Windows, Mac OS or Linux-based operating system
  - 10/100/1000 Ethernet adapter on a PC for configuration
  - Web browser such as Internet Explorer, Google Chrome, Mozilla Firefox or Safari

1.3.2 Hardware installation

1.3.2.1 Important notes on installation

Warning:

- The NTC-400 Series Router may be powered by a DC12V or DC24V car system. If the router is not installed in a vehicle, we recommend using a DC12V/2A power adapter to power the unit.
- The surface temperature of the metallic enclosure can be very hot, especially after long periods of operation. Before attempting to perform any physical maintenance to the unit, power it down and allow some time for it to cool.
- Do not attempt to service the unit yourself. If repairs are required, contact your sales representative.

1.3.2.2 Mount the unit

Using an appropriately sized screwdriver, attach the two mounting brackets to the sides of the device with the provided screws as shown below:

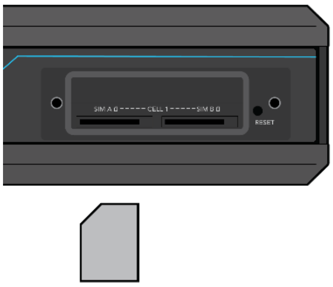
1.3.2.3 Insert the SIM card(s)

Warning – Before changing or inserting a SIM card, ensure that the unit is powered OFF.

Note: SIM B is disabled on units purchased through Telstra. On these units, insert the SIM card into slot A.

1 Using an appropriately sized screwdriver, remove the two screws from the SIM card cover on the front panel of the device.

2 Insert the SIM card(s) into the SIM slots as illustrated below.



3 To eject an inserted SIM, push it in again.

4 After the SIM card(s) have been inserted, screw the SIM card cover back into place.

1.3.2.4 Connecting power

The NTC-400 Series Router accepts DC power in the range of 9 V to 36 V. Follow the picture below to ensure that the power source is connected with the correct polarity.

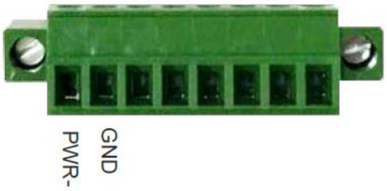


Figure 3 – Power pins on terminal block

1.3.2.5 Connecting digital input/output devices and ignition

There are two digital input pins, one digital output pin and an ignition pin. Refer to the picture below to ensure that the pins are correctly connected.

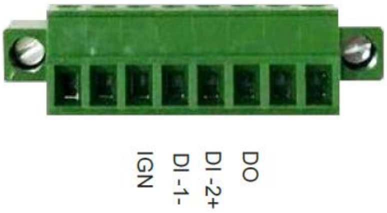


Figure 4 – Digital input, digital output and ignition pins on terminal block

1.3.2.6 I/O specifications

The table below lists the voltage specifications of the digital input and output ports.

Mode	Specification	
Digital Input (DI-1 and DI-2)	Trigger voltage (high)	Logic level 1: 5 V to 30 V
	Normal voltage (low)	Logical level 0: 0 V to 1.0 V
Digital Output (DO)	Voltage (Relay mode)	Logic level 1: Depends on external device. Maximum voltage is 36 V. Logic level 0: Floating, External pull-down resister (10 K Ohm, ½ W) is required. **Note** DO power is relayed from the "PWR" pin on the 8-pin terminal block connector.
	Maximum current	1 Amp @ 12 V, or 0.33 Amp @ 36 V

Table 3 – I/O specifications

1.3.2.7 Connecting serial devices

The NTC-400 Series Router features one RS-232 serial port with RX and TX signals located on the terminal block as shown below.

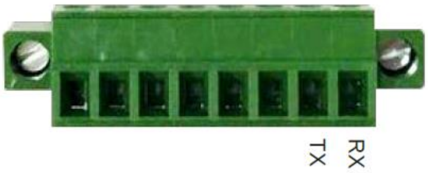


Figure 5 – Serial pins on terminal block

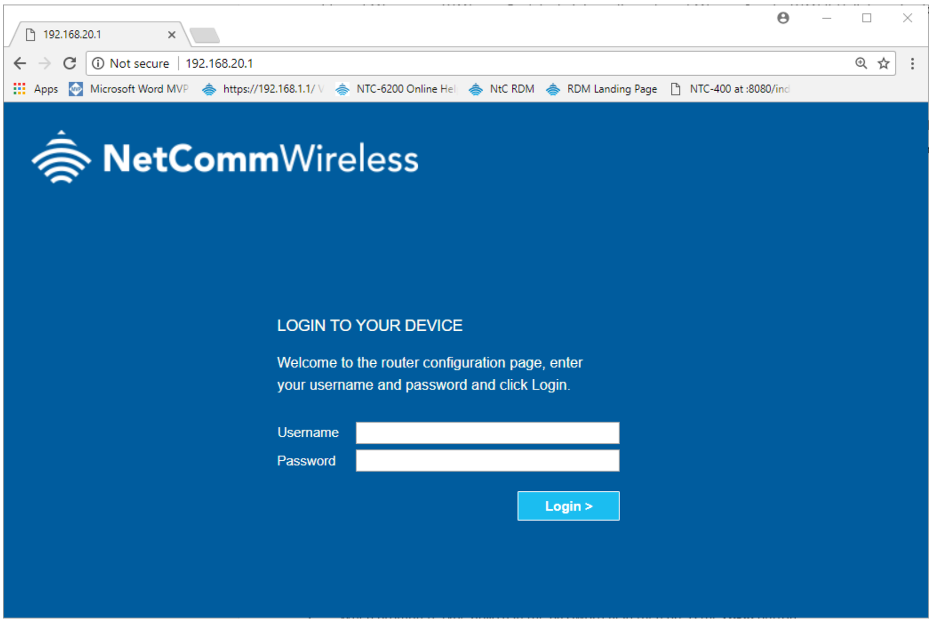
1.3.2.8 Connecting to the network via Ethernet

The NTC-400 Series Router provides three RJ-45 10/100/1000 Mbps Ethernet ports with auto-MDIX. WAN/LAN1 may be used as either a LAN port or a WAN port. By default, it is configured as a LAN port. See the WAN & Uplink section for details on configuring a WAN connection.

1.4 Logging on to the web interface

When all components have been connected, the unit has been powered up and the client PC is connected either by Ethernet or Wi-Fi, you can access the web interface for configuration of the NTC-400 Series Router. To access the web interface:

1 Open a web browser and navigate to: http://192.168.20.1



LOGIN TO YOUR DEVICE

Welcome to the router configuration page, enter your username and password and click Login.

Username

Password

Login >

Figure 6 – NTC-400 Series Router Login screen

2 When prompted, enter the username and password printed on the back cover of the Quick Start Guide and on the label affixed to the bottom of the device, then press the **Login** button.

The web interface is displayed.

Note – We highly recommend that you secure the Wi-Fi networks upon initial installation and change the password used to access the web interface.

2 Status

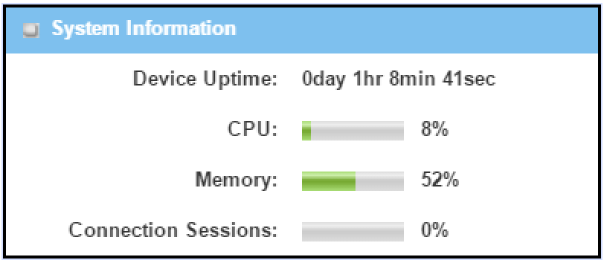
2.1 Dashboard

The **Device Dashboard** window shows the current status in graph or tables for quickly viewing the operation status of the router. They are the System Information, System Information History, and Network Interface Status.

From the menu on the left, select the **Status > Dashboard > Device Dashboard** tab.

System Information Status

The System Information screen shows the device Up-time and the resource utilization for the CPU, Memory, and Connection Sessions.



System Information

Device Uptime: 0day 1hr 8min 41sec

CPU: 8%

Memory: 52%

Connection Sessions: 0%

Figure 7 – System Information

System Information History

The **System Information History** screen shows the statistic graphs for the CPU and memory.

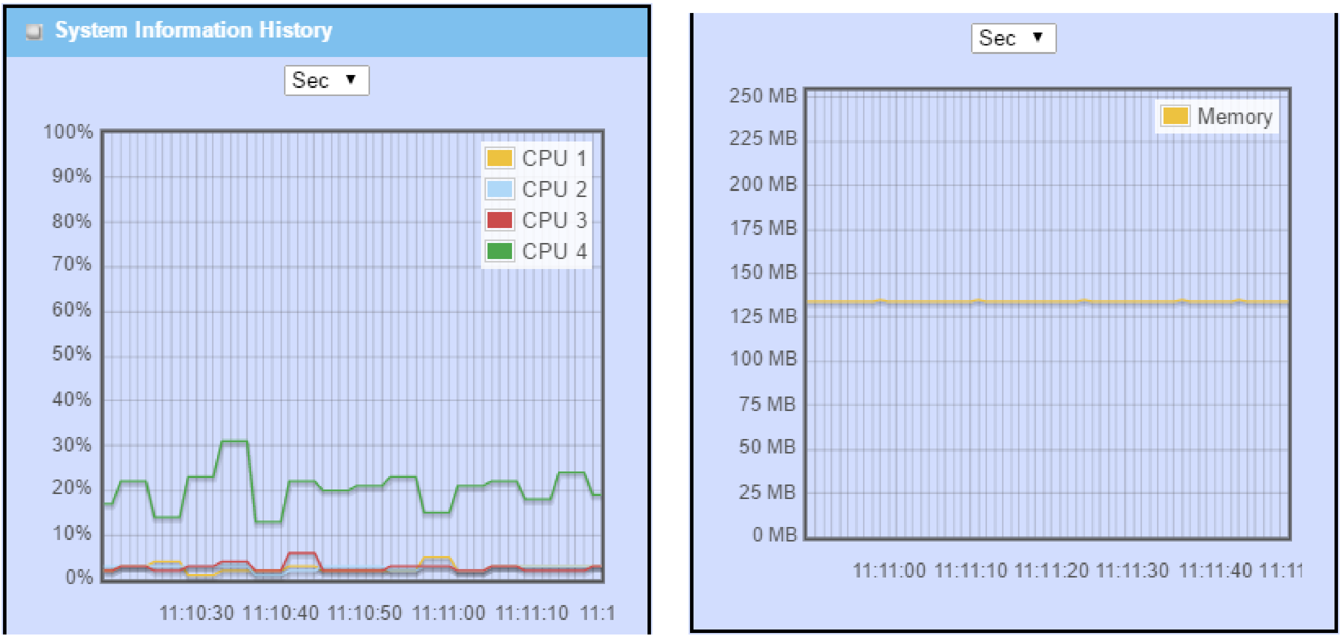
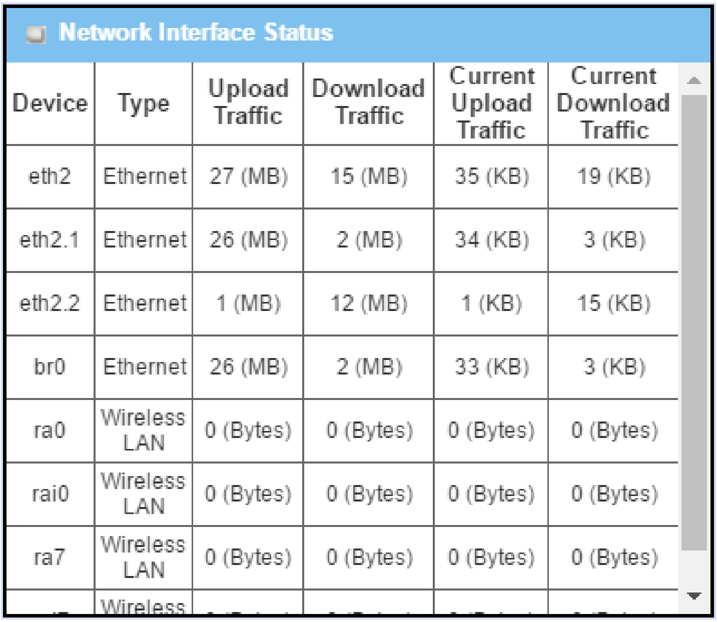


Figure 8 – System Information History displays

Network Interface Status

The **Network Interface Status** screen shows the statistic information for each network interface of the gateway. The statistic information includes the Interface Type, Upload Traffic, Download Traffic, and Current Upload / Download Traffic.



Network Interface Status

Device	Type	Upload Traffic	Download Traffic	Current Upload Traffic	Current Download Traffic
eth2	Ethernet	27 (MB)	15 (MB)	35 (KB)	19 (KB)
eth2.1	Ethernet	26 (MB)	2 (MB)	34 (KB)	3 (KB)
eth2.2	Ethernet	1 (MB)	12 (MB)	1 (KB)	15 (KB)
br0	Ethernet	26 (MB)	2 (MB)	33 (KB)	3 (KB)
ra0	Wireless LAN	0 (Bytes)	0 (Bytes)	0 (Bytes)	0 (Bytes)
rai0	Wireless LAN	0 (Bytes)	0 (Bytes)	0 (Bytes)	0 (Bytes)
ra7	Wireless LAN	0 (Bytes)	0 (Bytes)	0 (Bytes)	0 (Bytes)
	Wireless				

Figure 9 – Network Interface Status

2.2 Basic Network

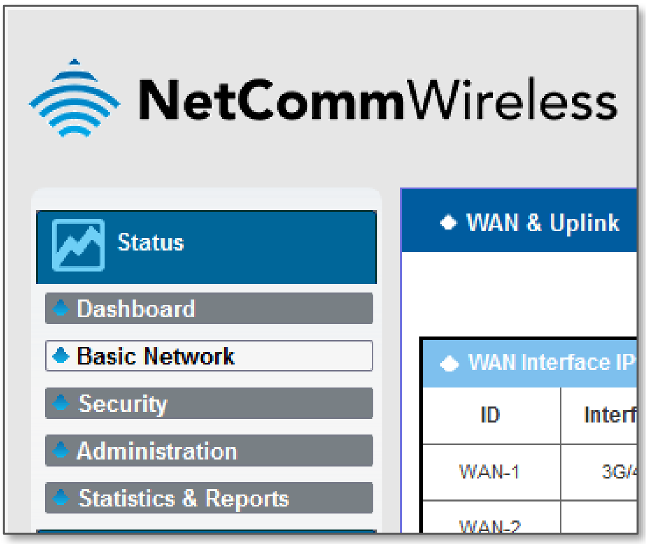


Figure 10 – Basic Network menu item

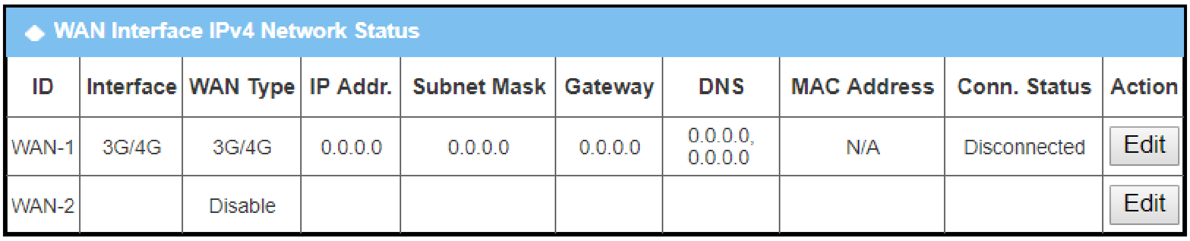
2.2.1 WAN & Uplink Status

Navigate to the **Status > Basic Network > WAN & Uplink** tab.

The **WAN & Uplink Status** window shows the current status for different network type, including network configuration, connecting information, modem status and traffic statistics.

WAN interface IPv4 Network Status

The **WAN interface IPv4 Network Status** screen shows status information for IPv4 network.



◆ WAN Interface IPv4 Network Status

ID	Interface	WAN Type	IP Addr.	Subnet Mask	Gateway	DNS	MAC Address	Conn. Status	Action
WAN-1	3G/4G	3G/4G	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0, 0.0.0.0	N/A	Disconnected	Edit
WAN-2		Disable							Edit

Figure 11 – WAN interface IPv4 Network Status

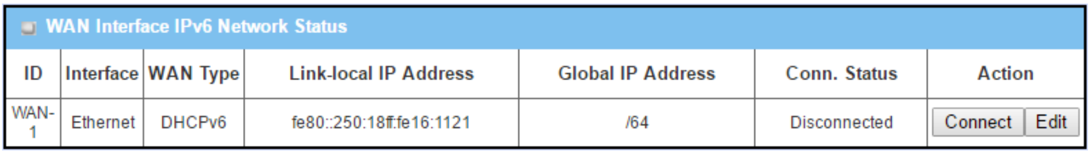
Item	Value setting	Description
ID	System generated.	Displays corresponding WAN interface WAN IDs.
Interface	System generated.	Displays the type of WAN physical interface. Depending on the model purchased, it can be **Ethernet**, **3G/4G**, etc...
WAN Type	System generated.	Displays the method which public IP address is obtained from your ISP. Depending on the model purchased, it can be: **Static IP**, **Dynamic IP**, **PPPoE**, **PPTP**, **L2TP**, **3G/4G**
IP Addr.	System generated.	Displays the public IP address obtained from your ISP for Internet connection. Default value is 0.0.0.0 if left unconfigured.
Subnet Mask	System generated.	Displays the Subnet Mask for public IP address obtained from your ISP for Internet connection. Default value is 0.0.0.0 if left unconfigured.
Gateway	System generated.	Displays the Gateway IP address obtained from your ISP for Internet connection. Default value is 0.0.0.0 if left unconfigured.
DNS	System generated.	Displays the IP address of DNS server obtained from your ISP for Internet connection. Default value is 0.0.0.0 if left unconfigured.
MAC Address	System generated.	Displays the MAC Address for your ISP to allow you for Internet access. **Note** – Not all ISP may require this field.
Conn. Status	System generated.	Displays the connection status of the device to your ISP: **Connected** or **Disconnected**
Action	Buttons	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 – 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

Item	Value setting	Description
		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.

Table 4 – WAN interface IPv4 Network Status

WAN interface IPv6 Network Status

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



WAN Interface IPv6 Network Status

ID	Interface	WAN Type	Link-local IP Address	Global IP Address	Conn. Status	Action
WAN-1	Ethernet	DHCPv6	fe80::250:18ff:fe16:1121	/64	Disconnected	Connect Edit

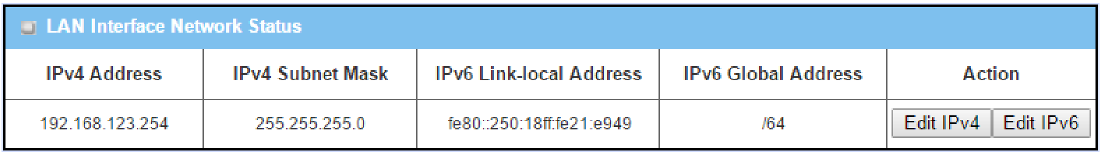
Figure 12 – WAN interface IPv6 Network Status

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

Table 5 – WAN interface IPv6 Network Status

LAN Interface Network Status

The **LAN Interface Network Status** screen shows IPv4 and IPv6 information of LAN network.



LAN Interface Network Status

IPv4 Address	IPv4 Subnet Mask	IPv6 Link-local Address	IPv6 Global Address	Action
192.168.123.254	255.255.255.0	fe80::250:18ff:fe21:e949	/64	Edit IPv4 Edit IPv6

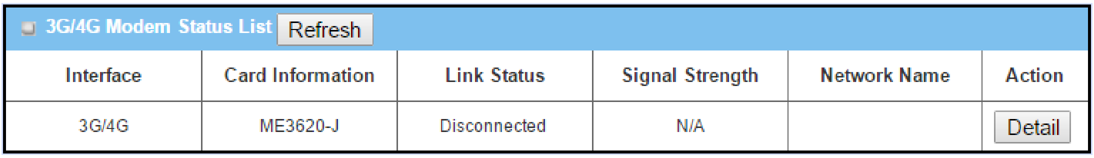
Figure 13 – LAN Interface Network Status

Item	Value setting	Description
IPv4 Address	System data.	Displays the current IPv4 IP Address of the gateway This is also the IP Address user use to access Router's Web-based Utility.
IPv4 Subnet Mask	System data.	Displays the current mask of the subnet.
IPv6 Link-local Address	System data.	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	System data.	Displays the current IPv6 global IP address assigned by your ISP for your Internet connection.
Action	Button	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**.)

Table 6 – LAN Interface Network Status

3G/4G Modem Status

The **3G/4G Modem Status List** screen shows status information for 3G/4G WAN network(s).



3G/4G Modem Status List Refresh

Interface	Card Information	Link Status	Signal Strength	Network Name	Action
3G/4G	ME3620-J	Disconnected	N/A		Detail

Figure 14 – 3G/4G Modem Status

Item	Value setting	Description
Physical Interface	System data.	Displays the type of WAN physical interface. 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	System data.	Displays the vendor's 3G/4G modem model name.

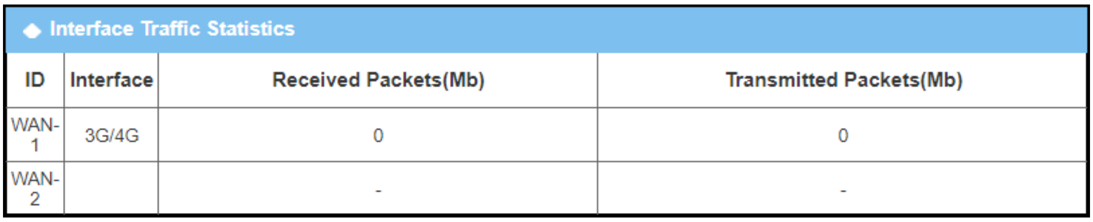
Item	Value setting	Description
Link Status	System data.	Displays the 3G/4G connection status. The status can be Connecting, Connected, Disconnecting, and Disconnected.
Signal Strength	System data.	Displays the 3G/4G wireless signal level.
Network Name	System data.	Displays the name of the service network carrier.
Refresh	Button	Click the **Refresh** button to renew the information.
Action	Button	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.

Table 7 – 3G/4G Modem Status

When the **Detail** button is pressed, 3G/4G modem information windows such as Modem Information, SIM Status, Service Information, and Signal Strength / Quality will appear.

Interface Traffic Statistics

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



Interface Traffic Statistics

ID	Interface	Received Packets(Mb)	Transmitted Packets(Mb)
WAN-1	3G/4G	0	0
WAN-2		-	-

Figure 15 – Interface Traffic Statistics

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

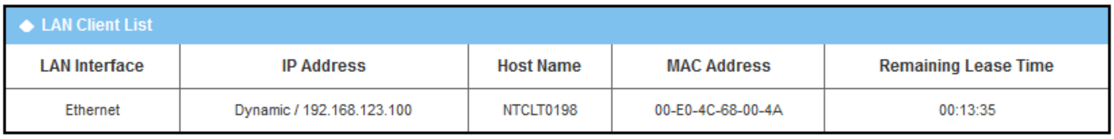
Table 8 – Interface Traffic Statistics

2.2.2 LAN & VLAN Status

Navigate to the **Status > Basic Network > LAN & VLAN** tab.

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 gateway.



◆ LAN Client List

LAN Interface	IP Address	Host Name	MAC Address	Remaining Lease Time
Ethernet	Dynamic / 192.168.123.100	NTCLT0198	00-E0-4C-68-00-4A	00:13:35

Figure 16 – Client List

Item	Value setting	Description
LAN Interface	System data.	Client record of LAN Interface. String Format.
IP Address	System data.	Client record of IP Address Type and the IP Address. Type is String Format and the IP Address is IPv4 Format.
Host Name	System data.	Client record of Host Name. String Format.
MAC Address	System data.	Client record of MAC Address. MAC Address Format.
Remaining Lease Time	System data.	Client record of Remaining Lease Time. Time Format.

Table 9 – Client List

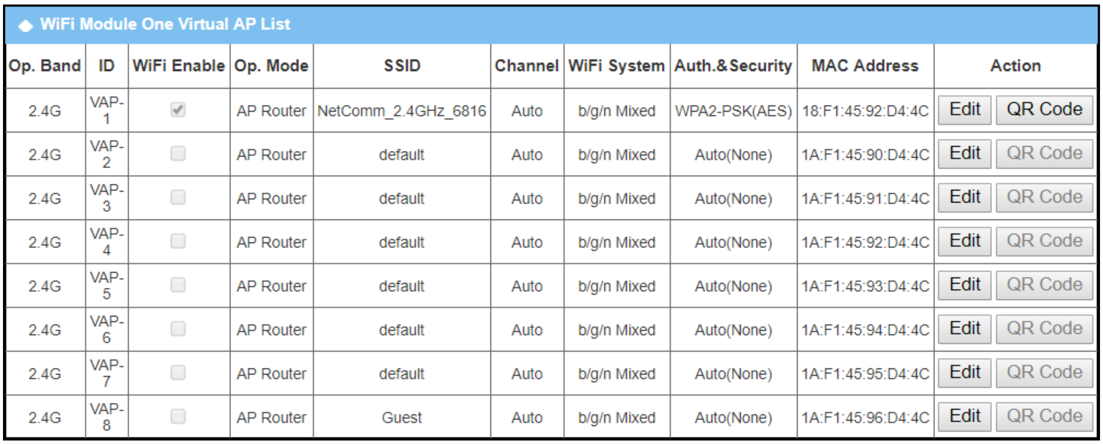
2.2.3 Wi-Fi Status

Navigate to the **Status > Basic Network > Wi-Fi** tab.

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

Wi-Fi 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	☑	AP Router	NetComm_2.4GHz_6816	Auto	b/g/n Mixed	WPA2-PSK(AES)	18:F1:45:92:D4:4C	Edit QR Code
2.4G	VAP-2	☐	AP Router	default	Auto	b/g/n Mixed	Auto(None)	1A:F1:45:90:D4:4C	Edit QR Code
2.4G	VAP-3	☐	AP Router	default	Auto	b/g/n Mixed	Auto(None)	1A:F1:45:91:D4:4C	Edit QR Code
2.4G	VAP-4	☐	AP Router	default	Auto	b/g/n Mixed	Auto(None)	1A:F1:45:92:D4:4C	Edit QR Code
2.4G	VAP-5	☐	AP Router	default	Auto	b/g/n Mixed	Auto(None)	1A:F1:45:93:D4:4C	Edit QR Code
2.4G	VAP-6	☐	AP Router	default	Auto	b/g/n Mixed	Auto(None)	1A:F1:45:94:D4:4C	Edit QR Code
2.4G	VAP-7	☐	AP Router	default	Auto	b/g/n Mixed	Auto(None)	1A:F1:45:95:D4:4C	Edit QR Code
2.4G	VAP-8	☐	AP Router	Guest	Auto	b/g/n Mixed	Auto(None)	1A:F1:45:96:D4:4C	Edit QR Code

Figure 17 – Wi-Fi Virtual AP List

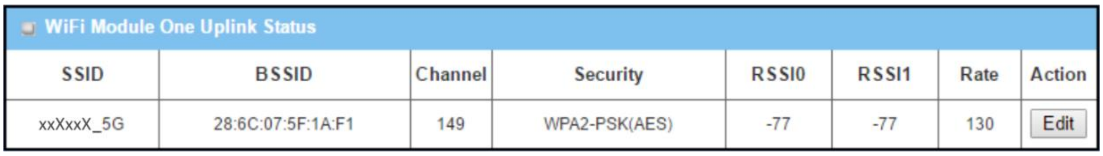
Item	Value setting	Description
Op. Band	System data.	Displays the Wi-Fi Operation Band (2.4G or 5G) of VAP.
ID	System data.	Displays the ID of VAP.

Item	Value setting	Description
Wi-Fi Enable	System data.	Displays whether the VAP wireless signal is enabled or disabled.
Op. Mode	System data.	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	System data.	Displays the network ID of VAP.
Channel	System data.	Displays the wireless channel used.
Wi-Fi System	System data.	The Wi-Fi System of VAP.
Auth. & Security	System data.	Displays the authentication and encryption type used.
MAC Address	System data.	Displays MAC Address of VAP.
Action	Button	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.

Table 10 – Wi-Fi Virtual AP List

Wi-Fi Uplink Status

The Wi-Fi Uplink Status shows all information of connected Wi-Fi uplink network.



WiFi Module One Uplink Status

SSID	BSSID	Channel	Security	RSSI0	RSSI1	Rate	Action
xxXxxX_5G	28:6C:07:5F:1A:F1	149	WPA2-PSK(AES)	-77	-77	130	Edit

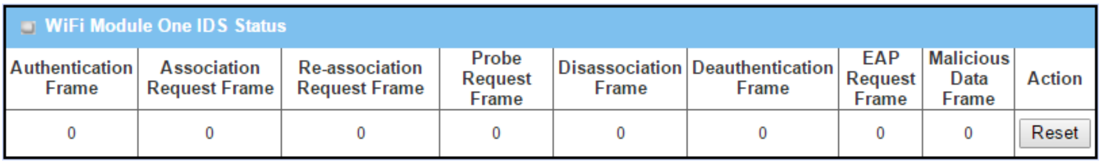
Figure 18 – Wi-Fi Uplink Status

Item	Value setting	Description
SSID	System data.	Displays the network ID of VAP.
BSSID	System data.	Displays the BSSID for the connected wireless network.
Channel	System data.	Displays the wireless channel used.
Security	System data.	Displays the authentication and encryption setting for the Wi-Fi uplink connection.
RSSI0, RSSI1	System data.	Displays the Rx sensitivity on each radio path..
Rate	System data.	Displays the link rate for the Wi-Fi uplink connection.
Action	Button	Click the **Edit** button to make a quick access to the Wi-Fi uplink configuration page. (**Basic Network > WAN & Uplink > Internet Setup** tab)

Table 11 – Wi-Fi Uplink Status

Wi-Fi 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

Figure 19 – Wi-Fi IDS Status

Item	Value setting	Description
Authentication Frame	System data.	Displays the receiving Authentication Frame count.
Association Request Frame	System data.	Displays the receiving Association Request Frame count.
Re-association Request Frame	System data.	Displays the receiving Re-association Request Frame count.
Probe Request Frame	System data.	Displays the receiving Probe Request Frame count.
Disassociation Frame	System data.	Displays the receiving Disassociation Frame count.
Deauthentication Frame	System data.	Displays the receiving Deauthentication Frame count.
EAP Request Frame	System data.	Displays the receiving EAP Request Frame count.
Malicious Data Frame	System data.	Displays the number of receiving unauthorized wireless packets.
Action	Button	Click the **Reset** button to clear the entire statistic and reset counter to 0.

Table 12 – Wi-Fi IDS Status

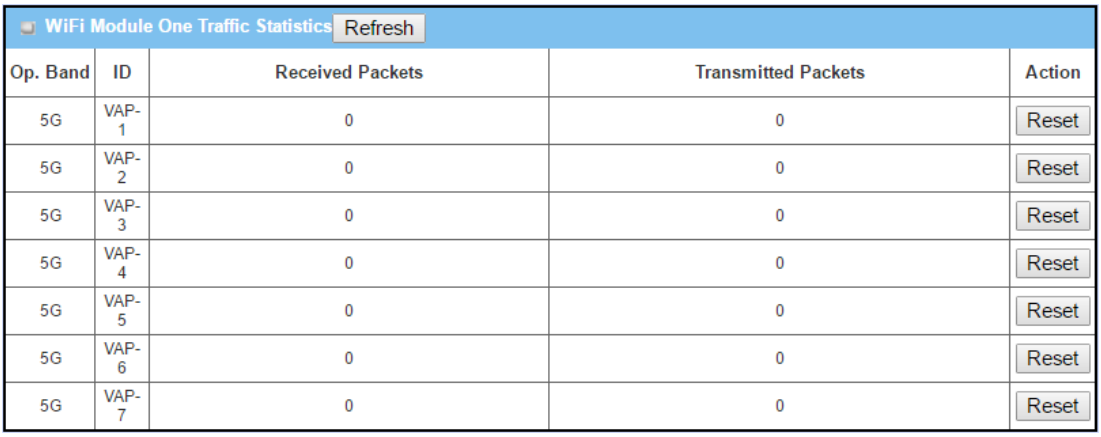
Ensure WIDS function is enabled

Go to **Basic Network** > **Wi-Fi** > **Advanced Configuration tab**

Note that the WIDS of **2.4G** or **5G** should be configured **separately**.

Wi-Fi Traffic Statistic

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



WiFi Module One Traffic Statistics Refresh

Op. Band	ID	Received Packets	Transmitted Packets	Action
5G	VAP-1	0	0	Reset
5G	VAP-2	0	0	Reset
5G	VAP-3	0	0	Reset
5G	VAP-4	0	0	Reset
5G	VAP-5	0	0	Reset
5G	VAP-6	0	0	Reset
5G	VAP-7	0	0	Reset

Figure 20 – Wi-Fi Traffic Statistic

Item	Value setting	Description
Op. Band	System data.	Displays the Wi-Fi Operation Band (**2.4G** or **5G**) of VAP.

Item	Value setting	Description
ID	System data.	Displays the VAP ID.
Received Packets	System data.	Displays the number of received packets.
Transmitted Packet	System data.	Displays the number of transmitted packets.
Action	Button	Click the **Reset** button to clear individual VAP statistics.
Refresh Button	Button	Click the **Refresh** button to update the entire VAP Traffic Statistic instantly.

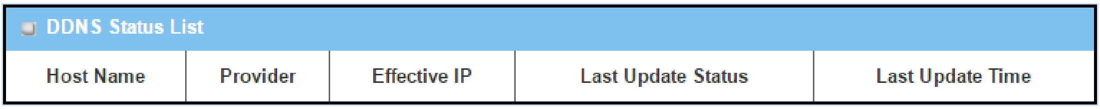
Table 13 – Wi-Fi Traffic Statistic

2.2.4 DDNS Status

Navigate to the **Status > Basic Network > DDNS** tab.

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.

DDNS Status



DDNS Status List

Host Name	Provider	Effective IP	Last Update Status	Last Update Time

Figure 21 – DDNS Status

Item	Value Setting	Description
Host Name	System data.	Displays the name you entered to identify DDNS service provider
Provider	System data.	Displays the DDNS server of DDNS service provider
Effective IP	System data.	Displays the public IP address of the device updated to the DDNS server
Last Update Status	System data.	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	System data.	Displays time stamp of the last update of public IP address to the DDNS server.
Refresh	Button	The **refresh** button allows user to force the display to refresh information.

Table 14 – DDNS Status

2.3 Security

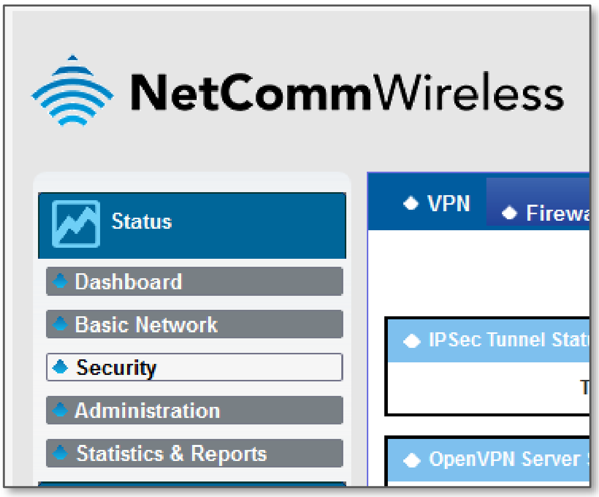


Figure 22 – Security menu item

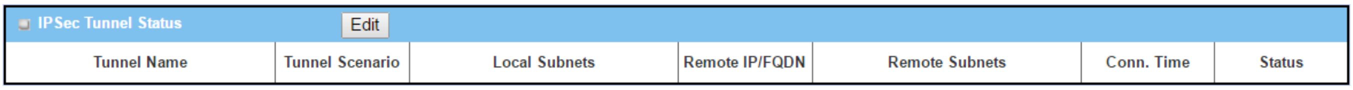
2.3.1 VPN Status

Navigate to the **Status > Security > VPN** tab.

The **VPN Status** widow shows the overall VPN tunnel status.

IPSec Tunnel Status

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



Tunnel Name	Tunnel Scenario	Local Subnets	Remote IP/FQDN	Remote Subnets	Conn. Time	Status

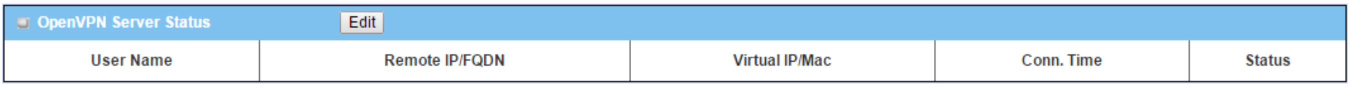
Figure 23 – IPSec Tunnel Status

Item	Value setting	Description
Tunnel Name	System data.	Displays the tunnel name you have entered to identify.
Tunnel Scenario	System data.	Displays the Tunnel Scenario specified.
Local Subnets	System data.	Displays the Local Subnets specified.
Remote IP/FQDN	System data.	Displays the Remote IP/FQDN specified.
Remote Subnets	System data.	Displays the Remote Subnets specified.
Conn. Time	System data.	Displays the connection time for the IPSec tunnel.
Status	System data.	Displays the Status of the VPN connection: **Connected**, **Disconnected**, **Wait for traffic**, or **Connecting**
Edit Button	Button	Click on **Edit** Button to change IPSec setting, the web-based utility will take you to the IPSec configuration page. (**Security > VPN > IPSec** tab)

Table 15 – IPSec Tunnel Status

OpenVPN Server Status

According to OpenVPN configuration, the **OpenVPN Server/Client Status** shows the status and statistics for the OpenVPN connection from the server side or client side.



OpenVPN Server Status Edit

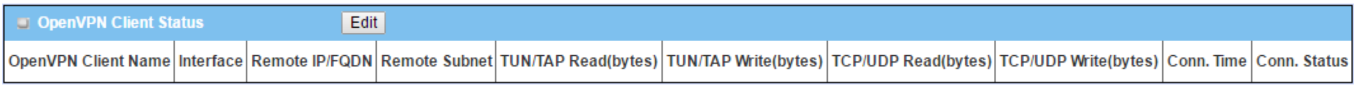
User Name	Remote IP/FQDN	Virtual IP/Mac	Conn. Time	Status

Figure 24 – OpenVPN Server Status

Item	Value setting	Description
User Name	System data.	Displays the Client name you have entered for identification.
Remote IP/FQDN	System data.	Displays the public IP address (the WAN IP address) of the connected OpenVPN Client
Virtual IP/MAC	System data.	Displays the virtual IP/MAC address assigned to the connected OpenVPN client.
Conn. Time	System data.	Displays the connection time for the corresponding OpenVPN tunnel.
Status	System data.	Displays the connection status of the corresponding OpenVPN tunnel. The status can be Connected, or Disconnected.

Table 16 – OpenVPN Server Status

OpenVPN Client Status



OpenVPN Client Status Edit

OpenVPN Client Name	Interface	Remote IP/FQDN	Remote Subnet	TUN/TAP Read(bytes)	TUN/TAP Write(bytes)	TCP/UDP Read(bytes)	TCP/UDP Write(bytes)	Conn. Time	Conn. Status

Figure 25 – OpenVPN Client Status

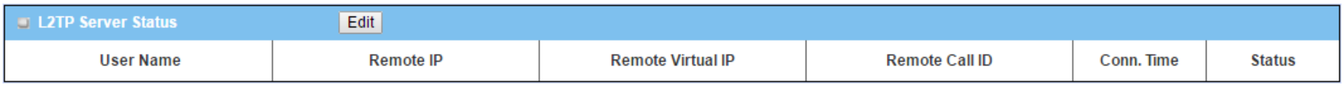
Item	Value setting	Description
OpenVPN Client Name	System data.	Displays the Client name you have entered for identification.
Interface	System data.	Displays the WAN interface specified for the OpenVPN client connection.
Remote IP/FQDN	System data.	Displays the peer OpenVPN Server's Public IP address (the WAN IP address) or FQDN.
Remote Subnet	System data.	Displays the Remote Subnet specified.
TUN/TAP Read(bytes)	System data.	Displays the TUN/TAP Read Bytes of OpenVPN Client.
TUN/TAP Write(bytes)	System data.	Displays the TUN/TAP Write Bytes of OpenVPN Client.
TCP/UDP Read(bytes)	System data.	Displays the TCP/UDP Read Bytes of OpenVPN Client.

Item	Value setting	Description
TCP/UDP Write(bytes)	System data.	Displays the TCP/UDP Write Bytes of OpenVPN Client. Connection
Conn. Time	System data.	Displays the connection time for the corresponding OpenVPN tunnel.
Conn. Status	System data.	Displays the connection status of the corresponding OpenVPN tunnel. The status can be Connected, or Disconnected.

Table 17 – OpenVPN Client Status

L2TP Server/Client Status

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



L2TP Server Status

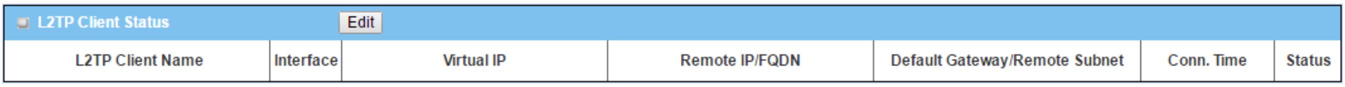
Edit

User Name	Remote IP	Remote Virtual IP	Remote Call ID	Conn. Time	Status

Figure 26 – L2TP Server Status

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

Table 18 – L2TP Server Status



L2TP Client Status

Edit

L2TP Client Name	Interface	Virtual IP	Remote IP/FQDN	Default Gateway/Remote Subnet	Conn. Time	Status

Figure 27 – L2TP Client Status

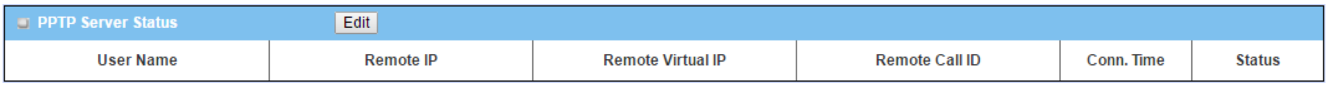
Item	Value setting	Description
Client Name	System data.	Displays Name for the L2TP Client specified.
Interface	System data.	Displays the WAN interface with which the gateway will use to request PPTP tunnelling connection to the PPTP server.
Virtual IP	System data.	Displays the IP address assigned by Virtual IP server of L2TP server.

Item	Value setting	Description
Remote IP/FQDN	System data.	Displays the L2TP Server's Public IP address (the WAN IP address) or FQDN.
Default Gateway/Remote Subnet	System data.	Displays the specified IP address of the gateway device used to connect to the internet to connect to the L2TP server –the default gateway. Or other specified subnet if the default gateway is not used to connect to the L2TP server –the remote subnet.
Conn. Time	System data.	Displays the connection time for the L2TP tunnel.
Status	System data.	Displays the Status of the VPN connection. The status displays Connected, Disconnect, and Connecting.
Edit	Button	Click on **Edit** Button to change L2TP client setting, web-based utility will take you to the L2TP client page. (**Security > VPN > L2TP** tab)

Table 19 – L2TP Client Status

PPTP Server/Client Status

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



PPTP Server Status

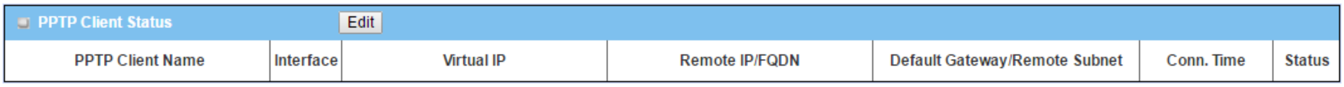
Edit

User Name	Remote IP	Remote Virtual IP	Remote Call ID	Conn. Time	Status

Figure 28 – PPTP Server Status

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

Table 20 – PPTP Server Status



PPTP Client Status

Edit

PPTP Client Name	Interface	Virtual IP	Remote IP/FQDN	Default Gateway/Remote Subnet	Conn. Time	Status

Figure 29 – PPTP Client Status

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

Table 21 – PPTP Client Status

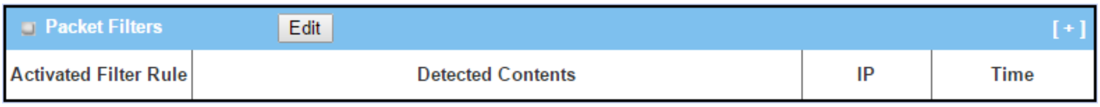
2.3.2 Firewall Status

Navigate to the **Status > Security > Firewall Status** Tab.

The **Firewall Status** provides user a quick view of the firewall status and current firewall settings. It also keeps the log history of the dropped packets by the firewall rule policies, and includes the administrator remote login settings specified in the Firewall Options.

By clicking the icon [+], the status table will be expanded to display log history. Clicking the **Edit** button displays the configuration page.

Packet Filter Status



Packet Filters	Edit		[+]
Activated Filter Rule	Detected Contents	IP	Time

Figure 30 – Packet Filter Status

Item	Value setting	Description
Activated Filter Rule	System data.	This is the Packet Filter Rule name.
Detected Contents	System data.	This is the logged packet information, including the source IP, destination IP, protocol, and destination port –the TCP or UDP. String format:

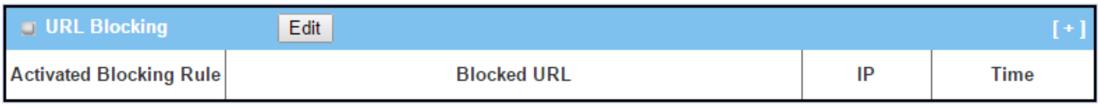
Item	Value setting	Description
		Source IP to Destination IP : Destination Protocol (TCP or UDP)
IP	System data.	The Source IP (IPv4) of the logged packet.
Time	System data.	The Date and Time stamp of the logged packet. Date & time format. ("Month" "Day" "Hours":"Minutes":"Seconds")

Table 22 – Packet Filter Status

Note – Ensure **Packet Filter Log Alert** is enabled.

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

URL Blocking Status



URL Blocking Edit [+]

Activated Blocking Rule	Blocked URL	IP	Time

Figure 31 – URL Blocking Status

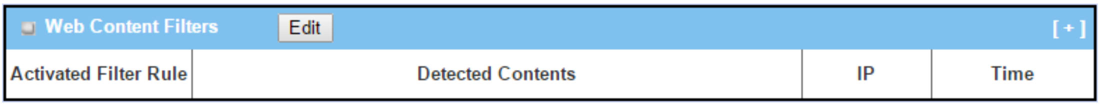
Item	Value setting	Description
Activated Blocking Rule	System data.	This is the URL Blocking Rule name.
Blocked URL	System data.	This is the logged packet information.
IP	System data.	The Source IP (IPv4) of the logged packet.
Time	System data.	The Date and Time stamp of the logged packet. Date & time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

Table 23 – URL Blocking Status

Note – Ensure **URL Blocking Log Alert** is enabled.

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

Web Content Filter Status



Web Content Filters Edit [+]

Activated Filter Rule	Detected Contents	IP	Time

Figure 32 – Web Content Filter Status

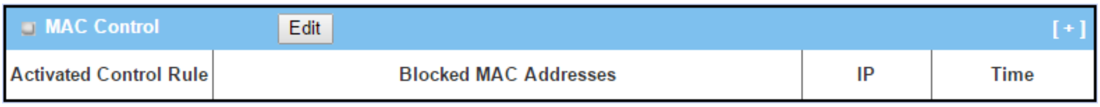
Item	Value setting	Description
Activated Filter Rule	System data.	Logged packet of the rule name. String format.
Detected Contents	System data.	Logged packet of the filter rule. String format.
IP	System data.	Logged packet of the Source IP. IPv4 format.
Time	System data.	Logged packet of the Date Time. Date time format ("Month" "Day" "Hours":"Minutes":"Seconds")

Table 24 – Web Content Filter Status

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

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

MAC Control Status



Activated Control Rule	Blocked MAC Addresses	IP	Time

Figure 33 – MAC Control Status

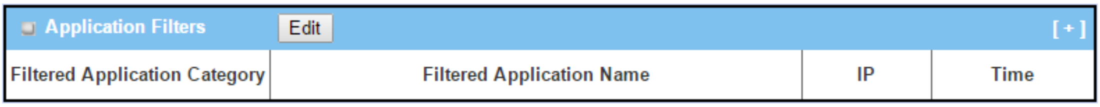
Item	Value setting	Description
Activated Control Rule	System data.	This is the MAC Control Rule name.
Blocked MAC Addresses	System data.	This is the MAC address of the logged packet.
IP	System data.	The Source IP (IPv4) of the logged packet.
Time	System data.	The Date and Time stamp of the logged packet.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

Table 25 – MAC Control Status

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

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

Application Filters Status



Filtered Application Category	Filtered Application Name	IP	Time

Figure 34 – Application Filters Status

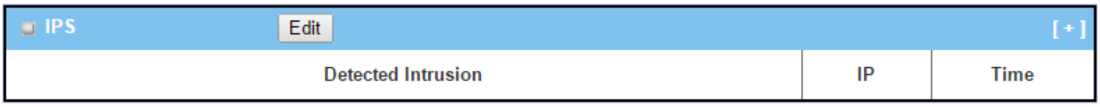
Item	Value setting	Description
Filtered Application Category	System data.	The name of the Application Category being blocked.
Filtered Application Name	System data.	The name of the Application being blocked.
IP	System data.	The Source IP (IPv4) of the logged packet.
Time	System data.	The Date and Time stamp of the logged packet. Date & time format. ("Month" "Day" "Hours":"Minutes":"Seconds")

Table 26 – Application Filters Status

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

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

IPS Status



Detected Intrusion	IP	Time

Figure 35 – IPS Status

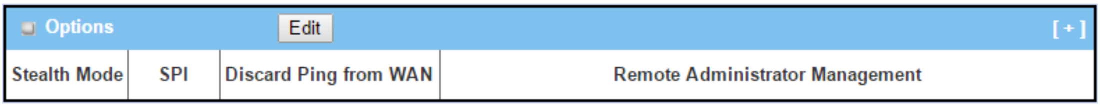
Item	Value setting	Description
Detected Intrusion	System data.	This is the intrusion type of the packets being blocked.
IP	System data.	The Source IP (IPv4) of the logged packet.
Time	System data.	The Date and Time stamp of the logged packet. Date & time format. ("Month" "Day" "Hours":"Minutes":"Seconds")

Table 27 – IPS Status

Note – Ensure **IPS Log Alert** is enabled.

Refer to **Security > Firewall > IPS** tab. Check ☑ **Log Alert** and save the setting.

Firewall Options Status



Stealth Mode	SPI	Discard Ping from WAN	Remote Administrator Management

Figure 36 – Firewall Options Status

Item	Value setting	Description
Stealth Mode	System data.	Enable or Disable setting status of Stealth Mode on Firewall Options. String Format: Disable or Enable
SPI	System data.	Enable or Disable setting status of SPI on Firewall Options. String Format : Disable or Enable
Discard Ping from WAN	System data.	Enable or Disable setting status of Discard Ping from WAN on Firewall Options. String Format: Disable or Enable
Remote Administrator Management	System data.	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

Table 28 – Firewall Options Status

Note – Ensure **Firewall Options Log Alert** is enabled.

Refer to **Security > Firewall > Firewall Options** tab. Check ☑ **Log Alert** and save the setting.

2.4 Administration

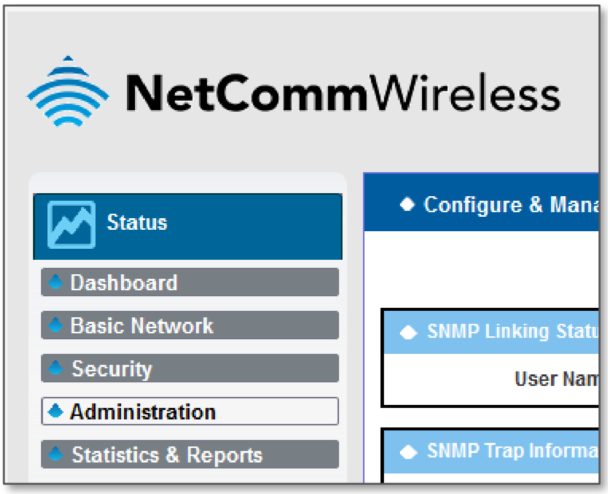


Figure 37 – Status > Administration menu item

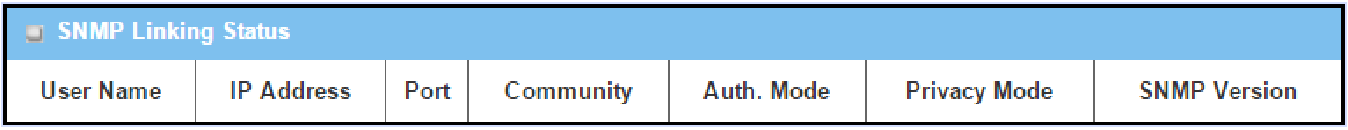
2.4.1 Configure & Manage Status

Navigate to the **Status > Administration > Configure & Manage** tab.

The **Configure & Manage Status** window shows the status for managing remote network devices. The type of management available in your device is depended on the device model purchased. The commonly used ones are the SNMP, TR-069, and UPnP.

SNMP Linking Status

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



SNMP Linking Status

User Name	IP Address	Port	Community	Auth. Mode	Privacy Mode	SNMP Version

Figure 38 – SNMP Linking Status

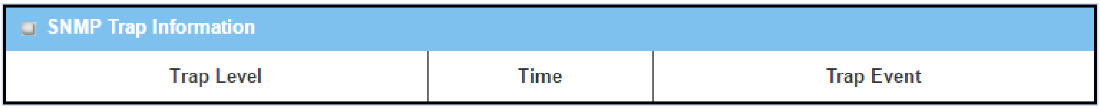
Item	Value setting	Description
User Name	System data.	Displays the user name for authentication. This is only available for SNMP version 3.
IP Address	System data.	Displays the IP address of SNMP manager.
Port	System data.	Displays the port number used to maintain connection with the SNMP manager.
Community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

Item	Value setting	Description
SNMP Version	System data.	Displays the SNMP Version employed.

Table 29 – SNMP Linking Status

SNMP Trap Information

SNMP Trap Information screen shows the status of current received SNMP traps.



SNMP Trap Information

Trap Level	Time	Trap Event

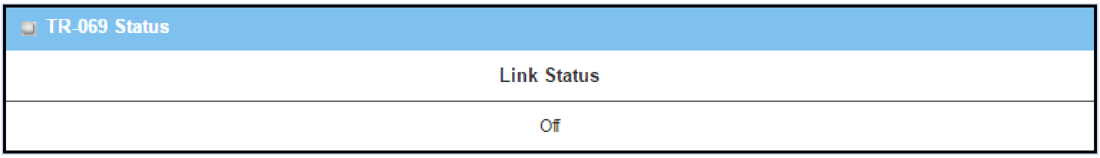
Figure 39 – SNMP Trap Information

Item	Value setting	Description
Trap Level	System data.	Displays the trap level.
Time	System data.	Displays the timestamp of trap event.
Trap Event	System data.	Displays the IP address of the trap sender and event type.

Table 30 – SNMP Trap Information

TR-069 Status

TR-069 Status screen shows the current connection status with the TR-068 server.



TR-069 Status

Link Status
Off

Figure 40 – TR-069 Status

Item	Value setting	Description
Link Status	System data.	Displays the current connection status with the TR-068 server. The connection status is either On when the device is connected with the TR-068 server or Off when disconnected.

Table 31 – TR-069 Status

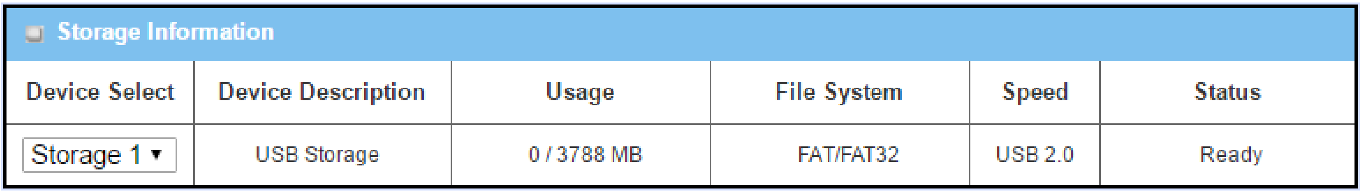
2.4.2 Log Storage Status

Go to **Status > Administration > Log Storage** tab.

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

Log Storage Status

Log Storage Status screen shows the status of current the selected device storage. The status includes Device Select, Device Description, Usage, File System, Speed, and status



Storage Information

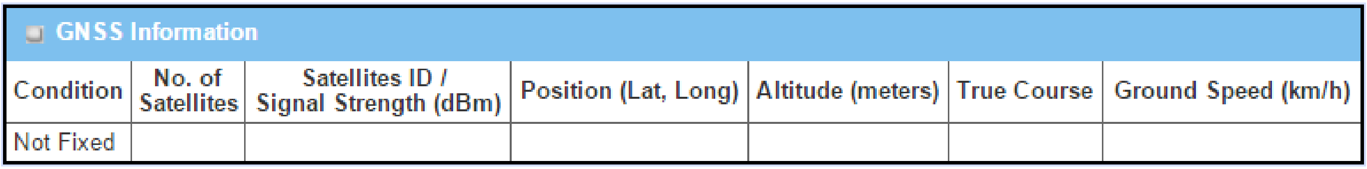
Device Select	Device Description	Usage	File System	Speed	Status
Storage 1 ▼	USB Storage	0 / 3788 MB	FAT/FAT32	USB 2.0	Ready

Figure 41 – Log Storage Status

2.4.3 GNSS Status

Go to **Status > Administration > GNSS** tab.

The **GNSS Information** screen shows the status for current GNSS positioning information for the gateway.



GNSS Information

Condition	No. of Satellites	Satellites ID / Signal Strength (dBm)	Position (Lat, Long)	Altitude (meters)	True Course	Ground Speed (km/h)
Not Fixed						

The available GNSS information includes GNSS Condition, No. of Satellites, Satellites ID / Signal Strength, Position (Lat., Long.), Altitude (meters), True Course, and the equivalent Ground Speed (km/h).

Figure 42 – GNSS Status

2.5 Statistics & Report

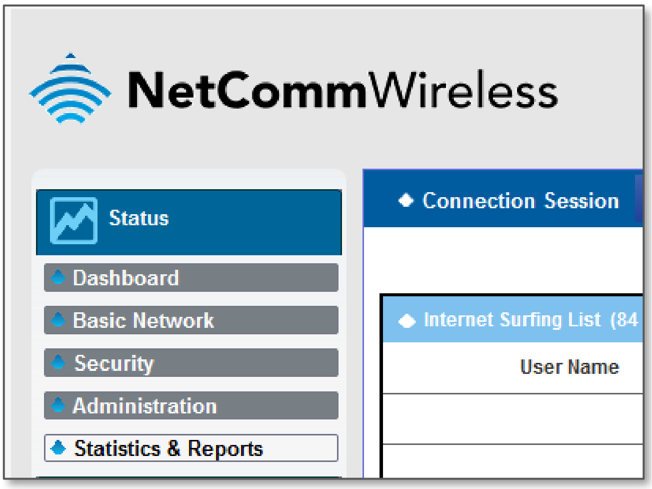
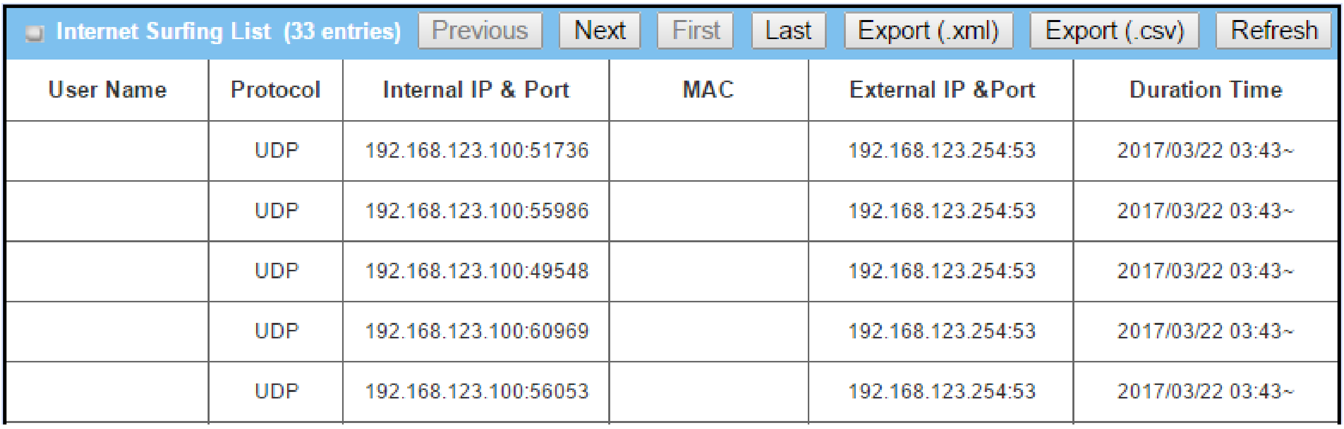


Figure 43 – Status > Statistics & Report menu item

2.5.1 Connection Session

Navigate to the **Status > Statistics & Reports > Connection Session** tab.

Internet Surfing Statistic shows the connection tracks on this router.



User Name	Protocol	Internal IP & Port	MAC	External IP &Port	Duration Time
	UDP	192.168.123.100:51736		192.168.123.254:53	2017/03/22 03:43~
	UDP	192.168.123.100:55986		192.168.123.254:53	2017/03/22 03:43~
	UDP	192.168.123.100:49548		192.168.123.254:53	2017/03/22 03:43~
	UDP	192.168.123.100:60969		192.168.123.254:53	2017/03/22 03:43~
	UDP	192.168.123.100:56053		192.168.123.254:53	2017/03/22 03:43~

Figure 44 – Internet Surfing list

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

Table 32 – Connection Session controls

2.5.2 Network Traffic

Navigate to the **Status > Statistics & Reports > Network Traffic** tab.

Network Traffic Statistics screen shows the historical graph for the selected network interface.

You can change the interface drop list and select the interface you want to monitor.

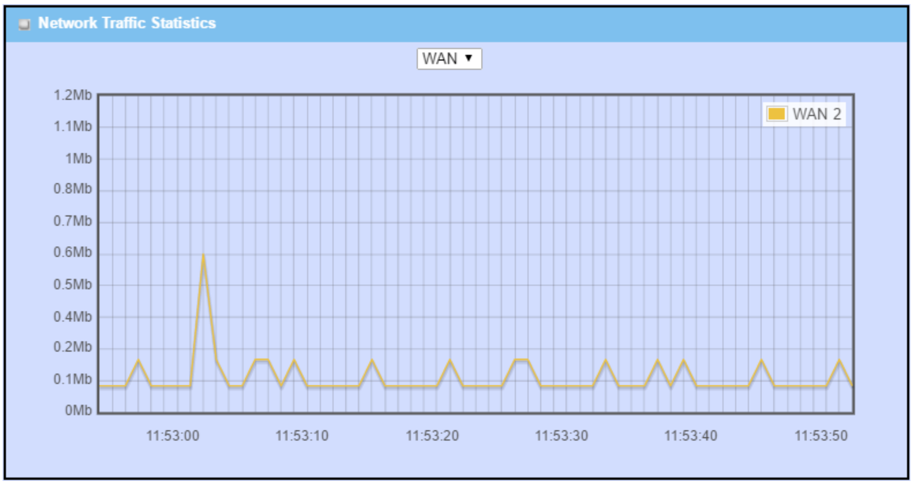
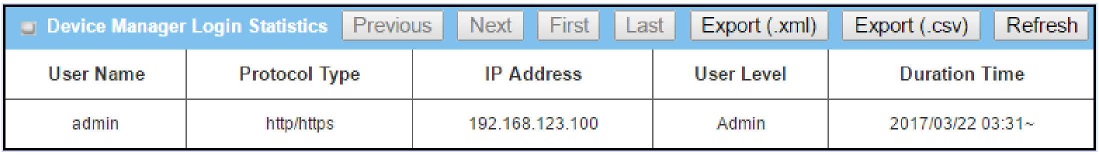


Figure 45 – Network Traffic Statistics

2.5.3 Device Administration

Navigate to the **Status > Statistics & Reports > Device Administration** tab.

Device Administration shows the login information.



User Name	Protocol Type	IP Address	User Level	Duration Time
admin	http/https	192.168.123.100	Admin	2017/03/22 03:31~

Figure 46 – Device Administration list

Item	Value setting	Description
Previous	Button	Click the **Previous** button; you will see the previous page of login statistics.
Next	Button	Click the **Next** button; you will see the next page of login statistics.
First	Button	Click the **First** button; you will see the first page of login statistics.
Last	Button	Click the **Last** button; you will see the last page of login statistics.
Export (.xml)	Button	Click the **Export (.xml)** button to export the login statistics to xml file.
Export (.csv)	Button	Click the **Export (.csv)** button to export the login statistics to csv file.

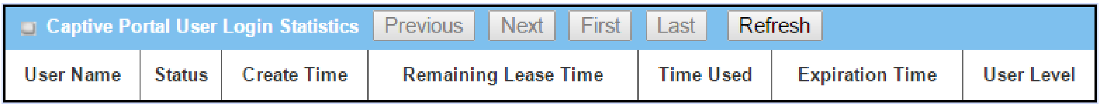
Item	Value setting	Description
Refresh	Button	Click the **Refresh** button to refresh the login statistics.

Table 33 – Device Administration controls

2.5.4 Portal Usage

Navigate to the **Status > Statistics & Reports > Portal Usage** tab.

Portal Usage shows the information about internal Captive Portal user login statistics.



Captive Portal User Login Statistics Previous Next First Last Refresh

User Name	Status	Create Time	Remaining Lease Time	Time Used	Expiration Time	User Level

Figure 47 – Captive Portal User Login Statistics list

Item	Value setting	Description
User Name	System data.	Displays the **User Name** of user account created in **Object Define > User > User Profile**.
Status	System data.	Displays the **Status** of user account about logging captive portal. **Online** for the user logged in to the captive portal; **Offline** for the user already logged out.
Create Time	System data.	Displays the **Create Time** that user account created.
Remaining Lease Time	System data.	Displays the **Remaining Lease Time** of the user account. If the remaining time is zero, the corresponding user account can't be use for login captive portal anymore. If the **Lease Time** of user account is empty, the remaining lease time field is shown empty. It means that the user account can be used all the time.
Time Used	System data.	Displays the **Time Used** since the user login to the captive portal.
Expiration Time	System data.	Displays the **Expiration Time** of the user account. Tell user that what time the user account will be useless. If the **Lease Time** of user account is empty, the expiration time field is also empty. It means that the user account can be used all the time.
User Level	System data.	Displays the **User Level** of the user account. It can be **Admin**, **Staff**, **Guest**, and **Passenger**.
Previous	Button	Click the **Previous** button; you will see the previous page of login statistics.
Next	Button	Click the **Next** button; you will see the next page of login statistics

Item	Value setting	Description
First	Button	Click the **First** button; you will see the first page of login statistics
Last	Button	Click the **Last** button; you will see the last page of login statistics
Refresh	Button	Click the **Refresh** button to refresh the login statistics

Table 34 – Captive Portal User Login Statistics

2.5.5 Cellular Usage

Navigate to the **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.

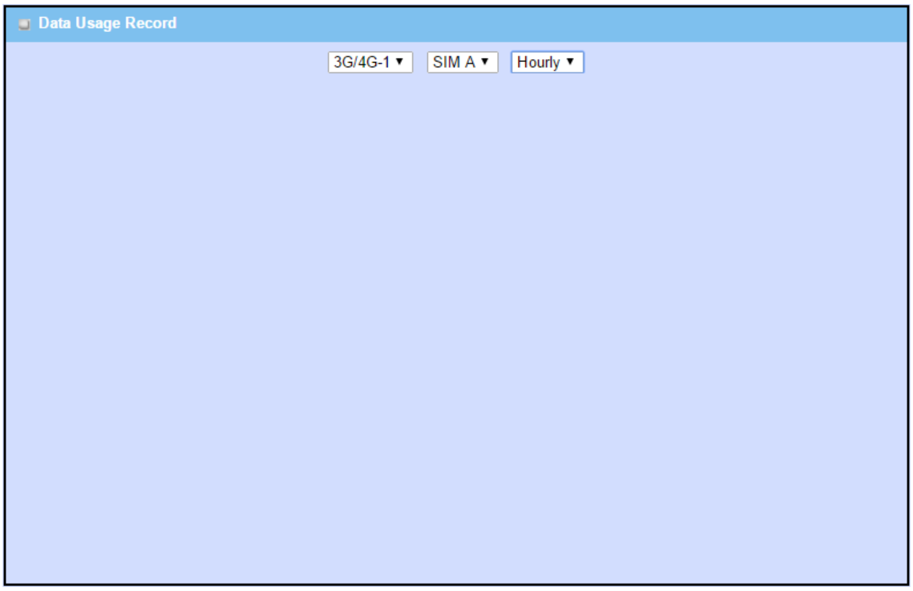


Figure 48 – Data Usage Record

3 Basic Network

3.1 WAN & Uplink

The NTC-400 Series Router provides multiple WAN interfaces to let all client hosts behind the router to access the Internet. The **WAN Connection** lets you specify the **WAN Physical Interface** or **WAN Internet Setup** for computers behind the router to access the Internet. For each WAN interface, you must specify its physical interface first and then its Internet setup to connect to your ISP.

3.1.1 Physical Interface

WAN interfaces can be configured individually to provide the desired internet connection setup. The first step to configuring a WAN interface is to specify the kind of connection medium to be used for the WAN connection, as shown in "Physical Interface" page. On the "Physical Interface" page, there are two configuration windows, "Physical Interface List" and "Interface Configuration". The "Physical Interface List" window shows all the available physical interfaces. After clicking on the "Edit" button for the interface on the "Physical Interface List" window, the "Interface Configuration" window will appear to let you configure a WAN interface.

Physical Interface

- Ethernet WAN: The router has one RJ-45 WAN port that can be configured to be a WAN connection. You can directly connect to an external DSL modem or setup behind a firewall device.
- 3G/4G WAN: The router has one built-in 3G/4G cellular module which operates as a WAN connection. You can insert two SIM cards to use the failover feature.
- Wi-Fi Uplink WAN: One of the Wi-Fi networks can be used as a WAN connection.

Operation Mode

There are three options: **Always on**, **Failover**, and **Disable** for the operation mode setting.

- **Always on**: Set this WAN interface to be active all the time
- **Failover**: A failover interface is a backup connection to the primary. That means only when its primary WAN connection is broken, the backup connection will be started up to substitute the primary connection.

  WAN-2 is a backup for WAN-1. WAN-1 serves as the primary connection with operation mode "Always on". WAN-2 won’t be activated until WAN-1 disconnected. When WAN-1 connection is recovered back with a connection, it will take over data traffic again. At that time, WAN-2 connection will be terminated.

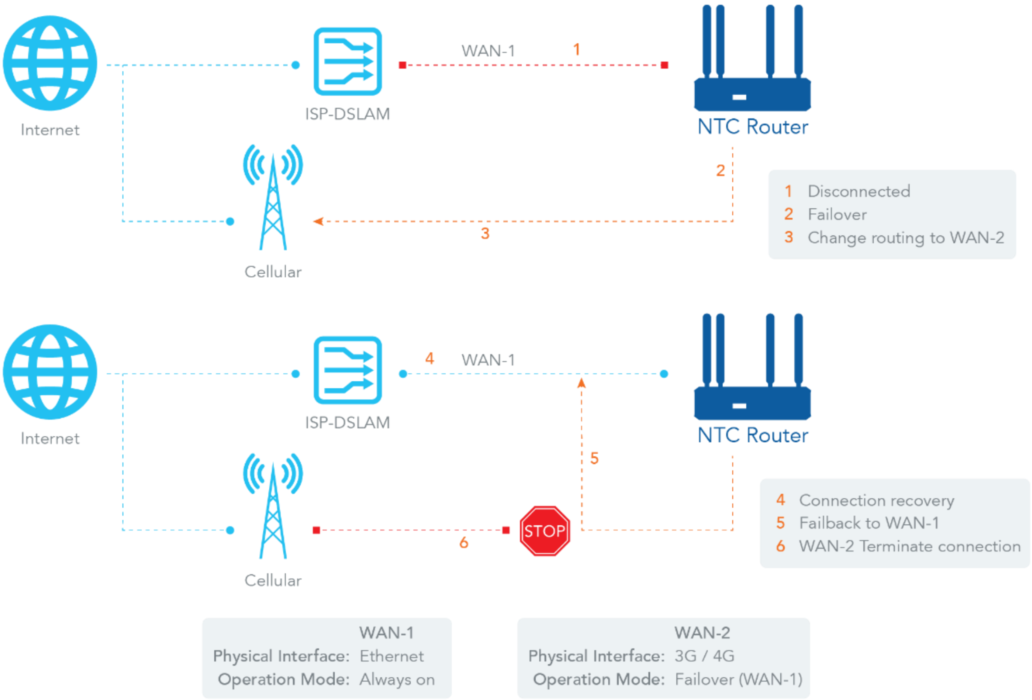

Internet
ISP-DSLAM
WAN-1
1
NTC Router
2
Cellular
3
1 Disconnected
2 Failover
3 Change routing to WAN-2
Internet
ISP-DSLAM
4
WAN-1
NTC Router
5
Cellular
6
STOP
4 Connection recovery
5 Failback to WAN-1
6 WAN-2 Terminate connection
WAN-1
Physical Interface: Ethernet
Operation Mode: Always on
WAN-2
Physical Interface: 3G / 4G
Operation Mode: Failover (WAN-1)

Figure 49 – Failover diagram

- **Seamless Failover** – In addition, there is a "Seamless" option for Failover operation mode. When seamless option is activated by checking on the "Seamless" box in configuration window, both the primary connection and the failover connection are started up after the system reboots. Only the primary connection executes the data transfer, while the failover connection just keeps the connection alive. As soon as the primary connection is broken, the system will switch (failover) the routing path to the failover connection to save the dial up time of the failover connection since it is kept alive.

  When the “Seamless” enable checkbox is activated, it allows the Failover interface to be connected continuously from system boot up. The failover WAN interface stays connected without data traffic. The purpose is to shorten the switch time during the failover process. So, when the primary connection is disconnected, the failover interface takes over the data transfer instantly by only changing the routing path to the failover interface. The time to connect to the failover connection has been saved since it was already connected.

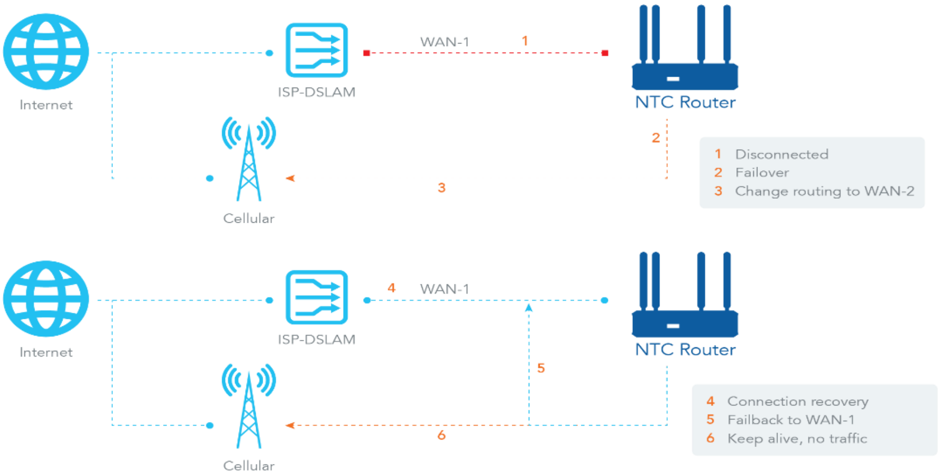


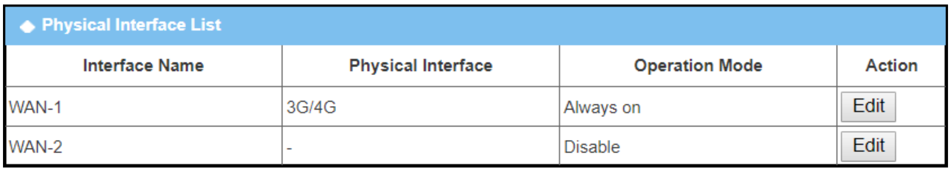
Figure 50 – Seamless Failover diagram

VLAN Tagging

Sometimes ISPs require a VLAN tag to be inserted into the WAN packets from the router for specific services. To enable these services, enable VLAN tagging and specify the tag on the WAN physical interface. Note that only Ethernet and ADSL physical interfaces support the feature.

3.1.1.1 Configuring a physical interface

Click on the **Edit** button for the WAN interface that you wish to configure.

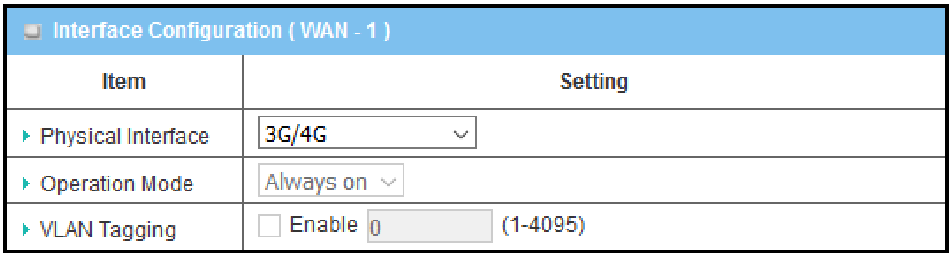


Physical Interface List

Interface Name	Physical Interface	Operation Mode	Action
WAN-1	3G/4G	Always on	Edit
WAN-2	-	Disable	Edit

Figure 51 – Physical Interface List

The Interface Configuration screen appears.



Interface Configuration (WAN - 1)

Item	Setting
Physical Interface	3G/4G
Operation Mode	Always on
VLAN Tagging	□ Enable 0 (1-4095)

Figure 52 – Interface Configuration

Item	Notes	Description
Physical Interface	Mandatory field. WAN-1 is the primary interface is factory set to Always On.	Select an interface from the available interface dropdown list.
Operation Mode	Mandatory field.	Select **Always on** to make this WAN always active. Select Disable to disable this WAN interface. Select **Failover** to make this WAN a Failover WAN when the primary or the secondary WAN link fails, then select the primary or the existing secondary WAN interface to switch Failover from. **Note** – For WAN-1 the only available option is: **Always on**
VLAN Tagging	Optional setting.	Check ☑ **Enable** to enter tag values provided by your ISP. Otherwise uncheck the box. Value Range: 1 - 4096. **Note** – This feature is NOT available for 3G/4G WAN connection.

Table 35 – Interface Configuration screen

3.1.2 Internet Setup

After specifying the physical interface for each WAN connection, you must configure at least one connection profile to satisfy the connection process of the SIP/mobile carrier, so that all client hosts on the Intranet of the router can access the Internet. On the "Internet Setup" page, there are three configuration windows: "Internet Connection List", "Internet Connection

Configuration", "WAN Type Configuration" and related configuration windows for each WAN type. For the Internet setup of each WAN interface, you must specify its WAN type of physical interface first and then its related parameter configuration for that WAN type. After clicking on the "Edit" button of a physical interface on the "Internet Setup List" window, the "Internet Connection Configuration" window appears to let you specify the kind of WAN type that you will use for that physical interface to make an Internet connection. Based on your chosen WAN type, you can configure necessary parameters in each corresponding configuration window.

WAN Type for Ethernet Interface

Ethernet is a common WAN and uplink interface for M2M routers. Often an xDSL or cable modem is used to provide an Internet connection. There are various WAN types that can be used to make a connection with your ISP.

- Static IP: Select this option if your ISP provides a fixed IP to you when you subscribe to the service.
- Dynamic IP: The IP address for the WAN is assigned by a DHCP server each time a connection is made.
- PPP over Ethernet: Also known as PPPoE. This WAN type is widely used for ADSL connections. The IP is usually different for every connection instance.
- PPTP: This WAN type is popular in some countries, like Russia.
- L2TP: This WAN type is popular in some countries, like Israel.

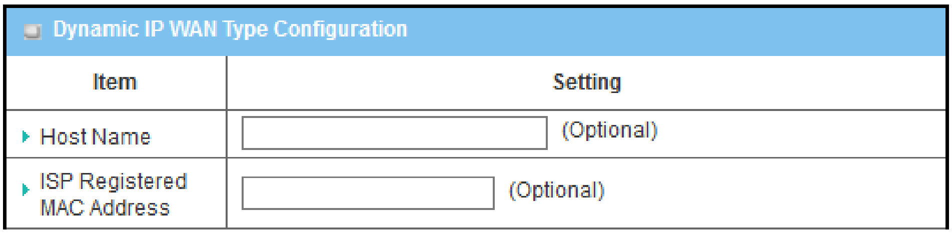
Configure Ethernet WAN Setting

When the Edit button is applied, the Internet Connection Configuration screen appears. WAN-1 interface is used in this example.

3.1.2.1 WAN Type

Dynamic IP

When WAN Type is set to Dynamic IP, the following options are displayed:



Dynamic IP WAN Type Configuration

Item	Setting
Host Name	(Optional)
ISP Registered MAC Address	(Optional)

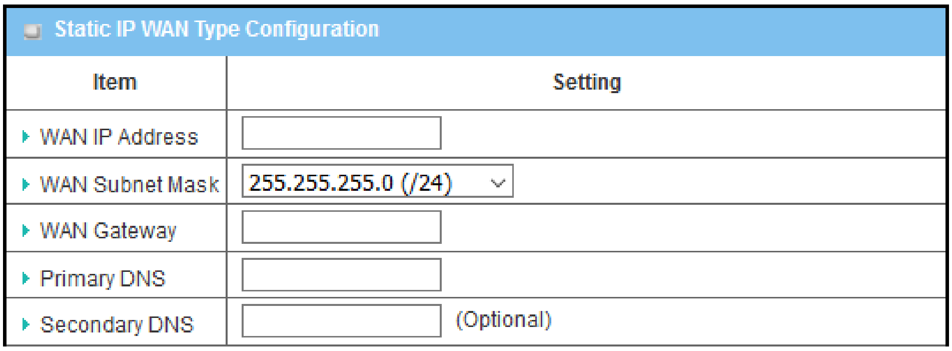
Figure 53 – Dynamic IP WAN Type Configuration

Item	Notes	Description
Host Name	Optional setting.	Enter the host name provided by your Service Provider.
ISP Registered MAC Address	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.

Table 36 – Dynamic IP WAN Type Configuration

Static IP

When WAN Type is set to Static IP, the following options are displayed:



Static IP WAN Type Configuration

Item	Setting
WAN IP Address	
WAN Subnet Mask	255.255.255.0 (/24)
WAN Gateway	
Primary DNS	
Secondary DNS	(Optional)

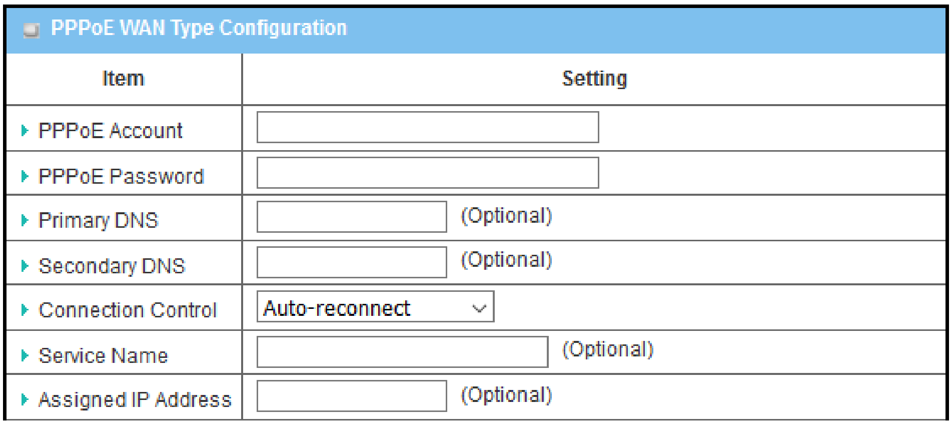
Figure 54 – Static IP WAN Type Configuration

Item	Notes	Description
WAN IP Address	Mandatory field.	Enter the WAN IP address given by your Service Provider
WAN Subnet Mask	Mandatory field.	Enter the WAN subnet mask given by your Service Provider
WAN Gateway	Mandatory field.	Enter the WAN gateway IP address given by your Service Provider
Primary DNS	Mandatory field.	Enter the primary WAN DNS IP address given by your Service Provider
Secondary DNS	Optional setting	Enter the secondary WAN DNS IP address given by your Service Provider

Table 37 – Static IP WAN Type Configuration

PPPoE

When WAN Type is set to PPPoE, the following options are displayed:



PPPoE WAN Type Configuration

Item	Setting
PPPoE Account	
PPPoE Password	
Primary DNS	(Optional)
Secondary DNS	(Optional)
Connection Control	Auto-reconnect
Service Name	(Optional)
Assigned IP Address	(Optional)

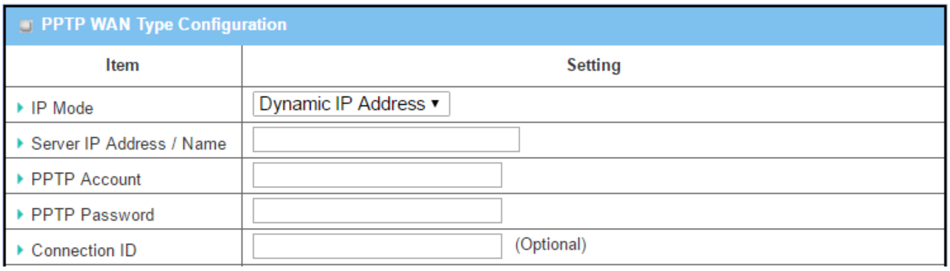
Figure 55 – PPPoE WAN Type Configuration

Item	Notes	Description
PPPoE Account	Mandatory field.	Enter the PPPoE User Name provided by your Service Provider.
PPPoE Password	Mandatory field.	Enter the PPPoE password provided by your Service Provider.
Primary DNS	Optional setting.	Enter the IP address of Primary DNS server.
Secondary DNS	Optional setting.	Enter the IP address of Secondary DNS server.
Service Name	Optional setting.	Enter the service name if your ISP requires it
Assigned IP Address	Optional setting.	Enter the IP address assigned by your Service Provider.

Table 38 – PPPoE WAN Type Configuration

PPTP

When WAN Type is set to PPTP, the following options are displayed:



PPTP WAN Type Configuration

Item	Setting
IP Mode	Dynamic IP Address ▾
Server IP Address / Name	
PPTP Account	
PPTP Password	
Connection ID	(Optional)

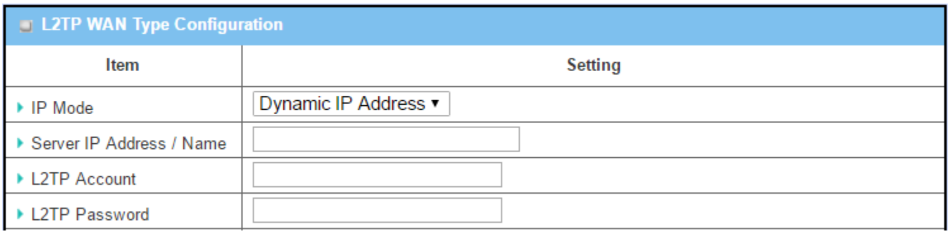
Figure 56 – PPTP WAN Type Configuration

Item	Notes	Description
IP Mode	Mandatory field.	Select either Static or Dynamic IP address for PPTP Internet connection. - When Static IP Address is selected, you will need to enter the WAN IP Address, WAN Subnet Mask, and WAN Gateway. - WAN IP Address (mandatory field) – Enter the WAN IP address given by your Service Provider. - WAN Subnet Mask (mandatory field) – Enter the WAN subnet mask given by your Service Provider. - WAN Gateway (mandatory field) – Enter the WAN gateway IP address given by your Service Provider. - 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 Service Provider.
Connection ID	Optional setting	Enter a name to identify the PPTP connection.
MPPE	Optional setting	Select Enable to enable MPPE (Microsoft Point-to-Point Encryption) security for PPTP connection.

Table 39 – PPTP WAN Type Configuration

L2TP

When WAN Type is set to L2TP, the following options are displayed:



L2TP WAN Type Configuration

Item	Setting
IP Mode	Dynamic IP Address ▾
Server IP Address / Name	
L2TP Account	
L2TP Password	

Figure 57 – L2TP WAN Type Configuration

Item	Notes	Description
IP Mode	Mandatory field.	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 Gateway. - **WAN IP Address** (mandatory field) – Enter the WAN IP address given by your Service Provider. - **WAN Subnet Mask** (mandatory field) – Enter the WAN subnet mask given by your Service Provider. - **WAN Gateway** (mandatory field) – Enter the WAN gateway IP address given by your Service Provider. When Dynamic IP is selected, there are no above settings required.
Server IP Address/Name	Mandatory field.	Enter the L2TP server name or IP Address.
L2TP Account	Mandatory field.	Enter the L2TP username provided by your Service Provider.
L2TP Password	Mandatory field.	Enter the L2TP connection password provided by your Service Provider.
Service Port	Mandatory field.	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	Optional setting	Select ☑ **Enable** to enable MPPE (Microsoft Point-to-Point Encryption) security for PPTP connection.

Table 40 – L2TP WAN Type Configuration

3.1.2.2 Ethernet Connection Common Configuration

There are some important parameters to be configured, regardless of the selected WAN type.

3.1.2.3 Connection Control

Auto-reconnect – The router will establish an Internet connection automatically when it has booted up and try to reconnect when the connection is down. We recommend that you choose this scheme for mission critical applications to ensure the Internet connection is always on.

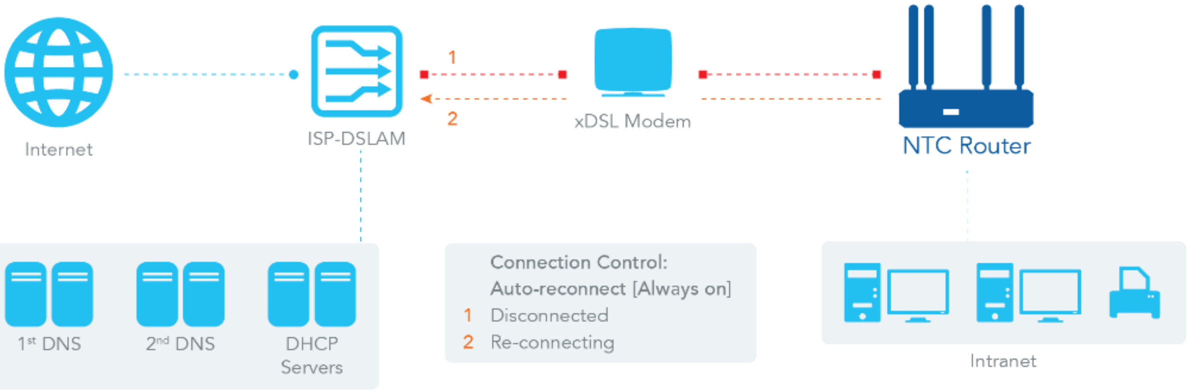


Figure 58 – Connection Control - Auto-reconnect

Connect-on-demand – The router won't start to establish an Internet connection until local data is sent to the WAN side. After normal data transferring between LAN and WAN sides, the router will disconnect the WAN connection if idle time reaches the Maximum Idle Time value.

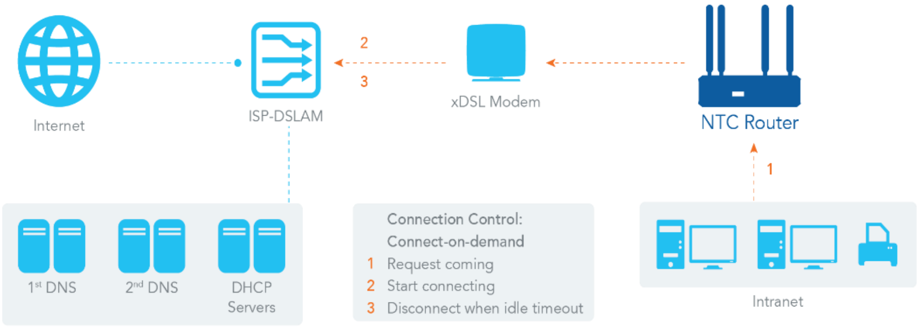


Figure 59 – Connection Control - Connect-on-demand

Manually – The router won't start to establish a WAN connection until you press the "Connect" button on the web UI. After normal data transferring between the LAN and WAN sides, the router will disconnect the WAN connection if idle time reaches value of Maximum Idle Time.

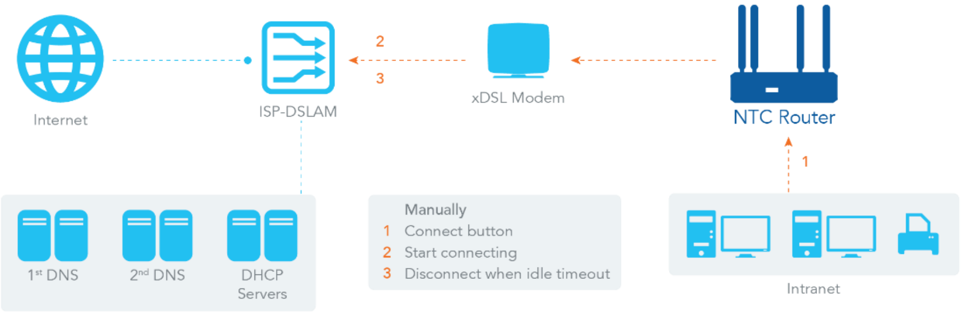


Figure 60 – Connection Control - Manually

Note – If the WAN interface serves as the primary interface for another WAN interface as a **Failover**, the **Connection Control** parameter will not be available to you to configure as the system must set it to “**Auto-reconnect (Always on)**”.

3.1.2.4 Network Monitoring

"ICMP Check" and "FQDN Query" are used to check the network status. When there is traffic on a connection, the checking packet consumes bandwidth. The response time of reply packets may also increase. Enabling "Checking Loading" option will stop the connection check when there is traffic on the internet. The router will then wait for another "Check Interval" and then continue checking the interface again.

When the Network Monitoring function is enabled and the reply time is longer than Latency or if no response is received before the Checking Timeout period, the "Fail" count register will be increased. If there are repeated failures and the Fail count exceeds the Fail Threshold, the router performs the exception handling process and re-initializes the connection. If there are no repeated failures, the network monitoring process will be start again.

Set up “Ethernet Common Configuration”

Item	Notes	Description
Connection Control	Mandatory field.	There are three connection modes. - Auto-reconnect (Always on) enables the router to always keep the Internet connection on. - Connect-on-demand enables the router to 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	Mandatory field. Default setting: **Auto (value zero)** 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 best Internet connection performance.
NAT	Optional field. Default setting: **NAT**	Enable NAT to apply NAT on the WAN connection. Uncheck the box to disable NAT function.
Network Monitoring	Optional field. Enabled by default.	When the Network Monitoring feature is enabled, the gateway will use DNS Query or ICMP to periodically check Internet connection –connected or disconnected. - Choose either DNS Query or ICMP Checking to detect WAN link. With DNS Query, the system checks the connection by sending DNS Query packets to the destination specified in Target 1 and Target 2. With ICMP Checking, the system will check connection by sending ICMP request packets to the destination specified in Target 1 and Target 2. - Loading Check Enable Loading Check allows the router to ignore unreturned DNS Queries or ICMP requests when WAN bandwidth is fully occupied. This is to prevent false link-down status. - Check Interval defines the transmitting interval between two DNS Query or ICMP checking packets. - Check Timeout defines the timeout of each DNS query/ICMP. - Latency Threshold defines the tolerance threshold of responding time. - Fail Threshold specifies the detected disconnection before the router recognize the WAN link down status. Enter a number of detecting disconnection times to be the threshold before disconnection is acknowledged. - Target1 (DNS1 set by default) specifies the first target of sending DNS query/ICMP request.

Item	Notes	Description
		- DNS1: set the primary DNS to be the target. - DNS2: set the secondary DNS to be the target. - Gateway: set the Current gateway to be the target. - Other Host: enter an IP address to be the target. - Target2 (None set by default) specifies the second target of sending 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. - Gateway: set the Current gateway to be the target. - Other Host: enter an IP address to be the target.
IGMP	Mandatory field. Disabled by default.	Enable IGMP (Internet Group Management Protocol) would enable the router to listen to IGMP packets to discover which interfaces are connected to which device. The router 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	Optional field. Disabled by default.	Enable WAN IP Alias then enter the IP address provided by your service provider. WAN IP Alias is used by the device router and is treated as a second set of WAN IP to provide dual WAN IP address to your LAN network.
Save	Button	Click **Save** to save the settings.
Undo	Button	Click **Undo** to cancel the settings.

Table 41 – Ethernet Common Configuration

3.1.2.5 Preferred SIM Card – Dual SIM Fail Over

With a single module, the router can create only one cellular WAN interface at any time. However, the NTC-400 Series Router accepts two SIM cards and allows you to switch between them so that one SIM card is available at all times as a backup or failover. This feature is called Dual SIM Failover and is useful for switching between ISPs when the router moves to another location where network coverage changes. There are various configurations including "SIM-A First", "SIM-B First“ with “Failback” enabled or disabled, and “SIM-A Only and “SIM-B Only”.

SIM-A/SIM-B only – When “SIM-A Only” or “SIM-B Only” is used, the specified SIM slot card is the only one to be used for negotiation parameters between the router and cellular ISP.

SIM-A / SIM-B first without enable Failback – By default, the router is configured to use “SIM-A First”. When “SIM-A First” or “SIM-B First” are selected, the router will try to connect to the Internet using SIM-A or SIM-B card first and when the connection is broken, the router will switch to use the other SIM card automatically and will not switch back to use the original SIM card except where that connection is broken too. That is, SIM-A and SIM-B are used so long as the connection is still alive.

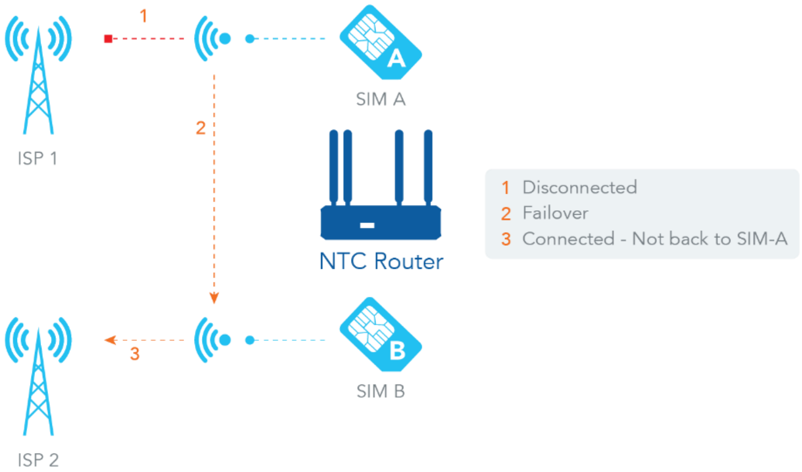


Figure 61 – SIM-A / SIM-B first without enable Failback

SIM-A / SIM-B first with Failback enable – With Failback option enabled, the router fails over when the primary SIM connection fails and fails back when it has recovered.

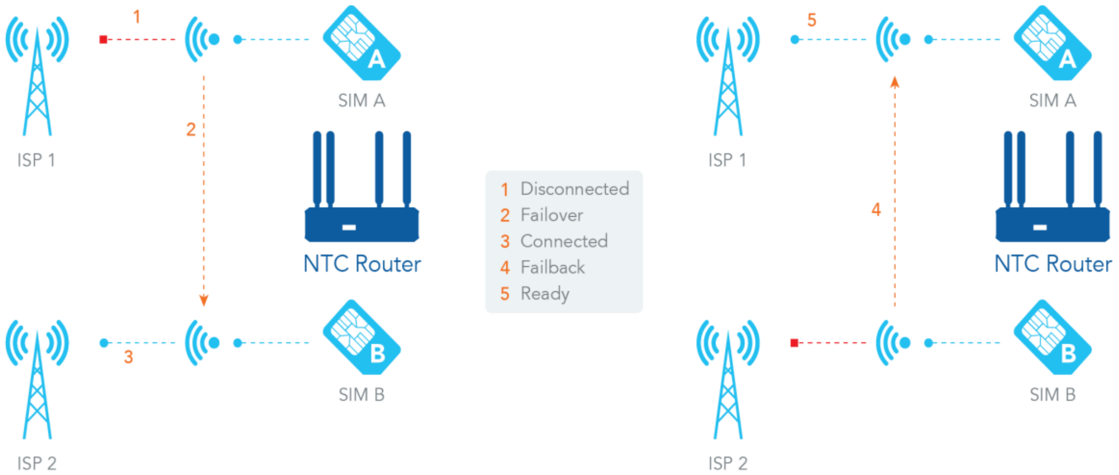
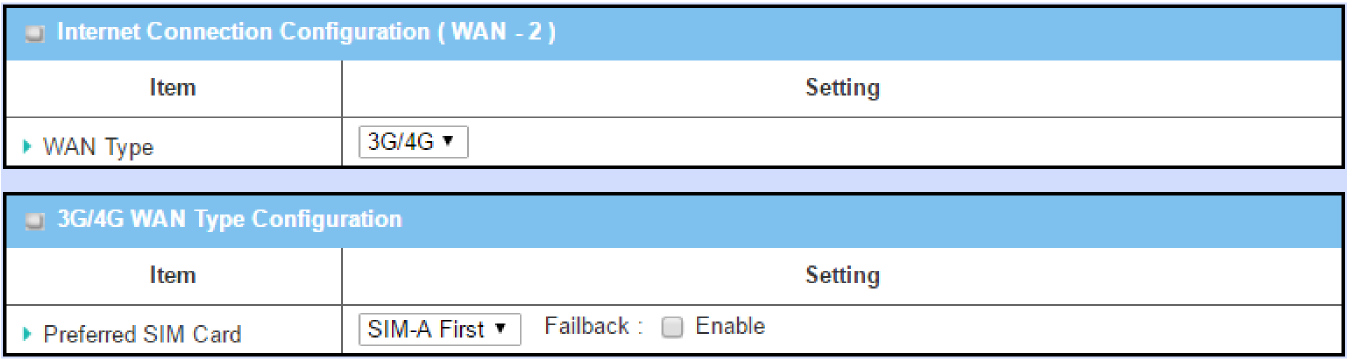


Figure 62 – SIM-A / SIM-B first with enable Failback

3.1.2.6 Configure 3G/4G WAN Setting

When the **Edit** button is clicked, **Internet Connection Configuration**, and **3G/4G WAN Configuration** screens will appear. WAN-2 interface is used in this example.



Internet Connection Configuration (WAN - 2)

Item	Setting
WAN Type	3G/4G ▼

3G/4G WAN Type Configuration

Item	Setting
Preferred SIM Card	SIM-A First ▼ Failback : □ Enable

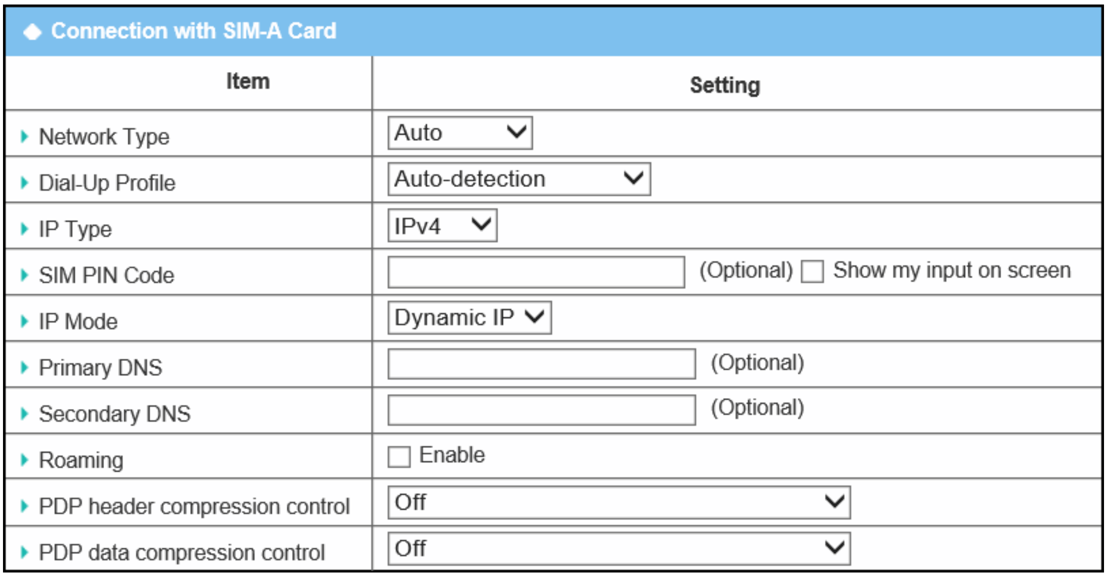
Figure 63 – 3G/4G WAN Type Configuration

Item	Notes	Description
WAN Type	Mandatory field. Default setting: **3G/4G**	From the dropdown box, select the Internet connection method for 3G/4G WAN Connection. Only 3G/4G is available.
Preferred SIM Card	Mandatory field. Default setting: **SIM-A First** 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 established using SIM A or SIM B and if the connection is fails, the router changes to use the other SIM card until the connection is established. When SIM-A only or SIM-B only is selected, the router only attempts a connection using the SIM card you selected. When Failback is checked, it means if the connection is made using the unselected SIM, the router will failback to the main SIM and try to establish the connection periodically. **Note –** Failback is available only when **SIM-A First** or **SIM-B First** is selected.

Table 42 – 3G/4G WAN Type Configuration

3.1.2.7 Configure SIM-A / SIM-B Card

Here you can configure the cellular connection profile.



Connection with SIM-A Card

Item	Setting
Network Type	Auto
Dial-Up Profile	Auto-detection
IP Type	IPv4
SIM PIN Code	(Optional) □ Show my input on screen
IP Mode	Dynamic IP
Primary DNS	(Optional)
Secondary DNS	(Optional)
Roaming	□ Enable
PDP header compression control	Off
PDP data compression control	Off

Figure 64 – Connection with SIM-A Card

Note – The configuration of SIM-B Card is the same as SIM-A. SIM-A Card is shown here as an example.

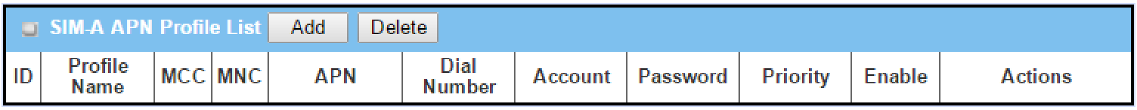
Item	Notes	Description
Network Type	Mandatory field. Default setting: **Auto**	Select Auto to register on a network automatically, regardless of the network type. The NTC-400 Series Router will give preference to high-speed networks. Select 2G Only to register the 2G network only. Select 2G Prefer to 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 – Options may be different due to the specification of the module.
Dial-Up Profile	Mandatory field. Default setting: **Auto-detection**	Specify the type of connection profile for your 3G/4G network. It can be Manual-configuration, APN Profile List, or Auto-detection. Select Manual-configuration to set APN (Access Point Name), Dial Number, Account, and Password to what your carrier provides. Select APN Profile List to set more than one profile to attempt to connect to in order until the connection is established. Select Auto-detection to automatically select the best configuration by detecting the SIM card and comparing it to the list on the router.
APN	Mandatory field.	Enter the APN you want to use to establish the connection. If Dial-up profile is set to Manual configuration, this field must be completed.
PIN code	String format: integer	Enter the PIN (Personal Identification Number) code if required to unlock your SIM card.

Item	Notes	Description
Authentication	Mandatory field. Default setting: **Auto**	Select either PAP (Password Authentication Protocol) or CHAP (Challenge Handshake Authentication Protocol) to authenticate with the carrier's server. When Auto is selected, it means it will authenticate with the server using either PAP or CHAP.
IP Mode	Mandatory field. Default setting: **Dynamic IP**	When Dynamic IP is selected, all IP configuration is taken from the carrier's server and set on the device automatically. If your carrier has provided you with a Static IP, you can switch to Static IP mode and fill in all required parameters. Note – IP Subnet Mask is Mandatory field.
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 the carrier while connecting.
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 given by the carrier while connecting.
Roaming	Disabled by default.	Check the box to establish a connection on other networks if a home network is not available. Note – Enabling this function may incur additional charges by your carrier.

Table 43 – Connection with SIM-A / SIM-B Card

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

You can add a new APN profile for the connection, or modify the content of the APN profile you added. It is available only when you select **Dial-Up Profile** as **APN Profile List**.

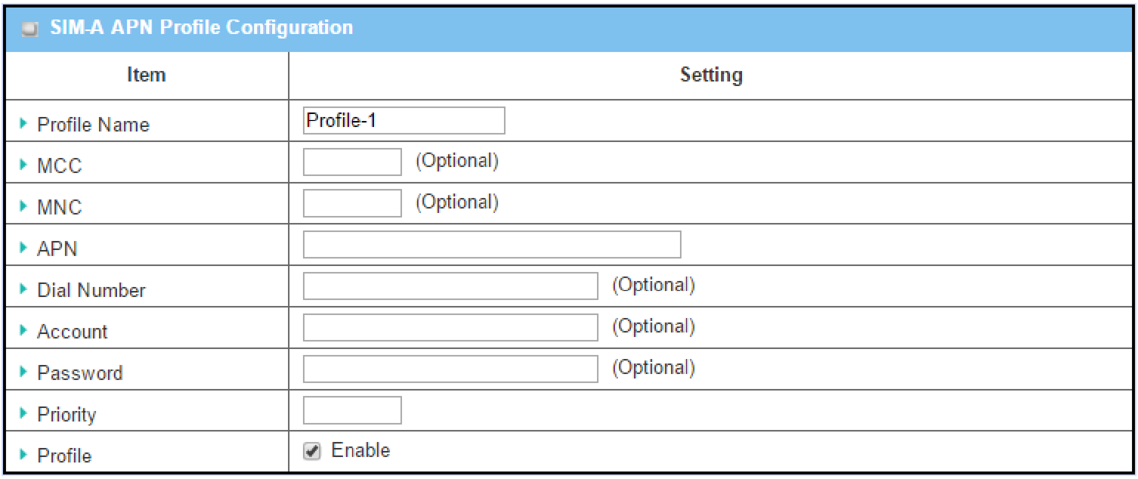


ID	Profile Name	MCC	MNC	APN	Dial Number	Account	Password	Priority	Enable	Actions

Table 44 – SIM-A / SIM-B APN Profile List

The SIM-A APN Profile List displays all the APN profiles you have created. It is available only when you select **Dial-Up Profile** as **APN Profile List**.

When **Add** button is applied, an **APN Profile Configuration** screen will appear.



Item	Setting
Profile Name	Profile-1
MCC	(Optional)
MNC	(Optional)
APN	
Dial Number	(Optional)
Account	(Optional)
Password	(Optional)
Priority	
Profile	☑ Enable

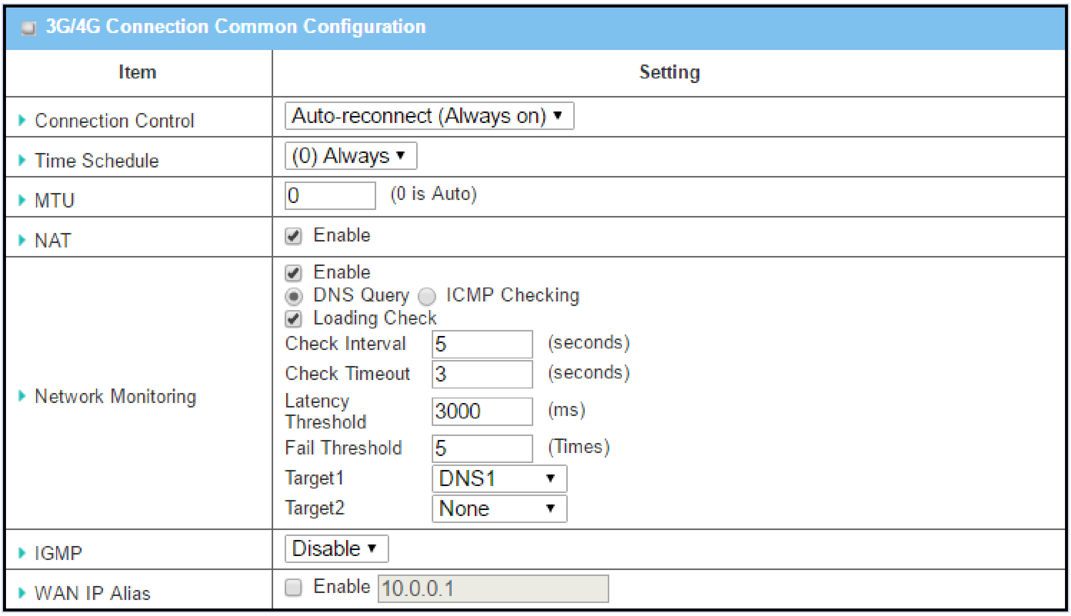
Figure 65 – SIM-A / SIM-B APN Profile Configuration

Item	Notes	Description
Profile Name	By default Profile-x is listed. String format: any text	Enter the profile name you want to describe for this profile.
MCC	String format: integer	Enter the MCC (Mobile Country Code) you want to use for this profile. **Note** – the MCC is related to the MNC and can't be blank or set to an 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** – the MNC is related to the MCC and can't be blank or set to an invalid value if MCC is filled-in.
APN	String format: any text	Enter the APN you want to use to establish the connection.
Account	String format: any text	Enter the Account you want to use for the authentication. Value Range: 0 - 53 characters.
Password	String format: any text	Enter the Password you want to use for the authentication.
Authentication	Mandatory field. Default setting: **Auto**	Select the Authentication method for the 3G/4G connection: **Auto**, **PAP**, **CHAP**, or **None**
Priority	Mandatory field. String format: integer	Enter a value for the connection order. Valid values are 1 to 16. The router will attempt to connect to profiles with a lower value. Value Range: 1 - 16.
Profile	Enabled by default.	Check the box to enable this profile. Uncheck the box to disable this profile in the dial-up action.
Save	Button	Click the **Save** button to save the configuration.
Undo	Button	Click the **Undo** button to restore what you just configured back to the previous setting.
Back	Button	When the **Back** button is clicked, the screen will return to the previous page.

Table 45 – SIM-A / SIM-B APN Profile Configuration

3.1.2.9 Setup 3G/4G Connection Common Configuration

Here you can change common configurations for the 3G/4G WAN interface.



3G/4G Connection Common Configuration

Item	Setting
Connection Control	Auto-reconnect (Always on) ▾
Time Schedule	(0) Always ▾
MTU	0 (0 is Auto)
NAT	☑ Enable
Network Monitoring	☑ Enable ● DNS Query ○ ICMP Checking ☑ Loading Check Check Interval 5 (seconds) Check Timeout 3 (seconds) Latency Threshold 3000 (ms) Fail Threshold 5 (Times) Target1 DNS1 ▾ Target2 None ▾
IGMP	Disable ▾
WAN IP Alias	□ Enable 10.0.0.1

Figure 66 – 3G/4G Connection Common Configuration

Item	Notes	Description
Connection Control	Default setting: **Auto-reconnect**	When **Auto-reconnect** is selected, the router will automatically attempt to re-establish a connection if it has dropped. When **Connect-on-demand** is selected, the router will only attempt to establish a connection only when detecting 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 > Basic Network > WAN & Uplink** tab for details. **Note** – This field is available only when **Basic Network > WAN > Physical Interface > Operation Mode** is selected to **Always on**.
Time Schedule	Mandatory field. Default setting: **(0) Always**	When **(0) Always** is selected, the selected WAN is in operation all the time. Once you have set other schedule rules, there are other options to select. Go to **Object Definition > Scheduling** for details.
MTU	Mandatory field. Default setting: **0**	Specify the MTU (Maximum Transmission Unit) for the 3G/4G connection. Value Range: 512 - 1500, but 0 is for auto.
NAT	Enabled by default.	Uncheck the box to disable NAT (Network Address Translation) function.
Network Monitoring	Optional field. Enabled by default.	When the Network Monitoring feature is enabled, the gateway will use DNS Query or ICMP to periodically check if the Internet connection is connected. Choose either DNS Query or ICMP Checking to detect a WAN link. With DNS Query, the system checks the connection by sending DNS Query packets to the destination specified in Target 1 and Target 2. With ICMP Checking, the system will check the connection by sending ICMP request packets to the specified destination.

Item	Notes	Description
		- Loading Check Enable Loading Check allows the router to ignore unreturned DNS Queries or ICMP requests when WAN bandwidth is fully occupied. This is to prevent false link-down status. - Check Interval defines the transmitting interval between two DNS Query or ICMP checking packets. Value Range: 2 - 30 seconds. - Check Timeout defines the timeout of each DNS query/ICMP. Value Range: 2 - 5 seconds. - Latency Threshold defines the threshold of responding time. Value Range: 2000 - (1000* Check Timeout) ms. - Fail Threshold specifies the detected disconnection before the router recognizes the WAN link is down. Enter a number of detecting disconnection times to be the threshold before disconnection is acknowledged. Value Range: 2 - 10 seconds. - Target1 (DNS1 set by default) specifies the first target of sending DNS query/ICMP request. - DNS1: set the primary DNS to be the target. - DNS2: set the secondary DNS to be the target. - Gateway: set the Current gateway to be the target. - Other Host: enter an IP address to be the target. - Target2 (None set by default) specifies the second target of sending 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. - Gateway: set the Current gateway to be the target. - Other Host: enter an IP address to be the target.
IGMP	Disabled by default.	Select **Auto** to enable IGMP function. Check ☑ **Enable** to enable IGMP Proxy.
WAN IP Alias	Disabled by default. String format: IP address (IPv4 type)	Check ☑ to enable WAN IP Alias, and fill in the IP address you want to assign.

Table 46 – 3G/4G Connection Common Configuration

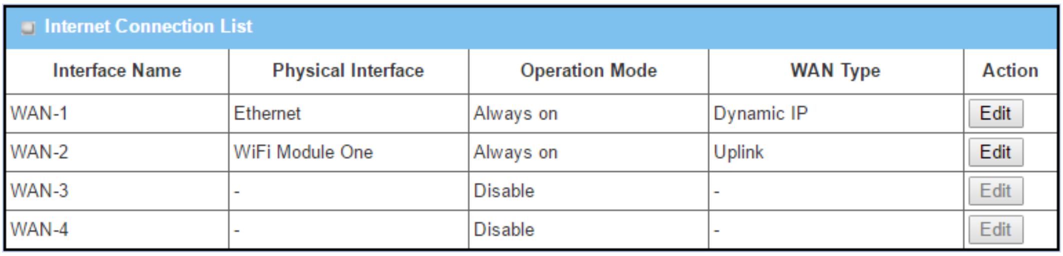
3.1.3 Wi-Fi Uplink Setup

If the device connects to the Internet through a Wi-Fi Uplink, this section will help you to complete the Wi-Fi Uplink connection setup.

Navigate to the **Basic Network > WAN & Uplink > Internet Setup** tab.

Wi-Fi Uplink interface: The Uplink network is a wireless network, and the router can connect to the Uplink network through a Wi-Fi connection.

If you have access permission to a certain wireless network, you can setup a Wi-Fi Uplink connection using the NTC-400 Series Router. The router can support 802.11ac/n/g/b data connections and can connect to a wireless network (access point) under the regular infrastructure mode.



Internet Connection List

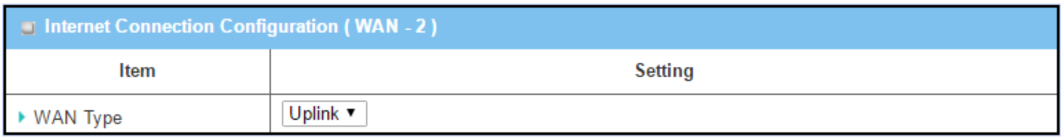
Interface Name	Physical Interface	Operation Mode	WAN Type	Action
WAN-1	Ethernet	Always on	Dynamic IP	Edit
WAN-2	WiFi Module One	Always on	Uplink	Edit
WAN-3	-	Disable	-	Edit
WAN-4	-	Disable	-	Edit

Figure 67 – Internet Connection List

3.1.3.1 Configure Ethernet WAN Setting

When the **Edit** button is applied, **Internet Connection Configuration**

screen appears. WAN-2 interface is used in this example.



Internet Connection Configuration (WAN - 2)

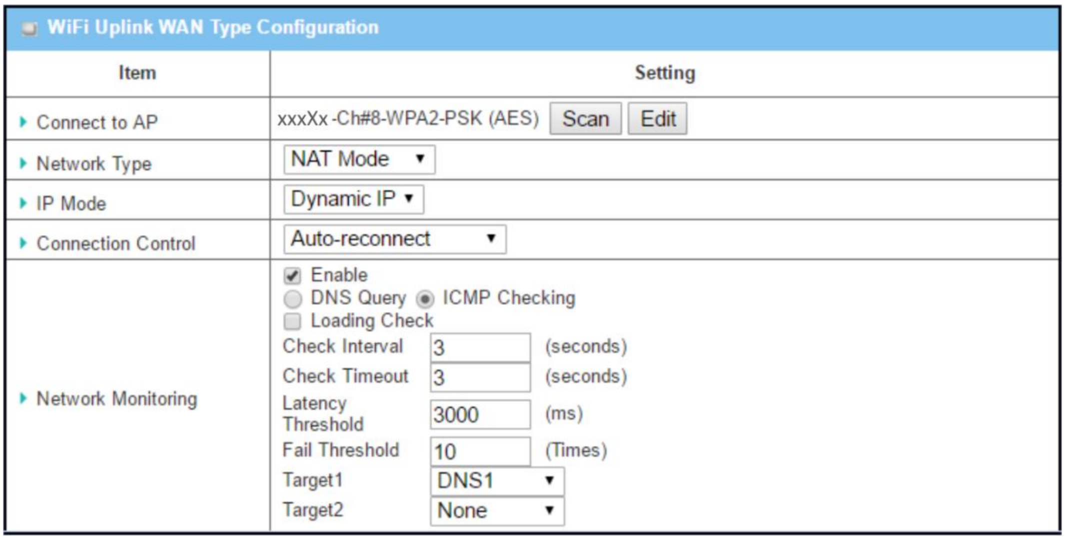
Item	Setting
WAN Type	Uplink ▾

Figure 68 – Internet Connection Configuration (WAN-2)

Item	Notes	Description
WAN Type	Mandatory field. Default setting: **Uplink**	From the dropdown box, select the Internet connection method for the Wi-Fi Uplink Connection. Only Uplink is available.

Table 47 – Internet Connection Configuration (WAN-2)

3.1.3.2 Wi-Fi Uplink



WiFi Uplink WAN Type Configuration

Item	Setting
Connect to AP	xxxXx -Ch#8-WPA2-PSK (AES) Scan Edit
Network Type	NAT Mode ▾
IP Mode	Dynamic IP ▾
Connection Control	Auto-reconnect ▾
Network Monitoring	☑ Enable ○ DNS Query ● ICMP Checking □ Loading Check Check Interval 3 (seconds) Check Timeout 3 (seconds) Latency Threshold 3000 (ms) Fail Threshold 10 (Times) Target1 DNS1 ▾ Target2 None ▾

Figure 69 – Wi-Fi Uplink WAN Type Configuration

Item	Notes	Description
Connect to AP	N/A	Display the information of AP for connecting. You can click the Scan button and select an AP for the uplink network. You can also create uplink profile(s) for ease of connecting to an available Uplink network. Refer to the **Basic Network > Wi-Fi > Uplink Profile** tab.
Network Type	Mandatory field. Default setting: **NAT Mode**	Select the expected network type for the Wi-Fi Uplink connection. It can be NAT Mode, Bridge Mode, or NAT Disable. When NAT Mode is selected, the NAT function is activated on the Wireless Uplink connection; when Bridge Mode is selected, the bridge function is activated on the Wireless Uplink connection. Bridge mode support depends on the product specification. If the purchased device doesn't support bridge mode, it will be greyed out from selection. When NAT Disable is selected, the NAT function is deactivated on the Wireless Uplink connection, and it can function as a router with manually configured routing settings.
IP Mode	Mandatory field. Default setting: **Dynamic IP**	Specify the IP mode for the wireless uplink Interface: **Dynamic IP** or **Static IP** When **Dynamic IP** is selected, the device will request an IP from the Uplink Network as the IP for the uplink interface. When **Static IP** is selected, you have to manually configure the IP address settings for the uplink interface. The settings include IP address, subnet mask, gateway, and primary/secondary DNS.
Connection Control	Mandatory field.	There are three connection modes. - **Auto-reconnect (Always on)** enables the router to always keep the Internet connection on. - **Connect-on-demand** enables the router to automatically re-establish the Internet connection as soon as the user attempts to access the Internet. The Internet connection will be disconnected when it has been inactive for a specified idle time.

Item	Notes	Description
		- **Connect Manually** allows user to connect to the Internet manually. The Internet connection will be inactive after it has been inactive for a specified idle time.
Network Monitoring	Optional setting. Enabled by default.	When the Network Monitoring feature is enabled, the router uses DNS Query or ICMP to periodically check the Internet connection state. - Choose either **DNS Query** or **ICMP Checking** to detect WAN link. With **DNS Query**, the system checks the connection by sending DNS Query packets to the destination specified in Target 1 and Target 2. With **ICMP Checking**, the system will check the connection by sending ICMP request packets to the destination specified in Target 1 and Target 2. - Loading Check Enable Loading Check allows the router to ignore unreturned DNS Queries or ICMP requests when WAN bandwidth is fully occupied. This is to prevent false link-down status. - Check Interval defines the transmitting interval between two DNS Query or ICMP checking packets. - Check Timeout defines the timeout of each DNS query/ICMP. - Latency Threshold defines the tolerance threshold of responding time. - Fail Threshold specifies the detected disconnection before the router recognizes the WAN link down status. Enter a number of disconnection times before disconnection is acknowledged as the threshold. - Target1 (DNS1 set by default) specifies the first target of sending DNS query/ICMP request. - DNS1: set the primary DNS to be the target. - DNS2: set the secondary DNS to be the target. - Gateway: set the Current gateway to be the target. - Other Host: enter an IP address to be the target. - Target2 (None set by default) specifies the second target of sending 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. - Gateway: set the Current gateway to be the target. - Other Host: enter an IP address to be the target.
Save	Button	Click **Save** to save the settings.
Undo	Button	Click **Undo** to cancel the settings.

Table 48 – Wi-Fi Uplink WAN Type Configuration

3.2 LAN & VLAN

This section provides details on the configuration of LANs and VLANs.

3.2.1 Ethernet LAN

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

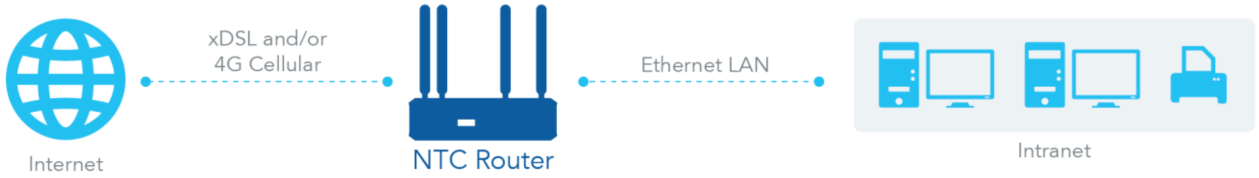
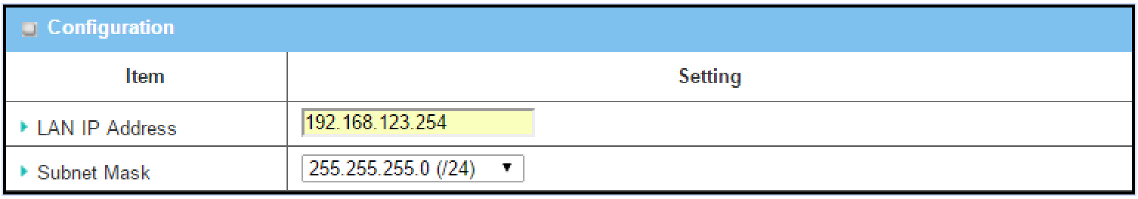


Figure 70 – Ethernet LAN



Configuration

Item	Setting
LAN IP Address	192.168.123.254
Subnet Mask	255.255.255.0 (/24) ▼

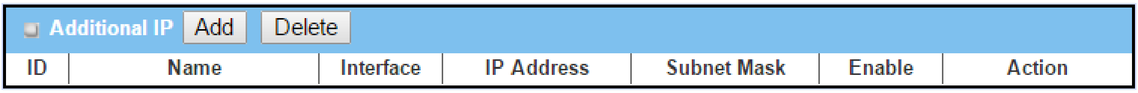
Figure 71 – Ethernet LAN Configuration

Item	Notes	Description
LAN IP Address	Mandatory field. Default setting: 192.168.1.1	Enter the local IP address of this device. The network device(s) on your network must use the LAN IP address of this device as their Default Gateway. You can change it if necessary. Note – This is also the IP address of web UI. If you change it, you need to type the new IP address in the browser to access the web interface.
Subnet Mask	Mandatory field. Default setting: 255.255.255.0 (/24)	Select the subnet mask for the router from the dropdown list. 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 IP addresses are allowed in this subnet. However, one of them is occupied by LAN IP address of this gateway, so there are maximum 253 clients allowed in LAN network. Value Range: **255.0.0.0 (/8) - 255.255.255.252 (/30)**
Save	Button	Click the **Save** button to save the configuration
Undo	Button	Click the **Undo** button to restore what you just configured back to the previous setting.

Table 49 – Ethernet LAN Configuration

3.2.1.1 Create / Edit Additional IP

The router provides the LAN IP alias function for some special management consideration. You can add additional LAN IPs for the router and access to the router using the additional IP.

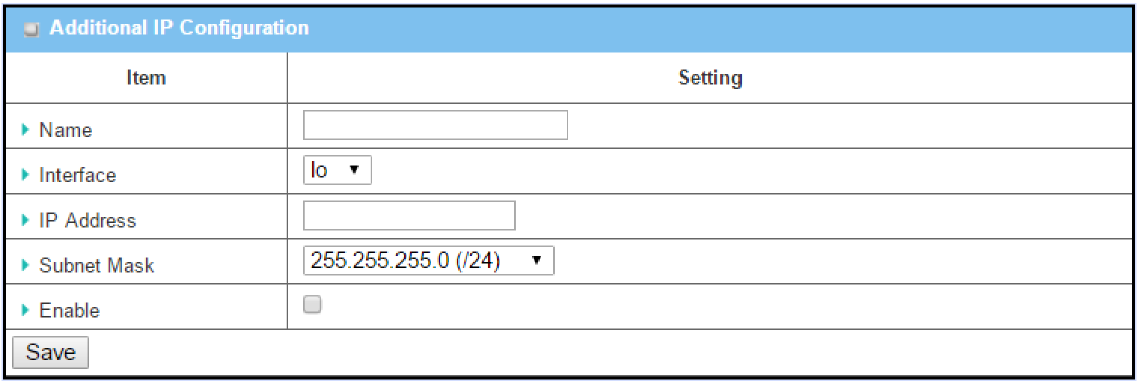


Additional IP Add Delete

ID	Name	Interface	IP Address	Subnet Mask	Enable	Action

Figure 72 – Create/Edit Additional IP

Click the **Add** button to display the **Additional IP Configuration** screen.



Additional IP Configuration

Item	Setting
Name	
Interface	lo ▾
IP Address	
Subnet Mask	255.255.255.0 (/24) ▾
Enable	□

Save

Figure 73 – Additional IP Configuration

Item	Notes	Description
Name	Optional Setting	Enter the name for the alias IP address.
Interface	Mandatory field. Default setting: **Lo**	Specify the Interface type: **Lo** or **Br0**
IP Address	Optional setting. Default setting: **192.168.1.1**	Enter the additional IP address for this device.
Subnet Mask	Mandatory field. Default setting: **255.255.255.0 (/24)**	Select the subnet mask for this gateway from the dropdown list. 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 means a maximum of 254 IP addresses are allowed in this subnet. However, one of them is occupied by the LAN IP address of the router so there are a maximum of 253 clients allowed on the LAN. Value Range: 255.0.0.0 (/8) - 255.255.255.255 (/32).
Save	NA	Click the **Save** button to save the configuration

Table 50 – Additional IP Configuration

3.2.2 VLAN

VLAN (Virtual LAN) is a logical network under a certain switch or router device to group client hosts with a specific VLAN ID. The NTC-400 Series Router supports both Port-based VLAN and Tag-based VLAN. These functions allow you to divide the local network into different “virtual LANs”.

3.2.2.1 Port-based VLAN

The Port-based VLAN function groups Ethernet ports (Port-1 to Port-4) and Wi-Fi Virtual Access Points (VAP-1 - VAP-8) together for differentiated services like Internet access, multimedia and VoIP services. There are two operation modes, NAT and Bridge, which can be applied to each VLAN group. One DHCP server can be allocated to a NAT VLAN group to allow group host members to get their IP addresses. Thus, each host can access the Internet via the NAT mechanism. In bridge mode, Intranet packet flow is delivered out of the WAN trunk port with VLAN tags to upper links for different services.

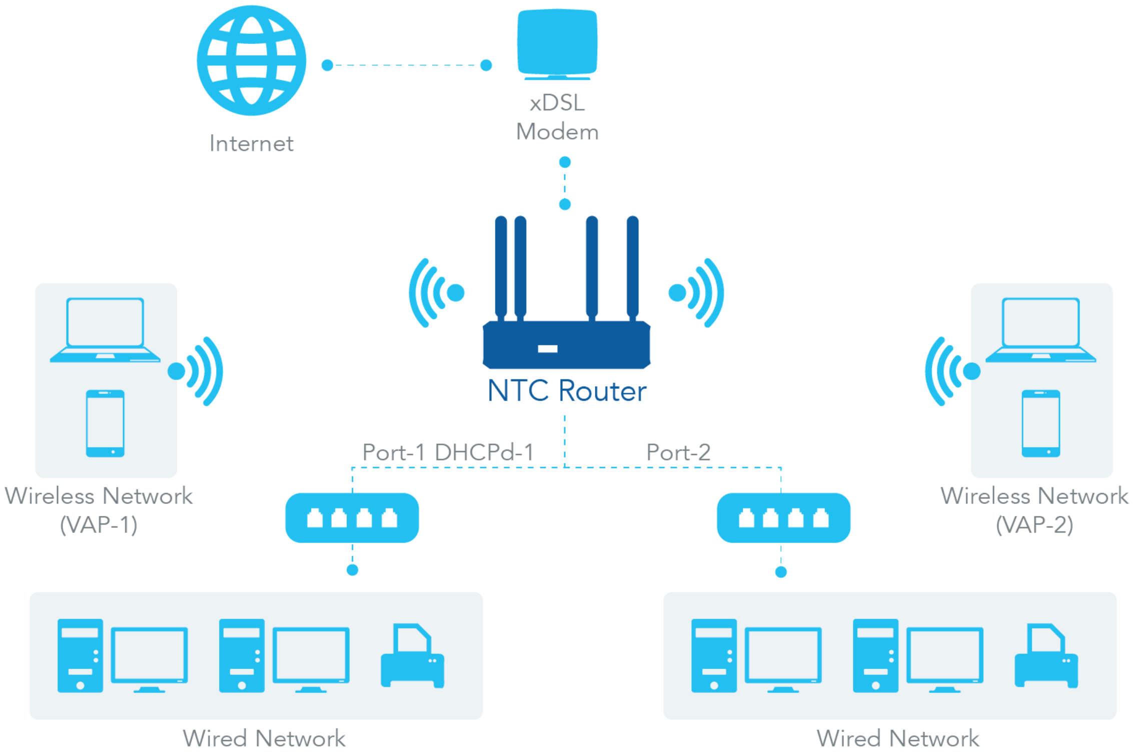


Figure 74 – Port-based VLAN

A port-based VLAN is a group of ports on an Ethernet or Virtual APs on a wired or wireless gateway that form a logical LAN segment. For example, in a company where the administrator has created 3 network segments; Lobby/Meeting Room, Office, and Data Centre, the administrator can configure the 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. They may also configure 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 administrator may also configure Data Centre segment with VLAN ID 1.

The VLAN group includes Port-1 with NAT mode to WAN interface as shown in following diagram.

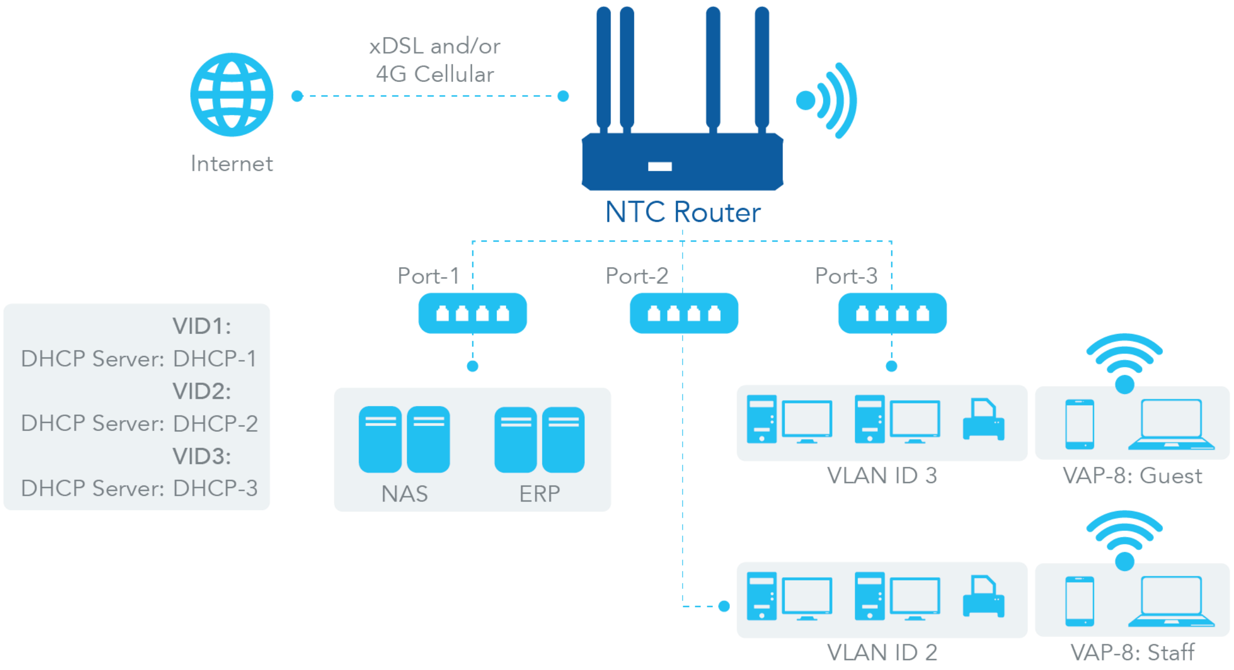


Figure 75 – Port-based VLAN example

3.2.2.2 Tag-based VLAN

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

The Tag-based VLAN function can group Ethernet ports, Port-1 to 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 for the Intranet. These flows can be directed to different destinations because they have different tags. This approach is very useful to group hosts in different geographic locations to be in the same workgroup.

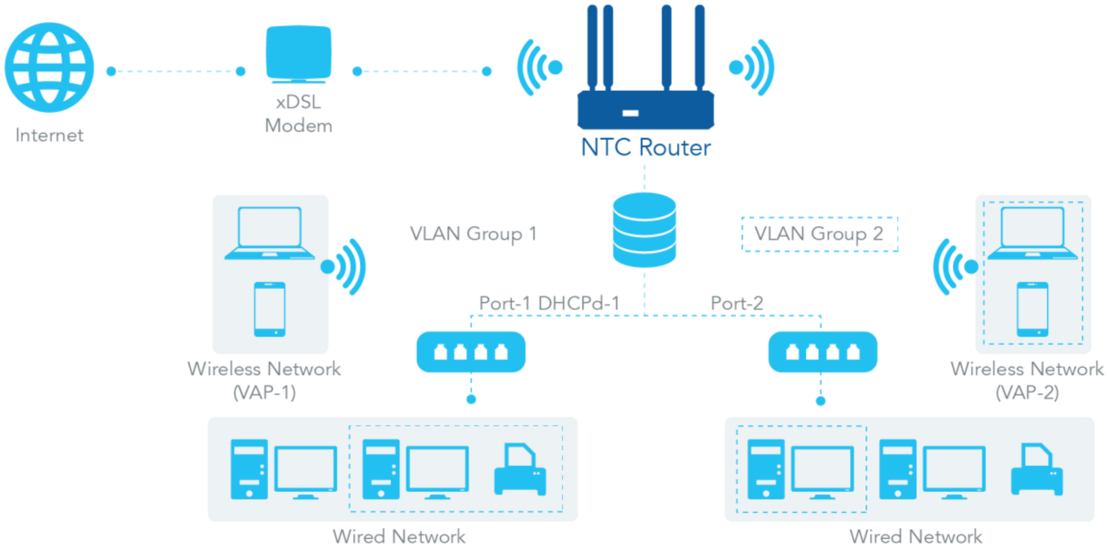


Figure 76 – Tag-based VLAN

For example, in a company where the administrator has created 3 network segments; Lab, Meeting Rooms, and Office the administrator can configure the Office segment with VLAN ID 12. The VLAN group is equipped with DHCP-3 server to construct a 192.168.12.x subnet. They may also configure the Meeting Rooms segment with VLAN ID 11. The VLAN group is equipped with DHCP-2 server to construct a 192.168.11.x subnet for Intranet only. That is, any client host in VLAN 11 group can't access the Internet. They can also configure the Lab segment with VLAN ID 10. The VLAN group is equipped with DHCP-1 server to construct a 192.168.10.x subnet.

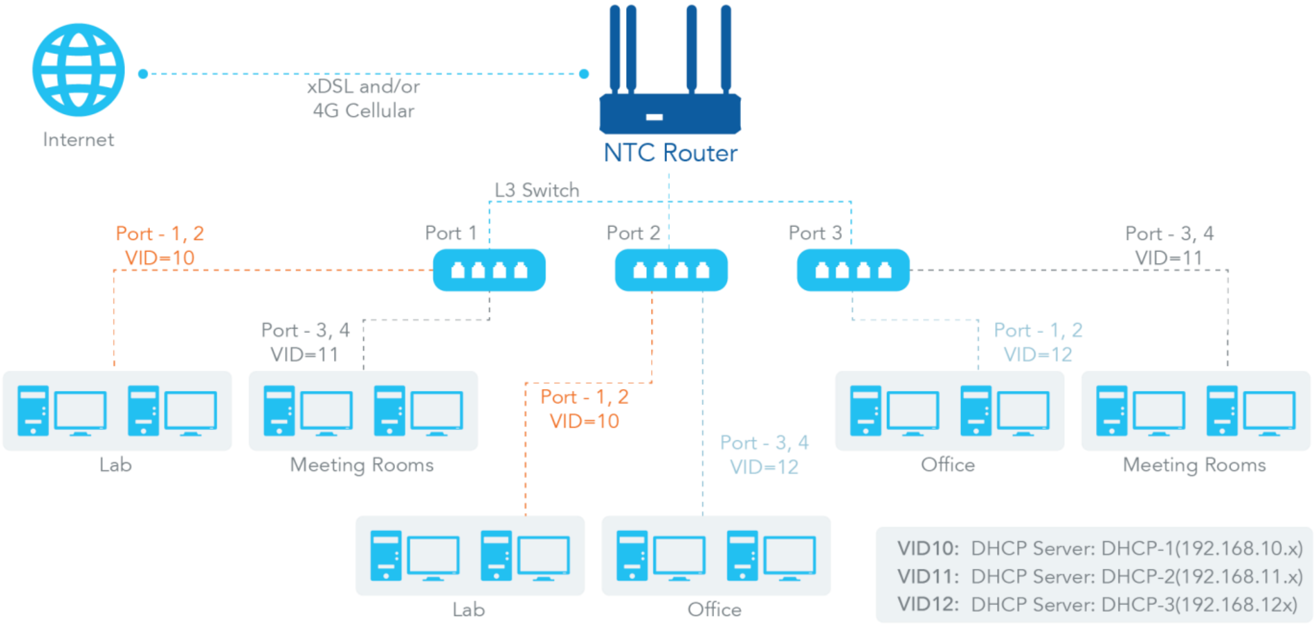


Figure 77 – Tag-based VLAN example

3.2.2.3 VLAN Groups Access Control

The administrator can specify the Internet access permission for all VLAN groups and configure which VLAN groups are allowed to communicate with each other.

3.2.2.4 VLAN Group Internet Access

The administrator can allow or deny Internet access to specific members of a VLAN group. For example, VLANs VID-2 and VID-3 can access the Internet but VID1 cannot access the Internet. The following is an example where VLAN IDs 2 and 3 can access Internet but the one with VID is 1 cannot access Internet. That is, visitors in the meeting room and staff in the office network can access the Internet but the computers/servers in the data centre cannot access the Internet due to security considerations. Servers in the data centre are only for trusted staff or are accessed via secure tunnels.

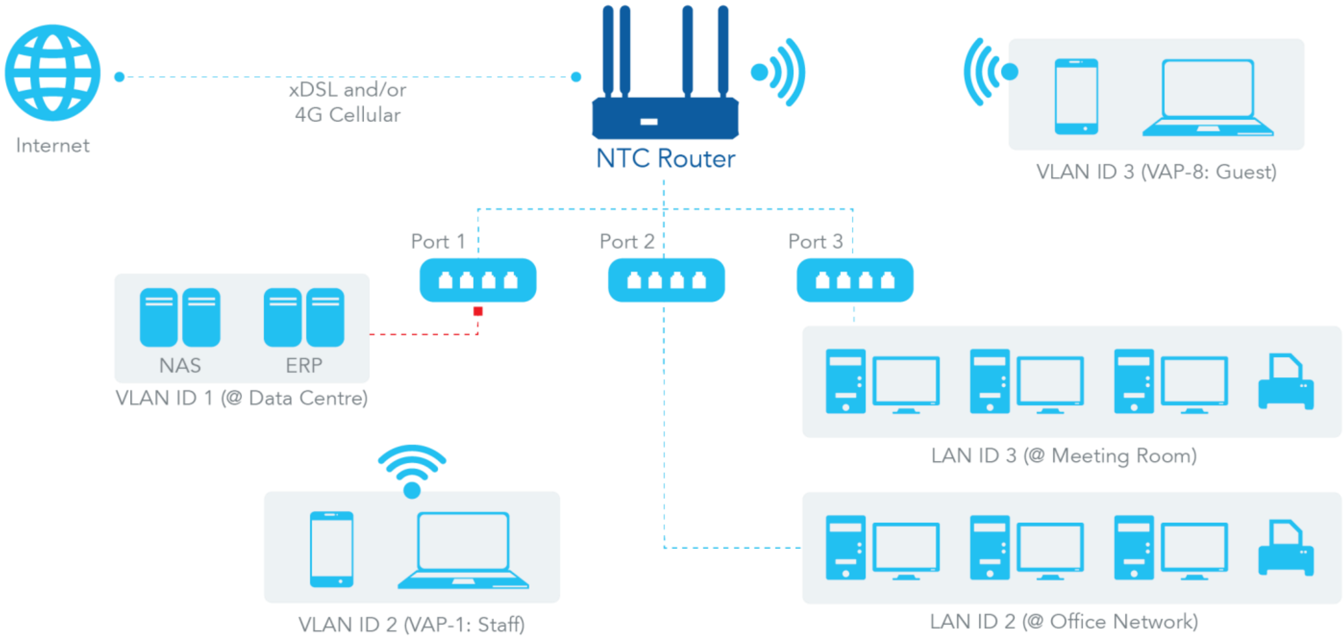


Figure 78 – VLAN Group Internet Access example

3.2.2.5 Inter VLAN Group Routing

In Port-based tagging, the administrator can specify member hosts of one VLAN group to be able to communicate with the ones in another VLAN group or not. This is a communication pair and one VLAN group can join many communication pairs. However, A can communicate with B, and B can communicate with C, but that doesn't mean that A can communicate with C.

An example is shown in the following diagram: VLAN groups 1 and 2 can access each other but the ones between VLAN ID 1 and VLAN ID 3 and between VLAN ID 2 and VLAN ID 3 cannot.

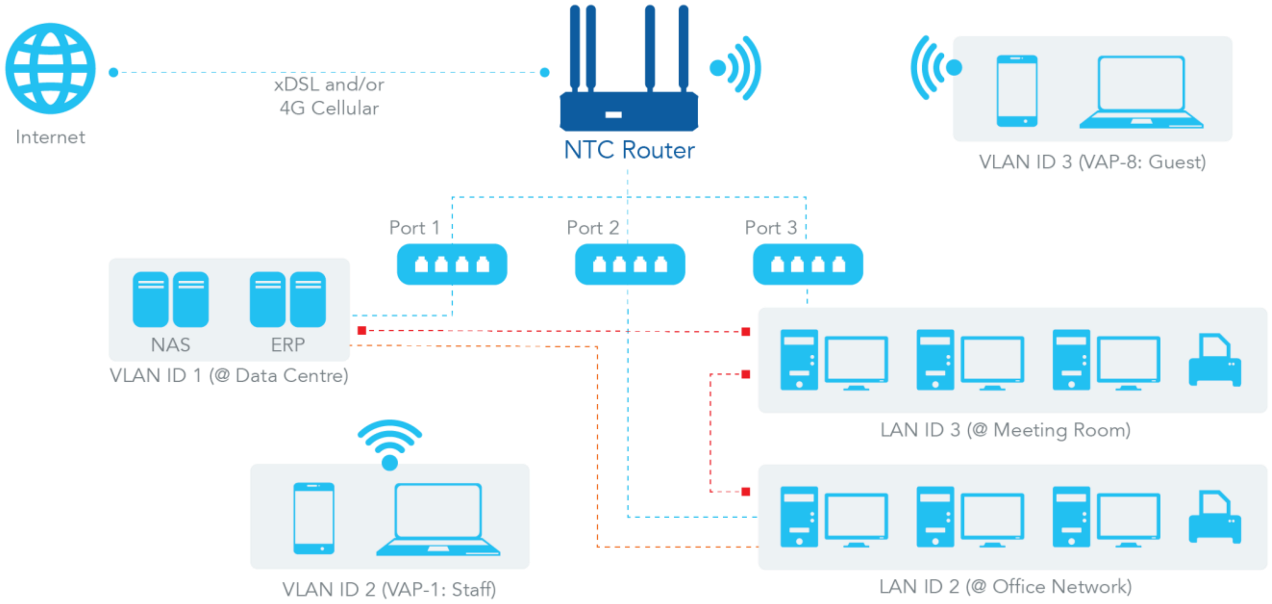
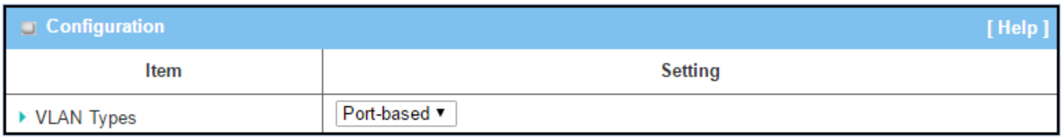


Figure 79 – Inter VLAN Group Routing

3.2.2.6 VLAN Setting

Navigate to the **Basic Network > LAN & VLAN > VLAN** tab.

The VLAN function allows you to divide the local network into different virtual LANs. There are Port-based and Tag-based VLAN types. Select one that applies.



Configuration [Help]

Item	Setting
VLAN Types	Port-based ▾

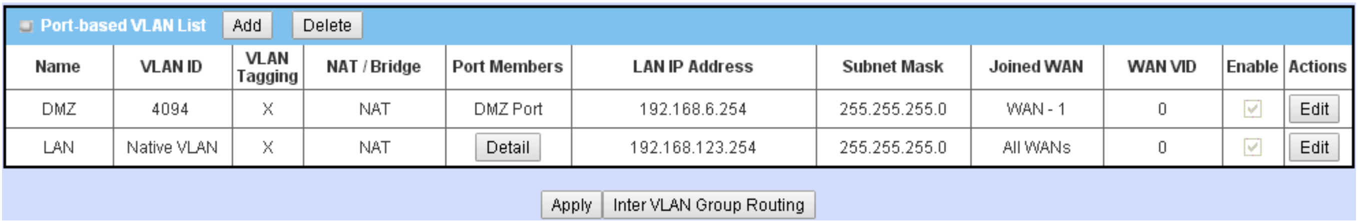
Figure 80 – VLAN Setting

Item	Notes	Description
VLAN Type	Default setting: **Port-based**	Select the VLAN type that you want to adopt for organizing your local subnets. **Port-based** – A Port-based VLAN allows you to add rules for each LAN port and advanced control with its VLAN ID. **Tag-based –** Tag-based VLAN allows you to add a VLAN ID and select members and a DHCP Server for this VLAN ID. See the Tag-based VLAN List table.
Save	Button	Click the **Save** button to save the configuration.

Table 51 – VLAN Setting

3.2.2.7 Port-based VLAN – Create/Edit VLAN Rules

The port-based VLAN allows you to customise each LAN port. There is a default rule that shows the configuration of all LAN ports. If your device has a DMZ port, you will also see DMZ configuration. The maximum number of rules is based on LAN port numbers.

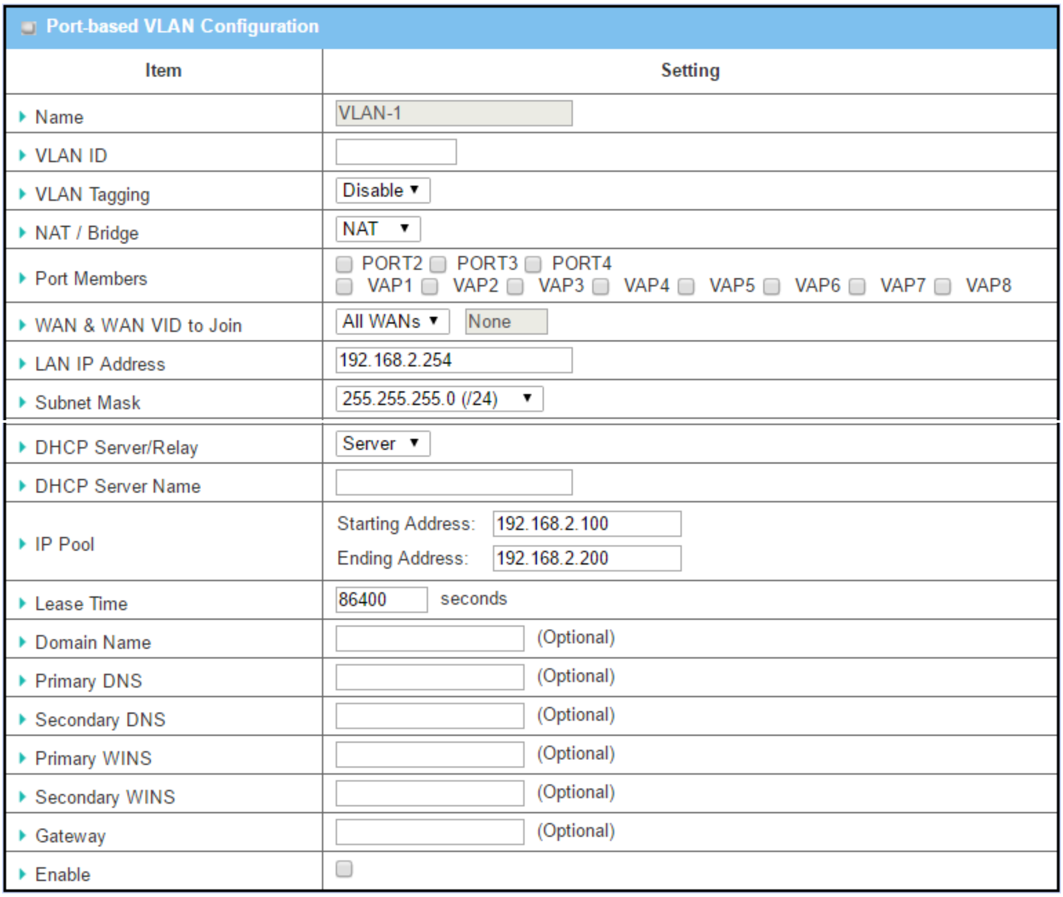


Name	VLAN ID	VLAN Tagging	NAT / Bridge	Port Members	LAN IP Address	Subnet Mask	Joined WAN	WAN VID	Enable	Actions
DMZ	4094	X	NAT	DMZ Port	192.168.6.254	255.255.255.0	WAN - 1	0	☑	Edit
LAN	Native VLAN	X	NAT	Detail	192.168.123.254	255.255.255.0	All WANs	0	☑	Edit

Figure 81 – Port-based VLAN

Click the **Add** button to display the Port-based VLAN Configuration screen which is consists of 3 sections: **Port-based VLAN Configuration**, **IP Fixed Mapping Rule List,** and **Inter VLAN Group Routing**

3.2.2.8 Port-based VLAN – Configuration



Item	Setting
Name	VLAN-1
VLAN ID	
VLAN Tagging	Disable ▾
NAT / Bridge	NAT ▾
Port Members	☐ PORT2 ☐ PORT3 ☐ PORT4 ☐ VAP1 ☐ VAP2 ☐ VAP3 ☐ VAP4 ☐ VAP5 ☐ VAP6 ☐ VAP7 ☐ VAP8
WAN & WAN VID to Join	All WANs ▾ None
LAN IP Address	192.168.2.254
Subnet Mask	255.255.255.0 (/24) ▾
DHCP Server/Relay	Server ▾
DHCP Server Name	
IP Pool	Starting Address: 192.168.2.100 Ending Address: 192.168.2.200
Lease Time	86400 seconds
Domain Name	(Optional)
Primary DNS	(Optional)
Secondary DNS	(Optional)
Primary WINS	(Optional)
Secondary WINS	(Optional)
Gateway	(Optional)
Enable	☐

Figure 82 – Port-based VLAN Configuration

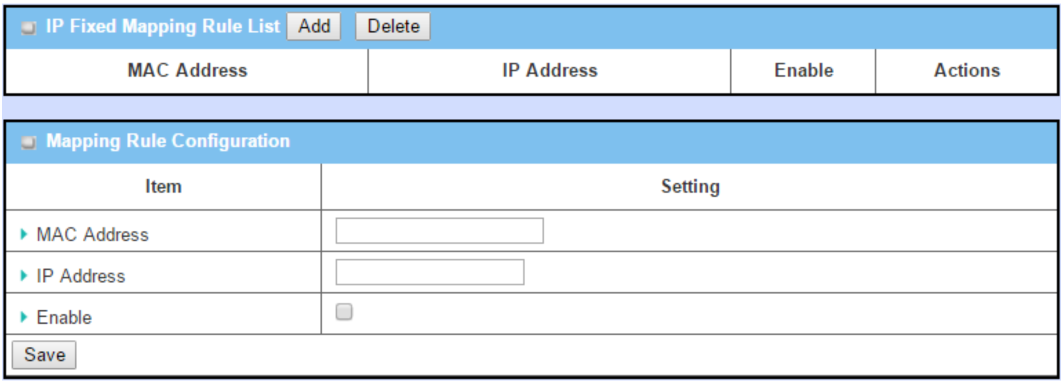
Item	Notes	Description
Name	Mandatory field. String format: Pre-defined, not customisable.	Define the Name of this rule. This field is pre-defined and is not customisable.

Item	Notes	Description
VLAN ID	Mandatory field.	Define the VLAN ID number. The range is 1 to 4094.
VLAN Tagging	Default setting: **Disable**	The rule is activated according to VLAN ID and Port Members configuration when **Enable** is selected. The rule is activated according to Port Members configuration when **Disable** is selected.
NAT / Bridge	Default setting: **NAT**	Select NAT mode or Bridge mode for the rule.
Port Members	These boxes are unchecked by default.	Select which LAN port(s) and VAP(s) that you want to add to the rule.
WAN & WAN VID to Join	All WANs are selected by default.	Select which WAN or All WANs that allow access to the Internet. Note – If Bridge mode is selected, you need to select a WAN and enter a VID.
LAN IP Address	Mandatory field.	Assign an IP Address for the DHCP Server that the rule uses. This IP address is a router IP.
Subnet Mask	255.255.255.0(/24)Default setting:	Select a Subnet Mask for the DHCP Server.
DHCP Server /Relay	Default setting: **Server**	Define the DHCP Server type. There are three types you can select: **Server, Relay** or **Disable** **Relay –** Select Relay to enable DHCP Relay function for the VLAN group, then fill in the DHCP Server IP Address field. **Server –** Select Server to enable DHCP Server function for the VLAN group, then specify 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 field.	If you select Relay type of DHCP Server, assign a DHCP Server IP Address that the router will relay the DHCP requests to.
DHCP Server Name	Mandatory field.	Define name of the DHCP Server.
IP Pool	Mandatory field.	Define the IP Pool range. There are Starting Address and Ending Address fields. If a client requests an IP address from this DHCP Server, it will assign an IP address in the range of IP pool.
Lease Time	Mandatory field.	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. Value Range: 0 to 31 characters.
Primary DNS	IPv4 format	The Primary DNS of this DHCP Server.
Secondary DNS	IPv4 format	The Secondary DNS of this DHCP Server.

Item	Notes	Description
Primary WINS	IPv4 format	The Primary WINS of this DHCP Server.
Secondary WINS	IPv4 format	The Secondary WINS of this DHCP Server.
Gateway	IPv4 format	The Gateway of this DHCP Server.
Enable	Disabled by default.	Click ☑ **Enable** to activate this rule.
Save	Button	Click the **Save** button to save the configuration
Undo	Button	Click the **Undo** button to restore what you just configured back to the previous setting.

Table 52 – Port-based VLAN Configuration

You can add IP rules in the **IP Fixed Mapping Rule List** if a DHCP Server for the VLAN groups is required.



IP Fixed Mapping Rule List

MAC Address	IP Address	Enable	Actions

Mapping Rule Configuration

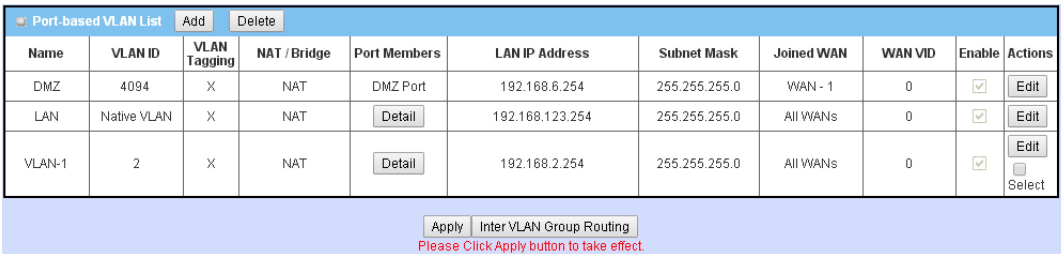
Item	Setting
MAC Address	
IP Address	
Enable	□

Figure 83 – IP Fixed Mapping Rule List

Click the **Add** button to display the **Mapping Rule Configuration** screen.

Item	Notes	Description
MAC Address	Mandatory field.	Define the MAC Address target that the DHCP Server wants to match.
IP Address	Mandatory field.	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 matches the rule.
Enable	Disabled by default.	Click ☑ **Enable** to activate this rule.
Save	Button	Click the **Save** button to save the configuration

Table 53 – IP Fixed Mapping Rule List



Port-based VLAN List

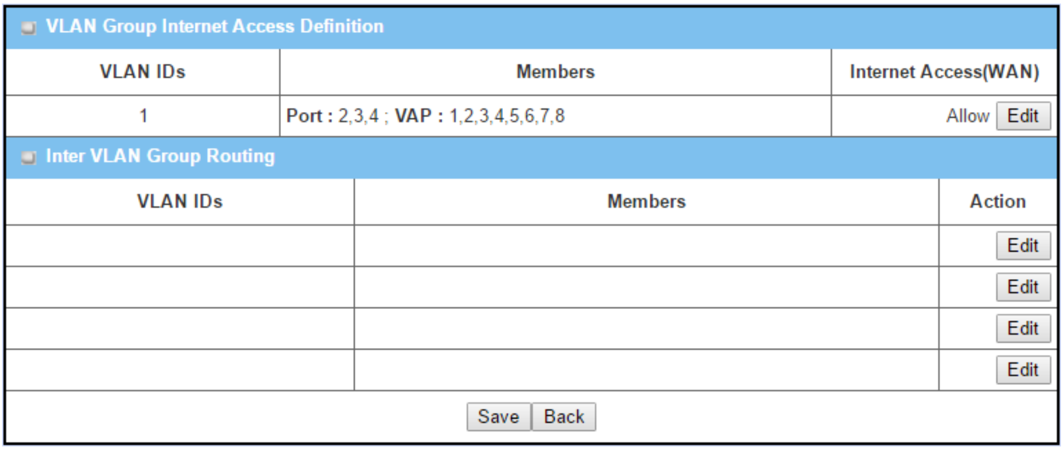
Name	VLAN ID	VLAN Tagging	NAT / Bridge	Port Members	LAN IP Address	Subnet Mask	Joined WAN	WAN VID	Enable	Actions
DMZ	4094	X	NAT	DMZ Port	192.168.6.254	255.255.255.0	WAN - 1	0	☑	Edit
LAN	Native VLAN	X	NAT	Detail	192.168.123.254	255.255.255.0	All WANs	0	☑	Edit
VLAN-1	2	X	NAT	Detail	192.168.2.254	255.255.255.0	All WANs	0	☑	Edit □ Select

Please Click Apply button to take effect.

Figure 84 – Port-based VLAN List

3.2.2.9 Port-based VLAN – Inter VLAN Group Routing

Click the **VLAN Group Routing** button. The VLAN Group Internet Access Definition and Inter VLAN Group Routing are displayed.



VLAN Group Internet Access Definition

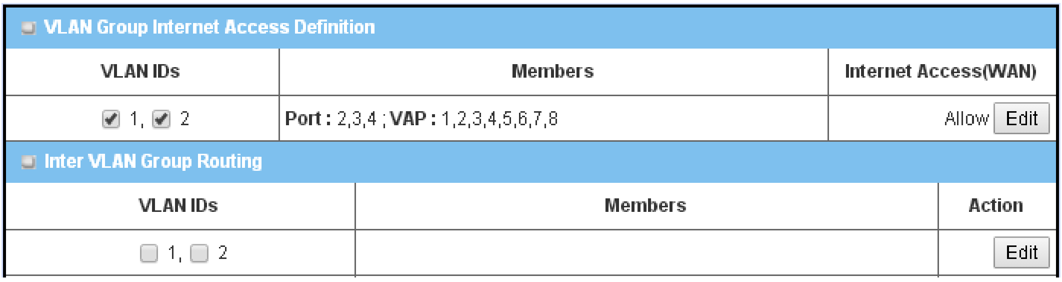
VLAN IDs	Members	Internet Access(WAN)
1	**Port :** 2,3,4 ; **VAP :** 1,2,3,4,5,6,7,8	Allow Edit

Inter VLAN Group Routing

VLAN IDs	Members	Action
		Edit
		Edit
		Edit
		Edit

Figure 85 – VLAN Group Internet Access Definition

When the **Edit** button is applied, the following screen is displayed:



VLAN Group Internet Access Definition

VLAN IDs	Members	Internet Access(WAN)
☑ 1, ☑ 2	**Port :** 2,3,4 ; **VAP :** 1,2,3,4,5,6,7,8	Allow Edit

Inter VLAN Group Routing

VLAN IDs	Members	Action
□ 1, □ 2		Edit

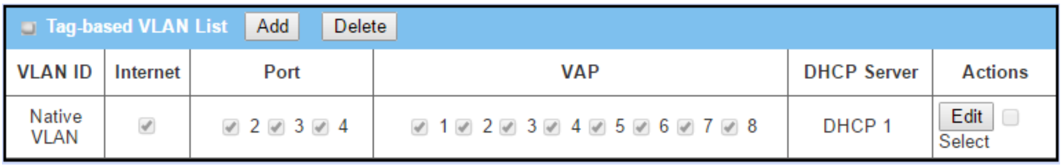
Figure 86 – VLAN Group Internet Access Definition

Item	Notes	Description
VLAN Group Internet Access Definition	All boxes are checked by default.	The default settings mean all VLAN ID members are allowed to access the WAN interface. If a VLAN ID box is unchecked, that VLAN ID member can't access the Internet anymore. **Note** – VLAN ID 1 is available always; it is the default VLAN ID of the LAN rule. The other VLAN IDs are available only when they are enabled.
Inter VLAN Group Routing	Disabled by default.	Click the expected VLAN IDs box to enable the Inter VLAN access function. By default, members in different VLAN IDs can't access each other. The router supports up to 4 rules for Inter VLAN Group Routing. For example, if ID_1 and ID_2 are checked, members in VLAN ID_1 can access members of VLAN ID_2 and vice versa.
Save	Button	Click the **Save** button to save the configuration

Table 54 – VLAN Group Internet Access Definition

3.2.2.10 Tag-based VLAN – Create/Edit VLAN Rules

The **Tag-based VLAN** allows you to customize each LAN port according to VLAN ID. There is a default rule shows the configuration of all LAN ports and all VAPs.

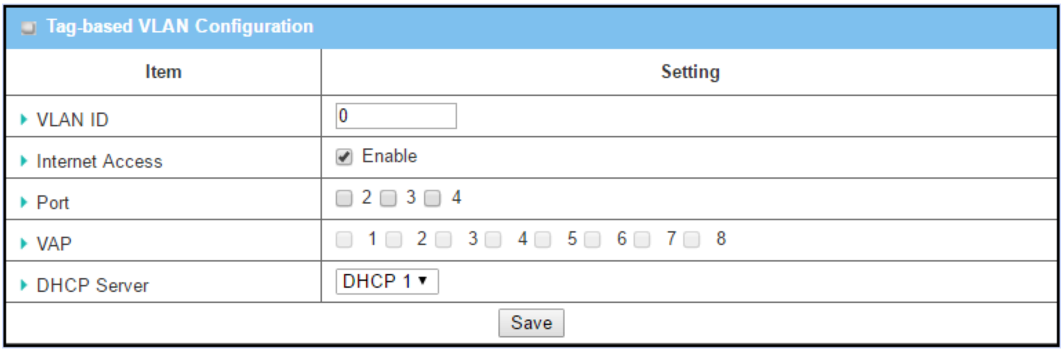


Tag-based VLAN List | Add | Delete

VLAN ID	Internet	Port	VAP	DHCP Server	Actions
Native VLAN	☑	☑ 2 ☑ 3 ☑ 4	☑ 1 ☑ 2 ☑ 3 ☑ 4 ☑ 5 ☑ 6 ☑ 7 ☑ 8	DHCP 1	Edit □ Select

Figure 87 – Tag-based VLAN List

Click the **Add** button to display the **Tag-based VLAN Configuration** screen.



Tag-based VLAN Configuration

Item	Setting
VLAN ID	0
Internet Access	☑ Enable
Port	□ 2 □ 3 □ 4
VAP	□ 1 □ 2 □ 3 □ 4 □ 5 □ 6 □ 7 □ 8
DHCP Server	DHCP 1 ▾

Save

Figure 88 – Tag-based VLAN Configuration

Item	Notes	Description
VLAN ID	Mandatory field.	Define the VLAN ID number. Range: 6 - 4094
Internet Access	Enabled by default.	Check ☑ **Enable** to allow the members in the VLAN group access to the Internet.
Port	Disabled by default.	Check the LAN port box(es) to join the VLAN group.
VAP	Disabled by default.	Check the VAP box(es) to join the VLAN group.
DHCP Server	Default setting: **DHCP 1**	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	Button	Click the **Save** button to save the configuration. **Note** – After clicking the **Save** button, always click the **Apply** button to apply the settings.

Table 55 – Tag-based VLAN Configuration

3.2.3 DHCP Server

3.2.3.1 DHCP Server

The router supports up to 4 DHCP servers to fulfil the DHCP requests from different VLAN groups (please refer to the VLAN section for more detail). You can add more DHCP server configurations by clicking on the “Add” button behind “DHCP Server List”, or clicking on the “Edit” button at the end of each DHCP Server on the list to edit its settings. You can select a DHCP Server and delete it by clicking on the “Select” check-box and then the “Delete” button.

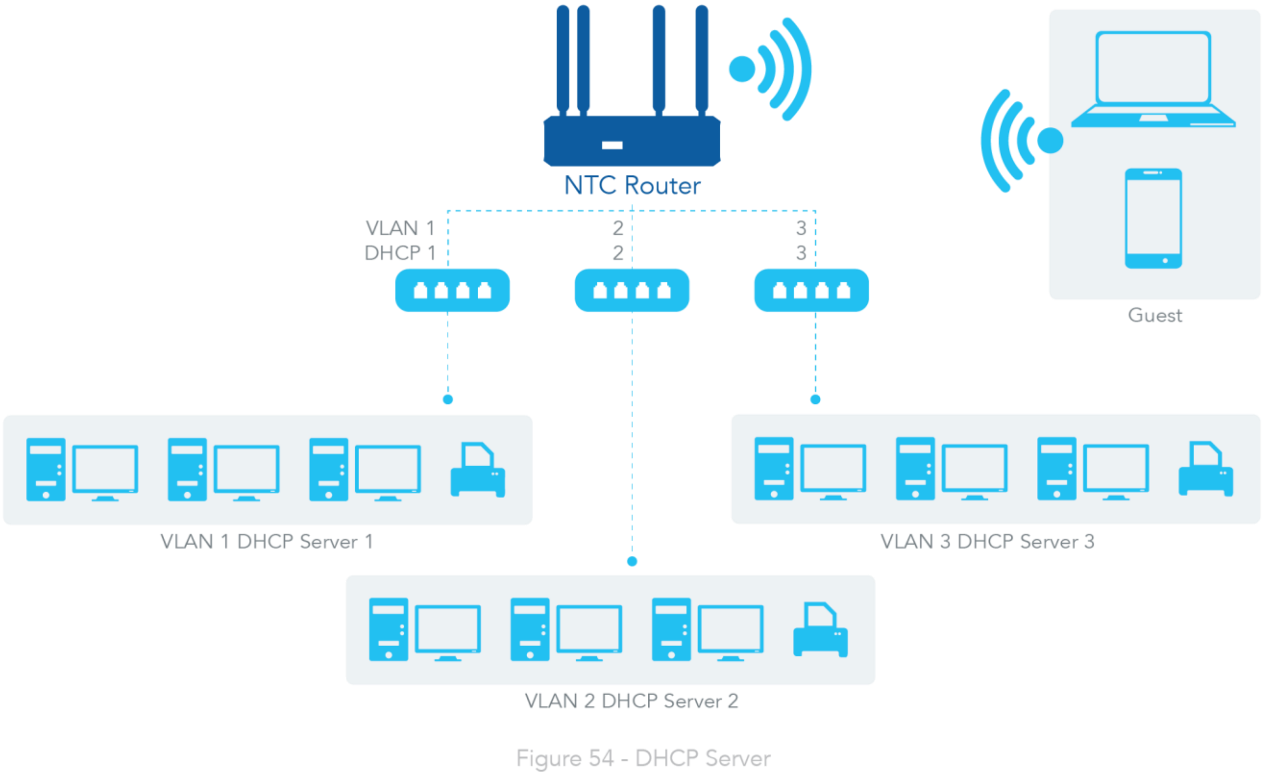
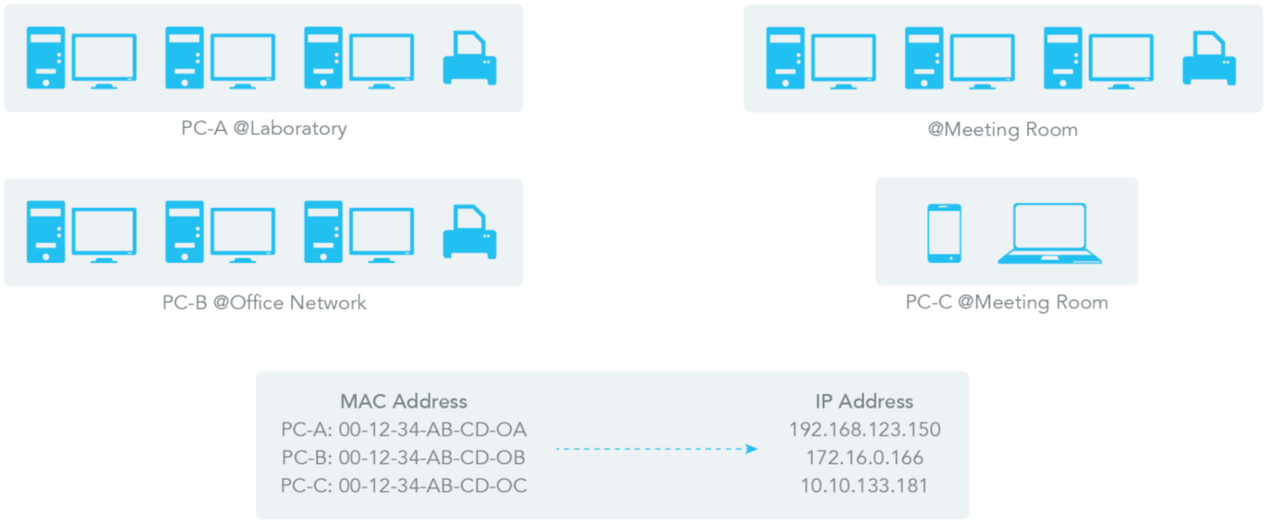


Figure 89 – DHCP Server

3.2.3.2 Fixed Mapping

When there are entries in the DHCP Client List, you can assign a fixed IP address to map the specific MAC addresses by selecting them and then selecting “Copy”. You can also do this manually if you know the MAC address of the devices.



MAC Address	IP Address
PC-A: 00-12-34-AB-CD-OA	192.168.123.150
PC-B: 00-12-34-AB-CD-OB	172.16.0.166
PC-C: 00-12-34-AB-CD-OC	10.10.133.181

Figure 90 – Fixed Mapping

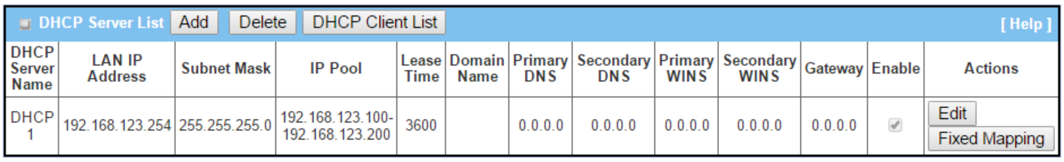
3.2.3.3 DHCP Server Setting

Navigate to the **Basic Network > LAN & VLAN > DHCP Server** tab**.**

The DHCP Server setting allows you to create and customize DHCP Server policies to assign IP Addresses to the devices on the local area network (LAN).

3.2.3.4 Create / Edit DHCP Server Policy

The gateway allows you to custom your DHCP Server Policy. If multiple LAN ports are available, you can define one policy for each LAN (or VLAN group), and it supports up to a maximum of 4 policy sets.

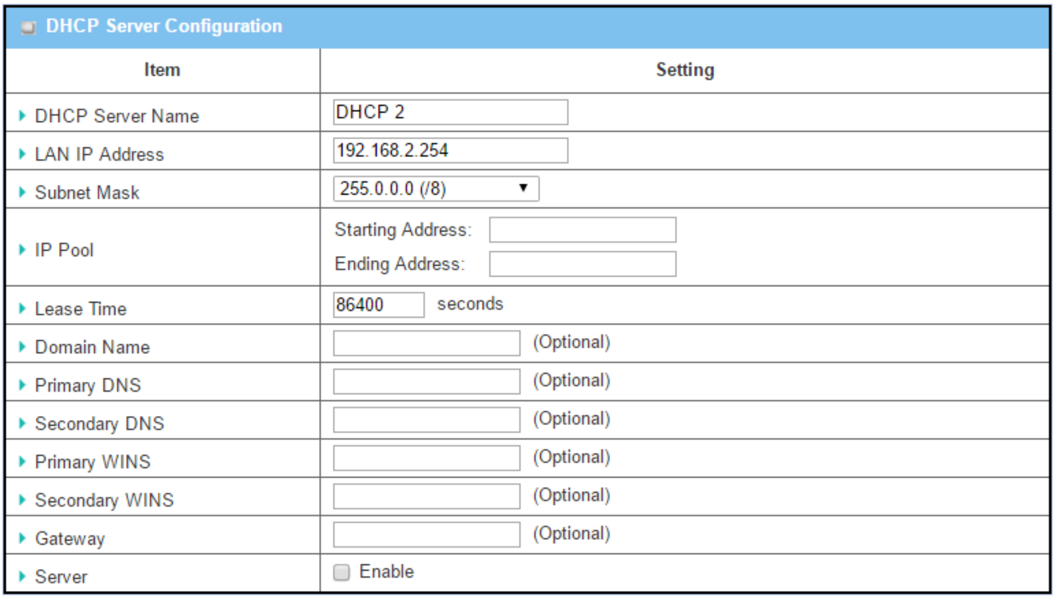


DHCP Server List | Add | Delete | DHCP Client List | [Help]

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	192.168.123.254	255.255.255.0	192.168.123.100- 192.168.123.200	3600		0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	☑	Edit Fixed Mapping

Figure 91 – Create/Edit DHCP Server Policy

Click the **Add** button to display the **DHCP Server Configuration** screen.



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

Figure 92 – DHCP Server Configuration

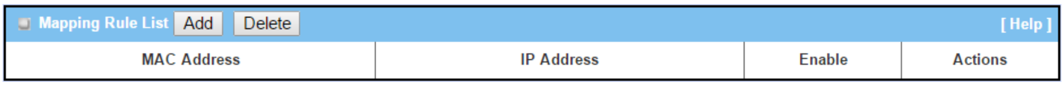
Item	Notes	Description
DHCP Server Name	Mandatory field. String format.	Enter a meaningful DHCP Server name.
LAN IP Address	Mandatory field. IPv4 format.	The LAN IP Address of this DHCP Server.
Subnet Mask	Default setting: **255.0.0.0 (/8)**	The Subnet Mask of this DHCP Server.
IP Pool	Mandatory field. IPv4 format.	The IP Pool of this DHCP Server. It composed of Starting Address entered in this field and Ending Address entered in this field.
Lease Time	Mandatory field. Integer format.	The Lease Time of this DHCP Server. Value Range: 300 - 604800 seconds
Domain Name	String format.	The Domain Name of this DHCP Server.

Item	Notes	Description
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.
Gateway	IPv4 format	The Gateway of this DHCP Server.
Server	Disabled by default.	Check ☑ **Enable** to activate this DHCP Server.
Save	Button	Click the **Save** button to save the configuration
Undo	Button	Click the **Undo** button to restore what you just configured back to the previous setting.
Back	Button	When the **Back** button is clicked the screen will return to the DHCP Server Configuration page.

Table 56 – DHCP Server Configuration

3.2.3.5 Create / Edit Mapping Rule List on DHCP Server

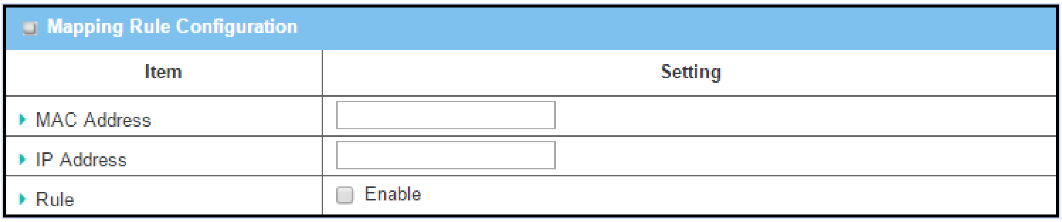
The router allows you to customize your Mapping Rule List on the DHCP Server. It supports up to a maximum of 64 rule sets. When the **Fix Mapping** button is applied, the **Mapping Rule List** screen appears.



MAC Address	IP Address	Enable	Actions

Figure 93 – Create / Edit Mapping Rule List on DHCP Server

Click the **Add** button to display the **Mapping Rule Configuration** screen.


Mapping Rule Configuration

Item	Setting
MAC Address	
IP Address	
Rule	□ Enable

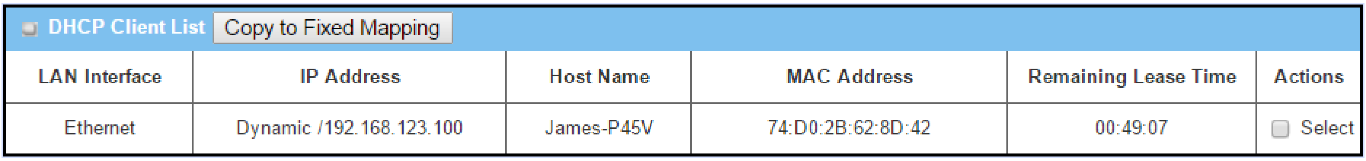
Figure 94 – Mapping Rule Configuration

Item	Notes	Description
MAC Address	Mandatory field. MAC Address string format.	The MAC Address of this mapping rule.
IP Address	Mandatory field. IPv4 format.	The IP Address of this mapping rule.
Rule	Disabled by default.	Check ☑ **Enable** to activate this rule.
Save	Button	Click the **Save** button to save the configuration
Undo	Button	Click the **Undo** button to restore what you just configured back to the previous setting.
Back	Button	When the **Back** button is clicked the screen will return to the DHCP Server Configuration page.

Table 57 – Mapping Rule Configuration

3.2.3.6 View / Copy DHCP Client List

When the **DHCP Client List** button is applied, the **DHCP Client List** screen appears.



DHCP Client List | Copy to Fixed Mapping

LAN Interface	IP Address	Host Name	MAC Address	Remaining Lease Time	Actions
Ethernet	Dynamic /192.168.123.100	James-P45V	74:D0:2B:62:8D:42	00:49:07	□ Select

Figure 95 – View/Copy DHCP Client List

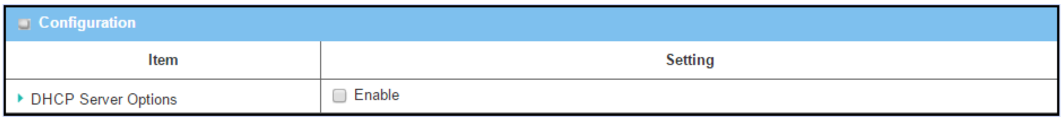
When the DHCP Client is selected and **Copy to Fixed Mapping** button is applied. The IP and MAC address of DHCP Client will apply to the Mapping Rule List on the specified DHCP Server automatically.

3.2.3.7 Enable / Disable DHCP Server Options

The **DHCP Server Options** setting allows you to set **DHCP OPTIONS 66**, **72**, or **114**. Click the **Enable** button to activate the DHCP option function and the DHCP Server will add the expected options in sending out DHCPOFFER DHCPACK packages.

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

Table 58 – Enable/Disable DCHCP Server Options



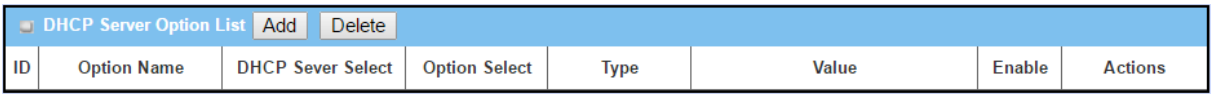
Configuration

Item	Setting
DHCP Server Options	□ Enable

Figure 96 – Enable/Disable DCHCP Server Options

3.2.3.8 Create / Edit DHCP Server Options

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

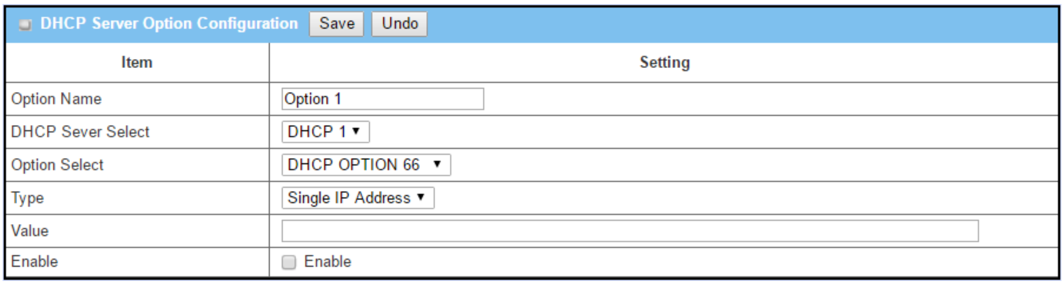


DHCP Server Option List | Add | Delete

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

Figure 97 – Create / Edit DHCP Server Options

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



DHCP Server Option Configuration | Save | Undo

Item	Setting
Option Name	Option 1
DHCP Sever Select	DHCP 1 ▾
Option Select	DHCP OPTION 66 ▾
Type	Single IP Address ▾
Value	
Enable	□ Enable

Figure 98 – DHCP Server Option Configuration

Item	Notes	Description
Option Name	Mandatory field. String format.	Enter a DHCP Server Option name that is meaningful to you.

Item	Notes	Description
DHCP Server Select	Dropdown list of all available DHCP servers.	Choose the DHCP server this option should apply to.
Option Select	Mandatory field. Default setting: Option 66	Choose the specific option from the dropdown list: **Option 66**, **Option 72** or **Option 144** **Option 66** for **tftp** **Option 72** for **www** **Option 144** for **url**
Type	Dropdown list of the type of DHCP server option values.	Each option has different value settings. **66** | Single IP Address **72** | Single FQDN **114** | IP Addresses List, separated by ","
Value	Mandatory field. Must contain data in the following formats: • IPv4 format • FQDN format • IP list • URL format	Should conform to type: | Type | Value **66** | Single IP Address | IPv4 format **72** | Single FQDN | FQDN format **114** | Single URL | URL format
Enable	Disabled by default.	Check ☑ **Enable** to activate thés setting.
Save	Button	Click the **Save** button to save the setting.
Undo	Button	When the **Undo** button is clicked the screen will return back with nothing changed.

Table 59 – DHCP Server Option Configuration

3.3 Wi-Fi

The router provides an IEEE 802.11ac/n/g/b Wi-Fi interface with dual band (2.4GHz/5GHz) operation for mobile wireless devices to connect for Internet/Intranet access. There are several wireless operation modes provided by this device. They are: “**AP Router Mode**”, “**WDS Only Mode**”, and “**WDS Hybrid Mode**”. You can choose the expected mode from the wireless operation mode list.

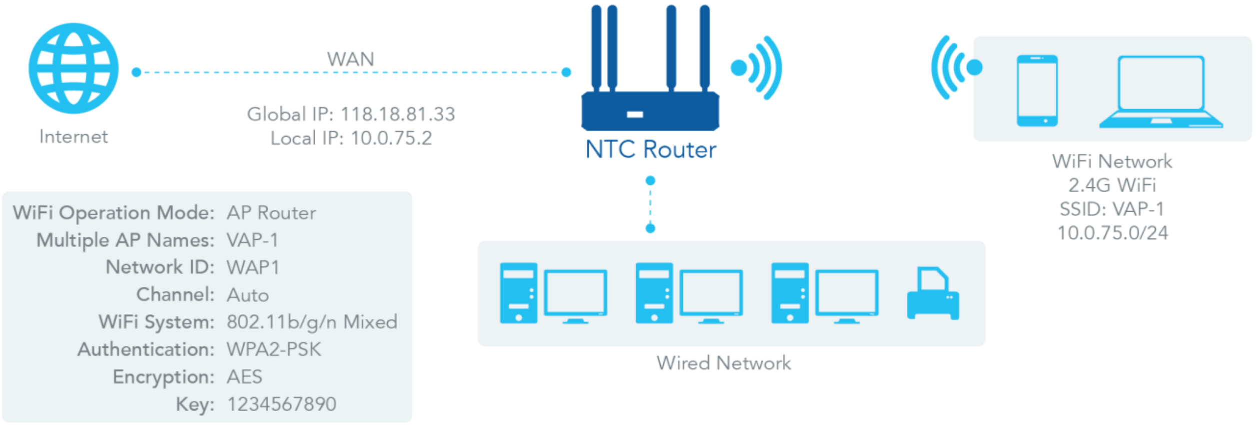
There are some sub-sections for you to configure the Wi-Fi function, including “Basic Configuration” and “Advanced Configuration”. In the Basic Configuration section, you are required to complete most of the settings to use the Wi-Fi function and the Advanced Configuration section provides more parameters for advanced users to fine tune the connectivity performance of the Wi-Fi function.

3.3.1 Wi-Fi Configuration

Below are the scenarios for each wireless operation mode.

3.3.1.1 AP Router Mode

This mode allows you to get your wired and wireless devices connected to the Internet using Network Address Translation (NAT). The router behaves as both a Wi-Fi AP (Access Point) and a Wi-Fi hotspot to provide Internet access. This means local Wi-Fi clients can connect to it and access the Internet through it without the need to obtain a public IP address from the ISP.



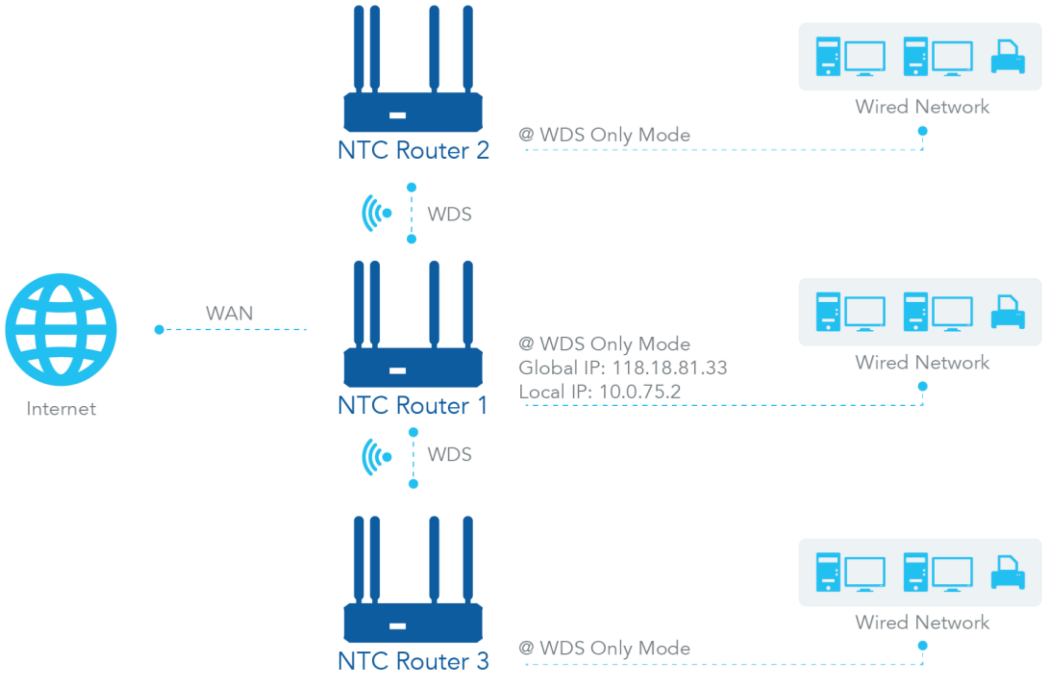
WiFi Operation Mode: AP Router
Multiple AP Names: VAP-1
Network ID: WAP1
Channel: Auto
WiFi System: 802.11b/g/n Mixed
Authentication: WPA2-PSK
Encryption: AES
Key: 1234567890

Figure 99 – Wi-Fi Configuration - AP Router Mode

3.3.1.2 WDS Only Mode

WDS (Wireless Distributed System) Only mode configures the router to act as a bridge for its wired Intranet and a repeater to extend wireless reach. You can use multiple Wi-Fi routers as Wi-Fi repeaters in a chain setup in "WDS Only" mode. All gateways can communicate with each other through Wi-Fi. All wired client hosts behind each router can also communicate with each other in this scenario. Only one router within the repeater chain can be the DHCP server to provide IP addresses for all the wired client hosts of the other routers which should have their DHCP servers disabled. This router can be also be configured as a NAT router to provide internet access.

The diagram below illustrates that there are two wireless gateways (Wi-Fi Gateway 2 and Wi-Fi Gateway 3) running in "WDS Only" mode. They both use channel 3 to link to local Gateway 1 through WDS. Both gateways connected by WDS need to know the remote AP MAC of the other. All client hosts under gateway 2 and 3 can request IP addresses from the DHCP server of gateway 1. Wireless Gateway 1 also executes the NAT mechanism for all client hosts accessing the Internet.



Global IP: 118.18.81.33
Local IP: 10.0.75.2

Router 2 & 3 Settings:
[Configuration]-[WiFi Configuration]
WiFi Operation Mode: WDS Only
Channel: 3
Authentication: WPA2-PSK
Encryption: AES
Key: 1234567890

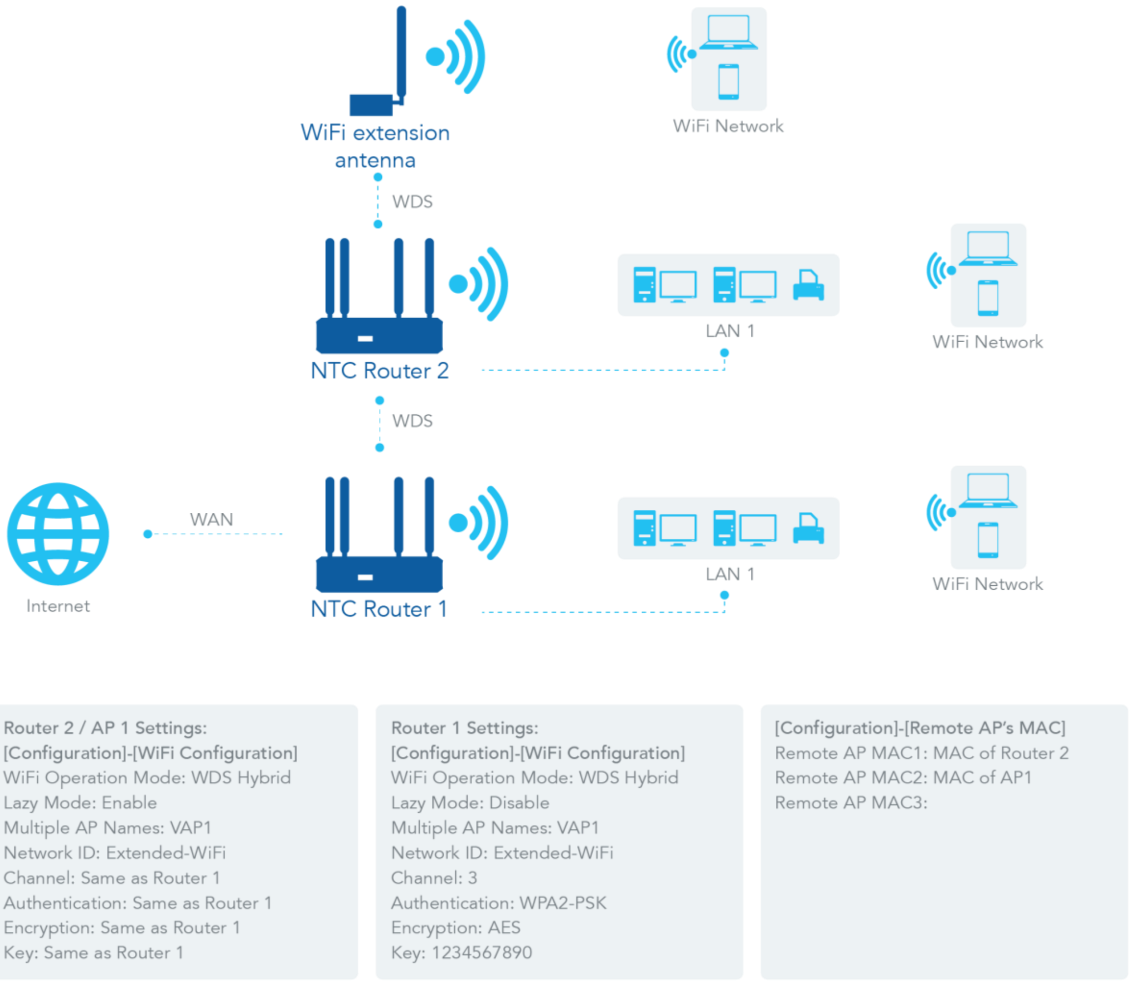
Router 1 Settings:
[Configuration]-[WiFi Configuration]
WiFi Operation Mode: WDS Only
Lazy Mode: Disable
Authentication: WPA2-PSK
Encryption: AES
Key: 1234567890

[Configuration]-[Remote AP's MAC]
Remote AP MAC1: MAC of Router 2
Remote AP MAC2: MAC of Router 3
Remote AP MAC3:

Figure 100 – Wi-Fi Configuration - WDS Only Mode

3.3.1.3 WDS Hybrid Mode

WDS Hybrid mode includes both WDS and AP Router mode. WDS Hybrid mode can act as an access point for its Wi-Fi Intranet and a Wi-Fi bridge for its wired and Wi-Fi Intranets at the same time. This mode allows you to build up a large wireless network in a large space like airports, hotels or school campus.



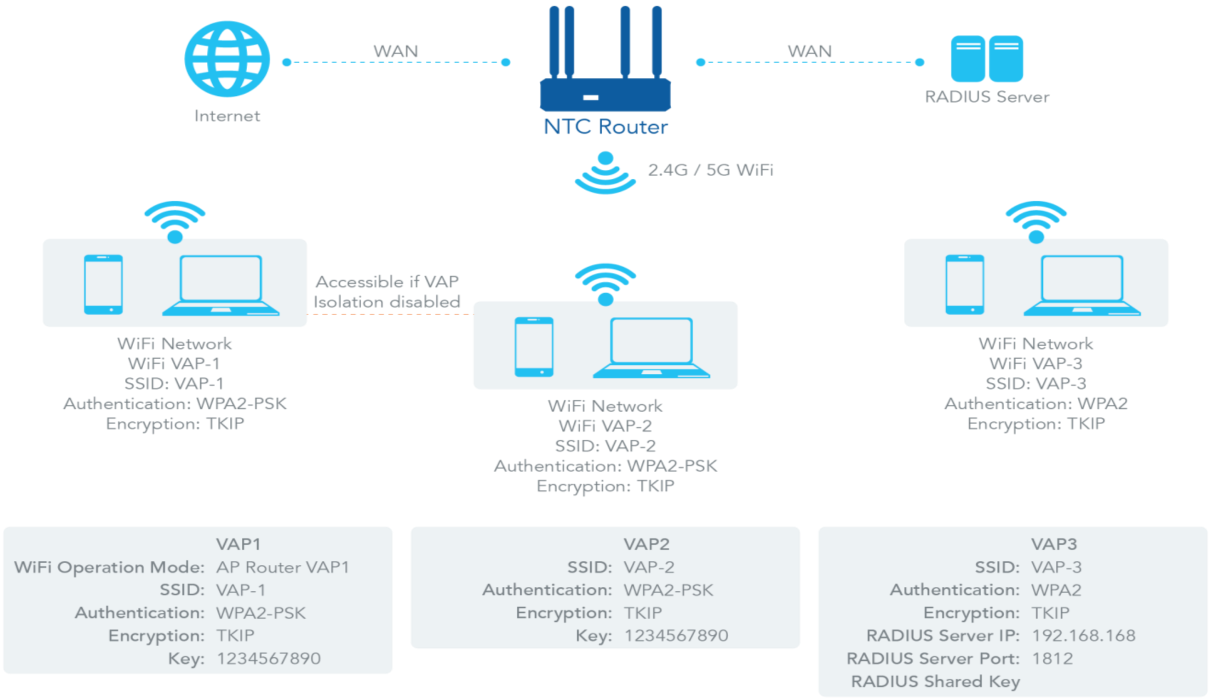
Router 2 / AP 1 Settings:
[Configuration]-[WiFi Configuration]
WiFi Operation Mode: WDS Hybrid
Lazy Mode: Enable
Multiple AP Names: VAP1
Network ID: Extended-WiFi
Channel: Same as Router 1
Authentication: Same as Router 1
Encryption: Same as Router 1
Key: Same as Router 1

Router 1 Settings:
[Configuration]-[WiFi Configuration]
WiFi Operation Mode: WDS Hybrid
Lazy Mode: Disable
Multiple AP Names: VAP1
Network ID: Extended-WiFi
Channel: 3
Authentication: WPA2-PSK
Encryption: AES
Key: 1234567890

[Configuration]-[Remote AP's MAC]
Remote AP MAC1: MAC of Router 2
Remote AP MAC2: MAC of AP1
Remote AP MAC3:

Figure 101 – Wi-Fi Configuration - WDS Hybrid Mode

The diagram above illustrates Gateway 1, Gateway 2 and AP 1 connected by WDS. Each gateway has access point functionality for Wi-Fi client access. Gateway 1 has a DHCP server to assign IP addresses to each of the client hosts. All gateways and AP are running in WDS hybrid mode. To setup WDS hybrid mode, you must fill all configuration items similar to that of AP-router and WDS modes.



VAP1

WiFi Operation Mode: AP Router VAP1
SSID: VAP-1
Authentication: WPA2-PSK
Encryption: TKIP
Key: 1234567890

VAP2

SSID: VAP-2
Authentication: WPA2-PSK
Encryption: TKIP
Key: 1234567890

VAP3

SSID: VAP-3
Authentication: WPA2
Encryption: TKIP
RADIUS Server IP: 192.168.168
RADIUS Server Port: 1812
RADIUS Shared Key

Figure 102 – Wi-Fi Configuration - Multiple VAPs

3.3.1.4 Multiple VAPs

VAP (Virtual Access Point) is a function that allows the partitioning of a wireless network into multiple broadcast domains. It can simulate multiple APs on one physical AP. The wireless router supports up to 8 VAPs. For each VAP, you need to setup an SSID, authentication and encryption to control Wi-Fi client access.

There is also a VAP isolation option to manage the access among VAPs. You can allow or block communication for the wireless clients connected to different VAPs.

3.3.1.5 Wi-Fi Security - Authentication & Encryption

Wi-Fi security provides complete authentication and encryption mechanisms to enhance data security while your data is transferred wirelessly. The wireless router supports Shared, WPA-PSK / WPA2-PSK and WPA / WPA2 authentication. You can select one authentication scheme to validate the wireless clients while they are connected to the AP. For data encryption, the router supports WEP, TKIP and AES. The selected encryption algorithm will be applied to the data while the wireless connection is established.

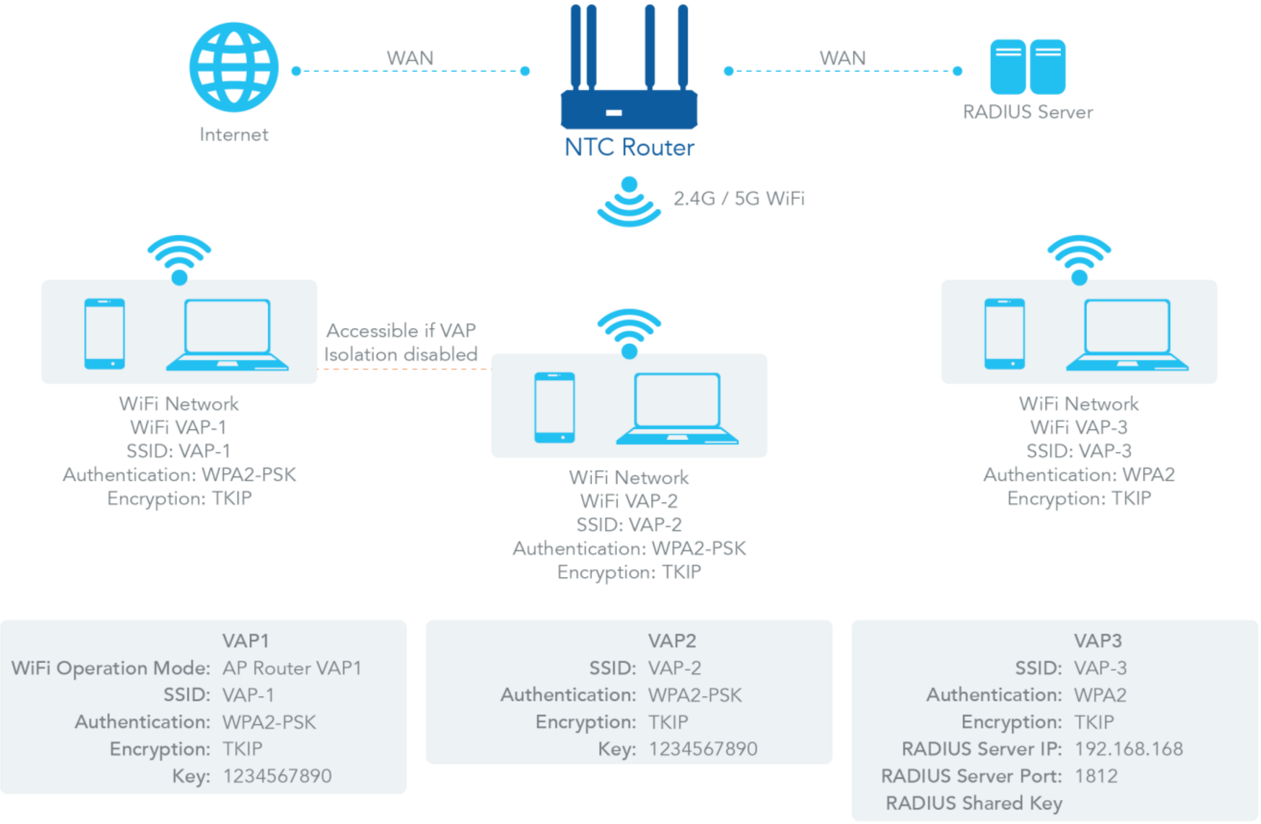


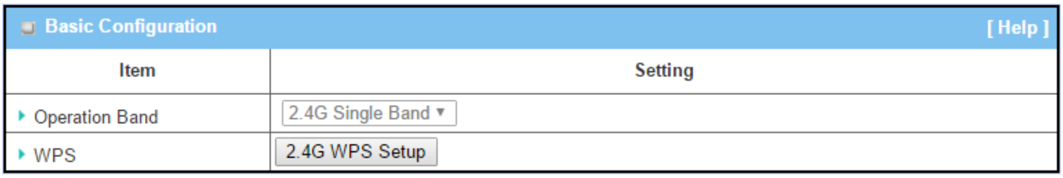
Figure 103 – Wi-Fi Configuration – Wi-Fi Security - Authentication and Encryption

3.3.1.6 Wi-Fi Configuration Setting

The Wi-Fi configuration allows you to configure 2.4GHz and 5GHz Wi-Fi settings.

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

3.3.1.7 Basic Configuration



Basic Configuration [Help]

Item	Setting
Operation Band	2.4G Single Band ▾
WPS	2.4G WPS Setup

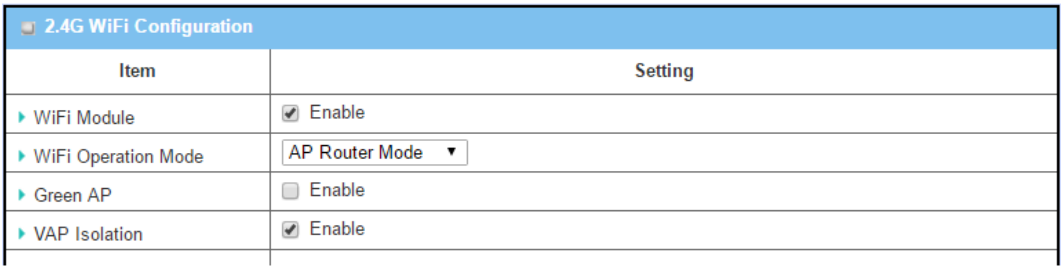
Figure 104 – Wi-Fi Configuration Setting - Basic Configuration

Item	Notes	Description
Operation Band	A mandatory setting	Specifies the intended operation band for the Wi-Fi module.

Item	Notes	Description
WPS	N/A	Pressing the **2.4G** or **5G** button directs you to the Wi-Fi Protected Setup page.

Table 60 – Wi-Fi Configuration Setting - Basic Configuration

3.3.1.8 Configure Wi-Fi Setting



2.4G WiFi Configuration

Item	Setting
WiFi Module	☑ Enable
WiFi Operation Mode	AP Router Mode ▾
Green AP	□ Enable
VAP Isolation	☑ Enable

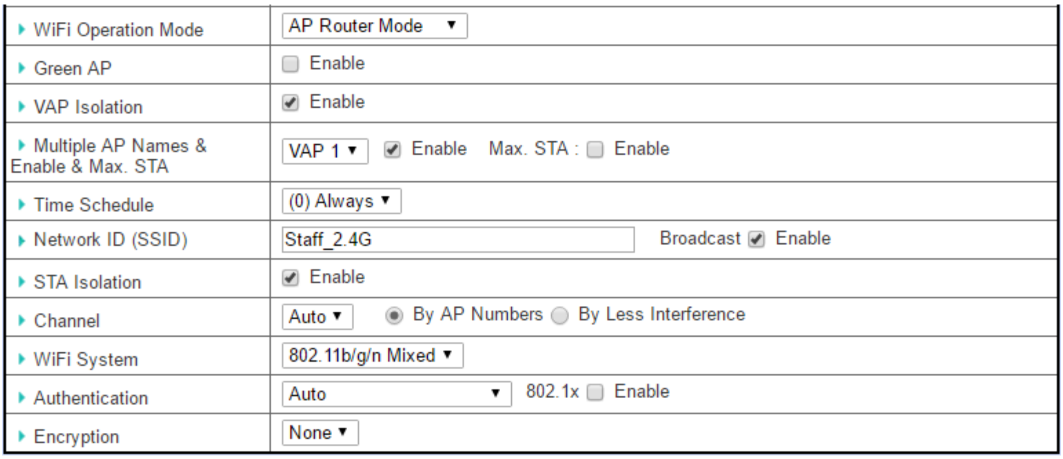
Figure 105 – Wi-Fi Configuration Setting - 2.4G/5G Wi-Fi Configuration

Item	Notes	Description
Wi-Fi Module	Enabled by default.	Check the Enable box to activate the Wi-Fi function.
Wi-Fi Operation Mode		Specify the Wi-Fi Operation Mode according to your application. Refer to the following table for AP Router Mode, WDS Only Mode, WDS Hybrid Mode, Universal Repeater Mode, AP Only Mode, and Client Mode settings.

Table 61 – Wi-Fi Configuration Setting - 2.4G/5G Wi-Fi Configuration

3.3.1.9 AP Router Mode

In AP Router mode, the device not only supports the connection of other stations but also the router function. The **WAN** port and the **NAT** function are **enabled**.



WiFi Operation Mode	AP Router Mode ▾
Green AP	□ Enable
VAP Isolation	☑ Enable
Multiple AP Names & Enable & Max. STA	VAP 1 ▾ ☑ Enable Max. STA : □ Enable
Time Schedule	(0) Always ▾
Network ID (SSID)	Staff_2.4G Broadcast ☑ Enable
STA Isolation	☑ Enable
Channel	Auto ▾ ● By AP Numbers ○ By Less Interference
WiFi System	802.11b/g/n Mixed ▾
Authentication	Auto ▾ 802.1x □ Enable
Encryption	None ▾

Figure 106 – AP Router Mode

Item	Notes	Description
Green AP	Disabled by default.	Check the Enable box to activate the Green AP function. Green AP attempts to optimise wireless throughput and power consumption.
VAP Isolation	Enabled by default.	Check the Enable box to activate this function.

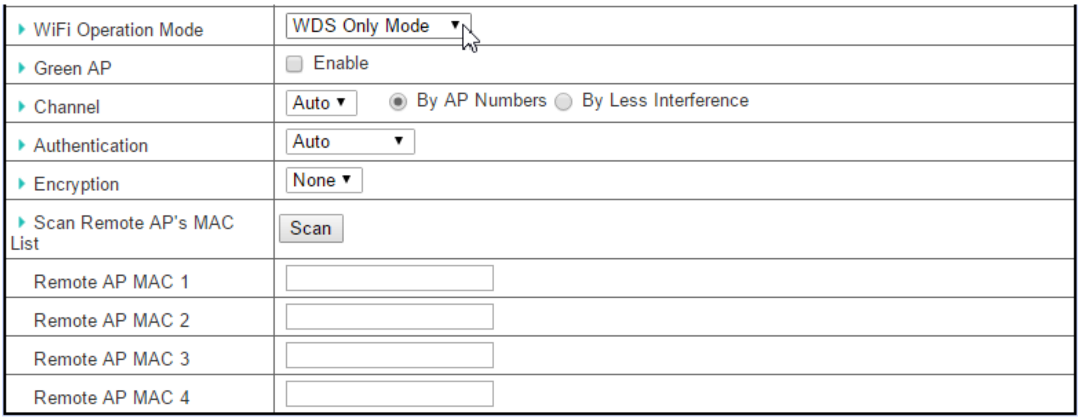
Item	Notes	Description
		By default, the box is checked; it means that stations which are associated to different VAPs cannot communicate with each other.
Multiple AP Names	Mandatory field. VAP1 and VAP8 are activated by default.	**Multiple AP Names (VAP)** - Multiple SSID feature and the device support up to 8 virtual SSIDs. Select one VAP to configure its setting. **Enable -** Check the enable box to activate the selected VAP. **Max. STA -** Limit the maximum number of client stations. Check this box and enter a limitation. The box is unchecked (unlimited) by default.
Time Schedule	Mandatory field.	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 the **Object Definition > Scheduling > Configuration** tab.
Network ID (SSID)	String format. Enabled by default.	Enter the SSID for the VAP, and decide whether to broadcast the SSID or not. The SSID is used for identifying the wireless network from another AP, and client stations will associate with the AP according to the SSID. If the broadcast SSID option is enabled, it means the SSID will be broadcasted, and the stations can associate with this device by scanning for available SSIDs.
STA Isolation	Enabled by default.	Check the Enable box to activate this function. The default setting does not allow stations which are associated to the same VAP to communicate with each other.
Channel	Mandatory field. Default setting: **Auto**	Select a radio channel for the VAP. Each channel corresponds to a different radio band. The permissible channels depend on the Regulatory Domain. There are two available options when Auto is selected: By AP Numbers - The channel will be selected according to AP numbers (lower channels are better). By Interference - The channel will be selected according to interference. (lower interference is better).
Wi-Fi System	Mandatory field.	Specify the preferred Wi-Fi System. The dropdown list of the Wi-Fi system is based on IEEE 802.11 standard. 2.4G Wi-Fi can use b, g and n only or mixed with each other. 5G Wi-Fi can select a, n and ac only or mixed with each other.
Authentication	Mandatory field. Default setting: **Auto**	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 (Disabled by default.) - When 802.1x is enabled, the client stations will be authenticated by a 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 the client automatically.

Item	Notes	Description
		The check box named 802.1x shows up next to the dropdown list. 802.1x (Disabled by default.) - When 802.1x is enabled, 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. WPA and WPA2 are implementations 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, the client stations can associate with this device via WPA or WPA2.
		When WPA-PSK or WPA2-PSK is selected, the authentication uses pre-shared keys instead of RADIUS server.
		When WPA-PSK / WPA2-PSK is selected, the client stations can associate with this device via WPA-PSK or WPA2-PSK.
Encryption	Mandatory field. Default setting: **None**	Select the desired encryption method and enter the required key(s). The available method in the dropdown list depends on the Authentication you selected. **None** – the device is open with no encryption. **WEP** - Up to 4 WEP keys can be set and you have to 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** - TKIP was proposed instead of WEP without upgrading hardware. Enter a Pre-shared Key for it. The length of the key is from 8 to 63 characters. **AES** - The newest encryption system in Wi-Fi. This is also designed for the fast 802.11n high bitrates schemes. Enter a Pre-Shared Key. The length of the key is from 8 to 63 characters. We recommend that you use AES encryption for security as it is the most secure. **TKIP / AES** - TKIP / AES mixed mode. Client stations can associate with this device via TKIP or AES. Enter a Pre-Shared Key. The length of the key is from 8 to 63 characters.
Save	Button	Click the **Save** button to save the current configuration.
Undo	Button	Click the **Undo** button to restore configuration to previous setting before saving.
Apply	Button	Click the **Apply** button to apply the saved configuration.

Table 62 – AP Router Mode

3.3.1.10 WDS Only Mode

In WDS Only mode, the device only bridges the connected wired clients to other WDS-enabled Wi-Fi devices that are associated with it.



WiFi Operation Mode	WDS Only Mode ▾
Green AP	□ Enable
Channel	Auto ▾ ● By AP Numbers ○ By Less Interference
Authentication	Auto ▾
Encryption	None ▾
Scan Remote AP's MAC List	Scan
Remote AP MAC 1	
Remote AP MAC 2	
Remote AP MAC 3	
Remote AP MAC 4	

Figure 107 – WDS Only Mode

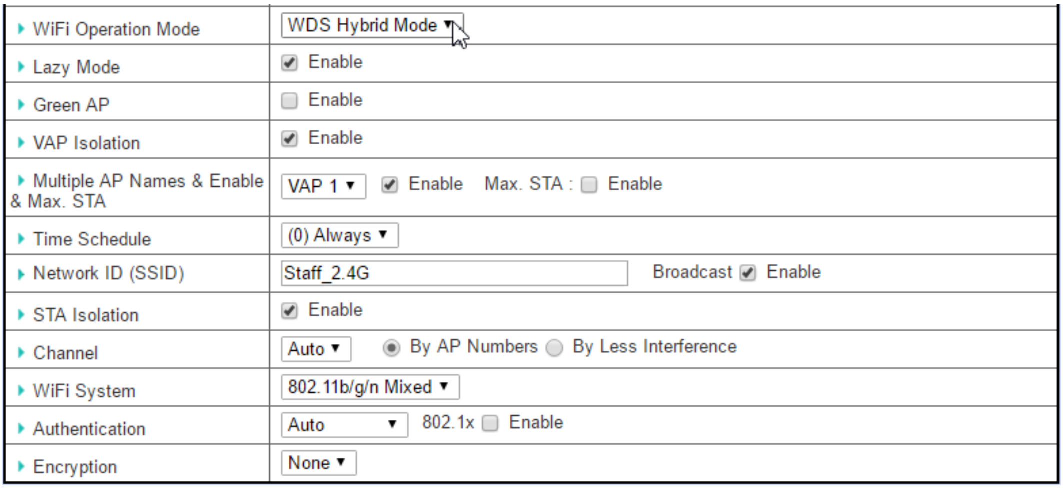
Item	Notes	Description
Green AP	Disabled by default.	Check ☑ Enable to activate the Green AP function. Green AP attempts to optimise wireless throughput and power consumption.
Channel	Mandatory field. Default setting: **Auto**	Select a radio channel for the VAP. Each channel corresponds to a different radio band. The permissible channels depend on the Regulatory Domain. There are two available options when Auto is selected: **By AP Numbers** - The channel will be selected according to AP numbers (lower channels are better). **By Interference** - The channel will be selected according to interference. (lower interference is better).
Authentication	Mandatory field. Default setting: **Auto**	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 (Disabled by default.) - When 802.1x is enabled, the client stations will be authenticated by a 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 the client automatically. The check box named 802.1x shows up next to the dropdown list. 802.1x (Disabled by default.) - When 802.1x is enabled, the client stations will be authenticated by RADIUS server. RADIUS Server IP (The default IP is 0.0.0.0)

Item	Notes	Description
		RADIUS Server Port (The default value is 1812) RADIUS Shared Key
		When WPA-PSK is selected, the authentication uses pre-shared key instead of RADIUS server.
		When WPA2-PSK is selected, the authentication uses pre-shared key instead of RADIUS server.
Encryption	Mandatory field. Default setting: **None**	Select the desired encryption method and enter the required key(s). The available method in the dropdown list depends on the Authentication you selected. **None** – the device is open with no encryption. **WEP** - Up to 4 WEP keys can be set and you have to 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** - TKIP was proposed instead of WEP without upgrading hardware. Enter a Pre-shared Key for it. The length of the key is from 8 to 63 characters. **AES** - The newest encryption system in Wi-Fi. This is also designed for the fast 802.11n high bitrates schemes. Enter a Pre-Shared Key. The length of the key is from 8 to 63 characters. We recommend that you use AES encryption for security as it is the most secure. **TKIP / AES** - TKIP / AES mixed mode. Client stations can associate with this device via TKIP or AES. Enter a Pre-Shared Key. The length of the key is from 8 to 63 characters.
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 the selected AP will be automatically entered in the following Remote AP MAC table.
Remote AP MAC 1 - 4	Mandatory field.	Enter the remote AP's MAC manually or via auto-scan. The device will bridge the traffic to the remote AP when associated successfully.
Save	Button	Click the **Save** button to save the current configuration.
Undo	Button	Click the **Undo** button to restore configuration to previous setting before saving.
Apply	Button	Click the **Apply** button to apply the saved configuration.

Table 63 – WDS Only Mode

3.3.1.11 WDS Hybrid Mode

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



WiFi Operation Mode	WDS Hybrid Mode ▾
Lazy Mode	☑ Enable
Green AP	□ Enable
VAP Isolation	☑ Enable
Multiple AP Names & Enable & Max. STA	VAP 1 ▾ ☑ Enable Max. STA : □ Enable
Time Schedule	(0) Always ▾
Network ID (SSID)	Staff_2.4G Broadcast ☑ Enable
STA Isolation	☑ Enable
Channel	Auto ▾ ● By AP Numbers ○ By Less Interference
WiFi System	802.11b/g/n Mixed ▾
Authentication	Auto ▾ 802.1x □ Enable
Encryption	None ▾

Figure 108 – WDS Hybrid Mode

Item	Notes	Description
Lazy Mode	Enabled by default.	Check ☑ **Enable** to activate this function. With this function enabled, the device can automatically learn of WDS peers without manually entering other AP's MAC address, but at least one of the APs has to fill the remote AP MAC addresses.
Green AP	Disabled by default.	Check ☑ **Enable** to activate the Green AP function. Green AP attempts to optimise wireless throughput and power consumption.
VAP Isolation	Enabled by default.	Check ☑ **Enable** to activate this function. By default, the box is checked; it means that stations which are associated to different VAPs cannot communicate with each other.
Multiple AP Names	Mandatory field. VAP1 and VAP8 are activated by default.	Multiple AP Names (VAP) - The device supports up to 8 virtual SSIDs. Select one of VAP to configure its setting at a time. Enable - Check the enable box to activate the selected VAP. Max. STA - Limit the maximum number of client stations. Check this box and enter a limitation. The box is unchecked (unlimited) by default.
Time Schedule	Mandatory field.	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.
Network ID (SSID)	String format Enabled by default.	Enter the SSID for the VAP, and decide whether to broadcast the SSID or not. The SSID is used for identifying the wireless network from another AP, and client stations will associate with the AP according to the SSID. If the broadcast SSID option is enabled, it means the SSID will be broadcasted, and the stations can associate with this device by scanning for available SSIDs.
STA Isolation	Enabled by default.	Check ☑ **Enable** to activate this function. The default setting does not allow stations which are associated to the same VAP to communicate with each other.
Channel	Mandatory field. Default setting: **Auto**	Select a radio channel for the VAP. Each channel corresponds to a different radio band. The permissible channels depend on the Regulatory Domain. There are two available options when Auto is selected:

Item	Notes	Description
		By AP Numbers - The channel will be selected according to AP numbers (lower channels are better). By Interference - The channel will be selected according to interference. (lower interference is better).
Wi-Fi System	Mandatory field.	Specify the preferred Wi-Fi System. The dropdown list of the Wi-Fi system is based on IEEE 802.11 standard. 2.4G Wi-Fi can use b, g and n only or mixed with each other. 5G Wi-Fi can select a, n and ac only or mixed with each other.
Authentication	Mandatory field. Default setting: **Auto**	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 (Disabled by default.) - When 802.1x is enabled, the client stations will be authenticated by a 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 the client automatically. The check box named 802.1x shows up next to the dropdown list. 802.1x (Disabled by default.) - When 802.1x is enabled, 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-PSK is selected, the authentication uses pre-shared key instead of RADIUS server.
		When WPA2-PSK is selected, the authentication uses pre-shared key instead of RADIUS server.
Encryption	Mandatory field. Default setting: **None**	Select the desired encryption method and enter the required key(s). The available method in the dropdown list depends on the Authentication you selected. None - the device is open with no encryption. WEP - Up to 4 WEP keys can be set and you have to 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 - TKIP was proposed instead of WEP without upgrading hardware. Enter a Pre-shared Key for it. The length of the key is from 8 to 63 characters. AES - The newest encryption system in Wi-Fi. This is also designed for the fast 802.11n high bitrates schemes. Enter a Pre-Shared Key. The length of the key is from 8 to 63 characters. We recommend that you use AES encryption for security as it is the most secure.

Item	Notes	Description
		TKIP / AES - TKIP / AES mixed mode. Client stations can associate with this device via TKIP or AES. Enter a Pre-Shared Key. The length of the key is from 8 to 63 characters.
Save	Button	Click the **Save** button to save the current configuration.
Undo	Button	Click the **Undo** button to restore configuration to previous setting before saving.
Apply	Button	Click the **Apply** button to apply the saved configuration.

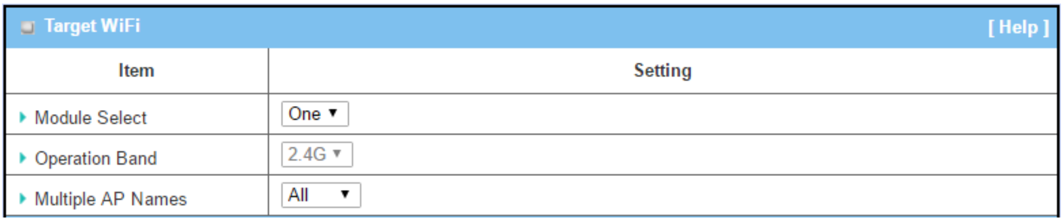
Table 64 – WDS Hybrid Mode

3.3.2 Wireless Client List

The **Wireless Client List** page shows the information of wireless clients which are associated with this device.

Go to **Basic Network > Wi-Fi > Wireless Client List** Tab.

3.3.2.1 Select Target Wi-Fi



Target WiFi [Help]

Item	Setting
Module Select	One ▾
Operation Band	2.4G ▾
Multiple AP Names	All ▾

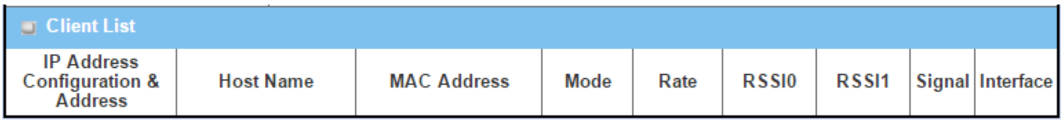
Figure 109 – Target Wi-Fi

Item	Notes	Description
Operation Band	(mandatory field)	Specify the intended operation band for the Wi-Fi module.
Multiple AP Names	Mandatory field. Default setting: **All**	Specify the VAP to show the associated clients information in the following Client List. By default, All VAPs are selected.

Figure 110 – Target Wi-Fi

3.3.2.2 Show Client List

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



Client List

IP Address Configuration & Address	Host Name	MAC Address	Mode	Rate	RSSI0	RSSI1	Signal	Interface

Figure 111 – Client List

Item	Description
IP Address Configuration & Address	It shows the Client's IP address and the method that it was obtained. 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 the client.
Host Name	Displays the host name of the client.
MAC Address	Displays the MAC address of the client.

Item	Description
Mode	Displays what kind of Wi-Fi system the client used to associate with this device.
Rate	Displays the data rate between client and this device.
RSSI0, RSSI1	Displays the RX sensitivity (RSSI) value for each radio path.
Signal	The signal strength between the client and this device.
Interface	Displays the VAP ID that the client associated with.
Refresh	Click the Refresh button to update the Client List immediately.

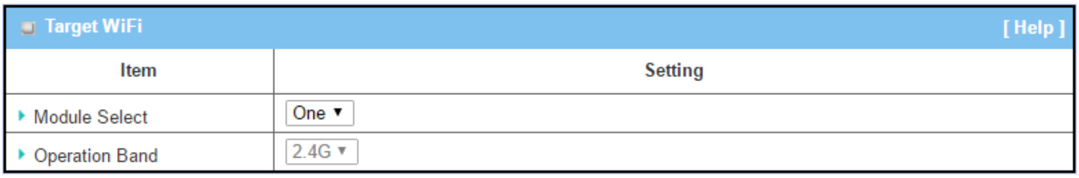
Table 65 – Client List

3.3.3 Advanced Configuration

The router provides advanced wireless configuration for advanced users to optimize the wireless performance under the specific installation environment. Please note that if you are not familiar with Wi-Fi technology, do not adjust the Advanced Configuration section or the connectivity and performance may be adversely affected with improper settings.

Navigate to the **Basic Network > Wi-Fi > Advanced Configuration** Tab.

3.3.3.1 Select Target Wi-Fi



Target WiFi [Help]

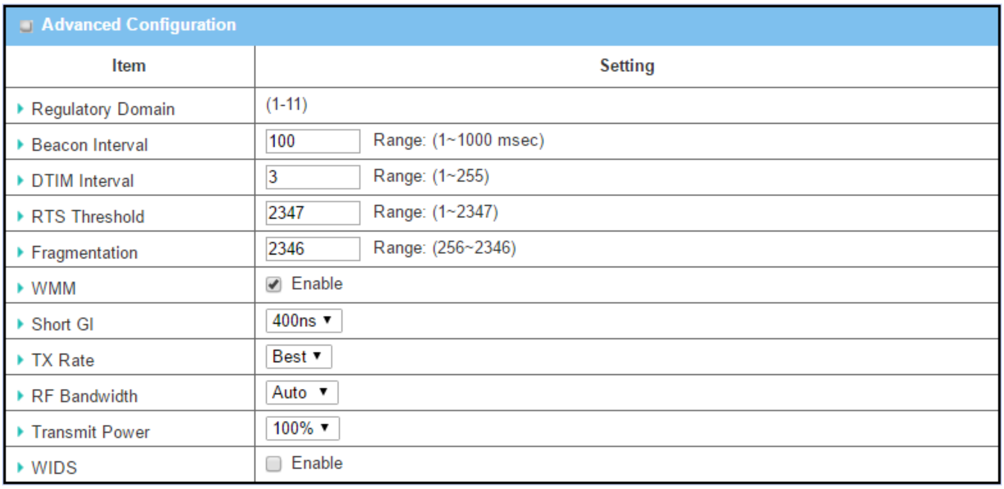
Item	Setting
Module Select	One ▾
Operation Band	2.4G ▾

Table 66 – Target Wi-Fi

Item	Notes	Description
Operation Band	Mandatory field.	Specify the intended operation band for the Wi-Fi module.

Table 67 – Target Wi-Fi

3.3.3.2 Setup Advanced Configuration



Advanced Configuration

Item	Setting
Regulatory Domain	(1-11)
Beacon Interval	100 Range: (1~1000 msec)
DTIM Interval	3 Range: (1~255)
RTS Threshold	2347 Range: (1~2347)
Fragmentation	2346 Range: (256~2346)
WMM	☑ Enable
Short GI	400ns ▾
TX Rate	Best ▾
RF Bandwidth	Auto ▾
Transmit Power	100% ▾
WIDS	□ Enable

Figure 112 – Advanced Configuration

Item	Notes	Description
Regulatory Domain	This value is determined by the region of sale.	This displays the range of available radio channels that may be used for Wi-Fi. The permissible channels depend on the Regulatory Domain.
Beacon Interval	100	Shows the time interval between each beacon packet broadcasted. The beacon packet contains the SSID, Channel ID and Security settings.
DTIM Interval	3	A DTIM (Delivery Traffic Indication Message) is a countdown informing clients of the next window for listening to the broadcast message. When the device has buffered the 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. If RTS is set to 2347, it is never activated.
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	Enabled by default.	WMM (Wi-Fi Multimedia) can help control latency and jitter when transmitting multimedia content over a wireless connection.
Short GI	Default setting: **400ns**	Short GI (Guard Interval) is defined to set the send interval between each packet. Note that a lower value could increase not only the transition rate but also the error rate.
TX Rate	Default setting: **Best**	The data transmission rate. When Best is selected, the device will choose an appropriate data rate according to the signal strength.
RF Bandwidth	Default setting: **Auto**	The setting of RF bandwidth limits the maximum data rate.
Transmit Power	Default setting: **100%**	Controls the transmission power of the wireless radio.
5G Band Steering	Disabled by default.	When a wireless client connects to the 2.4G Wi-Fi network, the router will send the client to the 5GHz network automatically if the client is capable of accessing it.
WIDS	Disabled by default.	The WIDS (Wireless Intrusion Detection System) will analyse all packets and log statistics in a table on the Wi-Fi status page.

Item	Notes	Description
		Navigate to the **Status > Basic Network > Wi-Fi** tab for detailed WIDS status.
Save	Button	Click the **Save** button to save the current configuration.
Undo	Button	Click the **Undo** button to restore configuration to previous setting before saving.

Table 68 – Advanced Configuration

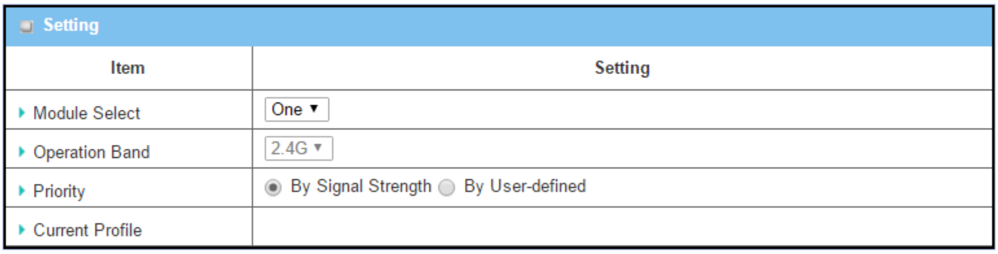
3.3.4 Uplink Profile

This device provides a Wi-Fi Uplink function for connecting to a wireless access point just like connecting to a wired WAN or cellular WAN connection. It can operate as a NAT gateway and link the devices wirelessly to the uplink network or hosts.

To connect to the wireless access point, you must enable the wireless Uplink function (refer to **Basic Network > WAN & Uplink > Physical Interface**, **Internet Setup** tabs) first, and then configure the Uplink profile(s) for the access point to be connected to in the **Uplink Profile** page.

Go to **Basic Network > Wi-Fi > Uplink Profile** tab to configure the Uplink Profile page.

3.3.4.1 Uplink Profile Setting



Setting

Item	Setting
Module Select	One ▾
Operation Band	2.4G ▾
Priority	● By Signal Strength ○ By User-defined
Current Profile	

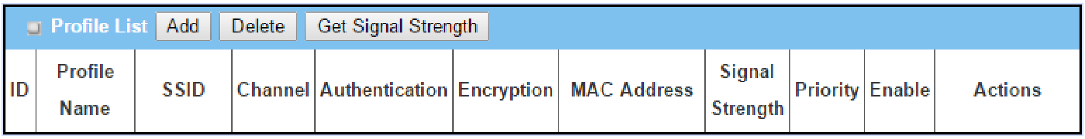
Figure 113 – Uplink Profile Setting

Item	Notes	Description
Operation Band	Mandatory field.	Specify the intended operation band for the Wi-Fi module
Priority	Mandatory field. Default setting: **By Signal Strength**	Specify the network selection methodology for connecting to an available wireless uplink network: **By Signal Strength** or **By User-defined priority** When **By Signal Strength** is selected, the router will try to connect to the available uplink network whose wireless signal strength is the strongest. When **By User-defined** is selected, the router will try to connect to the available uplink network whose priority is the highest (1 is the highest priority, and 16 is the lowest priority).

Table 69 – Uplink Profile Setting

Note – To apply the defined Uplink profile(s) for the router to find a best fit profile for connecting to a certain uplink network, you must **Enable** the Profile auto-connect function (Refer to **Basic Network > Wi-Fi > (Module 1/ Module 2) Wi-Fi Configuration** tab.

3.3.4.2 Create/Edit Uplink Profile

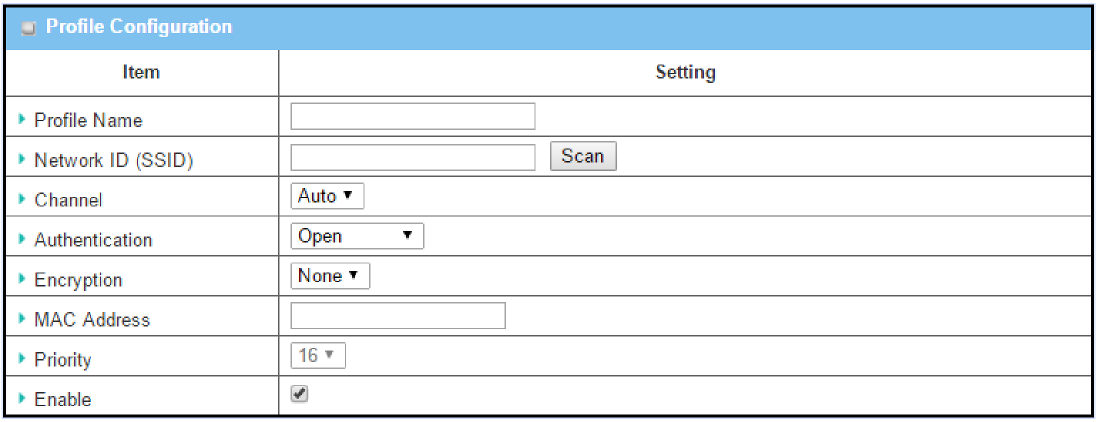


ID	Profile Name	SSID	Channel	Authentication	Encryption	MAC Address	Signal Strength	Priority	Enable	Actions

Figure 114 – Create/Edit Uplink Profile

The Profile List shows the settings for the created uplink profiles. The information includes Profile Name, SSID, Channel, Authentication, Encryption, MAC Address, Signal Strength, Priority, and Enable.

Click the **Add** button to display the **Profile Configuration** screen.



Profile Configuration

Item	Setting
Profile Name	
Network ID (SSID)	Scan
Channel	Auto ▾
Authentication	Open ▾
Encryption	None ▾
MAC Address	
Priority	16 ▾
Enable	☑

Figure 115 – Create/Edit Uplink Profile - Profile Configuration

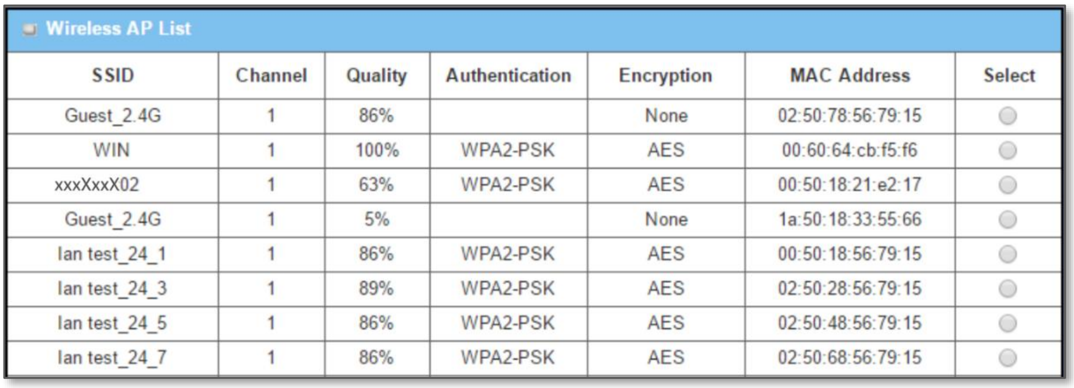
Item	Notes	Description
Profile Name	Mandatory field. String format. .	Enter a profile name for the uplink network specified below. This should be something that is memorable and meaningful. Value Range: 1 - 64 characters.
Network ID (SSID)	String format Enabled by default.	Enter the SSID for the VAP, and decide whether to broadcast the SSID or not. The SSID is used for identification from another AP and client stations will associate with the AP according to the SSID. If the broadcast SSID option is enabled, the SSID will be broadcasted, and the stations can associate with this device by scanning for available SSIDs.
Channel	Mandatory field. Default setting: **Auto**	Select a radio channel for the VAP. Each channel corresponds to different radio band. The permissible channels depend on the Regulatory Domain. There are two available options when Auto is selected: **By AP Numbers** – The channel will be selected according to AP numbers (lower values are better). **By Interference** – The channel will be selected according to interference level (lower values are better).
Authentication	Mandatory field. Default setting: **Open**	Specify the authentication method for connecting with the uplink network: **Open**, **Shared**, **WPA-SPK** or **WPA2-PSK**. When **Open** is selected, the preshared WEP key can be set for authentication; When **Shared** is selected, the preshared WEP key should be set for authentication; When **WPA-PSK or WPA2-PSK** is selected, the TKIP or AES preshared key should be set for authentication;
Encryption	Mandatory field. Default setting: **None**	Select the desired encryption method and enter the required key(s). The available method in the dropdown list depends on the Authentication you selected. **None** – the device is open with no encryption. **WEP** – Up to 4 WEP keys can be set and you have to 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.

Item	Notes	Description
		TKIP – TKIP was proposed instead of WEP without upgrading hardware. Enter a Pre-shared Key for it. The length of the key is from 8 to 63 characters. **AES** – The newest encryption system in Wi-Fi. This is also designed for the fast 802.11n high bitrates schemes. Enter a Pre-Shared Key. The length of the key is from 8 to 63 characters. We recommend that you use **AES** encryption for security as it is the most secure. **TKIP / AES - TKIP / AES** mixed mode – Client stations can associate with this device via TKIP or AES. Enter a Pre-Shared Key. The length of the key is from 8 to 63 characters.
MAC Address	Mandatory field. MAC Address string format.	Specify the MAC Address of the access point (with the Network ID) to connect to.
Priority	Optional field. Default setting: **16**	Specify a priority setting for the uplink profile when the By User-defined methodology is selected. The priority value can be **1 - 16**. 1 is the highest priority, and 16 is the lowest priority).
Enable	Enabled by default.	Click ☑ **Enable** to activate this profile.
Save	Button	Click the **Save** button to save the configuration.
Undo	Button	Click the **Undo** button to restore what you just configured back to the previous setting.
Back	Button	When the **Back** button is clicked, the screen will return to the Profile List page.

Table 70 – Create/Edit Uplink Profile - Profile Configuration

Instead of manually entering the information for the uplink network, you can also click the **Scan** button to get the available wireless networks around the device, and select one as the uplink network.

When the **Scan** button is applied, the **Wireless AP List** is displayed after a few seconds.



Wireless AP List

SSID	Channel	Quality	Authentication	Encryption	MAC Address	Select
Guest_2.4G	1	86%		None	02:50:78:56:79:15	○
WIN	1	100%	WPA2-PSK	AES	00:60:64:cb:f5:f6	○
xxxXxxX02	1	63%	WPA2-PSK	AES	00:50:18:21:e2:17	○
Guest_2.4G	1	5%		None	1a:50:18:33:55:66	○
lan test_24_1	1	86%	WPA2-PSK	AES	00:50:18:56:79:15	○
lan test_24_3	1	89%	WPA2-PSK	AES	02:50:28:56:79:15	○
lan test_24_5	1	86%	WPA2-PSK	AES	02:50:48:56:79:15	○
lan test_24_7	1	86%	WPA2-PSK	AES	02:50:68:56:79:15	○

Figure 116 – Wireless AP List

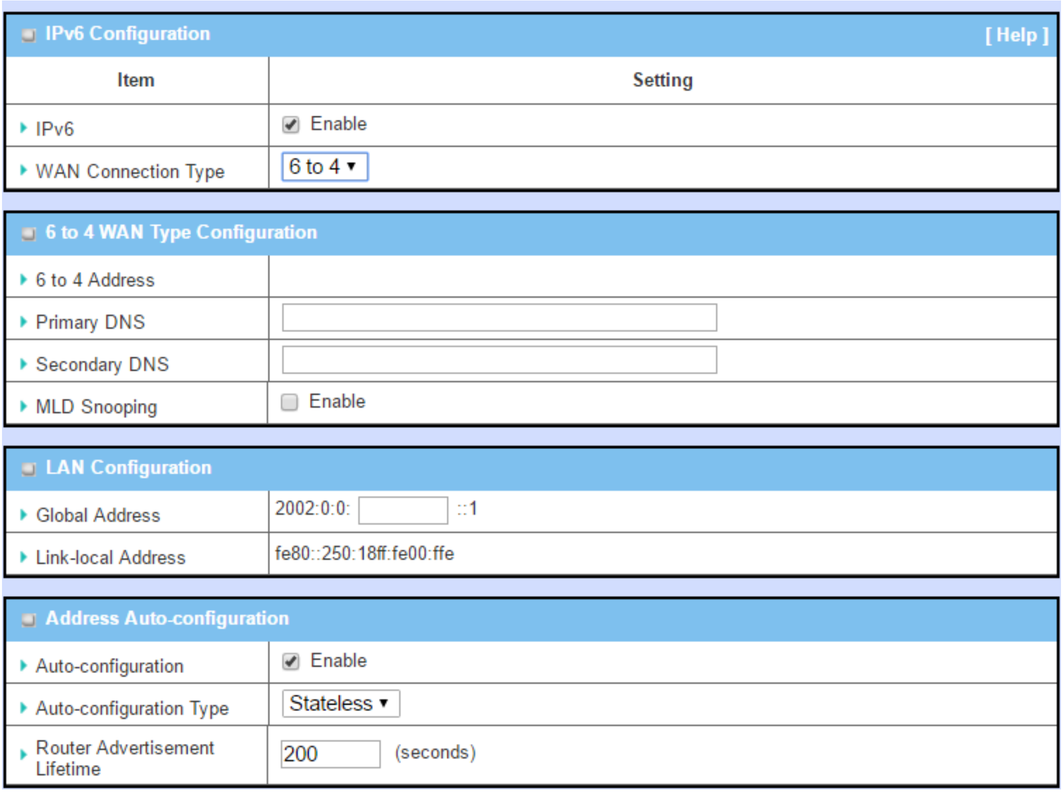
When you have selected an AP from the AP list, the **Channel**, **SSID**, **Authentication**, **Encryption**, and **MAC address** will be automatically completed in the profile. If required, you must enter a key for the uplink connection.

3.4 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, which is the protocol currently used to direct most Internet traffic. IPv6 also implements additional features not present in IPv4. It simplifies aspects of address assignment (stateless address auto-configuration), network renumbering and router announcements when changing Internet connectivity providers.

3.4.1 IPv6 Configuration

The **IPv6 Configuration** setting allows you to set the IPv6 connection type to access the IPv6 network. The router supports various types of IPv6 connection, including **Static IPv6**, **DHCPv6**, **PPPoEv6**, **6to4**, and **6in4**



IPv6 Configuration [Help]

Item	Setting
IPv6	☑ Enable
WAN Connection Type	6 to 4 ▾

6 to 4 WAN Type Configuration

6 to 4 Address	
Primary DNS	
Secondary DNS	
MLD Snooping	□ Enable

LAN Configuration

Global Address	2002:0:0: ::1
Link-local Address	fe80::250:18ff:fe00:ffe

Address Auto-configuration

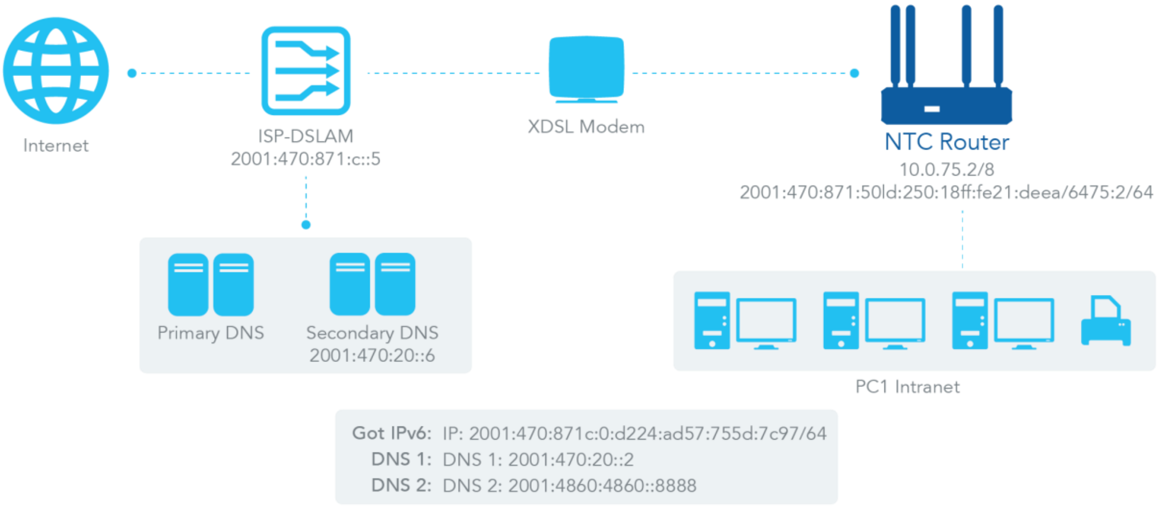
Auto-configuration	☑ Enable
Auto-configuration Type	Stateless ▾
Router Advertisement Lifetime	200 (seconds)

Figure 117 – IPv6 Configuration

3.4.1.1 IPv6 WAN Connection Types

Static IPv6

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



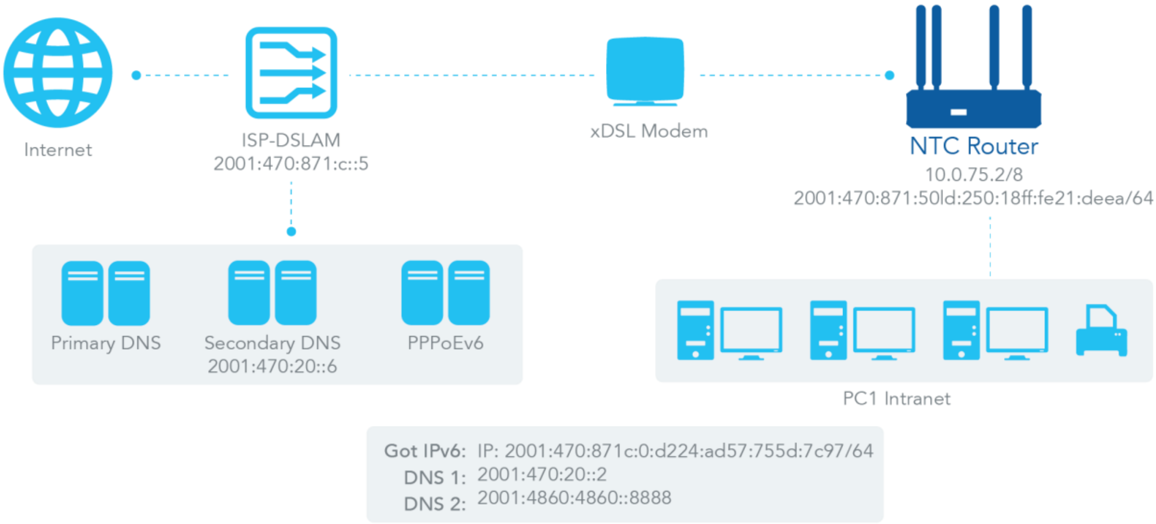
Got IPv6: IP: 2001:470:871c:0:d224:ad57:755d:7c97/64
DNS 1: DNS 1: 2001:470:20::2
DNS 2: DNS 2: 2001:4860:4860::8888

Figure 118 – IPv6 WAN Connection Types - Static IPv6

The diagram above depicts the IPv6 IP addressing. Enter the information provided by your ISP to setup the IPv6 network.

DHCPv6

DHCP in IPv6 performs the same function as DHCP in IPv4. The DHCP server sends an IP address, DNS server addresses and other possible data to the DHCP client to configure it automatically. The server also sends a lease time of the address and time to re-contact the server for IPv6 address renewal. The client must then resend a request to renew the IPv6 address.



Got IPv6: IP: 2001:470:871c:0:d224:ad57:755d:7c97/64
DNS 1: 2001:470:20::2
DNS 2: 2001:4860:4860::8888

Figure 119 – IPv6 WAN Connection Types - DHCPv6

PPPoEv6

PPPoEv6 in IPv6 does the same function as PPPoE in IPv4. The PPPoEv6 server provides configuration parameters based on the PPPoEv6 client request. When the PPPoEv6 server gets a client request and successfully authenticates it, the server sends the IP address, DNS server addresses and other required parameters to automatically configure the client.

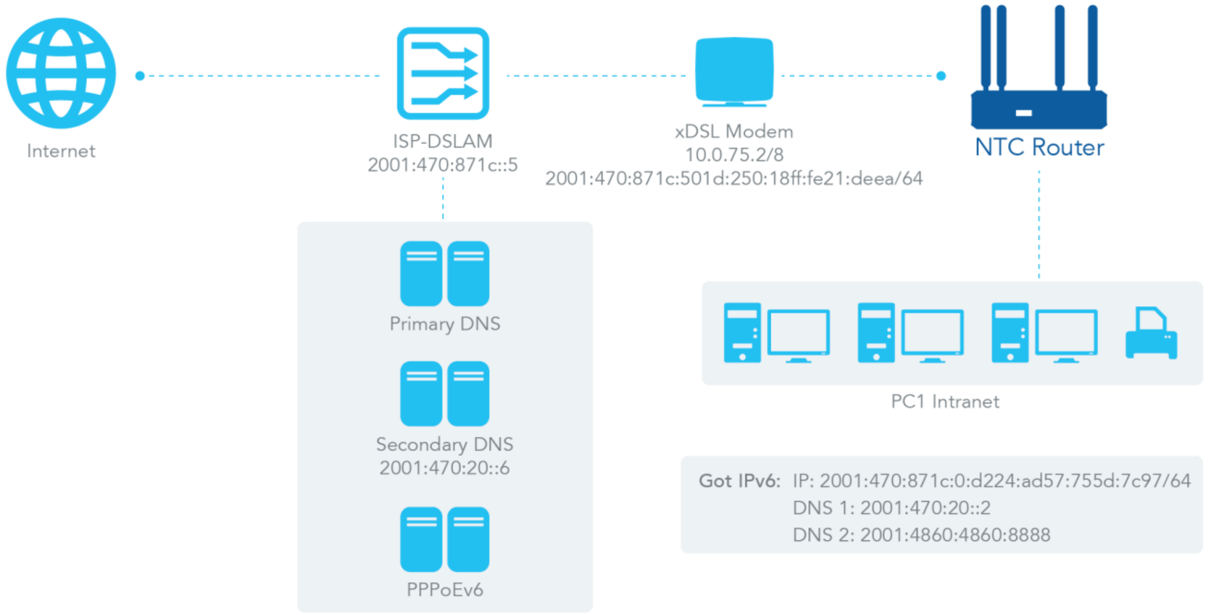


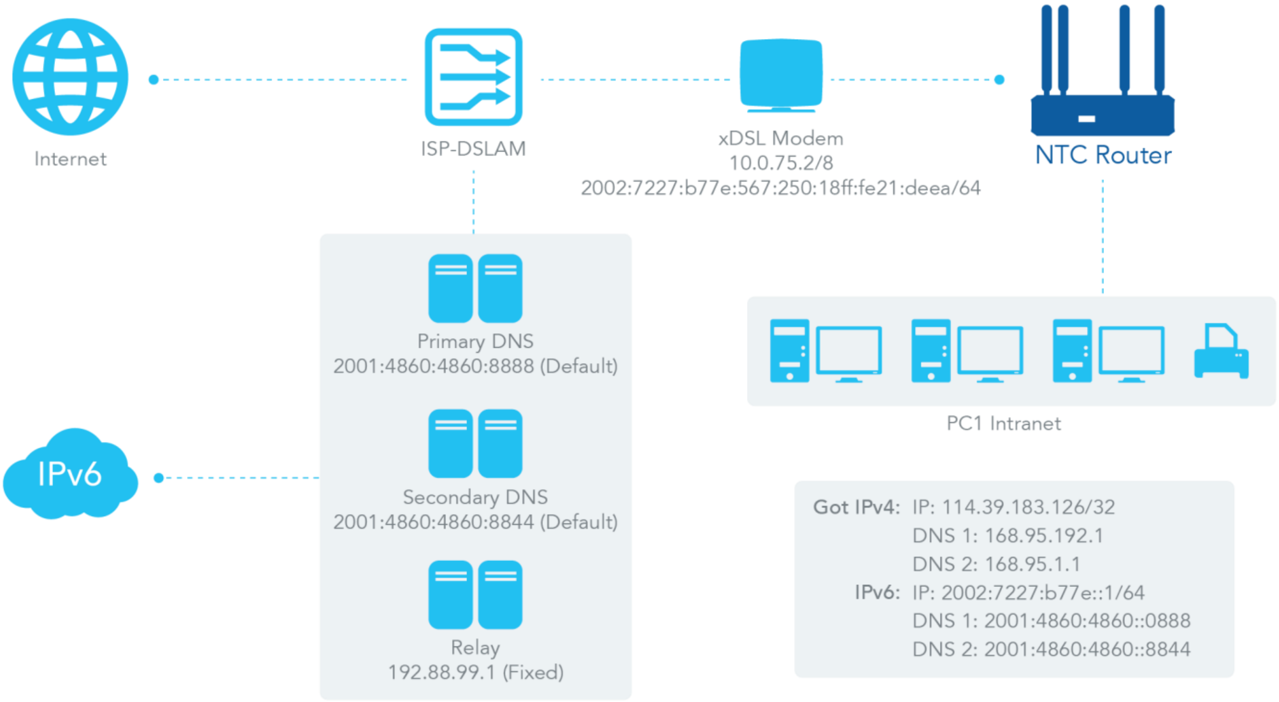
Figure 120 – IPv6 WAN Connection Types - PPPoEv6

The diagram above depicts the IPv6 addressing through PPPoE. The PPPoEv6 server (DSLAM) on the ISP side provides IPv6 configuration upon receiving the PPPoEv6 client request. When the PPPoEv6 server gets a client request and successfully authenticates it, the server sends an IP address, DNS server addresses and other required parameters to automatically configure the client.

6to4

6to4 is one mechanism to establish automatic IPv6 in IPv4 tunnels and to enable complete IPv6 sites communication. The only thing a 6to4 user needs is a global IPv4 address.

6to4 may be used by an individual host, or by a local IPv6 network. When used by a host, it must have a global IPv4 address connected and the host is responsible for encapsulation of outgoing IPv6 packets and decapsulation of incoming 6to4 packets. If the host is configured to forward packets for other clients, often a local network, it is then a router.



Internet
ISP-DSLAM
xDSL Modem
10.0.75.2/8
2002:7227:b77e:567:250:18ff:fe21:deea/64
NTC Router
Primary DNS
2001:4860:4860:8888 (Default)
Secondary DNS
2001:4860:4860:8844 (Default)
Relay
192.88.99.1 (Fixed)
IPv6
PC1 Intranet
Got IPv4: IP: 114.39.183.126/32
DNS 1: 168.95.192.1
DNS 2: 168.95.1.1
IPv6: IP: 2002:7227:b77e::1/64
DNS 1: 2001:4860:4860::0888
DNS 2: 2001:4860:4860::8844

Figure 121 – IPv6 WAN Connection Types - 6to4

In the diagram above, the 6to4 means there is no need to set a gateway address "automatic" tunnelling solution. The relay server, as defined in RFC 3068, has included segments drawing on 192.88.99.0/24 used as 6to4 relay of any-cast address to complete the 6in4 setting.

6in4

6in4 is an Internet transition mechanism for Internet IPv4 to IPv6 migration. 6in4 uses tunnelling to encapsulate IPv6 traffic over explicitly-configured IPv4 links. As defined in RFC 4213, 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.

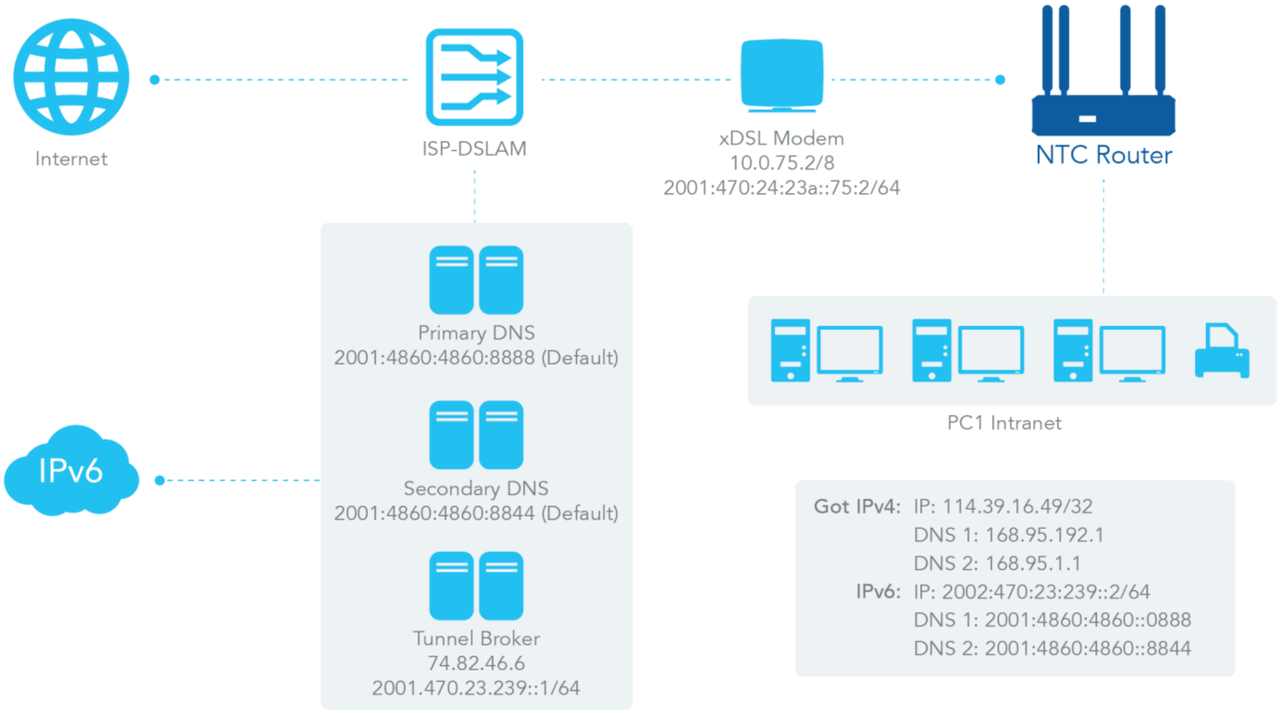


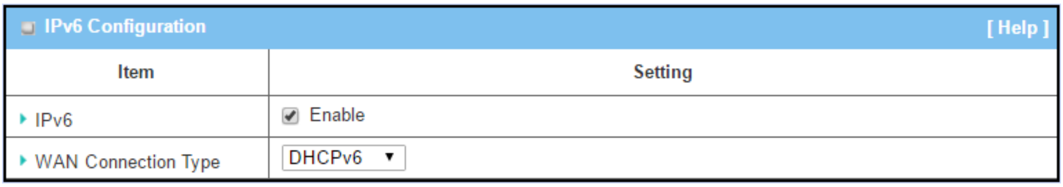
Figure 122 – IPv6 WAN Connection Types - 6in4

In the diagram above, the 6in4 usually needs to register to a 6in4 tunnel service, known as a Tunnel Broker. It also needs the end point global IPv4 address 114.39.16.49 to complete the 6in4 setting.

3.4.1.2 IPv6 Configuration Setting

Navigate to **Basic Network > IPv6 > Configuration**.

The **IPv6 Configuration** setting allows you to set the IPv6 connection type to access the IPv6 network.



IPv6 Configuration [Help]

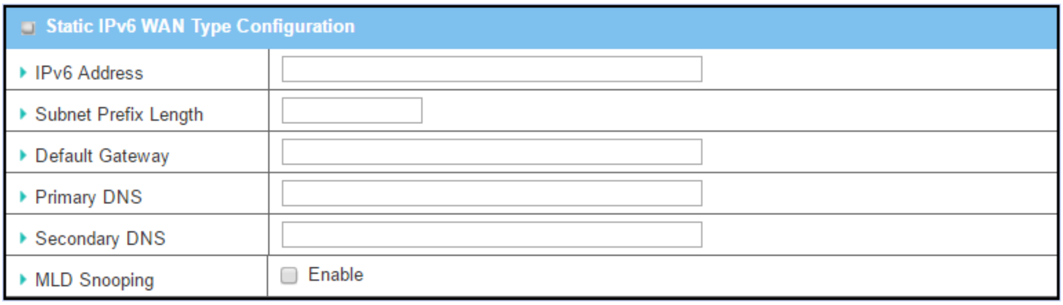
Item	Setting
IPv6	☑ Enable
WAN Connection Type	DHCPv6 ▾

Figure 123 – IPv6 Configuration

Item	Notes	Description
IPv6	Disabled by default.	Check the Enable box to activate the IPv6 function.
WAN Connection Type	Only can be selected when IPv6 is Enabled. Mandatory field.	Define the selected IPv6 WAN Connection Type to establish the IPv6 connectivity. Select Static IPv6 when your ISP provides you with a set of IPv6 addresses. Then go to Static IPv6 WAN Type Configuration. Select DHCPv6 when your ISP provides you with DHCPv6 services. Select PPPoEv6 when your ISP provides you with PPPoEv6 account settings. Select 6to4 when you want to use an IPv6 connection over IPv4. Select 6in4 when you want to use an IPv6 connection over IPv4.

Table 71 – IPv6 Configuration

3.4.1.3 Static IPv6 WAN Type Configuration



Static IPv6 WAN Type Configuration

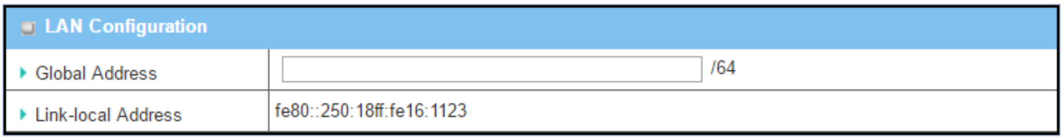
IPv6 Address	
Subnet Prefix Length	
Default Gateway	
Primary DNS	
Secondary DNS	
MLD Snooping	□ Enable

Figure 124 – Static IPv6 WAN Type Configuration

Item	Notes	Description
IPv6 Address	Mandatory field.	Enter the WAN IPv6 Address for the router.
Subnet Prefix Length	Mandatory field.	Enter the WAN Subnet Prefix Length for the router.
Default Gateway	Mandatory field.	Enter the WAN Default Gateway IPv6 address.
Primary DNS	An optional field.	Enter the WAN primary DNS Server.
Secondary DNS	An optional field.	Enter the WAN secondary DNS Server.
MLD Snooping	Disabled by default.	Enable/Disable the MLD Snooping function.

Table 72 – Static IPv6 WAN Type Configuration

3.4.1.4 LAN Configuration



LAN Configuration

Global Address	/64
Link-local Address	fe80::250:18ff:fe16:1123

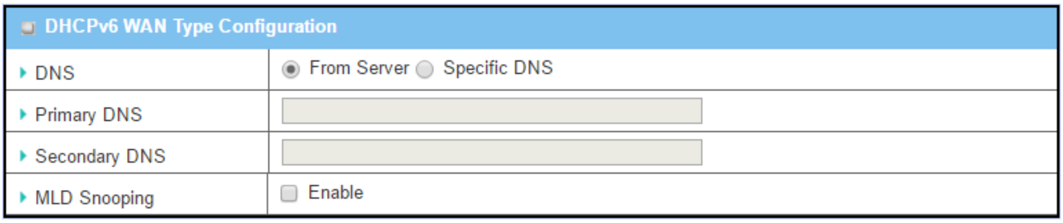
Figure 125 – LAN Configuration

Item	Notes	Description
Global Address	Mandatory field.	Enter the LAN IPv6 Address for the router.
Link-local Address	Value auto-created	Show the link-local address for LAN interface of router.

Table 73 – LAN Configuration

Navigate to **Address Auto-configuration (summary)** for setting LAN environment.

3.4.1.5 DHCPv6 WAN Type Configuration



DHCPv6 WAN Type Configuration

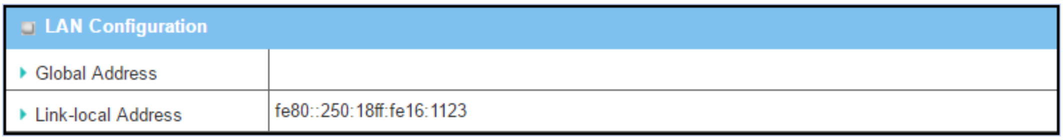
DNS	● From Server ○ Specific DNS
Primary DNS	
Secondary DNS	
MLD Snooping	□ Enable

Figure 126 – DHCPv6 WAN Type Configuration

Item	Notes	Description
DNS	The option [From Server]Default setting:	Select the [Specific DNS] option to activate Primary DNS and Secondary DNS. Then enter 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	Disabled by default	Enable/Disable the MLD Snooping function.

Table 74 – DHCPv6 WAN Type Configuration

3.4.1.6 LAN Configuration



LAN Configuration

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

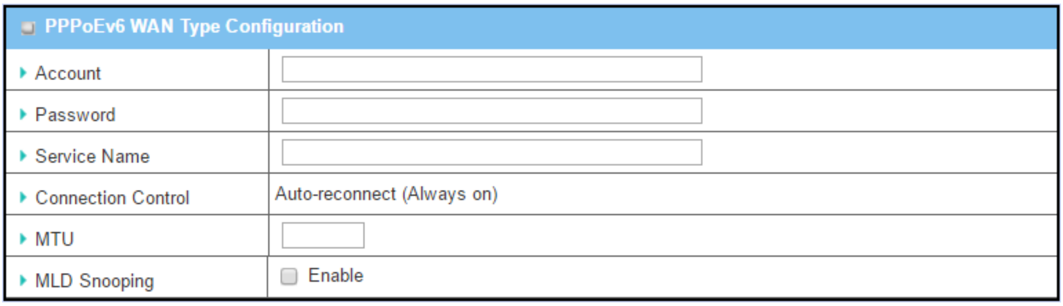
Figure 127 – LAN Configuration

Item	Notes	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.

Table 75 – LAN Configuration

Navigate to **Address Auto-configuration (summary)** to set the LAN environment.

3.4.1.7 PPPoEv6 WAN Type Configuration



PPPoEv6 WAN Type Configuration

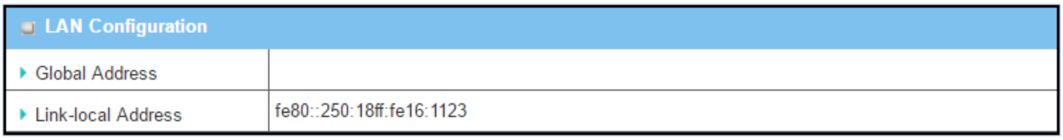
Account	
Password	
Service Name	
Connection Control	Auto-reconnect (Always on)
MTU	
MLD Snooping	□ Enable

Figure 128 – PPPoEv6 WAN Type Configuration

Item	Notes	Description
Account	Mandatory field.	Enter the Account to set up a PPPoEv6 connection. If you want more information, please contact your ISP. Value Range: 0 - 45 characters.
Password	Mandatory field.	Enter the Password to set up a PPPoEv6 connection. If you want more information, please contact your ISP.
Service Name	Mandatory field.	Enter the Service Name to set up a PPPoEv6 connection. If you want more information, please contact your ISP. Value Range: 0 - 45 characters.
Connection Control	Fixed value	The value is Auto-reconnect(Always on).
MTU	Mandatory field.	Enter the MTU to set up a PPPoEv6 connection. If you want more information, please contact your ISP. Value Range: 1280 - 1492.
MLD Snooping	Disabled by default.	Enable/Disable the MLD Snooping function

Table 76 – PPPoEv6 WAN Type Configuration

3.4.1.8 LAN Configuration



LAN Configuration

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

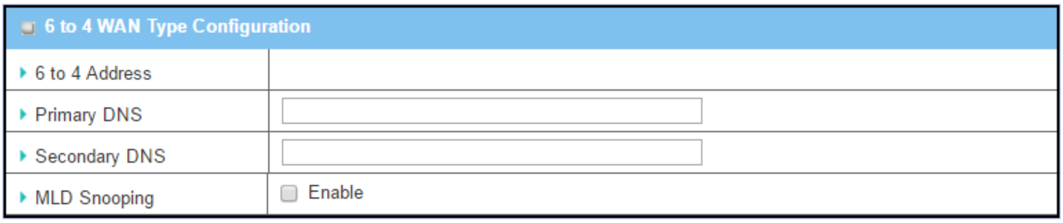
Figure 129 – LAN Configuration

Item	Notes	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.

Table 77 – LAN Configuration

Navigate to **Address Auto-configuration (summary)** to set up the LAN environment.

3.4.1.9 6to4 WAN Type Configuration



6 to 4 WAN Type Configuration

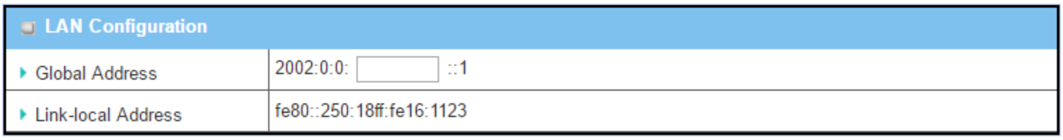
6 to 4 Address	
Primary DNS	
Secondary DNS	
MLD Snooping	□ Enable

Figure 130 – 6to4 WAN Type Configuration

Item	Notes	Description
6to4 Address	Value auto-created	IPv6 address for access the IPv6 network.
Primary DNS	Optional field.	Enter the WAN primary DNS Server.
Secondary DNS	Optional field.	Enter the WAN secondary DNS Server.
MLD	Disabled by default.	Enable/Disable the MLD Snooping function

Table 78 – 6to4 WAN Type Configuration

3.4.1.10 LAN Configuration



LAN Configuration

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

Figure 131 – LAN Configuration

Item	Notes	Description
Global Address	Optional field.	Enter the LAN IPv6 Address for the router. Value Range: 0 - FFFF.
Link-local Address	Auto-created value	Show the link-local address for LAN interface of router.

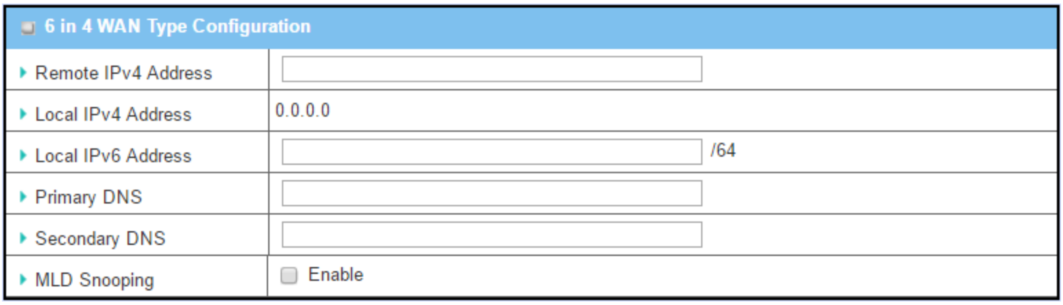
Table 79 – LAN Configuration

Navigate to **Address Auto-configuration (summary)** to set the LAN environment.

3.4.1.11 6in4 WAN Type Configuration

To establish a 6in4 tunnel, find an IPv6 tunnel broker. You can find a list of IPv6 tunnel brokers that support the 6in4 service on Wikipedia.

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



6 in 4 WAN Type Configuration

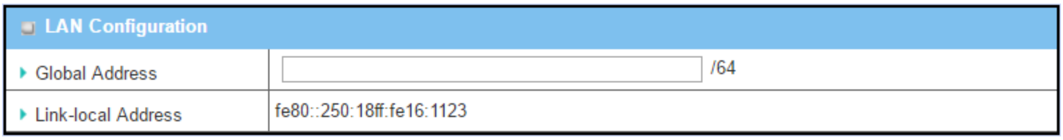
Remote IPv4 Address	
Local IPv4 Address	0.0.0.0
Local IPv6 Address	/64
Primary DNS	
Secondary DNS	
MLD Snooping	□ Enable

Figure 132 – 6in4 WAN Type Configuration

Item	Notes	Description
Remote IPv4 Address	Mandatory field.	Enter the Server IPv4 Address from your tunnel broker in this field.
Local IPv4 Address	Value auto-created	The IPv4 address of this router.
Local IPv6 Address	Mandatory field.	Enter the Client IPv6 Address from the tunnel broker in this field.
Primary DNS	Optional field.	Enter the WAN primary DNS Server.
Secondary DNS	Optional field.	Enter the WAN secondary DNS Server.
MLD	Disabled by default.	Enable/Disable the MLD Snooping function

Table 80 – 6in4 WAN Type Configuration

3.4.1.12 LAN Configuration



LAN Configuration

Global Address	/64
Link-local Address	fe80::250:18ff:fe16:1123

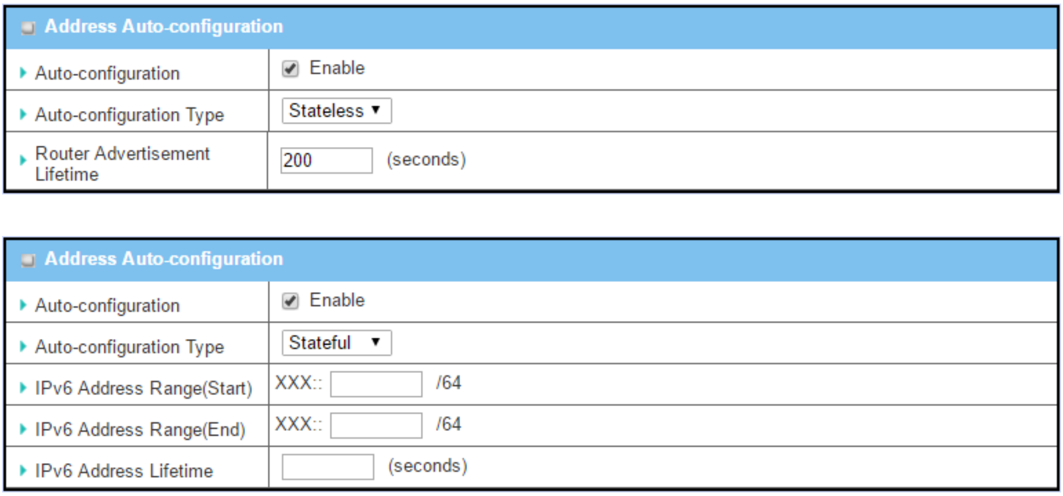
Figure 133 – 6in4 WAN Type Configuration

Item	Notes	Description
Global Address	Mandatory field.	Filled Routed /64 gotten from tunnel broker in this field.
Link-local Address	Auto-created value	Show the link-local address for LAN interface of router.

Table 81 – LAN Configuration

Navigate to **Address Auto-configuration (summary)** to set the LAN environment.

3.4.1.13 Address Auto-configuration



Address Auto-configuration

Auto-configuration	☑ Enable
Auto-configuration Type	Stateless ▾
Router Advertisement Lifetime	200 (seconds)

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)

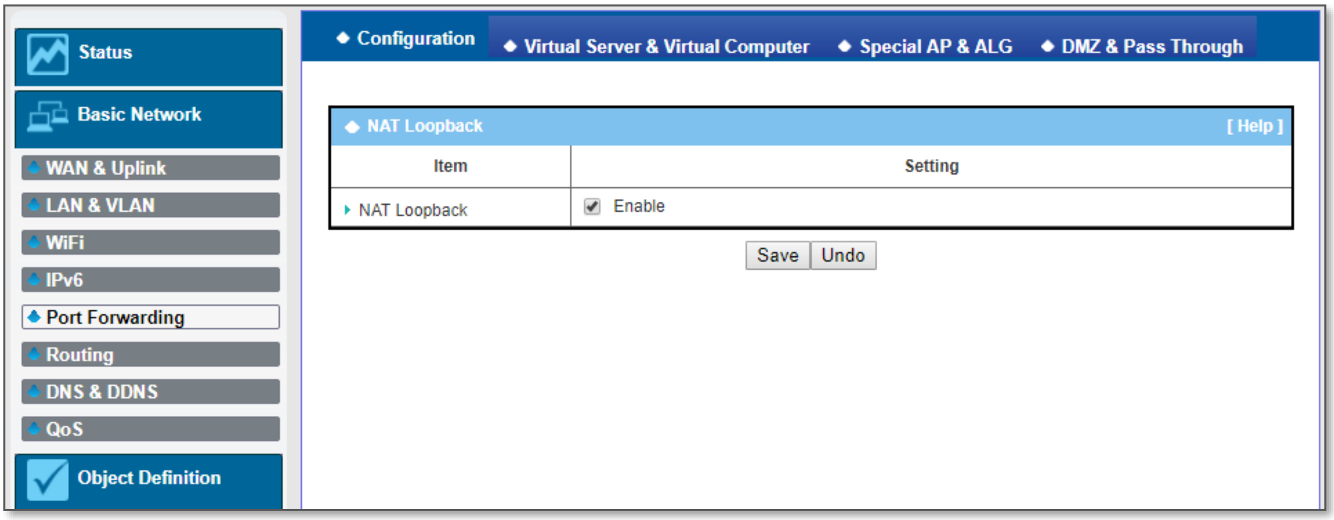
Figure 134 – Address Auto-configuration

Item	Notes	Description
Auto-configuration	Disabled by default.	Check to enable the Auto configuration feature.
Auto-configuration Type	Can only be selected when Auto-configuration is enabled. Default setting: **Stateless**	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** (mandatory field) – Enter the Router Advertisement Lifetime (in seconds). 200Default setting: Value Range: 0 - 65535. Select Stateful to manage the Local Area Network to be Stateful (DHCPv6). **IPv6 Address Range (Start)** (mandatory field) – Enter the start IPv6 Address for the DHCPv6 range for your local computers. Default setting: 0100 Value Range: 0001 - FFFF. **IPv6 Address Range (End)** (mandatory field) – Enter the end IPv6 Address for the DHCPv6 range for your local computers. Default setting: 0200 Value Range: 0001 - FFFF. **IPv6 Address Lifetime** (mandatory field) – Enter the DHCPv6 lifetime for your local computers. Default setting: 36000 Value Range: 0 - 65535.

Table 82 – Address Auto-configuration

3.5 Port Forwarding

Network address translation (NAT) is a method of remapping one IP address space into another by modifying network address information in Internet Protocol (IP) datagram packet headers while they are in transit across a traffic routing device. The technique was originally used for ease of rerouting traffic in IP networks without renumbering every host. It has become a popular and essential tool in conserving global address space allocations in the face of IPv4 address exhaustion. The NTC-400 Series Router supports NAT. You can disable the NAT function on the **[Basic Network]-[WAN & Uplink]-[Internet Setup]-[WAN Type Configuration]** page.



NAT Loopback [Help]

Item	Setting
NAT Loopback	☑ Enable

Figure 135 – NAT Loopback

Usually all local hosts or servers behind the corporate gateway are protected by a NAT firewall. The NAT firewall filters out unrecognized packets to protect your Intranet. All local hosts are invisible to the outside world. Port forwarding or port mapping is a function that redirects a communication request from one address and port number combination to an assigned one. This technique is most commonly used to make services on a host residing on a protected or masqueraded (internal) network available to hosts on the opposite side of the router (external network), by remapping the destination IP address and port number.

There are several optional Port Forwarding related functions on the NTC-400 Series Router. They are **Virtual Server**, **Virtual Computer**, **IP Translation**, **Special AP & ALG**, **DMZ**, **Pass Through**, etc.

3.5.1 Configuration

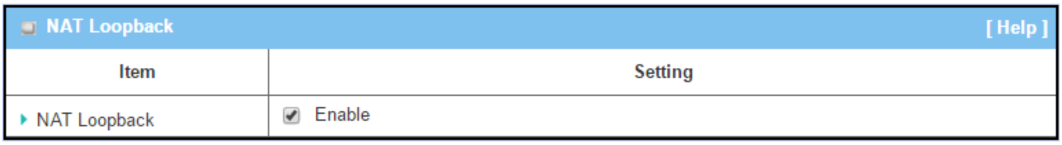
3.5.1.1 NAT Loopback

This feature allows you to access the WAN global IP address from inside your NAT local network. It is useful when you run a server inside your network. For example, if you set up a mail server on the LAN side, your local devices can access this mail server through the router’s global IP address when the NAT loopback feature is enabled. Regardless of which side the email server is being accessed from, the IP address of the mail server does not need to be changed.

3.5.1.2 Configuration Setting

Navigate to the **Basic Network > Port Forwarding > Configuration** tab. The NAT Loopback feature allows you to access the WAN IP address from inside your local network.

3.5.1.3 Enable NAT Loopback



NAT Loopback [Help]

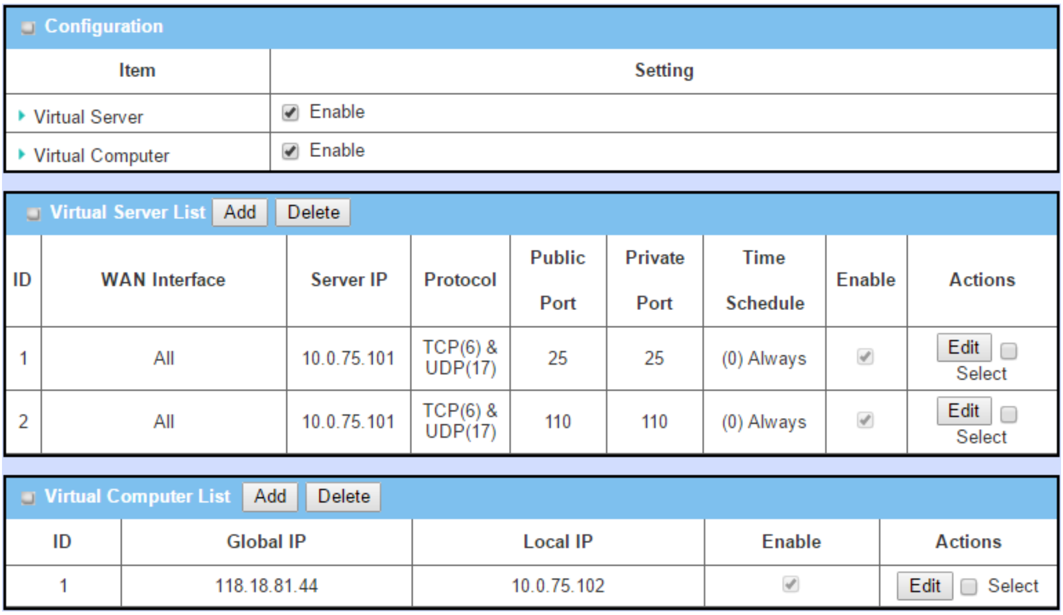
Item	Setting
NAT Loopback	☑ Enable

Figure 136 – Enable NAT Loopback

Item	Notes	Description
NAT Loopback	Enabled by default.	Check ☑ **Enable** to activate the NAT function
Save	Button	Click the **Save** button to save the settings.
Undo	Button	Click the **Undo** button to cancel the settings

Table 83 – Enable NAT Loopback

3.5.2 Virtual Server & Virtual Computer



Configuration

Item	Setting
Virtual Server	☑ Enable
Virtual Computer	☑ Enable

Virtual Server List Add Delete

ID	WAN Interface	Server IP	Protocol	Public Port	Private Port	Time Schedule	Enable	Actions
1	All	10.0.75.101	TCP(6) & UDP(17)	25	25	(0) Always	☑	Edit □ Select
2	All	10.0.75.101	TCP(6) & UDP(17)	110	110	(0) Always	☑	Edit □ Select

Virtual Computer List Add Delete

ID	Global IP	Local IP	Enable	Actions
1	118.18.81.44	10.0.75.102	☑	Edit □ Select

Figure 137 – Virtual Server & Virtual Computer

There are some important Port Forwarding functions implemented within the router, including "Virtual Server", "NAT loopback" and "Virtual Computer".

These are useful for staff who travel and want to access various servers behind the office router. You can set up those servers by using the "Virtual Server" feature. Upon returning to the office, to access those servers from the LAN side using a global IP and without changing the original setting, use the NAT Loopback feature.

"Virtual computer" is a host behind the NAT router whose IP address is a global one and is visible to the outside world. Since it is behind NAT, it is protected by the router firewall. To configure a Virtual Computer, you must map the local IP of the virtual computer to a global IP.

3.5.2.1 Virtual Server & NAT Loopback

"Virtual Server" allows you to access servers with the global IP address or FQDN of the router as if they are servers that exist on the Internet. In fact, these servers are located on the Intranet and are physically behind the router. The router serves the requests by port forwarding the requests to the LAN servers and transfers the replies from LAN servers to the requester on the WAN side.

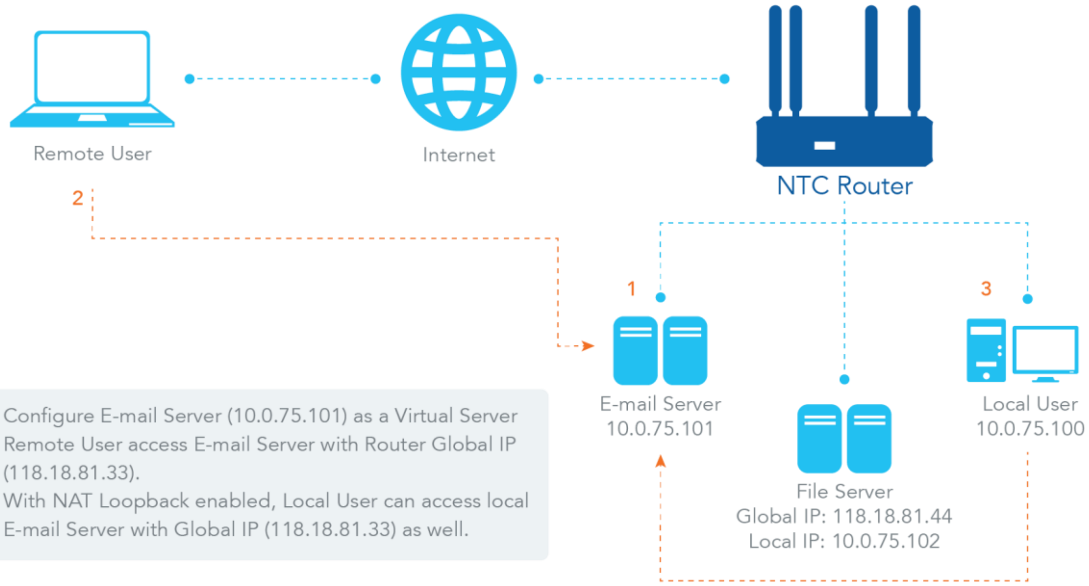

Remote User
Internet
NTC Router
2
1
3
E-mail Server
10.0.75.101
File Server
Global IP: 118.18.81.44
Local IP: 10.0.75.102
Local User
10.0.75.100
1 Configure E-mail Server (10.0.75.101) as a Virtual Server
2 Remote User access E-mail Server with Router Global IP (118.18.81.33).
3 With NAT Loopback enabled, Local User can access local E-mail Server with Global IP (118.18.81.33) as well.

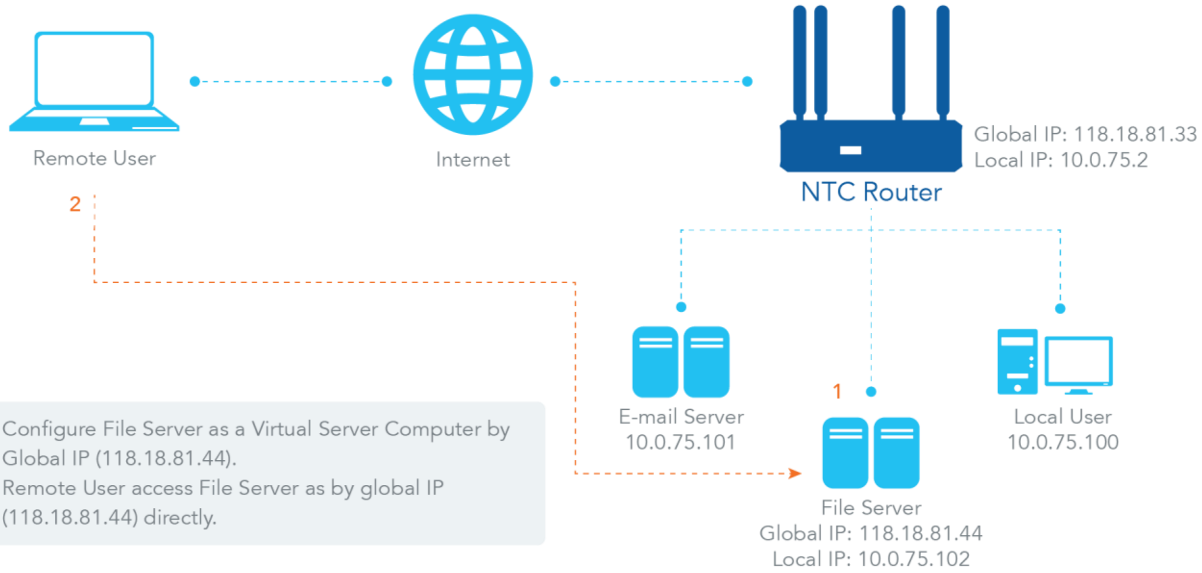
Figure 138 – Virtual Server & NAT Loopback

As shown in the above example, an e-mail virtual server is defined to be located on a server with IP address 10.0.75.101 in the Intranet of Network-A, including the SMTP service port 25 and POP3 service port 110. The remote user can access the e-mail server with the router's global IP 118.18.81.33 from its WAN side, but the real e-mail server is located on the LAN side and the router is the port forwarder for the e-mail service.

NAT Loopback allows you to access the WAN global IP address from inside your local network. It is useful when you run a server inside your network. For example, if you configure an e-mail server on the LAN side, your local devices can access this e-mail server through the router's global IP address when the NAT loopback feature is enabled. From that point, you do not need to change the IP address of the e-mail server to access it from either side of the LAN or WAN.

3.5.2.2 Virtual Computer

"Virtual Computer" allows you to assign LAN hosts to global IP addresses, so that they can be visible to the outside world. While they are visible to the outside world, they are also protected by the router firewall as being client hosts in the Intranet.



1 Configure File Server as a Virtual Server Computer by Global IP (118.18.81.44).
2 Remote User access File Server as by global IP (118.18.81.44) directly.

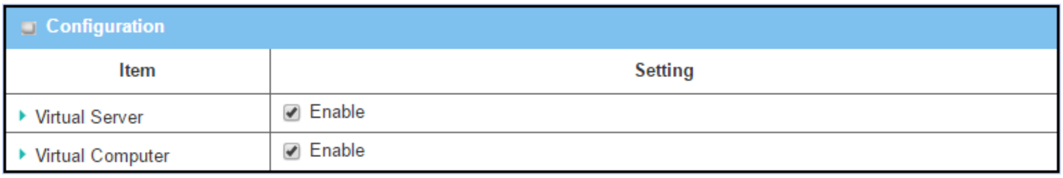
Figure 139 – Virtual Computer

For example, if you set an FTP file server on the LAN side with the local IP address “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 gateway. That is because the router takes care of all access to the IP address 118.18.82.44, including forwarding the access requests to the file server and to send the replies from the server to the outside world**.**

3.5.2.3 Virtual Server & Virtual Computer Setting

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

3.5.2.4 Enable Virtual Server and Virtual Computer



Configuration

Item	Setting
Virtual Server	☑ Enable
Virtual Computer	☑ Enable

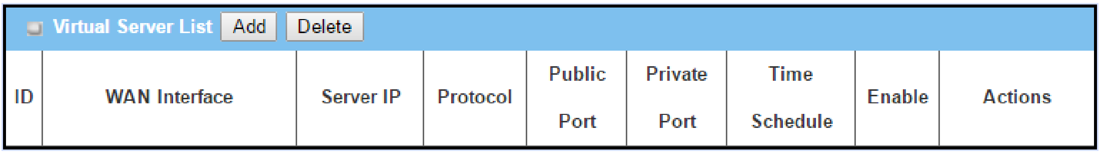
Figure 140 – Enable Virtual Server and Virtual Computer

Item	Notes	Description
Virtual Server	Disabled by default.	Check ☑ **Enable** to activate this port forwarding function.
Virtual Computer	Enabled by default.	Check ☑ **Enable** to activate this port forwarding function.
Save	Button	Click the **Save** button to save the settings.
Undo	Button	Click the **Undo** button to cancel the settings.

Table 84 – Enable Virtual Server and Virtual Computer

3.5.2.5 Create / Edit Virtual Server

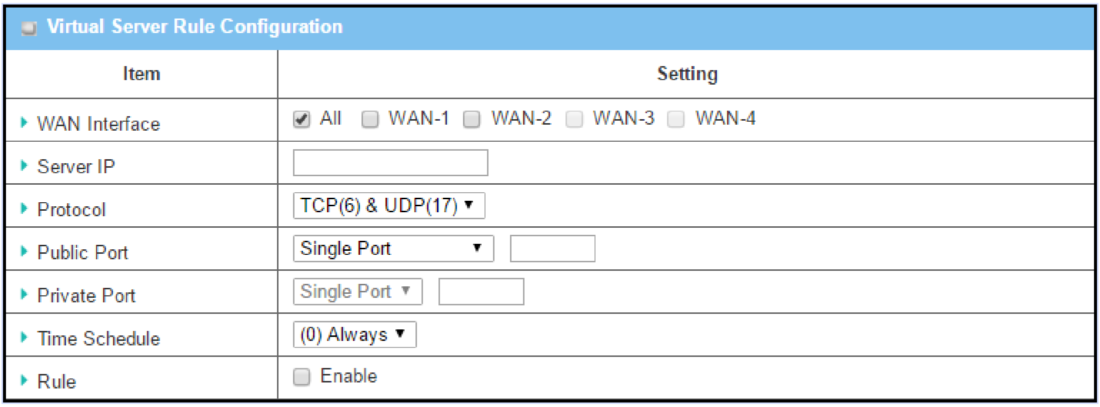
The router allows you to custom your Virtual Server rules. It supports up to a maximum of 20 rule-based Virtual Server sets.



ID	WAN Interface	Server IP	Protocol	Public Port	Private Port	Time Schedule	Enable	Actions

Figure 141 – Create / Edit Virtual Server

Click the **Add** button to display the **Virtual Server Rule Configuration** screen.



Item	Setting
WAN Interface	☑ All ☐ WAN-1 ☐ WAN-2 ☐ WAN-3 ☐ WAN-4
Server IP	
Protocol	TCP(6) & UDP(17) ▾
Public Port	Single Port ▾
Private Port	Single Port ▾
Time Schedule	(0) Always ▾
Rule	☐ Enable

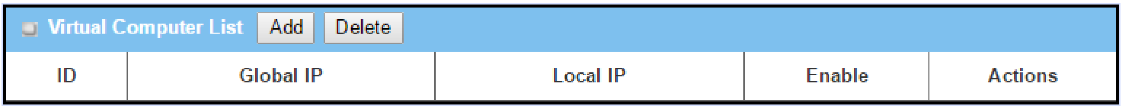
Table 85 – Create / Edit Virtual Server

Item	Notes	Description
WAN Interface	Mandatory field. Default is **ALL.**	Defines the selected interface as the interface that packets enter the router. Select ALL for packets coming into the router from any interface. Note – The available check boxes (WAN-1 - WAN-4) depend on the number of WAN interfaces for the product.
Server IP	Mandatory field.	This field is to specify the IP address of the interface selected in the WAN Interface setting above.
Protocol	Mandatory field.	When “ICMPv4” is selected, the “Protocol” option of the packet filter rule is ICMPv4. Select a Time Schedule to apply to this rule, otherwise leave it as Always. (refer to Scheduling setting under Object Definition) Check ☑ **Enable** to enable this rule.
		When “TCP” is selected the “Protocol” option of the packet filter rule is TCP. When Public Port is set to a predefined port from a well-known service, Private Port is the same as the Public Port number. When Public Port is set to Single Port, specify a port number. Private Port can be set to a Single Port number. When Public Port is set to Port Range, specify a port range. Private Port can be set to Single Port or Port Range. Value Range: 1 - 65535 for both Public Port and Private Port.
		When “UDP” is selected, the “Protocol” option of the packet filter rule is UDP.

Item	Notes	Description
		When Public Port is set to a predefined port from a well-known service, Private Port is the same as the Public Port number. When Public Port is set to Single Port, specify a port number. Private Port can be set to a Single Port number. When Public Port is set to Port Range, specify a port range. Private Port can be set to Single Port or Port Range. Value Range: 1 - 65535 for both Public Port and Private Port.
		When "TCP & UDP" is selected, the "Protocol" option of the packet filter rule is TCP and UDP. When Public Port is set to a predefined port from a well-known service, Private Port is the same as the Public Port number. When Public Port is set to Single Port, specify a port number. Private Port can be set to a Single Port number. When Public Port is set to Port Range, specify a port range. Private Port can be set to Single Port or Port Range. Value Range: 1 - 65535 for both Public Port and Private Port.
		When "GRE" is selected, the "Protocol" option of the packet filter rule is GRE.
		When "ESP" is selected, the "Protocol" option of the packet filter rule is ESP.
		When "SCTP" is selected, the "Protocol" option of the packet filter rule is SCTP.
		When "User-defined" is selected, the "Protocol" option of the packet filter rule is User-defined. For Protocol Number, enter a port number.
Time Schedule	Optional field. Default setting: **(0) Always**	Apply a Time Schedule to this rule; otherwise leave it as (0)Always. (refer to Scheduling setting under Object Definition)
Rule	Optional field. Disabled by default.	Check ☑ **Enable** to activate the rule.
Save	Button	Click the **Save** button to save the settings.
Undo	Button	Click the **Undo** button to cancel the settings.
Back	Button	When the **Back** button is clicked the screen will return to previous page.

3.5.2.6 Create / Edit Virtual Computer

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

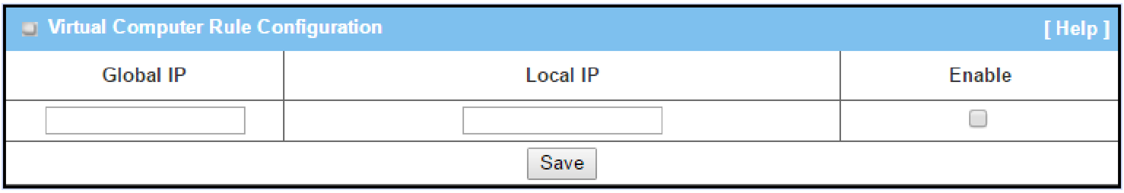


Virtual Computer List Add Delete

ID	Global IP	Local IP	Enable	Actions

Figure 142 – Create / Edit Virtual Computer

Click the **Add** button to display the **Virtual Computer Rule Configuration** screen.



Virtual Computer Rule Configuration [Help]

Global IP	Local IP	Enable
		□

Save

Figure 143 – Virtual Computer Rule Configuration

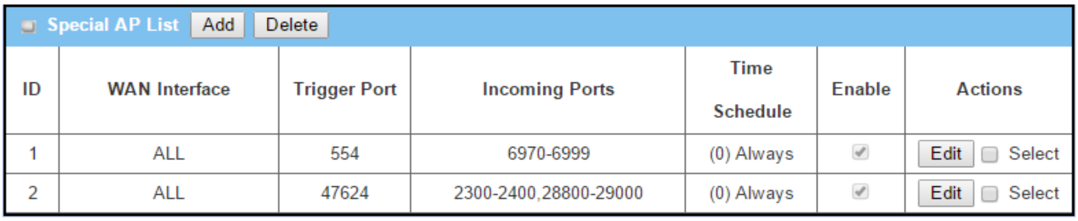
Item	Notes	Description
Global IP	Mandatory field.	This field is to specify the IP address of the WAN IP.
Local IP	Mandatory field.	This field is to specify the IP address of the LAN IP.
Enable	N/A	Then check Enable box to enable this rule.
Save	N/A	Click the Save button to save the settings.

Table 86 – Virtual Computer Rule Configuration

3.5.3 Special AP & ALG

As a NAT router, the NTC-400 Series Router doesn't allow an active connection request from the outside world while client hosts on the Intranet may use applications that need more service ports to be allowed for passing through the NAT router. The "Special AP (application)" feature of the router can get around this problem by allowing certain applications requiring multiple connections to pass through the NAT feature of the router.

The application-level gateway (ALG) allows customised NAT traversal filters to be plugged into the router to support address and port translation for certain application layer protocols such as FTP, SIP, RTSP, file transfer in IM applications, etc. In order for these protocols to work through NAT or a firewall, either the application has to know about an address/port number combination that allows incoming packets, or the NAT has to monitor the control traffic and open up port mappings (firewall pinhole) dynamically as required. Legitimate application data can thus be passed through the security checks of the firewall or NAT that would have otherwise restricted the traffic for not meeting its limited filter criteria.



ID	WAN Interface	Trigger Port	Incoming Ports	Time Schedule	Enable	Actions
1	ALL	554	6970-6999	(0) Always	☑	Edit □ Select
2	ALL	47624	2300-2400,28800-29000	(0) Always	☑	Edit □ Select

Figure 144 – Special AP List

The Special AP feature allows you to request the router to open pre-defined service ports for incoming packets to pass through once the trigger port is activated by local hosts. As shown in the diagram below, a special AP rule defines port 554 as trigger port and 6970-6999 as incoming ports. With this setting, the local user at host 10.0.75.100 can access services located on the Internet. When you open the application, it will activate the Trigger Port and then incoming data packets from the remote application server will pass through incoming ports 6970~6999.

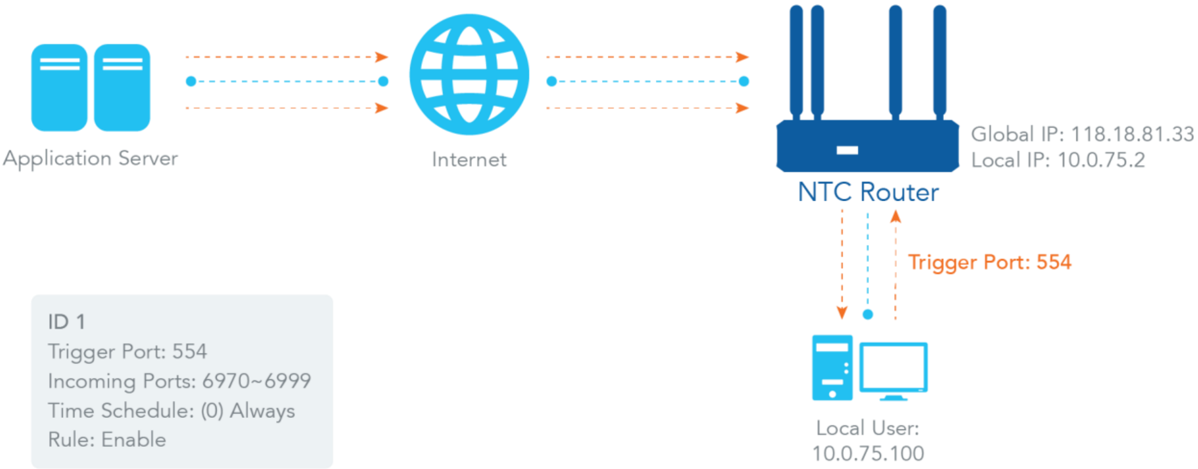


Figure 145 – Special AP feature

3.5.3.1 SIP ALG

The NTC-400 Series Router supports the SIP ALG feature to allow one SIP phone behind the NAT router to call another SIP phone in the Internet, even if the router executes its NAT mechanism between the Intranet and the Internet. The NAT router monitors the control traffic and opens up port mappings (firewall pinhole) dynamically to know about an address/port number combination that allows incoming packets, so it will support address and port translation for SIP application layer protocols as shown in following diagram.

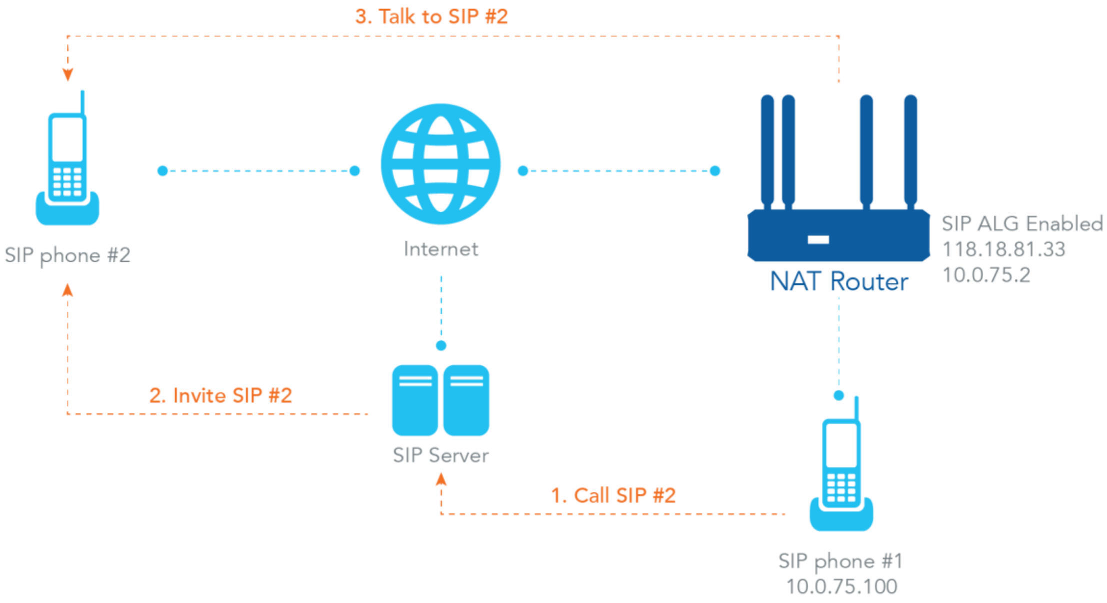


Figure 146 – SIP ALG

The NAT router enables the SIP ALG feature, so it will monitor the actions of SIP Phone #1, open up the required ports and make the address and port translation in a SIP voice communication.

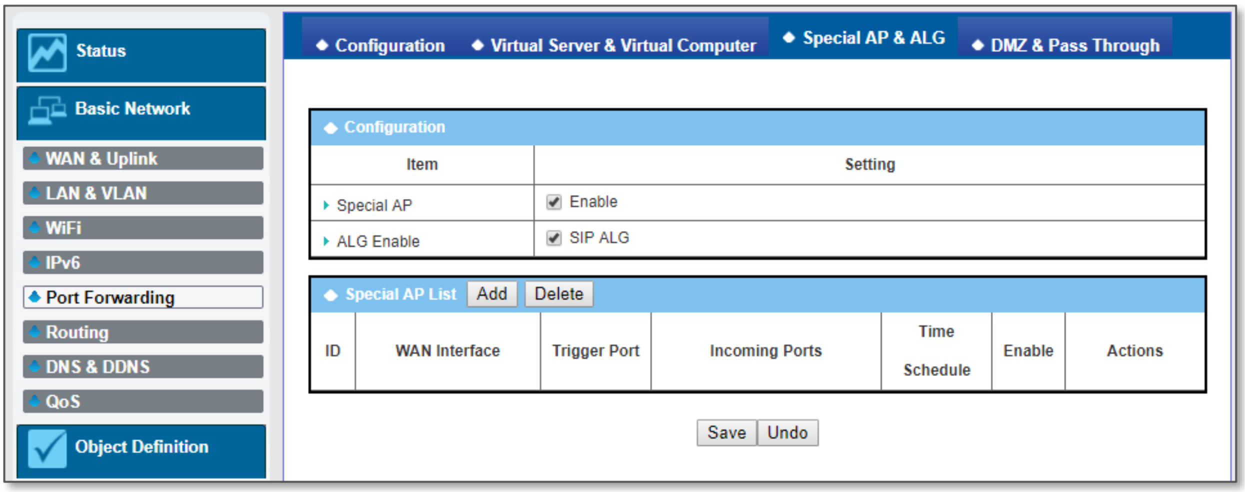
As shown in the diagram above, the calling starts from the SIP Phone #1 to the SIP server via the NAT router. Then the SIP server invites SIP Phone #2 and SIP Phone #1 talks to the SIP Phone #2. But for the NAT router, SIP Phone #2 is an unknown host, so the active access from the Phone #2 will be treated as unexpected traffic and will be blocked out. With the SIP ALG function enabled, the NAT router will monitor the control traffic for the SIP calls, and recognise the traffic from SIP Phone #2 is part of the connection sessions with SIP Phone #1.

3.5.3.2 Special AP & ALG Setting

Navigate to **Basic Network > Port Forwarding > Special AP & ALG** tab**.**

The Special AP setting allows some applications requiring multiple connections. The ALG setting allows the support of some SIP ALGs, like STUN.

3.5.3.3 Enable Special AP & ALG



Configuration

Item	Setting
Special AP	☑ Enable
ALG Enable	☑ SIP ALG

Special AP List [Add] [Delete]

ID	WAN Interface	Trigger Port	Incoming Ports	Time Schedule	Enable	Actions

[Save] [Undo]

Figure 147 – Enable Special AP & ALG and Special AP List

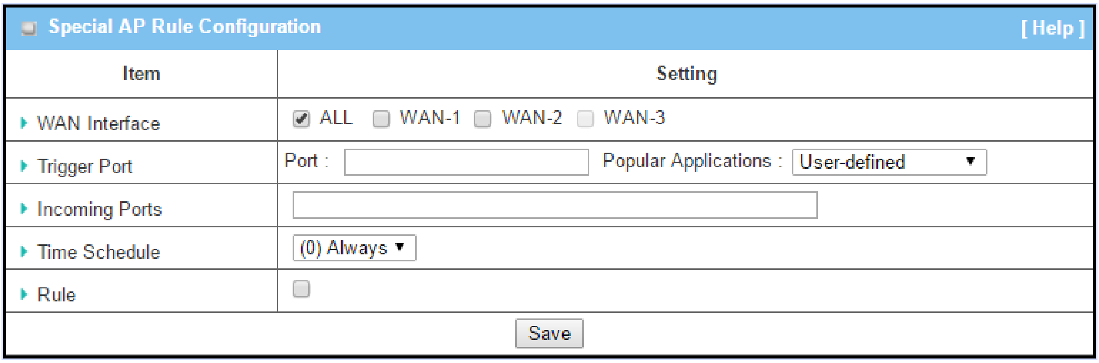
Item	Value setting	Description
Special AP	Enabled by default.	Check ☑ **Enable** to activate the Special AP function.
ALG Enable	Enabled by default.	Check ☑ **Enable** to activate the SIP ALG function.
Save	N/A	Click the **Save** button to save the settings.
Undo	N/A	Click the **Undo** button to cancel the settings

Table 87 – Enable Special AP & ALG

3.5.3.4 Create / Edit Special AP Rule

The router allows you to customise your Special AP rules. It supports up to a maximum of 8 rule-based Special AP sets.

Click the **Add** button in the title bar of the **Special AP List** to display the **Special AP Rule Configuration** screen.



Special AP Rule Configuration [Help]

Item	Setting
WAN Interface	☑ ALL ☐ WAN-1 ☐ WAN-2 ☐ WAN-3
Trigger Port	Port : [ ] Popular Applications : User-defined ▾
Incoming Ports	[ ]
Time Schedule	(0) Always ▾
Rule	☐

[Save]

Figure 148 – Special AP Rule Configuration

Item	Value setting	Description
WAN Interface	Mandatory field. **All** is checked by default.	Check the interface box(es) to apply the Special AP rule. By default, **All** is checked, and the Special AP rule will be applied to all WAN interfaces.

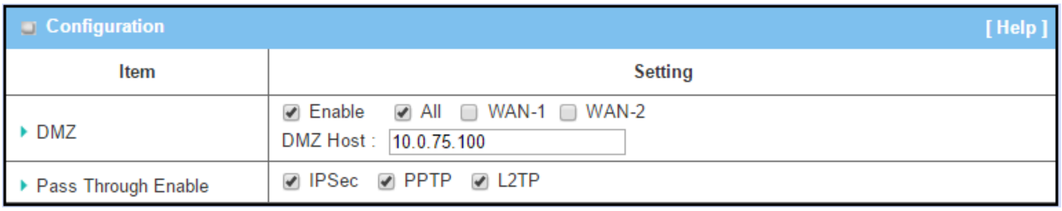
Item	Value setting	Description
Trigger Port	Mandatory field. **User-defined** is selected by default.	Enter the expected trigger port (or port range) if **User-defined** is selected in the dropdown list. If you select another popular application from the dropdown list, the corresponding trigger port(s) and incoming ports will be defined automatically. Value Range: 1 - 65535.
Incoming Ports	Mandatory field.	Enter the expected Incoming ports if **User-defined** is selected in the **Trigger Port** dropdown list. If you select another popular application from the dropdown list, the corresponding incoming ports will be defined automatically. Value Range: 1 - 65535; It can be a single port, multiple ports separated by ",", or a port range.
Time Schedule	Mandatory field. Default setting: **(0) Always**	Apply a **Time Schedule** to this rule, otherwise leave it as **Always**. If the dropdown list is empty, ensure **Time Schedule** is pre-configured. Refer to the **Object Definition > Scheduling > Configuration** tab.
Rule	Disabled by default.	Check ☑ **Enable** to activate the special AP rule.
Save	Button	Click the **Save** button to save the settings.
Undo	Button	Click the **Undo** button to cancel the settings

Table 88 – Special AP Rule Configuration

3.5.4 DMZ & Pass Through

DMZ (De Militarized Zone) Host is a host that is exposed to the Internet but still within the protection of the router firewall. The function allows a computer to execute two-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 indicate that LAN computer as a DMZ host to solve this problem.

The DMZ function allows you to ask the router to pass through all normal packets to the DMZ host behind the NAT router only when these packets are not expected to be received by applications on the router or by other client hosts in the Intranet. Activate the feature and specify the DMZ host with a host in the Intranet when needed.



Configuration [Help]

Item	Setting
DMZ	☑ Enable ☑ All □ WAN-1 □ WAN-2 DMZ Host : 10.0.75.100
Pass Through Enable	☑ IPSec ☑ PPTP ☑ L2TP

Figure 149 – DMZ Configuration

3.5.4.1 VPN Pass through Scenario

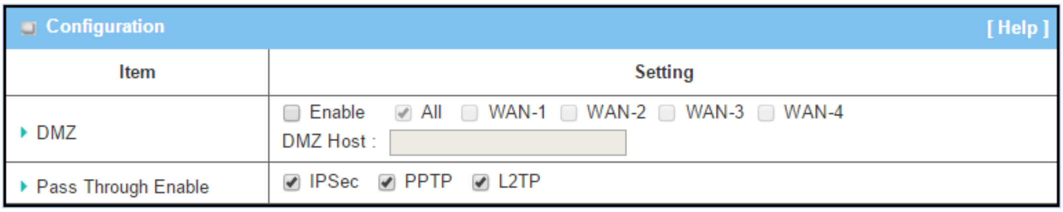
Since VPN traffic is different from that of TCP or UDP, it will be blocked by the NAT router. To support the pass-through function for VPN connections initiated by VPN clients behind the NAT router, the router must implement some kind of VPN pass through function for such application. The router supports the pass-through function for IPSec, PPTP, and L2TP connections.

3.5.4.2 DMZ & Pass Through Setting

Navigate to the **Basic Network > Port Forwarding > DMZ & Pass Through** tab**.**

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

3.5.4.3 Enable DMZ and Pass Through



Configuration [Help]

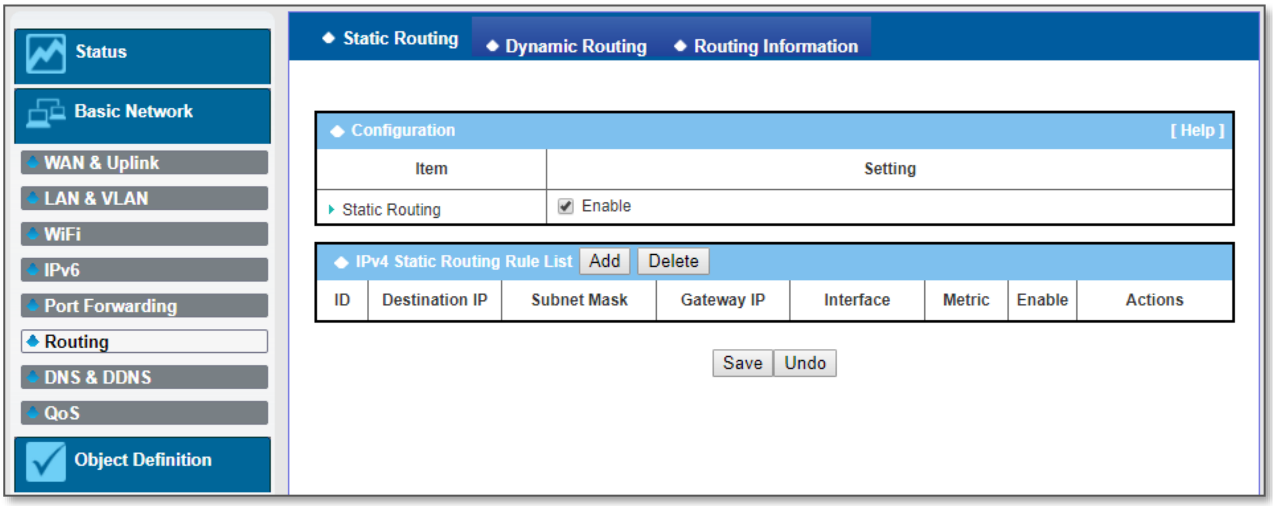
Item	Setting
DMZ	□ Enable ☑ All □ WAN-1 □ WAN-2 □ WAN-3 □ WAN-4 DMZ Host :
Pass Through Enable	☑ IPSec ☑ PPTP ☑ L2TP

Figure 150 – Enable DMZ and Pass-through

Item	Notes	Description
DMZ	Mandatory field. Default is: **ALL**	Check ▯ **Enable** to activate the DMZ function. Define the selected interface as the interface that packets enter the router then fill in the IP address of the Host LAN IP in the DMZ Host field. Select **ALL** for packets coming into the router from any interface.
Pass Through Enable	The boxes are checked by default	Check the box to enable the pass-through function for IPSec, PPTP, and L2TP. With the pass-through function enabled, the VPN hosts behind the router still can connect to remote VPN servers.
Save	Button	Click the **Save** button to save the settings.
Undo	Button	Click the **Undo** button to cancel the settings

Table 89 – Enable DMZ and Pass-through

3.6 Routing



Configuration

Item	Setting
Static Routing	☑ Enable

IPv4 Static Routing Rule List

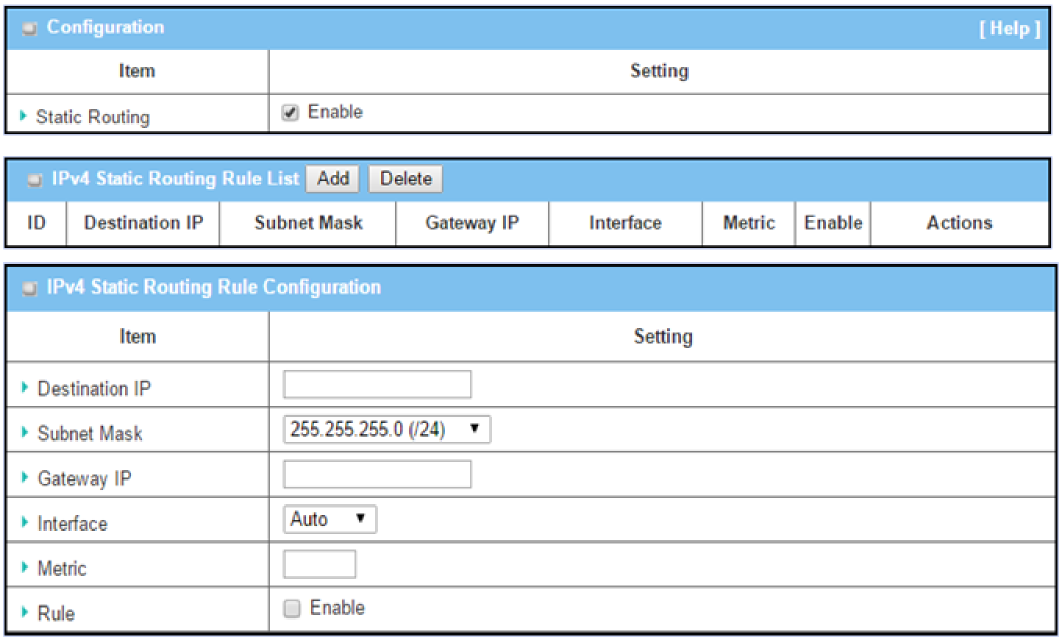
ID	Destination IP	Subnet Mask	Gateway IP	Interface	Metric	Enable	Actions

Figure 151 – Routing

If you have more than one router and subnet, you will need to enable the routing function to allow packets to find the proper routing path and allow different subnets to communicate with each other. Routing is the process of selecting the best path through a network. It is performed for many kinds of networks, like electronic data networks (such as the Internet), by using packet switching technology. The routing process usually directs forwarding 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.

The routing tables record your pre-defined routing paths for specific destination subnets. These are static routes. However, if the contents of routing tables record the obtained routing paths from neighbour routers by using some protocols, such as RIP, OSPF and BGP, this is called dynamic routing.

3.6.1 Static Routing



Configuration

Item	Setting
Static Routing	☑ Enable

IPv4 Static Routing Rule List

ID	Destination IP	Subnet Mask	Gateway IP	Interface	Metric	Enable	Actions

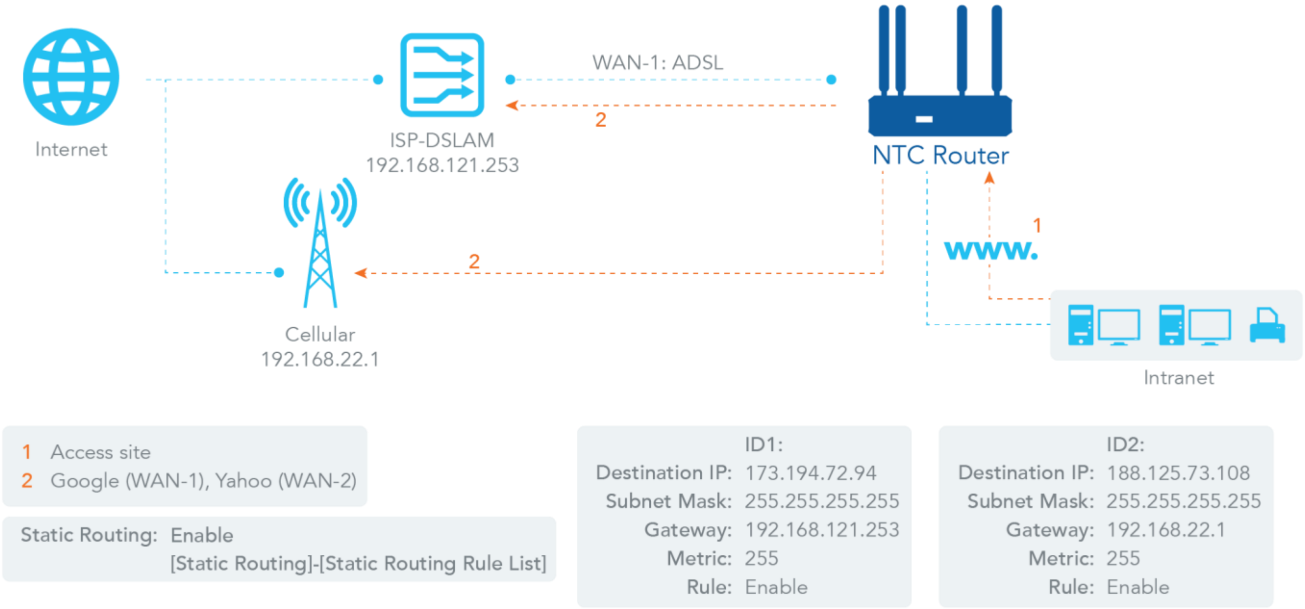
IPv4 Static Routing Rule Configuration

Item	Setting
Destination IP	
Subnet Mask	255.255.255.0 (/24) ▼
Gateway IP	
Interface	Auto ▼
Metric	
Rule	□ Enable

Figure 152 – Static Routing

The Static Routing function lets you define the routing paths for dedicated hosts/servers or subnets to store in the routing table. The router routes incoming packets to different peer gateways based on the routing table.

The administrator of the router can specify what kinds of packets to be transferred via which interface and which peer gateway to their destination. This can be carried out by the Static Routing feature. Dedicated packet flows from the Intranet will be routed to their destination via the pre-defined peer gateway and corresponding router interface that are manually defined in the system routing table.



1 Access site
2 Google (WAN-1), Yahoo (WAN-2)

Static Routing: Enable
[Static Routing]-[Static Routing Rule List]

ID1:	
Destination IP:	173.194.72.94
Subnet Mask:	255.255.255.255
Gateway:	192.168.121.253
Metric:	255
Rule:	Enable

ID2:	
Destination IP:	188.125.73.108
Subnet Mask:	255.255.255.255
Gateway:	192.168.22.1
Metric:	255
Rule:	Enable

Figure 153 – Static Routing

3.6.1.1 Static Routing Setting

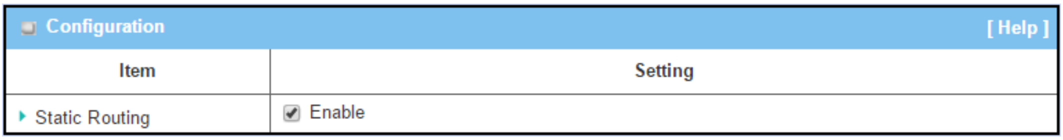
Navigate to the **Basic Network > Routing > Static Routing** tab.

There are three configuration windows for the static routing feature including "Configuration", "Static Routing Rule List" and "Static Routing Rule Configuration" windows. The Configuration window lets you activate the global static routing feature. Even if there are already routing rules, if you want to disable routing temporarily, uncheck the ☐ **Enable** box to disable it. The Static Routing Rule List window lists all your defined static routing rule entries. Use the "Add" or "Edit" buttons to add and create a new static routing rule or to modify an existed one.

When the "Add" or "Edit" buttons are applied, the Static Routing Rule Configuration window appears to let you define a static routing rule.

3.6.1.2 Enable Static Routing

Check ☑ Enable to activate the "Static Routing" feature.



Item	Setting
Static Routing	☑ Enable

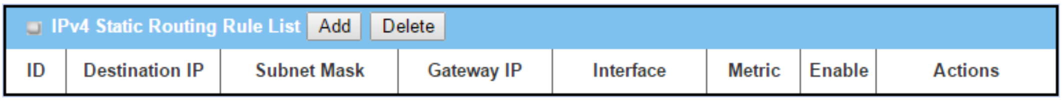
Figure 154 – Enable Static Routing

Item	Notes	Description
Static Routing	Disabled by default.	Check the **Enable** box to activate this function

Table 90 – Enable Static Routing

3.6.1.3 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 the dedicated host/server or subnet, the IP address of a peer gateway, the metric and the rule activation.

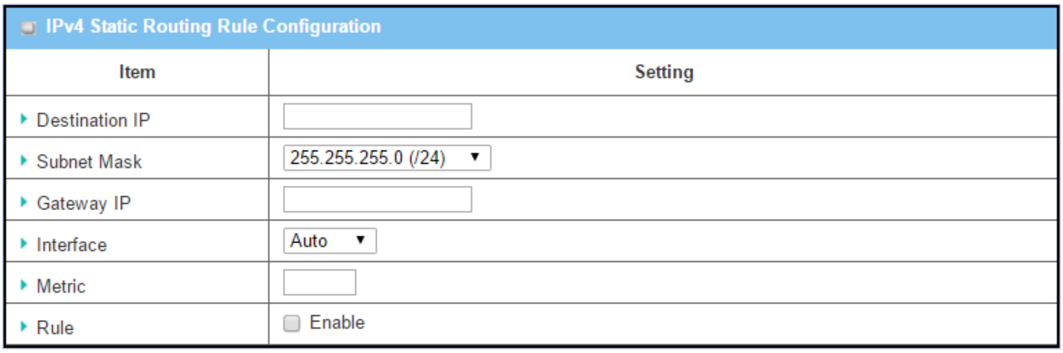


IPv4 Static Routing Rule List Add Delete

ID	Destination IP	Subnet Mask	Gateway IP	Interface	Metric	Enable	Actions

Figure 155 – Create / Edit Static Routing Rules

The router allows you to customise 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 Rule Configuration

Item	Setting
Destination IP	
Subnet Mask	255.255.255.0 (/24) ▼
Gateway IP	
Interface	Auto ▼
Metric	
Rule	□ Enable

Figure 156 – IPv4 Static Routing Rule Configuration

Item	Notes	Description
Destination IP	Mandatory field. Enter in IPv4 format.	Specify the Destination IP of this static routing rule.
Subnet Mask	255.255.255.0 Default setting: **(/24)**	Specify the Subnet Mask of this static routing rule.
Gateway IP	Mandatory field. Enter in IPv4 format.	Specify the Gateway IP of this static routing rule.
Interface	Default setting: **Auto**	Select the Interface of this static routing rule. It can be **Auto**, or the available WAN / LAN interfaces.
Metric	Mandatory field. Numeric string format.	The Metric of this static routing rule. Value Range: 0 - 255.
Rule	Disabled by default.	Click ☑ **Enable** to activate this rule.
Save	Button	Click the **Save** button to save the configuration
Undo	Button	Click the **Undo** button to restore what you just configured back to the previous setting.

Item	Notes	Description
Back	Button	When the **Back** button is clicked the screen will return to the **Static Routing Configuration** page.

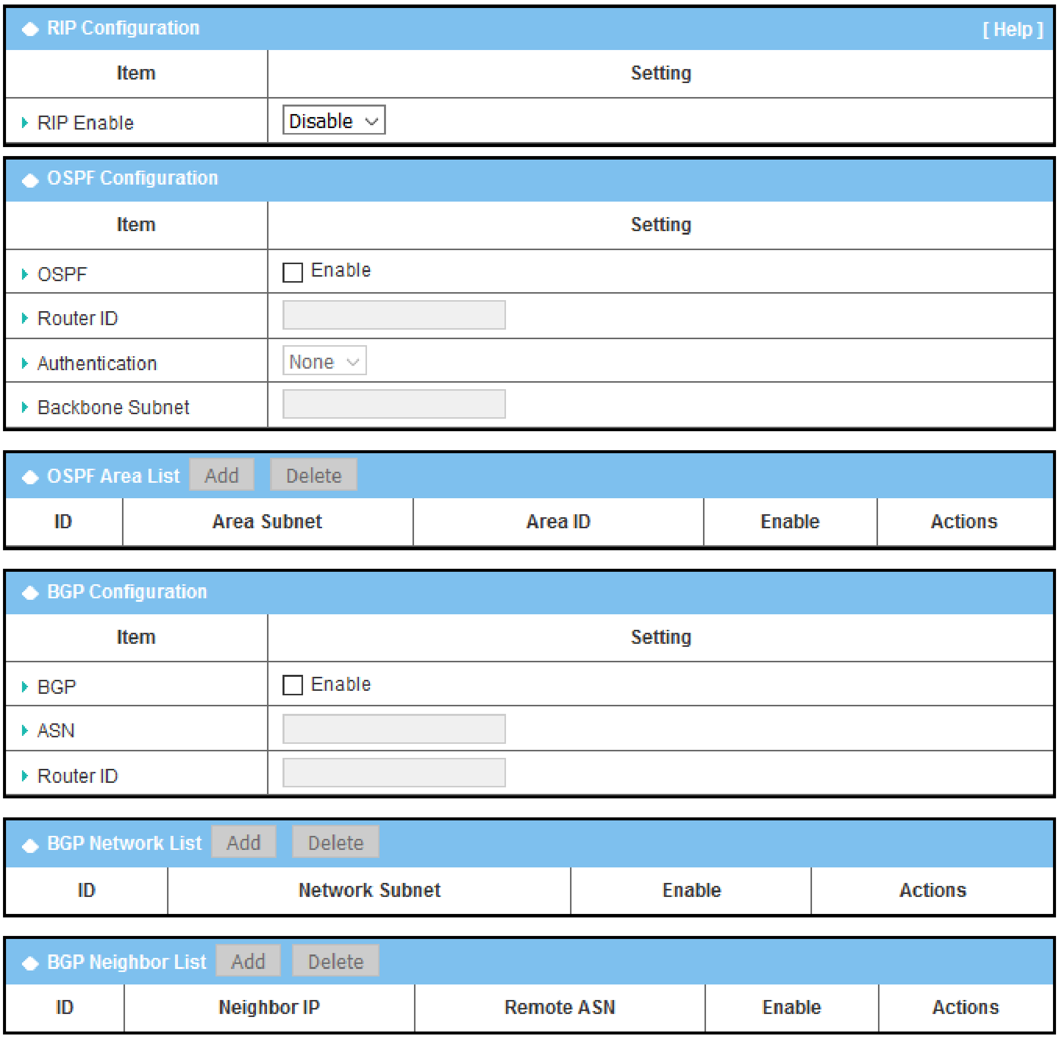
Table 91 – IPv4 Static Routing Rule Configuration

3.6.2 Dynamic Routing

Dynamic Routing, also called adaptive routing, describes the capability of a system through which routes are characterized by their destination, to alter the path that the route takes through the system in response to a change in network conditions.

The NTC-400 Series Router supports dynamic routing protocols, including RIPv1/RIPv2 (Routing Information Protocol), OSPF (Open Shortest Path First), and BGP (Border Gateway Protocol), for you to establish the routing table automatically. The feature of dynamic routing will be very useful when there are lots of subnets in your network. RIP is suitable for small networks while OSPF is more suitable for medium networks. BGP is more suitable for use in a big network infrastructure.

The supported dynamic routing protocols are described as follows.



RIP Configuration [Help]

Item	Setting
RIP Enable	Disable

OSPF Configuration

Item	Setting
OSPF	□ Enable
Router ID	
Authentication	None
Backbone Subnet	

OSPF Area List Add Delete

ID	Area Subnet	Area ID	Enable	Actions

BGP Configuration

Item	Setting
BGP	□ Enable
ASN	
Router ID	

BGP Network List Add Delete

ID	Network Subnet	Enable	Actions

BGP Neighbor List Add Delete

ID	Neighbor IP	Remote ASN	Enable	Actions

Figure 157 – Dynamic Routing

3.6.2.1 RIP Scenario

The Routing Information Protocol (RIP) is one of the oldest distance-vector routing protocols, which employs the hop count as a routing metric. RIP prevents routing loops by implementing a limit on the number of hops allowed in a path from the source to a destination. The maximum number of hops allowed for RIP is 15. This hop limit, however, also limits the size of networks that RIP can support. A hop count of 16 is considered an infinite distance. In other words, the route is considered unreachable. RIP implements the split horizon, route poisoning and hold-down mechanisms to prevent incorrect routing information from being propagated.

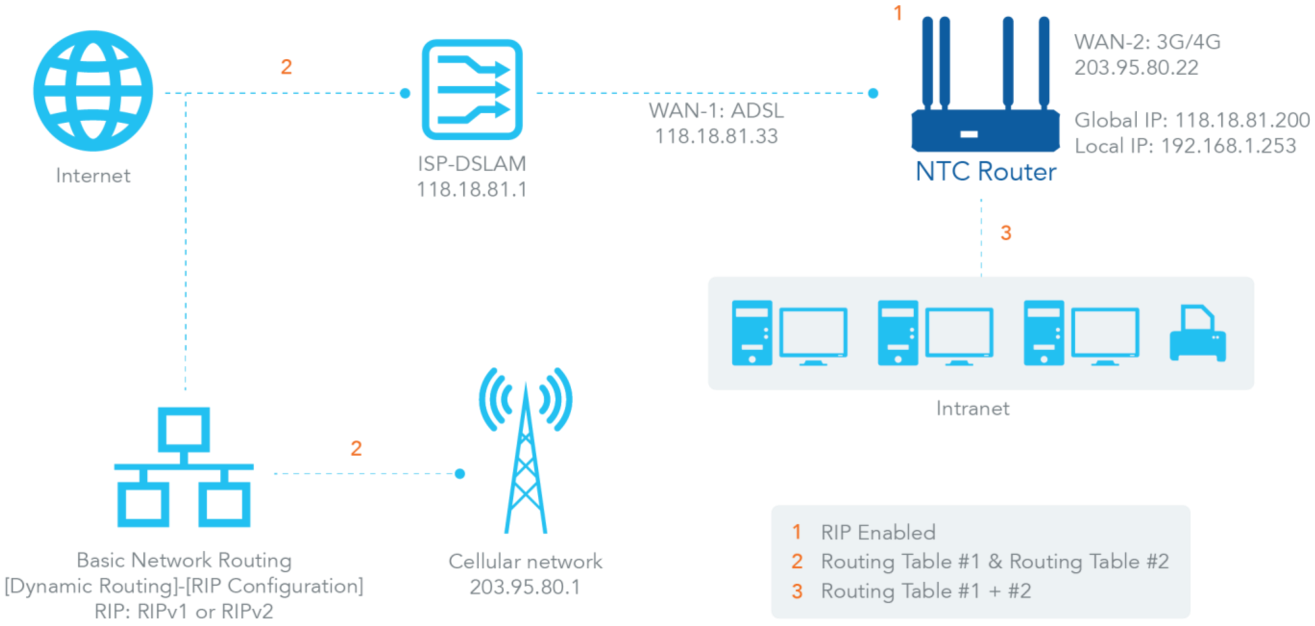


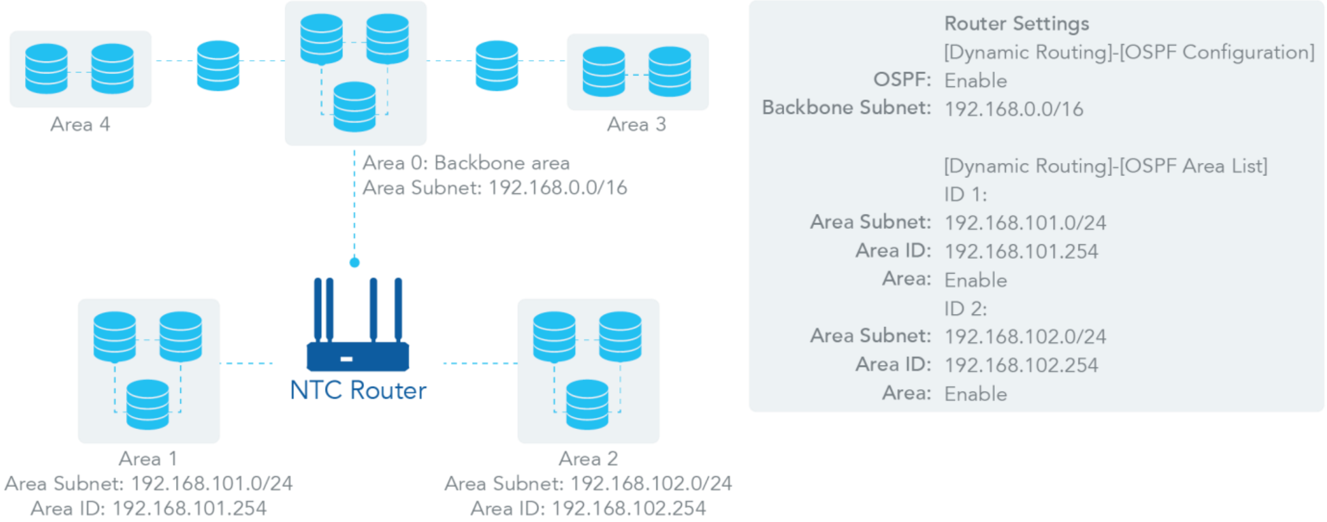
Figure 158 – RIP Scenario

3.6.2.2 OSPF Scenario

Open Shortest Path First (OSPF) is a routing protocol that uses the link state routing algorithm. It is the most widely used interior gateway protocol (IGP) in large enterprise networks. It gathers link state information from available routers and constructs a topology map of the network. The topology is presented as a routing table which routes datagrams based solely on the destination IP address.

The Network administrator can deploy an OSPF gateway in a large enterprise network to get its routing table from the enterprise backbone, and forward routing information to other routers, which are not linked to the enterprise backbone. Usually, an OSPF network is subdivided into routing areas to simplify administration and optimise traffic and resource utilization.

In the diagram below, the OSPF router gathers routing information from the backbone gateways in area 0, and will forward its routing information to the routers in area 1 and area 2 which are not in the backbone.



Router Settings
[Dynamic Routing]-[OSPF Configuration]
OSPF: Enable
Backbone Subnet: 192.168.0.0/16

[Dynamic Routing]-[OSPF Area List]
ID 1:
Area Subnet: 192.168.101.0/24
Area ID: 192.168.101.254
Area: Enable
ID 2:
Area Subnet: 192.168.102.0/24
Area ID: 192.168.102.254
Area: Enable

Figure 159 – OSPF Scenario

3.6.2.3 BGP Scenario

Border Gateway Protocol (BGP) is a standard exterior gateway protocol designed to exchange routing and reachability information between autonomous systems (AS) on the Internet. It usually makes routing decisions based on paths, network policies, or rule-sets.

Most ISPs use BGP to establish routing between one another. Very large private IP networks also use BGP internally. The major BGP gateway within one AS links with some other border gateways for exchanging routing information. It distributes the collected data in AS to all routers in other AS.

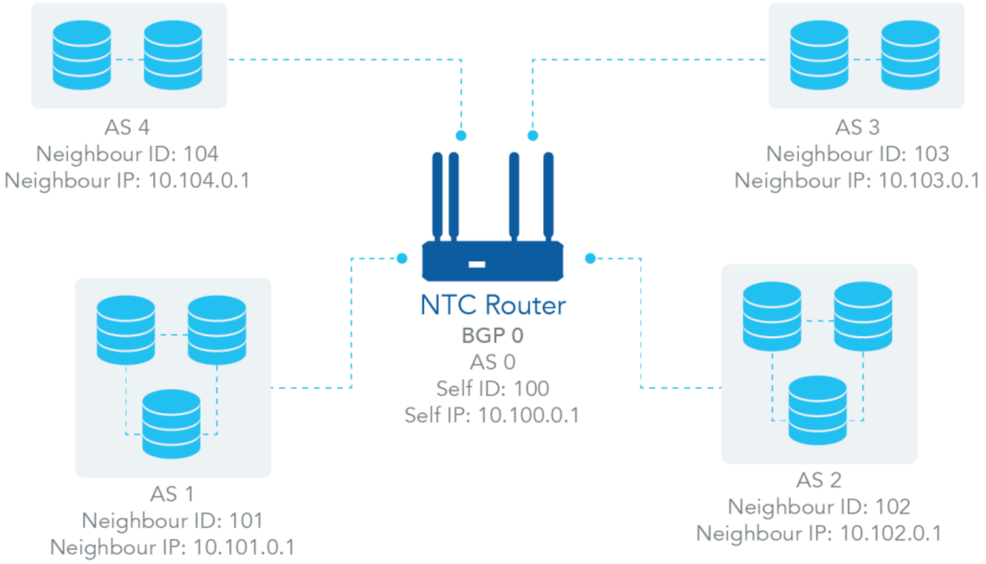


Figure 160 – BGP Scenario

3.6.2.4 Advanced Configurable Routing

The NTC-400 Series Router features configurable routing software called Quagga. It is a routing software package that provides TCP/IP based routing services with routing protocols support such as OSPF and BGP. Quagga is made from a collection of several daemons that work together to build the routing table, so it provides an interactive user interface for each routing protocol and supports common client commands.

3.6.2.5 Dynamic Routing Setting

Navigate to the **Basic Network > Routing > Dynamic Routing** tab.

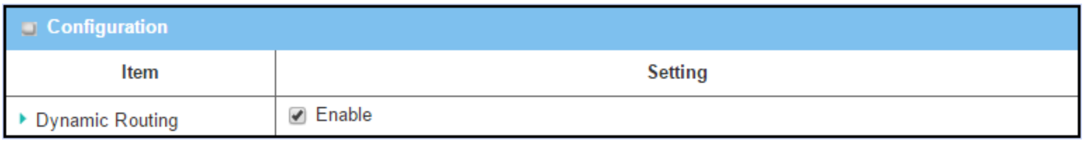
The dynamic routing setting allows user to customize RIP, OSPF, and BGP protocol through the router based on their office setting.

On the "Dynamic Routing" page, there are seven configuration windows for the dynamic routing feature. They are the "RIP Configuration" window, "OSPF Configuration" window, "OSPF Area List", "OSPF Area Configuration", "BGP Configuration", "BGP Neighbor List" and "BGP Neighbor 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 disable it. The "OSPF Configuration" window lets you activate the OSPF dynamic routing protocol and specify its backbone subnet, while the "OSPF Area List" window lists all defined areas in the OSPF network. The "BGP Configuration" window allows you to activate the BGP dynamic routing protocol and specify its self ID. The "BGP Neighbor List" window lists all defined neighbors in the BGP network.

3.6.2.6 Enable Dynamic Routing

Check the "**Enable**" box to activate the "Dynamic Routing" feature.



Configuration

Item	Setting
Dynamic Routing	☑ Enable

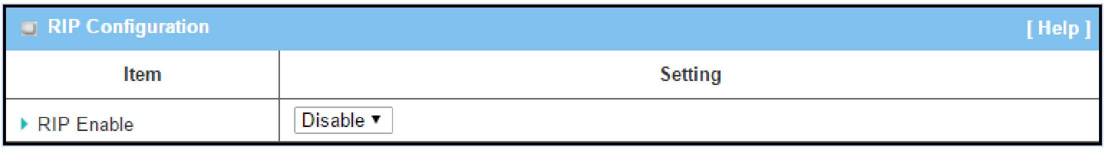
Figure 161 – Dynamic Routing Configuration

Item	Notes	Description
Dynamic Routing	Disabled by default.	Check ☑ **Enable** to activate this function

Table 92 – Dynamic Routing Configuration

3.6.2.7 RIP Configuration

The RIP configuration setting allows you to customise the RIP protocol.



RIP Configuration [Help]

Item	Setting
RIP Enable	Disable ▾

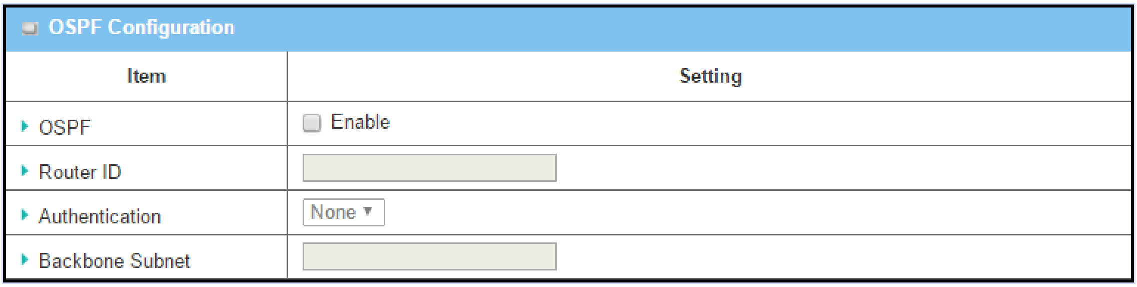
Figure 162 – RIP Configuration

Item	Notes	Description
RIP Enable	Default setting: **Disable**	Select **Disable, RIP v1** or **RIP v2**.

Table 93 – RIP Configuration

3.6.2.8 OSPF Configuration

The OSPF configuration setting allows you to customise the OSPF protocol.



OSPF Configuration

Item	Setting
OSPF	□ Enable
Router ID	
Authentication	None ▾
Backbone Subnet	

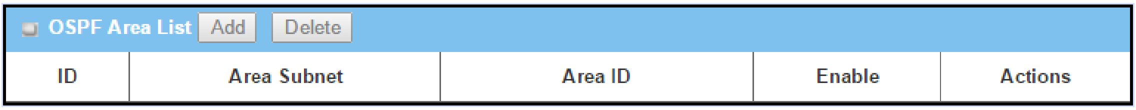
Figure 163 – OSPF Configuration

Item	Notes	Description
OSPF	DisableDefault setting:	Select the Enable box to activate the OSPF protocol.
Router ID	Mandatory field. IPv4 format.	The Router ID of this router on the OSPF protocol.
Authentication	NoneDefault setting:	The Authentication method of this router on OSPF protocol. Select None to disable Authentication on the OSPF protocol. Select Text to enable Text Authentication with entered Key in this field on the OSPF protocol. Select MD5 to enable MD5 Authentication with entered ID and Key in these fields on the OSPF protocol.
Backbone Subnet	Mandatory field. Classless Inter Domain Routing (CIDR) Subnet Mask Notation. (Ex: 192.168.1.0/24)	The Backbone Subnet of this router on the OSPF protocol.

Table 94 – OSPF Configuration

3.6.2.9 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.

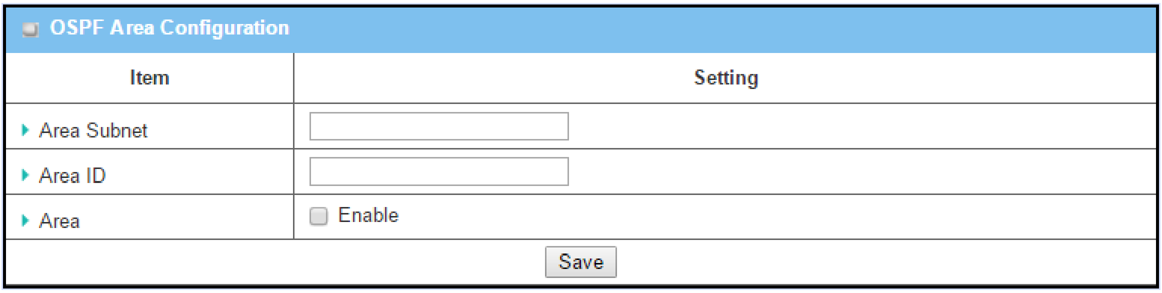


OSPF Area List

ID	Area Subnet	Area ID	Enable	Actions

Figure 164 – Create / Edit OSPF Area Rules

Click the **Add** button to display the **OSPF Area Rule Configuration** screen.



OSPF Area Configuration

Item	Setting
Area Subnet	
Area ID	
Area	□ Enable

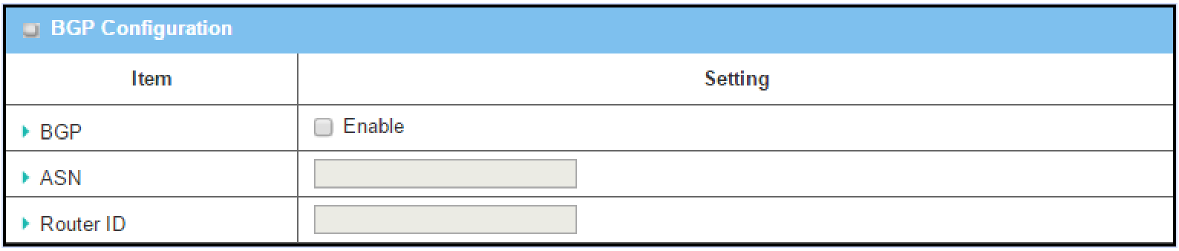
Figure 165 – OSPF Area Configuration

Item	Notes	Description
Area Subnet	Mandatory field. Classless Inter Domain Routing (CIDR) Subnet Mask Notation. (Ex: 192.168.1.0/24)	The Area Subnet of this router on the OSPF Area List.
Area ID	Mandatory field. IPv4 format.	The Area ID of this router on the OSPF Area List.
Area	Disabled by default..	Click the **Enable** box to activate this rule.
Save	Button	Click the **Save** button to save the configuration.

Table 95 – OSPF Area Configuration

3.6.2.10 BGP Configuration

The BGP configuration setting allows you to customise the BGP protocol.



BGP Configuration

Item	Setting
BGP	□ Enable
ASN	
Router ID	

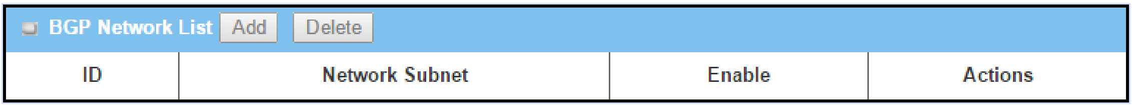
Figure 166 – BGP Configuration

Item	Notes	Description
BGP	Disabled by default.	Check the **Enable** box to activate the BGP protocol.
ASN	Mandatory field. Numeric string.	The ASN Number of this router on the BGP protocol. Value Range: 1 - 4294967295.
Router ID	Mandatory field. IPv4 format.	The Router ID of this router on the BGP protocol.

Table 96 – BGP Configuration

3.6.2.11 Create / Edit BGP Network Rules

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

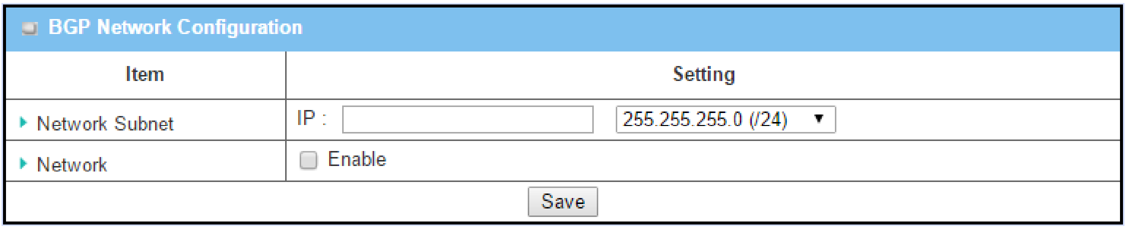


BGP Network List

ID	Network Subnet	Enable	Actions

Figure 167 – Create / Edit BGP Network Rules

Click the **Add** button to display the **BGP Network Rule Configuration** screen.



BGP Network Configuration

Item	Setting
Network Subnet	IP : [ ] 255.255.255.0 (/24) ▼
Network	□ Enable

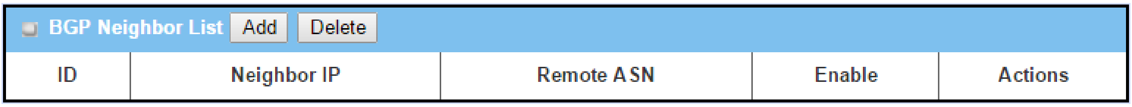
Figure 168 – BGP Network Configuration

Item	Notes	Description
Network Subnet	Mandatory field. IPv4 format.	The Network Subnet of this router on the BGP Network List. It is composed of the IP address in this field and the selected subnet mask.
Network	Disabled by default.	Click the **Enable** box to activate this rule.
Save	Button	Click the **Save** button to save the configuration

Table 97 – BGP Network Configuration

3.6.2.12 Create / Edit BGP Neighbour Rules

The router allows you to customise your BGP Neighbor rules. It supports up to a maximum of 32 rule sets.

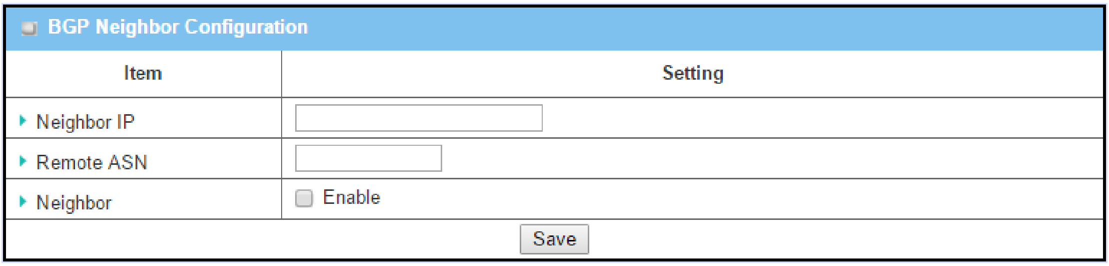


BGP Neighbor List Add Delete

ID	Neighbor IP	Remote ASN	Enable	Actions

Figure 169 – Create / Edit BGP Neighbor Rules

Click the **Add** button to display the **BGP Neighbor Rule Configuration** screen.



BGP Neighbor Configuration

Item	Setting
Neighbor IP	[ ]
Remote ASN	[ ]
Neighbor	□ Enable

Figure 170 – BGP Neighbor Configuration

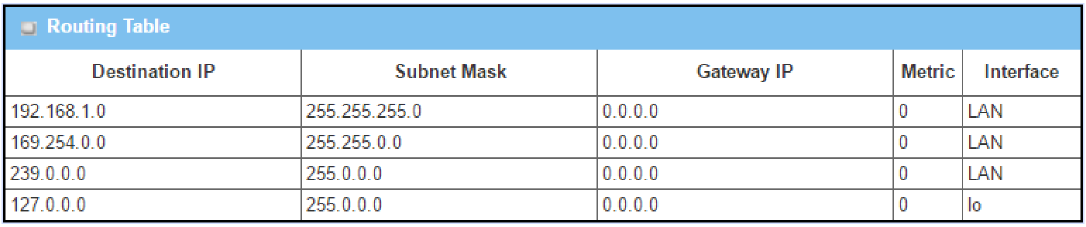
Item	Notes	Description
Neighbor IP	Mandatory field. IPv4 format.	The Neighbor IP of this router on the BGP Neighbor List.
Remote ASN	Mandatory field. Numeric string format.	The Remote ASN of this router on the BGP Neighbor List. Value Range: 1 - 4294967295.
Neighbor	Disabled by default.	Click the Enable box to activate this rule.
Save	Button	Click the Save button to save the configuration

Table 98 – BGP Neighbor Configuration

3.6.3 Routing Information

Routing information allows you to view the routing table and policy routing information.

Navigate to the **Basic Network > Routing > Routing Information** tab**.**



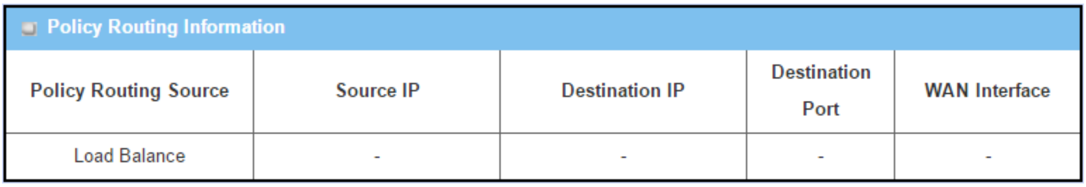
Routing Table

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

Figure 171 – Routing Table

Item	Notes	Description
Destination IP	N/A	Routing record of Destination IP. IPv4 Format.
Subnet Mask	N/A	Routing record of Subnet Mask. IPv4 Format.
Gateway IP	N/A	Routing record of Gateway IP. IPv4 Format.
Metric	N/A	Routing record of Metric. Numeric String Format.
Interface	N/A	Routing record of Interface Type. String Format.

Table 99 – Routing Table



Policy Routing Information

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

Figure 172 – Policy Routing Information

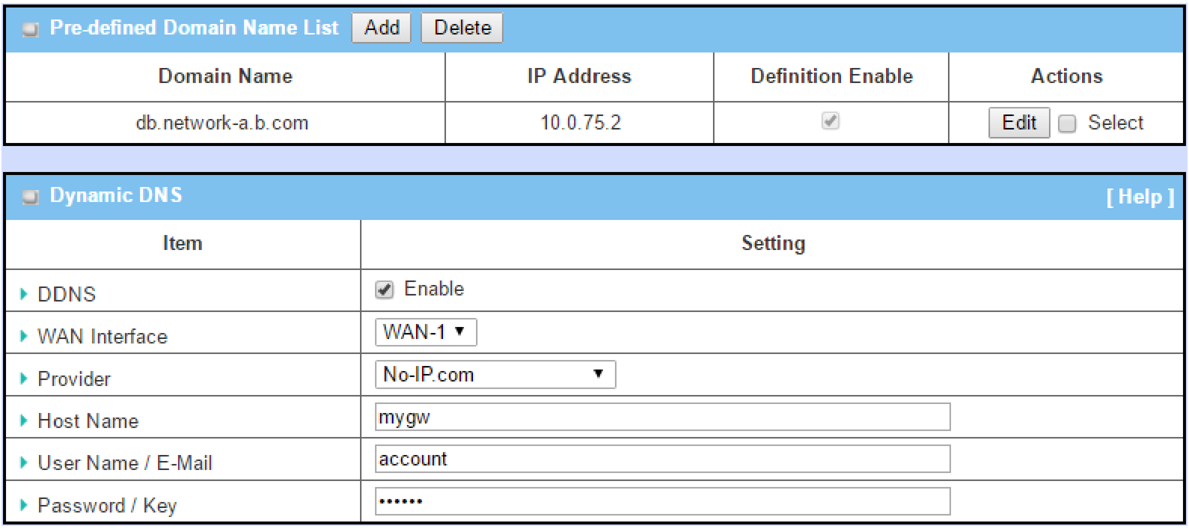
Item	Notes	Description
Policy Routing Source	N/A	Policy Routing of Source. String Format.
Source IP	N/A	Policy Routing of Source IP. IPv4 Format.
Destination IP	N/A	Policy Routing of Destination IP. IPv4 Format.
Destination Port	N/A	Policy Routing of Destination Port. String Format.
WAN Interface	N/A	Policy Routing of WAN Interface. String Format.

Table 100 – Policy Routing Information

3.7 DNS & DDNS

When you have an Internet plan that provides a dynamic IP address, that is, an address which is dynamically assigned and changes each time you connect, an easy way to provide a permanent address is to use a Dynamic DNS service. There are both free and paid DDNS services available.

3.7.1 DNS & DDNS Configuration



Domain Name	IP Address	Definition Enable	Actions
db.network-a.b.com	10.0.75.2	☑	Edit □ Select

Item	Setting
DDNS	☑ Enable
WAN Interface	WAN-1 ▾
Provider	No-IP.com ▾
Host Name	mygw
User Name / E-Mail	account
Password / Key	••••••

Figure 173 – DNS & DDNS Configuration

3.7.1.1 DNS

The NTC-400 Series Router can operate as a DNS server for the connected local clients which get their LAN IPs from the dynamic IP scheme. You can create a private host list for easy access to the hosts / servers in your intranet with corresponding domain names.

3.7.1.2 Dynamic DNS

To host your server on a changing IP address, you must use a dynamic domain name service (DDNS). Therefore, anyone wishing to reach your host only needs to know the domain name. Dynamic DNS maps the name of your host to your current IP address, which changes each time you connect your Internet service provider.

The Dynamic DNS service allows the gateway to alias a public dynamic IP address to a static domain name, allowing the gateway to be more easily accessed from anywhere on the Internet.

In the diagram below, the user has registered a domain name with a third-party DDNS service provider (NO-IP) to use the DDNS function. Once the IP address of the designated WAN interface has changed, the dynamic DNS agent on the router will inform the DDNS server of the new IP address. The server automatically re-maps the domain name with the changed IP address. Other hosts or remote users on the Internet can connect to the router by using the domain name regardless of the changing global IP address.

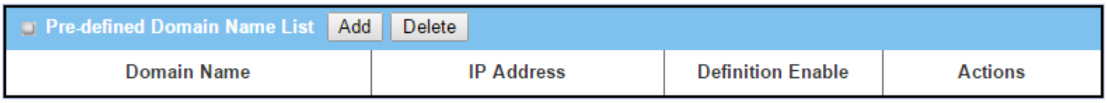
3.7.1.3 DNS & DDNS Setting

Navigate to the **Basic Network > DNS & DDNS > Configuration** tab.

The DNS & DDNS setting allows you to create/modify a pre-defined domain name list and setup the Dynamic DNS feature.

3.7.1.4 Create / Edit Pre-defined Domain Name List

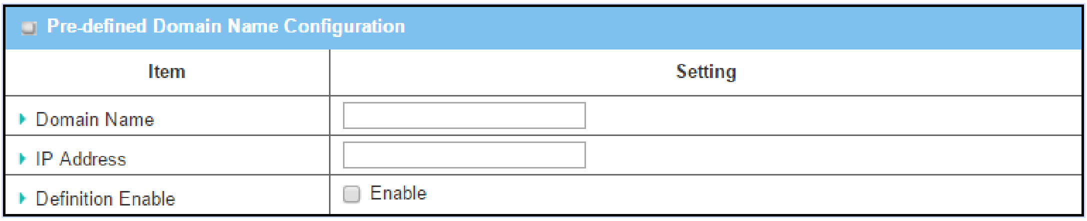
The NTC-400 Series Router allows you to customise your pre-defined domain name list. It supports up to a maximum of 128 sets.



Domain Name	IP Address	Definition Enable	Actions

Figure 174 – Pre-defined Domain Name List

Click the **Add** button to display the **Pre-defined Domain Name Configuration** screen.



Item	Setting
Domain Name	
IP Address	
Definition Enable	□ Enable

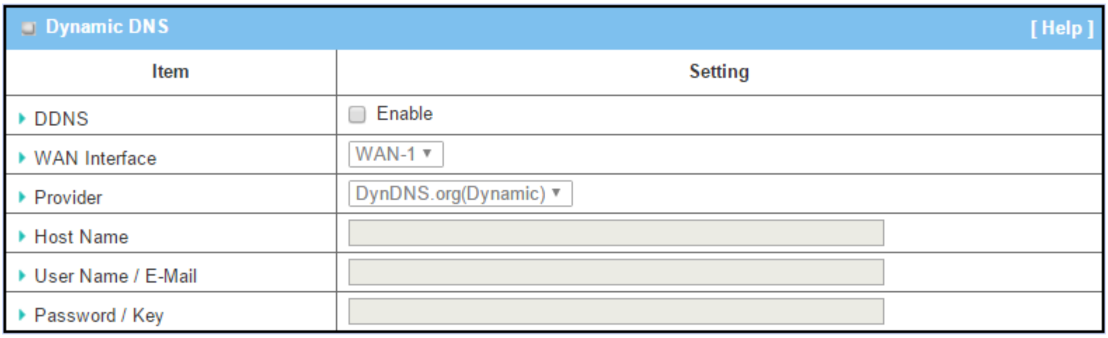
Figure 175 – Pre-defined Domain Name Configuration

Item	Notes	Description
Domain Name	Mandatory field. String format.	Enter a domain name to map to the IP Address. Value Range: at least 1 character is required.
IP Address	Mandatory field. IPv4 format.	Enter an IP Address that the Domain Name is mapped to.
Definition Enable	Disabled by default.	Click ☑ **Enable** to activate this rule.
Save	Button	Click **Save** to save the settings
Undo	Button	Click **Undo** to cancel the settings
Back	Button	When the **Back** button is clicked the screen will return to the Dynamic DNS configuration page.

Table 101 – Pre-defined Domain Name Configuration

3.7.1.5 Setup Dynamic DNS

The NTC-400 Series Router allows you to customise your Dynamic DNS settings.



Dynamic DNS [Help]

Item	Setting
DDNS	□ Enable
WAN Interface	WAN-1 ▾
Provider	DynDNS.org(Dynamic) ▾
Host Name	
User Name / E-Mail	
Password / Key	

Figure 176 – Dynamic DNS

Item	Notes	Description
DDNS	Disabled by default.	Check the Enable box to activate this function.
WAN Interface	WAN 1Default setting:	Select the WAN Interface IP Address of the gateway.
Provider	Default setting: **DynDNS.org (Dynamic)**	Select your DDNS provider for Dynamic DNS: **DynDNS.org(Dynamic)**, **DynDNS.org(Custom)**, **NO-IP.com**, etc..
Host Name	Mandatory field. String format.	Your registered host name of Dynamic DNS. Value Range: 0 - 63 characters.
User Name / E-Mail	Mandatory field. String format.	Enter your User name or E-mail addresss of Dynamic DNS.
Password / Key	Mandatory field. String format.	Enter your Password or Key of Dynamic DNS.
Save	Button	Click **Save** to save the settings
Undo	Button	Click **Undo** to cancel the settings

Figure 177 – Dynamic DNS

3.8 QoS

Total Internet traffic has increased rapidly as the demand for mobile applications including games, messaging apps, voice over IP, peer-to-peer file transfers and video use goes up. To enable the smooth operation of all of these services, the entire network must ensure them via a connection service guarantee.

The main goal of QoS (Quality of Service) is prioritizing incoming data, and preventing data loss due to factors such as jitter, delay and dropping. Another important aspect of QoS is ensuring that prioritizing one data flow doesn’t interfere with other data flows. So, QoS helps to prioritize data as it enters your router. By attaching special identification marks or headers to incoming packets, QoS determines which queue the packets enter, based on priority. This is useful when there are certain types of data you want to give higher priority to, such as voice packets given higher priority than Web data packets.

To utilize your network throughput completely, the administrator must define bandwidth control rules carefully to balance the utilization of network bandwidth for all users to access. An access gateway must satisfy the requirements of latency-critical applications, minimum access right guarantee, fair bandwidth usage for the same subscribed condition and flexible bandwidth management.

3.8.1 QoS Configuration

The NTC-400 Series Router provides lots of flexible rules for you to set QoS policies. You need to know who needs to be managed, what kind of service needs to be managed and how should traffic be prioritized before you create your own policies. Once you have this information, you can continue to learn functions in this section in more detail.

3.8.1.1 QoS Rule Configuration

To add a new QoS rule or edit an existing one, navigate to the "QoS Rule Configuration" window. The parameters in a rule include the applied 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. Following diagram illustrates how to organize a QoS rule.

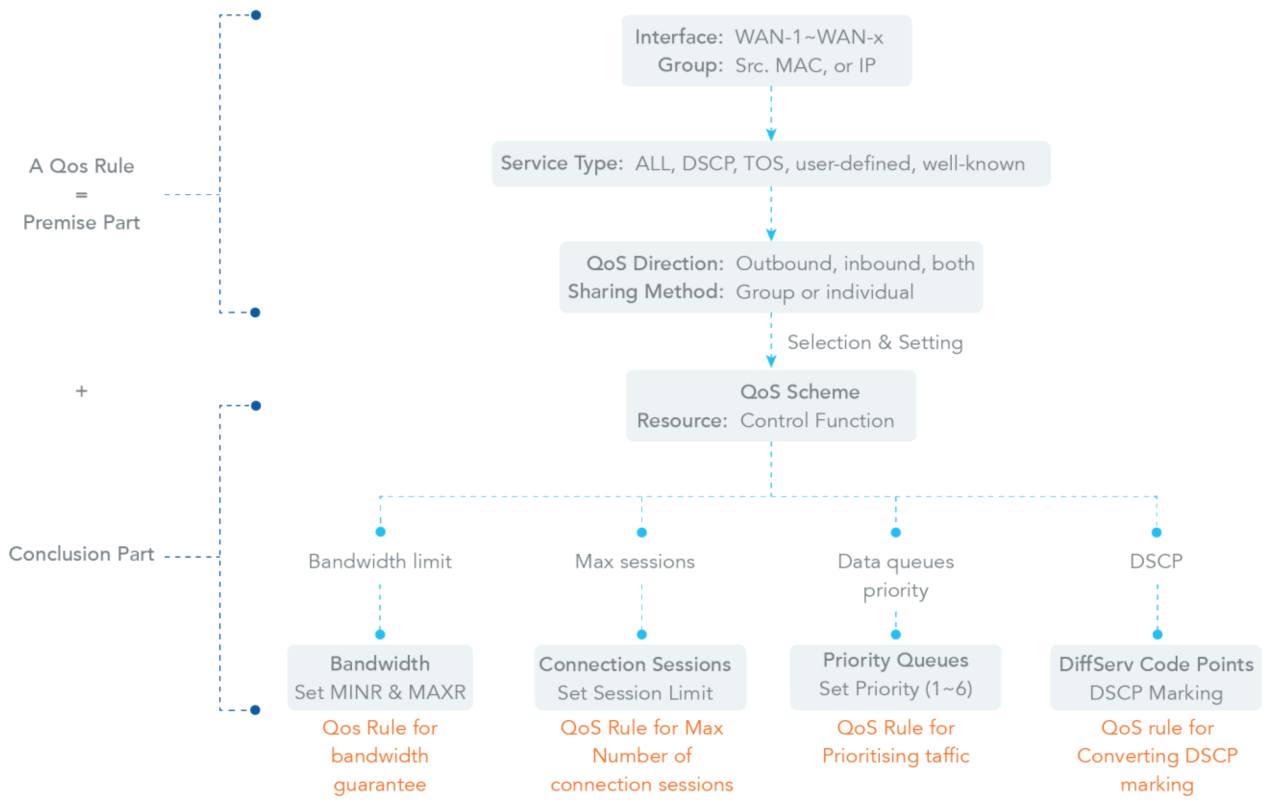

A Qos Rule
=
Premise Part
+
Conclusion Part
Interface: WAN-1~WAN-x
Group: Src. MAC, or IP
Service Type: ALL, DSCP, TOS, user-defined, well-known
QoS Direction: Outbound, inbound, both
Sharing Method: Group or individual
Selection & Setting
QoS Scheme
Resource: Control Function
Bandwidth limit
Max sessions
Data queues priority
DSCP
Bandwidth
Set MINR & MAXR
Connection Sessions
Set Session Limit
Priority Queues
Set Priority (1~6)
DiffServ Code Points
DSCP Marking
Qos Rule for bandwidth guarantee
QoS Rule for Max Number of connection sessions
QoS Rule for Prioritising taffic
QoS rule for Converting DSCP marking

Figure 178 – QoS Rule Configuration

In the above diagram, a QoS rule is organized 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 monitored and the sharing method of group control or individual control. However, in the conclusion part, you must specify the kind of system resource to distribute and the control function based on the chosen system resource for the rule.

Rule-based QoS has the 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

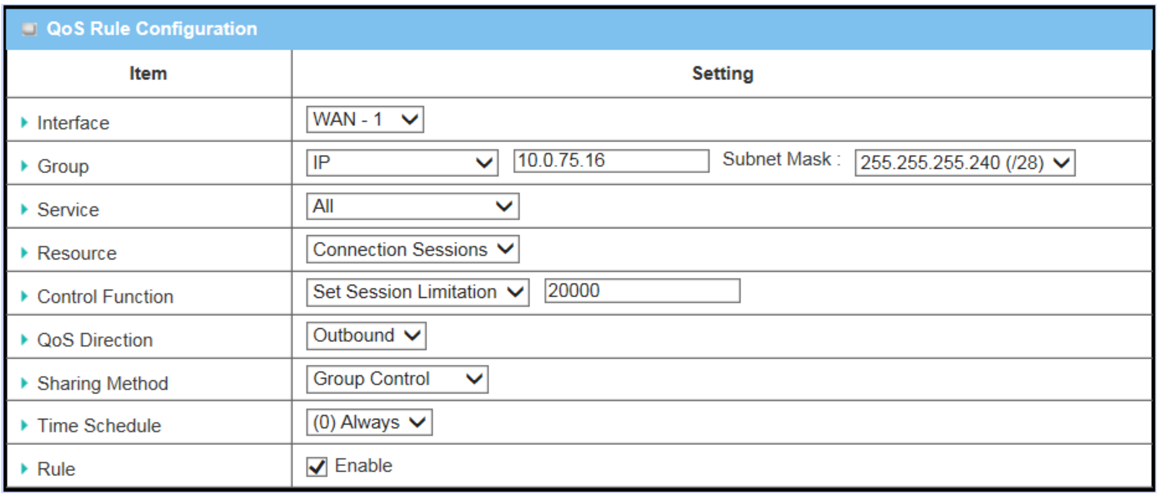
  One QoS rule can be applied to an individual member or a whole group in the target group.

- Outbound / Inbound Control

  One QoS rule can be applied to the outbound or inbound direction of packet flow or both.

Two QoS rule examples are listed below.

3.8.1.2 QoS Rule Example #1 - Connection Sessions



QoS Rule Configuration

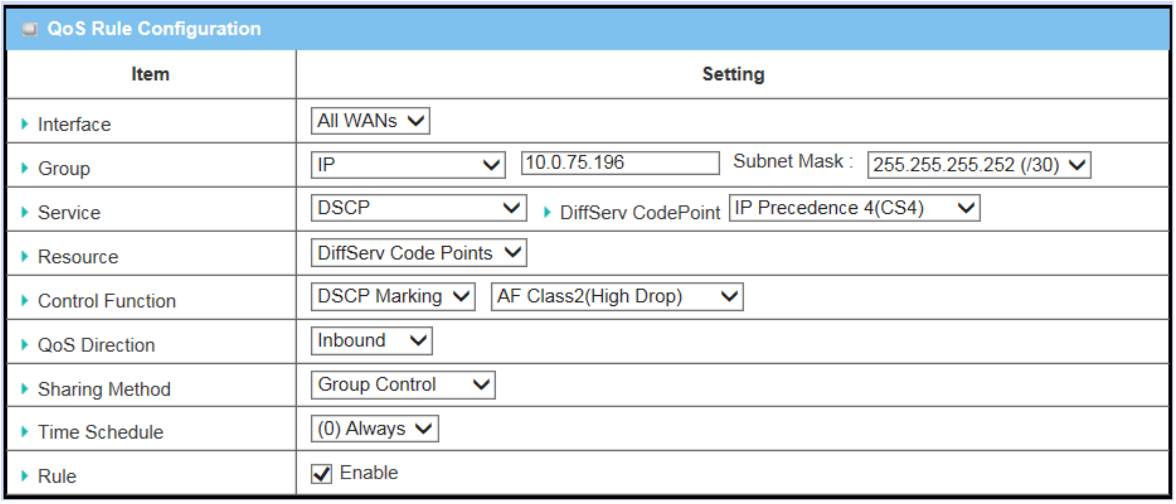
Item	Setting
Interface	WAN - 1
Group	IP; 10.0.75.16; Subnet Mask : 255.255.255.240 (/28)
Service	All
Resource	Connection Sessions
Control Function	Set Session Limitation; 20000
QoS Direction	Outbound
Sharing Method	Group Control
Time Schedule	(0) Always
Rule	☑ Enable

Figure 179 – QoS Rule Example #1 - Connection Sessions

When the administrator wants to limit the maximum number of connection sessions from client hosts (IP 10.0.75.16 - 31) to 20000 to avoid resource shortage, they can configure a rule as shown above.

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

3.8.1.3 QoS Rule Example #2 – DifferServ Code Points



QoS Rule Configuration

Item	Setting
Interface	All WANs
Group	IP; 10.0.75.196; Subnet Mask : 255.255.255.252 (/30)
Service	DSCP; DiffServ CodePoint: 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

Figure 180 – QoS Rule Example #2 - DifferServ Code Points

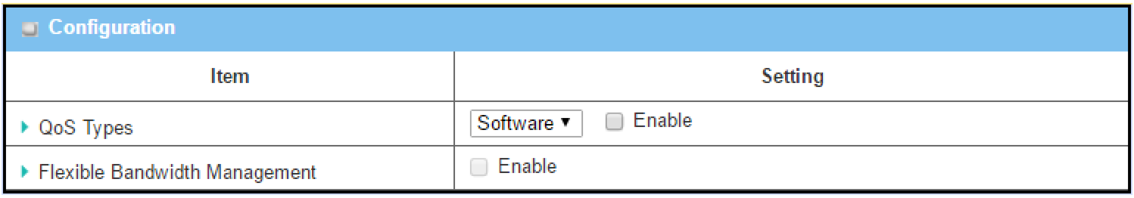
When the administrator of the router wants to convert the code point value, "IP Precedence 4(CS4)", in the packets from client hosts (IP 10.0.75.196 - 199) to the code value, "AF Class2(High Drop)", they can use the "Rule-based QoS" function to carry out this rule by defining a QoS rule as shown in the above configuration. Under such configuration, all packets from WAN interfaces to LAN IP address 10.0.75.196 - 10.0.75.199 which have DiffServ code points with the “IP Precedence 4(CS4)” value will be modified by the “DSCP Marking” control function with “AF Class 2(High Drop)” value at any time.

3.8.1.4 QoS Configuration Setting

Navigate to the **Basic Network > QoS > Configuration t**ab.

The "Configuration" window allows you to activate the Rule-based QoS function. In addition, you can also enable the "Flexible Bandwidth Management" (FBM) feature for better utilization of system bandwidth. On the “System Configuration” window, you can configure the total bandwidth and session of each WAN. The "QoS Rule List" window displays all your defined QoS rules.

3.8.1.5 Enable QoS Function



Configuration

Item	Setting
QoS Types	Software ▾ □ Enable
Flexible Bandwidth Management	□ Enable

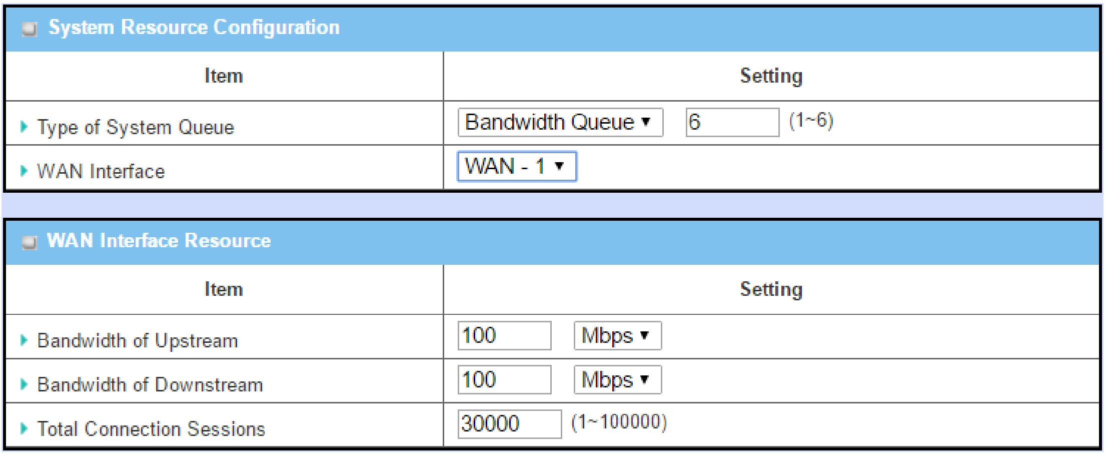
Figure 181 – QoS Configuration

Item	Notes	Description
QoS Type	SoftwareDefault setting: The function is disabled by default.	Select the QoS Type from the dropdown list, and then click the Enable box to activate the QoS function.
Flexible Bandwidth Management	Disabled by default.	Click the Enable box to activate the Flexible Bandwidth Management function.
Save	Button	Click the Save button to save the settings.

Table 102 – QoS Configuration

Check the "Enable" box to activate the "Rule-based QoS" function. You can also enable the Flexible Bandwidth Management (FBM) feature when needed. When FBM is enabled, the system adjusts the bandwidth distribution dynamically based on the current bandwidth usage situation to reach maximum system network performance transparently to all users. The bandwidth subscription profiles of all current users are considered in the system's automatic adjusting algorithm.

3.8.1.6 Setup System Resource



System Resource Configuration

Item	Setting
Type of System Queue	Bandwidth Queue ▾ 6 (1~6)
WAN Interface	WAN - 1 ▾

WAN Interface Resource

Item	Setting
Bandwidth of Upstream	100 Mbps ▾
Bandwidth of Downstream	100 Mbps ▾
Total Connection Sessions	30000 (1~100000)

Figure 182 – System Resource Configuration

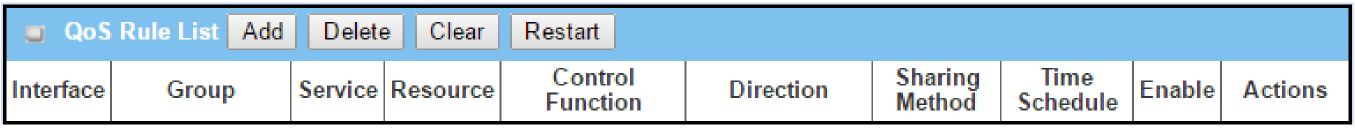
Item	Notes	Description
Type of System Queue	Mandatory field. Default setting: **Bandwidth Queue, 6**	Define the system queues that are available for the QoS settings. The supported type of system queues: **Bandwidth Queue** and **Priority Queues** Value Range: 1 - 6.
WAN Interface	Default setting: **WAN-1**	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	Button	Click the **Save** button to save the settings.

Table 103 – System Resource Configuration

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

3.8.1.7 Create / Edit QoS Rules

After enabling the QoS function and configured the system resources, you have to further specify some QoS rules for provide better service on the interested traffics. The gateway supports up to a maximum of 128 rule-based QoS rule sets.

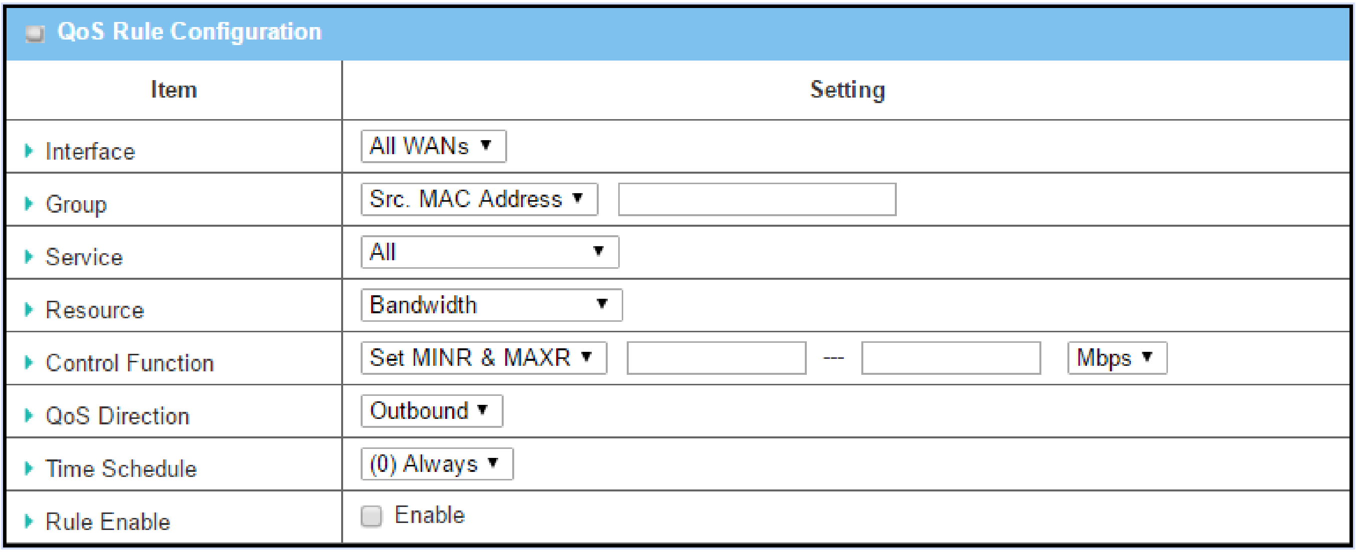


QoS Rule List

Interface	Group	Service	Resource	Control Function	Direction	Sharing Method	Time Schedule	Enable	Actions

Figure 183 – QoS Rule List

Click the **Add** button to display the **QoS Rule Configuration** screen.



QoS Rule Configuration

Item	Setting
Interface	All WANs ▾
Group	Src. MAC Address ▾
Service	All ▾
Resource	Bandwidth ▾
Control Function	Set MINR & MAXR ▾ --- Mbps ▾
QoS Direction	Outbound ▾
Time Schedule	(0) Always ▾
Rule Enable	□ Enable

Figure 184 – QoS Rule Configuration

Item	Notes	Description
Interface	Mandatory field. Default setting: **All WANs**	Specify the WAN interface to apply the QoS rule to. Select **All WANs** or a particular WAN interface to filter the packets entering to or leaving from the interface(s).
Group	Mandatory field. Default setting: **Src. MAC Address**	Specify the Group category for the QoS rule: **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; • Select **Host Name** to prioritize packets based on a group of a pre-configured group of hosts 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 the corresponding ☑ **QoS** checkbox in the **Multiple Bound Services** field is checked before the **Host Group** option becomes available. Refer to **Object Definition > Grouping > Host Grouping**.
Service	Mandatory field. Default setting: **All**	Specify the service type of traffic that must be applied with the QoS rule: **All, DSCP**, **TOS**, **User-defined Service**, or **Well-known Service** • Select **All** for all packets. • Select **DSCP** for DSCP type packets only.

Item	Notes	Description
		- Select **TOS** for TOS type packets only. You must 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 must define the port range and protocol as well. - Select **Well-known Service** for specific application packets only. You must select the required service from the dropdown list as well.
Resource, and Control Function	Mandatory field.	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 Direction	Mandatory field. Default setting: **Outbound**	Specify the traffic flow direction for the packets to apply the QoS rule. It can be Outbound, Inbound, or Both. - **Outbound** – Select Outbound to prioritize the traffic going to the Internet via the specified interface. Under such situation, the hosts specified in the Group field is a source group. - **Inbound** – Select Inbound to prioritize 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 prioritize the traffic 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	Mandatory field. Default setting: **Group Control**	Specify the preferred sharing method for how to apply the QoS rule on the selected group: **Individual Control** or **Group Control** - **Individual Control** – If Individual Control is selected, each host in the group will have their 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	Mandatory field. Default setting: **(0) Always**	Apply a Time Schedule to this rule; otherwise leave it as **(0) Always**. (refer to **Object Definition > Scheduling > Configuration settings**)

Item	Notes	Description
Rule Enable	Disabled by default.	Click ☑ **Enable** to activate this QoS rule.
Save	Button	Click the **Save** button to save the settings.

Table 104 – QoS Rule Configuration

4 Object Definition

4.1 Scheduling

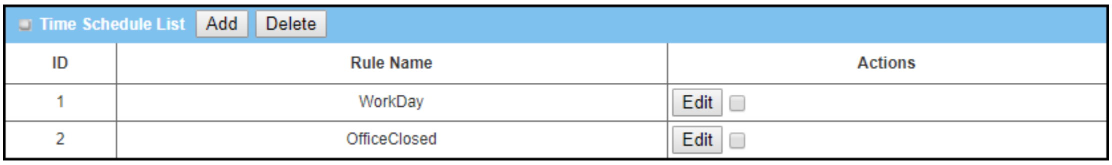
Scheduling allows you to create time schedule rules which can be consistently applied to a range of NTC-400 Series Router functionality. For example, you may want a schedule rule for Office Hours and one for Closing Hours.

4.1.1 Scheduling Configuration

To create a pre-defined scheduling rule:

1 From the **Object Definition** submenu select **Scheduling** then click its **Configuration** tab.

2 In the **Time Schedule List** you can manage existing schedules or create new ones:



Time Schedule List [Add] [Delete]

ID	Rule Name	Actions
1	WorkDay	Edit □
2	OfficeClosed	Edit □

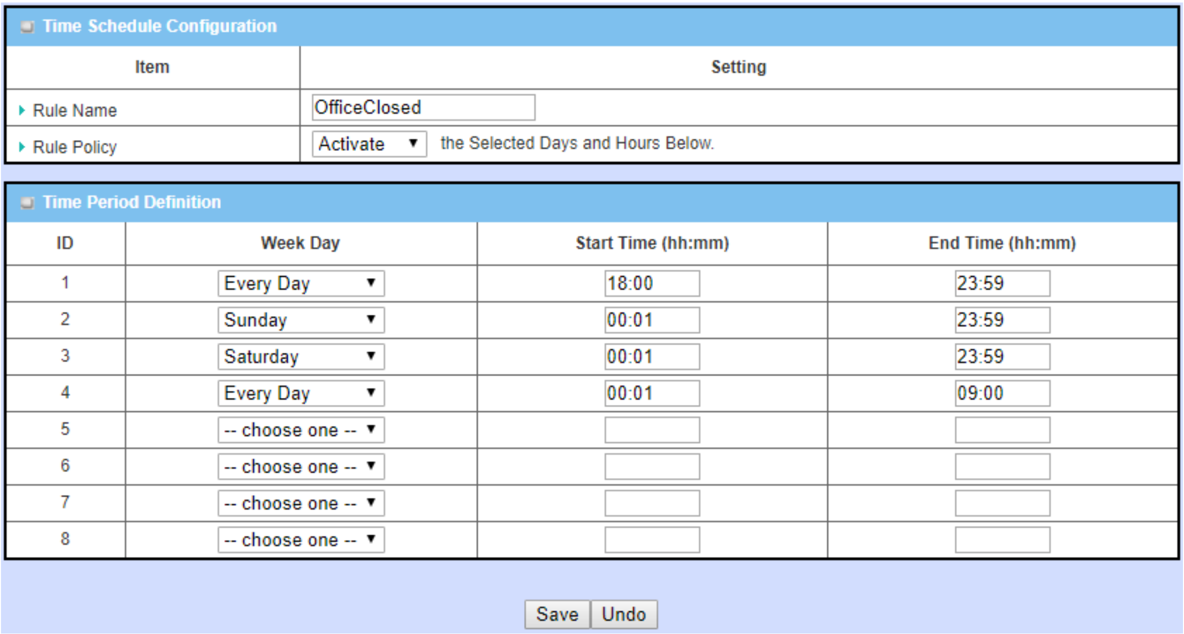
Figure 185 – Time Schedule list

Item	Notes	Description
ID	Integer. Auto-fill.	The Time Schedule's system-generated reference number.
Rule Name	Uneditable in this list.	The Rule Names in this list will populate drop down lists throughout the NTC-400 Series Router that reference Scheduling Rules. Rule Name is entered in Time Schedule Configuration section, see next. Click this group's **Edit** button in the Actions column to change this name.
Actions - Edit	Button	Modify an existing Time Schedule by clicking its corresponding **Edit** button in the Actions section.
Actions - select	Checkbox	Redundant or obsolete time schedules can be permanently removed by checking ☑ for those schedules and then clicking the **Delete** button in the Time Schedule List's title bar.
Add	Button	Click the **Add** button to configure a new time schedule rule, see next section.
Delete	Button	Use the **Delete** button in conjunction with the ☑ checkbox in the Actions section to permanently delete schedules that are no longer required.
Save	Button	Click **Save** to save the settings.
Refresh	Button	Click **Refresh** to update the list.

Table 105 – Time Schedule List

4.1.1.1 Create a Time Schedule

When **Add** button is clicked the **Time Schedule Configuration** and **Time Period Definition** sections display.



Time Schedule Configuration

Item	Setting
Rule Name	OfficeClosed
Rule Policy	Activate ▼ the Selected Days and Hours Below.

Time Period Definition

ID	Week Day	Start Time (hh:mm)	End Time (hh:mm)
1	Every Day ▼	18:00	23:59
2	Sunday ▼	00:01	23:59
3	Saturday ▼	00:01	23:59
4	Every Day ▼	00:01	09:00
5	-- choose one -- ▼		
6	-- choose one -- ▼		
7	-- choose one -- ▼		
8	-- choose one -- ▼		

Figure 186 – Time Schedule configuration

Item	Notes	Description
Rule Name	Enter string: any text, spaces allowed	Enter a meaningful name. This Rule Name will be included in the drop down lists throughout the NTC-400 Series Router that reference Scheduling Rules.
Rule Policy	Default setting: Inactive	Inactivate/activate the function during the time periods defined below.

Table 106 – Time Schedule Configuration

Item	Notes	Description
ID	Reference Integer	Use this reference number to apply the time schedule rule to various applications found throughout the NTC-400 Series Router.
Week Day	Drop down list	Select **Every Day** or one week day.
Start Time	Time format (hh:mm) 24 hour time.	Start time in the selected weekday(s)
End Time	Time format (hh:mm) 24 hour time.	End time in the selected weekday(s)
Save	Button	Click **Save** to save the settings.
Undo	Button	Click **Undo** to cancel the settings.
Refresh	Button	Click the **Refresh** button to refresh the time schedule list.

Table 107 – Time Period Definition

4.1.1.2 Edit an existing Time Schedule

When the **Edit** button corresponding to an existing Time Schedule is clicked, the same **Time Schedule Configuration** and **Time Period Definition** sections as above opens and they are populated with that Time Schedule's details.

Make the required changes an click **Save.**

4.2 User

The needs of individual users as well as groups of users requiring the same access or restrictions can be managed with NTC-400 Series Router's User objects. The NTC400's user management tools include individual User Lists, User Profiles and User Groups.

The User List contains all user accounts, and User Profiles allow you add new accounts or edit existing ones. User Groups offer the convenience of segregating several similar user accounts in to one group sharing common properties and services. For example, one individual user account also can be a in unique group such as the "Administrator" group.

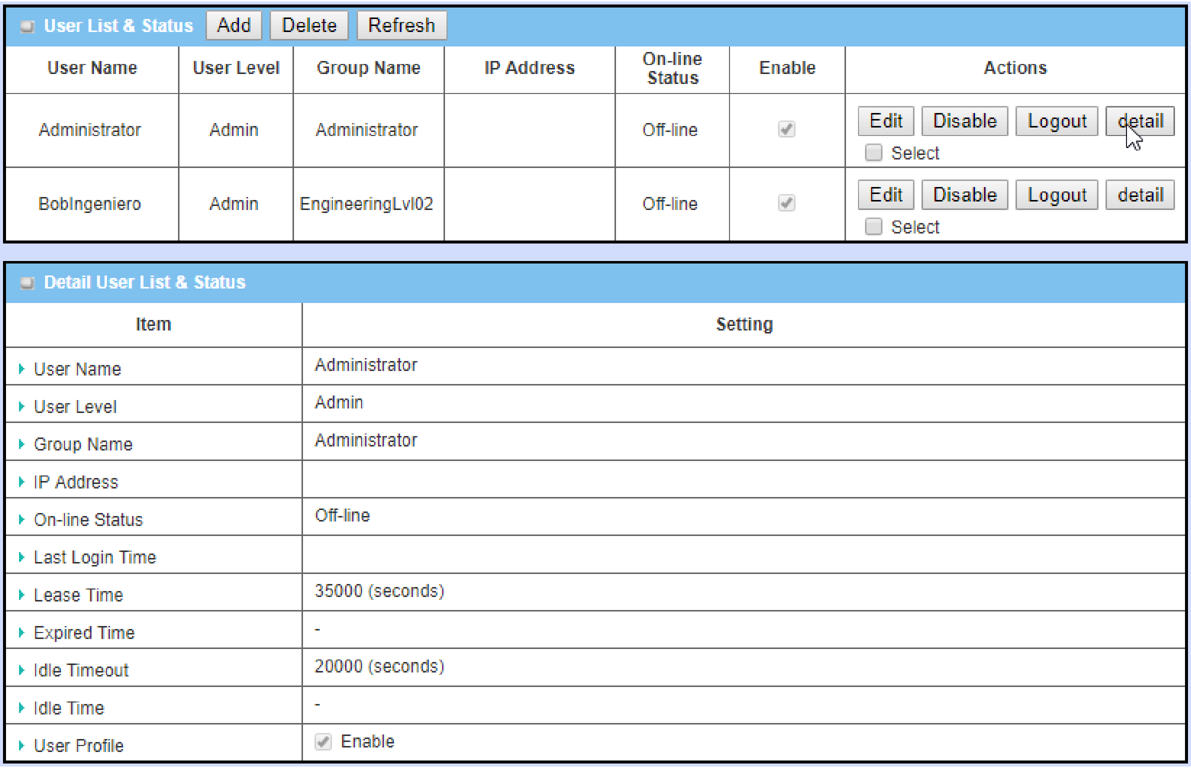
The User Account database is embedded in the device and is accessible by a AAA server, such as RADIUS server, for user authentication. It has the following feature set:

- Supports Multiple User Levels in User Management
  - One user account includes following information: name, password, user level, lease time, idle timeout and the group that it belongs to.
  - Four (4) different user levels are supported: Admin, Staff, Guest and Passenger
  - Remaining lease time and idle time for each user account are recorded and monitored each time they successfully log in to the router.
  - Each individual can be one group by itself or join other defined groups which share common properties.
  - The router can export and import user profiles.
  - User groups with their own name can be bound with multiple services, like X-Auth, NAS*, RADIUS, VPN, Accounting & Billing, SNMPv3 and CLI.
  - Administrators can define flexible access policies and bandwidth controls for user objects in a rule. The user object can be an individual user or a user group.

4.2.1 User List & Status

The User List & Status section shows all user accounts and their on-line or offline status.

To view the **User List & Status** page from the **Object Definition** submenu select **User** then click its **User List** tab:



User List & Status | Add | Delete | Refresh

User Name	User Level	Group Name	IP Address	On-line Status	Enable	Actions
Administrator	Admin	Administrator		Off-line	☑	Edit Disable Logout detail □ Select
BobIngeniero	Admin	EngineeringLvl02		Off-line	☑	Edit Disable Logout detail □ Select

Detail User List & Status

Item	Setting
User Name	Administrator
User Level	Admin
Group Name	Administrator
IP Address	
On-line Status	Off-line
Last Login Time	
Lease Time	35000 (seconds)
Expired Time	-
Idle Timeout	20000 (seconds)
Idle Time	-
User Profile	☑ Enable

Figure 187 – User List & Status and individual Detail User List & Status

To view the **Detail User List & Status** section for an individual user, click on the **detail** button in the **Actions** column corresponding to that user record.

Item	Notes	Description
User Name	Uneditable in the list or details section.	This User Name will be included in drop down lists throughout the NTC-400 Series Router that reference individual users. The User Name is entered in **User Profile Configuration** section, see next. Click this user’s **Edit** button in the **Actions** column to change this name.
User Level	Uneditable in the list or details section.	There are four user levels in the drop down list: **Admin**, **Staff**, **Guest** and **Passenger** **Admin** – Gives the user full control to configure the device. **Staff** – User can access both the Intranet resources and the Internet resources. **Guest** – Users have a specified bandwidth of Internet access, but cannot access the Intranet. **Passenger** – User account for mobile users to access the Internet via the device. Other users on this level share available bandwidth equally.
Group Name	Uneditable in the list or details section.	The Group Name is entered in **User Profile Configuration** section, see next. Click this user’s **Edit** button in the Action column to change this name.
IP Address	System generated.	If the User is logged in to the router, this is the IP address that the user logged in from.
On-line Status	System generated.	Indicates whether or not a user is logged in to the router.

Item	Notes	Description
		To confirm the current status, click the **Refresh** button in the User List & Status title bar to update the current user status.
Enable	Checkbox	When enabled, the user will be globally included in User Name drop down lists throughout NTC-400 Series Router functionality. If disabled it will not be available for selection, but its details will be retained in the system. Click the Disable button in a user's Action column to disable the user. To enable a disabled user, click the user's Edit button in the Action column to change this setting in the **User Profile Configuration** section, see next.
Actions	**Edit** button	Modify an existing user account by clicking its corresponding Edit button in the Actions section at the end of each account record.
	Disable Button	If a user is enabled, click the **Disable** button in the user's **Actions** column to disable the user.
	Logout Button	Click to log the user account out of its current session.
	Details Button	Click the **Details** button to show additional detail information except the ones in User List about the user account, including Last Login Time, Lease Time, Expired Time, Idle Timeout and current Idle Time.
	Select checkbox	Redundant or obsolete accounts can be permanently removed by checking ☑ **Select** for those accounts and then clicking the **Delete** button at the User List & Status section's title bar.
Add	Button	Click the **Add** button to create a new user account.
Delete	Button	Use the **Delete** button in conjunction with the ☑ **Select** checkbox in the **Actions** section to permanently delete accounts that are no longer required. **Note** – If you want to keep details of the user account record you can also deselect the ☐ **Enable** button.
Refresh	Button	Click **Refresh** in the User List & Status title bar to update the current user status.

Table 108 – User Details

When the **Add** button is clicked the **User Profile Configuration** section will appear. For the detail about the configuration, please refer to the next section.

4.2.2 Create/Edit User Profile

To create a new User Profile:

1 From the **Object Definition** submenu select **User** then click its **User Profile** tab, or click **Add** from the title bar of the **User List & Status** section.

2 The **User Profile Configuration** page will open.

3 Enter the new user's details here and click **Save**.

To edit an existing User Profile :

1 Select **User** from the **Object Definition** submenu and click the **User List** tab.

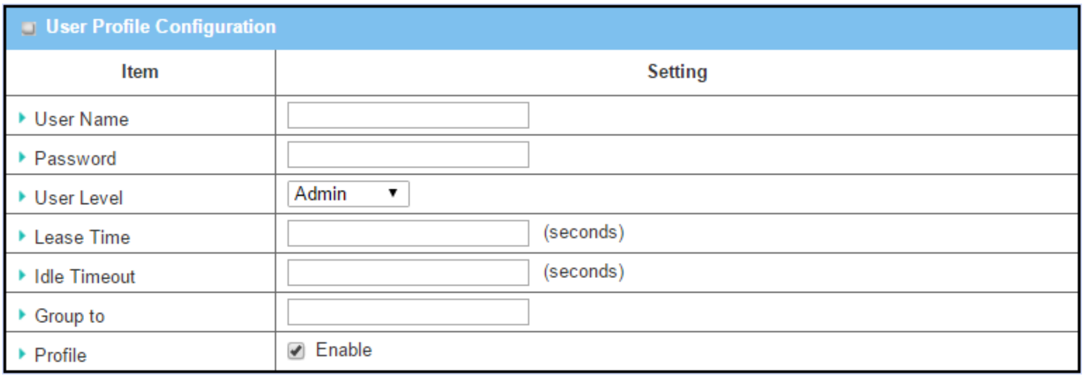
2 In the **User List & Status** section find the User Name record in the list and click the **Edit** button in the **Actions** column of the list

3 The User Profile Configuration section will open.

4 Make the necessary corrections or changes to the existing user's details and click **Save**.

4.2.2.1 User Profile Configuration

The **User Profile Configuration** section is used to create new, or edit existing, User Profiles:



User Profile Configuration

Item	Setting
User Name	
Password	
User Level	Admin ▼
Lease Time	(seconds)
Idle Timeout	(seconds)
Group to	
Profile	☑ Enable

Figure 188 – User Profile Configuration

Item	Notes	Description
User Name	Mandatory field. Enter text string, no spaces allowed.	Enter the name of user account.
Password	Mandatory field. Enter text string.	Enter a strong password for the user account.
User Level	Mandatory field. Default selection: **Admin**	There are four user levels in the drop down list: **Admin**, **Staff**, **Guest** and **Passenger** **Admin** – Gives the user full control to configure the device. **Staff** – User can access both the Intranet resources and the Internet resources. **Guest** – Users have a specified bandwidth of Internet access, but cannot access the Intranet. **Passenger** – User account for mobile users to access the Internet via the device. Other users on this level share available bandwidth equally.
Lease Time	Any integer. Optional field.	Specify the lease time (in seconds) for the user account to login the device. The device will log the user out of the account if he has logged in for the time longer than the **Lease Timeout**.
Idle Time	Any integer. Optional field.	Specify the idle time (in seconds) for the user account. The device will log the user out of the account if it is idle for the time longer than the **Idle Timeout**.

Item	Notes	Description
Group to	Enter text string. Optional field.	Enter a group name if you would like to assign the user to a particular user group.
Profile	Mandatory field. Enabled by default.	Check ☑ **Enable** to activate the user profile.
Save	Button	Click the **Save** button to save the settings
Undo	Button	Click the **Undo** button to cancel the settings

Table 109 – User Profile Configuration

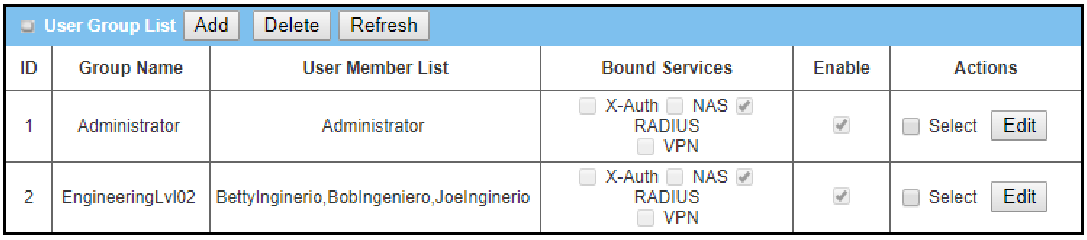
4.2.3 User Group

User Groups are composed of several user accounts which share common properties.

The User Group List section shows all user groups and some of their settings.

To view the User Group List section open the **Object Definition** submenu, select **User** and then click its **User Group** tab.

The **User Group List** contains basic details of all currently defined User Groups:



User Group List Add Delete Refresh

ID	Group Name	User Member List	Bound Services	Enable	Actions
1	Administrator	Administrator	□ X-Auth □ NAS ☑ RADIUS □ VPN	☑	□ Select Edit
2	EngineeringLvl02	BettyInginerio,BobIngeniero,JoeInginerio	□ X-Auth □ NAS ☑ RADIUS □ VPN	☑	□ Select Edit

Figure 189 – User Group List

Item	Notes	Description
ID	Auto-filled with an integer.	The user group's system generated reference number.
Group Name	System generated.	Name entered in **User Group Configuration** section, see next. Click this group's **Edit** button in the **Actions** column to change this name.
User Member List	System generated.	Multiple users are selected using the **Choice** button in the **User Group Configuration** section, see next. Click this group's **Edit** button in the **Actions** column to add or remove user members.
Bound Services	System generated.	To change these settings, click this group's **Edit** button in the **Actions** column and make the required changes in the **User Group Configuration** section, see next.
Enable	Checkbox. Cannot be changed from this list.	Check ☑ **Enable** to activate the user group for use in other applications throughout the NTC-400 Series Router interface. When ☐ **Enable** is unchecked, it is not available for use in other NTC-400 Series Routersettings.

Item	Notes	Description
		To change this setting, click this group's **Edit** button in the **Actions** column and make the changes in the **User Group Configuration** section, see next.
Actions	**Select** checkbox	Redundant or obsolete groups can be permanently removed by checking ☑ **Select** for those groups and then clicking the **Delete** button at the User Group List caption bar.
	Edit button	Modify an existing user group by clicking its corresponding Edit button in the Actions section at the end of each user group record.
Add	Button	Click the **Add** button to create a new user group.
Delete	Button	Use the **Delete** button in conjunction with the ☑ **Select** checkbox in the **Actions** section to permanently delete groups that are no longer required. **Note** – If you want to keep details of the user group record (but do not want to permanently delete it) you can deselect the ☐ **Enable** button.
Refresh	Button	Click **Refresh** in the **User List & Status** caption bar to update the current user status.

Table 110 – User Group List

4.2.3.1 Create/Edit User Group

To create a new User Group:

1 From the **Object Definition** submenu select **User** then click its click the **User Group** tab.

2 In the **User Group List** section click the **Add** button in the caption bar.

3 The **User Group Configuration** section will open.

4 Enter the new user group's details here and click **Save**.

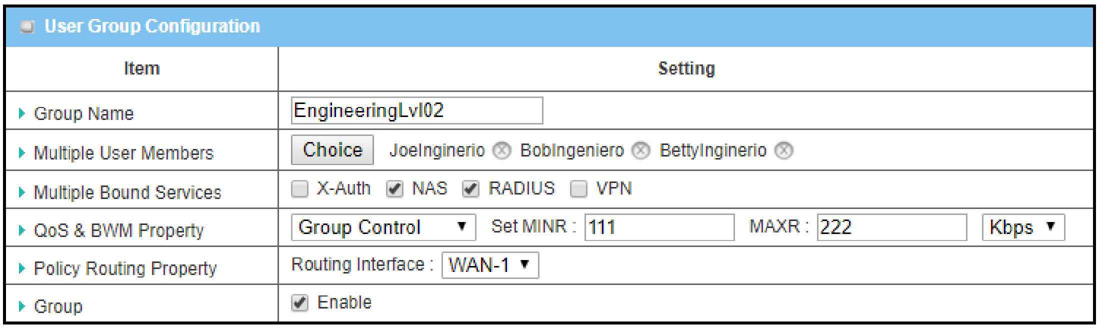
To edit an existing User Group:

1 From the **Object Definition** submenu select **User** then click its **User Group** tab.

2 In the **User Group List** section find the user group record in the list and click the **Edit** button in the **Actions** column of the list.

3 The **User Group Configuration** section will open.

4 Make the necessary corrections or changes to the existing user group's details and click **Save**.



User Group Configuration

Item	Setting
Group Name	EngineeringLvl02
Multiple User Members	Choice JoeInginerio ⊗ BobIngeniero ⊗ BettyInginerio ⊗
Multiple Bound Services	□ X-Auth ☑ NAS ☑ RADIUS □ VPN
QoS & BWM Property	Group Control ▼ Set MINR : 111 MAXR : 222 Kbps ▼
Policy Routing Property	Routing Interface : WAN-1 ▼
Group	☑ Enable

Figure 190 – User Group Configuration section

Item	Notes	Description
Group Name	Mandatory field. Enter an alpha-numeric string.	Enter the name of user group. Value Range: at least 1 character, can be A - Z, a - z, or 0 - 9
Multiple User Members	Button	Click the Choice button to select multiple user accounts to join the group. The names of users selected will appear after the Choice button. Click the circled x ⊗ to remove members.
Multiple Bound Services	Button	Check the available service box(es) to apply one or more to the user group.
QoS & BWM Property	Mandatory field. Default selection: Individual Control	Specify the preferred sharing method for how to apply a QoS rule on the selected group (**Individual** or **Group**), and define the guaranteed and limited bandwidth usage for the group **Individual Control** – Each user in the group will have his own QoS service resource as specified in the rule. **Group Control** – The entire user group shares the same QoS service resource. Other settings: **MINR** – Guaranteed minimum bandwidth usage. **MAXR** – Maximum bandwidth usage. Select **Kbps** or **Mbps** for the download speed.
Policy Routing Property	Mandatory field. Default setting: **WAN-1**	Specify the routing interface. All packets from the group members will be routed via the specified interface.
Group	Mandatory field. Enabled by default.	Check ☑ **Enable** to activate the user group.
Save	Button	Click the **Save** button to save the settings
Undo	Button	Click the **Undo** button to cancel the settings

Table 111 – User Group Configuration

4.3 Grouping

The Grouping function allows users to make groups for some services.

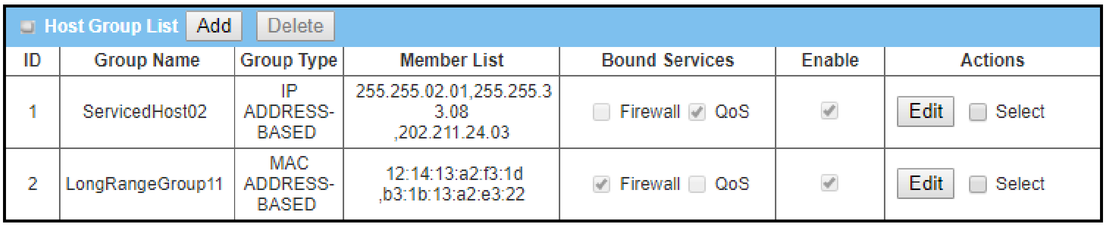
4.3.1 Host Grouping

Host Groups are groupings of several user accounts which share a common IP address or groups of IP addresses.

Users can make host groups for some services, such as QoS, Firewall, and Communication Bus. The service types available may vary depending on the model purchased.

The **Host Group List** section shows all currently defined host groups and some of their settings.

To view the Host Group List open the **Object Definition** submenu, select **Grouping** and then click its **Host Grouping** tab:



Host Group List Add Delete

ID	Group Name	Group Type	Member List	Bound Services	Enable	Actions
1	ServicedHost02	IP ADDRESS-BASED	255.255.02.01,255.255.33.08 ,202.211.24.03	□ Firewall ☑ QoS	☑	Edit □ Select
2	LongRangeGroup11	MAC ADDRESS-BASED	12:14:13:a2:f3:1d ,b3:1b:13:a2:e3:22	☑ Firewall □ QoS	☑	Edit □ Select

Figure 191 – Host Group list

Item	Notes	Description
ID	Integer. Auto-fill.	The host group's system generated reference number.
Group Name	System generated.	Name entered in **Host Group Configuration** section, see next. Click this group's **Edit** button in the **Actions** column to change this name.
Group Type	System generated.	The type is selected from a drop down list in the **Host Group Configuration** section, see next. Click this group's **Edit** button in the **Actions** column to change this setting.
Member List	System generated.	Multiple users are selected using the **Choice** button in the **Host Group Configuration** section, see next. Click this group's **Edit** button in the **Actions** column to add or remove user members.
Bound Services	System generated.	To change these settings, click this group's **Edit** button in the **Actions** column and make the required changes in the **Host Group Configuration** section, see next.
Enable	Checkbox. Cannot be changed from this list.	Check ☑ **Enable** to activate the **Host Group** for use in other applications throughout the NTC-400 Series Router interface. When ☐ **Enable** is unchecked, it is not available for use in other NTC-400 Series Router settings. To change this setting, click this group's **Edit** button in the **Actions** column and make the changes in the **Host Group Configuration** section, see next.
Actions	**Select** Checkbox	Redundant or obsolete groups can be permanently removed by checking ☑ Select for those groups and then clicking the Delete button at the Host Group List caption bar.

Item	Notes	Description
	Edit button	Modify an existing **Host Group** by clicking its corresponding **Edit** button in the **Actions** section at the end of each Host Group record.
Add	Button	Click the **Add** button to create a new Host Group.
Delete	Button	Use the **Delete** button in conjunction with the ☑ Select checkbox in the Actions section to permanently delete groups that are no longer required. **Note** – If you want to keep details of the Host Group record (but do not want to permanently delete it) you can deselect the ☐ **Enable** button.

Table 112 – Host Group List

4.3.2 Create/Edit Host Group

To create a new Host Group:

1 Select **Grouping** from the **Object Definition** submenu and click the **Host Grouping** tab.

2 In the **Host Group List** section click the **Add** button in the caption bar.

3 The **Host Group Configuration** section will open.

4 Enter the new Host Group's details here and click **Save**.

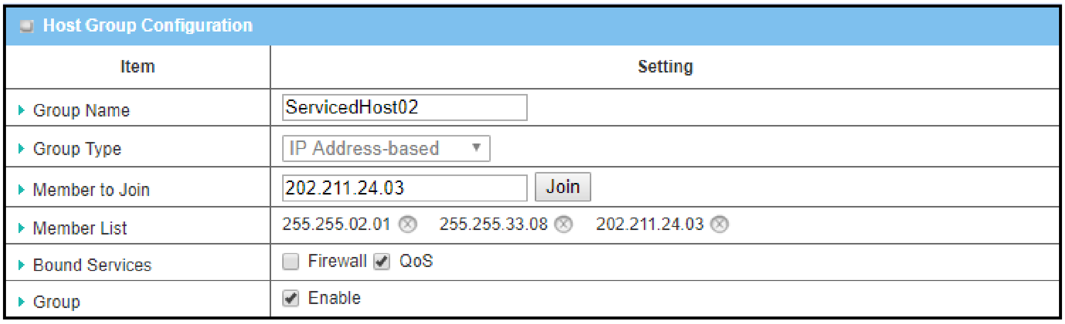
To edit an existing Host Group:

1 From the **Object Definition** submenu select **Grouping** and click its **Host Grouping** tab.

2 In the **Host Group List** section find the Host Group's record in the list and click the **Edit** button in the **Actions** column of the list

3 The **Host Group Configuration** section will open.

4 Make the necessary corrections or changes to the existing Host Group's details and click **Save**.



Host Group Configuration

Item	Setting
Group Name	ServicedHost02
Group Type	IP Address-based
Member to Join	202.211.24.03 Join
Member List	255.255.02.01 ⊗ 255.255.33.08 ⊗ 202.211.24.03 ⊗
Bound Services	☐ Firewall ☑ QoS
Group	☑ Enable

Figure 192 – Host Group Configuration section

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

Item	Notes	Description
Group Name	Enter text string. Mandatory field.	Enter a meaningful group name for the rule.

Item	Notes	Description
Group Type	Mandatory field. Default selection: **IP Address-based**	Select the member type for the host group from the drop down list: **IP Address-based**, **MAC Address-based**, or **Host Name-based** **IP Address-based** – Only IP address can be added in Member to Join. **MAC Address** – Only MAC address can be added in Member to Join. **Host Name-based** – Only host name can be added in Member to Join.
Member to Join	Button	Add the members to the group in this field. You can enter the member information that corresponds with the **Member Type** above, and press the **Join** button to add to the **Member List**, see next.
Member List	List	The names of users selected will appear in the row after they are added using the **Join** button, see previous. Click the circled x ⊗ to remove members.
Group	Disabled by default	Check ☑ **Enable** to activate this host group rule. Enabled **Host Groups** can be bound to selected service(s) for further configuration.
Save	Button	Click **Save** to save the settings
Undo	Button	Click **Undo** to cancel the settings

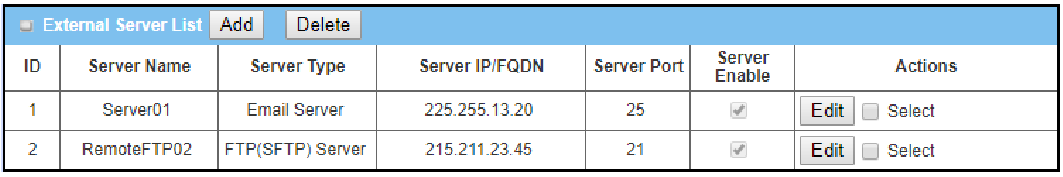
Table 113 – Host Group Configuration

4.4 External Server

External Servers allow you to define a range of different types of servers that are external to the NTC-400 Series Router and which then may be referenced by the NTC-400 Series Router during its operations.

The **External Server List** section shows all currently defined external servers and some of their settings.

To view the External Server List open the **Object Definition** submenu, select **External Server** and then click its **External Server** tab:



External Server List Add Delete

ID	Server Name	Server Type	Server IP/FQDN	Server Port	Server Enable	Actions
1	Server01	Email Server	225.255.13.20	25	☑	Edit □ Select
2	RemoteFTP02	FTP(SFTP) Server	215.211.23.45	21	☑	Edit □ Select

Figure 193 – External Server list

Item	Notes	Description
ID	Integer. Auto-fill.	The External Server's system generated reference number.
Server Name	System generated.	Name entered in External Server Configuration section, see next.

Item	Notes	Description
		Click this group’s **Edit** button in the **Actions** column to change this name.
Server Type	System generated.	The **Server Type** selected from the drop down list in the **External Server Configuration** section, see next. Click this group’s **Edit** button in the **Actions** column to change this name.
Server IP/FQDN	System generated.	Enter these details in the **External Server Configuration** section, see next. Click this group’s **Edit** button in the **Actions** column to add or edit these details.
Server Port	System generated.	To change these settings, click this group’s **Edit** button in the **Actions** column and make the required changes in the **External Server Configuration** section, see next.
Server Enable	Checkbox. Cannot be changed from this list.	Check ☑ **Enable** to activate the **External Server** for use in other applications throughout the NTC-400 Series Router interface. When ☐ **Enable** is unchecked, it is not available for use in other NTC-400 Series Router settings. To change this setting, click this group’s **Edit** button in the Actions **column** and make the changes in the **External Server Configuration** section, see next.
Actions	**Select** checkbox	Redundant or obsolete groups can be permanently removed by checking ☑ **Select** for those groups and then clicking the **Delete** button at the External Server List caption bar.
	Edit button	Modify an existing External Server by clicking its corresponding **Edit** button in the **Actions** section at the end of each External Server record.
Add	Button	Click the **Add** button to create a new External Server.
Delete	Button	Use the **Delete** button in conjunction with the ☑ **Select** checkbox in the **Actions** section to permanently delete groups that are no longer required. **Note** – If you want to keep details of the External Server record (but do not want to permanently delete it) you can deselect the ☐ **Enable** button.

Table 114 – External Server List

4.4.1 Create/Edit External Server

To create a new External Server:

1 From the Object Definition submenu select External Server and click its External Server tab.

2 In the External **Server List** section click the **Add** button in the caption bar.

3 The **External Server Configuration** section will open, see below.

4 Enter the new External Server’s details here and click **Save**.

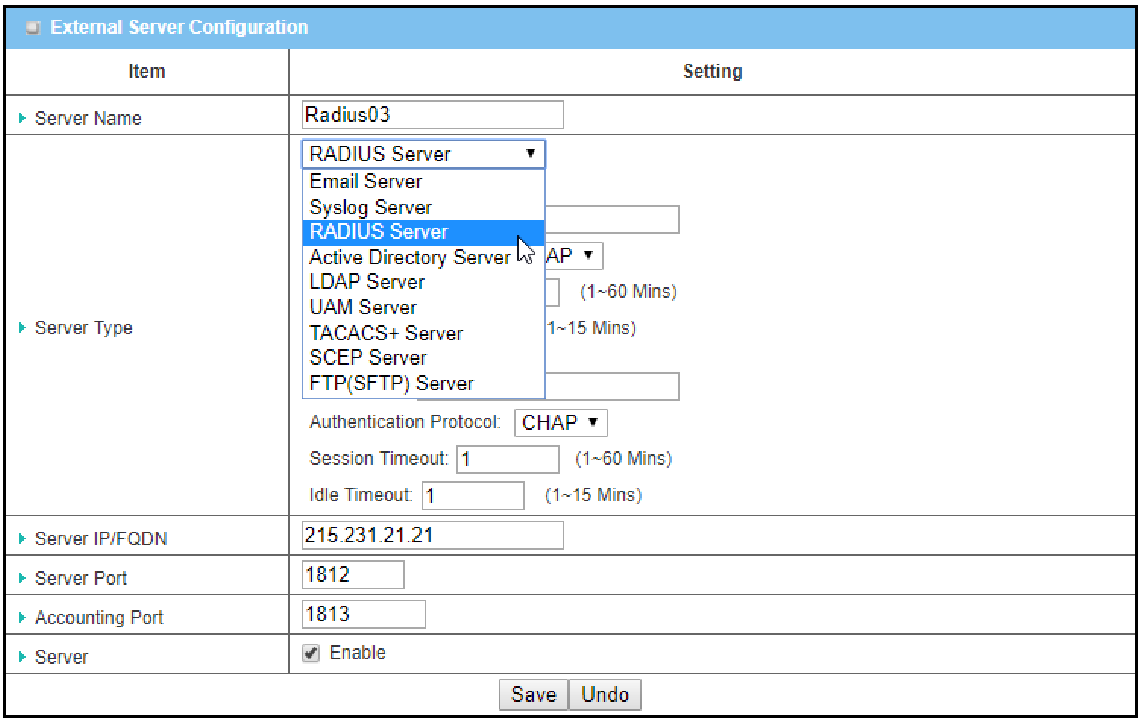
To edit an existing External Server:

1 From the **Object Definition** submenu select **External Server** and then click its **External Server** tab.

2 In the **External Server List** section find the User Profile record in the list and click its corresponding **Edit** button in the **Actions** column of the list.

3 The **External Server Configuration** section will open, see below.

4 Make the necessary corrections or changes to the existing External Server's details and click **Save**.



External Server Configuration

Item	Setting
Server Name	Radius03
Server Type	RADIUS Server ▼ Authentication Protocol: CHAP ▼ Session Timeout: 1 (1~60 Mins) Idle Timeout: 1 (1~15 Mins)
Server IP/FQDN	215.231.21.21
Server Port	1812
Accounting Port	1813
Server	☑ Enable

Figure 194 – External Server Configuration

Item	Notes	Description
Server Name	Enter text string. Mandatory field.	Enter a meaningful name for the external server.
Server Type	Mandatory field. Select from drop down list. Default selection: **Email Server**	**Email Server** When Email Server is selected, User Name, and Password are also required. **User Name** (String format: any text) **Password** (String format: any text)
		Syslog Server – No further settings required
		RADIUS Server When RADIUS Server is selected, the following settings are also required: *Primary*: **Shared Key** (String format: any text) **Authentication Protocol** (Default: **CHAP**) **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.

Item	Notes	Description
		Secondary: **Shared Key** (String format: any text) **Authentication Protocol** (Default: **CHAP**) **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 When Active Directory Server is selected, Domain setting is also required. **Domain** (String format: any text)
		LDAP Server 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 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 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 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)
		FTP(SFTP) Server When FTP(SFTP) Server is selected, the following settings are also required: **User Name** (String format: any text) **Password** (String format: any text) **Protocol** (Select FTP or SFTP) **Encryption** (Select Plain, Explicit FTPS or Implicit FTPS) **Transfer mode** (Select Passive or Active)

Item	Notes	Description
Server IP/FQDN	Mandatory field.	Specify the **IP address** or **FQDN** used for the external server.
Server Port	Mandatory field.	Specify the **Port** used for the external server. The default server port number will be differ depending on which server type you select: **Email Server**: port **25** by default **Syslog Server**: port **514** by default **RADIUS Server**: port **1812** by default **Active Directory Server**: port **389** by default **LDAP Server**: port **389** by default **UAM Server**: port **80** by default **TACACS+ Server**: port **49** by default **SCEP Server**: port **80** by default **FTP**(**SFTP**) **Server**: port **21** by default
Server	Enabled by default	Click ☑ **Enable** to activate this External Server.
Save	Button	Click **Save** to save the settings
Undo	Button	Click **Undo** to cancel the settings
Refresh	Button	Click the **Refresh** button to refresh the external server list.

Table 115 – External Server Configuration

4.5 Certificate

In cryptography, a public key certificate (also known as a digital certificate or identity certificate) is an electronic document used to prove ownership of a public key. The certificate includes information about the key, information about its owner's identity, and the digital signature of an entity that has verified the certificate's contents as genuine. If the signature is valid, and the person examining the certificate trusts the signer, then they know they can use that key to communicate with its owner.

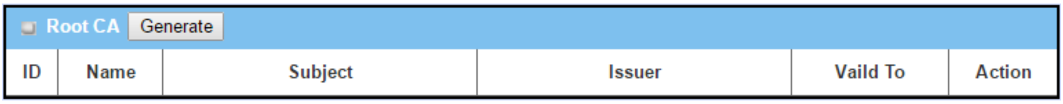
In a typical public-key infrastructure (PKI) scheme, the signer is a certificate authority (CA), usually a company such as VeriSign™ which charges customers to issue certificates for them. In a web of trust scheme, the signer is either the key's owner (a self-signed certificate) or other users ("endorsements") whom the person examining the certificate might know and trust.

Certificates are an important component of Transport Layer Security (TLS, also known by its older name SSL), where they prevent an attacker from impersonating a secure website or other server. They are also used in other important applications, such as email encryption and code signing or in IPSec tunnelling for user authentication.

4.5.1 Configuration

NTC-400 Series Router allows users to create a Root Certificate Authority (CA) certificate and enable the use of SCEP. A Root CA is the primary certificate of the tree, the private key of which is used to "sign" other certificates. Only one Root CA can be set for the router at a time.

To view the current **Root CA** details, from the **Object Definition** submenu select **Certificate** then click its **Configuration** tab:



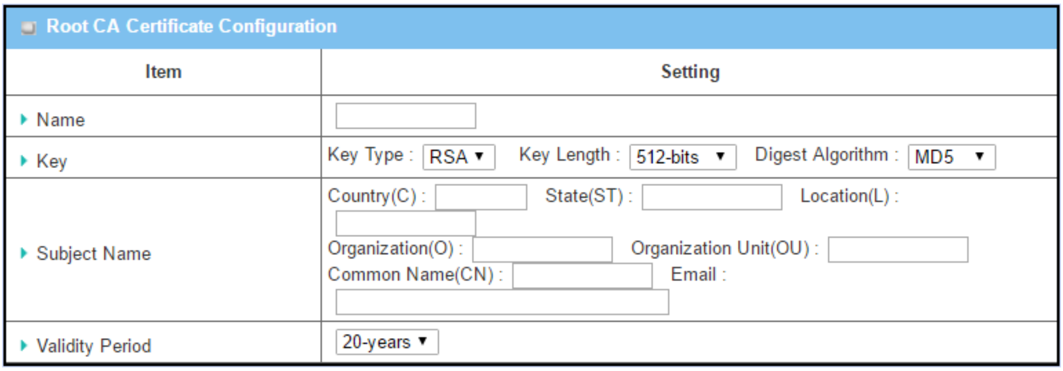
Root CA Generate

ID	Name	Subject	Issuer	Vaild To	Action

Figure 195 – Root CA

4.5.1.1 Create Root CA

Click the **Generate** button to open the **Root CA Certificate Configuration** section. Enter the required details to create a CA Certificate.



Root CA Certificate Configuration

Item	Setting
Name	
Key	Key Type : RSA ▾ Key Length : 512-bits ▾ Digest Algorithm : MD5 ▾

Subject Name	Country(C) : State(ST) : Location(L) :
	Organization(O) : Organization Unit(OU) :
	Common Name(CN) : Email :

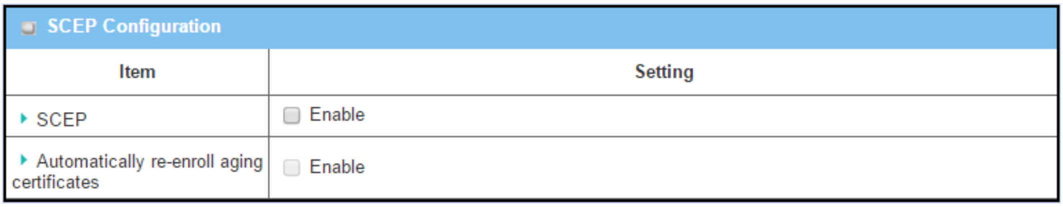
Validity Period	20-years ▾

Item	Notes	Description
Name	Enter text string. Mandatory field.	Enter a Root CA Certificate name. It will be a certificate file name. Maximum length: 8 letters (no numbers or special characters)
Key	Mandatory field.	This field is to specify the key attributes of the certificate. **Key Type** to set public-key cryptosystems. It only supports RSA now. **Key Length** to sets 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	Mandatory fields.	Specify the following details for the certificate. **Country (C)** – The two-letter ISO code for the country where your organisation is located. **State (ST)** – The state where your organisation is located. **Location (L)** – The location where your organisation is located. **Organization (O)** –The name of your organisation. **Organization Unit (OU)** – The name of your organisation unit. **Common Name (CN)** – The name of your organization. **Email** - The email of your organisation. Must be in the email address style, e.g. john.doe@gmail.com
Validity Period	Mandatory field.	Select the validity period of certificate from the drop down list.

Table 116 – Root CA Certificate Configuration

4.5.1.2 Setup SCEP

If you want to use a SCEP server to obtain a copy of a Certificate Authority (CA) certificate and validate it, you must first enable the SCEP functionality here.



SCEP Configuration

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

Figure 196 – SCEP Configuration

Item	Notes	Description
SCEP	Disabled by default.	Check ☑ **Enable** to activate SCEP function.
Automatically re-enroll aging certificates	Disabled by default.	When SCEP is activated, check ☑ **Enable** to activate this function. It will be automatically check which certificate is aging. If certificate is aging, it will activate SCEP's function to re-enroll it automatically.
Save	Button	Click **Save** to save the settings
Undo	Button	Click **Undo** to cancel the settings

Table 117 – SCEP Configuration details

4.5.2 My Certificate

My Certificate includes a Local Certificate List. The Local Certificate List shows all generated certificates by the root CA for the router and it stores the generated Certificate Signing Requests (CSR) which will be signed by other external CAs. The signed certificates can be imported as the local ones of the gateway.

4.5.2.1 Self-signed Certificate Usage Scenario

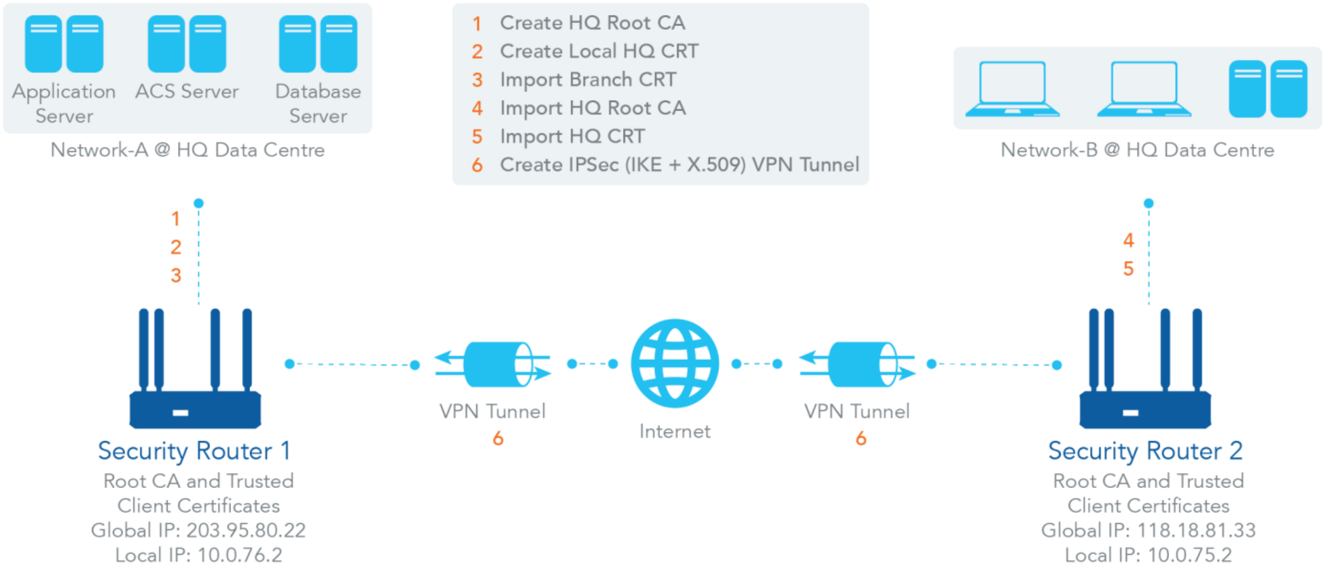


Figure 197 – Self-signed Certificate Usage Scenario

Scenario Application Timing

When the enterprise gateway owns the root CA and VPN tunnelling function, it can generate its own local certificates by being signed by itself or import any local certificates that are signed by other external CAs. It can also import the trusted certificates for other CAs and Clients. In addition, since it has the root CA, it also can sign Certificate Signing Requests (CSR) to form corresponding certificates for others. These certificates can be used for two remote peers to verify their identity during establishment of a VPN tunnel.

Scenario Description

Router 1 generates the root CA and a local certificate (HQCRT) signed by itself. Import a trusted certificate (BranchCRT) –a BranchCSR certificate of Gateway 2 signed by root CA of Router 1.

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 Router 2 as a local certificate. Import the certificates of the root CA of the Router 1 onto Router 2 as the trusted ones.

Establish an IPSec VPN tunnel with IKE and X.509 protocols by starting from either peer so that all client hosts in both of these subnets can communicate with each other.

Parameter Setup Example

For Network-A at HQ

The following tables list the parameter configuration as an example for the "My Certificate" function used in the user authentication of the IPSec VPN tunnel establishing, as shown in the diagram above. The configuration example must be combined with the ones in the following two sections to complete the whole user scenario.

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

Configuration Path	[My Certificate]-[Root CA Certificate Configuration]
Name	*NTCRootCA*
Key	Key Type: *RSA* Key Length: *1024-bits*
Subject Name	Country(C): AU State(ST): *NSW* Location(L): *Sydney* Organization(O): *NetCommWireless* Organization Unit(OU): *NTC* Common Name(CN): *NTCRootCA* E-mail: *ntcrootca@netcommwireless.com*

Configuration Path	[My Certificate]-[Local Certificate Configuration]
Name	*NTCCRT* Self-signed: ■
Key	Key Type: *RSA* Key Length: *1024-bits*
Subject Name	Country(C): *AU* State(ST): *NSW* Location(L): *Sydney* Organization(O): *NetCommWireless* Organization Unit(OU): *NTC* Common Name(CN): *NTCCRT* E-mail: *ntccrt@netcommwireless.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*

For Network-B at Branch Office

Following tables list the parameter configuration as an example for the "My Certificate" function used in the user authentication of IPSec VPN tunnel establishing, as shown in above diagram. The configuration example must be combined with the ones in following two sections to complete the whole user scenario.

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): *AU* State(ST): *NSW* Location(L): *Sydney* Organization(O): *NetCommWireless* Organization Unit(OU): *NTC* Common Name(CN): *NTCCRT* E-mail: *ntccrt@netcommwireless.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: *NTCCRT*
Local ID	*User Name* *Network-B*
Remote ID	*User Name* *Network-A*

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

Scenario Operation Procedure

In the diagram above, "Router 1" is the gateway of Network-A at headquarters and the subnet of its Intranet 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 WAN-1 interface. "Router 2" is the gateway of Network-B in the branch office and the subnet of its Intranet 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 WAN-1 interface. They both serve as the NAT security gateways.

Router 1 generates the root CA and a local certificate (NTCCRT) that is signed by itself. Import the certificates of the root CA and NTCCRT into the "Trusted CA Certificate List" and "Trusted Client Certificate List" of Router 2.

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

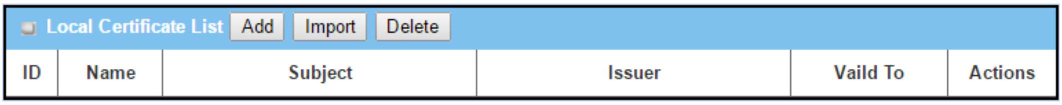
Router 2 can establish an IPSec VPN tunnel with "Site to Site" scenario and IKE and X.509 protocols to Router 1.

The client hosts in two subnets of 10.0.75.0/24 and 10.0.76.0/24 can communicate with each other.

4.5.3 Local Certificate

Navigate to the **Object Definition > Certificate > My Certificate** tab.

The My Certificate setting allows you to create local certificates. On the "My Certificate" page, there are two configuration windows for the "My Certificate" function. The "Local Certificate List" window shows the stored certificates or CSRs for representing the gateway. The "Local Certificate Configuration" window allows you to enter the required information necessary for the corresponding certificate to be self-generated, or the corresponding CSR to be signed by other CAs.



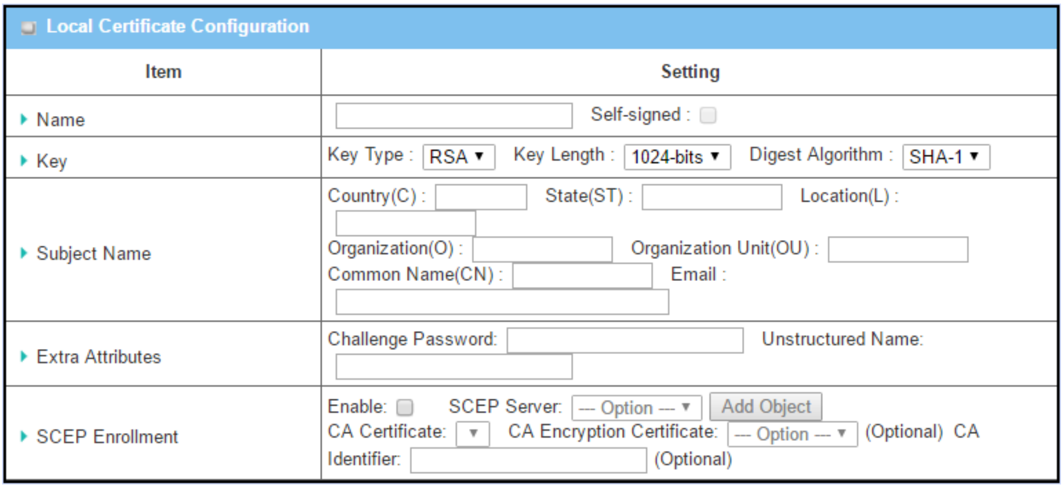
Local Certificate List Add Import Delete

ID	Name	Subject	Issuer	Vaild To	Actions

Figure 198 – Local Certificate List

4.5.3.1 Create Local Certificate

Click the **Add** button in the **Local Certificate List's** title bar to open the **Local Certificate Configuration** section. Here you enter information necessary for a certificate to be generated by itself, or for a CSR to be signed by other CAs.



Local Certificate Configuration

Item	Setting
Name	Self-signed : □
Key	Key Type : RSA ▾ Key Length : 1024-bits ▾ Digest Algorithm : SHA-1 ▾

Subject Name	Country(C) : State(ST) : Location(L) :
	Organization(O) : Organization Unit(OU) :
	Common Name(CN) : Email :

Extra Attributes	Challenge Password: Unstructured Name:
SCEP Enrollment	Enable: □ SCEP Server: --- Option --- ▾ Add Object CA Certificate: ▾ CA Encryption Certificate: --- Option --- ▾ (Optional) CA Identifier: (Optional)

Figure 199 – Local Certificate Configuration

Item	Notes	Description
Name	Enter text string. Mandatory field.	Enter a certificate name. It will be used as the certificate file name Check ☑ **Self-signed** for a certificate signed by the root CA . If **Self-signed** is □ not checked, a certificate signing request (CSR) will be generated.
Key	Mandatory field.	This field is to specify the key attributes of the certificate. **Key Type** to set public-key cryptosystems. It only supports RSA now. **Key Length** to sets the size measured 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	Mandatory field.	Specify the following details for the certificate. **Country (C)** – The two-letter ISO code for the country where your organisation is located. **State (ST)** – The state where your organisation is located. **Location (L)** – The location where your organisation is located. **Organization (O)** –The name of your organisation. **Organization Unit (OU)** – The name of your organisation unit. **Common Name (CN)** – The name of your organization. **Email** - The email of your organisation. Must be in the email address style, e.g. john.doe@gmail.com
Extra Attributes	Mandatory field.	In this field specify extra information for generating a certificate, for example: **Challenge Password** – The password used to request certificate revocation in the future. **Unstructured Name** – Additional information.
SCEP Enrollment	Mandatory field.	This field is to specify the information of SCEP.

Item	Notes	Description
		Check the ☑ **Enable** box to generate an online certificate signing request (CSR) for signature by a SCEP server. Select a SCEP Server from the drop down list to send the CSR to. The SCEP server is defined in Object Definition > External Server > External Server. 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.
Save	Button	Click the **Save** button to save the configuration.
Back	Button	Click the **Back** button to return to previous page.

Table 118 – Local Certificate Configuration

4.5.3.2 Import Existing Certificates

When **Import** button in the **Local Certificate List's** title bar is applied, the Import section appears. You can import a certificate from an external certificate file, or directly paste a PEM code string in to the **PEM Encoded** field to define the certificate.

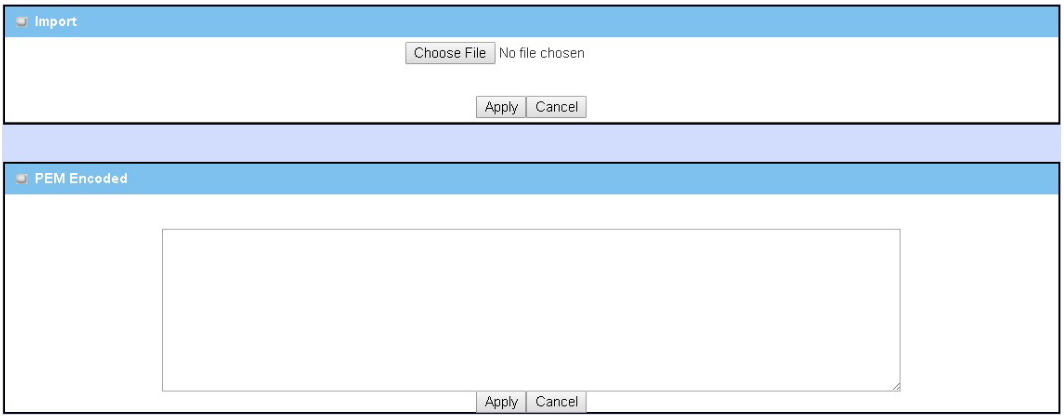


Figure 200 – Import and PEM Encoded

Item	Notes	Description
Import	Mandatory field.	Select a certificate file from user's computer, and click the **Apply** button to import the specified certificate file to the router.
PEM Encoded	Enter text string. Mandatory field.	This is an alternative approach to importing a certificate file. Directly copy (**Ctrl+C**) and paste (**Ctrl+V**) the PEM encoded certificate string into the text box in the **PEM Encoded** section, and click the **Apply** button to import the certificate code in to the router.
Apply	Button	Click the **Apply** button to import the certificate.
Cancel	Button	Click the **Cancel** button to discard the import operation and return to the My Certificates page.

Table 119 – Import and PEM Encoded

4.5.4 Trusted Certificate

Trusted Certificate includes the Trusted CA Certificate List, Trusted Client Certificate List, and Trusted Client Key List. The Trusted CA Certificate List displays details of external CA certificates that you can readily use.

The Trusted Client Certificate List third party certificates that you trust and the Trusted Client Key List details the third party keys that you trust.

4.5.4.1 Self-signed Certificate Usage Scenario

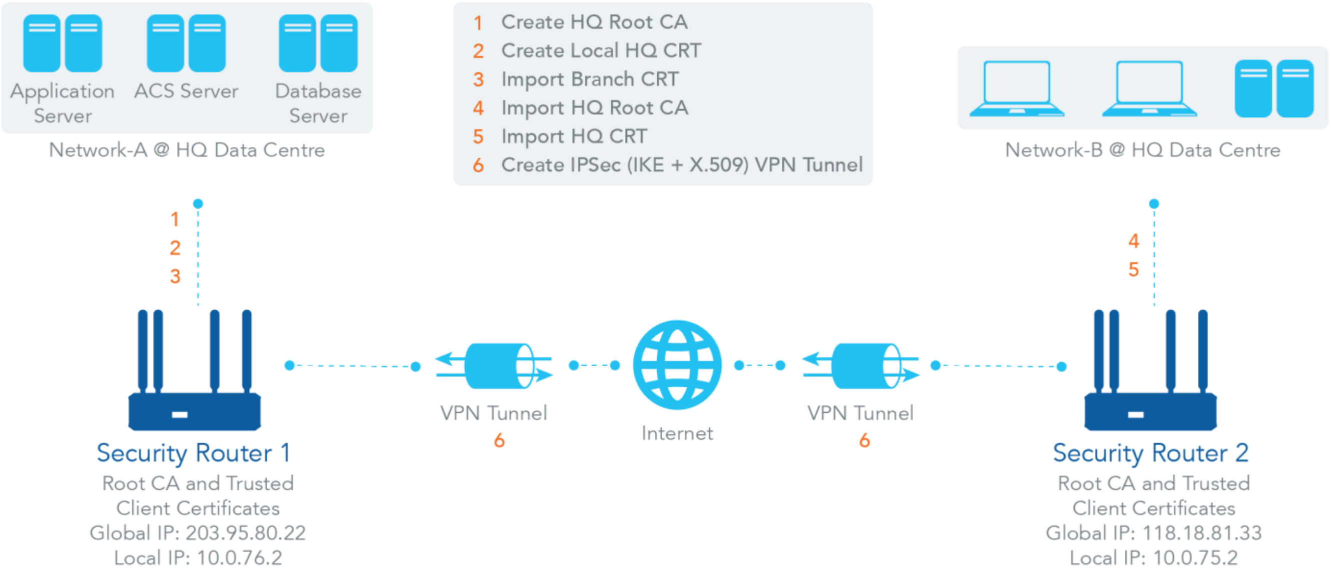


Figure 201 – Self-signed Certificate Usage Scenario

Scenario Application Timing

(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 by self-signing it. It also imports the trusted certificates for other CAs and Clients. These certificates can be used for two remote peers to verify their identity during establishment of a VPN tunnel.

Scenario Description

(same as the one described in "My Certificate" section)

Router 1 generates the root CA and a local certificate (NTCCRT) self-signed. Import a trusted certificate (BranchCRT) –a BranchCSR certificate of Router 2 signed by root CA of Router 1.

Router 2 creates a CSR (BranchCSR) to let the root CA of the Router 1 sign it to be the BranchCRT certificate. Import the certificate into Router 2 as a local certificate. It imports the certificates of the root CA of Router 1 into Router 2 as the trusted ones. (Please also refer to "My Certificate" and "Issue Certificate" sections).

Establish an IPSec VPN tunnel with IKE and X.509 protocols by starting from either peer so that all client hosts in both of these subnets can communicate with each other.

Parameter Setup Example

(same as the one described in "My Certificate" section)

For Network-A at HQ

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

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-B at Branch Office

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

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*

Scenario Operation Procedure

(same as the one described in "My Certificate" section)

In the above diagram, "Router 1" is the gateway of Network-A at headquarters and the subnet of its Intranet is 10.0.76.0/24. It has the IP address of 10.0.76.2 for LAN interface and 203.95.80.22 for WAN-1 interface. "Router 2" is the gateway of Network-B in the branch office and the subnet of its Intranet is 10.0.75.0/24. It has the IP address of 10.0.75.2 for the LAN interface and 118.18.81.33 for the WAN-1 interface. They both serve as the NAT security gateways.

On Router 2 import the certificates of the root CA and HQCRT that were generated and signed by Router 1 into the "Trusted CA Certificate List" and "Trusted Client Certificate List" of Router 2.

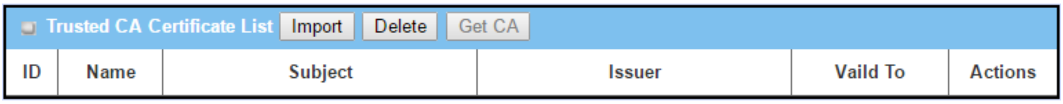
Import the obtained BranchCRT certificate (the derived BranchCSR certificate after Router 1’s root CA signature) into the "Trusted Client Certificate List" of the Router 1 and the "Local Certificate List" of the Router 2. For more details, refer to the Network-B operation procedure in the "My Certificate" section of this manual.

Router 2 can establish an IPSec VPN tunnel with "Site to Site" scenario and IKE and X.509 protocols to Router 1.

The client hosts in two subnets of 10.0.75.0/24 and 10.0.76.0/24 can communicate with each other.

4.5.4.2 Trusted CA Certificate List

To view the Trusted CA Certificate List open the **Object Definition** submenu, select **Certificate** and then click its **Trusted Certificate** tab, the **Trusted CA Certificate List** will appear in its own section:



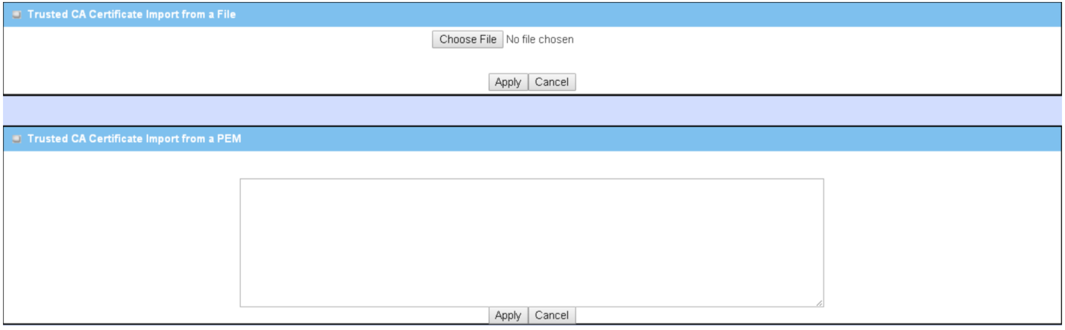
Trusted CA Certificate List Import Delete Get CA

ID	Name	Subject	Issuer	Vaild To	Actions

Figure 202 – Trusted CA Certificate List

4.5.4.3 Import Trusted CA Certificate

Click the **Import** button in the **Trusted CA Certificate List's** title bar to either import an existing Trusted CA certificate file or create a CA certificate by copying and pasting a PEM code string into the text entry field.



Trusted CA Certificate Import from a File

Choose File No file chosen

Apply Cancel

Trusted CA Certificate Import from a PEM

Apply Cancel

Figure 203 – Trusted CA Certificate Import – From File & From a PEM

Item	Notes	Description
Import from a File	Mandatory field.	Select a CA certificate file from a directory, and click the **Apply** button to import the specified CA certificate file in to the router.
Import from a PEM	Mandatory field. Enter text string.	Alternatively, copy (**Ctrl+C**) and paste (**Ctrl+V**) the PEM CA certificate code string into the text entry field, and click the **Apply** button to create the CA certificate in the router.
Apply	Button	Click the **Apply** button to import or create the certificate.
Cancel	Button	Click the **Cancel** button to discard the import operation and the screen will return to the Trusted Certificate page.

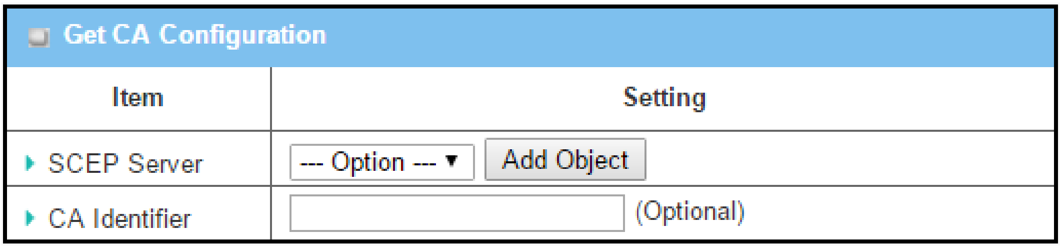
Table 120 – Trusted CA Certificate List

4.5.4.4 CA Certificate from SCEP Server

Providing SCEP is enabled, as an alternative to importing a Trusted CA certificates suing the import tools mentioned above, you can also generate the CA certificate from the SCEP server.

To enable SCEP go to **Object Definition > Certificate > Configuration**. When enabled, the **Get CA** button in the **Trusted CA certificate List's** caption bar will be available

Click the **Get CA** button to open the **Get CA Configuration** screen.



Get CA Configuration

Item	Setting
SCEP Server	--- Option --- ▼ Add Object
CA Identifier	(Optional)

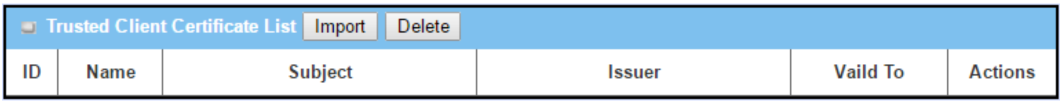
Figure 204 – Get CA Configuration

Item	Notes	Description
SCEP Server	Mandatory field.	Select a SCEP Server from the drop down list and then click the **Add Object** button to generate.
CA Identifier	String format can be any text. Optional field.	Identifies the CA to use for signing certificates.
Save	Button	Click **Save** to save the settings.
Close	Button	Click the **Close** button to return to the Configuration page.

Table 121 – Get CA Configuration settings

4.5.4.5 Trusted Client Certificate

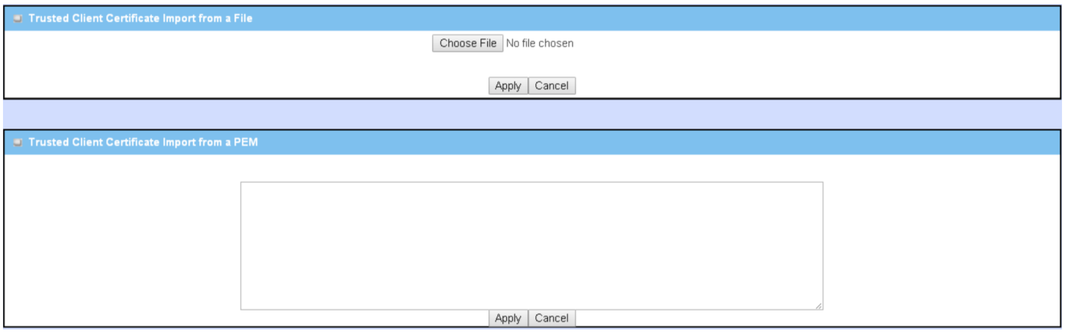
To view the Trusted Client Certificate List open the **Object Definition** submenu, select **Certificate** and then click its **Trusted Certificate** tab, the **Trusted Client Certificate List** will appear in its own section:



Trusted Client Certificate List Import Delete

ID	Name	Subject	Issuer	Vaild To	Actions

Figure 205 – Trusted Client Certificate List



Trusted Client Certificate Import from a File

Choose File No file chosen

Apply Cancel

Trusted Client Certificate Import from a PEM

Apply Cancel

Figure 206 – Trusted Client Certificate Import – From File & From a PEM

When **Import** button in the **Trusted Client Certificate List's** title bar is applied, two Import sections appear. You can either import a Trusted Client Certificate from an external certificate file, or directly paste a PEM code string in to the **Trusted Client Certificate Import from a PEM** field to define the trusted client certificate.

Item	Notes	Description
Import from a File	Mandatory field.	Select a trusted client Certificate file from a directory, and click the **Apply** button to import the specified file in to the router.

Item	Notes	Description
Import from a PEM	Enter text string. Mandatory field.	Alternatively, copy (**Ctrl+C**) and paste (**Ctrl+V**) the PEM trusted client certificate code string into the text entry field, and click the **Apply** button to create the trusted client certificate in the router.
Apply	Button	Click the **Apply** button to import or create the trusted client certificate.
Cancel	Button	Click the **Cancel** button to discard the import operation and the screen will return to the Trusted Certificate page.

Table 122 – Trusted Client Certificate import tools

4.5.4.6 Trusted Client Key

To view the Trusted Client Key List open the **Object Definition** submenu, select **Certificate** and then click its **Trusted Certificate** tab, the **Trusted Client Key List** will appear in its own section:

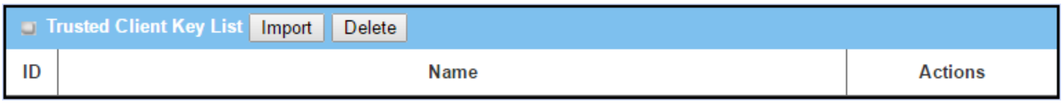


Figure 207 – Trusted Client Key List

When the **Import** button in the **Trusted Client Key List's** title bar is applied, two Import sections appear. You can either import a Trusted Client Key from an external key file, or directly paste a PEM code string in to the **Trusted Client Key Import from a PEM** field to define the client key.

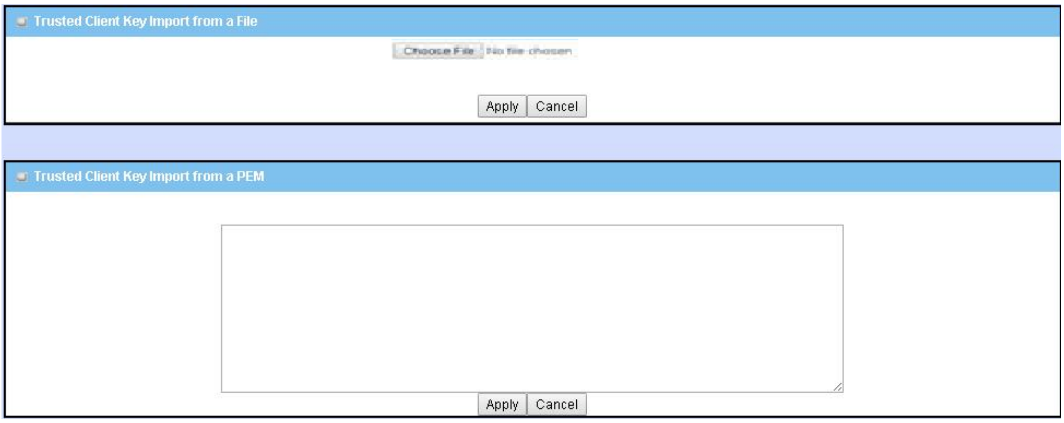

Trusted Client Key Import from a File
Choose File
No file chosen
Apply
Cancel
Trusted Client Key Import from a PEM
Apply
Cancel

Figure 208 – Trusted Client Key Import - From File & From a PEM

Item	Notes	Description
Import from a File	Mandatory field.	Select a trusted client key file from a directory, and click the **Apply** button to import the specified file in to the router.
Import from a PEM	Enter text string. Mandatory field.	Alternatively, copy (**Ctrl+C**) and paste (**Ctrl+V**) the PEM trusted client key code string into the text entry field, and click the **Apply** button to create the trusted client key in the router.
Apply	Button	Click the **Apply** button to import or create the trusted client certificate.

Item	Notes	Description
Cancel	Button	Click the **Cancel** button to discard the import operation and the screen will return to the Trusted Certificate page.

Table 123 – Trusted Client Key Import - From File & From a PEM

4.5.5 Issue Certificate

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

- Import a CSR file from the managing PC and then click on the **Sign** button, or
- Copy-paste the CSR codes into the router's web- based utility and then click on the **Sign** button.

If the router signs a CSR successfully, the **Signed Certificate View** section will display the signed certificate's contents.

Use the **Download** button to save a backup copy of the signed certificate as a file on the managing PC.

Self-signed Certificate Usage Scenario

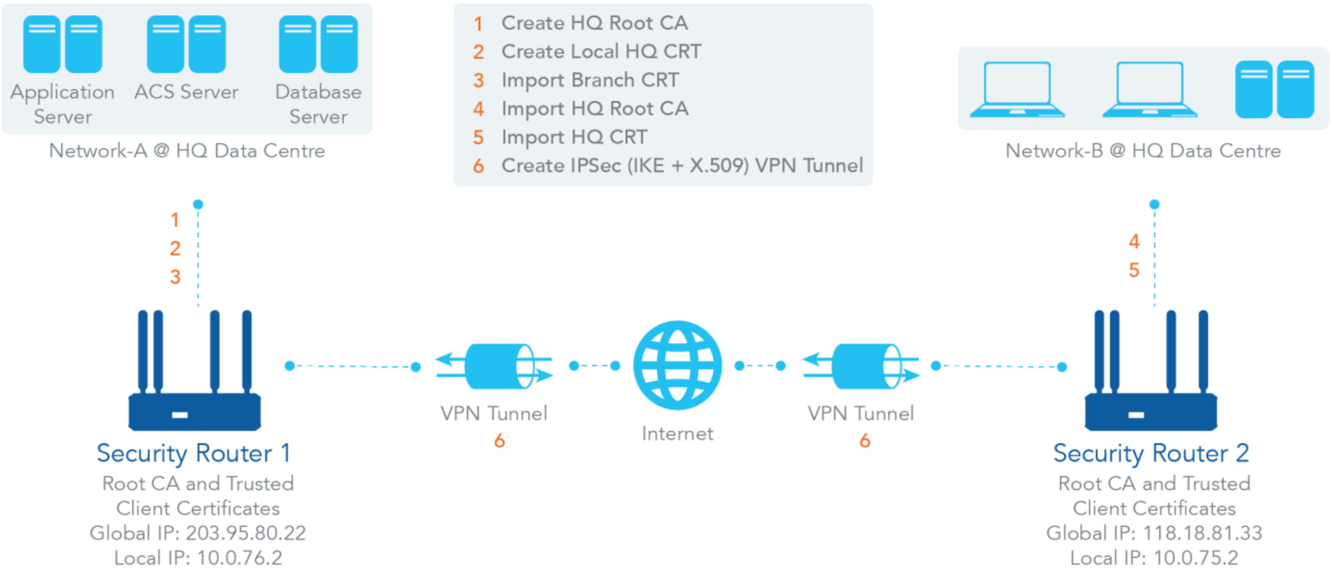


Figure 209 – Self-signed Certificate Usage Scenario

Scenario Application Timing

(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 by self-signing them. It also imports the trusted certificates for other CAs and Clients. These certificates can be used for two remote peers to verify their identity during establishment of a VPN tunnel.

Scenario Description

(same as the one described in "My Certificate" section)

Router 1 generates the root CA and a local certificate (HQCRT) signed by itself. It also imports a trusted certificate (BranchCRT) –a BranchCSR certificate of Router 2 signed by root CA of Router 1.

Router 2 creates a CSR (BranchCSR) to let the root CA of Router 1 sign it to be the BranchCRT certificate. Import the certificate into Router 2 as a local certificate. It also imports the certificates of the root CA of the Router 1 into the Router 2 as the trusted ones. (Please also refer to "My Certificate" and "Trusted Certificate" sections).

Establish an IPSec VPN tunnel with IKE and X.509 protocols by starting from either peer so that all client hosts in both of these subnets can communicate with each other.

Parameter Setup Example

(same as the one described in "My Certificate" section)

For Network-A at HQ

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

(same as the one described in "My Certificate" section)

In the diagram above, the "Router 1" is the gateway of Network-A in headquarters and the subnet of its Intranet is 10.0.76.0/24. It has the IP address of 10.0.76.2 for the LAN interface and 203.95.80.22 for the WAN-1 interface. “Router 2" is the gateway of Network-B in branch office and the subnet of its Intranet is 10.0.75.0/24. It has the IP address of 10.0.75.2 for the LAN interface and 118.18.81.33 for the WAN-1 interface. They both serve as the NAT security gateways.

Router 1 generates the root CA and a local certificate (HQCRT) that is signed by itself. Import the certificates of the root CA and HQCRT into the "Trusted CA Certificate List" and "Trusted Client Certificate List" of Router 2.

Router 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 Router 2, and click on the "View" button for that CSR). Take the CSR to be signed by the root CA of Router 1 and obtain the BranchCRT certificate (you need rename it). Import the certificate into the "Trusted Client Certificate List" of the Router 1 and the "Local Certificate List" of the Router 2.

Router 2 can establish an IPSec VPN tunnel with "Site to Site" scenario and IKE and X.509 protocols to Router 1.

The client hosts in two subnets of 10.0.75.0/24 and 10.0.76.0/24 can communicate with each other.

4.5.5.1 Import and Sign Certificate

To import Certificate Signing Request (CSR) to be signed by root CA open the **Object Definition** submenu, select **Certificate** and then click its **Issue Certificate** tab, use either the import or create from PEM section to import the signing request:

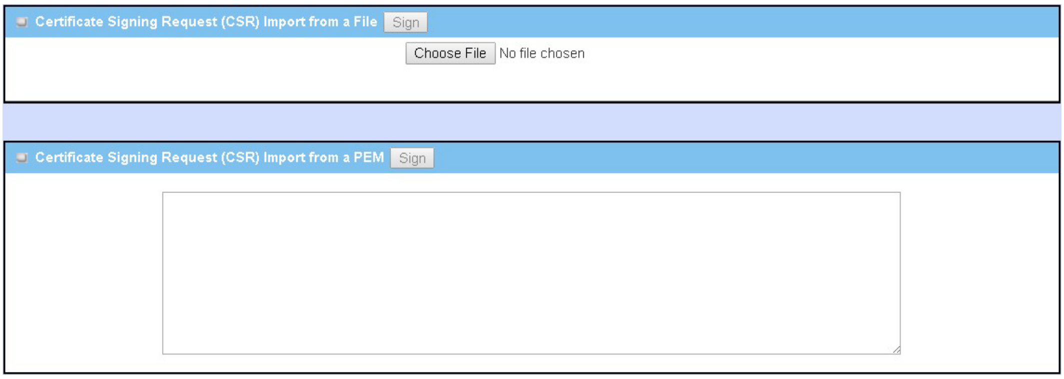

Certificate Signing Request (CSR) Import from a File
Sign
Choose File
No file chosen
Certificate Signing Request (CSR) Import from a PEM
Sign

Figure 210 – Certificate Signing Request (CSR) - From File & From a PEM

Item	Notes	Description
Certificate Signing Request (CSR) Import from a File	Mandatory field.	Select a trusted client key file from a directory, and click the **Apply** button to import the specified file in to the router.
Certificate Signing Request (CSR) Import from a PEM	Enter text string. Mandatory field.	Alternatively, copy (**Ctrl+C**) and paste (**Ctrl+V**) the PEM trusted client key code string into the text entry field, and click the **Apply** button to create the trusted client key in the router.
Sign	Button	Providing that a root CA exists, click the **Sign** button to sign and issue the imported certificate by the root CA.

Table 124 – Certificate Signing Request (CSR) - From File & From a PEM

5 Field Communication

5.1 Bus & Protocol

The NTC-400 Series Router router can use a DB-9 male port or other type of serial port to connect via an RS-232 serial device to an IP-based Ethernet LAN. These communication protocols give users access to serial devices anywhere over a local LAN or the Internet. They can be either "Virtual COM" and "Modbus".

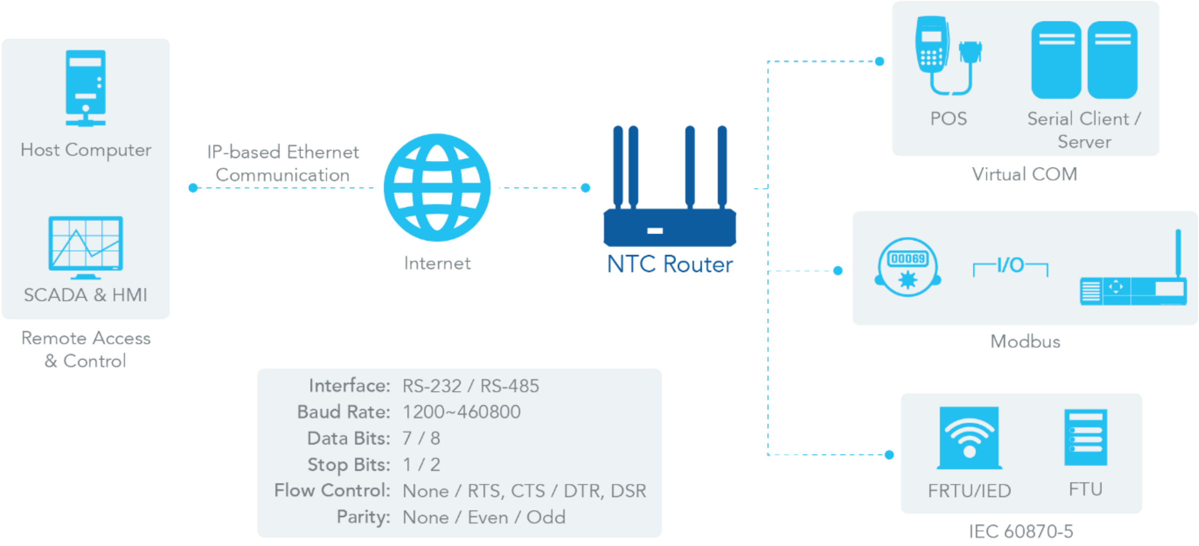


Figure 211 – Bus & Protocol

5.1.1 Port Configuration

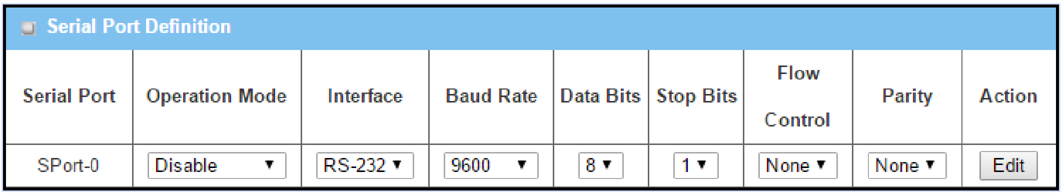
Before using the field communication function you need to configure the physical communication port.

The port configuration screen allows you to configure the operation mode and physical layer settings for each serial interface, and to quickly switch from one communication protocol to another for the serial port.

5.1.1.1 Port Configuration Setting

To view or change the serial port settings, open the **Field Communication** submenu, select **Bus & Protocol** and then click its **Port Configuration** tab, the current **Serial Port Definition** settings will appear in a static display.

When you click the **Edit** button in the **Action** column the serial port definition fields become enabled and you can enter new, or change existing, serial port parameters.



Serial Port Definition

Serial Port	Operation Mode	Interface	Baud Rate	Data Bits	Stop Bits	Flow Control	Parity	Action
SPort-0	Disable ▼	RS-232 ▼	9600 ▼	8 ▼	1 ▼	None ▼	None ▼	Edit

Figure 212 – Edit Serial Port Definition

Item	Notes	Description
Serial Port	System generated.	The serial port ID number of the serial port.

Item	Notes	Description
		The number of serial ports varies depending on the model you purchased.
Operation Mode	Disabled by default	The current operation mode for the serial interface. Depending on the model you purchased, the available modes are: **Virtual COM**, **Modbus**, or **IEC 60870-5**
Interface	Default setting: RS-232	Select **RS-232** as the physical interface for connecting to access device(s) with the same interface specification.
Baud Rate	Default setting: 19200	Select the appropriate baud rate for serial device communication. **RS-232**: 1200 / 2400 / 4800 / 9600 / 19200 / 38400 / 57600 / 115200
Data Bits	Default setting: 8	Select **8** or **7** for data bits.
Stop Bits	Default setting: 1	Select **1** or **2** for stop bits.
Flow Control	Default setting: None	Select **None**, **RTS**, **CTS**, **DTS** or **DSR** for Flow Control in RS-232 mode. Flow Control may not be supported depending on the model you have purchased.
Parity	Default setting: None	Select **None**, **Even** or **Odd** for Parity bit.
Action	Button	Click **Edit** to change the operation mode, or modify the parameters mentioned above for the serial interface communication.
Save	Button	Click **Save** button to save the settings.
Undo	Button	Click **Undo** to cancel the changes to settings.

Table 125 – Serial Port settings

5.1.2 Virtual COM

Create a virtual COM port on user's PC/Host to provide access to a serial device connected to the serial port on the router. Once set up, users can access, control, and manage the connected serial device through Internet (fixed line, or cellular network) anywhere. This application is also known as Ethernet pass-through communication.

Virtual COM setting screen enables user to connect a Virtual COM port based device to the Internet using one of four modes: **TCP Client**, **TCP Server**, **UDP**, and **RFC-2217**

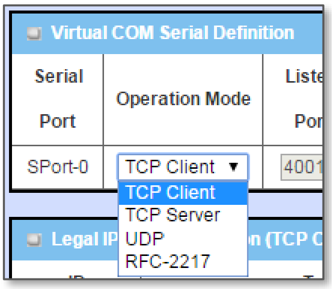


Figure 213 – Virtual COM Serial Port Operation Mode Selector

The exact parameters and definitions available for your Virtual COM port will depend on your selection in the **Operation Mode** drop down list. Each operation modes will be explained in the following sections.

5.1.2.1 Operation Mode – TCP Client

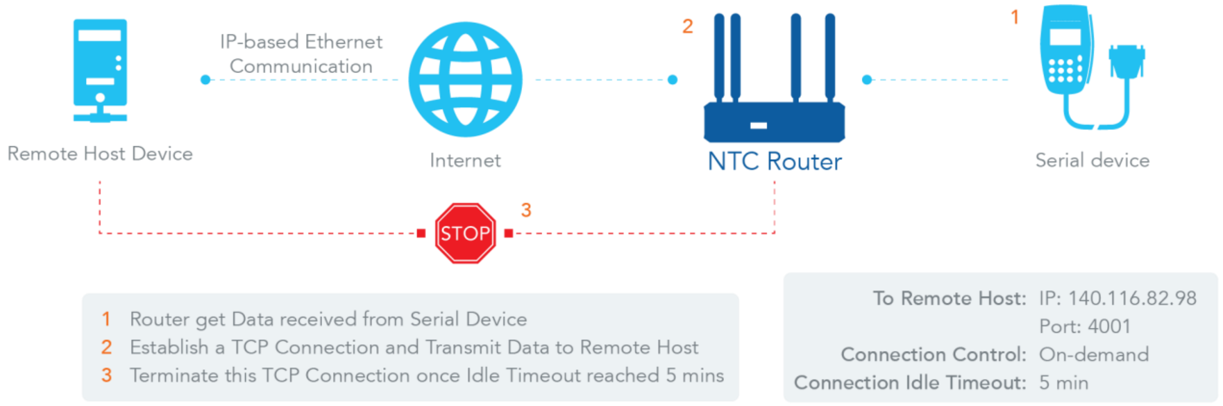
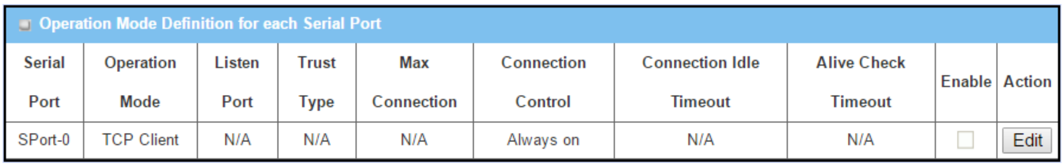

IP-based Ethernet Communication
Remote Host Device
Internet
2
NTC Router
1
Serial device
STOP
3
1 Router get Data received from Serial Device
2 Establish a TCP Connection and Transmit Data to Remote Host
3 Terminate this TCP Connection once Idle Timeout reached 5 mins
To Remote Host: IP: 140.116.82.98
Port: 4001
Connection Control: On-demand
Connection Idle Timeout: 5 min

Figure 214 – TCP Client Mode

When the administrator expects the router to actively establish a TCP connection to a pre-defined host computer when serial data arrives, the operation mode for the "Virtual COM" function is must be set to "TCP Client". When the connection control of virtual COM is "On-demand", when the router receives data from the connected serial device, it will establish a TCP connection to transfer the received serial data to the remote host. After the data has been transferred, the router automatically disconnects the established TCP session from the host computer by using the TCP alive check timeout or idle timeout settings.

When configured as a TCP (Transmission Control Protocol) Client, the device initiates a TCP connection with a TCP server when there is data to transmit. The device can be set to disconnect from the server when the connection is Idle for a specified period or it can be set to maintain a full-time connection with the TCP server.



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	N/A	N/A	N/A	Always on	N/A	N/A	□	Edit

Figure 215 – Operation Mode Definition for each Serial Port – TCP Client

Item	Notes	Description
Operation Mode	Mandatory setting.	Select **TCP Client**.
Listen Port	n/a	Field is disabled – it is not a relevant TCP Client setting.
Trust Type	n/a	Field is disabled – it is not a relevant TCP Client setting.
Max Connection	n/a	Field is disabled – it is not a relevant TCP Client setting.
Connection Control	Default setting: **Always on**	Two options: **Always on** – Full time TCP connection.

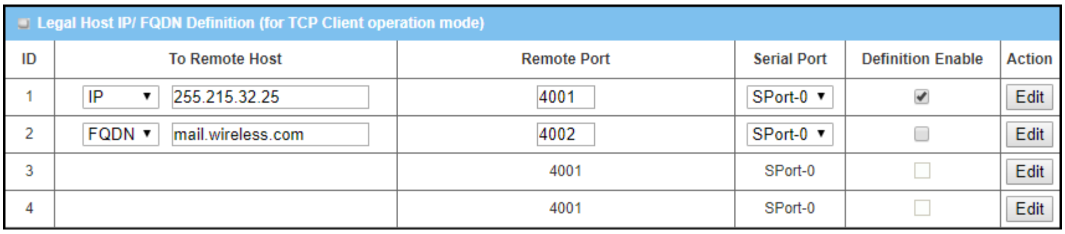
Item	Notes	Description
		On-Demand – Initiates TCP connection only when required to transmit and disconnect at idle timeout.
Connection Idle Timeout	Default setting: **0** Value Range: 0 - 60 minutes	The TCP connection is disconnected when the idle time has elapsed. Enter the idle timeout period in minutes. **Note** – Idle timeout is only available when **On-Demand** is selected in the **Connection Control** field, see above.
Alive Check Timeout	Default setting: **0** Value Range: 0 - 60 minutes	The TCP connection is terminated if it does not receive a response from an alive-check before this time period has elapsed. Enter the time period of alive check timeout in minutes.
Enable	Disabled by default.	Check ☑ **Enable** to activate the corresponding serial port in specified operation mode.
Save	Button	Click the **Save** button to save the configuration
Undo	Button	Click **Undo** to cancel the changes to settings.

Table 126 – Operation Mode Definition for each Serial Port – TCP Client

5.1.2.2 Specify Remote TCP Server

When **TCP Client** is selected as the Virtual COM **Operation Mode** the **Legal Host OIP/FQDN Definition (for TCP Client operation mode)** is displayed in a separate section on the **Virtual COM** tabbed page.

Press the **Edit** button to activate the fields for entering details of a new server or to edit the details of an existing one.



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

ID	To Remote Host	Remote Port	Serial Port	Definition Enable	Action
1	IP ▼ 255.215.32.25	4001	SPort-0 ▼	☑	Edit
2	FQDN ▼ mail.wireless.com	4002	SPort-0 ▼	□	Edit
3		4001	SPort-0	□	Edit
4		4001	SPort-0	□	Edit

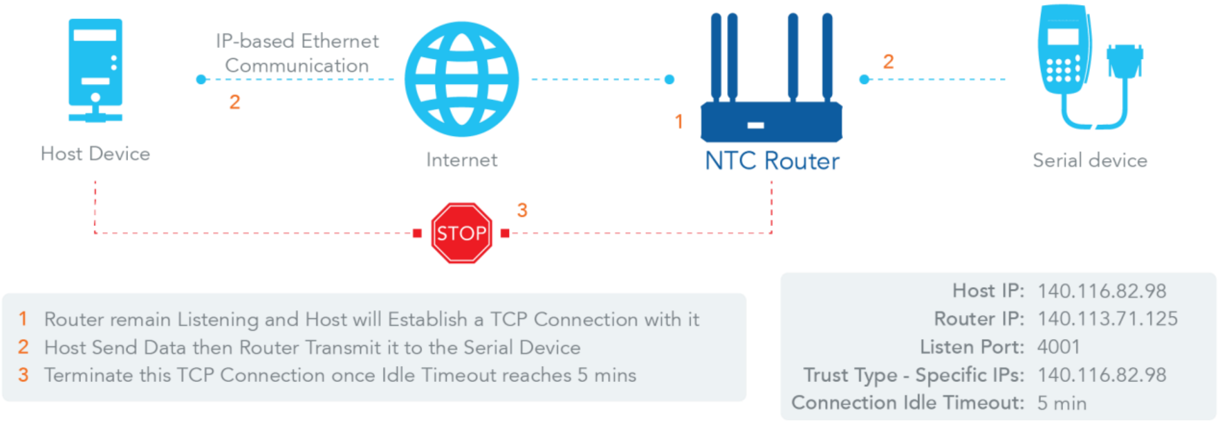
Figure 216 – Operation Mode Definition for each Serial Port – TCP Client

Item	Notes	Description
To Remote Host	Mandatory setting.	Press **Edit** button to enter **IP** address or **FQDN** of the remote TCP server for transmission of serial data.
Remote Port	Mandatory setting. Default setting: 4001 Value Range: 1 - 65535	Enter the TCP port number. This is the listening port of the remote TCP server.
Serial Port	Default setting: **SPort-0**	Apply the TCP server connection for a selected serial port. Up to four (4) TCP servers can be configured at the same time for each serial port.
Definition Enable	Disabled by default	Check ☑ **Enable** to enable the TCP server configuration.

Item	Notes	Description
Save	Button	Click the **Save** button to save the configuration.
Undo	Button	Click **Undo** to cancel the changes to settings.

Table 127 – Operation Mode Definition for each Serial Port – TCP Client

5.1.2.3 Operation Mode – TCP Server



1 Router remain Listening and Host will Establish a TCP Connection with it
2 Host Send Data then Router Transmit it to the Serial Device
3 Terminate this TCP Connection once Idle Timeout reaches 5 mins

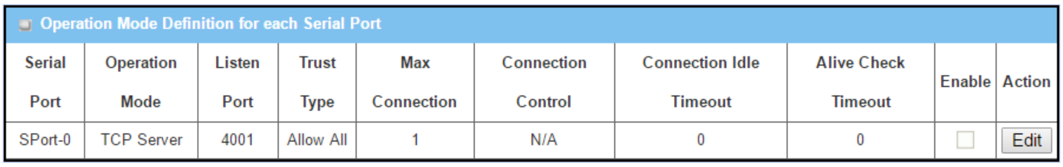
Host IP: 140.116.82.98
Router IP: 140.113.71.125
Listen Port: 4001
Trust Type - Specific IPs: 140.116.82.98
Connection Idle Timeout: 5 min

Figure 217 – TCP Server Mode

When the administrator expects the router to wait passively for the serial data requests from the Host Device (usually we use a computer to play as a Host), and the Host will establish a TCP connection to get data from the serial device, the operation mode for the "Virtual COM" function is must be set to "TCP Server". In this mode, the router 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. After the data has been transferred, the TCP connection will be automatically disconnected from the host computer by using the TCP alive check timeout or idle timeout settings.

When configured as the TCP (Transmission Control Protocol) Server the device waits for connections to be initiated by a remote TCP client device to receive serial data.

Users can designate specific TCP clients or allow any clients to send serial data for serial data transmission bandwidth control and access control. The TCP Server supports up to four (4) simultaneous connections to receive serial data from multiple TCP clients.


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 Server	4001	Allow All	1	N/A	0	0	□	Edit

Figure 22 – Operation Mode Definition for each Serial Port – TCP Server

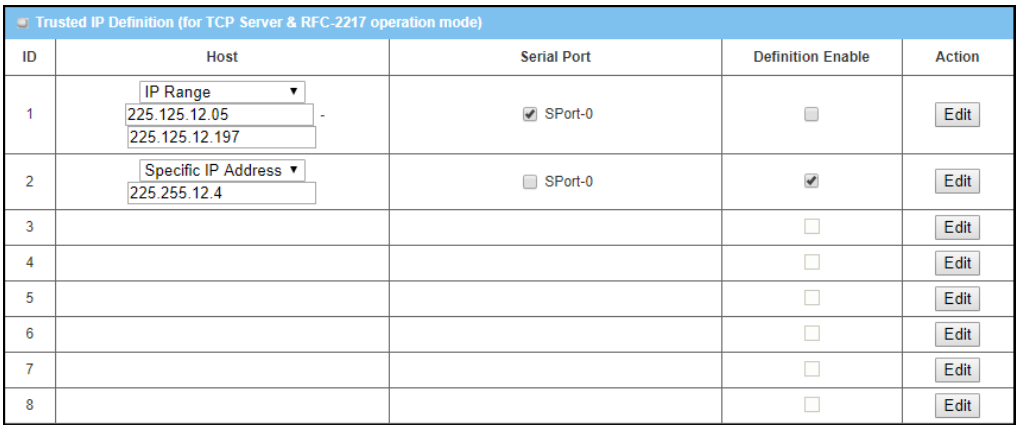
Item	Notes	Description
Operation Mode	Mandatory field.	Select TCP Server mode.
Listen Port	Default setting: 4001 Value Range: 1 - 65535	Indicate the listening port of TCP connection.

Item	Notes	Description
Trust Type	Default setting: **Allow All**	Two options: **Allow All** – Allow any TCP clients to connect. **Specific IP** – Limit access only to certain TCP clients.
Max Connection	Default setting: 1 Value Range: 1 - 4	Set the maximum number of concurrent TCP connections. Up to four (4) simultaneous TCP connections can be established.
Connection Idle Timeout	Default setting: 0 Value Range: 0 - 60 minutes	The TCP connection is disconnected when the idle time has elapsed. Enter the idle timeout period in minutes. **Note** – Idle timeout is only available when **On-Demand** is selected in the **Connection Control** field, see above.
Alive Check Timeout	Default setting: 0 Value Range: 0 - 60 minutes	The TCP connection is terminated if it does not receive a response from an alive-check before this time period has elapsed. Enter the time period of alive check timeout in minutes.
Enable	Disabled by default.	Check ☑ **Enable** to activate the corresponding serial port in specified operation mode.
Save	Button	Click **Save** button to save the settings.

Table 128 – Operation Mode Definition for each Serial Port – TCP Server

5.1.2.4 Specify TCP Clients for TCP Server Access

If you selected **Specific IPs** as the **Trust Type** for the TCP Server, the **Trusted IP Definition** section appears. The settings are valid for both TCP Server and RFC-2217 modes.



Trusted IP Definition (for TCP Server & RFC-2217 operation mode)

ID	Host	Serial Port	Definition Enable	Action
1	IP Range ▾ 225.125.12.05 - 225.125.12.197	☑ SPort-0	□	Edit
2	Specific IP Address ▾ 225.255.12.4	□ SPort-0	☑	Edit
3			□	Edit
4			□	Edit
5			□	Edit
6			□	Edit
7			□	Edit
8			□	Edit

Figure 218 – Trusted IP Definition - TCP Server

Item	Notes	Description
Host	Mandatory field.	Select from the two options in the drop down list: **Specific IP address** –Enter the IP address of the trusted host.

Item	Notes	Description
		IP Range – Enter the beginning and end IP addresses of the range of trusted TCP clients.
Serial Port	Disabled by default.	Check the box ☑ to apply the rule to this Serial Port.
Definition Enable	Disabled by default.	Check ☑ **Enable** box to enable the rule.
Edit	Button	Click **Edit** to add or change a Trusted IP address.
Save	Button	Click **Save** to save the settings
Undo	Button	Click **Undo** to cancel the settings

Table 129 – Trusted IP Definition - TCP Server

5.1.2.5 Operation Mode – UDP

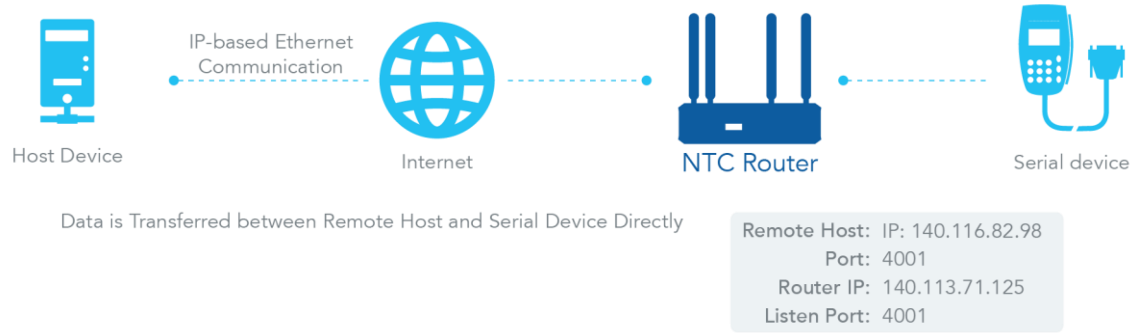
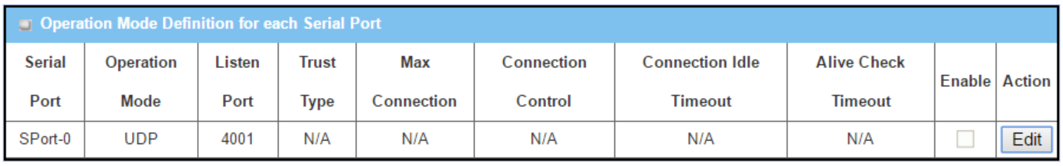

IP-based Ethernet Communication
Host Device
Internet
NTC Router
Serial device
Data is Transferred between Remote Host and Serial Device Directly
Remote Host: IP: 140.116.82.98
Port: 4001
Router IP: 140.113.71.125
Listen Port: 4001

Figure 219 – UDP Mode

If both the Remote Host Computer and the serial device are expected to initiate a data transfer, the operation mode for the "Virtual COM" function on the router must be set to "UDP". In this mode, the UDP data can be transferred between the router and multiple host computers from either peer, making this mode ideal for message display applications.

The remote host computer can directly send UDP data to the serial device via the gateway, and also receive UDP data from the serial device via the router at the same time. The router supports up to 4 legal hosts to connect simultaneously to the serial device via the router.

UDP (User Datagram Protocol) enables applications using UDP socket programs to communicate with the serial ports on the serial server. The UDP mode provides connectionless communications, which enable you to multicast data from the serial device to multiple host computers, and vice versa, making this mode ideal for message display applications.



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	UDP	4001	N/A	N/A	N/A	N/A	N/A	□	Edit

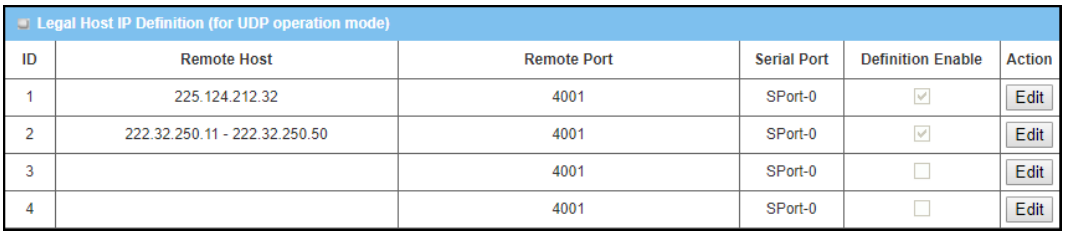
Figure 22 – Operation Mode Definition for each Serial Port – UDP Mode

Item	Notes	Description
Operation Mode	Mandatory field.	Select UDP mode.
Listen Port	Default setting: 4001	Indicate the listening port of the UDP connection. Value Range: 1 - 65535

Item	Notes	Description
Trust Type	n/a	Field is disabled – it is not relevant to the UDP operation mode.
Max Connection	n/a	Field is disabled – it is not relevant to the UDP operation mode.
Connection Control	n/a	Field is disabled – it is not relevant to the UDP operation mode.
Connection Idle Timeout	n/a	Field is disabled – it is not relevant to the UDP operation mode.
Alive Check Timeout	n/a	Field is disabled – it is not relevant to the UDP operation mode.
Enable	n/a	Field is disabled – it is not relevant to the UDP operation mode.
Edit	Button	Click Edit to add or change an Operation Mode definition.
Save	Button	Click Save to save the settings
Undo	Button	Click Undo to cancel the settings

Table 130 – Operation Mode Definition for each Serial Port – UDP Mode

5.1.2.6 Specify Remote UDP



Legal Host IP Definition (for UDP operation mode)

ID	Remote Host	Remote Port	Serial Port	Definition Enable	Action
1	225.124.212.32	4001	SPort-0	☑	Edit
2	222.32.250.11 - 222.32.250.50	4001	SPort-0	☑	Edit
3		4001	SPort-0	□	Edit
4		4001	SPort-0	□	Edit

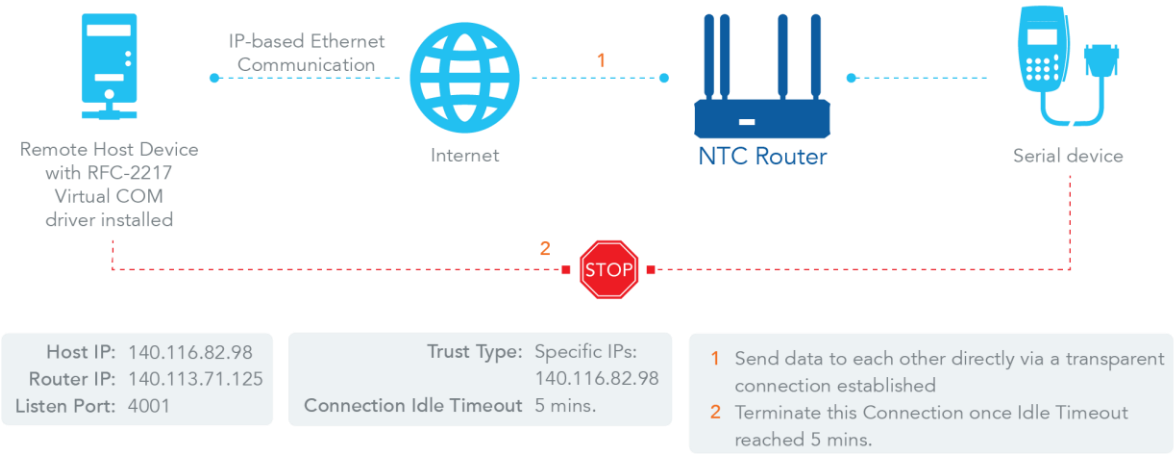
Figure 220 – Legal Host IP Definition - UDP operation mode

Item	Notes	Description
Remote Host	Mandatory field.	Select from the two options in the drop down list: **Specific IP address** –Enter the IP address of the trusted host. **IP Range** – Enter the beginning and end IP addresses of the range of trusted TCP clients.
Remote Port	Default setting: 4001 Value Range: 1 - 65535	Indicate the UDP port of peer UDP hosts.
Serial Port	SPort-0Default setting:	Apply the UDP hosts for a selected serial port. Up to four (4) UDP servers can be configured at the same time for each serial port.
Definition Enable	Disabled by default.	Check ☑ **Enable** to enable the access to this host.

Item	Notes	Description
Edit	Button	Click **Edit** to add or change a Legal Host IP address.
Save	Button	Click **Save** to save the settings
Undo	N/A	Click **Undo** to cancel the settings

Table 131 – Legal Host IP Definition - UDP operation mode

5.1.2.7 Operation Mode – RFC-2217


IP-based Ethernet Communication
1
Remote Host Device with RFC-2217 Virtual COM driver installed
Internet
NTC Router
Serial device
2
STOP

Host IP: 140.116.82.98
Router IP: 140.113.71.125
Listen Port: 4001

Trust Type: Specific IPs: 140.116.82.98
Connection Idle Timeout 5 mins.

1 Send data to each other directly via a transparent connection established
2 Terminate this Connection once Idle Timeout reached 5 mins.

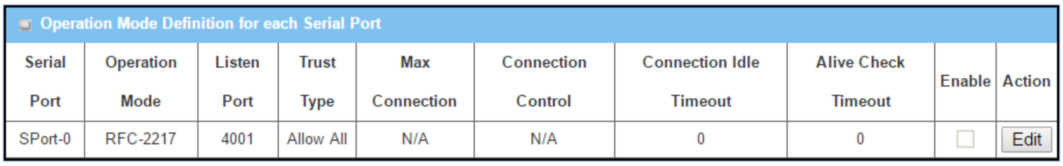
Figure 221 – RFC-2217 Mode

RFC-2217 defines general COM port control options based on the telnet protocol. A host computer with an RFC-2217 driver installed can monitor and manage the remote serial device attached to the router'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, you must specify the IP address of the host computers to establish connection with.

Any 3rd party driver supporting RFC-2217 can be installed on the host computer. The driver establishes a transparent connection between the host and a serial device by mapping the IP:Port of the router's serial port to a virtual local COM port on the host computer.

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

RFC-2217 defines general COM port control options based on the telnet protocol. In RFC-2217 mode, a remote host can monitor and manage remote serial devices in the same manner as if they were connected to the local serial port. When a virtual serial port on the local serial device is created, you must specify the IP address of the remote hosts to establish connections with.



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	RFC-2217	4001	Allow All	N/A	N/A	0	0	□	Edit

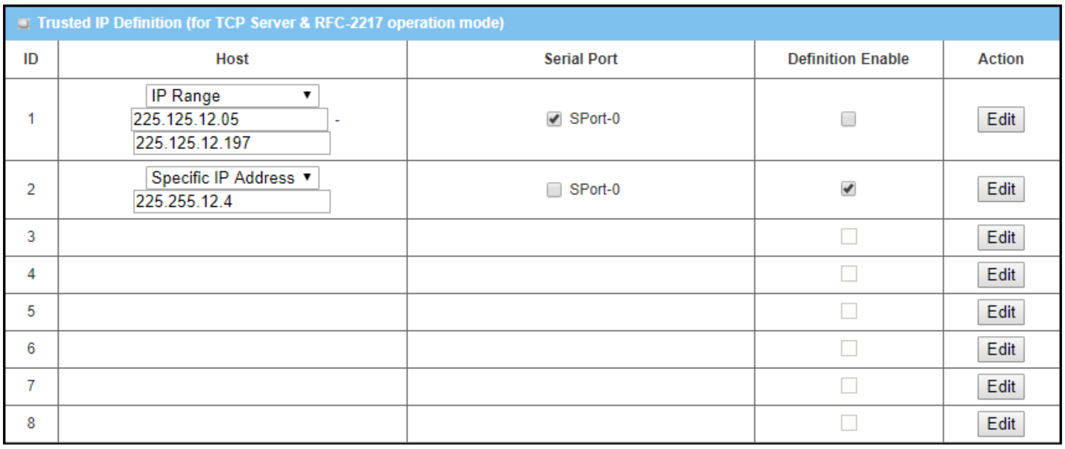
Figure 22 – Operation Mode Definition for each Serial Port – RFC-2217 Mode

Item	Notes	Description
Operation Mode	Mandatory field.	Select RFC-2217 mode.
Listen Port	Default setting: 4001 Value Range: 1 - 65535	Enter the listening port of the RFC-2217 connection. Value Range: 1 - 65535
Trust Type	Default setting: Allow All	Choose Allow All to allow any clients to connect. Otherwise choose Specific IP to limit certain clients.
Connection Idle Timeout	Default setting: 0	The TCP connection is disconnected when the idle time has elapsed. Enter the idle timeout period in minutes. **Note** – Idle timeout is only available when **On-Demand** is selected in the **Connection Control** field, see above.
Alive Check Timeout	Default setting: 0	The TCP connection is terminated if it does not receive a response from an alive-check before this time period has elapsed. Enter the time period of alive check timeout in minutes.
Enable	Disabled by default.	Check ☑ **Enable** to activate the corresponding serial port in the specified operation mode.
Edit	Button	Click **Edit** to add or change an Operation Mode Definition.
Save	Button	Click **Save** to save the settings
Undo	Button	Click **Undo** to cancel the settings

Table 132 – Operation Mode Definition for each Serial Port –RFC-2217 Mode

5.1.2.8 Specify Remote Host for Access

If you selected **Specific IPs** as the **Trust Type**, the T**rusted IP Definition** section appears. The settings are valid for both TCP Server and RFC-2217 modes.



Trusted IP Definition (for TCP Server & RFC-2217 operation mode)

ID	Host	Serial Port	Definition Enable	Action
1	IP Range ▾ 225.125.12.05 - 225.125.12.197	☑ SPort-0	□	Edit
2	Specific IP Address ▾ 225.255.12.4	□ SPort-0	☑	Edit
3			□	Edit
4			□	Edit
5			□	Edit
6			□	Edit
7			□	Edit
8			□	Edit

Figure 222 – Trusted IP Definition - TCP Server

Item	Notes	Description
Host	Mandatory field.	Enter the IP address range of allowed TCP clients.

Item	Notes	Description
Serial Port	Disabled by default.	Check the box to specify the rule for selected Serial Port.
Definition Enable	Disabled by default.	Check ☑ **Enable** box to enable the rule.
Edit	Button	Click **Edit** to add or change a Trusted IP address.
Save	Button	Click **Save** to save the settings
Undo	Button	Click **Undo** to cancel the settings

Table 133 – Trusted IP Definition for each Serial Port - RFC-2217 Mode

6 Security

6.1 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 shared or public networks as if it were directly connected to the private network, while benefitting from the functionality, security and management policies of the 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. Tunnel technology supports data confidentiality, data origin authentication and data integrity of network information by utilizing encapsulation protocols, encryption algorithms, and hashing algorithms.

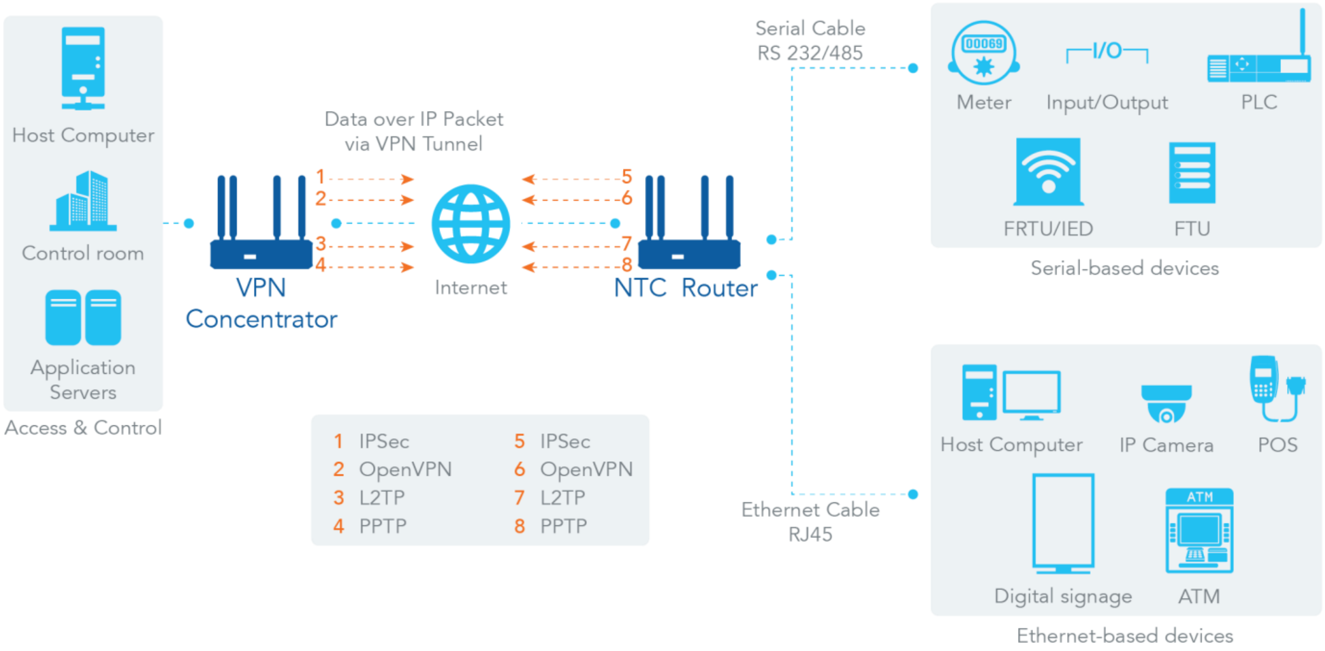


Figure 223 – VPN

The NTC-400 Series Router supports different tunnelling technologies such as IPSec, OpenVPN, L2TP (over IPSec), PPTP and GRE to establish secure tunnels between multiple sites for data transfer. More advanced functions such as Full Tunnel, Tunnel Failover, NetBIOS over IPSec, NAT Traversal and Dynamic VPN are also supported.

6.1.1 IPSec

Internet Protocol Security (IPSec) is a protocol suite for securing Internet Protocol (IP) communications by authenticating and encrypting each IP packet of a communication session. 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 IPSec client and server. The IPSec VPN client is referred to as the initiator and the IPSec VPN server as the responder.

6.1.1.1 IPSec Tunnel Scenarios

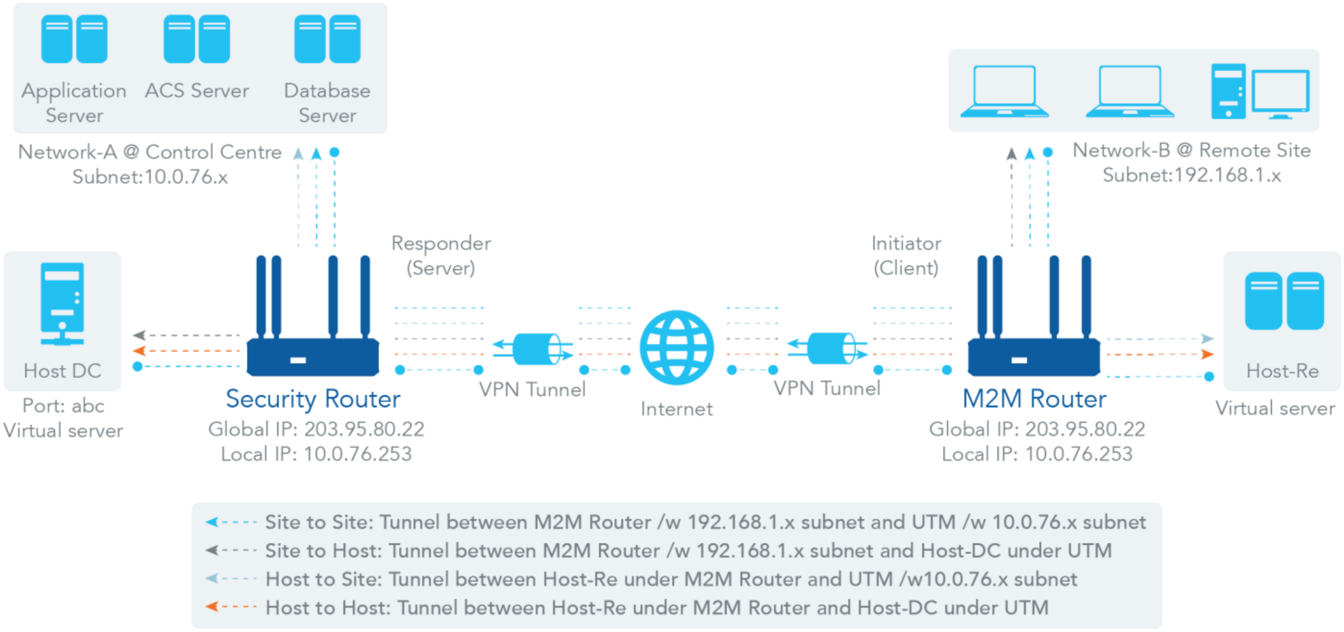

Application Server
ACS Server
Database Server
Network-A @ Control Centre
Subnet:10.0.76.x
Network-B @ Remote Site
Subnet:192.168.1.x
Responder (Server)
Initiator (Client)
Host DC
Port: abc
Virtual server
Security Router
Global IP: 203.95.80.22
Local IP: 10.0.76.253
VPN Tunnel
Internet
VPN Tunnel
M2M Router
Global IP: 203.95.80.22
Local IP: 10.0.76.253
Host-Re
Virtual server
Site to Site: Tunnel between M2M Router /w 192.168.1.x subnet and UTM /w 10.0.76.x subnet
Site to Host: Tunnel between M2M Router /w 192.168.1.x subnet and Host-DC under UTM
Host to Site: Tunnel between Host-Re under M2M Router and UTM /w10.0.76.x subnet
Host to Host: Tunnel between Host-Re under M2M Router and Host-DC under UTM

Figure 224 – IPSec Tunnel Scenarios

To build an IPSec tunnel, you must fill in the remote gateway global IP and optional subnet if the hosts behind IPSec peer can access to remote site or hosts. Under such configuration, there are four scenarios:

Site to Site: You need to setup a remote gateway IP and the subnet of both gateways. After the IPSec tunnel is established, hosts behind both gateways can communicate with each other through the tunnel.

Site to Host: Site to Host is suitable for tunnelling between clients in a subnet and an application server (host). As in the diagram above, the clients behind the M2M gateway can access the host "Host-DC" located in the control centre through the Site to Host VPN tunnel.

Host to Site: For a single host (or mobile user) to access the resources located on an intranet, the Host to Site scenario can be applied.

Host to Host: Host to Host is a special configuration for building a VPN tunnel between two single hosts.

6.1.1.2 Site to Site with "Full Tunnel" enabled

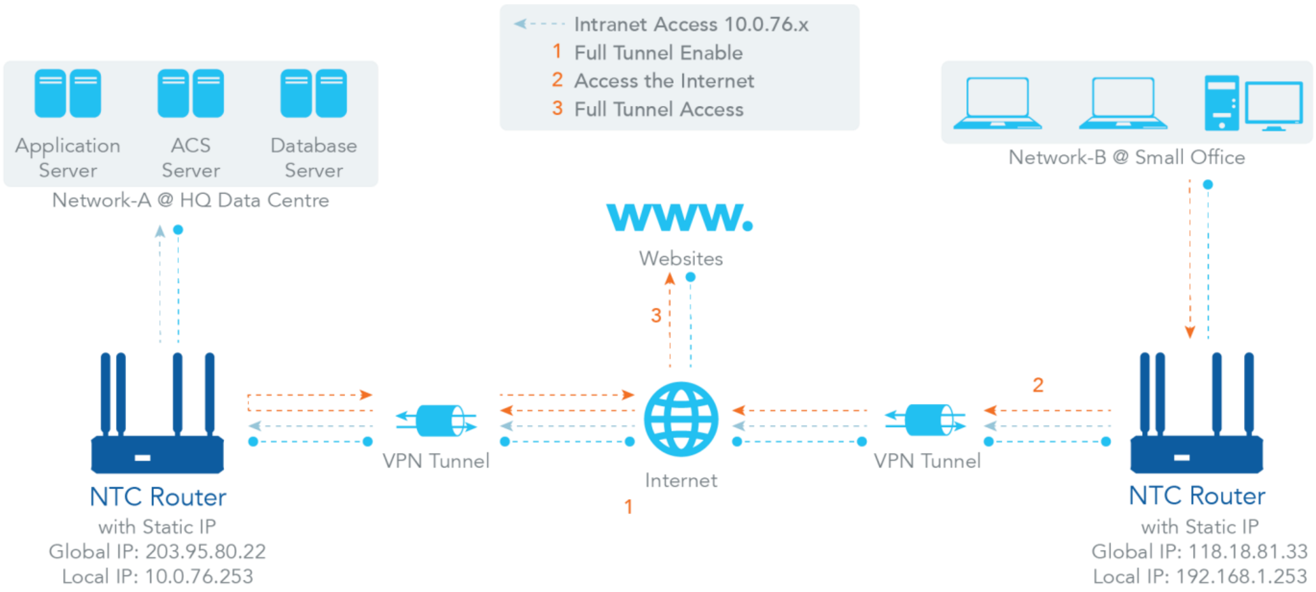


Figure 225 – Site to Site with Full Tunnel enabled

In a "Site to Site" scenario, client hosts at the remote site can access the enterprise resources on the Intranet of the HQ gateway via an established IPSec tunnel, as described above. However, Internet access requests from the remote site still go through its regular WAN connection. If you want all packets from the remote site to be routed via this IPSec tunnel, including HQ server access and Internet access, you can enable the “Full Tunnel" setting. As a result, every time users access the Internet or the HQ server, all traffic is routed through the secure IPSec tunnel and routed by the Security Gateway in the control centre.

6.1.1.3 Site to Site with "Hub and Spoke" mechanism

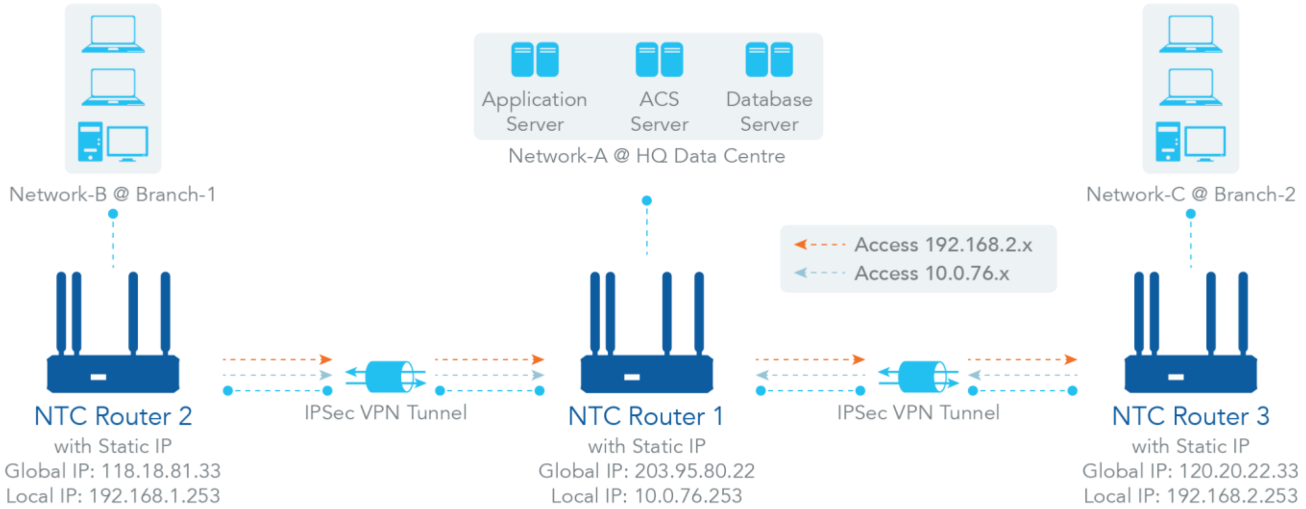


Figure 226 – Site to Site with Hub and Spoke mechanism

For a control centre to manage the secure Intranet among all of its remote sites, there is a simple configuration, called **Hub and Spoke** for the whole VPN network. A Hub and Spoke VPN Network is set up in organizations with centralized control centres over all its remote sites. The control centre acts as the Hub and the remote sites act as Spokes. All VPN tunnels from remote sites terminate at this Hub which acts as a concentrator. Site-to-site connections between spokes do not exist. Traffic originating from one spoke and destined for another spoke must go via the Hub. Under this configuration, you don't need to maintain VPN tunnels between each two remote clients.

6.1.1.4 Dynamic VPN Server Scenario

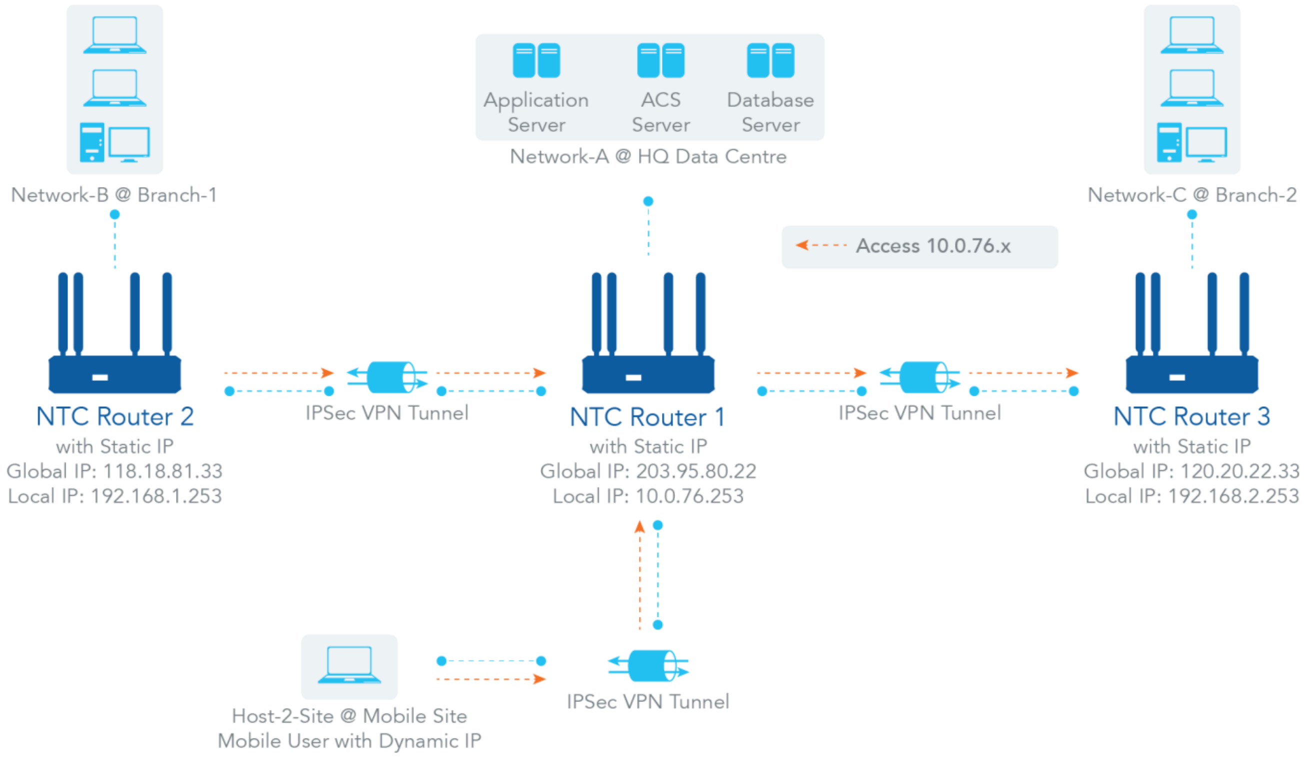
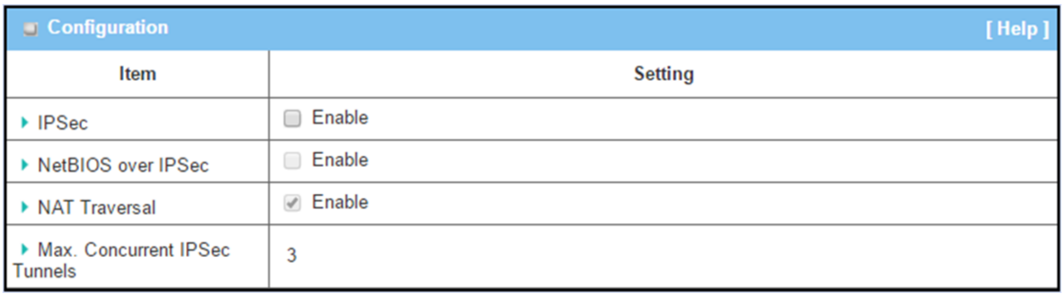


Figure 227 – Dynamic VPN Server Scenario

Dynamic VPN Server Scenario is an efficient way to build multiple tunnels with remote sites, especially for mobile clients with dynamic IP addresses. In this scenario, the router can only take the role of a server (responder), and it must have a "Static IP" or "FQDN". It can allow many VPN clients (initiators) to connect to various tunnel scenarios. In short, with a simple Dynamic VPN server setting, many VPN clients can connect to the server. In comparison to the Hub and Spoke mechanism direct communication between any two clients via the Dynamic VPN server is not allowed. You can configure one Dynamic VPN server for each WAN interface of the NTC-400 Series Router.

To create and configure IPSec tunnels, go to the **Security** menu, select **VPN** from the submenu and click its **IPSec** tab.


Configuration [Help]

Item	Setting
IPSec	□ Enable
NetBIOS over IPSec	□ Enable
NAT Traversal	☑ Enable
Max. Concurrent IPSec Tunnels	3

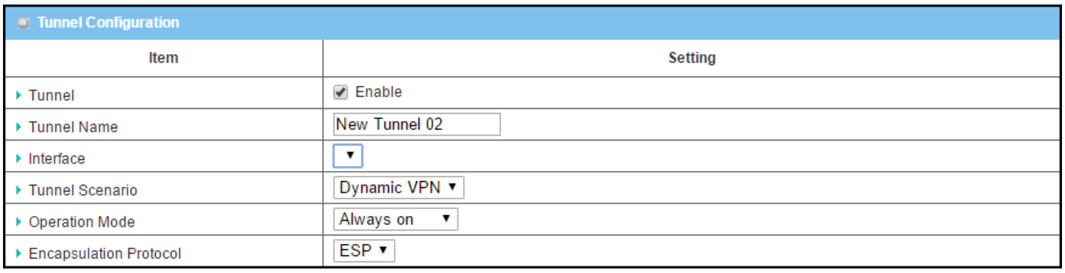
Figure 228 – Enable IPSec

Item	Notes	Description
IPsec	Disabled by default	Check ☑ **Enable** to enable IPSec function.
NetBIOS over IPSec	Disabled by default	Check ☑ **Enable** to enable NetBIOS over IPSec function.
NAT Traversal	Enabled by default	Un-check ☐ **Enable** to disable NAT Traversal functionality.
Max. Concurrent IPSec Tunnels	System setting.	Limits the maximum number of simultaneous IPSec tunnel connections. The default value varies from model to model.
Save	Button	Click **Save** to save the settings.
Undo	Button	Click **Undo** to cancel the settings.

Table 134 – Enable IPSec

To create an IPSec tunnel, check **IPSec ☑ Enable** in the **Configuration** section, and then click the enabled **Add** button in the **IPSec Tunnel List** section.

The **Tunnel Configuration** section, along with six other settings boxes (**Local & Remote Configuration**, **Authentication**, **IKE Phase**, **IKE Proposal Definition**, **IPSec Phase** and **IPSec Proposal Definition**), will open for the new tunnel.



Tunnel Configuration

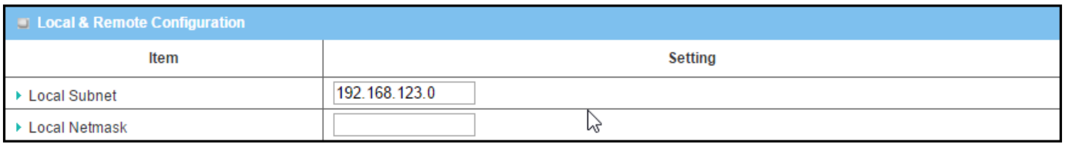
Item	Setting
Tunnel	☑ Enable
Tunnel Name	New Tunnel 02
Interface	▾
Tunnel Scenario	Dynamic VPN ▾
Operation Mode	Always on ▾
Encapsulation Protocol	ESP ▾

Figure 229 – IPSec Tunnel Configuration

Item	Notes	Description
Tunnel	Disabled by default	Select ☑ **Enable** to activate the IPSec tunnel
Tunnel Name	Mandatory field. String format can be any text.	Enter a meaningful tunnel name. Value Range: 1 - 19 characters
Interface	Mandatory field. Default setting: **WAN 1**	Select the IPSec tunnel interface type: **WAN** or **LAN**
Tunnel Scenario	Mandatory field. Default setting: **Site-to-Site**	Select an IPSec tunnelling scenario from the dropdown list: **Site-to-Site**, **Site-to-Host**, **Host-to-Site**, or **Host-to-Host** If the **LAN** interface is selected (see previous setting, above), only **Host-to-Host** scenario is available. With **Site-to-Site**, **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.

Item	Notes	Description
Operation Mode	Mandatory field. Default setting: **Always on**	Set the operation mode for the IPSec Tunnel: **Always On** or **Failover** If this tunnel is set as a failover tunnel, you need to further select a primary tunnel from which to failover to. **Note** – **Failover** mode is not available for the router with single **WAN**.
Encapsulation Protocol	Mandatory field. Default setting: **ESP**	Select the Encapsulation Protocol from the dropdown list for this IPSec tunnel. Available encapsulations are: **ESP** or **AH**

Table 135 – IPSec Tunnel Configuration



Local & Remote Configuration

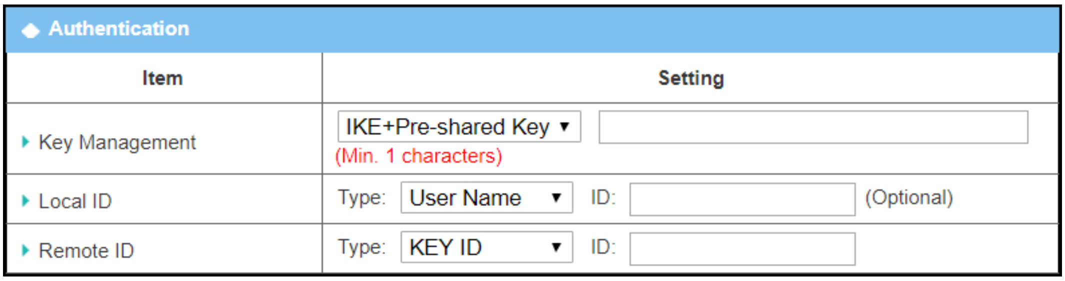
Item	Setting
Local Subnet	192.168.123.0
Local Netmask	

Figure 230 – Local & Remote Configuration

Item	Notes	Description
Local Subnet List	Mandatory field.	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
Local Netmask	Mandatory field.	Enter the subnet mask of the local subnet.

Table 136 – IPSec Local & Remote Configuration

6.1.1.5 Authentication



Authentication

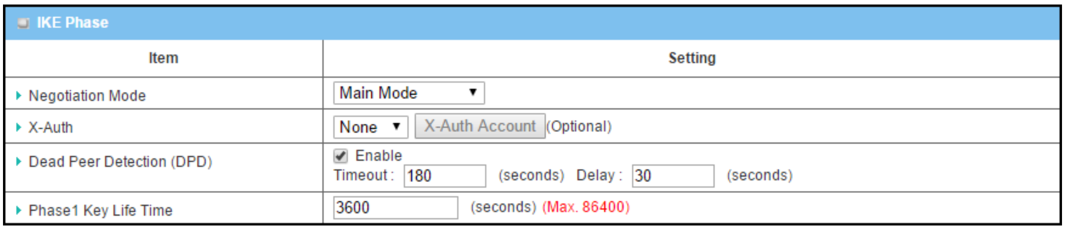
Item	Setting
Key Management	IKE+Pre-shared Key ▾ (Min. 1 characters)
Local ID	Type: User Name ▾ ID: (Optional)
Remote ID	Type: KEY ID ▾ ID:

Figure 231 – IPSec Authentication

Item	Notes	Description
Key Management	Mandatory field. 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 (8 - 32 characters). **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	Optional setting.	Specify the Local ID for this IPSec tunnel to authenticate: **User Name** – The username may include letters and numbers, but cannot be all numbers. **FQDN** – Enter the FQDN. **User@FQDN** – Enter the User@FQDN. **Key ID** – The Key ID can be letters and/or numbers.
Remote ID	Optional setting.	Specify the Remote ID for this IPSec tunnel to authenticate. **User Name** – The username may include letters and numbers, but cannot be all numbers. **FQDN** – Enter the FQDN. **User@FQDN** – Enter the User@FQDN. **Key ID** – The Key ID can be letters and/or numbers. **Note** – **Remote ID** will be not available when **Dynamic VPN** option in **Tunnel Scenario** is selected.

Table 137 – IPSec Authentication

6.1.1.6 IKE Phase



IKE Phase

Item	Setting
Negotiation Mode	Main Mode ▾
X-Auth	None ▾ X-Auth Account (Optional)
Dead Peer Detection (DPD)	☑ Enable Timeout : 180 (seconds) Delay : 30 (seconds)
Phase1 Key Life Time	3600 (seconds) (Max. 86400)

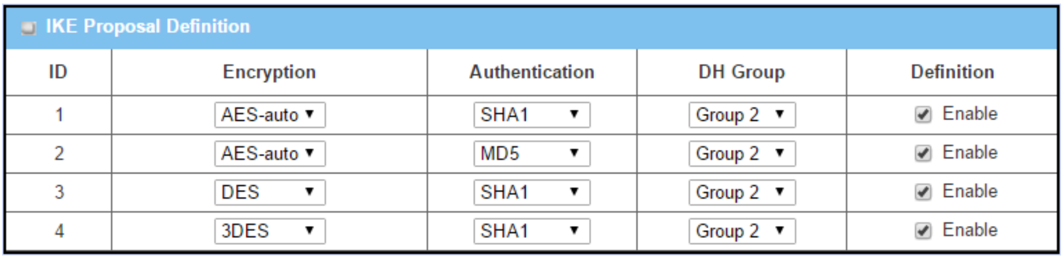
Figure 232 – IPSec IKE Phase

Item	Notes	Description
Negotiation Mode	Default setting: **Main Mode**	Choose **Main Mode** or **Aggressive Mode**
X-Auth	Default setting: None	Specify the X-Auth role for this IPSec tunnel: **Select Server**, **Client**, or **None** **None** – No X-Auth authentication is required.

Item	Notes	Description
		Selected Server – This router will be an X-Auth server. Click on the X-Auth Account button to create remote X-Auth client account. **Selected Client** –This router will be an X-Auth client. Enter User name and Password to be authenticated by the X-Auth server router. **Note** – **X-Auth Client** will not be available if the **Dynamic VPN** option was selected in Tunnel Scenario.
Dead Peer Detection (DPD)	Mandatory field. Disabled by default.	Select ☑ **Enable** to activate the DPD function. Specify the Timeout and Delay time in seconds. *Value Range*: 0 - 999 seconds for Timeout and Delay.
Phase1 Key Life	Mandatory field Default setting: **3600s** Maximum: 86400s	Specify the Phase1 Key Life Time. *Value Range*: 30 - 86400.

Table 138 – IPSec IKE Phase

6.1.1.7 IKE Proposal Definition



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

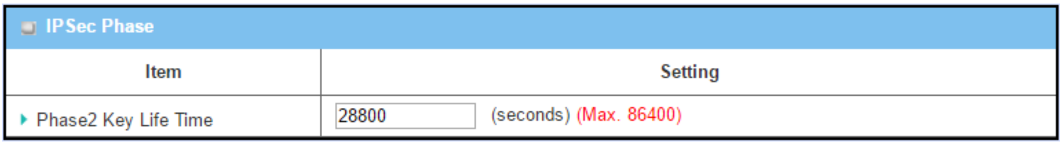
Figure 233 – IKE Proposal Definition

Item	Notes	Description
ID	Static integer	System generated IKE Proposal Definition reference number.
Encryption	Drop-down list	Choose from the following encryption methods from the drop down list: **DES** **3DES** **AES-auto** **AES-128** **AES-192** **AES-256**
Authentication	Drop-down list	Choose from the following authentication methods from the drop down list: **None** **MD5** **SHA1** **SHA2-256**
DH Group	Drop-down list	Select the **DH Group** from the drop down list, it can be:

Item	Notes	Description
		None **Group1** **Group2** **Group5** **Group14** **Group15** **Group16** **Group17** **Group18**
Definition	Check-box	Check ☑ **Enable** to activate each setting.

Table 139 – IKE Proposal Definition

6.1.1.8 IPSec Phase



IPSec Phase

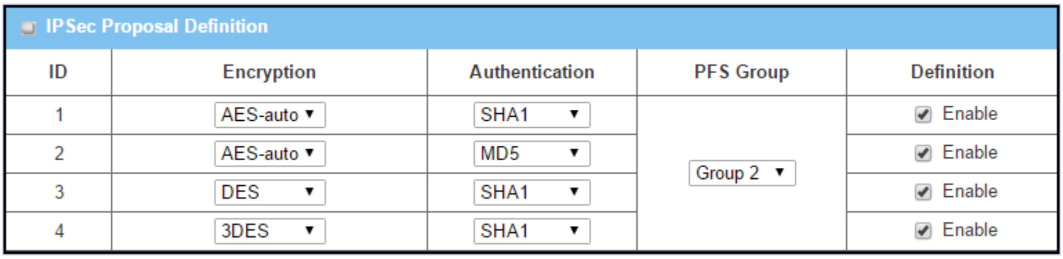
Item	Setting
Phase2 Key Life Time	28800 (seconds) (Max. 86400)

Figure 234 – IPSec Phase

Item	Notes	Description
Phase2 Key Life Time	Mandatory field. Default setting: 28800s Maximum= 86400s	Specify the Phase2 Key Life Time in seconds. Value Range: 30 - 86400.

Table 140 – IPSec Phase

6.1.1.9 IPSec Proposal Definition



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

Figure 235 – IPSec Proposal Definition

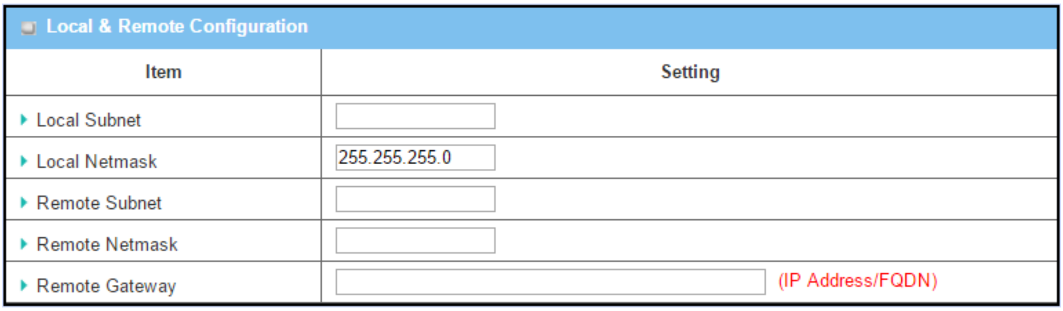
Item	Notes	Description
ID	Static integer	System generated IKE Proposal Definition reference number.
Encryption	Drop-down list	Choose from the following encryption methods from the drop down list: **DES** **3DES** **AES-auto**

Item	Notes	Description
		AES-128 **AES-192** **AES-256**
Authentication	Drop-down list	Choose from the following authentication methods from the drop down list: **None** **MD5** **SHA1** **SHA2-256**
PF $ Group	Drop-down list	Select the **PF$ Group** to be applied to all IPSec Proposal Definitions from the drop down list, it can be: **None** **Group1** **Group2** **Group5** **Group14** **Group15** **Group16** **Group17** **Group18**
Definition	Check-box	Check ☑ Enable to activate each setting.

Table 141 – IPSec Proposal Definition

6.1.1.10 Manual Key Management

When the **Manually** option is selected for Key Management as described in Authentication Configuration , a series of configuration windows for Manual IPSec Tunnel configuration will appear. The configuration windows are the **Local & Remote Configuration**, the **Authentication**, and the **Manual Proposal**.


Local & Remote Configuration

Item	Setting
Local Subnet	
Local Netmask	255.255.255.0
Remote Subnet	
Remote Netmask	
Remote Gateway	(IP Address/FQDN)

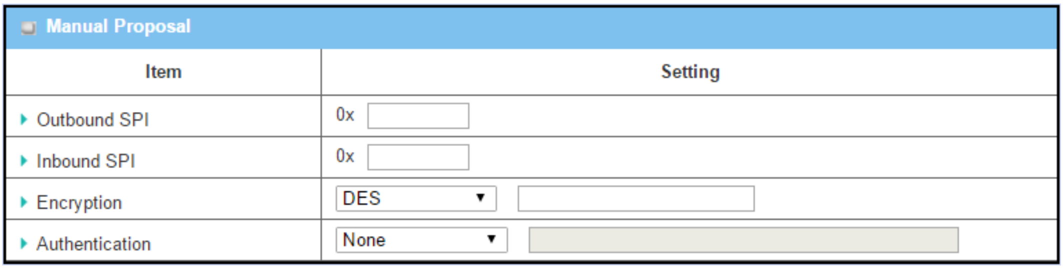
Figure 236 – Manual Key Management

Item	Notes	Description
Local Subnet	Mandatory field.	Enter the Local Subnet IP address and Subnet Mask.
Local Netmask	Mandatory field.	Enter the Local Subnet Mask.

Item	Notes	Description
Remote Subnet	Mandatory field.	Enter the Remote Subnet IP address
Remote Netmask	Mandatory field.	Enter the Remote Subnet Mask.
Remote Gateway	Mandatory field.	Enter the Remote Router's IPv4 address or FQDN name.

Table 142 – Manual Key Management

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



Manual Proposal

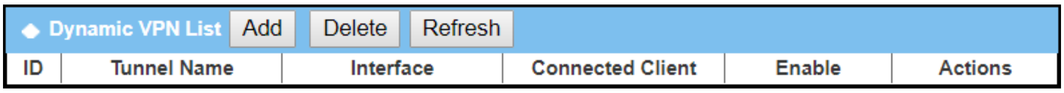
Item	Setting
Outbound SPI	0x
Inbound SPI	0x
Encryption	DES ▼
Authentication	None ▼

Figure 237 – Manual Proposal

Item	Notes	Description
Outbound SPI	Hexadecimal format	Enter the **Outbound SPI** for this IPSec tunnel. Value Range: 0 - FFFF.
Inbound SPI	Hexadecimal format	Enter the **Inbound SPI** for this IPSec tunnel. Value Range: 0 - FFFF.
Encryption	Mandatory field. Hexadecimal format	Enter the **Encryption Method** and **Encryption key**. Available encryption methods are **DES**, **3DES**, **AES-128**, **AES-192** or **AES-256.** The key length for DES is **16**, 3DES is **48**, AES-128 is **32**, AES-192 is **48**, and AES-256 is **64**. **Note** – When AH option in Encapsulation is selected, encryption will not be available.
Authentication	Mandatory field. Hexadecimal format	Enter the **Authentication Method** and **Authentication key**. Available encryptions are **None**, **MD5**, **SHA1** or **SHA2-256** The key length for MD5 is **32**, SHA1 is **40**, and SHA2-256 is **64**. **Note** – When **AH option** in **Encapsulation Protocol** is selected, **None** option in Authentication will not be available.
Save	Button	Click **Save** to save the settings
Undo	Button	Click **Undo** to cancel the settings
Back	Button	Click **Back** to return to the previous page.

Table 143 – Manual Proposal

6.1.1.11 Create/Edit Dynamic VPN Server List



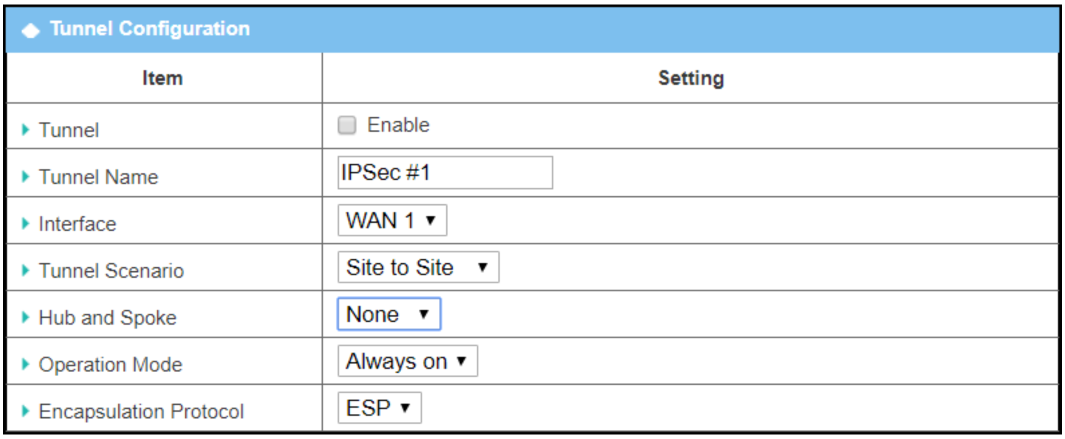
Dynamic VPN List | Add | Delete | Refresh

ID	Tunnel Name	Interface	Connected Client	Enable	Actions

Figure 238 – Dynamic VPN List

Similar to creating an IPSec VPN Tunnel for site/host to site/host scenario, when **Edit** button is applied a series of configuration screen will appear. They are **Tunnel Configuration**, **Local & Remote Configuration**, **Authentication**, **IKE Phase**, **IKE Proposal Definition**, **IPSec Phase**, and **IPSec Proposal Definition**. You have to configure the tunnel details for the router as a Dynamic VPN server.

Note – You can configure one **Dynamic VPN server** for each **WAN** interface.



Tunnel Configuration

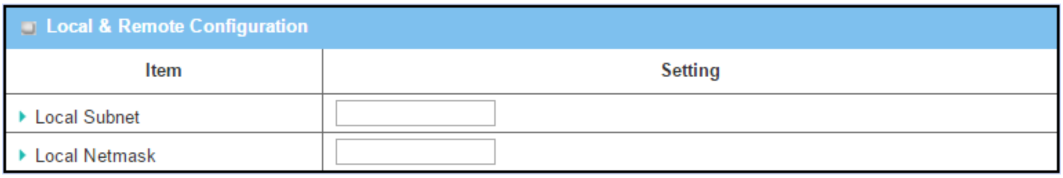
Item	Setting
Tunnel	□ Enable
Tunnel Name	IPSec #1
Interface	WAN 1 ▾
Tunnel Scenario	Site to Site ▾
Hub and Spoke	None ▾
Operation Mode	Always on ▾
Encapsulation Protocol	ESP ▾

Figure 239 – Dynamic VPN Server

Item	Notes	Description
Tunnel	Disabled by default.	Check the ☑ **Enable** box to activate the Dynamic IPSec VPN tunnel.
Tunnel Name	Mandatory field. String format can be any text.	Enter a meaningful tunnel name. Value Range: 1 - 19 characters.
Interface	Mandatory field. Default setting: **WAN 1**	Select the **WAN** interface on which the IPSec tunnel is to be established.
Tunnel Scenario	Mandatory field. Default setting: **Dynamic VPN**	The IPSec tunnelling scenario is fixed to **Dynamic VPN**.
Hub and Spoke	Mandatory field. Default setting: **None**	Select **None**, **Hub** or **Spoke**
Operation Mode	Mandatory field. Default setting: **Always on**	The available operation mode is: **Always On** **Failover** option is not available for the Dynamic IPSec scenario.

Item	Notes	Description
Encapsulation Protocol	Mandatory field. Default setting: **ESP**	Select the Encapsulation Protocol from the dropdown box for this IPSec tunnel. Available encapsulations are ESP and AH.

Table 144 – Dynamic VPN Server



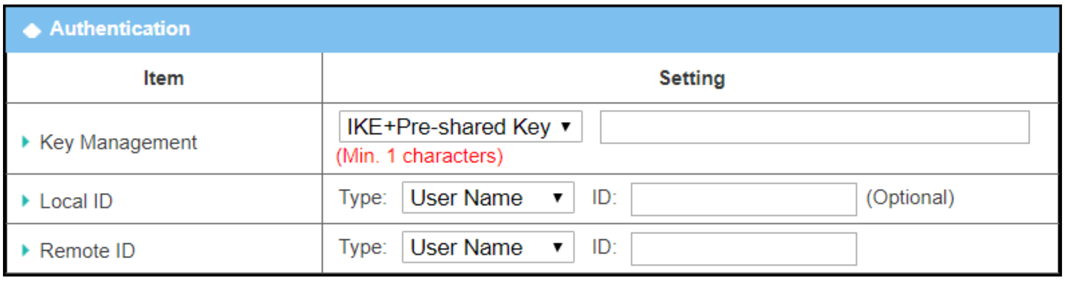
Local & Remote Configuration

Item	Setting
Local Subnet	
Local Netmask	

Figure 240 – Local & Remote Configuration

Item	Notes	Description
Local Subnet	Mandatory field.	Enter the Local Subnet IP address.
Local Netmask	Mandatory field.	Enter the Local Subnet Mask.

Table 145 – Local & Remote Configuration



Authentication

Item	Setting
Key Management	IKE+Pre-shared Key ▾ (Min. 1 characters)
Local ID	Type: User Name ▾ ID: (Optional)
Remote ID	Type: User Name ▾ ID:

Figure 241 – Authentication

Item	Notes	Description
Key Management	Mandatory field. 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 (1 - 32 characters). **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	Optional field.	Specify the Local ID for this IPSec tunnel to authenticate: **User Name** – The username may include letters and numbers, but cannot be all numbers. **FQDN** – Enter the FQDN. **User@FQDN** – Enter the User@FQDN. **Key ID** – The Key ID can be letters and/or numbers.
Remote ID	Optional field.	Specify the Remote ID for this IPSec tunnel to authenticate.

Item	Notes	Description
		User Name – The username may include letters and numbers, but cannot be all numbers. **FQDN** – Enter the FQDN. **User@FQDN** – Enter the User@FQDN. **Key ID** – The Key ID can be letters and/or numbers. **Note** – **Remote ID** will be not available when **Dynamic VPN** option in **Tunnel Scenario** is selected.

Table 146 – Authentication

For the rest (**IKE Phase**, **IKE Proposal Definition**, **IPSec Phase**, and **IPSec Proposal Definition settings**) they are the same as that of creating an IPSec Tunnel described in previous section. Please refer to the related description.

6.1.2 OpenVPN

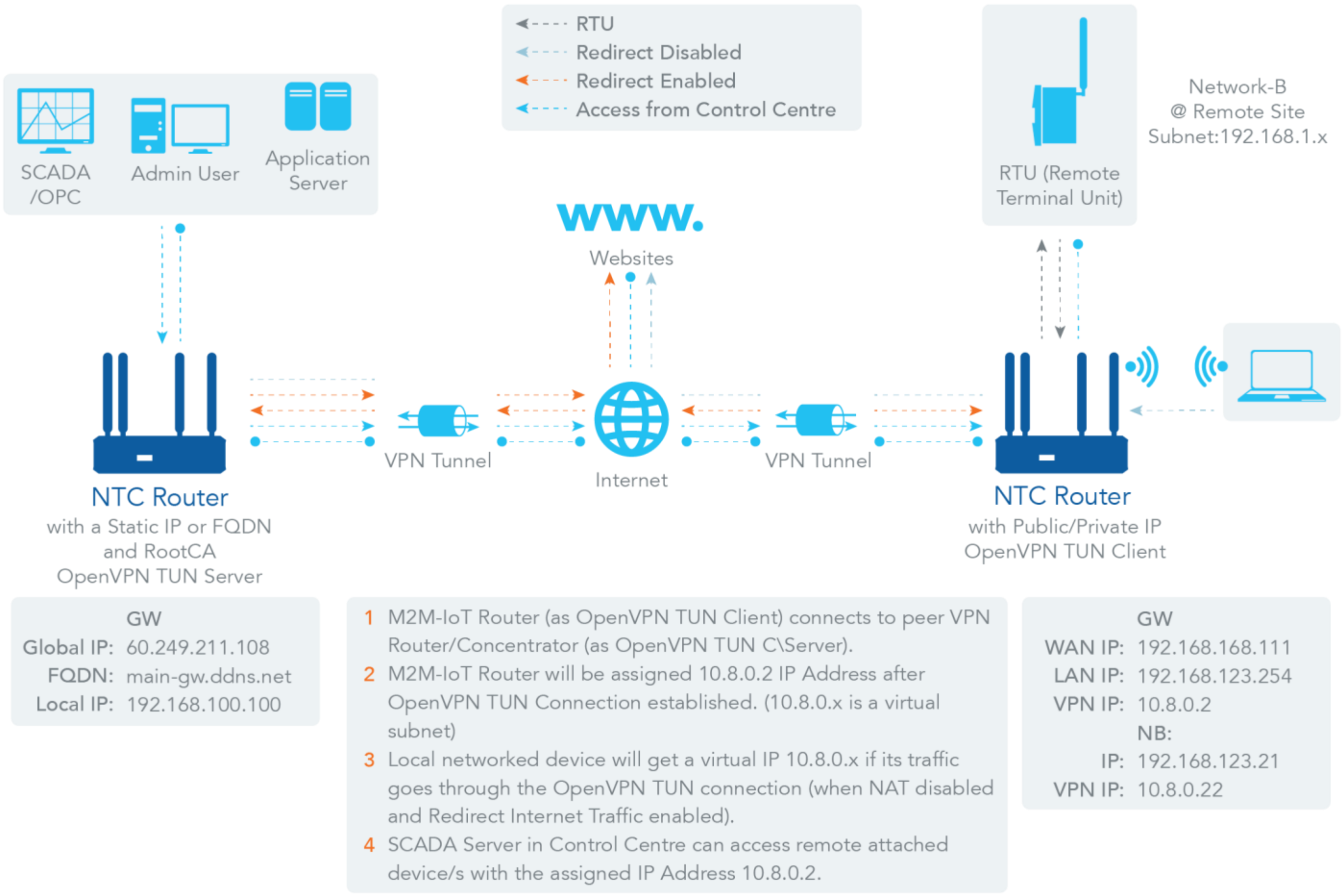
OpenVPN is an application that implements virtual private network (VPN) techniques for creating secure point-to-point or site-to-site connections in routed or bridged configurations and remote access facilities. It uses a custom security protocol that utilizes SSL/TLS for key exchange. It is capable of traversing network address translators (NATs) and firewalls.

OpenVPN 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 extensively, as well as the SSLv3/TLSv1 protocol, 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 public IP or private IP, and requesting the OpenVPN tunnel connection. The product supports both OpenVPN Server and OpenVPN Client features to meet different application requirements.

There are two OpenVPN connection scenarios: TAP and TUN. The router 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. In addition to configuring the device as a Server or Client, you have to specify which type of OpenVPN connection scenario is to be adopted.

6.1.2.1 OpenVPN TUN Scenario


RTU
Redirect Disabled
Redirect Enabled
Access from Control Centre
SCADA /OPC
Admin User
Application Server
RTU (Remote Terminal Unit)
Network-B @ Remote Site Subnet:192.168.1.x
www.
Websites
VPN Tunnel
Internet
VPN Tunnel
NTC Router
with a Static IP or FQDN and RootCA OpenVPN TUN Server
NTC Router
with Public/Private IP OpenVPN TUN Client

GW
Global IP: 60.249.211.108
FQDN: main-gw.ddns.net
Local IP: 192.168.100.100

1 M2M-IoT Router (as OpenVPN TUN Client) connects to peer VPN Router/Concentrator (as OpenVPN TUN C\Server).
2 M2M-IoT Router will be assigned 10.8.0.2 IP Address after OpenVPN TUN Connection established. (10.8.0.x is a virtual subnet)
3 Local networked device will get a virtual IP 10.8.0.x if its traffic goes through the OpenVPN TUN connection (when NAT disabled and Redirect Internet Traffic enabled).
4 SCADA Server in Control Centre can access remote attached device/s with the assigned IP Address 10.8.0.2.

GW
WAN IP: 192.168.168.111
LAN IP: 192.168.123.254
VPN IP: 10.8.0.2
NB:
IP: 192.168.123.21
VPN IP: 10.8.0.22

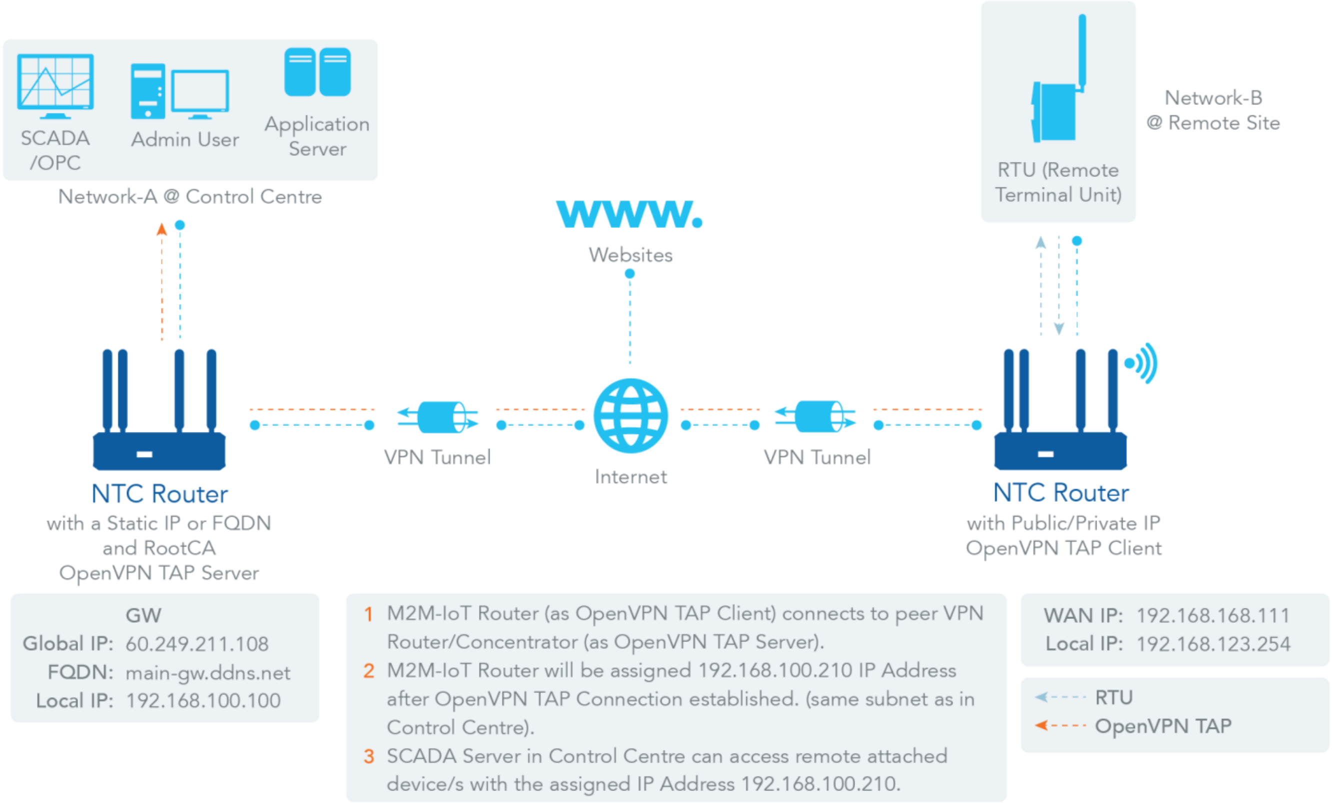
Figure 242 – OpenVPN TUN Scenario

The term "TUN" refers to the routing mode and operates with layer 3 packets. In routing mode, the VPN client is given an IP address on a different subnet than the local LAN under the OpenVPN server. This virtual subnet is created for connecting to remote VPN computers. In routing mode, the OpenVPN 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 OpenVPN resides.

If you want to offer remote access to a VPN server from clients and inhibit the access to remote LAN resources under VPN server, OpenVPN TUN mode is the simplest solution.

As shown in the diagram, the NTC-400 Series Router is configured as an OpenVPN TUN Client and connects to an OpenVPN TUN Server. Once the OpenVPN TUN connection is established, the connected TUN client will be assigned a virtual IP (10.8.0.2) which belongs to a virtual subnet that is different to the local subnet in the Control Centre. With such connection, the local networked devices will get a virtual IP 10.8.0.x if its traffic goes through the OpenVPN TUN connection when Redirect Internet Traffic settings is enabled. The SCADA Server in the Control Centre can access remotely attached serial device(s) with the virtual IP address (10.8.0.2).

6.1.2.2 OpenVPN TAP Scenario


SCADA /OPC
Admin User
Application Server
Network-A @ Control Centre
www.
Websites
RTU (Remote Terminal Unit)
Network-B @ Remote Site
VPN Tunnel
Internet
VPN Tunnel
NTC Router
with a Static IP or FQDN and RootCA OpenVPN TAP Server
NTC Router
with Public/Private IP OpenVPN TAP Client
RTU
OpenVPN TAP

GW
Global IP: 60.249.211.108
FQDN: main-gw.ddns.net
Local IP: 192.168.100.100

1 M2M-IoT Router (as OpenVPN TAP Client) connects to peer VPN Router/Concentrator (as OpenVPN TAP Server).
2 M2M-IoT Router will be assigned 192.168.100.210 IP Address after OpenVPN TAP Connection established. (same subnet as in Control Centre).
3 SCADA Server in Control Centre can access remote attached device/s with the assigned IP Address 192.168.100.210.

WAN IP: 192.168.168.111
Local IP: 192.168.123.254

Figure 243 – OpenVPN TAP 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 resided under the OpenVPN server. 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 NTC-400 Series Router is configured as an OpenVPN 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 (192.168.100.210) which is the same subnet as that of local subnet in the Control Centre. With such connection, the SCADA Server in Control Centre can access remotely attached serial device(s) with the virtual IP address (192.168.100.210).

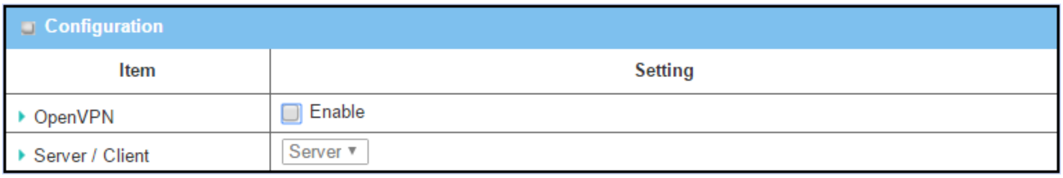
6.1.2.3 Enable OpenVPN

The OpenVPN setting allows user to create and configure OpenVPN tunnels.

To enable the OpenVPN functionality:

1 From the **Security** submenu select **VPN** and click its **Open VPN** tab.

2 Go to the **Configuration** section:



Configuration

Item	Setting
OpenVPN	□ Enable
Server / Client	Server ▾

Figure 244 – Open VPN Configuration

3 Click ☑ **Enable** OpenVPN and select a configuration type, either **Server** or **Client**, for the router to operate as.

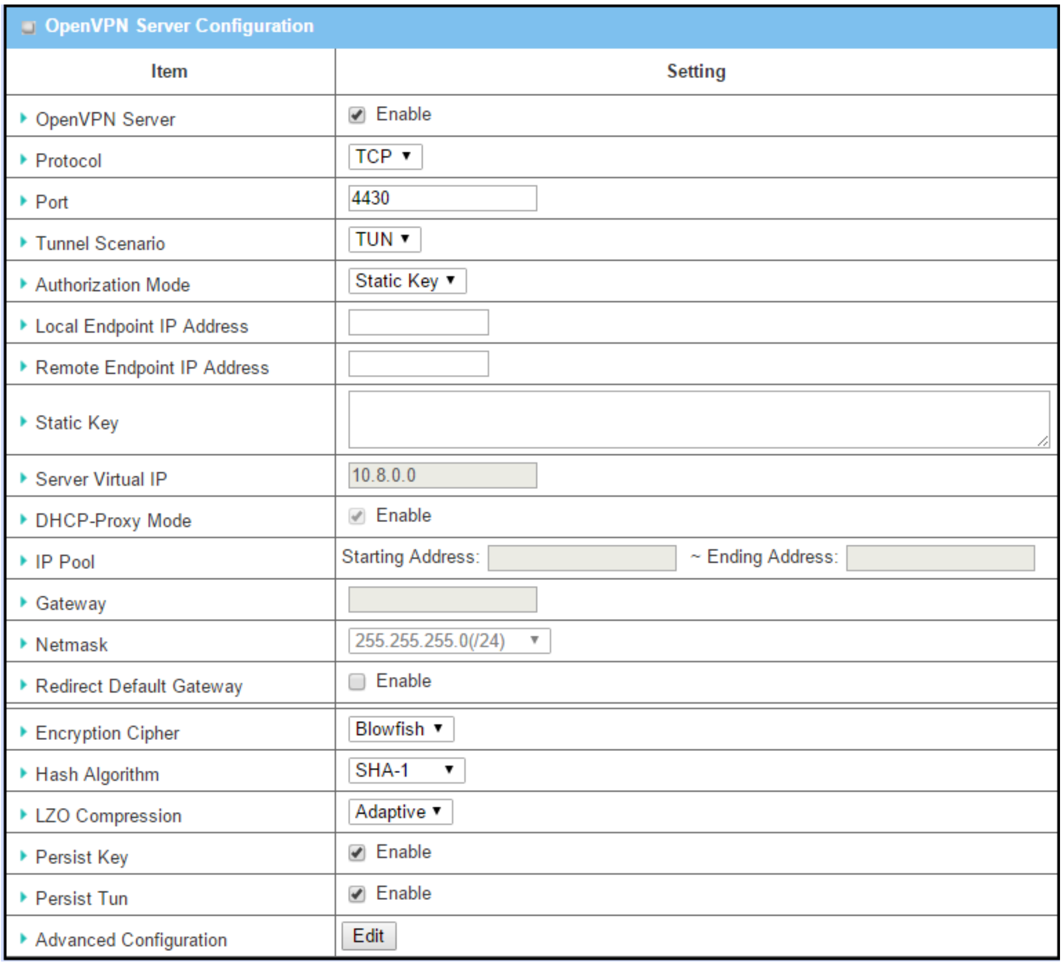
Item	Notes	Description
OpenVPN	Disabled by default.	Check ☑ **Enable** to activate the OpenVPN function.
Server/ Clients	Server is the default selection.	When Server is selected the server configuration fields are displayed in the **OpenVPN Server Configuration** section. When Client is selected, you can specify the client settings in another client configuration window.

Table 147 – Open VPN Configuration

6.1.2.4 OpenVPN Server

If **Server** is selected, the **OpenVPN Server Configuration** section displays fields required to configure the OpenVPN server function including: the virtual IP address of OpenVPN server, when remote OpenVPN clients can dial in, the authentication protocol, etc.

The OpenVPN Server supports up to 4 TUN/TAP tunnels at the same time.



OpenVPN Server Configuration

Item	Setting
OpenVPN Server	☑ Enable
Protocol	TCP ▾
Port	4430
Tunnel Scenario	TUN ▾
Authorization Mode	Static Key ▾
Local Endpoint IP Address	
Remote Endpoint IP Address	
Static Key	
Server Virtual IP	10.8.0.0
DHCP-Proxy Mode	☑ Enable
IP Pool	Starting Address: ~ Ending Address:
Gateway	
Netmask	255.255.255.0(/24) ▾
Redirect Default Gateway	□ Enable
Encryption Cipher	Blowfish ▾
Hash Algorithm	SHA-1 ▾
LZO Compression	Adaptive ▾
Persist Key	☑ Enable
Persist Tun	☑ Enable
Advanced Configuration	Edit

Figure 245 – OpenVPN Server Configuration

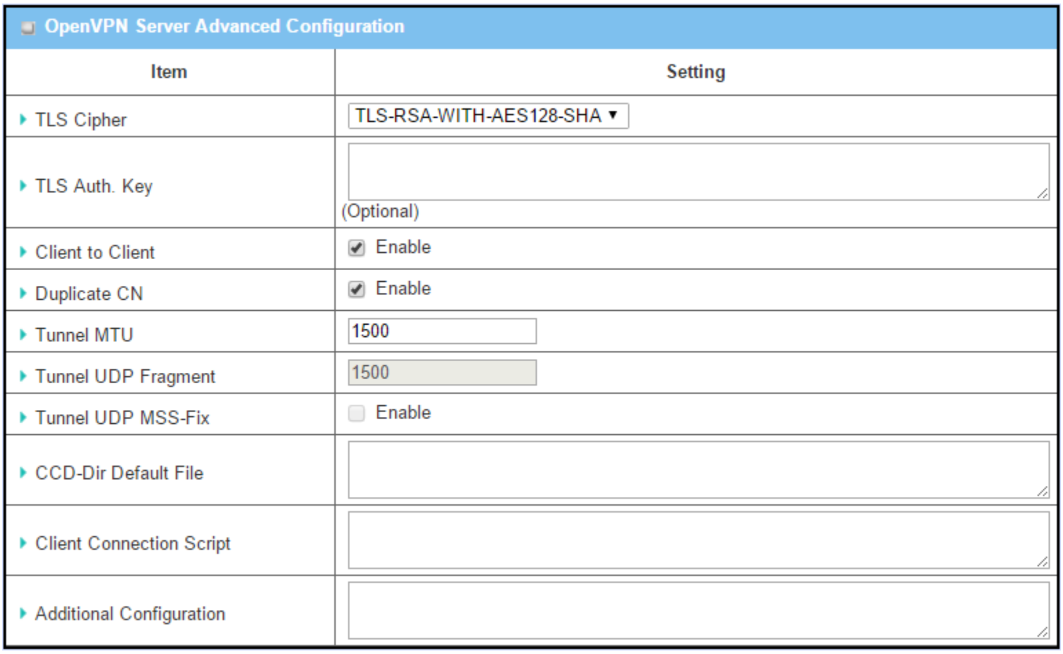
Item	Notes	Description
OpenVPN Server	Disabled by default.	Click ☑ **Enable** to activate OpenVPN Server functions.
Protocol	Mandatory field. Default setting: **TCP**	Select the Protocol for connecting to the OpenVPN Server: **TCP** or **UDP** **TCP** – The TCP protocol will be used to access the OpenVPN Server, and Port will be automatically set at 4430. **UDP** – The UDP protocol will be used to access the OpenVPN Server, and Port will be automatically set at 1194.
Port	Mandatory field. Default setting: **4430**	Specify the Port for connecting to the OpenVPN Server. Value Range: 1 - 65535.
Tunnel Scenario	Mandatory field. Default setting: **TUN**	Specify the type of Tunnel Scenario for connecting to the OpenVPN Server. It can be TUN for TUN tunnel scenario, or TAP for TAP tunnel scenario.
Authorization Mode	Mandatory field. Default setting: **Static Key**	Select the authorization mode for the OpenVPN Server: **TLS** or **Static Key** **TLS –** OpenVPN will use TLS authorization mode, and the following items **CA Cert.**, **Server Cert.** and **DH PEM** will be displayed. The **CA Cert**. can be generated in **Object Definition > Certificate > Trusted Certificate**. The **Server Cert.** can be generated in **Object Definition > Certificate > My Certificate**. **Static Key** – The OpenVPN will use static key (pre-shared) authorization mode, and the following parameters are displayed: **Local Endpoint IP Address**, **Remote Endpoint IP Address** and **Static Key** **Note – Static Key** will be available only when **TUN** is chosen in Tunnel Scenario.
Local Endpoint IP Address	Mandatory field.	Specify the virtual Local Endpoint IP Address of this OpenVPN router. 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	Mandatory field.	Specify the virtual Remote Endpoint IP Address of the peer OpenVPN router. 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	Mandatory field.	Specify the Static Key. **Note –** Static Key will be available only when Static Key is chosen in Authorization Mode.
Server Virtual IP	Mandatory field.	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 Authorization Mode.

Item	Notes	Description
DHCP-Proxy Mode	Mandatory field. Enabled by default.	Check ☑ **Enable** to activate the DHCP-Proxy Mode. **Note –** DHCP-Proxy Mode will be available only when TAP is chosen in Tunnel Device.
IP Pool	Mandatory field.	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, and DHCP-Proxy Mode is unchecked (disabled).
Gateway	Mandatory field.	Specify the gateway setting for the OpenVPN server. It will be assigned to the connected OpenVPN clients. **Note –** The gateway will be available only when TAP is chosen in the Tunnel Device, and DHCP-Proxy Mode is unchecked (disabled).
Netmask	Default setting: **- select one -**	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, and DHCP-Proxy Mode is unchecked (disabled). **Note 2 –** Netmask will also be available when TUN is chosen in Tunnel Device.
Redirect Default Router	Optional setting. Disabled by default.	Check ☑ **Enable** to activate the Redirect Default Router function.
Encryption Cipher	Mandatory field. Default setting: **Blowfish**	Specify the Encryption Cipher from the dropdown list. Available cipher types: **Blowfish**, **AES-256**, **AES-192**, **AES-128** or **None**
Hash Algorithm	Default setting: **SHA-1**	Specify the Hash Algorithm from the dropdown list. Available algorithm types: **SHA-1**, **MD5**, **MD4**, **SHA2-256**, **SHA2-512**, **None** or **Disable**
LZO Compression	Default setting: **Adaptive**	Specify the LZO Compression scheme. Available schemes: **Adaptive**, **YES**, **NO** or **Default**
Persis Key	Optional setting. Enabled by default.	Check ☑ Enable to activate the Persis Key function.
Persis TUN	Optional setting.	Check ☑ Enable to activate the Persis TUN function.
Advanced Configuration	Button	Click the **Edit** button to open the **Advanced Configuration** screen where you can enter advanced settings for the OpenVPN server. See next section below.
Save	Button	Click **Save** to save the settings.
Undo	Button	Click **Undo** to cancel the changes.

Table 148 – OpenVPN Server Configuration

6.1.2.5 Advanced Configuration

When **Advanced Configuration** is selected, the **OpenVPN Server Advanced Configuration** screen will appear:



OpenVPN Server Advanced Configuration

Item	Setting
TLS Cipher	TLS-RSA-WITH-AES128-SHA ▾
TLS Auth. Key	(Optional)
Client to Client	☑ Enable
Duplicate CN	☑ Enable
Tunnel MTU	1500
Tunnel UDP Fragment	1500
Tunnel UDP MSS-Fix	☐ Enable
CCD-Dir Default File	
Client Connection Script	
Additional Configuration	

Figure 246 – OpenVPN Server Advanced Configuration

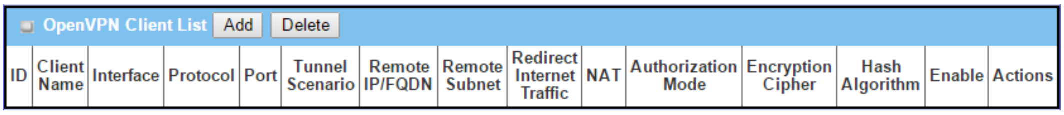
Item	Notes	Description
TLS Cipher	Mandatory field. Default setting: **TLS-RSA-WITH-AES128-SHA**	Specify the TLS Cipher from the drop-down list. It can be: **None**, **TLS-RSA-WITH-RC4-MD5**, **TLS-RSA-WITH-AES128-SHA**, **TLS-RSA-WITH-AES256-SHA**, **TLS-DHE-DSS-AES128-SHA** or **TLS-DHE-DSS-AES256-SHA** **Note** – TLS Cipher will be available only when TLS is chosen in Authorization Mode.
TLS Auth. Key	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	Enabled by default.	Note – Client to Client will be available only when TLS is chosen in Authorization Mode
Duplicate CN	Enabled by default.	**Note** – Duplicate CN will be available only when TLS is chosen in Authorization Mode.
Tunnel MTU	Mandatory field. Default value: **1500**	Specify the Tunnel MTU. Value Range: 0 - 1500
Tunnel UDP Fragment	Mandatory field. Default value: **1500**	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.

Item	Notes	Description
Tunnel UDP MSS-Fix	Optional setting. Disabled 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	Optional setting. String format: any text	Specify the CCD-Dir Default File. Value Range: 0 - 256 characters.
Client Connection Script	Optional setting. String format: any text	Specify the Client Connection Script. Value Range: 0 - 256 characters.
Additional Configuration	Optional setting. String format: any text	Specify the Additional Configuration. Value Range: 0 - 256 characters.

Table 149 – OpenVPN Server Advanced Configuration

6.1.2.6 OpenVPN Client

If **Client** is selected in the OpenVPN **Configuration** section, the **OpenVPN Client List** screen appears.

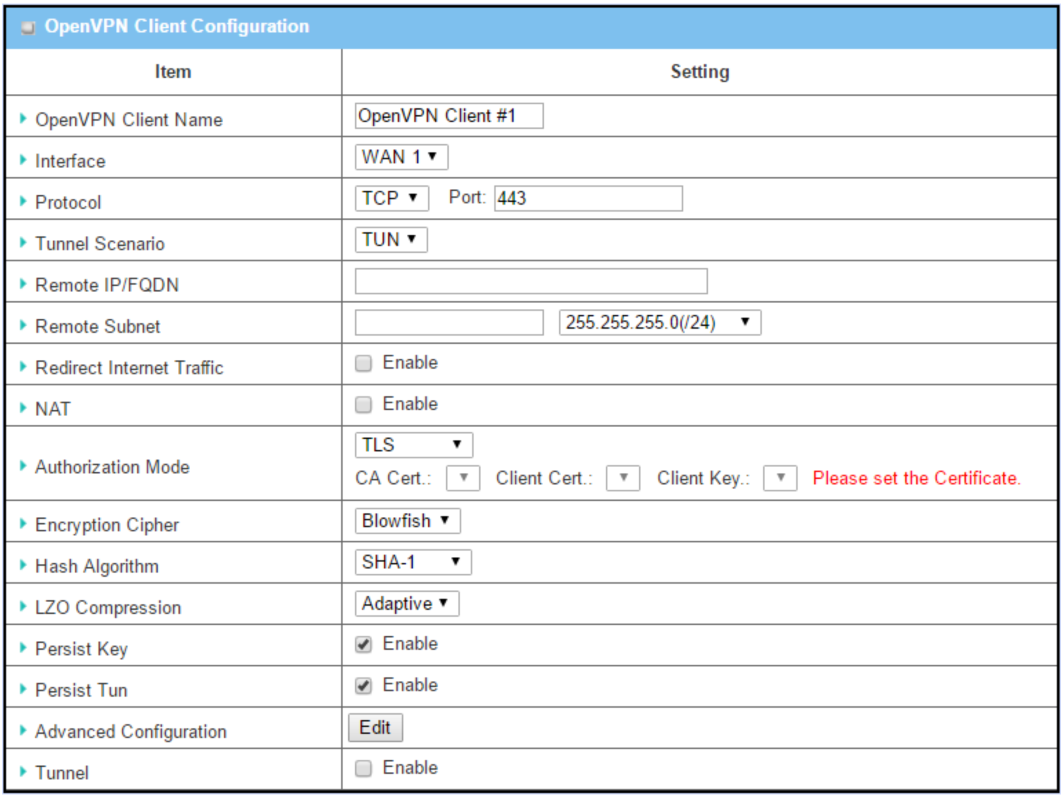


OpenVPN Client List Add Delete

ID	Client Name	Interface	Protocol	Port	Tunnel Scenario	Remote IP/FQDN	Remote Subnet	Redirect Internet Traffic	NAT	Authorization Mode	Encryption Cipher	Hash Algorithm	Enable	Actions

Figure 247 – OpenVPN Client List

Click the **Add** to open the **OpenVPN Client Configuration** screen where you enter the parameters for the new OpenVPN VPN client.



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

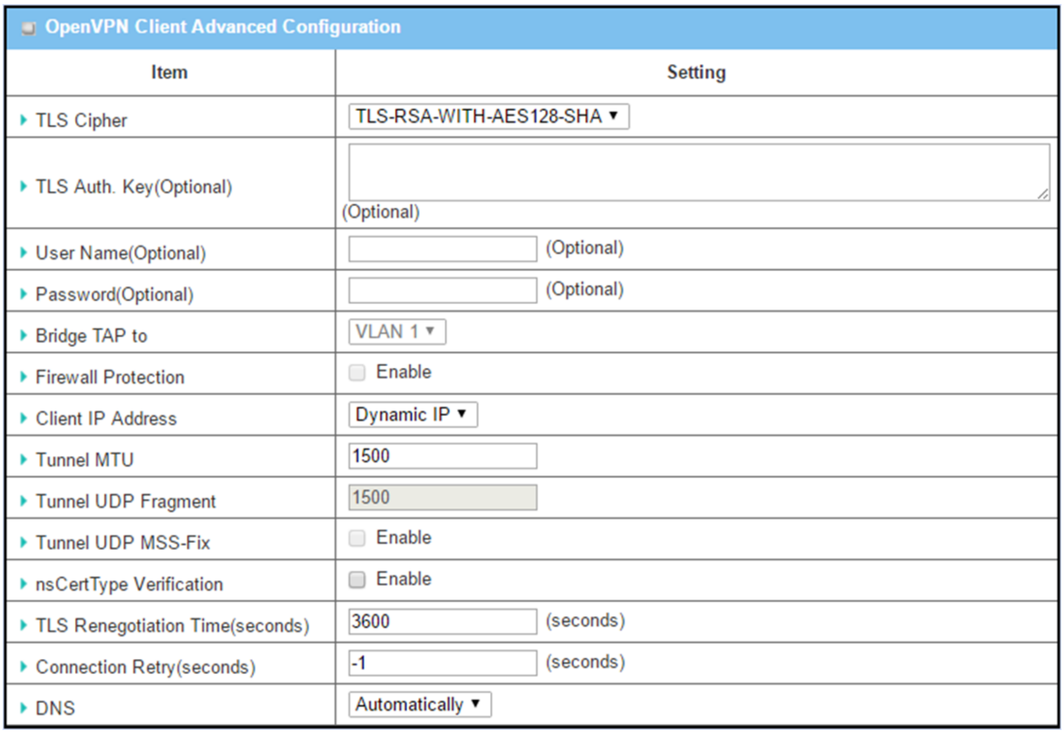
Figure 248 – OpenVPN Client Configuration

Item	Notes	Description
OpenVPN Client Name	Mandatory field.	The OpenVPN Client Name will be used to identify the client in the tunnel list. Value Range: 1 - 32 characters.
Interface	Mandatory field. Default setting: **WAN-1**	Define the physical interface to be used for this OpenVPN Client tunnel.
Protocol	Mandatory field. Default setting: **TCP**	Select the Protocol for connecting to the OpenVPN Client: **TCP** or **UDP** **TCP** – The TCP protocol will be used to access the OpenVPN Client, and Port will be automatically set at 4430. **UDP** – The UDP protocol will be used to access the OpenVPN Client, and Port will be automatically set at 1194.
Port	Mandatory field. Default setting: **443**	Specify the Port for the OpenVPN Client to use. Value Range: 1 - 65535.
Tunnel Scenario	Mandatory field. Default setting: **TUN**	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 field.	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 field.	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	Optional setting. Disabled by default.	Check ☑ Enable to activate the Redirect Internet Traffic function.
NAT	Optional setting. Disabled by default.	Check ☑ Enable to activate the NAT function.
Authorization Mode	Mandatory field. Default setting: **TLS**	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

Item	Notes	Description
		Local Endpoint IP Address, Remote Endpoint IP Address and Static Key will be displayed.
Local Endpoint IP Address	Mandatory field.	Specify the virtual Local Endpoint IP Address of this OpenVPN router. 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	Mandatory field.	Specify the virtual Remote Endpoint IP Address of the peer OpenVPN router. 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	Mandatory field.	Specify the Static Key. **Note** – **Static Key** will be available only when **Static Key** is chosen in **Authorization Mode**.
Encryption Cipher	Default setting: **Blowfish**	Specify the Encryption Cipher. It can be Blowfish/AES-256/AES-192/AES-128/None.
Hash Algorithm	Default setting: **SHA-1**	Specify the Hash Algorithm. Available settings: **SHA-1**, **MD5**, **MD4**, **SHA2-256**, **SHA2-512**, **None** or **Disable**
LZO Compression	Default setting: **Adaptive**	Specify the LZO Compression scheme. Available settings: **Adaptive**, **YES**, **NO** or **Default**
Persis Key	Optional setting. Enabled by default.	Check ☑ **Enable** to activate the Persis Key function.
Persis Tun	Optional setting. Enabled by default.	Check ☑ **Enable** to activate the Persis TUN function.
Advanced Configuration	Button	Click the **Edit** button to specify the Advanced Configuration setting for the OpenVPN serve in the Advanced Configuration section.
Tunnel	Disabled by default.	Check ☑ **Enable** to activate this OpenVPN tunnel.
Save	Button	Click **Save** to save the settings.
Undo	Button	Click **Undo** to cancel the changes.
Back	Button	Click **Back** to return to last page.

Table 150 – OpenVPN Client Configuration

When **Advanced Configuration** is selected, the **OpenVPN Client Advanced Configuration** section is displayed.



OpenVPN Client Advanced Configuration

Item	Setting
TLS Cipher	TLS-RSA-WITH-AES128-SHA ▾
TLS Auth. Key(Optional)	(Optional)
User Name(Optional)	(Optional)
Password(Optional)	(Optional)
Bridge TAP to	VLAN 1 ▾
Firewall Protection	□ Enable
Client IP Address	Dynamic IP ▾
Tunnel MTU	1500
Tunnel UDP Fragment	1500
Tunnel UDP MSS-Fix	□ Enable
nsCertType Verification	□ Enable
TLS Renegotiation Time(seconds)	3600 (seconds)
Connection Retry(seconds)	-1 (seconds)
DNS	Automatically ▾

Figure 249 – OpenVPN Client Advanced Configuration

Item	Notes	Description
TLS Cipher	Mandatory field. The default setting is: TLS-RSA-WITH-AES128-SHA	Specify the TLS Cipher from the dropdown list. It can be None / TLS-RSA-WITH-RC4-MD5 / TLS-RSA-WITH-AES128-SHA / TLS- RSA-WITH-AES256-SHA / TLS-DHE-DSS-AES128-SHA / TLS-DHE-DSS-AES256- SHA. **Note** – TLS Cipher will be available only when TLS is chosen in Authorization Mode.
TLS Auth. Key	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	Optional field.	Enter the User account for connecting to an OpenVPN server, if the server required it. **Note** – User Name will be available only when TLS is chosen in Authorization Mode.
Password	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 Authorization Mode.
Bridge TAP to	The default setting is: VLAN 1	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.

Item	Notes	Description
Firewall Protection	Disabled by default.	Check ☑ **Enable** to activate the Firewall Protection function. Note – Firewall Protection will be available only when NAT is enabled.
Client IP Address	The default setting is: Dynamic IP	Specify the virtual IP Address for the OpenVPN Client as: Dynamic IP or Static IP
Tunnel MTU	Mandatory field. The default value is: 1500	Specify the value of Tunnel MTU. Value Range: 0 - 1500.
Tunnel UDP Fragment	The default value is: 1500	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	Disabled by default.	Check ☑ **Enable** 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	Disabled by default.	Check ☑ **Enable** 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 default value is: 3600	Specify the time interval of TLS Renegotiation Time. Value Range: -1 - 86400.
Connection Retry (seconds)	The default value is: -1	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	The default setting is: Automatically	Specify the setting of DNS: **Automatically** or **Manually**

Table 151 – OpenVPN Client Advanced Configuration

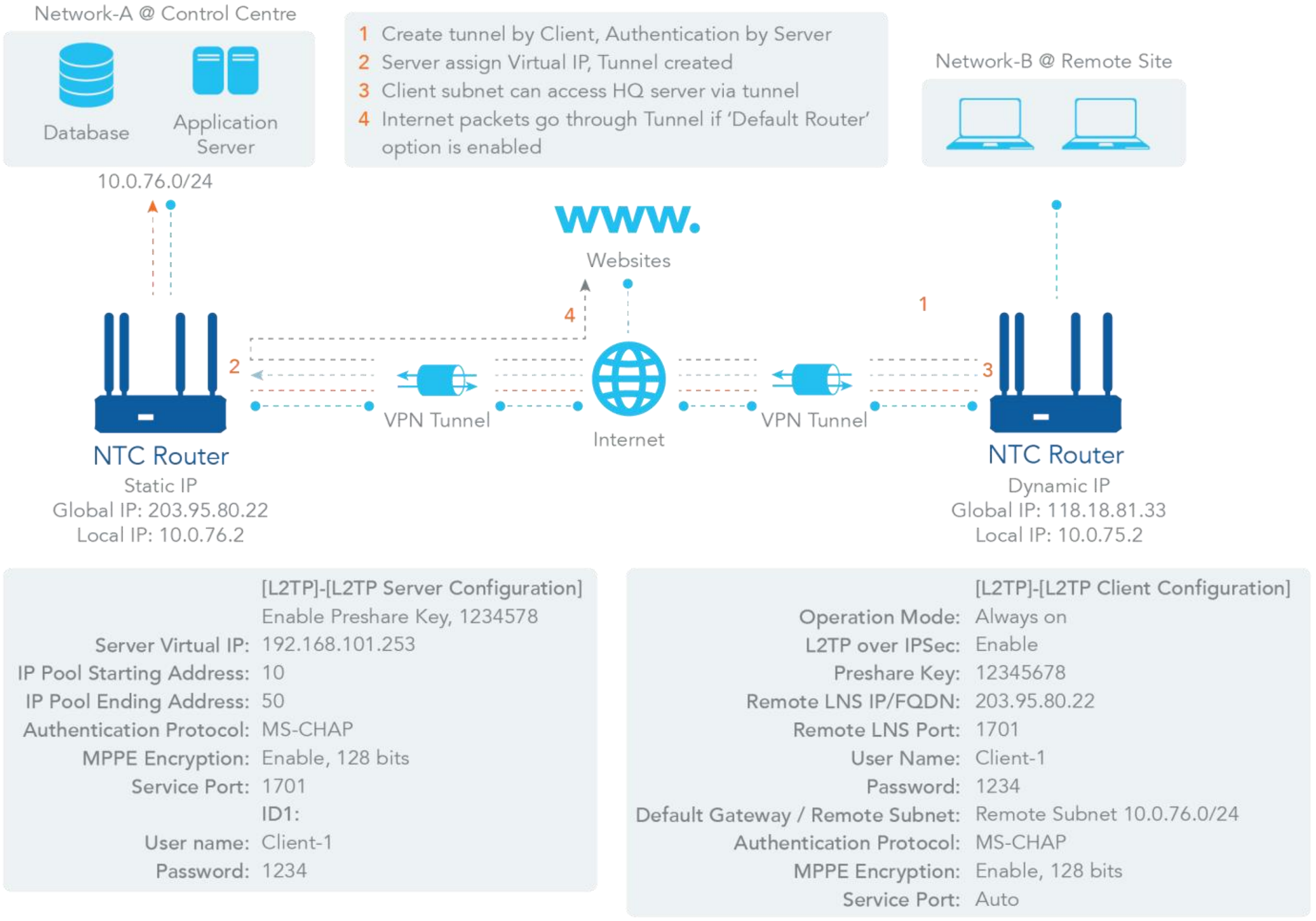
6.1.3 L2TP

Layer 2 Tunnelling Protocol (L2TP) is a tunnelling protocol used to support virtual private networks (VPNs) or as part of the delivery of services by ISPs. It does not provide any encryption or confidentiality by itself. Rather, it relies on an encryption protocol that it passes within the tunnel to provide privacy.

This router can behave as a L2TP server and a L2TP client both at the same time.

L2TP Server - You must have a static IP or an FQDN for clients to create L2TP tunnels. It also maintains “User Account list” (user name/ password) for client login authentication. There is a virtual IP pool to assign virtual IP to each connected L2TP client.

L2TP Client - Clients may be mobile users or routers in remote offices with dynamic IP addresses. To setup a tunnel, the client should have the “user name” and “password” and global IP address of the server. In addition, you must identify the operation mode for each tunnel as the main connection or failover for another tunnel to increase overall bandwidth. It needs to decide the “Default Router” or “Remote Subnet” for packet flow. You can also define what kind of traffic will pass through the L2TP tunnel in the “Default Router / Remote Subnet” parameter.


Network-A @ Control Centre
Database
Application Server
10.0.76.0/24
1 Create tunnel by Client, Authentication by Server
2 Server assign Virtual IP, Tunnel created
3 Client subnet can access HQ server via tunnel
4 Internet packets go through Tunnel if ‘Default Router’ option is enabled
Network-B @ Remote Site
www.
Websites
4
2
1
3
VPN Tunnel
Internet
VPN Tunnel
NTC Router
Static IP
Global IP: 203.95.80.22
Local IP: 10.0.76.2
NTC Router
Dynamic IP
Global IP: 118.18.81.33
Local IP: 10.0.75.2

[L2TP]-[L2TP Server Configuration]

	Enable Preshare Key, 1234578
Server Virtual IP:	192.168.101.253
IP Pool Starting Address:	10
IP Pool Ending Address:	50
Authentication Protocol:	MS-CHAP
MPPE Encryption:	Enable, 128 bits
Service Port:	1701
	ID1:
User name:	Client-1
Password:	1234

[L2TP]-[L2TP Client Configuration]

Operation Mode:	Always on
L2TP over IPSec:	Enable
Preshare Key:	12345678
Remote LNS IP/FQDN:	203.95.80.22
Remote LNS Port:	1701
User Name:	Client-1
Password:	1234
Default Gateway / Remote Subnet:	Remote Subnet 10.0.76.0/24
Authentication Protocol:	MS-CHAP
MPPE Encryption:	Enable, 128 bits
Service Port:	Auto

Figure 250 – L2TP

There are two options, "Default Gateway" and "Remote Subnet" for the "Default Gateway / Remote Subnet" configuration item. When you choose "Remote Subnet", you need to specify one more setting: the remote subnet. This is for the Intranet of the L2TP VPN server. At the L2TP client peer, the packets whose destination is in the dedicated subnet will be transferred via the L2TP VPN tunnel. Others will be transferred based on the current routing policy of the security gateway at the L2TP client peer. If you choose the "Default Gateway" option for the L2TP client peer, all packets will go through the established L2TP VPN tunnel. That means the remote L2TP VPN server controls the flowing of any packets from the L2TP client peer.

6.1.3.1 L2TP tunnel.

For the L2TP client peer, a Remote Subnet item is required. This is for the Intranet of the L2TP server peer. At the L2TP client peer, the packets whose destination is in the dedicated subnet will be transferred via the L2TP tunnel. Others will be transferred based on the current routing policy of the router at L2TP client peer. If you entered 0.0.0.0/0 in the Remote Subnet field, it will be treated as a "Default Router" setting for the L2TP client peer. All packets will go through the established L2TP tunnel. That means the remote L2TP server peer controls the flow of any packets from the L2TP client peer.

6.1.3.2 L2TP Setting

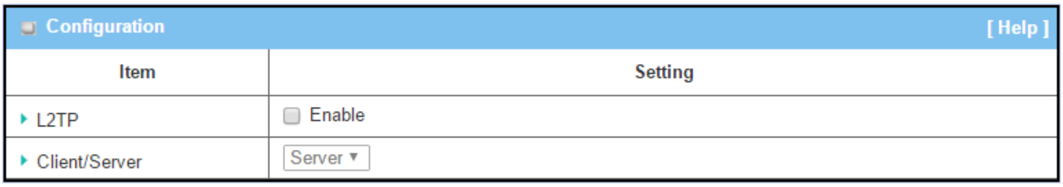
The L2TP setting allows user to create and configure L2TP tunnels.

6.1.3.3 Enable L2TP

To enable the Layer 2 Tunnelling Protocol functionality:

1 Select **VPN** from the **Security** submenu and click the **L2TP** tab.

2 Go to the **Configuration** section:



Configuration [Help]

Item	Setting
L2TP	□ Enable
Client/Server	Server ▾

Figure 251 – Enable L2TP VPN Security

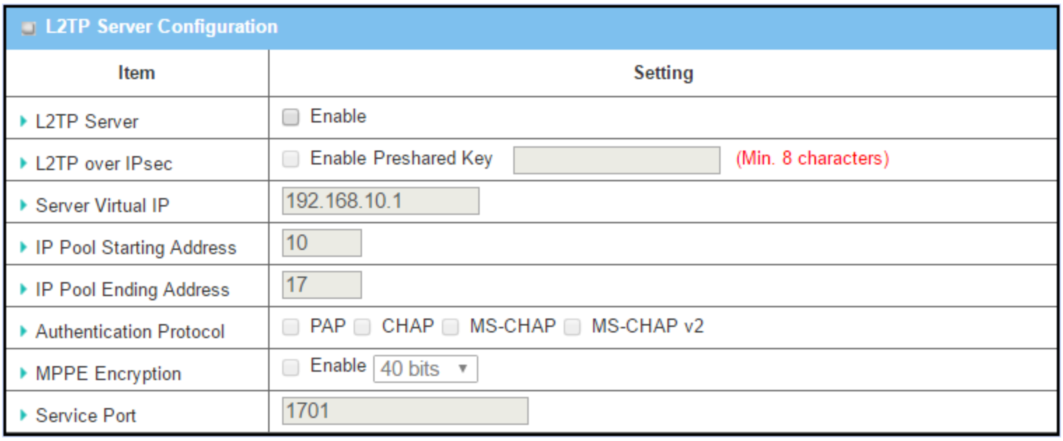
3 Click ☑ **Enable** L2TP and select a configuration type, either **Server** or **Client**, for the router to operate as.

Item	Notes	Description
L2TP	Disabled by default.	Check ☑ Enable to activate the L2TP functionality.
Server/ Clients	Default selection: **Server**	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.

Table 152 – Enable L2TP VPN Security

6.1.3.4 L2TP Server

When **Server** is selected in the **Configuration** section the **L2TP Server Configuration** screen will appear. Configure the router to act as a L2TP server here.



L2TP Server Configuration

Item	Setting
L2TP Server	□ Enable
L2TP over IPsec	□ Enable Preshared Key (Min. 8 characters)
Server Virtual IP	192.168.10.1
IP Pool Starting Address	10
IP Pool Ending Address	17
Authentication Protocol	□ PAP □ CHAP □ MS-CHAP □ MS-CHAP v2
MPPE Encryption	□ Enable 40 bits ▾
Service Port	1701

Figure 252 – L2TP Server Configuration

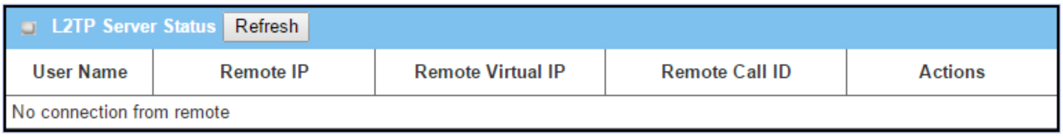
Item	Notes	Description
L2TP Server	Disabled by default.	Click ☑ Enable to activate L2TP Server functions.
L2TP over IPSec	Disabled by default.	Click ☑ Enable Preshared Key to enable L2TP over IPSec functionality.

Item	Notes	Description
		This will require a preshared key to be entered. 8 (min) - 32 (max) characters
Server Virtual IP	Mandatory field.	Enter the L2TP server Virtual IP Address to set this L2TP server as the local virtual IP.
IP Pool Starting Address	Mandatory field. Default setting: 10	Enter the L2TP server starting IP of the virtual IP pool. This sets the starting IP which is assigned to L2TP clients. Value Range: 1 - 254
IP Pool Ending Address	Mandatory field. Default setting: 17	Enter the L2TP server ending IP of the virtual IP pool. This sets the ending IP which is assigned to L2TP clients. Value Range: >= Starting Address, and < (Starting Address + 8) or 254
Authentication Protocol	Mandatory field.	Select single or multiple Authentication Protocols for the L2TP server with which to authenticate L2TP clients. Available authentication protocols include: **PAP**, **CHAP**, **MS-CHAP** or **MS-CHAP v2**
MPPE Encryption	Mandatory field.	Specify whether to support MPPE Protocol. Check ☑ **Enable** to enable MPPE and from dropdown box select: **40 bits**, **56 bits** or **128 bits** **Note** – when **MPPE Encryption** is enabled, the **Authentication Protocol PAP / CHAP** options will not be available.
Service Port	Mandatory field.	Specify the Service Port which L2TP server use. Value Range: 1 - 65535
Save	Button	Click **Save** to save the settings.
Undo	Button	Click **Undo** to cancel the changes.

Table 153 – L2TP Server Configuration

6.1.3.5 L2TP Server Status list

After the L2TP server has been set up L2TP clients connected to it will be listed in the **L2TP Server Status** list:



L2TP Server Status Refresh

User Name	Remote IP	Remote Virtual IP	Remote Call ID	Actions
No connection from remote				

Figure 253 – L2TP Server Status list

The following details of each connected L2TP client are listed: **User Name**, **Remote IP**, **Remote Virtual IP**, **Remote Call ID** and current **Actions**

Click the **Refresh** button to renew the L2TP client information.

6.1.3.6 L2TP User Accounts

The **User Account List** contains details of L2TP user accounts that are able to establish remote L2TP VPN connections to the router. Up to ten (10) User Accounts can be created.

Click **Add** button to add user account in the **User Account Configuration** screen:

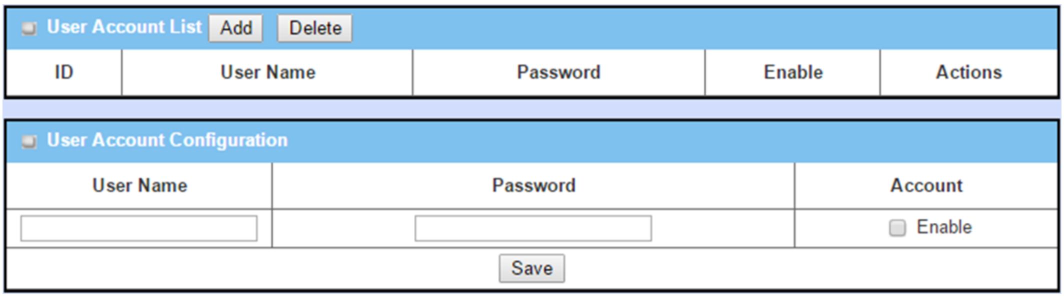


Figure 254 – User Account Configuration

Item	Notes	Description
Add	Button	Click the **Add** button in the User Account List to open the User Account Configuration screen where you can create new user accounts. Up to ten (10) User Accounts can be created.
User Name	Mandatory field. 1 - 32 characters	Enter a user name for the user account.
Password	Mandatory field. 1 - 32 characters	Enter a secure password.
Account	Checkbox	Click ☑ **Enable** to activate the user account.
Delete	Button	Click ☑ Select for the User Account that you want to permanently delete and then click the Delete button.
Edit	Button	Click the **Edi**t button to change the User Name or Password of an existing user account. Note that you can uncheck ☐ **Enable** rather than permanently Delete, this will allow you to retain the user details while disabling its access to the L2TP server.
Save	Button	Click **Save** to create the user account.

Table 154 – User Account Configuration

6.1.3.7 L2TP as a Client

When **Client** is selected in the **Configuration** section the **L2TP Client Configuration** screen will appear. Create clients for the L2TP server here.

6.1.3.8 Enable L2TP

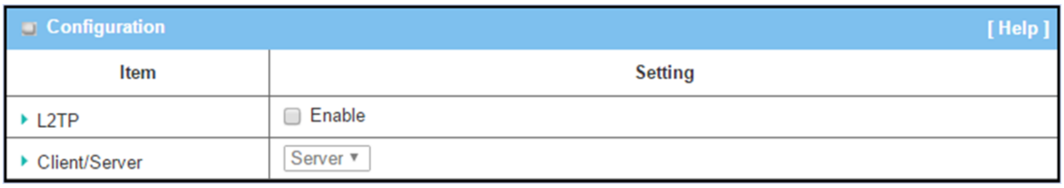


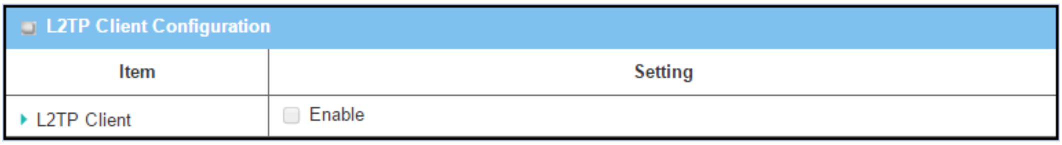
Figure 255 – L2TP Client Configuration

Item	Notes	Description
L2TP	Checkbox	Click ☑ **Enable** to activate the L2TG functionality
Client Server	Drop-down list	Select **Client** from the drop-down list to create an L2TP Client.

Item	Notes	Description
Save	Button	Click **Save** to create the user account.

Table 155 – L2TP Client Configuration

When Client is selected the **L2TP Client Configuration** and the **L2TP Client List & Status** sections display below the **Configuration** window.



L2TP Client Configuration

Item	Setting
L2TP Client	□ Enable

Figure 256 – L2TP Client List & Status

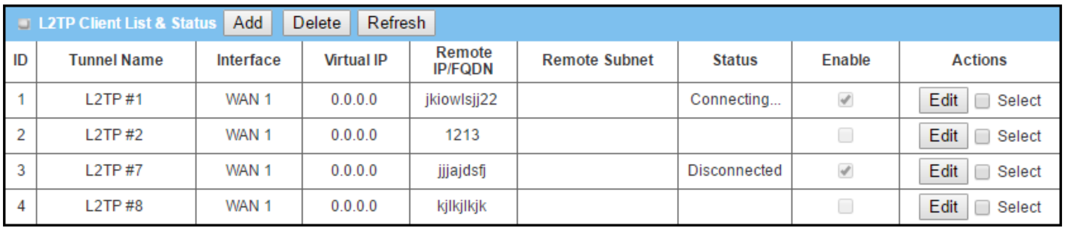
Item	Notes	Description
L2TP Client	Checkbox	Click ☑ **Enable** to activate the L2TG client functionality
Save	Button	Click **Save** to create the user account.

Table 156 – L2TP Client List & Status

When **L2TP** Client is enabled the **Add**, **Delete** and **Refresh** buttons on the **L2TP Client List & Status** become active.

6.1.3.9 Create/Edit L2TP Client

Click on the **Add** button to create a new client in the list. You can create up to eight L2TP clients.



ID	Tunnel Name	Interface	Virtual IP	Remote IP/FQDN	Remote Subnet	Status	Enable	Actions
1	L2TP #1	WAN 1	0.0.0.0	jkiowlsjj22		Connecting...	☑	Edit □ Select
2	L2TP #2	WAN 1	0.0.0.0	1213			□	Edit □ Select
3	L2TP #7	WAN 1	0.0.0.0	jjjajdsfj		Disconnected	☑	Edit □ Select
4	L2TP #8	WAN 1	0.0.0.0	kjlkjlkjk			□	Edit □ Select

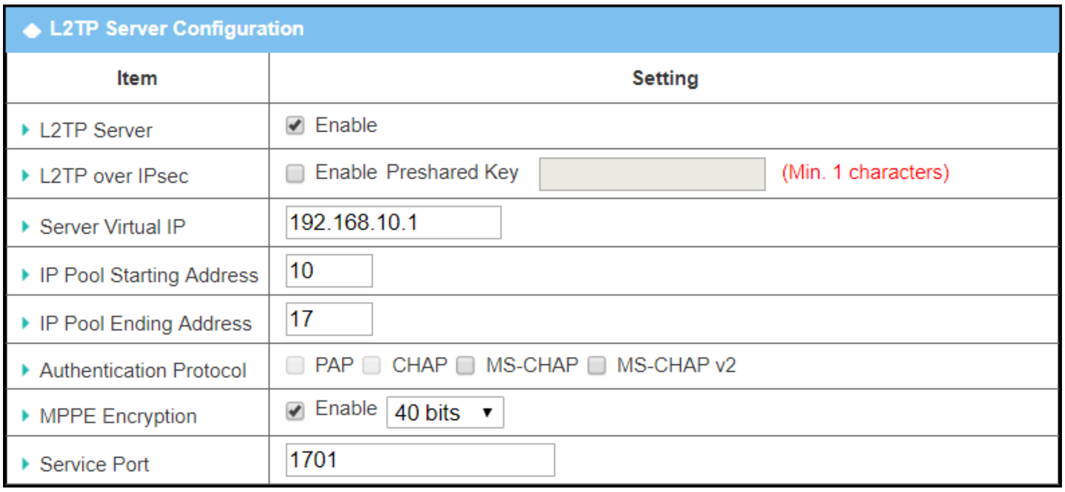
Figure 257 – L2TP Client List & Status

Item	Notes	Description
Add	Button	Click the **Add** button in the User Account List to open the User Account Configuration screen where you can create new user accounts, see next section. Up to eight (8) client accounts can be created.
Delete	Button	Click ☑ **Select** on one or more Client descriptions and then click the Delete button to permanently remove them from the list.
Refresh	Button	Click the **Refresh** button to test the connection.
Client details	Fields in row.	The following details are displayed for each client: **ID number**, **Tunnel Name**, **Interface**, **Virtual OP address**, **Remote IP/FQDN address**, **Remote Subnet address**, **connection Status**, and **Enable/Disabled status**. These are all set in the L2TP Client Configuration window. See the next section for details regarding these settings.

Item	Notes	Description
Delete	Button	Click ☑ **Select** for the User Account that you want to permanently delete and then click the Delete button.
Enable	Button	Click the **Edit** button to select **Tunnel** ☑ **Enable** in the L2TP Client Configuration window. Note that you can uncheck ☐ **Enable** rather than permanently Delete, this will allow you to retain the user details while disabling its access to the L2TP client.
Edit	Button	Click the **Edit** button to make changes to the client in the L2TP Client Configuration window.
Select	Checkbox	Click ☑ **Select** on one or more Client descriptions and then click the Delete button to permanently remove them from the list..

Table 157 – L2TP Client List & Status

When **Add** or **Edit** button is applied, the **L2TP Client Configuration** window will appear:



L2TP Server Configuration

Item	Setting
L2TP Server	☑ Enable
L2TP over IPsec	☐ Enable Preshared Key (Min. 1 characters)
Server Virtual IP	192.168.10.1
IP Pool Starting Address	10
IP Pool Ending Address	17
Authentication Protocol	☐ PAP ☐ CHAP ☐ MS-CHAP ☐ MS-CHAP v2
MPPE Encryption	☑ Enable 40 bits ▼
Service Port	1701

Figure 258 – L2TP Client Configuration

Item	Notes	Description
Tunnel Name	Mandatory field. 1 - 32 characters	Add a meaningful name.
Interface	Mandatory field.	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 field.	There are two available operation modes: **Always on** or **Failover** **Failover/ Always on**: 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.
L2TP over IPSec	Checkbox – disabled by default.	Check ☑ **Enable** to activate L2TP over IPSec and specify a Preshared Key (1 - 32 characters)

Item	Notes	Description
Remote LNS IP/FQDN	Mandatory field.	Enter the public IP address or the FQDN of the L2TP server.
Remote LNS Port	Mandatory field.	Enter the Remote LNS Port for this L2TP tunnel. Value Range: 1 - 65535
User Name	Mandatory field.	Enter the User Name for this L2TP tunnel to be authenticated with when connecting to L2TP server. Value Range: 1 - 32 characters
Password	Mandatory field.	Enter a secure password for this L2TP tunnel to be authenticated with when connecting to L2TP server.
Tunnelling Password	Optional field. Disabled by default.	Enter the Tunnelling Password for authenticating this L2TP tunnel.
Remote Subnet	Mandatory field.	Specify the remote subnet for this L2TP tunnel to reach the L2TP server. The Remote Subnet format must be IP address/netmask (e.g. 10.0.0.2/24). It is for the Intranet of L2TP VPN server. At the L2TP client peer, the packets whose destination is in the dedicated subnet will be transferred via the L2TP VPN tunnel. Others will be transferred based on current routing policy of the security gateway at the L2TP client peer. If you enter 0.0.0.0/0 in the Remote Subnet field, it will be treated as a default gateway setting for the L2TP client peer, all packets, including the Internet accessing of L2TP Client peer, will go through the established L2TP VPN tunnel. That means the remote L2TP VPN server controls the flow of any packets from the L2TP client peer.
Authentication Protocol	Mandatory field. All unselected by default.	Specify one or more Authentication Protocol(s) for this L2TP tunnel. Available authentication methods are: **PAP**, **CHAP**, **MS-CHAP** or **MS-CHAP v2**
MPPE Encryption	Optional field – disabled by default.	Specify whether L2TP server supports MPPE Protocol. Check ☑ **Enable** to enable MPPE. **Note** – when MPPE Encryption is enabled, the Authentication Protocol PAP /CHAP options will not be available.
LCP Echo Type	Auto = default setting. Value Ranges: 1 - 99999 for Interval Time 1 - 999 for Failure Times	Specify the LCP Echo Type for this L2TP tunnel: **Auto, User-defined, or Disable** **Auto** – the system sets the Interval and Max. Failure Time. **User-defined** – enter the Interval and Max. Failure Time. The default value for Interval is 30 seconds, and Maximum Failure Times is 6 times **Disable** – disable the LCP Echo.
Service Port	Mandatory field. Value Range: 0 - 65535	Specify the Service Port for this L2TP tunnel to use: **Auto, (1701) for Cisco), or User-defined** **Auto** – The system determines the service port.

Item	Notes	Description
		1701 (for Cisco) – The system use port 1701 for connecting with CISCO L2TP Server. **User-defined** – Enter the service port. The default value is 0.
Tunnel	Disabled by default.	Check ☑ **Enable** to enable this L2TP tunnel.
Edit	Button	Click **Save** to create the client account.
Undo	Button	Click **Undo** button to cancel the settings.
Back	Button	Click **Back** button to return to the previous page.

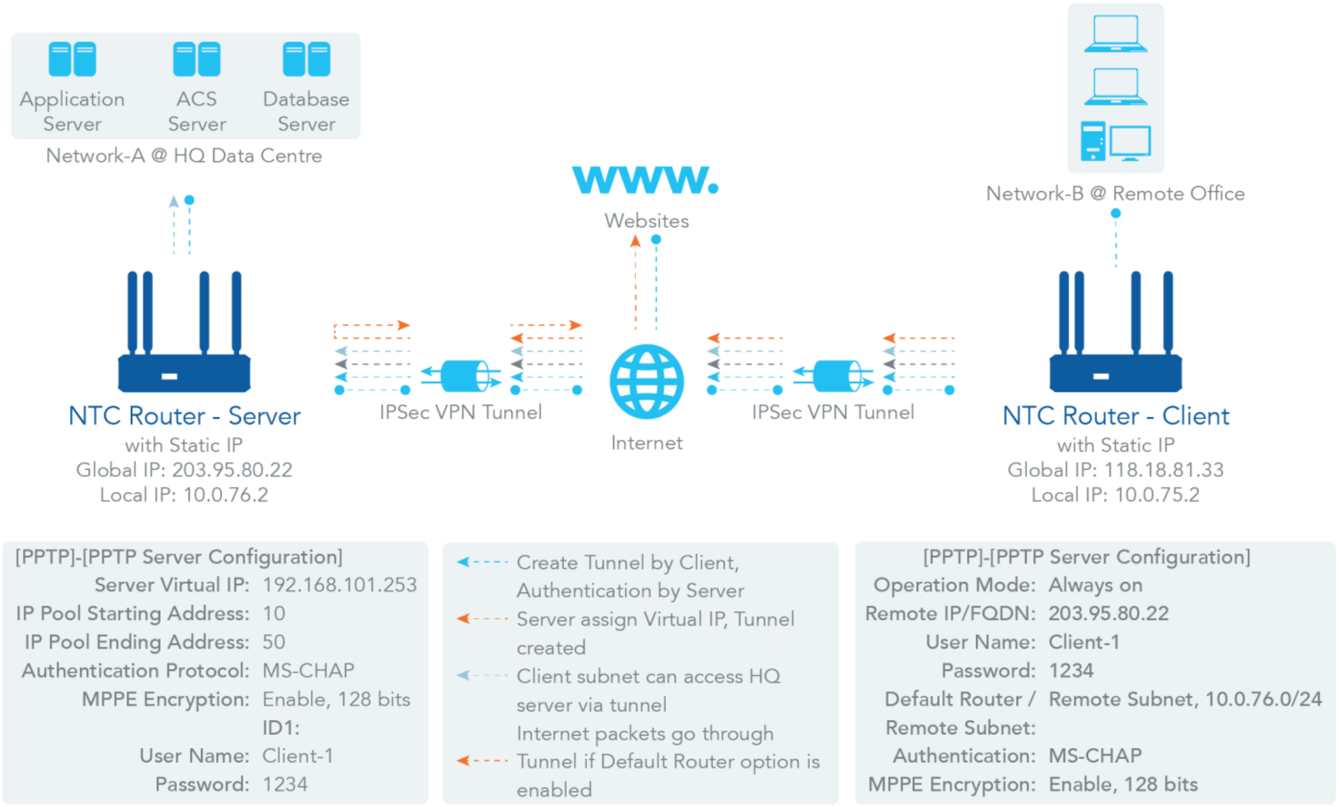
Table 158 – L2TP Client Configuration

6.1.4 PPTP

Point-to-Point Tunnelling Protocol (PPTP) is a method for implementing virtual private networks. It is a client-server based technology. PPTP uses a control channel over TCP and a GRE tunnel operating to encapsulate PPP packets. There are various levels of authentication and encryption for PPTP tunnelling, usually natively as standard features of the Windows PPTP stack. The security router can play either "PPTP Server" role or "PPTP Client" role for a PPTP VPN tunnel, or both at the same time for different tunnels. PPTP tunnel process is nearly the same as L2TP.

PPTP Server – It must have a static IP or a FQDN for clients to create PPTP tunnels. It also maintains “User Account list” (user name / password) for client login authentication; There is a virtual IP pool to assign virtual IP to each connected PPTP client.

PPTP Client – This can be mobile users or routers in remote offices with dynamic IP. To setup tunnel, it should get “user name”, “password” and server’s global IP. In addition, it is required to identify the operation mode for each tunnel as either main connection or failover for another tunnel to increase overall bandwidth. It needs to decide “Default Router” or “Remote Subnet” for packet flow. You can also define what kind of traffic will pass through the PPTP tunnel in the “Default Router / Remote Subnet” parameter.



[PPTP]-[PPTP Server Configuration]

Server Virtual IP:	192.168.101.253
IP Pool Starting Address:	10
IP Pool Ending Address:	50
Authentication Protocol:	MS-CHAP
MPPE Encryption:	Enable, 128 bits
	ID1:
User Name:	Client-1
Password:	1234

Create Tunnel by Client, Authentication by Server

Server assign Virtual IP, Tunnel created

Client subnet can access HQ server via tunnel

Internet packets go through Tunnel if Default Router option is enabled

[PPTP]-[PPTP Server Configuration]

Operation Mode:	Always on
Remote IP/FQDN:	203.95.80.22
User Name:	Client-1
Password:	1234
Default Router / Remote Subnet:	Remote Subnet, 10.0.76.0/24
Authentication:	MS-CHAP
MPPE Encryption:	Enable, 128 bits

Figure 259 – PPTP

There are two options, "Default Gateway" and "Remote Subnet" for the "Default Gateway / Remote Subnet" configuration item. When you choose "Remote Subnet", you need to specify one more setting: the remote subnet. This is for the Intranet of the PPTP VPN server. At the PPTP client peer, the packets whose destination is in the dedicated subnet will be transferred via the PPTP VPN tunnel. Others will be transferred based on current routing policy of the security gateway at PPTP client peer. If you choose "Default Gateway" option for the PPTP client peer, all packets will go through the established PPTP VPN tunnel. That means the remote PPTP VPN server controls the flowing of any packets from the PPTP client peer.

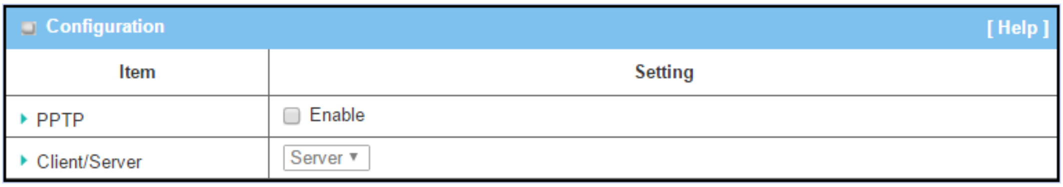
6.1.4.1 PPTP Setting

Enable PPTP

To enable the PPTP functionality:

1 Select **VPN** from the **Security** submenu and click the **PPTP** tab.

2 Go to the **Configuration** section:



Item	Setting
PPTP	□ Enable
Client/Server	Server ▾

Figure 260 – Enable PPTP

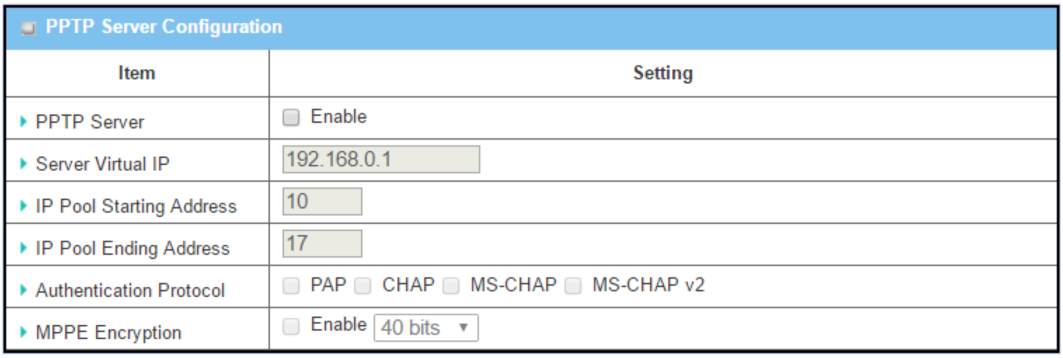
3 Click **PPTP** ☑ **Enable** and select a configuration type, either **Server** or **Client**, for the router to operate as.

Item	Notes	Description
PPTP	Checkbox, disabled by default.	Check ☑ **Enable** to activate the PPTP functionality.
Server/ Clients	Drop-down list. Server is the default selection.	When Server is selected the server configuration screen will be displayed below for further setup. When Client is selected the client configuration will be displayed instead.
Save	Button	Click **Save** to save the setting.

Table 159 – Enable PPTP

As a PPTP Server

If **Server** is selected the **PPTP Server Configuration** displays where you can enable the PPTP server function and specify its settings. Configure the router to act as a PPTP server here.



PPTP Server Configuration

Item	Setting
PPTP Server	□ Enable
Server Virtual IP	192.168.0.1
IP Pool Starting Address	10
IP Pool Ending Address	17
Authentication Protocol	□ PAP □ CHAP □ MS-CHAP □ MS-CHAP v2
MPPE Encryption	□ Enable 40 bits ▾

Figure 261 – PPTP Server Configuration

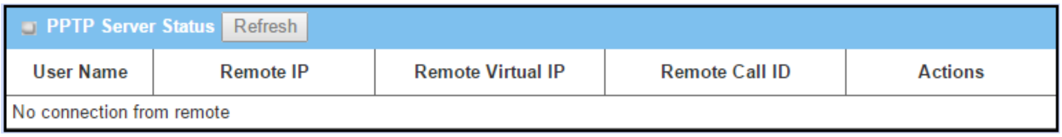
Item	Notes	Description
PPTP Server	Disabled by default.	Click ☑ **Enable** to activate PPTP Server functions.
Server Virtual IP	Mandatory field. Default setting: 192.168.0.1	Specify the PPTP server Virtual IP address. The virtual IP address will serve as the virtual DHCP server for the PPTP clients. Clients will be assigned a virtual IP address from it after the PPTP tunnel has been established.
IP Pool Starting Address	Mandatory field. Default setting: 10	Enter 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. Value Range: 1 - 254
IP Pool Ending Address	Mandatory field. Default setting: 17	Enter the PPTP server's Virtual IP DHCP server. Specify the last IP address for the subnet from which the PPTP client's IP address will be assigned Value Range: >= Starting Address, and < (Starting Address + 8) or 254

Item	Notes	Description
Authentication Protocol	Mandatory field. Disabled by default.	Select single or multiple Authentication Protocols for the PPTP server with which to authenticate PPTP clients. Available authentication protocols include: **PAP, CHAP, MS-CHAP or MS-CHAP v2**
MPPE Encryption	Mandatory field. Disabled by default.	Specify whether to support MPPE Protocol. Click ☑ Enable to enable MPPE and select 40 bits, 56 bits or 128 bits from dropdown box. **Note** - when MPPE Encryption is enabled, the Authentication Protocol PAP / CHAP options will not be available.
Save	Button	Click **Save** to save the settings.
Undo	Button	Click **Undo** to cancel the changes.

Table 160 – PPTP Server Configuration

6.1.4.2 PPTP Server Status list

After the PPTP server has been set up PPTP clients connected to it will be listed in the **PPTP Server Status** list:



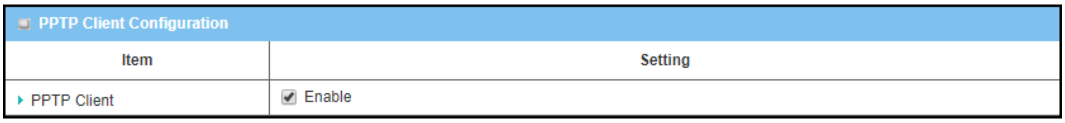
User Name	Remote IP	Remote Virtual IP	Remote Call ID	Actions
No connection from remote				

Figure 262 – PPTP Server Status

The following details of each connected PPTP client are listed: **User Name, Remote IP, Remote Virtual IP, Remote Call ID** and current **Actions**

Click the **Refresh** button to renew the PPTP client information.

To create a new client, select Client from the Client/Server drop down list on the Configuration section and then check ☑ **Enable** in the PPTP Client Configuration section.

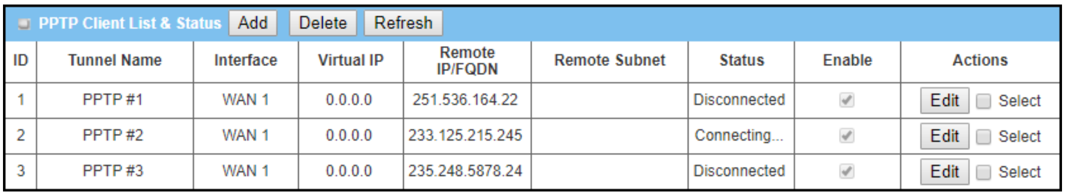


Item	Setting
PPTP Client	☑ Enable

Figure 263 – PPTP Client Configuration

When ☑ **Enable** is selected, the buttons on the **PPTP Client List & Status** section become active.

Click on the **Add** button to create a new client in the list. You can create up to ten (10) PPTP client user accounts.



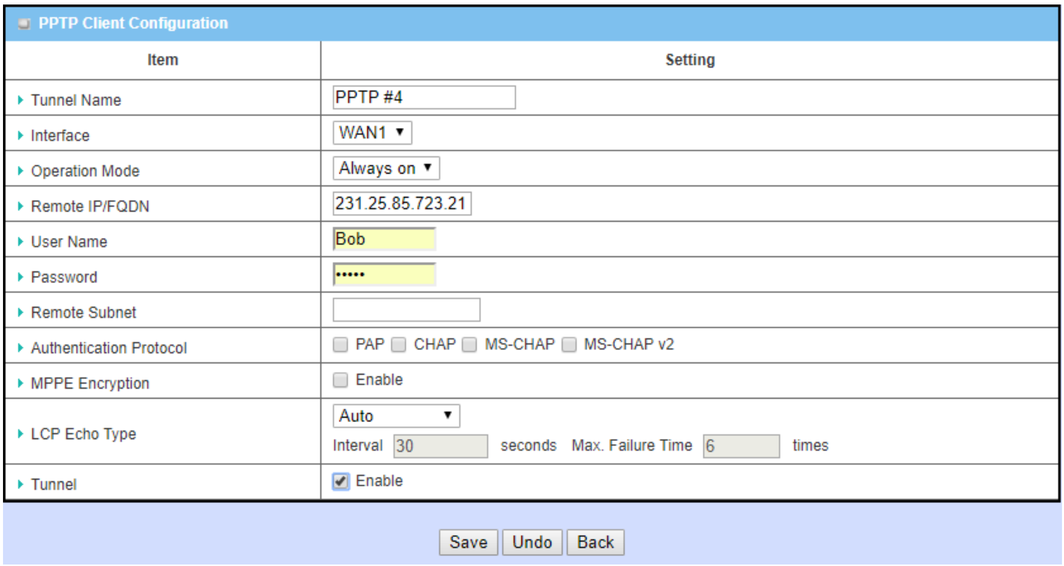
ID	Tunnel Name	Interface	Virtual IP	Remote IP/FQDN	Remote Subnet	Status	Enable	Actions
1	PPTP #1	WAN 1	0.0.0.0	251.536.164.22		Disconnected	☑	Edit □ Select
2	PPTP #2	WAN 1	0.0.0.0	233.125.215.245		Connecting...	☑	Edit □ Select
3	PPTP #3	WAN 1	0.0.0.0	235.248.5878.24		Disconnected	☑	Edit □ Select

Figure 264 – PPTP Client List & Status

Item	Notes	Description
Add	Button	Click the **Add** button in the User Account List to open the User Account Configuration screen where you can create new user accounts, see next section. Up to ten (10) client accounts can be created.
Delete	Button	Click ☑ **Select** on one or more Client descriptions and then click the Delete button to permanently remove them from the list.
Refresh	Button	Click the **Refresh** button to test the connection.
Client details	Fields in row.	The following details are displayed for each client: ID number, Tunnel Name, Interface, Virtual OP address, Remote IP/FQDN address, Remote Subnet address, connection Status, and Enable/Disabled status. These are all set in the PPTP Client Configuration window. See the next section for details regarding these settings.
Delete	Button	Click ☑ **Select** for the User Account that you want to permanently delete and then click the Delete button.
Enable	Button	Click the **Edit** button to select Tunnel ☑ **Enable** in the PPTP Client Configuration window. Note that you can uncheck ☐ **Enable** rather than permanently Delete, this will allow you to retain the user details while disabling its access to the PPTP client.
Edit	Button	Click the **Edit** button to make changes to the client in the PPTP Client Configuration window.
Select	Checkbox	Click ☑ **Select** on one or more Client descriptions and then click the Delete button to permanently remove them from the list.

Table 161 – PPTP Client List & Status

When **Add** or **Edit** button is applied, the **PPTP Client Configuration** window will appear:



PPTP Client Configuration

Item	Setting
Tunnel Name	PPTP #4
Interface	WAN1 ▾
Operation Mode	Always on ▾
Remote IP/FQDN	231.25.85.723.21
User Name	Bob
Password	•••••
Remote Subnet	
Authentication Protocol	☐ PAP ☐ CHAP ☐ MS-CHAP ☐ MS-CHAP v2
MPPE Encryption	☐ Enable
LCP Echo Type	Auto ▾ Interval 30 seconds Max. Failure Time 6 times
Tunnel	☑ Enable

Figure 265 – PPTP Client Configuration

Item	Notes	Description
Tunnel Name	Mandatory field. 1 - 32 characters	Add a meaningful name.
Interface	Mandatory field.	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 field.	There are two available operation modes: **Always on** or **Failover** **Failover/Always on**: 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.
Remote IP/FQDN	Mandatory field. Format can be ipv4 address or FQDN	Enter the public IP address or the FQDN of the PPTP server.
User Name	Mandatory field.	Enter the User Name for this PPTP tunnel to be authenticated with when connecting to PPTP server. Value Range: 1 - 32 characters
Password	Mandatory field.	Enter a secure password for this PPTP tunnel to be authenticated with when connecting to PPTP server.
Default Gateway / Remote Subnet	Mandatory field.	Specify a gateway for this PPTP tunnel to reach PPTP server. When you choose Remote Subnet, you need to specify one more setting: the remote subnet. It is for the Intranet of PPTP VPN server. So, at PPTP client peer, the packets whose destination is in the dedicated subnet will be transferred via the PPTP VPN tunnel. Others will be transferred based on current routing policy of the security gateway at PPTP client peer. If you choose Default Gateway option for the PPTP client peer, all packets, including the Internet accessing of PPTP Client peer, will go through the established PPTP VPN tunnel. That means the remote PPTP VPN server controls the flowing of any packets from the PPTP client peer. Certainly, those packets come through the PPTP VPN tunnel. The Remote Subnet format must be IP address/netmask (e.g. 10.0.0.2/24)
Authentication Protocol	Mandatory field. All unselected by default.	Specify one or more Authentication Protocol(s) for this PPTP tunnel. Available authentication methods are: PAP, CHAP, MS-CHAP or MS-CHAP v2
MPPE Encryption	Optional field – disabled by default.	Specify whether PPTP server supports MPPE Protocol. Check ☑ **Enable** to enable MPPE. **Note** – when MPPE Encryption is enabled, the Authentication Protocol PAP /CHAP options will not be available.
NAT before Tunnelling	Optional field – disabled by default.	Check ☑ **Enable** to enable NAT function for this PPTP tunnel.

Item	Notes	Description
LCP Echo Type	Auto = default setting. Value Ranges: 1 - 99999 for Interval Time 1 - 999 for Failure Times	Specify the LCP Echo Type for this PPTP tunnel: **Auto, User-defined**, or **Disable** **Auto** – the system sets the Interval and Max. Failure Time. **User-defined** – enter the Interval and Max. Failure Time. The default value for Interval is 30 seconds, and Maximum Failure Times is 6 times **Disable** – disable the LCP Echo.
Tunnel	Disabled by default.	Check ☑ **Enable** to enable this PPTP tunnel.
Edit	Button	Click **Save** to create the client account.
Undo	Button	Click **Undo** button to cancel the settings.
Back	Button	Click **Back** button to return to the previous page.

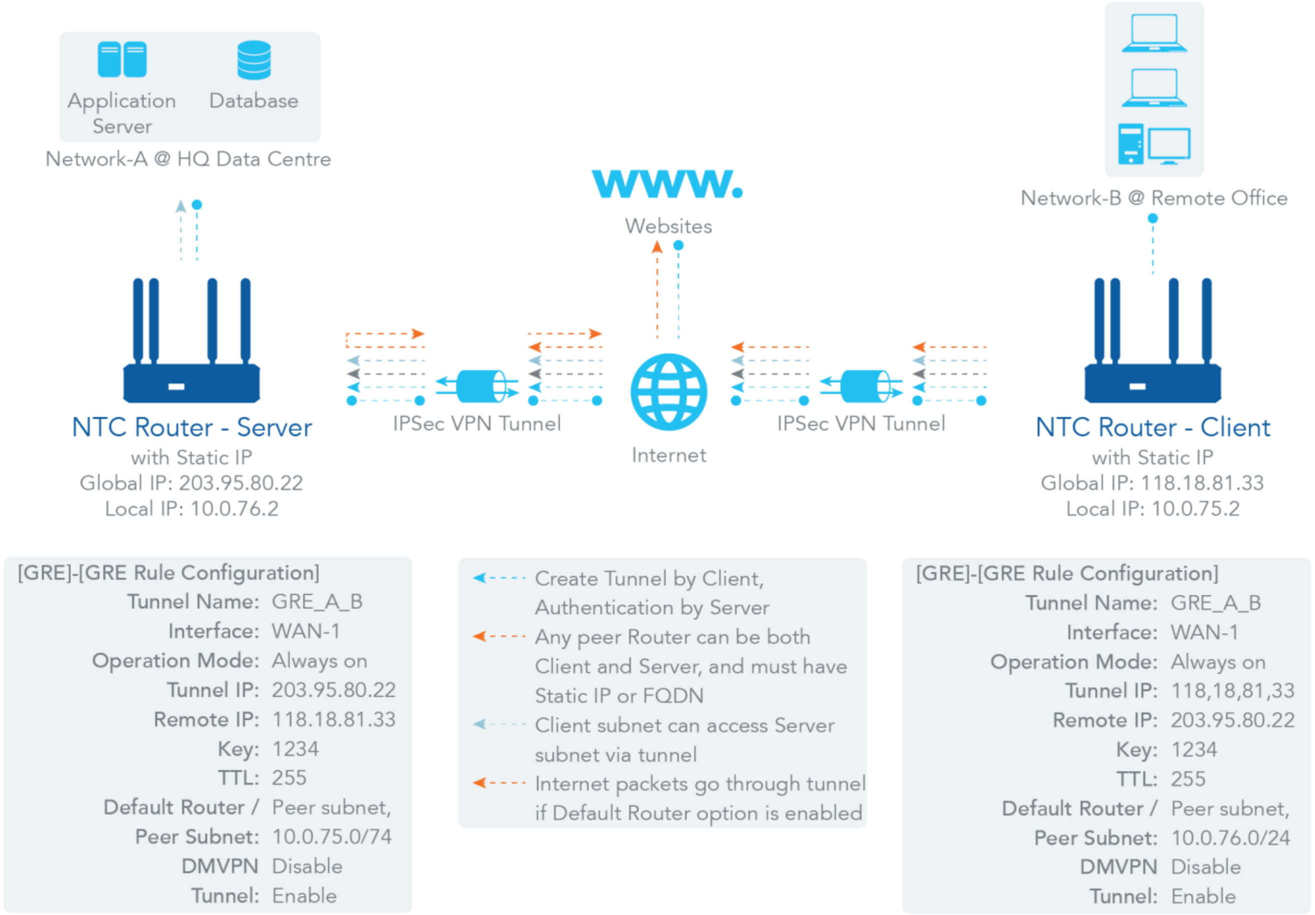
Table 162 – PPTP Client Configuration

6.1.5 GRE

Generic Routing Encapsulation (GRE) is a tunnelling protocol developed by Cisco Systems that encapsulates a wide variety of network layer protocols inside virtual point-to-point links over an Internet Protocol internetwork.

Deploy an NTC-400 Series Router router at a remote site and establish a virtual private network with the control centre using GRE tunnelling. All client hosts behind the router can make data communication with server hosts behind control centre router.

GRE Tunnelling is similar to IPSec Tunnelling where the client requests the tunnel establishment with the server. Both the client and the server must have a Static IP or an FQDN. Any peer router can work as either a client or a server, even using the same set of configuration rules.



[GRE]-[GRE Rule Configuration]

Tunnel Name:	GRE_A_B
Interface:	WAN-1
Operation Mode:	Always on
Tunnel IP:	203.95.80.22
Remote IP:	118.18.81.33
Key:	1234
TTL:	255
Default Router / Peer Subnet:	Peer subnet, 10.0.75.0/74
DMVPN	Disable
Tunnel:	Enable

Create Tunnel by Client, Authentication by Server

Any peer Router can be both Client and Server, and must have Static IP or FQDN

Client subnet can access Server subnet via tunnel

Internet packets go through tunnel if Default Router option is enabled

[GRE]-[GRE Rule Configuration]

Tunnel Name:	GRE_A_B
Interface:	WAN-1
Operation Mode:	Always on
Tunnel IP:	118,18,81,33
Remote IP:	203.95.80.22
Key:	1234
TTL:	255
Default Router / Peer Subnet:	Peer subnet, 10.0.76.0/24
DMVPN	Disable
Tunnel:	Enable

Figure 266 – GRE Tunnel Scenario

To setup a GRE tunnel, each peer needs to setup its global IP as the tunnel IP and fill in the other's global IP as remote IP.

Each peer must further specify the Remote Subnet item. This is for the Intranet of GRE server peer. At the GRE client peer, the packets whose destination is in the dedicated subnet will be transferred via the GRE tunnel. Others will be transferred based on current routing policy of the router at GRE client peer. If you entered 0.0.0.0/0 in the Remote Subnet field, it will be treated as a "Default Router" setting for the GRE client peer and all packets will go through the established GRE tunnel. That means the remote GRE server peer controls the flow of any packets from the GRE client peer.

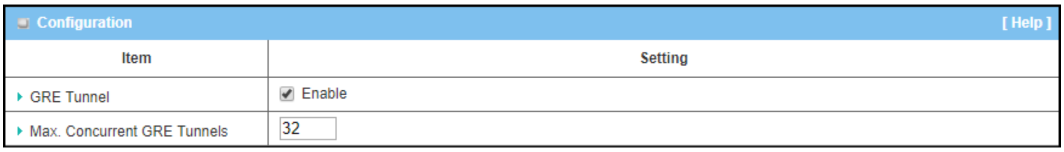
If the GRE server supports DMVPN Hub function, like a Cisco router as the VPN concentrator, the GRE client can activate the DMVPN spoke function here since it is implemented by GRE over IPSec tunnelling.

6.1.5.1 Enable GRE

To enable the **GRE** functionality:

1 Select **VPN** from the **Security** submenu and click the **GRE** tab.

2 Go to the **Configuration** section:



Item	Setting
GRE Tunnel	☑ Enable
Max. Concurrent GRE Tunnels	32

Figure 267 – Enable GRE Tunnel

3 Click GRE Tunnel ☑ Enable and set the Maximum number of Concurrent GRE Tunnels

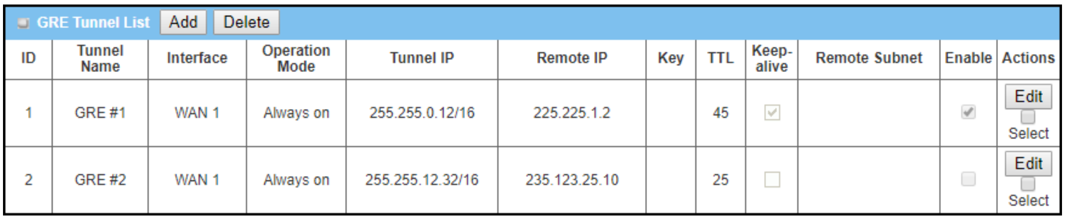
Item	Notes	Description
GRE Tunnel	Checkbox, disabled by default.	Check ☑ **Enable** to activate the GRE functionality.
Max. Concurrent GRE Tunnels	32 is the default setting. 32 is the maximum number.	Specify the maximum number of simultaneous GRE tunnel connections. **Note** – The maximum number of supported tunnels may vary depending on your model.
Save	Button	Click **Save** to save the setting.
Undo	Button	Click **Undo** to cancel the changes to settings.

Table 163 – Enable GRE Tunnel

6.1.5.2 Create/Edit GRE Tunnel

When ☑ **Enable** is selected, the buttons on the **GRE Tunnel List** section become active.

Click on the **Add** button to create a new client in the list. You can create up to the maximum number of concurrent GRE tunnels that you had set previously in the **Configuration** section, see above.



GRE Tunnel List Add Delete

ID	Tunnel Name	Interface	Operation Mode	Tunnel IP	Remote IP	Key	TTL	Keep-alive	Remote Subnet	Enable	Actions
1	GRE #1	WAN 1	Always on	255.255.0.12/16	225.225.1.2		45	☑		☑	Edit □ Select
2	GRE #2	WAN 1	Always on	255.255.12.32/16	235.123.25.10		25	□		□	Edit □ Select

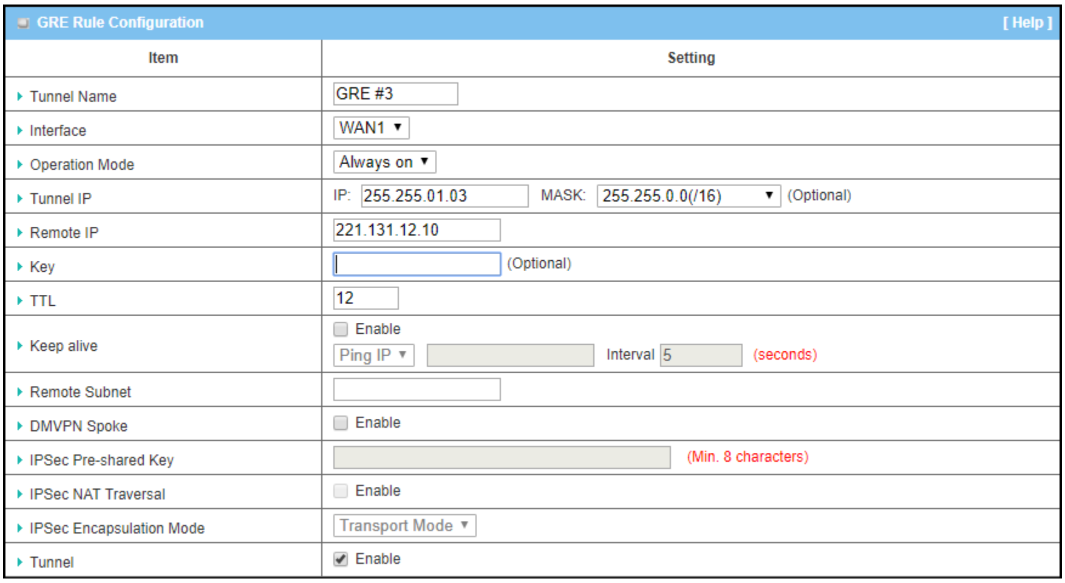
Figure 268 – GRE Tunnel List

Item	Notes	Description
Add	Button	Click the **Add** button in the GRE Tunnel List to open the **GRE Rule Configuration** screen where you can create new GRE Tunnels, see next section.
Delete	Button	Click ☑ **Select** in the **Actions** column for one or more GRE Tunnel descriptions and then click the **Delete** button to permanently remove them from the list.
Client details	Fields in row.	The following details are displayed for each client: **ID number, Tunnel Name, Interface, Operation Mode, Tunnel IP, Remote IP, Key, TTL, Keep-alive status, Remote Subnet address**, and **Enable/Disabled status** These are all set in the GRE Rule Configuration window. See the next section for details regarding these settings.
Delete	Button	Click ☑ **Select** for the GRE Tunnel that you want to permanently delete and then click the **Delete** button.
Enable	Button	Click the **Edit** button to select Tunnel ☑ **Enable** in the GRE Rule Configuration window. Note that you can uncheck ☐ **Enable** rather than permanently Delete, this will allow you to retain the user details while disabling its access to the PPTP client.

Item	Notes	Description
Edit	Button	Click the **Edit** button to make changes to the client in the GRE Rule Configuration window.
Select	Checkbox	Click ☑ **Select** on one or more tunnel rules and then click the Delete button to permanently remove them from the list.

Table 164 – GRE Tunnel List

When **Add** or **Edit** button is applied, the **GRE Rule Configuration** window will appear:



GRE Rule Configuration [Help]

Item	Setting
Tunnel Name	GRE #3
Interface	WAN1 ▾
Operation Mode	Always on ▾
Tunnel IP	IP: 255.255.01.03 MASK: 255.255.0.0(/16) ▾ (Optional)
Remote IP	221.131.12.10
Key	(Optional)
TTL	12
Keep alive	□ Enable Ping IP ▾ Interval 5 (seconds)
Remote Subnet	
DMVPN Spoke	□ Enable
IPSec Pre-shared Key	(Min. 8 characters)
IPSec NAT Traversal	□ Enable
IPSec Encapsulation Mode	Transport Mode ▾
Tunnel	☑ Enable

Figure 269 – GRE Rule Configuration

Item	Notes	Description
Tunnel Name	Mandatory field. 1 - 32 characters	Add a meaningful name.
Interface	Mandatory field. **WAN-1** is the default setting.	Select the interface on which GRE tunnel is to be established. It can be via either the WAN and LAN interface32- 32.
Operation mode	Mandatory field. **Always on** is the default setting.	Define the operation mode for the GRE Tunnel: **Always On**, or **Failover** If this tunnel is set as a Failover tunnel, you need to further select a primary tunnel from which to failover to. **Note** – Failover mode is not available for the router with single WAN.
Tunnel IP	Optional field.	Enter the tunnel IP address and corresponding subnet mask.
Remote IP	Mandatory field.	Enter the Remote IP address of remote GRE tunnel router. Normally this is the public IP address of the remote GRE router.
Key	Optional field.	Enter the Key for the GRE connection. Value Range: 0 - 9999999999
TTL	Mandatory field.	Specify TTL hop-count value for this GRE tunnel.

Item	Notes	Description
		Value Range: 1 - 255
Keep alive	Disabled by default. Default setting: 5 seconds	Check ☑ Enable 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: 5 - 999 seconds
Remote Subnet	Mandatory field.	Specify the remote subnet for this GRE tunnel. The Remote Subnet format must be IP address/netmask (e.g. 10.0.0.2/24). It is for the Intranet of GRE server peer. So, at GRE client peer, the packets whose destination is in the dedicated subnet will be transferred via the GRE tunnel. Others will be transferred based on current routing policy of the security router at GRE client peer. If you entered 0.0.0.0/0 in the Remote Subnet field, it will be treated as a default router setting for the GRE client peer, all packets, including the Internet accessing of GRE client peer, will go through the established GRE tunnel. That means the remote GRE server peer controls the flow of any packets from the GRE client peer. Certainly, those packets come through the GRE tunnel.
DMVPN Spoke	Disabled by default.	Check ☑ **Enable** to have the router support DMVPN Spoke for this GRE tunnel.
IPSec Pre-shared Key	Mandatory field.	Enter a DMVPN spoke authentication Pre-shared Key Value Range: 8 - 32 characters **Note** – Pre-shared Key is available only when DMVPN Spoke is enabled, see previous setting.
IPSec NAT Traversal	Disabled by default.	Check ☑ **Enable** to enable NAT-Traversal. **Note** – IPSec NAT Traversal will not be available when DMVPN is not enabled.
IPSec Encapsulation Mode	Disabled by default.	Specify the IPSec Encapsulation Mode from the dropdown box: Transport mode or Tunnel mode **Note** – IPSec Encapsulation Mode will not be available when DMVPN is not enabled, see above.
Tunnel	Disabled by default.	Check ☑ **Enable** to enable this GRE tunnel.
Save	Button	Click **Save** to create the GRE Tunnel Rule.
Undo	Button	Click **Undo** button to cancel the settings.
Back	Button	Click **Back** button to return to the previous page.

Table 165 – GRE Rule Configuration

6.2 Firewall

The firewall functions include Packet Filter, URL Blocking, Content Filter, MAC Control, Application Filter, IPS and some firewall options.

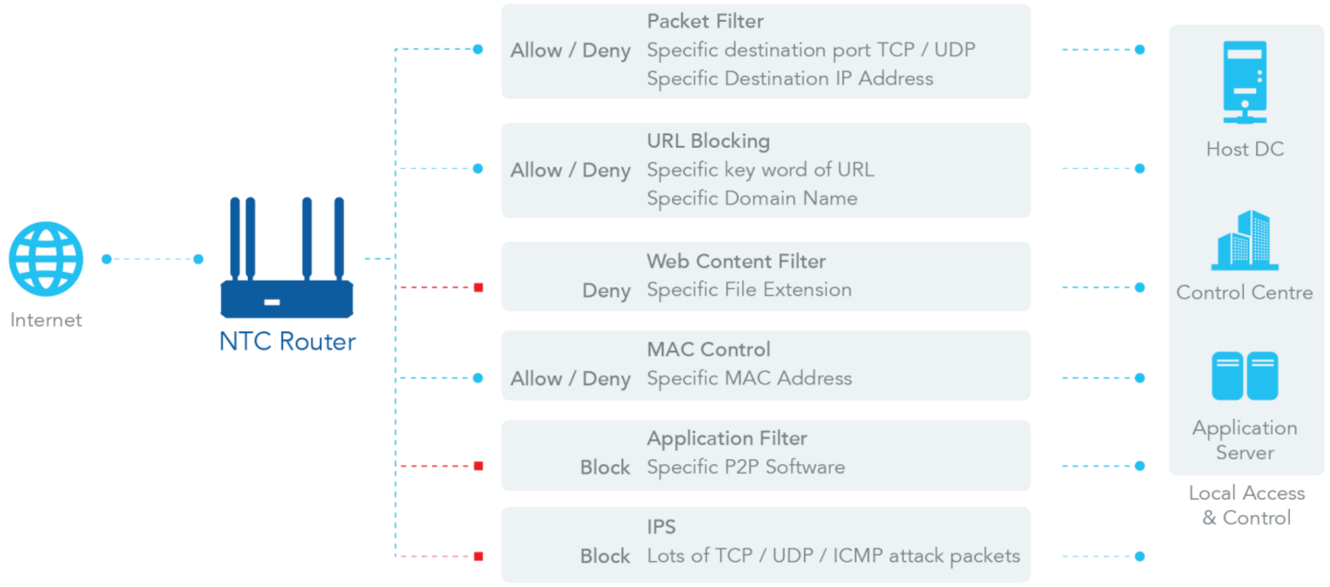

Internet
NTC Router
Packet Filter
Allow / Deny Specific destination port TCP / UDP
Specific Destination IP Address
URL Blocking
Allow / Deny Specific key word of URL
Specific Domain Name
Web Content Filter
Deny Specific File Extension
MAC Control
Allow / Deny Specific MAC Address
Application Filter
Block Specific P2P Software
IPS
Block Lots of TCP / UDP / ICMP attack packets
Host DC
Control Centre
Application Server
Local Access & Control

Figure 270 – Firewall

6.2.1 Packet filters

The Packet Filter function allows you to define filtering rules for incoming and outgoing packets effectively controlling which packets are allowed or blocked from passing through it. A packet filter rule can indicate which interface the packet uses to enter and leave the router, the source and destination IP addresses, and the destination service port type and port number. In addition, you can be schedule a rule to be active or inactive at specified times.

6.2.1.1 Packet Filter with White List Scenario

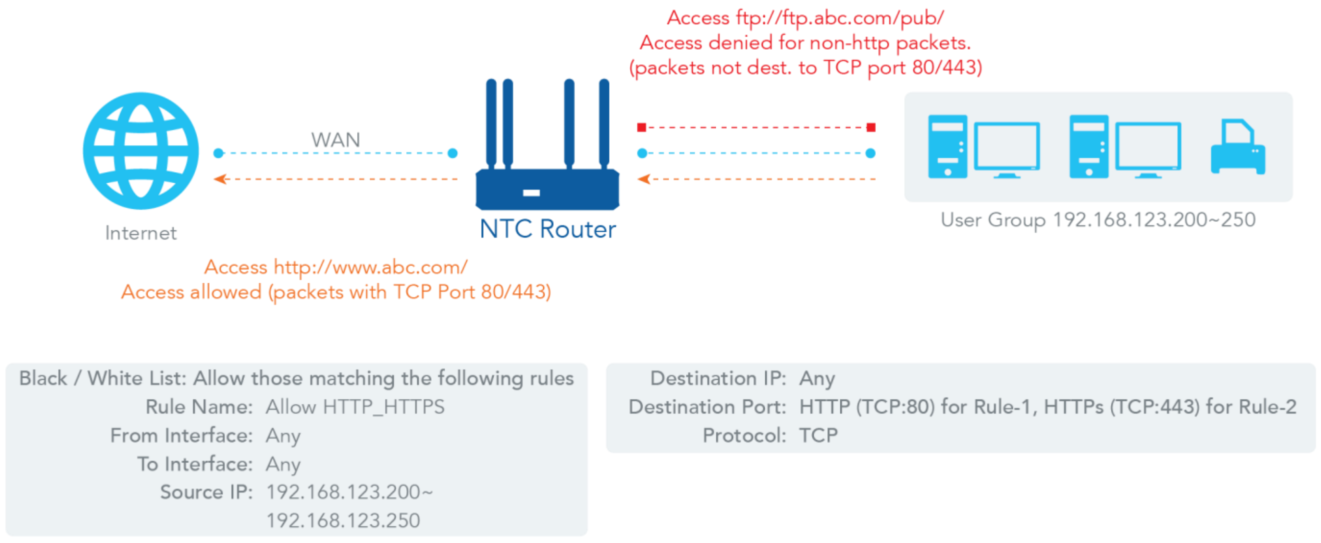

Access ftp://ftp.abc.com/pub/
Access denied for non-http packets.
(packets not dest. to TCP port 80/443)
WAN
Internet
NTC Router
User Group 192.168.123.200~250
Access http://www.abc.com/
Access allowed (packets with TCP Port 80/443)
Black / White List: Allow those matching the following rules
Rule Name: Allow HTTP_HTTPS
From Interface: Any
To Interface: Any
Source IP: 192.168.123.200~ 192.168.123.250
Destination IP: Any
Destination Port: HTTP (TCP:80) for Rule-1, HTTPs (TCP:443) for Rule-2
Protocol: TCP

Figure 271 – Packet Filter with White List Scenario

As shown in the diagram above, specify "Packet Filter Rule List" as white list (*Allow those matching the following rules*) and define the rules. Rule-1 is to allow HTTP packets to pass, and Rule-2 is to allow HTTPS packets to pass.

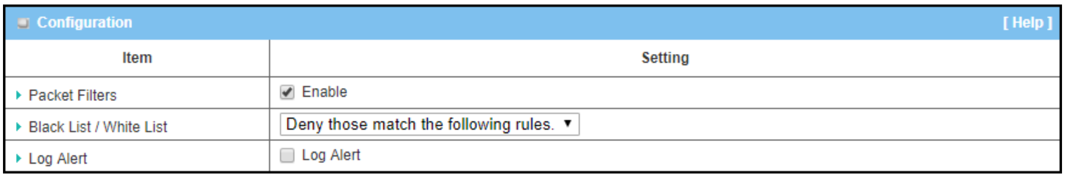
Under such configuration, the router will allow only HTTP and HTTPS packets, issued from the IP range 192.168.123.200 to 250, which are targeted to TCP port 80 or 443 to pass the WAN interface.

6.2.1.2 Packet Filter Settings

To enable the Packet Filter functionality:

1 Select **Firewall** from the **Security** submenu on the left and then open the **Packet Filters** tab.

2 Go to the **Configuration** section of the **Packet Filters** page:



Configuration [Help]

Item	Setting
Packet Filters	☑ Enable
Black List / White List	Deny those match the following rules. ▼
Log Alert	□ Log Alert

Figure 272 – Enable Packet Filters

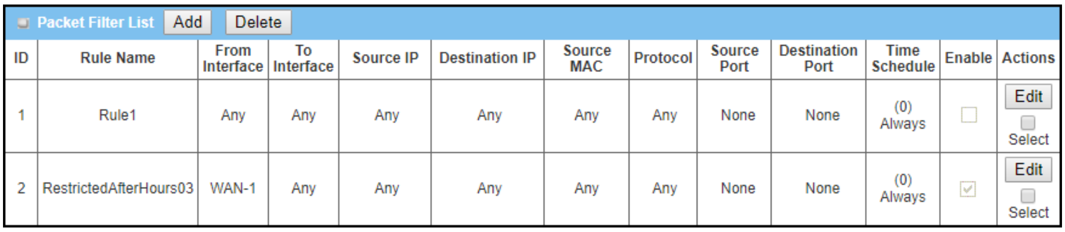
3 Click **Packet Filters** ☑ **Enable** and set the following parameters:

Item	Notes	Description
Packet Filters	Checkbox, disabled by default.	Check ☑ **Enable** to activate the Packet Filter functionality.
Black List / White List	Drop down list Deny those match the following rules is the default setting.	When Deny those match the following rules is selected packets that meet the criteria of the rule will be blocked – "black listed"– and any other packets will be allowed to pass. In contrast, Allow those match the following rules will allow those packets that meet the criteria of the rule to pass, that is be part of the "White List", and the rest will be blocked.
Log Alert	Disabled by default	Check ☑ **Log Alert** to activate event logging.
Save	Button	Click **Save** to save the setting.
Undo	Button	Click **Undo** to cancel the changes to settings.

Table 166 – Enable Packet Filters

6.2.1.3 Create/Edit Packet Filter Rules

When ☑ **Enable** is selected, the buttons on the **Packet Filter List** section become active.

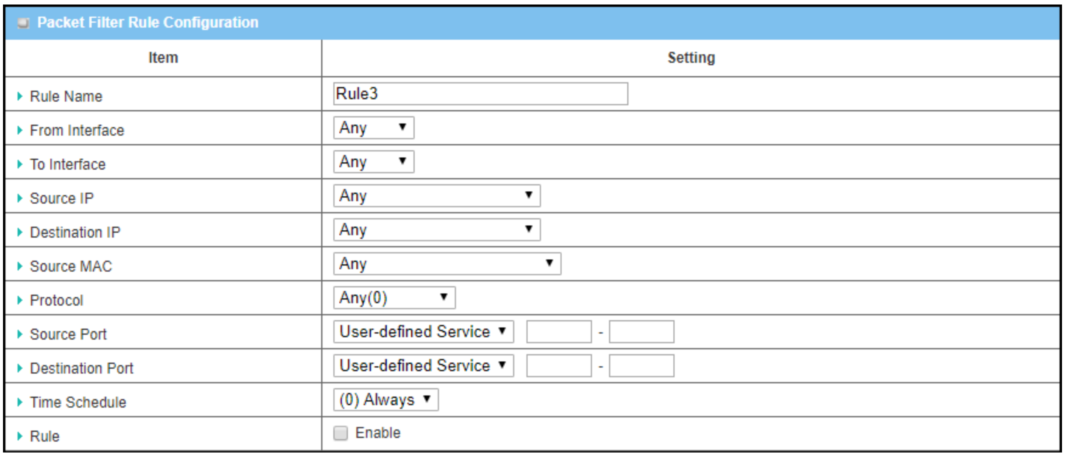


Packet Filter List Add Delete

ID	Rule Name	From Interface	To Interface	Source IP	Destination IP	Source MAC	Protocol	Source Port	Destination Port	Time Schedule	Enable	Actions
1	Rule1	Any	Any	Any	Any	Any	Any	None	None	(0) Always	□	Edit □ Select
2	RestrictedAfterHours03	WAN-1	Any	Any	Any	Any	Any	None	None	(0) Always	☑	Edit □ Select

Figure 273 – Packet Filter Rule Configuration

Click on the **Add** button to create a new client in the list. You can create up to the maximum number of concurrent GRE tunnels that you had set previously in the **Packet Filter Rule Configuration** section, see above.



Packet Filter Rule Configuration

Item	Setting
Rule Name	Rule3
From Interface	Any ▾
To Interface	Any ▾
Source IP	Any ▾
Destination IP	Any ▾
Source MAC	Any ▾
Protocol	Any(0) ▾
Source Port	User-defined Service ▾ -
Destination Port	User-defined Service ▾ -
Time Schedule	(0) Always ▾
Rule	□ Enable

Figure 274 – Packet Filter Rule Configuration

Item	Notes	Description
Rule Name	Mandatory field. String format.	Enter a meaningful packet filter rule name of up to 30 characters.
From Interface	Mandatory field. Default setting: **Any**	The “From” interface is defined to be the packet-entering interface of the router, that is the service that the packets are being delivered by. 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 or VLAN-1 to WAN. Select Any to filter packets coming into the router from any interface. **Note** – Two identical interfaces are not accepted by the router. For example *VLAN-1 to VLAN-1* will result in an error message.
To Interface	Mandatory field. Default selection: **Any**	The “To” interface is defined to be the packet-leaving interface of the router, that is the service that the packets are being sent with. 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. **Note** – Two identical interfaces are not accepted by the router. For example *VLAN-1 to VLAN-1* will result in an error message.
Source IP	Mandatory field. Default selection: **Any**	This field specifies the Source IP address or addresses. Select Any to filter packets coming from any IP addresses. Select Specific IP Address to filter packets coming from an IP address which you enter into the following text box. Select IP Range to filter packets coming from a specified range of IP address. Define the range in the two following text boxes. 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.

Item	Notes	Description
Destination IP	Mandatory field. Default selection: **Any**	This field specifies the Destination IP address or addresses. 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** – Groups 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	Mandatory field. Default selection: **Any**	This field specifies the Source MAC address or addresses. 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 from the drop down list to filter packets coming from the selected group. **Note** – Groups must be pre-defined before this selection become available in the drop down list. Refer to Object Definition > Grouping > Host grouping. Alternatively, click the Add Rule button that displays when this drop down list is empty to create a new group.
Protocol	Mandatory field. Drop-down list. Your selection determines the options which follow. Default selection: **Any (0)**	If the Protocol selection is: **Any**, **ICMPv4**, **TCP** or **UDP** The Source Port drop down list will have two options: **User-defined Service** –specify a port range(1 - 65535), or **Well-known Service** –select a predefined port from the drop-down list. The Destination Port drop down list will have the same two options: **User-defined Service** – specify a port range (1 - 65535), or **Well-known Service** – select a predefined port from the drop-down list. **Note** – Any will apply to all packets regardless of their protocol.
		If the Protocol selection is **GRE** the packet filter will only apply to GRE packets.
		If the Protocol selection is **ESP** the packet filter will only apply to ESP packets.
		If the Protocol selection is **SCTP** the packet filter will only apply to SCTP packets.

Item	Notes	Description
		If the Protocol selection is **User-defined** then only packets with a protocol number specified by you in the Protocol Number box will be filtered. Enter an Internet Assigned Numbers Authority protocol number.
Time Schedule	Mandatory field.	Select a Time Schedule from the drop down list to apply to this rule or leave it as Always (i.e. without a time parameter). If the drop down list is empty you will need to define a Time Schedule using the **Object Definition > Scheduling > Configuration** tab.
Rule	Disabled by default.	Click ☑ **Enable** to activate this rule then save the settings.
Save	Button	Click **Save** to save the settings.
Undo	Button	Click **Undo** to cancel the settings.
Back	Button	When the **Back** button is clicked the screen will return to the Packet Filter Configuration page.

Table 167 – Packet Filter Rule Configuration

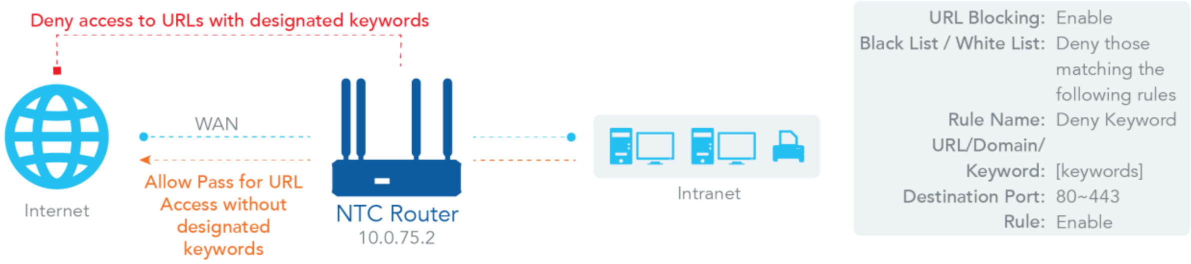
6.2.2 URL Blocking

Use **URL Blocking** to define rules to block or allow incoming and outgoing Web request packets. The rules can control the Web requests containing complete URLs, partial domain names, or pre-defined keywords. For example, you can filter out or allow only Web requests containing domain suffixes like .com, .edu or .org or keywords like “torrent” or “warez”.

Each rule is designated either as a **Black List**, blocking access from defined addresses, or a **White List** which specifically allows access.

In addition to rule parameters regarding addresses and keywords, rules can be set to run on schedules and the blocking activity can be logged, monitored and reported.

6.2.2.1 URL Blocking Rule with Black List


Deny access to URLs with designated keywords
WAN
Internet
Allow Pass for URL Access without designated keywords
NTC Router
10.0.75.2
Intranet

URL Blocking: Enable
Black List / White List: Deny those matching the following rules
Rule Name: Deny Keyword
URL/Domain/ Keyword: [keywords]
Destination Port: 80~443
Rule: Enable

Figure 275 – URL Blocking Rule with Black List

When the administrator of the router wants to block Web requests with dedicated patterns, they can use the "URL Blocking" function to block specific Web requests by defining the black list as shown in the diagram above. When the administrator wants to allow only Web requests with dedicated patterns to go through the router, they can also use the "URL Blocking" function by defining the white list to meet the requirement.

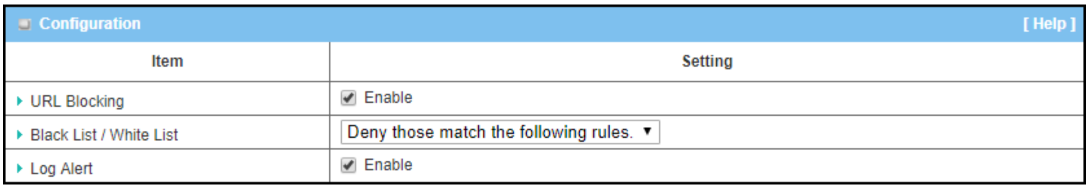
As shown in the diagram above, enable the URL blocking function and create the first rule to deny Web requests with the defined patterns to go through the router. The system will block Web requests with the defined patterns to pass through the router.

6.2.2.2 URL Blocking Settings

To enable the URL Blocking functionality:

1 Select **Firewall** from the **Security** submenu on the left and then open the **URL Blocking** tab.

2 Go to the **Configuration** section of the **URL Blocking** page:



Configuration [Help]

Item	Setting
URL Blocking	☑ Enable
Black List / White List	Deny those match the following rules. ▼
Log Alert	☑ Enable

Figure 276 – Enable URL Blocking

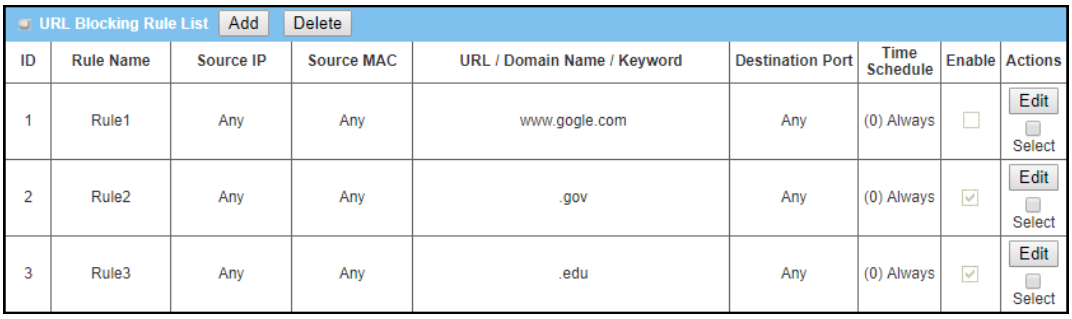
3 Click **Packet Filters** ☑ **Enable** and set the following parameters:

Item	Notes	Description
URL Blocking	Checkbox, disabled by default.	Check ☑ Enable to activate the URL Blocking functionality.
Black List / White List	Drop down list Deny those match the following rules is the default setting.	When Deny those match the following rules is selected packets that meet the criteria of the rule will be blocked – "black listed"– and any other packets will be allowed to pass. In contrast, Allow those match the following rules will allow those packets that meet the criteria of the rule to pass, that is be part of the "White List", and the rest will be blocked.
Log Alert	Disabled by default	Check ☑ **Log Alert** to activate event logging for the selected rules.
Save	Button	Click **Save** to save the setting.
Undo	Button	Click **Undo** to cancel the changes to settings.

Table 168 – Enable URL Blocking

6.2.2.3 Create/Edit Packet Filter Rules

When ☑ **Enable** is selected, the buttons on the **Packet Filter List** section become active.

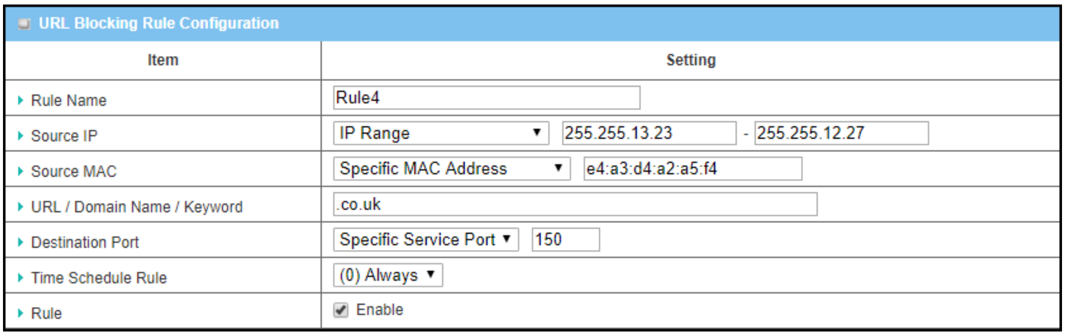


URL Blocking Rule List [Add] [Delete]

ID	Rule Name	Source IP	Source MAC	URL / Domain Name / Keyword	Destination Port	Time Schedule	Enable	Actions
1	Rule1	Any	Any	www.gogle.com	Any	(0) Always	☐	Edit ☐ Select
2	Rule2	Any	Any	.gov	Any	(0) Always	☑	Edit ☐ Select
3	Rule3	Any	Any	.edu	Any	(0) Always	☑	Edit ☐ Select

Figure 277 – URL Blocking Rule List

Click on the **Add** button to create a new rule in the list. You can add up to twenty (20) **URL Blocking** rules.



URL Blocking Rule Configuration

Item	Setting
Rule Name	Rule4
Source IP	IP Range ▾ 255.255.13.23 - 255.255.12.27
Source MAC	Specific MAC Address ▾ e4:a3:d4:a2:a5:f4
URL / Domain Name / Keyword	.co.uk
Destination Port	Specific Service Port ▾ 150
Time Schedule Rule	(0) Always ▾
Rule	☑ Enable

Figure 278 – URL Blocking Rule Configuration

Item	Notes	Description
Rule Name	Mandatory field. String format.	Enter a meaningful name of up to 30 characters for the URL blocking rule.
Source IP	Mandatory field. Default setting: Any	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 from the drop down list to filter packets coming from the selected group. **Note** – Groups must be pre-defined before this selection become available in the drop down list. Refer to Object Definition > Grouping > Host grouping. Alternatively, click the Add Rule button that displays when this drop down list is empty to create a new group.
Source MAC	Mandatory field. Default selection: Any	This field specifies the source MAC address or addresses. Select Any to filter packets coming from any MAC address. Select Specific MAC Address to filter packets coming from a MAC address entered in this field.

Item	Notes	Description
		Select MAC Address-based Group from the drop down list to filter packets coming from the selected group. **Note** – Groups must be pre-defined before this selection become available in the drop down list. Refer to Object Definition > Grouping > Host grouping. Alternatively, click the Add Rule button that displays when this drop down list is empty to create a new group.
URL / Domain Name / Keyword	Mandatory field. Default selection: Any	Specify the URL, Domain Name, or Keyword to be included in the URL blocking rule. Use the delimiter ";" to include a maximum of ten (10) Keywords in a rule string. 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 do not match any rule will be dropped.
Destination Port	Mandatory field. Default selection: Any	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 the Port number (1 - 65535) entered in this field. Select Port Range to filter packets going to a specific range of Ports entered in the 'from' and 'to' fields.
Time Schedule	Mandatory field.	Select a Time Schedule from the drop down list to apply to this rule or leave it as Always (i.e. without a time parameter). If the drop down list is empty you will need to define a Time Schedule using the Object Definition > Scheduling > Configuration tab.
Rule	Disabled by default.	Click ☑ **Enable** to activate this rule then save the settings.
Save	Button	Click **Save** to save the settings.
Undo	Button	Click **Undo** to cancel the settings.
Back	Button	When the **Back** button is clicked the screen will return to the Packet Filter Configuration page.

Table 169 – URL Blocking Rule Configuration

6.2.3 Content Filter

The **Content Filter** function can block HTML requests with some specific file name extensions such as ".exe", ".bat" (applications), "mpeg" (video), and so on. It can also block HTML requests containing certain script types, like Java Applets, Java Script code, cookies and Active X.

In addition, Content Filter blocking activity can be logged, monitored and reported.

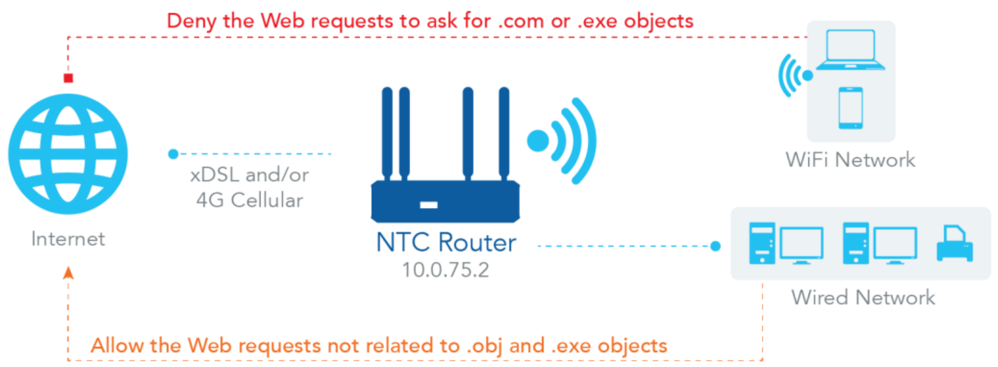

Deny the Web requests to ask for .com or .exe objects
Internet
xDSL and/or
4G Cellular
NTC Router
10.0.75.2
WiFi Network
Wired Network
Allow the Web requests not related to .obj and .exe objects

Figure 279 – Content filter

6.2.3.1 Content Filter Scenario

When the administrator of the gateway wants to block Web requests for dedicated contents or objects, they can use the "Web Content Filters" function.

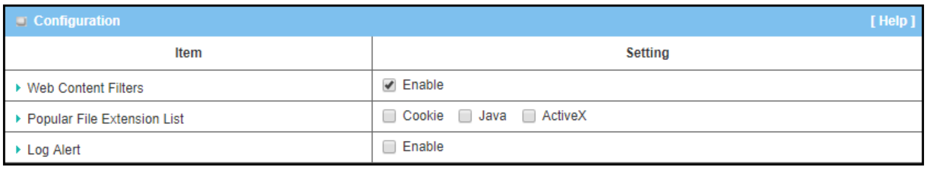
As shown in the diagram above, enable the Web content filters function to check and filter out Web requests on Cookies, Java and ActiveX objects then define further objects in the “Web Content Filter List” that may include extension ".exe" and ".com". The system will block requests containing objects with extension ".exe" or ".com".

6.2.3.2 Content Filter Settings

To enable the Content Filter functionality:

1 Select **Firewall** from the **Security** submenu on the left and then open the **Content Filter** tab.

2 Go to the **Configuration** section of the **Content Filter** page:



Configuration [Help]

Item	Setting
Web Content Filters	☑ Enable
Popular File Extension List	□ Cookie □ Java □ ActiveX
Log Alert	□ Enable

Figure 280 – Enable Web content Filters

3 Click **Content Filter** ☑ **Enable** and set the following parameters:

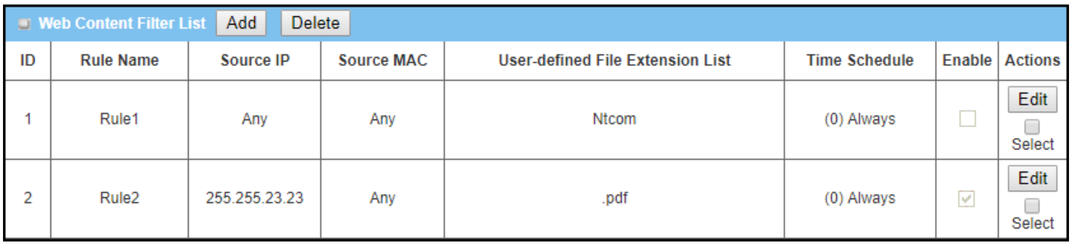
Item	Notes	Description
Web Content Filters	Checkbox, disabled by default.	Check ☑ Enable to activate the Content Filter functionality.
Popular File Extension List	Multiple selection boxes. By default none are selected.	☑ **Cookie** – Select to activate this pattern matching rule which filters out packets containing the keyword: ‘**Cookie:**’ ☑ **Java** – Select to activate this pattern matching rule which filters out packets containing any of the following keywords: **.js**, **.class**, **.jar**, **.jsp**, **.java**, **.jse**, **.jcm**, **.jtk** or **.jad** ☑ **ActiveX** – Select to activate this pattern matching rule which filters out packets containing any of the

Item	Notes	Description
		following keywords: **.ocx**, **.cab**, **.ole**, **.olb**, **.com**, **.vbs**, **.vrm** or **.viv** When selected if any one of the matching criteria is found it a packet, it packets will be dropped.
Log Alert	Disabled by default	Check Log Alert ☑ **Enable** to activate event logging for the selected rules.
Save	Button	Click **Save** to save the setting.
Undo	Button	Click **Undo** to cancel the changes to settings.

Table 170 – Enable Web content Filters

6.2.3.3 Create/Edit Content Filter Rules

When ☑ **Enable** is selected, the buttons on the **Content Filter List** section become active.

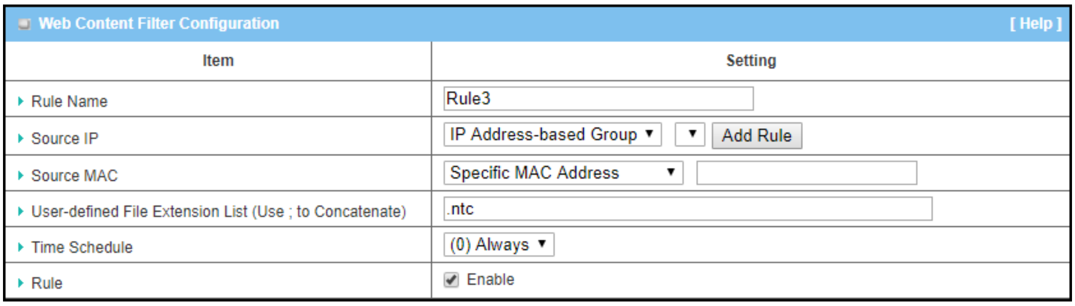


Web Content Filter List Add Delete

ID	Rule Name	Source IP	Source MAC	User-defined File Extension List	Time Schedule	Enable	Actions
1	Rule1	Any	Any	Ntcom	(0) Always	□	Edit □ Select
2	Rule2	255.255.23.23	Any	.pdf	(0) Always	☑	Edit □ Select

Figure 281 – Web Content Filter List

Click on the **Add** button to create a new rule in the list. You can add up to twenty (20) **Content Filter** rules.



Web Content Filter Configuration [Help]

Item	Setting
Rule Name	Rule3
Source IP	IP Address-based Group ▾ ▾ Add Rule
Source MAC	Specific MAC Address ▾
User-defined File Extension List (Use ; to Concatenate)	.ntc
Time Schedule	(0) Always ▾
Rule	☑ Enable

Table 171 – Web Content Filter List

Item	Notes	Description
Rule Name	Mandatory field. String format.	Enter a meaningful name of up to 30 characters for the Content Filter rule.
Source IP	Mandatory field. Default setting: **Any**	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 from the drop down list to filter packets coming from the selected group.

Item	Notes	Description
		Note – Groups must be pre-defined before this selection become available in the drop down list. Refer to Object Definition > Grouping > Host grouping. Alternatively, click the Add Rule button that displays when this drop down list is empty to create a new group.
Source MAC	Mandatory field. Default selection: **Any**	This field specifies the source MAC address or addresses. Select Any to filter packets coming from any MAC address. Select Specific MAC Address to filter packets coming from a MAC address entered in this field. Select MAC Address-based Group from the drop down list to filter packets coming from the selected group. **Note** – Groups must be pre-defined before this selection become available in the drop down list. Refer to **Object Definition > Grouping > Host grouping**. Alternatively, click the **Add Rule** button that displays when this drop down list is empty to create a new group.
User defined File Extension List	Mandatory field.	Specify a file extension list for the content filter rule. Use the delimiter ";" to list up to a maximum of ten (10) file extensions.
Time Schedule	Mandatory field.	Select a Time Schedule from the drop down list to apply to this rule or leave it as Always (i.e. without a time parameter). If the drop down list is empty you will need to define a Time Schedule using the Object Definition > Scheduling > Configuration tab.
Rule	Disabled by default.	Click ☑ **Enable** to activate this rule then save the settings.
Save	Button	Click **Save** to save the settings.
Undo	Button	Click **Undo** to cancel the settings.
Back	Button	When the **Back** button is clicked the screen will return to the **Content Filter Configuration** page.

Table 172 – Web Content Filter List

6.2.4 MAC Control

The **MAC Control** function allows you to assign the accessibility to the router for different users based on device's MAC (Media Access Control) address. You can define up to twenty (20) MAC Control Rules which are designated as either **Black Lists** or **White Lists**.

When designated as a **Black List** all the MAC addresses in enabled rules will be prevented from accessing the router.

When designated as a **White List** all the MAC addresses in enabled rules will be allowed to access the router.

In addition, MAC Control activity can be logged, monitored and reported.

6.2.4.1 MAC Control with Black List Scenario

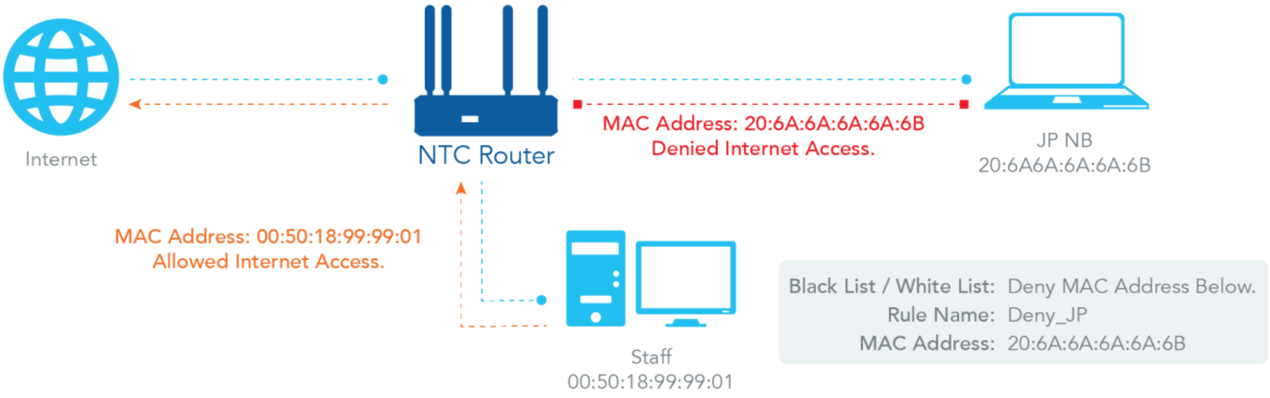

Internet
NTC Router
MAC Address: 20:6A:6A:6A:6A:6B
Denied Internet Access.
JP NB
20:6A6A:6A:6A:6B
MAC Address: 00:50:18:99:99:01
Allowed Internet Access.
Staff
00:50:18:99:99:01
Black List / White List: Deny MAC Address Below.
Rule Name: Deny_JP
MAC Address: 20:6A:6A:6A:6A:6B

Figure 282 – MAC Control with Black List Scenario

As shown in the diagram above, enable the MAC control function and specify the "MAC Control Rule List" as a black list, and configure one MAC control rule for the router to deny the connection request from the "JP NB" with its own MAC address 20:6A:6A:6A:6A:6B.

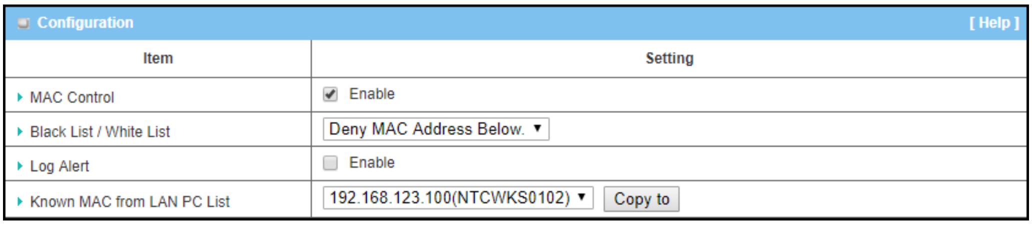
The system will block the connection from "JP NB" to the router but allow others.

6.2.4.2 MAC Control Settings

To enable the MAC Control functionality:

1 Select **Firewall** from the **Security** submenu on the left and then open the **MAC Control** tab.

2 Go to the **Configuration** section of the **MAC Control** page:



Configuration [Help]

Item	Setting
MAC Control	☑ Enable
Black List / White List	Deny MAC Address Below. ▼
Log Alert	□ Enable
Known MAC from LAN PC List	192.168.123.100(NTCWKS0102) ▼ Copy to

Figure 283 – Enable MAC Control

3 Click **MAC Control ☑ Enable** and set the following parameters:

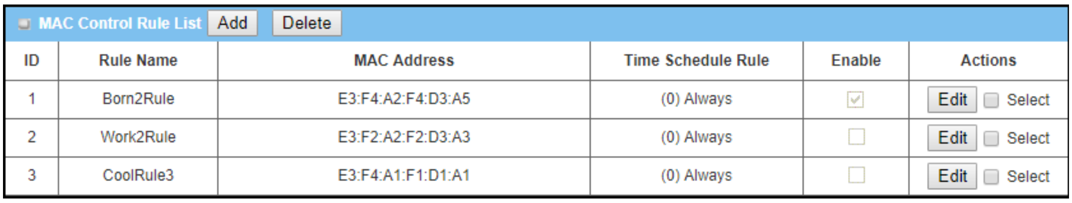
Item	Notes	Description
MAC Controls	Checkbox, disabled by default.	Check ☑ Enable to activate the MAC Control functionality.
Black List / White List	Drop down list Deny those match the following rules is the default setting.	When Deny those match the following rules is selected packets that meet the criteria of the rule will be blocked – "black listed"– and any other packets will be allowed to pass. In contrast, Allow those matching the following rules will allow those packets that meet the criteria of the rule to pass, i.e. those that are part of the "White List", and the rest will be blocked.

Item	Notes	Description
Log Alert	Disabled by default	Check **Log Alert** ☑ **Enable** to activate event logging for the selected rules.
Known MAC from LAN PC List	Text Entry box and Button	Select a MAC Address from LAN Client List and paste it into the text entry box. Click the Copy to button to copy the selected MAC Address into the filter rule.
Save	Button	Click **Save** to save the setting.
Undo	Button	Click **Undo** to cancel the changes to settings.

Table 173 – Enable MAC Control

6.2.4.3 Create/Edit MAC Control Rules

When ☑ **Enable** is selected, the **Add** and **Delete** buttons on the **MAC Control List** section become active.

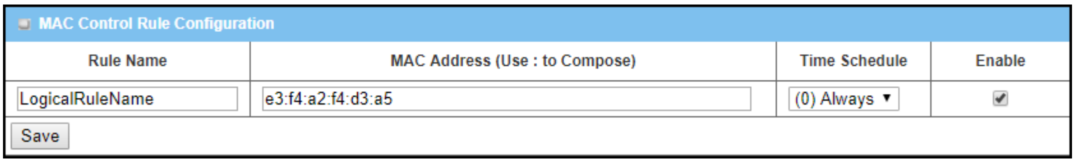


MAC Control Rule List

ID	Rule Name	MAC Address	Time Schedule Rule	Enable	Actions
1	Born2Rule	E3:F4:A2:F4:D3:A5	(0) Always	☑	Edit □ Select
2	Work2Rule	E3:F2:A2:F2:D3:A3	(0) Always	□	Edit □ Select
3	CoolRule3	E3:F4:A1:F1:D1:A1	(0) Always	□	Edit □ Select

Figure 284 – MAC Control List

Click on the **Add** button to create a new rule in the list. You can add up to twenty (20) **MAC Control** rules.



MAC Control Rule Configuration

Rule Name	MAC Address (Use : to Compose)	Time Schedule	Enable
LogicalRuleName	e3:f4:a2:f4:d3:a5	(0) Always ▼	☑

Figure 285 – MAC Control Rule Configuration

Item	Notes	Description
Rule Name	Mandatory field. String format.	Enter a meaningful name of up to 30 characters for the MAC Control rule.
MAC Address	Mandatory field.	Enter the source **MAC address** of the device affected by the rule. Use colons (:) to separate the six octets in the MAC address.
Time Schedule	Mandatory field.	Select a **Time Schedule** from the drop down list to apply to this rule or leave it as **Always** (i.e. without a time parameter). If the drop down list is empty you will need to define a Time Schedule using the **Object Definition > Scheduling > Configuration** tab.
Enable	Disabled by default.	Click ☑ **Enable** to activate this rule then save the settings.
Save	Button	Click **Save** to save the settings.
Undo	Button	Click **Undo** to cancel the settings.

Item	Notes	Description
Back	Button	When the **Back** button is clicked the screen will return to the **MAC Control Configuration** page.

Table 174 – MAC Control Rule Configuration

6.2.5 Application Filter

The Application Filter function can categorize Internet Protocol packets based on their application layer data and allow or deny access to the router. The tool contains specific application filters for various Internet chat software, P2P download, Proxy, and A/V streaming applications. In addition, MAC Control activity can be logged, monitored and reported.

6.2.5.1 Application Filter Scenario

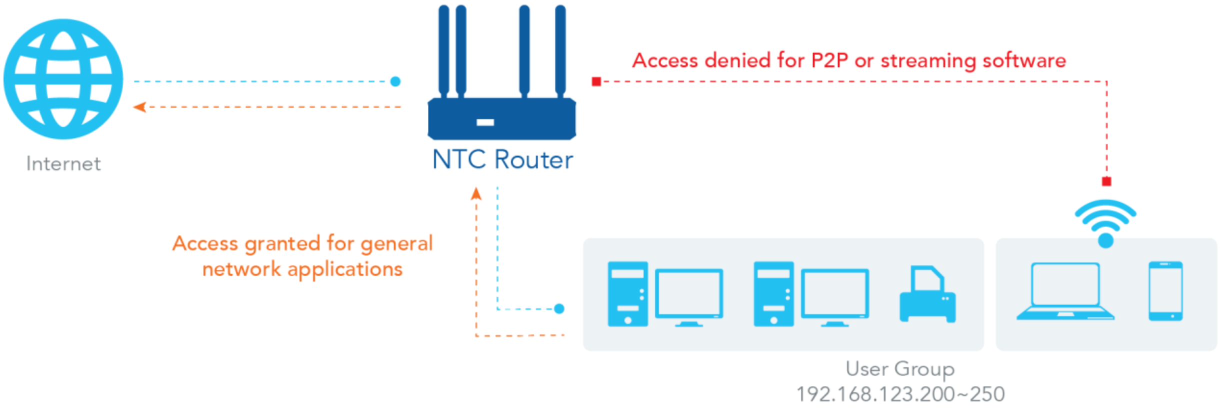

Internet
NTC Router
Access denied for P2P or streaming software
Access granted for general network applications
User Group
192.168.123.200~250

Figure 286 – Application Filter Scenario

When the administrator of the gateway wants to block some P2P or Stream applications, he can use the "Application Filters" function.

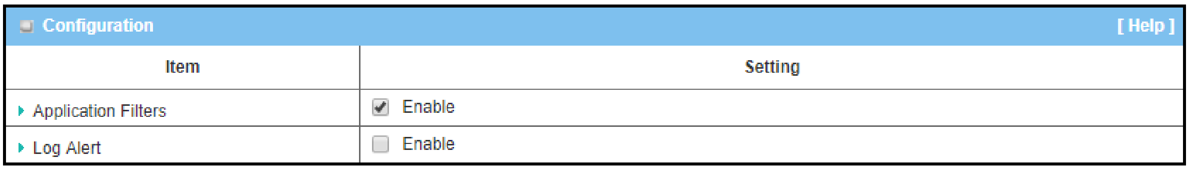
As shown in the diagram, the Gateway is the gateway as a NAT router. Specify IP Range 192.168.123.200~250, and enable the Application filters function “BT(BitTorrent, BitSpirit, BitComet)”, “MMS”, “RTSP”, “PPStream”, “PPSLive” and “Qvcd” by checking the "Enable" box. The gateway will block those applications to internet.

6.2.5.2 Application Filter Settings

To enable the Application Filter functionality:

1 Select **Firewall** from the **Security** submenu on the left and then open the **Application Filter** tab.

2 Go to the **Configuration** section of the **Application Filter** page:



Configuration [Help]

Item	Setting
Application Filters	☑ Enable
Log Alert	□ Enable

Figure 287 – Enable Application Filter

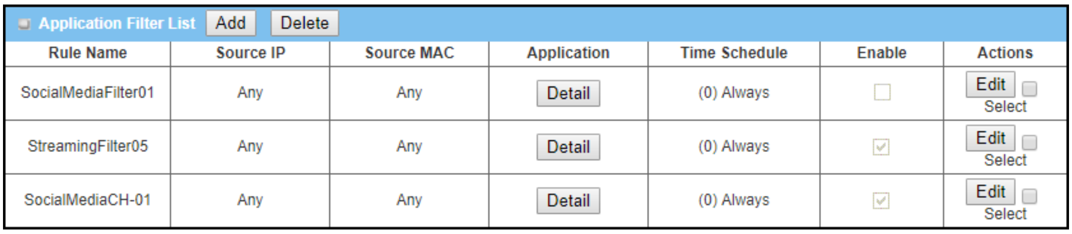
3 Click **Application Filter ☑ Enable** and set the following parameters:

Item	Notes	Description
Application Filter	Checkbox, disabled by default.	Check ☑ **Enable** to activate the Application Filter functionality.
Log Alert	Disabled by default	Check ☑ **Log Alert** to activate event logging for the selected rules.
Save	Button	Click **Save** to save the setting.
Undo	Button	Click **Undo** to cancel the changes to settings.

Table 175 – Enable Application Filter

6.2.5.3 Create/Edit Application Filter Rules

When ☑ **Enable** is selected, the buttons on the **Application Filter List** section become active.

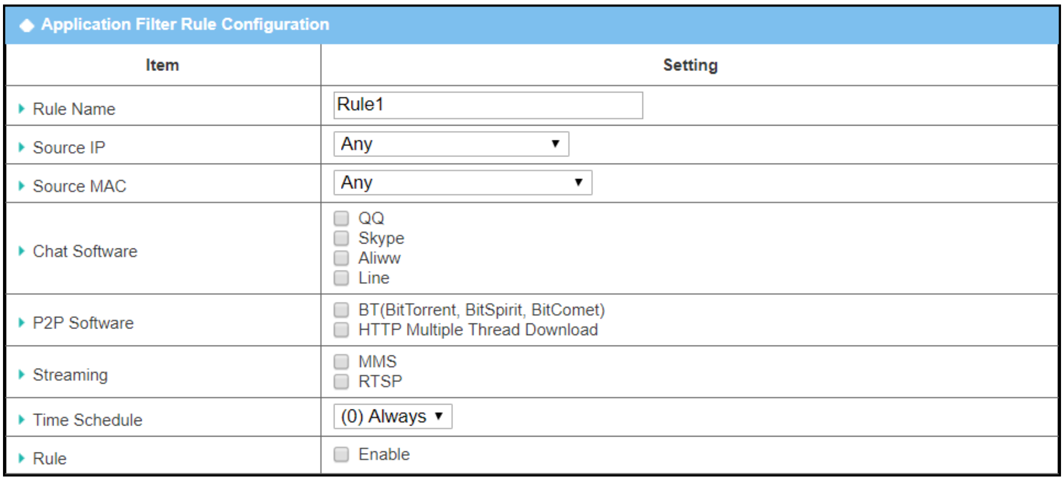


Application Filter List [Add] [Delete]

Rule Name	Source IP	Source MAC	Application	Time Schedule	Enable	Actions
SocialMediaFilter01	Any	Any	Detail	(0) Always	□	Edit □ Select
StreamingFilter05	Any	Any	Detail	(0) Always	☑	Edit □ Select
SocialMediaCH-01	Any	Any	Detail	(0) Always	☑	Edit □ Select

Figure 288 – Application Filter List

Click on the **Add** button to create a new rule in the list. You can add up to twenty (20) **Application Filter** rules.

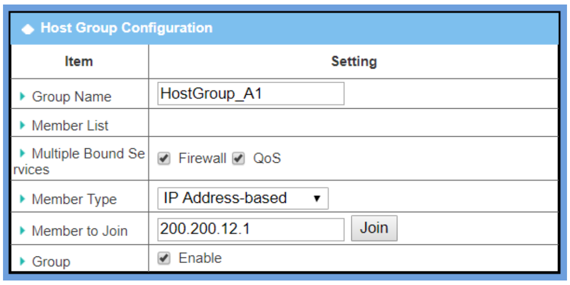


Application Filter Rule Configuration

Item	Setting
Rule Name	Rule1
Source IP	Any ▾
Source MAC	Any ▾
Chat Software	□ QQ □ Skype □ Aliww □ Line
P2P Software	□ BT(BitTorrent, BitSpirit, BitComet) □ HTTP Multiple Thread Download
Streaming	□ MMS □ RTSP
Time Schedule	(0) Always ▾
Rule	□ Enable

Figure 289 – Application Filter Rule Configuration

Item	Notes	Description
Rule Name	Mandatory field. String format.	Enter a meaningful name of up to 30 characters for the Application Filter rule.
Source IP	Mandatory field. Default setting: Any	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.

Item	Notes	Description
		Select IP Address-based Group from the drop down list to filter packets coming from the selected group. **Note** – Groups must be pre-defined before this selection become available in the drop down list. Refer to **Object Definition > Grouping > Host grouping**. Alternatively, click the **Add Rule** button that displays when this drop down list is empty to create a new group.
Source MAC	Mandatory field. Default selection: Any	This field specifies the source MAC address or addresses. Select **Any** to filter packets coming from any MAC address. Select **Specific MAC Address** to filter packets coming from a MAC address entered in this field. Select **MAC Address-based Group** from the drop down list to filter packets coming from the selected group. **Note** – Groups must be pre-defined before this selection become available in the drop down list. Refer to **Object Definition > Grouping > Host grouping**. Alternatively, click the **Add Rule** button that displays when this drop down list is empty to create a new group.  Host Group Configuration Item – Setting Group Name – HostGroup_A1 Member List – Multiple Bound Services – ☑ Firewall ☑ QoS Member Type – IP Address-based Member to Join – 200.200.12.1 Join Group – ☑ Enable
Chat Software	Multiple check boxes. All unselected by default.	Check one or more Chat Software application filter functions you want activate for this rule. Available chat applications include: **QQ, Facebook, Aliww** and **Line**
P2P Software	Multiple check boxes. All unselected by default.	Check one or more P2P Software application filter functions you want activate for this rule. Available P2P applications include: **BT**, **HTTP Multiple**, and **Thread Download**
Streaming	Multiple check boxes. All unselected by default.	Check one or more data Streaming application filter functions you want activate for this rule. Available streaming applications include: **MMS** or **RTSP**
Time Schedule	Mandatory field.	Select a **Time Schedule** from the drop down list to apply to this rule or leave it as Always (i.e. without a time parameter). If the drop down list is empty you will need to define a Time Schedule using the **Object Definition > Scheduling > Configuration** tab.
Rule	Disabled by default.	Click ☑ **Enable** to activate this rule then save the settings.
Save	Button	Click **Save** to save the settings.

Item	Notes	Description
Undo	Button	Click **Undo** to cancel the settings.
Back	Button	When the **Back** button is clicked the screen will return to the Packet Filter Configuration page.

Table 176 – Application Filter Rule Configuration

6.2.6 IPS

When the router is used to provide application server services over the Internet specific ports will need to remain open to support those services. Open service ports always entail the risk of security breaches and in order to mitigate these risks it is important to employ an Intrusion Prevention Systems (IPS) regime.

IPS are network security appliances that monitor network and/or system activities for malicious activity, log information about this activity, attempt to block/stop it and report it. Enable the NTC-400 Series Router's IPS function to periodically check some or all of the intrusion activities that it safeguards against. You can also enable the logging feature to record intrusion events as they are detected.

6.2.6.1 IPS Scenario

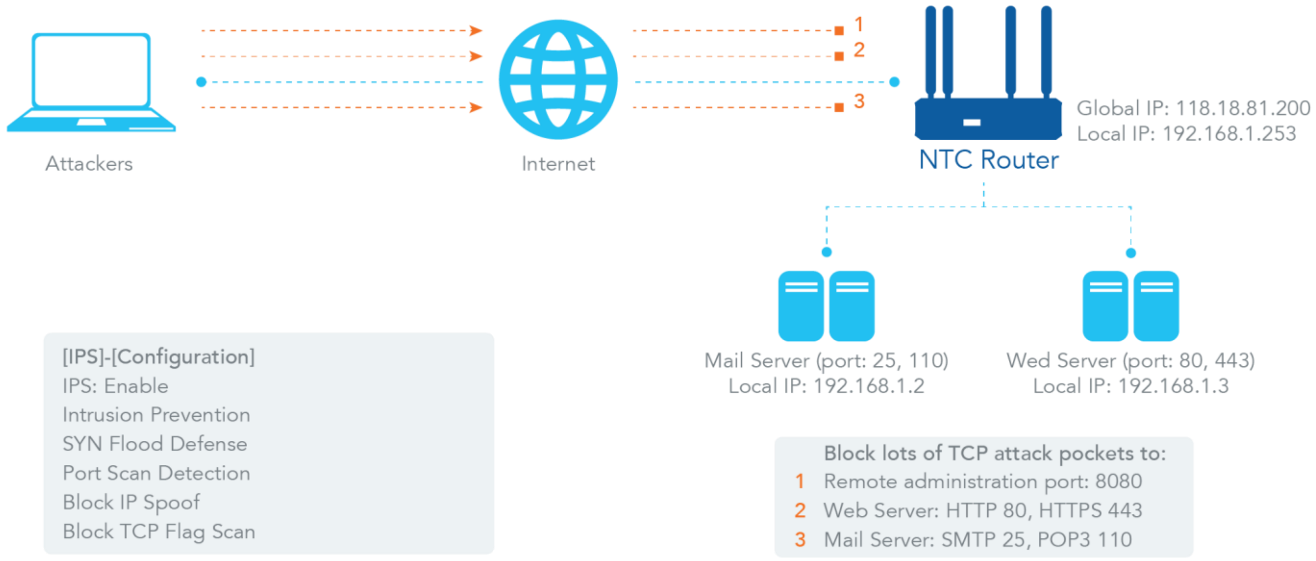


Figure 290 – IPS Scenario

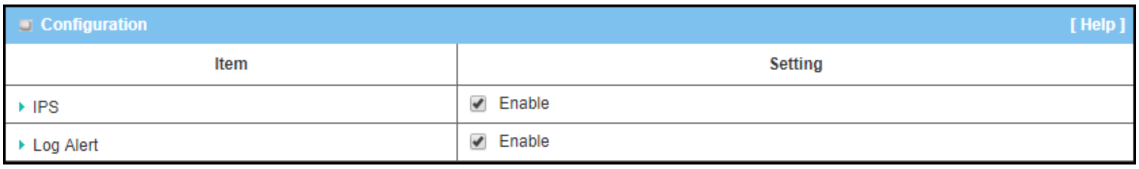
As shown in the diagram above, the router serves as an e-mail server, Web Server and also provides TCP port 8080 for remote administration. Remote users or unknown users can request those services from the Internet. With IPS enabled, the router can detect incoming attack packets, including the TCP ports (25, 80, 110, 443 and 8080) with services. It will block the attack packets and let the normal access to pass through the router.

6.2.6.2 IPS Settings

To enable the Intrusion Prevention System functionality:

1 Select **Firewall** from the **Security** submenu on the left and then open the **IPS** tab.

2 Go to the **Configuration** section of the **IPS** page:



Configuration [Help]

Item	Setting
IPS	☑ Enable
Log Alert	☑ Enable

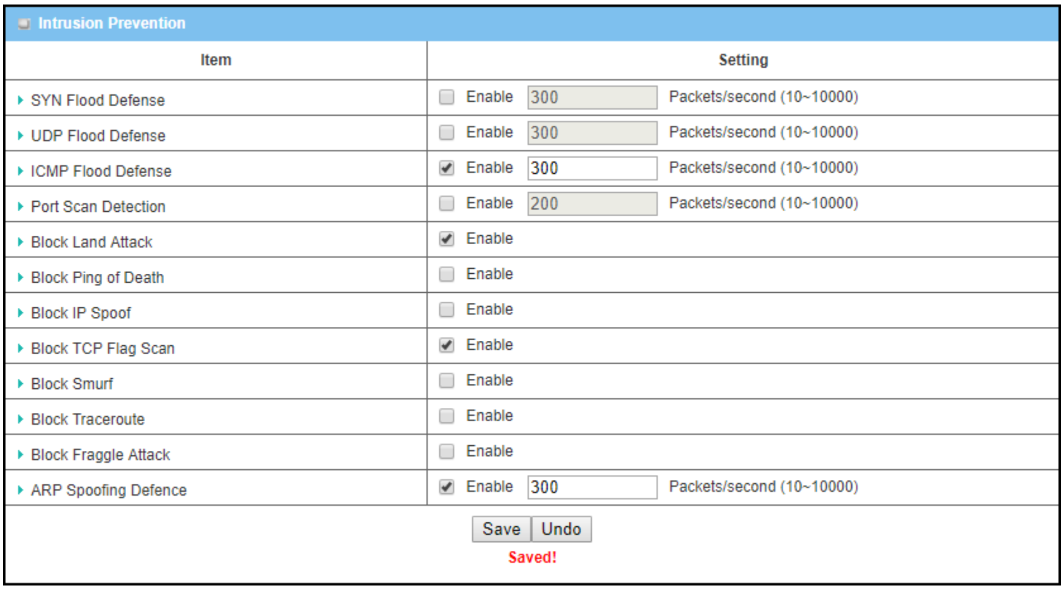
Figure 291 – Enable IPS

Item	Notes	Description
IPS	Checkbox, disabled by default.	Check ☑ **Enable** to activate the Intrusion Prevention System functionality.
Log Alert	Disabled by default	Check ☑ **Enable** to activate event logging for the selected threats and activities.
Save	Button	Click Save to save the setting.
Undo	Button	Click Undo to cancel the changes to settings.

Table 177 – Enable IPS

6.2.6.3 Create/Edit IPS Rules

When **IPS** ☑ **Enable** is selected, the checkboxes and parameter text boxes on the **Intrusion Prevention** section become active. Select the intrusion activities that you want to monitor.



Intrusion Prevention

Item	Setting
SYN Flood Defense	□ Enable 300 Packets/second (10~10000)
UDP Flood Defense	□ Enable 300 Packets/second (10~10000)
ICMP Flood Defense	☑ Enable 300 Packets/second (10~10000)
Port Scan Detection	□ Enable 200 Packets/second (10~10000)
Block Land Attack	☑ Enable
Block Ping of Death	□ Enable
Block IP Spoof	□ Enable
Block TCP Flag Scan	☑ Enable
Block Smurf	□ Enable
Block Traceroute	□ Enable
Block Fraggle Attack	□ Enable
ARP Spoofing Defence	☑ Enable 300 Packets/second (10~10000)

Saved!

Figure 292 – Intrusion Prevention Parameters

Item	Notes	Description
SYN Flood Defense	Mandatory field. Disabled by default. Default setting: 300	Click ☑ **Enable** to activate this intrusion prevention rule and enter the traffic threshold in this field. Value Range: 10 - 10000
UDP Flood Defense	Mandatory field. Disabled by default. Default setting: 300	Click ☑ **Enable** to activate this intrusion prevention rule and enter the traffic threshold in this field. Value Range: 10 - 10000

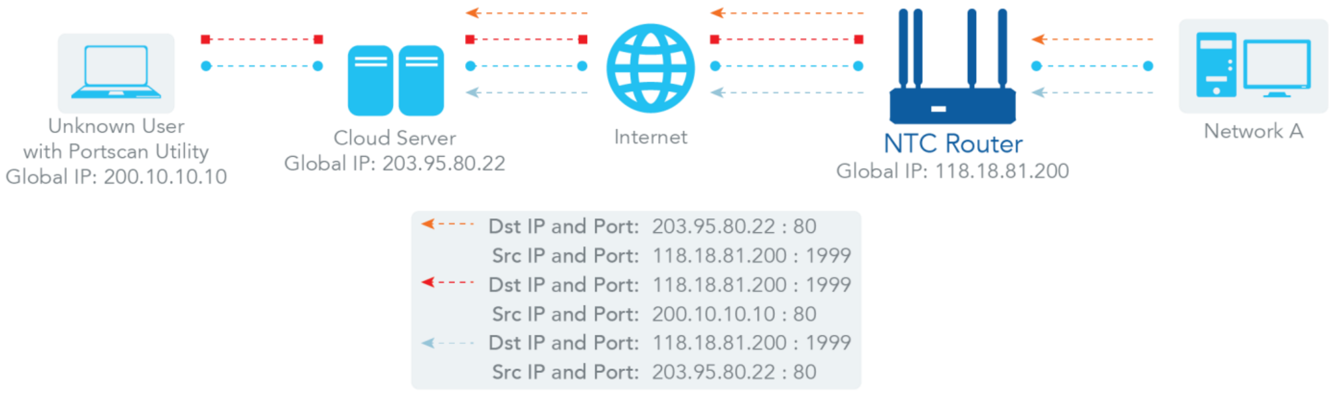
Item	Notes	Description
ICMP Flood Defense	Mandatory field. Disabled by default. Default setting: 300	Click ☑ **Enable** to activate this intrusion prevention rule and enter the traffic threshold in this field. Value Range: 10 - 10000
Port Scan Defection	Mandatory field. Disabled by default. Default setting: 200	Click ☑ **Enable** to activate this intrusion prevention rule and enter the traffic threshold in this field. Value Range: 10 - 10000
Block Land Attack	Optional setting. Disabled by default.	Click ☑ **Enable** to activate this intrusion prevention rule.
Block Ping of Death	Optional setting. Disabled by default.	Click ☑ **Enable** to activate this intrusion prevention rule.
Block IP Spoof	Optional setting. Disabled by default.	Click ☑ **Enable** to activate this intrusion prevention rule.
Block TCP Flag Scan	Optional setting. Disabled by default.	Click ☑ **Enable** to activate this intrusion prevention rule.
Block Smurf	Optional setting. Disabled by default.	Click ☑ **Enable** to activate this intrusion prevention rule.
Block Traceroute	Optional setting. Disabled by default.	Click ☑ **Enable** to activate this intrusion prevention rule.
Block Fraggle Attack	Optional setting. Disabled by default.	Click ☑ **Enable** to activate this intrusion prevention rule.
ARP Spoofing Defence	Mandatory field. Disabled by default. Default setting: **300**	Click ☑ **Enable** to activate this intrusion prevention rule and enter the traffic threshold in this field. Value Range: 10 - 10000
Save	Button	Click **Save** to save the settings.
Undo	Button	Click **Undo** to cancel the settings.

Table 178 – Intrusion Prevention

6.2.7 Options

The firewall options setting allows the network administrator to modify the behaviour of the firewall and to enable Remote Router Access Control.

6.2.7.1 Enable SPI Scenario



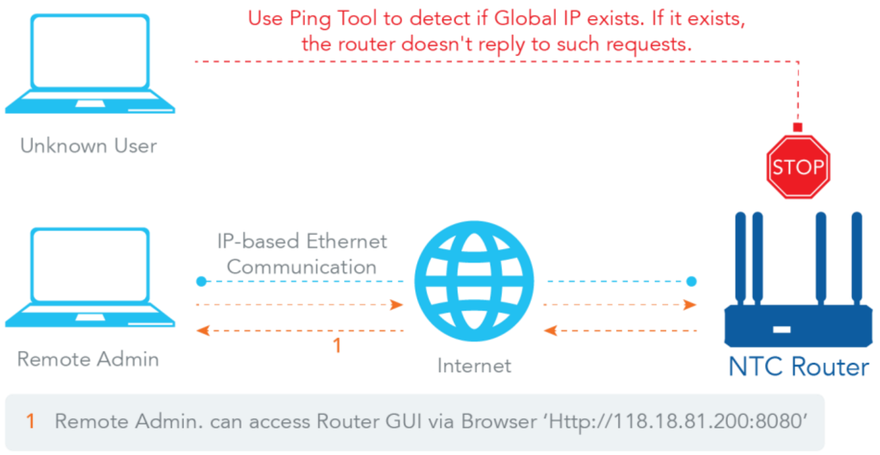
Dst IP and Port: 203.95.80.22 : 80
Src IP and Port: 118.18.81.200 : 1999
Dst IP and Port: 118.18.81.200 : 1999
Src IP and Port: 200.10.10.10 : 80
Dst IP and Port: 118.18.81.200 : 1999
Src IP and Port: 203.95.80.22 : 80

Fig 300 - Enable SPI Scenario

Figure 293 – Enable SPI Scenario

As shown in the diagram above, the router has the IP address of 118.18.81.200 for the WAN interface and 192.168.1.253 for the LAN interface. It serves as a NAT gateway. Users in Network-A initiate to access the cloud server through the router. Sometimes unknown users will simulate the packets but use different source IP addresses to masquerade. With the SPI feature enabled on the router, it will block such packets from unknown users.

6.2.7.2 Allow Ping from WAN & Remote Administrator Hosts Scenario


Use Ping Tool to detect if Global IP exists. If it exists,
the router doesn't reply to such requests.
Unknown User
STOP
IP-based Ethernet
Communication
Remote Admin
1
Internet
NTC Router

1 Remote Admin. can access Router GUI via Browser 'Http://118.18.81.200:8080'

Figure 294 - Allow Ping from WAN & Remote Administrator Hosts Scenario

By default ☐ **Allow Ping from WAN** is disabled, this setting prevents security leaks when local users access the internet.

Selecting ☑ **Allow Ping from WAN** specifically allows any host on the WAN side to be able to receive a reply to any ICMP (ping) packets.

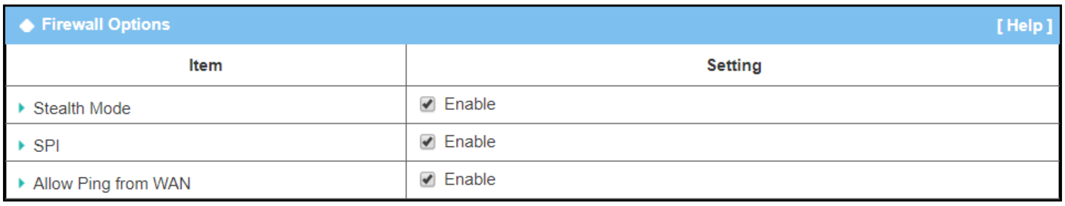
The Remote administrator knows the gateway's global IP, and he can access the Gateway GUI via TCP port 8080.

6.2.7.3 Firewall options

To enable the Intrusion Prevention System functionality:

1 Select **Firewall** from the **Security** submenu on the left and then open the **Options** tab.

2 Go to the **Firewall Options** section of the Options page:



◆ Firewall Options [Help]

Item	Setting
▸ Stealth Mode	☑ Enable
▸ SPI	☑ Enable
▸ Allow Ping from WAN	☑ Enable

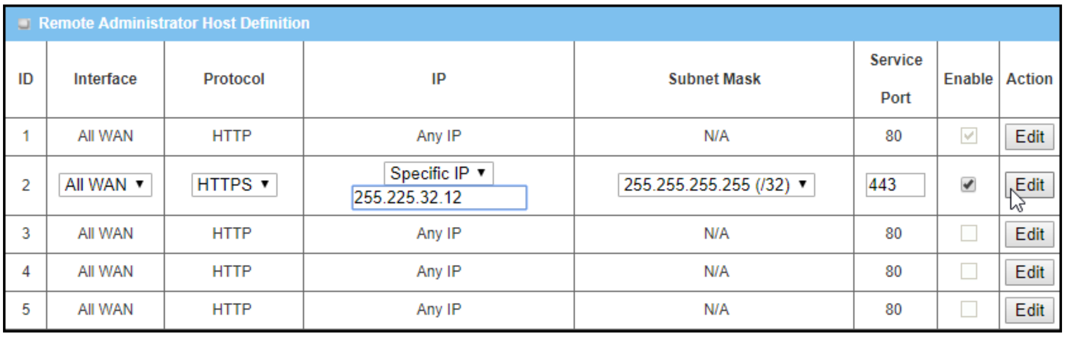
Figure 295 – Firewall Options

Item	Notes	Description
Stealth Mode	Checkbox, ☐disabled by default.	Stealth Mode turns off the router's response to port scans from the WAN making it less susceptible to discovery and attack. Check ☑ **Enable** to activate the Stealth Mode functionality.
SPI	Checkbox, ☑ enabled by default.	SPI enables the router to check that every incoming packet is valid and to record packet information such as IP address, port address, ACK, SEQ, etc. while they pass through the router. Uncheck ☐ **Enable** to deactivate the SPI functionality.
Allow Ping from WAN	Checkbox, ☐ disabled by default.	When disabled, hosts on the WAN side cannot ping the NTC-400. Check ☑ **Enable** to allow any host on the WAN side to ping this router.
Save	Button	Click **Save** to save the setting.
Undo	Button	Click **Undo** to cancel the changes to settings.

Table 179 – Firewall Options

6.2.7.4 Edit Access Rules

When ☑ **Enable** is selected, the checkboxes and parameter text boxes on the **Remote Administrator Host Definition** section become active. Select the WAN interfaces that you want to monitor.



Remote Administrator Host Definition

ID	Interface	Protocol	IP	Subnet Mask	Service Port	Enable	Action
1	All WAN	HTTP	Any IP	N/A	80	☑	Edit
2	All WAN ▾	HTTPS ▾	Specific IP ▾ 255.225.32.12	255.255.255.255 (/32) ▾	443	☑	Edit
3	All WAN	HTTP	Any IP	N/A	80	☐	Edit
4	All WAN	HTTP	Any IP	N/A	80	☐	Edit
5	All WAN	HTTP	Any IP	N/A	80	☐	Edit

Figure 296 – Remote Administrator Host Definition

Item	Notes	Description
ID	Integer	Reference number.
Interface	Mandatory field. All WAN is the default setting.	Select the appropriate WAN interface.
Protocol	Mandatory field. Default setting: **HTTP**	Select either **HTTP** or **HTTPS** as the method for accessing the router.
IP	Mandatory field. Default setting: **Any IP**	Identifies remote hosts that have access rights for remote access. **Any IP** – This setting will allow access to any remote host. **Specific IP** – This setting will allow access only to a remote host coming from a specific subnet. Enter the IP address of the remote host and then select the Subnet Mask used to compose the subnet, see next.
Subnet Mask	Mandatory field. Default setting: **N/A**	If IP is set to **Any IP** this setting is: **N/A** When IP is set to Specific IP, the user must select the **Subnet Mask** of the IP address from the drop down list.
Service Port	Mandatory field. Default port for HTTP: **80** Default port for HTTPS: **443**	Specify a Service Port for an HTTP or HTTPS connection. Value Range: **1 - 65535**
Enable	Checkbox	Click ☑ **Enable** to activate this
Action	Edit Button	Click **Edit** to display text entry boxes for changing the parameters of the Host Definition in that row. Make the required changes and click Save to apply them.
Save	Button	Click **Save** to save the settings.
Undo	Button	Click **Undo** to cancel the settings.

Table 180 – Remote Administrator Host Definition

6.3 Authentication

Use either the Captive Portal or MAC Authentication tools to set up a Wi-Fi Hotspot using the NTC-400 Series Router router.

6.3.1 Captive Portal

A captive portal, also known as a gateway, is a portal web page that is displayed before a user can browse Internet through your router. The portal is often used to present a login web page which can include an authentication process and/or payment, or simply display an acceptable use policy and require the user to agree. Captive portals are used to provide Wi-Fi hotspot services or can be used to control wired access, for example: apartment buildings, hotel rooms, business premises, "open" Ethernet jacks, etc.

The gateway supporting the Captive Portal function can be implemented via two approaches: **External Web Portal** or **Internal Web Portal**

For an external captive portal, you must specify an external RADIUS (Remote Authentication Dial In User Service) server and an external UAM (Universal Access Method) server. In contrast, the internal captive portal uses the “Internal RADIUS Server” option for user authentication. The user account database can be an embedded database, an external AD database or an external LDAP database. However, the UAM server is not necessary for this case and that the captive portal Web site is embedded in the device.

External Captive Portal

For external captive portal, you must specify an external RADIUS (Remote Authentication Dial In User Service) server and external UAM (Universal Access Method) server.

Before enabling the external Captive Portal function, Go to **[Object Definition]-[External Server]** to setup external server objects, like RADIUS server and UAM server. Return to this page to configure the Captive Portal function for the specific WAN Interface. Select external Authentication Server and UAM Server from the pre-defined external server object list.

Internal Captive Portal

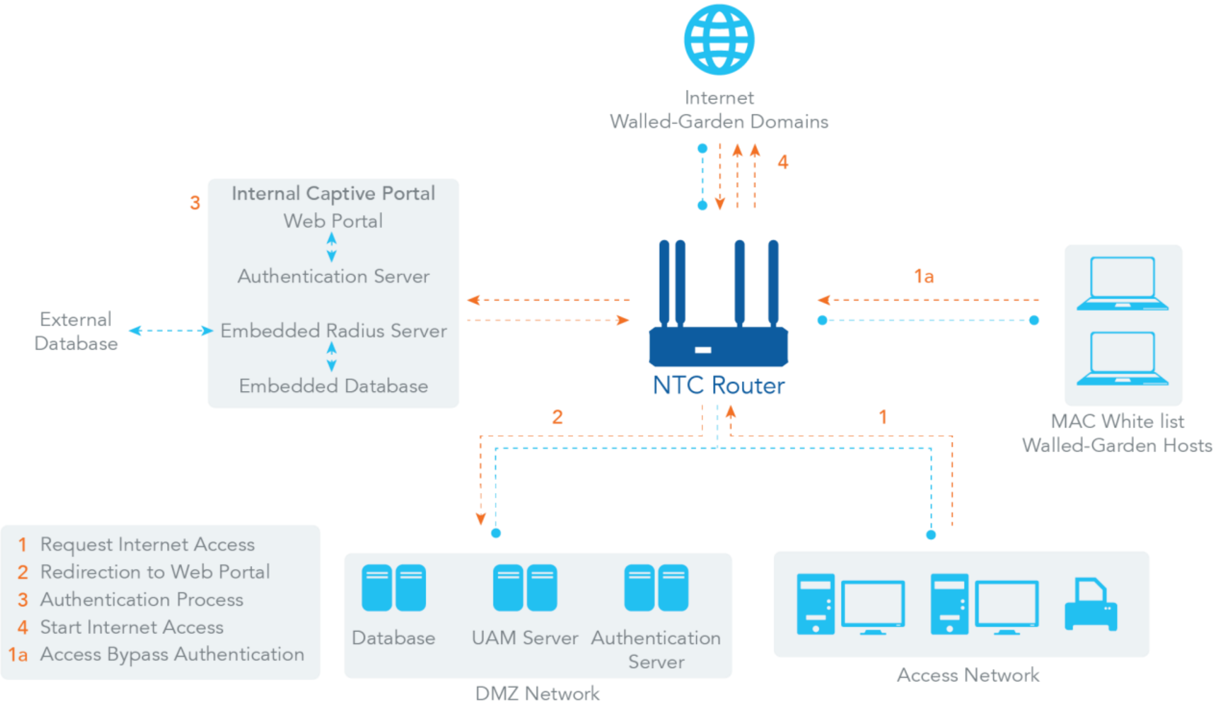


Figure 297 – Internal Captive Portal

In contrast, for an internal captive portal, you will only select “Internal RADIUS Server” option for user authentication. The user account database can be an embedded database, an external AD database or an external LDAP database. However, the UAM server is not necessary for this case and that the captive portal Web site is embedded in the device.

Before enabling the internal Captive Portal function, Go to **[Object Definition]-[External Server]** to define external server objects, like LDAP server or AD server if necessary. Return to this page to configure the Captive Portal function for a specific WAN Interface. Select the “Internal RADIUS Server” option for user authentication and specify its user database to be the embedded one, an external LDAP server or an external AD server from the pre-defined external server object list.

> **Note** – All Internet Packets will be forwarded to the Captive Portal page of the router when the Captive portal feature is enabled. Please make sure that at least one user account is created.

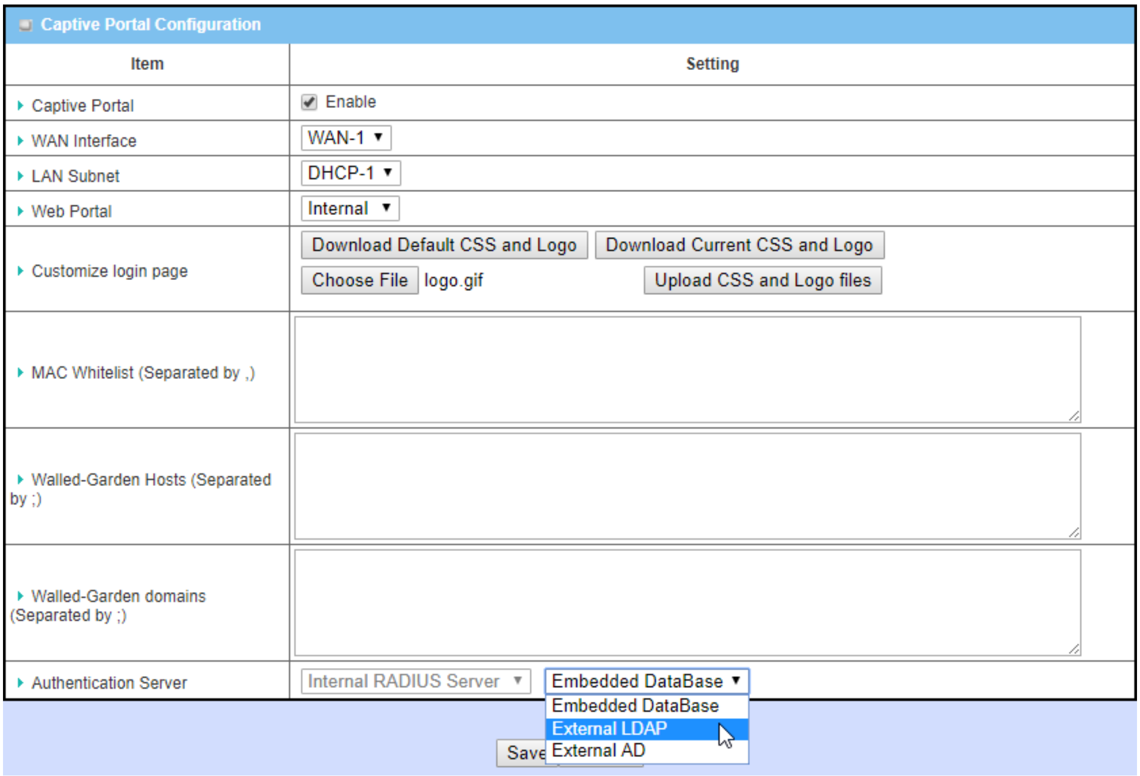
When the user authentication process completes successfully, the router redirects the web page to the requested one. The router also records the MAC address of the guest client host and allows its incoming Internet access requests.

Each account has its own lease time and it will not be reused for authentication once the lease time has run out. The client host with that account will be rejected to access the Internet. However, there is a timeout setting for each account. When the client host with that account has been idle the timeout setting, the router will re-authenticate the client host for further Internet connections.

6.3.1.1 Captive Portal settings

To set up a Captive Portal, select **Authentication** from the **Security** submenu on the left and then open the **Captive Portal** tab.

The options available in the **Captive Portal Configuration** page depend on whether Internal or External Web Portal is selected:



Captive Portal Configuration

Item	Setting
Captive Portal	☑ Enable
WAN Interface	WAN-1
LAN Subnet	DHCP-1
Web Portal	Internal
Customize login page	Download Default CSS and Logo · Download Current CSS and Logo Choose File logo.gif · Upload CSS and Logo files
MAC Whitelist (Separated by ,)	
Walled-Garden Hosts (Separated by ;)	
Walled-Garden domains (Separated by ;)	
Authentication Server	Internal RADIUS Server · Embedded DataBase

Figure 298 – Captive Portal Configuration

Item	Notes	Description
Captive Portal	Disabled by default.	Check ☑ Enable to activate the Captive Portal function.
WAN Interface	Mandatory field Default setting: **WAN-1**	Specify a WAN Interface for the authenticated clients or hosts. All traffic coming from the hosts will be directed to the specified WAN interface.
LAN Subnet	Mandatory field Default setting: **DHCP-1**	Specify the LAN subnet which is to be bound with captive portal function. It can be **DHCP-1 - DHCP-4**, if you have configured additional DHCP servers in **Basic Network > LAN & VLAN > DHCP Server**. If DHCP-1 is selected, users connected to the physical LAN port assigned to the DHCP-1 server will be re-directed to a login page when accessing the Internet.
Web Portal	Mandatory field	Specify which kind of authentication server is to be used for the captive portal function.

Item	Notes	Description
		Note – Depending on the router model purchased, the Internal captive portal may or may NOT be supported*, some models ONLY have the external option*. **Internal** – User must define the portal login page using the Customize login page tools and select an Authentication Server, see below. **External** – No Customize login page can be configured, the user must specify an external Authentication Server and UAM Server for authentication.
Customize login page	N/A	These tools are only available for Internal Web Portals, see previous setting. Click the **Download Default CSS and Logo** button to download the default CSS file and Logo of login page for the internal authentication server. Click the Download Current CSS and Logo button to download the current CSS file and Logo of login page for the internal authentication server. User can externally edit the CSS file or Logo downloaded from above buttons and then upload the altered files using the Upload CSS and Logo files button.
MAC Whitelist (Separated by,)	Optional setting	Specify a MAC whitelist for the client devices that will not be subjected to the captive portal authentication process. The MAC(s) listed here can directly access the Internet instead of being re-directed to the login page.
Walled-Garden Hosts (Separated by;)	Optional setting	Specify the host IP(s) for devices that will not be subjected to the captive portal authentication process. The IP(s) listed here can directly access the Internet instead of being re-directed to the login page.
Walled-Garden domains (Separated by;)	Optional setting	Specify the domain name(s) for the devices that will not be subjected to the captive portal authentication process. The domain names(s) listed here can directly access the Internet instead of being re-directed to the login page.
Authentication Server	Mandatory field	The type of authentication server and corresponding user database available will vary depending on whether Internal or External is selected above. Internal Web Portal The Internal RADIUS Server is used to authentication by default, and there are three databases you can choose from: **Embedded DataBase** – the login IDs and Passwords are created in Object Definition > User > User Profile tab. **External LDAP** – the login IDs and passwords are from an external LDAP server. Please specify it as well. **External AD**–The login IDs and passwords are from an external AD server. Please specify it as well. External Web Portal If Web Portal is External, user needs to specify an external RADIUS server. The external radius server can:

Item	Notes	Description
		1. Have been previously created at **Object Definition > External Server > External Server** tab and selected from the drop down list, or 2. Be defined by pressing **AddObject** button, entering its details in the **External Server Configuration** dialog and checking **Server** ☑ **Enabled**.
UAM Server	Mandatory field	UAM Server is available only when External Web Portal is selected. Click ☑ **Enable** and specify an external UAM server from the external server list. The UAM Server can: 1. Have been previously created at **Object Definition > External Server > External Server** tab and selected from the drop down list, or 2. Be defined by pressing **AddObject** button, entering its details in the **External Server Configuration** dialog and checking **Server** ☑ **Enabled**.
Save	Button	Click the **Save** button to save changes
Refresh	Button	Click the **Refresh** button to refresh current page

Table 181 – Captive Portal Configuration

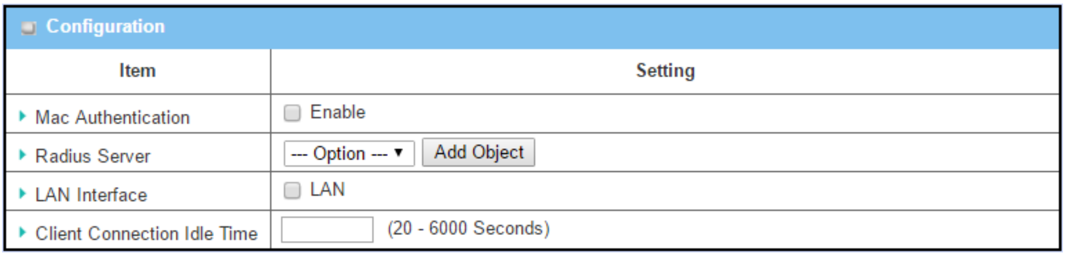
6.3.2 MAC Authentication

For some application, a RADIUS server is used to authenticate the Internet accessing permission. For those authorized devices (MACs), they are allowed to access internet, and on the other hand, for those not authorized devices, the internet accessing traffics will be blocked.

This gateway supports such MAC authentication function, the administrator has to configure the settings and create a permissible user account list for those authorized devices. When the MAC Authentication function is enabled, the traffics from the specified interface(s) will be applied with the MAC Authentication process transparently. The gateway will interact with the RADIUS server, and provide the corresponding user information for authentication process.

6.3.2.1 MAC Authentication settings

To set up a Captive Portal, select **Authentication** from the **Security** submenu on the left and then open the **MAC Authentication** tab:



Configuration

Item	Setting
Mac Authentication	□ Enable
Radius Server	--- Option --- ▾ Add Object
LAN Interface	□ LAN
Client Connection Idle Time	(20 - 6000 Seconds)

Figure 299 – Enable MAC Authentication

Item	Notes	Description
MAC Authentication	Disabled by default.	Check ☑ **Enable** to activate the MAC Authentication function.
Radius Server	Mandatory field.	Specify an external RADIUS server for authentication.

Item	Notes	Description
		When the MAC Authentication is enabled, the gateway sends out the connecting client's information to the RADIUS server for authentication.
LAN Interface	Mandatory field. Default setting: **LAN**	Select the network interface(s) to apply the MAC Authentication function: LAN or VLAN(s) (port-based) **Note** – DO NOT choose the interface used by the RADIUS server.
Client Connection Idle Time	Mandatory field.	Specify the idle time (in seconds) for a client connection. If a client did not access network for the specified idle time period, its authentication will be deemed invalid and the connection terminated.
Save	Button	Click the **Save** button to save changes.
Refresh	Button	Click the **Refresh** button to refresh current page.

Table 182 – Enable MAC Authentication

6.3.2.2 Create/Edit User List

There is a User List for listing the information of the available users. Administrator can create, edit, delete, or even search with a certain key and filter function to quick access to the information you are looking for.

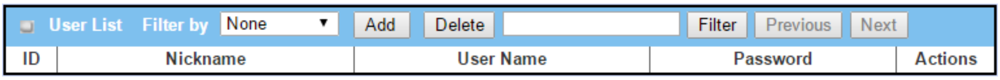
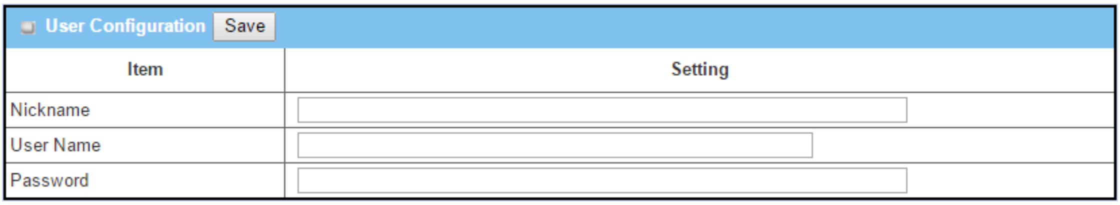


Figure 300 – User List

Item	Notes	Description
ID	Integer	Identification reference only.
Nickname	Any text string entry.	Displays the nickname for a user.
User Name	Any text string entry.	Displays the MAC address for a user.
Password	Any text string entry.	Displays the password for a user.
Add	Button	Add information of new device authentication
Delete	Button	Delete information of exists device authentication
Filter	Button	Search information of exists device authentication
Previous	Button	Navigation button of authentication list
Next	Button	Navigation button of authentication list

Table 183 – User List

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



Item	Setting
Nickname	
User Name	
Password	

Figure 301 – User Configuration

Item	Notes	Description
Nickname	Mandatory field. String format can be any text (max. 64 characters).	Enter a nickname for the user that is easy for you to understand. Value Range: 1 - 64 characters.
User Name	Mandatory field. MAC address format.	Enter the MAC address for the user. Value Range: 0 - 17 characters, MAC format with ‘:’ or ‘-‘.
Password	Mandatory field. String format can be any text (max. 64 characters).	Enter the password for the user.
Save	Button	Click the **Save** button to save changes.

Table 184 – User Configuration

For MAC authentication function to work properly on authorized users (MACs), an administrator has to enter corresponding user information in to the User List. Otherwise, even for those authorized users, the authentication result will be false, and there will be no internet access for the users.

7 Administration

7.1 Configure & Manage

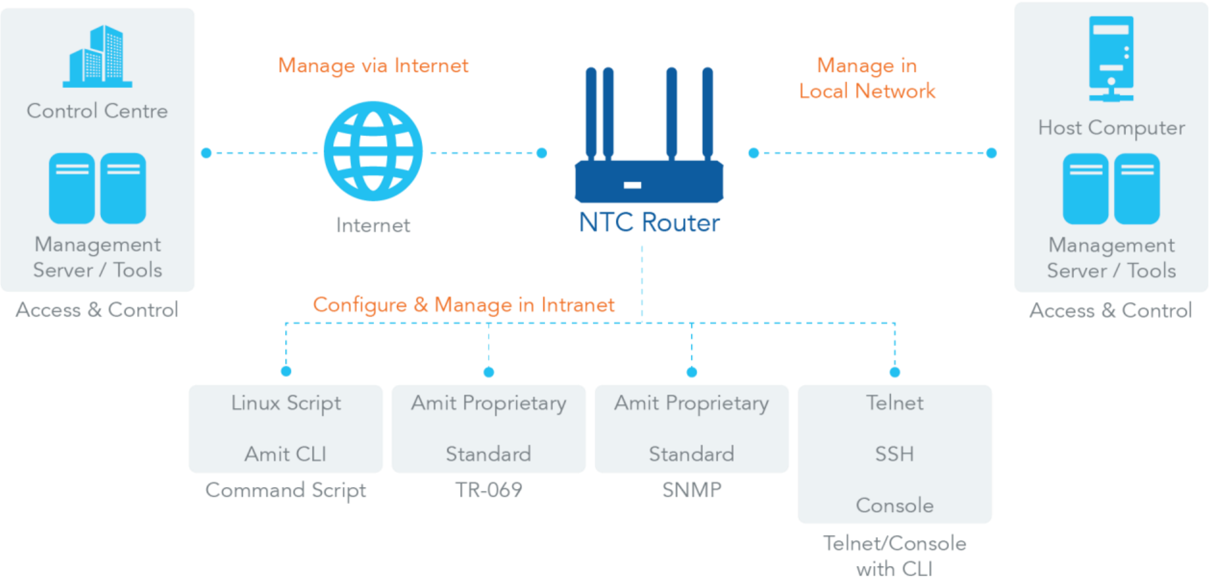


Figure 302 – Configure & Manage

The NTC-400 Series Router allows for enterprise-wide administration of distributed systems. The **Configure & Manage** tool group supports a range of system management protocols including Command Script, TR-069, SNMP, and Telnet with CLI.

7.1.1 Command Script

The **Command Script** configuration tool allows an administrator to set up a pre-defined configuration in plain text style and apply configuration on startup.

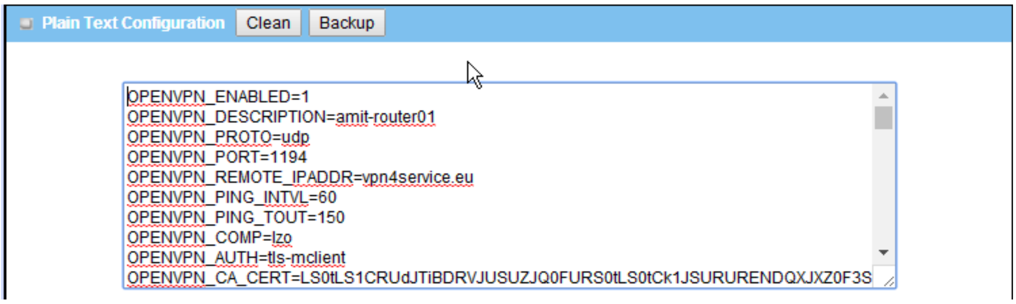
To apply a pre-defined configuration:

1 Select Configure and Manage from the Administration submenu and click the Command Script tab.

2 In the **Configuration** table check the ☑ **Enable** box to activate the Command Script function.

Note – The Enable box is unchecked by default.

3 Type your plain text configuration settings one line at a time in the **Plain Text Configuration** text box:



```
OPENVPN_ENABLED=1
OPENVPN_DESCRIPTION=amit-router01
OPENVPN_PROTO=udp
OPENVPN_PORT=1194
OPENVPN_REMOTE_IPADDR=vpn4service.eu
OPENVPN_PING_INTVL=60
OPENVPN_PING_TOUT=150
OPENVPN_COMP=lzo
OPENVPN_AUTH=tls-mclient
OPENVPN_CA_CERT=LS0tLS1CRUdJTiBDRVJUSUZJQ0FURS0tLS0tCk1JSURURENDQXJXZ0F3S
```

Figure 303 – Plain Text Configuration

- Click the **Clean** button to clear script from the text box that you no longer require or want to replace.

- Type in the configuration settings one line at a time and click **Save** to apply the settings.
- To save a copy of the settings, click the **Via Web UI** button next to **Backup Script** and save the .txt file to a known location.

  Note – The default name of the backup file is: `command_script_backup.txt`

- To upload settings from a remote source, or to restore setting you had previously saved using the **Backup Script** function, then click the **Via Web UI** button next to **Upload Script**, **Browse** to the .txt file and click the **Upload** button to populate the text box with the settings.

7.1.1.1 Supported configuration content

Specify the required value for each configuration setting after an 'equal' sign (=), for example:

```
OPENVPN_PING_TOUT=180
```

The following table contains supported plain text configuration items.

Key	Notes	Description
OPENVPN_ENABLED	1 = enable 0 = disable	Enable or disable OpenVPN Client function.
OPENVPN_DESCRIPTION	Mandatory field	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 field	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.

Key	Notes	Description
OPENVPN_CA_CERT	Mandatory field	Specify the Trusted CA certificate for the OpenVPN client. It will go through Base64 Conversion.
OPENVPN_LOCAL_CERT	Mandatory field	Specify the local certificate for OpenVPN client. It will go through Base64 Conversion.
OPENVPN_LOCAL_KEY	Mandatory field	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

Table 185 – Configuration Content

7.1.1.2 Configuration via Linux

For the settings that can be executed with standard Linux commands, you can put them in a script file, and apply to the system configuration with STARTUP command. For those configurations without a corresponding Linux command set to configure, you can configure them with proprietary command set.

7.1.1.3 Plain Text System Configuration with Telnet

In addition to the web-style plain text configuration mentioned above, the router also allows for configuration via the 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. Example: `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. Example: `txtConfig commit /tmp/config`
`enable`	NA	Enable plain text system config. Example: `txtConfig enable`
`disable`	NA	Disable plain text system config. Example: `txtConfig disable`
`run_immediately`	NA	Apply the configuration content that has been committed in database. Example: `txtConfig run_immediately`
`run_immediately`	an existing file	Assign a configuration file to apply. Example: `txtConfig run_immediately /tmp/config`

Table 186 – Plain system configuration using Telnet Commands

7.1.2 TR-069

TR-069 (Technical Report 069) is a technical specification originally published by the Broadband Forum entitled CPE WAN Management Protocol (CWMP). It defines an application layer protocol for remote management of end-user devices such as the NTC-400 Series Router. As a bi-directional SOAP/HTTP-based protocol, it supports communication between customer-premises equipment (CPE) and Auto Configuration Servers (ACS). The NTC-400 Series Router is such a CPE.

TR-069 is a customised feature for ISPs. We do not recommend that you change the configuration unless instructed by your ISP. If you have any problem in using this feature for device management, please contact with your ISP or the ACS provider for help.

7.1.2.1 Scenario - Managing deployed gateways through an ACS Server

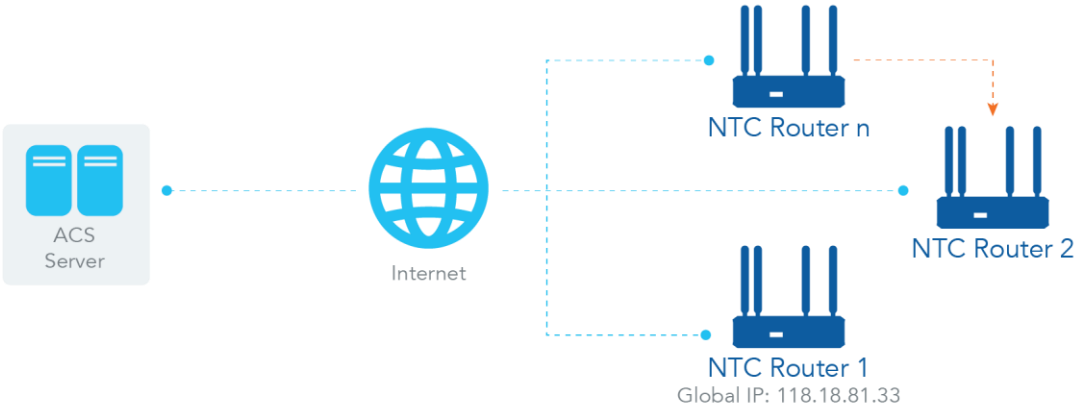


Figure 304 – Managing deployed gateways through an ACS Server

Scenario Application Timing

When the enterprise data centre wants to use an ACS server to manage remote routers geographically distributed elsewhere in the world, the routers in all branch offices must have an embedded TR-069 agent to communicate with the ACS server so that the ACS server can configure, upgrade firmware and monitor these gateways and their corresponding Intranets.

Scenario Description

The ACS server can configure, upgrade the firmware and monitor these routers. Remote gateways contact the ACS server for jobs to do in each time period. The ACS server can ask the gateways to execute some urgent jobs.

Parameter Setup Example

The following tables list the parameter configuration as an example for Router 1 in the above diagram with "TR-069" enabled. Use default values for those parameters that are not mentioned in the tables.

Configuration Path	[TR-069]-[Configuration]
TR-069	■ *Enable*
ACS URL	http://qantc.acslite.com/cpe.php
ACS User Name	*ACSUserName*
ACS Password	*ACSPassword*
ConnectionRequest Port	*8099*
ConnectionRequest User Name	*ConnReqUserName*
ConnectionRequest Password	*ConnReqPassword*
Inform	■ *Enable* *Interval 900*

Scenario Operation Procedure

In the diagram above, the ACS server can manage multiple gateways on the Internet. “Router 1" is one of them and has 118.18.81.33 IP address for its WAN-1 interface.

When all remote routers have booted up, they will try to connect to the ACS server.

Once the connections are established successfully, the ACS server can configure, upgrade the firmware and monitor these gateways.

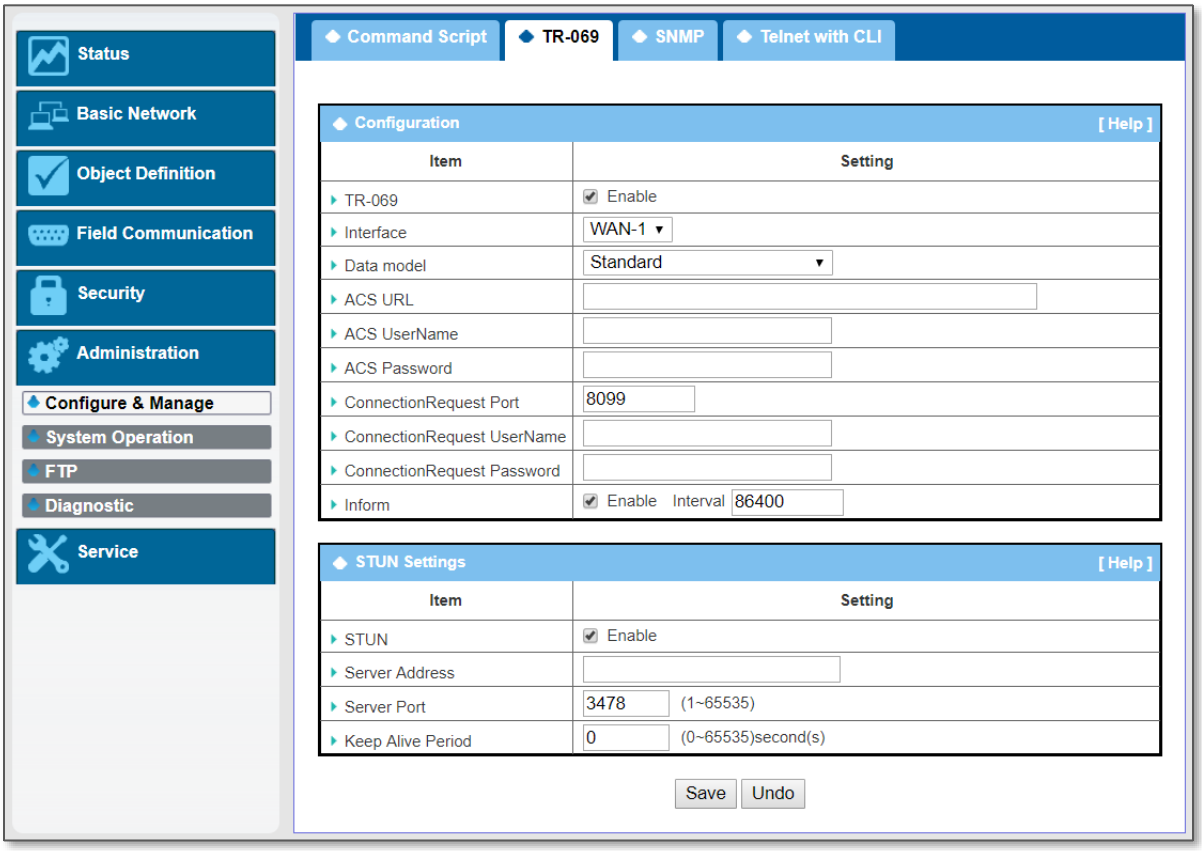
Remote gateways contact the ACS server for jobs to do in each time period.

If the ACS server has urgent jobs to be done by the gateways, it will issue the "Connection Request" command to those routers and those routers make immediate connections in response to the ACS server's immediate connection request for executing the urgent jobs.

7.1.2.2 TR-069 settings

To configure TR-069 for NTC-400 Series Router:

1 Select **Configure and Manage** from the **Administration** submenu and click the **TR-069** tab:



Configuration [Help]

Item	Setting
TR-069	☑ Enable
Interface	WAN-1 ▾
Data model	Standard ▾
ACS URL	
ACS UserName	
ACS Password	
ConnectionRequest Port	8099
ConnectionRequest UserName	
ConnectionRequest Password	
Inform	☑ Enable Interval 86400

STUN Settings [Help]

Item	Setting
STUN	☑ Enable
Server Address	
Server Port	3478 (1~65535)
Keep Alive Period	0 (0~65535)second(s)

Figure 305 – Enable TR-069

2 In the **Configuration** table check the ☑ **Enable** box to activate the TR-069 functionality.

Note – The Enable box is unchecked by default

3 Enter the other TR-069 settings as per the following table.

Item	Notes	Description
Interface	WAN-1 is the default.	Up to four WAN interfaces can be configured. Choose one at a time from the drop-down menu to define its TR-069 settings.
Data Model	Standard is the default.	Select the TR-069 data model for the remote management.

Item	Notes	Description
		Standard: the ACS Server is a standard one, which is fully comply with TR- 069.
ACS URL	Mandatory field	Manually enter the URL of your ACS
ACS Username	Mandatory field	Manually enter your username to access the ACS
ACS Password	Mandatory field	Manually enter your password to access the ACS
ConnectionRequest Port	Mandatory field. Default setting: **8099**	Manually enter the ConnectionRequest Port for your ACS Value Range: 0 - 65535
ConnectionRequest UserName	Mandatory field	Manually enter the ConnectionRequest UserName for your ACS
ConnectionRequest Password	Mandatory field	Manually enter the ConnectionRequest Password for your ACS
Inform	Default Interval value: **300 seconds** (five minutes).	When the ☑ **Enable** box is checked, the router (CPE) will periodically send an inform message to the ACS Server according to the Interval setting. Value Range: **0 - 86400** seconds for the inform Interval.
Save	Button	Click **Save** to save the settings

Table 187 – Enable TR-069

4 Enter the STUN (Session Traversal Utilities for Network Address Translation (NAT)) settings as per the following table.

Item	Notes	Description
STUN	Disabled by default.	Select ☑ **Enable** to use STUN as a mechanism for reaching devices that are connected behind NAT (e.g. IP-Phones, Set-top boxes). STUN is defined in TR-069 Annex G (formerly in TR-111).
Server Address		Enter the STUN Server address
Server Port		Enter the STUN server port
Keep Alive Period		Set the duration in seconds between two keepalive transmissions. Keepalive signals indicate that the connection should be preserved and not drop after timeout.
Save	Button	Click **Save** to save the STUN settings

Table 188 – STUN Settings

When you have set the ACS URL, Username and Password, your NTC-400 Series Router can periodically send an inform message to the ACS Server at the inform interval.

When you have set the ConnectionRequest Port, Username and Password, the ACS Server can ask the NTC-400 Series Router to send an inform message to the ACS Server.

7.1.3 SNMP

SNMP (Simple Network Management Protocol) is a protocol designed to give users the capability to remotely manage a computer network by polling and setting terminal values and monitoring network events.

A typical example of SNMP in use is when one or more administrative computers, called managers, have the task of monitoring or managing a group of hosts or devices on a computer network. Each managed system executes, at all times, a software component called an agent which reports information via SNMP to the manager.

SNMP agents expose management data on the managed 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 device supports several public MIBs and one private MIB for the SNMP agent.

The 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

7.1.3.1 SNMP Management Scenario

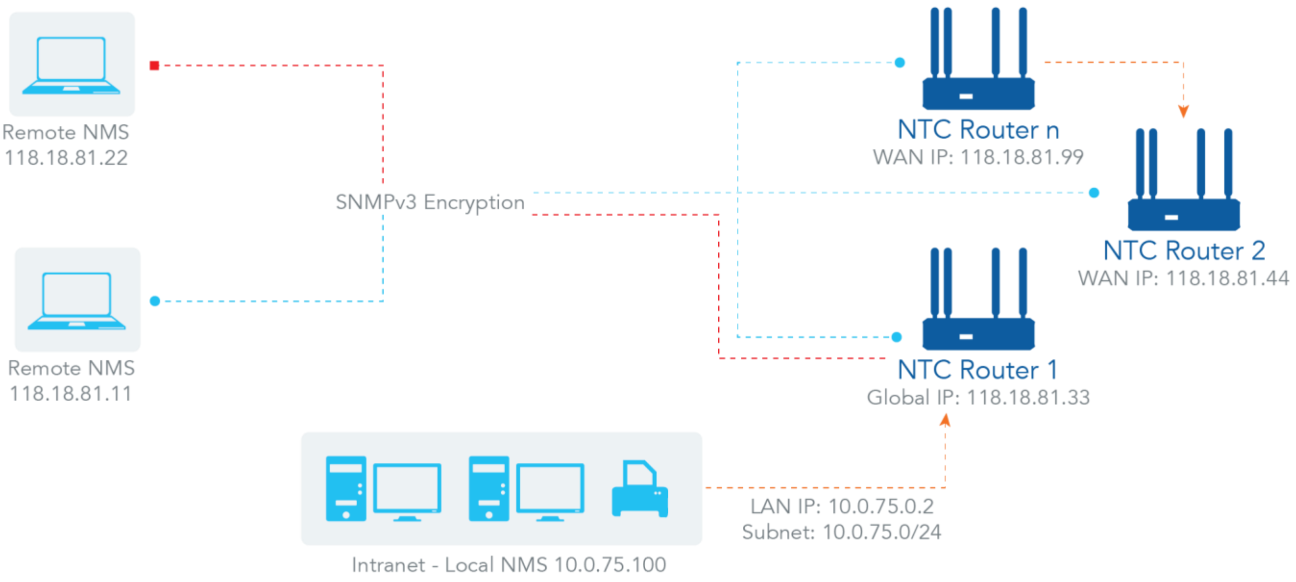


Figure 306 – SNMP Management Scenario

Scenario Application Timing

There are two application scenarios of SNMP Network Management Systems (NMS). Local NMS is in the Intranet and manages all devices that support the SNMP protocol in the Intranet. Another one is the Remote NMS to manage devices whose WAN interfaces are connected together by using a switch or a router with UDP forwarding. If you want to manage some devices and they all support the SNMP protocol, use either application scenario. For managing devices in the Internet, TR-069 is the better solution. Please refer to last sub-section.

Scenario Description

The NMS server can monitor and configure the managed devices by using the SNMP protocol and those devices are located where UDP packets can be reached from NMS. The managed devices report urgent trap events to the NMS servers. Use SNMPv3 version of protocol can protected the transmitting of SNMP commands and responses. The remote NMS with privilege IP address can manage the devices, but other remote NMS can't.

Parameter Setup Example

The following tables list the parameter configuration as an example for Router 1 in above diagram with "SNMP" enabling at LAN and WAN interfaces.

Use the 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*

Scenario Operation Procedure

In the diagram above, the NMS server can manage multiple devices on the Intranet or a UDP-reachable network. "Router 1" is one of the managed devices, and it has the IP address of 10.0.75.2 for the LAN interface and 118.18.81.33 for the WAN-1 interface. It serves as a NAT router.

The NMS manager prepares related information for all managed devices and records them in the NMS system. The NMS system gets the status of all managed devices by using SNMP get commands.

When the manager wants to configure the managed devices, the NMS system allows them to do that by using SNMP set commands. The "UserName1" account is used if the manager uses the SNMPv3 protocol for configuring "Router 1". Only the "UserName1" account can let "Router 1" accept the configuration from the NMS since the authority of the account is "Read/Write".

Once a managed device has an urgent event to send, the device will issue a trap to the Trap Event Receivers. The NMS itself could be one of them.

If you want to secure the transmitted SNMP commands and responses between the NMS and the managed devices, use SNMPv3 version of protocol.

The remote NMS without a privileged IP address can't manage "Router 1", since "Router 1" allows only the NMS with a privileged IPaddress to manage it via its WAN interface.

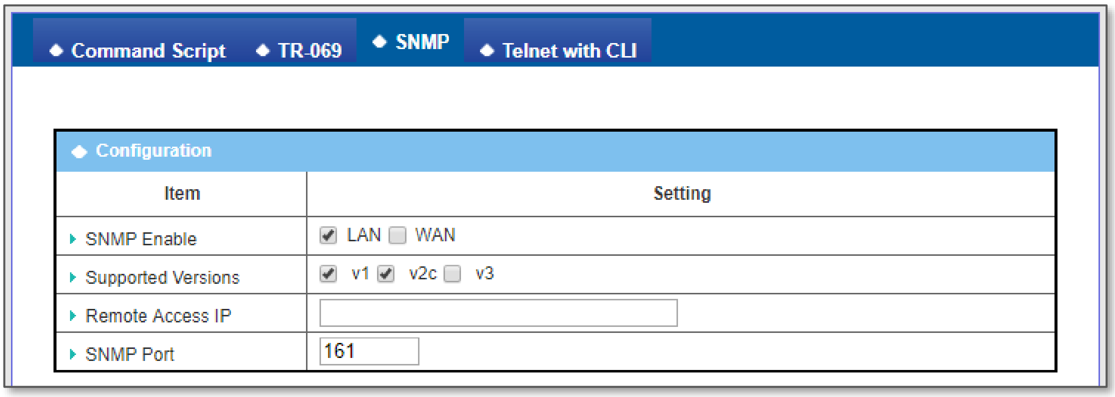
7.1.3.2 SNMP settings

The SNMP allows user to configure SNMP relevant setting which include interface, version, access control and trap receiver.

7.1.3.3 Enable SNMP

To configure SNMP for NTC-400 Series Router it must be enabled:

1 Select **Configure and Manage** from the **Administration** submenu and click the **SNMP** tab:



Item	Setting
SNMP Enable	☑ LAN ☐ WAN
Supported Versions	☑ v1 ☑ v2c ☐ v3
Remote Access IP	
SNMP Port	161

Figure 307 – Enable SNMP

2 The following configurations settings are available to enable SNMP on the NTC-400 Series Router:

Item	Notes	Description
SNMP Enable	Disabled 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.
Supported Versions	☑ **v1 box** enabled by default	Select the version for the SNMP When Check the v1 box.

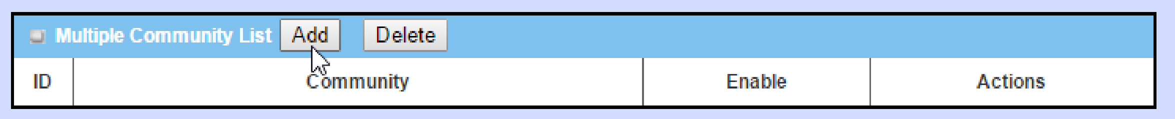
Item	Notes	Description
	☑ **v2c box** enabled by default	It means you can access SNMP by version 1. When Check the v2c box. It means you can access SNMP by version 2c. When Check the v3 box. It means you can access SNMP by version 3.
Remote Access IP	String format: any Ipv4 address It is an optional item.	Specify the Remote Access IP for WAN. If you filled in a certain IP address. It means only this IP address can access SNMP from WAN side. If you left it as blank, it means any IP address can access SNMP from WAN side.
SNMP Port	Mandatory field String format: any port number Default SNMP port: **161**	Specify the SNMP Port. You can fill in any port number. But you must ensure the port number is not to be used. Value Range: 1 - 65535.
Save	Button	Click **Save** to save the settings.
Undo	Button	Click **Undo** to cancel the settings.

Table 189 – Enable SNMP

7.1.3.4 Create/Edit Multiple Communities

The SNMP allows you to custom your access control for version 1 and version 2 user.

The router supports up to a maximum of 10 community sets.

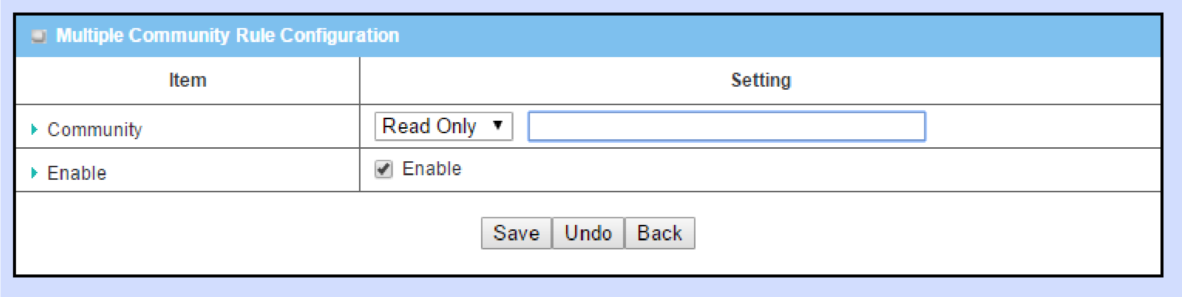


Multiple Community List Add Delete

ID	Community	Enable	Actions

Figure 308 – Multiple Community List

When **Add** button is applied, **Multiple Community Rule Configuration** page will display:



Multiple Community Rule Configuration

Item	Setting
Community	Read Only ▼
Enable	☑ Enable

Save Undo Back

Figure 309 – Multiple Community Rule Configuration

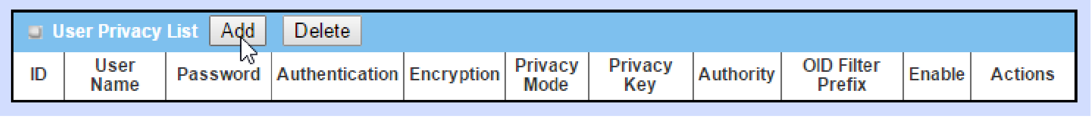
The following settings are available to configure Multiple Community Rules:

Item	Notes	Description
Community	Mandatory field. String format: any text Default setting: **Read Only**	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	Enabled by default	Enables the community as a version 1 or version v2c user.
Save	Button	The **Save** button saves the configuration settings, but it does not apply them to SNMP functions. When you return to the SNMP main page the "Click on save button to apply your changes" reminder appears, this reminds the user to click main page Save button at which point the settings will be applied.
Undo	Button	Click the **Undo** button to cancel the settings.
Back	Button	Click the **Back** button to return to SNMP configuration page.

Table 190 – Multiple Community Rule Configuration

7.1.3.5 Create/Edit User Privacy

The SNMP allows you to customise your access control for version 3 users. The router supports up to a maximum of 128 User Privacy sets.

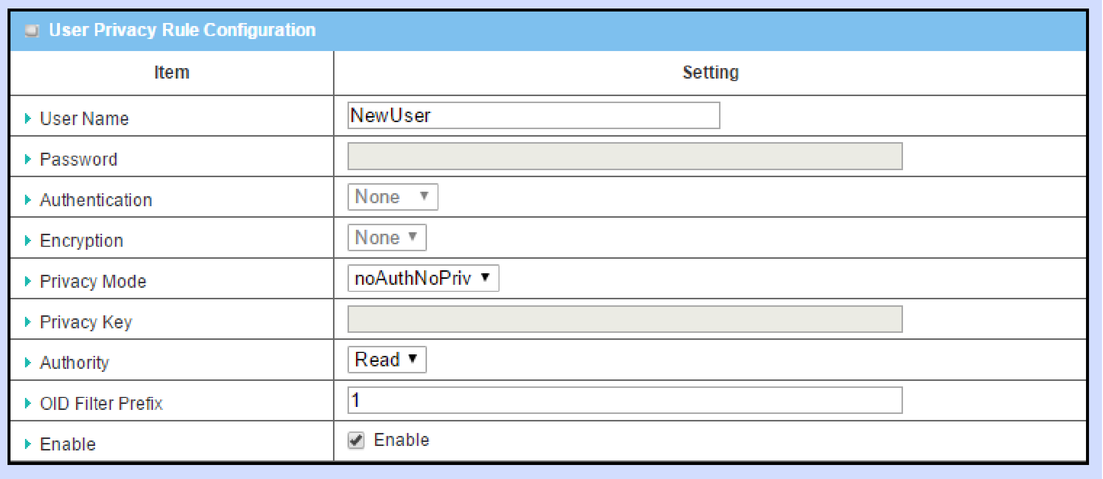


User Privacy List Add Delete

ID	User Name	Password	Authentication	Encryption	Privacy Mode	Privacy Key	Authority	OID Filter Prefix	Enable	Actions

Figure 310 – User Privacy List

When **Add** button is applied, **User Privacy Rule Configuration** page will display:



User Privacy Rule Configuration

Item	Setting
User Name	NewUser
Password	
Authentication	None ▾
Encryption	None ▾
Privacy Mode	noAuthNoPriv ▾
Privacy Key	
Authority	Read ▾
OID Filter Prefix	1
Enable	☑ Enable

Figure 311 – User Privacy Rule Configuration

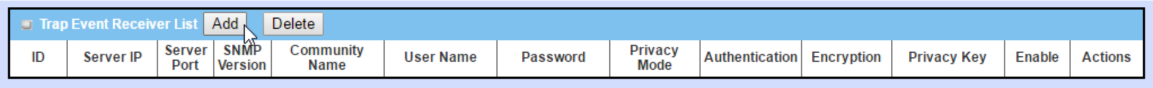
The following settings are available to configure User Privacy Rules:

Item	Notes	Description
User Name	Mandatory field String format: any text	Specify the User Name for this version 3 user. Value Range: 1 - 32 characters.
Password	String format: any text	When your Privacy Mode is authNoPriv or authPriv, you must specify the Password for this version 3 user. Value Range: 8 - 64 characters.
Authentication	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	None is selected by default	When your Privacy Mode is authPriv, you must specify the Encryption protocols for this version 3 user. Select either the DES or AES encryption protocol.
Privacy Mode	noAuthNoPriv is the default setting	Specify the Privacy Mode for this version 3 user: **noAuthNoPriv** = Default selection **authNoPriv** = Select if you do not use any authentication types and encryption protocols. **authPriv** = When selected you must specify the Authentication and Password. You must specify the Authentication, Password, Encryption and Privacy Key.
Privacy Key	String format: any text	When your Privacy Mode is authPriv, you must specify the Privacy Key (8 - 64 characters) for this version 3 user.
Authority	Default setting: **Read**	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	Mandatory field String format: any legal OID Default setting: **1**	The OID Filter Prefix restricts access for this version 3 user to the sub-tree rooted at the given OID. Value Range: 1 - 2080768.
Enable	Enabled by default.	Enables this version 3 user.
Save	Button	The **Save** button saves the configuration settings, but it does not apply them to SNMP functions. When you return to the SNMP main page the "Click on save button to apply your changes" reminder appears, this reminds the user to click main page Save button at which point the settings will be applied.
Undo	Button	Click the **Undo** button to cancel the settings.
Back	Button	Click the **Back** button to return to SNMP configuration page.

Table 191 – User Privacy Rule Configuration

7.1.3.6 Create/Edit Trap Event Receiver

The SNMP allows you to customise your trap event receiver. The router supports up to a maximum of four Trap Event Receiver sets.



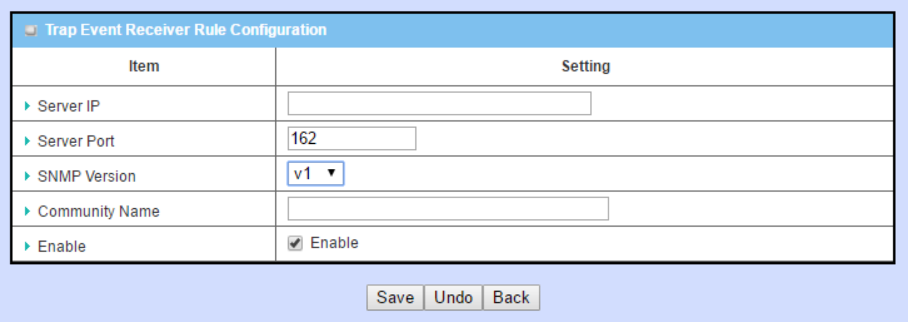
Trap Event Receiver List

ID	Server IP	Server Port	SNMP Version	Community Name	User Name	Password	Privacy Mode	Authentication	Encryption	Privacy Key	Enable	Actions

Figure 312 – Trap Event Receiver List

Click the **Add** button to open the **Trap Event Receiver Rule Configuration** screen.

Both default **SNMP Version** of **v1** and the user-selected **SNMP Version v2c** use the following configuration settings:

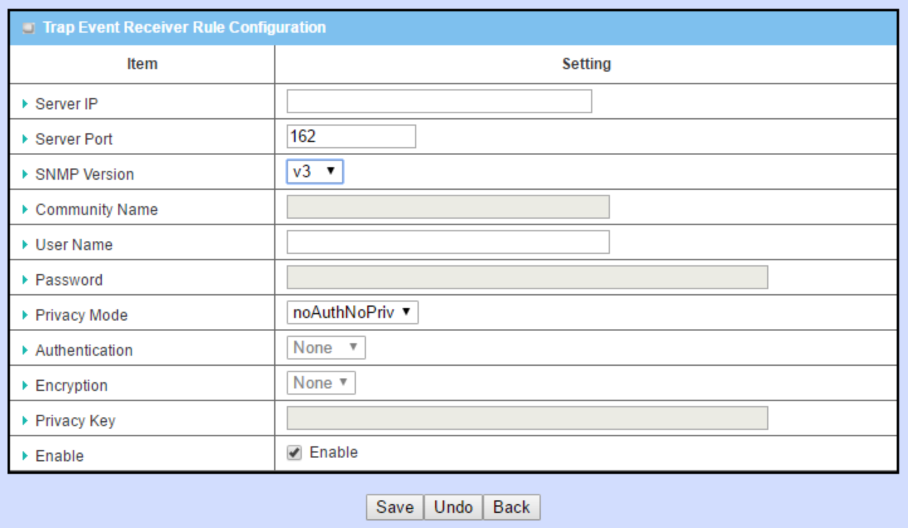


Trap Event Receiver Rule Configuration

Item	Setting
Server IP	
Server Port	162
SNMP Version	v1 ▾
Community Name	
Enable	☑ Enable

Figure 313 – Trap Event Receiver Rule Configuration

If you select **SNMP Version v3** the following configuration screen containing more settings will be displayed:



Trap Event Receiver Rule Configuration

Item	Setting
Server IP	
Server Port	162
SNMP Version	v3 ▾
Community Name	
User Name	
Password	
Privacy Mode	noAuthNoPriv ▾
Authentication	None ▾
Encryption	None ▾
Privacy Key	
Enable	☑ Enable

Figure 314 – Trap Event Receiver Rule Configuration

Item	Notes	Description
Server IP	Mandatory field. String format: any IPv4 address.	Specifies the trap Server IP. The NTC-400 Series Router sends trap to the server IP.
Server Port	Mandatory field. String format: any port number	Specify the trap Server Port. You can enter in any port number, but you must ensure the port number is not already in use.

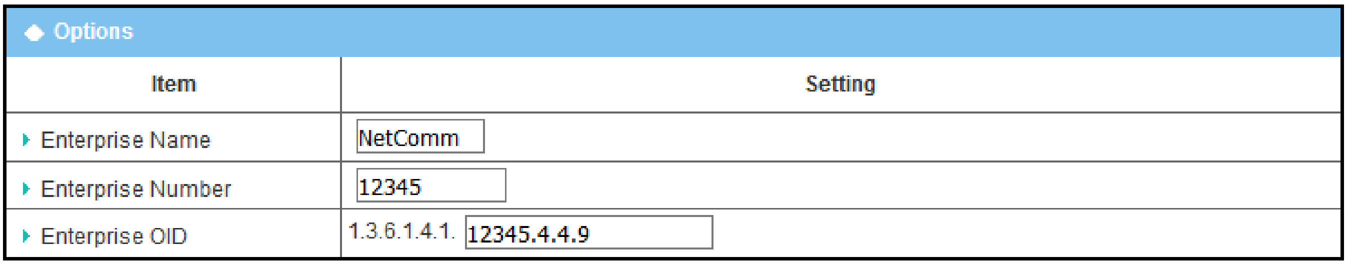
Item	Notes	Description
	Server Port 162 is the default SNMP trap port.	Value Range: 1 - 65535.
SNMP Version	v1 is the default setting	Select the version for the trap. Selecting v1 or v2c will display a smaller configuration screen containing five settings. If v3 is selected six additional configuration settings will be included in the configuration screen.
Community Name	Mandatory field for SNMP Version v1 and v2c. String format: any text	Specify the Community Name for a version 1 or version v2c trap. Value Range: 1 - 32 characters.
User Name	Mandatory field for SNMP Version v3. String format: anytext	Specify the **User Name** for this version 3 trap. Value Range: 1 - 32 characters.
Password	Mandatory field for SNMP Version v3. String format: anytext	When your Privacy Mode is authNoPriv or authPriv, you must specify the Password for this version 3 trap. Value Range: 8 - 64 characters.
Privacy Mode	Mandatory field for SNMP Version v3. Default setting: **noAuthNoPriv**	Specify the Privacy Mode for this version 3 trap. Select **noAuthNoPriv** if you do not use any authentication types and encryption protocols. If **authNoPriv** is selected you must specify the Authentication and Password. If **authPriv** is selected you must specify the Authentication, Password, Encryption and Privacy Key.
Authentication	Mandatory field for SNMP Version v3 Default setting: **None**	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	Mandatory field for SNMP Version v3 Default setting: **None**	When your Privacy Mode is authPriv, you must specify the Encryption protocols for this version 3 trap. Select either the DES or AES encryption protocol.
Privacy Key	Mandatory field for SNMP Version v3 String format: any text	When your Privacy Mode is authPriv, you must specify the Privacy Key (8 - 64 characters) for this version 3 trap.
Enable	Enabled by default	Click **Enable** to enable this trap receiver.
Save	Button	The **Save** button saves the configuration settings, but it does not apply them to SNMP functions. When you return to the SNMP main page the "Click on save button to apply your changes" reminder appears,

Item	Notes	Description
		this reminds the user to click main page Save button at which point the settings will be applied.
Undo	Button	Click the **Undo** button to cancel the settings.
Back	Button	Click the **Back** button to return to SNMP configuration page.

Table 192 – Trap Event Receiver Rule Configuration

7.1.3.7 Edit SNMP options

If you use a private MIB, you must enter the enterprise name, number and OID.



Options

Item	Setting
Enterprise Name	NetComm
Enterprise Number	12345
Enterprise OID	1.3.6.1.4.1. 12345.4.4.9

Figure 315 – Edit SNMP Options

Item	Value setting	Description
Enterprise Name	Mandatory field. String format: any text	Specify the **Enterprise Name** for the particular private MIB. Value Range: 1 - 10 characters, and only string with A-Z, a-z, 0-9, ’–‘, ‘_’.
Enterprise Number	Mandatory field. String format: any number	Specify the **Enterprise Number** for the particular private MIB. Value Range: 1 - 2080768.
Enterprise OID	Mandatory field. String format: any legal OID.	Specify the **Enterprise OID** for the particular private MIB. The range of the each OID number is 1-2080768. The maximum length of the enterprise OID is 31. The seventh number must be identical with the enterprise number.
Save	Button	Click the **Save** button to save the configuration and apply your changes to SNMP functions.
Undo	Button	Click the **Undo** button to cancel the settings.

Table 193 – Edit SNMP Options

7.1.4 Telnet with CLI settings

Command-line interface (CLI), also known as command-line user interface or console user interface, is a computer program where the user (or client) types lines of text into a command line shell which converts the commands to appropriate operating system functions. Programs with command-line interfaces are generally easier to automate via scripting. The NTC-400 Series Router supports both Telnet and SSH (Secure Shell) CLI with default service port 23 and 22, respectively.

Telnet & SSH Scenario

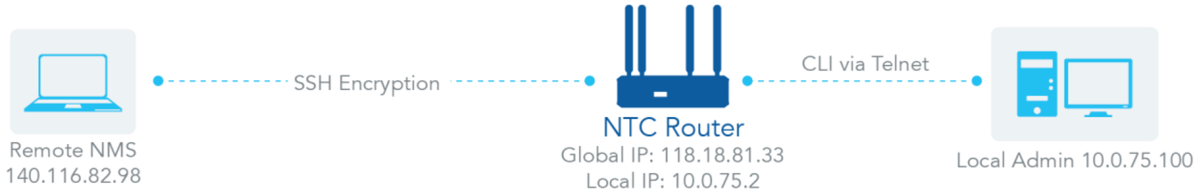


Figure 316 – Telnet & SSH Scenario

Scenario Application Timing

When the administrator of the router wants to manage it from remote site on the Intranet or Internet, they may use the "Telnet with CLI" function.

Scenario Description

The Local Admin or the Remote Admin can manage the router by using a "Telnet" or "SSH" utility with a privileged user name and password.

Data packets between the Local Admin and the router or between the Remote Admin and the router can be plain texts or encrypted texts. We recommend that they are plain text in the Intranet for Local Admin to use a "Telnet" utility, and encrypted texts in the Internet for Remote Admin to use an "SSH" utility.

Parameter Setup Example

The following table lists the parameter configuration as an example for the router in the diagram above with "Telnet with CLI" enabled on the LAN and WAN interfaces.

Use default values 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*

Table 194 – Telnet Parameter Setup Example

Scenario Operation Procedure

In the diagram above, "Local Admin" or "Remote Admin" can manage the router on the Intranet or Internet. The router is the gateway of Network-A, and the subnet of its Intranet is 10.0.75.0/24. It has the IP address of 10.0.75.2 for the LAN interface and 118.18.81.33 for the WAN-1 interface. It serves as a NAT gateway.

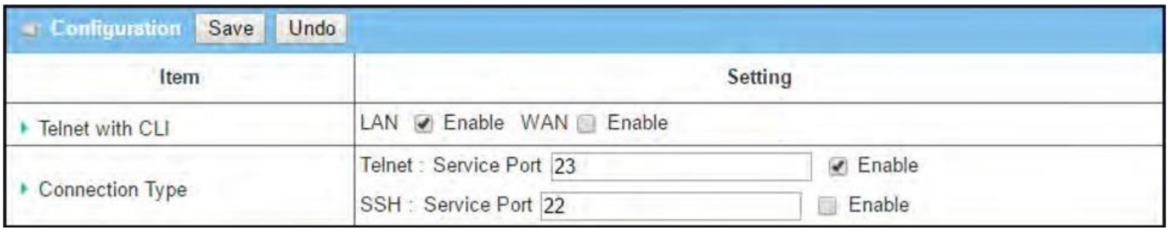
The "Local Admin" on the Intranet uses a "Telnet" utility with a privileged account to log in the router and the "Remote Admin" on the Internet uses an "SSH" utility with a privileged account to login the router.

The administrator of the router can control the device as if they are in front of it.

7.1.4.1 Enable Telnet with CLI

To use the Telnet with CLI tool:

1 Select Configure and Manage from the Administration submenu and click the Telnet with CLI tab.



Item	Setting
Telnet with CLI	LAN ☑ Enable WAN □ Enable
Connection Type	Telnet : Service Port 23 ☑ Enable SSH : Service Port 22 □ Enable

Figure 317 – Telnet with CLI Settings

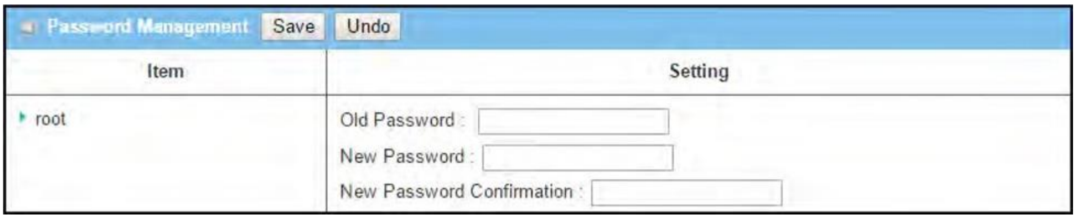
The Telnet with CLI setting allows a user with administrator privileges to access this device through the traditional Telnet program. Before you can telnet (login) to the device, please configure the related settings and password with care. The password management part allows you to set the root password for telnet and SSH and access.

Item	Notes	Description
Telnet with CLI	The LAN Enable box is checked by default. Disabled by default.	Check the ☑ **Enable** box to activate the Telnet with CLI function for connecting from WAN/LAN interfaces.
Connection Type	Telnet □ **Enable** box is disabled by default. Default Telnet Service Port: **23** SSH ☑ **Enable** box is checked by default. Default SSH Service Port: **22**	Check the Telnet ☑ **Enable** box to activate telnet service. Check the SSH ☑ **Enable** box to activate SSH service. You can set which number of Service Port you want to provide for the corresponding service. Value Range: 1 - 65535.
Save	Button	Click **Save** to save the settings
Undo	Button	Click **Undo** to cancel the settings

Table 195 – Telnet with CLI

7.1.4.2 Password management

To reset the password:



Item	Setting
root	Old Password : New Password : New Password Confirmation :

Figure 318 – Password Management

Item	Notes	Description
root	String: any number or character, no blank characters The default password for telnet is 'admin'.	First type the old password and then specify a new password and confirm it to change the root password. **Note** - We highly recommend changing the default Telnet password with your own before the device is deployed.
Save	Button	Click **Save** to save the settings.
Undo	Button	Click **Undo** to cancel the settings.

Table 196 – Password Management

7.2 System Operation

System Operation allows the network administrator to manage system settings such as web-based utility access password change, system information, system time, system log, firmware/configuration backup & restore, and reset & reboot.

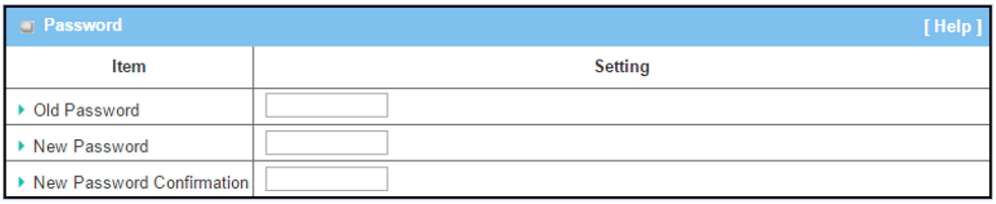
7.2.1 Password & MMI

7.2.1.1 Change Password

To manage access to the Web-User Interface:

1 Select **System Operation** from the **Administration** submenu and click the **Password & MMI** tab and go to the **Password** section.

2 The **Password** settings allow a network administrator to change the MMI login password:



Password	[Help]
Item	Setting
Old Password	
New Password	
New Password Confirmation	

Figure 319 – Password setting

Item	Notes	Description
Old Password	String: any alpha-numeric character The default password for web-based MMI is ‘admin’.	Enter the current password to enable you to unlock and change to the new password.
New Password	String: any alpha-numeric character	Enter new password.
New Password Confirmation	String: any alpha-numeric character	Enter new password again to confirm.
Save	Button	Click **Save** button to save the settings.
Undo	Button	Click **Undo** button to cancel the settings.

Table 197 – Password setting

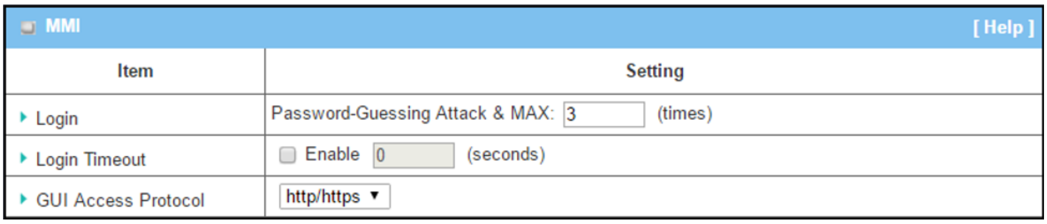
7.2.1.2 Manage access settings

The Web-User Interface section allows an administrator to make various security related settings to prevent unauthorised access or use.

To change the MMI access settings:

1 Select **System Operation** from the **Administration** submenu and click the **Password & Web-User Interface** tab and go to the **Web-User Interface** section.

2 Settings allow the administrator to set the number of unsuccessful login attempts and to enable automatic logout after a defined idle time. Alternatively, the timeout function can be disabled.



MMI [Help]

Item	Setting
Login	Password-Guessing Attack & MAX: 3 (times)
Login Timeout	□ Enable 0 (seconds)
GUI Access Protocol	http/https ▾

Figure 320 – MMI

Item	Notes	Description
Login	Default value: **Three attempts**	Enter the maximum login attempts value. Value Range: 3 - 10. If someone fails to log in to the web GUI more times than the maximum setting, a warning message "*Already reaching maximum Password-Guessing times, please wait a few seconds!*" will be displayed and further attempts will not be allowed for a few seconds.
Login Timeout	Disabled by default	Check the ☑ **Enable** box to activate the auto logout function, and specify the maximum idle time in seconds. Value Range: 30 - 65535. If there has been no activity on the NTC-400 Series Router web interface for the designated time, the interface will automatically log out and you will have to enter your password to log in. When disabled, the text box displays zero.
GUI Access Protocol	Default setting: **http/https**	Select the protocol that will be used for GUI access. It can be http/https, http only, or https only.
Save	Button	Click **Save** button to save the settings
Undo	Button	Click **Undo** button to cancel the settings

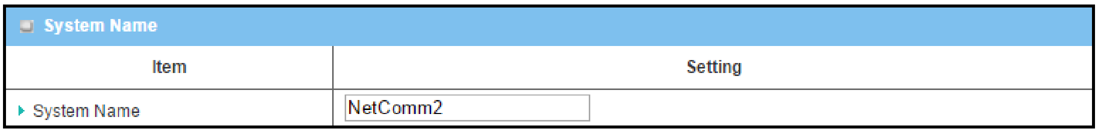
Table 198 – MMI setting

7.2.2 System Information

The system information screen allows the network administrator to quickly view system details.

To access the System Information page:

1 Select System Operation from the Administration submenu and click the System information tab.



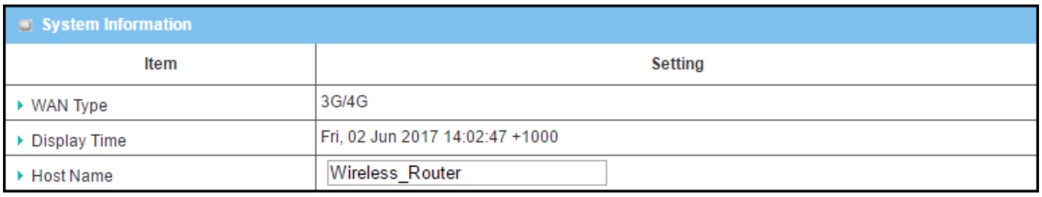
System Name

Item	Setting
System Name	NetComm2

Figure 321 – System Name

Item	Notes	Description
System Name	Optional item.	Enter a system name for identification purposes. It can be any name.

2 The System Information section displays important information about the router:



System Information

Item	Setting
WAN Type	3G/4G
Display Time	Fri, 02 Jun 2017 14:02:47 +1000
Host Name	Wireless_Router

Figure 322 – System Information

Item	Notes	Description
WAN Type	System data, no user input.	Displays the WAN Type of the WAN-1 internet connection.
Display Time	System data, no user input.	Displays the time that you logged in for the current session. Its display is controlled by settings in **Administration |System Time**, see next section.
Host Name	It is an optional item Default setting: **Cellular_Router**	Enter the host name for the router. It can be used to interact with external network servers for identifying the name of requesting device.
Save	Button	Click the Save button to save the settings.
Refresh	Button	Click the Refresh button to update the system Information immediately.

Table 199 – System Information

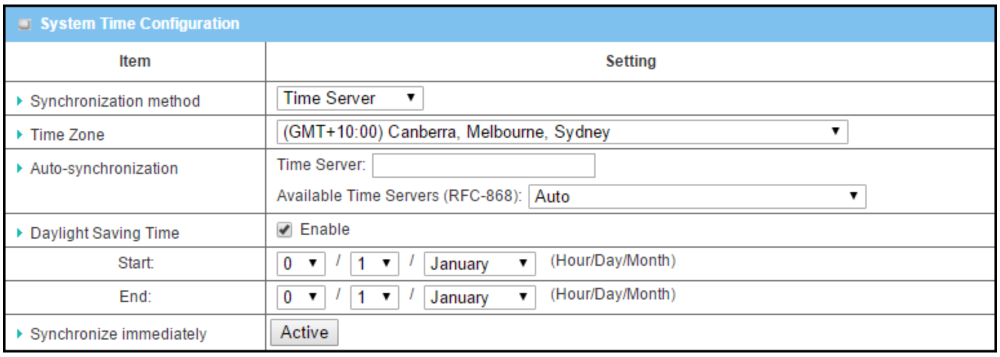
7.2.3 System Time

System time can be automatically synchronised from a time server or may be manually configured by the administrator.

The settings vary depending on the synchronization method chosen in the first drop down list.

7.2.3.1 Time Server method

When the **Time Server Synchronization method** is chosen the following configuration settings are available:



System Time Configuration

Item	Setting
Synchronization method	Time Server ▼
Time Zone	(GMT+10:00) Canberra, Melbourne, Sydney ▼
Auto-synchronization	Time Server: Available Time Servers (RFC-868): Auto ▼
Daylight Saving Time	☑ Enable
Start:	0 ▼ / 1 ▼ / January ▼ (Hour/Day/Month)
End:	0 ▼ / 1 ▼ / January ▼ (Hour/Day/Month)
Synchronize immediately	Active

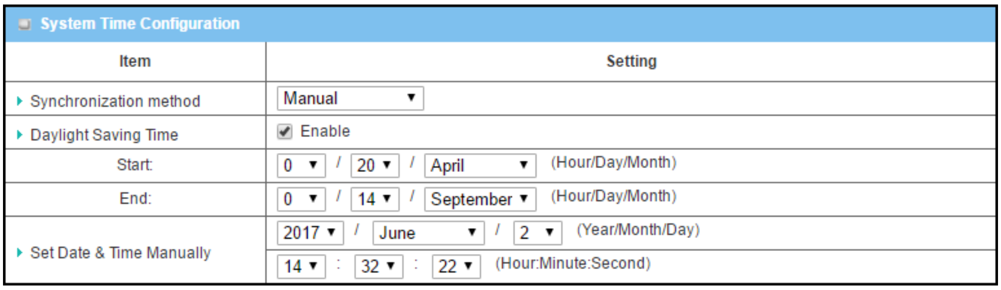
Figure 323 – System Time Configuration - Time Server Synchronization

Item	Notes	Description
Synchronization method	Time Server	This setting determines the configuration settings available.
Time Zone	This item is Optional field. GMT+00:00 is the default setting.	Select a time zone, normally where the router is located, from the drop down list.
Auto-synchronization	Checked by default. Auto is the default setting.	Check the ☑ **Enable** button to activate the time auto-synchronization function with a NTP server. You can enter the IP or FQDN for the NTP server you will use, or leave it as auto mode so that the available server will be used for time synchronization one by one.
Time Server		
Daylight Saving Time	This is an optional item. Disabled by default.	Check the ☑ **Enable** button to activate the daylight saving function. When you enable this function, you have to specify the start date and end date for daylight saving time in your region.
Synchronize Immediately	Button	Based on your selection of time zone and time server above , when you click the Active button the system will communicate with time server by NTP Protocol to get system date and time.
Sync Result	System generated and button	When the **Active** button is clicked, the **Time Synchronization Results** pane will display first the progress of the synchronisation and then the server and time of sync. Click the **Close** button to hide the results details.
Save	Button	Click the **Save** button to save the settings.

Table 200 – System Time Configuration - Time Server Synchronization

7.2.3.2 Manual method

When the **Manual Synchronization method** is chosen the following configuration settings are available:



System Time Configuration

Item	Setting
Synchronization method	Manual ▾
Daylight Saving Time	☑ Enable
Start:	0 ▾ / 20 ▾ / April ▾ (Hour/Day/Month)
End:	0 ▾ / 14 ▾ / September ▾ (Hour/Day/Month)
Set Date & Time Manually	2017 ▾ / June ▾ / 2 ▾ (Year/Month/Day) 14 ▾ : 32 ▾ : 22 ▾ (Hour:Minute:Second)

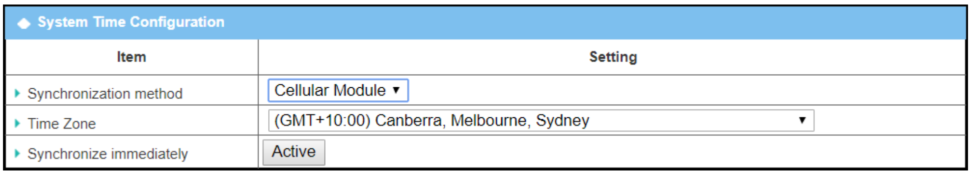
Figure 324 – System Time Configuration - Manual Synchronization

Item	Notes	Description
Synchronization method	Manual	This setting determines the configuration settings available.
Daylight Saving Time	This is an optional item. Disabled by default.	Check the ☑ **Enable** button to activate the daylight saving function. When you enable this function, you have to specify the start date and end date for daylight saving time in your region.
Set Date and Time Manually	Date and time settings	Enter the date and exact time that you want the clock to run from when the Save button is clicked.
Save	Button	Click the **Save** button to save the settings. The system clock will be reset to begin at the time entered.

Table 201 – System Time Configuration - Manual Synchronization

7.2.3.3 Time Server method

When the **Time Server Synchronization method** is chosen the following configuration settings are available:



System Time Configuration

Item	Setting
Synchronization method	Cellular Module ▾
Time Zone	(GMT+10:00) Canberra, Melbourne, Sydney ▾
Synchronize immediately	Active

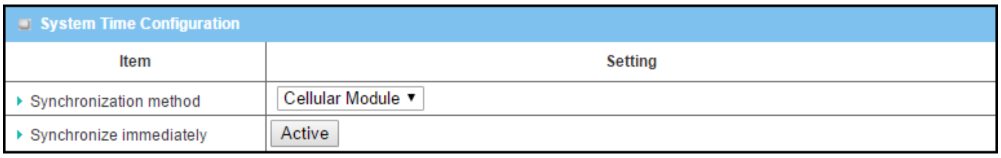
Figure 325 – System Time Configuration - Local PC

Item	Notes	Description
Synchronization method	PC	This setting will use the system time of the PC that you have opened the web interface on.
Time Zone	Drop down menu	Select the time zone of your device.
Synchronize Immediately	Button	Click the **Active** button the system will be set to the local PC's system date and time.
Sync Result	System generated and button	When the **Active** button is clicked, the **Time Synchronization Results** panel will display the time the synchronisation occurred. Click the **Close** button to hide the panel.
Save	Button	Click the **Save** button to save the settings.

Table 202 – System Time Configuration - Local PC

7.2.3.4 Cellular Module method

When the **Cellular Module Synchronization method** is chosen the following configuration settings are available:



System Time Configuration

Item	Setting
Synchronization method	Cellular Module ▾
Synchronize immediately	Active

Figure 326 – System Time Configuration - Cellular Module Synchronization

Item	Notes	Description
Synchronization method	Cellular Module	This setting will use the system time of your service provider that is used by the router's phone module.
Synchronize Immediately	Button	Click the **Active** button the system will be set to the router's phone module system date and time.
Sync Result	System generated and button	When the Active button is clicked, the Time Synchronization Results panel will display the time the synchronisation occurred. Click the **Close** button to hide the panel.
Save	Button	Click the **Save** button to save the settings.

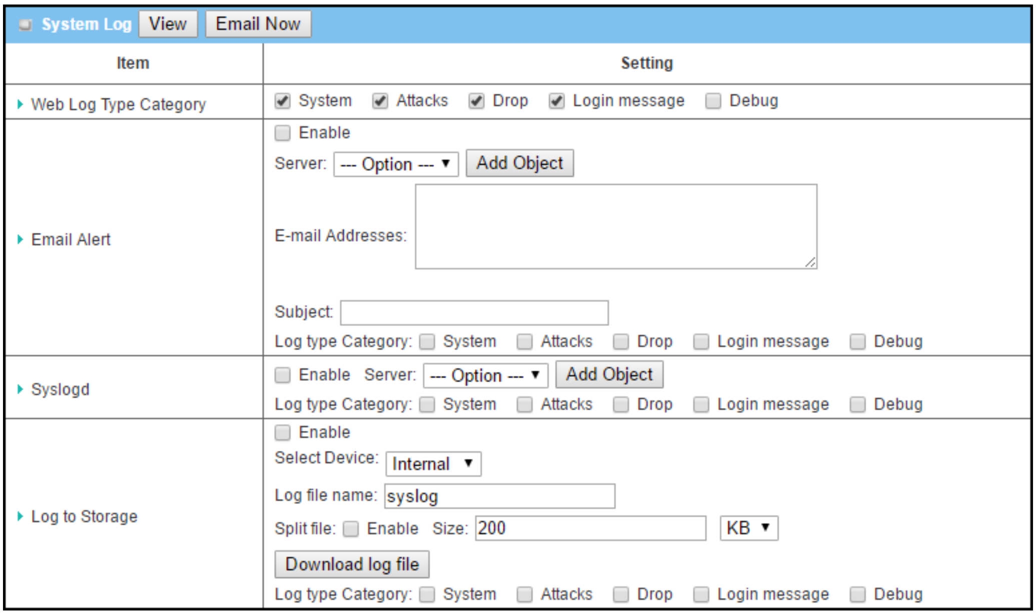
Table 203 – System Time Configuration - Cellular Module Synchronization

7.2.4 System Log

The System Log screen provides the administrator with various tools to perform local event logging and remote reporting functions.

To access the **System Log** page:

1 Select System Operation from the Administration submenu and click the System Log tab.



System Log | View | Email Now

Item	Setting
Web Log Type Category	☑ System ☑ Attacks ☑ Drop ☑ Login message □ Debug
Email Alert	□ Enable Server: --- Option --- ▾ Add Object E-mail Addresses: Subject: Log type Category: □ System □ Attacks □ Drop □ Login message □ Debug
Syslogd	□ Enable Server: --- Option --- ▾ Add Object Log type Category: □ System □ Attacks □ Drop □ Login message □ Debug
Log to Storage	□ Enable Select Device: Internal ▾ Log file name: syslog Split file: □ Enable Size: 200 KB ▾ Download log file Log type Category: □ System □ Attacks □ Drop □ Login message □ Debug

Figure 327 – System Log

7.2.4.1 View & Email buttons

The buttons in the page header bar determine what is done with the log data.

The settings on the page determine what log data is collected.

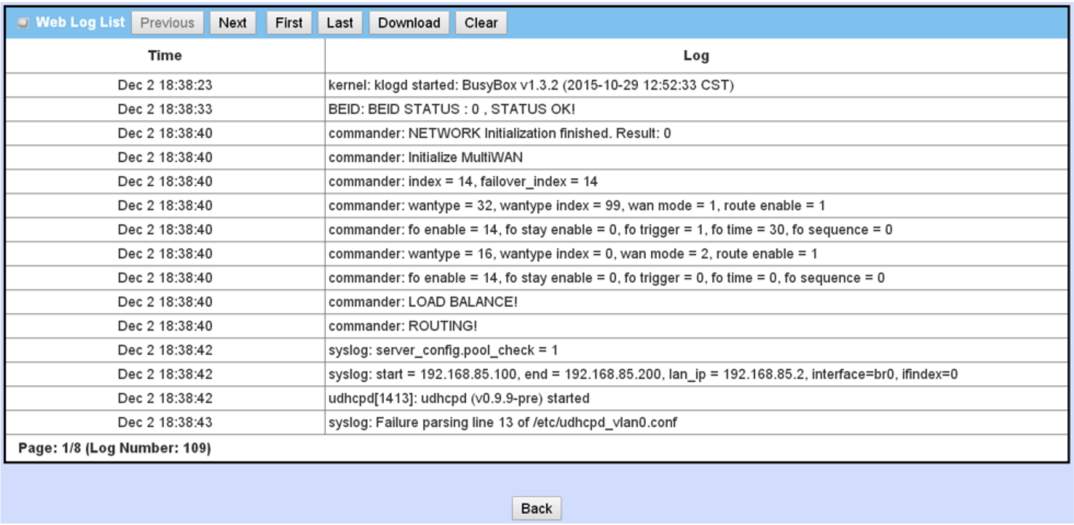
The **View** button allows a network administrator to view log history on the router. The **Email Now** button enables administrator to send instant Emails for notification or analysis.

Item	Description
View button	The System Log View button displays the log history in Web Log List window, see below.
Email Now button	Click the System Log Email Now button to send the current log history via Email. Refer to Email Alert settings below for details on configuring the email addresses and content.

Table 204 – System Log

7.2.4.2 Web Log List window

When the System Log **View** button is clicked, the **Web Log List** window is displayed.



Time	Log
Dec 2 18:38:23	kernel: klogd started: BusyBox v1.3.2 (2015-10-29 12:52:33 CST)
Dec 2 18:38:33	BEID: BEID STATUS : 0 , STATUS OK!
Dec 2 18:38:40	commander: NETWORK Initialization finished. Result: 0
Dec 2 18:38:40	commander: Initialize MultiWAN
Dec 2 18:38:40	commander: index = 14, failover_index = 14
Dec 2 18:38:40	commander: wantype = 32, wantype index = 99, wan mode = 1, route enable = 1
Dec 2 18:38:40	commander: fo enable = 14, fo stay enable = 0, fo trigger = 1, fo time = 30, fo sequence = 0
Dec 2 18:38:40	commander: wantype = 16, wantype index = 0, wan mode = 2, route enable = 1
Dec 2 18:38:40	commander: fo enable = 14, fo stay enable = 0, fo trigger = 0, fo time = 0, fo sequence = 0
Dec 2 18:38:40	commander: LOAD BALANCE!
Dec 2 18:38:40	commander: ROUTING!
Dec 2 18:38:42	syslog: server_config.pool_check = 1
Dec 2 18:38:42	syslog: start = 192.168.85.100, end = 192.168.85.200, lan_ip = 192.168.85.2, interface=br0, ifindex=0
Dec 2 18:38:42	udhcpd[1413]: udhcpd (v0.9.9-pre) started
Dec 2 18:38:43	syslog: Failure parsing line 13 of /etc/udhcpd_vlan0.conf

Page: 1/8 (Log Number: 109)

Figure 328 – Web Log List

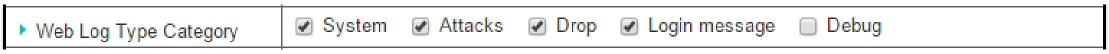
The following items appear on the Web Log List window:

Item	Notes	Description
Time	Column Heading	Displays event time stamps.
Log	Column Heading	Displays Log messages.
Previous	Button	Move to the previous page.
Next	Button	Move to the next page.
First	Button	Jump to the first page.
Last	Button	Jump to the last page.
Download	Button	Download log to your PC in .tar file format.
Clear	Button	Clear all log entries.
Back	Button	Return to the previous page.

Table 205 – Web Log List

7.2.4.3 Web Log Type Category

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. When your log settings have been made, the System Log **View** button to view Log History in the Web Log List window.



Web Log Type Category ☑ System ☑ Attacks ☑ Drop ☑ Login message □ Debug

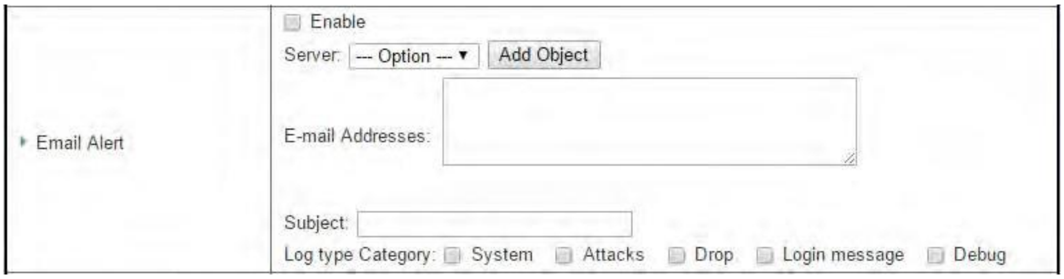
Figure 329 – Web Log Type Category

Item	Notes	Description
System	☑ Enabled by default.	Select ☑ to log system events and to display in the Web Log List window.
Attacks	☑ Enabled by default.	Select ☑ to log attack events and to display in the Web Log List window.
Drop	☑ Enabled by default.	Select ☑ to log packet drop events and to display in the Web Log List window.
Login message	☑ Enabled by default.	Select ☑ to log system login events and to display in the Web Log List window.
Debug	☐ Disabled by default	Select ☑ to log debug events and to display in the Web Log List window.

Table 206 – Web Log Type Category

7.2.4.4 Email Alert

In the **Email Alert** section the network administrator can select the type(s) of events to log and specify the recipient Email account(s).



Email Alert

□ Enable

Server: --- Option --- ▾ Add Object

E-mail Addresses:

Subject:

Log type Category: □ System □ Attacks □ Drop □ Login message □ Debug

Figure 330 – Email Alert

Item	Notes	Description
Enable	Disabled by default.	Check the ☑ **Enable** box to enable sending event log messages to destined Email account defined in the E-mail Addresses blank space.
Server	N/A	Select an email server from the Server dropdown list to send Email. If none has been available, click the **Add Object** button to create an outgoing Email server.

Item	Notes	Description
		You may also add an outgoing Email server from the **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 alphanumeric character	Enter an Email subject that is easy for you to identify on the Email client.
Log type category	Unselected by default	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**

Table 207 – Email Alert

7.2.4.5 Syslogd

The **Syslogd** section allows the network administrator to select the type of event to log and to be sent to the designated Syslog server.

The following settings are available:

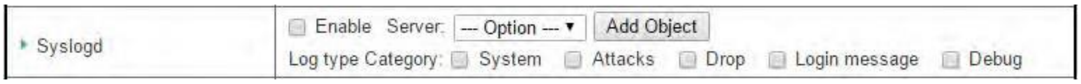

Syslogd
□ Enable Server: --- Option --- ▾ Add Object
Log type Category: □ System □ Attacks □ Drop □ Login message □ Debug

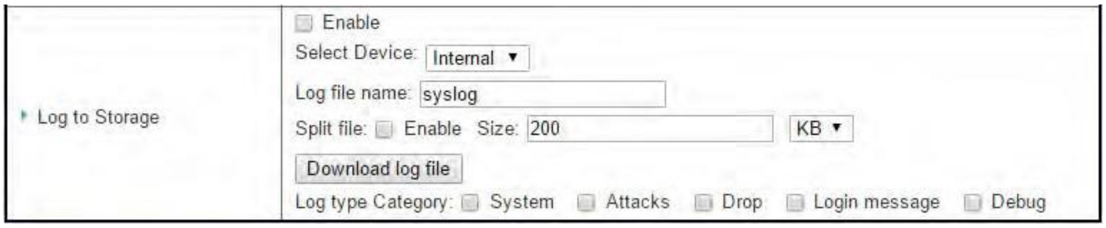
Figure 331 – Syslogd settings

Item	Notes	Description
Enable	Disabled by default.	Check the ☑ **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 list to send the 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 Serve**r tab.
Log type category	Disabled by default.	Select ☑ the type(s) of events to be logged and be sent to the destination syslog server. Available events are **System, Attacks**, **Drop, Login message** and **Debug**

Table 208 – Syslogd settings

7.2.4.6 Log to Storage

The Log to Storage section allows network administrators to select the type(s) of events to log and be stored at an internal or an external storage device or location.



Log to Storage	□ Enable Select Device: Internal ▼ Log file name: syslog Split file: □ Enable Size: 200 KB ▼ Download log file Log type Category: □ System □ Attacks □ Drop □ Login message □ Debug

Figure 332 – Log to Storage

Item	Notes	Description
Enable	Disabled by default	Check to enable sending log to storage.
Select Device	**Internal** is the default setting.	Select **Internal** or **External** storage. The NTC-400 has 8GB of internal SD storage.
Log file name	Disabled by default	Enter a log file name to save logs in designated storage as.
Split file Enable	Disabled by default	Check ☑ **Enable** to split the log file output whenever the file reaches the specified size limit.
Split file Size	**200 KB** is the default setting.	Enter the file size limit for each split log file. Value Range: **10 - 1000 KB**
Log type category	Disabled by default	Select ☑ which type of logs to send: **System, Attacks, Drop, Login message, Debug**
Download log file	button	Click to download a log file based on the current Log to Storage settings.

Table 209 – Log to Storage

7.2.5 Backup & Restore

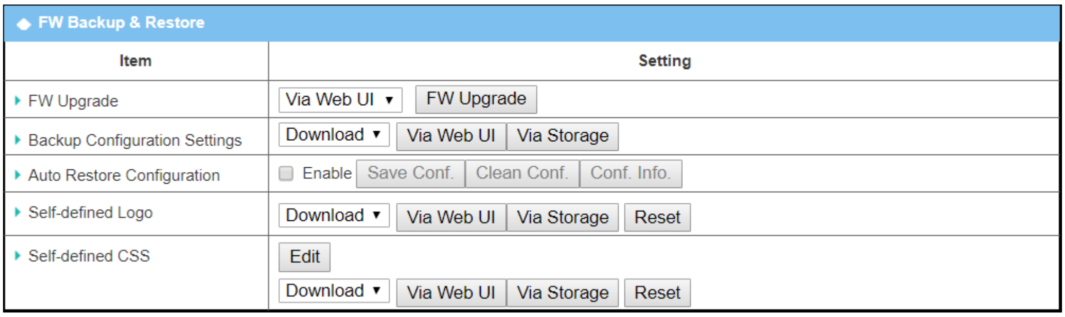
From the Backup & Restore screen you can upgrade the device firmware when new firmware is available as well as backup and then restore the device configuration.

7.2.5.1 FW Backup & Restore

To access the **Backup & Restore** screen:

1 Select **System Operation** from the **Administration** submenu and click the **Backup & Restore** tab.

2 The **FW Backup & Restore** section contains tools to manage your upgrade, backup and restore functions:



FW Backup & Restore

Item	Setting
FW Upgrade	Via Web UI ▼ FW Upgrade
Backup Configuration Settings	Download ▼ Via Web UI Via Storage
Auto Restore Configuration	□ Enable Save Conf. Clean Conf. Conf. Info.
Self-defined Logo	Download ▼ Via Web UI Via Storage Reset
Self-defined CSS	Edit Download ▼ Via Web UI Via Storage Reset

Figure 333 – FW Backup & Restore

Item	Notes	Description
FW Upgrade	Default setting: **Via Web UI**	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** button use the **Browse** tool to find and select the firmware file, then click the **Upgrade** button to start the firmware upgrade process on this device.
Backup Configuration Settings	Default setting: **Download**	Click the Via Web UI button to backup or restore the device configuration settings. The action is determined by the following settings in the dropdown list: **Download** – Use this setting to back up the device configuration to a config.bin file. **Upload** – Use this setting to restore a designated configuration file previously downloaded from the device. **Via Web UI** – to retrieve a configuration file via Web GUI, for example from the manufacturer's website.
Auto Restore Configuration	Disabled by default.	Check the ☑ **Enable** button to activate the customized default setting function. Once the function is activated, click the **Save Conf.** button to save the current settings as a configuration file. Click the **Clean Conf.** button to erase the stored configuration. The **Conf. Info** button displays information about the currently stored configuration.
Self-defined Logo	Download is the default setting	Insert your company logo into the top left corner of the web interface. The graphic must be in .gif format and be called:"logo.gif" Select **Upload** and browse to the file containing the file. You can also choose **Download** to export the file.

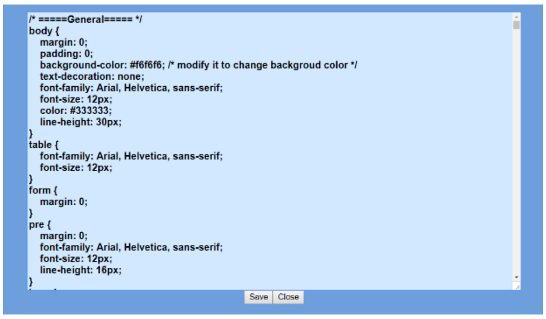
Self-defined CSS		Add cascading style sheet (.css) code and click **Save**.
		
		/* =====General===== */
		body {
		    margin: 0;
		    padding: 0;
		    background-color: #f6f6f6; /* modify it to change backgroud color */
		    text-decoration: none;
		    font-family: Arial, Helvetica, sans-serif;
		    font-size: 12px;
		    color: #333333;
		    line-height: 30px;
		}
		table {
		    font-family: Arial, Helvetica, sans-serif;
		    font-size: 12px;
		}
		form {
		    margin: 0;
		}
		pre {
		    margin: 0;
		    font-family: Arial, Helvetica, sans-serif;
		    font-size: 12px;
		    line-height: 16px;
		}

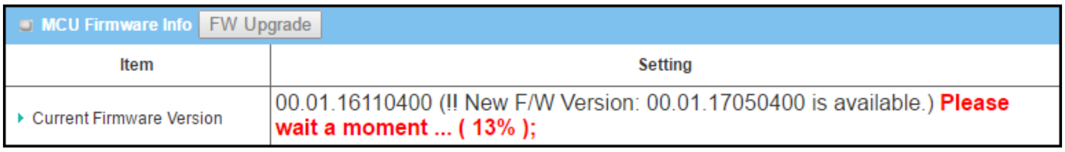
Table 210 – FW Backup & Restore

7.2.5.2 MCU Firmware Info

The **MCU Firmware Info** section displays the current firmware version and allows you to download and install a new firmware version when it is available.

If a newer version is available, the **FW Upgrade** button is displayed in the title bar and the **Setting** text box will display a message: **(!! New F/W Version: XX.XX.XXXX is available.)**

Click the **FW Upgrade** button to download it:



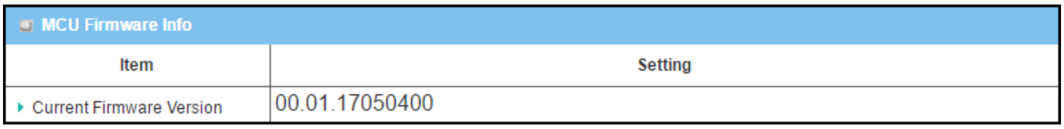
MCU Firmware Info | FW Upgrade

Item	Setting
Current Firmware Version	00.01.16110400 (!! New F/W Version: 00.01.17050400 is available.) **Please wait a moment ... (13%);**

Figure 334 – MCU Firmware Upgrade

The percent of progress of the download will be indicated. When the download is complete, the following message will display: **Upload status: Successful**

Click the **Save** button to install the new firmware. The new firmware details will display in the **Current Firmware Version Setting** box:



MCU Firmware Info

Item	Setting
Current Firmware Version	00.01.17050400

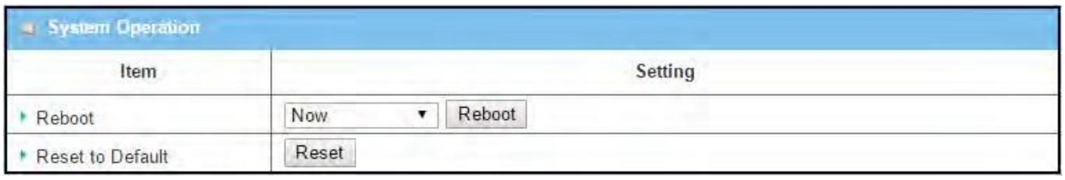
Figure 335 – MCU Firmware Info

The **FW Upgrade** button will be hidden until new firmware becomes available.

7.2.6 Reboot & Reset

To access the Reboot and Reset controls:

1 Select **System Operation** from the **Administration** submenu and click the **Reboot & Reset** tab:



System Operation

Item	Setting
Reboot	Now ▾ Reboot
Reset to Default	Reset

***Figure 336** – System Operation*

Item	Notes	Description
Reboot	Now is the default setting	Reboot turns the router off, then turns it back on and applies the current configuration. Depending on the selection in the dropdown list, clicking the Reboot button will immediately reboot the router or will reboot at a pre-defined time or schedule. **Now** – Click the Reboot button and the router will immediately reboot after you confirm by clicking OK to reboot. **Time Schedule** – Select a pre-defined auto-reboot time schedule rule from the drop-down list to reboot the router at a designated time. To define a time schedule rule, go to the **Object Definition > Scheduling > Configuration** tab.

Item	Notes	Description
		Note – This Reboot function has the same effect as switching the router's power source off and on.
Reset to Default	Button	Click the **Reset** button to turn the router off, then turn it back on and apply the device's factory default configuration values. **Note** – This Reset to Default function has the same effect as pressing the reset button on the device panel.

Table 211 – System Operation

7.3 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 architecture 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). SSH File Transfer Protocol (SFTP) is sometimes also used instead, but it is technologically different.

The NTC-400 Series Router includes an embedded FTP / SFTP server for administrator to download the log files to his computer or database. In the following two sections, you can configure the FTP server and create the user accounts that can log in to the server. After logging in to the FTP server, you can browse the log directory, download the stored log files and delete the files you have downloaded to make more storage space for further data logs. The NTC-400 has 8GB of SD storage.

The available log files can be system logs (refer to Administration > System Operation > System Log), Network Packets (refer to Administrator > Diagnostic > Packet Analyzer), Data Log (refer to Field Communication > Data Logging > Log File Management), and GNSS Log (refer to Service > Location Tracking > GNSS).

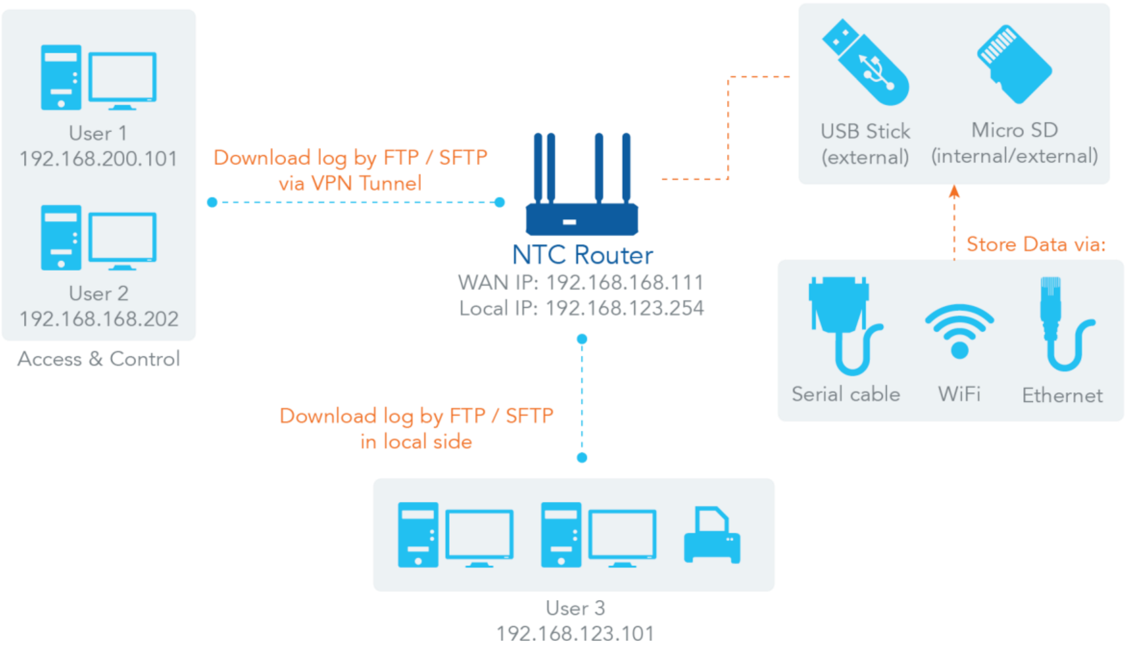
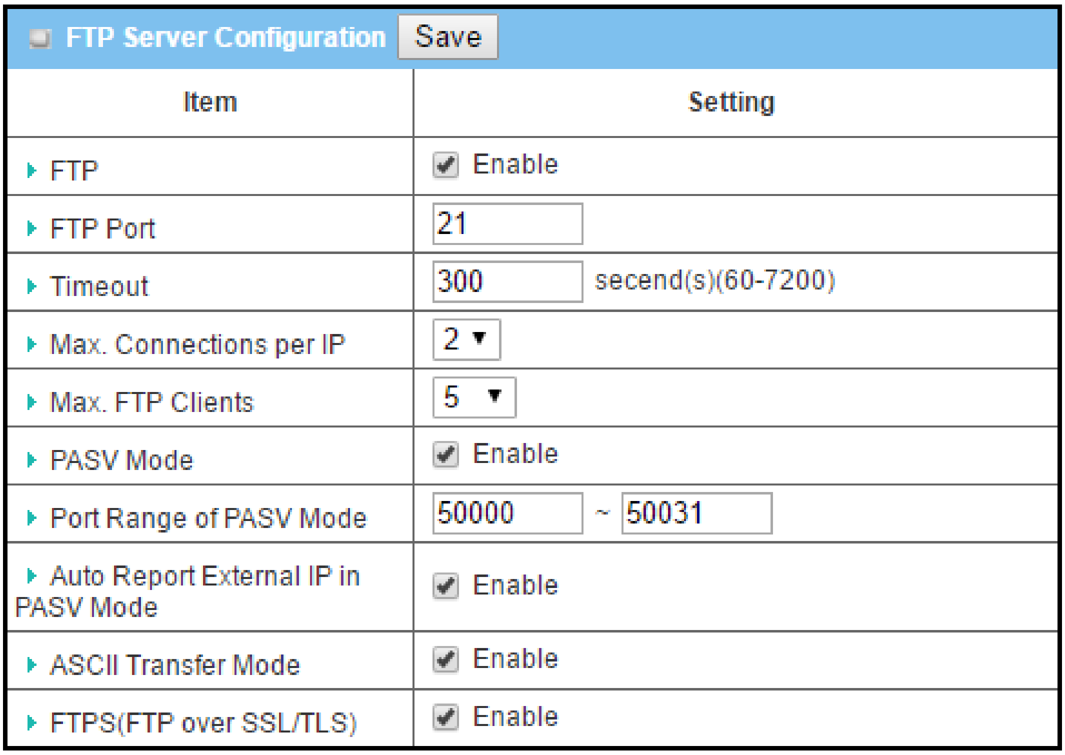


Figure 337 – FTP Example

7.3.1 FTP Server Configuration

To access the **FTP Server Configuration** screen, select **FTP** from the **Administration** submenu.



FTP Server Configuration

Item	Setting
FTP	☑ Enable
FTP Port	21
Timeout	300 second(s)(60-7200)
Max. Connections per IP	2 ▾
Max. FTP Clients	5 ▾
PASV Mode	☑ Enable
Port Range of PASV Mode	50000 ~ 50031
Auto Report External IP in PASV Mode	☑ Enable
ASCII Transfer Mode	☑ Enable
FTPS(FTP over SSL/TLS)	☑ Enable

Figure 338 – FTP Server Configuration

Item	Notes	Description
FTP	Disabled 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 this FTP connection. **Note** – The embedded FTP Server is only for downloading log files. There is no write access for the user to upload files.
FTP Port	**Port 21** is the default setting.	Specify a port number for FTP connection. The router will listen for incoming FTP connections on the specified port. Value Range = 1 - 65535.
Timeout	300 seconds is the default setting.	Specify the maximum timeout interval for the FTP connection. Supported range = 60 to 7200 seconds (i.e. one minute – two hours)
Max. Connections per IP	2 Clients are the default setting.	Specify the maximum number of clients from the same IP address for the FTP connection. Up to 5 clients from the same IP address are supported.

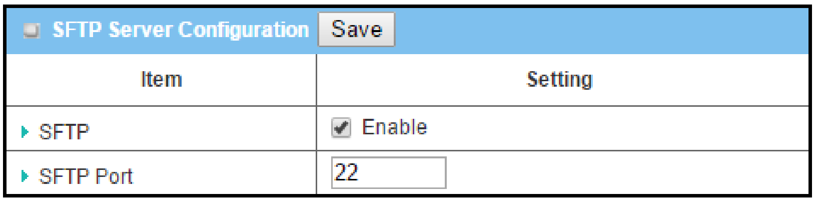
Item	Notes	Description
Max. FTP Clients	5 Clients are the default setting.	Specify the maximum number of clients for the FTP connection. Up to 32 clients are supported.
PASV Mode	Optional setting	Check ☑ **Enable** to activate the support of PASV mode for a FTP connection from FTP clients.
Port Range of PASV Mode	Port 50000 - 50031 is the default setting.	Specify the port range to allocate for PASV style data connection. Value Range: 1024 - 65535.
Auto Report External IP in PASV Mode	Optional setting.	Check ☑ **Enable** to activate the support of overriding the IP address advertising in response to the PASV command.
ASCII Transfer Mode	Optional setting.	Check ☑ **Enable** to activate the support of ASCII mode data transfers. Binary mode is supported by default.
FTPS (FTP over SSL/TLS)	Optional setting.	Check ☑ **Enable** to activate the support of secure FTP connections via SSL/TLS.

Table 212 – FTP Server Configuration

7.3.1.1 Enable SFTP Server

Additional security for FTP transmissions is provided by the SFTP server option.

To access the **SFTP Server Configuration** screen, select **FTP** from the **Administration** submenu and go to the **SFTP Server Configuration** section:



SFTP Server Configuration Save

Item	Setting
SFTP	☑ Enable
SFTP Port	22

Figure 339 – SFTP Server Configuration

Item	Notes	Description
SFTP	Disabled by default.	Check ☑ **Enable** 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. The NTC-400 has 8GB of SD storage.
SFTP Port	Port 22 is the default setting.	Specify a port number for SFTP connection. The router will listen for incoming SFTP connections on the specified port. Value Range = 1 - 65535.

Table 213 – SFTP Server Configuration

7.3.2 User Account

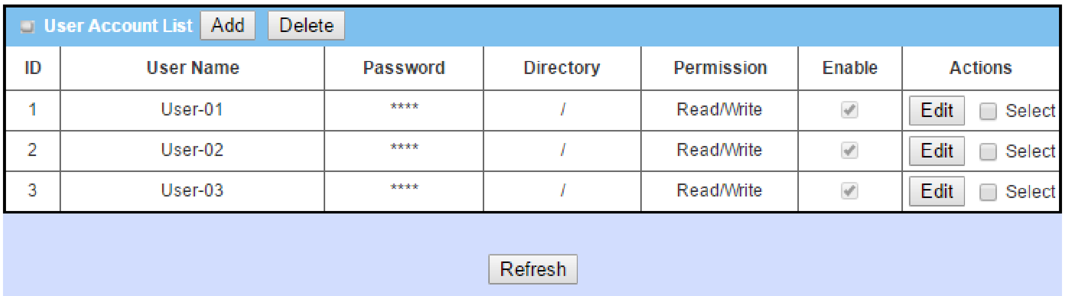
This feature allows users to set up and manage user accounts for logging in to the embedded FTP and SFTP log file servers.

7.3.2.1 View/manage User Accounts

To create and manage FTP/SFTP user accounts:

1 Select **FTP** from the **Administration** submenu and click the **User Account** tab.

2 The **User Account List** containing all current FTP/SFTP log file server users.



User Account List Add Delete

ID	User Name	Password	Directory	Permission	Enable	Actions
1	User-01	****	/	Read/Write	☑	Edit ☐ Select
2	User-02	****	/	Read/Write	☑	Edit ☐ Select
3	User-03	****	/	Read/Write	☑	Edit ☐ Select

Refresh

Figure 340 – User Account List

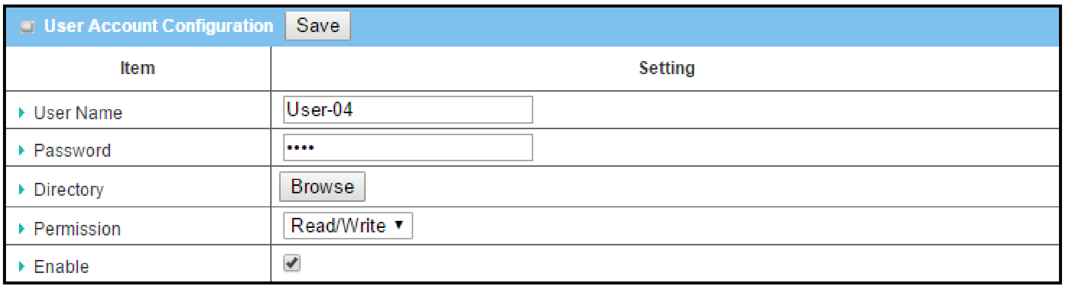
7.3.2.2 Manage User Accounts

Click the **Edit** button to make changes to existing accounts.

When an account is no longer required, check ☑ **Select** and click the **Delete** button to permanently remove it. Alternatively, you can retain the account and its details, but disable it. This is accomplished using the account's **Edit** button and unchecking its ☐ **Enable** setting.

7.3.2.3 Add User Accounts

Click the **Add** button to display the **User Account Configuration** screen.



User Account Configuration Save

Item	Setting
User Name	User-04
Password	••••
Directory	Browse
Permission	Read/Write ▾
Enable	☑

Figure 341 – User Account Configuration

Item	Notes	Description
User Name	String = no blank spaces	Enter the user account name for login to the FTP server. Value Range = 1 - 15 characters.
Password	Alphanumeric string with no blank spaces	Enter the user password for login to the FTP server.
Directory	N/A	Select a root directory after user login.
Permission	**Read/Write** is the default setting.	Select the **Read/write** permission.

Item	Notes	Description
		Note –The embedded FTP Server is only for log file downloading, no write permission is implemented for the user to upload files even where the **Read/Write** option is selected.
Enable	Enabled by default.	Check ☑ **Enable** to activate the FTP user account.

Table 214 – User Account Configuration

7.4 Diagnostic

The NTC-400 Series Router router include a set of simple network diagnosis tools for the administrator to troubleshoot abnormal behaviour or monitor traffic passing through the router. The Packet Analyzer records packets for a designated interface or specific source/destination host. Ping and Tracert tools for testing the network connectivity issues are also available.

7.4.1 Packet Analyzer

The Packet Analyzer can capture packets from specified interface and filter them by user defined rules.

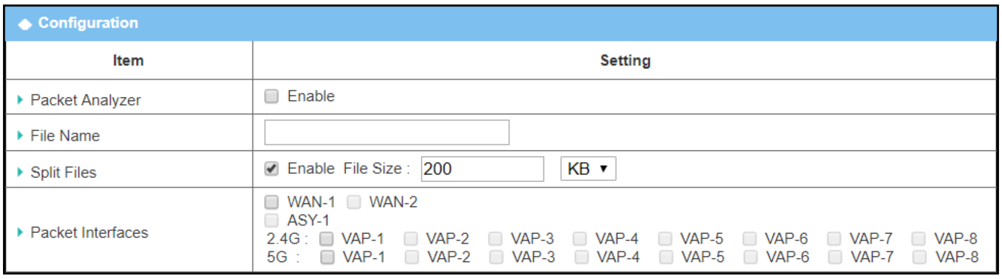
Note that adequate the log storage space must be available either on the embedded SD-Card or external USB Storage, otherwise the Packet Analyzer cannot be enabled.

7.4.1.1 Configure the Packet Analyser

To configure the packet analyser:

1 Select **Diagnostic** from the **Administration** submenu and click the Packet Analyser tab.

2 The packet analyser **Configuration** screen will open:



◆ Configuration

Item	Setting
▸ Packet Analyzer	□ Enable
▸ File Name	
▸ Split Files	☑ Enable File Size : 200 KB ▾
▸ Packet Interfaces	□ WAN-1 □ WAN-2 □ ASY-1 2.4G : □ VAP-1 □ VAP-2 □ VAP-3 □ VAP-4 □ VAP-5 □ VAP-6 □ VAP-7 □ VAP-8 5G : □ VAP-1 □ VAP-2 □ VAP-3 □ VAP-4 □ VAP-5 □ VAP-6 □ VAP-7 □ VAP-8

Figure 342 – Enable Packet Analyzer

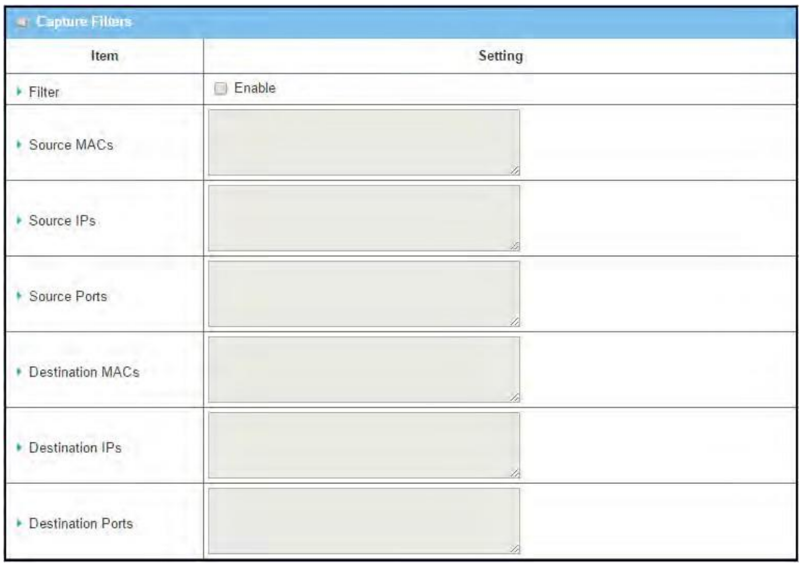
Item	Notes	Description
Packet Analyzer	Disabled by default.	Check ☑ **Enable** activate the Packet Analyzer function. If you cannot enable the checkbox, please check if adequate storage is available. If not, plug in a USB storage device and then enable the Package Analyzer function.
File Name	This setting is optional and is blank by default.	Enter the file name to save the captured packets in log storage. The naming format is: <Interface>_<Date>_<index>

Item	Notes	Description
		If **Split Files** option is also enabled, the file name will be appended with an index code "_<index>". The file extension is: .pcap
Split Files	Optional field. Default File Size: **200 KB**	Check ☑ **Enable** to split the file whenever log file reaches a specified limit. If the **Split Files** option is enabled, you can specify the **File Size** and **Unit** (KB or MB) for the split files. Value Range for file size: 10 - 99999. **NOTE** – File Size cannot be less than 10 KB
Packet Interfaces	Optional field.	Define the interface(s) that Packet Analyzer will work on. At least, one interface is required, but multiple selections are also accepted. The supported interfaces are: **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 a specific field communication protocol, like Modbus, is enabled.
VAP	This means the virtual AP.	When Wi-Fi and VAP are enabled it can be selected here.
Save	Button	Click the **Save** button to save the configuration.
Undo	Button	Click the **Undo** button to restore to the previous setting.

Table 215 – Enable Packet Analyzer

7.4.1.2 Packet Capture Filters

Once the Packet Analyzer function is enabled on specific Interface(s), you can specify filter rules to restrict the capture to packets which match the filter parameters.



Capture Filters

Item	Setting
Filter	□ Enable
Source MACs	
Source IPs	
Source Ports	
Destination MACs	
Destination IPs	
Destination Ports	

Figure 343 – Packet Capture Filters

Item	Notes	Description
Filter	Optional setting	Check ☑ **Enable** box to activate the **Capture Filters** function.
Source MACs	Optional setting	Define the filter rule to include only specific source MAC addresses of packets. Packets which match the rule will be captured. Up to ten MAC addresses are supported and they must be separated with ";". For example: AA:BB:CC:DD:EE:FF; 11:22:33:44:55:66 The packets will be captured when they match any one of the MAC addresses listed in this text box.
Source IPs	Optional setting	Define the filter rule to include only specific source IP addresses of the packets. Packets which match the rule will be captured. Up to ten IPs are supported, but they must be separated with ";". For example: 192.168.1.1; 192.168.1.2 The packets will be captured when they match any one of the IP addresses listed in this text box.
Source Ports	Optional setting	Define the filter rule to include only the source port of packets. Packets which match any port number listed in this text box will be captured. Up to 10 ports are supported, but they must be separated with ";". For example: 80; 53 Value Range = 1 - 65535.

Item	Notes	Description
Destination MACs	Optional setting	Define the filter rule to include only specific destination MAC addresses of packets. Packets which match the rule will be captured. Up to ten MAC addresses are supported and they must be separated with ";". For example: AA:BB:CC:DD:EE:FF; 11:22:33:44:55:66 The packets will be captured when they match any one of the MAC addresses listed in this text box.
Destination IPs	Optional setting	Define the filter rule to include only specific destination IP addresses of the packets. Packets which match the rule will be captured. Up to ten IPs are supported, but they must be separated with ";". For example: 192.168.1.1; 192.168.1.2 The packets will be captured when they match any one of the IP addresses listed in this text box.
Destination Ports	Optional setting	Define the filter rule to include only the destination port of packets. Packets which match any port number listed in this text box will be captured. Up to 10 ports are supported, but they must be separated with ";". For example: 80; 53 Value Range = 1 - 65535.

Table 216 – Packet Capture Filters

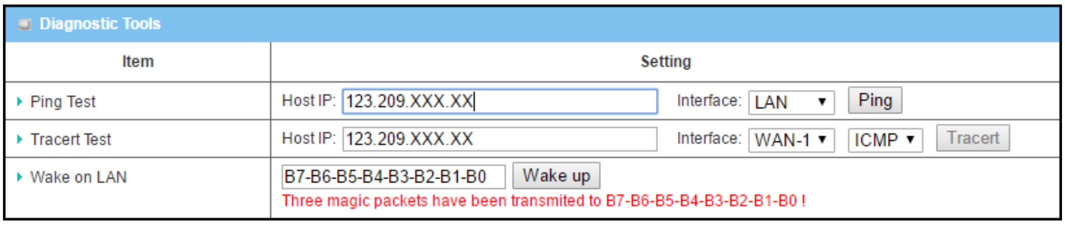
7.4.2 Diagnostic Tools

The Diagnostic Tools provide some frequently used network connectivity diagnostic tools (approaches) for the network administrator to check the device connectivity.

To access the Diagnostic Tools:

1 Select **Diagnostic** from the **Administration** submenu and click the **Diagnostic Tools** tab.

2 The **Diagnostic Tools** screen will display:



Diagnostic Tools

Item	Setting
Ping Test	Host IP: 123.209.XXX.XX Interface: LAN Ping
Tracert Test	Host IP: 123.209.XXX.XX Interface: WAN-1 ICMP Tracert
Wake on LAN	B7-B6-B5-B4-B3-B2-B1-B0 Wake up Three magic packets have been transmited to B7-B6-B5-B4-B3-B2-B1-B0 !

Figure 344 – Diagnostic Tools

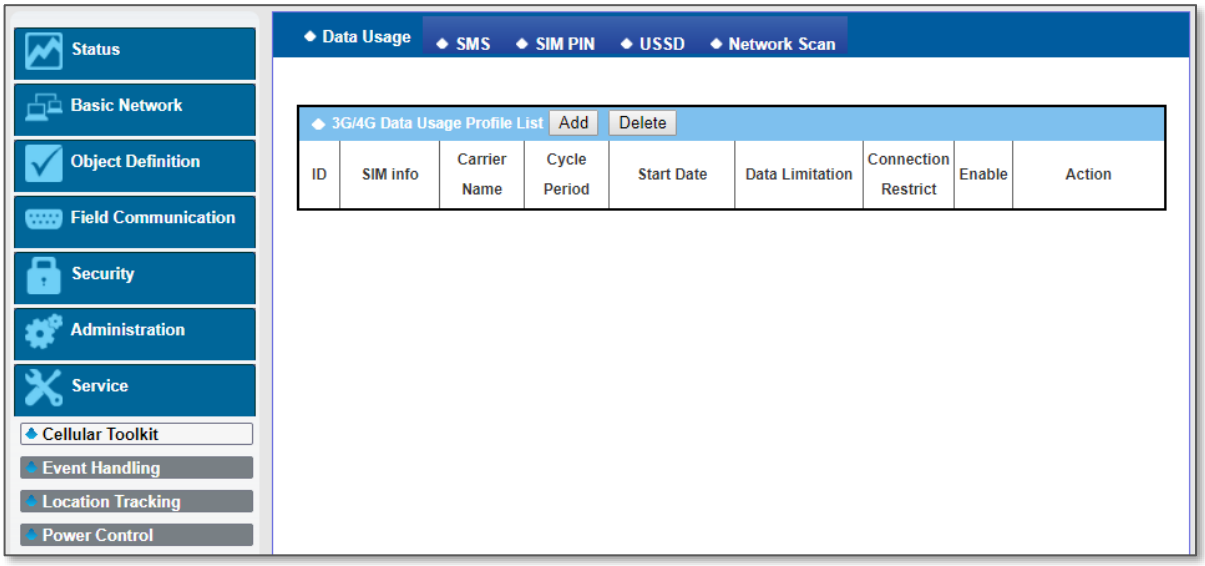
Item	Notes	Description
Ping Test	**Host IP**	Specify an IP / FQDN that the system can 'ping' to test whether the connection is functioning.
	Interface	Select **Auto**, **WAN-1** or **LAN** from the drop-down list. **Auto** is the default setting.
	Ping button	Click the **Ping** button and the **Ping Test Results** window will appear beneath the tools section.
Tracert Test	**Host IP**	Tracert (Trace route) 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. In the **Host IP** text box specify an IP / FQDN address, the test interface (**Auto**) and the protocol (**UDP**, the default, or **ICMP**).
	Interface	Select **Auto**, **WAN-1** or **LAN** from the drop-down list. **Auto** is the default setting.
	Protocol	Select **UDP** or **ICMP** from the drop-down list. **UDP** is the default setting.
	Tracert button	When the **Tracert** button is clicked the system will try to trace the specified host to test whether it is 'alive'. The **Tracert Test Results** window will appear beneath the tools section.
Wake on LAN	Optional setting	Wake on LAN (WOL) is an Ethernet networking standard that allows a computer to be turned on or awakened by a network message. Specify the MAC address of the computer, in your LAN network, to be remotely turned on when the **Wake up** button is clicked.
Save	Button	Click the **Save** button to save the configuration.

Table 217 – Diagnostic Tools

8 Service

8.1 Cellular Toolkit

The **Cellular Toolkit** includes several useful features that are related to cellular configuration or applications. From the toolkit menu, you can configure settings of Data Usage, SMS, SIM PIN, USSD, and Network Scan.



3G/4G Data Usage Profile List

ID	SIM info	Carrier Name	Cycle Period	Start Date	Data Limitation	Connection Restrict	Enable	Action

Figure 345 – Cellular Toolkit - 3G/4G Data Usage Profile list

Note – A valid SIM card is required to be inserted to device before you can work with the settings in this section.

8.1.1 Data Usage

The Data Usage tool can be used to continuously monitor cellular data usage and take action as required. For example, when data usage reaches a set limit the data connection can be stopped. Alternatively, if a secondary SIM card is inserted, at a set limit the device can switch to the secondary SIM and establish another cellular data connection automatically.

If the Data Usage feature is enabled, the cellular data usage history can be viewed at Status > Statistics & Reports > Cellular Usage tab.

In order to set the Data Usage parameters, you need to know your billing start date, billing period, and data quota. This information is normally available from your carrier or ISP.

3G/4G Data Usage

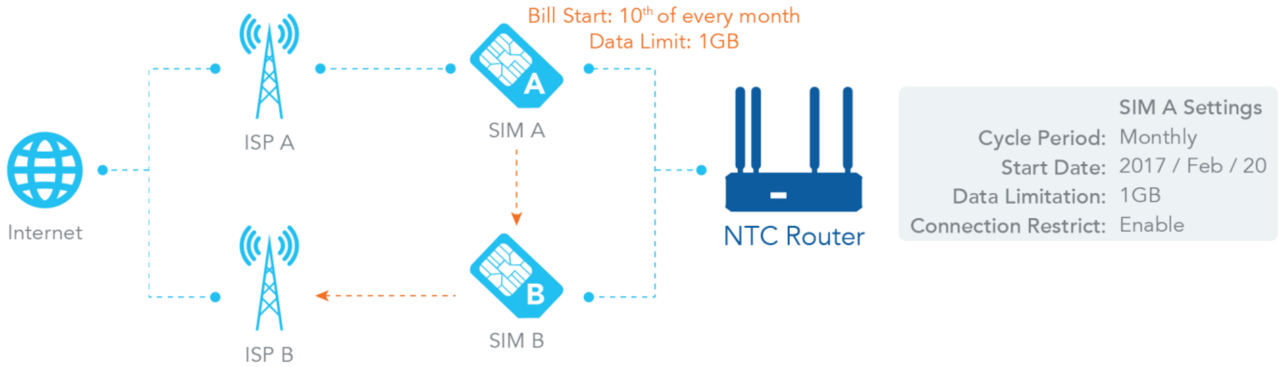


Figure 346 – 3G/4G Data Usage

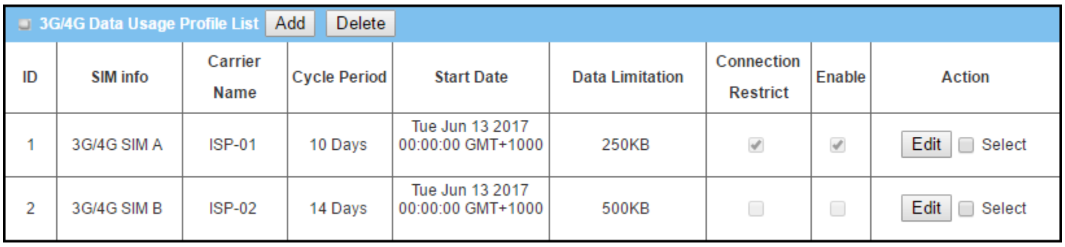
The Data Usage feature enables the router to continuously monitor cellular data usage. In the diagram above, the quota of SIM A is **1Gb** per month and the bill start date is the **20th** of every month. The device starts a new calculation of data usage on the 20th of every month. Enable Connection Restrict forces the router to drop the cellular connection of SIM A when data usage reaches the quota (1Gb in this case). If the SIM failover feature is configured in **Internet Setup**, the router will switch to SIM B and establish a new cellular data connection automatically.

8.1.1.1 3G/4G Data Usage Profile List

To access the Data Usage tools:

1 Select **Cellular Toolkit** from the **Service** submenu and click the **Data Usage** tab.

2 The 3G/4G Data Usage Profile List screen will open:

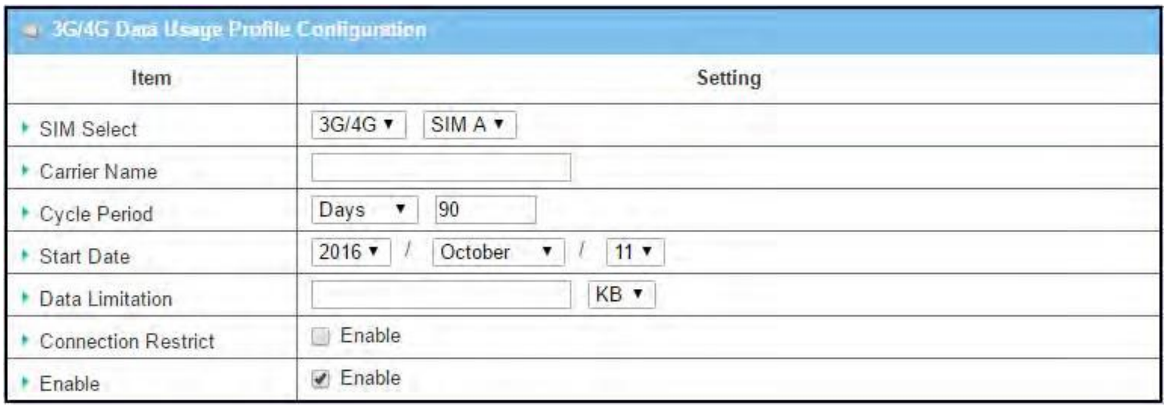


ID	SIM info	Carrier Name	Cycle Period	Start Date	Data Limitation	Connection Restrict	Enable	Action
1	3G/4G SIM A	ISP-01	10 Days	Tue Jun 13 2017 00:00:00 GMT+1000	250KB	☑	☑	Edit □ Select
2	3G/4G SIM B	ISP-02	14 Days	Tue Jun 13 2017 00:00:00 GMT+1000	500KB	□	□	Edit □ Select

Figure 347 – 3G/4G Data Usage Profile List

8.1.1.2 Create / Edit 3G/4G Data Usage Profile

Click the **Add** button to open the **3G/4G Data Usage Profile Configuration** screen. You can create up to two data usage profiles, one profile for each SIM card used in the router.



3G/4G Data Usage Profile Configuration

Item	Setting
SIM Select	3G/4G ▾ SIM A ▾
Carrier Name	
Cycle Period	Days ▾ 90
Start Date	2016 ▾ / October ▾ / 11 ▾
Data Limitation	KB ▾
Connection Restrict	□ Enable
Enable	☑ Enable

Figure 348 – 3G/4G Data Usage Profile Configuration

Item Setting	Notes	Description
SIM Select	**3G/4G-1** and **SIM A** are the default selections.	Choose a cellular interface (**3G/4G-1** or **3G/4G-2**), and a SIM card (**SIM A** or **SIM B**) associated with the selected cellular interface.
Carrier Name	Optional	Fill in the Carrier Name for the selected SIM card for identification purposes.
Cycle Period	Days by default	Select the cycle period type rom the dropdown list: **Days, Weekly** or **Monthly** **Days –** For per Days cycle periods, you have to further specify the number of days in the second box. Value Range: 1 - 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 ☑ **Enable** 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 ☑ **Enable** to activate the data usage profile.

Table 218 – 3G/4G Data Usage Profile Configuration

8.1.2 SMS

Short Message Service (SMS) is a text messaging service which is widely used on mobile phones. It uses standardized communications protocols to allow mobile phones or cellular devices to exchange short text messages.

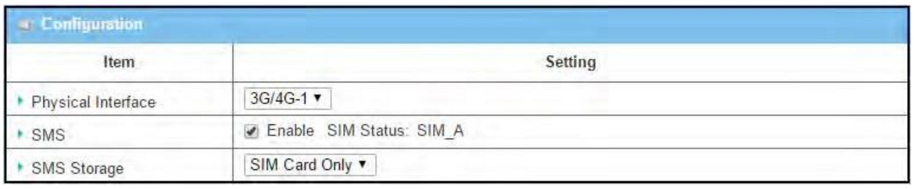
The NTC-400 Series Router router can send SMS text messages or browse received SMS messages.

1 Select **Cellular Toolkit** from the **Service** submenu and click the **SMS** tab.

2 The **SMS** screen containing the **Configuration** and **SMS Summary** sections will open.

8.1.2.1 SMS Configuration

Enable the SMS service and defined its parameters in the **Configuration** section.



Configuration

Item	Setting
Physical Interface	3G/4G-1 ▾
SMS	☑ Enable SIM Status: SIM_A
SMS Storage	SIM Card Only ▾

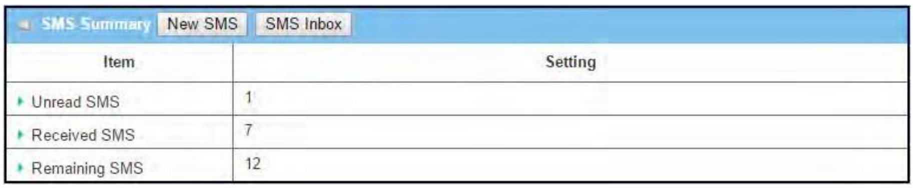
Figure 349 – SMS Configuration

Item	Notes	Description
Physical Interface	3G/4G-1 is the default	Choose between the 3G/4G-1 or 3G/4G-2 cellular interface.
SMS	Enabled by default	Check ☑ **Enable** to activate the SMS service.
SIM Status	System Generated	Displays which SIM is currently in use, either SIM_A or SIM_B.
SMS Storage	SIM Card Only is the default setting.	This is where SMS data is stored. Currently the only option is: SIM Card Only
Save	Button	Click the **Save** button to save the settings

Table 219 – SMS Configuration

8.1.2.2 SMS Summary

The summary page provides a quick view of SMS messages currently on the router, as well as buttons to send a new SMS or view the SMS Inbox.



Item	Setting
Unread SMS	1
Received SMS	7
Remaining SMS	12

Figure 350 – SMS Summary

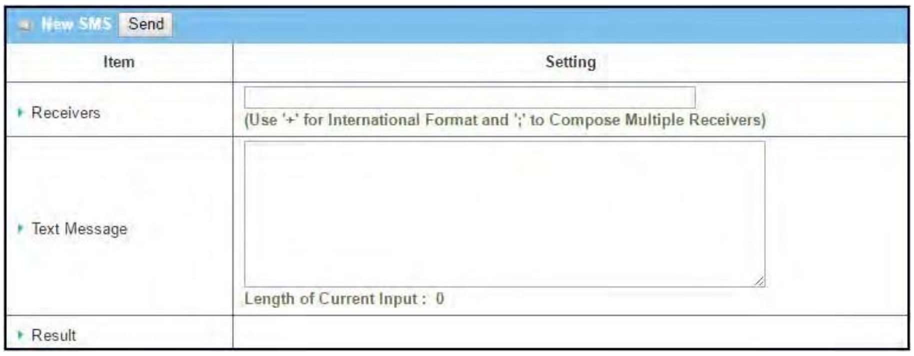
Item	Notes	Description
Unread SMS	System generated.	Number of new SMS messages which have not yet been viewed.

Item	Notes	Description
Received SMS	System generated.	Total number of SMS messages that have been received and displayed.
Remaining SMS	System generated.	The remaining SMS message capacity on the SIM card.
New SMS	Button	Click **New SMS** button to create a new SMS message. Refer to *New SMS* in the next section.
SMS Inbox	Button	Click **SMS Inbox** button to display a list of SMS messages and tools. You can read, delete, reply to or forward SMS messages from this screen. Refer to *SMS Inbox List* in the following section.
Refresh	Button	Click the **Refresh** button to update the SMS summary immediately.

Table 220 – SMS Summary

8.1.2.3 New SMS

Click the **New SMS** button on the SMS Summary screen to create a new SMS message.



Item	Setting
Receivers	(Use '+' for International Format and ';' to Compose Multiple Receivers)
Text Message	Length of Current Input : 0
Result	

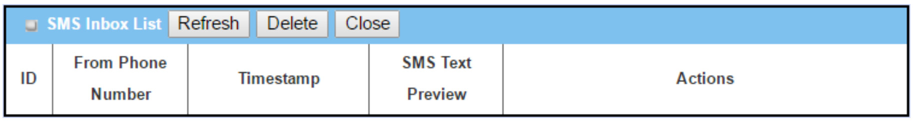
Figure 351 – New SMS

Item	Notes	Description
Receivers	N/A	Enter recipients' SMS numbers/addresses. Separate multiple recipients' details with a semicolon (;).
Text Message	N/A	Write the SMS message content.
Send	Button	Click the **Send** button to transmit the SMS message.
Result	System generated.	If the SMS is successfully transmitted, **OK** will display. Otherwise **Send Failed** will be displayed.

Table 221 – New SMS

8.1.2.4 SMS Inbox List

You can read or delete SMS, reply SMS or forward SMS from this screen.



ID	From Phone Number	Timestamp	SMS Text Preview	Actions

Figure 352 – SMS Inbox List

Item	Notes	Description
ID	System generated.	The number or SMS.
From Phone Number	System generated.	The phone number that sent the SMS
Timestamp	System generated.	Time when the SMS was received.
SMS Text Preview	System generated.	Preview the SMS text. Click the **Detail** button to read the entire message.
Action	Disabled by default	Click the **Detail** button to read the SMS. Click **Reply / Forward** button to reply to or forward the SMS. Check the box(es), and then click the **Delete** button to delete the SMS(s) that are checked.
Refresh	Button	**Refresh** the SMS Inbox List.
Delete	Button	**Delete** the SMS(s) that are checked.
Close	Button	**Close** the Detail SMS Message screen.

Table 222 – SMS Inbox List

8.1.3 SIM PIN

Enabling a PIN code for the SIM card is an easy and effective way of protecting cellular devices from unauthorized access. The NTC-400 Series Router allows you to activate and manage PIN code on a SIM card through its web GUI.

Activate PIN code on SIM card

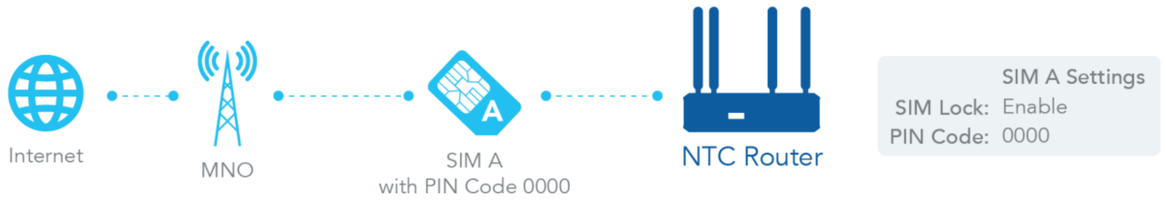


Figure 353 – Activate PIN code on SIM card

The NTC-400 Series Router allows you to activate a PIN code on the SIM card. This example shows a PIN code on SIM-A for 3G/4G-1 with default PIN code “**0000**”.

Change PIN code on SIM card

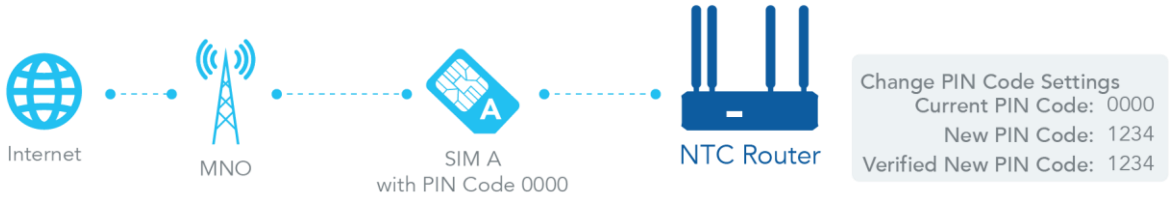


Figure 354 – Change PIN code on SIM card

The NTC-400 Series Router allows you to change the PIN code on the SIM card. In the example above, you need to type original PIN code “**0000**” and then type the new PIN code ‘**1234**’, if you want to set the new PIN code as ‘**1234**’. To confirm the new PIN code, re-type the new PIN code in the Verified New PIN Code field again.

Unlock SIM card by PUK Code

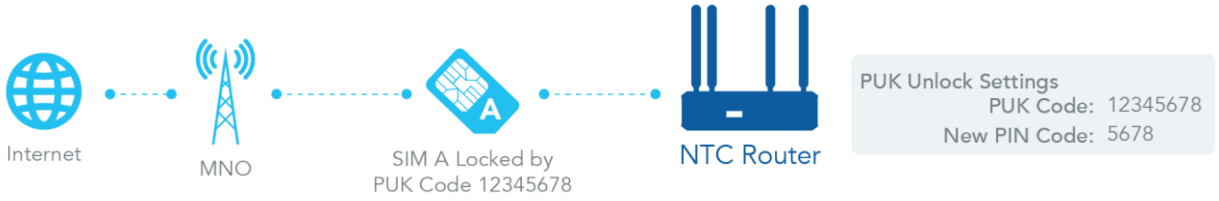


Figure 355 – Unlock SIM card by PUK code

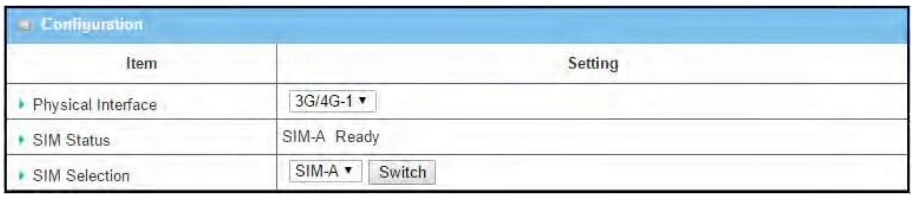
If you entered an incorrect PIN code at the configuration page for 3G/4G-1 WAN more than three times, it causes the SIM card to be “PUK locked”. To unlock a PUK locked SIM, you have to contact your carrier to get a PUK unlock code. In the diagram above, the PUK code is “**12345678**” and new PIN code is “**5678**”.

1 Select **Cellular Toolkit** from the **Service** submenu and click the **SIM PIN** tab.

2 The packet analyser **SIM PIN** screen will open. It contains three sections: **Configuration**, **PUK function** and **SIM function**.

8.1.3.1 SIM PIN Configuration

With the SIM PIN Configuration section allows you to select a SIM and set its status and interface.



Configuration

Item	Setting
Physical Interface	3G/4G-1 ▾
SIM Status	SIM-A Ready
SIM Selection	SIM-A ▾ Switch

Figure 356 – SIM PIN Configuration

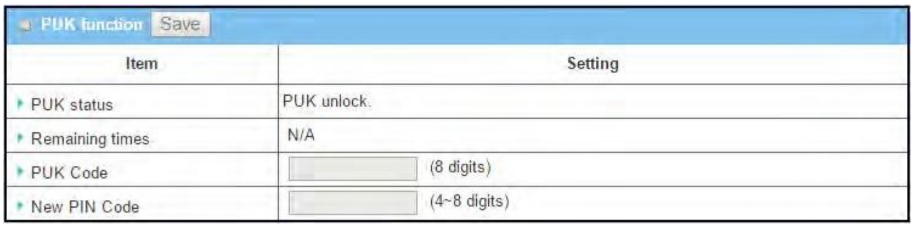
Item	Notes	Description
Physical Interface	The box is 3G/4G-1 by default	Choose a cellular interface (3G/4G-1 or 3G/4G-2) to change the SIM PIN setting for the selected SIM Card.
SIM Status	System generated	Indication for the selected SIM card and the SIM card status. The status can be: **Ready**, **Not Insert**, or **SIM PIN** **Ready** – A SIM card is inserted and ready to use. It can be a SIM card without PIN protection or a SIM card unlocked by its correct PIN code. **Not Insert** – The SIM slot currently does not have a SIM card inserted. **SIM PIN** -- SIM card is protected by PIN code, and it’s not unlocked by a correct PIN code yet. The SIM card is still in locked status.
SIM Selection	Drop down list and button	Select the SIM card for further SIM PIN configuration. Press the **Switch** button to have the router switch from one SIM card to another. After that, you can configure the SIM card.

Table 223 – SIM PIN Configuration

8.1.3.2 Unlock with a PUK Code

The **PUK Function** window is only available if the SIM card is locked by its PUK (PIN Unblocking Key) lock. Usually this happens after too many entries of an incorrect PIN code (normally three attempts) and the SIM card becomes locked. At this point it can only be unlocked using its PUK.

Normally you will be supplied with the PUK code when you purchase the SIM card. If you have misplaced or otherwise forgotten the PUK code you will need to contact your service provider and request a PUK code for your SIM card.



Item	Setting
PUK status	PUK unlock.
Remaining times	N/A
PUK Code	(8 digits)
New PIN Code	(4~8 digits)

Figure 357 – Unlock with PUK Code

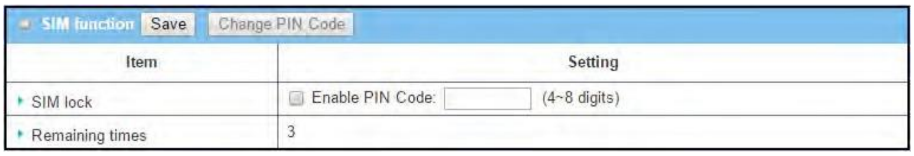
Item	Notes	Description
PUK status	PUK Unlock / PUK Lock	Indicates the current PUK status. As mentioned previously the SIM card will be locked by PUK code after too many failed PIN code entry attempts. In this case, the PUK Status will turns to PUK Lock. In normal situations, it will display PUK Unlock.
Remaining times	Depends on the SIM card	The remaining number of attempts before the PUK lock is applied. ⚠ **Warning** – **DO NOT** set Remaining times at zero as this will damage the SIM card **FOREVER!** Call for your ISP to get a correct PUK if you have forgotten or otherwise do not have the correct PUK code.
PUK Code	Required field.	Enter the PUK code that can unlock the SIM card.
New PIN Code	Required field.	Enter the New PIN Code for the SIM card. Remember the PIN code (password).
Save	Button	Click the **Save** button to apply the setting.

Table 224 – Unlock with PUK Code

⚠ **Important** – When you change the PUK code and PIN code for the SIM card, you must also change the corresponding PIN code specified in the **Basic Network | WAN & Uplink | Internet Setup | Connection with SIM Card** page.

8.1.3.3 Enable / Change PIN Code

Go to the **SIM function** section to enable or disable the PIN code (password) function, or to change the PIN code.



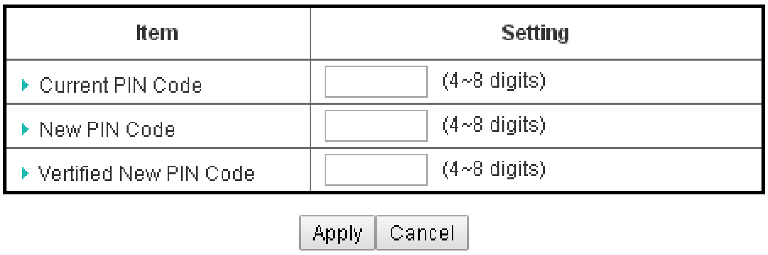
Item	Setting
SIM lock	□ Enable PIN Code: (4~8 digits)
Remaining times	3

Figure 358 – Enable / Change PIN Code

Item Setting	Notes	Description
SIM lock	Depends on the SIM card	Click ☑ **Enable** to activate the SIM lock function. To enable the SIM lock function, enter the PIN code and click Save to apply the setting.
Remaining times	Depends on the SIM card	Represent the remaining number of attempts to enter the SIM PIN. If you exceed the number of allowed attempts, a PUK code will be required to unlock the SIM card.
Save	Button	Click the **Save** button to apply the setting.
Change PIN Code	Button	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 that case, if you want to change the PIN code, you have to first enable the SIM Lock function, 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.

Table 225 – Enable / Change PIN Code

When **Change PIN Code** button is clicked, the following screen appears.



Item	Setting
Current PIN Code	(4~8 digits)
New PIN Code	(4~8 digits)
Verified New PIN Code	(4~8 digits)

Figure 359 – Change PIN Code

Item	Notes	Description
Current PIN Code	Required field.	Enter the current (old) PIN code of the SIM card.
New PIN Code	Required field.	Enter the new PIN Code you want to change.
Verified New PIN Code	Required field.	Re-enter the new PIN Code to confirm the new PIN Code.
Apply	Button	Click the **Apply** button to change the old PIN code to the new PIN code.
Cancel	Button	Click the **Cancel** button to cancel the changes and keep current PIN code.

Table 226 – Change PIN Code

Important – When you change the PIN code for the SIM card, you must also change the corresponding PIN code specified in the **Basic Network | WAN & Uplink | Internet Setup | Connection with SIM Card** page.

8.1.4 USSD

Unstructured Supplementary Service Data (USSD) is a protocol used by GSM cellular telephones to communicate with the service provider's computers via instant bi-directional communication. USSD can be used for WAP browsing, 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.

A USSD message can be 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 data. This makes USSD more responsive than services that use SMS.

USSD Scenario

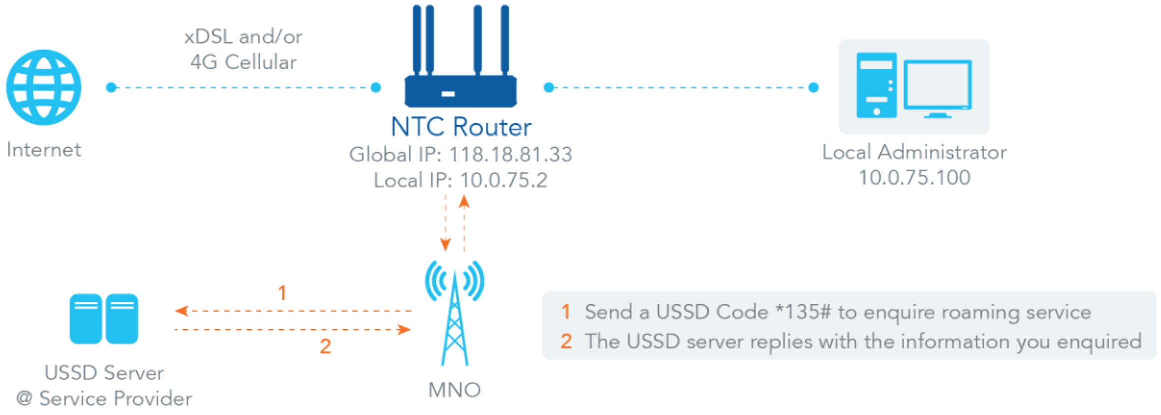


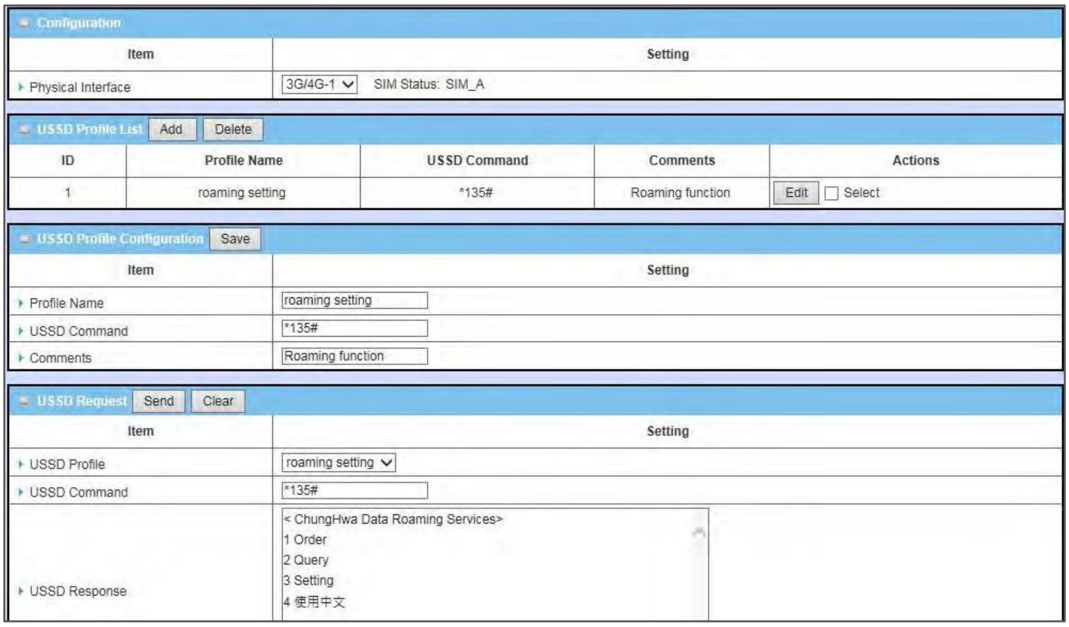
Figure 360 – USSD Scenario

USSD allows you to have an instant bi-directional communication with your carrier. In the diagram above, the USSD command '***135#**' refers to data roaming services. After sending that USSD command to your carrier, you will see a response on the USSD Response window. Please note the USSD command varies for different carriers.

The NTC-400 Series Router allows you to activate and manage USSD services via a SIM card through its web GUI.

1 Select **Cellular Toolkit** from the **Service** submenu and click the **USSD** tab.

2 The USSD screen will open. It contains up to four sections: **Configuration**, **USSD Profile List**, **USSD Profile Configuration** and **USSD Request**



Configuration

Item	Setting
Physical Interface	3G/4G-1 SIM Status: SIM_A

USSD Profile List Add Delete

ID	Profile Name	USSD Command	Comments	Actions
1	roaming setting	*135#	Roaming function	Edit □ Select

USSD Profile Configuration Save

Item	Setting
Profile Name	roaming setting
USSD Command	*135#
Comments	Roaming function

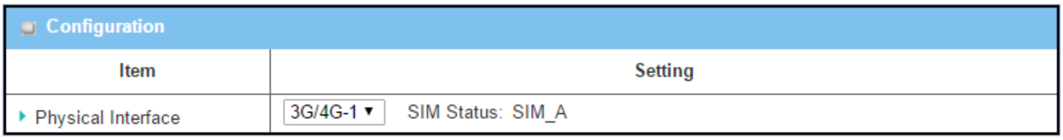
USSD Request Send Clear

Item	Setting
USSD Profile	roaming setting
USSD Command	*135#
USSD Response	< ChungHwa Data Roaming Services> 1 Order 2 Query 3 Setting 4 使用中文

Figure 361 – USSD interface

8.1.4.1 USSD Configuration

In the **Configuration** section you specify which 3G/4G module (physical interface) is used for the USSD function and the system will show which SIM card is currently being used.



Configuration

Item	Setting
Physical Interface	3G/4G-1 SIM Status: SIM_A

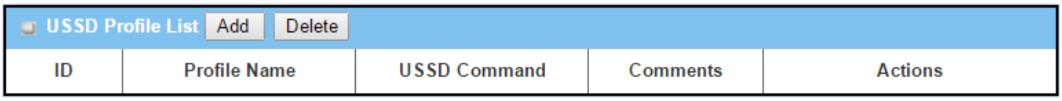
Figure 362 – USSD Configuration

Item	Notes	Description
Physical Interface	The default setting is: 3G/4G-1	Choose a cellular interface (3G/4G-1 or 3G/4G-2) to configure the USSD setting for the connected cellular service.
SIM Status	System generated	The SIM card (identified with SIM_A or SIM_B) that is associated with the selected cellular service.

Table 227 – USSD Configuration

8.1.4.2 Create / Edit USSD Profile

The **USSD Profile List** section shows all your defined USSD profiles that store pre-commands for activating USSD sessions.



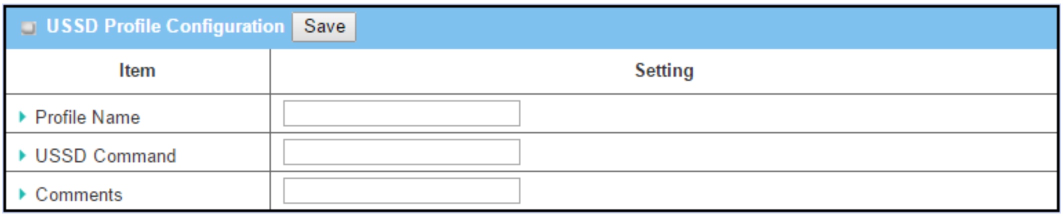
USSD Profile List Add Delete

ID	Profile Name	USSD Command	Comments	Actions

Figure 363 – USSD Profile List

You can add a maximum of 35 custom USSD profiles.

When **Add** button is applied, **USSD Profile Configuration** screen displays.



USSD Profile Configuration Save

Item	Setting
Profile Name	
USSD Command	
Comments	

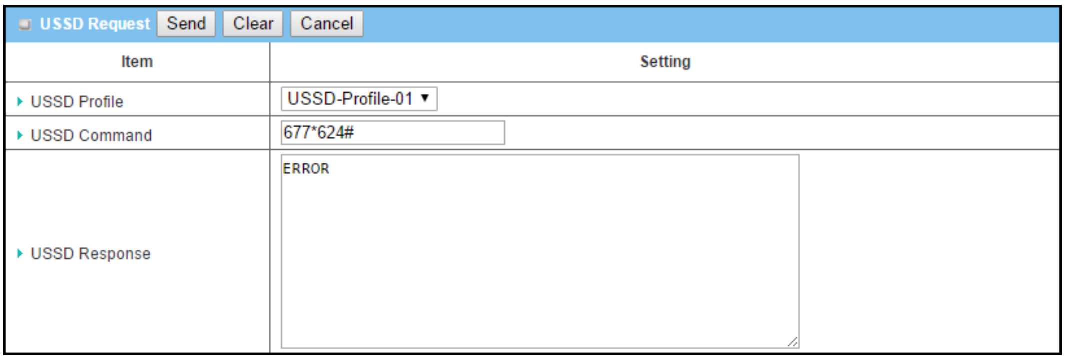
Figure 364 – USSD Profile Configuration

Item	Notes	Description
Profile Name	Text entry box.	Enter a name for the USSD profile.
USSD Command	Text entry box.	Enter the USSD command defined for the profile. Normally, it is a command string composed with numeric keypad “0 - 9”, “*”, and “#”. The USSD commands are specific to your cellular service, please check with your service provider for details.
Comments	Text entry box.	Enter a brief comment for the profile.

Table 228 – USSD Profile Configuration

8.1.4.3 USSD Request and Response

Send USSD commands from the **USSD Request** screen, once sent, the **USSD Response** text box will appear.



USSD Request Send Clear Cancel

Item	Setting
USSD Profile	USSD-Profile-01 ▾
USSD Command	677*624#
USSD Response	ERROR

Figure 365 – USSD Request

Item	Notes	Description
USSD Profile	Text entry box.	Select a USSD profile name from the dropdown list. User defined USSD profiles store pre-defined commands for activating an USSD session.

Item	Notes	Description
USSD Command	Text entry box.	The USSD Command string of the selected profile will be shown here.
USSD Response	buttons	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. The **Clear** button will cause the USSD Response text box to disappear.

Table 229 – USSD Profile Configuration

8.1.5 Network Scan

The Network Scan function allows an administrator to specify how to connect the device to the mobile system for data communication in each 3G/4G interface. For example, administrator can specify the mobile system, 2G, 3G or LTE, used for a connection and can set the router to automatically connect to the mobile system. The Administrator can also manually scan the mobile systems, select a target system and apply it. The manual scanning approach is often used for diagnostics.

8.1.5.1 Network Scan Setting

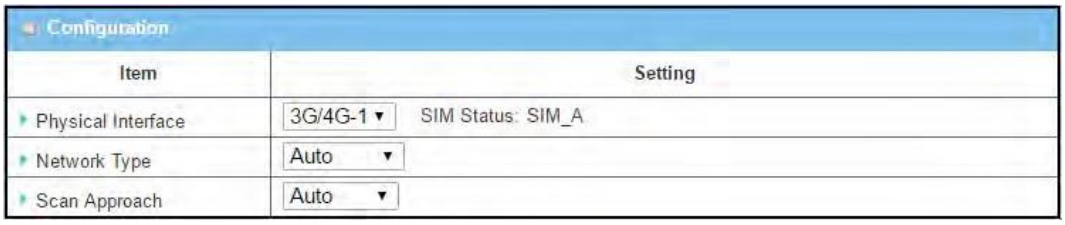
To access the Network Scan settings and tools:

1 Select **Cellular Toolkit** from the **Service** submenu and click the **Network Scan** tab.

2 The **Network Scan** page contains two sections relating to the USSD functionality:

8.1.5.2 Configuration

The **Configuration** section contains settings for network scans.


Configuration

Item	Setting
Physical Interface	3G/4G-1 ▾ SIM Status: SIM_A
Network Type	Auto ▾
Scan Approach	Auto ▾

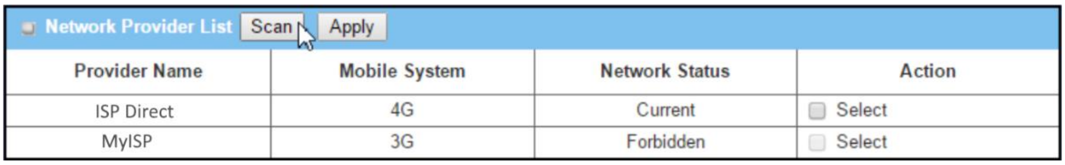
Figure 366 – Network Scan Configuration

Item	Notes	Description
Physical Interface	Default setting: **3G/4G-1**	Choose a cellular interface (3G/4G-1 or 3G/4G-2) for the network scan service.
SIM Status	System generated	The system displays the SIM card (identified with **SIM_A** or **SIM_B**) associated with the selected cellular service.
Network Type	Default setting: **Auto**	Specify the network type for the network scan function. **Auto** – When Auto is selected, the network will be register automatically; **2G prefer or 3G prefer** – If the 'prefer' option is selected, network will be registered for your chosen option first;

Item	Notes	Description
		2G Only, 3G Only or 4G Only – If an 'only' option is selected, network will be register for your chosen option only.
Scan Approach	Default setting: **Auto**	When **Auto** is selected, the cellular module registers automatically. If the Manually option is selected, a Network Provider List screen appears, see next section for details. Press the Scan button to scan for the nearest access point.. Select the preferred base stations then click Apply button to apply settings.
Save	Button	Click **Save** to save the settings

Table 230 – USSD Request

When **Manually** is selected in the **Scan Approach** configuration setting, press the **Scan** button to scan for a list of the nearest available access point. The scan may last for 1 to 3 minutes and the base stations will be added to the Network Provider List as they are identified.



Provider Name	Mobile System	Network Status	Action
ISP Direct	4G	Current	□ Select
MyISP	3G	Forbidden	□ Select

Figure 367 – Network Provider List

Item	Notes	Description
Provider Name	Name of provider	
Mobile System	3G/4G	The system displays the SIM card (identified with **SIM_A** or **SIM_B**) associated with the selected cellular service.
Network Status	System generated	**Current** – the currently selected network **Forbidden** – a detected network but one which is not available to connect to.
Select	button	☑ Select the preferred network then click **Apply** button to apply settings.
Scan	button	Click the **Scan** button to scan for the nearest network.
Apply	button	Click the **Apply** button to apply settings.

Table 231 – Network Provider List

Click again on the "Apply" button to drive system to connect to that mobile operator system for the dedicated 3G/4G interface.

8.2 Event Handling

Event handling allows an administrator to set up pre-defined event profiles of scenarios or incidents for which a standard response can be defined and pre-assigned. The response can be an action or a message.

An action response is referred to as a *Managing Event* in which the router takes action to change functionality, collect status details and change the status of relevant processes or devices.

A message generated in response to an event is referred to as a *Notifying Event*. Examples including an event generated from a connected sensor which results in a SMS message, Email or SNMP Trap being used to alert an administrator.

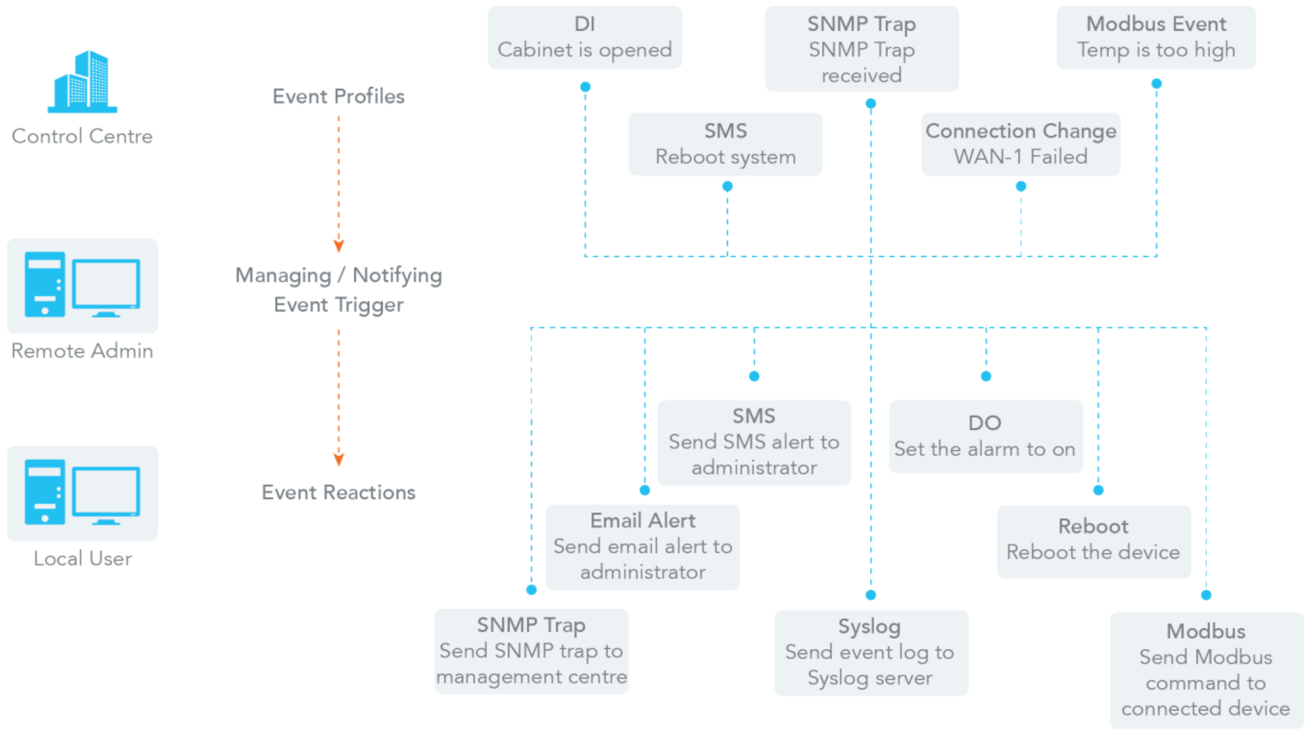


Figure 368 – Event Handling

To use the event handling functionality, you must first define the triggering events in the **Configuration** tabbed sections, then you assign either a **Managed Event** response or a **Notifying Event** response on their respective tabbed pages.

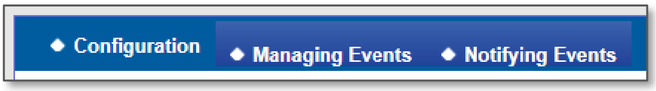
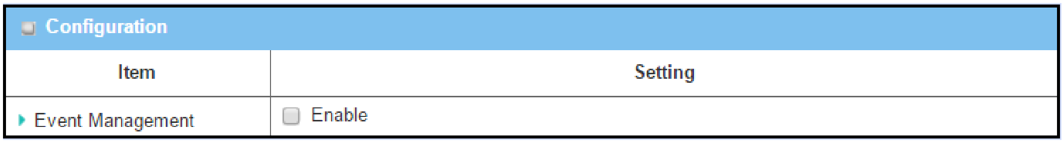


Figure 369 – Event Handling tabs

8.2.1 Configuration

Event handling is the service that allows administrator to setup the pre-defined events, handlers, or response behaviour with individual profiles.

8.2.1.1 Enable Event Management



Configuration

Item	Setting
Event Management	□ Enable

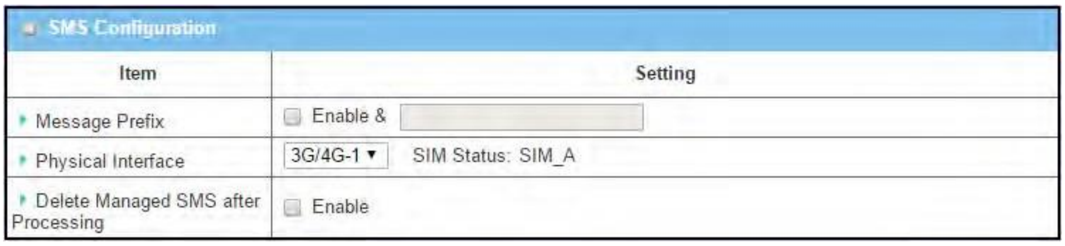
Figure 370 – Enable Event Management

Item	Notes	Description
Event Management	Disabled by default.	Check the ☑ **Enable** box to activate the Event Management function.

Table 232 – Enable Event Management

8.2.1.2 Enable SMS Management

To use the SMS management function, you must nominate an SMS message prefix that triggers the Event Handler to treat the message in a specific way.



SMS Configuration

Item	Setting
Message Prefix	□ Enable &
Physical Interface	3G/4G-1 ▾ SIM Status: SIM_A
Delete Managed SMS after Processing	□ Enable

Figure 371 – Enable SMS Management

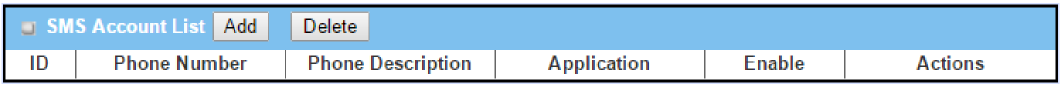
8.2.1.3 SMS Configuration

Item	Notes	Description
Message Prefix	Disabled by default.	Check the ☑ **Enable** box to activate the SMS prefix for validating the received SMS. Once the function is enabled, enter the text of the prefix in the text box. 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	Default setting: **3G/4G-1**	Choose a cellular interface (**3G/4G-1** or **3G/4G-2**) to handle the SMS messaging.
SIM Status	System generated.	Show the connected cellular service (identified with **SIM_A** or **SIM_B**).
Delete Managed SMS after Processing	Disabled by default.	Check ☑ **Enable** to delete the received managing event SMS after it has been processed.

Table 233 – Enable SMS Management

8.2.1.4 Create / Edit SMS Account

Setup an SMS Account for managing the router through the SMS. It supports up to a maximum of 5 accounts.



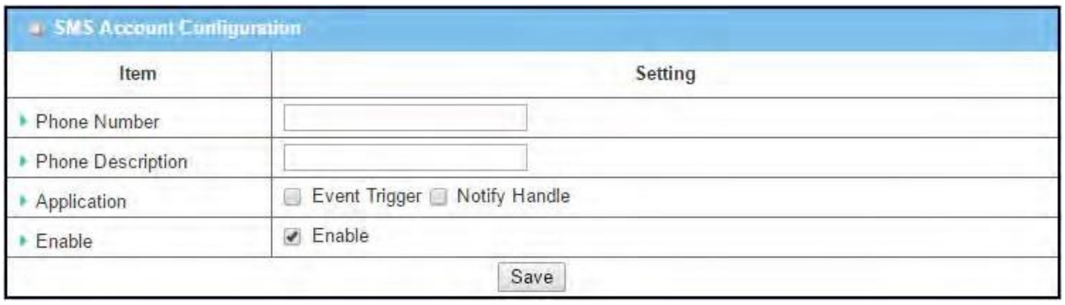
SMS Account List Add Delete

ID	Phone Number	Phone Description	Application	Enable	Actions

Figure 372 – SMS Account List

8.2.1.5 SMS Account Configuration

Click the **Add / Edit** button to configure the SMS account.



SMS Account Configuration

Item	Setting
Phone Number	
Phone Description	
Application	□ Event Trigger □ Notify Handle
Enable	☑ Enable

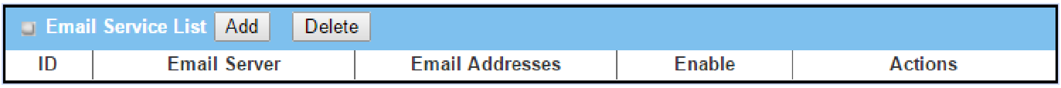
Figure 373 – MS Account Configuration

Item	Notes	Description
Phone Number	Mobile phone number format Mandatory field.	Specify a mobile phone number as the SMS account identifier. Value Range: -1 - 32 digits.
Phone Description	Any text Optional field.	Specify a brief description for the SMS account.
Application	Mandatory field.	Specify the application type: Event Trigger, Notify Handle, or Both.
Enable	Disabled by default.	Click ☑ **Enable** to activate this account.
Save	Button	Click the **Save** button to save the configuration.

Table 234 – MS Account Configuration

8.2.1.6 Create / Edit Email Service Account

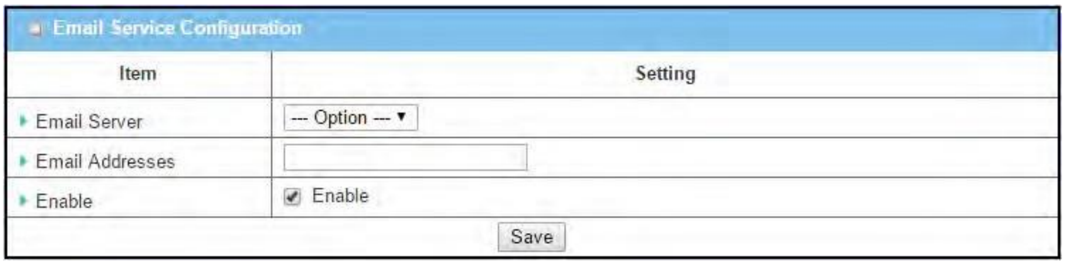
You can create up to five Email Service Accounts for event notification.



ID	Email Server	Email Addresses	Enable	Actions

Figure 374 – Email Service List

Click the **Add / Edit** button to configure the Email account.



Email Service Configuration

Item	Setting
Email Server	--- Option --- ▾
Email Addresses	
Enable	☑ Enable

Figure 375 – Email Service Configuration

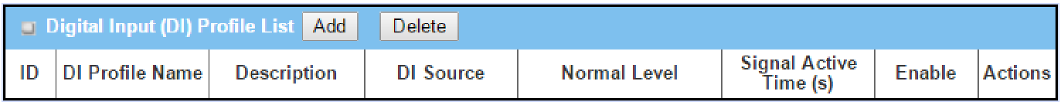
Item	Notes	Description
Email Server	--- Option ---	Select an Email Server profile from External Server setting for the email account setting.
Email Addresses	Internet E-mail address format Mandatory field.	Specify the Destination Email Addresses.

Item	Notes	Description
Enable	Disabled by default.	Click ☑ **Enable** to activate this account.
Save	Button	Click the **Save** button to save the configuration.

Table 235 – Email Service Configuration

8.2.1.7 Create / Edit Digital Input (DI) Profile Rule

If you have DI/DO support you can create up to ten Digital Input (DI) Profile rules.

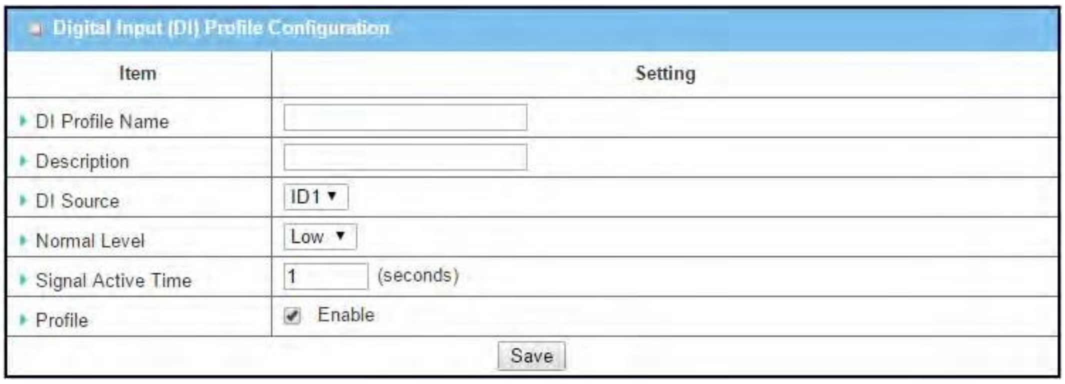


Digital Input (DI) Profile List Add Delete

ID	DI Profile Name	Description	DI Source	Normal Level	Signal Active Time (s)	Enable	Actions

Figure 376 – Digital Input (DI) Profile List

When **Add** button is applied, the **Digital Input (DI) Profile Configuration** screen appears.



Digital Input (DI) Profile Configuration

Item	Setting
DI Profile Name	
Description	
DI Source	ID1 ▾
Normal Level	Low ▾
Signal Active Time	1 (seconds)
Profile	☑ Enable

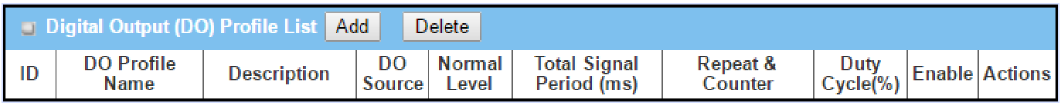
Figure 377 – Digital Input (DI) Profile Configuration

Item	Notes	Description
DI Profile Name	Mandatory field. String format.	Specify the DI Profile Name. Value Range: -1 - 32 characters.
Description	Optional field. Any text string.	Write a brief, meaningful description of the profile.
DI Source	ID1 by default	Specify the DI Source: 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: Low or High
Signal Active Time	Mandatory field. Numeric String format.	Specify the Signal Active Time. Value Range: 1 - 10 seconds.
Profile	Disabled by default.	Click ☑ **Enable** to activate this account.
Save	Button	Click the **Save** button to save the configuration.

Table 236 – Digital Input (DI) Profile Configuration

8.2.1.8 Create / Edit Digital Output (DO) Profile Rule

If you have DI/DO support you can create up to ten Digital Output (DO) Profile rules.

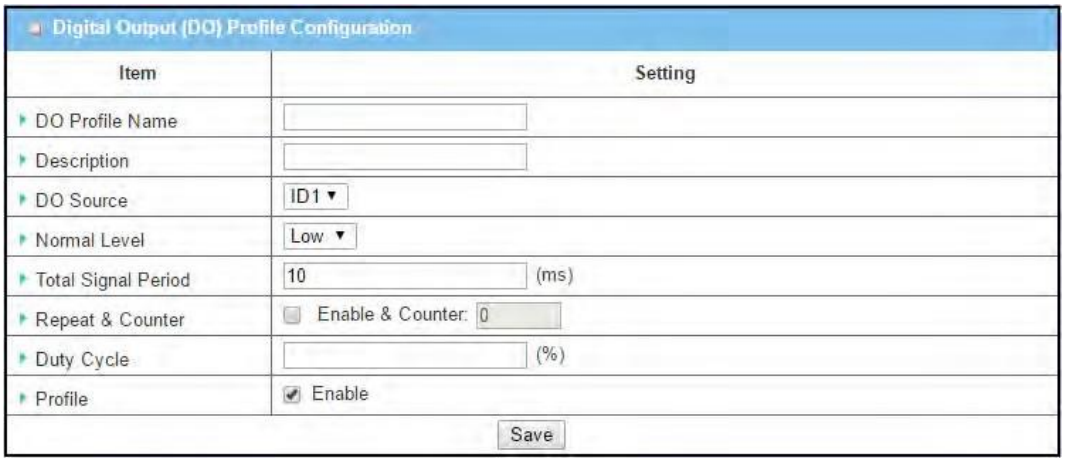


Digital Output (DO) Profile List | Add | Delete

ID	DO Profile Name	Description	DO Source	Normal Level	Total Signal Period (ms)	Repeat & Counter	Duty Cycle(%)	Enable	Actions

Figure 378 – Digital Output (DO) Profile List

When **Add** button is applied, the **Digital Output (DO) Profile Configuration** screen will appear.



Digital Output (DO) Profile Configuration

Item	Setting
DO Profile Name	
Description	
DO Source	ID1 ▾
Normal Level	Low ▾
Total Signal Period	10 (ms)
Repeat & Counter	□ Enable & Counter: 0
Duty Cycle	(%)
Profile	☑ Enable

Save

Figure 379 – Digital Output (DO) Profile Configuration

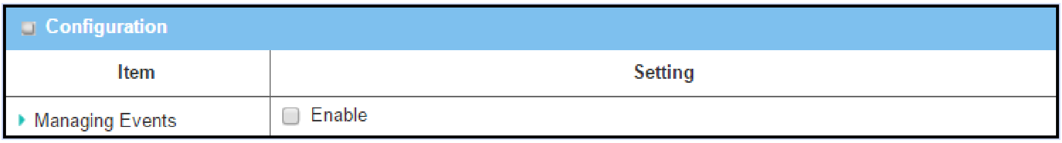
Item	Notes	Description
DO Profile Name	Mandatory field. String format.	Specify the DO Profile Name. Value Range: -1 - 32 characters.
Description	Optional field. Any text.	Write a brief, meaningful description of the profile.
DO Source	Default setting: **ID1**	Specify the DO Source as ID1.
Normal Level	Default setting: **Low**	Specify the Normal Level: Low or High
Total Signal Period	Mandatory field. Numeric String format	Specify the Total Signal Period. Value Range: 10 - 10000 ms.
Repeat & Counter	Disabled by default.	Click ☑ **Enable** to activate the repeated Digital Output, and specify the Repeat times. Value Range: 0 - 65535.
Duty Cycle	Mandatory field. Numeric String format	Specify the Duty Cycle for the Digital Output. Value Range: 1 - 100 %
Profile	Disabled by default.	Click ☑ **Enable** to activate this profile setting.
Save	Button	Click the **Save** button to save changes to the configuration.

Table 237 – Digital Output (DO) Profile Configuration

8.2.2 Managing Events

Managing Events allow administrator to define the relationships (rules) between event triggers, handlers and responses.

Managing Events functionality is disabled by default, to enable this tool select **Event Handling** from the **Service** submenu and click on the **Managing Events** tab.



Configuration

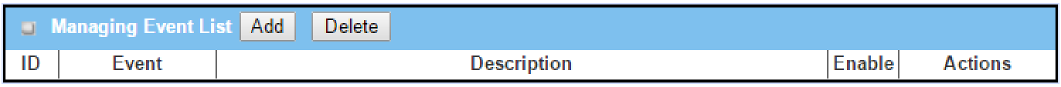
Item	Setting
Managing Events	□ Enable

Figure 380 – Enable Managing Events

Item	Notes	Description
Managing Events	Disabled by default.	Click ☑ **Enable** to activate the Managing Events functionality.

Table 238 – Enable Managing Events

The **Managing Event List** supports a maximum of 128 rules.



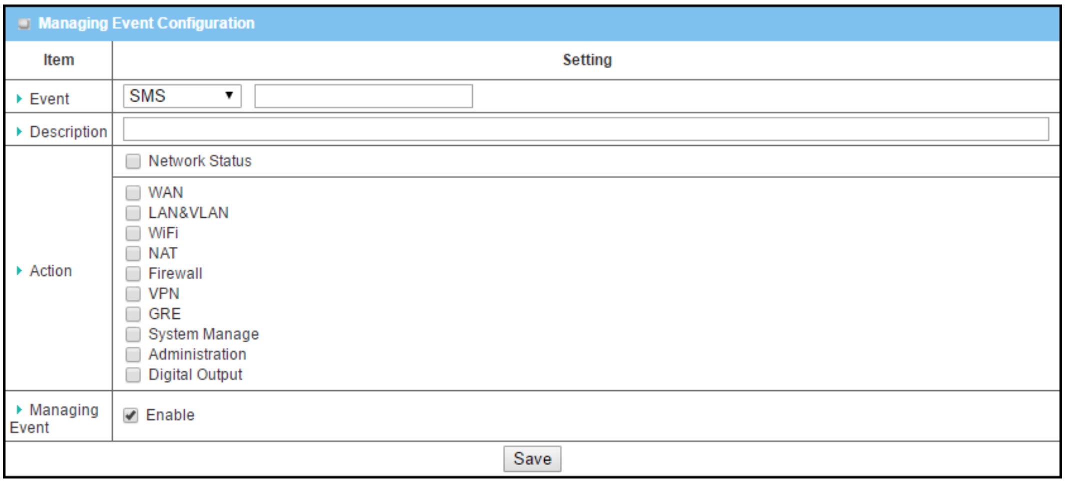
Managing Event List Add Delete

ID	Event	Description	Enable	Actions

Figure 381 – Managing Event List

Click the **Add** button.

The **Managing Event Configuration** screen will display.



Managing Event Configuration

Item	Setting
Event	SMS ▾
Description	
Action	□ Network Status □ WAN □ LAN&VLAN □ WiFi □ NAT □ Firewall □ VPN □ GRE □ System Manage □ Administration □ Digital Output
Managing Event	☑ Enable

Save

Figure 382 – Managing Event Configuration

Item	Notes	Description
Event	SMS by default	Specify the Event type (SMS, SNMP Trap, or DI) and an event identifier / profile. **SMS** – Select SMS and type the trigger condition for the event in the textbox; **SNMP Trap** – Select SNMP Trap and specify the SNMP Trap Event in the textbox; **Digital Input** – Select Digital Input and a DI profile you defined to specify a certain Digital Input Event; **Note** – Available Event Types can differ between products.

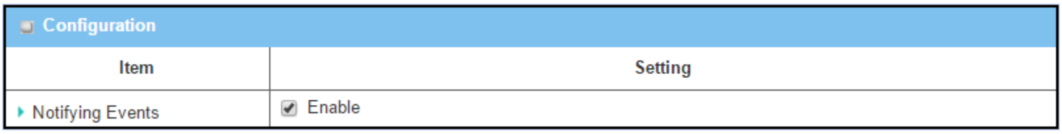
Item	Notes	Description
Description	Any text.	Write a brief, meaningful description of the event rule.
Action	All disabled by default.	Specify Network Status, or at least one rest action to take when the expected event is triggered. **Network Status** – Uses the network status as the action for the event. If this is selected, not other Actions are available.; **LAN** – Allows the event to trigger the following settings: – Connect/Disconnect Port link – Set to Auto, LTE or 3G – Switch to SIM A or SIM B **LAN&VLAN** – Three Port Links can be turned On or Off when the event is triggered; **Wi-Fi** – Allows the event to turn Wi-Fi 2.4G or Wi-Fi 5G on or off; **NAT** – Allows the event to trigger predefined Virtual Server Rules to be turned on or off and the DMZ to be turned on or off; **Firewall** – Allows the event to trigger five Remote Administrator Host IDs to be turned on or off, and to turn WAN Discard Ping on or off; **VPN** – Allows the event to trigger a number of IPSec, PPTP Client, L2TP Client and Open VPN Client settings; **GRE** – Allows the event to trigger on or off a number of GRE (Generic Routing Encapsulation) connections; **System Manage** – Allows the event to trigger on or off either WAN SSH or TR-069 services; **Administration** – Allows the event to trigger one of the following administrative activities: **– Backup Config;** **– Restore Config;** **– Reboot;** **– Save Current Setting as Default;** **Digital Output** – Allows the event to trigger a Digital Output (DO) profile you defined; **Modbus** – Select the Modbus checkbox and a Modbus Managing Event profile you defined as the action for the event; **Note** – Available Actions can differ between products.
Managing Event	Disabled by default.	Click ☑ **Enable** to activate the Managing Events rule.
Save	Button	Click the **Save** button to save the configuration
Undo	Button	Click the **Undo** button to restore what you just configured back to the previous setting.

Table 239 – Managing Event Configuration

8.2.3 Notifying Events

The Notifying Events settings allow administrator to define the relationships (rules) between event triggers and handlers.

Notifying Events functionality is disabled by default, to enable this tool select **Event Handling** from the **Service** submenu and click on the **Notifying Events** tab.



Configuration

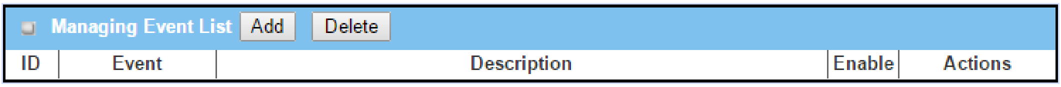
Item	Setting
Notifying Events	☑ Enable

Figure 383 – Enable Notifying Events

Item	Notes	Description
Notifying Events	Disabled by default.	Click ☑ **Enable** to activate the Notifying Events functionality.

Table 240 – Enable Notifying Events

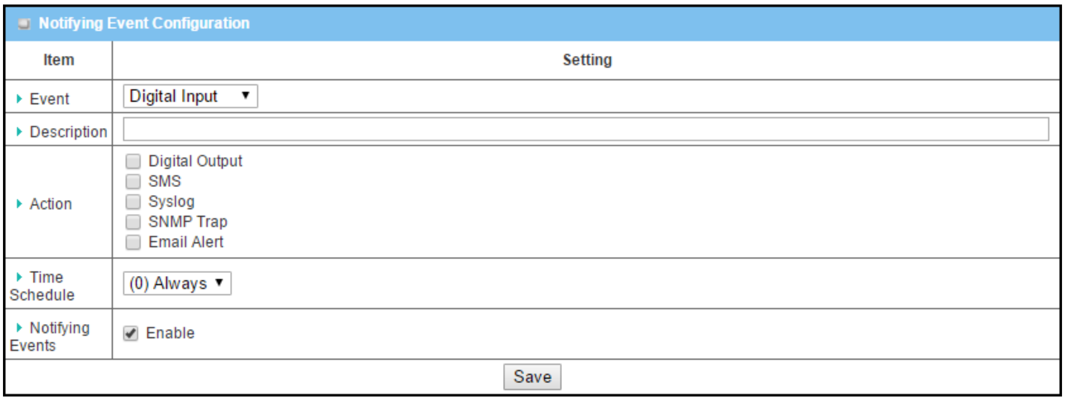
The **Notifying Event List** supports a maximum of 128 rules.



ID	Event	Description	Enable	Actions

Figure 384 – Notifying Event List

Click the **Add** button and the **Notifying Event Configuration** screen will display.



Notifying Event Configuration

Item	Setting
Event	Digital Input ▾
Description	
Action	□ Digital Output □ SMS □ Syslog □ SNMP Trap □ Email Alert
Time Schedule	(0) Always ▾
Notifying Events	☑ Enable

Figure 385 – Notifying Event Configuration

Item	Notes	Description
Event	Digital Input (or WAN) by default	Specify the Event type and then define its corresponding event configuration. The supported Event Types include: **Digital Input** – Select Digital Input and a DI profile from the drop-down list of DI profiles you defined in the Event Handling Configuration window; **WAN** – Select WAN and then select a trigger condition from its associated drop-down list; **LAN&VLAN** – Select LAN&VLAN and then select a trigger condition from its associated drop-down list; **Wi-Fi** – Select Wi-Fi and then select a trigger condition from its associated drop-down list; **DDNS** – Select DDNS and then select a trigger condition from its associated drop-down list; **Administration** – Select Administration and then select a trigger condition from its associated drop-down list of possible administration events; **Modbus** – Select Modbus and a Modbus Notifying Event profile you defined to specify a certain Modbus Event; **Data Usage** – Select Data Usage, then select one of the SIM Cards (Cellular Service) and then set a percentage of Data Usage (1% - 100%) as the trigger condition; **Note** – Available Event Types can differ between products.
Description	Any text.	Write a brief, meaningful description of the event rule.
Action	No default selection.	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 router 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; **SNMP Trap** – Select SNMP Trap, and the router will send out a SNMP Trap to the defined SNMP Event Receivers as the action for the event; **Email Alert** – Select Email Alert and the router to send out an Email to the defined Email accounts as the action for the event; **Note** – Available Actions can differ between products.
Time Schedule	Default setting = (0) Always	Set a time scheduling rule for the Notifying Event.
Notifying Events	Disabled by default.	Click **Enable** to activate this Notifying Event functionality.

Item	Notes	Description
Save	Button	Click the **Save** button to save the configuration
Undo	Button	Click the **Undo** button to restore what you just configured back to the previous setting.

Table 241 – Notifying Event Configuration

8.3 Location Tracking

Global Navigation Satellite System (GNSS) infrastructure allows the NTC-400 Series Router to determine its position, velocity, and time by processing signals received from satellites orbiting Earth. GNSS can access a variety of satellite systems and Satellite-Based Augmentation Systems (SBAS). SBAS is used to improve positioning accuracy.

Major GNSS Systems in the world

GNSS System	Owner
GPS	USA
GLONASS	Russia
Galileo	European Union
BeiDou (COMPASS)	China

Table 242 – Major GNSS Systems

Satellite-Based Augmentation Systems (SBAS)

SBAS	Area Coverage
EGNOS	Europe
WAAS	North America
GAGAN	India
MSAS	Japan

Table 243 – Satellite-Based Augmentation Systems (SBAS)

Position applications are widely-used by a variety of industrial applications, including Location-Based Services (LBS), Automatic Vehicle Location (AVL), Fleet Management, or assets tracking. However, in most cases, GNSS is a one-way communication. That means GNSS-compatible devices can only locate their location by receiving a GNSS signal, but they can’t forward their location data to any other identity through the GNSS system. Because of this limitation of the GNSS system, devices usually need to equip other technology to transmit their location data to back-end servers for tracking or further analysis. Furthermore, as the position applications are more applied on moving objects, a kind of wireless technology would be more suitable to be adopted to transmit location data. Nowadays, thanks to the popularity and wide coverage of cellular technology (GSM, 3G, 4G/LTE), transmitting location data to a remote centre in real time is no longer a hurdle. In addition, the data format of the location data is NMEA 0183 compatible, so the back-end server will be able to interpret the collected location data.

The diagram below illustrates the main features of the GNSS function.

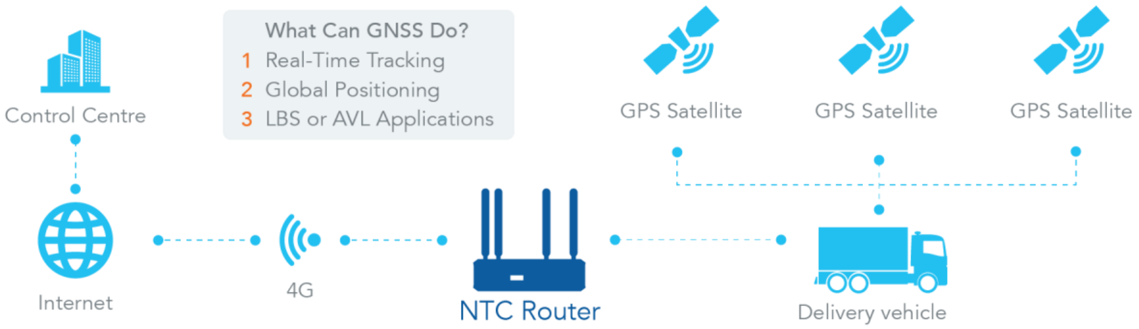


Figure 386 – GNSS

- Retrieve GNSS data from satellites and send to a remote operation centre periodically or save in local storage.
- Global positioning with multiple GNSS systems, including GPS, and optional for GLONASS, Galileo, or BeiDou.
- Mandatory for varieties of LBS (Location-Based Service) applications, such as advertisements, emergency calls.
- Easy integration with AVL (Automatic Vehicle Location) applications, for managing fleets of service vehicles.
- Other value-added applications, such as asset tracking, electronic toll collection, intelligent transport systems.

8.3.1 GNSS

On the GNSS configuration page, you can configure those functions that are mentioned above.

The configuration steps include following items.

- Activate GNSS feature in gateway and finish settings of cellular WAN.
- Support NMEA 0183 (compatible to 3.0) protocol, and allow customized prefix and suffix.
- Configurable GPS data logging on local microSD card storage for route record tracking.
- Indicate remote host, time interval, TCP/UDP, and type of GPS data that would be sent.

GPS Message Type

This item shows all supported types of NMEA 0183 data format. NMEA 0183 data format was defined and maintained by National Marine Electronics Association (NMEA). Select one or more types that you want to use for transmitting GPS data. In most cases, this configuration depends on which data format your central server can recognise. Only select the type you need, otherwise it will consume unnecessary network bandwidth. The table below shows more information for different types of NMEA 0183 message.

Type	Description	Example
GGA	Fix Information	$GPGGA,123519,4807.038,N,01131.000,E,1,08,0.9,545.4,M,46.9,M,,*47
GLL	Lat/Lon Data	$GPGLL,4916.45,N,12311.12,W,225444,A,*1D
GSA	Overall Satellite Data	$GPGSA,A,3,04,05,,09,12,,,24,,,,,2.5,1.3,2.1*39
GSV	Detailed Satellite Data	$GPGSV,2,1,08,01,40,083,46,02,17,308,41,12,07,344,39,14,22,228,45*75

Type	Description	Example
RMC	Recommended Minimum Data	$GPRMC,123519,A,4807.038,N,01131.000,E,022.4,084.4,230394,003.1,W*6A
VTG	Vector Track and Speed Over the Ground	$GPVTG,054.7,T,034.4,M,005.5,N,010.2,K*48

Table 244 – GPS Message Types

SBAS

SBAS is Satellite-Based Augmentation Systems that is used to improve the accuracy of location data. There are several SBAS systems for different areas in the world.

SBAS	Area Coverage
EGNOS	Europe
WAAS	North America
GAGAN	India
MSAS	Japan

Table 245 – Satellite-Based Augmentation Systems (SBAS)

Assisted GPS

Assisted GPS (as known as A-GPS) is used for speeding up location fixing, especially when the satellite signal is weak. If activating this option, the NTC-400 Series Router will download almanac data from an A-GPS server through the IP network instead of from the satellite. You can also choose a different valid period of almanac data. Almanac data with a shorter valid period will result in higher accuracy. However, almanac data with a shorter valid period needs to be updated more frequently, consuming more network bandwidth.

Data to Storage

Besides transmitting location data to a remote server, you can also store location data on internal storage (e.g. microSD card) or external storage (e.g. USB drive). The data format can be NMEA 0183 raw data or GPX file format. The location data will be saved to a new file if the original file size is bigger than the pre-defined file size. The “Download log file” button allows you to browse all saved log files and download to your personal devices.

Scenario of location tracking for fleet management

A fleet owner would like to see the locations of his trucks in real time. He also likes to know where his trucks have been with time information. In his operation office, there is a server (IP: 100.100.100.1) which can interpret NMEA RMC data format and show the truck’s location and track on map. This server is listening on TCP port 888 to receive NMEA RMC packet from trucks. The IMEI number will be added before NMEA RMC data to identify each truck. Below is the configuration of each truck.

Basic Settings

Configuration Path	[GNSS]-[Configuration]
GNSS	*Enable*
GNSS Type	*GPS*

Configuration Path	[GNSS]-[Configuration]
GPS Message Types	*RMC*
SBAS	*Enable*
Assisted GPS	*Enable, 1*
Data to Storage	*Disable*

Table 246 – Basic Settings

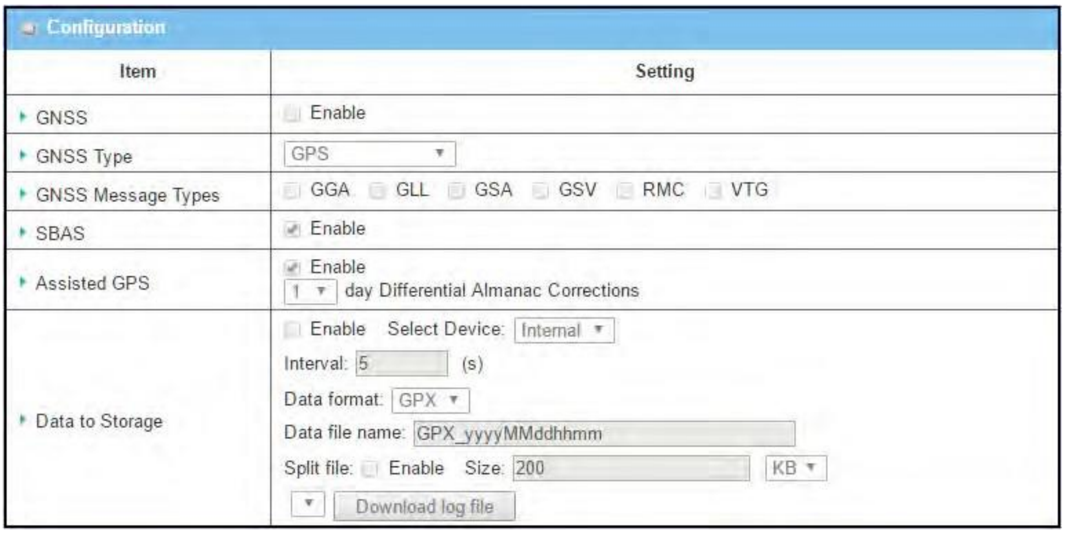
Settings for Remote Host

Configuration Path	[GNSS]-[Remote Host Configuration]
Host Name	*Truck-1*
Host IP	*100.100.100.1*
Protocol Type	*TCP*
Port Number	*888*
Interval(s)	*15*
Prefix Message	*123456789012345*
Suffix Message	*[blank]*
Enable Checkbox	*[Checked]*

Table 247 – Settings for Remote Host

8.3.1.1 Enable Location Tracking

Location Tracking functionality is disabled by default, to enable this tool select **Location Tracking** from the **Service** submenu and click on the **GNSS** tab. The location tracking Configuration section will be displayed.



Configuration

Item	Setting
GNSS	□ Enable
GNSS Type	GPS ▾
GNSS Message Types	□ GGA □ GLL □ GSA □ GSV □ RMC □ VTG
SBAS	☑ Enable
Assisted GPS	☑ Enable 1 ▾ day Differential Almanac Corrections
Data to Storage	□ Enable Select Device: Internal ▾ Interval: 5 (s) Data format: GPX ▾ Data file name: GPX_yyyyMMddhhmm Split file: □ Enable Size: 200 KB ▾ ▾ Download log file

Figure 387 – Enable Location Tracking

Item	Notes	Description
GNSS	Disabled by default.	Check ☑ **Enable** to activate GNSS functions.
GNSS Type	GPS is the default.	Only GPS is available.

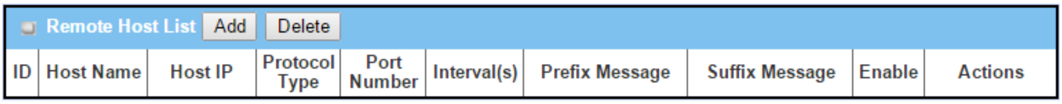
Item	Notes	Description
GNSS Message Types	No default setting.	Select one or more GNSS Message Types to use for transmitting or recording GPS data. Only select the type you need, otherwise it will consume unnecessary network bandwidth.
SBAS	Disabled by default.	Check ☑ **Enable** to activate satellite-based augmentation system (SBAS).
Assisted GPS	Enabled by default.	Check ☑ **Enable** to activate Assisted GPS (A-GPS). Select the duration for downloading the Differential Almanac Corrections data from A-GPS server through IP network. Note – Some devices may not support this function.
Data to Storage	Disabled by default.	Check ☑ Enable to activate GNSS data to storage functions. Select Internal or External Device to store log data to from the drop-down list (required setting). Specify the time interval between two continuous data log refreshes. - Five (5) seconds is the default setting. - Value Range: 5 - 60 seconds. Data Format (required setting): RAW, or GPX Data file name (required setting) Define the file naming convention. Split file Check ☑ **Enable** to activate GNSS data file splitting functions. - Enter the Size in KB or MB (select from drop down list) Download log file Select a log file from the drop down list and click the Download log file button to download through the Web GUI. If the log format specified to download is .gpx, the standard GPX format is used.
Save	Button	Click the **Save** button to save the configuration

Table 248 – Enable Location Tracking

8.3.1.2 Create / Edit Remote Host

Remote Host rules allows you to create custom rules for sending NMEA data (National Marine Electronics Association data has a standard data format supported by all GPS manufacturers) to specific IP addresses and Ports.

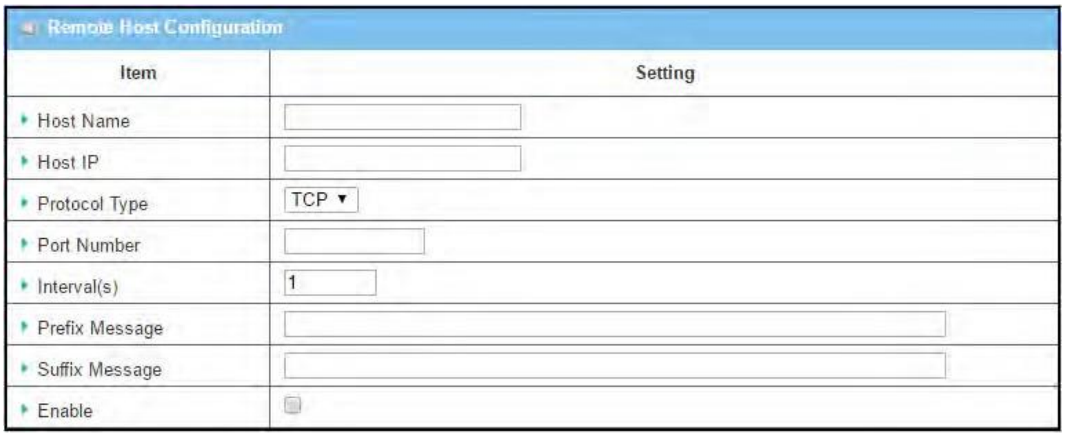
The router supports ten Remote Host rule sets.



ID	Host Name	Host IP	Protocol Type	Port Number	Interval(s)	Prefix Message	Suffix Message	Enable	Actions

Figure 388 – Remote Host List

Click the **Add** button is applied to open the **Remote Host Configuration** screen.



Remote Host Configuration

Item	Setting
Host Name	
Host IP	
Protocol Type	TCP ▾
Port Number	
Interval(s)	1
Prefix Message	
Suffix Message	
Enable	□

Figure 389 – Remote Host Configuration

Item	Notes	Description
Host Name	Any text. String format.	Enter the host name for the designated remote host. Value Range: -1 - 64 characters.
Host IP	Mandatory field.	Specify the IP Address of remote host. It will be use as destination IP for sending NMEA packets.
Protocol Type	TCP is the default.	Specify the Protocol (**TCP** or **UDP**) to use for sending NMEA packets.
Port Number	Mandatory field.	Specify a Port Number as destination port for sending NMEA packets. Value Range: 1 - 65535.
Interval(s)	Mandatory field.	Specify the time interval (seconds) between two NMEA packets. Value Range: 1 - 255 seconds.
Prefix Message	Optional field. Any text. String format.	Specify optional prefix string with specific information if your backend server can recognize. For example, you can input the IMEI code of this device here, and then your backend server can recognize this GPS data is sent from this device. You can also leave this field blank.
Suffix Message	Any text. String format.	Specify optional suffix string with specific information if your backend server can recognize.
Enable	Disabled by default	Check ☑ **Enable** to activate this remote host rule.
Save	Button	Click the **Save** button to save the configuration

Table 249 – Remote Host Configuration

8.3.2 Track Viewer

Track Viewer allows you to see the recent locations of the device using Google Maps or from the GPX file recorded by GNSS. In addition, when GNSS is enabled, current position will also be displayed in Track Viewer.

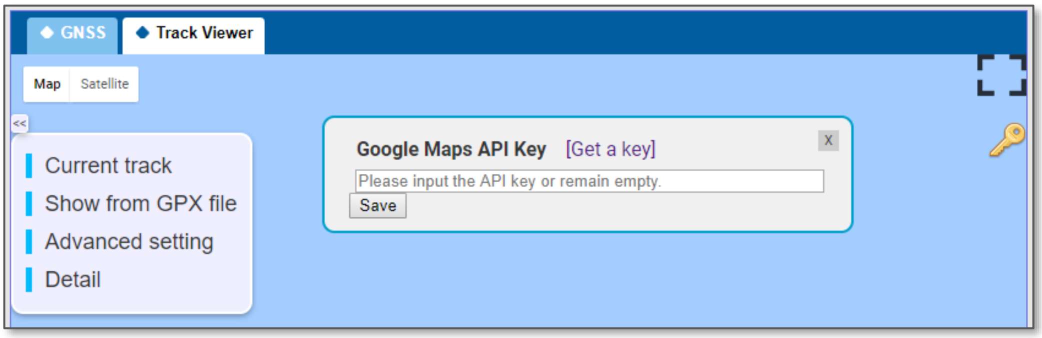
Navigate to the **Service > Location Tracking > Track Viewer** tab.

8.3.2.1 Setup Google Maps API Key

On first use you will need to download a Google API Key.

From the **Service > Location Tracking > Track Viewer** tab page, either:

- Enter the valid API key that you have, or
- Click the **[Get a key]** link and follow the instructions on the Google Maps APIs website.



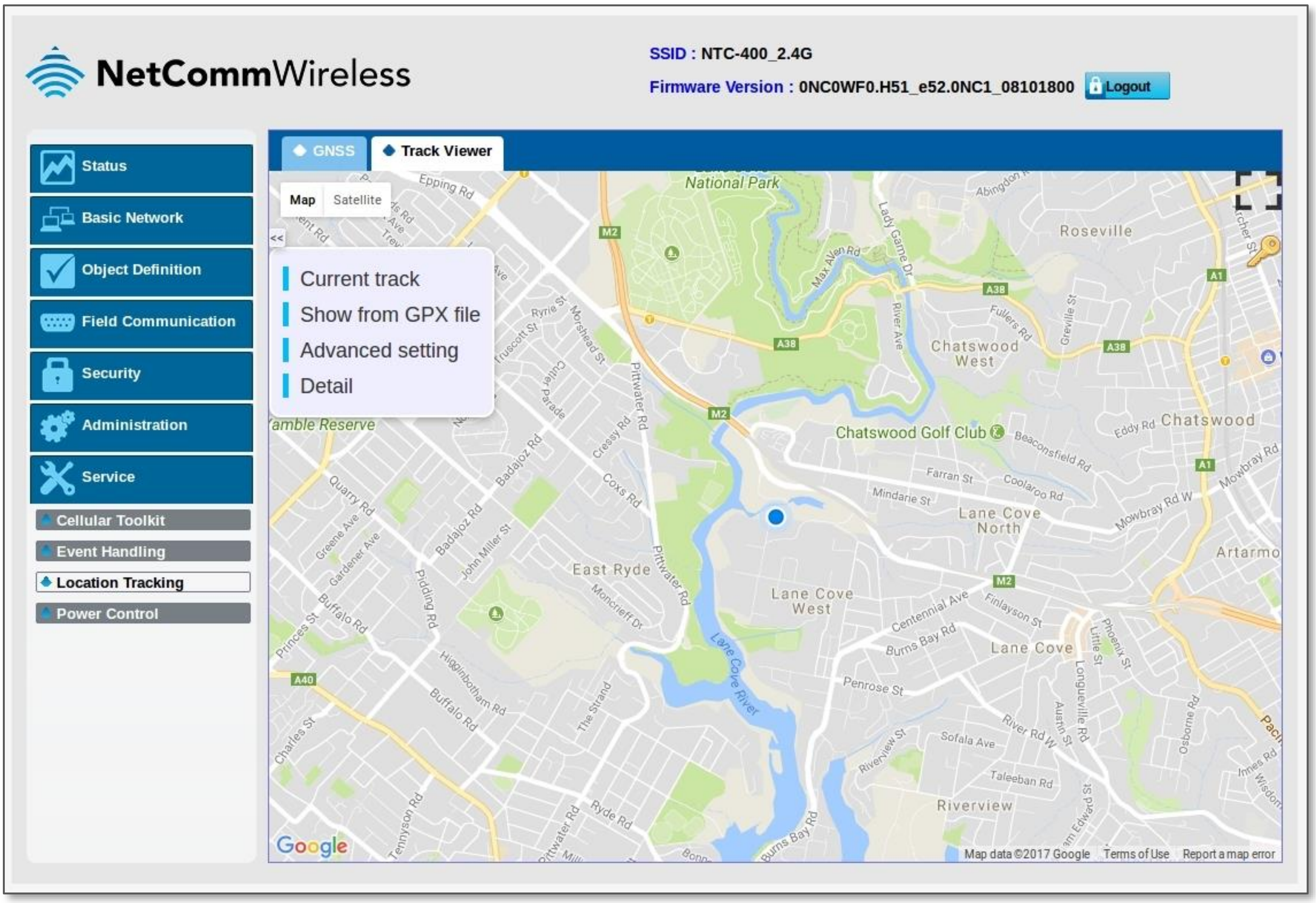
Google Maps API Key [Get a key]

Please input the API key or remain empty.

Save

Figure 390 – Setup Google Maps API Key

When the Google Maps API key has been downloaded and saved, the **Track Viewer / Map** screen will be activated.



SSID : NTC-400_2.4G

Firmware Version : 0NCOWF0.H51_e52.0NC1_08101800

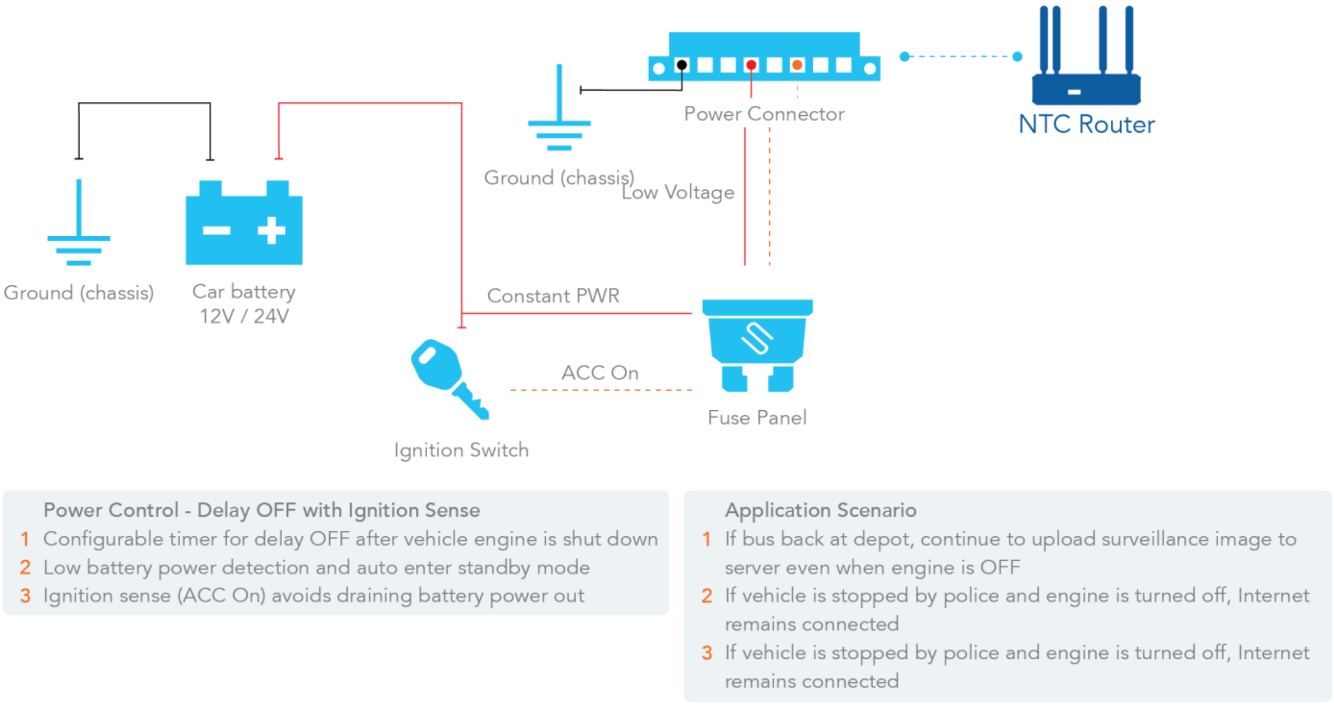
Figure 391 – Track Viewer screen shot

8.4 Power Control

8.4.1 Ignition Sense

When the router is deployed in a vehicle, it can be configured to power-on only when the ignition is on.

In most cases, electronic devices in a vehicle will be shut down when car engine is turned off, but in some circumstances, you may need devices continue to work. An obvious problem is the power supply to almost all in-vehicle devices will be terminated when the car engine is off to prevent in-vehicle devices draining the battery. To have a solution for this situation, the NTC-400 Series Router has been equipped with an Ignition Sense function. The main advantages of this feature are:



Power Control - Delay OFF with Ignition Sense

1 Configurable timer for delay OFF after vehicle engine is shut down
2 Low battery power detection and auto enter standby mode
3 Ignition sense (ACC On) avoids draining battery power out

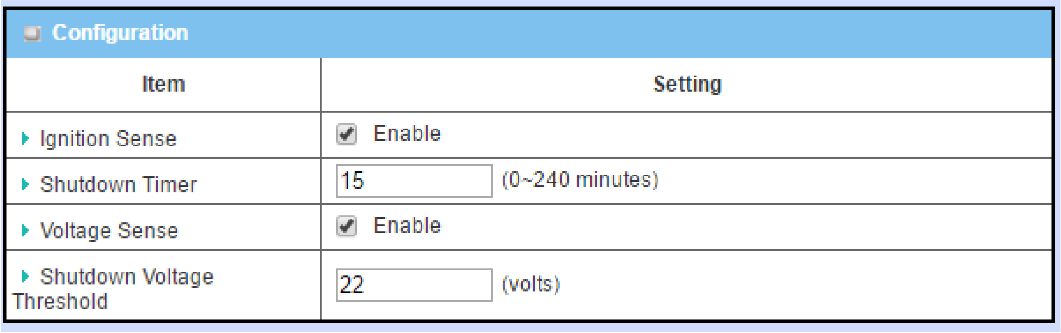
Application Scenario

1 If bus back at depot, continue to upload surveillance image to server even when engine is OFF
2 If vehicle is stopped by police and engine is turned off, Internet remains connected
3 If vehicle is stopped by police and engine is turned off, Internet remains connected

Figure 392 – Ignition Sense

- The NTC-400 Series Router can continue to operate when car engine is shut down.
- The NTC-400 Series Router will enter standby mode automatically when a pre-set timer is due. If in standby mode, the NTC-400 Series Router will stop consuming battery power to prevent draining power out.
- The NTC-400 Series Router will enter standby mode automatically if a low input power voltage is detected.
- The NTC-400 Series Router will be return from standby mode to operation mode when the car is started.

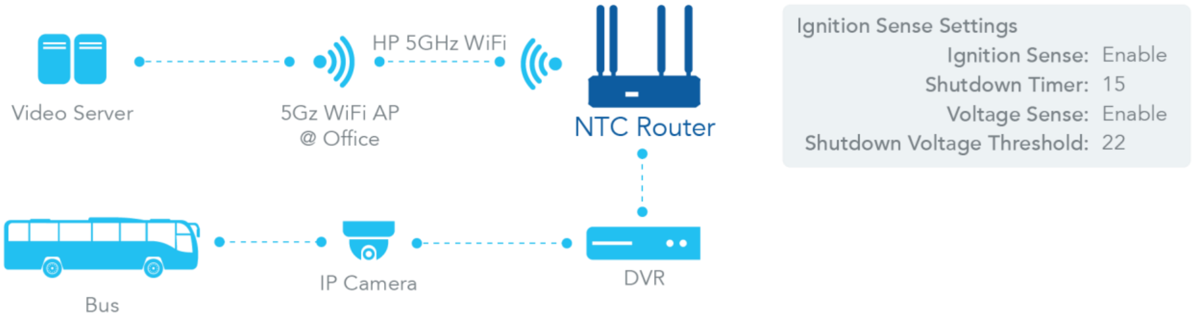
Delay Off and Low Power Detection



Configuration

Item	Setting
Ignition Sense	☑ Enable
Shutdown Timer	15 (0~240 minutes)
Voltage Sense	☑ Enable
Shutdown Voltage Threshold	22 (volts)

Figure 393 – Ignition Sense configuration



Ignition Sense Settings
Ignition Sense: Enable
Shutdown Timer: 15
Voltage Sense: Enable
Shutdown Voltage Threshold: 22

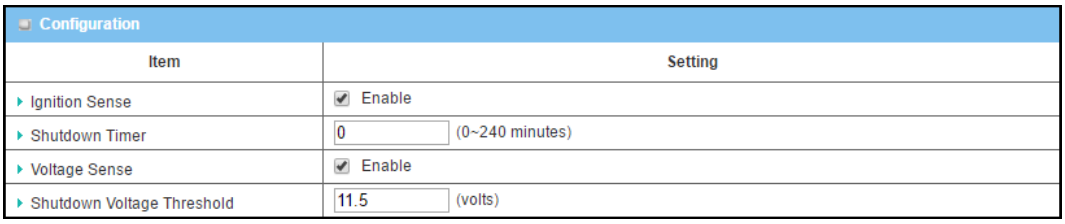
Figure 394 – Ignition Sense Example

In this example, the surveillance system on the bus will transmit video files back to the back-end server when the bus returns to the depot. The driver will shut the bus off and leave the bus parked in the depot, but the uplink connection for the surveillance system still needs to be available until all video files are completely uploaded. Usually, video files on each bus can be uploaded completely within **15** minutes. To prevent draining the battery, the bus driver activates the low voltage detection function to force the router to shut down if the battery voltage reaches **22V** (regular voltage is 24V).

To make the router ignition-dependant select **Power Control** from the **Service** menu. The **Ignition Sense** tab will display.

Attention – The **Ignition Sense** feature is ☐ disabled by default.

When ☑ enabled, the router will not power on until power from the ignition pin of its terminal block is detected (ACC ON).



Configuration

Item	Setting
Ignition Sense	☑ Enable
Shutdown Timer	0 (0~240 minutes)
Voltage Sense	☑ Enable
Shutdown Voltage Threshold	11.5 (volts)

Figure 395 – Ignition Sense configuration

Item	Notes	Description
Ignition Sense	Disabled by default.	Click ☑ **Enable** to activate the Ignition Sense function. By default, the function is disabled, and the router will be always ON when the power source is attached.

Item	Notes	Description
Shutdown Timer	Number format: any number between 0 and 240. 0 is the default setting.	Enter a shutdown timer period (0 - 240 minutes) to power off the router after the engine has been stopped for the specified time. '0' means the router will never be shut down even if ignition is turned off (ACC OFF). Value Range: 0 - 240 minutes
Voltage Sense	Disabled by default.	Click ☑ **Enable** to activate the Voltage Sense function. When enabled, if the input voltage is less than the specified threshold value the router will be shut down when ACC is OFF regardless of the Shutdown Timer's setting.
Shutdown Voltage Threshold	Optional setting.	Specify a voltage threshold at which the router will turn off.
Save	Button	Click the **Save** button to save the configuration.
Undo	Button	Click the **Undo** button to restore what you just configured back to the previous setting.

Table 250 – Ignition Sense configuration

Appendices

Appendix A – Table of Figures

Appendix B – Table of Tables

Appendix C – Wi-Fi Performance Measurement Results

2.4GHz

Wireless Coverage Distance and Throughput

Channel: 6, HT40				
Distance(m)	LAN->WLAN Average (Mbps)	WLAN->LAN Average (Mbps)	WLAN<->LAN Average (Mbps)	RSSI
15	195	169	206	-42
50	196	158	205	-42
100	165	156	165	-46
150	166	159	162	-57
200	163	158	161	-58

Table 251 –Wi-Fi Performance Test Results – 2.4GHZ, Channel:6,HT40

5GHz

Wireless Coverage Distance and Throughput

Channel:44,HT80				
Distance(m)	LAN->WLAN Average (Mbps)	WLAN->LAN Average (Mbps)	WLAN<->LAN Average (Mbps)	RSSI
50	370	283	413	-67
100	348	262	371	-67
200	280	217	292	-69
300	218	197	214	-74
400	183	176	192	-78
500	150	146	162	-82

Table 252 –Wi-Fi Performance Test Results – 5GHZ, Channel:44,HT80

Appendix D – Open Source Software Disclaimer

This product contains Open Source software that has been released by the developers of that software under specific licensing requirements such as the “General Public License“ (GPL) Version 2 or 3, the “Lesser General Public License“ (LGPL), the “Apache License“ or similar licenses. For detailed information on the Open Source software, the copyright, the respective licensing requirements and ways of obtaining the source code, contact NetComm Wireless or your local sales representative.

Appendix E – Safety and product care

Electrical safety

Accessories

Only use approved accessories.

Do not connect with incompatible products or accessories.

Connection to a car

Seek professional advice when connecting a device interface to the vehicle electrical system.

External antenna

Any optional external antenna used for this transmitter must be installed to **provide a separation distance of at least 20 cm** (**8 inches**) from all persons and must not be co-located or operated in conjunction with any other antenna or transmitter. Please consult the health and safety guide of the chosen antenna for specific body separation guidelines as a greater distance of separation may be required for high-gain antennas. Any external antenna gain must meet RF exposure and maximum radiated output power limits of the applicable rule section. The maximum antenna gain for this device is:

NTC-402

WLAN:	2.5dBi
WLAN antenna type:	Dipole antenna

Distraction

Operating machinery

Full attention must be given to operating the machinery in order to reduce the risk of an accident.

Driving

Full attention must be given to driving at all times in order to reduce the risk of an accident. Using the device in a vehicle can cause distraction and can lead to an accident. You must comply with local laws and regulations restricting the use of mobile communication devices while driving.

Product handling

You alone are responsible for how you use your device and any consequences of its use.

You must always switch off your device wherever the use of a mobile phone is prohibited. Do not use the device without the clip-on covers attached, and do not remove or change the covers while using the device. Use of your device is subject to safety measures designed to protect users and their environment.

Always treat your device and its accessories with care and keep it in a clean and dust-free place.

Do not expose your device or its accessories to open flames or lit tobacco products.

Do not expose your device or its accessories to liquid, moisture or high humidity.

Do not drop, throw or try to bend your device or its accessories.

Do not use harsh chemicals, cleaning solvents, or aerosols to clean the device or its accessories.

Do not paint your device or its accessories.

Do not attempt to disassemble your device or its accessories, only authorised personnel must do so.

Do not expose your device or its accessories to extreme temperatures. Ensure that the device is installed in an area where the temperature is within the supported operating temperature range (-30°C to +70°C).

Do not use your device in an enclosed environment or where heat dissipation is poor. Prolonged use in such space may cause excessive heat and raise ambient temperature, which will lead to automatic shutdown of your device or the disconnection of the mobile network connection for your safety. To use your device normally again after such shutdown, cool it in a well-ventilated place before turning it on.

Please check local regulations for disposal of electronic products.

Do not operate the device where ventilation is restricted.

Installation and configuration should be performed by trained personnel only.

Do not use or install this product near water to avoid fire or shock hazard. Avoid exposing the equipment to rain or damp areas.

Arrange power and Ethernet cables in a manner such that they are not likely to be stepped on or have items placed on them.

Ensure that the voltage and rated current of the power source match the requirements of the device. Do not connect the device to an inappropriate power source.

Small children

Do not leave your device and its accessories within the reach of small children or allow them to play with it.

They could hurt themselves or others, or could accidentally damage the device.

Your device contains small parts with sharp edges that may cause an injury or which could become detached and create a choking hazard.

Demagnetisation

To avoid the risk of demagnetisation, do not allow electronic devices or magnetic media close to your device for a long time.

Avoid other magnetic sources as these may cause the internal magnetometer or other sensors to malfunction and provide incorrect data.

Electrostatic discharge (ESD)

Do not touch the SIM card's metal connectors.

Air Bags

Do not place the device in the area near or over an air bag or in the air bag deployment area

Mount the device safely before driving your vehicle.

Emergency & other situations requiring continuous connectivity

This device, like any wireless device, operates using radio signals, which cannot guarantee connection in all conditions. Therefore, you must never rely solely on any wireless device for emergency communications or otherwise use the device in situations where the interruption of data connectivity could lead to death, personal injury, property damage, data loss, or other loss.

Device heating

Your device may become warm during normal use.

Faulty and Damaged Products

Do not attempt to disassemble the device or its accessory.

Only qualified personnel should service or repair the device or its accessory.

If your device or its accessory has been submerged in water or other liquid, punctured, or subjected to a severe fall, do not use it until you have taken it to be checked at an authorised service centre

Interference

Care must be taken when using the device near personal medical devices, such as pacemakers and hearing aids.

Pacemakers

Pacemaker manufacturers recommend that a minimum separation of 15cm be maintained between a device and a pacemaker to avoid potential interference with the pacemaker.

Hearing aids

People with hearing aids or other cochlear implants may experience interfering noises when using wireless devices or when one is nearby.

The level of interference will depend on the type of hearing device and the distance from the interference source, increasing the separation between them may reduce the interference. You may also consult your hearing aid manufacturer to discuss alternatives.

Medical devices

Please consult your doctor and the device manufacturer to determine if operation of your device may interfere with the operation of your medical device.

Hospitals

Switch off your wireless device when requested to do so in hospitals, clinics or health care facilities. These requests are designed to prevent possible interference with sensitive medical equipment.

Aircraft

Switch off your wireless device whenever you are instructed to do so by airport or airline staff.

Consult the airline staff about the use of wireless devices on board the aircraft, if your device offers a ‘flight mode’ this must be enabled prior to boarding an aircraft.

Interference in cars

Please note that because of possible interference to electronic equipment, some vehicle manufacturers forbid the use of devices in their vehicles unless an external antenna is included in the installation.

Explosive environments

Petrol stations and explosive atmospheres

In locations with potentially explosive atmospheres, obey all posted signs to turn off wireless devices such as your device or other radio equipment.

Areas with potentially explosive atmospheres include fuelling areas, below decks on boats, fuel or chemical transfer or storage facilities, areas where the air contains chemicals or particles, such as grain, dust, or metal powders.

Blasting caps and areas

Turn off your device or wireless device when in a blasting area or in areas posted turn off “two-way radios” or “electronic devices” to avoid interfering with blasting operations.