

TW-LTE 600

**3G/4G LTE Embedded with Dual-SIM Slots
Wireless-N
VPN Firewall Router**

User Manual

Copyright © TeleWell Oy

Table of Contents

Chapter 1: Introduction	5
Introduction to your Router	5
Features	6
Hardware Specifications	9
Physical Interface	9
Chapter 2: Installing the Router	10
Package Contents.....	10
Important note for using this router.....	10
Device Description	11
The Front LEDs.....	11
The Rear Ports	12
Chapter 3: Basic Installation.....	13
Network Configuration	14
Configuring a PC in Windows 7/8	14
Factory Default Settings.....	17
Chapter 4: Configuration	18
Configuration via Web Interface	18
Status	18
Summary	18
Statistics	20
LAN	20
WAN Service	21
Bandwidth Usage	21
3G/LTE Status.....	22
Route	22
ARP	23
DHCP	24
VPN	24
IPSec	24
PPTP.....	25
L2TP.....	25
OpenVPN.....	26
GRE.....	27
Log	27
System Log	27
Security Log.....	28
Configuration	29
LAN - Local Area Network	29
Ethernet	29
IPv6 Autoconfig.....	31
Interface Grouping	34
Wireless	36
Basic.....	36
Security	37
MAC Filter.....	47
Wireless Bridge.....	47
Advanced	49
Station Info.....	51
Schedule Control.....	51
WAN-Wide Area Network.....	52
WAN Service	52
Dual SIM.....	59

System	60
Internet Time	60
Firmware Upgrade	61
Backup / Update	61
Access Control	62
Mail Alert	63
SMS Alert	64
Configure Log	64
USB	65
Storage Device Info	65
User Account	65
Print Server	69
DLNA	73
IP Tunnel	73
IPv6inIPv4	74
IPv4inIPv6	75
Security	76
IP Filtering Outgoing	76
IP Filtering Incoming	78
MAC Filtering	79
Blocking WAN PING	80
Time Restriction	81
URL Filter	82
Parental Control Provider	84
QoS - Quality of Service	85
QoS Port Shaping	89
NAT	89
Exceptional Rule Group	89
Virtual Servers	90
DMZ Host	92
One-to-One NAT	93
Port Triggering	94
ALG	96
Wake On LAN	96
VPN	97
IPSec	97
VPN Account	106
Exceptional Rule Group	106
PPTP	107
PPTP Server	108
PPTP Client	108
L2TP	118
L2TP Server	119
L2TP Client	120
OpenVPN	131
OpenVPN Server	131
OpenVPN CA	131
OpenVPN Client	132
GRE	134
Advanced Setup	135
Routing	135
Default Gateway	135
Static Route	135
Policy Routing	137
RIP	137
DNS	138
DNS	138
Dynamic DNS	139
DNS Proxy	140
Static DNS	140
Static ARP	141
UPnP	141
Certificate	142
Trusted CA	142
Multicast	143
Management	145

SNMP Agent	145
TR-069 Client	146
Remote Access	146
Mobile Network	147
3G/LTE Usage Allowance	147
Power Management.....	148
Time Schedule.....	148
Auto Reboot	149
Diagnostics	149
Diagnostics Tools.....	149
Push Service	151
Diagnostics.....	Virhe. Kirjanmerkkiä ei ole määritetty.
Restart	152

Chapter 1: Introduction

Introduction to your Router

The triple-WAN 3G/LTE firewall router is integrated with the 802.11n Wireless Access Point and 4-port switch. It is a cutting-edge networking product for SOHO and office users. Uniquely, the router allows users to directly insert 3G/4G LTE SIM card into its built-in SIM slots instead of requiring external USB modems. This design will avoid compatibility issues of many different 3G/LTE USB modems. With the increasing popularity of the 3G/4G LTE standard, communication via the router is becoming more convenient and widely available - enabling users to use a 3G/4G LTE, UMTS, EDGE, GPRS, or GSM Internet connection, making downstream rates of up to 100Mbps possible. Users can watch movies, download music or access e-mail wherever a 3G/4G LTE connection is available.

3G/4G LTE Mobility and Always-on Connectivity

The advanced dual-SIM 3G/4G LTE router allows you to insert 3G/4G LTE SIM card to its built-in SIM slots, enabling you to use a 3G/4G LTE Internet connection, which makes downstream rates of up to 100Mbps possible. With the increasing popularity of the 3G/4G LTE standard, communication via the router is becoming more convenient and widely available - allowing you to watch movies, download music on the road, or access e-mail no matter where you are. You can even share your Internet connection with others, no matter if you're in a meeting, or speeding across the country on a train.

Optimal wireless performance

With an integrated 802.11n Wireless Access Point, the router delivers up to 6 times the speed of an 802.11a/b/g network device. It supports a data rate of up to 300Mbps and is also compatible with 802.11a/b/g equipment. The Wireless Protected Access (WPA-PSK/WPA2-PSK) and Wireless Encryption Protocol (WEP) features enhance the level of transmission security and access control over wireless LAN. The router also supports the Wi-Fi Protected Setup (WPS) standard, allowing users to establish a secure wireless network by simply pushing a button. If your network requires wider coverage, the built-in Wireless Distribution System (WDS) repeater function allows you to expand your wireless network without the need for any external wires or cables.

Secure VPN Connections

The advanced router supports all currently popular secure VPNs, including embedded IPSec VPN, PPTP, L2TP, OpenVPN, GRE, which satisfies different users' needs, allowing users to establish encrypted private connections over the Internet with your optimum VPN options. You can access your corporate Intranet and transmit sensitive data between branch offices and remote sites anytime; even when you are out of office, thus enhancing productivity.

Smooth, Responsive Net Connection

Quality of Service (QoS) gives user full control over outgoing data traffic. Priority can be assigned by the router to ensure that important transmissions like gaming packets, or IPTV/streaming content passes through the router at lightning speed, even when there is heavy Internet traffic. The speed of different types of outgoing data passing through the router is also controlled to ensure that users do not saturate bandwidth with their browsing activities.

Virtual AP

A “Virtual Access Point” is a logical entity that exists within a physical Access Point (AP). When a single physical AP supports multiple “Virtual APs”, each Virtual AP appears to stations (STAs) to be an independent physical AP, even though only a single physical AP is present. For example, multiple Virtual APs might exist within a single physical AP, each advertising a distinct SSID and capability set. Alternatively, multiple Virtual APs might advertise the same SSID but a different capability set – allowing access to be provided via Web Portal, WEP, and WPA simultaneously. Where APs are shared by multiple providers, Virtual APs provide each provider with separate authentication and accounting data for their users, as well as diagnostic information, without sharing sensitive management traffic or data between providers. You can enable the virtual AP.

Web Based GUI

It supports web based GUI for configuration and management. It is user-friendly and comes with online help. It also supports remote management capability for remote users to configure and manage this product.

Firmware Upgradeable

Device can be upgraded to the latest firmware through the WEB based GUI.

Features

- 3G/4G LTE embedded with dual SIM card slots
- Ethernet port #4 can be configured as a WAN interface for broadband connectivity
- Auto fail-over to ensure an always-on WAN connection
- IEEE 802.11 b/g/n compliant Wireless Access Point with Wi-Fi Protected Setup (WPS)
- Wi-Fi Protected Access (WPA-PSK/ WPA2-PSK) and Wired Equivalent Privacy (WEP) support
- Secured 16 IPSec VPN tunnels with powerful DES/ 3DES/ AES
- PPTP VPN with Pap/ Chap/ MS-CHAPv2 authentication
- Pure L2TP and L2TP over IPSec
- OpenVPN with CA authentication and extensive OpenSSL encryption
- GRE tunnel
- SOHO Firewall Security with DoS Preventing and Packet Filtering
- Quality of Service Control for traffic prioritization and Bandwidth management
- Universal Plug and Play (UPnP) Compliance
- USB port for print server, NAS (Samba), FTP server DLNA media server

Network Protocols and Features

- IPv4
- NAT, static (v4) routing and RIP-1 / 2
- Universal Plug and Play (UPnP) Compliant
- Dynamic Domain Name System (DDNS)
- Virtual Server, DMZ
- SNTP, DNS relay, IGMP snooping and IGMP proxy for video service
- MLD snooping and MLD proxy for video service
- Management based-on IP protocol, port number and address
- SMTP client with SSL/TLS
- Supports port-based and tag-based Interface Grouping (VLAN)

3G/4G LTE

- LTE: peak downlink speed of up to 100Mbps and peak uplink speed of up to 50Mbps
 - Supports multi-band LTE: 2100MHz (B1), 1800MHz (B3), 2600MHz (B7), 900MHz (B8), 800MHz (B20).
 - Supports multi-band WCDMA: 2100MHz (B1), 1900MHz (B2), 850MHz (B5), 900MHz (B8)
- 3G/HSPA+: peak downlink speed of up to 14.4Mbps and peak uplink speed of up to 5.76Mbps
 - Supports dual-band WCDMA: 900MHz and 2100MHz or multi-band WCDMA: 850MHz, 1900MHz and 2100MHz
 - Supports Quad-band EDGE/GPRS/GSM: 850MHz, 900MHz, 1800MHz, 1900MHz
- Web-based GUI for configuration and management

Firewall

- Built-in NAT Firewall
- Stateful Packet Inspection (SPI)
- DoS attack prevention
- Supports Web (http)/SSH/FTP/Telnet/SNMP
- Packet Filtering (v4) - port, source IP address, destination IP address
- URL Content Filtering (v4) – string or domain name detection in URL string
- MAC Filtering
- Password protection for system management

Quality of Service Control

- Supports the DiffServ approach
- Traffic prioritization and bandwidth management based-on IPv4 protocol, port number and address

IPTV Applications

- IGMP Snooping and IGMP Proxy
- MLD Snooping and MLD Proxy
- Interface Grouping (VLAN)
- Quality of Service (QoS)
- Supports VLAN MUX

Wireless LAN

- Compliant with IEEE 802.11 b/ g/ n standards
- 2.4-2.484GHz radio band for wireless
- Up to 300 Mbps wireless operation rate
- 64 / 128 bits WEP supported for encryption
- WPS (Wi-Fi Protected Setup) for easy setup
- Supports WPS v2
- Wireless Security with WPA-PSK / WPA2-PSK support
- Multiple wireless SSIDs with wireless guest access and client isolation
- WDS repeater function support
- 802.1x radius authentication supported

USB Application Server

- Storage/NAS: Samba server, FTP Server, DLNA media server
- Printer Server

Virtual Private Network (VPN)

- 16 IPSec VPN tunnels
- IKE key management
- DES, 3DES and AES encryption for IPSec
- L2TP over IPSec
- Pap/ Chap/ MS-CHAPv2 authentication for PPTP
- IPSec pass-through
- OpenVPN with CA authentication and extensive OpenSSL encryption
- GRE tunnel

Management

- Web-based GUI for remote and local management (IPv4)
- Firmware upgrades and configuration data upload and download via web-based GUI
- Embedded Telnet server for remote and local management
- Supports DHCP server / client / relay
- Supports SNMP v1, v2, MIB-I and MIB-II
- Available Syslog
- Mail alert for WAN IP changed
- Auto failover and fallback

Hardware Specifications

Physical Interface

- WLAN: internal antennas
- Antennas:
 - in 3G use: one antenna is connected to a front view of the left connector
 - in 4G use : two antennas is connected to
- USB 2.0 port for storage service (Samba, FTP server), printer server
- Dual SIM card slots
- Factory default reset button
- WPS push button
- Power jack
- Power switch

Chapter 2: Installing the Router

Package Contents

- TW-LTE 600
- Manual
- Ethernet cable
- Power adapter
- 3G antenna: 3G antenna x 1 PCS (only for 3G mode)
- LTE antennas x 2 PCS (only for LTE mode)

Important note for using this router



Warning

1. Do not use the router in high humidity or high temperatures.
2. Do not use the same power source for the router as other equipment.
3. Do not open or repair the case yourself. If the router is too hot, turn off the power immediately and have it repaired at a qualified service center.
4. Avoid using this product and all accessories outdoors.

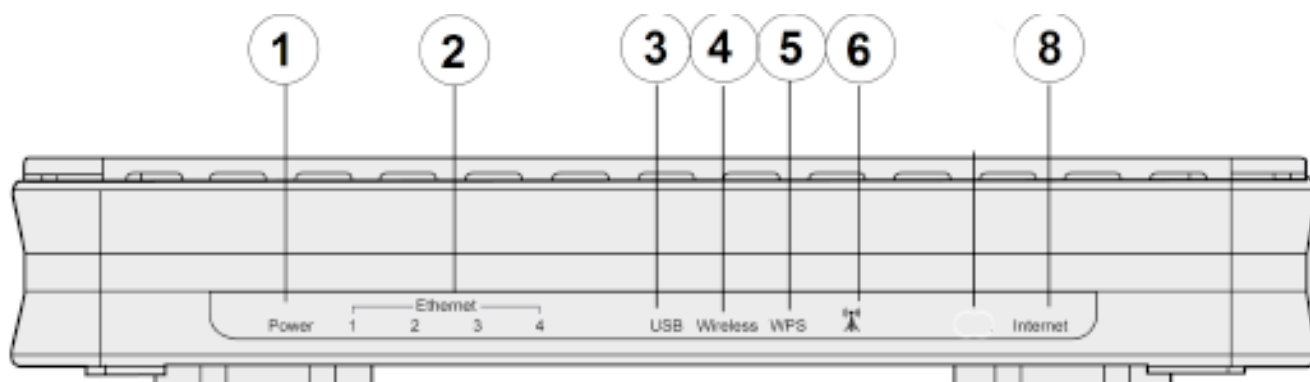


Attention

1. Place the router on a stable surface.
2. Only use the power adapter that comes with the package. Using a different voltage rating power adapter may damage the router.

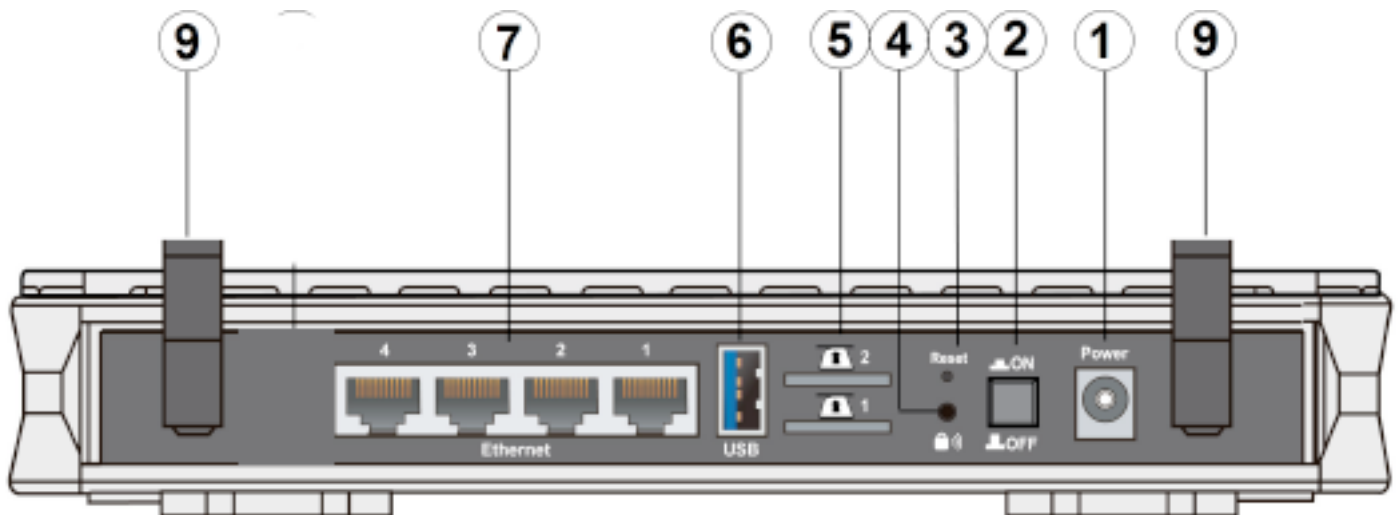
Device Description

The Front LEDs



LED		Status	Meaning
1	Power	Red	Boot failure or in emergency mode
		Green	System ready
2	Ethernet Port 1-4 (EWAN)	Green	Transmission speed hitting 10/100Mbps
		Blinking	Data being transmitted/received
3	USB	Green	Connected to the USB device (USB 2.0 Storage, Printer).
4	Wireless	Green	Wireless connection established
		Green blinking	Sending/receiving data
5	WPS	Green blinking	WPS configuration being in progress
		Off	WPS process completed or WPS is off
6	3G/LTE	Green	3G/LTE service(down) is up.
		Slow blinking orange	Weak 3G/LTE signal
		Quick blinking orange	Moderate 3G/LTE signal
		Solid orange	Strong 3G/LTE signal
8	Internet	Green	Having obtained an IP address successfully
		Off	Router in bridge mode or internet connection not present.

The Rear Ports



Port		Meaning
1	Power	Connect the supplied power adapter to this jack.
2	Power Switch	Power ON / OFF switch.
3	RESET	After the device is powered on, press it 5 seconds or above : to restore to factory default settings (this is used when you cannot login to the router, e.g. forgot the password)
4	WPS	<p>1 <u>WPS button</u>: Push WPS button to trigger Wi-Fi Protected Setup function.</p> <p>2. <u>Wireless on/off</u>: When WPS is disabled, WPS button can act as wireless on/off button.</p> <p>Press WPS button more than 2 seconds to switch on/off the wireless connectivity,.</p>
5	SIM card slots	The router provides dual-SIM failover mobile connection with two embedded SIM slots. Please plug SIM card into the slot.
6	USB	Connect the USB device (USB 2.0 hard driver, Printer) to this port to server.
7	Ethernet	<p>Connect a UTP Ethernet cable (Cat-5 or Cat-5e) to one of the four LAN ports when connecting to a PC or an office/home network of 10Mbps /100Mbps.</p> <p>Note: Port #4 can be configured as a WAN Interface for Broadband connectivity.</p>
9	Antennas	<p>The detachable antennas.</p> <ul style="list-style-type: none"> • 3G antenna: 3G antenna x 1 PCS (only for 3G mode) • 4G LTE antennas x 2 PCS (only for 4G LTE mode)

Chapter 3: Basic Installation

The router can be configured through your web browser. A web browser is included as a standard application in the following operating systems: Linux, Mac OS, Windows 7 / 98 / NT / 2000 / XP / Me / Vista, etc. The product provides an easy and user-friendly interface for configuration.

Please check your PC network components. The TCP/IP protocol stack and Ethernet network adapter must be installed. If not, please refer to your Windows-related or other operating system manuals.

There are ways to connect the router, either through an external repeater hub or connect directly to your PCs. However, make sure that your PCs have an Ethernet interface installed properly prior to connecting the router device. You ought to configure your PCs to obtain an IP address through a DHCP server or a fixed IP address that must be in the same subnet as the router. The default IP address of the router is 192.168.0.254 and the subnet mask is 255.255.255.0 (i.e. any attached PC must be in the same subnet, and have an IP address in the range of 192.168.0.1 to 192.168.0.253). The best and easiest way is to configure the PC to get an IP address automatically from the router using DHCP. If you encounter any problem accessing the router web interface it is advisable to uninstall your firewall program on your PCs, as they can cause problems accessing the IP address of the router. Users should make their own decisions on what is best to protect their network.

Please follow the following steps to configure your PC network environment.

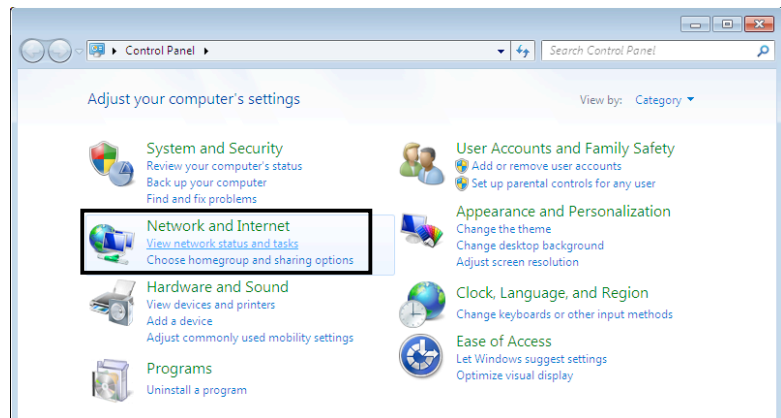


Any TCP/IP capable workstation can be used to communicate with or through this router. To configure other types of workstations, please consult your manufacturer documentation.

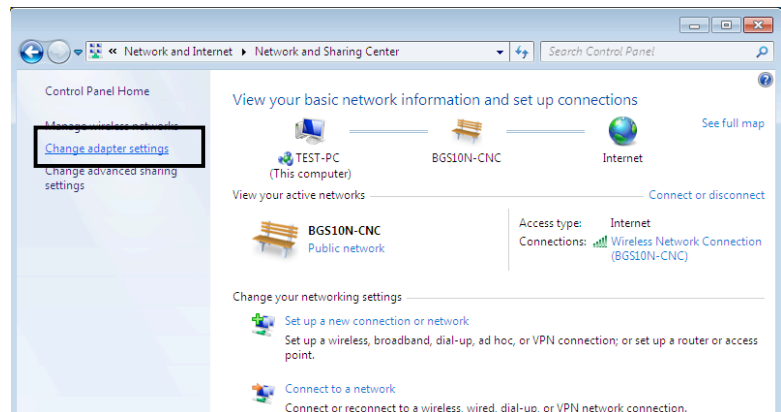
Network Configuration

Configuring a PC in Windows 7/8

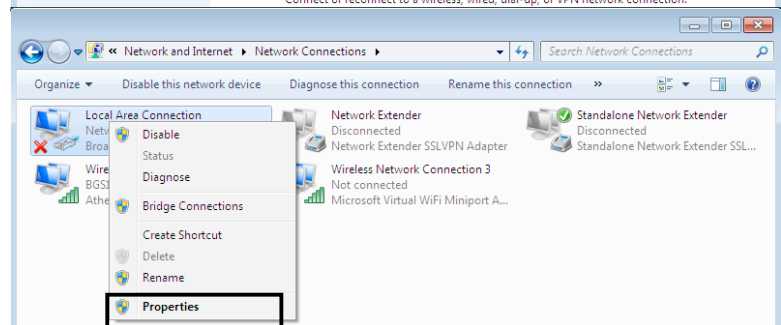
1. Go to **Start**. Click on **Control Panel**. Then click on **Network and Internet**.



2. When the **Network and Sharing Center** window pops up, select and click on **Change adapter settings** on the left window panel.

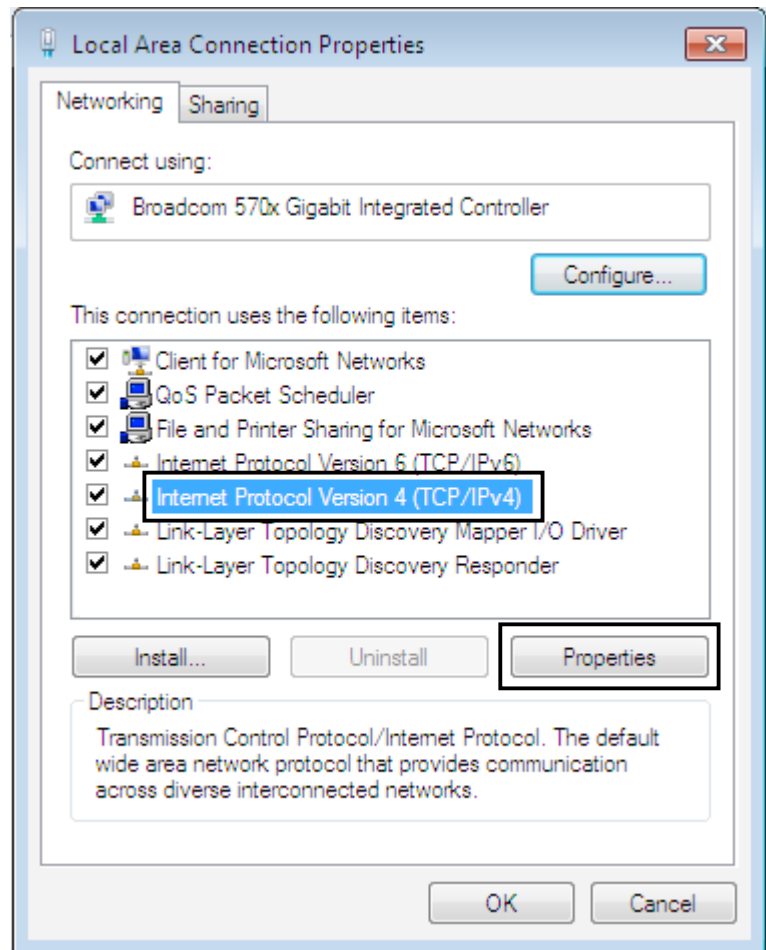


3. Select the **Local Area Connection**, and right click the icon to select **Properties**.

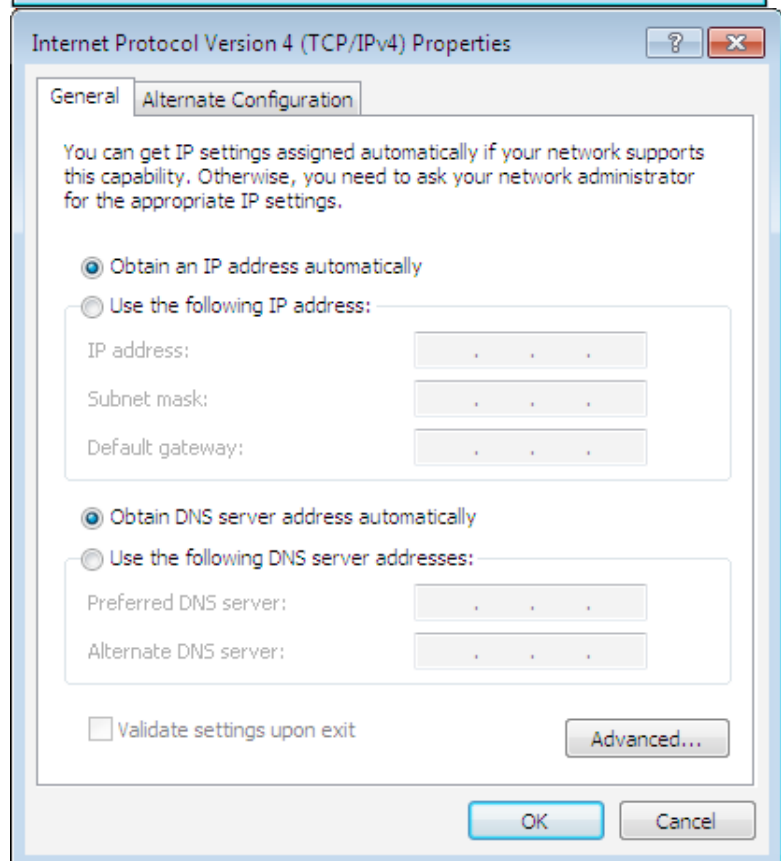


IPv4:

4. Select **Internet Protocol Version 4 (TCP/IPv4)** then click **Properties**

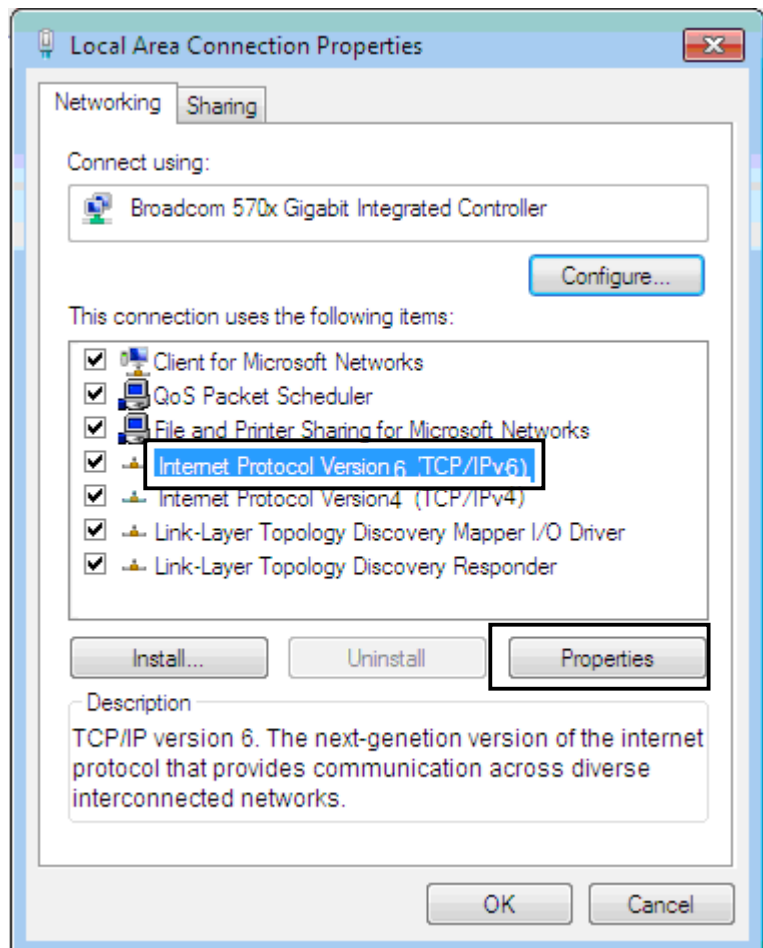


5. In the **TCP/IPv4 properties** window, select the **Obtain an IP address automatically** and **Obtain DNS Server address automatically** radio buttons. Then click **OK** to exit the setting.
6. Click **OK** again in the **Local Area Connection Properties** window to apply the new configuration.

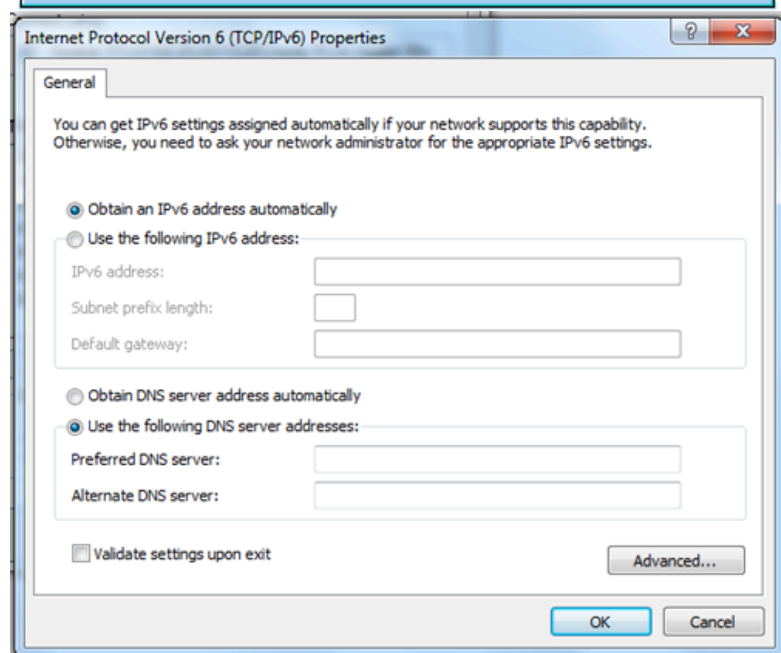


IPv6:

4. Select **Internet Protocol Version 6 (TCP/IPv6)** then click **Properties**



5. In the **TCP/IPv6 properties** window, select the **Obtain an IPv6 address automatically** and **Obtain DNS Server address automatically** radio buttons. Then click **OK** to exit the setting.
6. Click **OK** again in the **Local Area Connection Properties** window to apply the new configuration.



Factory Default Settings

Before configuring your router, you need to know the following default settings.

Web Interface (Username and Password)

- ▶ Username: admin
- ▶ Password: admin



Attention

If you have forgotten the username and/or password of the router, you can restore the device to its default setting by pressing the **Reset Button** more than **5** seconds.

Device LAN IPv4 settings

- ▶ IPv4 Address: 192.168.0.254
- ▶ Subnet Mask: 255.255.255.0

DHCP server for IPv4


- ▶ DHCP server is enabled.
- ▶ Start IP Address: 192.168.0.100
- ▶ IP pool counts: 100

Wireless LAN settings:

- ▶ Default SSID: TW-LTE600xxxx (xxxx = four last mark from device mac address)
- ▶ Wireless LAN default key: Can be found on bottom label.

Chapter 4: Configuration

Configuration via Web Interface

Open your web browser; enter the IP address of your router, which by default is 192.168.0.254, and click  or press 'Enter' key on the keyboard, a login prompt window will appear. The default root username and password are "admin" and "admin" respectively.

Once you have logged on to your Router via your web browser, you can begin to set it up according to your requirements. On the configuration homepage, the left navigation pane links you directly to the setup pages, which include:

● **Status** (Summary, WAN, Statistics, Bandwidth Usage, Route, 3G/LTE Status, Route, ARP, DHCP, VPN, Log, VRRP Status)

● **Configuration** (LAN, Wireless, WAN, System, USB, IP Tunnel, Security, Quality of Service, NAT, Wake On LAN)

● **VPN** (IPSec, VPN Account, Exceptional Rule Group, PPTP, L2TP, OpenVPN, GRE)

● **Advanced Setup** (Routing, DNS, Static ARP, UPnP, Certificate, Multicast, Management, Diagnostics)

Status

This Section gives users an easy access to the information about the working router and access to view the current status of the router.

Here [Summary](#), [WAN](#), [Statistics](#), [Bandwidth Usage](#), [3G/LTE Status](#), [Route](#), [ARP](#), [DHCP](#), [VPN](#) and [Log](#) subsections are included.

Summary

The basic information about the device is provided here (the following is a configured screenshots to let users understand clearly).

Status	
▼ Device Information	
Model Name	TW-LTE 600 Dual Sim Wifi Router
Host Name	Telewell
System Up-Time	0D 0H 1M 14S
Date/Time	Thu Jan 1 00:01:14 1970 <input type="button" value="Sync"/>
Software Version	2.32c.7-14.da7
LAN IPv4 Address	192.168.0.254
LAN IPv6 Address	fe80::21e:abff:fe06:539a/64
MAC Address	00:1e:ab:06:53:9a
Wireless Driver Version	6.30.102.7.cpe4.12L08.4
▼ WAN	
Default Gateway / IPv4 Address	
Connection Time	
Primary DNS Server	0.0.0.0
Secondary DNS Server	0.0.0.0
Default IPv6 Gateway / IPv6 Address	

Device Information

Model Name: Displays the model name.

Host Name: Displays the name of the router.

System Up-Time: Displays the elapsed time since the device is on.

Date/Time: Displays the current exact date and time. Sync button is to synchronize the Date/Time with your PC time without regard to connecting to internet or not.

Software Version: Firmware version.

LAN IPv4 Address: Displays the LAN IPv4 address.

LAN IPv6 Address: Displays the LAN IPv6 address. Default is a Link-Local address, but when connects to ISP, it will display the Global Address, like above figure.

MAC Address: Displays the MAC address.

Wireless Driver Version: Displays wireless driver version.

WAN

Default Gateway/IPv4 Address: Display Default Gateway and the IPv4 address.

Primary DNS Server: Displays IPV4 address of Primary DNS Server.

Secondary DNS Server: Displays IPV4 address of Secondary DNS Server.

Default IPv6 Gateway/IPv6 Address: Display the IPv6 Gateway and the obtained IPv6 address.

WAN

This table displays the information of the WAN connections, users can turn here for WAN connection information.

Status							
WAN							
Wan Info							
Interface	Description	Type	Status	Connection Time	IPv4 Address	IPv6 Address	DNS
usb0	3G0	Direct IP	Fallover / Connected	00:01:02	10.189.81.73		195.197.54.100,195.74.0.47

Interface: The WAN connection interface.

Description: The description of this connection.

Type: The protocol used by this connection.

Status: To disconnect or connect the link.

Connection Time: The WAN connection time since WAN is up.

IPv4 Address: The WAN IPv4 Address the device obtained.

IPv6 Address: The WAN IPv6 Address the device obtained.

DNS: The DNS address the device obtained.

Statistics

LAN

The table shows the statistics of LAN.

Note: P4 can be configured as EWAN, and when the device is in EWAN profile, there is no P4/EWAN interface as P4 is working as a WAN port.

Status									
LAN Statistics									
Interface	Received				Transmitted				
	Bytes	Packets	Errors	Drops	Bytes	Packets	Errors	Drops	
P4/EWAN	0	0	0	0	0	0	0	0	
P3	0	0	0	0	0	0	0	0	
P2	398001	3178	0	0	3661257	4655	0	0	
P1	0	0	0	0	0	0	0	0	
wl0	0	0	0	0	3296	24	0	0	
Reset									

Interface: List each LAN interface. P1-P4 indicates the four LAN interfaces.

Bytes: Display the Received and Transmitted traffic statistics in Bytes.

Packets: Display the Received and Transmitted traffic statistics in Packets.

Errors: Display the statistics of errors arising in Receiving or Transmitting data.

Drops: Display the statistics of drops arising in Receiving or Transmitting data.

Reset: Press this button to refresh the statistics.

WAN Service

The table shows the statistics of WAN.

Status

WAN Service

Statistics

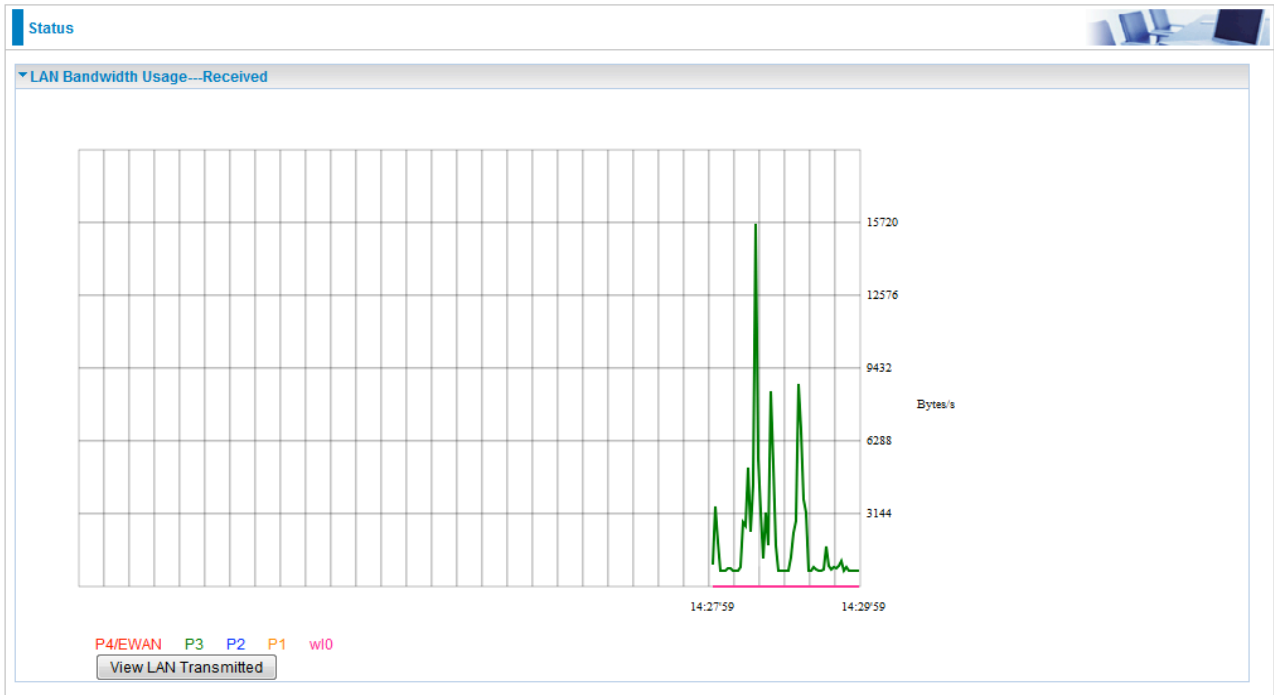
Interface	Description	Received				Transmitted			
		Bytes	Packets	Errors	Drops	Bytes	Packets	Errors	Drops
usb0	3G0	34025	190	0	0	35834	229	0	0

Reset

- Interface:** Display the connection interface.
- Description:** the description for the connection.
- Bytes:** Display the WAN Received and Transmitted traffic statistics in Bytes.
- Packets:** Display the WAN Received and Transmitted traffic statistics in Packests.
- Errors:** Display the statistics of errors arising in Receiving or Transmitting data.
- Drops:** Display the statistics of drops arising in Receiving or Transmitting data.
- Reset:** Press this button to refresh the statistics.

Bandwidth Usage

Press **View LAN or WAN Traffic concurrently** button to directly switch to the LAN or WAN Bandwidth Usage page to view the LAN or WAN traffic concurrently.



3G/LTE Status

▼ 3G/LTE Status	
Parameters	
Current SIM	SIM 1
Status	No SIM Card
Signal Strength	-----
Network Name	N/A
Network Mode	N/A
Card Name	MC7304
Card Firmware	SWI9X15C_05.05.16.02 r21040 carmd-fwbuild1 2014/03/17 23:49:48
Current TX Bytes / Packets	0 / 0
Current RX Bytes / Packets	0 / 0
Total TX Bytes / Packets	0 / 0
Total RX Bytes / Packets	0 / 0
Total Connection Time	00:00:00

Current SIM: The current SIM in use.

Status: The current status of the 3G/LTE card.

Signal Strength: The signal strength bar indicates current 3G/LTE signal strength.

Network Name: The network name that the device is connected to.

Network Mode: The current operation mode for 3G/LTE card, it depends on service provider and card's limitation, GSM or UMTS.

Card Name: The name of the 3G/LTE card.

Card Firmware: The current firmware for the 3G/LTE card.

Current TX Bytes / Packets: The statistics of transmitted Bytes / Packets, count for this call.

Current RX Bytes / Packets: The statistics of received Bytes / Packets, count for this call.

Total TX Bytes / Packets: The statistics of transmitted Bytes / Packets, count since 3G/LTE connection is ready.

Total RX Bytes / Packets: The statistics of received Bytes / Packets, count since 3G/LTE connection is ready.

Total Connection Time: The statistics of the connection time since 3G/LTE connection is ready.

Route

Status						
▼ Route						
Flags: U - up, I - reject, G - gateway, H - host, R - reinstate, D - dynamic (redirect), M - modified (redirect)						
Destination	Gateway	Subnet Mask	Flag	Metric	Service	Interface
10.189.81.72	0.0.0.0	255.255.255.252	U	0	3G0	usb0
192.168.0.0	0.0.0.0	255.255.255.0	U	0		br0
0.0.0.0	10.189.81.74	0.0.0.0	UG	0	3G0	usb0

Destination: The IP address of destination network.

Gateway: The IP address of the gateway this route uses.

Subnet Mask: The destination subnet mask.

Flag: Show the status of the route.

- ① **U:** Show the route is activated or enabled.
- ① **H (host):** destination is host not the subnet.
- ① **G:** Show that the outside gateway is needed to forward packets in this route.
- ① **R:** Show that the route is reinstated from dynamic routing.
- ① **D:** Show that the route is dynamically installed by daemon or redirecting.
- ① **M:** Show the route is modified from routing daemon or redirect.

Metric: Display the number of hops counted as the Metric of the route.

Service: Display the service that this route uses.

Interface: Display the existing interface this route uses.

ARP

This section displays the router's ARP (Address Resolution Protocol) Table, which shows the mapping of Internet (IP) addresses to Ethernet (MAC) addresses. This is useful as a quick way of determining the MAC address of the network interface of your PCs to use with the router's **Security – MAC Filtering** function. Here IPv6 Neighbor Table, listed with IPv6 address-MAC mapping, is supported.

▼ ARP				
ARP Table				
IP Address	Flag	MAC Address	Device	Mark
192.168.0.100	Complete	00:1b:63:9f:5b:7b	br0	

ARP table

IP Address: Shows the IP Address of the device that the MAC address maps to.

Flag: Shows the current status of the ARP entries.

- ① Complete: the route resolving is processing well.
- ① M(Marked as permanent entry): the route is permanent.
- ① P (publish entry): publish this route item.

MAC Address: Shows the MAC address that is corresponded to the IP address of the device it is mapped to.

Device: here refers to the physical interface, it is a concept to identify Clients from LAN or WAN. For example, the Clients in LAN, here displays “br0”.

Mark: Show clearly the SSID (WLAN) the device is in.

Neighbor Cache Table

IPv6 address: Shows the IPv6 Address of the device that the MAC address maps to.

MAC Address: Shows the MAC address that is corresponded to the IPv6 address of the device it is mapped to.

Device: here refers to the physical interface, it is a concept to identify Clients from LAN or WAN. For example, the Clients in LAN, here displays “br0”.

Mark: Show clearly the SSID (WLAN) the device is in.

DHCP

The DHCP Table lists the DHCP lease information for all IP addresses assigned by the DHCP server in the device.

Status				
▼ DHCP				
Leased Table				
Host Name	MAC Address	IP Address	Expires In	Mark
testi	20:6a:8a:2a:5c:39	192.168.0.100	23 hours, 59 minutes, 23 seconds	

Host Name: The Host Name of DHCP client.

MAC Address: The MAC Address of DHCP client host.

IP Address: The IP address which is assigned to the host with this MAC address.

Expires in: The remaining time of the IP being available for this host.

Mark: Show clearly the SSID (WLAN) the device is in.

VPN

VPN status viewing section provides users IPSec, PPTP, L2TP and GRE VPN status.

IPSec

Status					
▼ IPSec Status					
VPN Tunnels					
Name	Active	Local Subnet	Remote Subnet	Remote Gateway	SA
11	✗	192.168.1.0 -- 255.255.255.0	192.168.0.0 -- 255.255.255.0	172.16.1.235	
<input type="button" value="Refresh"/>					

Name: The IPSec connection name.

Active: Display the connection status.

Local Subnet: Display the local network.

Remote Subnet: Display the remote network.

Remote Gateway: The remote gateway address.

SA: The Security Association for this IPSec entry.

Refresh: Click this button to refresh the tunnel status.

PPTP

Status						
▼ PPTP Status						
PPTP Server ▶						
Name ▶	Enable	Status	Connection Type	Peer Network IP	Connect By	Action
test	✓	Connected	Remote Access		172.16.1.207	<button>Drop</button>
PPTP Client ▶						
Name	Enable	Status	Connection Type	Peer Network IP	Client IP	Action
<button>Refresh</button>						

PPTP Server

Name: The PPTP connection name.

Enable: Display the connection status with icon.

Status: The connection status.

Connection Type: Remote Access or LAN to LAN.

Peer Network IP: Display the remote (client side) network and subnet mask in LAN to LAN PPTP connection.

Connected By: Display the IP of remotely connected client.

Action: Act to the connection. Click Drop button to disconnect the tunnel connection.

PPTP Client

Name: The PPTP connection name.

Enable: Display the connection status with icon.

Status: The connection status.

Connection Type: Remote Access or LAN to LAN.

Peer Network IP: Display the remote (server side) network and subnet mask.

Client: Assigned IP by PPTP server.

Action: Act to the connection. Click Disconnect button to disconnect the tunnel connection.

Refresh: Click this button to refresh the connection status.

L2TP

Status						
▼ L2TP Status						
L2TP Server ▶						
Name ▶	Enable	Status	Connection Type	Peer Network IP	Connect By	Action
test1	✓	Connected	Remote Access		192.168.1.10	<button>Drop</button>
L2TP Client ▶						
Name	Enable	Status	Connection Type	Peer Network IP	Client IP	Action
<button>Refresh</button>						

L2TP Server

Name: The L2TP connection name.

Enable: Display the connection status with icon.

Status: The connection status.

Connection Type: Remote Access or LAN to LAN.

Peer Network IP: Display the remote (client side) network and subnet mask in LAN to LAN L2TP connection.

Connected By: Display the IP of remotely connected client.

Action: Act to the connection. Click Drop button to disconnect the tunnel connection.

L2TP Client

Name: The L2TP connection name.

Enable: Display the connection status with icon.

Status: The connection status.

Connection Type: Remote Access or LAN to LAN.

Peer Network IP: Display the network and subnet mask of server side.

Client: Assigned IP by L2TP server.

Action: Act to the connection. Click Disconnect button to disconnect the tunnel connection.

Refresh: Click this button to refresh the connection status.

OpenVPN

Status

▼ OpenVPN Status

OpenVPN Server ▾

Name ▾	Enable	Status	Connection Type	Peer Network IP	Server IP	Connect By	Action
test1	✓	Connected	Remote Access		192.168.15.1	192.168.15.22	Drop

OpenVPN Client ▾

Name	Enable	Status	Peer Network IP	Client IP	Action
test1	✓	Connected	192.168.15.1 (192.168.200.131)	192.168.15.22	Disconnect

Refresh

Status

▼ OpenVPN Status

OpenVPN Server ▾

Name ▾	Enable	Status	Connection Type	Peer Network IP	Server IP	Connect By	Action
test1	✓	Connected	Remote Access		192.168.15.1	192.168.15.22	Drop

OpenVPN Client ▾

Name	Enable	Status	Peer Network IP	Client IP	Action
test1	✓	Connected	192.168.15.1 (192.168.200.131)	192.168.15.22	Disconnect

Refresh

OpenVPN Server

Name: The OpenVPN connection name.

Enable: Display the connection status with icon.

Status: The connection status.

Connection Type: Remote Access or LAN to LAN.

Peer Network IP: Display the subnet address of client side in LAN to LAN mode.

Server IP: The tunnel virtual IP of server side assigned by server itself.

Connected By: The assigned tunnel virtual IP to remotely connected OpenVPN client.

Action: Act to the connection. Click Drop button to disconnect the tunnel connection.

OpenVPN Client

Name: The OpenVPN connection name.

Enable: Display the connection status with icon.

Status: The connection status.

Connection Type: Remote Access or LAN to LAN.

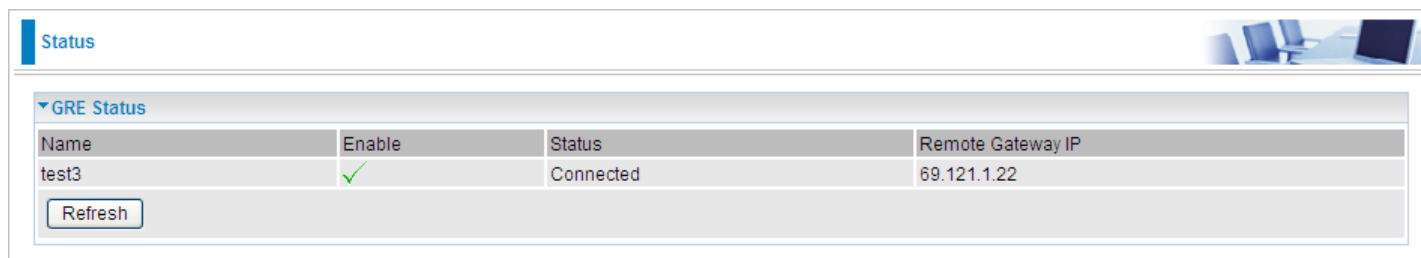
Peer Network IP: Display the tunnel virtual address (WAN address) of server side.

Client: Assigned tunnel virtual IP by OpenVPN server.

Action: Act to the connection. Click Disconnect button to disconnect the tunnel connection.

Refresh: Click this button to refresh the connection status.

GRE



Name	Enable	Status	Remote Gateway IP
test3	✓	Connected	69.121.1.22

Refresh

Name: The GRE connection name.

Enable: Display the connection status with icons.

Status: The connection status, connected or disable.

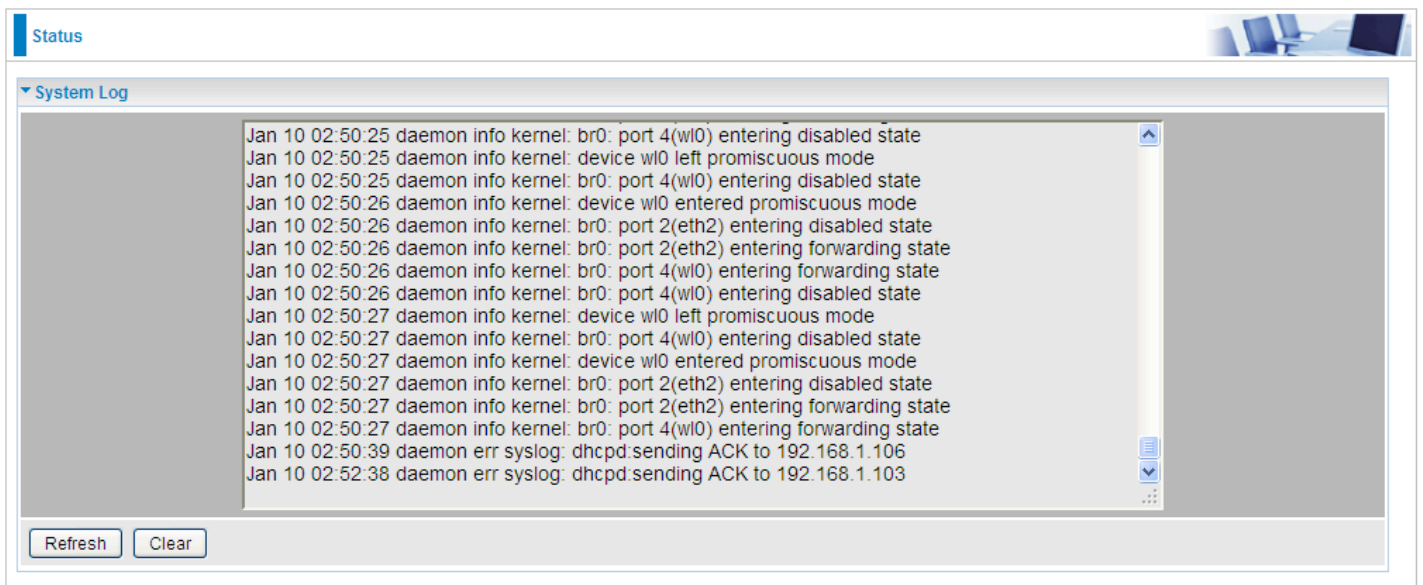
Remote Gateway: The IP of remote gateway.

Refresh: Click this button to refresh the connection status.

Log

System Log

Display system logs accumulated up to the present time. You can trace historical information with this function. And the log policy can be configured in [Configure Log](#) section.

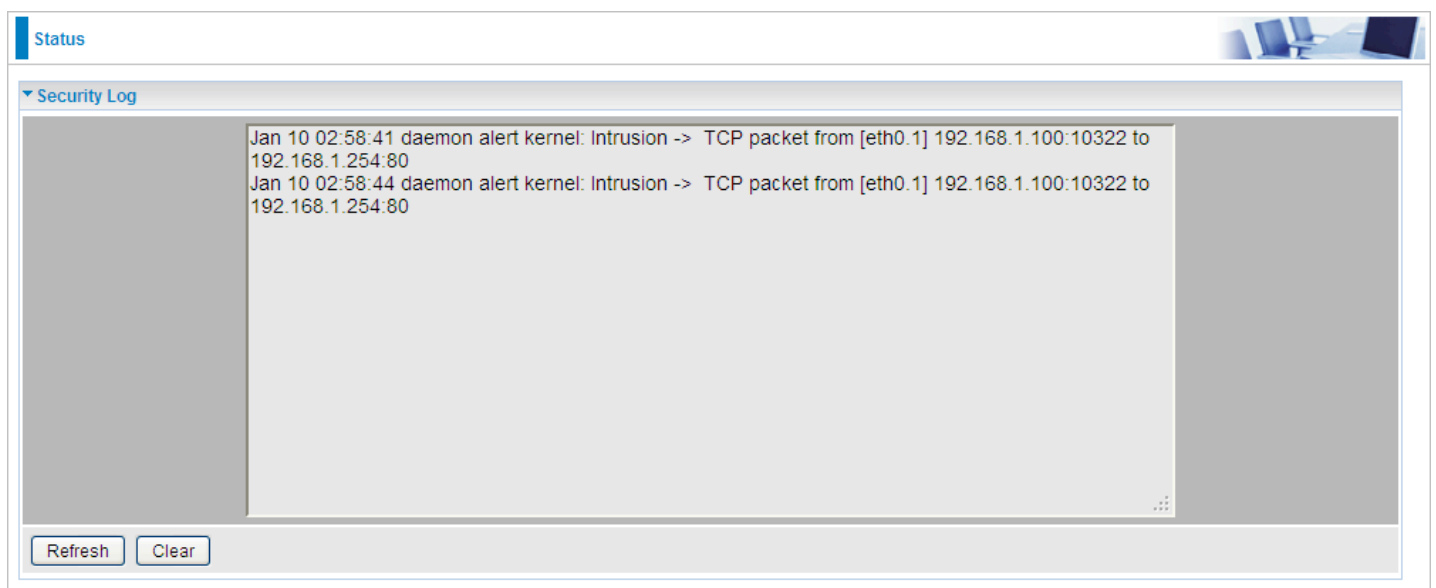


Refresh: Click to update the system log.

Clear: Click to clear the current log from the screen.

Security Log

Security log displays the message logged about security, like filter messages and some firewall message. You can turn to [IP Filtering Outgoing](#), [IP Filtering Incoming](#), [URL Filter](#) to determine if you want to log this information. Also you can turn to Configure Log section below to determine the level to log the message. You can use this to track potential threats to your system and network.



Refresh: Click to update the system log.

Clear: Click to clear the current log from the screen.

Configuration

When you click this item, the column will expand to display the sub-items that will allow you to further configure your router.

[LAN](#), [Wireless](#), [WAN](#), [System](#), [USB](#), [IP Tunnel](#), [Security](#), [Quality of Service](#), [NAT](#) and [Wake On LAN](#).

The function of each configuration sub-item is described in the following sections.

LAN - Local Area Network

A Local Area Network (LAN) is a shared communication system network where many computers are connected. This type of network is area defined and is usually limited to a confined region within a building.

Ethernet

LAN

Parameters

Group Name

Default

IP Address

192.168.0.254

Subnet Mask

255.255.255.0

IGMP Snooping

☒ Enable

IGMP Snooping Mode

☐ Standard Mode ☒ Blocking Mode

LAN side firewall

☐ Enable

DHCP Server

Enable

DHCP Server

Enable

Start IP Address

192.168.0.100

End IP Address

192.168.0.200

Leased Time (hour)

24

Option 66

☐ Enable

Use Router's setting as DNS Server

☒

Primary DNS server

Secondary DNS server

Static IP Lease List

Host Label

MAC Address

IP Address

Remove

Edit

Add

IP Alias

☐ Enable

IP Alias

IP Address

Subnet Mask

Apply

Cancel

Parameters

Group Name: This refers to the group you set in **Interface Grouping** section; you can set the parameters for the specific group. Select the group via the drop-down box. For more information please refer to [Interface Grouping](#) of this manual.

IP address: the IP address of the router. Default is 192.168.0.254.

Subnet Mask: the default Subnet mask on the router.

IGMP Snooping: Enable or disable the IGMP Snooping function. Without IGMP snooping, multicast traffic is treated in the same manner as broadcast traffic - that is, it is forwarded to all ports. With IGMP snooping, multicast traffic of a group is only forwarded to ports that have members of that group.”

When enabled, you will see two modes:

- ① **Standard Mode:** In standard mode, multicast traffic will flood to all bridge ports when no client subscribes to a multicast group.
- ① **Blocking Mode:** In blocking mode, the multicast data will be blocked when there are no client subscribes to a multicast group, it won't flood to the bridge ports.

LAN side firewall: Enable to drop all traffic from the specified LAN group interface. After activating it, all incoming packets by default will be dropped, and the user on the specified LAN group interface can't access CPE anymore. But, you can still access the internet service. If user wants to manage the CPE, please turn to [IP Filtering Incoming](#) to add the allowing rules. **Note** that all incoming packets by default will be dropped if the LAN side firewall is enabled and user cannot manage this CPE from the specified LAN group.

DHCP Server

You can disable or enable the DHCP (Dynamic Host Configuration Protocol) server or enable the router's DHCP relay functions. The DHCP protocol allows your router to dynamically assign IP addresses to PCs on your network if they are configured to obtain IP addresses automatically.

① Disable

DHCP Server	
DHCP Server	Disable ▼

Disable the DHCP Server function.

① Enable

Enable the DHCP function, enter the information wanted. Here as default.

Start IP Address: The start IP address of the range the DHCP Server used to assign to the Clients.

End IP Address: The end IP address of the range the DHCP Server used to assign to the Clients.

Leased Time (hour): The leased time for each DHCP Client.

Option 66: Click Enable to activate DHCP option 66 for some special devices, like IPTV Set Box. The devices can get firmware or some special service from the TFTP server. User needs to set the IP or hostname of the TFTP server.

User Router's setting as DNS server: Select whether to enable use router's setting as DNS server to allow different LAN group with different DNS server settings.

If enabled, the PCs on the LAN side obtain the router's setting as DNS server. If disabled, please specify exactly the primary/secondary DNS server.

Primary/Secondary DNS server: Specify your primary/secondary DNS server for your LAN devices.

① DHCP Server Relay

DHCP Server	
DHCP Server	DHCP Server Relay ▼
DHCP Server IP Address	<input type="text"/>

DHCP Server IP Address: Please enter the DHCP Server IP address.

Static IP List

The specified IP will be assigned to the corresponding MAC Address listed in the following table when DHCP Server assigns IP Addresses to Clients.

Static IP Lease List				
Host Label	MAC Address	IP Address	Remove	Edit
<div>Add</div>				

Press **Add** to the Static IP List.

Configuration

Static IP

Parameters

Host Label

MAC Address

IP Address

Apply

Cancel

Enter the MAC Address, IP Address, and then click Apply to confirm your settings. But the IP assigned should be outside the range of 192.168.0.100-192.168.0.199.

IP Alias

This function allows the creation of multiple virtual IP interfaces on this router. It helps to connect two or more local networks to the ISP or remote node.

IP Alias

IP Alias

IP Address

Subnet Mask

☐ Enable

Apply

Cancel

IP Alias: Check whether to enable this function.

IP Address: Specify an IP address on this virtual interface.

Subnet Mask: Specify a subnet mask on this virtual interface.

Click **Apply** to apply your settings.

IPv6 Autoconfig

The IPv6 address composes of two parts, the prefix and the interface ID.

There are two ways to dynamically configure IPv6 address on hosts. One is “stateful” configuration, for example using DHCPv6 (which resembles its counterpart DHCP in IPv4.) In the stateful auto-configuration model, hosts obtain interface addresses and/or configuration information and parameters from a DHCPv6 server. The Server maintains a database that keeps track of which addresses have been assigned to which hosts.

The second way is “stateless” configuration. Stateless auto-configuration requires no manual configuration of hosts, minimal (if any) configuration of routers, and no additional servers. The stateless mechanism allows a host to generate its own addresses using a combination of locally available information (MAC address) and information (prefix) advertised by routers. Routers advertise prefixes that identify the subnet(s) associated with a link, while hosts generate an “interface identifier” that uniquely identifies an interface on a subnet. An address is formed by combining the two. When using stateless configuration, you needn’t configure anything on the client.

Group Name: Here group refers to the group you set in **Interface Grouping** section, you can set the parameters for the specific group. Select the group by the drop-down box. For more information please refer to **Interface Grouping** of this manual.

Static LAN IPv6 Address Configuration

Interface Address / Prefix Length: Enter the static LAN IPv6 address.

IPv6 LAN application

DHCPv6 Server: Check whether to enable DHCPv6 server.

DHCPv6 Server Type: Select Stateless or Stateful. When DHCPv6 is enabled, this parameter is available. **Stateless:** If selected, the PCs in LAN are configured through RA mode, thus, the PCs in LAN are configured through RA mode, to obtain the prefix message and generate an address using a combination of locally available information (MAC address) and information (prefix) advertised by routers, but they can obtain such information like DNS from DHCPv6 Server. **Stateful:** if selected, the PCs in LAN will be configured like in IPv4 mode, thus obtain addresses and DNS information from DHCPv6 server.

Start interface ID: Enter the start interface ID. The IPv6 address composed of two parts, thus, the prefix and the interface ID. Interface is like the Host ID compared to IPv4.

End interface ID: Enter the end interface ID.

Note: Interface ID does NOT support ZERO COMPRESSION "::". Please enter the complete information.

For example: Please enter "0:0:0:2" instead of "::2".

Leased Time (hour): The leased time, similar to leased time in DHCPv4, is a time limit assigned to clients, when expires, the assigned ID will be recycled and reassigned.

Issue Router Advertisement: Check whether to enable issue Router Advertisement feature. It is to send Router Advertisement messages periodically.

ULA Prefix Advertisement: Enable this parameter to include the ipv6 ULA address in the RA messages. ULA, unique local address, is an IPv6 address in the block fc00::/7. It is approximately the IPv6 counterpart of the IPv4 private address. They are not routable in the global IPv6 Internet.

RADVD Type: The way that ULA prefix is generated.

- ① Randomly Generated
- ① Statically Configured: select to set manually in the following parameters.

Prefix: Set the prefix manually.

Preferred Life Time: The ULA prefix life time. When the time is over, the ULA prefix is invalid any more, -1 means no limit.

Valid Life Time: It is a time threshold, when the time is over, clients should obtain new IPv6 address from the router through RA; -1 means to be limitless.

MLD snooping: Similar to IGMP snooping, listens in on the MLD conversation between hosts and routers by processing MLD packets sent in a multicast network, and it analyzes all MLD packets between hosts and the connected multicast routers in the network. Without MLD snooping, multicast traffic is treated in the same manner as broadcast traffic - that is, it is forwarded to all ports. With MLD snooping, multicast traffic of a group is only forwarded to ports that have members of that group.

- ① **Standard Mode:** In standard mode, multicast traffic will flood to all bridge ports when no client subscribes to a multicast group.
- ① **Blocking Mode:** In blocking mode, the multicast data will be blocked when there is no client subscribes to a multicast group, it won't flood to the bridge ports.

Stateless and Stateful IPv6 address Configuration

Stateless: Two methods can be carried.

- ① With DHCPv6 disabled, but Issue Router Advertisement Enabled

DHCPv6 Server	<input type="checkbox"/> Enable
Issue Router Advertisements	<input checked="" type="checkbox"/> Enable

With this method, the PCs in LAN are configured through RA mode, thus, the PCs in LAN are configured through RA mode, to obtain the prefix message and generate an address using a combination of locally available information (MAC address) and information (prefix) advertised by routers.

- ① With both DHCPv6 and Issue Router Advertisement Enabled

DHCPv6 Server	<input checked="" type="checkbox"/> Enable
DHCPv6 Server Type	<input checked="" type="radio"/> Stateless <input type="radio"/> Stateful
Start interface ID	0:0:0:2
End interface ID	0:0:0:254
Leased Time (hour)	24
Issue Router Advertisements	<input checked="" type="checkbox"/> Enable

With this method, the PCs' addresses in LAN are configured like above method, but they can obtain such information like DNS from DHCPv6 Server.

Stateful: two methods can be adopted.

① With only DHCPv6 enabled

DHCPv6 Server	<input checked="" type="checkbox"/> Enable
DHCPv6 Server Type	<input type="radio"/> Stateless <input checked="" type="radio"/> Stateful
Start interface ID	0:0:0:2
End interface ID	0:0:0:254
Leased Time (hour)	24
Issue Router Advertisements	<input type="checkbox"/> Enable

With this method, the PCs' addresses are configured the same as in IPv4, that is addresses are assigned by DHCPv6 server.

① With both DHCPv6 and Issue Router Advertisement Enabled

DHCPv6 Server	<input checked="" type="checkbox"/> Enable
DHCPv6 Server Type	<input type="radio"/> Stateless <input checked="" type="radio"/> Stateful
Start interface ID	0:0:0:2
End interface ID	0:0:0:254
Leased Time (hour)	24
Issue Router Advertisements	<input checked="" type="checkbox"/> Enable

With this method, the PCs' addresses are configured the same like above, and the address information in RA packets will be neglected.

Interface Grouping

Interface grouping is a function to group interfaces, known as VLAN. A Virtual LAN, commonly known as a VLAN, is a group of hosts with the common set of requirements that communicate as if they were attached to the same broadcast domain, regardless of the physical location. A VLAN has the same attributes as a physical LAN, but it allows for end stations to be grouped together even if they are not located on the same network switch.

Each group will perform as an independent network. To support this feature, you must create mapping groups with appropriate LAN and WAN interfaces using the Add button.

(Please **Note:** P4 can be configured as EWAN, and when the device is in EWAN profile, there is no P4/EWAN interface as P4 is working as a WAN port.)

Interface Grouping

Groups Isolation ☐ Enable ☐

Group Configuration

Maximum number of entries can be configured : 16

Group Name	Remove	WAN Interface	LAN Interfaces	DHCP Vendor IDs
Default			P1	
			P2	
			P3	
			P4/EWAN	
			TW-LTE600539A	

Group Isolation: If enabled, devices in one group are not able to access those in the other group. Click **Add** to add groups.

Interface grouping Configuration

Parameters

If you like to automatically add LAN clients to a WAN Interface in the new group add the DHCP vendor ID string. By configuring a DHCP vendor ID string any DHCP client request with the specified vendor ID (DHCP option 60) will be denied an IP address from the local DHCP server. **IMPORTANT** If a vendor ID is configured for a specific client device, please REBOOT the client device attached to the modem to allow it to obtain an appropriate IP address.

Group Name

Grouped WAN Interfaces	Available WAN Interfaces
<div></div>	<div></div>

Grouped LAN Interfaces	Available LAN Interfaces
<div></div>	<div>P1 P2 P3 P4/EWAN TW-LTE600539A</div>

Automatically Add Clients With the following DHCP Vendor IDs

<input type="text"/>
<input type="text"/>
<input type="text"/>
<input type="text"/>
<input type="text"/>
<input type="text"/>
<input type="text"/>
<input type="text"/>
<input type="text"/>
<input type="text"/>

Group Name: Type a group name.

Grouped WAN Interfaces: Select from the box the WAN interface you want to applied in the group.

Grouped LAN Interfaces: Select the LAN interfaces you want to group as a single group from **Available LAN Interfaces**.

Automatically Add Clients with following DHCP Vendor IDs: Enter the DHCP Vendor IDs for which you want the Clients automatically added into the group. DHCP vendor ID (DHCP 60) is an Authentication for DHCP Messages.

Wireless

This section provides you ways to configure wireless access. The dual-SIM 3G/4G LTE router supports wireless on the 2.4GHz for users. This part has sub-items as **Basic**, **Security**, **MAC Filter**, **Wireless Bridge**, **Advanced** and **Station Info** here.

Basic

It let you determine whether to enable Wireless function and set the basic parameters of an AP and the Virtual APs.

Basic

Parameters

Wireless

☒ Enable

Hide SSID

☐ Enable

Clients Isolation

☐ Enable

Disable WMM Advertise

☐ Enable

Wireless Multicast Forwarding (WMF)

☐ Enable

SSID

BSSID

Country

Max Clients

[1-16]

Wireless - Guest/Virtual Access Points

SSID	Hidden	Clients Isolation	Disable WMM Advertise	WMF	Max Clients	BSSID	Enable
<input type="text" value="wl0_Guest1"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="16"/>	N/A	<input type="checkbox"/>
<input type="text" value="wl0_Guest2"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="16"/>	N/A	<input type="checkbox"/>
<input type="text" value="wl0_Guest3"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="16"/>	N/A	<input type="checkbox"/>

Apply

Cancel

Wireless: Default setting is set to Enable. If you do not have any wireless devices, check the checkbox again to unselect.

Hide SSID: It is function in which transmits its SSID to the air so that when wireless client searches for a network, router can then be discovered and recognized. Check the checkbox to determine whether you want to hide SSID.

Clients Isolation: if you enabled this function, then each of your wireless clients will not be able to communicate with each other.

Disable WMM Advertise: Stop the router from ‘advertising’ its Wireless Multimedia (WMM) functionality, which provides basic quality of service for time-sensitive applications (e.g. VoIP, Video). Check to disable or enable this function.

Wireless multicast Forwarding (WMF): check to enable or disable wireless multicast forwarding.

SSID: The SSID is the unique name of a wireless access point (AP) to be distinguished from another. For security purpose, change the default wlan-ap-2.4g to a unique ID name to the AP already built-in to the router’s wireless interface. It is case sensitive and must not exceed 32 characters. Make sure your wireless clients have exactly the SSID as the device, in order to get connected to your network.

Note: SSID is case sensitive and must not exceed 32 characters.

BSSID: Basic Set Service Identifier, it is a local managed IEEE MAC address, and is 48 bits value.

Country: Different countries have different wireless band resources, so you can select the appropriate Country according to your location.

Max Clients: enter the number of max clients the wireless network can supports,1-16.

Guest/virtual Access Points: A “Virtual Access Point” is a logical entity that exists within a physical Access Point (AP). When a single physical AP supports multiple “Virtual APs”, each Virtual AP appears to stations (STAs) to be an independent physical AP, even though only a single physical AP is present. For example, multiple Virtual APs might exist within a single physical AP, each advertising a distinct SSID and capability set. Alternatively, multiple Virtual APs might advertise the same SSID but a different capability set – allowing access to be provided via Web Portal, WEP, and WPA simultaneously. Where APs are shared by multiple providers, Virtual APs provide each provider with separate authentication and accounting data for their users, as well as diagnostic information, without sharing sensitive management traffic or data between providers. You can enable the virtual AP.

Here you can enable some Virtual APs according to the request. And the other parameters of virtual APs are the same to the above.

Click **Apply** to apply your settings.

Security

Wireless security prevents unauthorized access or damage to computers using wireless network.

▼ Security

If Hide Access Point enabled or Mac filter list is empty with 'allow' chosen, WPS2 will be disabled.

WPS Setup

WPS

Disable ▾

(Current: Disable)

Manual Setup AP

Select SSID

TW-LTE600539A ▾

Network Authentication

WPA-PSK ▾

WPA/WAPI passphrase

.....

[Click here to display](#)

WPA Group Rekey Interval

3600

[0-2147483647]

WPA/WAPI Encryption

AES ▾

Apply

Cancel

Note:

The WPS feature will also be unavailable when the security setting is not WPA2 or OPEN. So, if you manually set the wireless security setting, you should give notice to it, but you can find prompt indicating configuration.

Manual Setup AP

Select SSID: select the SSID you want these settings apply to.

Network Authentication

① **Open**

Network Authentication	Open
WEP Encryption	Enable
Encryption Strength	128-bit
Current Network Key	1
Network Key 1	1234567890123
Network Key 2	1234567890123
Network Key 3	1234567890123
Network Key 4	1234567890123

Enter 13 ASCII characters or 26 hexadecimal digits for 128-bit encryption keys.
Enter 5 ASCII characters or 10 hexadecimal digits for 64-bit encryption keys.

WEP Encryption: Select to enable or disable WEP Encryption. Here select Enable.

Encryption Strength: Select the strength, 128-bit or 64-bit.

Current Network Key: Select the one to be the current network key. Please refer to key 1- 4 below.

Network Key (1- 4): Enter 13 ASCII characters or 26 hexadecimal digits for 128-bit encryption keys.
Enter 5 ASCII characters or 10 hexadecimal digits for 64-bit encryption keys.

① Shared

This is similar to network authentication 'Open'. But here the WEP Encryption must be enabled.

Network Authentication	Shared
WEP Encryption	Enable
Encryption Strength	128-bit
Current Network Key	2
Network Key 1	1234567890123
Network Key 2	1234567890123
Network Key 3	1234567890123
Network Key 4	1234567890123

Enter 13 ASCII characters or 26 hexadecimal digits for 128-bit encryption keys.
Enter 5 ASCII characters or 10 hexadecimal digits for 64-bit encryption keys.

① 802.1x

Network Authentication	802.1X
RADIUS Server IP Address	0.0.0.0
RADIUS Port	1812
RADIUS Key	
WEP Encryption	Enable
Encryption Strength	128-bit
Current Network Key	2
Network Key 1	1234567890123
Network Key 2	1234567890123
Network Key 3	1234567890123
Network Key 4	1234567890123

Enter 13 ASCII characters or 26 hexadecimal digits for 128-bit encryption keys.
Enter 5 ASCII characters or 10 hexadecimal digits for 64-bit encryption keys.

RADIUS Server IP Address: RADIUS(Remote Authentication Dial In User Service), Enter the IP address of RADIUS authentication server.

RADIUS Server Port: Enter the port number of RADIUS authentication server here.

RADIUS Key: Enter the password of RADIUS authentication server.

WEP Encryption: Select to enable or disable WEP Encryption. Here select Enable.

Current Network Key: Select the one to be the current network key. Please refer to key 2- 3 below.

Network Key (1- 4): Enter 13 ASCII characters or 26 hexadecimal digits for 128-bit encryption keys. Enter 5 ASCII characters or 10 hexadecimal digits for 64-bit encryption keys.

① WPA

Network Authentication	WPA
WPA Group Rekey Interval	3600 [0-2147483647]
RADIUS Server IP Address	0.0.0.0
RADIUS Port	1812
RADIUS Key	
WPA/WAPI Encryption	TKIP+AES
WEP Encryption	Disabled

WPA Group ReKey Internal: The period of renewal time for changing the security key automatically between wireless client and Access Point (AP). This is in seconds.

RADIUS Server IP Address: RADIUS(Remote Authentication Dial In User Service), Enter the IP address of RADIUS authentication server.

RADIUS Server Port: Enter the port number of RADIUS authentication server here.

RADIUS Key: Enter the password of RADIUS authentication server.

WPA/WAPI Encryption: There are two Algorithms, AES (Advanced Encryption Standard) and TKIP(Temporal Key Integrity Protocol) which help to protect the wireless communication.

① WPA-PSK / WPA2-PSK

Network Authentication	WPA-PSK
WPA/WAPI passphrase	•••••••• Click here to display
WPA Group Rekey Interval	3600 [0-2147483647]
WPA/WAPI Encryption	TKIP+AES
WEP Encryption	Disabled

WPA/WAPI passphrase: Enter the WPA.WAPI passphrase; you can **click here to display** to view it.

WPA Group ReKey Internal: The period of renewal time for changing the security key automatically between wireless client and Access Point (AP). This is in seconds.

WPA/WAPI Encryption: There are two Algorithms, AES (Advanced Encryption Standard) and TKIP(Temporal Key Integrity Protocol) which help to protect the wireless communication.

① WPA2

Network Authentication	WPA2
WPA2 Preauthentication	Disable
Network Re-auth Interval	36000 [0-2147483647]
WPA Group Rekey Interval	3600 [0-2147483647]
RADIUS Server IP Address	0.0.0.0
RADIUS Port	1812
RADIUS Key	
WPA/WAPI Encryption	AES
WEP Encryption	Disabled

WPA2 Preauthentication: When a wireless client wants to handoff to another AP, with preauthentication, it can perform 802.1X authentication to the new AP, and when handoff happens, this mode will help reduce the association time.

Network Re-auth Interval: the interval for network Re-authentication. This is in seconds.

WPA Group ReKey Internal: The period of renewal time for changing the security key automatically between wireless client and Access Point (AP). This is in seconds.

RADIUS Server IP Address: RADIUS(Remote Authentication Dial In User Service), Enter the IP address of RADIUS authentication server. This is in seconds.

RADIUS Server Port: Enter the port number of RADIUS authentication server here.

RADIUS Key: Enter the password of RADIUS authentication server.

WPA/WAPI Encryption: There are two Algorithms, AES (Advanced Encryption Standard) and TKIP(Temporal Key Integrity Protocol) which help to protect the wireless communication.

① Mixed WPA2/WPA

Network Authentication	Mixed WPA2/WPA
WPA2 Preauthentication	Disable
Network Re-auth Interval	36000 [0-2147483647]
WPA Group Rekey Interval	3600 [0-2147483647]
RADIUS Server IP Address	0.0.0.0
RADIUS Port	1812
RADIUS Key	
WPA/WAPI Encryption	AES
WEP Encryption	Disabled

WPA2 Preauthentication: When a wireless client wants to handoff to another AP, with preauthentication, it can perform 802.1X authentications to the new AP, and when handoff happens, this mode will help reduce the association time used.

Network Re-auth Interval: the interval for network Re-authentication. The unit is second.

WPA Group ReKey Internal: The period of renewal time for changing the security key automatically between wireless client and Access Point (AP). This is in seconds.

RADIUS Server IP Address: RADIUS(Remote Authentication Dial In User Service), Enter the IP address of RADIUS authentication server.

RADIUS Server Port: Enter the port number of RADIUS authentication server here.

RADIUS Key: Enter the password of RADIUS authentication server.

WPA/WAPI Encryption: There are two Algorithms, AES (Advanced Encryption Standard) and TKIP(Temporal Key Integrity Protocol) which help to protect the wireless communication.

① Mixed WPA2/WPA-PSK

Network Authentication	Mixed WPA2/WPA-PSK
WPA/WAPI passphrase	•••••••• Click here to display
WPA Group Rekey Interval	3600 [0-2147483647]
WPA/WAPI Encryption	AES
WEP Encryption	Disabled

WPA/WAPI passphrase: enter the WPA.WAPI passphrase, you can **click here to display** to view it.

WPA Group ReKey Internal: The period of renewal time for changing the security key automatically between wireless client and Access Point (AP). The unit is second.

WPA/WAPI Encryption: There are two Algorithms, AES (Advanced Encryption Standard) and TKIP(Temporal Key Integrity Protocol) which help to protect the wireless communication.

WPS Setup

WPS (Wi-Fi Protected Setup) feature is a standard protocol created by Wi-Fi Alliance. WPS is used to exchange the AP setting with Station and configure Ap settings. This feature greatly simplifies the steps needed to create a Wi-Fi network for a residential or an office setting. The commonly known **PIN method** is supported to configure WPS.

WPS: Select enable to enable WPS function. Please note that WPS can only be available when WPA2-PSK or OPEN mode is configured.

Note:

- 1) WPS feature is only available when in WPA2 or OPEN mode in security settings.
- 2) Here wireless can be configured as **Registrar** and **Enrollee** mode respectively. When AP is configured as Registrar, you should select “Configured” in the WPS AP Mode below, and default WPS AP Mode is “Configured”. When AP is configured as Enrollee, the WPS AP Mode below should be changed to “Unconfigured”. Follow the following steps.

Configuration

▼ Security

If Hide Access Point enabled or Mac filter list is empty with 'allow' chosen, WPA2 will be disabled.

WPS Setup

WPS

Enable (Current: Disable)

Add Client

☒ Enter STA PIN ☐ Use AP PIN [Add Enrollee](#) (This feature is available only when WPA2 PSK or OPEN mode is configured)

PIN

[Help](#)

Authorized Station MAC

[Help](#)

WPS AP Mode

Configured

Setup AP

10864111 [Help](#)

Manual Setup AP

Select SSID

wlan-ap-2.4g

Network Authentication

Open

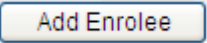
WEP Encryption

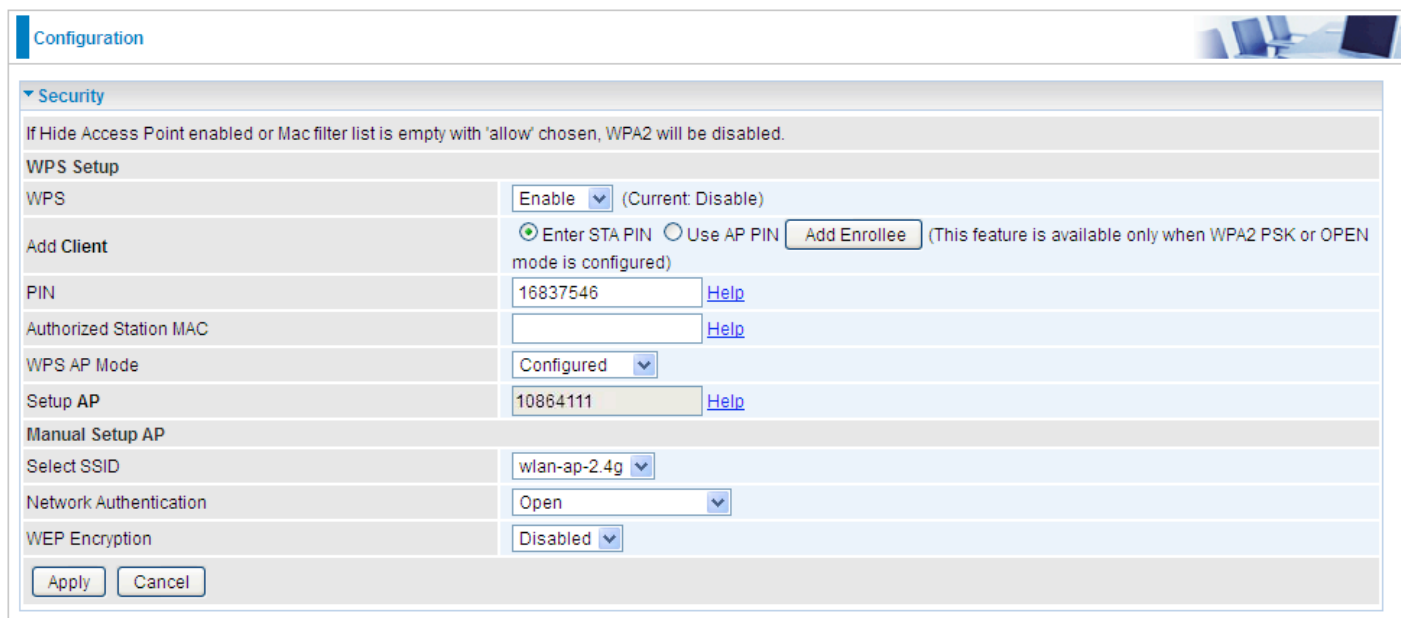
Disabled

[Apply](#) [Cancel](#)

Configure AP as Registrar

● Add Enrollee with PIN method

1. Select radio button “**Enter STA PIN**”.
2. Input PIN from Enrollee Station (16837546 in this example), Or else users can **alternatively** enter the authorized station MAC **Help**: it is to help users to understand the concept and correct operation.
3. Click .



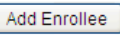
Configuration

▼ Security

If Hide Access Point enabled or Mac filter list is empty with 'allow' chosen, WPA2 will be disabled.

WPS Setup

WPS (Current: Disable)

Add Client ☒ Enter STA PIN ☐ Use AP PIN  (This feature is available only when WPA2 PSK or OPEN mode is configured)

PIN [Help](#)

Authorized Station MAC [Help](#)

WPS AP Mode



Setup AP [Help](#)

Manual Setup AP

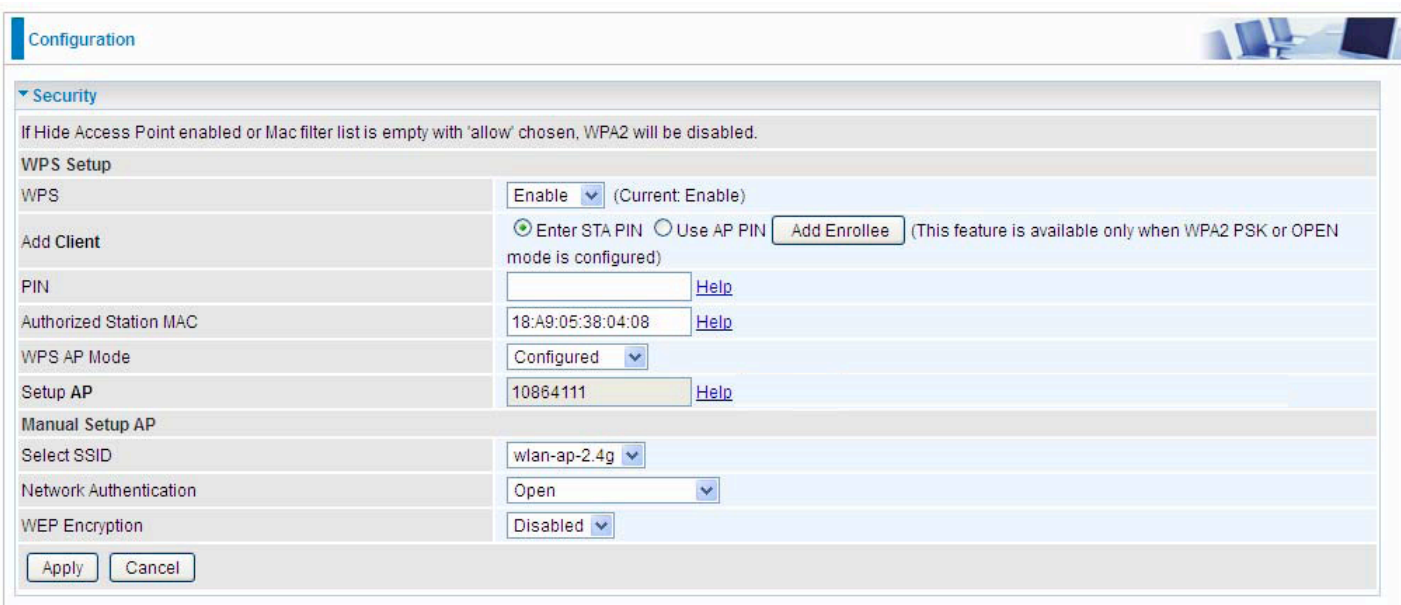
Select SSID

Network Authentication

WEP Encryption

(Station PIN)



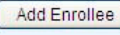
Configuration

▼ Security

If Hide Access Point enabled or Mac filter list is empty with 'allow' chosen, WPA2 will be disabled.

WPS Setup

WPS (Current: Enable)

Add Client ☒ Enter STA PIN ☐ Use AP PIN  (This feature is available only when WPA2 PSK or OPEN mode is configured)

PIN [Help](#)

Authorized Station MAC [Help](#)

WPS AP Mode



Setup AP [Help](#)

Manual Setup AP

Select SSID

Network Authentication

WEP Encryption

(Station MAC)

Note: Users can **alternatively** input PIN from Enrollee Station or enter the authorized station MAC.

4. Operate Station to start WPS Adding Enrollee. Launch the wireless client's WPS utility (eg. Ralink Utility). Set the Config Mode as Enrollee, press the WPS button on the top bar, select the AP (eg. Wlan-ap-2.4g) from the WPS AP List column. Then press the PIN button located on the middle left of the page to run the scan.

The screenshot displays the WPS utility interface with the following components:

- Top Navigation Bar:** Profile, Network, Advanced, Statistics, WMM, WPS, Radio On/Off, About.
- WPS AP List:** A table with columns for ID, Name, MAC, and Count.

ID	Name	MAC	Count
ID : 0x0000	wlan-ap	00-04-ED-01-00-02	1
ID :	wlan-ap-2.4g	00-04-ED-00-00-01	1
- WPS Profile List:** A table with columns for Name, MAC, and Count.

Name	MAC	Count
------	-----	-------
- Buttons:** PIN, PBC, WPS Associate IE, WPS Probe IE, Progress >> 0%, WPS status is disconnected.
- Right Panel:** Rescan, Information, Pin Code (16837546), Renew, Config Mode (Enrollee), Detail, Connect, Rotate, Disconnect, Export Profile, Delete.
- Bottom Section:** Status >> Disconnected, Extra Info >>, Channel >>, Authentication >>, Encryption >>, Network Type >>, IP Address >>, Sub Mask >>, Default Gateway >>, HT, BW >> n/a, SNR0 >> n/a, GI >> n/a, MCS >> n/a, SNR1 >> n/a, Transmit, Link Speed >> Max, Throughput >> 0.000 Kbps, Receive, Link Speed >> Max, Throughput >> 0.000 Kbps.

5. The client's SSID and security settings will now be configured to match the SSID and security settings of the registrar.

The screenshot displays the WPS configuration interface. At the top, there is a navigation bar with icons for Profile, Network, Advanced, Statistics, WMM, WPS, Radio On/Off, and About. The WPS tab is currently selected.

The main area is divided into two sections: WPS AP List and WPS Profile List.

WPS AP List: This section shows a table of available APs. The first entry is 'wlan-ap-2.4g' with MAC address '00-04-ED-01-00-01' and a value of '1'. The second entry is 'wlan-ap' with MAC address '00-04-ED-38-F7-2E' and a value of '1'.

WPS Profile List: This section shows the selected profile 'wlan-ap'. Below it, there are checkboxes for 'WPS Associate IE' and 'WPS Probe IE', both of which are checked. A progress bar indicates 'Progress >> 100%'. A message box states 'PIN - Get WPS profile successfully.'.

Right Panel: This panel contains buttons for 'Rescan', 'Information', 'Pin Code' (with a field showing '16837546' and a 'Renew' button), 'Config Mode' (with a dropdown menu set to 'Enrollee'), 'Detail', 'Connect', 'Rotate', 'Disconnect', 'Export Profile', and 'Delete'.

Status >> wlan-ap-2.4g <--> 00-04-ED-01-00-01: This section provides detailed information about the selected AP. It includes 'Extra Info >> Link is Up [TxPower:100%]', 'Channel >> 1 <--> 2412 MHz; central channel: 3', 'Authentication >> Open', 'Encryption >> NONE', 'Network Type >> Infrastructure', 'IP Address >> 192.168.1.100', 'Sub Mask >> 255.255.255.0', and 'Default Gateway >> 192.168.1.254'. A red ellipse highlights this status information.

Link Quality >> 100%: This section shows signal strength metrics: 'Signal Strength 1 >> 64%', 'Signal Strength 2 >> 34%', and 'Noise Strength >> 26%'.

Transmit: This section shows 'Link Speed >> 270.0 Mbps' and 'Throughput >> 5.600 Kbps'. It includes a graph showing 'Max' throughput of '38.624 Kbps'.

Receive: This section shows 'Link Speed >> 54.0 Mbps' and 'Throughput >> 81.608 Kbps'. It includes a graph showing 'Max' throughput of '146.840 Kbps'.

You can check the message in the red ellipse with the security parameters you set, here we all use the default.

Configure AP as Enrollee

Add Registrar with PIN Method

1. Set AP to “*Unconfigured Mode*”.

Configuration

▼ Security

If Hide Access Point enabled or Mac filter list is empty with 'allow' chosen, WPA2 will be disabled.

WPS Setup

WPS (Current: Disable)

Add Client ☐ Enter STA PIN ☒ Use AP PIN (This feature is available only when WPA2 PSK or OPEN mode is configured)

WPS AP Mode

Setup AP [Help](#)

Manual Setup AP

Select SSID

Network Authentication

WEP Encryption

2. Launch the wireless client's WPS utility. Set the Config Mode as **Registrar**. Enter the **PIN** number (10864111 (device) for example) in the PIN Code column then choose the correct AP (eg. wlan-ap-2.4g) from the WPS AP List section before pressing the PIN button to run the scan.

← Profile Network Advanced Statistics WMM WPS Radio On/Off About →

WPS AP List

ID : 0x0000	wlan-ap-2.4g	00-04-ED-01-00-01	1
ID :	D2-VPN	00-1B-11-E4-DA-D5	

WPS Profile

ExRegNWEA4036

PIN Progress >> 0%

Rescan Information Pin Code Config Mode Detail Connect Rotate Disconnect Export Profile

Status >> Disconnected

Extra Info >>

Channel >>

Authentication >>

Encryption >>

Network Type >>

IP Address >>

Sub Mask >>

Default Gateway >>

HT

BW >> n/a SNR0 >> n/a

GI >> n/a MCS >> n/a SNR1 >> n/a

Link Quality >> 0%

Signal Strength 1 >> 0%

Signal Strength 2 >> 0%

Noise Strength >> 0%

Transmit

Link Speed >> Max

Throughput >> 0.000 Kbps

Receive

Link Speed >> Max

Throughput >> 0.000 Kbps

3. The router's (AP's) SSID and security setting will now be configured to match the SSID and security setting of the registrar.

WPS AP List

ID	SSID	MAC	Channel
wlan-ap-2.4g	00-04-ED-01-00-01	1	
wlan-ap	00-04-ED-38-F7-2E	1	

WPS Profile List

Profile Name	MAC
ExRegNWEA4036	6229909

WPS Configuration

☐ WPS Associate IE
☒ WPS Probe IE

Progress >> 100%

PIN - Get WPS profile successfully.

Status >> wlan-ap-2.4g <-> 00-04-ED-01-00-01

Extra Info >> Link is Up [TxPower:100%]
 Channel >> 1 <-> 2412 MHz; central channel : 3
 Authentication >> WPA2-PSK
 Encryption >> AES
 Network Type >> Infrastructure
 IP Address >> 192.168.1.100
 Sub Mask >> 255.255.255.0
 Default Gateway >> 192.168.1.254

HT

BW >> 40
 GI >> long
 MCS >> 14
 SNR0 >> 20
 SNR1 >> n/a

Link Quality >> 100%

Signal Strength 1 >> 65%
 Signal Strength 2 >> 39%
 Noise Strength >> 26%

Transmit

Link Speed >> 243.0 Mbps
 Throughput >> 0.000 Kbps

Receive

Link Speed >> 40.5 Mbps
 Throughput >> 98.612 Kbps

4. Do Web Page refresh after ER complete AP Configuration to check the new parameters setting.

MAC Filter



▼ MAC Filter

Parameters

Select SSID: TW-LTE600539A

MAC Restrict Mode: ☒ Disable ☐ Allow ☐ Deny

* If 'allow' is chosen and mac filter is empty, WPS will be disabled.

MAC Address	Remove	Edit
-------------	--------	------

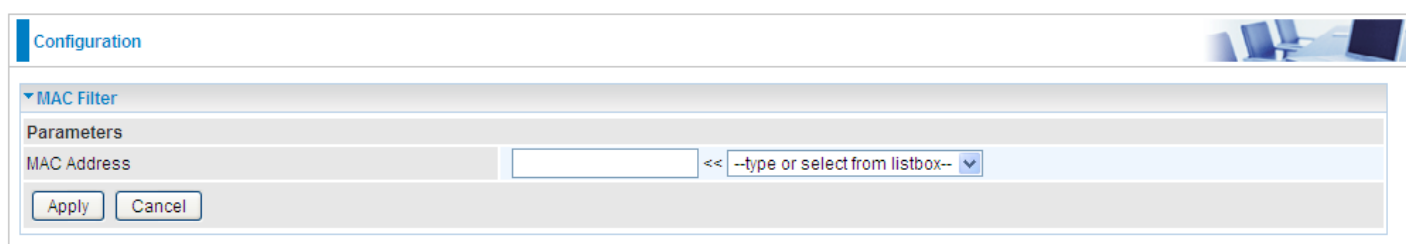
Add Remove

Select SSID: Select the SSID you want this filter applies to.

MAC Restrict Mode:

- ❶ **Disable:** disable the MAC Filter function.
- ❶ **Allow:** allow the hosts with the following listed MACs to access the wireless network.
- ❶ **Deny:** deny the hosts with the following listed MACs to access the wireless network.

Click **Add** to add the MACs.



Configuration

▼ MAC Filter

Parameters

MAC Address: << --type or select from listbox--

Apply Cancel

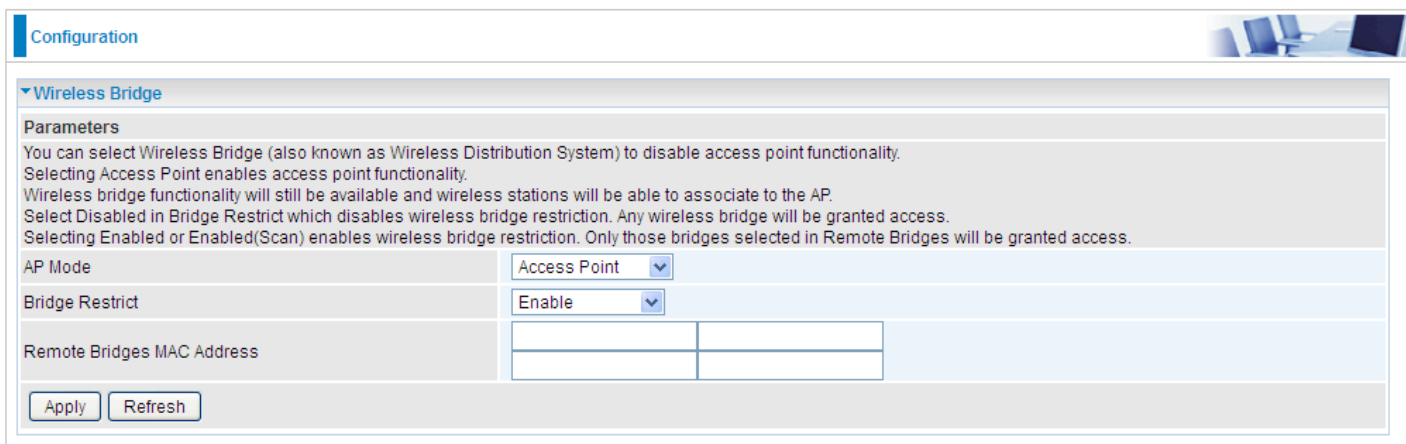
MAC Address: Enter the MAC address(es) or select the MAC address(es). The format of MAC address could be: xx:xx:xx:xx:xx:xx or xx-xx-xx-xx-xx-xx.

Click **Apply** to apply your settings and the item will be listed.

Wireless Bridge

WDS (wireless distributed system) is a wireless access point mode that enables wireless link and communication with other access points. It's easy to install, simply define the peer's MAC address of the connected AP. WDS takes advantage of cost saving and flexibility with no extra wireless client device required to bridge between two access points and extending an existing wired or wireless infrastructure network to create a larger network.

Here you can select what role the AP server has, AP or wireless bridge (WDS).



Configuration

▼ Wireless Bridge

Parameters

You can select Wireless Bridge (also known as Wireless Distribution System) to disable access point functionality. Selecting Access Point enables access point functionality. Wireless bridge functionality will still be available and wireless stations will be able to associate to the AP. Select Disabled in Bridge Restrict which disables wireless bridge restriction. Any wireless bridge will be granted access. Selecting Enabled or Enabled(Scan) enables wireless bridge restriction. Only those bridges selected in Remote Bridges will be granted access.

AP Mode: Access Point

Bridge Restrict: Enable

Remote Bridges MAC Address
<input type="text"/>
<input type="text"/>

Apply Refresh

AP Mode: determines whether the gateway will act as an Access point or as a Bridge.

- ① **Access Point:** the gateway communicates with both clients and bridges.
- ① **Wireless Bridge:** the gateway communicates with other WDS devices only. In this mode, the gateway doesn't communicate with client devices.

If your wireless network includes repeaters that use WDS, the gateway in wireless bridge mode will also communicate with your repeaters. The gateway in wireless bridge mode will not communicate with a repeater that uses a proprietary (non-WDS) mode.

Bridge Restrict: When **AP Mode** is set to **Wireless Bridge**, this determines whether the gateway will communicate with all other bridges or only specific ones:

- ① **Enable:** to enable wireless bridge restriction. Only those specified in the Remote MAC Address the gateway can communicate with.

Bridge Restrict	Enable	
Remote Bridges MAC Address	<input type="text"/>	<input type="text"/>
	<input type="text"/>	<input type="text"/>
<input type="button" value="Apply"/> <input type="button" value="Refresh"/>		

Remote Bridge MAC Address: enter the remote bridge MAC addresses. Here up to 4 bridge MAC addresses are supported.

- ① **Enabled (Scan):** to enable wireless bridge restriction. Only those scanned by the gateway can communicate.

Bridge Restrict	Enabled(Scan)		
Remote Bridges MAC Address	<input type="checkbox"/>	SSID	BSSID
		wlan-ap	00:04:ED:14:27:13
<input type="button" value="Apply"/> <input type="button" value="Refresh"/>			

Remote Bridge MAC Address: select the remote bridge MAC addresses.

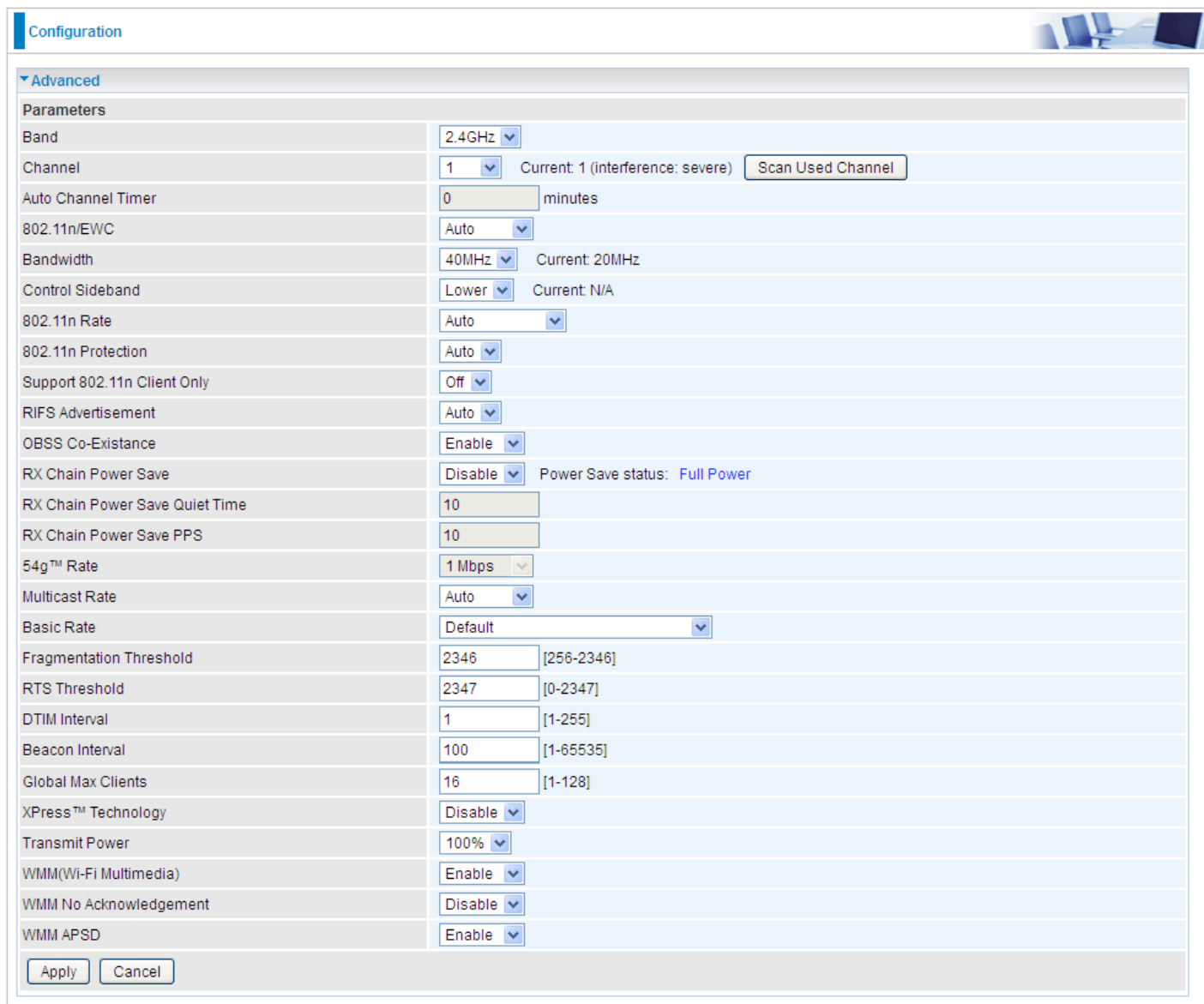
- ① **Disable:** Does not restrict the gateway communicating with bridges that have their MAC address listed, but it is still open to communicate with all bridges that are in the same network.

Bridge Restrict	Disable
<input type="button" value="Apply"/> <input type="button" value="Refresh"/>	

Click **Apply** to apply your settings.

Advanced

Here users can set some advanced parameters about wireless.



The screenshot shows a web-based configuration interface for wireless settings. The title bar at the top left says 'Configuration' and the top right has a small icon of a laptop and a chair. The main content area is titled 'Advanced' and contains a list of parameters. Each parameter has a label, a value field (either a dropdown menu or a text input), and sometimes a 'Current' status or a range. At the bottom of the form are 'Apply' and 'Cancel' buttons.

Parameters	
Band	2.4GHz
Channel	1 Current: 1 (interference: severe) Scan Used Channel
Auto Channel Timer	0 minutes
802.11n/EWC	Auto
Bandwidth	40MHz Current: 20MHz
Control Sideband	Lower Current: N/A
802.11n Rate	Auto
802.11n Protection	Auto
Support 802.11n Client Only	Off
RIFS Advertisement	Auto
OBSS Co-Existence	Enable
RX Chain Power Save	Disable Power Save status: Full Power
RX Chain Power Save Quiet Time	10
RX Chain Power Save PPS	10
54g™ Rate	1 Mbps
Multicast Rate	Auto
Basic Rate	Default
Fragmentation Threshold	2346 [256-2346]
RTS Threshold	2347 [0-2347]
DTIM Interval	1 [1-255]
Beacon Interval	100 [1-65535]
Global Max Clients	16 [1-128]
XPress™ Technology	Disable
Transmit Power	100%
WMM(Wi-Fi Multimedia)	Enable
WMM No Acknowledgement	Disable
WMM APSD	Enable

Apply Cancel

Band: select frequency band. Here 2.4GHz.

Channel: Allows channel selection of a specific channel (1-7) or Auto mode.

Scan Used Channel: Press the button to scan and list all channels being used.

Auto Channel Timer (min): The auto channel times length it takes to scan in minutes. Only available for auto channel mode.

802.11n/EWC: select to auto enable or disable 802.11n.

Bandwidth: Select bandwidth. The higher the bandwidth the better the performance will be.

Control Sideband: only available for 40MHz. It allows you to select upper sideband or lower sideband. Sideband refers to the frequency band either above (**upper sideband**) or below (**lower sideband**) the carrier frequency, within which fall the spectral components produced by modulation of a carrier wave.

802.11n Rate: This allows you to select the fixed transmission rate or auto.

802.11n Protection: turn off for maximize throughput. Auto for greater security.

Support 802.11n Client Only: turn on the option to only provide wireless access to the clients operating at 802.11n speeds.

RIFS Advertisement: Reduced Inter-frame Spacing (RIFS) is a 802.11n feature that also improves performance by reducing the amount of dead time required between OFDM transmissions. Select Off to disable this function or auto to enable this function.

OBSS Co-Existence: coexistence (or not) between 20 MHz and 40 MHz overlapping basic service sets (OBSS) in wireless local area networks.

RX Chain Power Save: Enabling this feature turns off one of the Receive chains, going from 2x2 to 2x1 to save power.

RX Chain Power Save Quiet Time: The number of seconds the traffic must be below the PPS value before the Rx Chain Power Save feature activates itself.

RX Chain Power Save PPS: The maximum number of packets per seconds that can be processed by the WLAN interface for a duration of Quiet Time, described above, before the Rx Chain Power Save feature activates itself.

Multicast Rate: Setting for multicast packets transmission rate.

Basic Rate: Setting for basic transmission rate. It is not a specific kind of rate, it is a series of rates supported. When set to Default, the router can transmit with all kinds of standardized rates.

Fragmentation Threshold: A threshold (in bytes) whether the packets will be fragmented and at what size. Packets succeeding the fragmentation threshold of 802.11n WLAN will be split into smaller units suitable for circuit size. While the packets smaller than fragmentation threshold will not be fragmented. Default is 2346, setting the fragmentation too low may result in poor performance.

RTS Threshold: Request to Send (RTS) threshold specifies the packet size, when exceeds the size, the RTS/CTS will be triggered. The default setting of 2347(max length) will disable the RTS.

DTIM Interval: Delivery Traffic Indication Message (DTIM). The entry range is a value between 1 and 255. A DTIM is countdown variable that informs clients of the next window for listening to broadcast and multicast messages. When the AP has buffered broadcast or multicast messages for associated clients, it sends the next DTIM with a DTIM interval value. AP clients hear the beacons and awaken to receive the broadcast and multicast messages. The default is 1.

Beacon Interval: The amount of time between beacon transmissions in is milliseconds. The default is 100ms and the acceptable is 1- 65535. The beacon transmissions identify the presence of an access point.

Global Max Clients: Here you have the option of setting the limit of the number of clients who can connect to your wireless network.

XPress™ Technology: It has been designed to improve the wireless network efficiency. Default is disabled.

Transmit Power: select the transmitting power of your wireless signal.

WMM (Wi-Fi Multimedia): you can choose to enable or disable this function which allows for priority of certain data over wireless network.

WMM No Acknowledgement: Refers to the acknowledge policy at the MAC level. Enabling WMM No Acknowledgement can result in more efficient throughput but higher error rates in noisy Radio Frequency (RF) environment.

WMM APSD: Automatic Power Save Delivery. Enable this to save power.

Station Info

Here you can view information about the wireless clients.



MAC Address	Associated	Authorized	SSID	Interface
-------------	------------	------------	------	-----------

Refresh

MAC Address: The MAC address of the wireless clients.

Associated: List all the stations that are associated with the Access Point. If a station is idle for too long, it is removed from this list

Authorized: List those devices with authorized access.

SSID: Show the current SSID of the client.

Interface: To show which interface the wireless client is connected to.

Refresh: To get the latest information.

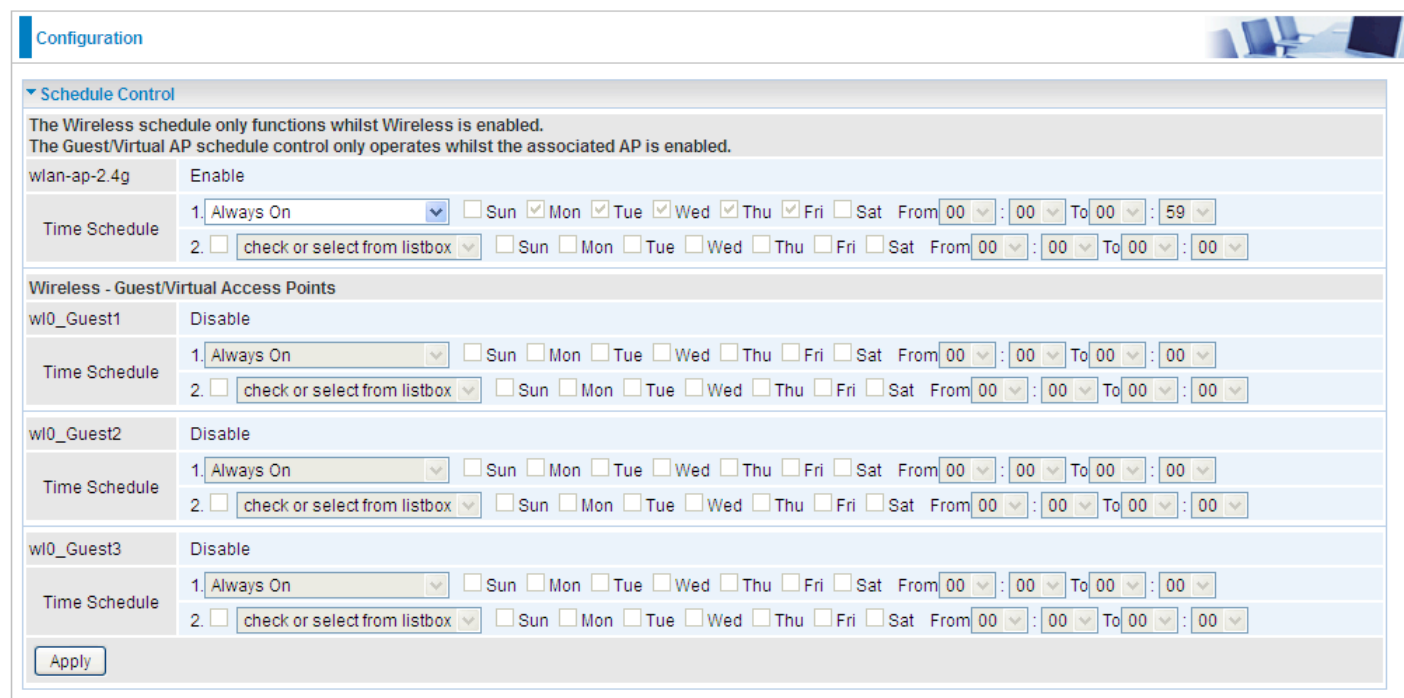
Schedule Control

Schedule control is aimed to offer methods to flexibly control when the wireless network (SSID) is allowed for access.

The Wireless schedule only functions whilst Wireless is enabled.

The Guest/Virtual AP schedule control only operates whilst the associated AP is enabled.

For detail setting the timeslot, user can turn to [Time Schedule](#).



The Wireless schedule only functions whilst Wireless is enabled.
The Guest/Virtual AP schedule control only operates whilst the associated AP is enabled.

wlan-ap-2.4g Enable

Time Schedule

1. Always On ☐ Sun ☒ Mon ☒ Tue ☒ Wed ☒ Thu ☒ Fri ☐ Sat From 00:00 To 00:59

2. ☐ check or select from listbox ☐ Sun ☐ Mon ☐ Tue ☐ Wed ☐ Thu ☐ Fri ☐ Sat From 00:00 To 00:00

Wireless - Guest/Virtual Access Points

w0_Guest1 Disable

Time Schedule

1. Always On ☐ Sun ☐ Mon ☐ Tue ☐ Wed ☐ Thu ☐ Fri ☐ Sat From 00:00 To 00:00

2. ☐ check or select from listbox ☐ Sun ☐ Mon ☐ Tue ☐ Wed ☐ Thu ☐ Fri ☐ Sat From 00:00 To 00:00

w0_Guest2 Disable

Time Schedule

1. Always On ☐ Sun ☐ Mon ☐ Tue ☐ Wed ☐ Thu ☐ Fri ☐ Sat From 00:00 To 00:00

2. ☐ check or select from listbox ☐ Sun ☐ Mon ☐ Tue ☐ Wed ☐ Thu ☐ Fri ☐ Sat From 00:00 To 00:00

w0_Guest3 Disable

Time Schedule

1. Always On ☐ Sun ☐ Mon ☐ Tue ☐ Wed ☐ Thu ☐ Fri ☐ Sat From 00:00 To 00:00

2. ☐ check or select from listbox ☐ Sun ☐ Mon ☐ Tue ☐ Wed ☐ Thu ☐ Fri ☐ Sat From 00:00 To 00:00

Apply

Time Schedule: Set when the SSID works. If user wants the SSID works all the time, please select "Always On"; if not, please set or select the exact time your want the SSID works. Here user can set two separate intervals.

For example: user wants the SSID "wlan-ap-2.4g" to work on weekdays except for Wednesday,

under this circumstance, user can set as shown below. (The router offers a optimal way to set two separate timeslots when user needs to activate the SSID during separate intervals.)

wlan-ap-2.4g

Enable

Time Schedule

1.

check or select from listbox

☐ Sun ☒ Mon ☒ Tue ☐ Wed ☐ Thu ☐ Fri ☐ Sat

 From

00

 :

00

 To

23

 :

59

2. ☒

check or select from listbox

☐ Sun ☐ Mon ☐ Tue ☐ Wed ☒ Thu ☒ Fri ☐ Sat

 From

00

 :

00

 To

23

 :

59

wlan-ap

Enable

Time Schedule

1.

check or select from listbox

☐ Sun ☒ Mon ☒ Tue ☐ Wed ☐ Thu ☐ Fri ☐ Sat

 From

00

 :

00

 To

23

 :

59

2. ☒

check or select from listbox

☐ Sun ☐ Mon ☐ Tue ☐ Wed ☒ Thu ☒ Fri ☐ Sat

 From

00

 :

00

 To

23

 :

59

WAN-Wide Area Network

A WAN (Wide Area Network) is a computer network that covers a broad geographical area (eg. Internet) that is used to connect LAN and other types of network systems.

WAN Service

WAN Service

3G/LTE Interface

Interface	Description	TEL No.	APN	Username	NAT	Firewall	Failover	Edit
USB3G0		*99***1#	internet		Enabled	Enabled	Enabled	<div>Edit</div>

Add

Remove

Click **Add** to add new WAN connections.

i

Ethernet

Ethernet WAN connection is well known as directly broadband WAN connection.

Configuration

WAN Service

Parameters

WAN Port

Ethernet

Type

PPP over Ethernet (PPPoE)

Description

802.1P Priority

-1

[tagged: 0-7; untagged: -1]

802.1Q VLAN ID

-1

[tagged: 0-4094; untagged: -1]

Username

Password

Service Name

Authentication Method

AUTO

Firewall

☒ Enable

NAT

☒ Enable

Fullcone NAT

☐ Enable

IPv4 Address

☐ Static

IP Address

Dial on demand

☐ Enable

Inactivity Timeout

(minutes) [1-4320]

IPv6 for this service

☒ Enable

IP Address

IPv6 Address

☐ Static

IP Address

MTU

1492

PPPoE with Pass-through

☐ Enable


IGMP Multicast Proxy

☐ Enable

MLD Multicast Proxy

☐ Enable

Next

Configuration


WAN Service

Parameters

WAN Port	Ethernet		
Type	PPP over Ethernet (PPPoE)		
Description			
802.1P Priority	-1	[tagged: 0-7; untagged: -1]	802.1Q VLAN ID
			-1 [tagged: 0-4094; untagged: -1]
Username			
Password			
Service Name			
Authentication Method	AUTO	Firewall	<input checked="" type="checkbox"/> Enable
NAT	<input checked="" type="checkbox"/> Enable	Fullcone NAT	<input type="checkbox"/> Enable
IPv4 Address	<input type="checkbox"/> Static	IP Address	
Dial on demand	<input type="checkbox"/> Enable	Inactivity Timeout	(minutes) [1-4320]
IPv6 for this service	<input checked="" type="checkbox"/> Enable		
IPv6 Address	<input type="checkbox"/> Static	IP Address	
MTU	1492		
PPPoE with Pass-through	<input type="checkbox"/> Enable		
IGMP Multicast Proxy	<input type="checkbox"/> Enable	MLD Multicast Proxy	<input type="checkbox"/> Enable

Next

Description: User-defined description for the connection, commonly for friendly use.

802.1P Priority: The parameter indicates the frame priority level from 0 (lowest) to 7 (highest), which can be used to prioritize different classes of traffic (voice, video, data, etc). Enter the priority identification, tagged: 0-1, untagged: -1.

802.1Q VLAN ID: It is a parameter to specify the VLAN which the frame belongs. Enter the VLAN ID identification, tagged: 0-4094, untagged : -1.

Username: Enter the account obtained from the ISP.

Password: Enter the password obtained from the ISP.

Service Name: The item is for identification purpose, user can define it yourselfe.

Authentication Method: Default is **Auto**. Or else your ISP will advise you the appropriate mode.

Firewall: Enable to drop all traffic from WAN side. If enabled, all incoming packets by default would be dropped, and please turn to [IP Filtering Incoming](#) to add allowing rules.

NAT: The NAT (Network Address Translation) feature allows multiple users to access the Internet through a single IP account by sharing the single IP address. If users on your LAN have their own public IP addresses to access the Internet, NAT function can be disabled. When enabled, a Fullcone NAT parameter will appear, you can determine whether to enable Fullcone NAT. While only NAT enabled, the default NAT type Port-Restricted cone NAT will be used.

Fullcone NAT: Enable or disable fullcone NAT. Fullcone is a kind of NAT, in this mode, all requests from the same internal IP address and port are mapped to the same external IP address and port. Furthermore, any external host can send a packet to the internal host by sending a packet to the mapped external address.

Note: In PPPoE connection, NAT is enabled by default, you can determine whether to enable Fullcone NAT. and while you disable Fullcone NAT and only use NAT, the default NAT type is Port Restricted or Port-Restricted cone NAT, the restriction includes port numbers. Specifically, an external host can send a packet, with source IP address X and source port P, to the internal host only if the internal host had previously sent a packet to IP address X and port P

IPv4 Address: Select whether to set static IPv4 address or obtain automatically.

IP Address: If **Static** is enabled in the above field, enter the static IPv4 address get from the ISP.

Dial on demand: It is a parameter to let users to dial for connection to internet themselves. It is useful when saving internet fees.

Inactivity Timeout: The set Inactivity timeout period, unit: minutes. It is combined use with Dial on Demand, users should specify the concrete time interval for dial on demand.

IPv6 for this service: Enable to use IPv6 service.

IPv6 Address: Select whether to set static IPv6 address or obtain automatically.

IP Address: If **Static** is enabled in the above field, enter the static IPv4 address.

MTU: Maximum Transmission Unit, the size of the largest datagram (excluding media-specific headers) that IP will attempt to send through the interface.

PPPoE with Pass-through: Enable or disable PPPoE pass-through. If it is enabled, PCs behind the router can dial itself.

IGMP Multicast Proxy: Check whether to enable this feature. IGMP (**I**nternet **G**roup **M**anagement **P**rotocol) Proxy intercepts the IGMP request from Clients and set up the multicast-forwarding table, it takes over some of the router's job, simplifying the router's job and multicast communication.

MLD Multicast Proxy: check whether to enable this function. MLD (**M**ulticast **L**istener **D**iscovery **P**rotocol) Proxy intercepts the MLD request from Clients a set up the multicast-forwarding table. it takes over some of the router's job, simplifying the router's job and multicast communication. Support MLDv1 and MLDv2.

Click **Next** to continue to set the default gateway and DNS for IPv4 and IPv6.

Configuration

▼ Default Gateway / DNS

Default Gateway

Selected Default Gateway Interfaces

ppp0.1

Available Routed WAN Interfaces

3G0/USB3G0

Selected WAN Interface As The System Default IPv6 Gateway

pppoe_eth0/ppp0.1

DNS

DNS Server Interface

Available WAN Interfaces Static DNS Address Parent Controls

Selected DNS Server Interfaces

ppp0.1

Available WAN Interfaces

3G0/USB3G0

Primary DNS server

Secondary DNS server

Note that selecting a WAN interface for IPv6 DNS server will enable DHCPv6 Client on that interface.

DNS Server Interface

Available WAN Interfaces Static DNS IPv6 Address

WAN Interface selected

pppoe_eth0/ppp0.1

Primary IPv6 DNS server

Secondary IPv6 DNS server

Next

Default Gateway

Select default gateway for you connection (IPv4 and IPv6).

DNS

➤ IPv4

Three ways to set an IPv4 DNS server

- ① **Available WAN interfaces:** Select a desirable WAN interface as the IPv4 DNS server.
- ① **Static DNS Address:** To specify DNS server manually by entering your primary and secondary DNS server addresses.
- ① **Parental Controls:** If user registers and gets a DNS account in the parental control provider website, expecting to enjoy a more reliable and safer internet surfing environment, please select this option (need to configure at [Parental Control Provider](#)).

➤ IPv6

Obtain IPv6 DNS info from a WAN interface

WAN Interface selected: Select one configured IPv6 WAN connection from the menu to be as an IPv6 DNS.

Static DNS IPv6 Address

Primary IPv6 DNS Server / Secondary IPv6 DNS Server: Type the specific primary and secondary IPv6 DNS Server address.

If you don't need the service, select the item you want to remove, check the checkbox, then press **Remove**, it will be OK.

Press **Edit** button to re-edit this service settings.

Configuration

▼ WAN Service

ETH Interface

Interface	Description	Type	Vlan8021p	VlanMuxId	Igmp	NAT	Firewall	IPv6	Mld	Remove	Edit
ppp0.1	pppoe_eth0	PPPoE	N/A	N/A	Disabled	Enabled	Enabled	Enabled	Disabled	<input type="checkbox"/>	<button>Edit</button>

3G/LTE Interface

Interface	Description	TEL No.	APN	Username	NAT	Firewall	Failover	Edit
USB3G0		*99***1#	internet		Enabled	Enabled	Enabled	<button>Edit</button>

Add Remove

Here the corresponding WAN Service have been configured, if it is OK, you can access the internet. You can go to **Status>WAN** or **Summary** to view the WAN connection information (if your ISP provides IPv6 service, then you will obtain an IPv6 address).

WAN Service			
Parameters			
WAN Port	Ethernet		
Type	IP over Ethernet		
Description			
802.1P Priority	-1 [tagged: 0-7; untagged: -1]	802.1Q VLAN ID	-1 [tagged: 0-4094; untagged: -1]
Obtain an IP address automatically	<input checked="" type="checkbox"/> Enable		
Option 60 Vendor ID			
Option 61 Client ID			
Option 125	<input checked="" type="radio"/> Disable <input type="radio"/> Enable		
WAN IP Address			
WAN Subnet Mask			
WAN gateway IP Address			
IPv6 for this service	<input checked="" type="checkbox"/> Enable		
Obtain an IPv6 address automatically	<input checked="" type="checkbox"/> Enable		
WAN IPv6 Address/Prefix Length			
WAN Next-Hop IPv6 Address			
NAT	<input checked="" type="checkbox"/> Enable	Fullcone NAT	<input type="checkbox"/> Enable
Firewall	<input checked="" type="checkbox"/> Enable	IGMP Multicast	<input type="checkbox"/> Enable
MLD Multicast Proxy	<input type="checkbox"/> Enable		
MTU	1500	MAC Spoofing	
<input type="button" value="Next"/>			

Description: User-defined description for the connection, commonly for friendly use.

802.1P Priority: The parameter indicates the frame priority level from 0 (lowest) to 7 (highest), which can be used to prioritize different classes of traffic (voice, video, data, etc). Enter the priority identification, tagged: 0-1, untagged: -1.

802.1Q VLAN ID: It is a parameter to specify the VLAN which the frame belongs. Enter the VLAN ID identification, tagged: 0-4094, untagged : -1.

Here two modes are supported for users to deal with the IP and DNS. You can select obtain automatically or manually input the information according to your ISP.

Obtain an IP address automatically: Check whether to enable this function.

Option 60 Vendor ID: Enter the associated information by your ISP. This option is used by DHCP clients to optionally identify the vendor type and configuration of a DHCP client. The information is a string of n octets, interpreted by servers. Vendors may choose to define specific vendor class identifiers to convey particular configuration or other identification information about a client.

Option 61 Client ID: Enter the associated information provided by your ISP.

Option 125: Option 125 is a complementary standard of DHCP protocol, it is used to encapsulate option 125 message into DHCP offer packet before forward it to clients. After the clients receive the packet, it check the option 125 field in the packet with the pre-stored message, if it is matched, then the client accepts this offer, otherwise it will be abandoned. Check Enable or Disable this function. Default setting is **Disable**.

WAN IP Address: Enter your IPv4 address to the device provided by your ISP.

WAN Subnet Mask: Enter your submask to the device provided by your ISP.

WAN gateway IP Address: Enter your gateway IP address to the device provided by your ISP.

IPv6 for this service: Enable to use IPv6 service.

Obtain an IPv6 address automatically: check whether to enable or disable this feature.

WAN IPv6 Address/Prefix Length: Enter the WAN IPv6 Address/Prefix Length from your ISP.

WAN Next-Hop IPv6 Address: Enter the WAN Next-Hop IPv6 Address from your ISP.

Note: If you don't know well about the DHCP Option, you can leave it empty or leave it as default.

NAT: The NAT (Network Address Translation) feature allows multiple users to access the Internet through a single IP account by sharing the single IP address. If users on your LAN have their own public IP addresses to access the Internet, NAT function can be disabled. When enabled, a Fullcone NAT parameter will appear, you can determine whether to enable Fullcone NAT. While only NAT enabled, the default NAT type Port-Restricted cone NAT will be used.

Fullcone NAT: Enable or disable fullcone NAT. Fullcone is a kind of NAT, in this mode, all requests from the same internal IP address and port are mapped to the same external IP address and port. Furthermore, any external host can send a packet to the internal host, by sending a packet to the mapped external address.

Firewall: Enable to drop all traffic from WAN side. If enabled, all incoming packets by default would be dropped, and please turn to [IP Filtering Incoming](#) to add allowing rules.

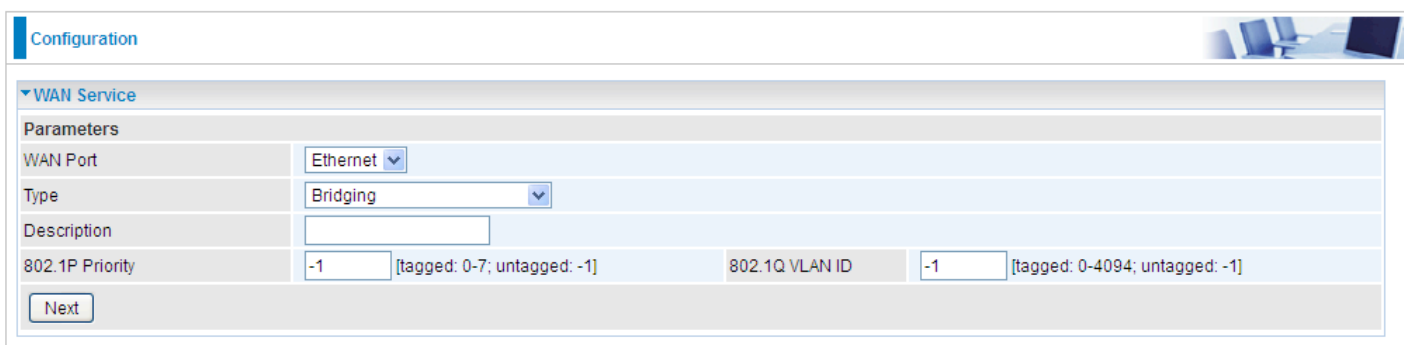
IGMP Multicast: IGMP (Internet Group Membership Protocol) is a protocol used by IP hosts to report their multicast group memberships to any immediately neighboring multicast routers. Check this item to enable IGMP multicast on that WAN interface for multicast forwarding.

MLD Multicast Proxy: check whether to enable this function. MLD (Multicast Listener Discovery Protocol) Proxy intercepts the MLD request from Clients a set up the multicast-forwarding table. it takes over some of the router's job, simplifying the router's job and multicast communication. Support MLDv1 and MLDv2.

MTU: Maximum Transmission Unit, the size of the largest datagram (excluding media-specific headers) that IP will attempt to send through the interface.

MAC Spoofing: This option is required by some service providers specifying some specific MAC allowed to join in network. You must fill in the MAC address specified by your service provider when this information is required.

Bridging



Configuration

WAN Service

Parameters

WAN Port: Ethernet

Type: Bridging

Description:

802.1P Priority: -1 [tagged: 0-7; untagged: -1] 802.1Q VLAN ID: -1 [tagged: 0-4094; untagged: -1]

Next

Description: User-defined description for the connection, commonly for friendly use.

802.1P Priority: The parameter indicates the frame priority level from 0 (lowest) to 7 (highest), which can be used to prioritize different classes of traffic (voice, video, data, etc). Enter the priority identification, tagged: 0-1, untagged: -1.

802.1Q VLAN ID: It is a parameter to specify the VLAN which the frame belongs. Enter the VLAN ID identification, tagged: 0-4094, untagged : -1.

3G/LTE

Select 3G/LTE to configure the route to enjoy the mobility. Given that the router supports dual -SIM mobile connectivity, please determine which SIM you are gonna use or both (3G/LTE failover), and set the exact required connecting information for each SIM (SIM1 and SIM2). By default the 3G/LTE interface is on, user can edit the parameters to meet your own requirements.

Click **Edit** button to enter the 3G/LTE configuration page.

Configuration			
WAN Service			
Parameters			
Failover	<input checked="" type="checkbox"/> Enable		
SIM 1 (Current)			
Mode	Automatic ▼		
TEL No.	*99#	APN	internet
Username		Password	
Authentication Method	AUTO ▼	PIN	
Dial on demand	<input type="checkbox"/> Enable		
Keep Alive	<input checked="" type="checkbox"/> Enable 7 seconds [1-86400]		
IP Address	8.8.8.8		
MTU	1500		
SIM 2			
Mode	Automatic ▼		
TEL No.	*99#	APN	internet
Username		Password	
Authentication Method	AUTO ▼	PIN	
Dial on demand	<input type="checkbox"/> Enable		
Keep Alive	<input checked="" type="checkbox"/> Enable 7 seconds [1-86400]		
IP Address	8.8.8.8		
MTU	1500		
NAT	<input checked="" type="checkbox"/> Enable		Firewall <input checked="" type="checkbox"/> Enable

SIM 1 & SIM 2

Mode: There are 6 options of phone service standards: GSM 2G only, UTMS 3G only, GSM 2G preferred, UMTS 3G preferred, Automatic, and Use 3G/LTE 3g dongle settings. If you are uncertain what services are available to you, and then please select Automatic.

TEL No.: The dial string to make a 3G/LTE user internetworking call. It may provide by your mobile service provider.

APN: An APN is similar to a URL on the WWW, it is what the unit makes a GPRS / UMTS call. The service provider is able to attach anything to an APN to create a data connection, requirements for APNs varies between different service providers. Most service providers have an internet portal which they use to connect to a DHCP Server, thus giving you access to the internet i.e. some 3G operators use the APN 'internet' for their portal. The default value is "internet".

Username/Password: Enter the username and password provided by your service provider. The username and password are case sensitive.

Authentication Protocol: Default is Auto. Please consult your service provider on whether to use PAP, CHAP or MSCHAP.

PIN: PIN stands for Personal Identification Number. A PIN code is a numeric value used in certain systems as a password to gain access, and authenticate. In mobile phones a PIN code locks the SIM card until you enter the correct code. If you enter the PIN code incorrectly into the phone 3 times in a row, then the SIM card will be blocked and you will require a PUK code from your network/ service provider.

- ① **Connect on Demand:** If you want to make UMTS/GPRS call only when there is a packet requesting access to the Internet (i.e. when a program on your computer attempts to access the Internet). In this mode, you must set Idle Timeout value at same time. Click on Connect on Demand, the Idle Timeout field will display.

Idle Timeout: Auto-disconnect the broadband firewall gateway when there is no activity on the line for a predetermined period of time. Default is 600 seconds.

Dial on demand	<input checked="" type="checkbox"/> Enable
Idle Timeout	600 seconds [10-86400]

- ① **Keep Alive:** Check Enable to allow the router to check the mobile connectivity every 7 (can be changed based on need) seconds by ping the IP address set below the keep the 3G/LTE link active.

IP Address: The IP address is used to “ping”, and router will ping the IP to find whether the connection is still on.

Dial on demand	<input type="checkbox"/> Enable
Keep Alive	<input checked="" type="checkbox"/> Enable 7 seconds [1-86400]
IP Address	8.8.8.8

NAT: Check to enable the NAT function.

Firewall: Enable to drop all traffic from WAN side. If enabled, all incoming packets by default would be dropped, and please turn to [IP Filtering Incoming](#) to add allowing rules.

MTU: MTU (Maximum Transmission Unit) is the size of the largest datagram that IP will attempt to send through the interface.

Dual SIM

The advanced dual-SIM 3G/4G LTE router offers dual-SIM slots for two mobile SIM cards. The SIM 1 will be in use when two SIM cards are both up. The current SIM connection will fail over to the other SIM connection when the situation below happens. But note when the failover is done, the connection cannot fail back to the previous SIM connection.

Configuration

▼ Dual SIM

Parameters

Failover	<input checked="" type="checkbox"/> Enable
Connectivity Decision	Not in service when probing failed after 5 consecutive times.
Failover Probe Cycle	Every 12 seconds.
Detect Rule	<input checked="" type="radio"/> SIM Lost <input type="radio"/> Ping Host Fail 1. 8.8.8.8 2.

Failover: Check Enable to activate failover feature.

Connectivity Decision: Set how many times of probing failure to switch to the other SIM.

Failover Probe Cycle: Set the time duration for the Probe Cycle to determine when the router will switch to the other SIM once the current SIM connection fails. For example, when set to 12 seconds, the probe will be conducted every 12 seconds.

Detect Rule: Choose the probe policy, to Ping Host or when SIM lost

- ① **SIM Lost:** SIM card absent or not be able to establish connection.
- ① **Ping Host Fail:** It will send ping packets to host pre-set, and wait for response from it in every “Probe Cycle” to check the connectivity to the mail SIM.

Note:

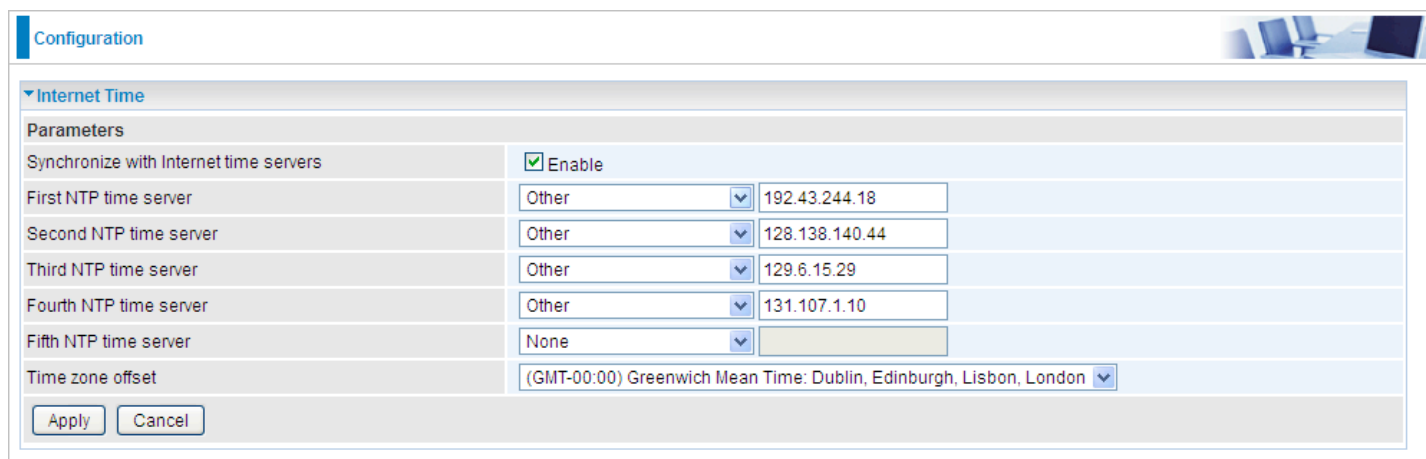
The time set is for each probe cycle, but the decision to change to the other SIM is determined by Probe Cycle multiplied by connection Decision amount (e.g. From the image above it will be 12 seconds multiplied by 5 consecutive fails, the router will determine failover to another SIM).

System

Internet Time

The router does not have a real time clock on board; instead, it uses the Network Time Protocol (NTP) to get the most current time from an NTP server.

NTP is a protocol for synchronization of computers. It can enable computers synchronize to the NTP server or clock source with a high accuracy.



Internet Time	
Parameters	
Synchronize with Internet time servers	<input checked="" type="checkbox"/> Enable
First NTP time server	Other [v] 192.43.244.18
Second NTP time server	Other [v] 128.138.140.44
Third NTP time server	Other [v] 129.6.15.29
Fourth NTP time server	Other [v] 131.107.1.10
Fifth NTP time server	None [v]
Time zone offset	(GMT-00:00) Greenwich Mean Time: Dublin, Edinburgh, Lisbon, London [v]
[Apply] [Cancel]	

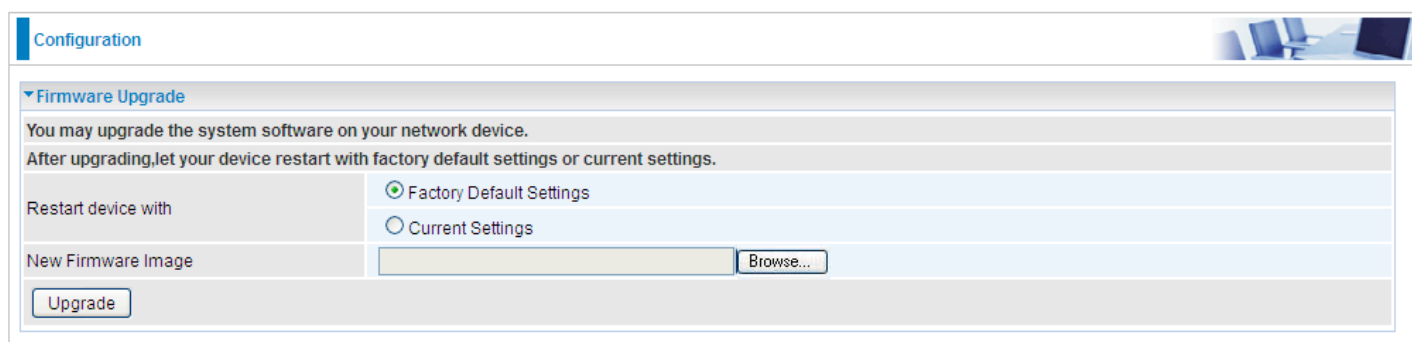
Choose the NTP time server from the drop-down menu, if you prefer to specify an NTP server other than those in the drop-down list, simply enter its IP address in their appropriate blanks provided as shown above. Your ISP may also provide an SNTP server for you to use.

Choose your local time zone from the drop-down menu. After a successful connection to the Internet, the router will retrieve the correct local time from the NTP server you have specified. If you prefer to specify an NTP server other than those in the drop-down list, simply enter its IP address in their appropriate blanks provided as shown above. Your ISP may also provide an NTP server for you to use.

Click **Apply** to apply your settings.

Firmware Upgrade

Software upgrading lets you experience new and integral functions of your router.



The screenshot shows the 'Configuration' tab with the 'Firmware Upgrade' section expanded. It contains instructions: 'You may upgrade the system software on your network device. After upgrading, let your device restart with factory default settings or current settings.' Below this, there are two radio buttons: 'Factory Default Settings' (selected) and 'Current Settings'. A text field for 'New Firmware Image' is followed by a 'Browse...' button. At the bottom is an 'Upgrade' button.

Restart device with:

- ① **Factory Default Settings:** Restart the device with factory default settings automatically when finishing upgrading.
- ① **Current Settings:** Restart the device with the current settings automatically when finishing upgrading.

Your router's "firmware" is the software that allows it to operate and provides all its functionality.

Think of your router as a dedicated computer, and the firmware as the software it runs. Over time this software may be improved and revised, and your router allows you to upgrade the software it runs to take advantage of these changes.

Clicking on **Browse** will allow you to select the new firmware image file you have downloaded to your PC. Once the correct file is selected, click **Upgrade** to update the firmware in your router.

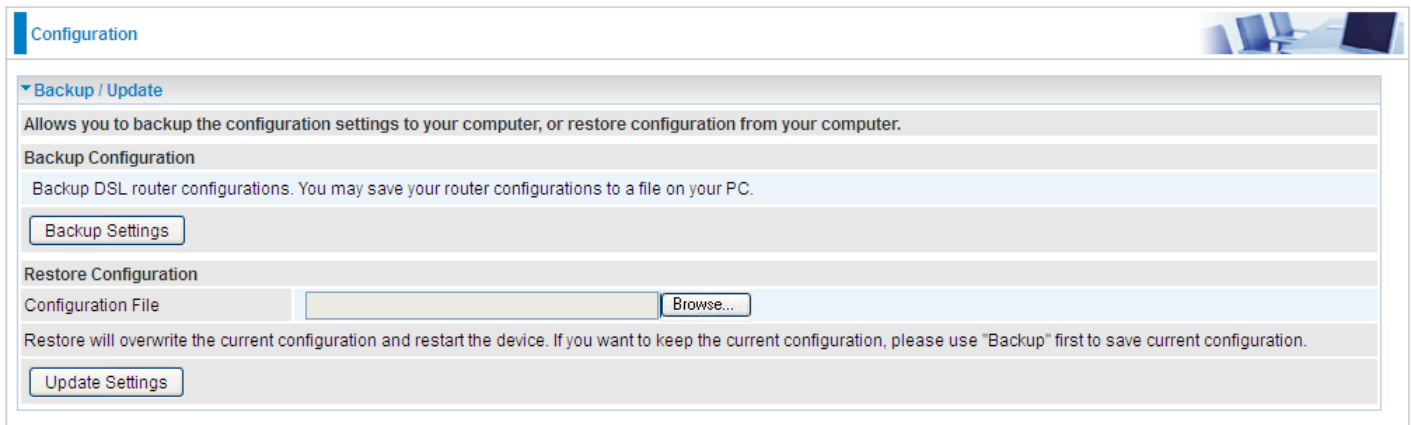


Warning

DO NOT power down the router or interrupt the firmware upgrading while it is still in process. Improper operation could damage the router.

Backup / Update

These functions allow you to save and backup your router's current settings to a file on your PC, or to restore from a previously saved backup. This is useful if you wish to experiment with different settings, knowing that you have a backup handy in the case of any mistakes. It is advisable to backup your router's settings before making any significant changes to your router's configuration.



Configuration

Backup / Update

Allows you to backup the configuration settings to your computer, or restore configuration from your computer.

Backup Configuration

Backup DSL router configurations. You may save your router configurations to a file on your PC.

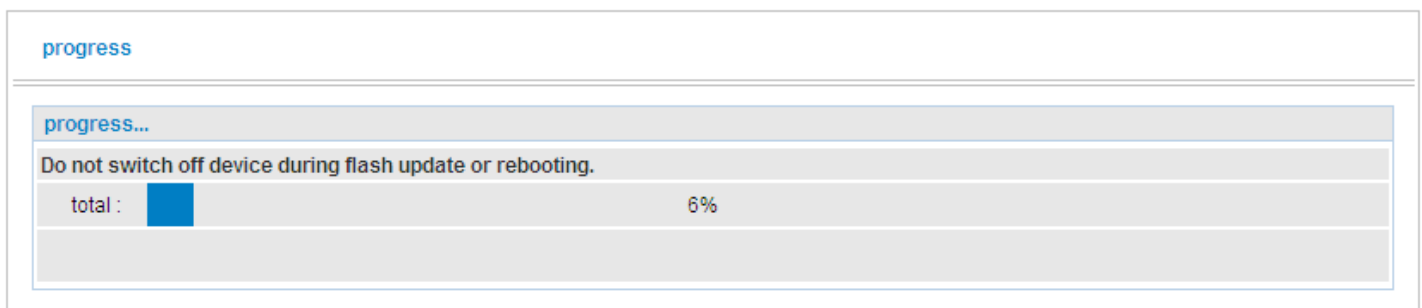
Restore Configuration

Configuration File

Restore will overwrite the current configuration and restart the device. If you want to keep the current configuration, please use "Backup" first to save current configuration.

Click **Backup Settings**, a window appears, click save , then browse the location where you want to save the backup file.

Click **Browse** and browse to the location where your backup file is saved, the click **Open**. Then in the above page, click **Update Settings**, the following process indicating screen will appear. Let it update to 100%, it will automatically turn to the Device Info page.



progress

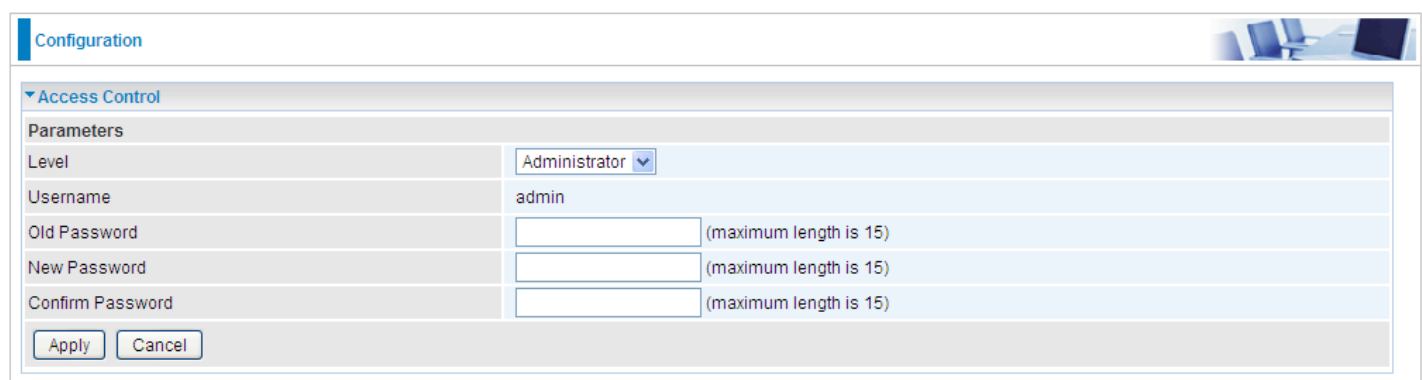
progress...

Do not switch off device during flash update or rebooting.

total : 6%

Access Control

Access Control is used to prevent unauthorized access to the router configuration page. Here you can change the login user password. Three user levels are provided here. Each user level there's a default provided user. You must access the router with the appropriate username and password. Here the corresponding passwords are allowed to change.



Configuration

Access Control

Parameters

Level

Username

Old Password (maximum length is 15)

New Password (maximum length is 15)

Confirm Password (maximum length is 15)

Level: select which level you want to change password to. There are three default levels.

- ① **Administrator:** the root user, corresponding default username and password are admin and admin respectively.

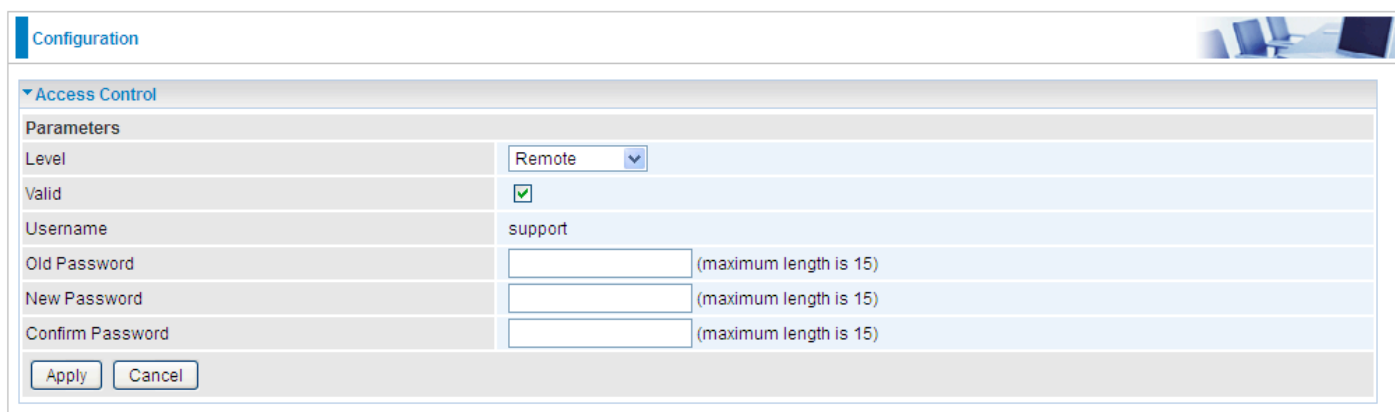
Username: the default username for each user level.

Old Password: Enter the old password.

New Password: Enter the new password.

Confirm Password: Enter again the new password to confirm.

Note: By default the accounts of **Remote** and **Local** are disabled, please click **Valid** check-box to activate the accounts.



Configuration

Access Control

Parameters

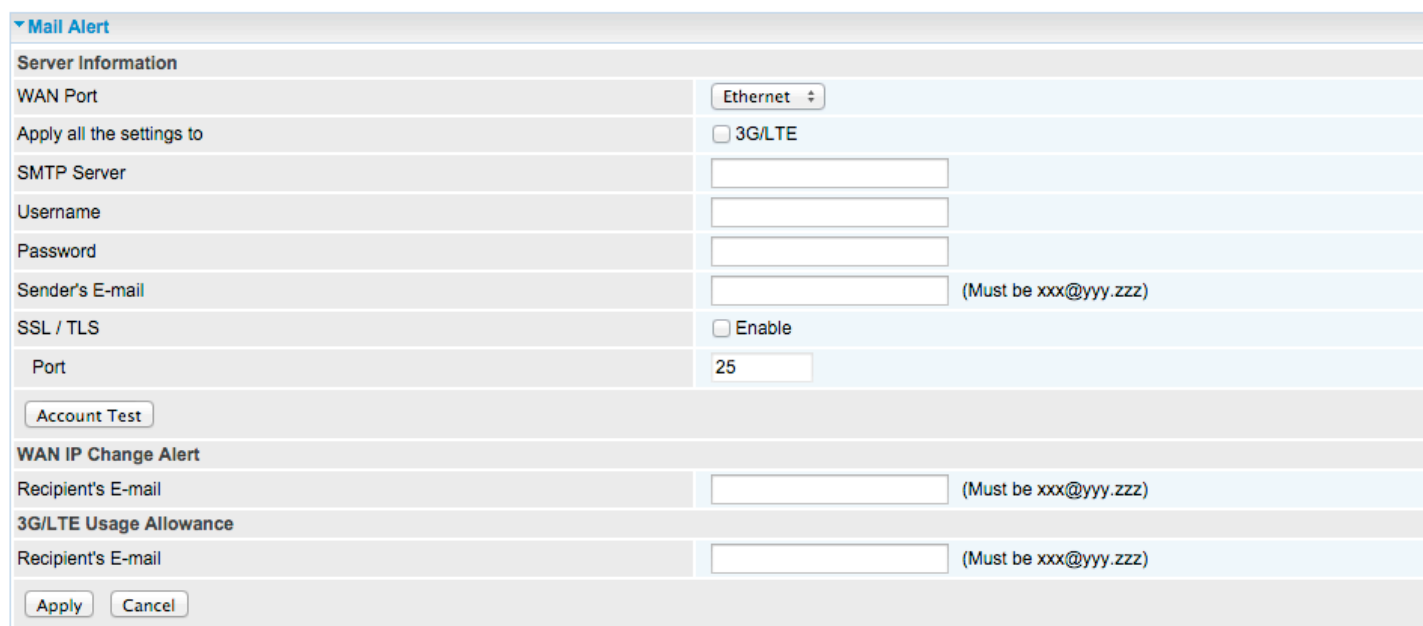
Level	Remote
Valid	<input checked="" type="checkbox"/>
Username	support
Old Password	<input type="text"/> (maximum length is 15)
New Password	<input type="text"/> (maximum length is 15)
Confirm Password	<input type="text"/> (maximum length is 15)

Apply Cancel

Click **Apply** to apply your new settings.

Mail Alert

Mail alert is designed to keep system administrator or other relevant personnel alerted of any unexpected events that might have occurred to the network computers or server for monitoring efficiency. With this alert system, appropriate solutions may be tackled to fix problems that may have arisen so that the server can be properly maintained.



Mail Alert

Server Information

WAN Port	Ethernet
Apply all the settings to	<input type="checkbox"/> 3G/LTE
SMTP Server	<input type="text"/>
Username	<input type="text"/>
Password	<input type="text"/>
Sender's E-mail	<input type="text"/> (Must be xxx@yyy.zzz)
SSL / TLS	<input type="checkbox"/> Enable
Port	25

Account Test

WAN IP Change Alert

Recipient's E-mail	<input type="text"/> (Must be xxx@yyy.zzz)
--------------------	--

3G/LTE Usage Allowance

Recipient's E-mail	<input type="text"/> (Must be xxx@yyy.zzz)
--------------------	--

Apply Cancel

WAN Port: Mail Alert feature can be applicable to every WAN mode: Ethernet and 3G/LTE. Select the port you want to use Mail Alert.

When there is any unexpected event, the alert message will be sent to your specified E-mail.

SMTP Server: Enter the SMTP server that you would like to use for sending emails.

Username: Enter the username of your email account to be used by the SMTP server.

Password: Enter the password of your email account.

Sender's Email: Enter your email address.

SSL: check to whether to enable SSL encryption feature.

Port: the port, default is 25.

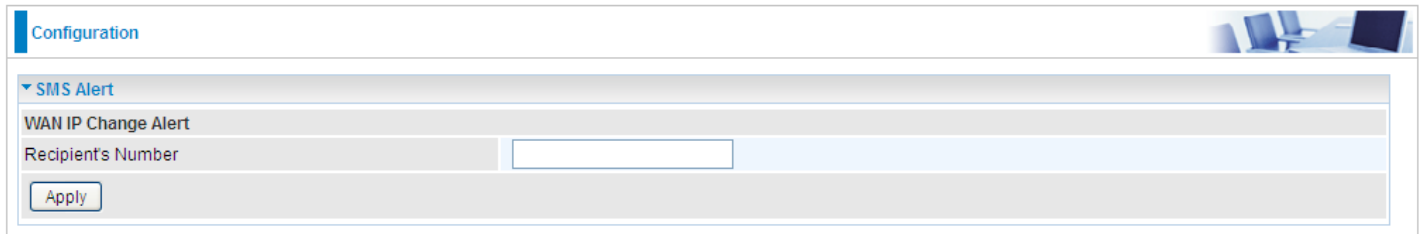
Account Test: Press this button to test the connectivity and feasibility to your sender's e-mail.

Recipient's Email (WAN IP Change Alert): Enter the email address that will receive the alert message once a WAN IP change has been detected.

Recipient's Email (3G/LTE Usage Allowance): Enter the email address that will receive the alert message once the 3G over Usage Allowance occurs.

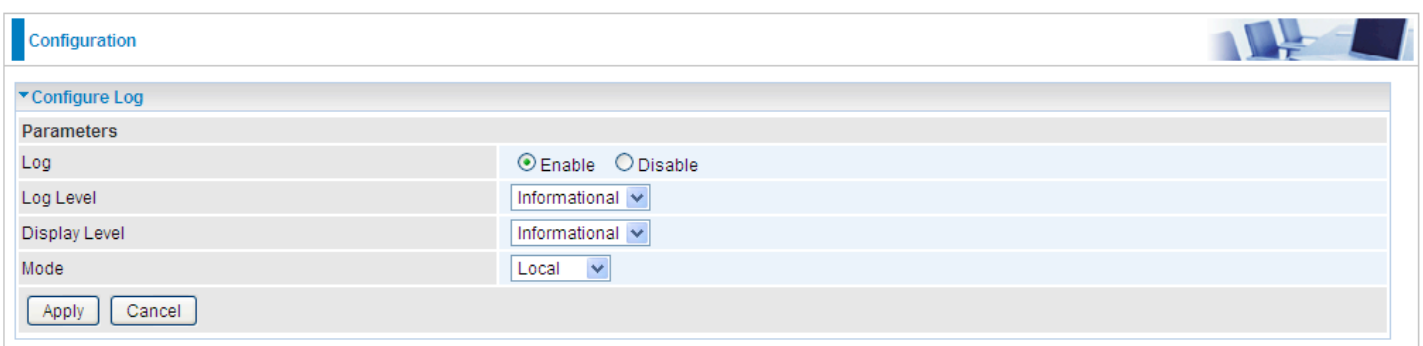
SMS Alert

SMS, Short Message Service, is to inform clients the information clients subscribe. The router offers SMS alert sending clients alert messages when a WAN IP change is detected.



Recipient's Number (WAN IP Change Alert): Enter the Recipient's number that will receive the alert message once a WAN IP change has been detected.

Configure Log



Log: Enable or disable this function.

Log level: Select your log level. The log level allows you to configure which types of events are logged. There are eight log levels from high to low are displayed below:

- ① **Emergency** = system is unusable
- ① **Alert** = action must be taken immediately
- ① **Critical** = critical conditions
- ① **Error** = error conditions
- ① **Warning** = warning conditions
- ① **Notice** = normal but significant conditions
- ① **Informational** = information events
- ① **Debugging** = debug-level messages

The gateway records all log events at the chosen level and above. For instance, if you set the log level to Critical, all critical, alert, and emergency events are logged, but none of the others are recorded

Display Level: Display the log according to the level you set when you view system log. Once you set the display level, the logs of the same or higher priority will be displayed.

Mode: Select the mode the system log adopted. Three modes: local, Remote and Both.

- ① **Local:** Select this mode to store the logs in the router's local memory.
- ① **Remote:** Select this mode to send the log information to a remote log server. Then you must assign the remote log server and port, 514 is often used.
- ① **Both:** Logs stored adopting above two ways.

Click **Apply** to save your settings.

USB

Storage here refers to network sharing in the network environment, USB devices act as the storage carrier for **DLNA**, NAS (**Samba server**, **FTP server**).

Storage Device Info

This part provides users direct access to the storage information like the total volume, the used and the remaining capacity of the device.

Configuration				
▼ Storage Device Info				
Storage Device Info				
Volume Name	FileSystem	Total Space	Used Space	Unmount
usb1_1	fat	990	42	<input type="button" value="Unmount"/>

Volume Name: Display the storage volume name

FileSystem: Display the storage device's file system format, well-known is FAT.

Total Space: Display the total space of the storage, with unit MB.

Used Space: Display the remaining space of each partition, unit MB.

Unmount: Click **Unmount** button if you want to uninstall the USB device. Please **Note** that first click **Unmount** before you uninstall your USB storage.

User Account

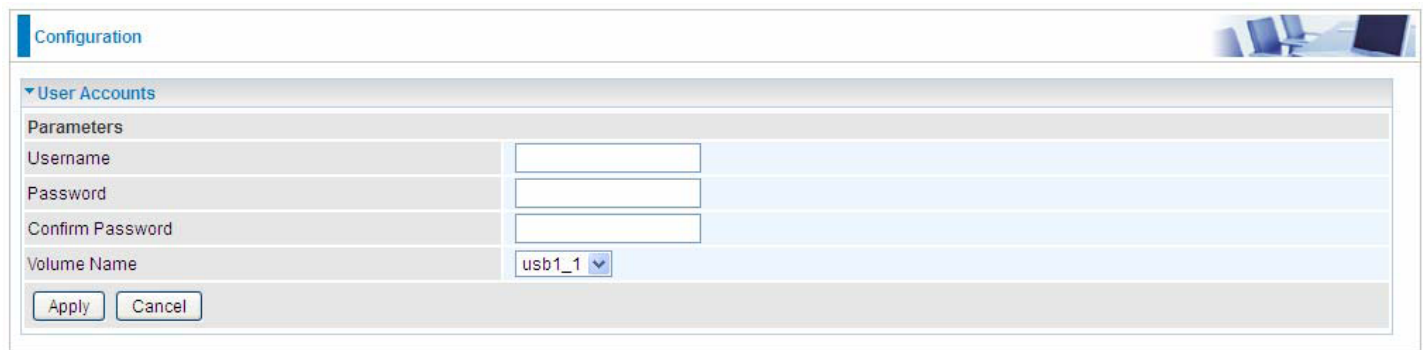
Users here can add user accounts for access to the storage, in this way users can access the network sharing storage with the specified account, and again protect their own data.

Users added here are entitled to have access to both **Samba server** and **FTP server**.

Default user admin.

Configuration			
▼ User Accounts			
User Accounts			
A maximum accounts can be configured: 16			
Username	Home Directory	Remove	Edit
admin	/		
<input type="button" value="Add"/> <input type="button" value="Remove"/>			

Click **Add** button, enter the user account-adding page:



Configuration

▼ User Accounts

Parameters

Username

Password

Confirm Password

Volume Name

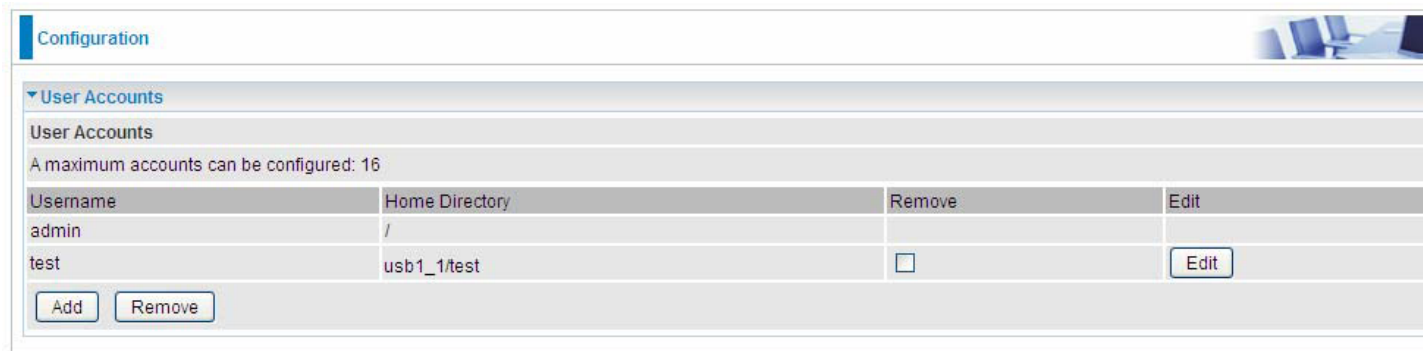
Username: user-defined name, but simpler and more convenient to remember would be favorable.

Password: Set the password.

Confirm Password: Reset the password for confirmation.

Volume Name: Select Volume name, as to create access to the volume of the specified partition of the storage.

For example, a user **test** is setup behind the usb1_1.



Configuration

▼ User Accounts

User Accounts

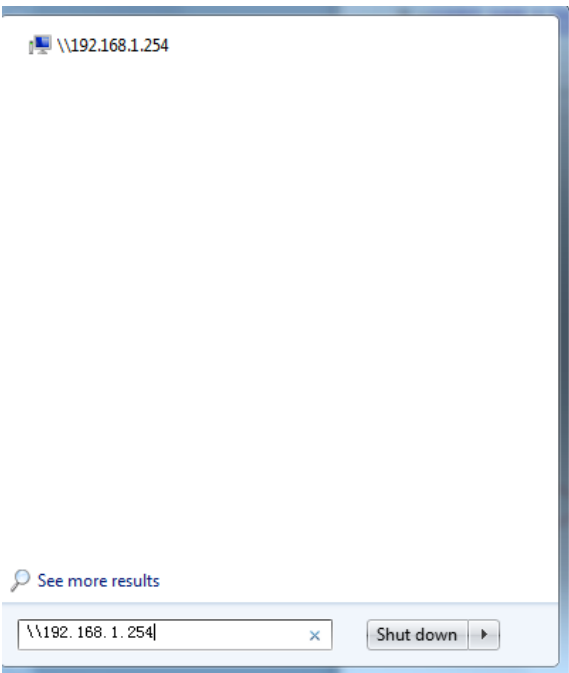
A maximum accounts can be configured: 16

Username	Home Directory	Remove	Edit
admin	/		
test	usb1_1/test	<input type="checkbox"/>	<input type="button" value="Edit"/>

The user “test” has the right to access both **Samba** and **FTP server**.

How to access Samba:

In your computer, Click **Start** > **Run**, enter [\\192.168.1.254](http://192.168.1.254) (LAN IP)



\\192.168.1.254

See more results

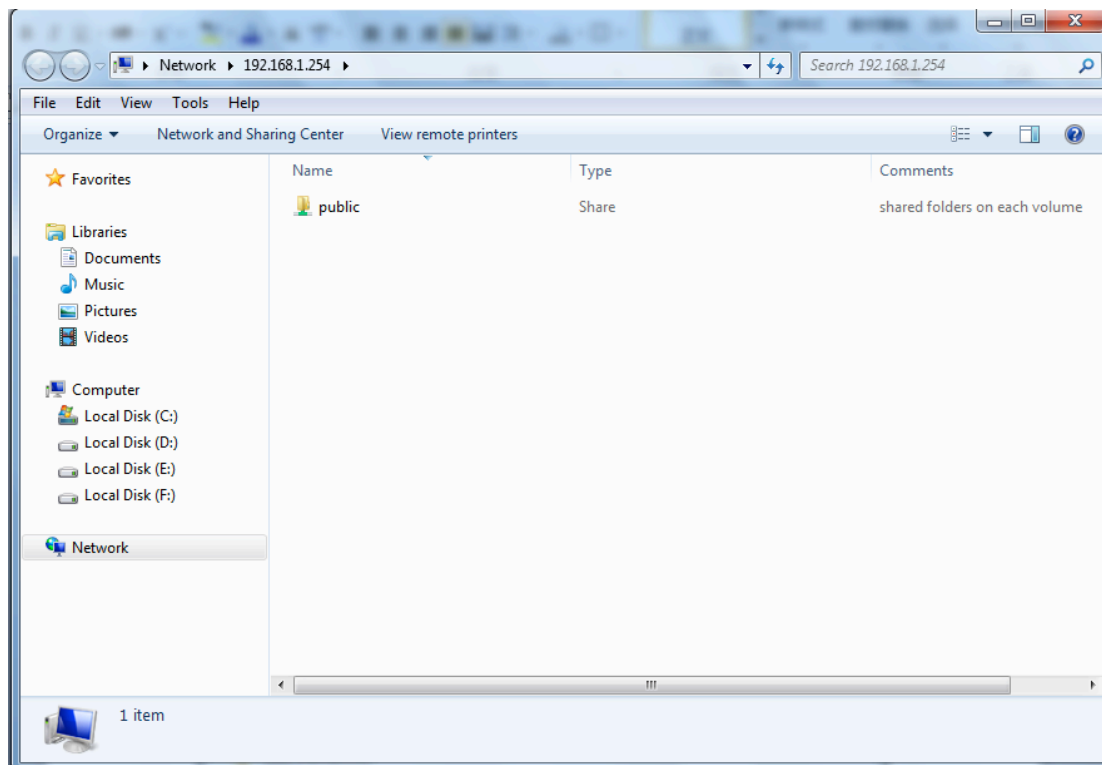
\\192.168.1.254 Shut down

When accessing the network storage, you can see a folder named “**public**”, users should have the account to enter, and the account can be set at the User Accounts section.

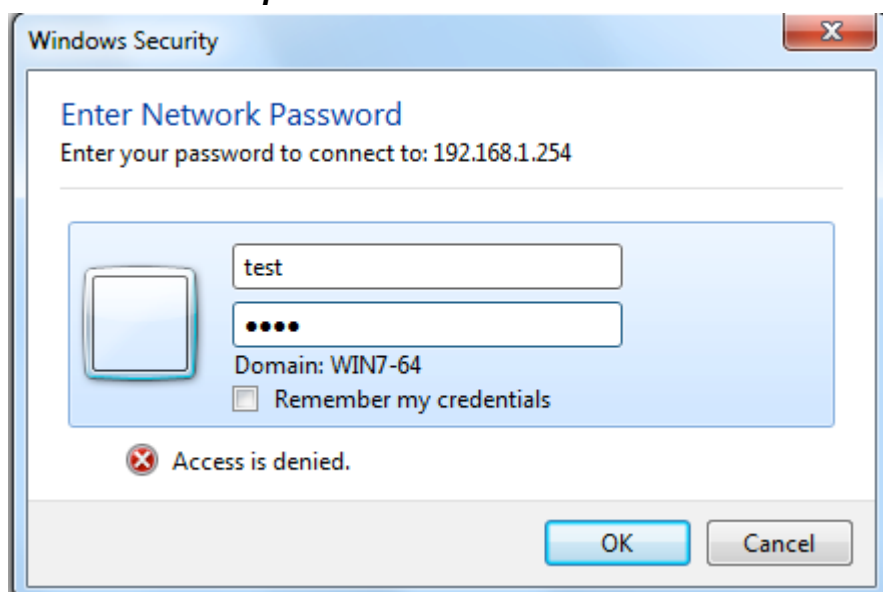
When first logged on to the network folder, you will see the “**public**” folder.

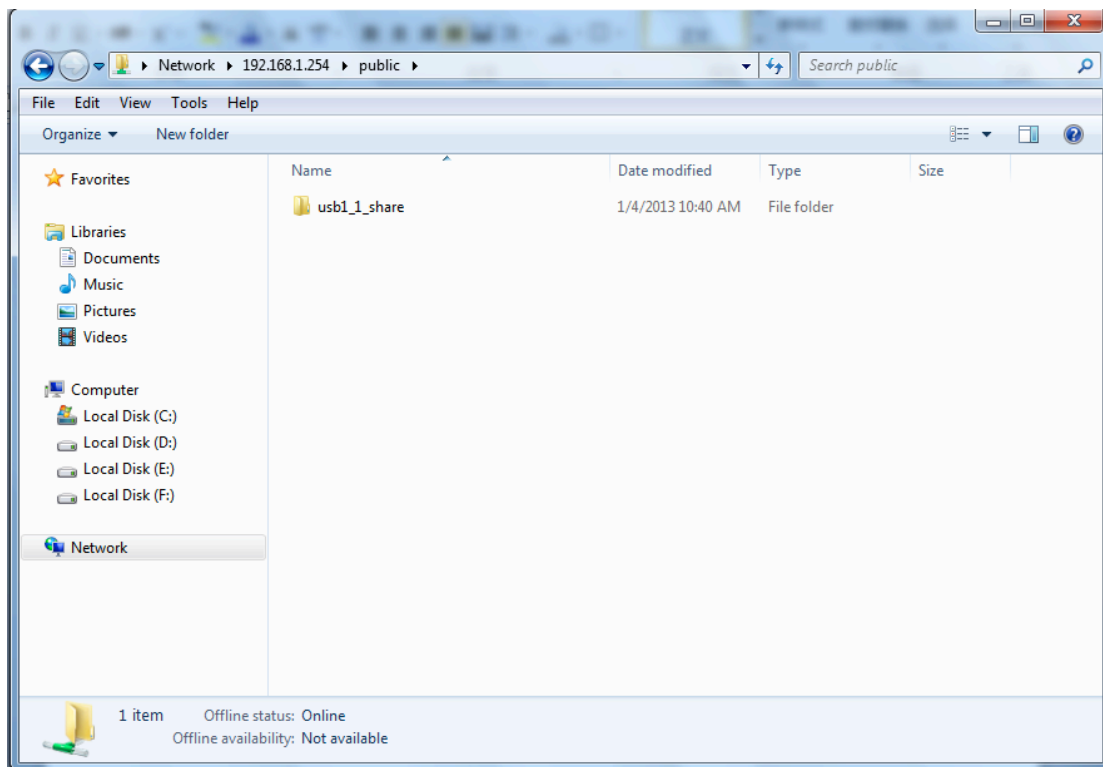
Public: The public sharing space for each user in the USB Storage.

When user register a USB account and log successfully, a private folder (the same name as the user account registered) exclusive for each user is established. Go on to see the details.

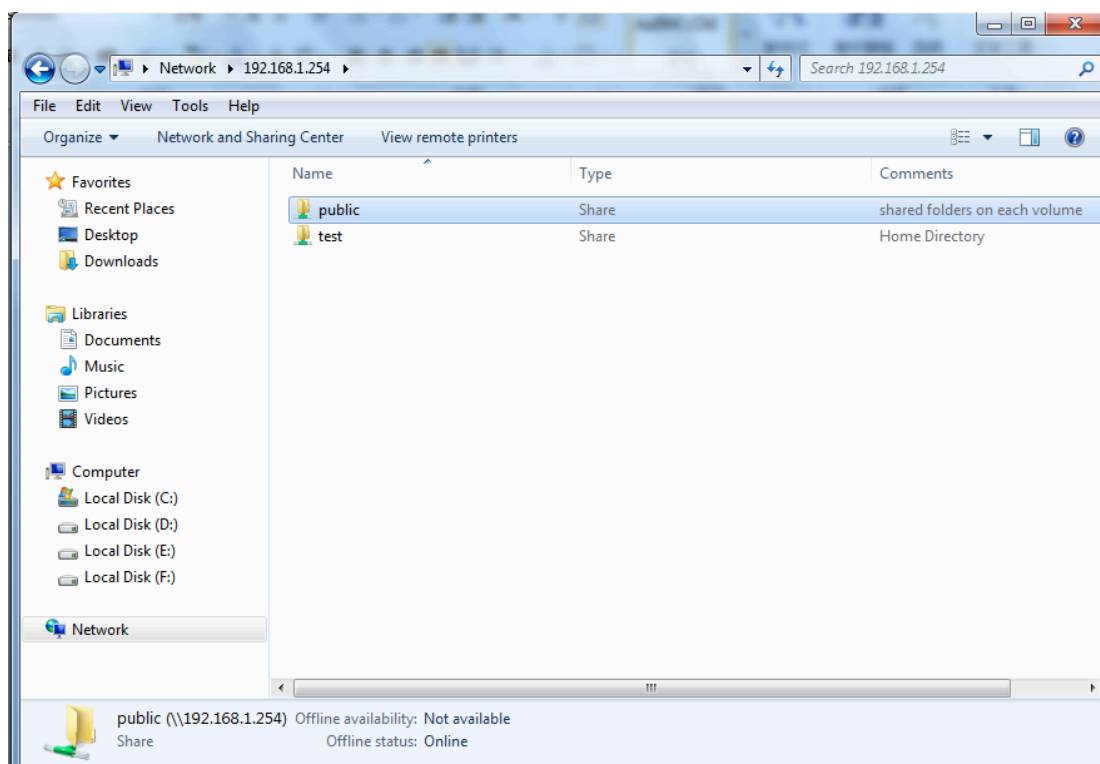


Access the folder **public**.





When successfully accessed, the private folder of each user is established, and user can see from the following picture. The **test** fold in the picture is the private space for each user.



How to use FTP:

Please **note** to enable remote FTP access in [Remote Access](#).

1. Access via FTP tools

Take popular FTP tool of FlashFXP for example:

- 1) Open FlashFXP
- 2) Create ftp sites (LAN IP / WAN IP, and set the account, port).
- 3) Connect to the ftp site.

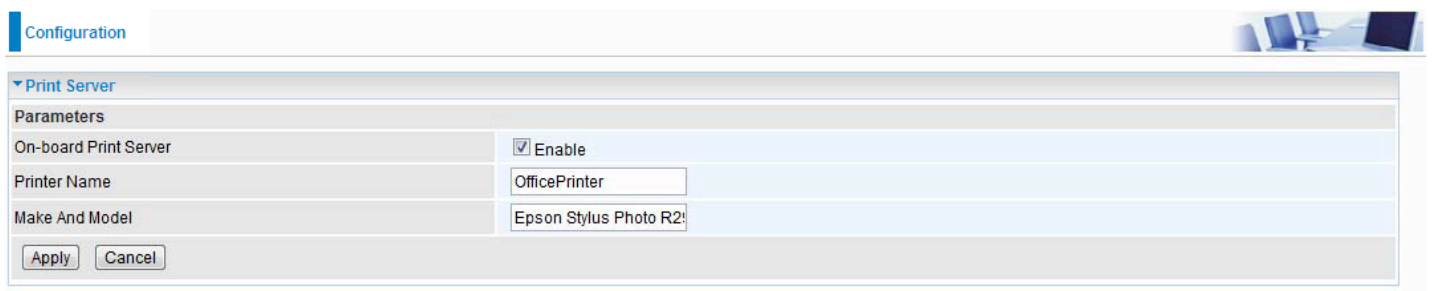
Print Server

The Print Server feature allows you to share a printer on your network by connecting a USB cable from your printer to the USB port on the router. This allows you to print from any location on your network.

Note: Only USB printers are supported

Setup of the printer is a 3 step process

1. Connect the printer to the USB port
2. Enable the print server on the router
3. Install the printer drivers on the PC you want to print from



The screenshot shows the 'Configuration' tab of a router's web interface. Under the 'Print Server' section, there are three main fields: 'On-board Print Server' with a checked checkbox labeled 'Enable', 'Printer Name' with the text 'OfficePrinter', and 'Make And Model' with the text 'Epson Stylus Photo R290'. At the bottom of this section are 'Apply' and 'Cancel' buttons.

On-board Print Server: Check Enable to activate the print server

Printer Name: Enter the Printer name, for example, *OfficePrinter*

Make and Model: Enter in the Make and Model information for the printer, for example, *Epson Stylus Photo R290*

Note:

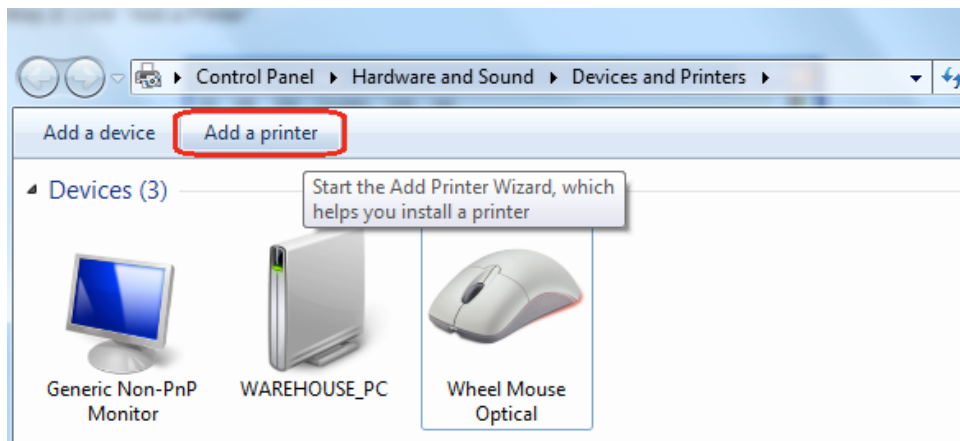
The **Printer name** can be any text string up to **40** characters. It cannot contain spaces.

The **Make and Model** can be any text string up to **128** characters.

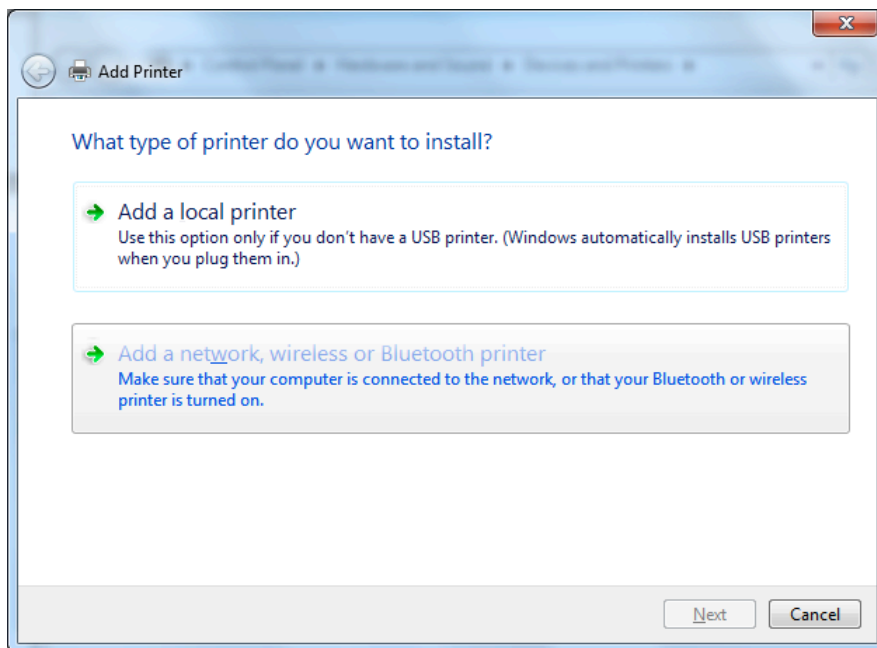
Set up of Printer client (Windows 7)

Step 1: Click **Start** and select "Devices and Printers"

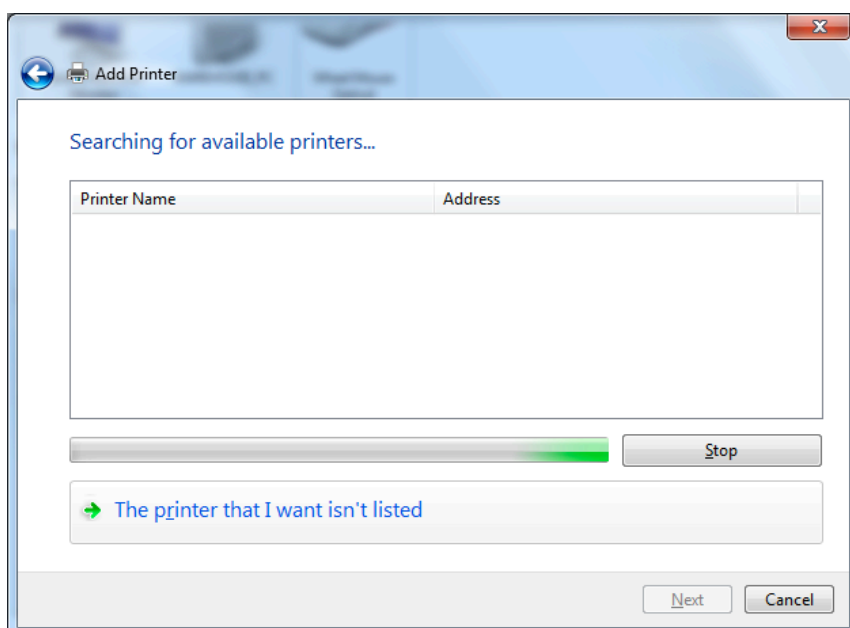
Step 2: Click "Add a Printer".



Step 3: Click “Add a network, wireless or Bluetooth printer



Step 4: Click “The printer that I want isn’t listed”

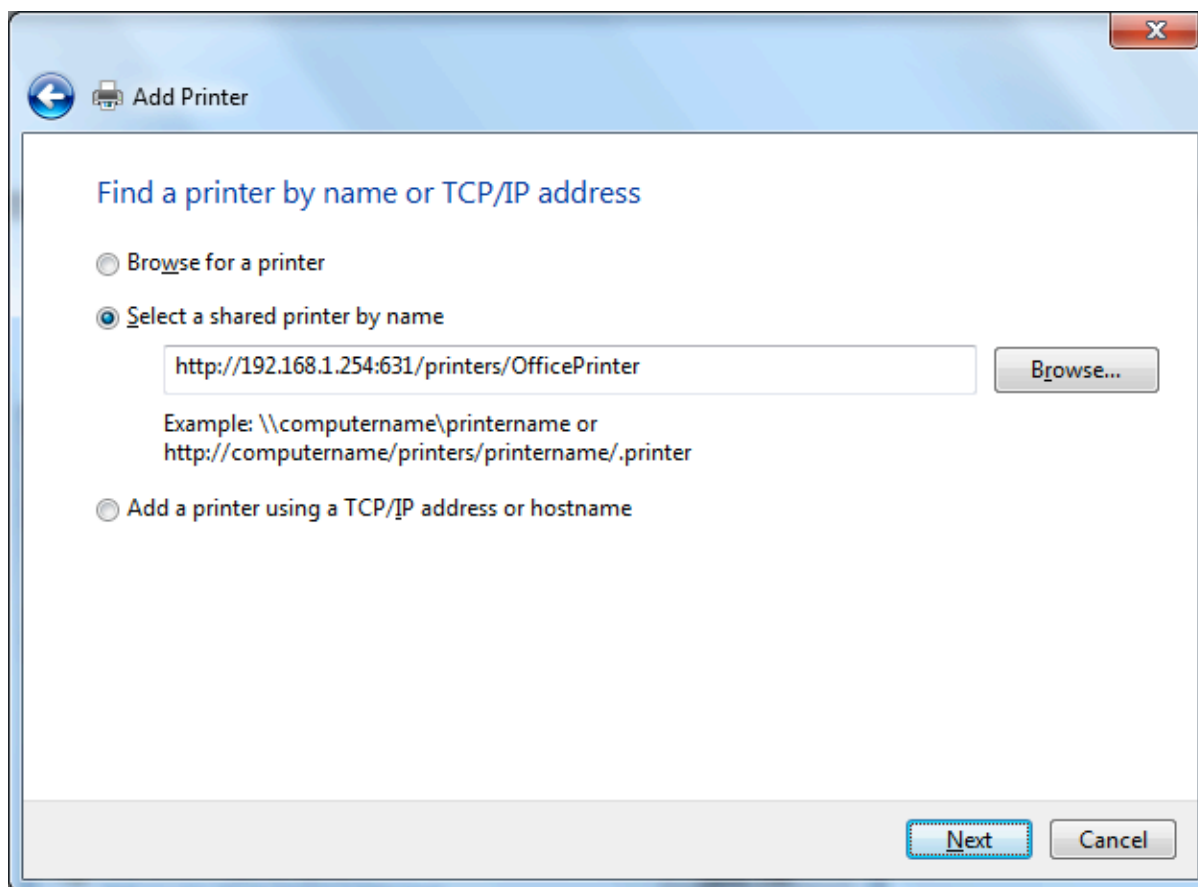


Step 5: Select “Select a shared printer by name”

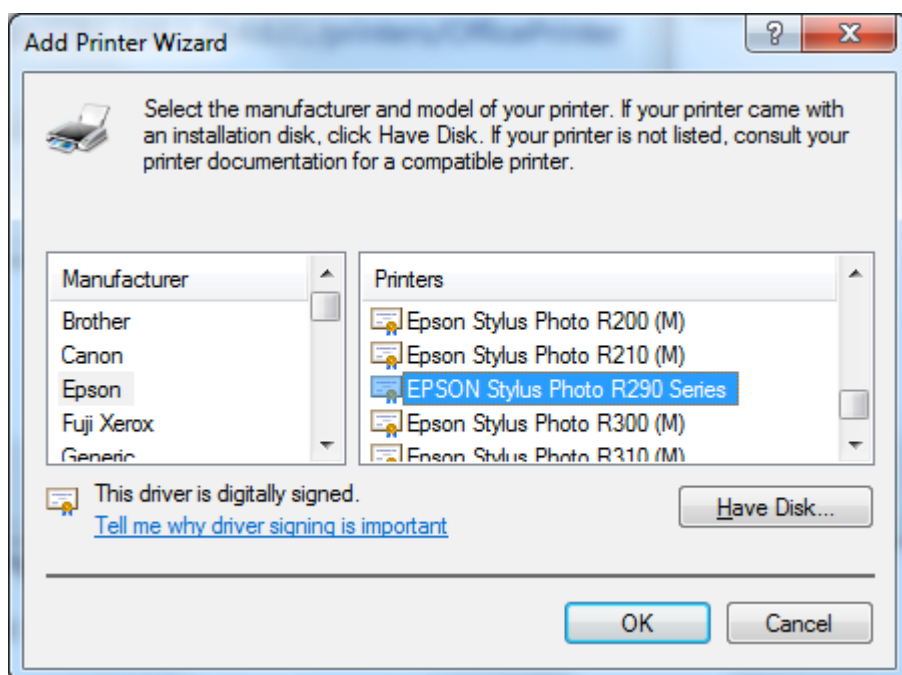
Enter `http:// LAN-IP:631/printers/printer-name` or. Make sure printer’s name is the same as what you set in the router earlier

For Example: `http://192.168.1.254:631/printers/OfficePrinter`

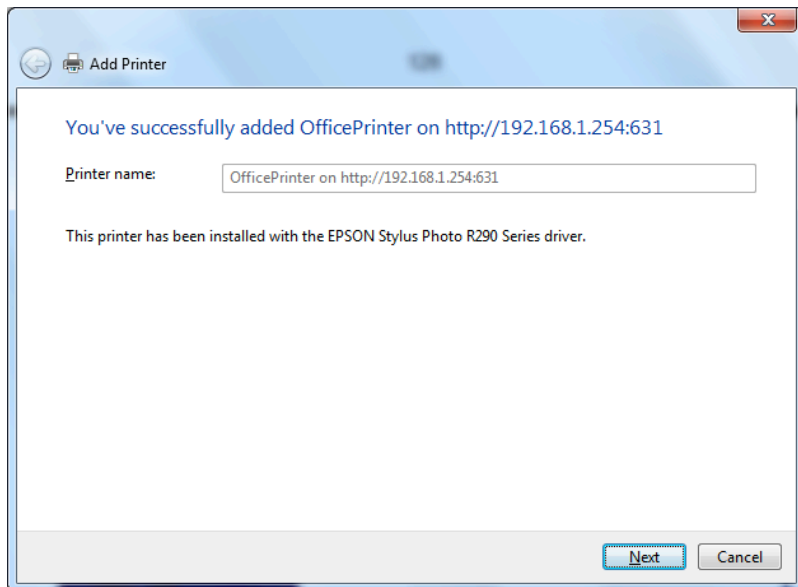
OfficePrinter is the Printer Name we setup earlier



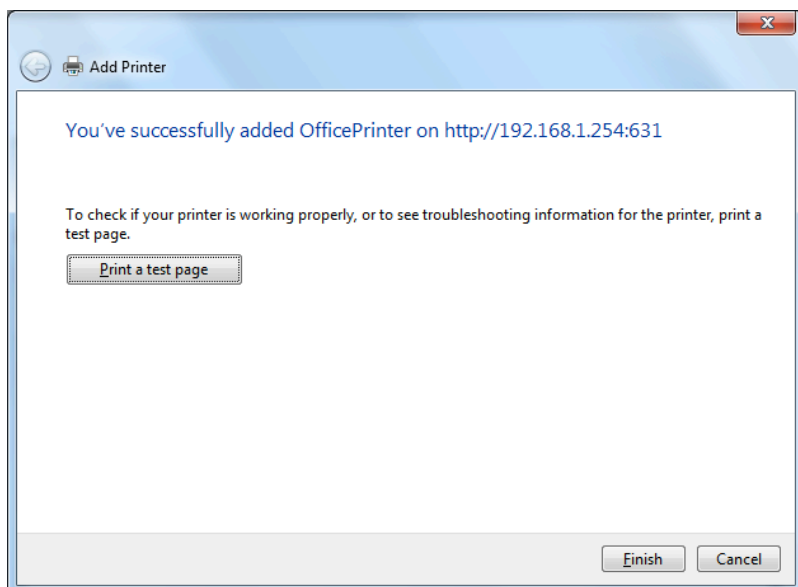
Step 6: Click “Next” to add the printer driver. If your printer is not listed and your printer came with an installation disk, click “Have Disk” find it and install the driver.



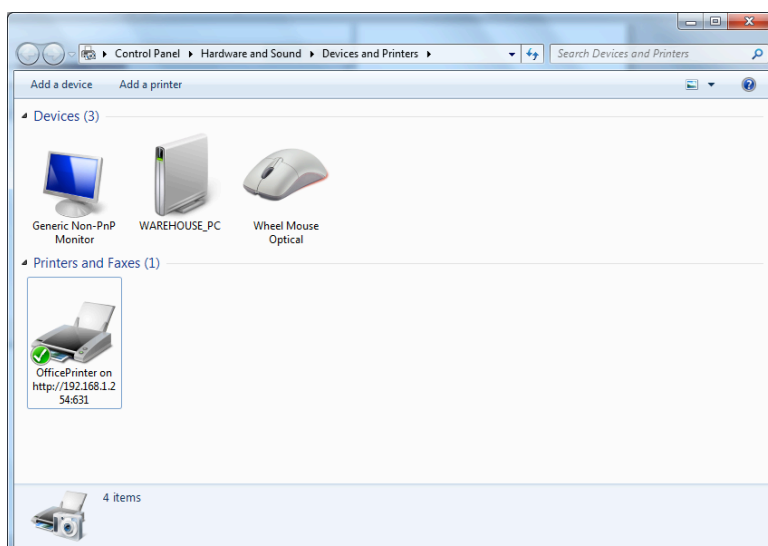
Step 7: Click "Next"



Step 8: Click "Next" and you are done



You will now be able to see your printer on the Devices and Printers Page



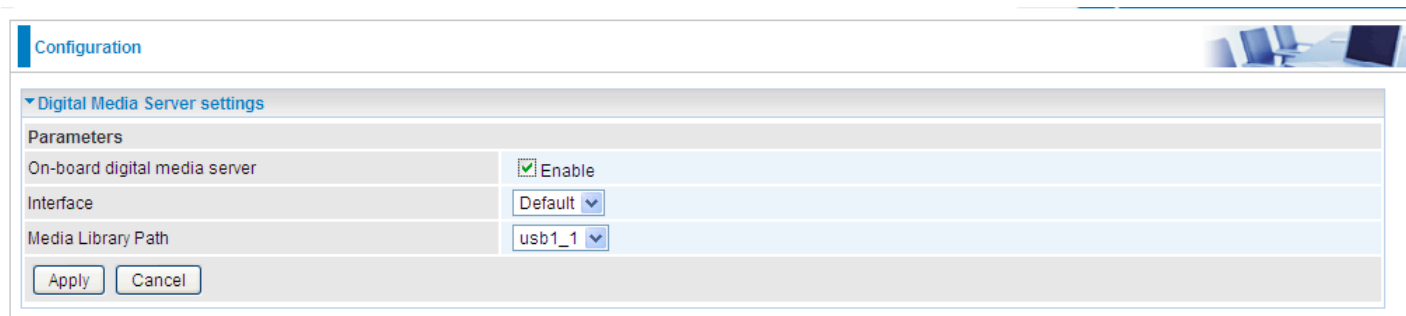
DLNA

The Digital Living Network Alliance (DLNA) is a non-profit collaborative trade organization established by Sony in June 2003, which is responsible for defining interoperability guidelines to enable sharing of digital media between consumer devices such as computers, printers, cameras, cell phones and other multiple devices.

DLNA uses Universal Plug and Play (UPnP) for media management, discovery and control. UPnP defines the types of devices ('server', 'renderer', 'controller') that DLNA supports and the mechanism for accessing media over a network.

Overall, DLNA allows more convenience, more choices and enjoyment of your digital content through DLNA certified devices. Any DLNA certified devices or software can access the DLNA server.

With USB storage, the device can serve as a DLNA server.



The screenshot shows a 'Configuration' window with a 'Digital Media Server settings' section. Under 'Parameters', there are three settings: 'On-board digital media server' is checked and labeled 'Enable'; 'Interface' is set to 'Default'; and 'Media Library Path' is set to 'usb1_1'. At the bottom of the settings section are 'Apply' and 'Cancel' buttons.

On-board digital media server: Enable to share the device as a DLNA server.

Interface: The VLAN group, it is the bound interface for DLNA server accessing.

Media Library Path: Default is usb1_1, total USB space (pictures, videos, music, etc, all can be accessed with this path).

Take Windows media player in Windows 7 accessing the DLNA server for example for usage of DLNA .

IP Tunnel

An IP Tunnel is an Internet Protocol (IP) network communication channels between two networks of different protocols. It is used to transport another network protocol by encapsulation of its packets.

IP Tunnels are often used to connect two disjoint IP networks that do not have a native routing path to each other, via an underlying routable protocol across an intermediate transport network, like VPN.

Another prominent use of IP Tunnel is to connect islands of IPv6 installations across the IPv4 internet.

IPv6inIPv4

6in4 is an Internet transition mechanism for migrating from IPv4 to IPv6. 6in4 uses tunneling to encapsulate IPv6 traffic over explicitly configured IPv4 links. 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 capsulation.

6RD:

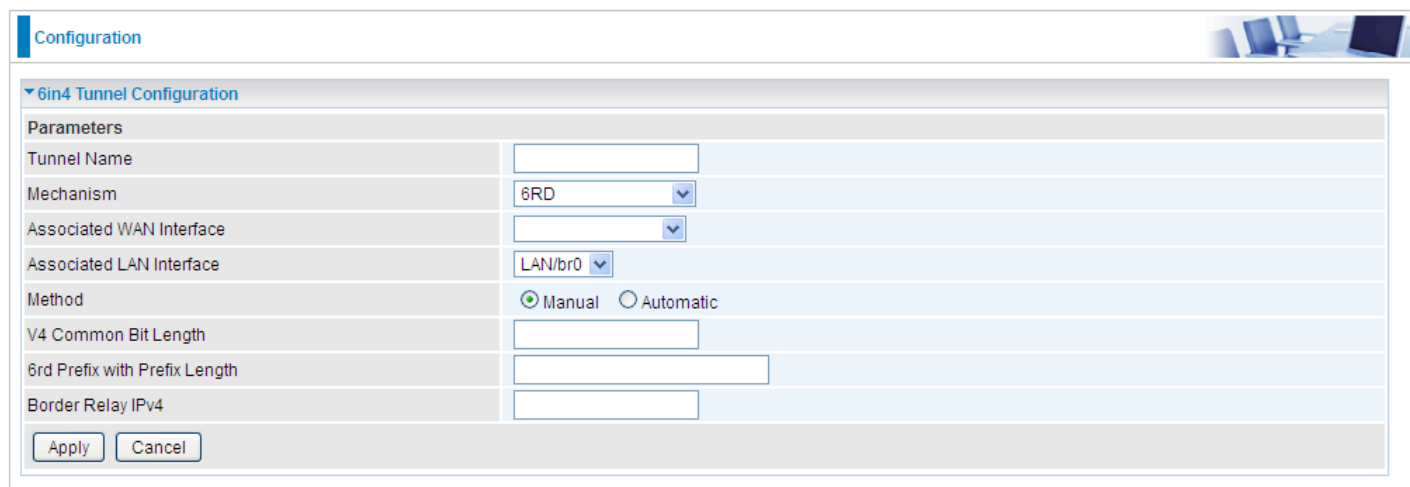
6RD is a mechanism to facilitate IPv6 rapid deployment across IPv4 infrastructures of internet service providers (ISPs).

It is derived from 6to4, a preexisting mechanism to transporting IPv6 packets over IPv4 infrastructure network, with the significant change that it operates entirely within the enduser's ISP network, thus avoiding the major architectural problems inherent in the original design of 6to4.



The screenshot shows the 'Configuration' page for 'IPv6inIPv4'. It features a table titled '6in4 Tunnel Configuration' with columns: Name, WAN, LAN, Dynamic, V4 Common Bit Length, 6rd Prefix with Prefix Length, Border Relay Address, and Remove. Below the table are 'Add' and 'Remove' buttons.

Click **Add** button to manually add the 6in4 rules.



The screenshot shows the '6in4 Tunnel Configuration' dialog box. It contains the following fields and options:

- Tunnel Name: Text input field.
- Mechanism: Dropdown menu with '6RD' selected.
- Associated WAN Interface: Dropdown menu.
- Associated LAN Interface: Dropdown menu with 'LAN/br0' selected.
- Method: Radio buttons for 'Manual' (selected) and 'Automatic'.
- V4 Common Bit Length: Text input field.
- 6rd Prefix with Prefix Length: Text input field.
- Border Relay IPv4: Text input field.
- Buttons: 'Apply' and 'Cancel'.

Tunnel Name: User-defined name.

Mechanism: Here only 6RD.

Associated WAN Interface: The applied WAN interface with the set tunnel, thus when there are packets from/to the WAN interface, the tunnel would be used to transport the packets.

Associated LAN Interface: Set the linked LAN interface with the tunnel.

Method: 6rd operation mechanism: manually configured or automatically configured. If manually, please fill out the following 6rd parameters.

V4 Common Bit Length: Specify the length of IPv4 address carried in IPv6 prefix, for example, 0 means to carry all the 32 bits of IPv4 address while 8 carries 24 bits of the IPv4 address.

6rd Prefix with Prefix Length: Enter the 6rd prefix and prefix length you uniquely designate to 6rd by the ISP(The 6rd prefix and prefix length are to replace the standard 6to4 prefix 2002::/16 by an IPv6 prefix that belongs to the ISP-assigned.)

Border Relay IPv4 Address: The IPv4 address of the border relay. The relay is used to unwrap encapsulated IPv4 packets into IPv6 packets and send them to the IPv6 network.

IPv4inIPv6

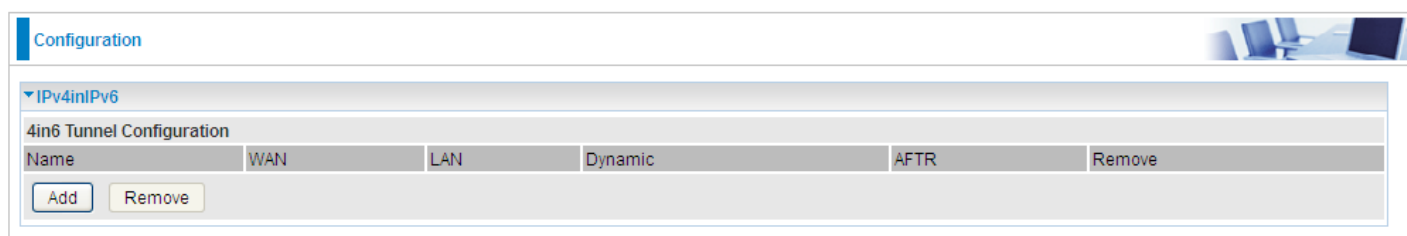
4in6 refers to tunneling of IPv4 in IPv6. It is an inherent internet interoperation mechanism allowing IPv4 to be used in an IPv6 only network.

4in6 uses tunneling to encapsulate IPv4 traffic over configured IPv6 tunnels. 4in6 tunnels are usually manually configured but they can be automated using protocols such as TSP to allow easy connection to a tunnel broker.

DS – Lite

DS –Lite, or Dual-Stack Lite, is designed to let an ISP omit the deployment of any IPv4 address to the customer's CPE. Instead, only global IPv6 addresses are provided (Regular Dual-Stack Lite deploys global addresses for both IPv4 and IPv6).

The CPE distributes private IPv4 addresses for the LAN clients, the same as a NAT device. The subnet information is chosen by the customer, identically to the NAT model. However, instead of performing the NAT itself, the CPE encapsulates the IPv4 packet inside an IPv6 packet.



Configuration

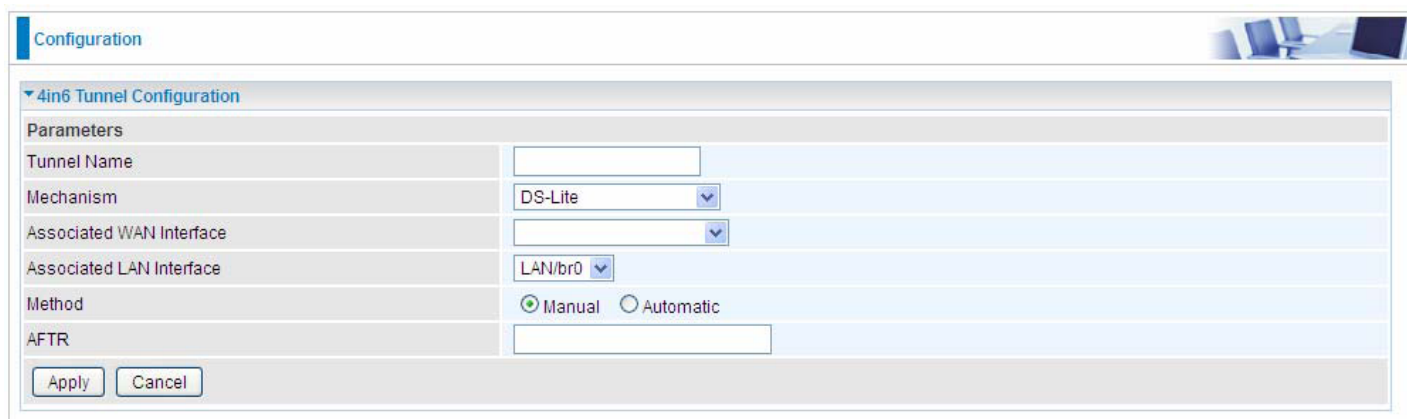
IPv4inIPv6

4in6 Tunnel Configuration

Name	WAN	LAN	Dynamic	AFTR	Remove

Add Remove

Click **Add** button to manually add the 4in6 rules.



Configuration

4in6 Tunnel Configuration

Parameters

Tunnel Name

Mechanism

Associated WAN Interface

Associated LAN Interface

Method

AFTR

Apply Cancel

Tunnel Name: User-defined tunnel name.

Mechanism: It is the 4in6 tunnel operation technology. Please select DS-Lite.

Associated WAN Interface: The applied WAN interface with the set tunnel, and when there are packets from/to the WAN interface, the tunnel would be used to transport the packets.

Associated LAN Interface: Specify the linked LAN interface with the tunnel.

Method: Manually to specify the AFTP (Address Family Transition Router) address or Automatic.

AFTR: Specify the address of AFTP (Address Family Transition Router) from your ISP.

Security

IP Filtering Outgoing

IP filtering enables you to configure your router to block specified internal/external users (**IP address**) from Internet access, or you can disable specific service requests (**Port number**) to /from Internet. The relationship among all filters is “**or**” operation, which means that the router checks these different filter rules one by one, starting from the first rule. As long as one of the rules is satisfied, the specified action will be taken.

Outbound IP Filtering by default is set to **forward** all outgoing traffic from LAN to go through the router, but user can set rules to **block** the specific outgoing traffic.

Note: The maximum number of entries: 32.

Configuration

IP Filtering

Outgoing IP Filtering Setup

A maximum entries can be configured: 32

Order	Filter Name	IP Version	Protocol	Source IP address	Source Port	Action	Log	Disable	Remove	Edit
				Destination IP address	Destination Port					

Add

Remove

Reorder

Click **Add** button to enter the exact rule setting page.

Configuration

Outgoing IP Filtering Setup

Parameters

Filter Name

<< --type or select from listbox--

IP Version

IPv4

Protocol

TCP/UDP

Protocol Number

[0 - 254]

Source IP address

~

Source Port

[port or port:port]

Destination IP address

~

Destination Port

[port or port:port]

Time Schedule

Always On

Sun

Mon

Tue

Wed

Thu

Fri

Sat

From

00

:

00

To

00

:

00

Action

forward

Log

Apply

Filter Name: A user-defined rule name. User can select simply from the list box for the application for quick setup.

IP Version: Select the IP Version, IPv4 or IPv6.


Protocol: Set the traffic type (TCP/UDP, TCP, UDP, ICMP) that the rule applies to.

Source IP address: This is the Address-Filter used to allow or block traffic to/from particular IP address(es) featured in the IP range. If you leave empty, it means any IP address.

Source Port [port or port:port]: The port or port range defines traffic from the port (specific application) or port in the set port range blocked to go through the router. Default is set port from range 1 – 65535.

Destination IP address: Traffic from LAN with the particular traffic destination address specified in the IP range is to be blocked from going through the router, similarly set as the Source IP address above.

Destination Port [port or port: port]: Traffic with the particular set destination port or port in the set port range is to be blocked from going through the router. Default is set port from port range: 1 – 65535.

Time Schedule: Select or set exactly when the rule works. When set to “Always On”, the rule will work all time; and also you can set the precise time when the rule works, like 01:00 - 19:00 from Monday to Friday. Or you can select the already set timeslot in “**Time Schedule**” during which the rule works. And when set to “Disable”, the rule is disabled or inactive and there will be an icon”  ” in list table indicating the rule is inactive. See [Time Schedule](#).

Action: Select to **drop** or **forward** the packets fit the outgoing filtering rule.

Log: check the check-box to record the security log. To check the log, users can turn to [Security Log](#).

Example: For example, if there is an outgoing rule set as follows, then the 21 application between source IP and destination IP will be forwarded. Or exactly in the rule below, all traffic trying to access FTP will be forwarded.

Configuration

▼ Outgoing IP Filtering Setup

Parameters

Filter Name

FTP

<< --type or select from listbox--

IP Version

IPv4

Protocol

TCP/UDP

Protocol Number

[0 - 254]

Source IP address

~

Source Port

[port or port:port]

Destination IP address

~

Destination Port

21

[port or port:port]

Time Schedule

Always On

☐ Sun ☐ Mon ☐ Tue ☐ Wed ☐ Thu ☐ Fri ☐ Sat

From

00

:

00

To

00

:

00

Action

forward

Log

☒

Apply

Configuration

▼ IP Filtering

Outgoing IP Filtering Setup

A maximum entries can be configured: 32

Filter Name	IP Version	Protocol	Source IP address	Source Port	Action	Log	Disable	Remove	Edit
			Destination IP address	Destination Port					
FTP	4	TCP	Any	Any	forward	Enable	<input type="checkbox"/>	<input type="button" value="Remove"/>	<input type="button" value="Edit"/>
			Any	21					

Add

Remove

(The rule is active; disable field shows the status of the rule, active or inactive)

Configuration

Outgoing IP Filtering Setup

Parameters

Filter Name: FTP << --type or select from listbox-- >>

IP Version: IPv4

Protocol: TCP Protocol Number: [0 - 254]

Source IP address: ~ Destination IP address: ~

Source Port: [port or port:port] Destination Port: 21 [port or port:port]

Time Schedule: **Disable** Sun Mon Tue Wed Thu Fri Sat From 00:00 To 00:00

Action: forward Log: ☒

Apply

Configuration

IP Filtering

Outgoing IP Filtering Setup

A maximum entries can be configured: 32

Filter Name	IP Version	Protocol	Source IP address Destination IP address	Source Port Destination Port	Action	Log	Disable	Remove	Edit
FTP	4	TCP	Any Any	Any 21	forward	Enable	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Edit

Add Remove

(Rule inactive)

IP Filtering Incoming

Incoming IP Filtering is set by default to **block** all incoming traffic, but user can set rules to **forward** the specific incoming traffic.

Note:

1. The maximum number of entries: 32.
2. When LAN side firewall or firewall in WAN interface(s) is enabled, user can move here to add allowing rules to pass through the firewall.

Configuration

IP Filtering

Incoming IP Filtering Setup

A maximum entries can be configured: 32

Filter Name	Interfaces	IP Version	Protocol	Source IP address Destination IP address	Source Port Destination Port	Log	Disable	Remove	Edit
-------------	------------	------------	----------	---	---------------------------------	-----	---------	--------	------

Add Remove

Click **Add** button to enter the exact rule setting page.

Filter Name: A user-defined rule name. User can select simply from the list box for the application for quick setup.

IP Version: Select the IP Version, IPv4 or IPv6.

Protocol: Set the traffic type (TCP/UDP, TCP, UDP, ICMP) that the rule applies to.

Source IP address: This is the Address-Filter used to allow or block traffic to/from particular IP address(es) featured in the IP range.. If you leave empty, it means any IP address.

Source Port [port or port:port]: The port or port range defines traffic from the port (specific application) or port in the set port range blocked to go through the router. Default is set port from range 1 – 65535.

Destination IP address: Traffic from LAN with the particular traffic destination address specified in the IP range is to be blocked from going through the router, similarly set as the Source IP address above.

Destination Port [port or port : port]: Traffic with the particular set destination port or port in the set port range is to be blocked from going through the router. Default is set port from port range: 1 – 65535

Interfaces: Check if the filter rule applies to all interfaces. User can base on need select interfaces to make the rule take effect with those interfaces.

Time Schedule: Select or set exactly when the rule works. When set to “Always On”, the rule will work all time; and also you can set the precise time when the rule works, like 01:00-19:00 from Monday to Friday. Or you can select the already set timeslot in “**Time Schedule**” during which the rule works. And when set to “Disable”, the rule is disabled or inactive and there will be an icon”

✓” in the list table indicating the rule is inactive. See [Time Schedule](#).

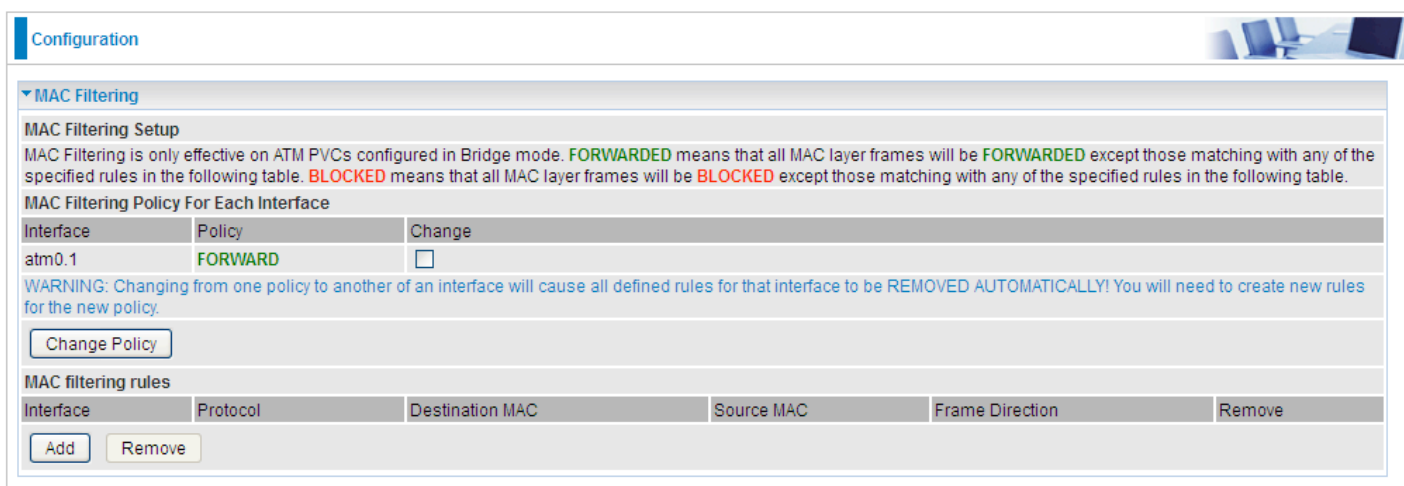
Log: check the check-box to record the security log. To check the log, users can turn to [Security Log](#).

MAC Filtering

MAC Filtering is only effective on ATM PVCs configured in Bridged mode.

FORWARDED means that all MAC layer frames will be **forwarded** except those matching with any of the specified rules in the following table.

BLOCKED means that all MAC layer frames will be **blocked** except those matching with any of the specified rules in the following table.



Configuration

MAC Filtering

MAC Filtering Setup

MAC Filtering is only effective on ATM PVCs configured in Bridge mode. **FORWARDED** means that all MAC layer frames will be **FORWARDED** except those matching with any of the specified rules in the following table. **BLOCKED** means that all MAC layer frames will be **BLOCKED** except those matching with any of the specified rules in the following table.

MAC Filtering Policy For Each Interface

Interface	Policy	Change
atm0.1	FORWARD	<input type="checkbox"/>

WARNING: Changing from one policy to another of an interface will cause all defined rules for that interface to be REMOVED AUTOMATICALLY! You will need to create new rules for the new policy.

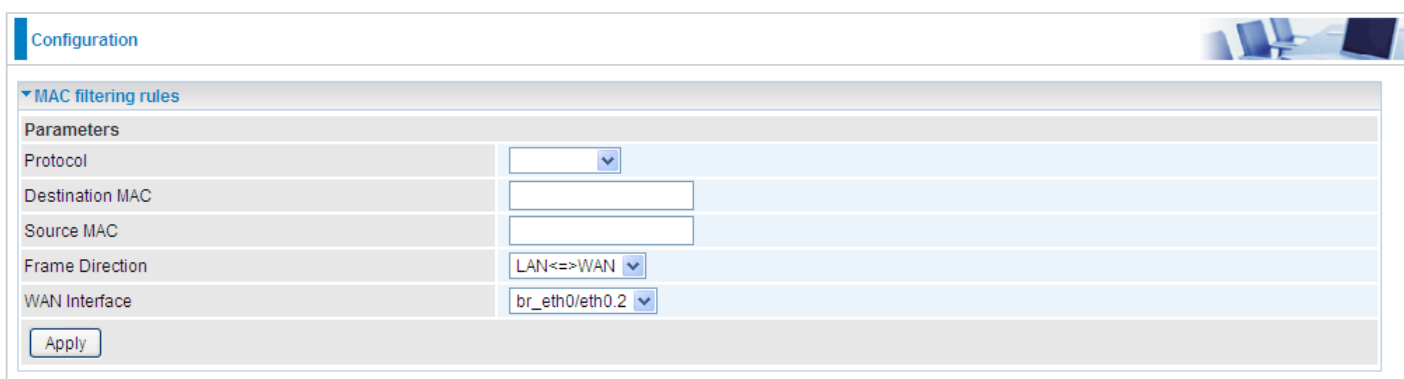
MAC filtering rules

Interface	Protocol	Destination MAC	Source MAC	Frame Direction	Remove
-----------	----------	-----------------	------------	-----------------	--------

By default, all MAC frames of the interface in Bridge Mode will be **forwarded**, you can check **Change** checkbox and then press **Change Policy** to change the settings to the interface.

For example, from above, the interface atm0.1 is of bridge mode, and all the MAC layer frames will be **forward**, but you can set some rules to let some item matched the rules to be **blocked**.

Click **Add** button to add the rules.



Configuration

MAC filtering rules

Parameters

Protocol:

Destination MAC:

Source MAC:

Frame Direction: LAN<=>WAN

WAN Interface: br_eth0/eth0.2

Protocol type: Select from the drop-down menu the protocol that applies to this rule.

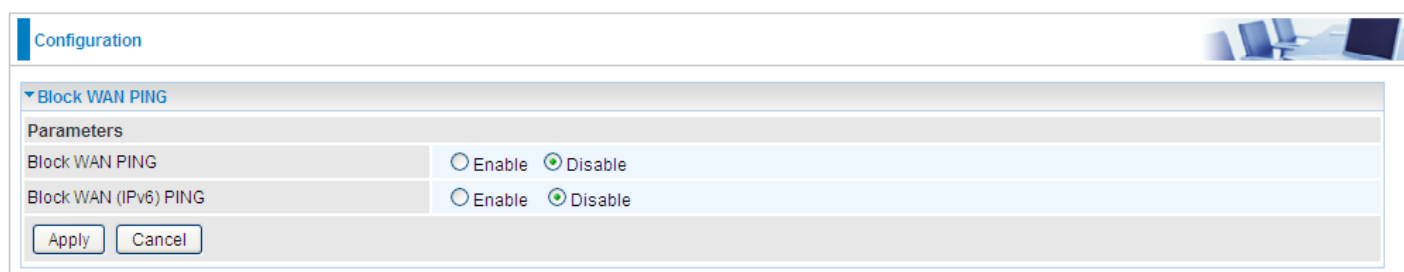
Destination /Source MAC Address: Enter the destination/source address.

Frame Direction: Select the frame direction this rule applies, both LAN and WAN: LAN <=>WAN, only LAN to WAN: LAN=>WAN, only WAN to LAN: WAN=>LAN.

WAN Interfaces: Select the interfaces configured in Bridge mode.

Blocking WAN PING

This feature is enabled to let your router not respond to any ping command when someone others "Ping" your WAN IP.



Configuration

Block WAN PING

Parameters

Block WAN PING: ☐ Enable ☒ Disable

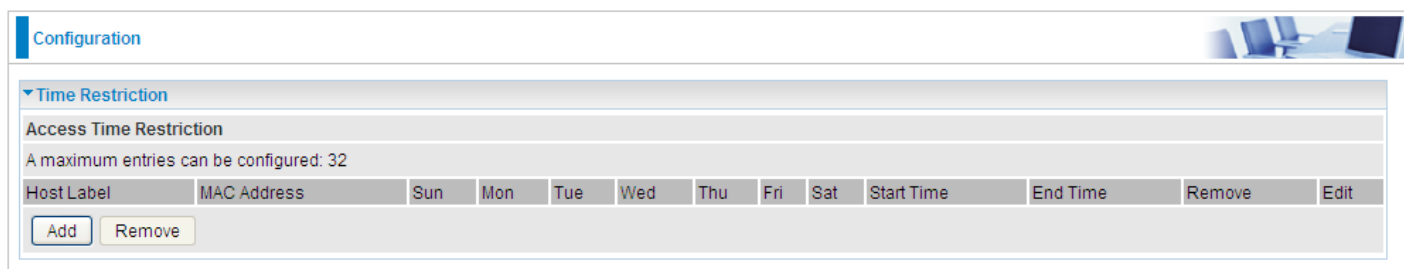
Block WAN (IPv6) PING: ☐ Enable ☒ Disable

Time Restriction

A MAC (Media Access Control) address is the unique network hardware identifier for each PC on your network's interface (i.e. its Network Interface Card or Ethernet card). Using your router's MAC Address Filter function, you can configure the network to block specific machines from accessing your LAN during the specified time.

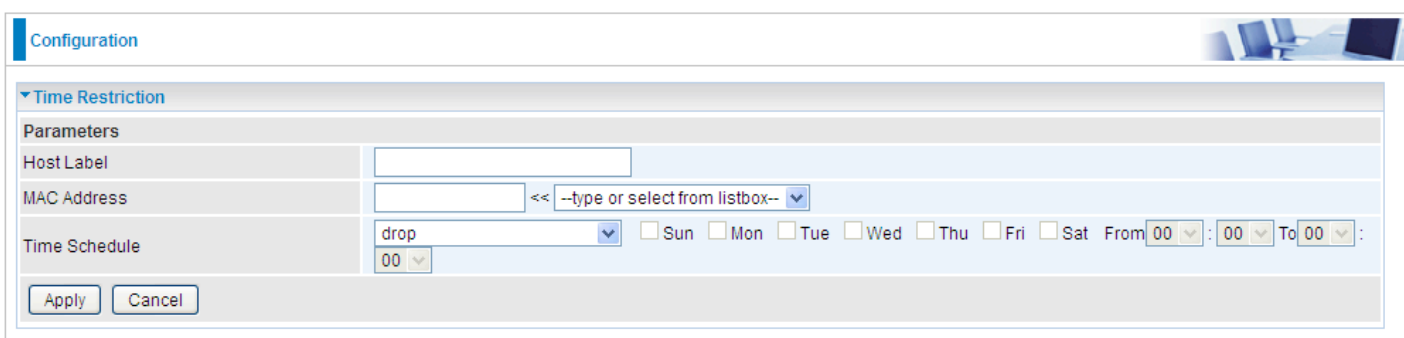
This page adds time of day restriction to a special LAN device connected to the router. To **Restrict** LAN device(s), please click Add button to add the device(s) from accessing internet under some set time. To find out the MAC address of a window based PC, go to command window, and type "ipconfig/all".

Note: The maximum entries configured: 32.



The screenshot shows the 'Configuration' page with a 'Time Restriction' section. It includes a table with columns: Host Label, MAC Address, Sun, Mon, Tue, Wed, Thu, Fri, Sat, Start Time, End Time, Remove, and Edit. Below the table are 'Add' and 'Remove' buttons. A note states: 'A maximum entries can be configured: 32'.

Click **Add** to add the rules.



The screenshot shows the 'Parameters' section of the 'Time Restriction' configuration. It includes input fields for 'Host Label' and 'MAC Address', a dropdown for 'Time Schedule' (set to 'drop'), and checkboxes for days of the week (Sun, Mon, Tue, Wed, Thu, Fri, Sat). It also has 'From' and 'To' time selectors. 'Apply' and 'Cancel' buttons are at the bottom.

Host Label: User-defined name.

MAC Address: Enter the MAC address(es) you want to allow or block to access the router and LAN. The format of MAC address could be: xx:xx:xx:xx:xx:xx or xx-xx-xx-xx-xx-xx. For convenience, user can select from the list box.

Time Schedule: To determine when the rule works.

- ① **Drop:** To drop the MAC entries always; in other words, the MACs are blocked access to router and internet always.
- ① **Forward:** To forward the MAC entries always; in other words, the MACs are granted access to the router and internet always.
- ① **Check or select from listbox:** To set the time duration during which the MACs are blocked from access the router and internet. "**select from listbox**" means that you can select the already set timeslot in "**Time Schedule**" section during which the MACs are blocked from access the router and internet.

Click **Apply** to confirm your settings. The following prompt window will appear to remind you of the attention.

An example:

Configuration

Time Restriction

Access Time Restriction

A maximum entries can be configured: 32

Host Label	MAC Address	Sun	Mon	Tue	Wed	Thu	Fri	Sat	Start Time	End Time	Remove	Edit
test	18:a9:05:38:04:03	forward									<input type="checkbox"/>	Edit
child-use	18:a9:05:04:12:23		x	x	x	x	x		00:00	23:59	<input type="checkbox"/>	Edit

Add Remove

Here you can see that the user “child-use” with a MAC of 18:a9:05:04:12:23 is blocked to access the router from 00:00 to 23:59 Monday through Friday. The “test” can access the internet always.

If you needn't this rule, you can check the box, press Remove, it will be OK.

URL Filter

URL (Uniform Resource Locator – e.g. an address in the form of <http://www.abcde.com> or <http://www.example.com>) filter rules allow you to prevent users on your network from accessing particular websites by their URL. There are no pre-defined URL filter rules; you can add filter rules to meet your requirements.

Note:

- 1) URL Filter rules apply to both IPv4 and IPv6 sources.
- 2) But in **Exception IP Address** part, user can click [Detail ▶](#) to set the exception IP address(es) for IPv4 and IPv6 respectively.

Configuration

URL Filter

Parameters

Keywords Filtering ☐ Enable [Detail ▶](#)

Domains Filtering ☐ Enable [Detail ▶](#)

Restrict URL Features BLOCK ☐ Java Applet ☐ ActiveX ☐ Cookie ☐ Proxy

Except IP Address [Detail ▶](#)

Log ☐

Time Schedule Always On ☐ Sun ☐ Mon ☐ Tue ☐ Wed ☐ Thu ☐ Fri ☐ Sat From : To :

Apply Cancel

Keywords Filtering: Allow blocking against specific keywords within a particular URL rather than having to specify a complete URL (e.g. to block any image called “advertisement.gif”). When enabled, your specified keywords list will be checked to see if any keywords are present in URLs accessed to determine if the connection attempt should be blocked. Please note that the URL filter blocks web browser (HTTP) connection attempts using port 80 only.

Domains Filtering: This function checks the whole URL address but not the IP address against your list of domains to block or allow. If it is matched, the URL request will either be sent (Trusted) or dropped (Forbidden).

Restrict URL Features: Click Block Java Applet to filter web access with Java Applet components. Click Block ActiveX to filter web access with ActiveX components. Click Block Cookie to filter web access with Cookie components. Click Block Proxy to filter web proxy access.

Exception IP Address: You can input a list of IP addresses as the exception list for URL filtering. These IPs will not be covered by the URL rules.

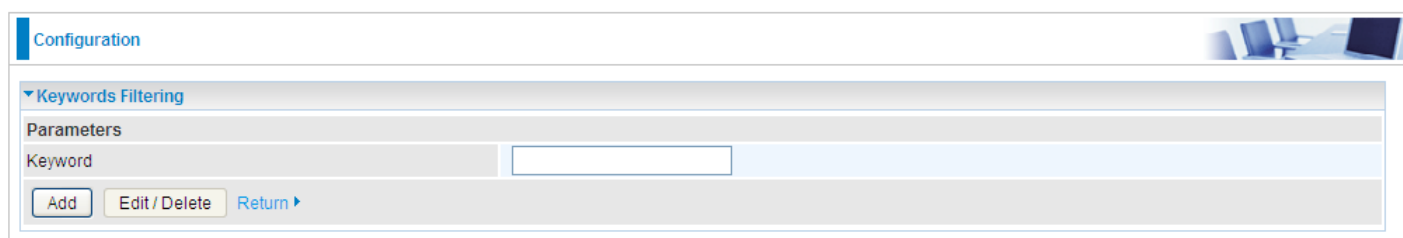
Time Schedule: Select or set exactly when the rule works. When set to “Always On”, the rule will work all time; and also you can set the precise time when the rule works, like 01:00-19:00 from Monday to Friday. Or you can select the already set timeslot in “**Time Schedule**” during which the rule works. And when set to “Disable”, the rule is disabled. See [Time Schedule](#).

Log: Select Enable for this option if you will like to capture the logs for this URL filter policy. To check the log, users can turn to [Security Log](#).

Keywords Filtering

Note: Maximum number of entries: 32.

Click [Detail ▶](#) to add the keywords.



Configuration

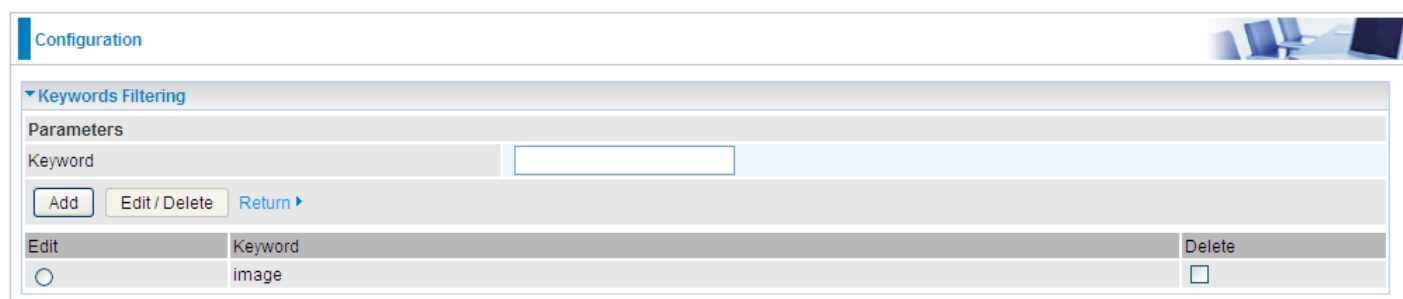
Keywords Filtering

Parameters

Keyword

Add Edit / Delete Return ▶

Enter the Keyword, for example image, and then click **Add**.



Configuration

Keywords Filtering

Parameters

Keyword

Add Edit / Delete Return ▶

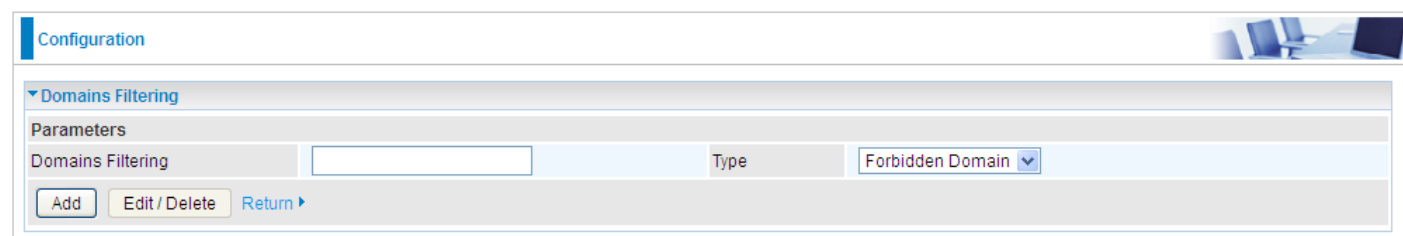
Edit	Keyword	Delete
<input type="radio"/>	image	<input type="checkbox"/>

You can add other keywords like this. The keywords you add will be listed as above. If you want to reedit the keyword, press the Edit radio button left beside the item, and the word will listed in the Keyword field, edit, and then press **Edit/Delete** to confirm. If you want to delete certain keyword, check Delete checkbox right beside the item, and press **Edit/Delete**. Click **Return** to be back to the previous page.

Domain Filtering

Note: Maximum number of entries: 32.

Click [Detail ▶](#) to add Domains.



Configuration

Domains Filtering

Parameters

Domains Filtering

Type

Forbidden Domain

Add Edit / Delete Return ▶

Domain Filtering: enter the domain you want this filter to apply.

Type: select the action this filter deals with the Domain.

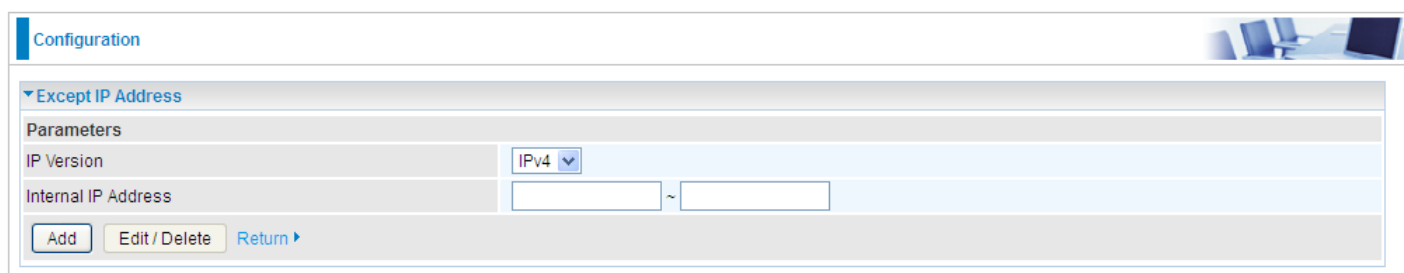
- ❶ **Forbidden Domain:** The domain is forbidden access.
- ❷ **Trusted Domain:** The domain is trusted and allowed access.

Enter a domain and select whether this domain is trusted or forbidden with the pull-down menu. Next, click **Add**. Your new domain will be added to either the Trusted Domain or Forbidden Domain listing, depending on which you selected previously. For specific process, please refer to **Keywords Filtering**.

Exception IP Address

In the section, users can set the exception IP respectively for IPv4 and IPv6.

Click [Detail ▶](#) to add the IP Addresses.



The screenshot shows a web interface titled 'Configuration'. Under the 'Exception IP Address' section, there is a 'Parameters' table. The table has two rows: 'IP Version' with a dropdown menu set to 'IPv4', and 'Internal IP Address' with two text input fields separated by a tilde (~). Below the table, there are three buttons: 'Add', 'Edit / Delete', and 'Return ▶'.


Enter the except IP address. Click **Add** to save your changes. The IP address will be entered into the **Exception List**, and excluded from the URL filtering rules in effect. For specific process, please refer to **Keywords Filtering**.

For example, users can set IPv4 client 192.168.1.103 in your network as a exception address that is not limited to the rules set in URL filter (or IPv4 clients (a range)). And also an IPv6 client (2000:1211:1002:6ba4:d160:5adb:9009:87ae) or IPv6 clients(a range) can be the exceptions from the URL rules.

At the URL Filter page, press **Apply** to confirm your settings.

Parental Control Provider

Parental Control Provider provides Web content filtering offering safer and more reliable web surfing for users. Please get an account and configure at the selected Provider “www.opendns.com” in advance. To use parental control (DNS), user needs to configure to use parental control (DNS provided by parental control provider) to access internet at WAN configuration or DNS page(See [DNS](#)).

Configuration


Parental Control Provider

Parameters

Parental Control Provider provides Web content filtering while surfing the web safer and more reliable. Please get an account and configure at the selected Provider in advance.

Providerwww.opendns.com

Host Name

Username


Password

ApplyCancel

Host Name, Username and Password: Enter your registered domain name and your username and password at the provider website www.opendns.com.

QoS - Quality of Service

QoS helps you to control the data upload traffic of each application from LAN (Ethernet) to WAN (Internet). This feature allows you to control the quality and speed of throughput for each application when the system is running with full upstream load.

Configuration


QoS Classification Setup

EWAN Line Speed

Upstream / Downstream0 / 0 kbps [0 : Disable]

Apply


Maximum rules can be configured: 32

Class Name	IP Version	Direction	Internal IP Address	Internal Port	Protocol	External IP Address	External Port	DSCP Mark	Rate Type	Disabled	Remove	Edit
AddRemove												

EWAN Line Speed

Upstream / Downstream: Specify the upstream and downstream rate of the EWAN interface. Click **Apply** to save the EWAN rate settings.

Click **Add** to enter QoS rules.

Configuration


Quality of Service

Non-Assigned Bandwidth Ratio => Upstream (LAN to WAN) : 100% Downstream (WAN to LAN) : 100%

IP VersionIPv4

Application
<< --type or select from listbox--

DirectionLAN to WAN

ProtocolAny

DSCP MarkingDisable

Rate TypePrioritization

Ratio%

PriorityNormal

Internal IP Address

Internal Port

External IP Address

External Port

Time Schedule
Always On
Sun Mon Tue Wed Thu Fri Sat From 00 : 00 To 00 : 00

Apply

IP Version: Select either IPv4 or IPv6 base on need.

Application: Assign a name that identifies the new QoS application rule. Select from the list box for quick setup.

Direction: Shows the direction mode of the QoS application.

- ① **LAN to WAN:** You want to control the traffic from local network to the outside (Upstream). You can assign the priority for the application or you can limit the rate of the application.
Eg: you have a FTP server inside the local network, and you want to have a limited control by the QoS policy and so you need to add a policy with LAN to WAN direction setting.
- ① **WAN to LAN:** Control traffic from WAN to LAN (Downstream).

Protocol: Select the supported protocol from the drop down list.

DSCP Marking: Differentiated Services Code Point (DSCP), it is the first 6 bits in the ToS byte. DSCP Marking allows users to classify the traffic of the application to be executed according to the DSCP value.

IP Precedence and DSCP Mapping Table

Mapping Table	
Default (000000)	Best Effort
EF(101110)	Expedited Forwarding
AF11 (001010)	Assured Forwarding Class1(L)
AF12 (001100)	Assured Forwarding Class1(M)
AF13 (001110)	Assured Forwarding Class1(H)
AF21 (010010)	Assured Forwarding Class1(L)
AF22 (010100)	Assured Forwarding Class1(M)
AF23 (010110)	Assured Forwarding Class1(H)
AF31 (011010)	Assured Forwarding Class1(L)
AF32 (011100)	Assured Forwarding Class1(M)
AF33 (011110)	Assured Forwarding Class1(H)
AF41 (100010)	Assured Forwarding Class1(L)
AF42 (100100)	Assured Forwarding Class1(M)
AF43 (100110)	Assured Forwarding Class1(H)
CS1(001000)	Class Selector(IP precedence)1
CS2(010000)	Class Selector(IP precedence) 2
CS3(011000)	Class Selector(IP precedence)3
CS4(100000)	Class Selector(IP precedence) 4
CS5(101000)	Class Selector(IP precedence) 5
CS6(110000)	Class Selector(IP precedence) 6
CS7(111000)	Class Selector(IP precedence) 7

DSCP offers three levels of service, Class Selector (CS), Assured Forwarding (AF) and Expedited Forwarding (EF). AF1, AF2, AF3 and AF4 are four levels of assured forwarding services. Each AF has three different packet loss priorities from high, medium, to low. Also, CS1-CS7 indicates the IP precedence.

Rate Type: You can choose **Limited** or **Prioritization**.

- ① **Limited (Maximum):** Specify a limited data rate for this policy. It also is the maximum rate for this policy. When you choose **Limited**, type the **Ratio** proportion. As above FTP server example, you may want to “throttle” the outgoing FTP speed to 20% of 256K and limit to it, you may use this type.

- ① **Prioritization:** Specify the rate type control for the rule to be used. If you choose **Prioritization** for the rule, the parameter **Priority** would be available, you can set the priority for this rule.
- ① **Set DSCP Marking:** When select **Set DSCP Marking**, the packets matching the rule will be forwarded according to the pre-set DSCP marking.

Ratio: The rate percent of each application/policy compared to total traffic on the interface with limited rate type. For example, we want to only allow 20% of the total data for the LAN-to-WAN direction to be used for FTP server. Then we can specify here with data ratio = 20.

Priority: Set the priority given to each policy/application. Specify the priority for the use of bandwidth. You can specify which application can have higher priority to acquire the bandwidth. Its default setting is set to Normal. You may adjust this setting to fit your policy / application.

Internal IP Address: The IP address values for Local LAN devices you want to give control.

Internal Port: The Port number on the LAN side, it is used to identify an application.

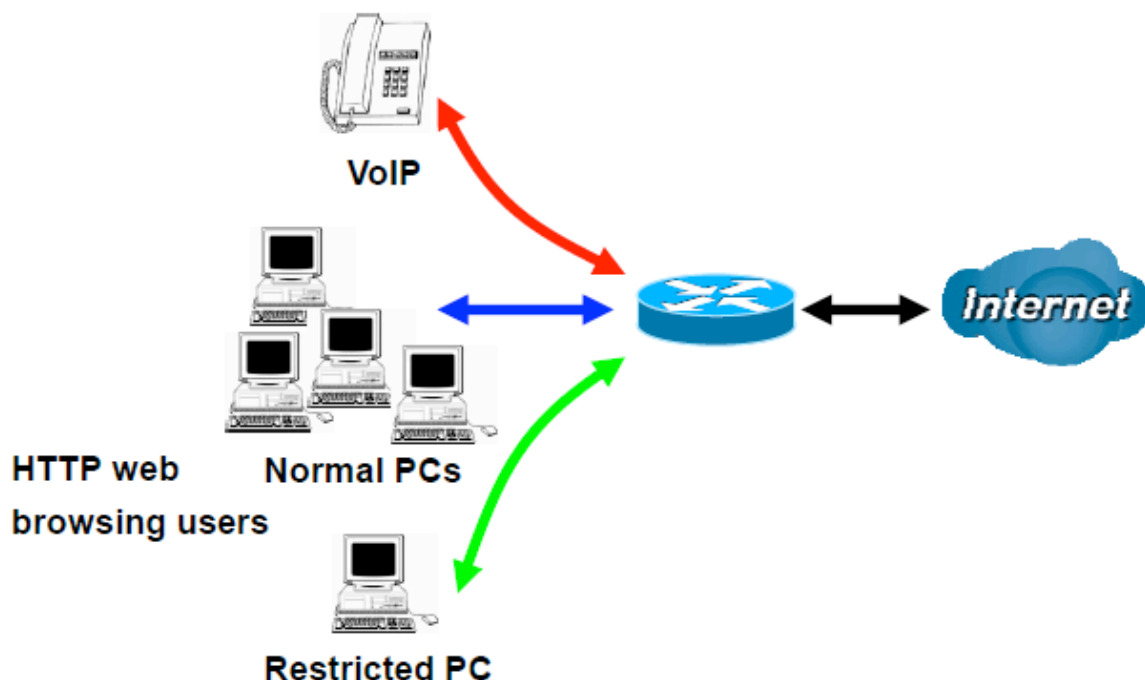
External IP Address: The IP address on remote / WAN side.

External Port: The Port number on the remote / WAN side.

Time Schedule: Select or set exactly when the rule works. When set to “Always On”, the rule will work all time; and also you can set the precise time when the rule works, like 01:00-19:00 from Monday to Friday. Or you can select the already set timeslot in “**Time Schedule**” during which the rule works. And when set to “Disable”, the rule is disabled or inactive and there will be an icon”

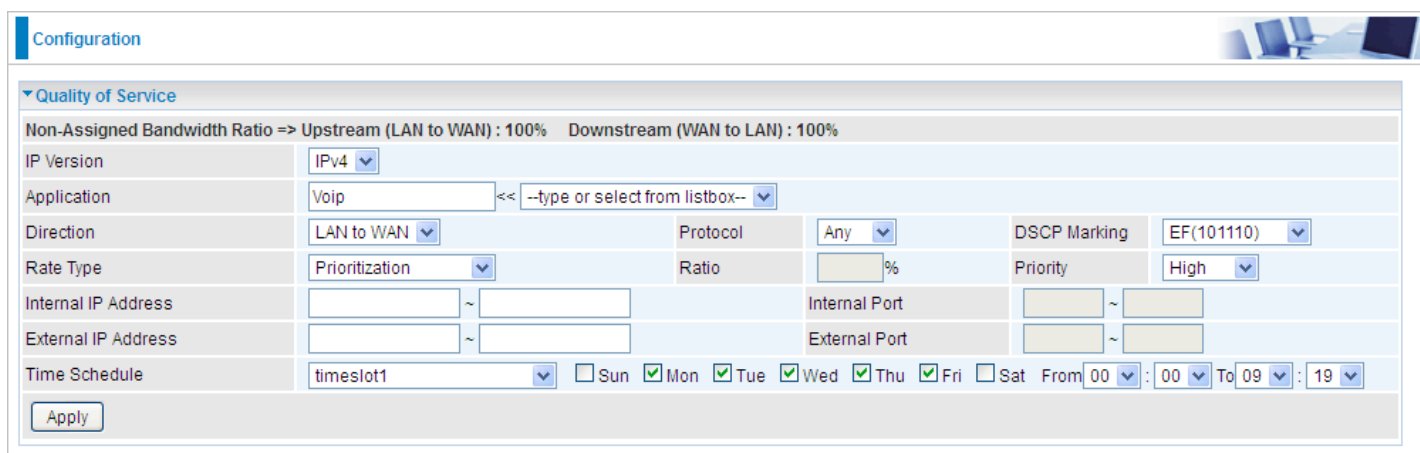
✓ ” indicating the rule is inactive. See [Time Schedule](#).

Examples: Common usage



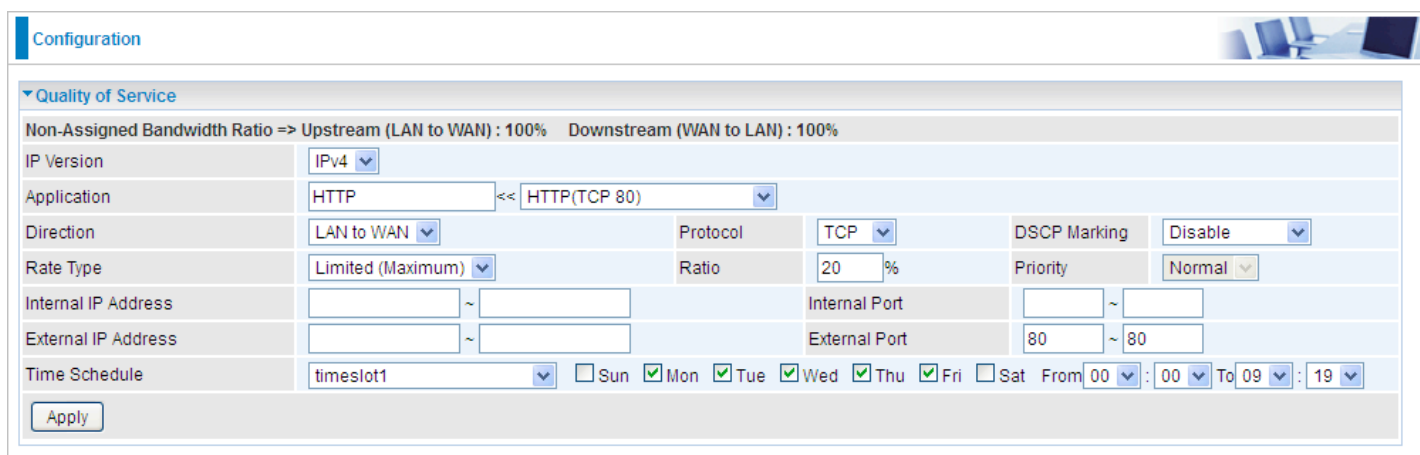
1. Give outgoing VoIP traffic more priority.

The default queue priority is normal, so if you have VoIP users in your local network, you can set a higher priority to the outgoing VoIP traffic.



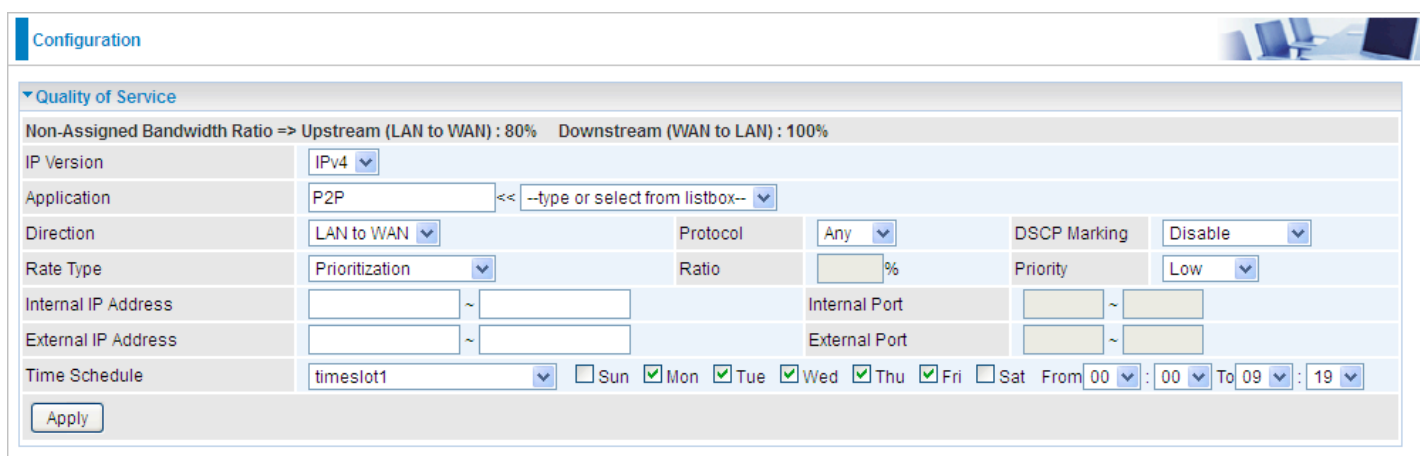
The screenshot shows the 'Configuration' page with the 'Quality of Service' section expanded. The 'Non-Assigned Bandwidth Ratio' is set to 'Upstream (LAN to WAN) : 100%' and 'Downstream (WAN to LAN) : 100%'. The 'IP Version' is 'IPv4'. The 'Application' is 'Voip'. The 'Direction' is 'LAN to WAN'. The 'Protocol' is 'Any'. The 'DSCP Marking' is 'EF(101110)'. The 'Rate Type' is 'Prioritization'. The 'Ratio' is set to a percentage. The 'Priority' is 'High'. The 'Time Schedule' is 'timeslot1' with checkboxes for Sun, Mon, Tue, Wed, Thu, Fri, and Sat. The 'Apply' button is visible at the bottom.

2. Give regular web http access a limited rate



The screenshot shows the 'Configuration' page with the 'Quality of Service' section expanded. The 'Non-Assigned Bandwidth Ratio' is set to 'Upstream (LAN to WAN) : 100%' and 'Downstream (WAN to LAN) : 100%'. The 'IP Version' is 'IPv4'. The 'Application' is 'HTTP'. The 'Direction' is 'LAN to WAN'. The 'Protocol' is 'TCP'. The 'DSCP Marking' is 'Disable'. The 'Rate Type' is 'Limited (Maximum)'. The 'Ratio' is '20 %'. The 'Priority' is 'Normal'. The 'Time Schedule' is 'timeslot1' with checkboxes for Sun, Mon, Tue, Wed, Thu, Fri, and Sat. The 'Apply' button is visible at the bottom.

3. If you are actively engaged in P2P and are afraid of slowing down internet access for other users within your network, you can then use QoS to set a rule that has low priority. In this way, P2P application will not congest the data transmission with other applications.

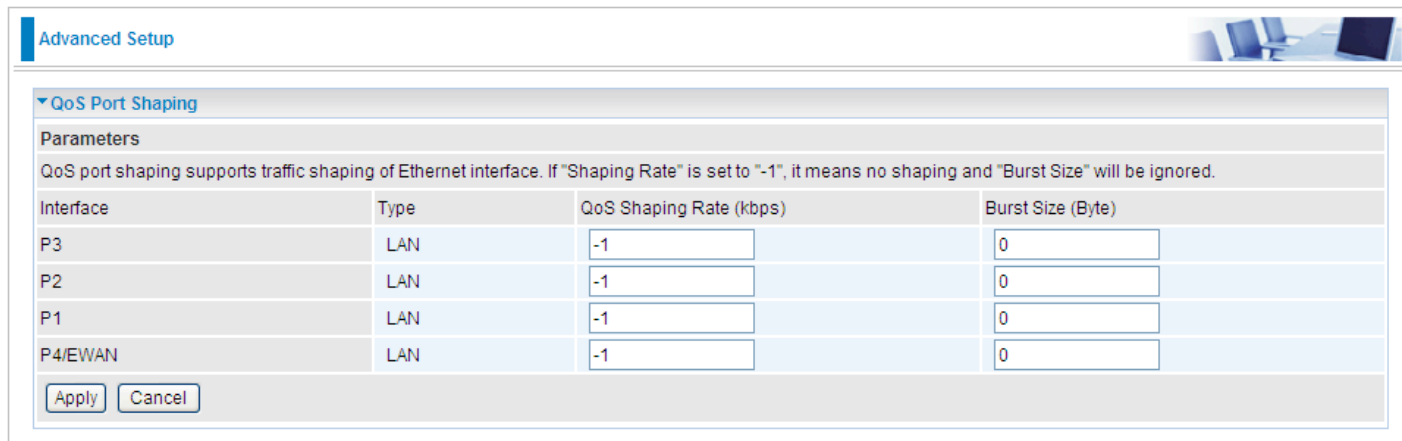


The screenshot shows the 'Configuration' page with the 'Quality of Service' section expanded. The 'Non-Assigned Bandwidth Ratio' is set to 'Upstream (LAN to WAN) : 80%' and 'Downstream (WAN to LAN) : 100%'. The 'IP Version' is 'IPv4'. The 'Application' is 'P2P'. The 'Direction' is 'LAN to WAN'. The 'Protocol' is 'Any'. The 'DSCP Marking' is 'Disable'. The 'Rate Type' is 'Prioritization'. The 'Ratio' is set to a percentage. The 'Priority' is 'Low'. The 'Time Schedule' is 'timeslot1' with checkboxes for Sun, Mon, Tue, Wed, Thu, Fri, and Sat. The 'Apply' button is visible at the bottom.

Other applications, like FTP, Mail access, users can use QoS to control based on need.

QoS Port Shaping

QoS port shaping supports traffic shaping of Ethernet interfaces. It forcefully maximizes the throughput of the Ethernet interface. When “Shaping Rate” is set to “-1”, no shaping will be in place and the “Burst Size” is to be ignored.



Interface	Type	QoS Shaping Rate (kbps)	Burst Size (Byte)
P3	LAN	-1	0
P2	LAN	-1	0
P1	LAN	-1	0
P4/EWAN	LAN	-1	0

Interface: P1-P4. P4 used as EWAN also covered.

Type: All LAN when P4 is LAN port; P4 used as EWAN, type WAN and all others LAN.

QoS Shaping Rate (Kbps): Set the forcefully maximum rate.

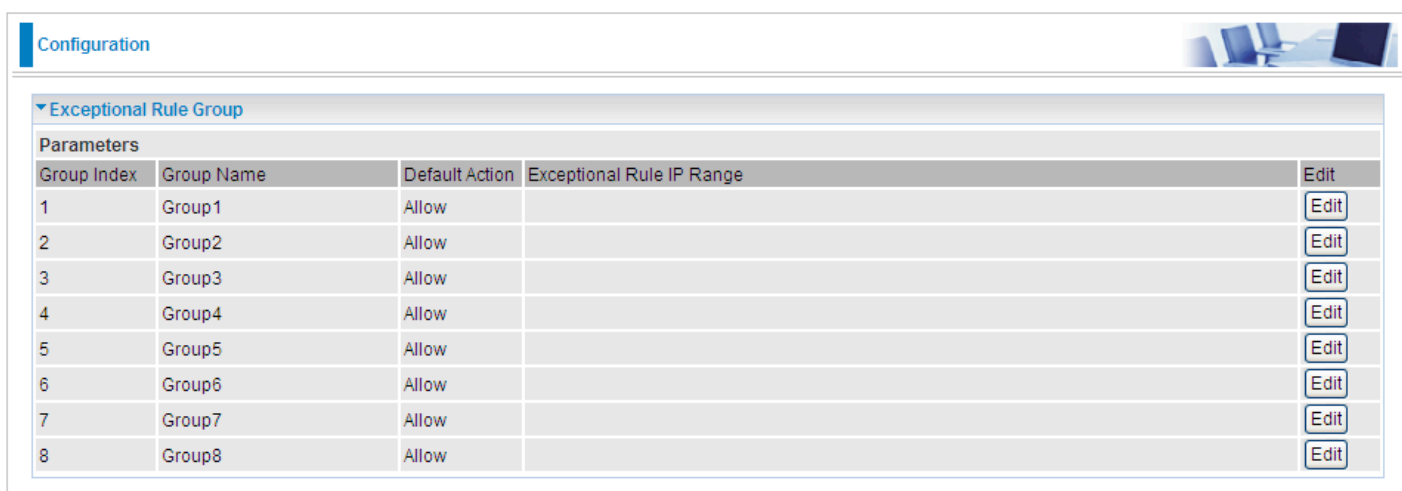
Burst Size(Bytes): Set the forcefully Burst Size.

NAT

NAT (Network Address Translation) feature translates a private IP to a public IP, allowing multiple users to access the Internet through a single IP account, sharing the single IP address. It is a natural firewall for the private network.

Exceptional Rule Group

Exceptional Rule is dedicated to giving or blocking Virtual Server/ DMZ access to some specific IP or IPs(range). Users are allowed to set 8 different exceptional rule groups at most. In each group, user can add specific IP or IP range.



Group Index	Group Name	Default Action	Exceptional Rule IP Range	Edit
1	Group1	Allow		Edit
2	Group2	Allow		Edit
3	Group3	Allow		Edit
4	Group4	Allow		Edit
5	Group5	Allow		Edit
6	Group6	Allow		Edit
7	Group7	Allow		Edit
8	Group8	Allow		Edit

Press **Edit** to set the exceptional IP (IP Range).

Configuration

Exceptional Rule Group

Parameters

Group Name

Group1

Default Action

☒ Allow

☐ Block

Apply

Exceptional Rule IP Range

IP Address Range

~

Add

Edit / Delete

Default Action: Please first set the range to make “**Default Action**” setting available. Set “Allow” to ban the listed IP or IPs to access the Virtual Server and DMZ Host
Check “Block” to grant access to the listed IP or IPs to Virtual Server and DMZ Host.
Apply: Press **Apply** button to apply the change.

Exceptional Rule Range

IP Address Range: Specify the IP address range; IPv4 address range can be supported.
Click **Add** to add the IP Range.

For instance, if user wants to block IP range of 172.16.1.102-172.16.1.106 from accessing your set virtual server and DMZ host, you can add this IP range and valid it.

Configuration

Exceptional Rule Group

Parameters

Group Name

Group1

Default Action

☒ Allow

☐ Block

Apply

Exceptional Rule IP Range

IP Address Range

~

Add

Edit / Delete

Edit	Action	IP Address Range	Delete
<input type="radio"/>	Block	172.16.1.102 ~ 172.16.1.106	<input type="checkbox"/>
<input type="radio"/>	Block	172.16.1.108 ~ 172.16.1.108	<input type="checkbox"/>

Virtual Servers

In TCP/IP and UDP networks a port is a 16-bit number used to identify which application program (usually a server) incoming connections should be delivered to. Some ports have numbers that are pre-assigned to them by the IANA (the Internet Assigned Numbers Authority), and these are referred to as “well-known ports”. Servers follow the well-known port assignments so clients can locate them.
If you wish to run a server on your network that can be accessed from the WAN (i.e. from other machines on the Internet that are outside your local network), or any application that can accept incoming connections (e.g. Peer-to-peer/P2P software such as instant messaging applications and P2P file-sharing applications) and are using NAT (Network Address Translation), then you will usually need to configure your router to forward these incoming connection attempts using specific ports to the PC on your network running the application. You will also need to use port forwarding if you want to host an online game server.

The reason for this is that when using NAT, your publicly accessible IP address will be used by and point to your router, which then needs to deliver all traffic to the private IP addresses used by your PCs. Please see the **WAN** configuration section of this manual for more information on NAT.

The device can be configured as a virtual server so that remote users accessing services such as Web or FTP services via the public (WAN) IP address can be automatically redirected to local servers in the LAN network. Depending on the requested service (TCP/UDP port number), the device redirects the external service request to the appropriate server within the LAN network.

This part is only available when NAT is enabled.

Note: The maximum number of entries: 64.

Configuration

Virtual Servers

Virtual Servers Setup

Server Name	External Port		Protocol	Internal Port		Server IP Address	WAN Interface	Disabled	Remove	Edit
	Start	End		Start	End					
<div>AddRemove</div>										

It is virtual server listing table as you see, Click **Add** to move on.

The following configuration page will appear to let you configure.

Configuration

Virtual Servers

Parameters

Interface

3G0/usb0

WAN IP

Server Name

Custom Service

Custom Service

Server IP Address

<< --type or select from listbox--

Time Schedule

Always On

Sun

Mon

Tue

Wed

Thu

Fri

Sat

From

00

:

00

To

00

:

00

Exceptional Rule Group

None


External Port		Protocol	Protocol Number	Internal Port	
Start	End			Start	End
		TCP			
		TCP			
		TCP			
		TCP			
		TCP			
		TCP			
		TCP			
		TCP			
		TCP			
		TCP			
		TCP			

- Interface:** select from the drop-down menu the interface you want the virtual server(s) to apply.
- Server Name:** select the server name from the drop-down menu.
- Custom Service:** It is a kind of service to let users customize the service they want. Enter the user-defined service name here. It is a parameter only available when users select **Custom Service** in the above parameter.
- Server IP Address:** Enter your server IP Address here. User can select from the list box for quick setup.
- External Port**
- ① **Start:** Enter a port number as the external starting number for the range you want to give access to internal network.
 - ① **End:** Enter a port number as the external ending number for the range you want to give access to internal network.

Internal Port

- ① **Start:** Enter a port number as the internal starting number.
- ① **End:** Here it will generate automatically according to the End port number of External port and can't be modified.

Protocol: select the protocol this service used: TCP/UDP, TCP, UDP.

Time Schedule: Select or set exactly when the Virtual Server works. When set to “Always On”, the Virtual Server will work all time; and also you can set the precise time when Virtual Server works, like 01:00 - 19:00 from Monday to Friday. Or you can select the already set timeslot in **Time Schedule** during which the Virtual Server works. And when set to “Disable”, the rule is disabled and there will be an icon  in the list table indicating the rule is disabled. See [Time Schedule](#).

Exceptional Rule Group: Select the exceptional group listed. It is to grant or block Virtual Server access to a group of IPs. For example, as we set previously group 1 blocking access to 172.16.1.102-172.16.1.106. If here you want to block Virtual Server access to this IP range, you can select Group1.

Set up

1. Select a Server Name from the drop-down menu, then the port will automatically appear, modify some as you like, or you can just leave it as default. Remember to enter your server IP Address.

2. Press **Apply** to conform, and the items will be list in the **Virtual Servers Setup** table.

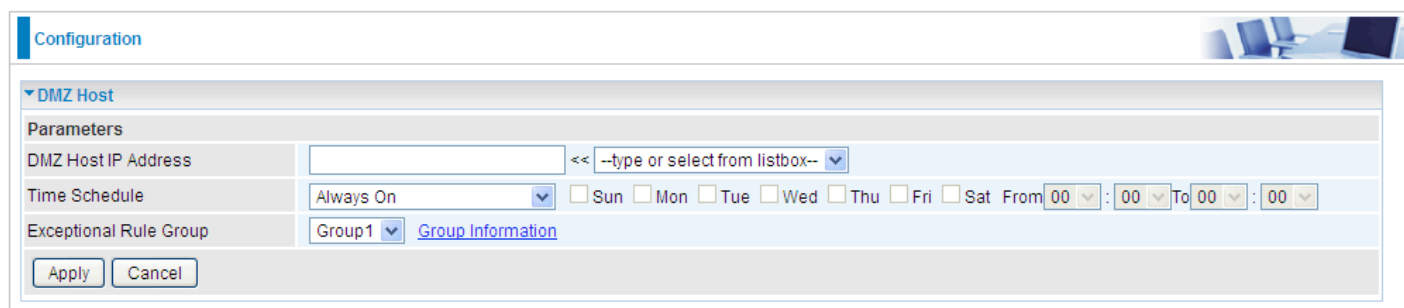
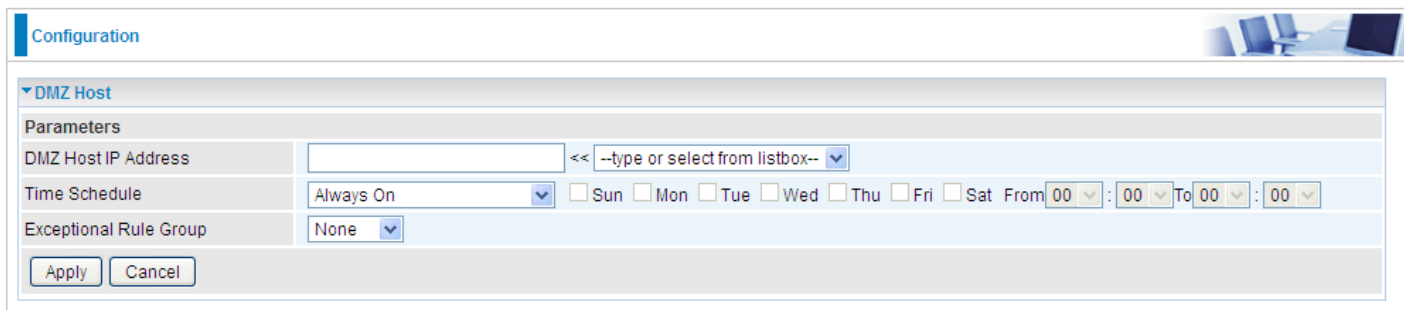
( Means the rule is inactive)

Remove

If you don't need a specified Server, you can remove it. Check the check box beside the item you want to remove, then press **Remove**, it will be OK.

DMZ Host

The DMZ Host is a local computer exposed to the Internet. When setting a particular internal IP address as the DMZ Host, all incoming packets will be checked by Firewall and NAT algorithms before being passed to the DMZ host, when a packet received does not use a port number used by any other Virtual Server entries.



Group Index	1
Group Name	Group1
Action	Block
IP Address Range	172.16.1.102~172.16.1.106 172.16.1.108~172.16.1.108

(Group Information)

DMZ Host IP Address: Enter the IP Address of a host you want it to be a DMZ host. Select from the list box to quick set the DMZ.

Time Schedule: Select or set exactly when the DMZ works. When set to “Always On”, the DMZ will work all time; and also you can set the precise time when DMZ works, like 01:00 - 19:00 from Monday to Friday. Or you can select the already set timeslot in **Time Schedule** during which the DMZ works. And when set to “Disable”, the DMZ Host is disabled. See [Time Schedule](#).

Exceptional Rule Group: Select the exceptional group listed. It is to grant or block DMZ access to a group of IPs. For example, as we set previously group 1 blocking access to 172.16.1.102-172.16.1.106. If here you want to block DMZ Access to this IP range, you can select Group1.



Using port mapping does have security implications, since outside users are able to connect to PCs on your network. For this reason you are advised to use specific Virtual Server entries just for the ports your application requires instead of simply using DMZ or creating a Virtual Server entry for “All” protocols, as doing so results in all connection attempts to your public IP address accessing the specified PC.



Attention

If you have disabled the NAT option in the WAN-ISP section, the Virtual Server function will hence be invalid.

If the DHCP server option is enabled, you have to be very careful in assigning the IP addresses of the virtual servers in order to avoid conflicts. The easiest way of configuring Virtual Servers is to manually assign static IP address to each virtual server PC, with an address that does not fall into the range of IP addresses that are to be issued by the DHCP server. You can configure the virtual server IP address manually, but it must still be in the same subnet as the router.

One-to-One NAT

One-to-One NAT maps a specific private/local address to a global/public IP address. If user has multiple global/public IP addresses from your ISP, you are free to use one-to-one NAT to assign some specific public IP for an internal IP like a public web server mapped with a global/public IP for outside access.

Configuration	
▼ One-to-One NAT	
Parameters	
Valid	<input type="checkbox"/>
WAN Interface	3G0/usb0 ▼
Global IP Address	<input type="text"/>
Internal IP Address	<input type="text"/>
Exceptional Rule Group	None ▼
<input type="button" value="Add"/> <input type="button" value="Edit / Delete"/>	

Valid: Check whether to valid the one-to-one NAT mapping rule.

WAN Interface: Select one based WAN interface to configure the one-to-one NAT.

Global IP address: The Global IP mapped to an internal device. It can be left empty, and under this circumstance, it can be reached through the WAN IP of interface set in the field above.

Internal Address: The IP address of an internal device in the LAN.

Exceptional Rule Group: Select the exceptional group listed. It is to give or block access to a group of IPs to the server after One-to-One NAT. For example, a server with 192.168.1.3 is mapped to 123.1.1.2 by One-to-One NAT, then the exceptional group can be designated to have or have not access to 123.1.1.2.

Port Triggering

Port triggering is a way to automate port forwarding with outbound traffic on predetermined ports ('triggering ports'), incoming ports are dynamically forwarded to the initiating host, while the outbound ports are in use. Port triggering triggers can open an incoming port when a client on the local network makes an outgoing connection on a predetermined port or a range of ports.

Configuration

Port Triggering

Port Triggering Setup

Application	Trigger		Open			WAN Interface	Remove	Edit
	Protocol	Port Range	Protocol	Port Range				
		StartEnd		Start	End			
<div>AddRemove</div>								

Click **Add** to add a port triggering rule.

Configuration

Port Triggering

Parameters

Interface3G0/usb0

ApplicationCustom Application

Custom Application

Trigger Port		Trigger Protocol	Open Port		Open Protocol
Start	End		Start	End	
		TCP			TCP
		TCP			TCP
		TCP			TCP
		TCP			TCP
		TCP			TCP
		TCP			TCP
		TCP			TCP
		TCP			TCP

Apply

Interface: Select from the drop-down menu the interface you want the port triggering rules apply to.

Application: Preinstalled applications or Custom Application user can customize the utility yourself.

Custom Application: It is a kind of service to let users themselves customizes the service they want. Enter the user-defined service name here.

Trigger Port

- Start:** Enter a port number as the triggering port starting number.
 - End:** Enter a port number as the triggering port ending number.
- Any port in the range delimited by the 'Start' and 'End' would be the trigger port.

Open port

Start: Enter a port number as the open port starting number.

End: Enter a port number as the open port ending number.

Any port in the range delimited by the ‘Start’ and ‘End’ would be the preset forwarding port or open port.

Protocol: select the protocol this service used: TCP/UDP, TCP, UDP.

Set up

An example of how port triggering works, when a client behind a NAT router connecting to Aim Talk, it is a TCP connection with the default port 4099.

When connecting to Aim Talk, the client typically makes an outgoing connection on port 4099 to the Aim Talk server, but when the computer is behind the NAT, the NAT silently drops this connection because it does not know which computer behind the NAT to send the request to connect.

So, in this case, port triggering in the router is working, when an outbound connection is attempted on port 4099 (or any port in the range set), it should allow inbound connections to that particular computer.

1. Select a Server Name from the drop-down menu, then the port will automatically appear, modify some as you like, or you can just leave it as default. Remember to enter your server IP Address.

Configuration

Port Triggering

Parameters

Interface

3G0/usb0

Application

Aim Talk

Custom Application

Trigger Port

Start	End	Trigger Protocol	Open Port	Open Protocol	
			Start	End	
4099	4099	TCP	5191	5191	TCP
		TCP			TCP
		TCP			TCP
		TCP			TCP
		TCP			TCP
		TCP			TCP
		TCP			TCP
		TCP			TCP
		TCP			TCP

Apply

2. Press **Apply** to conform, and the items will be list in the **Virtual Servers Setup** table.

Edit/Remove

If you don't need a specified Server, you can remove it. Check the check box beside the item you want to remove, and then press **Remove**.

Click **Edit** to re-edit your port-triggering rule.

ALG

The ALG Controls enable or disable protocols over application layer.

Configuration

ALG

Parameters

SIP

☐ Enable ☒ Disable

H.323

☒ Enable ☐ Disable

Apply

Cancel

Wake On LAN

Wake on LAN (WOL, sometimes WoL) is an Ethernet computer networking standard that allows a computer to be turned on or woken up remotely by a network message.

Configuration

Wake On LAN

Parameters

Host Label

MAC Address

 << --select-- >> (type or select from listbox)

Wake by Schedule

☐ Enable [Schedule](#)

Add

Edit / Delete

Host Label: Enter identification for the host.

Select: Select MAC address of the computer that you want to wake up or turn on remotely.

Wake by Schedule: Enable to wake up your set device at some specific time. For instance, user can set to get some device woken up at 8:00 every weekday. Click [Schedule](#) to enter time schedule configuring page to set the exact timeline.

Configuration

Wake up Time Schedule

Parameters

Name

Day in a week

☐ Sun ☐ Mon ☐ Tue ☐ Wed ☐ Thu ☐ Fri ☐ Sat

Time

00 : 00

Add

Edit / Delete

Edit	Name	Day in a week	Time	Delete
<input type="radio"/>	11	SMTWTFs	08:00	<input type="checkbox"/>

Add: After selecting, click Add then you can submit the Wake-up action.

Edit/Delete: Click to edit or delete the selected MAC address.

Ready:

“Yes” indicating the remote computer is ready for your waking up.

“No” indicating the machine is not ready for your waking up.

Delete: Delete the selected MAC address.

VPN

A **virtual private network (VPN)** is a private network that interconnects remote (and often geographically separate) networks through primarily public communication infrastructures such as the Internet. VPNs provide security through tunneling protocols and security procedures such as encryption. For example, a VPN could be used to securely connect the branch offices of an organization to a head office network through the public Internet.

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 also 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.

IPsec is an end-to-end security scheme operating in the Internet Layer of the Internet Protocol Suite. It can be used in protecting data flows between a pair of security gateways (*network-to-network*), or between a security gateway and a host (*network-to-host*).

Note: A maximum of 16 sessions for IPSec.

VPN

▼IPSec

NAT Traversal

NAT Traversal

☐ Enable

Keep Alive

Second(s) [1-60]

Apply

Tunnel Mode Connections

Active	L2TP	Connection Name	Local Network	Remote Network	Remote Security Gateway	Remove	Edit
<input type="button" value="Add"/>	<input type="button" value="Remove"/>						

NAT Traversal

NAT Traversal: This directive enables use of the NAT-Traversal IPsec extension (NAT-T). NAT-T allows one or both peers to reside behind a NAT gateway (i.e., doing address- or port-translation).

Keep Alive: Type the interval time(sec) for sending packets to keep the NAT Traversal alive.

Click **Apply** to save and apply your settings.

Click **Add** to create IPSec connections.

VPN

▼IPSec

IPSec Settings

L2TP over IPSec

☐ Enable

Connection Name

WAN Interface

Default

IP Version

IPv4

Local Network

Single Address

IP Address

Netmask

Remote Security Gateway

Anonymous

☐

Remote Network

Single Address

IP Address

Netmask

Key Exchange Method

IKE

IPsec Protocol

ESP

Pre-Shared Key

Local ID Type

Default

ID Content

Remote ID Type

Default

ID Content

Phase 1

Mode

Main

Encryption Algorithm

3DES

Integrity Algorithm

MD5

DH Group

MODP1024(DH2)

SA Lifetime

480

Minute(s) [60-1440]

Phase 2

Encryption Algorithm

3DES

Integrity Algorithm

MD5

DH Group

None

IPSec Lifetime

60

Minute(s) [60-1440]

Keep Alive

None

MTU

0

(0 : Default)

Apply

IPSec Settings

L2TP over IPSec: Select Enable if user wants to use L2TP over IPSec. See [L2TP over IPSec](#)

Connection Name: A given name for the connection, but it should contain no spaces (e.g. “connection-to-office”).

WAN Interface: Select the set used interface for the IPSec connection

IP Version: Select the IP version base on your network framework.

Local Network: Set the IP address or subnet of the local network.

- ① **Single Address:** The IP address of the local host, for establishing an IPSec connection between a security gateway and a host (*network-to-host*).
- ① **Subnet:** The subnet of the local network, for establishing an IPSec tunnel between a pair of security gateways (*network-to-network*)

IP Address: The local network address.

Netmask: The local network netmask.

Remote Secure Gateway: The IP address of the remote VPN device that is connected and establishes a VPN tunnel.

Anonymous: Enable any IP to connect in.

Remote Network: Set the IP address or subnet of the remote network.

- ① **Single Address:** The IP address of the local host, for establishing an IPSec connection between a security gateway and a host (*network-to-host*). If the remote peer is a host, select Single Address.
- ① **Subnet:** The subnet of the local network, for establishing an IPSec tunnel between a pair of security gateways (*network-to-network*), If the remote peer is a network, select Subnet.

Key Exchange Method: Displays key exchange method.

Pre-Shared Key: This is for the Internet Key Exchange (IKE) protocol, a string from 4 to 128 characters. Both sides should use the same key. IKE is used to establish a shared security policy and authenticated keys for services (such as IPSec) that require a key. Before any IPSec traffic can be passed, each router must be able to verify the identity of its peer. This can be done by manually entering the pre-shared key into both sides (router or hosts).

Local ID Type and Remote ID Type: When the mode of phase 1 is aggressive, Local and Remote peers can be identified by other IDs.

ID content: Enter ID content the name you want to identify when the Local and Remote Type are Domain Name; Enter ID content IP address you want to identify when the Local and Remote Type are IP addresses (IPv4 and IPv6 supported).

Phase 1

Mode: Select IKE mode from the drop-down menu: **Main** or **Aggressive**. This IKE provides secured key generation and key management.

Encryption Algorithm: Select the encryption algorithm from the drop-down menu. There are several options: 3DES and AES (128, 192 and 256). 3DES and AES are more powerful but increase latency.

- ① **DES:** Stands for Triple Data Encryption Standard, it uses 56 bits as an encryption method.
- ① **3DES:** Stands for Triple Data Encryption Standard, it uses 168 (56*3) bits as an encryption method.
- ① **AES:** Stands for Advanced Encryption Standards, you can use 128, 192 or 256 bits as encryption method.

Integrity Algorithm: Authentication establishes the integrity of the datagram and ensures it is not tampered with in transmit. There are 2 options: Message Digest 5 (MD5) and Secure Hash Algorithm (SHA1). SHA1 is more resistant to brute-force attacks than MD5. However, it is slower.

- ① **MD5:** A one-way hashing algorithm that produces a 128-bit hash.
- ① **SHA1:** A one-way hashing algorithm that produces a 160-bit hash.

DH Group: It is a public-key cryptography protocol that allows two parties to establish a shared secret over an unsecured communication channel (i.e. over the Internet). MODP stands for Modular Exponentiation Groups.

SA Lifetime: Specify the number of minutes that a Security Association (SA) will stay active before new encryption and authentication key will be exchanged. Enter a value to issue an initial connection request for a new VPN tunnel. Default is 480 minutes (28800 seconds). A short SA time increases security by forcing the two parties to update the keys. However, every time when the VPN tunnel re-negotiates, access through the tunnel will be temporarily disconnected.

Phase 2

Encryption Algorithm: Select the encryption algorithm from the drop-down menu. There are several options: 3DES and AES (128, 192 and 256). 3DES and AES are more powerful but increase latency.

Integrity Algorithm: Authentication establishes the integrity of the datagram and ensures it is not tampered with in transmit. There are 2 options: Message Digest 5 (MD5) and Secure Hash Algorithm (SHA1). SHA1 is more resistant to brute-force attacks than MD5. However, it is slower.

DH Group: It is a public-key cryptography protocol that allows two parties to establish a shared

secret over an unsecured communication channel (i.e. over the Internet). MODP stands for Modular Exponentiation Groups.

IPSec Lifetime: Specify the number of minutes that IPSec will stay active before new encryption and authentication key will be exchanged. Enter a value to negotiate and establish secure authentication. Default is 60 minutes (3600 seconds). A short time increases security by forcing the two parties to update the keys. However, every time when the VPN tunnel re- negotiates, access through the tunnel will be temporarily disconnected.

Ping for Keep Alive: Select the operation methods:

- ① **None:** The default setting is “None”. To this mode, it will not detect the remote IPSec peer has been lost or not. It only follows the policy of Disconnection time after no traffic, which the remote IPSec will be disconnected after the time you set in this function.
- ① **DPD:** Dead peer detection (DPD) is a keeping alive mechanism that enables the router to be detected lively when the connection between the router and a remote IPSec peer has lost. Please be noted, it must be enabled on the both sites.

Detection Interval	180	Second(s) [180-86400]	Idle Timeout	5	Consecutive times [5-99]
--------------------	-----	-----------------------	--------------	---	--------------------------

Detection Interval: The period cycle for dead peer detection. The interval can be 180~86400 seconds.

Idle Timeout: Auto-disconnect the IPSec connection after trying several consecutive times.

- ① **Ping:** This mode will detect whether the remote IPSec peer has lost or not by pinging specify IP address.

Ping IP (0.0.0.0 : NEVER)	0.0.0.0	Interval	10	Second(s) [0-3600, 0 : NEVER]
---------------------------	---------	----------	----	-------------------------------

Ping IP: Type the IP for ping operation. It is able to IP Ping the remote PC with the specified IP address and alert when the connection fails. Once alter message is received, Router will drop this tunnel connection. Reestablish of this connection is required. Default setting is 0.0.0.0 which disables the function.

Interval: This sets the time interval between Pings to the IP function to monitor the connection status. Default interval setting is 10 seconds. Time interval can be set from 0 to 3600 second, 0 second disables the function.

MTU: Maximum Transmission Unit, maximum value is 1500.

IPSec for L2TP

VPN

IPSec

IPSec Settings

L2TP over IPSec

☒ Enable

Connection Name

WAN Interface

Default

IP Version

IPv4

Remote Security Gateway

☐ Anonymous

Key Exchange Method

IKE

IPsec Protocol

ESP

Pre-Shared Key

Encryption Algorithm

3DES

Integrity Algorithm

MD5

DH Group

None

IPSec Lifetime

60

Minute(s) [60-1440]

Apply

Connection Name: A given name for the connection, but it should contain no spaces (e.g. “connection-to-office”).

WAN Interface: Select the set interface for the IPSec tunnel.

Remote Security Gateway: Input the IP of remote security gateway.

Key Exchange Method: Displays key exchange method.

Pre-Shared Key: This is for the Internet Key Exchange (IKE) protocol, a string from 4 to 128 characters. Both sides should use the same key. IKE is used to establish a shared security policy and authenticated keys for services (such as IPSec) that require a key. Before any IPSec traffic can be passed, each router must be able to verify the identity of its peer. This can be done by manually entering the pre-shared key into both sides (router or hosts).

Encryption Algorithm: Select the encryption algorithm from the drop-down menu. There are several options: 3DES and AES (128, 192 and 256). 3DES and AES are more powerful but increase latency.

- ① **DES:** Stands for Triple Data Encryption Standard, it uses 56 bits as an encryption method.
- ① **3DES:** Stands for Triple Data Encryption Standard, it uses 168 (56*3) bits as an encryption method.
- ① **AES:** Stands for Advanced Encryption Standards, you can use 128, 192 or 256 bits as encryption method.

Integrity Algorithm: Authentication establishes the integrity of the datagram and ensures it is not tampered with in transmit. There are 2 options: Message Digest 5 (MD5) and Secure Hash Algorithm (SHA1). SHA1 is more resistant to brute-force attacks than MD5. However, it is slower.

- ① **MD5:** A one-way hashing algorithm that produces a 128-bit hash.
- ① **SHA1:** A one-way hashing algorithm that produces a 160-bit hash.

DH Group: It is a public-key cryptography protocol that allows two parties to establish a shared secret over an unsecured communication channel (i.e. over the Internet). MODP stands for Modular Exponentiation Groups.

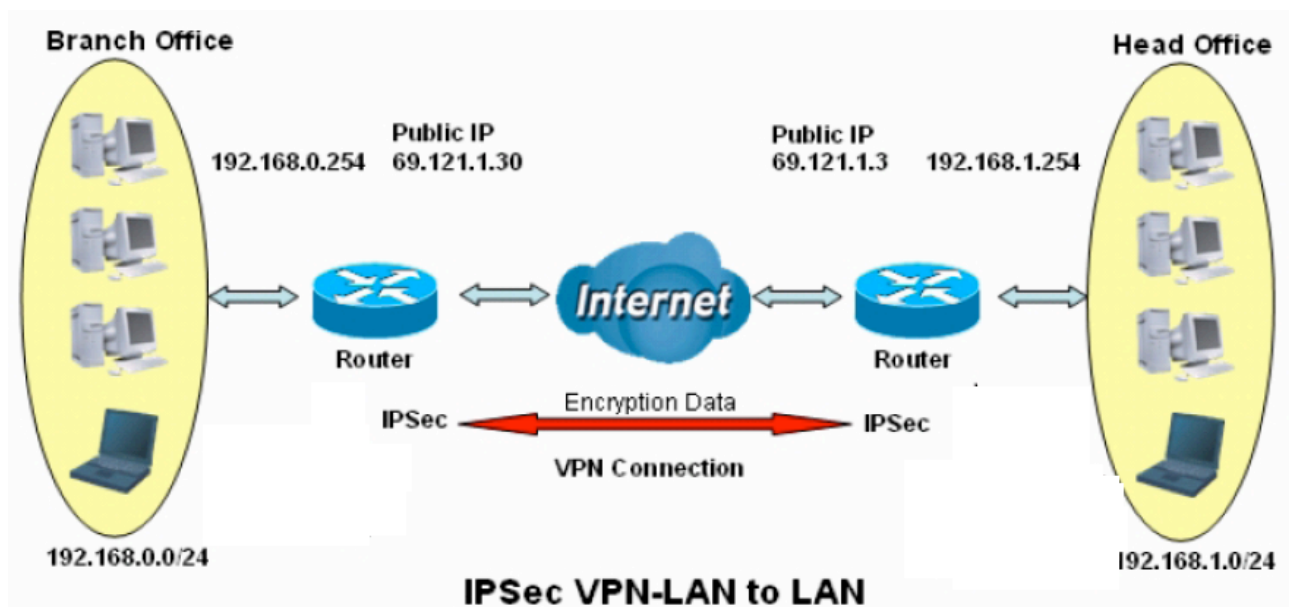
IPSec Lifetime: Specify the number of minutes that IPSec will stay active before new encryption and authentication key will be exchanged. Enter a value to negotiate and establish secure authentication. Default is 60 minutes (3600 seconds). A short time increases security by forcing the two parties to update the keys. However, every time when the VPN tunnel re- negotiates, access through the tunnel will be temporarily disconnected.

Examples:

1. LAN-to-LAN connection

Two routers want to setup a secure IPSec VPN tunnel

Note: The IPSec Settings shall be consistent between the two routers.



Head Office Side:

Setup details:

Item	Function		Description
1	Connection Name	H-to-B	Give a name for IPSec connection
2	Local Network		
	Subnet		Select Subnet
	IP Address	192.168.1.0	Head Office network
	Netmask	255.255.255.0	
3	Secure Gateway Address(Hostname)	69.121.1.30	IP address of the Branch office router (on WAN side)
4	Remote Network		
	Subnet		Select Subnet
	IP Address	192.168.0.0	Branch office network
	Netmask	255.255.255.0	
5	Proposal		
	Method	ESP	Security Plan
	Authentication	MD5	
	Encryption	3DES	
	Prefer Forward Security	MODP 1024(group2)	
	Pre-shared Key	123456	



▼ IPsec

IPsec Settings

L2TP over IPsec	<input type="checkbox"/> Enable				
Connection Name	H-to-B	WAN Interface	Default	IP Version	IPv4
Local Network	Subnet	IP Address	192.168.1.0	Netmask	255.255.255.0
Remote Security Gateway	69.121.1.30	<input type="checkbox"/> Anonymous			
Remote Network	Subnet	IP Address	192.168.0.0	Netmask	255.255.255.0
Key Exchange Method	IKE	IPsec Protocol	ESP		
Pre-Shared Key	123456				
Local ID Type	Default	ID Content			
Remote ID Type	Default	ID Content			

Phase 1

Mode	Main
Encryption Algorithm	3DES
Integrity Algorithm	MD5
DH Group	MODP1024(DH2)
SA Lifetime	480 Minute(s) [60-1440]

Phase 2

Encryption Algorithm	3DES
Integrity Algorithm	MD5
DH Group	None
IPsec Lifetime	60 Minute(s) [60-1440]
Keep Alive	DPD
Detection Interval	180 Second(s) [180-86400]
Idle Timeout	5 Consecutive times [5-99]
MTU	1500 (0 : Default)

Apply

Branch Office Side:

Setup details: the same operation as done in Head Office side

Item	Function		Description
1	Connection Name	B-to-H	Give a name for IPsec connection
2	Local Network		Branch Office network
	Subnet		
	IP Address	192.168.0.0	
	Netmask	255.255.255.0	
3	Remote Secure Gateway Address(Hostname)	69.121.1.3	IP address of the Head office router (on WAN side)
4	Remote Network		Head office network
	Subnet		
	IP Address	192.168.1.0	
	Netmask	255.255.255.0	
5	Proposal		Security Plan
	Method	ESP	
	Authentication	MD5	
	Encryption	3DES	
	Prefer Forward Security	MODP 1024(group2)	
	Pre-shared Key	123456	



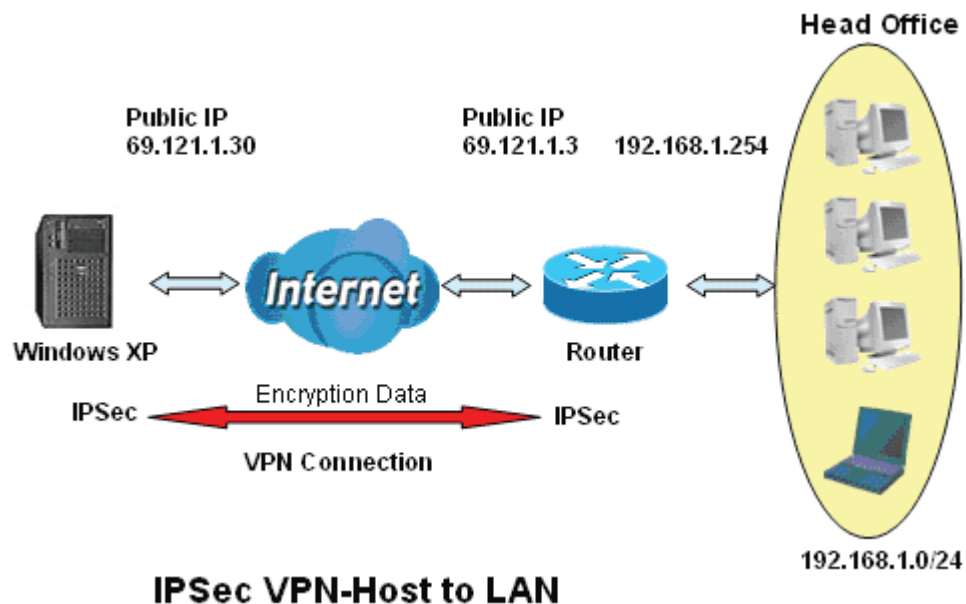
IPSec

IPSec Settings


L2TP over IPSec	<input type="checkbox"/> Enable				
Connection Name	B-to-H	WAN Interface	Default	IP Version	IPv4
Local Network	Subnet	IP Address	192.168.0.0	Netmask	255.255.255.0
Remote Security Gateway	69.121.1.3	<input type="checkbox"/> Anonymous			
Remote Network	Subnet	IP Address	192.168.1.0	Netmask	255.255.255.0
Key Exchange Method	IKE	IPsec Protocol	ESP		
Pre-Shared Key	123456				
Local ID Type	Default	ID Content			
Remote ID Type	Default	ID Content			
Phase 1					
Mode	Main				
Encryption Algorithm	3DES	Integrity Algorithm	MD5		
DH Group	MODP1024(DH2)	SA Lifetime	480 Minute(s) [60-1440]		
Phase 2					
Encryption Algorithm	3DES	Integrity Algorithm	MD5		
DH Group	None	IPsec Lifetime	60 Minute(s) [60-1440]		
Keep Alive	DPD				
Detection Interval	180 Second(s) [180-86400]	Idle Timeout	5 Consecutive times [5-99]		
MTU	1500 (0 : Default)				
<input type="button" value="Apply"/>					

1. Host to LAN

Router servers as VPN server, and host should install the IPSec client to connect to head office through IPSec VPN.



Item	Function		Description
1	Connection Name	Headoffice-to-Host	Give a name for IPSec connection
2	Local Network		Head Office network
	Subnet		
	IP Address	192.168.1.0	
	Netmask	255.255.255.0	
3	Remote Secure Gateway (Hostanme)	69.121.1.30	IP address of the Branch office router (on WAN side)
4	Remote Network		Host
	Single Address	69.121.1.30	
5	Proposal		Security Plan
	Method	ESP	
	Authentication	MD5	
	Encryption	3DES	
	Prefer Forward Security	MODP 1024(group2)	
	Pre-shared Key	123456	

VPN


IPSec

IPSec Settings

L2TP over IPSec

☐ Enable

Connection Name

Headoffice-to-H

WAN Interface

Default

IP Version

IPv4

Local Network

Subnet

IP Address

192.168.1.0

Netmask

255.255.255.0

Remote Security Gateway

69.121.1.30

☐ Anonymous

Remote Network

Single Address

IP Address

69.121.1.30

Netmask

255.255.255.0

Key Exchange Method

IKE

IPsec Protocol

ESP

Pre-Shared Key

123456

Local ID Type

Default

ID Content

Remote ID Type

Default

ID Content

Phase 1

Mode

Main

Encryption Algorithm

3DES

Integrity Algorithm

MD5

DH Group

MODP1024(DH2)

SA Lifetime

480

Minute(s) [60-1440]

Phase 2

Encryption Algorithm

3DES

Integrity Algorithm

MD5

DH Group

None

IPsec Lifetime

60

Minute(s) [60-1440]

Keep Alive

DPD

Detection Interval

180

Second(s) [180-86400]

Idle Timeout

5

Consecutive times [5-99]

MTU

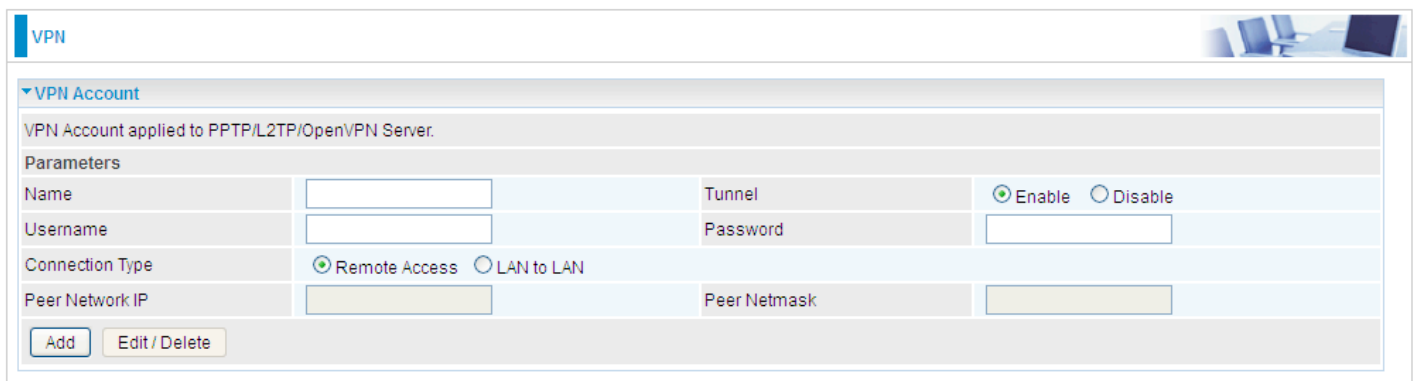
1500

(0 : Default)

Apply

VPN Account

PPTP and L2TP server share the same account database set in VPN Account page.



The interface shows a 'VPN Account' section with a sub-header 'VPN Account applied to PPTP/L2TP/OpenVPN Server.' Below this is a 'Parameters' section with several input fields and radio buttons. The fields are: Name, Username, Connection Type (with radio buttons for Remote Access and LAN to LAN), Peer Network IP, Tunnel (with radio buttons for Enable and Disable), Password, and Peer Netmask. There are 'Add' and 'Edit / Delete' buttons at the bottom.

Parameters			
Name	<input type="text"/>	Tunnel	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Username	<input type="text"/>	Password	<input type="password"/>
Connection Type	<input checked="" type="radio"/> Remote Access <input type="radio"/> LAN to LAN		
Peer Network IP	<input type="text"/>	Peer Netmask	<input type="text"/>

Name: A user-defined name for the connection.

Tunnel: Select **Enable** to activate the account. PPTP (L2TP) server is waiting for the client to connect to this account.

Username: Please input the username for this account.

Password: Please input the password for this account.

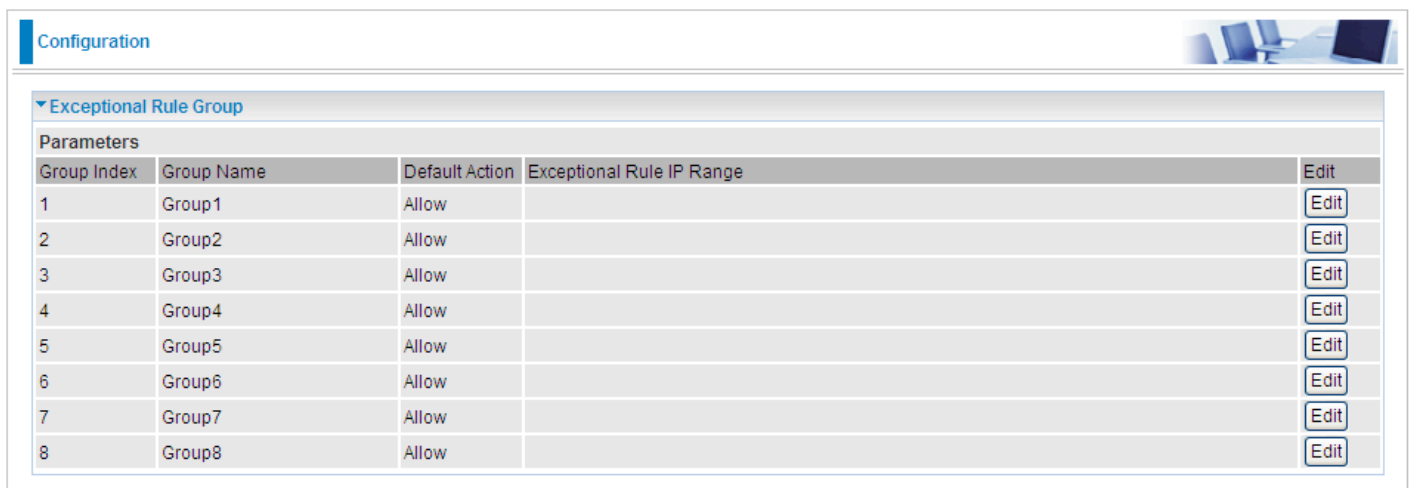
Connection Type: Select Remote Access for single user, Select LAN to LAN for remote gateway.

Peer Network IP: Please input the subnet IP for remote network.

Peer Netmask: Please input the Netmask for remote network.

Exceptional Rule Group

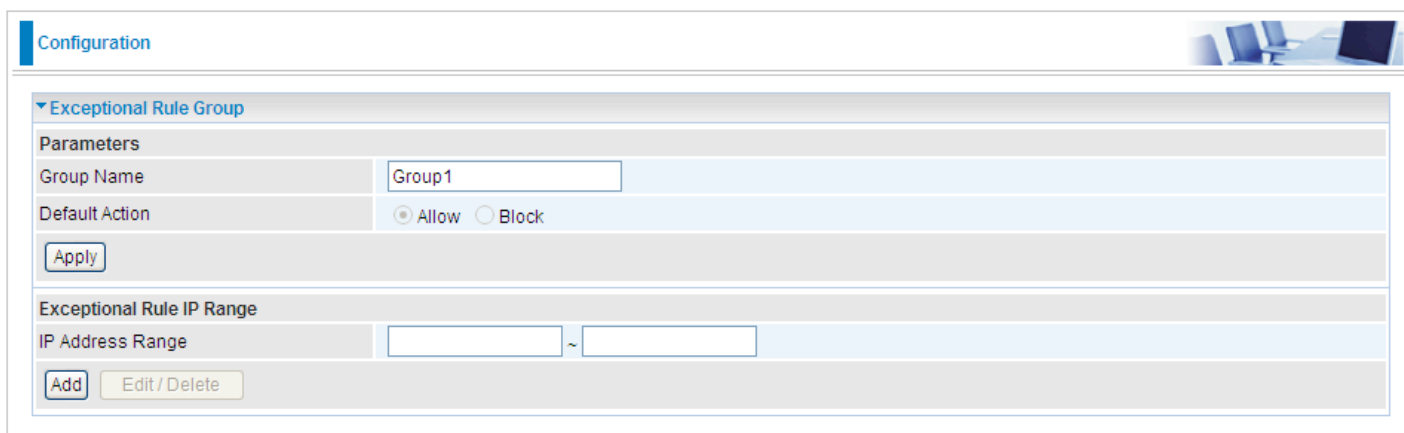
Exceptional Rule is dedicated to giving or blocking PPTP/L2TP server access to some specific IP or IPs(range). Users are allowed to set 8 different exceptional rule groups at most. In each group, user can add specific IP or IP range.



The interface shows a 'Configuration' section with a sub-header 'Exceptional Rule Group'. Below this is a table with 5 columns: Group Index, Group Name, Default Action, Exceptional Rule IP Range, and Edit. There are 8 rows, each representing a group. The 'Edit' column contains an 'Edit' button for each group.

Group Index	Group Name	Default Action	Exceptional Rule IP Range	Edit
1	Group1	Allow		<input type="button" value="Edit"/>
2	Group2	Allow		<input type="button" value="Edit"/>
3	Group3	Allow		<input type="button" value="Edit"/>
4	Group4	Allow		<input type="button" value="Edit"/>
5	Group5	Allow		<input type="button" value="Edit"/>
6	Group6	Allow		<input type="button" value="Edit"/>
7	Group7	Allow		<input type="button" value="Edit"/>
8	Group8	Allow		<input type="button" value="Edit"/>

Press **Edit** to set the exceptional IP (IP Range).



Configuration

▼ Exceptional Rule Group

Parameters

Group Name:

Default Action: ☒ Allow ☐ Block

Exceptional Rule IP Range

IP Address Range: ~

Default Action: Please first set the range to make “**Default Action**” setting available. Set “Allow” to ban the listed IP or IPs to access the PPTP and L2TP server.

Check “Block” to grant access to the listed IP or IPs to the PPTP and L2TP server.

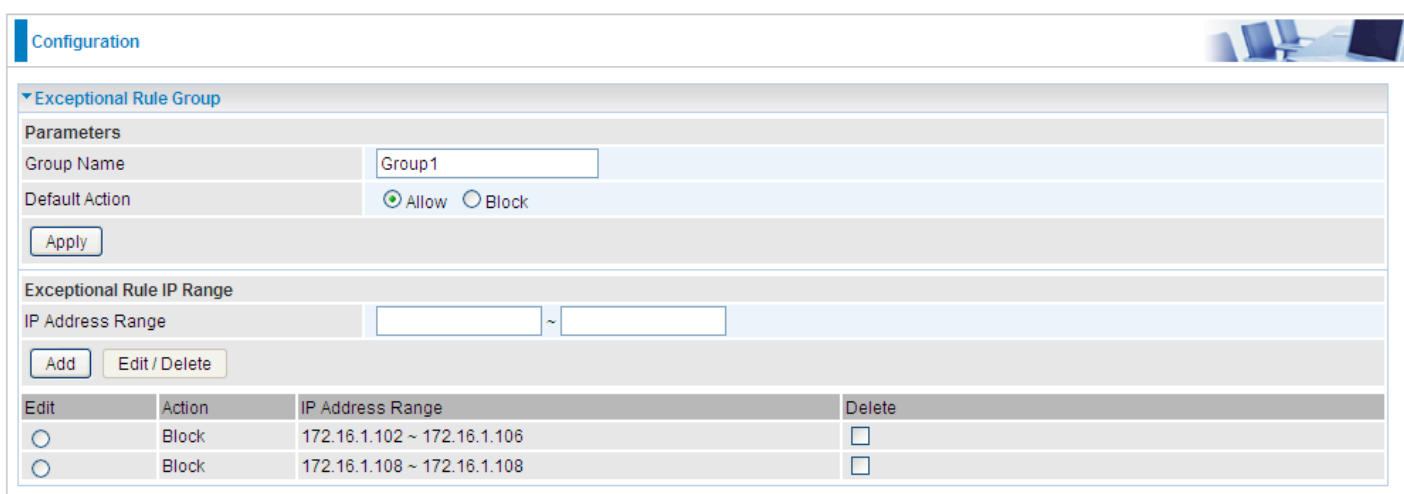
Apply: Press **Apply** button to apply the change.

Exceptional Rule Range

IP Address Range: Specify the IP address range; IPv4 address range can be supported.

Click **Add** to add the IP Range.

For instance, if user wants to block IP range of 172.16.1.102-172.16.1.106 from accessing your PPTP and L2TP server, you can add this IP range and valid it.



Configuration

▼ Exceptional Rule Group

Parameters

Group Name:

Default Action: ☒ Allow ☐ Block

Exceptional Rule IP Range

IP Address Range: ~

Edit	Action	IP Address Range	Delete
<input type="radio"/>	Block	172.16.1.102 ~ 172.16.1.106	<input type="checkbox"/>
<input type="radio"/>	Block	172.16.1.108 ~ 172.16.1.108	<input type="checkbox"/>

PPTP

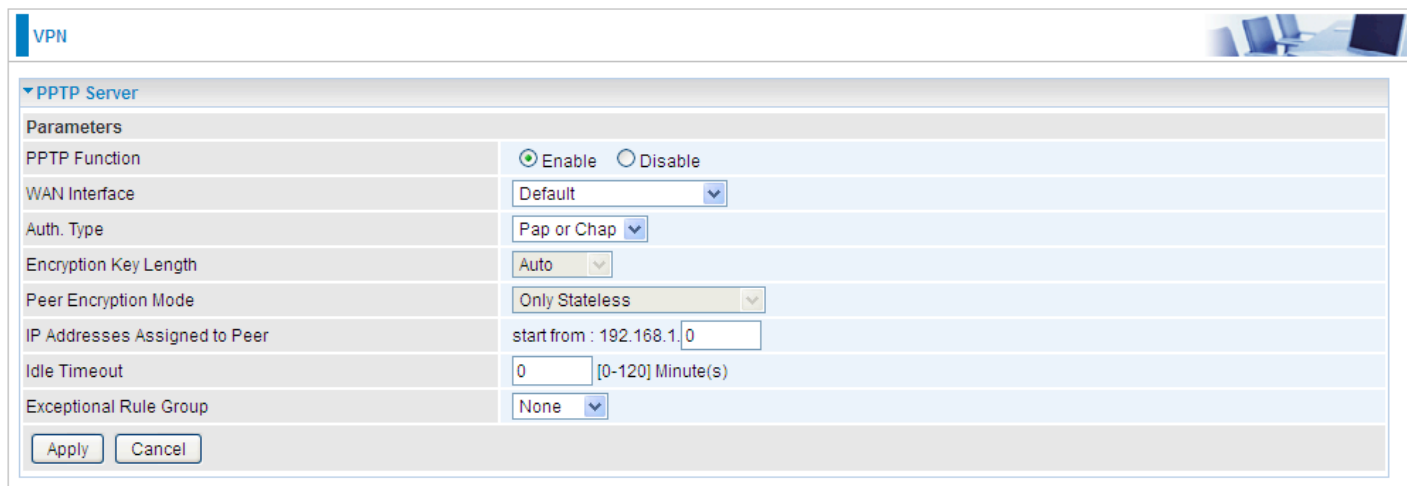
The **Point-to-Point Tunneling Protocol** (PPTP) is a Layer2 tunneling protocol for implementing virtual private networks through IP network. PPTP uses an enhanced GRE (Generic Routing Encapsulation) mechanism to provide a flow- and congestion-controlled encapsulated datagram service for carrying PPP packets.

In the Microsoft implementation, the tunneled PPP traffic can be authenticated with PAP, CHAP, Microsoft CHAP V1/V2 or EAP-TLS. The PPP payload is encrypted using Microsoft Point-to-Point Encryption (MPPE) when using MSCHAPv1/v2 or EAP-TLS.

Note: 4 sessions for Client and 4 sessions for Server respectively.

PPTP Server

In PPTP session, users can set the basic parameters (authentication, encryption, peer address, etc) for PPTP Server, and accounts in the next page of PPTP Account. They both constitute the PPTP Server setting.



PPTP Function: Select **Enable** to activate PPTP Server. **Disable** to deactivate PPTP Server function.

WAN Interface: Select the exact WAN interface configured for the tunnel. Select **Default** to use the now-working WAN interface for the tunnel.

Auth. Type: The authentication type, Pap or Chap, PaP, Chap and MS-CHAPv2. When using PAP, the password is sent unencrypted, whilst CHAP encrypts the password before sending, and also allows for challenges at different periods to ensure that an intruder has not replaced the client. When passed the authentication with MS-CHAPv2, the MPPE encryption is supported.

Encryption Key Length: The data can be encrypted by MPPE algorithm with 40 bits or 128 bits. Default is Auto, it is negotiated when establishing a connection. 128 bit keys provide stronger encryption than 40 bit keys.

Peer Encryption Mode: You may select “Only Stateless” or “Allow Stateless and Stateful” mode. The key will be changed every packet when you select Stateless mode.

IP Addresses Assigned to Peer: 192.168.1.x: please input the IP assigned range from 1~ 254.

Idle Timeout: Specify the time for remote peer to be disconnected without any activities, from 0~120 minutes.

Exceptional Rule Group: Select to grant or block access to a group of IPs to the PPTP server. See [Exceptional Rule Group](#). If there is not any restriction, select none.

Click **Apply** to submit your PPTP Server basic settings.

PPTP Client

PPTP client can help you dial-in the PPTP server to establish PPTP tunnel over Internet.

VPN

▼ PPTP Client

Parameters

Name	<input type="text"/>	WAN Interface	<div style="border: 1px solid #ccc; padding: 2px;">Default ▼</div>
Username	<input type="text"/>	Password	<input type="text"/>
Auth. Type	<div style="border: 1px solid #ccc; padding: 2px;">Pap or Chap ▼</div>	PPTP Server Address	<input type="text"/>
Connection Type	<input checked="" type="radio"/> Remote Access <input type="radio"/> LAN to LAN		Time to Connect
Peer Network IP	<input type="text"/>	Peer Netmask	<input type="text"/>

Add
Edit / Delete

Name: user-defined name for identification.

WAN Interface: Select the exact WAN interface configured for the tunnel. Select Default to use the now-working WAN interface for the tunnel.

Username: Enter the username provided by your VPN Server.

Password: Enter the password provided by your VPN Server.

Auth. Type: Default is Auto if you want the router to determine the authentication type to use, or else manually specify CHAP (Challenge Handshake Authentication Protocol) or PAP (Password Authentication Protocol) if you know which type the server is using (when acting as a client), or else the authentication type you want clients connecting to you to use (when acting as a server). When using PAP, the password is sent unencrypted, whilst CHAP encrypts the password before sending, and also allows for challenges at different periods to ensure that an intruder has not replaced the client.

PPTP Server Address: Enter the IP address of the PPTP server.

Connection Type: Select Remote Access for single user, Select LAN to LAN for remote gateway.

Time to Connect: Select Always to keep the connection always on, or Manual to connect manually any time.

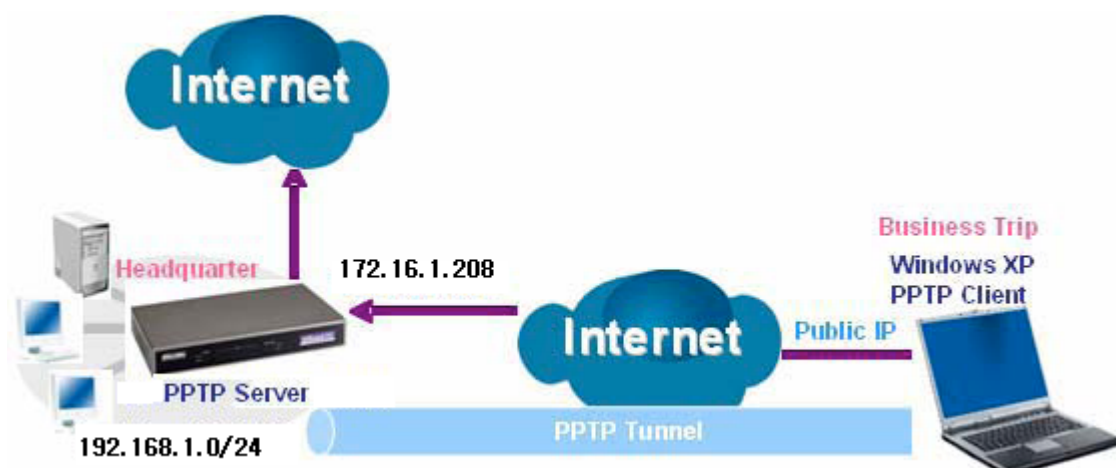
Peer Network IP: Please input the subnet IP for Server peer.

Peer Netmask: Please input the Netmask for server peer.

Click **Add** button to save your changes.

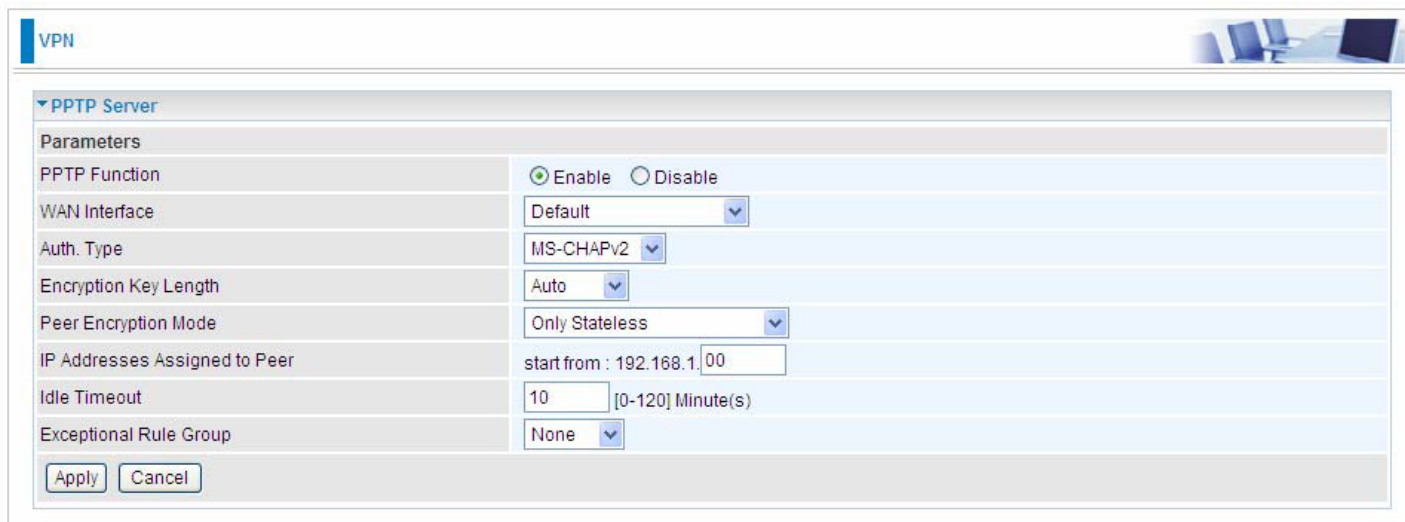
Example: PPTP Remote Access with Windows7

(Note: inside test with 172.16.1.208, just an example for illustration)



Server Side:

1. **Configuration > VPN > PPTP** and Enable the PPTP function, Click **Apply**.

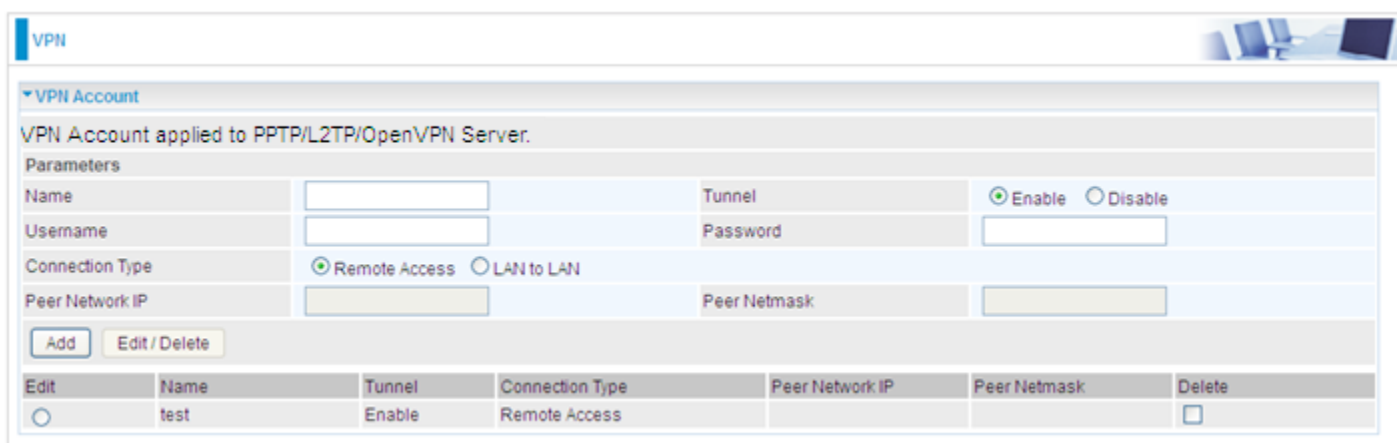


The screenshot shows the 'VPN' configuration page with the 'PPTP Server' section expanded. The 'Parameters' section contains the following settings:

Parameter	Value
PPTP Function	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
WAN Interface	Default
Auth. Type	MS-CHAPv2
Encryption Key Length	Auto
Peer Encryption Mode	Only Stateless
IP Addresses Assigned to Peer	start from : 192.168.1.00
Idle Timeout	10 [0-120] Minute(s)
Exceptional Rule Group	None

At the bottom of the configuration section are 'Apply' and 'Cancel' buttons.

2. Create a PPTP Account “test”.



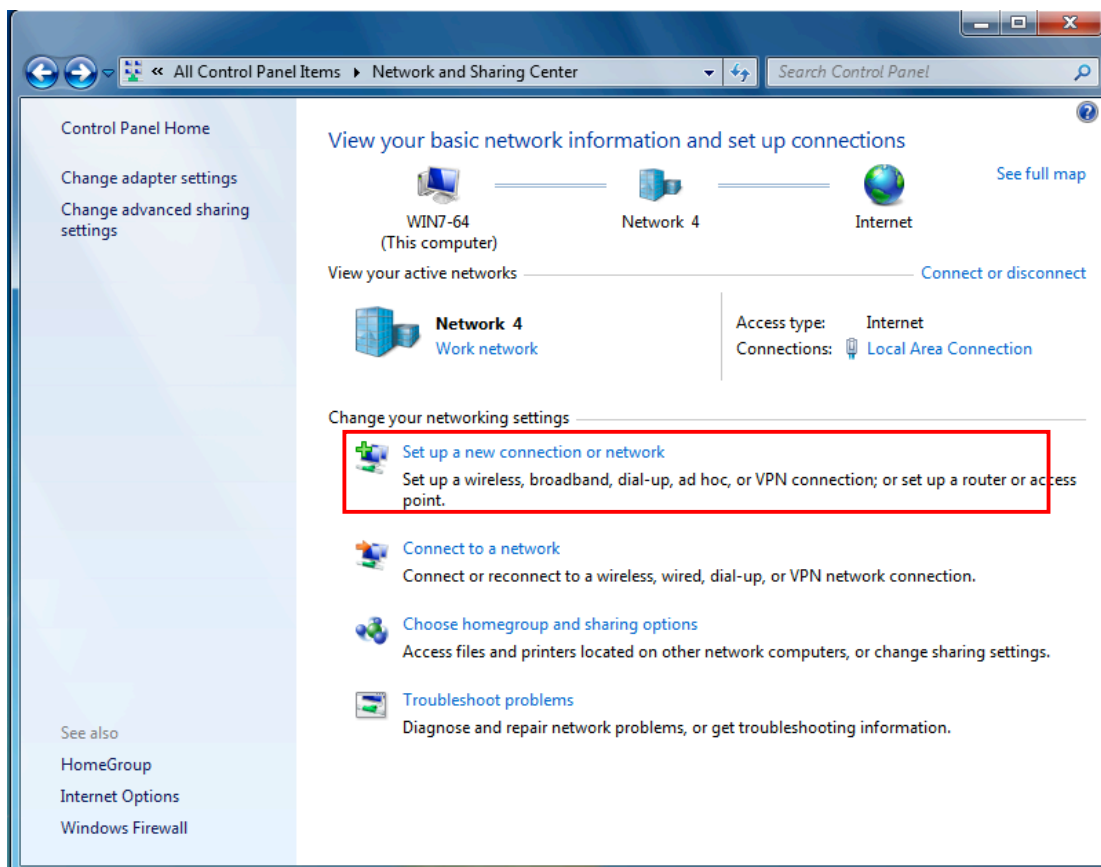
The screenshot shows the 'VPN Account' configuration page. It includes a section for 'VPN Account applied to PPTP/L2TP/OpenVPN Server.' with parameters for Name, Username, Connection Type (Remote Access selected), Peer Network IP, Peer Netmask, Tunnel (Enable selected), and Password. Below this is a table listing the configured accounts.

Edit	Name	Tunnel	Connection Type	Peer Network IP	Peer Netmask	Delete
<input type="radio"/>	test	Enable	Remote Access			<input type="checkbox"/>

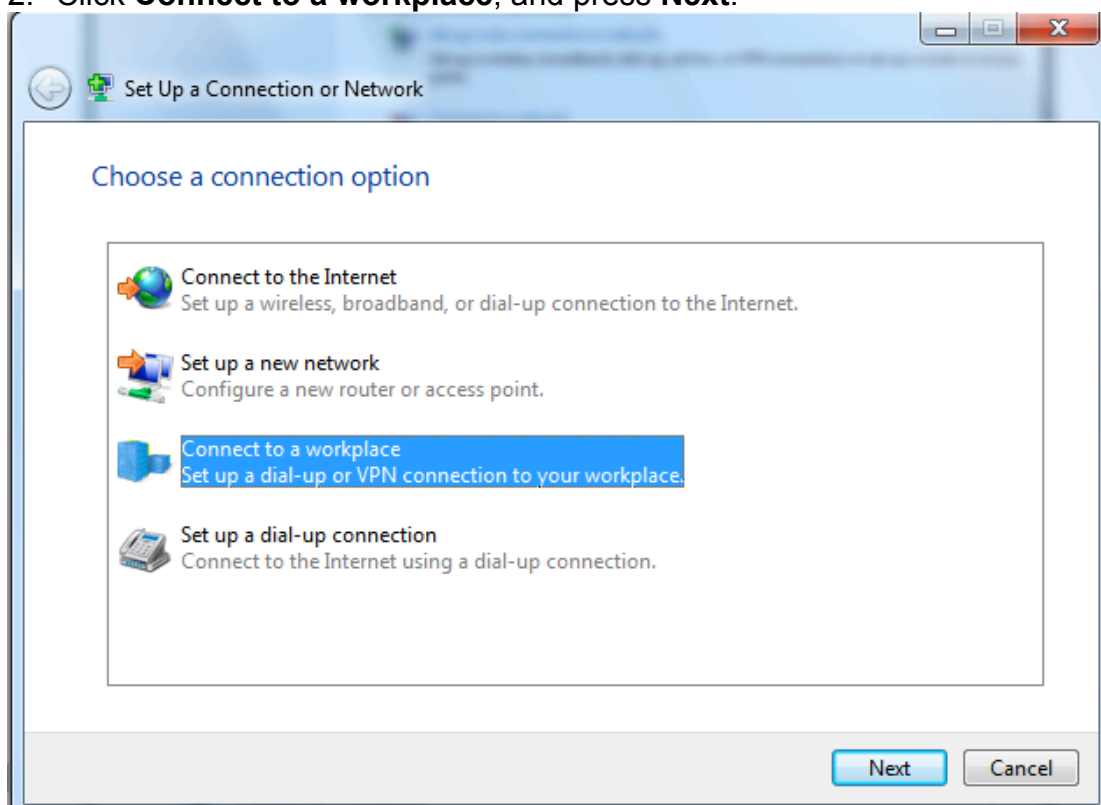
Buttons for 'Add' and 'Edit / Delete' are located above the table.

Client Side:

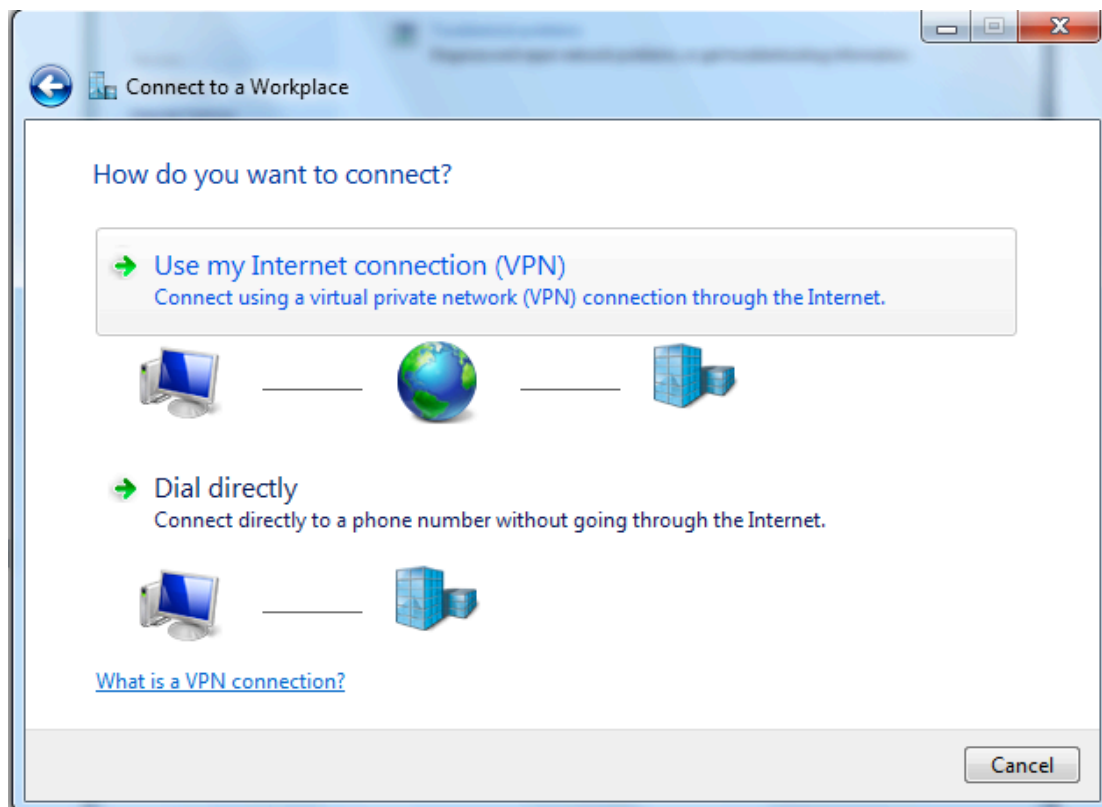
1. In Windows7 click **Start > Control Panel> Network and Sharing Center**, Click **Set up a new connection network**.



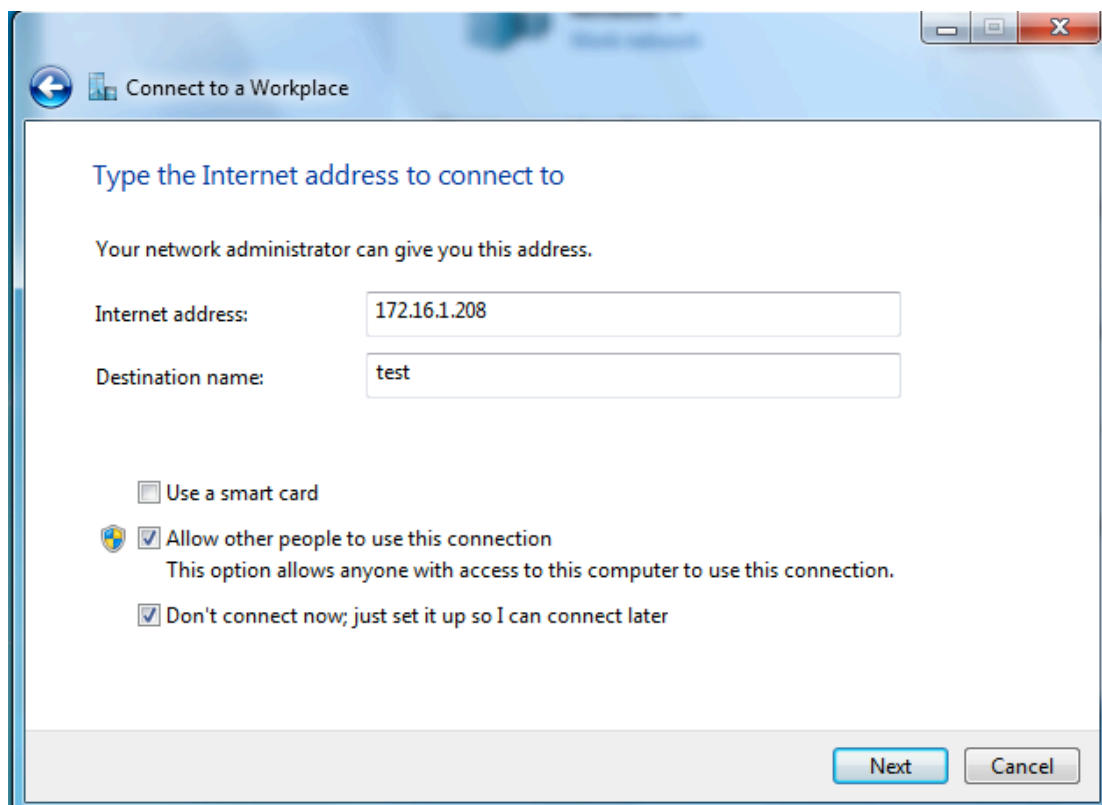
2. Click **Connect to a workplace**, and press **Next**.



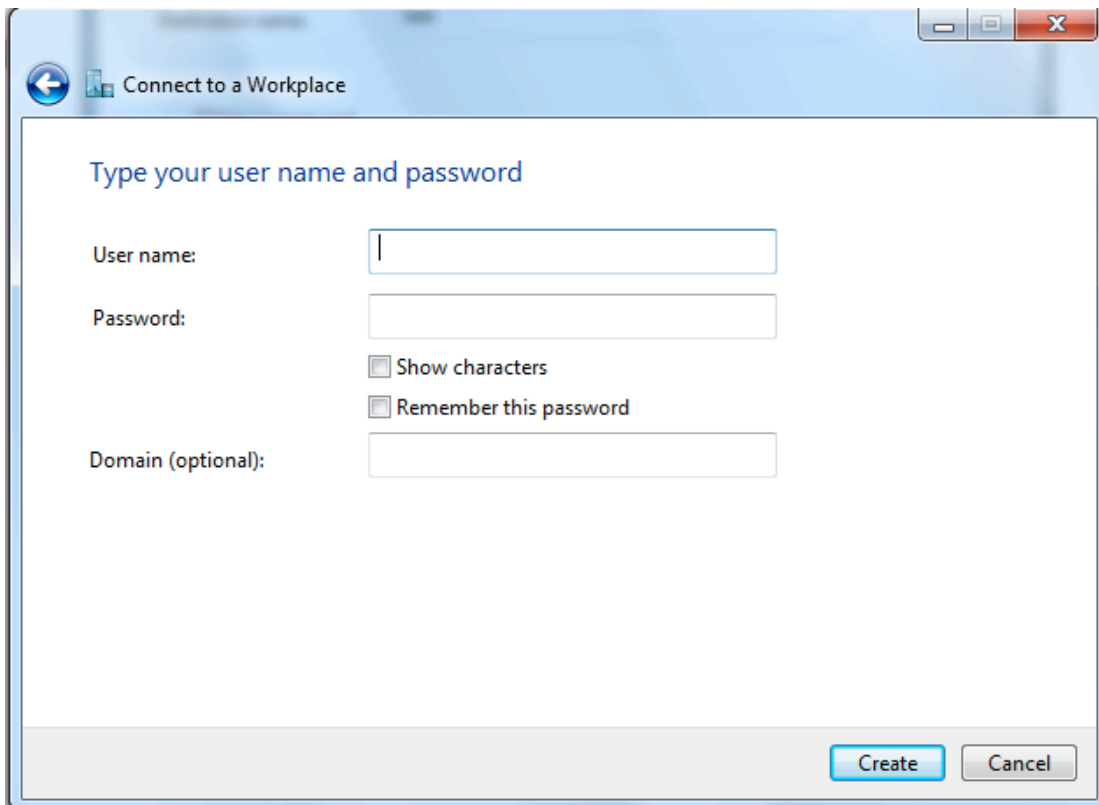
3. Select **Use my Internet connection (VPN)** and press **Next**.



4. Input **Internet address** and **Destination name** for this connection and press **Next**.



5. Input the account (**user name** and **password**) and press **Create**.



Connect to a Workplace

Type your user name and password

User name:

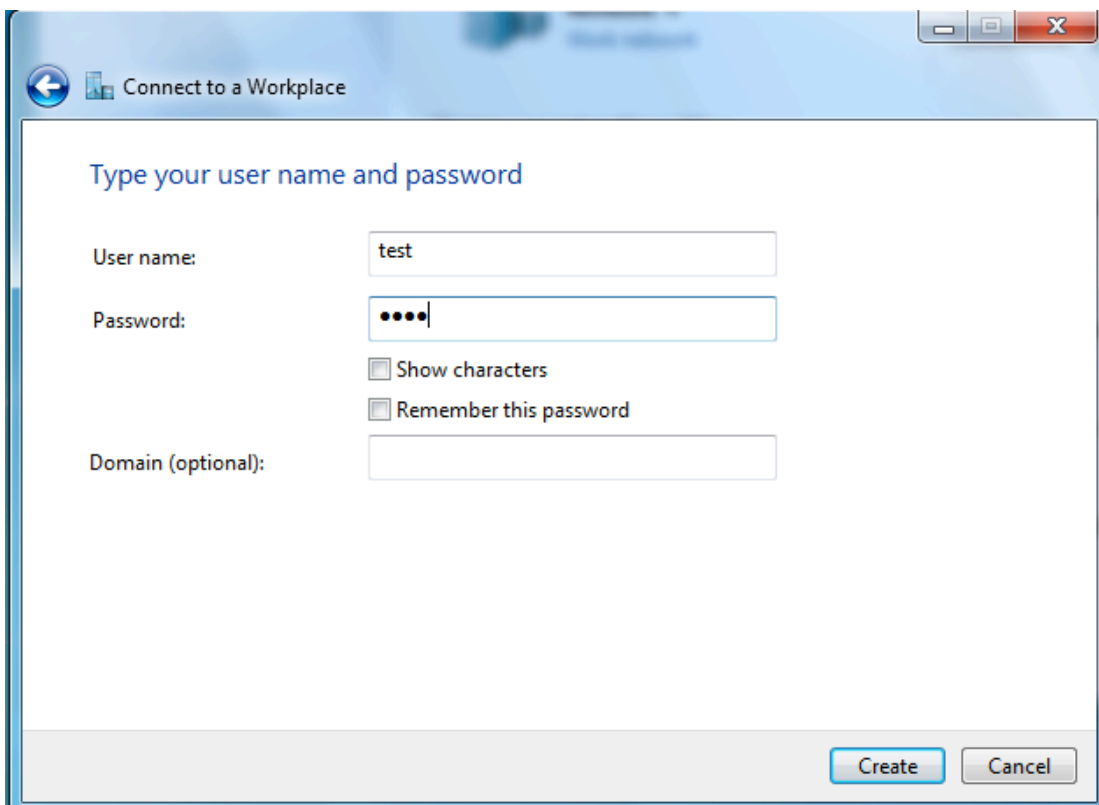
Password:

☐ Show characters

☐ Remember this password

Domain (optional):

Create Cancel



Connect to a Workplace

Type your user name and password

User name:

Password:

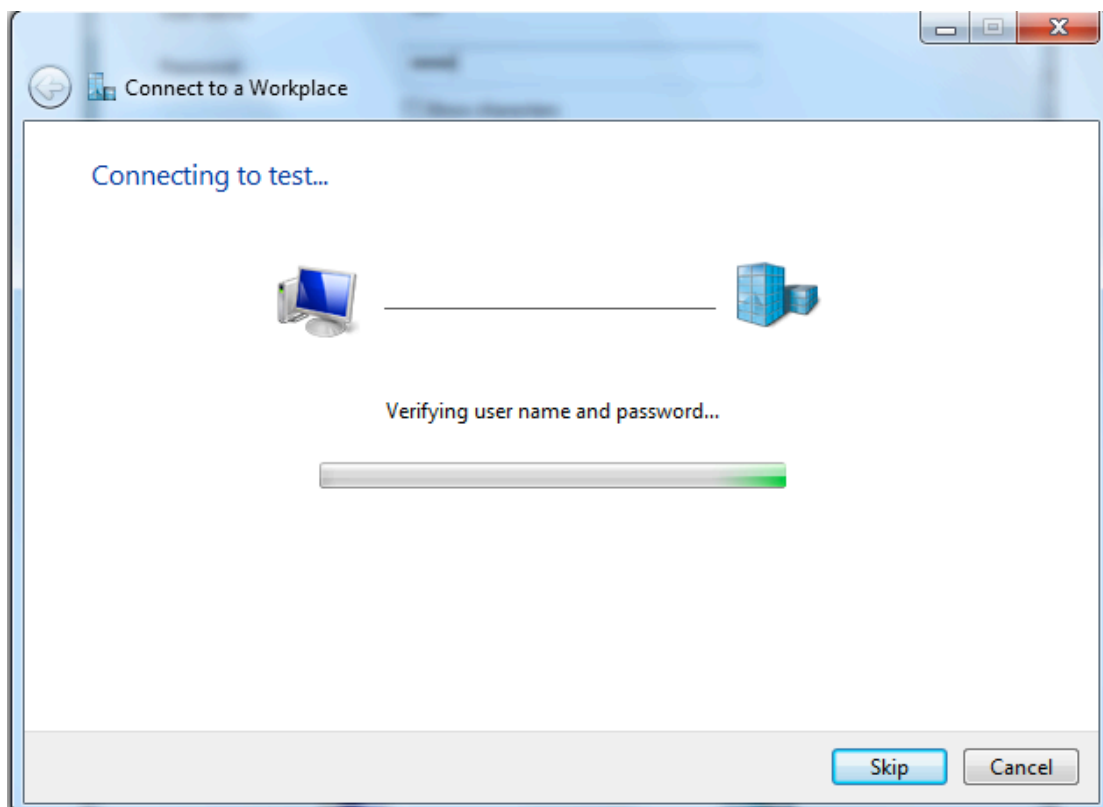
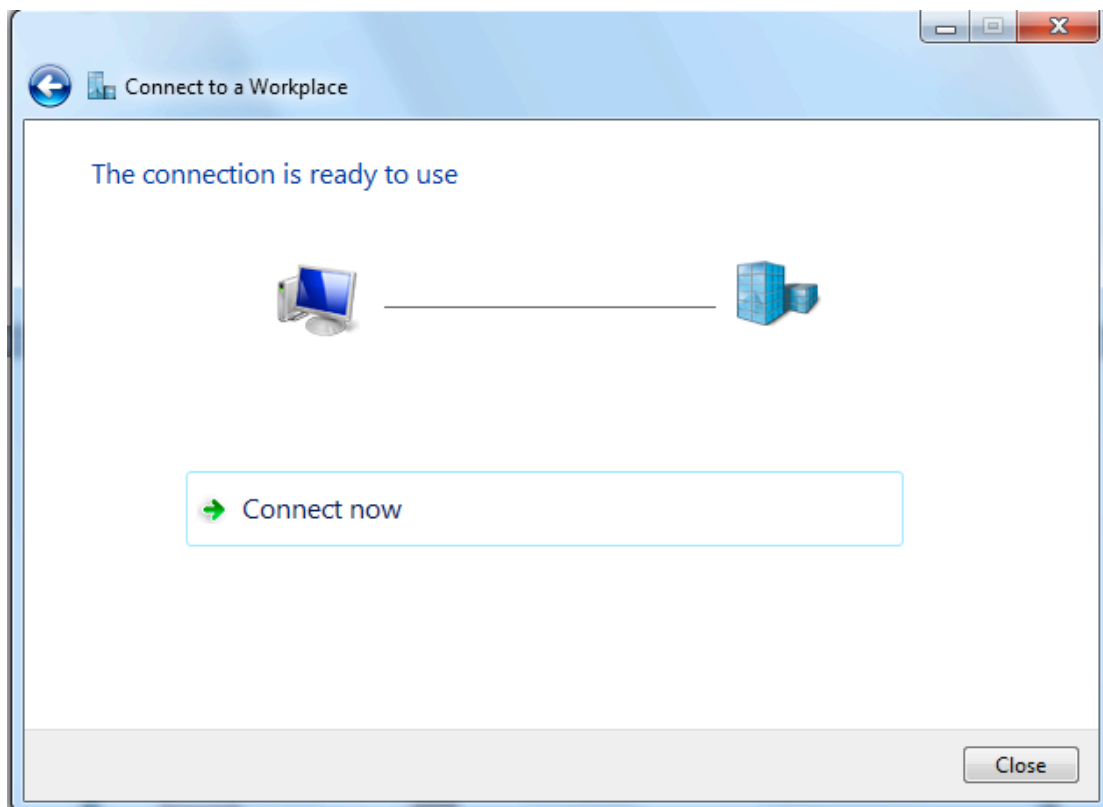
☐ Show characters

☐ Remember this password

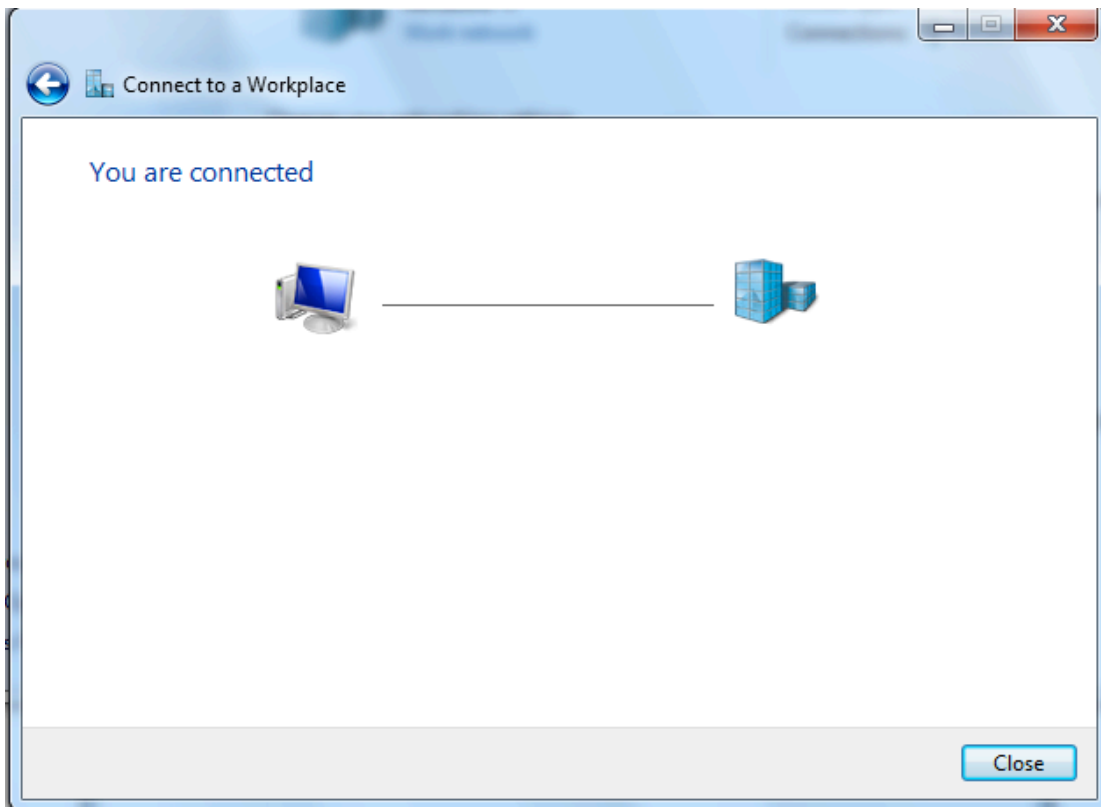
Domain (optional):

Create Cancel

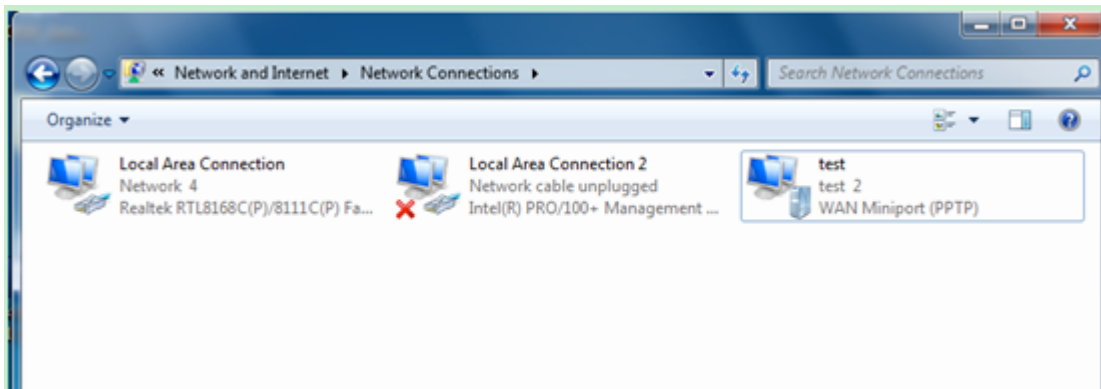
6. Connect to the server.

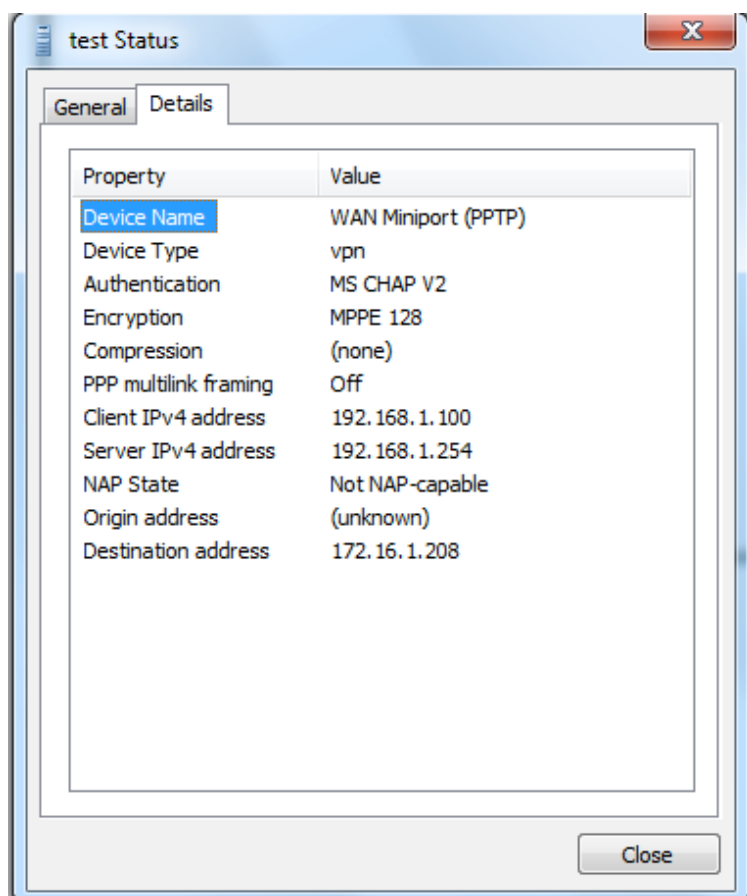
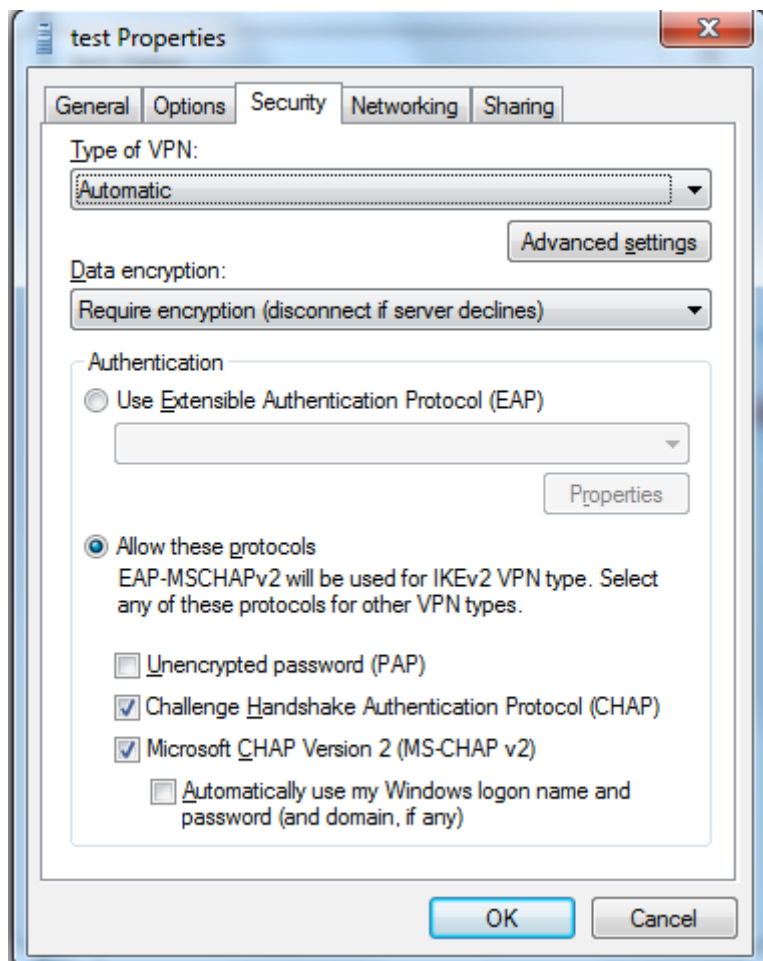


7. Successfully connected.



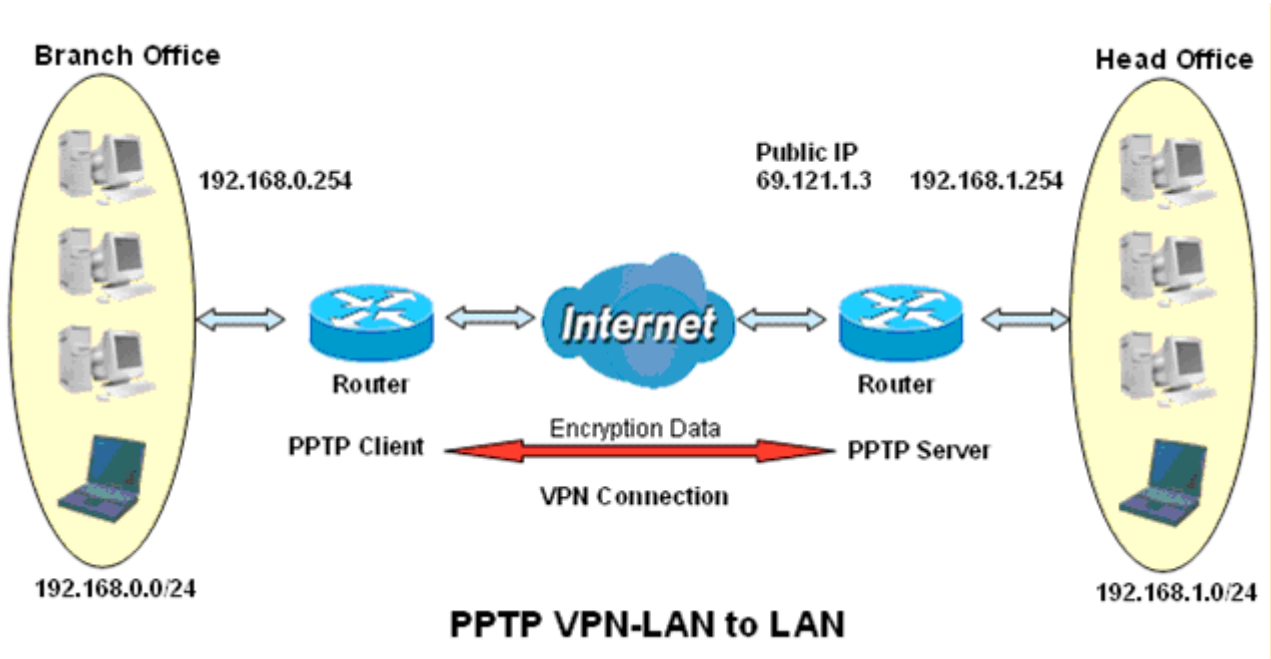
PS: You can also go to **Network Connections** shown below to check the detail of the connection. Right click "test" icon, and select "**Properties**" to change the security parameters (if the connection fails, users can go here to change the settings)





Example: Configuring a LAN-to-LAN PPTP VPN Connection

The branch office establishes a PPTP VPN tunnel with head office to connect two private networks over the Internet. The routers are installed in the head office and branch offices accordingly.



Server side: Head Office

VPN

PPTP Server

Parameters

PPTP Function

☒ Enable

☐ Disable

WAN Interface

Default

Auth. Type

MS-CHAPv2

Encryption Key Length

Auto

Peer Encryption Mode

Only Stateless

IP Addresses Assigned to Peer

start from : 192.168.1.00

Idle Timeout

10

[0-120] Minute(s)

Exceptional Rule Group

None

Apply

Cancel

The above is the common setting for PPTP Server, set as you like for authentication and encryption. The settings in Client side should be in accordance with settings in Server side.

Then the PPTP Account.

VPN

VPN Account

VPN Account applied to PPTP/L2TP/OpenVPN Server.

Parameters

Name	HO	Tunnel	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Username	HO	Password
Connection Type	<input type="radio"/> Remote Access <input checked="" type="radio"/> LAN to LAN		
Peer Network IP	192.168.0.0	Peer Netmask	255.255.255.0

Edit	Name	Tunnel	Connection Type	Peer Network IP	Peer Netmask	Delete
<input checked="" type="radio"/>	Ho	Enable	LAN to LAN	192.168.0.0	255.255.255.0	<input type="checkbox"/>

Client Side: Branch Office

The client user can set up a tunnel connecting to the PPTP server, and can also set the tunnel as the default route for all outgoing traffic.

VPN

PPTP Client

Parameters

Name	BO	WAN Interface	Default
Username	test	Password
Auth. Type	MS-CHAPv2	PPTP Server Address	69.121.1.3
Connection Type	<input type="radio"/> Remote Access <input checked="" type="radio"/> LAN to LAN		
Peer Network IP	192.168.1.0	Time to Connect	<input type="radio"/> Always <input checked="" type="radio"/> Manual
		Peer Netmask	255.255.255.0

Edit	Enable	Default Gateway	Name	Time to Connect	PPTP Server Address	Connection Type	Peer Network IP	Peer Netmask	Delete
<input checked="" type="radio"/>	<input type="checkbox"/>	<input type="checkbox"/>	BO	Manual	69.121.1.3	LAN to LAN	192.168.1.0	255.255.255.0	<input type="checkbox"/>

Note: users can see the “Default Gateway” item in the bar, and user can check to select the tunnel as the default gateway (default route) for traffic. If selected, all outgoing traffic will be forwarded to this tunnel and routed to the next hop.

L2TP

The **Layer 2 Tunneling Protocol (L2TP)** is a Layer2 tunneling protocol for implementing virtual private networks.

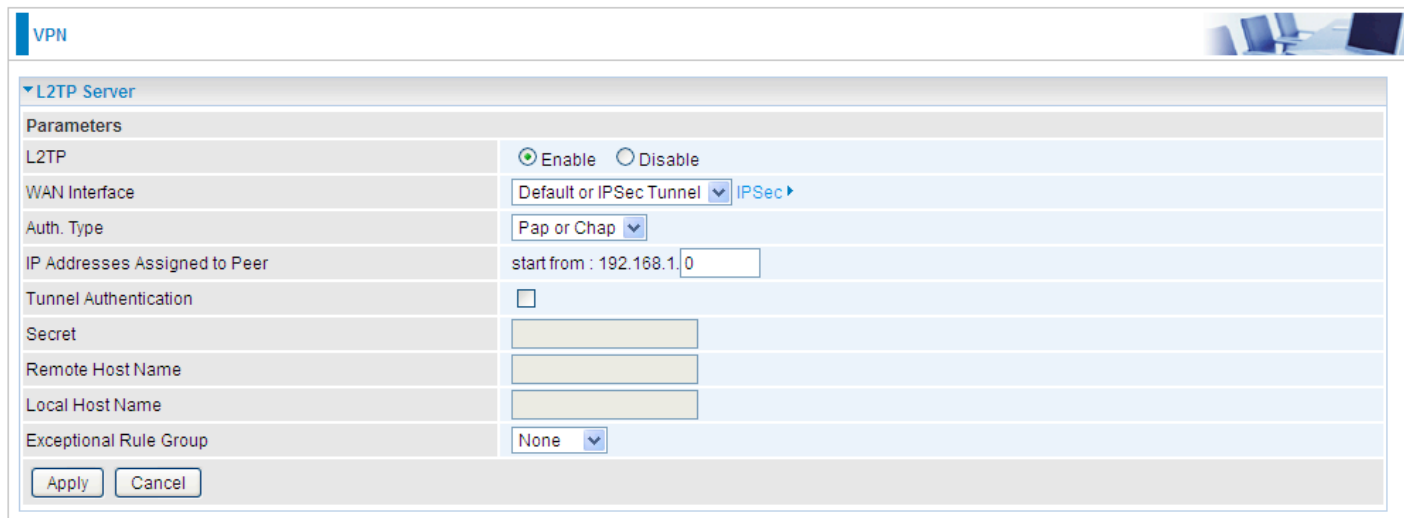
L2TP does not provide confidentiality or strong authentication by itself. IPsec is often used to secure L2TP packets by providing confidentiality, authentication and integrity. The combination of these two protocols is generally known as L2TP/IPsec.

In L2TP section, both pure L2TP and L2TP/IPSec are supported. Users can choose your preferable option for your own needs.

Note: 4 sessions for Client and only one for Server respectively.

L2TP Server

In L2TP session, users can set the basic parameters (authentication, encryption, peer address, etc) for L2TP Server, and accounts in the page of VPN Account. They both constitute the complete L2TP Server settings.



L2TP: Select **Enable** to activate L2TP Server. **Disable** to deactivate L2TP Server.

WAN Interface: Select the exact WAN interface configured as source for the tunnel. Select different interfaces, you will decide whether to use L2TP over IPsec or the pure L2TP.

- ① **L2TP over IPsec**, Select “Default or IPsec Tunnel” only when there is IPsec for L2TP rule in place.
- ① **Pure L2TP**, Select Default (there is no IPsec for L2TP in place) or other interface to activate the pure L2TP.

Auth. Type: The authentication type, Pap or Chap, PaP, Chap. When using PAP, the password is sent unencrypted, whilst CHAP encrypts the password before sending, and also allows for challenges at different periods to ensure that an intruder has not replaced the client.

IP Addresses Assigned to Peer: 192.168.1.x: please input the IP assigned range from 1~ 254.

Tunnel Authentication: Select whether to enable L2TP tunnel authentication. Enable it if needed and set the same in the client side.

Secret: Enter the secretly pre-shared password for tunnel authentication.

Remote Host Name: Enter the remote host name (of peer) featuring the destination of the L2TP tunnel.

Local Host Name: Enter the local host name featuring the source of the L2TP tunnel.

Exceptional Rule Group: Select to grant or block access to a group of IPs to the L2TP server. See [Exceptional Rule Group](#). If there is not any restriction, select none.

Click **Apply** to submit your L2TP Server basic settings.

L2TP Client

L2TP client can help you dial-in the L2TP server to establish L2TP tunnel over Internet.



VPN

L2TP Client

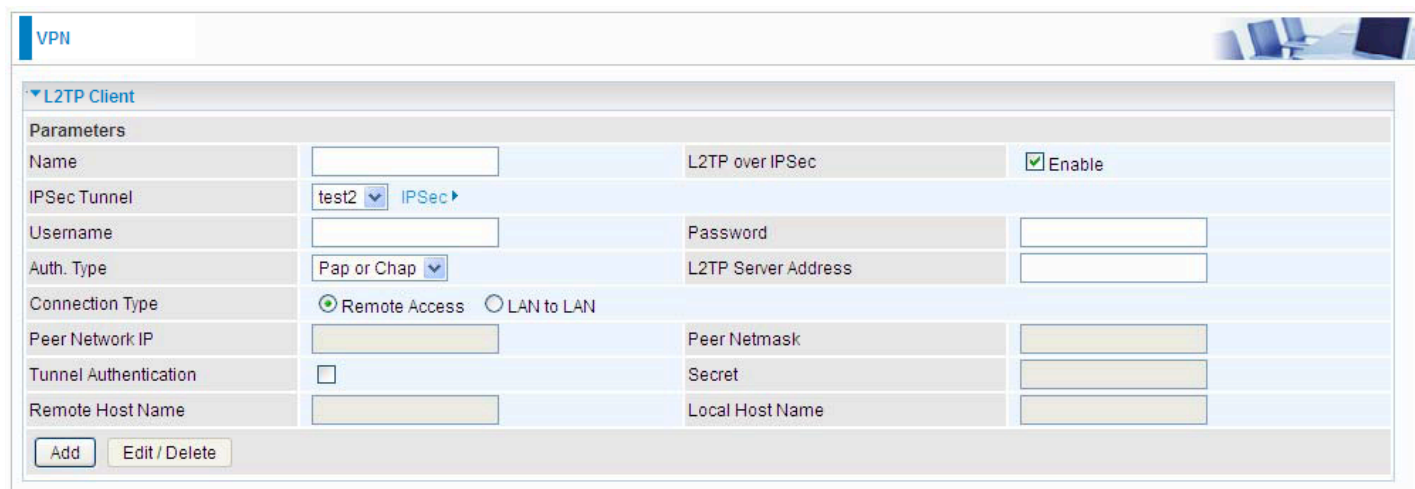
Parameters

Name	<input type="text"/>	L2TP over IPsec	<input type="checkbox"/> Enable
WAN Interface	Default		
Username	<input type="text"/>	Password	<input type="text"/>
Auth. Type	Pap or Chap	L2TP Server Address	<input type="text"/>
Connection Type	<input checked="" type="radio"/> Remote Access <input type="radio"/> LAN to LAN		
Peer Network IP	<input type="text"/>	Peer Netmask	<input type="text"/>
Tunnel Authentication	<input type="checkbox"/>	Secret	<input type="text"/>
Remote Host Name	<input type="text"/>	Local Host Name	<input type="text"/>

Name: user-defined name for identification.

L2TP over IPsec: If your L2TP server has used L2TP over IPsec feature, please enable this item. under this circumstance, client and server communicate using L2TP over IPsec.

① Enable



VPN

L2TP Client

Parameters

Name	<input type="text"/>	L2TP over IPsec	<input checked="" type="checkbox"/> Enable
IPsec Tunnel	test2	IPsec	
Username	<input type="text"/>	Password	<input type="text"/>
Auth. Type	Pap or Chap	L2TP Server Address	<input type="text"/>
Connection Type	<input checked="" type="radio"/> Remote Access <input type="radio"/> LAN to LAN		
Peer Network IP	<input type="text"/>	Peer Netmask	<input type="text"/>
Tunnel Authentication	<input type="checkbox"/>	Secret	<input type="text"/>
Remote Host Name	<input type="text"/>	Local Host Name	<input type="text"/>

IPsec Tunnel: Select the appropriate IPsec for L2TP rule configured for the L2TP Client.

Username: Enter the username provided by your L2TP Server.

Password: Enter the password provided by your L2TP Server.

Auth. Type: Default is Pap or CHap if you want the router to determine the authentication type to use, or else manually specify CHAP (Challenge Handshake Authentication Protocol) or PAP (Password Authentication Protocol) if you know which type the server is using. When using PAP, the password is sent unencrypted, whilst CHAP encrypts the password before sending, and also allows for challenges at different periods to ensure that an intruder has not replaced the client.

L2TP Server Address: Enter the IP address of the L2TP server.

Connection Type: Select Remote Access for single user, Select LAN to LAN for remote gateway.

Peer Network IP: Please input the subnet IP for Server.

Peer Netmask: Please input the Netmask for Server.

Tunnel Authentication: Select whether to enable L2TP tunnel authentication, if the server side enables this feature, please follow.

Secret: Enter the set secret password in the server side.

Remote Host Name: Enter the remote host name featuring the destination of the L2TP tunnel.

Local Host Name: Enter the local host name featuring the source of the L2TP tunnel.

Click **Add** button to save your changes.

❶ Disable



The screenshot shows the 'VPN' configuration page with a sub-section for 'L2TP Client'. Under 'Parameters', there are several fields: 'Name' (text input), 'WAN Interface' (dropdown menu showing 'Default'), 'Username' (text input), 'Auth. Type' (dropdown menu showing 'Pap or Chap'), 'Connection Type' (radio buttons for 'Remote Access' and 'LAN to LAN'), 'Peer Network IP' (text input), 'Tunnel Authentication' (checkbox), 'Remote Host Name' (text input), 'L2TP over IPSec' (checkbox labeled 'Enable'), 'Password' (text input), 'L2TP Server Address' (text input), 'Peer Netmask' (text input), 'Secret' (text input), and 'Local Host Name' (text input). At the bottom of the form are 'Add' and 'Edit / Delete' buttons.

WAN Interface: Select the exact WAN interface configured for the tunnel. Select Default to use the now-working WAN interface for the tunnel. Under this circumstance, client and server communicate through pure L2TP server.

Username: Enter the username provided by your L2TP Server.

Password: Enter the password provided by your L2TP Server.

Auth. Type: Default is Pap or CHap if you want the router to determine the authentication type to use, or else manually specify CHAP (Challenge Handshake Authentication Protocol) or PAP (Password Authentication Protocol) if you know which type the server is using. When using PAP, the password is sent unencrypted, whilst CHAP encrypts the password before sending, and also allows for challenges at different periods to ensure that an intruder has not replaced the client.

L2TP Server Address: Enter the IP address of the L2TP server.

Connection Type: Select Remote Access for single user, Select LAN to LAN for remote gateway.

Peer Network IP: Please input the subnet IP for Server.

Peer Netmask: Please input the Netmask for server.

Tunnel Authentication: Select whether to enable L2TP tunnel authentication, if the server side enables this feature, please follow.

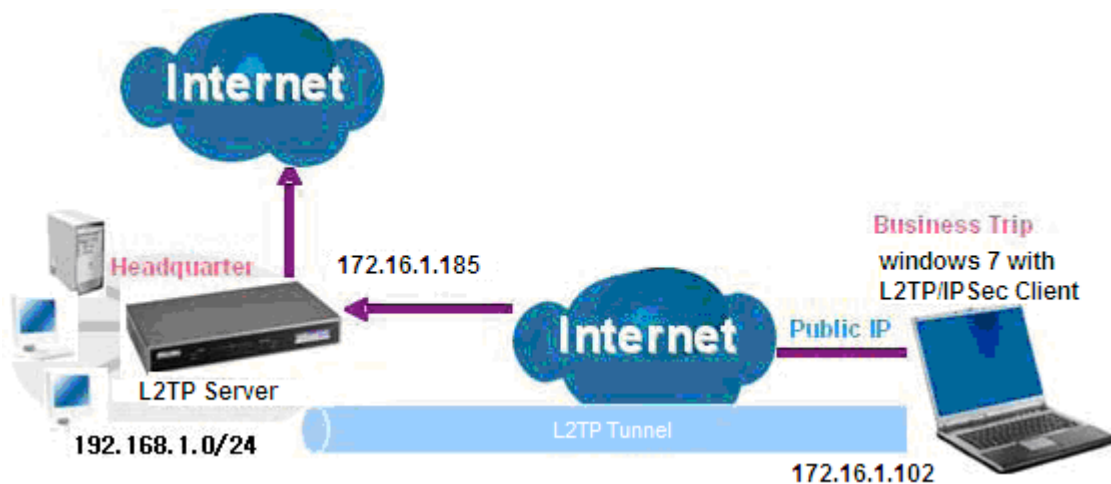
Secret: Enter the set secret password in the server side.

Remote Host Name: Enter the remote host name featuring the destination of the L2TP tunnel.

Local Host Name: Enter the local host name featuring the source of the L2TP tunnel.

Click **Add** button to save your changes.

Example: L2TP over IPSec Remote Access with Windows7
(Note: inside test with 172.16.1.185, just an example for illustration)



Server Side:

1. Configuration > VPN > L2TP and Enable the L2TP function, Click **Apply**.

VPN

L2TP Server

Parameters

L2TP ☒ Enable ☐ Disable

WAN Interface [IPSec >](#)

Auth. Type

IP Addresses Assigned to Peer start from : 192.168.1.10

Tunnel Authentication ☐

Secret

Remote Host Name

Local Host Name

Exceptional Rule Group

The IPSec for L2TP rule

VPN

IPSec

IPSec Settings

L2TP over IPSec ☒ Enable

Connection Name WAN Interface IP Version

Remote Security Gateway ☒ Anonymous

Key Exchange Method IPsec Protocol

Pre-Shared Key

2. Create a L2TP Account “test1”.

VPN Account applied to PPTP/L2TP/OpenVPN Server.

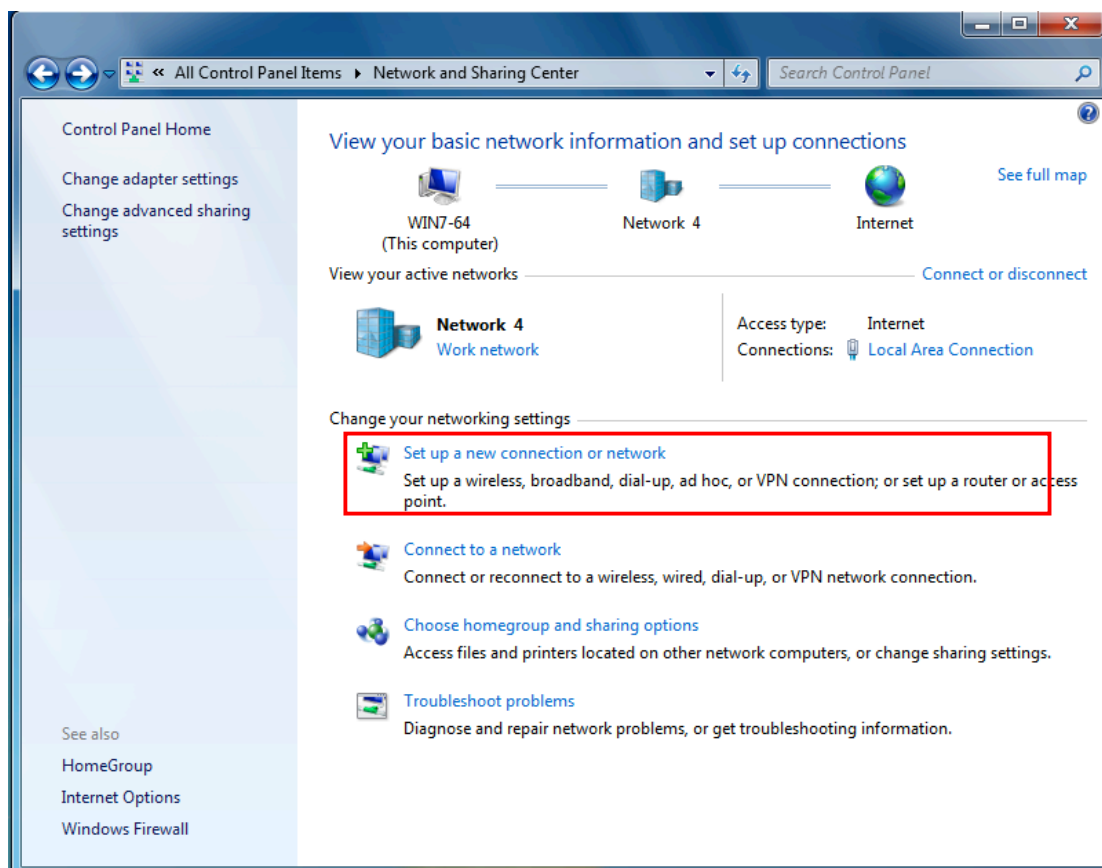
Parameters

Name	test1	Tunnel	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Username	test1	Password	*****
Connection Type	<input checked="" type="radio"/> Remote Access <input type="radio"/> LAN to LAN		
Peer Network IP		Peer Netmask	

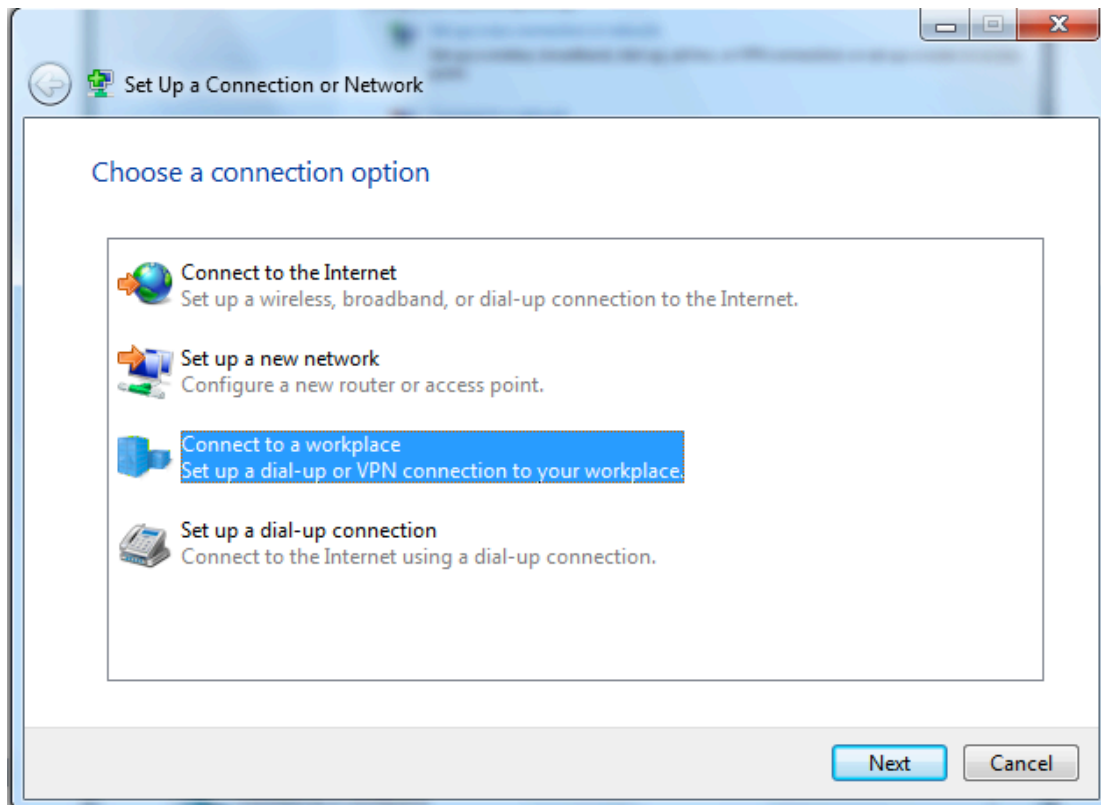
Edit	Name	Tunnel	Connection Type	Peer Network IP	Peer Netmask	Delete
<input checked="" type="checkbox"/>	test1	Enable	Remote Access			<input type="checkbox"/>

Client Side:

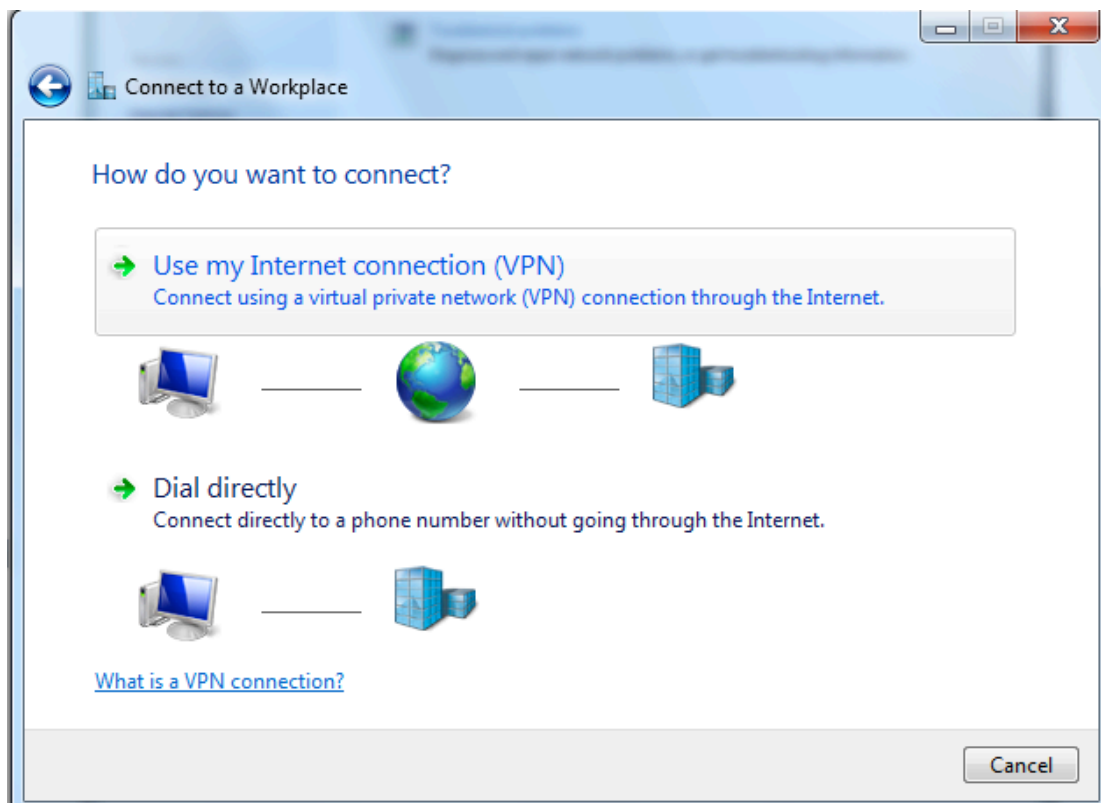
1. In Windows7 click **Start > Control Panel> Network and Sharing Center**, Click **Set up a new connection network**.



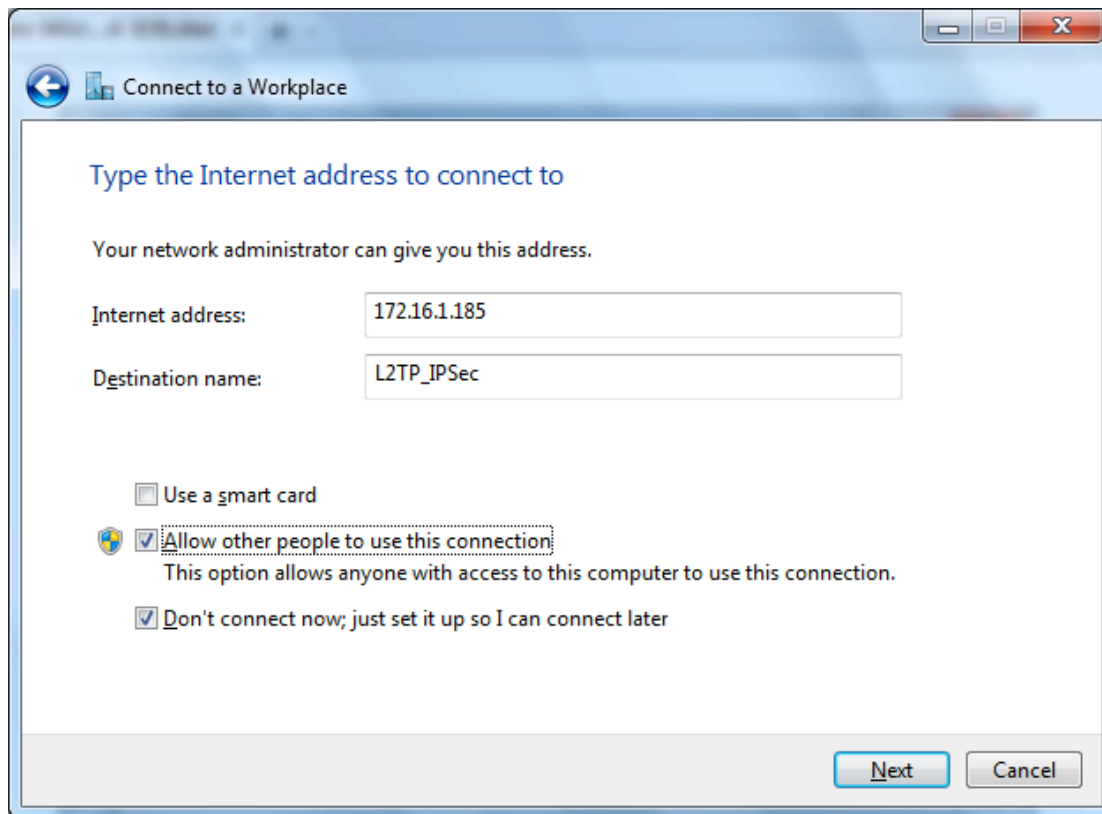
2. Click **Connect to a workplace**, and press **Next**.



3. Select **Use my Internet connection (VPN)** and press **Next**.



4. Input **Internet address** and **Destination name** for this connection and press **Next**.



The screenshot shows a Windows XP-style dialog box titled "Connect to a Workplace". The main heading is "Type the Internet address to connect to". Below this, a message states: "Your network administrator can give you this address." There are two text input fields: "Internet address:" containing "172.16.1.185" and "Destination name:" containing "L2TP_IPSec". Below the fields are three checkboxes: "Use a smart card" (unchecked), "Allow other people to use this connection:" (checked, with a tooltip that says "This option allows anyone with access to this computer to use this connection."), and "Don't connect now; just set it up so I can connect later" (checked). At the bottom right are "Next" and "Cancel" buttons.

Connect to a Workplace

Type the Internet address to connect to

Your network administrator can give you this address.

Internet address: 172.16.1.185

Destination name: L2TP_IPSec

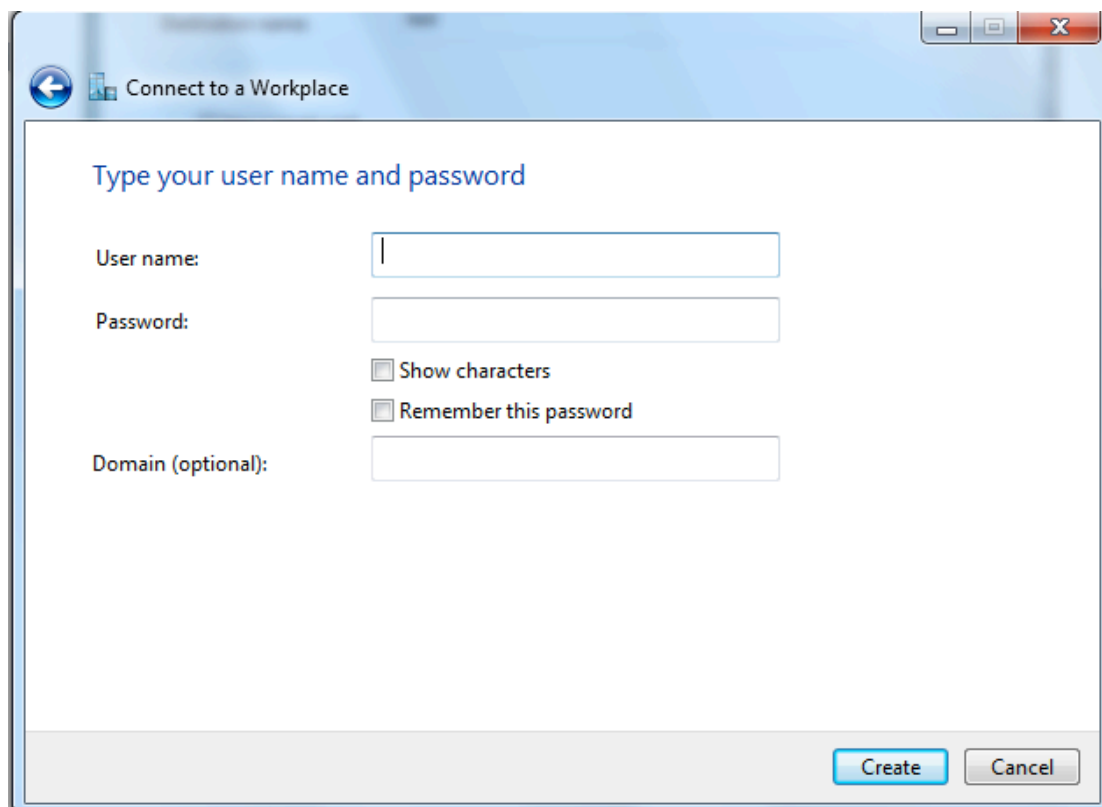
☐ Use a smart card

☒ Allow other people to use this connection:
This option allows anyone with access to this computer to use this connection.

☒ Don't connect now; just set it up so I can connect later

Next Cancel

5. Input the account (**user name** and **password**) and press **Create**.



The screenshot shows the same "Connect to a Workplace" dialog box, but at step 5. The heading is "Type your user name and password". There are three text input fields: "User name:", "Password:", and "Domain (optional):". Below the "Password:" field are two checkboxes: "Show characters" (unchecked) and "Remember this password" (unchecked). At the bottom right are "Create" and "Cancel" buttons.

Connect to a Workplace

Type your user name and password

User name:

Password:

☐ Show characters

☐ Remember this password

Domain (optional):

Create Cancel

Connect to a Workplace

Type your user name and password

User name: test1

Password: •••••

☐ Show characters

☐ Remember this password

Domain (optional):

Create Cancel

6. Connection created. Press **Close**.

Connect to a Workplace

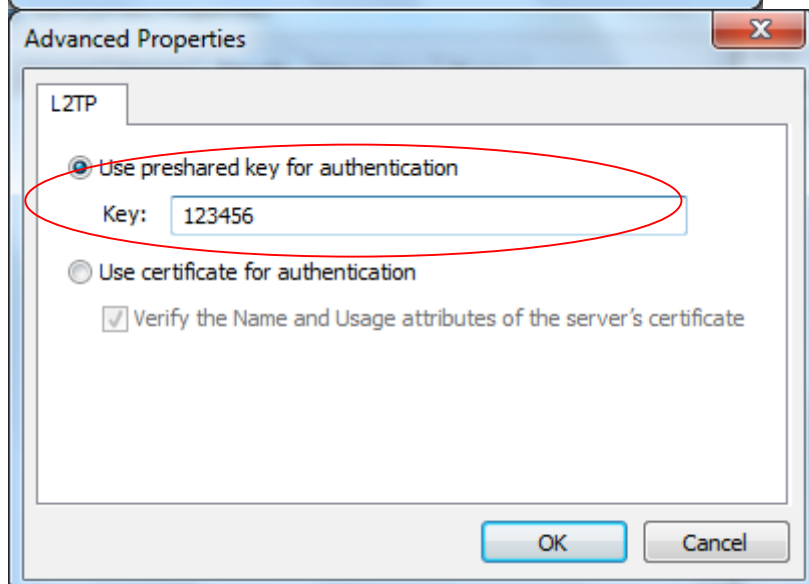
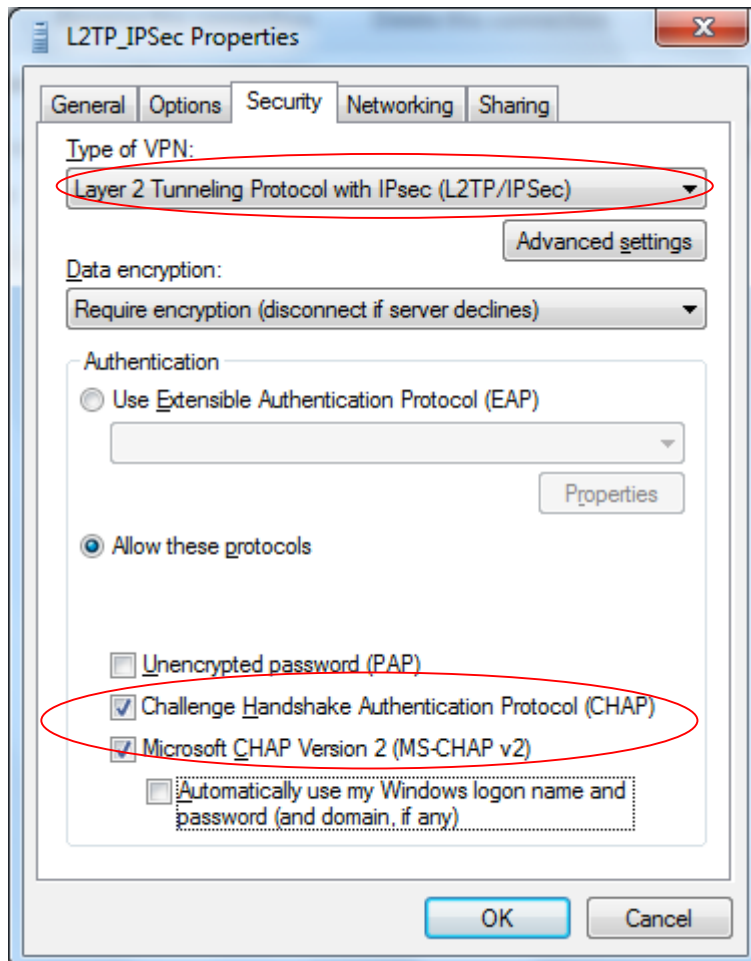
The connection is ready to use

→ Connect now

Close


7. Go to **Network Connections** shown below to check the detail of the connection. Right click “L2TP_IPSec” icon, and select “**Properties**” to change the security parameters.

8. Change the type of VPN to “**Layer 2 Tunneling Protocol with IPsec (L2TP/IPSec)**” and Click Advanced Settings to set the pre-shared (set in IPsec) key for authentication.



9. Go to **Network connections**, enter username and password to connect L2TP_IPSec and check the connection status.

Connect L2TP_IPSec



User name:

Password:

Domain:

☒ Save this user name and password for the following users:

☐ Me only

☒ Anyone who uses this computer

L2TP_IPSec Status

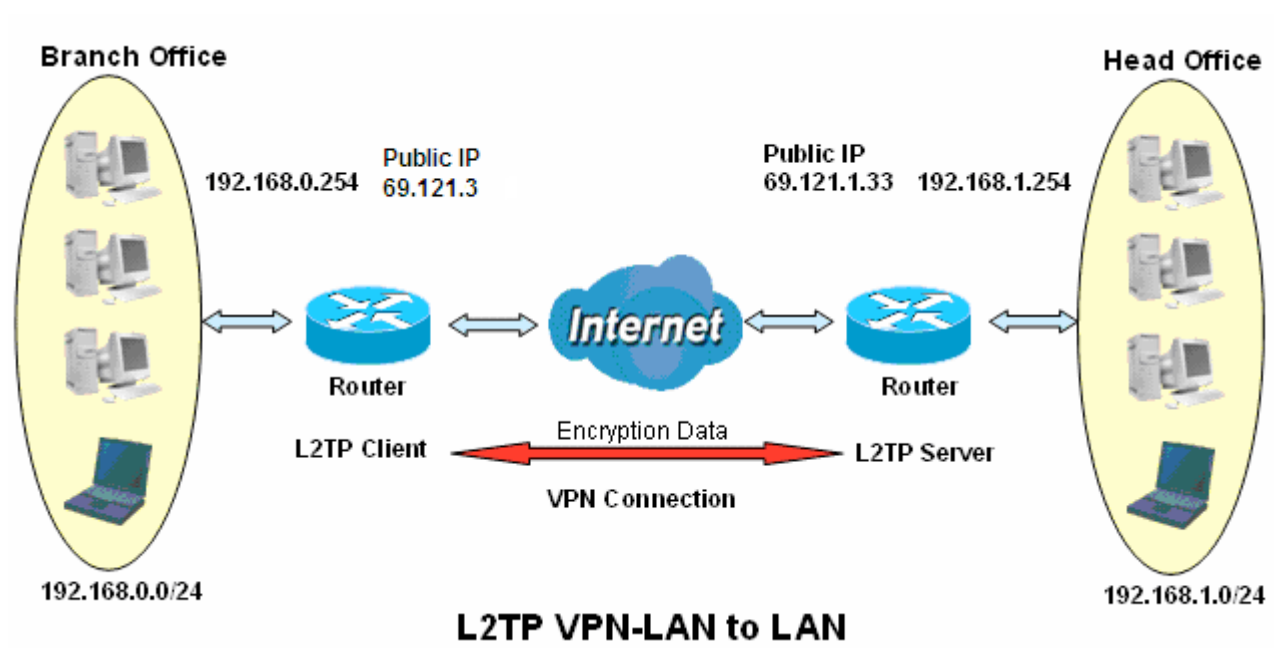
General Details

Property	Value
Device Name	WAN Miniport (L2TP)
Device Type	vpn
Authentication	CHAP
Encryption	IPsec: AES 128
Compression	(none)
PPP multilink framing	Off
Client IPv4 address	192.168.1.10
Server IPv4 address	192.168.1.254
NAP State	Not NAP-capable
Network Adapter Used	Wireless Network Connection
Origin address	172.16.1.102
Destination address	172.16.1.185

Example: Configuring L2TP LAN-to-LAN VPN Connection

The branch office establishes a L2TP VPN tunnel with head office to connect two private networks over the Internet. The routers are installed in the head office and branch office accordingly.

Note: Both office LAN networks must be in different subnets with the LAN-LAN application.



Server side: Head Office

VPN

L2TP Server

Parameters

L2TP ☒ Enable ☐ Disable

WAN Interface [IPSec ▶](#)

Auth. Type

IP Addresses Assigned to Peer start from : 192.168.1.10

Tunnel Authentication ☐

Secret

Remote Host Name

Local Host Name

Exceptional Rule Group

VPN

IPSec

IPSec Settings

L2TP over IPsec ☒ Enable

Connection Name WAN Interface IP Version

Remote Security Gateway ☐ Anonymous

Key Exchange Method IPsec Protocol

Pre-Shared Key

Encryption Algorithm Integrity Algorithm

DH Group IPsec Lifetime Minute(s) [60-1440]

Tunnel Mode Connections							
Active	L2TP	Connection Name	Local Network	Remote Network	Remote Security Gateway	Remove	Edit
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	test1			Anonymous	<input type="checkbox"/>	Edit
<input type="checkbox"/>	<input checked="" type="checkbox"/>	test2			69.121.1.3	<input type="checkbox"/>	Edit

The above is the common setting for L2TP Server, set as you like for authentication and encryption. The settings in Client side should be in accordance with settings in Server side.

Then account the L2TP Account.

VPN

VPN Account

VPN Account applied to PPTP/L2TP/OpenVPN Server.

Parameters

Name: HO Tunnel: ☒ Enable ☐ Disable

Username: test2 Password: *****

Connection Type: ☐ Remote Access ☒ LAN to LAN

Peer Network IP: 192.168.0.0 Peer Netmask: 255.255.255.0

Add Edit / Delete

Edit	Name	Tunnel	Connection Type	Peer Network IP	Peer Netmask	Delete
<input checked="" type="radio"/>	HO	Enable	LAN to LAN	192.168.0.0	255.255.255.0	<input type="checkbox"/>

Client Side: Branch Office

The client user can set up a tunnel connecting to the PPTP server, and can also set the tunnel as the default route for all outgoing traffic.

VPN

L2TP Client

Parameters

Name: BO L2TP over IPSec: ☒ Enable

IPSec Tunnel: test2 IPSec

Username: test2 Password: *****

Auth. Type: Chap L2TP Server Address: 69.121.1.33

Connection Type: ☐ Remote Access ☒ LAN to LAN

Peer Network IP: 192.168.1.0 Peer Netmask: 255.255.255.0

Tunnel Authentication: ☐ Secret:

Remote Host Name: Local Host Name:

Add Edit / Delete

Edit	Enable	Default Gateway	Name	L2TP Server Address	Connection Type	Peer Network IP	Peer Netmask	Delete
<input checked="" type="radio"/>	<input type="checkbox"/>	<input type="checkbox"/>	BO	69.121.1.33	LAN to LAN	192.168.1.0	255.255.255.0	<input type="checkbox"/>

Note: users can see the “Default Gateway” item in the bar, and user can check to select the tunnel as the default gateway (default route) for traffic. If selected, all outgoing traffic will be forwarded to this tunnel and routed to the next hop.

OpenVPN

OpenVPN is an open source software 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 translation (NAT) and firewalls.

OpenVPN allows peers to authenticate each other using a pre-shared secret key, certificates, or username/password. When used in a multiclient-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 is good at portability. OpenVPN has been ported and embedded to several systems.

OpenVPN Server

Users can set the basic parameters (source/destination address, protocol/port, authentication, encryption, etc) for OpenVPN Server.

OpenVPN Server: Select **Enable** to activate OpenVPN Server.

WAN Interface: Select the exact WAN interface configured as source for the tunnel. Select Default to use the now-working WAN interface for the tunnel.

Protocol: OpenVPN can run over User Datagram Protocol (UDP) or Transmission Control Protocol (TCP) transports. Select the protocol.

Port Number: Port 1194 is the official assigned port number for OpenVPN

Tunnel Virtual Subnet: Set the tunnel virtual subnet IP for OpenVPN server.

Tunnel Network: Set the tunnel virtual subnet mask.

Cipher Encryption: OpenVPN uses all the ciphers available in the OpenSSL package to encrypt both the data and channels. Select the encryption method.

HMAC Authentication: OpenVPN support [HMAC](#) authentication, please select authentication item from the list.

Lzo Compression: Enable to use the LZO compression library to compress the data stream.

Click **Apply** to submit your OpenVPN Server basic settings.

OpenVPN CA

OpenVPN offers pre-shared keys, certificate-based, and username/password-based authentication, with certificate-based being the most robust. Generally, the part offers the factory-defined authentication certificate.

Recipient's Email: Set the recipient's email address to send the trusted CA to the OpenVPN client. OpenVPN server and client need matched certificate to establish trusted VPN tunnel, on client side, please import this certificate in [Trusted CA](#).

OpenVPN Client

OpenVPN client can help you dial-in the OpenVPN server to establish a trusted OpenVPN tunnel over Internet.

The screenshot shows a configuration window for an OpenVPN client. The window is titled 'VPN' and contains a section for 'OpenVPN Server' parameters. The parameters are as follows:

Parameters	
OpenVPN Server	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
WAN Interface	Default
Protocol	TCP
Port Number	1194
Tunnel Virtual Subnet	
Tunnel Netmask	
Cipher Encryption	BF-CBC
HMAC Authentication	SHA1
Izo Compression	<input checked="" type="checkbox"/> Enable

At the bottom of the configuration area are two buttons: 'Apply' and 'Cancel'.

Name: user-defined name for identification.

WAN Interface: Select the exact WAN interface configured as source for the tunnel. Select Default to use the now-working WAN interface for the tunnel.

Username: Enter the username provided by your OpenVPN Server.

Password: Enter the password provided by your OpenVPN Server.

OpenVPN Server Address: Enter the WAN IP address of the OpenVPN server.

Protocol: The protocol, same as set in server side.

Port Number: 1194.

Cipher Encryption: Be consistent with what set on server side.

HMAC Authentication: Be consistent with what set on server side.

Izo Compression: Enable to use the LZIO compression library to compress the data stream

Certificate Authority: Select your trusted CA from your server side to establish the trusted VPN tunnel with server.

Click **Add** button to save your changes.

How to establish OpenVPN tunnel

1. Remote Access OpenVPN

(If the client wants to remotely access the OpenVPN Server, on client side, users had better install an OpenVPN client application/installer and connect to server accordingly. Here only give the configuration on server side.)

Server side on router

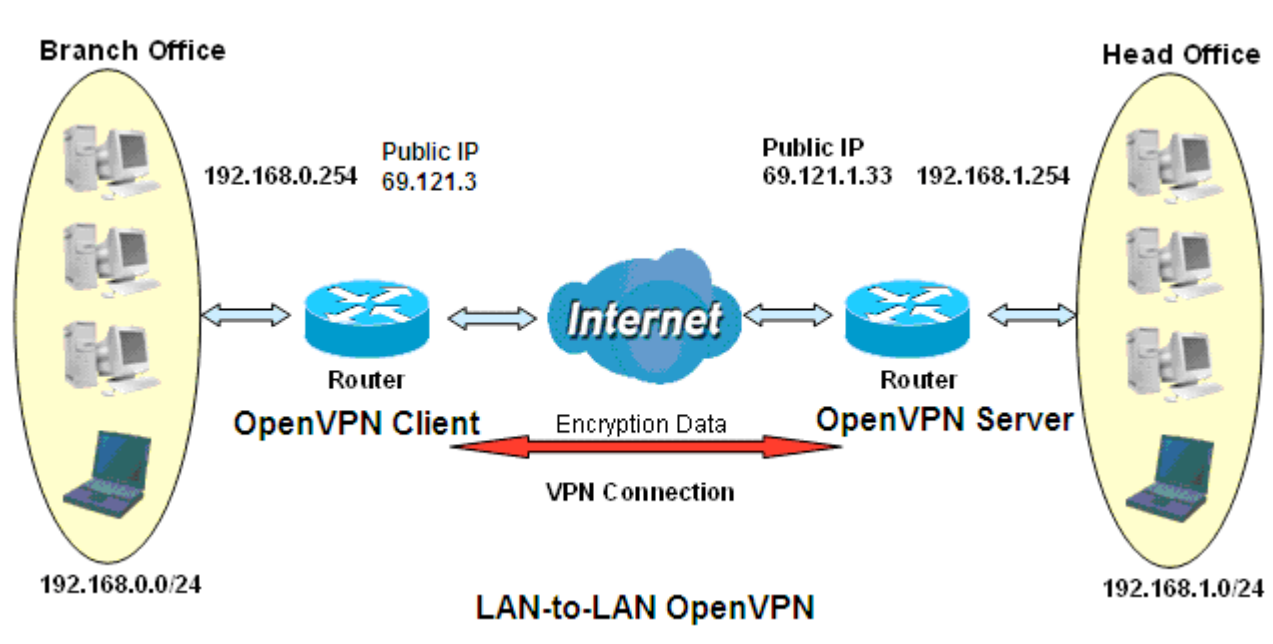
1. Set up parameters (WAN interface, port, tunnel virtual subnet IP/mask, encryption, authentication, etc) on OpenVPN server side.

2. Create an account for the OpenVPN tunnel for client to connect in.
3. Set the OpenVPN client's E-mail address to receive trusted CA from server to establish a trusted OpenVPN tunnel.

2. LAN-to-LAN OpenVPN

The branch office establishes a OpenVPN tunnel with head office to connect two private networks over the Internet. The routers are installed in the head office and branch office accordingly. Configured in this way, head office and branch office can access each other.

Note: Both office LAN networks must be in different subnets with the LAN-to-LAN application.



Server side: Head Office

1. Set up parameters (WAN interface, port, tunnel virtual subnet IP/mask, encryption, authentication, etc) on OpenVPN server side.
2. Create an account for client to connect in
3. Set the OpenVPN client's E-mail address to receive trusted CA from server to establish a trusted OpenVPN tunnel.

Client Side: Branch Office

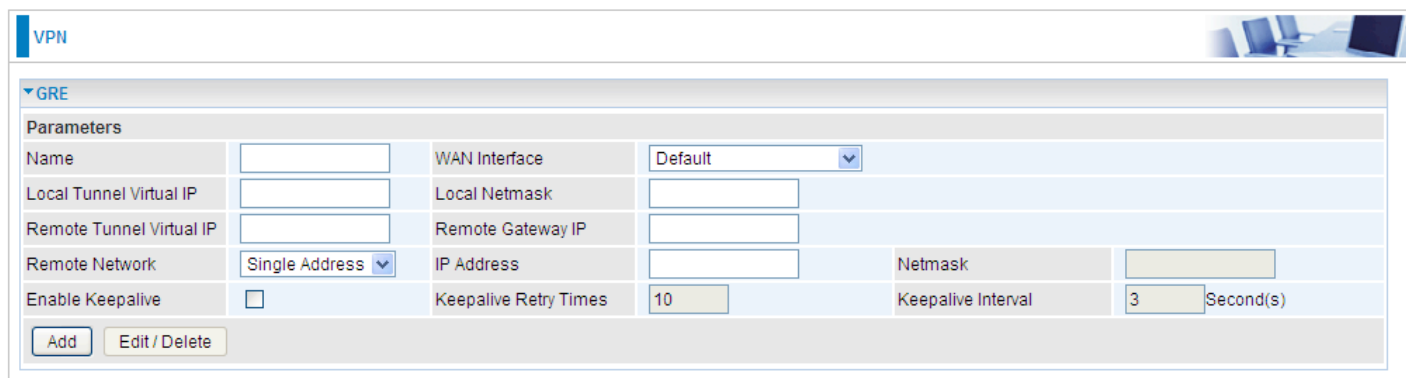
1. Import your trusted certificate from server side, which is used to authenticate between client and server for establishing trusted OpenVPN tunnel.
2. On the OpenVPN client side, fill in the parameters the same as set for OpenVPN server.

Note: users can see the "Default Gateway" item in the bar, and user can check to select the tunnel as the default gateway (default route) for traffic. If selected, all outgoing traffic will be forwarded to this tunnel and routed to the next hop.

GRE

Generic Routing Encapsulation (GRE) is a tunneling protocol that can encapsulate a wide variety of network layer protocol packets inside virtual point-to-point links over an Internet Protocol (IP) network. And the common use can be GRE over IPSec.

Note: up to 8 tunnels can be added, but only 4 can be activated.



The screenshot shows a web-based configuration interface for a VPN. At the top, there is a 'VPN' tab. Below it, a section titled 'GRE' is expanded. Under 'Parameters', there is a table of configuration fields:

Parameters			
Name	<input type="text"/>	WAN Interface	<input type="text" value="Default"/>
Local Tunnel Virtual IP	<input type="text"/>	Local Netmask	<input type="text"/>
Remote Tunnel Virtual IP	<input type="text"/>	Remote Gateway IP	<input type="text"/>
Remote Network	<input type="text" value="Single Address"/>	IP Address	<input type="text"/>
Enable Keepalive	<input type="checkbox"/>	Keepalive Retry Times	<input type="text" value="10"/>
		Keepalive Interval	<input type="text" value="3"/> Second(s)

At the bottom of the form, there are two buttons: 'Add' and 'Edit / Delete'.

Name: User-defined identification.

WAN Interface: Select the exact WAN interface configured for the tunnel as the source tunnel IP. Select Default to use the now-working WAN interface for the tunnel.

Local Tunnel Virtual IP: Please input the virtual IP for the local tunnel side.

Local Netmask: Input the netmask for the local tunnel side.

Remote Tunnel Virtual IP: Please input the virtual destination IP for tunnel.

Remote Gateway IP: Set the destination IP for the tunnel.

Remote Network: Select the peer topology, Single address (client) or Subnet.

IP Address: Set the IP address if the peer is a client. If the peer is a subnet, please enter the IP and netmask.

Enable Keepalive: Normally, the tunnel interface is always up. Enable keepalive to determine when the tunnel interface is to be closed. The local router sends keepalive packets to the peer router, if keepalive response is not received from peer router within the allowed time ('retry time' multiply 'interval', based on default settings, the time interval can be 30 seconds), the local router will shut up its tunnel interface.

Keepalive Retry Times: Set the keepalive retry times, default is 10.

Keepalive Interval: Set the keepalive Interval, unit in seconds. Default is 3 seconds.

Advanced Setup

There are sub-items within the System section: **Routing**, **DNS**, **Static ARP**, **UPnP**, **Certificate**, **Multicast**, **Management**, and **Diagnostics**.

Routing

Default Gateway

Advanced Setup

Default Gateway

Default Gateway Interface List

Only one default gateway interface will be used according to the priority with the first being the highest and the last one the lowest priority if the WAN interface is connected.

Selected Default Gateway Interfaces

usb0

Available Routed WAN Interfaces

Preferred WAN Interface As The System Default IPv6 Gateway



Selected WAN Interface

NO CONFIGURED INTERFACE

Apply

Cancel

WAN port: Select the port this gateway applies to.

To set **Default Gateway** and **Available Routed WAN Interface**. This interfaces are the ones you have set in WAN section, here select the one you want to be the default gateway by moving the interface via  or . And select a Default IPv6 Gateway from the drop-down menu.

Note: Only one default gateway interface will be used according to the priority with the first being the highest and the last one the lowest priority if the WAN interface is connected.

Static Route

With static route feature, you can control the routing of all the traffic across your network. With each routing rule created, you can specifically assign the destination where the traffic will be routed.

Advanced Setup

Static Route

Parameters

IP Version	Dst IP / Prefix Length	Gateway	Interface	Metric	Remove
<div><div>Add</div><div>Remove</div></div>					

Above is the static route listing table, click **Add** to create static routing.

Advanced Setup

Static Route

Parameters

IP Version

IPv4

Destination IP Address / Prefix Length

Interface

Gateway IP Address

Metric

[greater than or equal to zero]

Apply

Cancel

IP Version: Select the IP version, IPv4 or IPv6.

Destination IP Address / Prefix Length: Enter the destination IP address and the prefix length. For IPv4, the prefix length means the number of ‘1’ in the submask, it is another mode of presenting submask. One IPv4 address,192.168.1.0/24, submask is 255.255.255.0. While in IPv6, IPv6 address composes of two parts, thus, the prefix and the interface ID, the prefix is like the net ID in IPv4, and the interface ID is like the host ID in IPv4. The prefix length is to identify the net ID in the address. One IPv6 address, 3FFE:FFFF:0:CD30:0:0:0:0 / 64, the prefix is 3FFE:FFFF:0:CD3.

Interface: Select an interface this route associated.

Gateway IP Address: Enter the gateway IP address.

Metric: Metric is a policy for router to commit router, to determine the optimal route. Enter one number greater than or equal to 0.

Click **Apply** to apply this route and it will be listed in the route listing table.

In listing table you can remove the one you don’t want by checking the checking box and press **Remove** button.

Advanced Setup

Static Route

Parameters

IP Version	Dst IP/Prefix Length	Gateway	Interface	Metric	Remove
4	192.168.1.0/24		ppp0	1	<input checked="" type="checkbox"/>

Add

Remove

Policy Routing

Here users can set a route for the host (source IP) in a LAN interface to access outside through a specified Default Gateway or a WAN interface.

The following is the policy Routing listing table.

Advanced Setup

Policy Routing

Parameters

Policy Name	Source IP	LAN Port	WAN	Default Gateway	Remove
<div><div>Add</div><div>Remove</div></div>					

Click **Add** to create a policy route.

Advanced Setup

Policy Routing

Parameters

Policy Name	<input type="text"/>
Physical LAN Port	<div><div></div></div>
Source IP	<input type="text"/>
Interface	<div>pppoe_0_0_35/ppp0.1</div>
Default Gateway	<input type="text"/>
<div><div>Apply</div><div>Cancel</div></div>	

Policy Name: User-defined name.

Physical LAN Port: Select the LAN port.

Source IP: Enter the Host Source IP.

Interface: Select the WAN interface which you want the Source IP to access outside through.

Default Gateway: Enter the default gateway which you want the Source IP to access outside through.

Click **Apply** to apply your settings. And the item will be listed in the policy Routing listing table. Here if you want to remove the route, check the remove checkbox and press **Remove** to delete it.

RIP

RIP, Router Information Protocol, is a simple Interior Gateway Protocol (IGP). RIP has two versions, RIP-1 and RIP-2.

Advanced Setup

RIP

Parameters

RIP CANNOT BE CONFIGURED on the WAN interface which has NAT enabled (such as PPPoE).

Interface	Version	Operation	Enable
atm0.2	<div>2</div>	<div>Passive</div>	<input type="checkbox"/>

Apply

Cancel

Interface: the interface the rule applies to.

Version: select the RIP version, there are two versions, RIP-1 and RIP-2.

Operation: RIP has two operation mode.

- ① **Passive:** only receive the routing information broadcasted by other routers and modifies its routing table according to the received information.
- ① **Active:** working in this mode, the router sends and receives RIP routing information and modifies routing table according to the received information.

Enable: check the checkbox to enable RIP rule for the interface.

Note: RIP can't be configured on the WAN interface which has NAT enabled

Click **Apply** to apply your settings.

DNS

DNS, Domain Name System, is a distributed database of TCP/IP application. DNS provides translation of Domain name to IP.

DNS

Advanced Setup

DNS

Parameters

Select DNS Server Interface from available WAN interfaces OR enter static DNS server IP addresses OR IP addresses provided by Parental Control Provider for the system.
In ATM mode, if only a single PVC with IPoA or static IPoE protocol is configured, Static DNS server IP addresses must be entered.
DNS Server Interfaces can have multiple WAN interfaces served as system dns servers but only one will be used according to the priority with the first being the highest and the last one the lowest priority if the WAN interface is connected.
Priority order can be changed by removing all and adding them back in again.

☒ Select DNS Server Interface from available WAN interfaces

Selected DNS Server Interfaces		Available WAN Interfaces
usb0	<div>→ ←</div>	

☐ Use the following Static DNS IP address

Primary DNS server:

Secondary DNS server:

☐ Use the IP Addresses provided by Parental Control Provider

Apply Cancel

➤ IPv4

Three ways to set an IPv4 DNS server

- ① **Select DNS server from available WAN interfaces:** Select a desirable WAN interface as the IPv4 DNS server.
- ① **User the following Static DNS IP address:** To specify DNS server manually by entering your primary and secondary DNS server addresses.
- ① **Use the IP address provided by Parental Control Provider:** If user registers and gets an DNS account in the parental control provider website, expecting to enjoy a more reliable and safer internet surfing environment, please select this option (need to configure at [Parental Control Provider](#)).

➤ IPv6:

IPv6 DNS Server's operation is similar to IPv4 DNS server. There are two modes to get DNS server address: Auto and Static mode.

Obtain IPv6 DNS info from a WAN interface

WAN Interface selected: Select one configured IPv6 WAN connection from the drop-down menu to be as an IPv6 DNS.

Use the following Static IPv6 DNS address

Primary IPv6 DNS Server / Secondary IPv6 DNS Server: Type the specific primary and secondary IPv6 DNS Server address.

Dynamic DNS

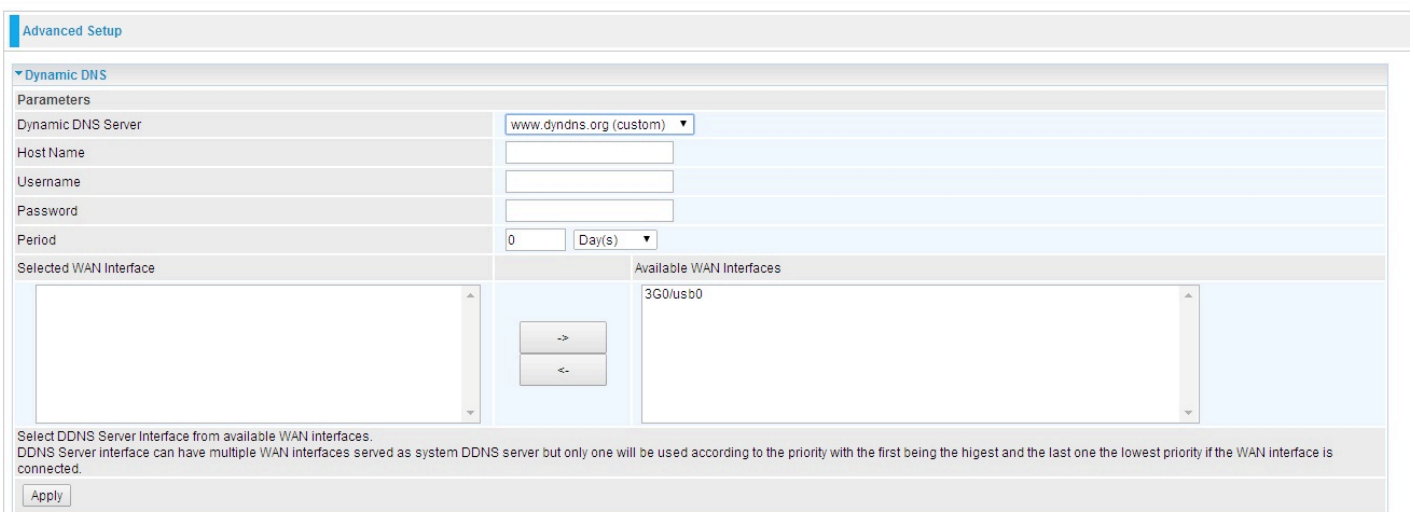
The Dynamic DNS function allows you to alias a dynamic IP address to a static hostname, allowing users whose ISP does not assign them a static IP address to use a domain name. This is especially useful for hosting servers via your 3G/LTE connection, so that anyone wishing to connect to you may use your domain name, rather than having to use your dynamic IP address, which changes from time to time. This dynamic IP address is the WAN IP address of the router, which is assigned to you by your ISP.

Here users can register different WAN interfaces with different DNS(es).



The screenshot shows the 'Advanced Setup' section with the 'Dynamic DNS' tab selected. Below the tab is a table with columns: Host Name, Username, Service, Interface, Remove, and Edit. There are 'Add' and 'Remove' buttons below the table.

Click **Add** to register a WAN interface with the exact DNS.



The screenshot shows the 'Dynamic DNS' configuration page with the following fields filled out: Dynamic DNS Server (www.dyndns.org (custom)), Host Name, Username, Password, Period (0 Day(s)). Below these fields is a section for 'Selected WAN Interface' and 'Available WAN Interfaces'. The 'Available WAN Interfaces' list contains '3G0/usb0'. There are buttons for adding and removing interfaces. At the bottom, there is an 'Apply' button.

You will first need to register and establish an account with the Dynamic DNS provider using their website, for example <http://www.dyndns.org/>

Dynamic DNS Server: Select the DDNS service you have established an account with.

Host Name, Username and Password: Enter your registered domain name and your username and password for this service.

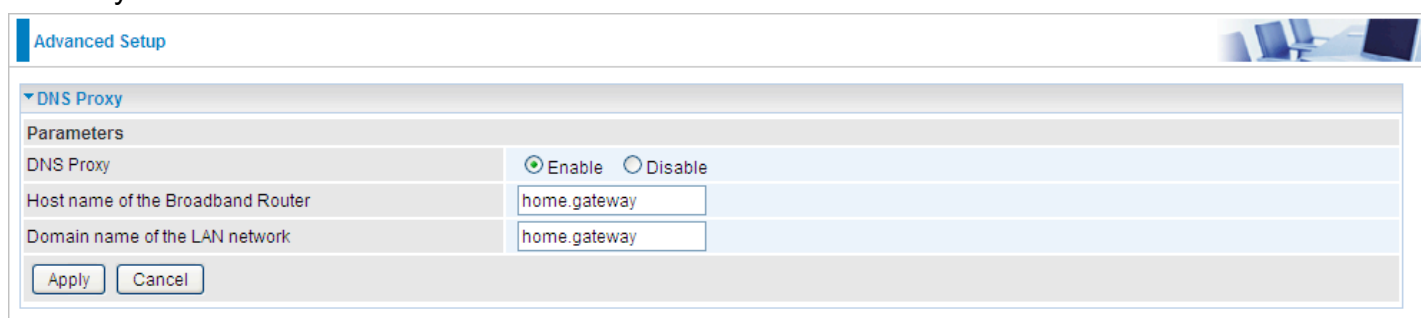
Period: Set the time period between updates, for the Router to exchange information with the DDNS server. In addition to updating periodically as per your settings, the router will perform an update when your dynamic IP address changes.

Selected WAN Interface: Select the Interface that is bound to the registered Domain name.

DNS Proxy

DNS proxy is used to forward request and response message between DNS Client and DNS Server.

Hosts in LAN can use router serving as a DNS proxy to connect to the DNS Server in public to correctly resolve Domain name to access the internet.



The screenshot shows the 'Advanced Setup' page with the 'DNS Proxy' section expanded. Under 'Parameters', there are three fields: 'DNS Proxy' with radio buttons for 'Enable' (selected) and 'Disable'; 'Host name of the Broadband Router' with a text box containing 'home.gateway'; and 'Domain name of the LAN network' with a text box containing 'home.gateway'. At the bottom of the section are 'Apply' and 'Cancel' buttons.

DNS Proxy: Select whether to enable or disable DNS Proxy function, default is enabled.

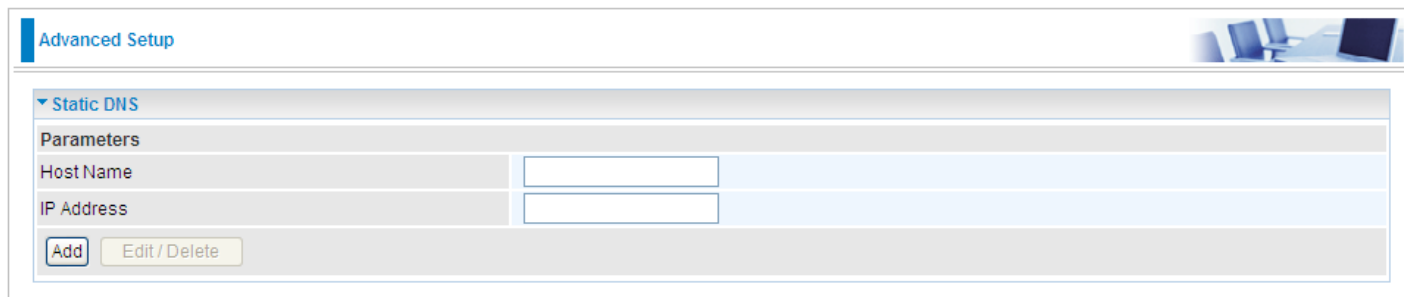
Host name of the Broadband Router: Enter the host name of the router. Default is home.gateway.

Domain name of the LAN network: Enter the domain name of the LAN network. home.gateway.

Static DNS

Static DNS is a concept relative to Dynamic DNS; in static DNS system, the IP mapped is static without change.

You can map the specific IP to a user-friendly domain name. In LAN, you can map a PC to a domain name for convenient access. Or you can set some well-known Internet IP mapping item so your router will response quickly for your DNS query instead of querying from the ISP's DNS server.



The screenshot shows the 'Advanced Setup' page with the 'Static DNS' section expanded. Under 'Parameters', there are two empty text boxes for 'Host Name' and 'IP Address'. At the bottom of the section are 'Add' and 'Edit / Delete' buttons.

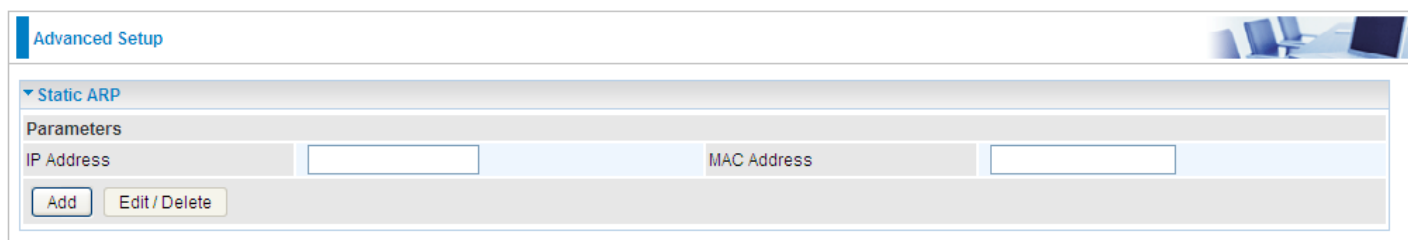
Host Name: Type the domain name (host name) for the specific IP .

IP Address: Type the IP address bound to the set host name above.

Click **Add** to save your settings.

Static ARP

ARP (Address Resolution Protocol) is a TCP/IP protocol that allows the resolution of network layer addresses into the link layer addresses. And “Static ARP” here allows user to map manually the layer-3 MAC (Media Access Control) address to the layer-2 IP address of the device.



The screenshot shows the 'Advanced Setup' tab with the 'Static ARP' section expanded. Under 'Parameters', there are two input fields: 'IP Address' and 'MAC Address'. Below these fields are two buttons: 'Add' and 'Edit / Delete'.

IP Address: Enter the IP of the device that the corresponding MAC address will be mapped to.

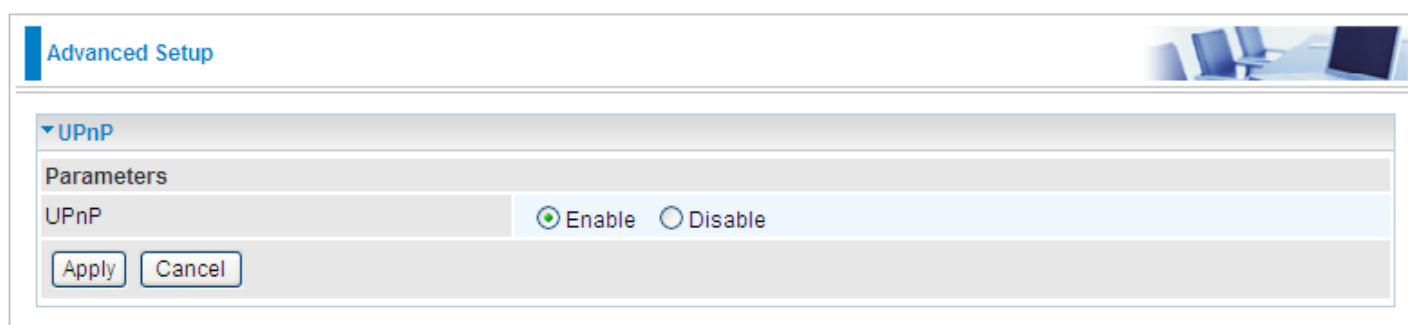
MAC Address: Enter the MAC address that corresponds to the IP address of the device.

Click **Add** to confirm the settings.

UPnP

UPnP offers peer-to-peer network connectivity for PCs and other network devices, along with control and data transfer between devices. UPnP offers many advantages for users running NAT routers through UPnP NAT Traversal, and on supported systems makes tasks such as port forwarding much easier by letting the application control the required settings, removing the need for the user to control advanced configuration of their device.

Both the user's Operating System and the relevant application must support UPnP in addition to the router. Windows XP and Windows Me natively support UPnP (when the component is installed), and Windows 98 users may install the Internet Connection Sharing client from Windows XP in order to support UPnP. Windows 2000 does not support UPnP.



The screenshot shows the 'Advanced Setup' tab with the 'UPnP' section expanded. Under 'Parameters', there is a label 'UPnP' followed by two radio buttons: 'Enable' (which is selected) and 'Disable'. Below these are two buttons: 'Apply' and 'Cancel'.

UPnP:

- ① **Enable:** Check to enable the router's UPnP functionality.
- ① **Disable:** Check to disable the router's UPnP functionality.

Certificate

The feature is to facilitate users to import different certificates for server certificate authentication, like TR-069, OpenVPN etc. If the imported certificate doesn't match the authorized certificate of the ACS Server, OpenVPN Server, the device will have no access to the server.

Trusted CA

Advanced Setup

Trusted CA

Trusted CA (Certificate Authority) Certificates

Maximum certificates can be stored: 4

Name	Subject	Type	Action
<div>Import Certificate</div>			



Certificate Name: The certificate identification name.

Subject: The certificate subject.

Type: The certificate type information. "ca", indicates that the certificate is a CA-signed certificate. "self", indicates that the certificate is a certificate owner signed one.

"x.509", indicates the certificate is the one created and signed according to the definition of Public-Key System suggested by x.509.

Action:

-  View: view the certificate.
-  Remove: remove the certificate.

Click **Import Certificate** button to import your certificate.

Advanced Setup

Trusted CA -- Import CA certificate

Parameters

Name	
Certificate	<div>-----BEGIN CERTIFICATE----- <insert certificate here> -----END CERTIFICATE-----</div>

Apply

Enter the certificate name and insert the certificate.

Click Apply to confirm your settings.

Multicast

Multicast is one of the three network transmission modes, Unicast, Multicast, Broadcast. It is a transmission mode that supports point-to-multipoint connections between the sender and the recipient. IGMP protocol is used to establish and maintain the relationship between IP host and the host directly connected multicast router.

IGMP stands for **Internet Group Management Protocol**, it is a communications protocols used to manage the membership of Internet Protocol multicast groups. IGMP is used by IP hosts and the adjacent multicast routers to establish multicast group members. There are three versions for IGMP, that is IGMPv1, IGMPv2 and IGMPv3.

MLD, short for **Multicast Listener Discovery** protocol, is a component if the Internet Protocol version 6(IPv6) suite. MLD is used by IPv6 to discover multicast listeners on a directly attached link, much as IGMP used in IPv4. The protocol is embedded in ICMPv6 instead of using a separate protocol. MLDv1 is similar to IGMPv2 and MLDv2 is similar to IGMPv3.

Advanced Setup

IGMP

Parameters

Multicast Precedence	Disable	lower value, higher priority
Default Version	3	[1-3]
Query Interval	125	
Query Response Interval	10	
Last Member Query Interval	10	
Robustness Value	2	
Maximum Multicast Groups	25	
Maximum Multicast Data Sources (for IGMPv3)	10	[1-24]
Maximum Multicast Group Members	25	
Fast Leave	<input checked="" type="checkbox"/> Enable	
LAN to LAN (Intra LAN) Multicast	<input type="checkbox"/> Enable	
Membership Join Immediate (IPTV)	<input type="checkbox"/>	

MLD

Default Version	2	[1-2]
Query Interval	125	
Query Response Interval	10	
Last Member Query Interval	10	
Robustness Value	2	
Maximum Multicast Groups	10	
Maximum Multicast Data Sources (for MLDv2)	10	[1-24]
Maximum Multicast Group Members	10	
Fast Leave	<input checked="" type="checkbox"/> Enable	
LAN to LAN (Intra LAN) Multicast	<input type="checkbox"/> Enable	

Apply

Cancel

IGMP

Multicast Precedence: It is for multicast QoS. With lower multicast precedence, IGMP packets will be put into higher-priority queue. Default is set to disable.

Default Version: Enter the supported IGMP version, 1-3, default is IGMP v3.

Query Interval: Enter the periodic query interval time (sec) the multicast router sending the query message to hosts to understand the group membership information.

Query Response Interval: Enter the response interval time (sec).

Last Member Query Interval: Enter the interval time (sec) the multicast router query the specified group after it has received leave message.

Robustness Value: Enter the router robustness parameter, 2-7, the greater the robustness value, the more robust the Querier is.

Maximum Multicast Groups: Enter the Maximum Multicast Groups.

Maximum Multicast Data Sources(for IGMP v3): Enter the Maximum Multicast Data Sources, 1-24.

Maximum Multicast Group Members: Enter the Maximum Multicast Group Members.

Fast leave: Check to determine whether to support fast leave. If this value is enabled, IGMP proxy removes the membership of a group member immediately without sending an IGMP membership query on downstream. This is very helpful if user wants fast channel (group change) changing in cases like IPTV environment.

LAN to LAN (Intra LAN) Multicast: Check to determine whether to support LAN to LAN (Intra LAN) Multicast. If user want to have a multicast data source on LAN side and he want to get IGMP snooping enabled, then this LAN-to-LAN multicast feature should be enabled.

Membership Join Immediate (IPTV): When a host joins a multicast session, it sends unsolicited join report to its upstream router immediately. The Startup Query Interval has been set to 1/4 of the General Query value to enable the faster join at startup.

MLD

Default Version: Enter the supported MLD version, 1-2, default is MLDv2.

Query Interval: Enter the periodic query interval time (sec) the multicast router sending the query message to hosts to understand the group membership information.

Query Response Interval: Enter the response interval time (sec).

Last Member Query Interval: Enter the interval time (sec) the multicast router query the specified group after it has received leave message.

Robustness Value: Enter the router robustness parameter, default is 2, the greater the robustness value, the more robust the Querier is.

Maximum Multicast Groups: Enter the Maximum Multicast Groups.

Maximum Multicast Data Sources(for MLDv2): Enter the Maximum Multicast Data Sources, 1-24.

Maximum Multicast Group Members: Enter the Maximum Multicast Group Members.

Fast leave: Check to determine whether to support fast leave. If this value is enabled, MLD proxy removes the membership of a group member immediately without sending an MLD membership query on downstream. This is very helpful if user wants fast channel (group change) changing in cases like IPTV environment.

LAN to LAN (Intra LAN) Multicast: Check to determine whether to support LAN to LAN (Intra LAN) Multicast. If user want to have a multicast data source on LAN side and he want to get MLD snooping enabled, then this LAN-to-LAN multicast feature should be enabled.

Management

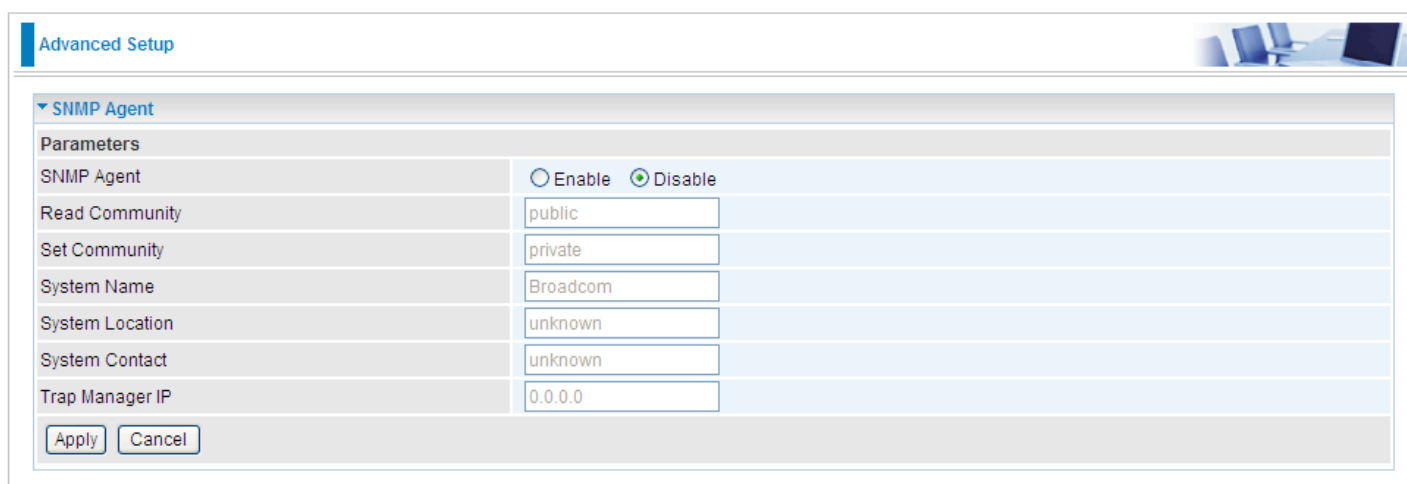
SNMP Agent

SNMP, Simple Network Management Protocol, is the most popular one in network. It consists of SNMP Manager, SNMP Agent and MIB. Every network device supporting SNMP will have a SNMP Agent which is a management software running in the device.

SNMP Manager, the management software running on the server, it uses SNMP protocol to send GetRequest, GetNextRequest, SetRequest message to Agent to view and change the information of the device.

SNMP Agents, the management software running in the device, accepts the message from the manager, Reads or Writes the management variable in MIB accordingly and then generates Response message to send it to the manager. Also, agent will send Trap message to the manager when agent finds some exceptions.

Trap message, is the message automatically sent by the managed device without request to the manager about the emergency events.



The screenshot shows a web interface titled "Advanced Setup" with a sub-section for "SNMP Agent". Under the "Parameters" heading, there is a table with the following fields and values:

Parameters	
SNMP Agent	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Read Community	public
Set Community	private
System Name	Broadcom
System Location	unknown
System Contact	unknown
Trap Manager IP	0.0.0.0

At the bottom of the configuration area, there are two buttons: "Apply" and "Cancel".

SNMP Agent: enable or disable SNMP Agent.

Read Community: Type the Get Community, which is the authentication for the incoming Get-and GetNext requests from the management station.

Set Community: Type the Set Community, which is the authentication for incoming Set requests from the management station.

System Name: here it refers to your router.

System Location: user-defined location.

System Contact: user-defined contact message.

Trap manager IP: enter the IP address of the server receiving the trap sent by SNMP agent.

TR-069 Client

▼ TR-069 Client	
Parameters	
Inform	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Inform Interval	300 [1-2147483647]
ACS URL	
ACS User Name	admin
ACS Password	*****
WAN Interface used by TR-069 client	Any_WAN ▾
Display SOAP messages on serial console	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Connection Request Authentication	<input checked="" type="checkbox"/>
Connection Request User Name	admin
Connection Request Password	*****
Connection Request URL	
<input type="button" value="Apply"/> <input type="button" value="GetRPCMethods"/>	

Remote Access

It is to allow remote access to the router to view or configure.

Advanced Setup	
▼ Remote Access	
Parameters	
Remote Access	<input checked="" type="checkbox"/> Enable
Enable Service	<input checked="" type="checkbox"/> HTTP <input type="checkbox"/> SSH <input type="checkbox"/> FTP <input type="checkbox"/> TELNET <input type="checkbox"/> SNMP
<input type="button" value="Apply"/>	
Allowed Access IP Address Range	
Valid	<input checked="" type="checkbox"/>
IP Version	IPv4 ▾ IP Address Range
<input type="button" value="Add"/> <input type="button" value="Edit / Delete"/>	

Remote Access: Select “Enable” to allow management access from remote side (mostly from internet). If disabled, no remote access is allowed for any IPs even if you set allowed access IP address. So, please note that enabling remote access is an essential step before granting remote access to IPs.

Enable Service: Select to determine which service(s) is (are) allowed for remote access when remote access is enabled. By default (on condition that remote access is enabled), the web service (HTTP) is allowed for remote access.

Click **Apply** button to submit your settings.

"Allowed Access IP Address Range" was used to restrict which IP address could login to access system web GUI.

Valid: Enable/Disable Allowed Access IP Address Range

IP Address Range: Specify the IP address Range, IPv4 and IPv6 address range can be supported, users can set IPv4 and IPv6 address range individually.

Click **Add** to add an IP Range to allow remote access.

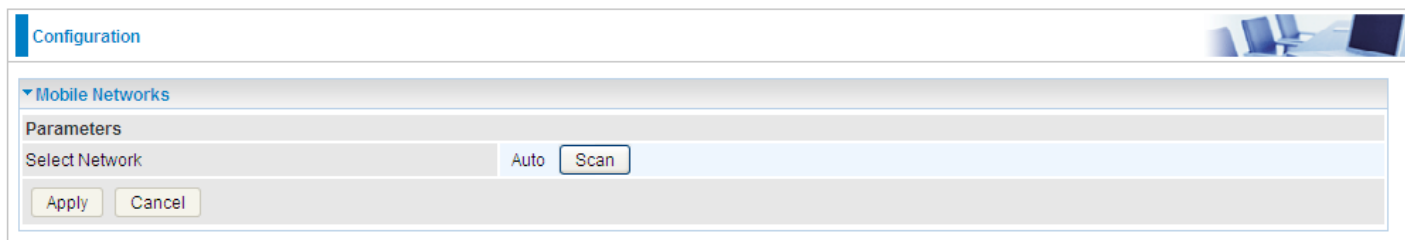
Note: 1. If user wants to grant remote access to IPs, first enable **Remote Access**.

2. Remote Access enabled:

- 1) Enable **Valid** for the specific IP(s) in the IP range to allow the specific IP(s) to remote access the router.
- 2) Disable **Valid** for all specific IP(s) in the IP range to allow any IP(s) to remote access the router.
- 3) No listing of IP range is to allow any IP(s) to remote access the router.

Mobile Network

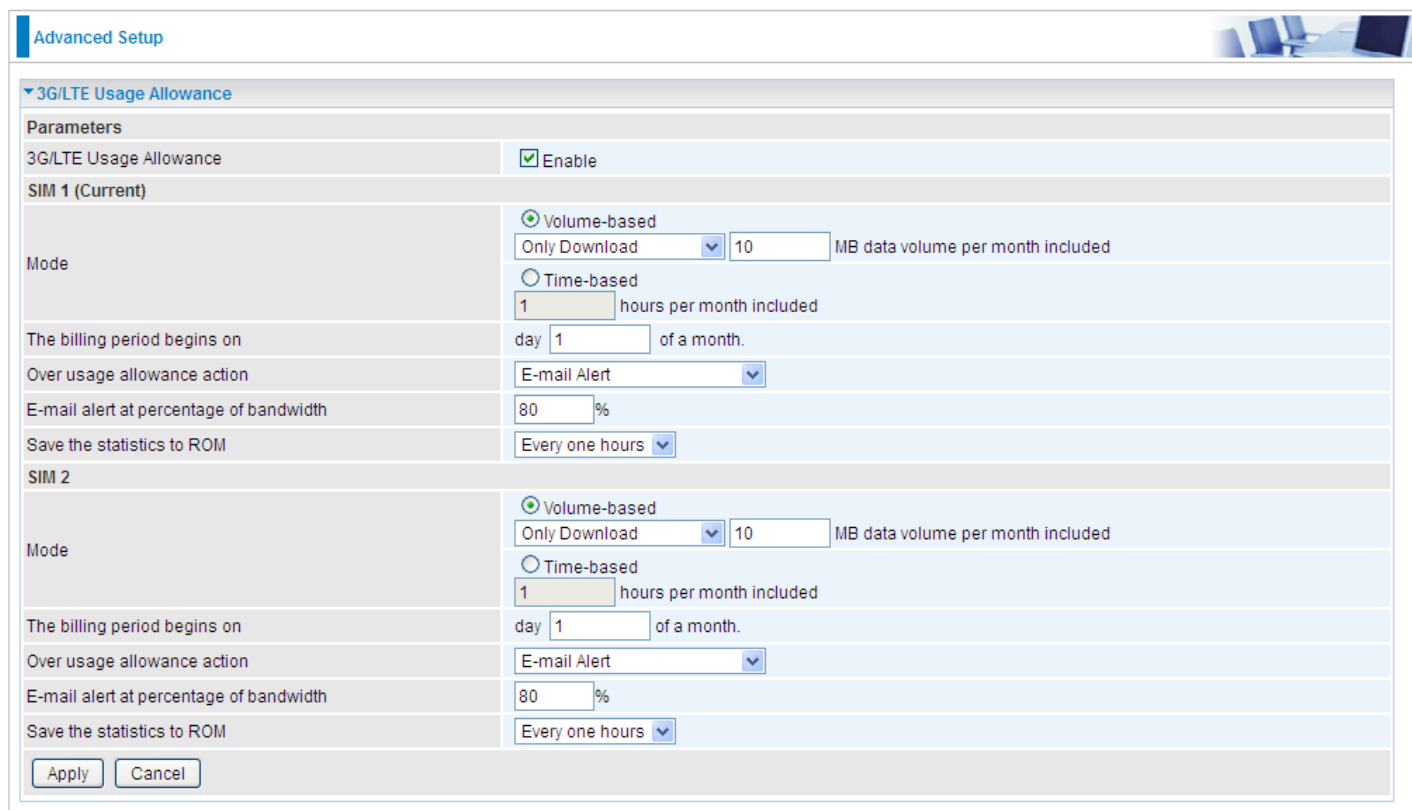
User can press **Scan** to discover available 3G/LTE mobile network.



The screenshot shows the 'Configuration' tab with the 'Mobile Networks' section expanded. Under 'Parameters', there is a 'Select Network' dropdown menu set to 'Auto'. To its right is a 'Scan' button. At the bottom of the section are 'Apply' and 'Cancel' buttons.

3G/LTE Usage Allowance

3G/LTE usage allowance is designated for users to monitor and control the 3G flow usage. The router's 3G/LTE usage allowance offers exact control settings for each SIM card.



The screenshot shows the 'Advanced Setup' tab with the '3G/LTE Usage Allowance' section expanded. The 'Parameters' section shows '3G/LTE Usage Allowance' is checked and 'Enable'. Below this, there are two identical configuration blocks for 'SIM 1 (Current)' and 'SIM 2'. Each block has a 'Mode' section with 'Volume-based' selected (radio button) and 'Only Download' chosen from a dropdown, with a value of '10' MB data volume per month included. The 'Time-based' option is unselected. For 'SIM 1', the 'The billing period begins on' is set to 'day 1 of a month'. The 'Over usage allowance action' is 'E-mail Alert', the 'E-mail alert at percentage of bandwidth' is '80%', and 'Save the statistics to ROM' is 'Every one hours'. The same settings are visible for 'SIM 2'. At the bottom of the section are 'Apply' and 'Cancel' buttons.

3G/LTE Usage Allowance: Enable to monitor 3G/LTE usage.

SIM 1 & SIM 2

Mode: include Volume-based and Time-based control.

① **Volume-based** include “only Download”, “only Upload” and “Download and Upload” to limit the flow.

① **Time-based** control the flow by providing specific hours per month.

The billing period begins on: The beginning day of billing each month.

Over usage allowance action: What to do when the flow is over usage allowance, the available methods are “E-mail Alert”, “Email Alert and Disconnect” and “Disconnect”.

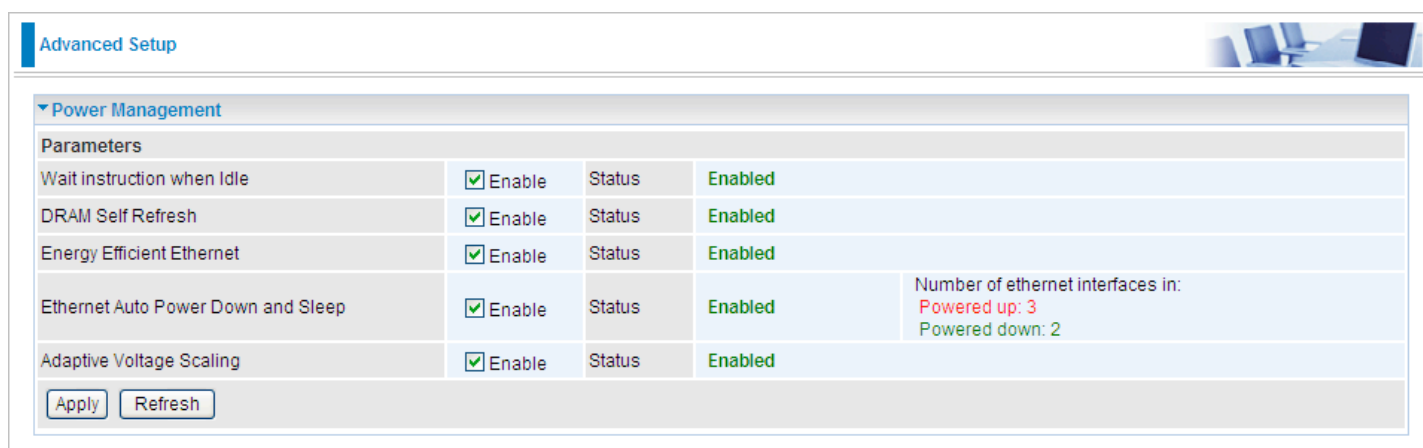
E-mail alert at percentage of bandwidth: When the used bandwidth exceeds the set proportion, the system will send email to alert.

Save the statistics to ROM: To save the statistics to ROM system.

Power Management

Power management is a feature of some electrical appliances, especially computers that turn off the power or switch to a low-power state when inactive.

Five main parameters are listed for users to check to manage the performance of the router.



The screenshot shows the 'Advanced Setup' page with the 'Power Management' section expanded. It contains a table of parameters with checkboxes to enable or disable them, and a status column showing if they are enabled. There are also buttons for 'Apply' and 'Refresh'.

Parameters			
Wait instruction when Idle	<input checked="" type="checkbox"/> Enable	Status	Enabled
DRAM Self Refresh	<input checked="" type="checkbox"/> Enable	Status	Enabled
Energy Efficient Ethernet	<input checked="" type="checkbox"/> Enable	Status	Enabled
Ethernet Auto Power Down and Sleep	<input checked="" type="checkbox"/> Enable	Status	Enabled
Adaptive Voltage Scaling	<input checked="" type="checkbox"/> Enable	Status	Enabled

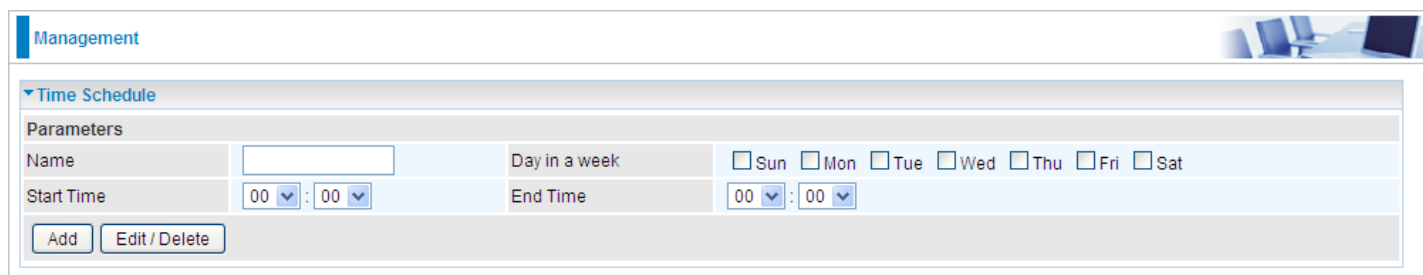
Number of ethernet interfaces in:
Powered up: 3
Powered down: 2

Buttons: Apply, Refresh

Time Schedule

The Time Schedule supports up to **32** timeslots which helps you to manage your Internet connection. In each time profile, you may schedule specific day(s) i.e. Monday through Sunday to restrict or allowing the usage of the Internet by users or applications.

This Time Schedule correlates closely with router's time, since router does not have a real time clock on board; it uses the Simple Network Time Protocol (SNTP) to get the current time from an SNTP server from the Internet. Refer to **Internet Times** for details.



The screenshot shows the 'Management' page with the 'Time Schedule' section expanded. It contains a form to create a new time schedule profile with fields for Name, Start Time, End Time, and Day in a week. There are also buttons for 'Add' and 'Edit / Delete'.

Parameters			
Name	<input type="text"/>	Day in a week	<input type="checkbox"/> Sun <input type="checkbox"/> Mon <input type="checkbox"/> Tue <input type="checkbox"/> Wed <input type="checkbox"/> Thu <input type="checkbox"/> Fri <input type="checkbox"/> Sat
Start Time	00 : 00	End Time	00 : 00

Buttons: Add, Edit / Delete

For example, user can add a timeslot named “timeslot1” features a period of 9:00-19:00 every weekday.

Management

Time Schedule

Parameters

Name

Day in a week

☐ Sun

☐ Mon

☐ Tue

☐ Wed

☐ Thu

☐ Fri

☐ Sat

Start Time

00 : 00

End Time

00 : 00

Add

Edit / Delete

Edit

Name

Day in a week

Start Time

End Time

Delete

☐

timeslot1

sMTWTfs

09:00

19:00

☐

Auto Reboot

Auto reboot offers flexible rebooting service (reboot with the current configuration) of router for users in line with scheduled timetable settings.

Advanced Setup

Auto Reboot

Parameters

Schedule

1. ☐ Enable

☐ Sun

☐ Mon

☐ Tue

☐ Wed

☐ Thu

☐ Fri

☐ Sat

Time

00 : 00

2. ☐ Enable

☐ Sun

☐ Mon

☐ Tue

☐ Wed

☐ Thu

☐ Fri

☐ Sat

Time

00 : 00

Apply

Enable to set the time schedule for rebooting.

For example, the router is scheduled to reboot at 22:00 every single weekday, and to reboot at 9:00 on Saturday and Sunday. You can set as follows:

Advanced Setup

Auto Reboot

Parameters

Schedule

1. ☒ Enable

☐ Sun

☒ Mon

☒ Tue

☒ Wed

☒ Thu

☒ Fri

☐ Sat

Time

22 : 00

2. ☒ Enable

☒ Sun

☐ Mon

☐ Tue

☐ Wed

☐ Thu

☐ Fri

☒ Sat

Time

09 : 00

Apply

Diagnostics

Diagnostics Tools

The router offers diagnostics tools including “Ping” and “Trace route test” tools to check for problems associated with network connections.

Advanced Setup

▼ Diagnostics Tools

Ping Test

Destination Host

Source Address ☒ Interface ☐ IP Address

Trace route Test

Destination Host

Source Address ☒ Interface ☐ IP Address

Max TTL value [2-30]

Wait time seconds [2-999]

Ping Test: to verify the connectivity between source and destination.

Destination Host: Enter the destination host (IP, domain name) to be checked for connectivity.

Source Address: Select or set the source address to test the connectivity from the source to the destination.

Ping Test: Press this button to proceed ping test.

Trace route Test: to trace the route to see how many hops (also see the exact hops) the packet of data has to take to get to the destination.

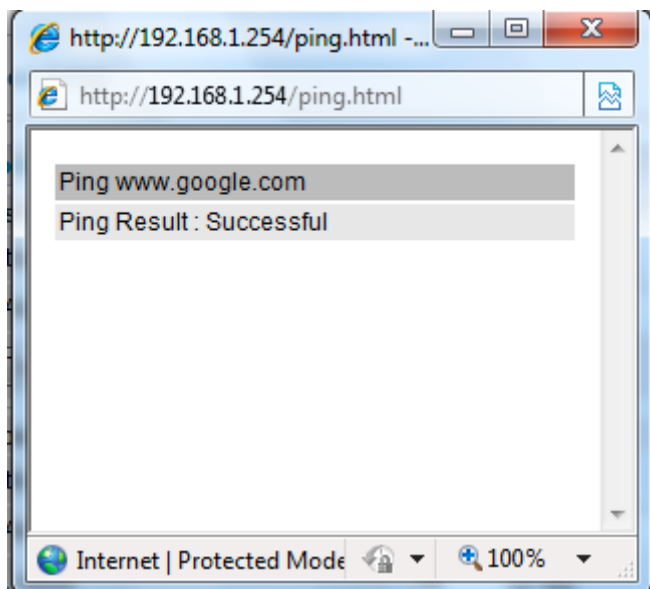
Destination Host: Set the destination host (IP, domain name) to be traced.

Source Address: Select or set the source address to trace the route from the source to the destination.

Max TTL value: Set the max Time to live (TTL) value.

Wait time: Set waiting time for each response in seconds.

Example: Ping www.google.com



Example: "trace" www.google.com

http://192.168.1.254/tracert.html - Windows Intern...

http://192.168.1.254/tracert.html

Trace www.google.com

No.	Route Address	Time
1	112.86.208.1	22.229 ms
2	221.6.9.93	20.352 ms
3	221.6.2.169	24.345 ms
4	219.158.24.41	52.837 ms
5	219.158.23.18	54.696 ms
6	219.158.19.190	54.904 ms
7	219.158.3.238	57.824 ms
8	72.14.215.130	58.851 ms
9	209.85.248.60	57.644 ms
10	209.85.250.122	81.242 ms
11	209.85.250.103	81.351 ms
12	*	* *
13	173.194.72.147	79.753 ms

Push Service

With push service, the system can send email messages with consumption data and system information.

Advanced Setup

▼ Push Service

Parameters


Recipient's E-mail (Must be xxx@yyy.zzz)

Push Now

Recipient's E-mail: Enter the destination mail address. The email is used to receive **system log**, **system configuration**, **security log** sent by the device when the **Push Now** button is pressed (information sent only when pressing the button), but the mail address is not remembered.

Note: Please first set correct the SMTP server parameters in [Mail Alert](#).

Restart

This section lets you restart your router if necessary. Click  **Restart** in the low right corner of each configuration page.

Configuration

Restart

After restarting. Please wait for several seconds to let the system come up.

Restart device with

☐ Factory Default Settings

☒ Current Settings

Restart

If you wish to restart the router using the factory default settings (for example, after a firmware upgrade or if you have saved an incorrect configuration), select Factory Default Settings to reset to factory default settings. Or you just want to restart after the current setting, the select the Current Settings, and Click Restart.

progress

progress...

Do not switch off device during flash update or rebooting.

total :

8%