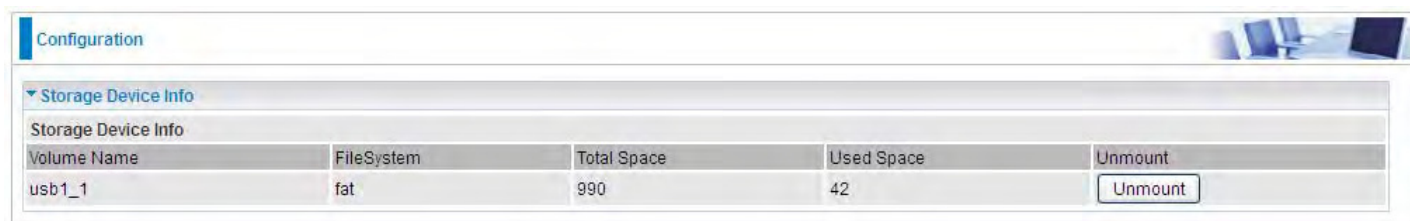


USB

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.



Volume Name	FileSystem	Total Space	Used Space	Unmount
usb1_1	fat	990	42	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.

The screenshot shows the 'Configuration' page with the 'User Accounts' section expanded. It displays a table with columns: Username, Home Directory, Remove, and Edit. The 'admin' user is listed with a home directory of '/'. Below the table are 'Add' and 'Remove' buttons.

Username	Home Directory	Remove	Edit
admin	/		

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

The screenshot shows the 'Configuration' page with the 'User Accounts' section expanded. It displays a form with fields for Username, Password, Confirm Password, and Volume Name. The 'Volume Name' dropdown is set to 'usb1_1'. Below the form are 'Apply' and 'Cancel' buttons.

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.

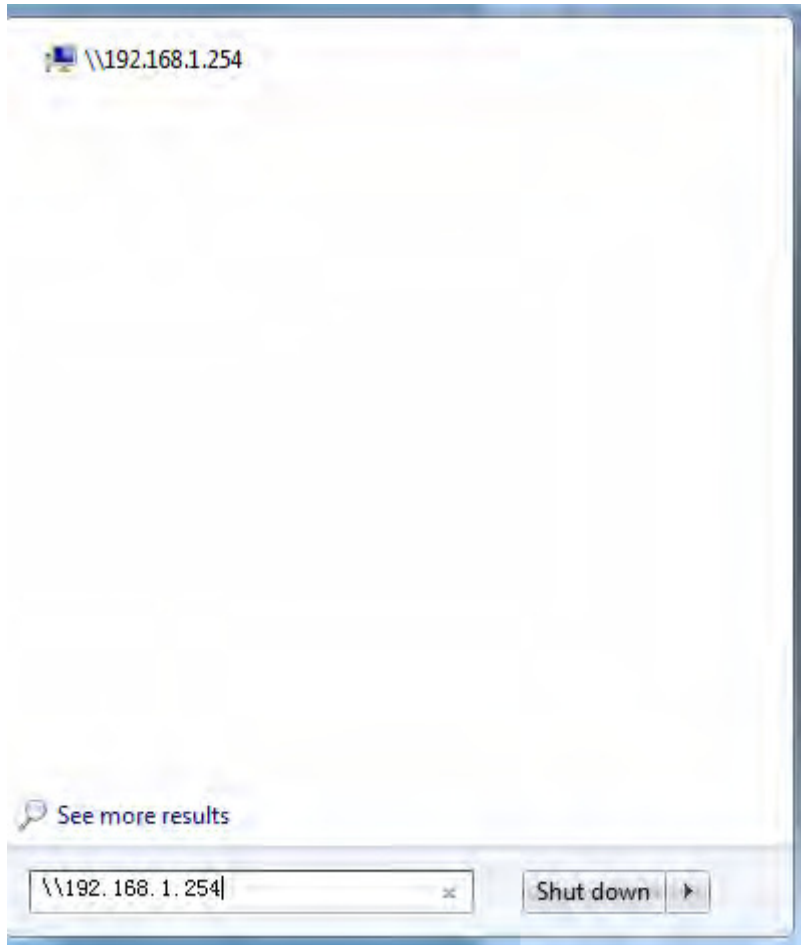
The screenshot shows the 'Configuration' page with the 'User Accounts' section expanded. It displays a table with columns: Username, Home Directory, Remove, and Edit. The 'test' user is listed with a home directory of 'usb1_1/test'. Below the table are 'Add' and 'Remove' buttons.

Username	Home Directory	Remove	Edit
admin	/		
test	usb1_1/test	☐	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](#) (LAN IP)

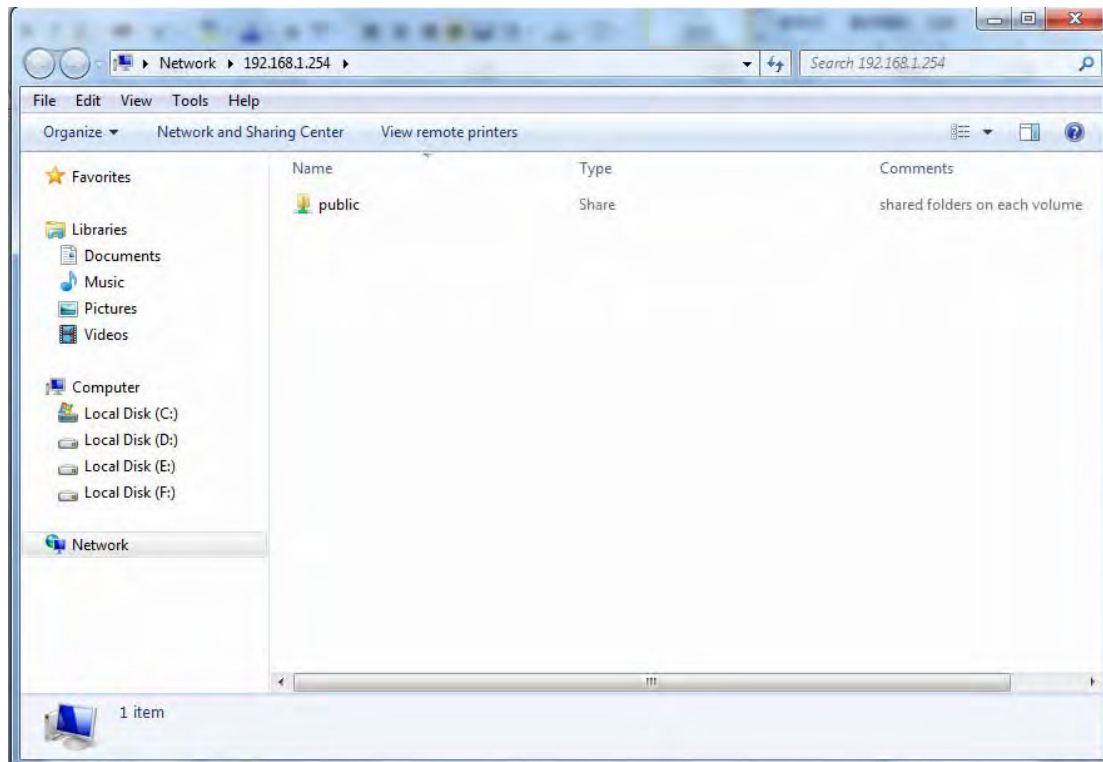


When accessing the network storage, you can see a folder named “**public**”, users should have the account to enter, and the account can be set at the User Accounts section.

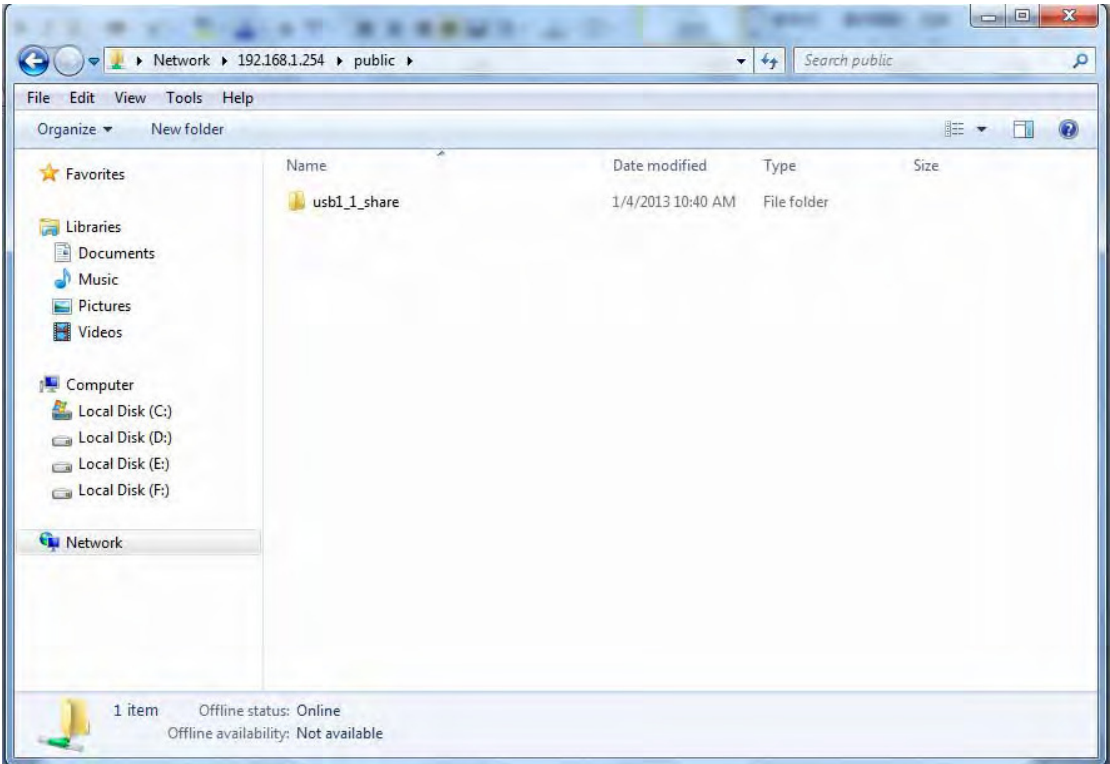
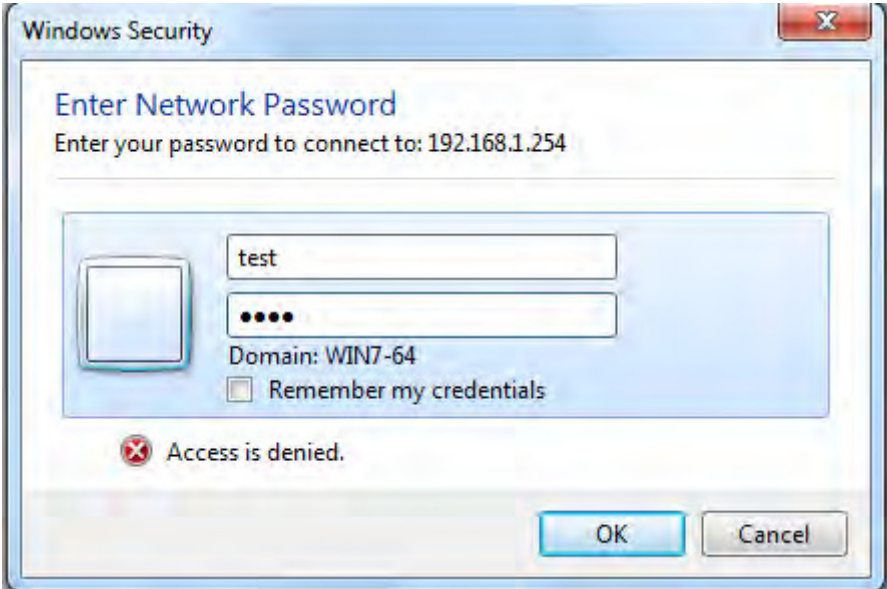
When first logged on to the network folder, you will see the “**public**” folder.

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

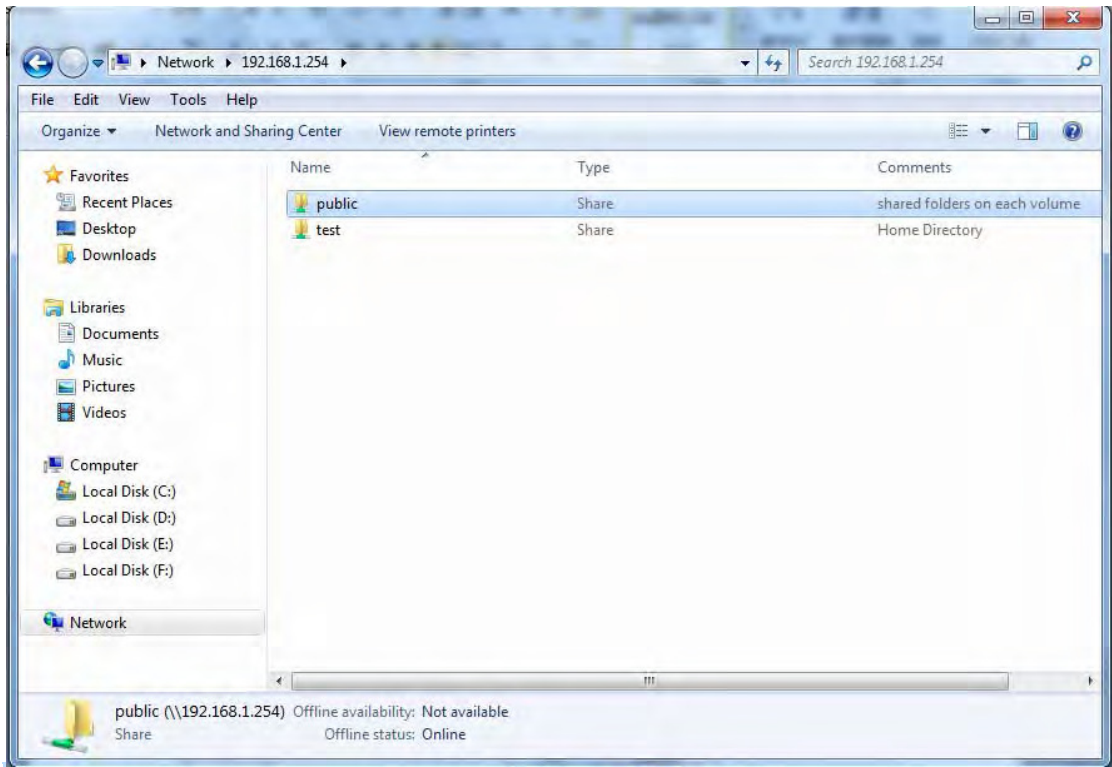
When user register a USB account and log successfully, a private folder (the same name as the user account registered) exclusive for each user is established. Go on to see the details.



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.



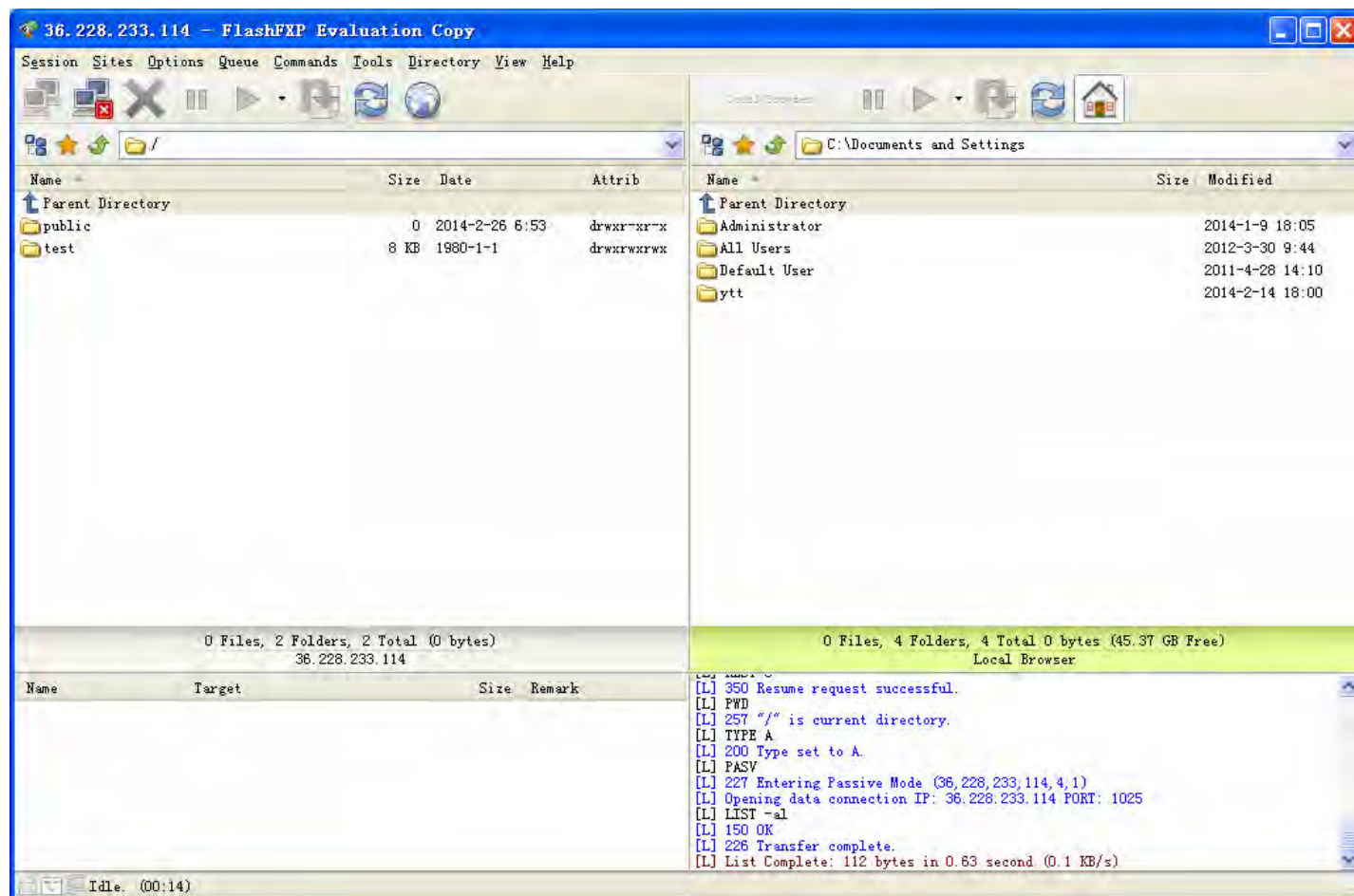
How to use FTP:

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

1. Access via FTP tools

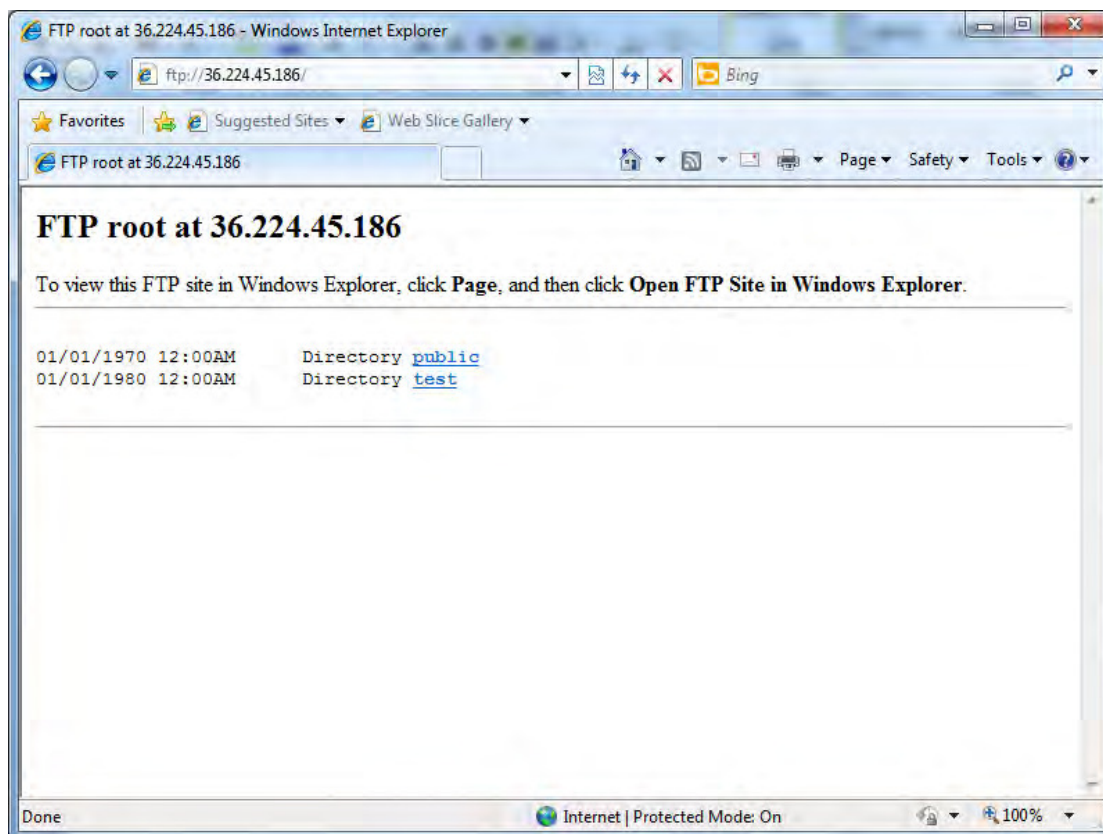
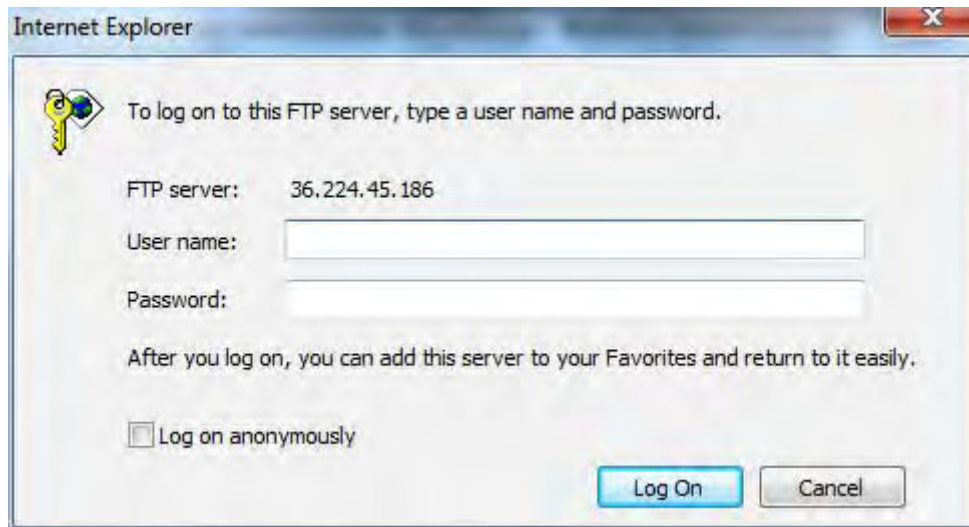
Take popular FTP tool of FlashFXP for example:

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



2. Web FTP access

- 1) Enter <ftp://admin@WAN-IP> or <ftp://admin@LAN-IP> at the address bar of the IE. In terms of other browsers, type <ftp://WAN-IP> or <ftp://LAN-IP> directly.
- 2) Enter the account's username and password.



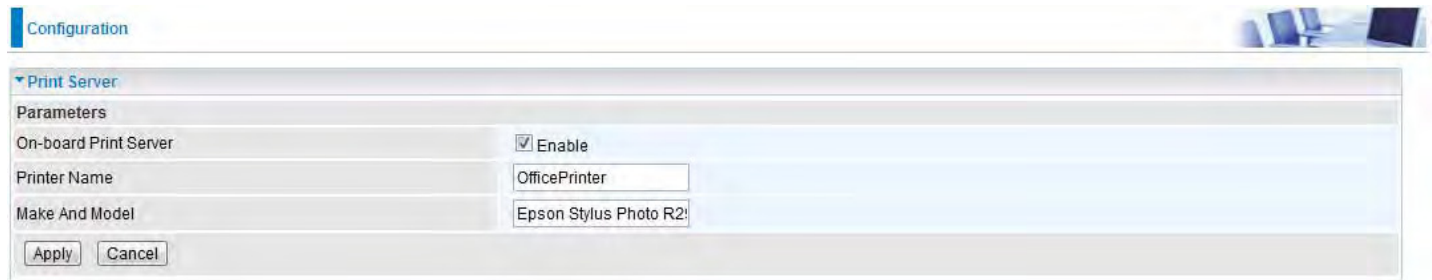
Print Server

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 7820NZ. 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 (7820NZ for example)

1. Connect the printer to the 7820NZ's USB port
2. Enable the print server on the 7820NZ
3. Install the printer drivers on the PC you want to print from



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)

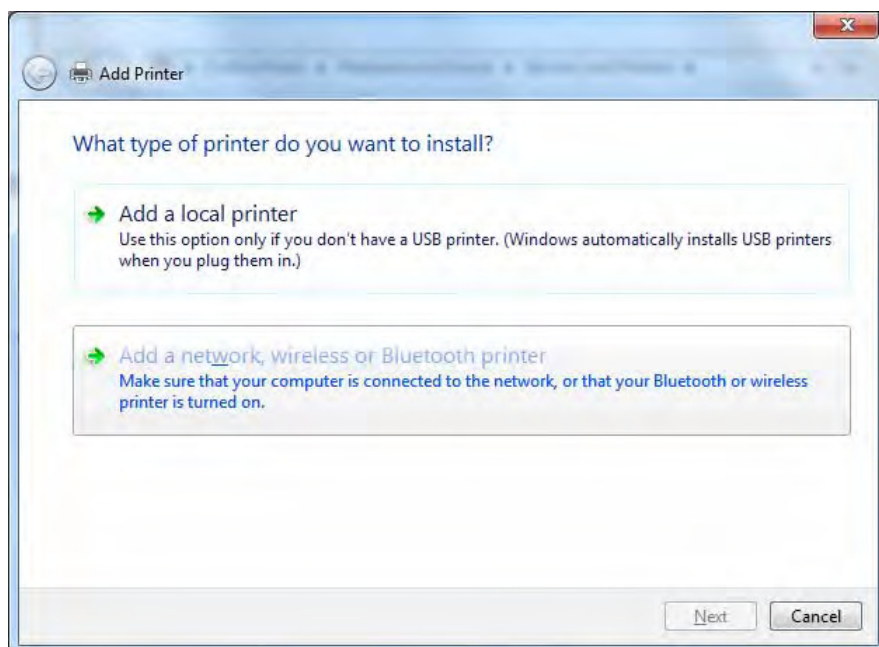
Step 1: Click **Start** and select "Devices and Printers"



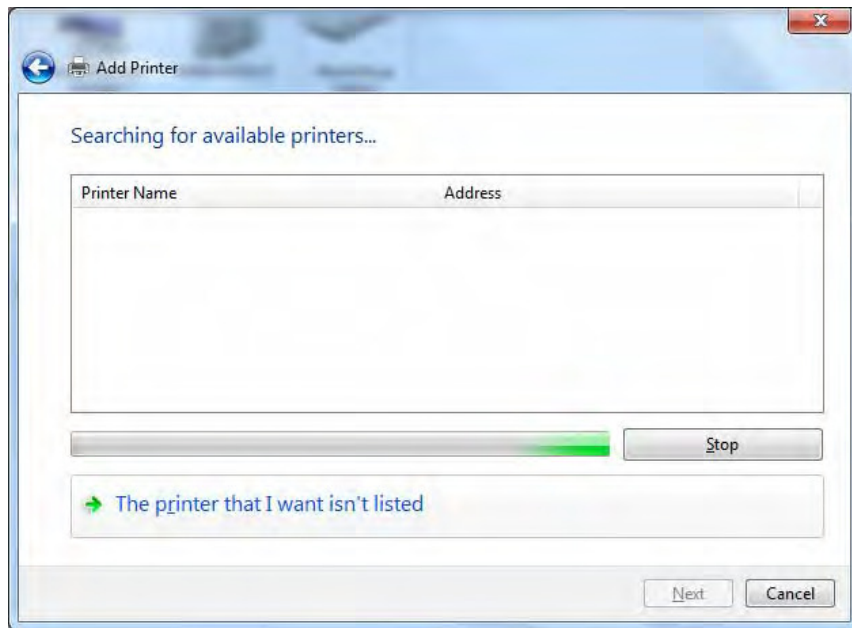
Step 2: Click “Add a Printer”.



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



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

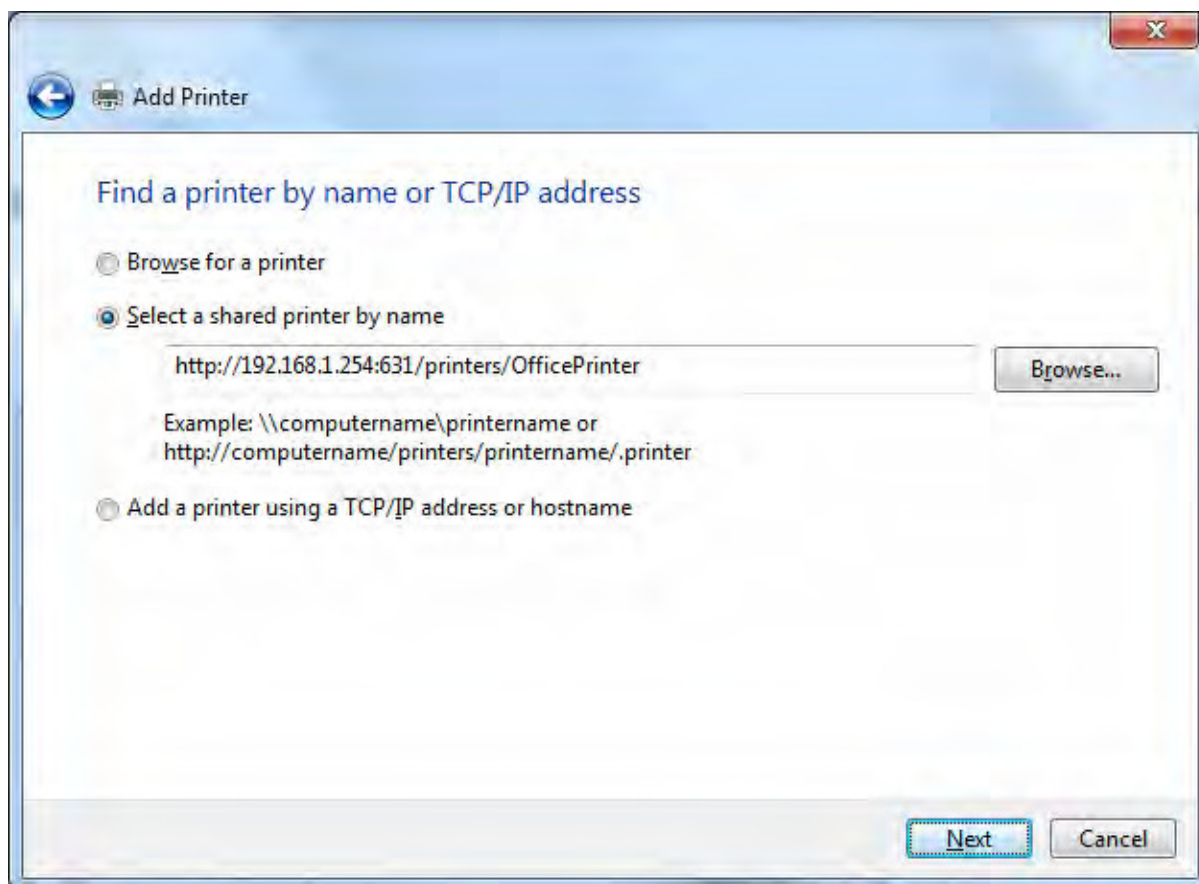


Step 5: Select “Select a shared printer by name”

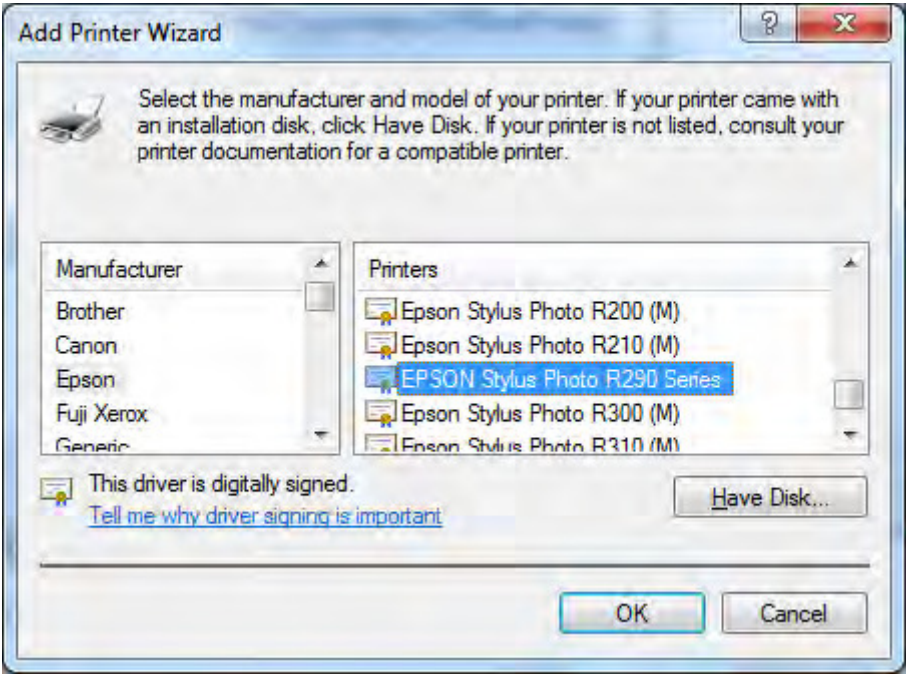
Enter `http://7820NZ- LAN-IP:631/printers/printer-name` or. Make sure printer’s name is the same as what you set in the 7820NZ earlier

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

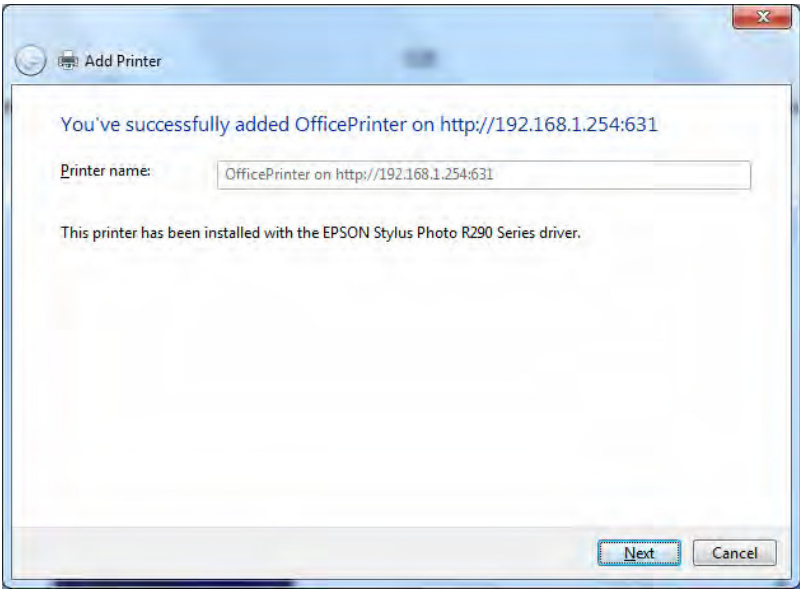
OfficePrinter is the Printer Name we setup earlier



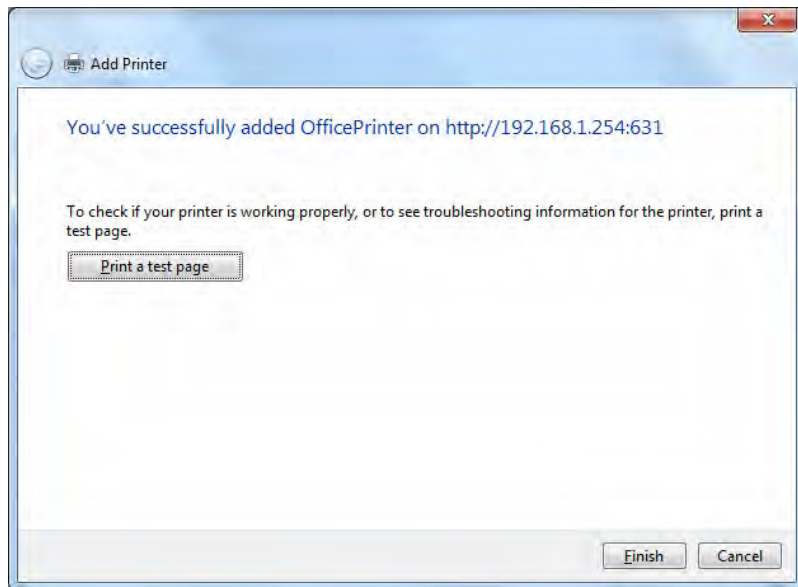
Step 6: Click “Next” to add the printer driver. If your printer is not listed and your printer came with an installation disk, click “Have Disk” find it and install the driver.



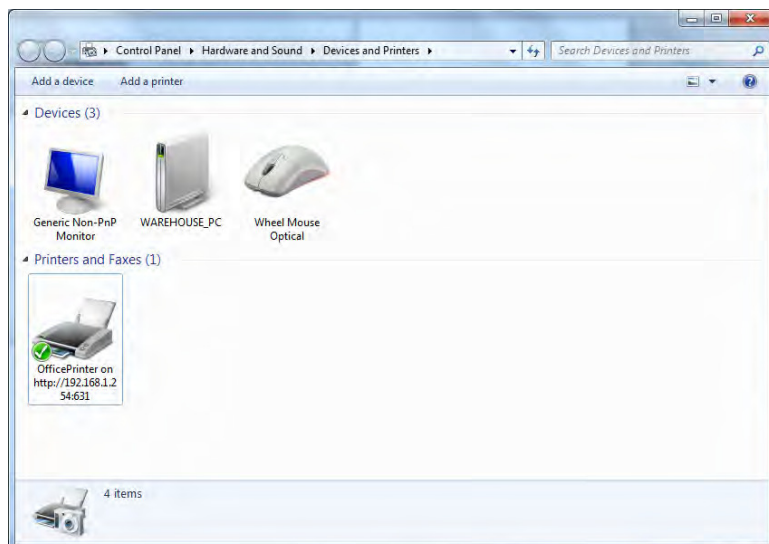
Step 7: Click “Next”



Step 8: Click “Next” and you are done



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



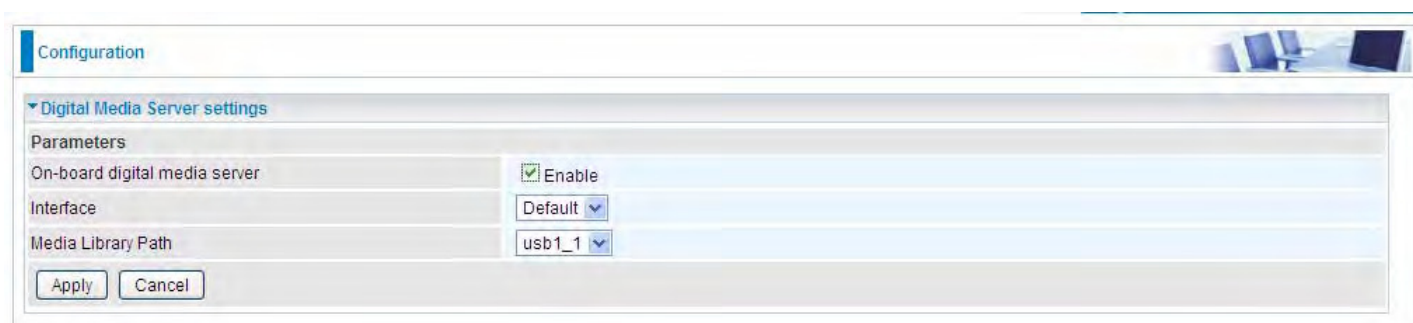
DLNA

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, 7820NZ can serve as a DLNA server.



The screenshot shows a web-based configuration interface. At the top, there is a 'Configuration' tab. Below it, a section titled 'Digital Media Server settings' is expanded. Under this section, there is a 'Parameters' table with three rows: 'On-board digital media server' with a checked 'Enable' checkbox, 'Interface' with a 'Default' dropdown menu, and 'Media Library Path' with a 'usb1_1' dropdown menu. At the bottom of the settings section, there are 'Apply' and 'Cancel' buttons.

Parameters	
On-board digital media server	☒ Enable
Interface	Default
Media Library Path	usb1_1

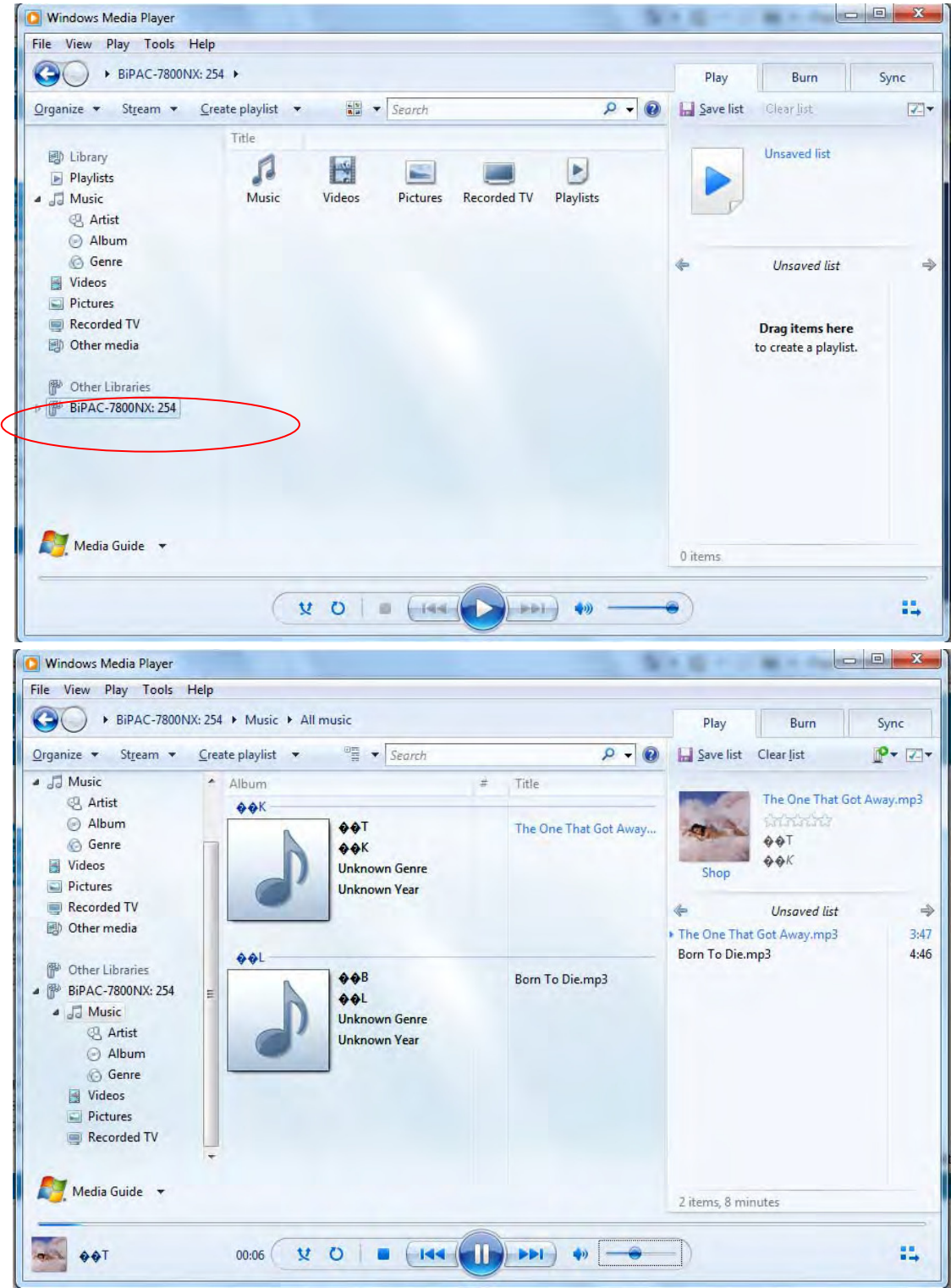
Apply Cancel

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.

Configuration

IPv6inIPv4

6in4 Tunnel Configuration

Name	WAN	LAN	Dynamic	V4 Common Bit Length	6rd Prefix with Prefix Length	Border Relay Address	Remove
Add Remove							

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

Configuration

6in4 Tunnel Configuration

Parameters

Tunnel Name

Mechanism

6RD

Associated WAN Interface

Associated LAN Interface

LAN/br0

Method

☒ Manual ☐ Automatic

V4 Common Bit Length

6rd Prefix with Prefix Length

Border Relay IPv4

Apply

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

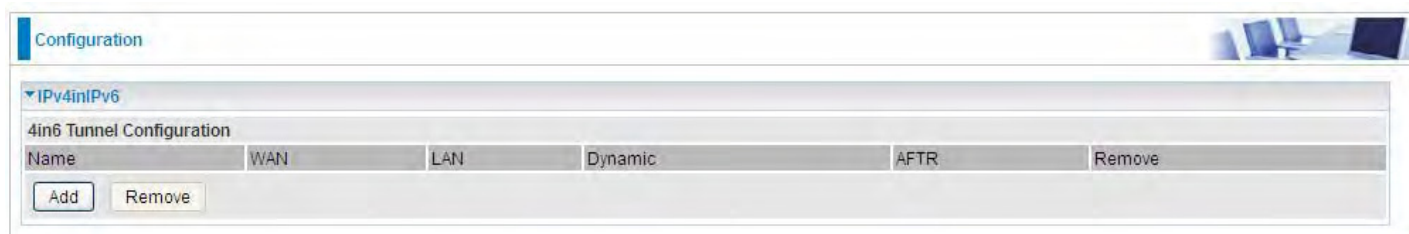
4in6 refers to tunneling of IPv4 in IPv6. It is an inherent internet interoperation mechanism allowing IPv4 to be used in an IPv6 only network.

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

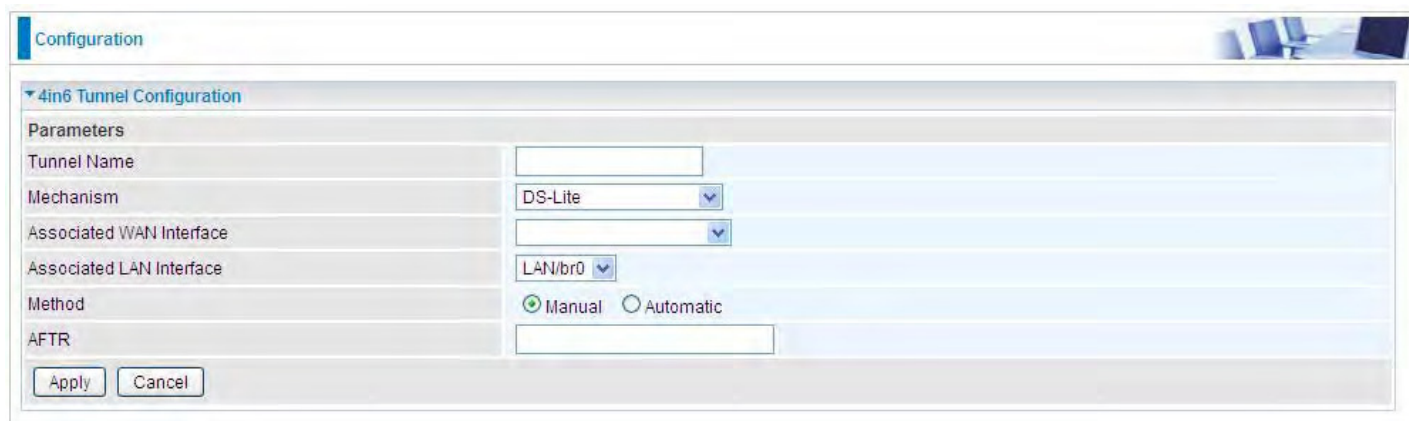
DS –Lite, or Dual-Stack Lite, is designed to let an ISP omit the deployment of any IPv4 address to the customer's CPE. Instead, only global IPv6 addresses are provided (Regular Dual-Stack Lite deploys global addresses for both IPv4 and IPv6).

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.



The screenshot shows a web interface titled "Configuration" with a sub-section "IPv4inIPv6". Below this is a "4in6 Tunnel Configuration" section containing a table with the following columns: Name, WAN, LAN, Dynamic, AFTR, and Remove. The table is currently empty. Below the table are two buttons: "Add" and "Remove".

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



The screenshot shows a "4in6 Tunnel Configuration" dialog box. It contains the following fields and options:

- Tunnel Name:** A text input field.
- Mechanism:** A dropdown menu with "DS-Lite" selected.
- Associated WAN Interface:** A dropdown menu.
- Associated LAN Interface:** A dropdown menu with "LAN/br0" selected.
- Method:** Radio buttons for "Manual" (selected) and "Automatic".
- AFTR:** A text input field.

At the bottom of the dialog are "Apply" and "Cancel" buttons.

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.

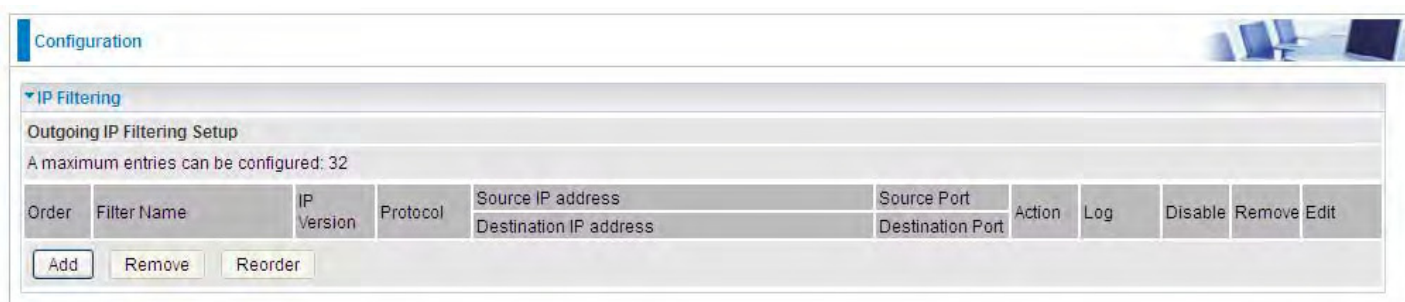
Security

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.

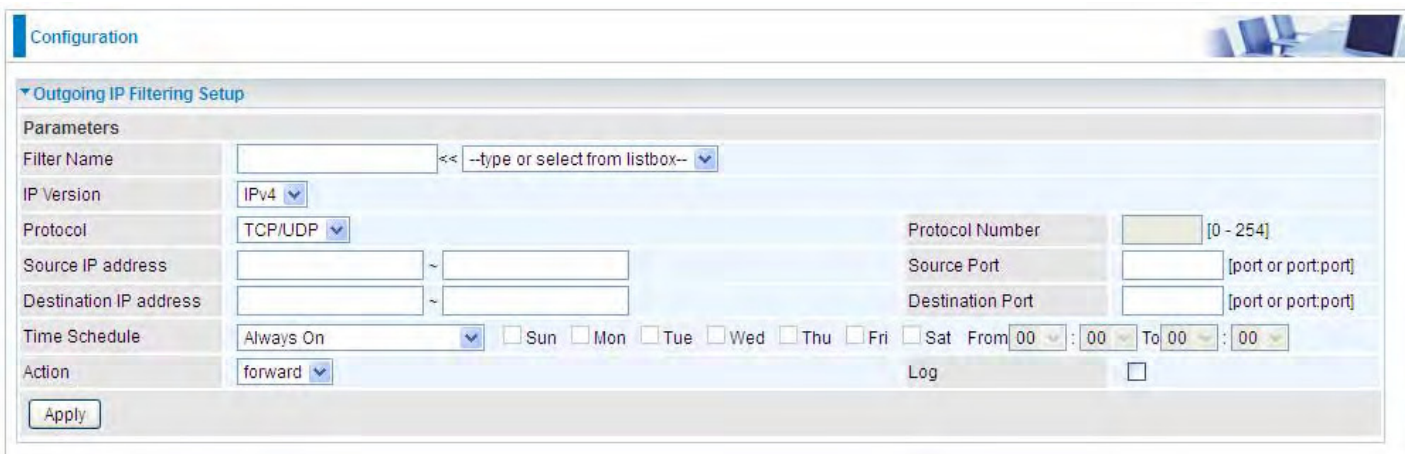
Outbound IP Filtering by default is set to **forward** all outgoing traffic from LAN to go through the router, but user can set rules to **block** the specific outgoing traffic.

Note: The maximum number of entries: 32.



The screenshot shows the 'Configuration' page with the 'IP Filtering' section expanded. Under 'Outgoing IP Filtering Setup', it states 'A maximum entries can be configured: 32'. Below this is a table with columns: Order, Filter Name, IP Version, Protocol, Source IP address, Destination IP address, Source Port, Destination Port, Action, Log, Disable, Remove, and Edit. At the bottom of the table are buttons for 'Add', 'Remove', and 'Reorder'.

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



The screenshot shows the 'Outgoing IP Filtering Setup' page. It contains the following fields and options:

- Filter Name:** A text input field followed by a dropdown menu labeled '--type or select from listbox--'.
- IP Version:** A dropdown menu currently set to 'IPv4'.
- Protocol:** A dropdown menu currently set to 'TCP/UDP'.
- Protocol Number:** A text input field with a range '[0 - 254]'.
- Source IP address:** Two text input fields separated by a tilde '~'.
- Destination IP address:** Two text input fields separated by a tilde '~'.
- Source Port:** A text input field with a range '[port or port:port]'.
- Destination Port:** A text input field with a range '[port or port:port]'.
- Time Schedule:** A dropdown menu set to 'Always On', followed by checkboxes for days of the week (Sun, Mon, Tue, Wed, Thu, Fri, Sat).
- Action:** A dropdown menu currently set to 'forward'.
- Log:** A checkbox.

An 'Apply' button is located at the bottom left of the form.

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	☐		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

~

Source Port

[port or port:port]

Destination IP address

~

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	Source Port	Action	Log	Disable	Remove	Edit
			Destination IP address	Destination Port					
FTP	4	TCP	Any	Any	forward	Enable	☒	☐	Edit
			Any	21					

Add

Remove

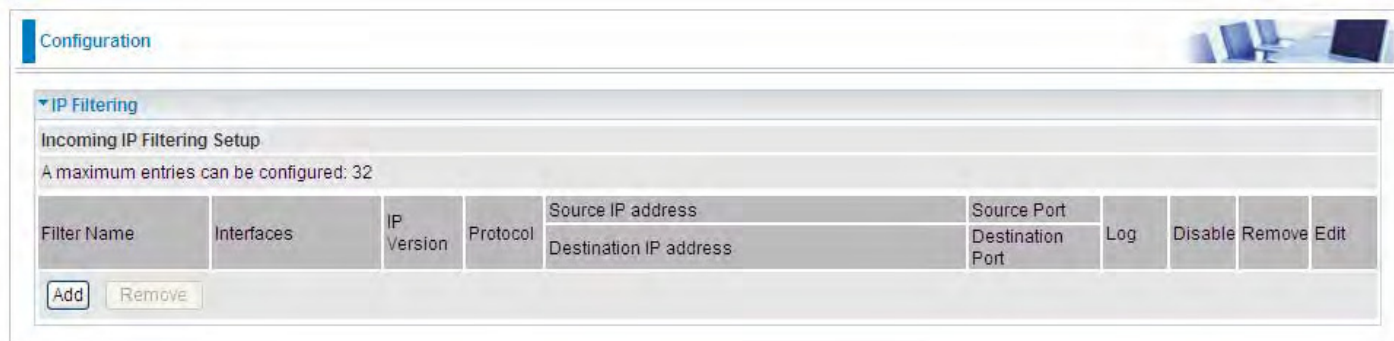
(Rule inactive)

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.

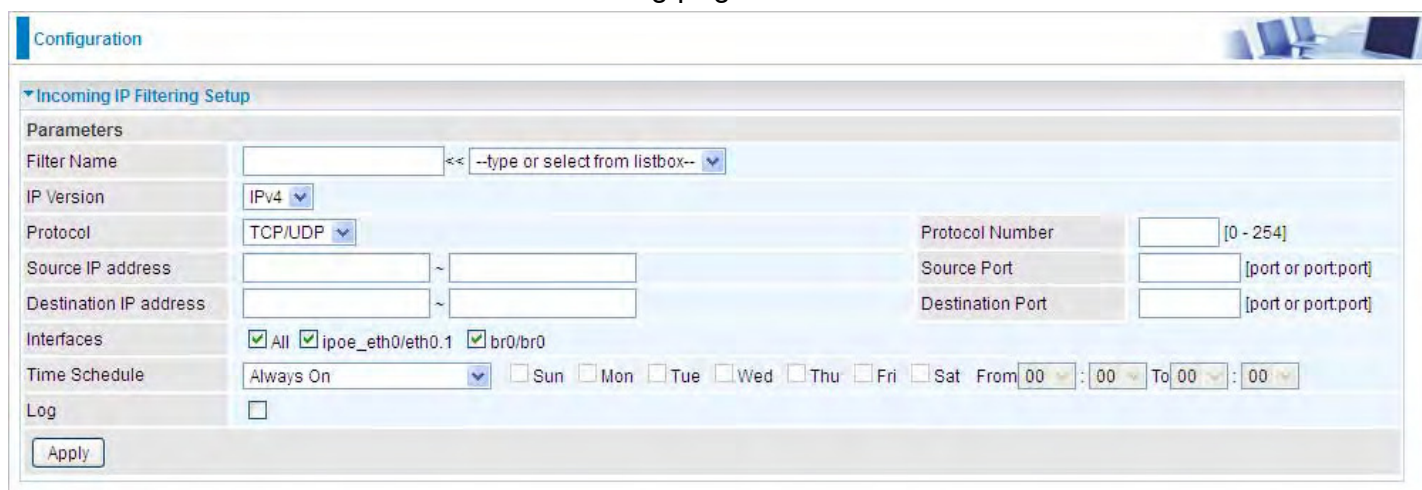
Note:

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.



The screenshot shows the 'Configuration' page with the 'IP Filtering' section expanded. Under 'Incoming IP Filtering Setup', it states 'A maximum entries can be configured: 32'. Below this is a table with columns: Filter Name, Interfaces, IP Version, Protocol, Source IP address, Source Port, Destination IP address, Destination Port, Log, Disable, Remove, and Edit. At the bottom of the table are 'Add' and 'Remove' buttons.

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



The screenshot shows the 'Incoming IP Filtering Setup' configuration page. It includes fields for Filter Name (with a dropdown), IP Version (IPv4), Protocol (TCP/UDP), Protocol Number (0-254), Source IP address, Destination IP address, Source Port, Destination Port, Interfaces (checkboxes for All, ipoe_eth0/eth0.1, br0/br0), Time Schedule (Always On, with day and time range options), and a Log checkbox. An 'Apply' button is at the bottom.

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](#).

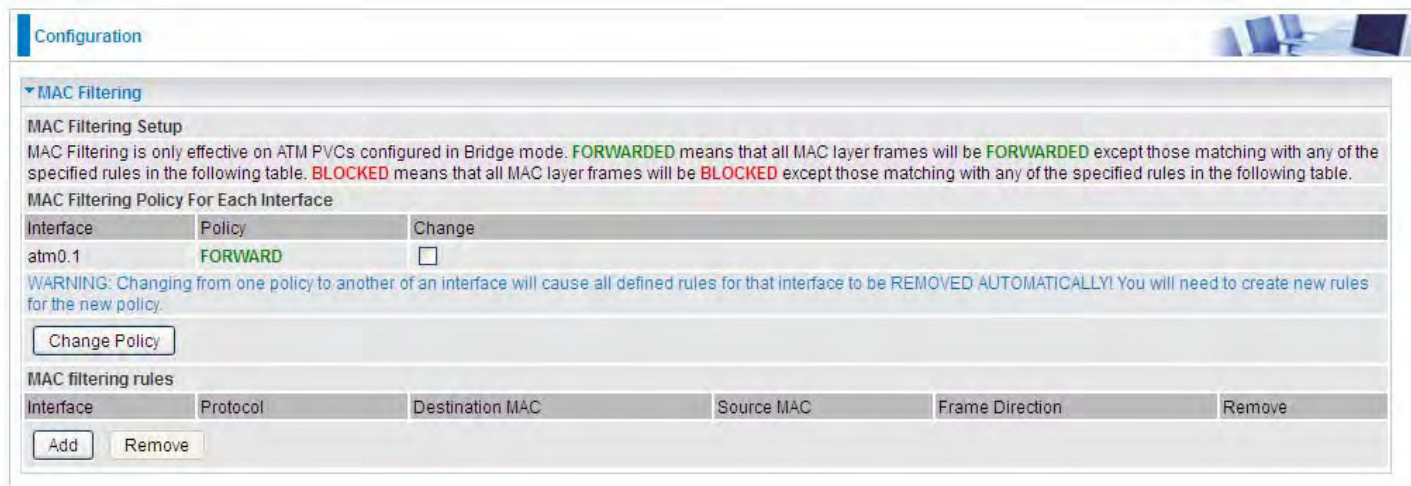
Log: check the check-box to record the security log. To check the log, users can turn to [Security Log](#).

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	☐

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.

Change Policy

MAC filtering rules

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

Add 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

Apply

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

Apply

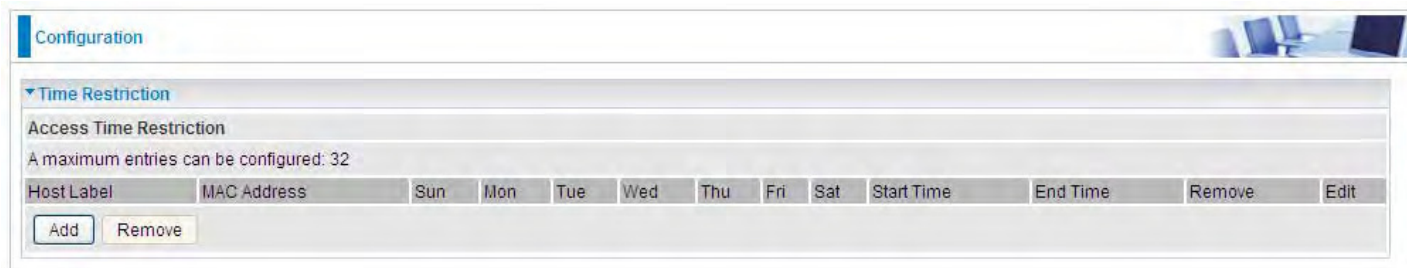
Cancel

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.

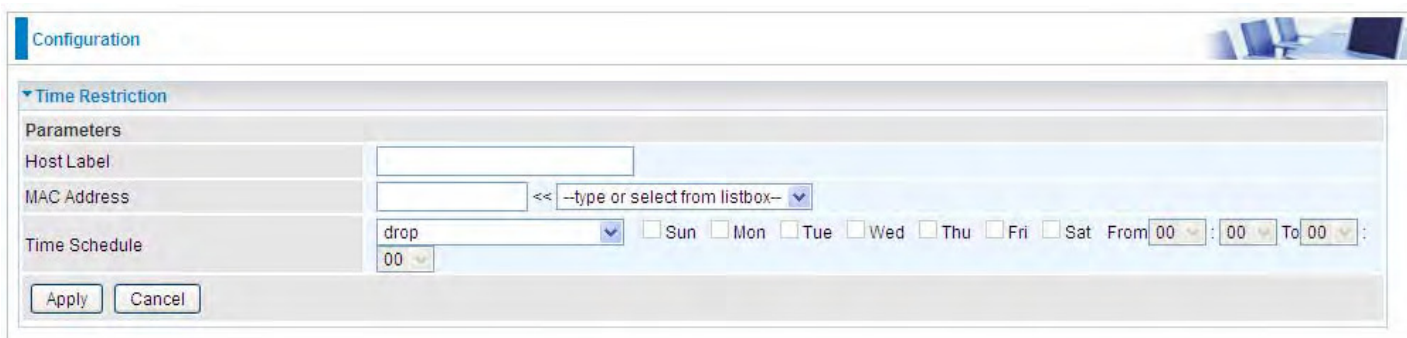
This page adds time of day restriction to a special LAN device connected to the router. To **Restrict** LAN device(s), please click Add button to add the device(s) from accessing internet under some set time. To find out the MAC address of a window based PC, go to command window, and type "ipconfig/all".

Note: The maximum entries configured: 32.



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

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). There are also 'From' and 'To' time selection fields. At the bottom are 'Apply' and 'Cancel' buttons.

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									☐	Edit
child-use	18:a9:05:04:12:23		x	x	x	x	x		00:00	23:59	☐	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.

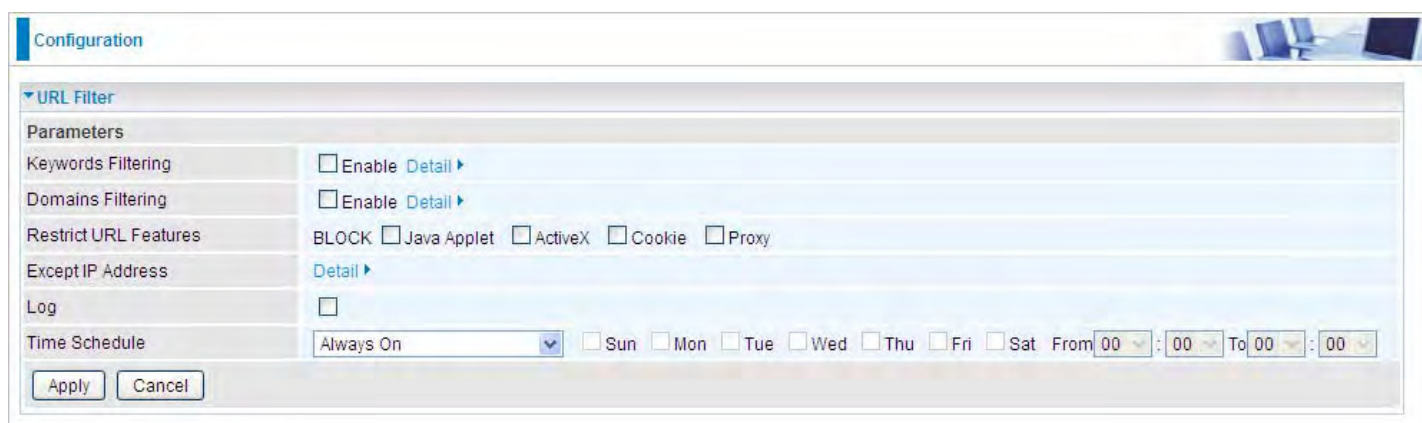
.

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.



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.

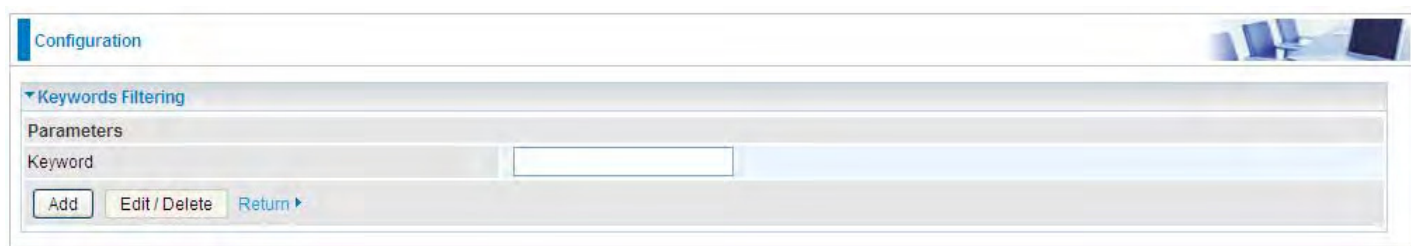
Time Schedule: Select or set exactly when the rule works. When set to “Always On”, the rule will work all time; and also you can set the precise time when the rule works, like 01:00-19:00 from Monday to Friday. Or you can select the already set timeslot in “**Time Schedule**” during which the rule works.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

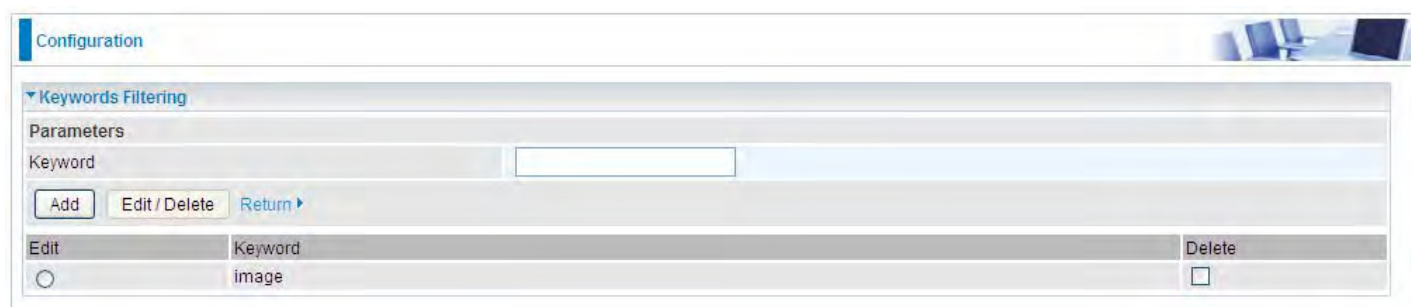
▼ Keywords Filtering

Parameters

Keyword

[Return ▶](#)

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



Configuration

▼ Keywords Filtering

Parameters

Keyword

[Return ▶](#)

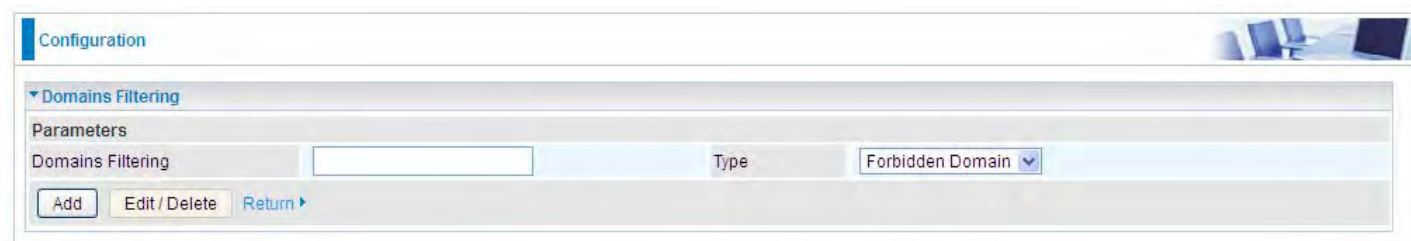
Edit	Keyword	Delete
☐	image	☐

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

[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 for configuring exception IP addresses. The main heading is 'Configuration'. Below it is a section titled 'Except IP Address'. Under this section, there is a 'Parameters' area. The 'IP Version' is set to 'IPv4' via a dropdown menu. The 'Internal IP Address' field is currently empty, followed by a tilde '~' and another empty field for a range. At the bottom of the configuration area, there are three buttons: 'Add', 'Edit / Delete', and 'Return ▶'.

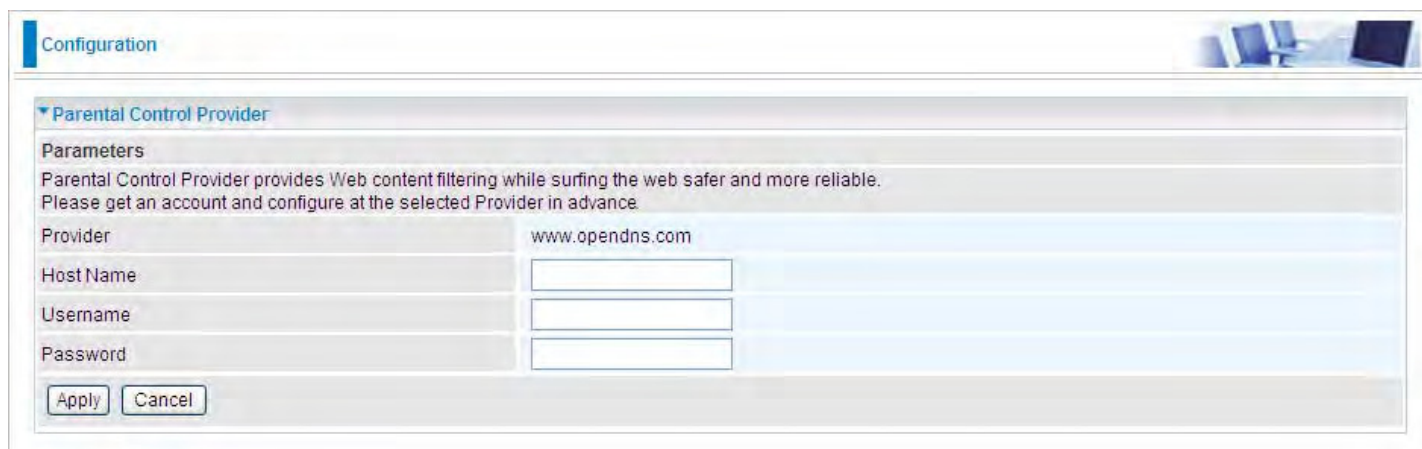
Enter the except IP address. Click **Add** to save your changes. The IP address will be entered into the **Exception List**, and excluded from the URL filtering rules in effect. For specific process, please refer to **Keywords Filtering**.

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](#)).



The screenshot shows a configuration window titled "Configuration" with a sub-section "Parental Control Provider". Under "Parameters", there is a descriptive text: "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." Below this, there are four input fields: "Provider" (pre-filled with "www.opendns.com"), "Host Name", "Username", and "Password". At the bottom left, there are "Apply" and "Cancel" buttons.

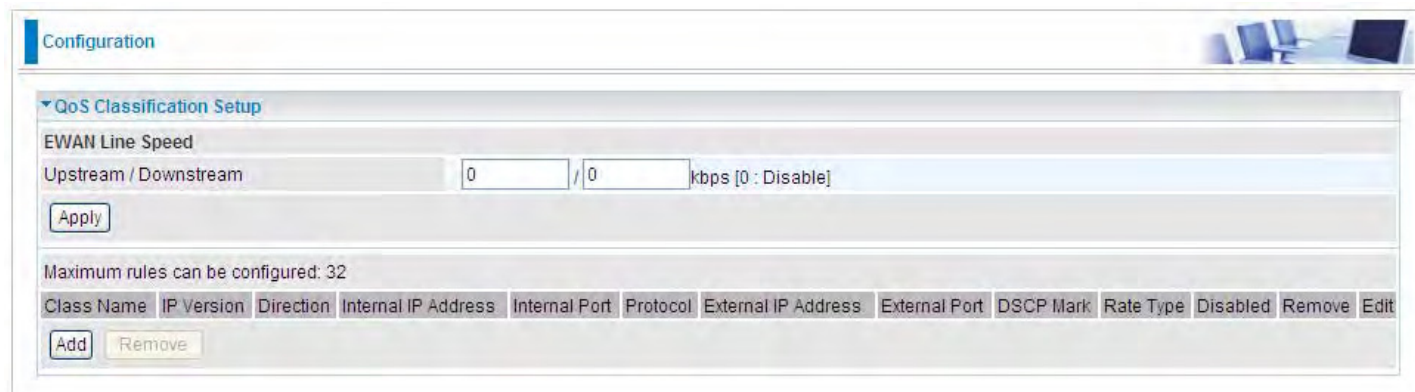
Parameters	
Parental Control Provider provides Web content filtering while surfing the web safer and more reliable. Please get an account and configure at the selected Provider in advance.	
Provider	www.opendns.com
Host Name	
Username	
Password	
Apply Cancel	

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.

Note: ADSL line speed is based on the ADSL sync rate. But there is no QoS on 3G/LTE as the 3G/LTE line speed is various and can not be known exactly.

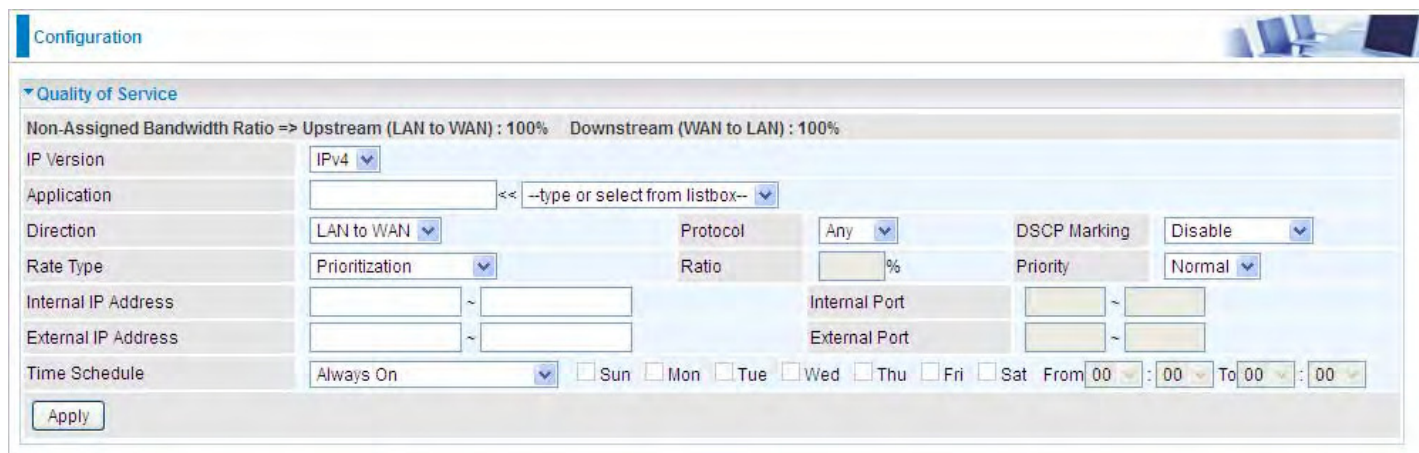


The screenshot shows the 'Configuration' page with the 'QoS Classification Setup' section expanded. It includes a form for 'EWAN Line Speed' with 'Upstream / Downstream' rate inputs (both set to 0) and a unit dropdown set to 'kbps [0 : Disable]'. Below this is an 'Apply' button. A message states 'Maximum rules can be configured: 32'. At the bottom is a table with columns: Class Name, IP Version, Direction, Internal IP Address, Internal Port, Protocol, External IP Address, External Port, DSCP Mark, Rate Type, Disabled, Remove, and Edit. There are 'Add' and 'Remove' buttons below the table.

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.



The screenshot shows the 'Configuration' page with the 'Quality of Service' section expanded. It displays 'Non-Assigned Bandwidth Ratio => Upstream (LAN to WAN) : 100% Downstream (WAN to LAN) : 100%'. The form includes fields for 'IP Version' (set to IPv4), 'Application' (with a search box and a dropdown), 'Direction' (set to LAN to WAN), 'Protocol' (set to Any), 'DSCP Marking' (set to Disable), 'Rate Type' (set to Prioritization), 'Ratio' (with a percentage input), 'Priority' (set to Normal), 'Internal IP Address' and 'Internal Port' ranges, 'External IP Address' and 'External Port' ranges, and a 'Time Schedule' section with checkboxes for days of the week and a time range (From 00:00 To 00:00). An 'Apply' button is at the bottom.

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, you 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. If you have ADSL LINE with 256K/bps.rate, the estimated data rate, in kbps, for this rule is $20\% \times 256 \times 0.9 = 46\text{kbps}$. (For 0.9 is an estimated factor for the effective data transfer rate for an ADSL LINE from LAN to WAN. For WAN-to-LAN, it is 0.85 to 0.8)

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.

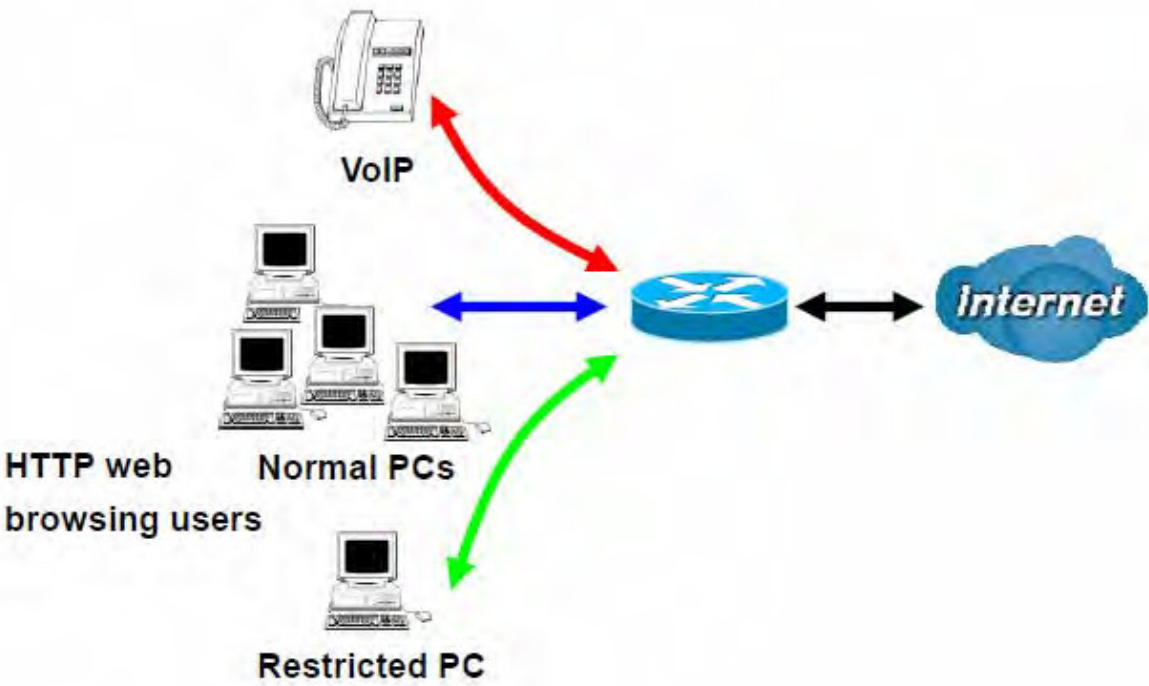
External Port: The Port number on the remote / WAN side.

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.

Configuration

Quality of Service

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

IP Version	IPv4			
Application	Voip << --type or select from listbox--			
Direction	LAN to WAN	Protocol	Any	
Rate Type	Prioritization	Ratio	%	
Internal IP Address			DSCP Marking	EF(101110)
External IP Address			Priority	High
Time Schedule	timeslot1 ☐ Sun ☒ Mon ☒ Tue ☒ Wed ☒ Thu ☒ Fri ☐ Sat From 00 : 00 To 09 : 19			

Apply

- 2. Give regular web http access a limited rate

Configuration

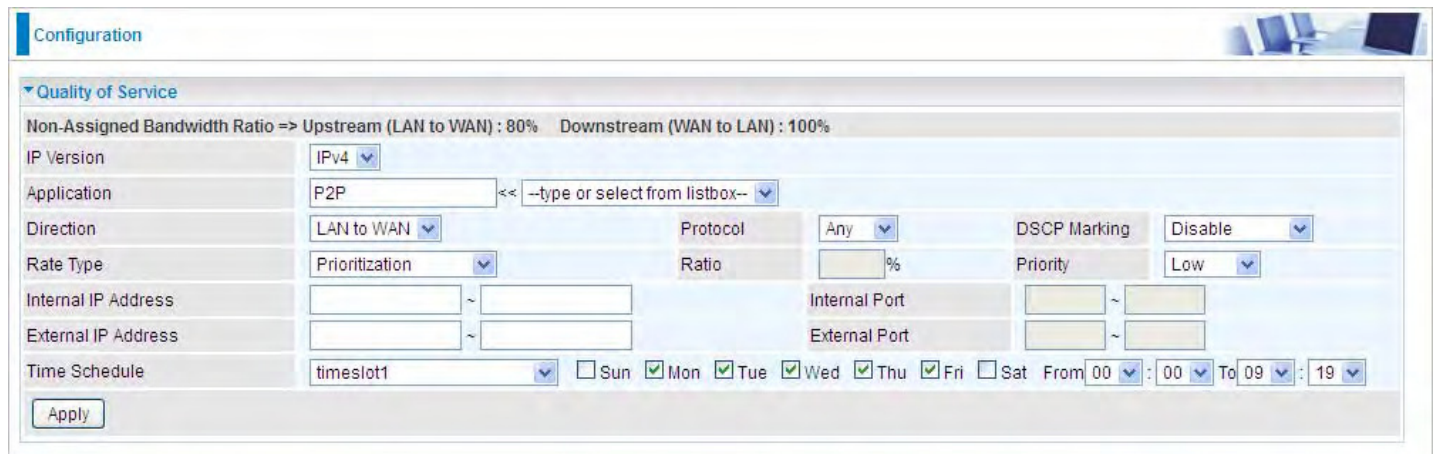
Quality of Service

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

IP Version	IPv4			
Application	HTTP << HTTP(TCP 80)			
Direction	LAN to WAN	Protocol	TCP	
Rate Type	Limited (Maximum)	Ratio	20 %	
Internal IP Address			DSCP Marking	Disable
External IP Address			Priority	Normal
Time Schedule	timeslot1 ☐ Sun ☒ Mon ☒ Tue ☒ Wed ☒ Thu ☒ Fri ☐ Sat From 00 : 00 To 09 : 19			

Apply

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 displays a network configuration window titled "Configuration". Inside, there is a section for "Quality of Service". At the top, it shows "Non-Assigned Bandwidth Ratio => Upstream (LAN to WAN) : 80% Downstream (WAN to LAN) : 100%". Below this, various settings are configured for a P2P application:

- IP Version:** IPv4
- Application:** P2P (with a dropdown menu for "--type or select from listbox--")
- Direction:** LAN to WAN
- Protocol:** Any
- DSCP Marking:** Disable
- Rate Type:** Prioritization
- Ratio:** (empty field) %
- Priority:** Low
- Internal IP Address:** (empty field) ~ (empty field)
- External IP Address:** (empty field) ~ (empty field)
- Internal Port:** (empty field) ~ (empty field)
- External Port:** (empty field) ~ (empty field)
- Time Schedule:** timeslot1 (dropdown), with checkboxes for days: Sun (unchecked), Mon (checked), Tue (checked), Wed (checked), Thu (checked), Fri (checked), Sat (unchecked). Time range: From 00:00 To 09:19.

An "Apply" button is located at the bottom left of the configuration section.

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

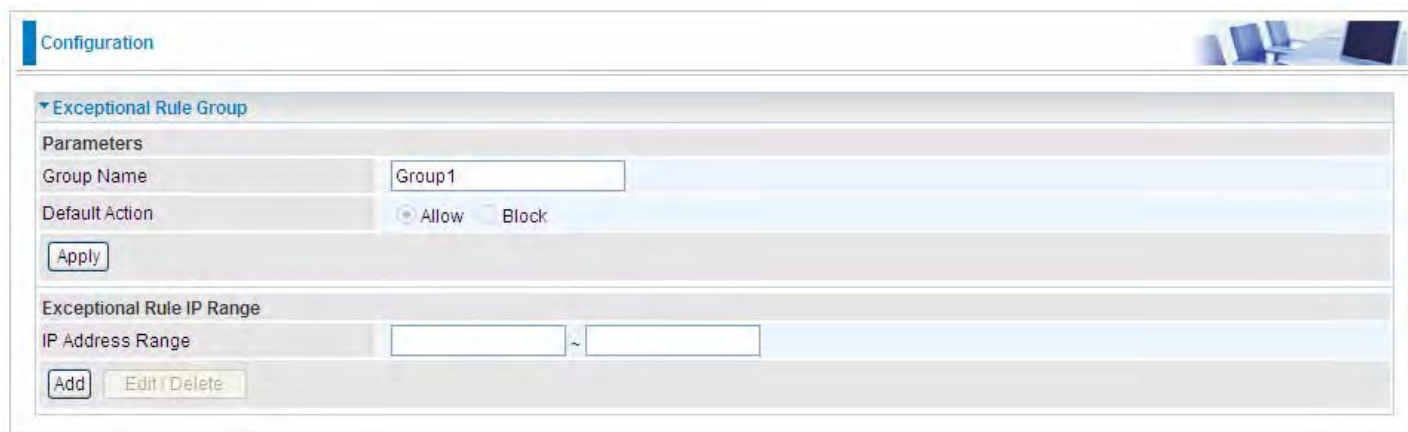
Exceptional Rule is dedicated to giving or blocking Virtual Server/ DMZ access to some specific IP or IPs(range). Users are allowed to set 8 different exceptional rule groups at most. In each group, user can add specific IP or IP range.



The screenshot shows the 'Configuration' page with a tab for 'Exceptional Rule Group'. Below the tab is a table with the following columns: Group Index, Group Name, Default Action, Exceptional Rule IP Range, and Edit. There are 8 rows, each representing a group from Group1 to Group8. All 'Default Action' values are set to 'Allow'. Each row has an 'Edit' button in the 'Exceptional Rule IP Range' column.

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).



The screenshot shows the 'Configuration' page with a tab for 'Exceptional Rule Group'. Below the tab is a form for editing a group. The form has two main sections: 'Parameters' and 'Exceptional Rule IP Range'. In the 'Parameters' section, there is a 'Group Name' field with 'Group1' entered, a 'Default Action' section with radio buttons for 'Allow' (selected) and 'Block', and an 'Apply' button. In the 'Exceptional Rule IP Range' section, there is an 'IP Address Range' field with two input boxes separated by a tilde (~), and buttons for 'Add', 'Edit', and '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
☐	Block	172.16.1.102 ~ 172.16.1.106	☐
☐	Block	172.16.1.108 ~ 172.16.1.108	☐

176

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.

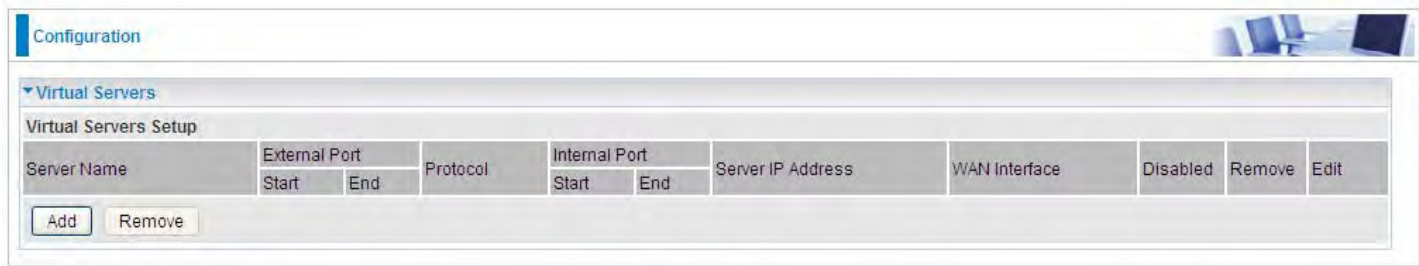
If you wish to run a server on your network that can be accessed from the WAN (i.e. from other machines on the Internet that are outside your local network), or any application that can accept incoming connections (e.g. Peer-to-peer/P2P software such as instant messaging applications and P2P file-sharing 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.



The screenshot shows a web interface for configuring virtual servers. At the top, there's a 'Configuration' tab. Below it, a section titled 'Virtual Servers' is expanded. Under this, there's a 'Virtual Servers Setup' section. It contains a table with the following columns: 'Server Name', 'External Port' (with sub-columns 'Start' and 'End'), 'Protocol', 'Internal Port' (with sub-columns 'Start' and 'End'), 'Server IP Address', 'WAN Interface', 'Disabled', 'Remove', and 'Edit'. Below the table, there are 'Add' and 'Remove' buttons.

Server Name	External Port		Protocol	Internal Port		Server IP Address	WAN Interface	Disabled	Remove	Edit
	Start	End		Start	End					
Add Remove										

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

The following configuration page will appear to let you configure.

Virtual Servers

Parameters

Interface

pppoe_0_8_35/ppp0.1

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

Exceptional Rule Group

None

External Port

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

Apply

Cancel

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.

Virtual Servers

Parameters

Interface

pppoe_0_8_35/ppp0.1

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			
		TCP			

Apply

Cancel

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

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					
Age of Empires	47624	47624	TCP	47624	47624	192.168.1.103	ppp0.1		☐	Edit
Age of Empires	6073	6073	TCP	6073	6073	192.168.1.103	ppp0.1		☐	Edit
Age of Empires	2300	2400	TCP	2300	2400	192.168.1.103	ppp0.1		☐	Edit
Age of Empires	2300	2400	UDP	2300	2400	192.168.1.103	ppp0.1		☐	Edit

Add

Remove

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					
Age of Empires	47624	47624	TCP	47624	47624	192.168.1.103	ppp0.1	✓	☐	Edit
Age of Empires	6073	6073	TCP	6073	6073	192.168.1.103	ppp0.1		☐	Edit
Age of Empires	2300	2400	TCP	2300	2400	192.168.1.103	ppp0.1		☐	Edit
Age of Empires	2300	2400	UDP	2300	2400	192.168.1.103	ppp0.1		☐	Edit

Add
Remove

( 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.

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					
Age of Empires	47624	47624	TCP	47624	47624	192.168.1.103	ppp0.1	✓	☐	Edit
Age of Empires	6073	6073	TCP	6073	6073	192.168.1.103	ppp0.1		☐	Edit
Age of Empires	2300	2400	TCP	2300	2400	192.168.1.103	ppp0.1		☐	Edit
Age of Empires	2300	2400	UDP	2300	2400	192.168.1.103	ppp0.1		☒	Edit

Add
Remove

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.

Configuration

DMZ Host

Parameters

DMZ Host IP Address

Time Schedule

Exceptional Rule Group

Apply

Cancel

Configuration

DMZ Host

Parameters

DMZ Host IP Address

Time Schedule

Exceptional Rule Group

Apply

Cancel

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.

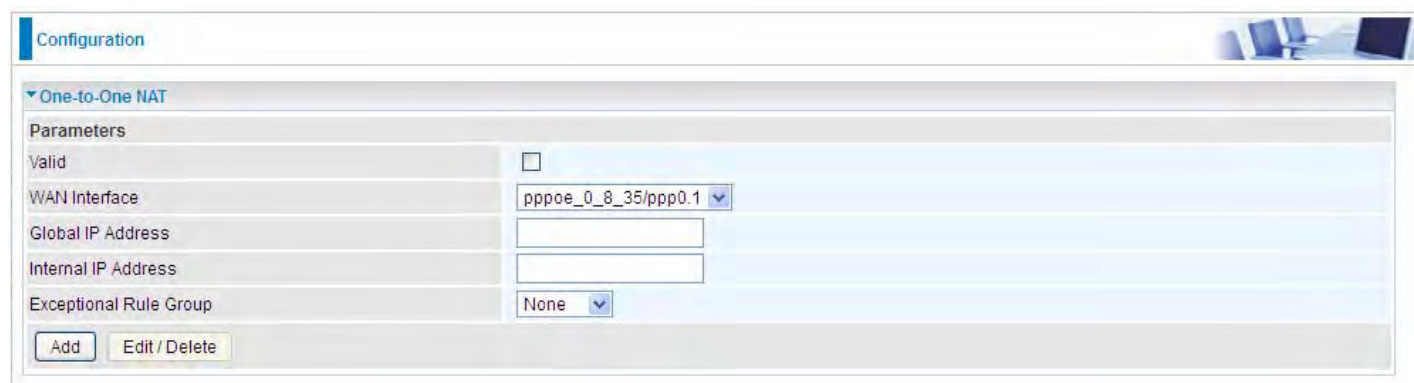
Using port mapping does have security implications, since outside users are able to connect to PCs on your network. For this reason you are advised to use specific Virtual Server entries just for the ports your application requires instead of simply using DMZ or creating a Virtual Server entry for “All” 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.



The screenshot shows a web-based configuration interface for 'One-to-One NAT'. The interface is titled 'Configuration' and has a sub-tab 'One-to-One NAT'. Under the 'Parameters' section, there are several fields: 'Valid' with a checkbox, 'WAN Interface' with a dropdown menu showing 'pppoe_0_8_35/ppp0.1', 'Global IP Address' with an empty text box, 'Internal IP Address' with an empty text box, and 'Exceptional Rule Group' with a dropdown menu showing 'None'. At the bottom of the configuration area, there are two buttons: 'Add' and 'Edit / Delete'.

Valid: Check whether to validate 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.

For example, you have an ADSL connection of pppoe_0_8_35/ppp0.1 interface with three fixed global IP, and you then can assign the other two global IPs to two internal devices respectively.

If you have a WEB server (IP address: 192.168.1.3) and a FTP server (IP address: 192.168.1.4) in local network, owning a public IP address range of 123.1.1.2 to 123.1.1.4 assigned by ISP. 123.1.1.2 is used as WAN IP address of the router, 123.1.1.3 is used for WEB server and 123.1.1.4 is used for FTP server. With One-to-One NAT, the servers with private IP addresses can be accessed at the corresponding valid public IP addresses.

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.

The screenshot shows the 'Port Triggering Setup' configuration page. It features a table with columns for 'Trigger' (Protocol, Port Range) and 'Open' (Protocol, Port Range). The 'Port Range' column is further divided into 'Start' and 'End' sub-columns. To the right of the table are columns for 'WAN Interface', 'Remove', and 'Edit'. Below the table are 'Add' and 'Remove' buttons.

Application	Trigger		Open			WAN Interface	Remove	Edit
	Protocol	Port Range	Protocol	Port Range				
		Start End		Start End				
Add Remove								

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

The screenshot shows the 'Port Triggering Parameters' configuration page. It includes dropdown menus for 'Interface' (set to 'pppoe_0_8_35/ppp0.1') and 'Application' (set to 'Custom Application'). Below these is a text field for 'Custom Application'. The main section is a table for defining trigger and open ports, with columns for 'Trigger Port' (Start, End), 'Trigger Protocol', 'Open Port' (Start, End), and 'Open Protocol'. The table contains eight rows, each with a 'TCP' protocol dropdown. An 'Apply' button is at the bottom left.

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

- ① **Start:** Enter a port number as the triggering port starting number.
 - ① **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

① **Start:** Enter a port number as the open port starting number.

① **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.

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

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

Application	Trigger		Open			WAN Interface	Remove	Edit
	Protocol	Port Range	Protocol	Port Range				
				Start	End			
Aim Talk	TCP	4099 - 4099	TCP	5191	5191	ppp0.1	☐	Edit

 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.

Configuration

Port Triggering

Port Triggering Setup

Application	Trigger			Open			WAN Interface	Remove	Edit			
	Protocol	Port Range		Protocol	Port Range							
		Start	End		Start	End						
Aim Talk	TCP	4099	4099	TCP	5191	5191	ppp0.1	☒	Edit			

Add

Remove

ALG

The ALG Controls enable or disable protocols over application layer.



The screenshot shows a 'Configuration' window with a tab labeled 'ALG'. Under the 'Parameters' section, there are three rows: 'SIP', 'H.323', and 'IPSec'. Each row has two radio buttons: 'Enable' (which is selected) and 'Disable'. At the bottom of the window, there are 'Apply' and 'Cancel' buttons.

Parameters	Enable	Disable
SIP	☒	☐
H.323	☒	☐
IPSec	☒	☐

SIP: Enable the SIP ALG when SIP phone needs ALG to pass through the NAT. Disable the SIP when SIP phone includes NAT-Traversal algorithm.

H.323: Enable to secure the voice communication using H.323 protocol when one or both terminals are behind a NAT.

IPSec: Enable IPSec ALG to allow one or both peers to reside behind a NAT gateway (i.e., doing address- or port-translation).

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
☐	11	SMTWTFs	08:00	☐

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.



▼ Wake On LAN

Parameters

Host Label

MAC Address << --select-- (type or select from listbox)

Wake by Schedule ☐ Enable [Schedule](#)

[Add](#)[Edit / Delete](#)

Edit	Action	Host Label	MAC Address	Ready	Delete
☐	Schedule	billion-17bc6f1	18:A9:05:38:04:03	Yes	☐

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
Add	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.

The screenshot shows the 'VPN' configuration window with the 'IPSec' tab selected. The 'IPSec Settings' section includes a checkbox for 'L2TP over IPsec', a 'Connection Name' field, a 'WAN Interface' dropdown (set to 'Default'), an 'IP Version' dropdown (set to 'IPv4'), and fields for 'Local Network' (Single Address), 'Remote Security Gateway', 'Remote Network' (Single Address), 'Key Exchange Method' (IKE), 'IPsec Protocol' (ESP), 'Pre-Shared Key', 'Local ID Type' (Default), and 'Remote ID Type' (Default). Below these are 'Phase 1' and 'Phase 2' settings, including 'Mode' (Main), 'Encryption Algorithm' (3DES), 'Integrity Algorithm' (MD5), 'DH Group' (MODP1024(DH2)), 'SA Lifetime' (480), 'IPsec Lifetime' (60), 'Keep Alive' (None), and 'MTU' (0). An 'Apply' button is located at the bottom left.

IPSec Settings

L2TP over IPSec: Select Enable if user wants to use L2TP over IPSec. See [L2TPover 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, when you select adsl pppoe_0_0_35/ppp0.1 interface, the IPSec tunnel would transmit data via this interface to connect to the remote peer.

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 1 to 32 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.

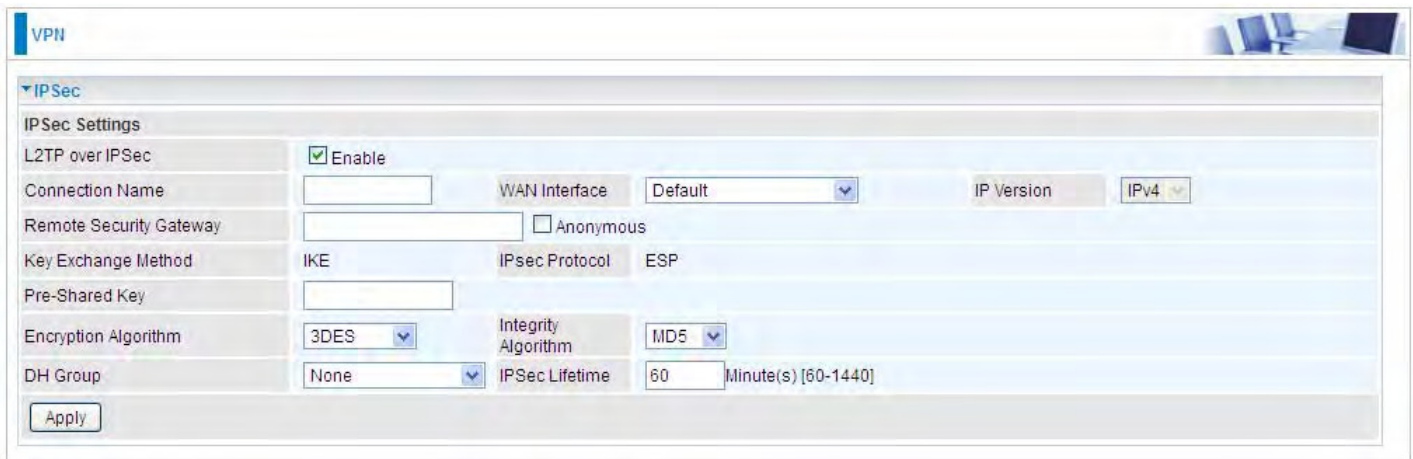
Ping IP (0.0.0.0 : NEVER)	0.0.0.0	Interval	10	Second(s) [0-3600, 0 : NEVER]
---------------------------	---------	----------	----	-------------------------------

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



The screenshot shows a web-based configuration interface for a VPN. The 'VPN' tab is selected at the top. Below it, the 'IPSec' sub-tab is active. The 'IPSec Settings' section contains the following fields:

- L2TP over IPSec:** A checkbox labeled 'Enable' which is checked.
- Connection Name:** An empty text input field.
- WAN Interface:** A dropdown menu with 'Default' selected.
- IP Version:** A dropdown menu with 'IPv4' selected.
- Remote Security Gateway:** An empty text input field.
- Anonymous:** An unchecked checkbox.
- Key Exchange Method:** A dropdown menu with 'IKE' selected.
- IPsec Protocol:** A dropdown menu with 'ESP' selected.
- Pre-Shared Key:** An empty text input field.
- Encryption Algorithm:** A dropdown menu with '3DES' selected.
- Integrity Algorithm:** A dropdown menu with 'MD5' selected.
- DH Group:** A dropdown menu with 'None' selected.
- IPsec Lifetime:** A text input field with '60' and a label 'Minute(s) [60-1440]'.

An 'Apply' button is located at the bottom left of the settings area.

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 1 to 32 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.

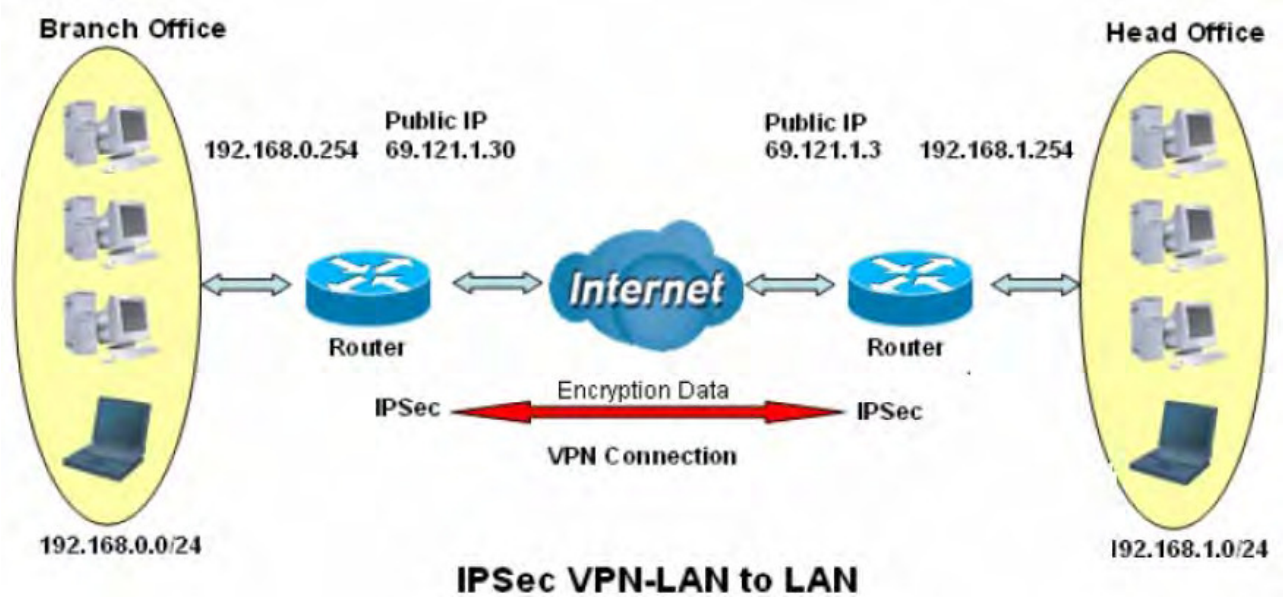
IPSec Lifetime: Specify the number of minutes that IPSec will stay active before new encryption and authentication key will be exchanged. Enter a value to negotiate and establish secure authentication. Default is 60 minutes (3600 seconds). A short time increases security by forcing the two parties to 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 BiPAC 7820NZs 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(Hostanme)	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	☐ 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	☐ 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)		

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	

VPN

IPSec

IPSec Settings

L2TP over IPSec

☐ 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

Anonymous

☐ 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

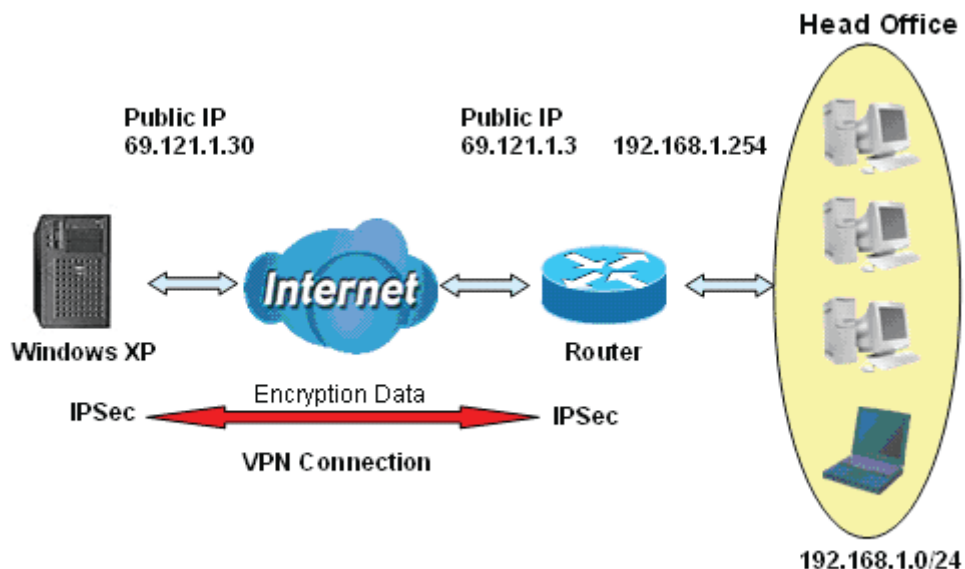
1500

(0 : Default)

Apply

3. Host to LAN

Router servers as VPN server, and host should install the IPSec client to connect to head office through IPSec VPN.



IPSec VPN-Host to LAN

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	



▼ IPsec

IPsec Settings

L2TP over IPsec	☐ Enable		
Connection Name	Headoffice-to-H	WAN Interface	Default
Local Network	Subnet	IP Address	192.168.1.0
Remote Security Gateway	69.121.1.30	☐ Anonymous	
Remote Network	Single Address	IP Address	69.121.1.30
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
DH Group	MODP1024(DH2)
Integrity Algorithm	MD5
SA Lifetime	480 Minute(s) [60-1440]

Phase 2

Encryption Algorithm	3DES
DH Group	None
Integrity Algorithm	MD5
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)

VPN Account

PPTP and L2TP server share the same account database set in VPN Account page.

VPN

VPN Account

VPN Account applied to PPTP/L2TP/OpenVPN Server.

Parameters

Name

Username

Connection Type ☒ Remote Access ☐ LAN to LAN

Peer Network IP

Tunnel ☒ Enable ☐ Disable

Password

Peer Netmask

Add Edit / Delete

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.

Configuration

▼ Exceptional Rule Group

Parameters

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 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

Group1

Default Action

☒ Allow

☐ Block

Apply

Exceptional Rule IP Range

IP Address Range

~

Add

Edit / Delete

Edit	Action	IP Address Range	Delete
☐	Block	172.16.1.102 ~ 172.16.1.106	☐
☐	Block	172.16.1.108 ~ 172.16.1.108	☐

201

PPTP

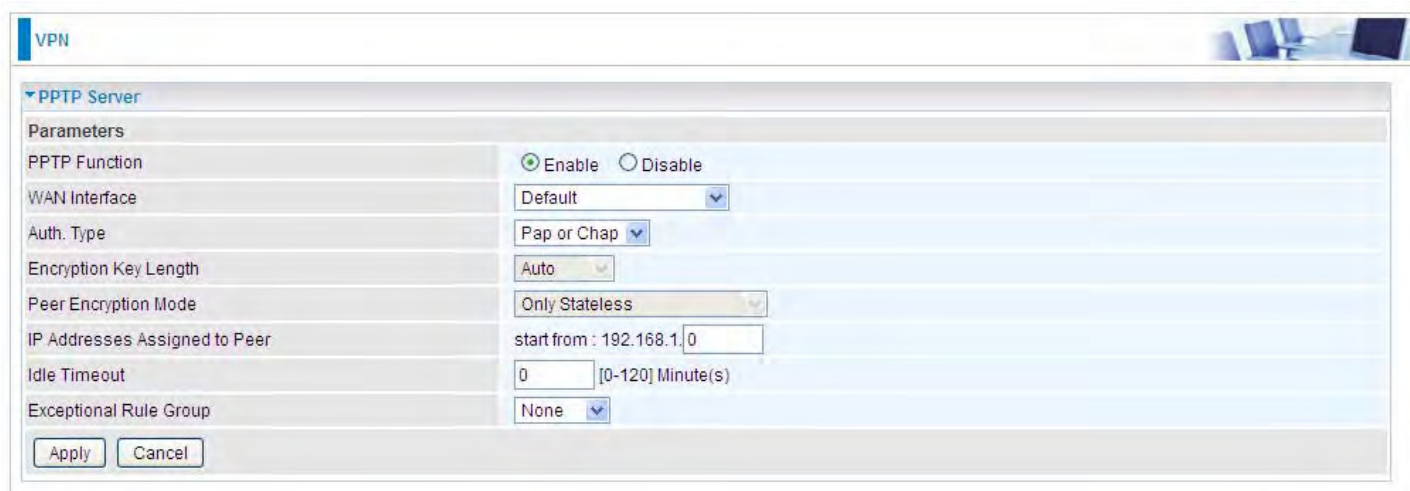
The **Point-to-Point Tunneling Protocol** (PPTP) is a Layer2 tunneling protocol for implementing virtual private networks through IP network. PPTP uses an enhanced GRE (Generic Routing Encapsulation) mechanism to provide a flow- and congestion-controlled encapsulated datagram service for carrying PPP 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 constitutes the PPTP Server setting.



The screenshot shows the 'PPTP Server' configuration window. It has a 'Parameters' section with the following fields:

- PPTP Function:** Radio buttons for 'Enable' (selected) and 'Disable'.
- WAN Interface:** A dropdown menu showing 'Default'.
- Auth. Type:** A dropdown menu showing 'Pap or Chap'.
- Encryption Key Length:** A dropdown menu showing 'Auto'.
- Peer Encryption Mode:** A dropdown menu showing 'Only Stateless'.
- IP Addresses Assigned to Peer:** A text field with 'start from : 192.168.1.0'.
- Idle Timeout:** A text field with '0' and a unit selector '[0-120] Minute(s)'.
- Exceptional Rule Group:** A dropdown menu showing 'None'.

At the bottom of the window are 'Apply' and 'Cancel' buttons.

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

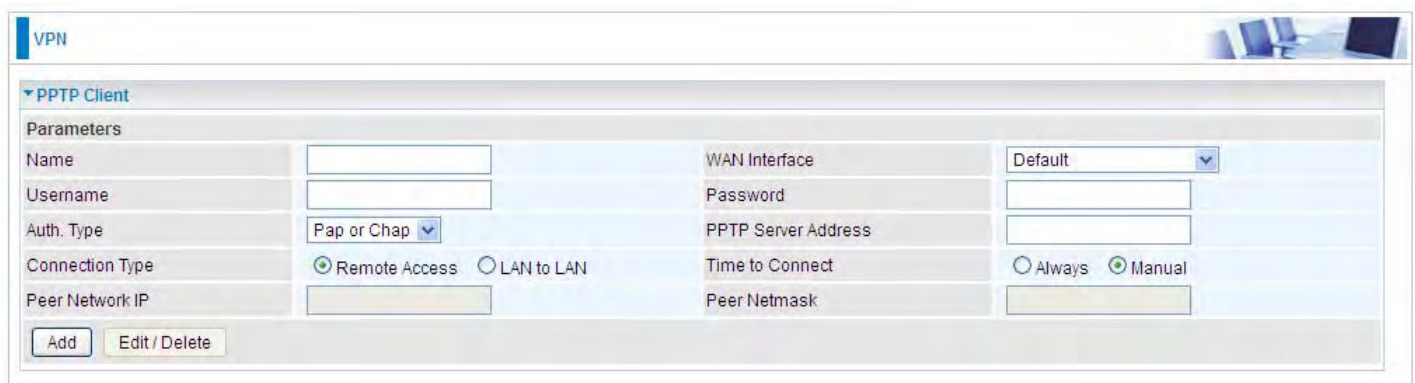
minutes.

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.



The screenshot shows a web-based configuration interface for a VPN. At the top, there is a 'VPN' tab. Below it, the 'PPTP Client' section is expanded. Under the 'Parameters' heading, there are two columns of fields. The left column includes 'Name' (text input), 'Username' (text input), 'Auth. Type' (dropdown menu with 'Pap or Chap' selected), 'Connection Type' (radio buttons for 'Remote Access' and 'LAN to LAN', with 'Remote Access' selected), and 'Peer Network IP' (text input). The right column includes 'WAN Interface' (dropdown menu with 'Default' selected), 'Password' (text input), 'PPTP Server Address' (text input), 'Time to Connect' (radio buttons for 'Always' and 'Manual', with 'Manual' selected), and 'Peer Netmask' (text input). At the bottom left of the form, there are two buttons: 'Add' and '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.

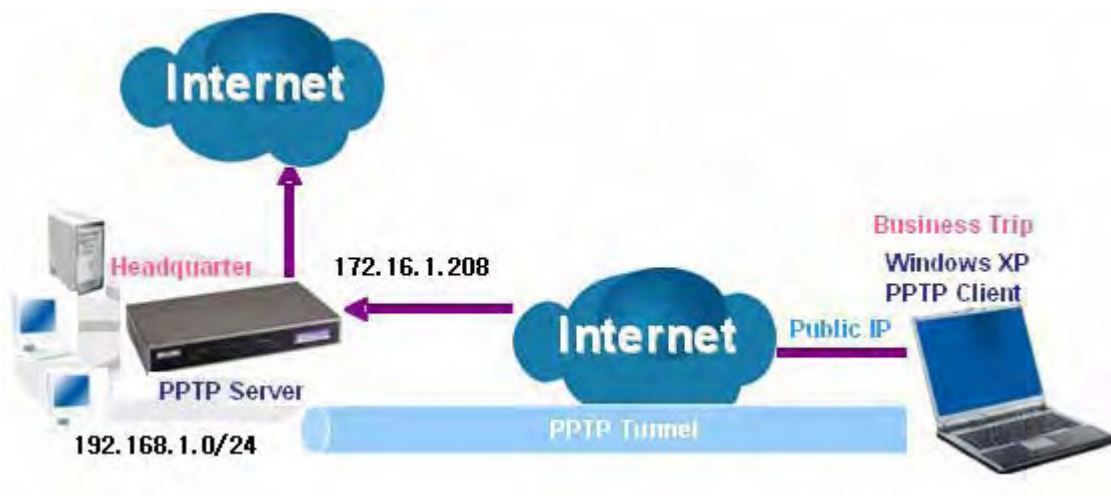
Peer Network IP: Please input the subnet IP for Server peer.

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 window with the 'PPTP Server' tab selected. The 'Parameters' section includes the following settings:

- 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

Buttons for 'Apply' and 'Cancel' are at the bottom left.

2. Create a PPTP Account "test".

The screenshot shows the 'VPN' configuration window with the 'VPN Account' tab selected. The 'Parameters' section includes the following settings:

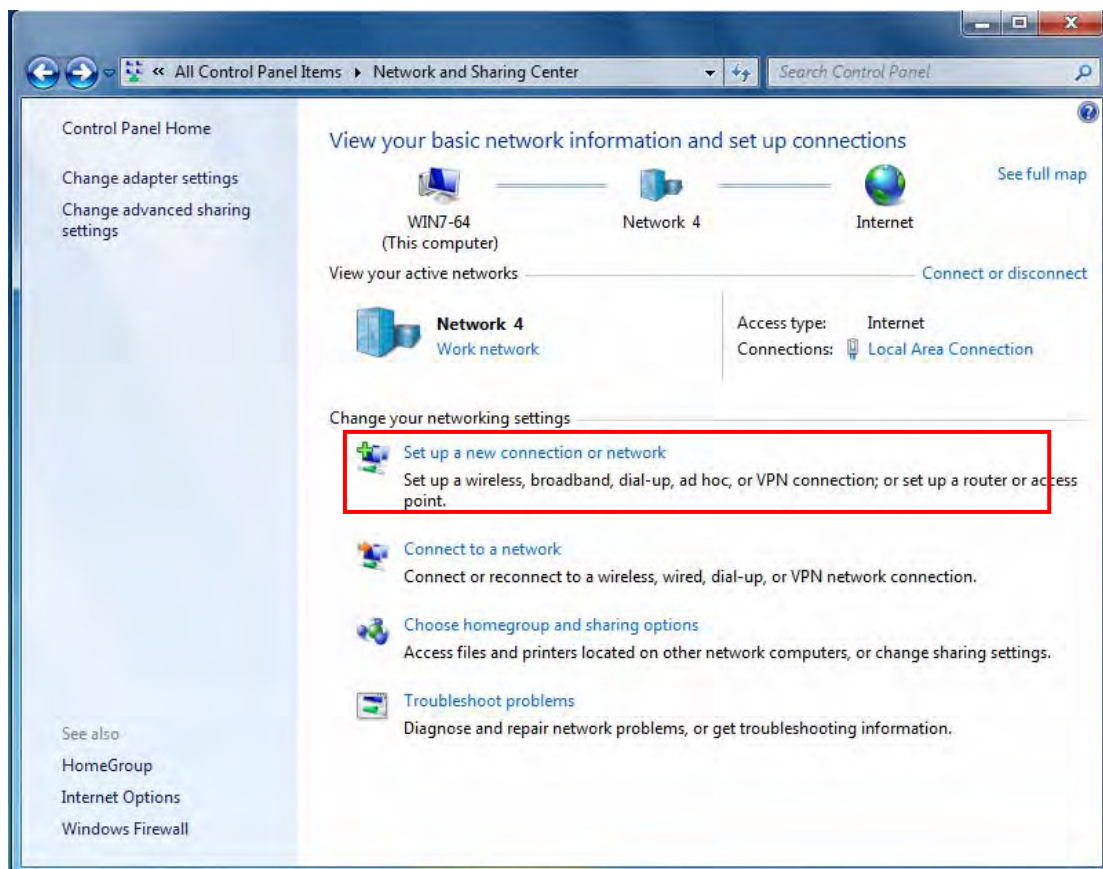
- Name: [Empty field]
- Username: [Empty field]
- Connection Type: ☒ Remote Access ☐ LAN to LAN
- Peer Network IP: [Empty field]
- Tunnel: ☒ Enable ☐ Disable
- Password: [Empty field]
- Peer Netmask: [Empty field]

Buttons for 'Add' and 'Edit / Delete' are at the bottom left.

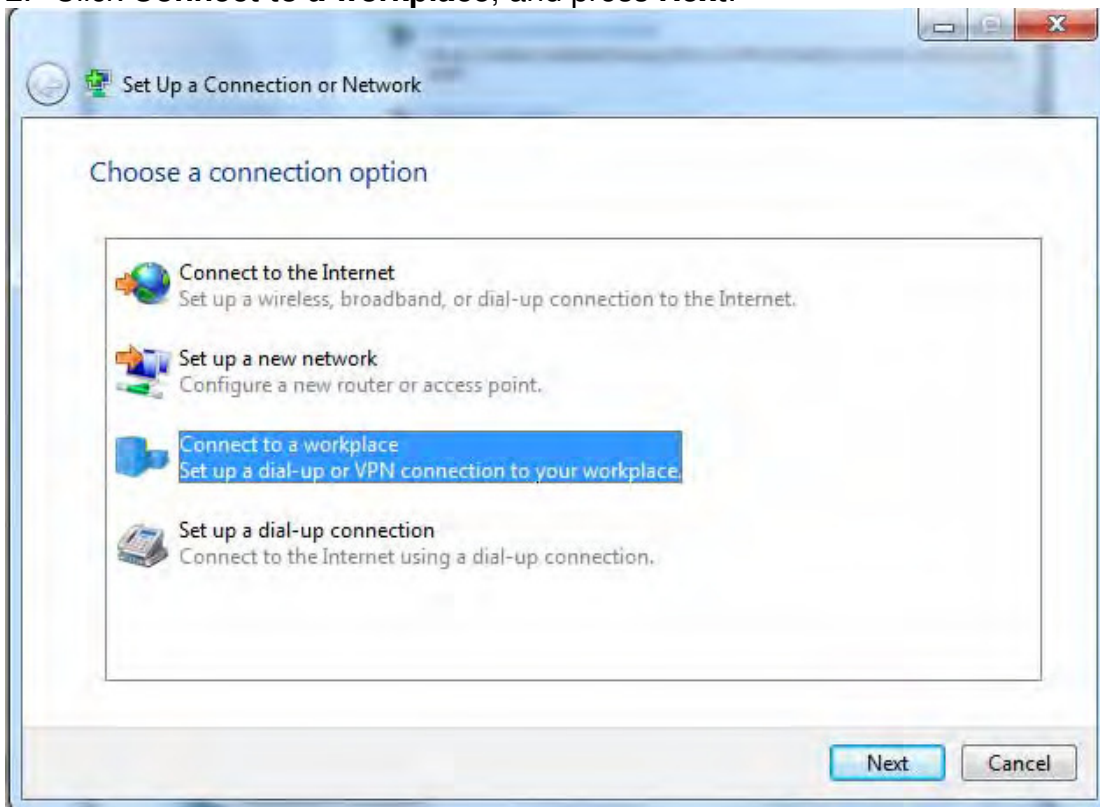
Edit	Name	Tunnel	Connection Type	Peer Network IP	Peer Netmask	Delete
☐	test	Enable	Remote Access			☐

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**.

Connect to a Workplace

Type the Internet address to connect to

Your network administrator can give you this address.

Internet address:

Destination name:

☐ 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

Connect to a Workplace

Type the Internet address to connect to

Your network administrator can give you this address.

Internet address:

Destination name:

☐ 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

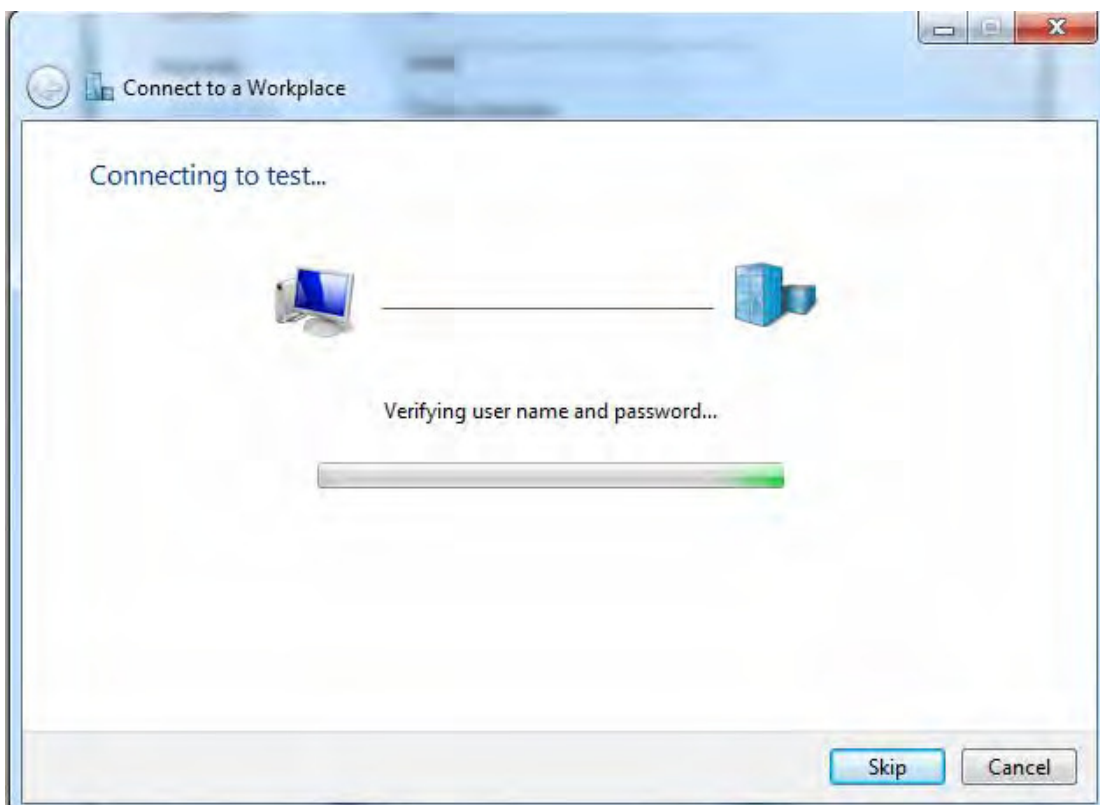
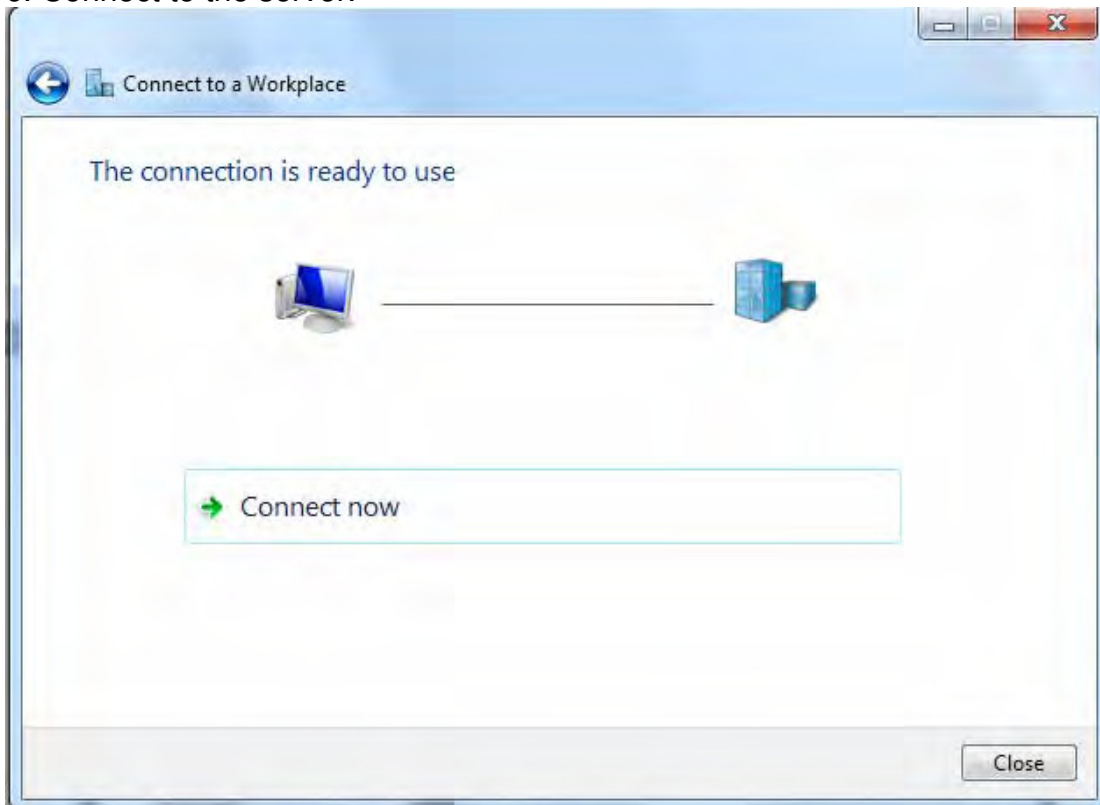
5. Input the account (**user name** and **password**) and press **Create**.

The image displays two sequential screenshots of a Windows-style dialog box titled "Connect to a Workplace".

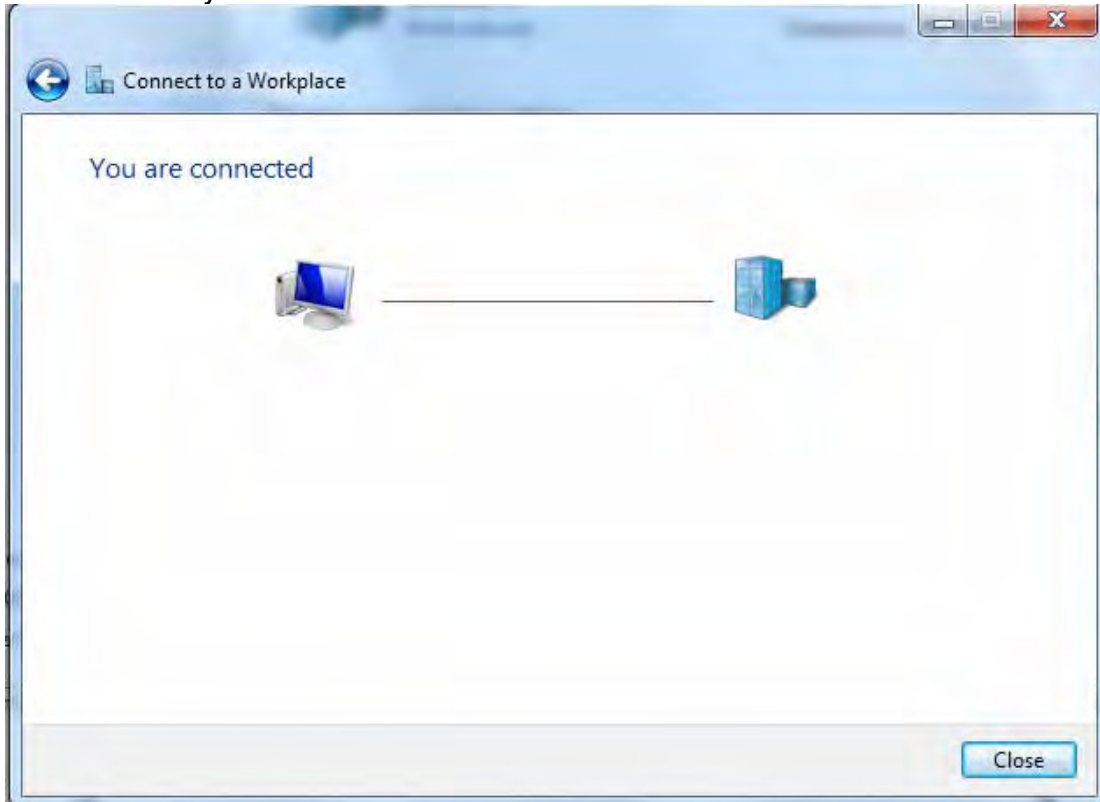
Top Screenshot: The dialog box contains the instruction "Type your user name and password". It features three input fields: "User name:", "Password:", and "Domain (optional):". The "Password:" field has two checkboxes below it: "Show characters" and "Remember this password", both of which are currently unchecked. At the bottom right, there are two buttons: "Create" (highlighted in blue) and "Cancel".

Bottom Screenshot: This screenshot shows the same dialog box after some input. The "User name:" field now contains the text "test". The "Password:" field contains four masked characters (dots). The "Domain (optional):" field remains empty. The "Show characters" and "Remember this password" checkboxes are still unchecked. The "Create" and "Cancel" buttons are present at the bottom right.

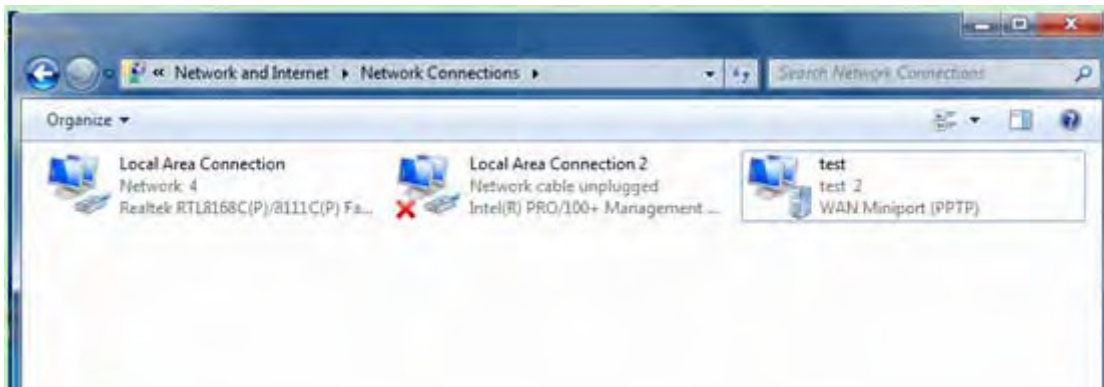
6. Connect to the server.

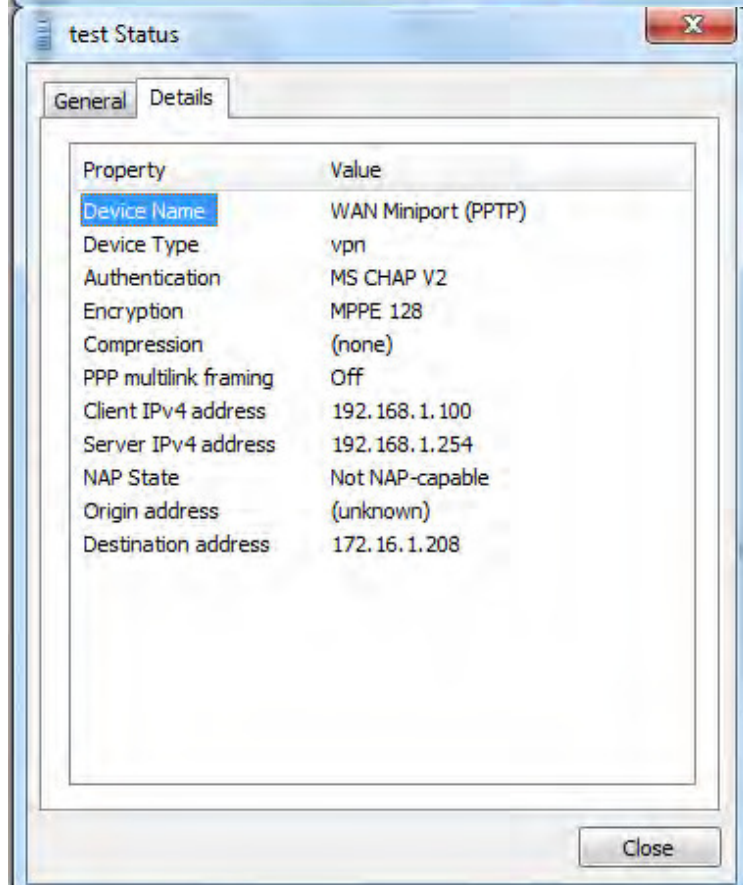
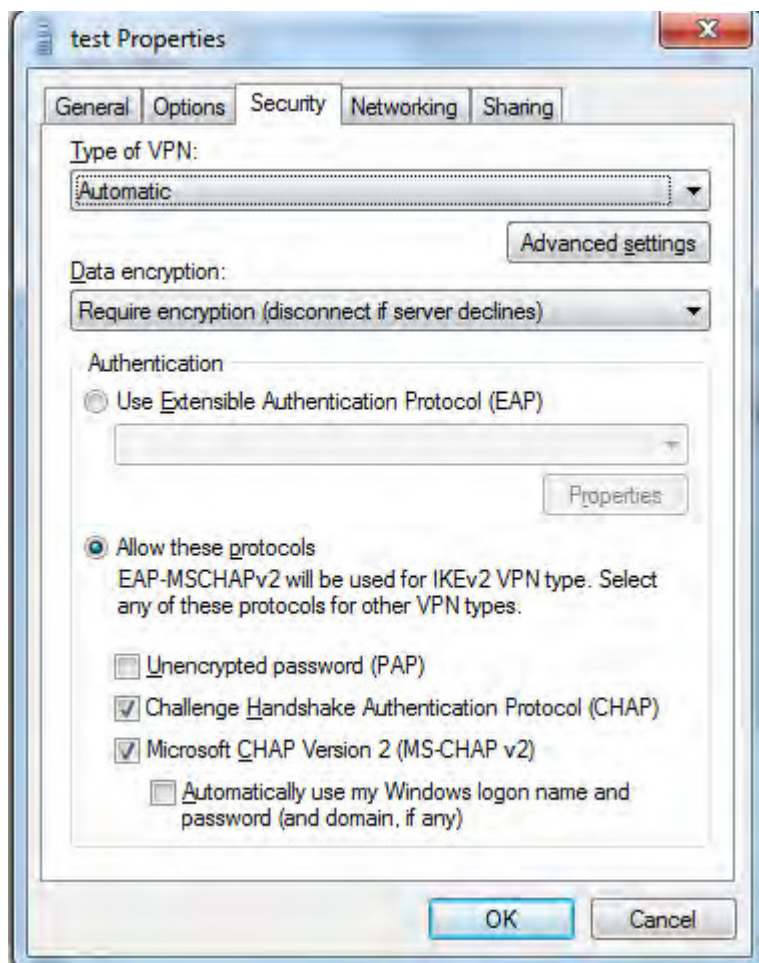


7. Successfully connected.



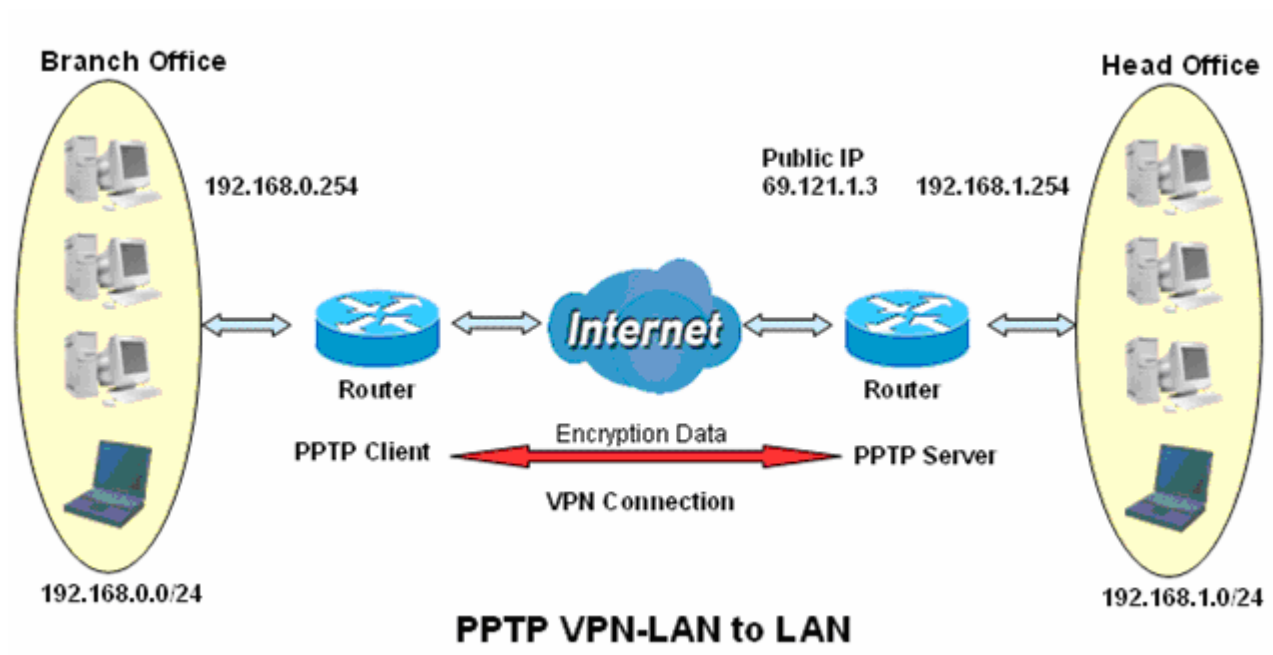
PS: You can also go to **Network Connections** shown below to check the detail of the connection. Right click "test" icon, and select "**Properties**" to change the security parameters (if the connection fails, users can go here to change the settings)





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

The screenshot shows the **VPN** configuration window, specifically the **PPTP Server** settings. The **Parameters** section is expanded, showing the following settings:

- 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

At the bottom of the window are **Apply** and **Cancel** buttons.

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

Enable

Disable

Username

HO

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
	Ho	Enable	LAN to LAN	192.168.0.0	255.255.255.0	

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

Remote Access

LAN to LAN

Time to Connect

Always

Manual

Peer Network IP

192.168.1.0

Peer Netmask

255.255.255.0

Add

Edit / Delete

Edit	Enable	Default Gateway	Name	Time to Connect	PPTP Server Address	Connection Type	Peer Network IP	Peer Netmask	Delete
			BO	Manual	69.121.1.3	LAN to LAN	192.168.1.0	255.255.255.0	

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 constitutes the complete L2TP Server settings.

The screenshot shows the 'L2TP Server' configuration window. It has a 'Parameters' section with the following fields:

- L2TP:** Radio buttons for 'Enable' (selected) and 'Disable'.
- WAN Interface:** A dropdown menu showing 'Default or IPsec Tunnel' and a link to 'IPsec'.
- Auth. Type:** A dropdown menu showing 'Pap or Chap'.
- IP Addresses Assigned to Peer:** A text field with 'start from : 192.168.1.0'.
- Tunnel Authentication:** A checkbox that is currently unchecked.
- Secret:** A text input field.
- Remote Host Name:** A text input field.
- Local Host Name:** A text input field.
- Exceptional Rule Group:** A dropdown menu showing 'None'.

At the bottom of the window are 'Apply' and 'Cancel' buttons.

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.

Parameters	
Name	
WAN Interface	Default
Username	
Auth. Type	Pap or Chap
Connection Type	☒ Remote Access ☐ LAN to LAN
Peer Network IP	
Tunnel Authentication	☐
Remote Host Name	
☐ L2TP over IPSec ☐ Enable	
Password	
L2TP Server Address	
Peer Netmask	
Secret	
Local Host Name	

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

Parameters	
Name	
IPSec Tunnel	test2 IPSec
Username	
Auth. Type	Pap or Chap
Connection Type	☒ Remote Access ☐ LAN to LAN
Peer Network IP	
Tunnel Authentication	☐
Remote Host Name	
☒ L2TP over IPSec ☒ Enable	
Password	
L2TP Server Address	
Peer Netmask	
Secret	
Local Host Name	

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 the 'L2TP Client' tab selected. The 'Parameters' section contains the following fields and controls:

- Name:** Text input field.
- WAN Interface:** Dropdown menu with 'Default' selected.
- Username:** Text input field.
- Auth. Type:** Dropdown menu with 'Pap or Chap' selected.
- Connection Type:** Radio buttons for 'Remote Access' (selected) and 'LAN to LAN'.
- Peer Network IP:** Text input field.
- Tunnel Authentication:** Check box (unchecked).
- Remote Host Name:** Text input field.
- L2TP over IPsec:** Check box (unchecked) with an 'Enable' label.
- Password:** Text input field.
- L2TP Server Address:** Text input field.
- Peer Netmask:** Text input field.
- Secret:** Text input field.
- Local Host Name:** Text input field.

At the bottom left, there are three buttons: 'Add', 'Edit', and 'Delete'.

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.

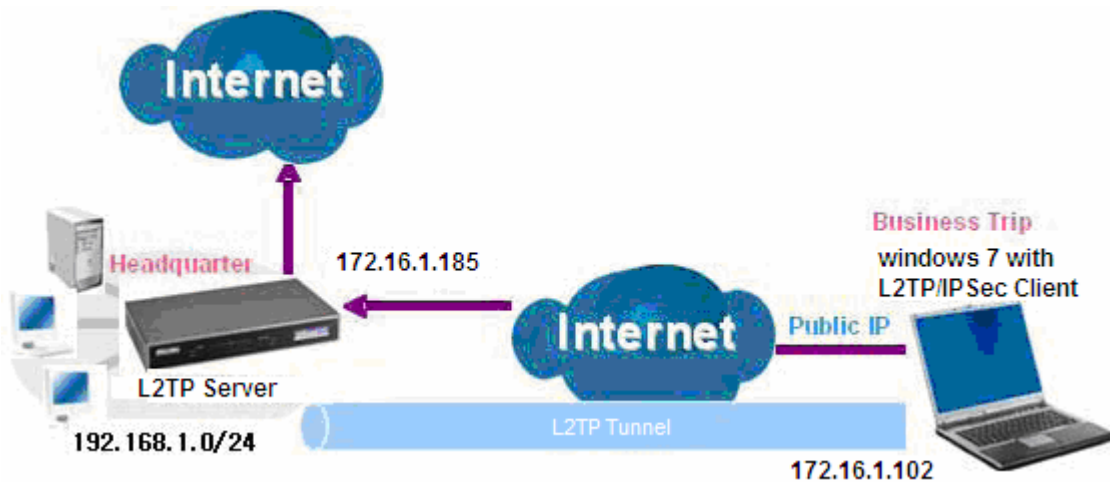
Secret: Enter the set secret password in the server side.

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**.

The screenshot shows the 'VPN' configuration window with the 'L2TP Server' tab selected. The 'Parameters' section is expanded, showing the following settings:

- L2TP:** ☒ Enable ☐ Disable
- WAN Interface:** Default or IPSec Tunnel (dropdown menu)
- Auth. Type:** Chap (dropdown menu)
- IP Addresses Assigned to Peer:** start from : 192.168.1.10 (text input)
- Tunnel Authentication:** ☐
- Secret:** (text input)
- Remote Host Name:** (text input)
- Local Host Name:** (text input)
- Exceptional Rule Group:** None (dropdown menu)

At the bottom of the configuration window, there are 'Apply' and 'Cancel' buttons.

The IPSec for L2TP rule

The screenshot shows the 'VPN' configuration window with the 'IPSec' tab selected. The 'IPSec Settings' section is expanded, showing the following settings:

- L2TP over IPSec:** ☒ Enable
- Connection Name:** (text input)
- WAN Interface:** Default (dropdown menu)
- IP Version:** IPv4 (dropdown menu)
- Remote Security Gateway:** (text input)
- Key Exchange Method:** IKE
- IPsec Protocol:** ESP
- Pre-Shared Key:** 123456 (text input)

At the bottom of the configuration window, there is an 'Apply' button.

2. Create a L2TP Account “test1”.

VPN Account applied to PPTP/L2TP/OpenVPN Server.

Parameters

Name: test1 Tunnel: ☒ Enable ☐ Disable

Username: test1 Password: *****

Connection Type: ☒ Remote Access ☐ LAN to LAN

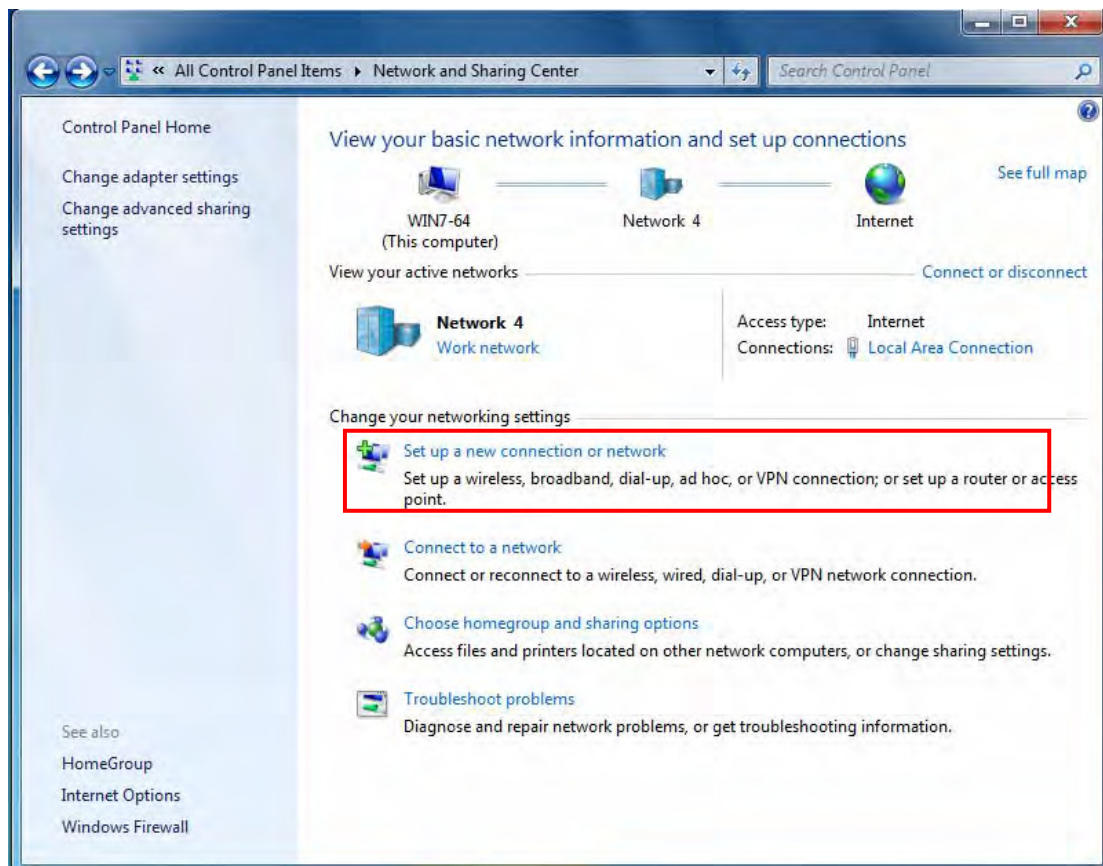
Peer Network IP: Peer Netmask:

Add Edit/Delete

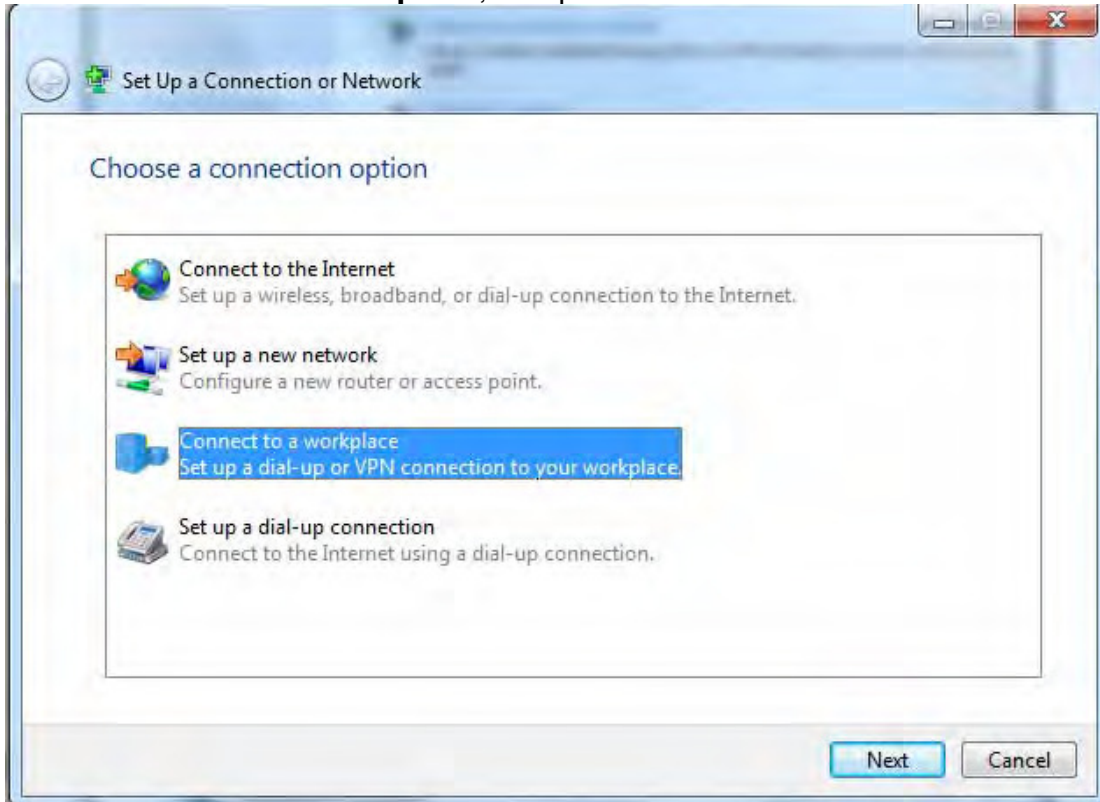
Edit	Name	Tunnel	Connection Type	Peer Network IP	Peer Netmask	Delete
☒	test1	Enable	Remote Access			☐

Client Side:

1. In Windows7 click **Start > Control Panel> Network and Sharing Center**, Click **Set up a new connection network**.



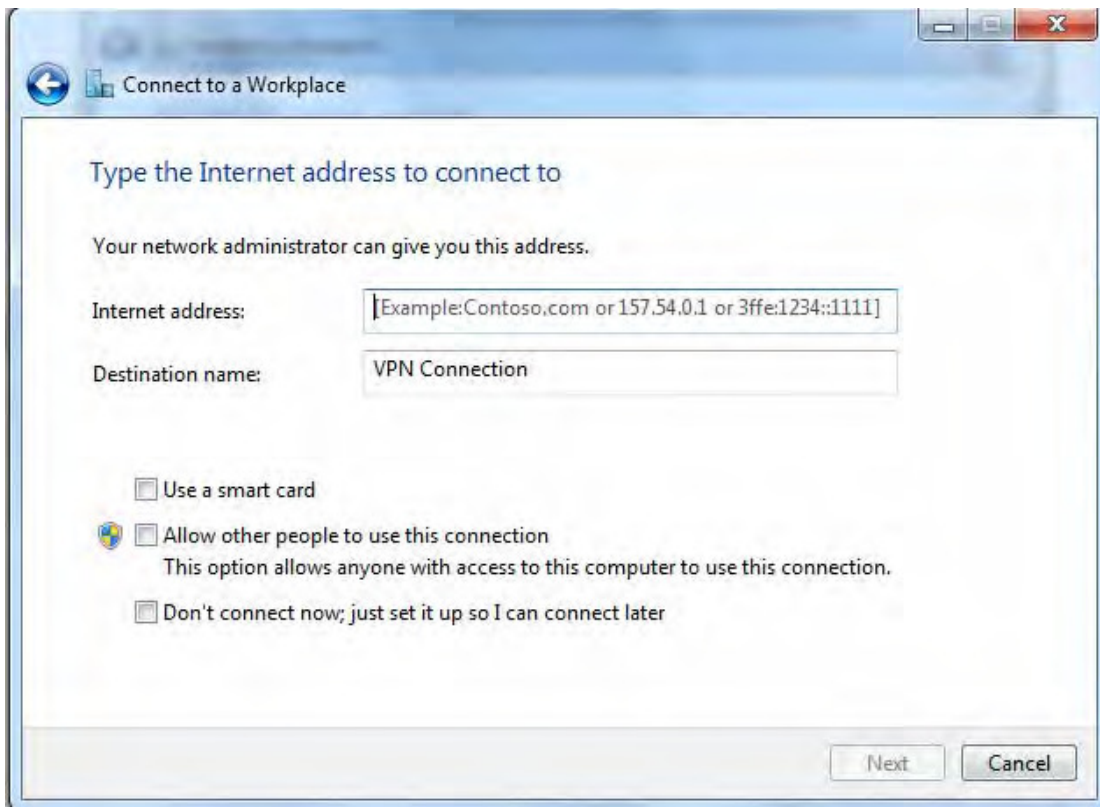
2. Click **Connect to a workplace**, and press **Next**.



3. Select **Use my Internet connection (VPN)** and press **Next**.



4. Input **Internet address** and **Destination name** for this connection and press **Next**.



Connect to a Workplace

Type the Internet address to connect to

Your network administrator can give you this address.

Internet address: [Example:Contoso.com or 157.54.0.1 or 3ffe:1234::1111]

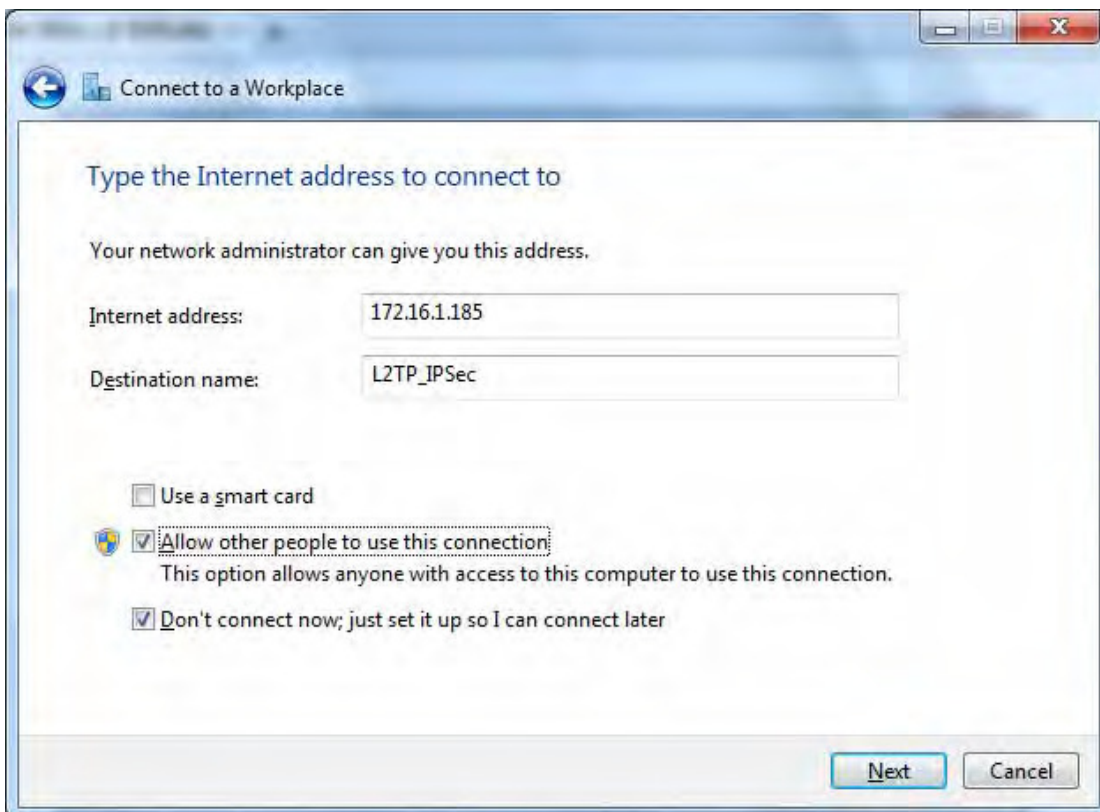
Destination name: VPN Connection

☐ 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



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

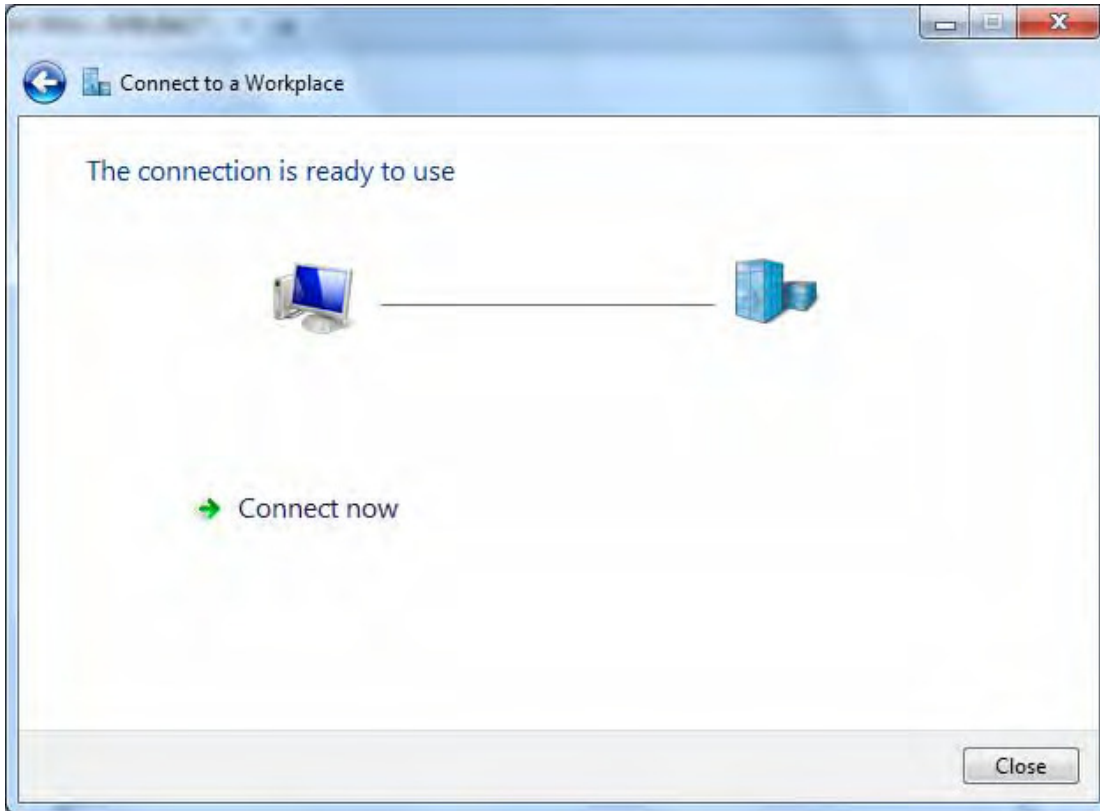
5. Input the account (**user name** and **password**) and press **Create**.

The image displays two sequential screenshots of a Windows-style dialog box titled "Connect to a Workplace".

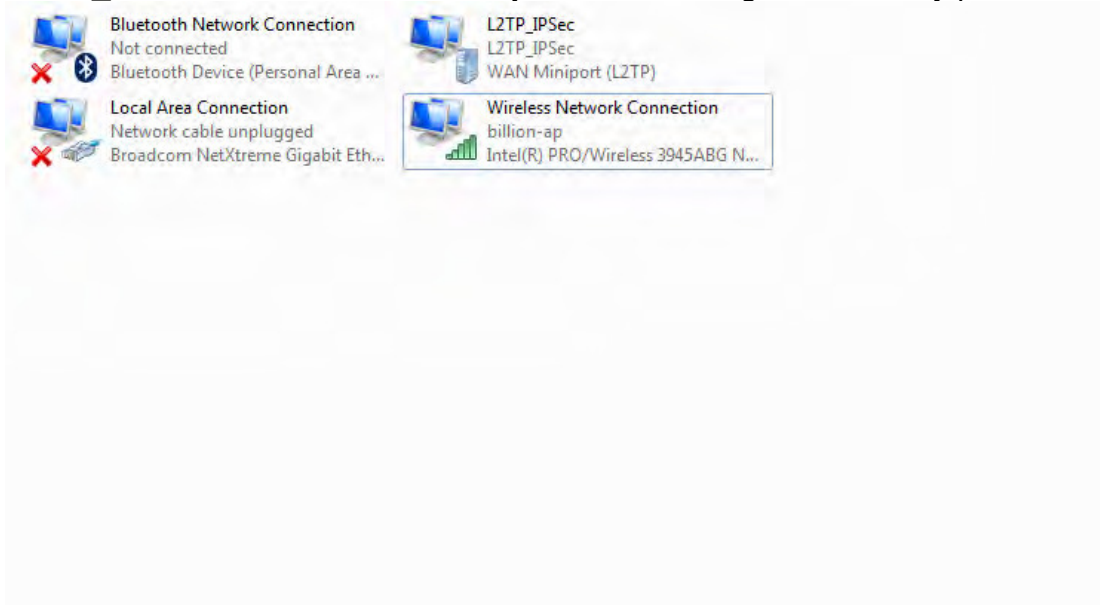
Top Screenshot: The dialog box contains the instruction "Type your user name and password". It features four input fields: "User name:", "Password:", "Show characters" (with a checkbox), and "Remember this password" (with a checkbox). Below these is a "Domain (optional):" field. At the bottom right are "Create" and "Cancel" buttons.

Bottom Screenshot: This screenshot shows the same dialog box after input. The "User name:" field contains the text "test1". The "Password:" field is filled with masked characters (dots). The checkboxes for "Show characters" and "Remember this password" remain unchecked. The "Domain (optional):" field is empty. The "Create" and "Cancel" buttons are still present at the bottom right.

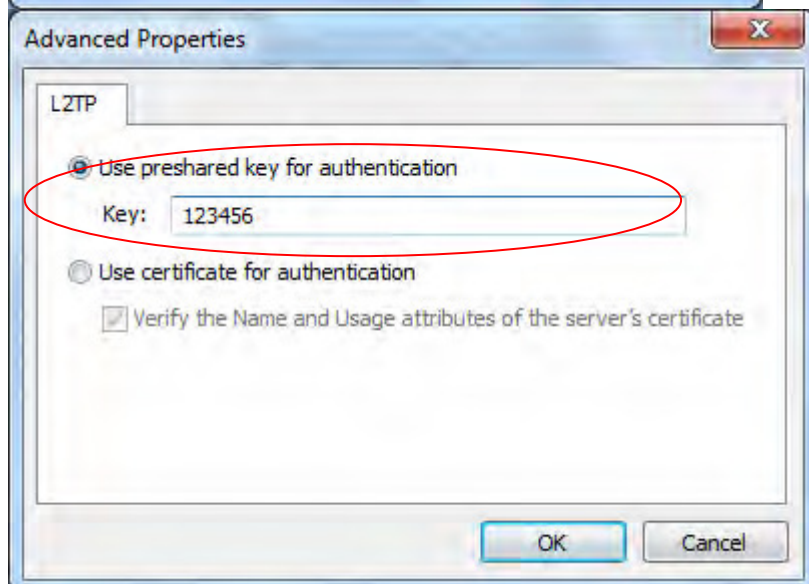
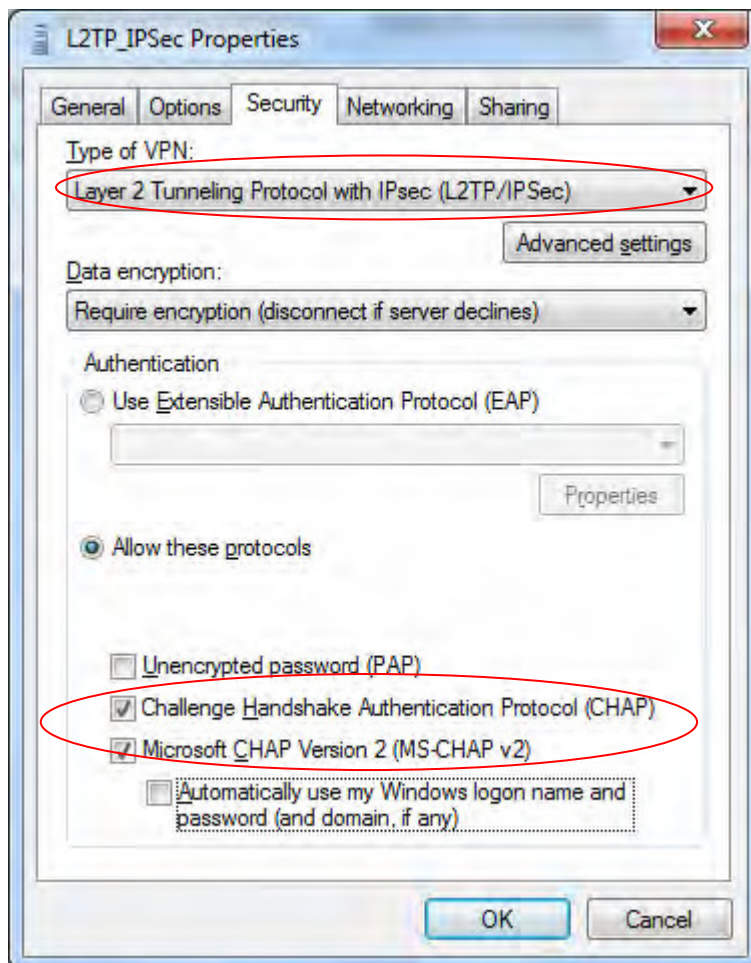
6. Connection created. Press **Close**.



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.



The 'Connect L2TP_IPSec' dialog box features a header with a globe and computer icons. It contains input fields for 'User name' (test1), 'Password' (masked with dots), and 'Domain'. Below these is a checkbox 'Save this user name and password for the following users:' with two radio button options: 'Me only' and 'Anyone who uses this computer' (selected). At the bottom are 'Connect', 'Cancel', 'Properties', and 'Help' buttons.

User name: test1

Password:

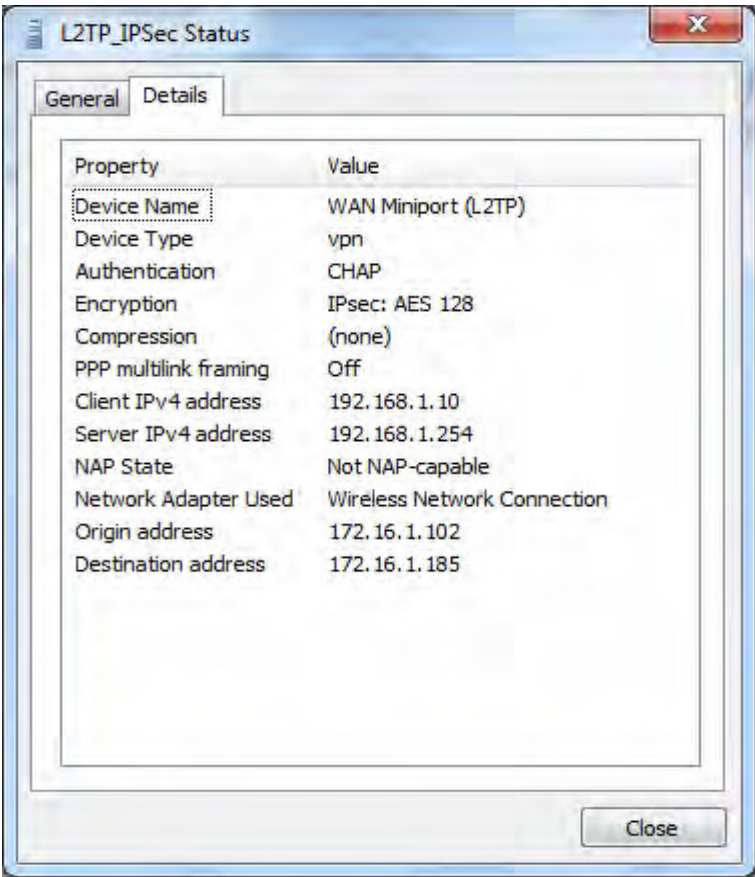
Domain:

☒ Save this user name and password for the following users:

☐ Me only

☒ Anyone who uses this computer

Connect Cancel Properties Help



The 'L2TP_IPSec Status' dialog box has 'General' and 'Details' tabs. The 'General' tab is active, showing a table of properties and values. A 'Close' button is at the bottom right.

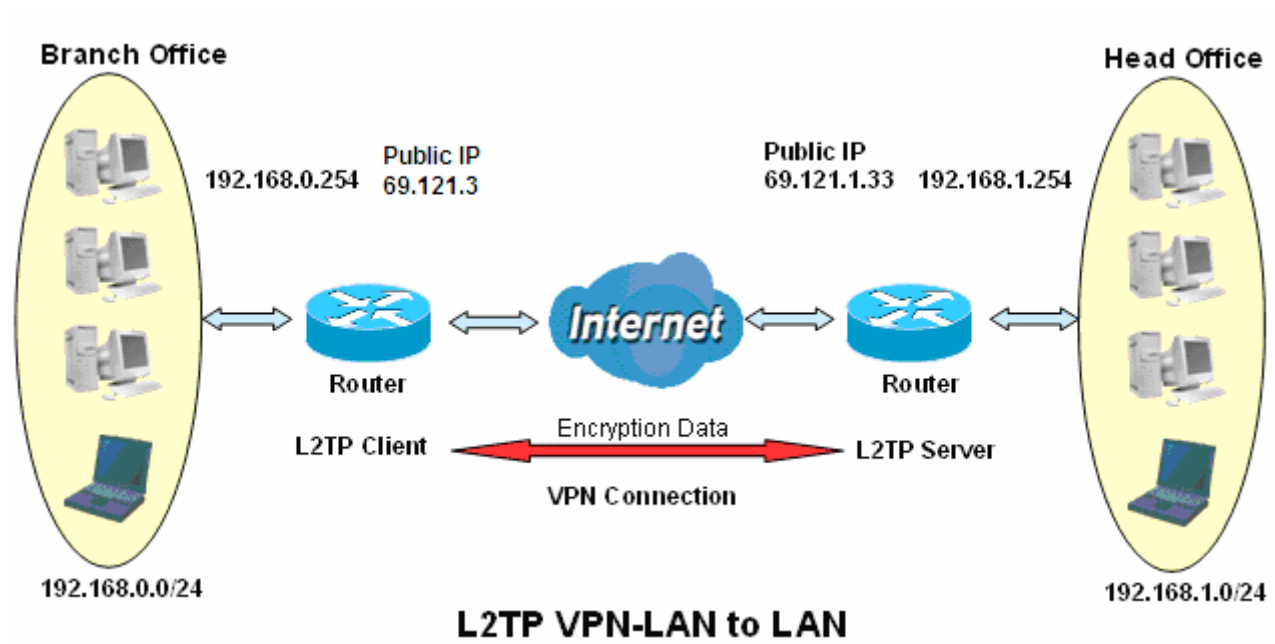
Property	Value
Device Name	WAN Miniport (L2TP)
Device Type	vpn
Authentication	CHAP
Encryption	IPsec: AES 128
Compression	(none)
PPP multilink framing	Off
Client IPv4 address	192.168.1.10
Server IPv4 address	192.168.1.254
NAP State	Not NAP-capable
Network Adapter Used	Wireless Network Connection
Origin address	172.16.1.102
Destination address	172.16.1.185

Close

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 **Default or IPsec Tunnel** **IPSec**

Auth. Type **Chap**

IP Addresses Assigned to Peer start from : 192.168.1.10

Tunnel Authentication ☐

Secret

Remote Host Name

Local Host Name

Exceptional Rule Group **None**

Apply Cancel

VPN

IPSec

IPSec Settings

L2TP over IPsec ☒ Enable

Connection Name **test2** WAN Interface **Default** IP Version **IPv4**

Remote Security Gateway **69.121.1.3** ☐ Anonymous

Key Exchange Method **IKE** IPsec Protocol **ESP**

Pre-Shared Key **123456**

Encryption Algorithm **3DES** Integrity Algorithm **MD5**

DH Group **MODP1024(DH2)** IPsec Lifetime **60** Minute(s) [60-1440]

Apply

Tunnel Mode Connections							
Active	L2TP	Connection Name	Local Network	Remote Network	Remote Security Gateway	Remove	Edit
☒	✓	test1			Anonymous	☐	Edit
☐	✓	test2			69.121.1.3	☐	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
☒	HO	Enable	LAN to LAN	192.168.0.0	255.255.255.0	☐

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

Auth. Type

Chap

Connection Type

☐ Remote Access

☒ LAN to LAN

Peer Network IP

192.168.1.0

Tunnel Authentication

☐

Remote Host Name

Password

.....

L2TP Server Address

69.121.1.33

Peer Netmask

255.255.255.0

Secret

Local Host Name

Add

Edit / Delete

Edit

Enable

Default Gateway

Name

L2TP Server Address

Connection Type

Peer Network IP

Peer Netmask

Delete

☒

☐

☒

BO

69.121.1.33

LAN to LAN

192.168.1.0

255.255.255.0

☐

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.

229

OpenVPN

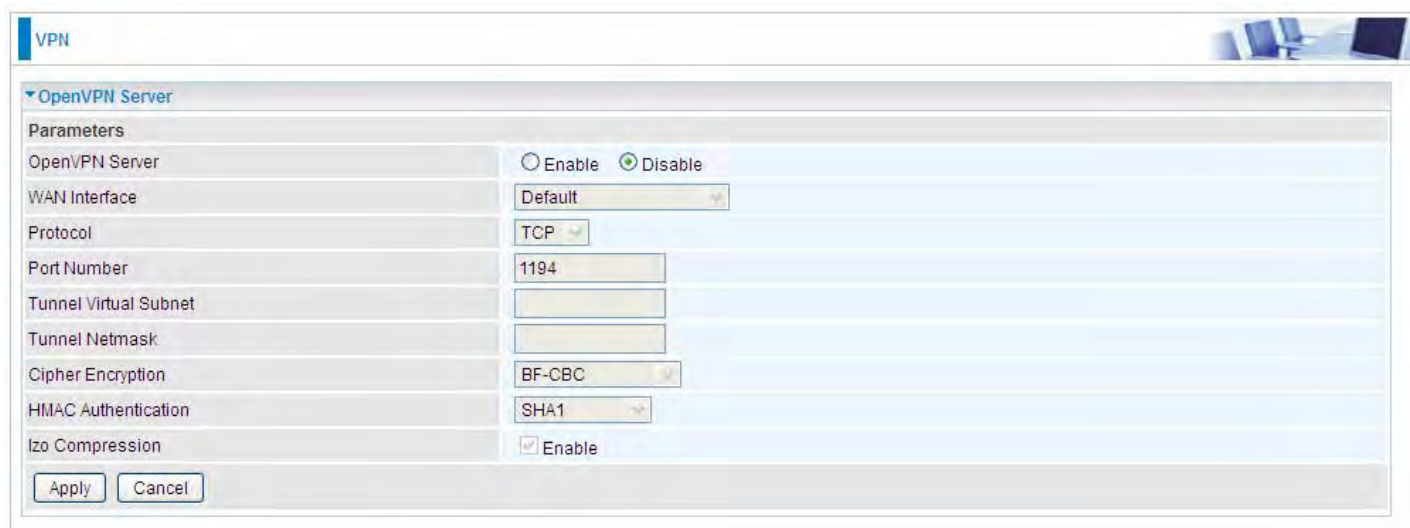
OpenVPN is an open source software application that implements virtual private network (VPN) techniques for creating secure point-to-point or site-to-site connections in routed or bridged configurations and remote access facilities. It uses a custom security protocol that utilizes SSL/TLS for key exchange. 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.



The screenshot shows a configuration window titled "VPN" with a sub-tab "OpenVPN Server". The "Parameters" section contains the following settings:

Parameter	Value
OpenVPN Server	☐ Enable ☒ Disable
WAN Interface	Default
Protocol	TCP
Port Number	1194
Tunnel Virtual Subnet	
Tunnel Netmask	
Cipher Encryption	BF-CBC
HMAC Authentication	SHA1
Lzo Compression	☒ Enable

At the bottom of the configuration area are "Apply" and "Cancel" buttons.

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.

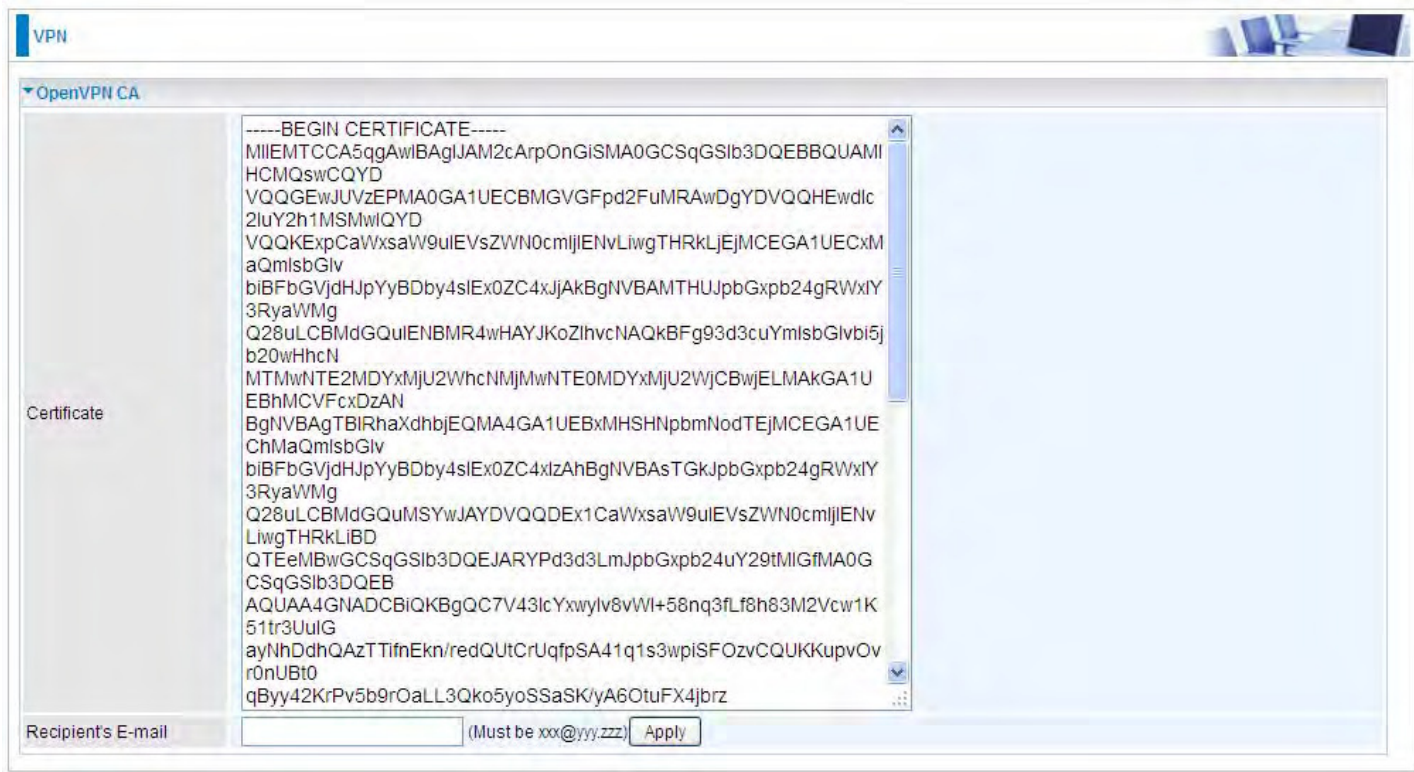
HMAC Authentication: OpenVPN support [HMAC](#) authentication, please select authentication item from the list.

Izo Compression: Enable to use the LZO compression library to compress the data stream.

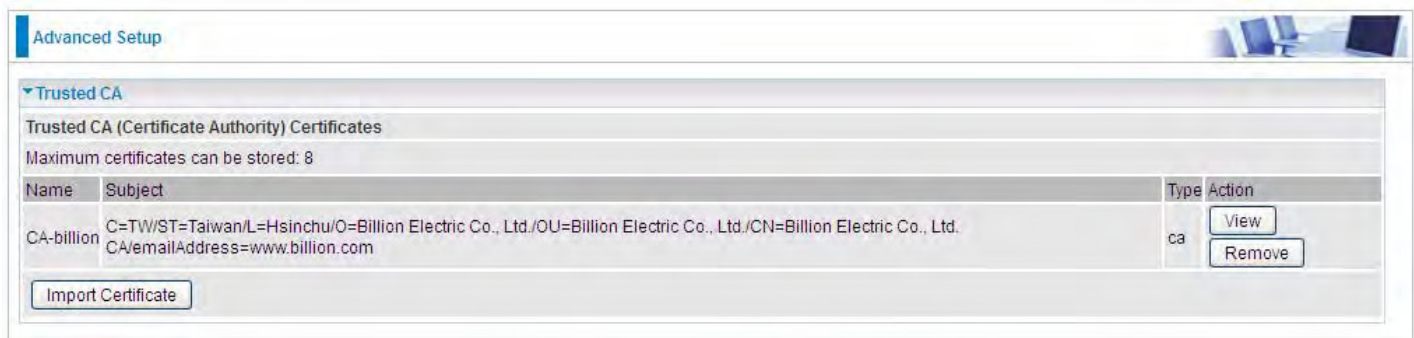
Click **Apply** to submit your OpenVPN Server basic settings.

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 billion 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](#).



(client side CA)

OpenVPN Client

OpenVPN client can help you dial-in the OpenVPN server to establish a trusted OpenVPN tunnel over Internet.

Parameters			
Name		WAN Interface	Default
Username		Password	
OpenVPN Server Address			
Protocol	TCP	Port Number	1194
Cipher Encryption	BF-CBC	HMAC Authentication	SHA1
Izo Compression	☒ Enable	Certificate Authority	CA-billion Trusted CA

Add Edit / Delete

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 LZO 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.

The screenshot shows the 'VPN' configuration page with the 'OpenVPN Server' tab selected. The 'Parameters' section contains the following settings:

Parameter	Value
OpenVPN Server	☒ Enable ☐ Disable
WAN Interface	Default
Protocol	TCP
Port Number	1194
Tunnel Virtual Subnet	192.168.2.0
Tunnel Netmask	255.255.255.0
Cipher Encryption	BF-CBC
HMAC Authentication	SHA1
Izo Compression	☒ Enable

At the bottom of the configuration area are 'Apply' and 'Cancel' buttons.

2. Create an account for the OpenVPN tunnel for client to connect in.

The screenshot shows the 'VPN Account' configuration page. It includes a section for 'Parameters' and a table of existing accounts.

Parameters:

Parameter	Value
Name	test4
Username	tes4
Connection Type	☒ Remote Access ☐ LAN to LAN
Peer Network IP	
Peer Netmask	

Buttons: 'Add', 'Edit / Delete'

VPN Account Table:

Edit	Name	Tunnel	Connection Type	Peer Network IP	Peer Netmask	Delete
☒	test4	Enable	Remote Access			☐

3. Set the OpenVPN client's E-mail address to receive trusted CA from server to establish a trusted OpenVPN tunnel.

VPN

OpenVPN CA

Certificate

-----BEGIN CERTIFICATE-----
MIIEMTCCA5qgAwIBAgIJAM2cArpOnGISMA0GCSqGSIb3DQEBBQUAMI
HCMQswCQYD
VQQGEwJUVzEPMA0GA1UECBMGVGFpd2FuMRAwDgYDVQQHEWdlc
2luY2h1MSMwIQYD
VQQKExpCaWxsaW9uLEVszWN0cmllJENvLiwgTHRkLjEjMCEGA1UECXM
aQmlsbGlv
biBFbGVjdHJpYyBDby4sIEs0ZC4xJjAkBgNVBAMTHUJpbGxpb24gRWxlY
3RyaWMg
Q28uLCBMdGQulENBMR4wHAYJKoZIhvcNAQkBFg93d3cuYmlsbGlvbi5j
b20wHhcN
MTMwNTE2MDYxMjU2WhcNMjMwNTE0MDYxMjU2WjCBwjELMAKGA1U
EBhMCVFcxDzAN
BgNVBAGTBIRhaXdhbjEQMA4GA1UEBxMHSNNpbmNodTEjMCEGA1UE
ChMaQmlsbGlv
biBFbGVjdHJpYyBDby4sIEs0ZC4xJzAhBgNVBAsTGkKpbGxpb24gRWxlY
3RyaWMg
Q28uLCBMdGQulMSYwJAYDVQQDEx1CaWxsaW9uLEVszWN0cmllJENv
LiwgTHRkLjIBD
QTEeMBwGCSqGSIb3DQEJARYPd3d3LmJpbGxpb24uY29tMIGfMA0G
CSqGSIb3DQEB
AQUAA4GNADCBiQKBgQC7V43lcYxwylv8vWI+58nq3fLf8h83M2Vcw1K
51tr3UulG
ayNhDdhQAztTIfnEkn/redQUtCrUqfpSA41q1s3wpiSFOzvCQUKKupvOv
r0nUBt0
qByy42KrPv5b9rOaLL3Qko5yoSSaSK/yA6OtuFX4jbrz

Recipient's E-mail

gangel@gmail.com

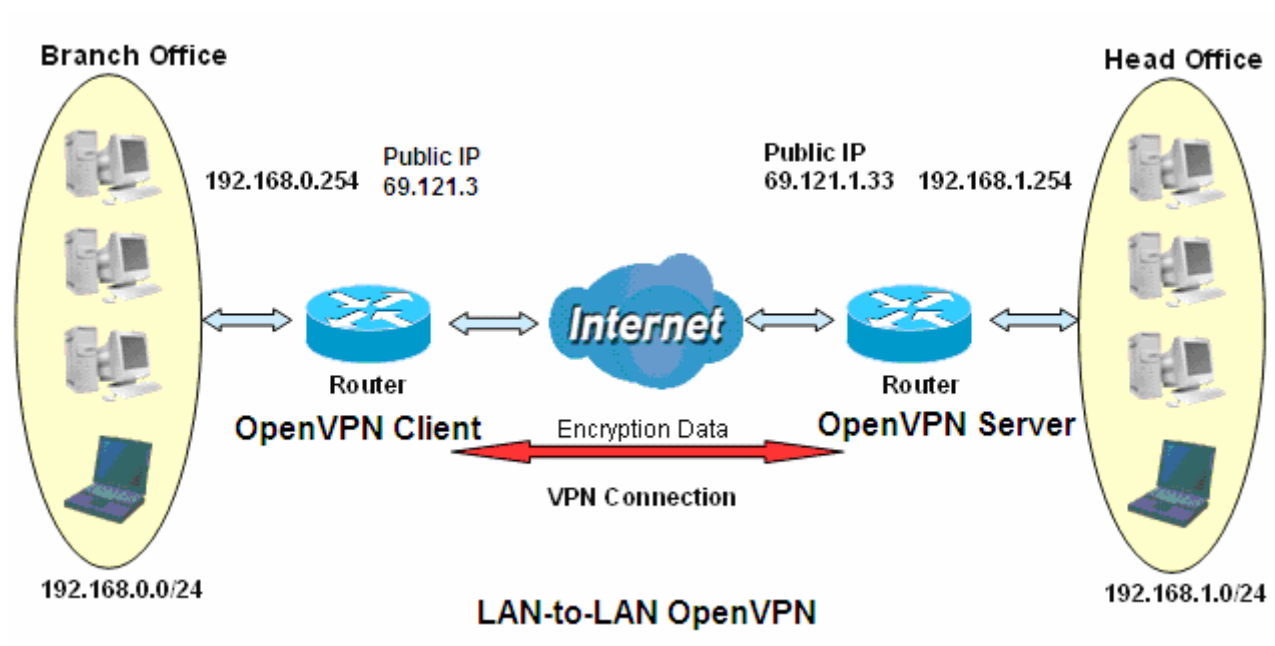
(Must be xxx@yyy.zzz)

Apply

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.

The screenshot shows the **VPN** configuration window with the **OpenVPN Server** tab selected. The **Parameters** section is expanded, showing the following settings:

Parameter	Value
OpenVPN Server	☒ Enable ☐ Disable
WAN Interface	Default
Protocol	TCP
Port Number	1194
Tunnel Virtual Subnet	192.168.2.0
Tunnel Netmask	255.255.255.0
Cipher Encryption	BF-CBC
HMAC Authentication	SHA1
Izo Compression	☒ Enable

At the bottom of the configuration window are **Apply** and **Cancel** buttons.

2. Create an account for client to connect in

VPN

VPN Account

VPN Account applied to PPTP/L2TP/OpenVPN Server.

Parameters

Name	test3	Tunnel	☒ Enable ☐ Disable
Username	test3	Password	
Connection Type	☐ Remote Access ☒ 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
☒	test3	Enable	LAN to LAN	192.168.0.0	255.255.255.0	☐

3. Set the OpenVPN client's E-mail address to receive trusted CA from server to establish a trusted OpenVPN tunnel.

VPN

OpenVPN CA

Certificate

```
-----BEGIN CERTIFICATE-----
MIIEMTCCA5qgAwIBAgIJAM2cArpOnGISMA0GCSqGSIb3DQEBBQUAMI
HCMQswCQYD
VQQGEwJUVzEPMA0GA1UECBMGVGFpd2FuMRAwDgYDVQQHEWdlc
2luY2h1MSMwIQYD
VQQKEwxCaWxsaW9uIEVsZW50cmJJENvLiwgTHRKLjEjMCEGA1UECXM
aQmlsbGlv
biBFbGVjdHJpYyBDby4sIEs0ZC4xJjAkBgNVBAMTHUJpbGxpY24gRWxIY
3RyaVMg
Q28uLCBMdGQulENBMR4wHAYJKoZIhvcNAQkBFg93d3cuYmlsbGlvbi5j
b20wHhcN
MTMwNTE2MDYxMjU2WWhcNMjMwNTE0MDYxMjU2WjCBwJELMAkGA1U
EBhMCVFcxZDZAN
BgNVBAGTBIRhaXdhbjEQMA4GA1UEBxMHSNpbmNodTEjMCEGA1UE
ChMaQmlsbGlv
biBFbGVjdHJpYyBDby4sIEs0ZC4xJzAhBgNVBAstGkKpbGxpY24gRWxIY
3RyaVMg
Q28uLCBMdGQulMSYwJAYDVQQDEw1CaWxsaW9uIEVsZW50cmJJENv
LiwgTHRKLjEj
QTEeMBwGCsqGSIb3DQEQJARYPd3d3LmJpbGxpY24uY29tMIGfMA0G
CSqGSIb3DQEB
AQUAA4GNADCBiQKBgQC7V43lcYxwylv8vWI+58nq3fL8h83M2Vcw1K
51tr3UulG
ayNhDdhQAztTifnEkn/redQUtCrUqfpSA41q1s3wpiSFOzvCQUKKupvOv
r0nUBt0
qByy42KrPv5b9rOaLL3Qko5yoSSaSK/ya6OtuFX4jbrz
-----
```

Recipient's E-mail

gangel@gmail.com (Must be xxx@yyy.zzz)

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.

Advanced Setup

Trusted CA - Import CA certificate

Parameters

Name: CA-billion

Certificate: -----BEGIN CERTIFICATE-----
MIIEMTCCA5qgAwIBAgIJAM2cArpOnGiSMA0GCSqGSIb3DQE
BBQUAMIHCMQswCQYD
VQQGEwJUVzEPMA0GA1UECBMGVGFpd2FuMRAwDgYDVQ
QHEwdlc2luY2h1MSMwIwYD
VQQKEwxCaWxsaW9uIEVsZW50cmJlJENvLiwgTHRKLjEjMCEG
A1UECxMaQmlsbGlv
biBFbGVjdHJpYyBDby4sIEExOZC4xJkBgNVBAMTHUJpbGxpb
24gRWxIY3RyaWVmg
Q28uLCBMdGQulENBMR4wHAYJKoZIhvcNAQkBFg93d3cuYm
lsbGlvbi5jb20wHhcN
MTMwNTE2MDYxMjU2WWhcNMjMwNTE2MDYxMjU2WjCBwJELM
AkGA1UEBhMCVFcxDzAN
BgNVBAGTBIRhaXdhbjEQMA4GA1UEBxMHSNpbmNodTEjM
CEGA1UEChMaQmlsbGlv
biBFbGVjdHJpYyBDby4sIEExOZC4xJkBgNVBAsTGkxpbGxpb2
4gRWxIY3RyaWVmg
Q28uLCBMdGQulMSYwJAYDVQQDEw1CaWxsaW9uIEVsZW50
cmJlJENvLiwgTHRKLjEjMCEG
QTEeMBwGCSqGSIb3DQEJARYPd3d3LmJpbGxpb24uY29tM
GfMA0GCSqGSIb3DQEBA
AQUAAAGNADCBiQKBgQC7V43lcYxwylv8vWI+58nq3fL8h83
M2Vcw1K51tr3UulG
ayNhDdhQAZT TifnEkn/redQUtCrUqfpSA41q1s3wpISFOzvCQU
KKupvOvr0nUBt0
qByy42KrPv5b9rOaLL3Qko5yoSSaSK/yA6OtuFX4jbrz
-----END CERTIFICATE-----

Apply

2. On the OpenVPN client side, fill in the parameters the same as set for OpenVPN server.

VPN

OpenVPN Client

Parameters

Name: test3, WAN Interface: Default, Username: test3, Password:, OpenVPN Server Address: 69.121.1.33, Protocol: TCP, Port Number: 1194, Cipher Encryption: BF-CBC, HMAC Authentication: SHA1, Izo Compression: ☒ Enable, Certificate Authority: CA-billion Trusted CA

Add Edit / Delete

VPN

OpenVPN Client

Parameters

Name: , WAN Interface: Default, Username: , Password: , OpenVPN Server Address: , Protocol: TCP, Port Number: 1194, Cipher Encryption: BF-CBC, HMAC Authentication: SHA1, Izo Compression: ☒ Enable, Certificate Authority: CA-billion Trusted CA

Add Edit / Delete

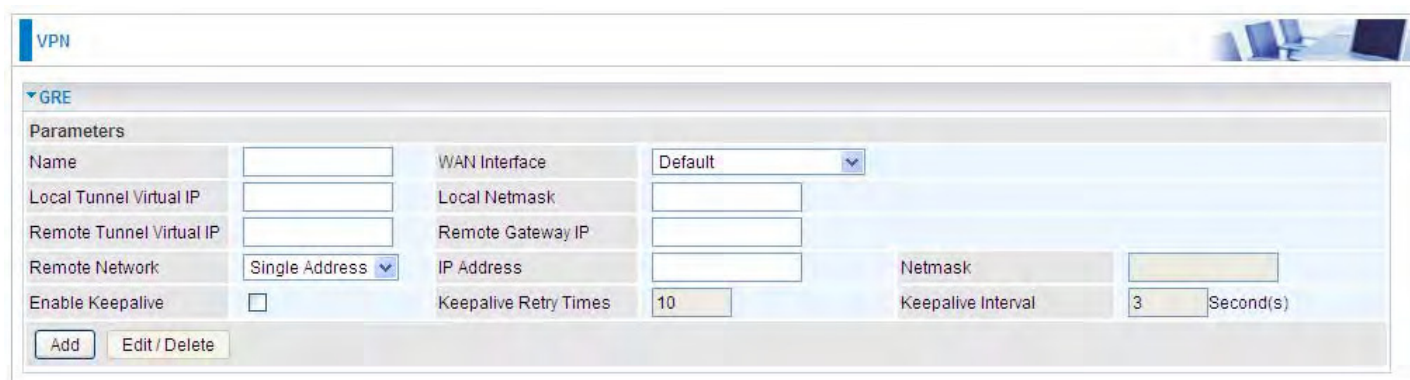
Edit	Enable	Name	WAN Interface	OpenVPN Server Address	Protocol	Port Number	Delete
☐	☒	test3	default	69.121.1.33	TCP	1194	☐

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 GRE tunnels. At the top, there is a 'VPN' tab. Below it, a 'GRE' section is expanded, showing a 'Parameters' table. The table has two columns for configuration fields. The first column contains: 'Name' (text input), 'Local Tunnel Virtual IP' (text input), 'Remote Tunnel Virtual IP' (text input), 'Remote Network' (dropdown menu with 'Single Address' selected), and 'Enable Keepalive' (checkbox). The second column contains: 'WAN Interface' (dropdown menu with 'Default' selected), 'Local Netmask' (text input), 'Remote Gateway IP' (text input), 'IP Address' (text input), 'Netmask' (text input), 'Keepalive Retry Times' (text input with '10'), and 'Keepalive Interval' (text input with '3' and a 'Second(s)' label). At the bottom of the table, 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](#).

▸ Status
▸ Quick Start
▸ Configuration
▸ VPN
▾ Advanced Setup
▸ Routing
▸ DNS
▸ Static ARP
▸ UPnP
▸ Certificate
▸ Multicast
▸ Management
▸ 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

ppp0.1

Available Routed WAN Interfaces

USB3G0

->

<-

Preferred WAN Interface As The System Default IPv6 Gateway

Selected WAN Interface

pppoe_0_8_35/ppp0.1

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.

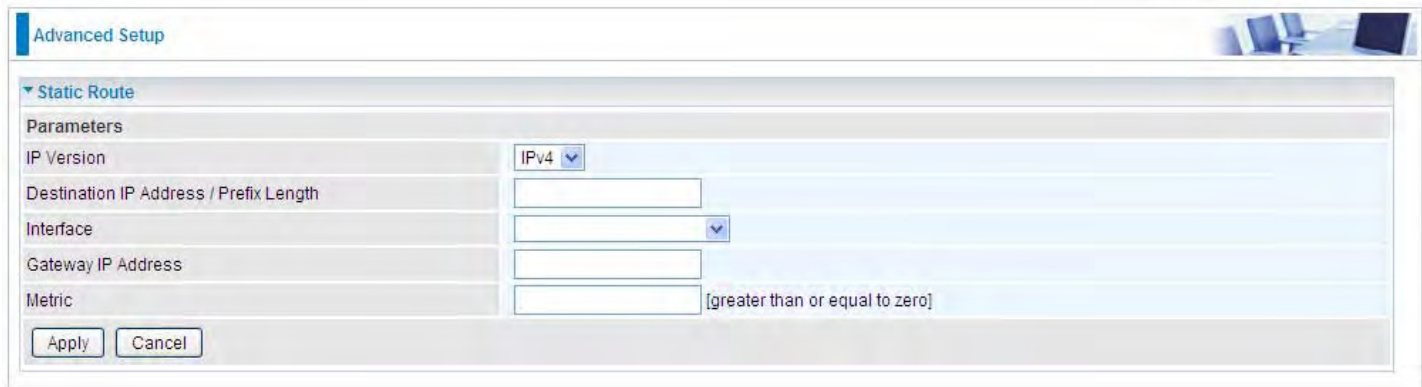
Static Route

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.



The screenshot shows the 'Advanced Setup' window with the 'Static Route' tab selected. Below the tab is a table with the following columns: IP Version, Dst IP / Prefix Length, Gateway, Interface, Metric, and Remove. At the bottom of the table are 'Add' and 'Remove' buttons.

Above is the static route listing table, click **Add** to create static routing.



The screenshot shows the 'Advanced Setup' window with the 'Static Route' tab selected. The configuration form contains the following fields: IP Version (set to IPv4), Destination IP Address / Prefix Length, Interface (dropdown), Gateway IP Address, and Metric (with a note '[greater than or equal to zero]'). At the bottom are 'Apply' and 'Cancel' buttons.

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	☒

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
-------------	-----------	----------	-----	-----------------	--------

Add

Remove

Click **Add** to create a policy route.

Advanced Setup

▼ Policy Routing

Parameters

Policy Name

Physical LAN Port

Source IP

Interface

Default Gateway

pppoe_0_0_35/ppp0.1

Apply

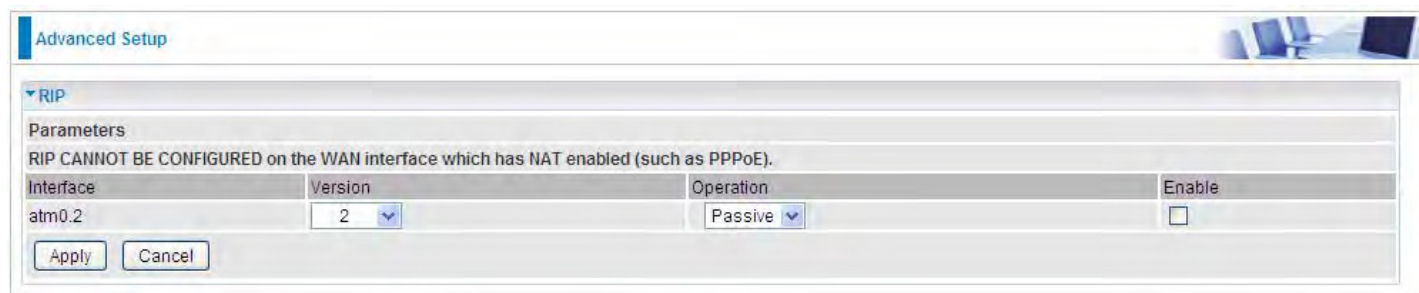
Cancel

- 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.



The screenshot shows a web-based configuration interface titled "Advanced Setup". Under the "RIP" section, there is a "Parameters" area. A message states: "RIP CANNOT BE CONFIGURED on the WAN interface which has NAT enabled (such as PPPoE)". Below this is a table with four columns: "Interface", "Version", "Operation", and "Enable". The first row shows "atm0.2" for the interface, "2" for the version, "Passive" for the operation, and an unchecked checkbox for the enable status. At the bottom of the table are "Apply" and "Cancel" buttons.

Interface	Version	Operation	Enable
atm0.2	2	Passive	☐

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 (such as PPPoE).

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

The screenshot shows a 'DNS' configuration window. At the top, there's a 'Parameters' section with explanatory text about DNS server selection. Below this, there are three radio buttons: 'Select DNS Server Interface from available WAN interfaces' (which is selected), 'Use the following Static DNS IP address', and 'Use the IP Addresses provided by Parental Control Provider'. The first option leads to two list boxes: 'Selected DNS Server Interfaces' (containing 'ppp0.1' and 'USB3G0') and 'Available WAN Interfaces' (empty). Between these boxes are right and left arrow buttons. The second option leads to input fields for 'Primary DNS server' and 'Secondary DNS server'. The third option leads to a note and a radio button for 'Obtain IPv6 DNS info from a WAN interface'. This option is selected and leads to a 'WAN Interface selected' dropdown menu (showing 'pppoe_0_8_35/ppp0.1') and another set of 'Primary IPv6 DNS server' and 'Secondary IPv6 DNS server' input fields. At the bottom are 'Apply' and 'Cancel' buttons.

➤ 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

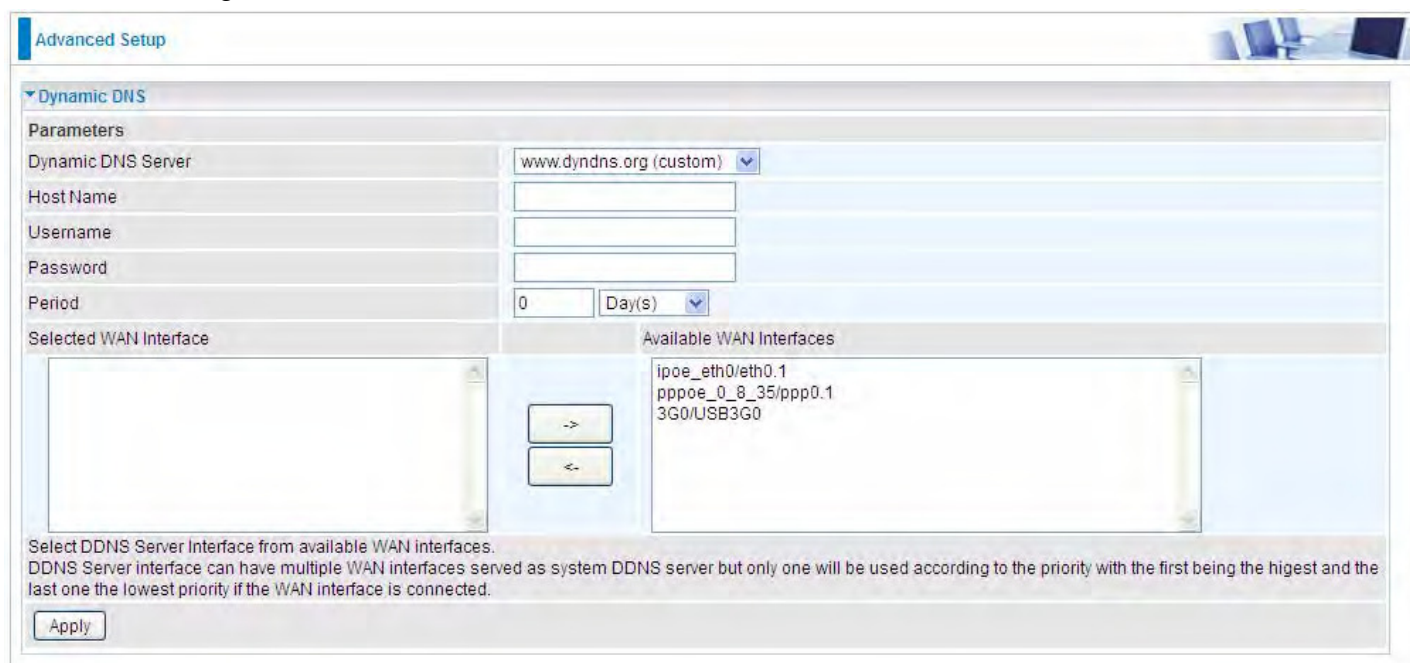
The Dynamic DNS function allows you to alias a dynamic IP address to a static hostname, allowing users whose ISP does not assign them a static IP address to use a domain name. This is especially useful for hosting servers via your ADSL connection, so that anyone wishing to connect to you may use your 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).



Host Name	Username	Service	Interface	Remove	Edit
-----------	----------	---------	-----------	--------	------

Click **Add** to register a WAN interface with the exact DNS.



Dynamic DNS Server:

Host Name:

Username:

Password:

Period: Day(s)

Selected WAN Interface:

Available WAN Interfaces:

- ipoe_eth0/eth0.1
- pppoe_0_8_35/ppp0.1
- 3G0/USB3G0

Select DDNS Server Interface from available WAN interfaces.
DDNS Server interface can have multiple WAN interfaces served as system DDNS server 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.

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.

User can register different DDNS to different interfaces.

Examples: **Note** first users have to go to the Dynamic DNS registration service provider to register an account.

User **test** register two Dynamic Domain Names in DDNS provider <http://www.dyndns.org/> .

- 1. pppoe_0_8_35 with DDNS: www.hometest.com using username/password test/test

Advanced Setup

Dynamic DNS

Parameters

Dynamic DNS Server

www.dyndns.org (custom)

Host Name

www.hometest.com

Username

test

Password

....

Period

25

Day(s)

Selected WAN Interface

pppoe_0_8_35/ppp0.1

Available WAN Interfaces

ipoe_eth0/eth0.1
3G0/USB3G0

Apply

Select DDNS Server Interface from available WAN interfaces.
DDNS Server interface can have multiple WAN interfaces served as system DDNS server 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.

Advanced Setup

Dynamic DNS

Parameters

Host Name	Username	Service	Interface	Remove	Edit
www.hometest.com	test	dyndns-custom	ppp0.1	☐	Edit

Add Remove

2. ipoe_eth0 with DDNS: www.hometest1.com using username/password test/test.

Advanced Setup

Dynamic DNS

Parameters

Dynamic DNS Server

www.dyndns.org (custom)

Host Name

www.hometest1.com

Username

test

Password

....

Period

25

Day(s)

Selected WAN Interface

ipoe_eth0/eth0.1

Available WAN Interfaces

pppoe_0_8_35/ppp0.1
3G0/USB3G0

->

<-

Select DDNS Server Interface from available WAN interfaces.
DDNS Server interface can have multiple WAN interfaces served as system DDNS server 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.

Apply

Advanced Setup

Dynamic DNS

Parameters

Host Name	Username	Service	Interface	Remove	Edit
www.hometest.com	test	dyndns-custom	ppp0.1	☐	Edit
www.hometest1.com	test	dyndns-custom	eth0.1	☐	Edit

Add

Remove

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 a web-based configuration interface for a router. At the top, there is a tab labeled "Advanced Setup". Below it, a section titled "DNS Proxy" is expanded. Under the "Parameters" heading, there are three rows of configuration options. The first row is "DNS Proxy" with radio buttons for "Enable" (selected) and "Disable". The second row is "Host name of the Broadband Router" with a text input field containing "home.gateway". The third row is "Domain name of the LAN network" with a text input field containing "home.gateway". At the bottom left of the configuration area, there are two buttons: "Apply" and "Cancel".

Parameters	
DNS Proxy	☒ Enable ☐ Disable
Host name of the Broadband Router	home.gateway
Domain name of the LAN network	home.gateway

DNS Proxy: Select whether to enable or disable DNS Proxy function, default is enabled.

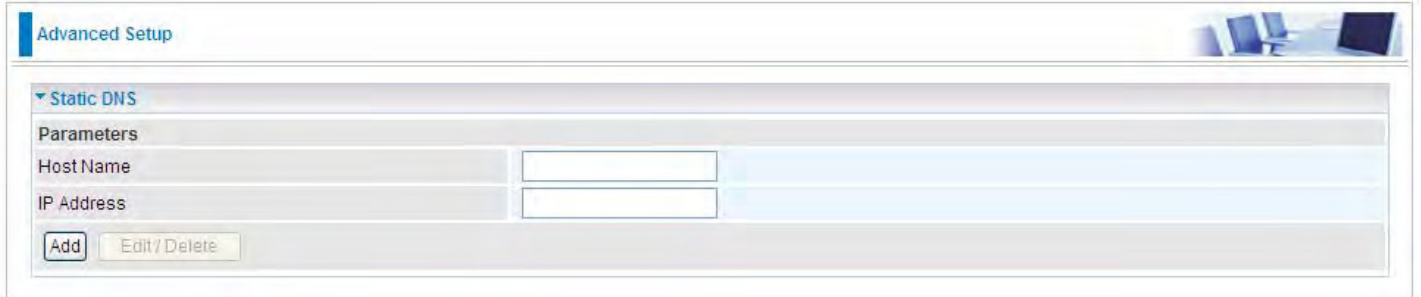
Host name of the Broadband Router: Enter the host name of the router. Default is home.gateway.

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 a web interface for a router's 'Advanced Setup'. The 'Static DNS' section is expanded, showing a table with two columns: 'Host Name' and 'IP Address'. There are two empty input fields for these columns. Below the table are two buttons: 'Add' and 'Edit/Delete'.

Parameters	
Host Name	
IP Address	

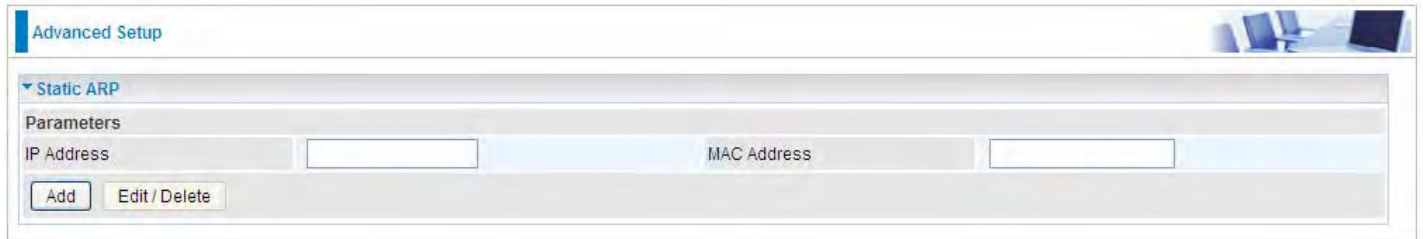
Host Name: Type the domain name (host name) for the specific IP .

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 a web-based configuration interface. At the top, there is a tab labeled "Advanced Setup" with a small icon of a desk and chairs to its right. Below this, a section titled "Static ARP" is expanded, showing a "Parameters" area. This area contains two input fields: "IP Address" and "MAC Address". Below these fields are two buttons: "Add" and "Edit / Delete".

Parameters	
IP Address	MAC Address
Add	Edit / Delete

IP Address: Enter the IP of the device that the corresponding MAC address will be mapped to.

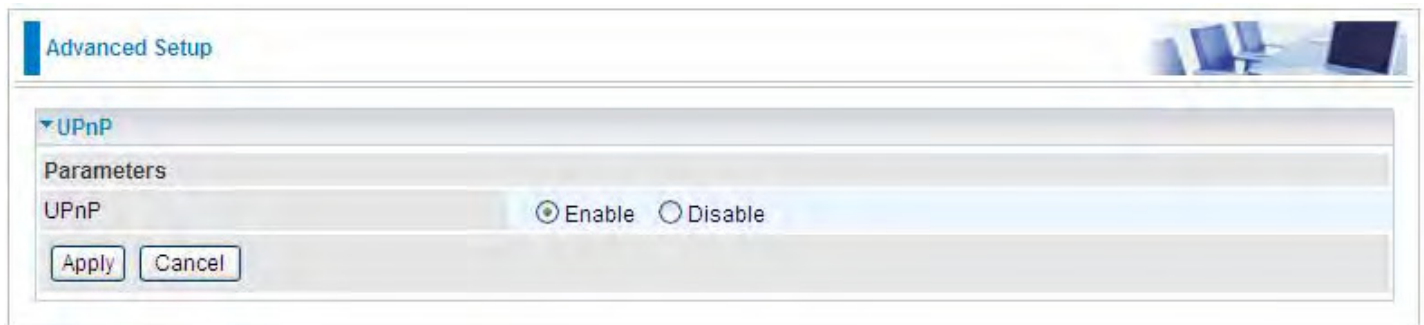
MAC Address: Enter the MAC address that corresponds to the IP address of the device.

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.



UPnP:

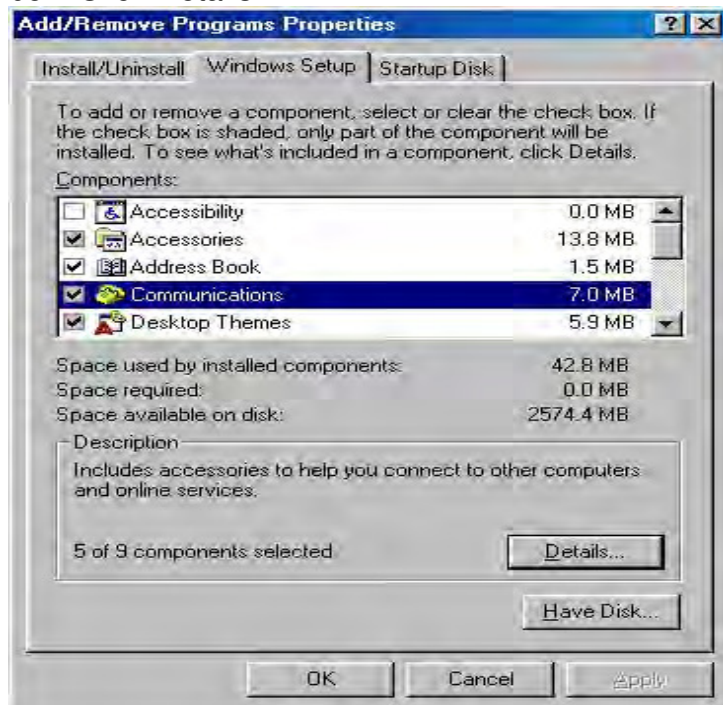
- ① **Enable:** Check to enable the router's UPnP functionality.
- ① **Disable:** Check to disable the router's UPnP functionality.

Installing UPnP in Windows Example

Follow the steps below to install the UPnP in Windows Me.

Step 1: Click Start and Control Panel. Double-click Add/Remove Programs.

Step 2: Click on the Windows Setup tab and select Communication in the Components selection box. Click Details.



Step 3: In the Communications window, select the Universal Plug and Play check box in the Components selection box.



Step 4: Click OK to go back to the Add/Remove Programs Properties window. Click Next.

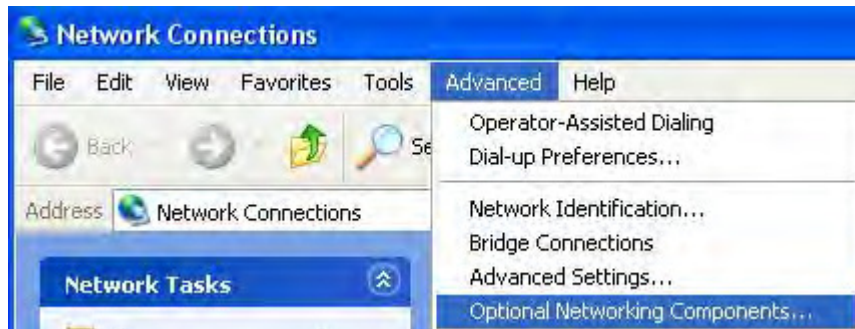
Step 5: Restart the computer when prompted.

Follow the steps below to install the UPnP in Windows XP.

Step 1: Click Start and Control Panel.

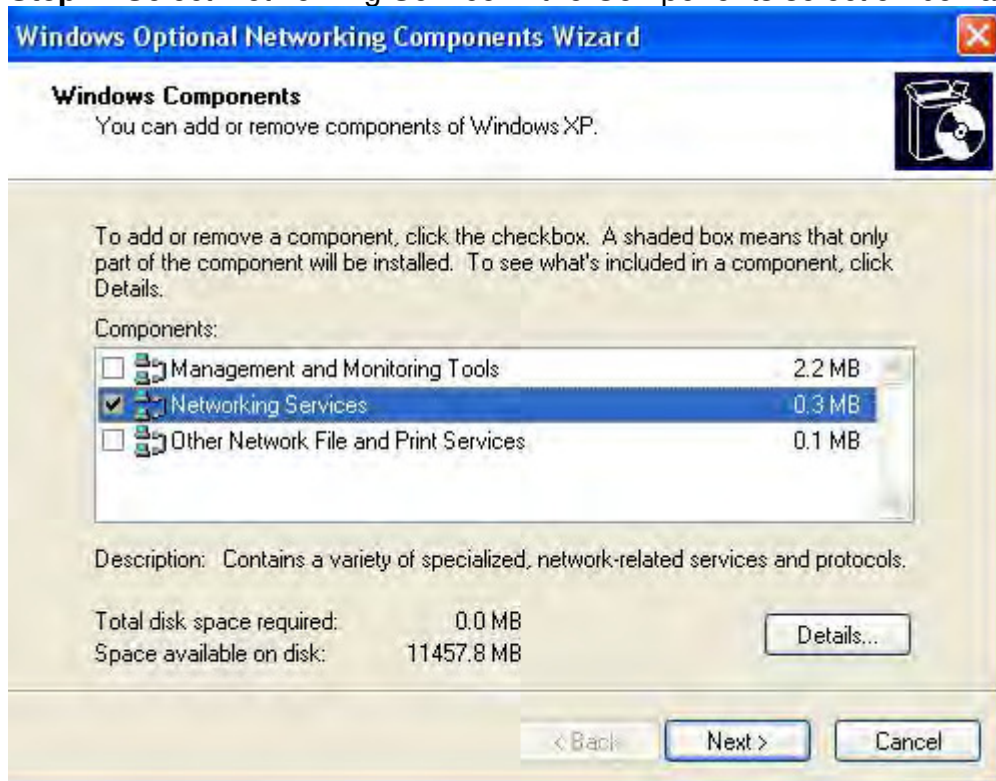
Step 2: Double-click Network Connections.

Step 3: In the Network Connections window, click Advanced in the main menu and select Optional Networking Components



The Windows Optional Networking Components Wizard window displays.

Step 4: Select Networking Service in the Components selection box and click Details.



Step 5: In the Networking Services window, select the Universal Plug and Play check box.

Step 6: Click **OK** to go back to the Windows Optional Networking Component Wizard window and click **Next**.



Auto-discover Your UPnP-enabled Network Device

Step 1: Click start and Control Panel. Double-click Network Connections. An icon displays under Internet Gateway.

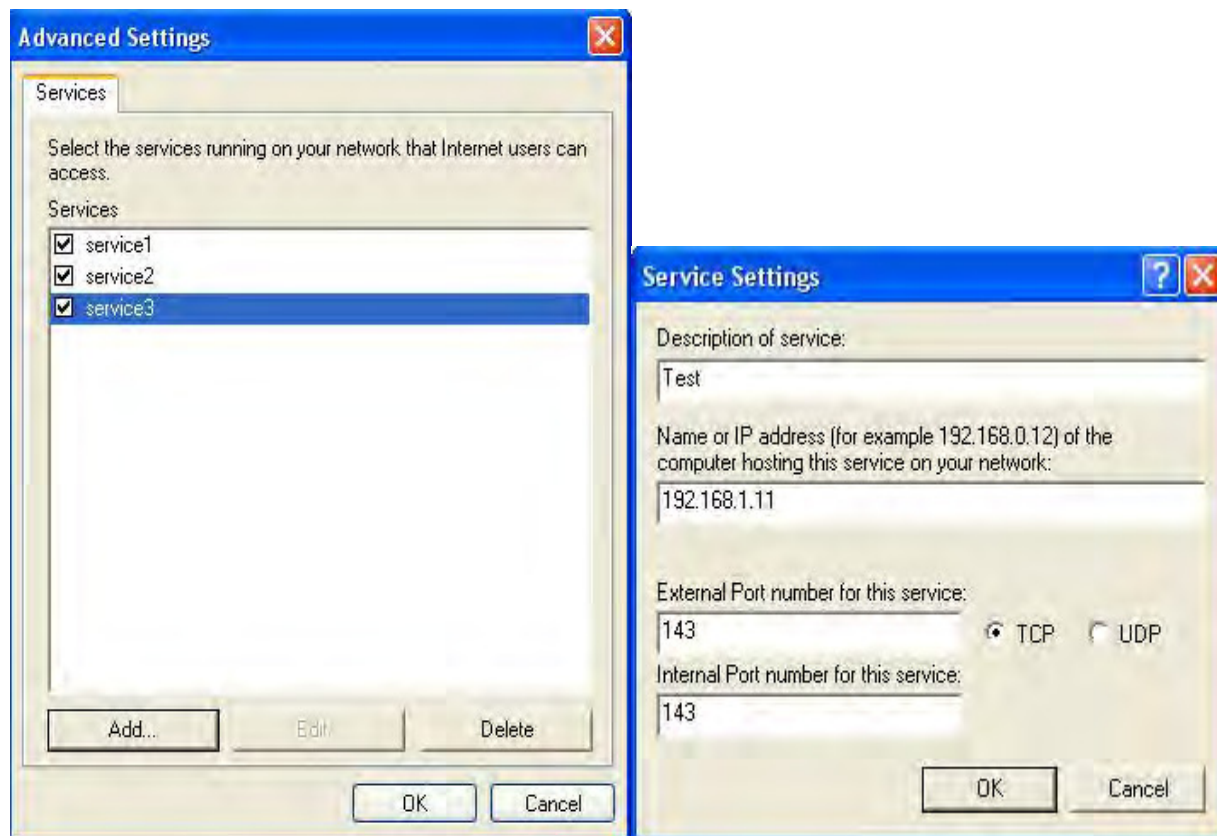
Step 2: Right-click the icon and select Properties.



Step 3: In the Internet Connection Properties window, click Settings to see the port mappings that were automatically created.

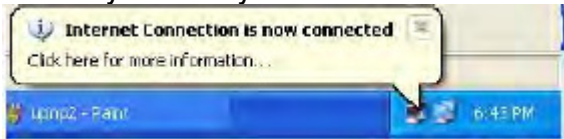


Step 4: You may edit or delete the port mappings or click Add to manually add port mappings.



Step 5: Select Show icon in notification area when connected option and click OK. An icon displays

in the system tray



Step 6: Double-click on the icon to display your current Internet connection status.



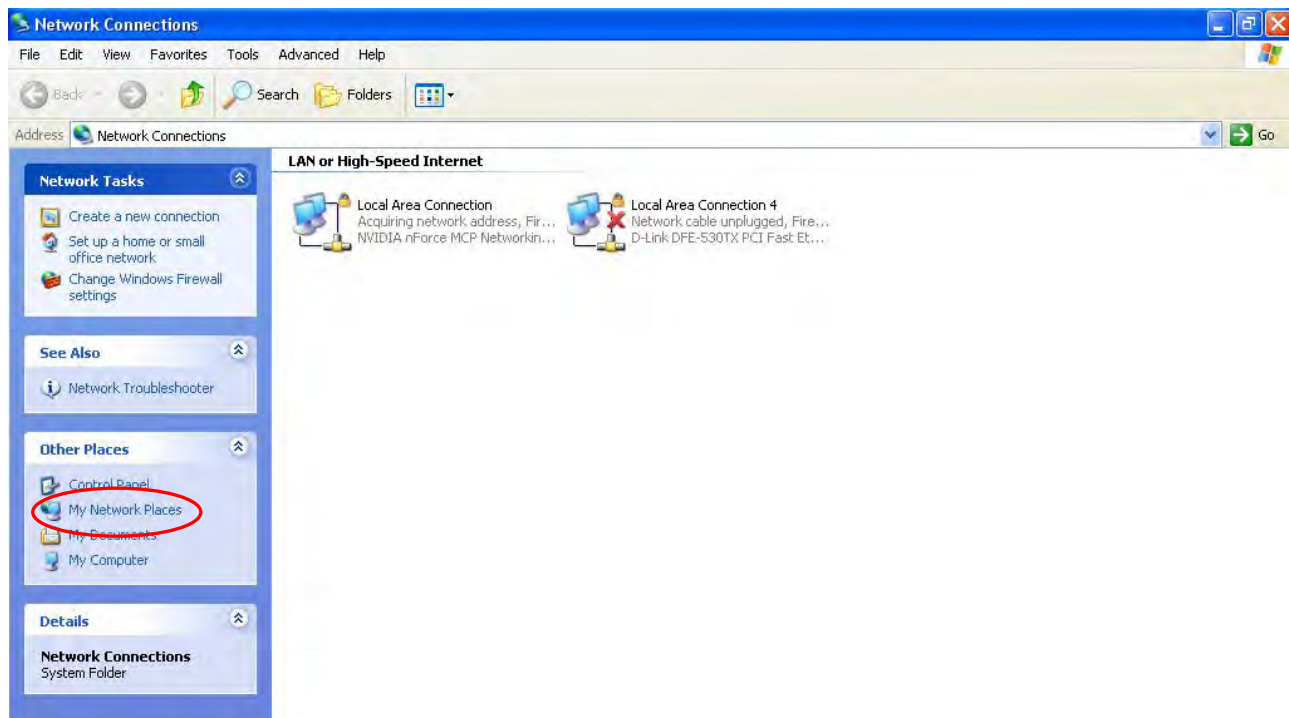
Web Configurator Easy Access

With UPnP, you can access web-based configuration for the BiPAC 7820NZ without first finding out the IP address of the router. This helps if you do not know the router's IP address. Follow the steps below to access web configuration.

Step 1: Click Start and then Control Panel.

Step 2: Double-click Network Connections.

Step 3: Select My Network Places under Other Places.



Step 4: An icon describing each UPnP-enabled device shows under Local Network.

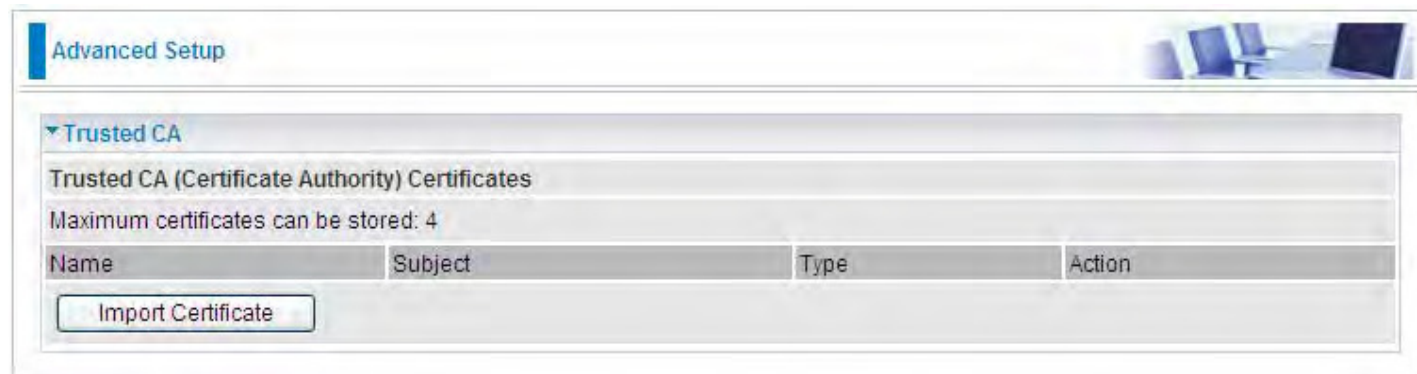
Step 5: Right-click on the icon of your BiPAC 7820NZ and select Invoke. The web configuration login screen displays.

Step 6: Right-click on the icon of your BiPAC 7820NZ and select Properties. A properties window displays basic information about the BiPAC 7820NZ.

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
------	---------	------	--------

Import Certificate

Certificate Name: The certificate identification name.

Subject: The certificate subject.

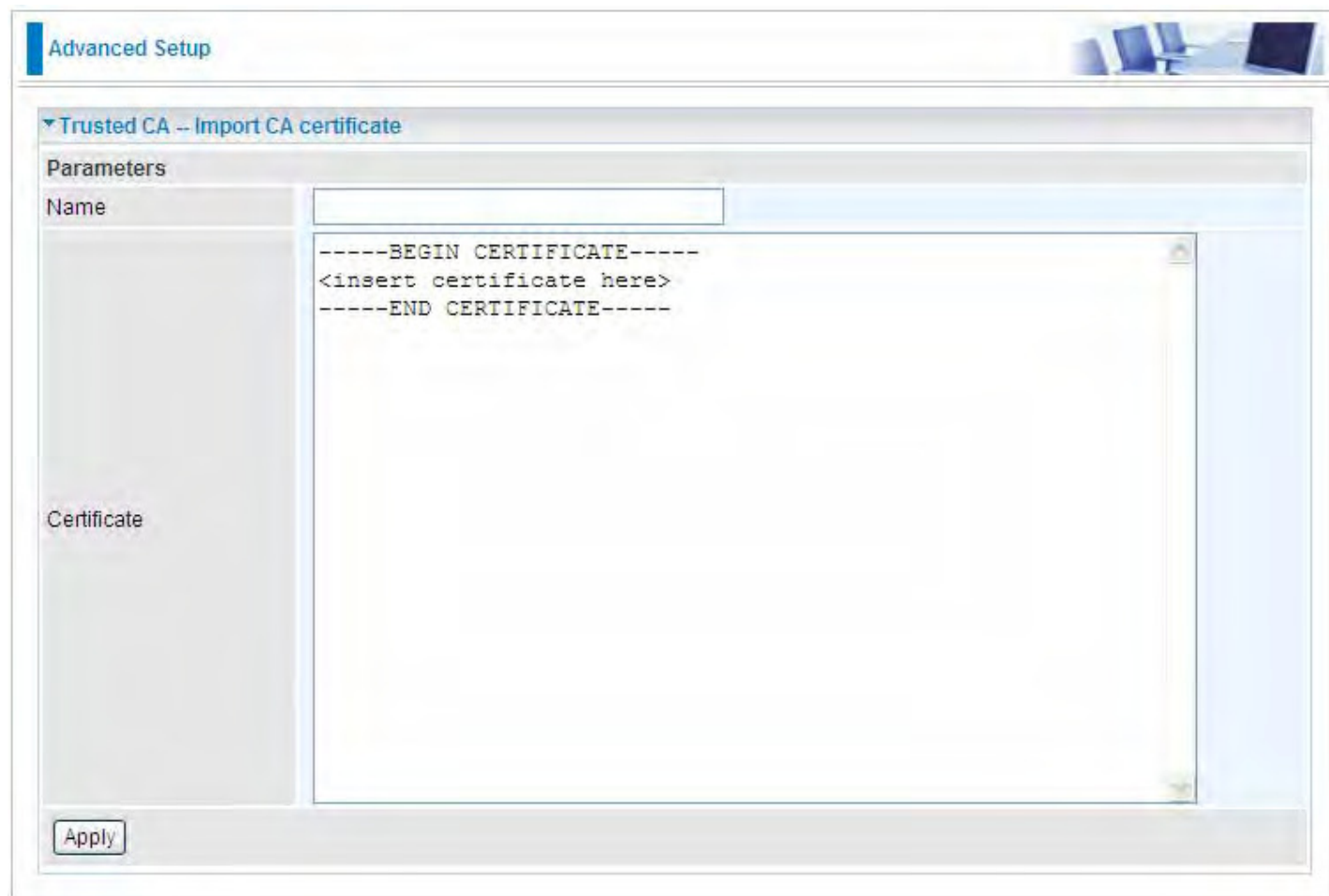
Type: The certificate type information. "ca", indicates that the certificate is a CA-signed certificate. "self", indicates that the certificate is a certificate owner signed one.

"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

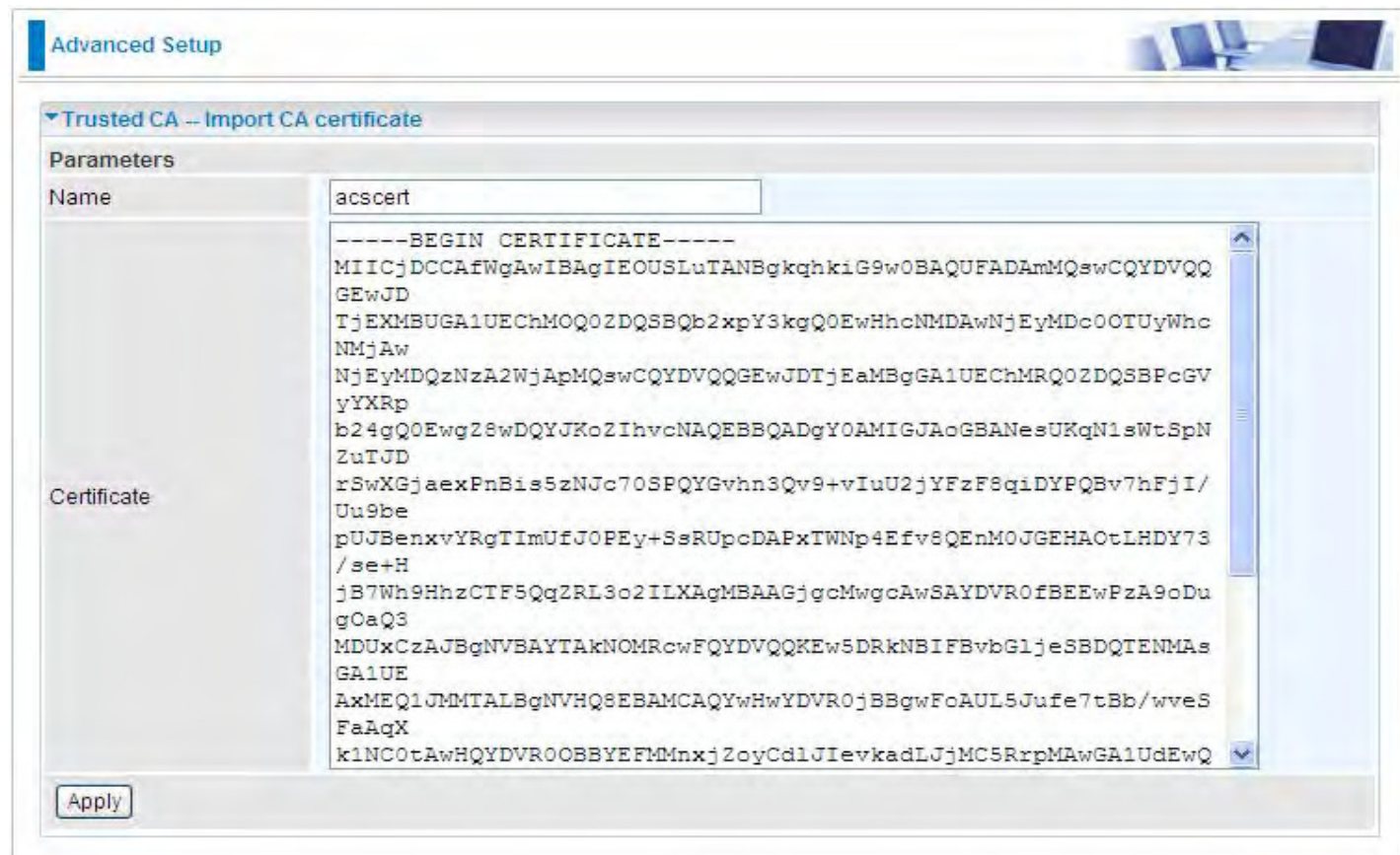
Name

Certificate

-----BEGIN CERTIFICATE-----
<insert certificate here>
-----END CERTIFICATE-----

Apply

Enter the certificate name and insert the certificate.



Advanced Setup

Trusted CA -- Import CA certificate

Parameters

Name

acscert

Certificate

-----BEGIN CERTIFICATE-----
MIICjDCCAfWgAwIBAgIEOUSLuTANBgkqhkiG9w0BAQUFADAmMQswCQYDVQQ
GEwJD
TjEXMBUGA1UEChMQQ0ZDQSBQb2xpY3kgQ0EwHhcNMDAwNjEyMDc0OTUyWhc
NMjAw
NjEyMDQzNzA2WjApMQswCQYDVQQGEwJDTjEaMBGGA1UEChMRQ0ZDQSBPcGV
yYXRp
b24gQ0EwgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBANesUKqN1sWtSpN
ZuTJD
rSwXGjaexPnBis5zNJc70SPQYGVhn3Qv9+vIuU2jYFzF8qiDYPQBv7hFjI/
Uu9be
pUJBenxvYRgTImUfJOPEy+SsRUpcDAPxTWNp4Efv8QEnMOJGEHAOtLHDY73
/se+H
jB7Wh9HhzCTF5QqZRL3o2ILXAgMBAAGjgcMwgcAwSAYDVROfBEEwPzA9oDu
gOaQ3
MDUxCzAJBgNVBAYTAKNOMRcwFQYDVQQKEw5DRkNBIFBvbG1jeSBBDQITENMA
GA1UE
AxMEQ1JUMMTALBgNVHQSEBAMCAQYwHwYDVROjBBgwFoAUL5Jufe7tBb/wveS
FaAqX
k1NCotAwHQYDVROBBYEFMMnxjZoyCd1JIEvkdLJjMC5RrpMAwGA1UdEwQ

Apply

Click Apply to confirm your settings.

Advanced Setup

Trusted CA

Trusted CA (Certificate Authority) Certificates

Maximum certificates can be stored: 4

Name	Subject	Type	Action
acscert	C=CN/O=CFCA Operation CA	ca	ViewRemove

Import Certificate

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

☒ Enable

LAN to LAN (Intra LAN) Multicast

☐ Enable

Membership Join Immediate (IPTV)

☐

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

☒ Enable

LAN to LAN (Intra LAN) Multicast

☐ 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

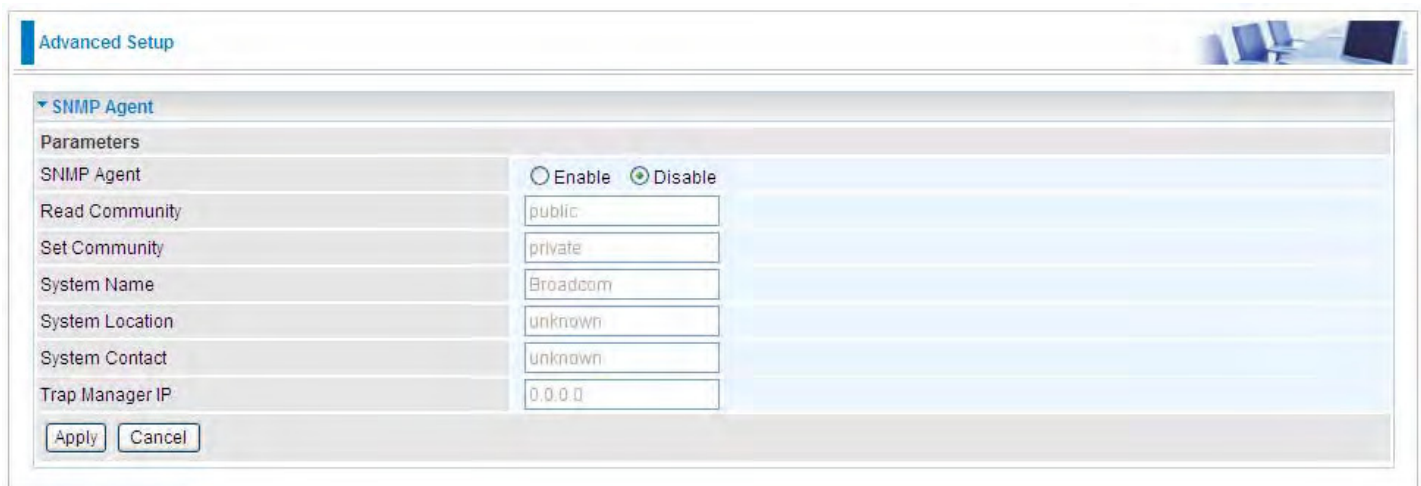
SNMP Agent

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-based configuration interface titled "Advanced Setup". Under the "SNMP Agent" section, there are several parameters to be configured:

Parameters	
SNMP Agent	☐ Enable ☒ 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.

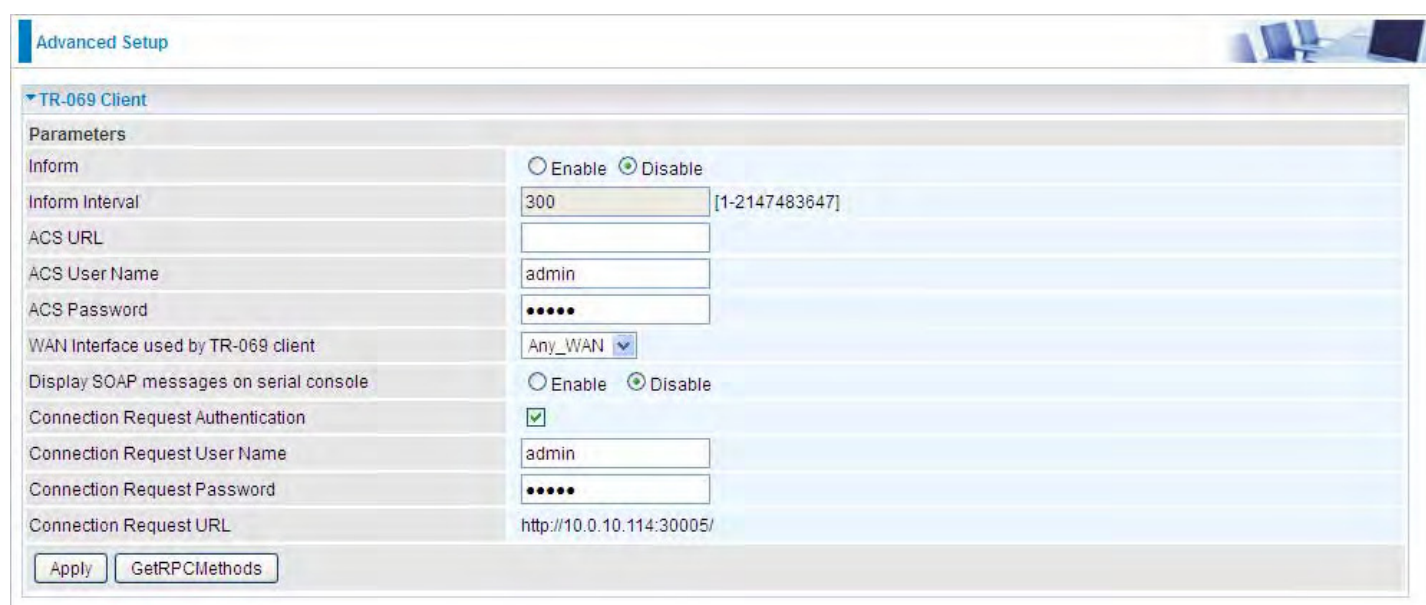
System Contact: user-defined contact message.

Trap manager IP: enter the IP address of the server receiving the trap sent by SNMP agent.

TR- 069 Client

TR-069 (short for Technical Report 069) is a DSL Forum (which was later renamed as Broadband Forum) technical specification entitled CPE WAN Management Protocol (CWMP). It defines an application layer protocol for remote management of end-user devices.

As a bidirectional SOAP/HTTP based protocol it can provides the communication between customer premises equipment (CPE) and Auto Configuration Server (ACS). It includes both a safe configuration and the control of other CPE management functions within an integrated framework. In the course of the booming broadband market, the number of different internet access possibilities grew as well (e.g. modems, routers, gateways, set-top box, VoIP-phones).At the same time the configuration of this equipment became more complicated –too complicated for end-users. For this reason, TR-069 was developed. It provides the possibility of auto configuration of the access types. Using TR-069 the terminals can get in contact with the Auto Configuration Servers (ACS) and establish the configuration automatically and let ACS configure CPE automatically.



Parameters	
Inform	☐ Enable ☒ 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	☐ Enable ☒ Disable
Connection Request Authentication	☒
Connection Request User Name	admin
Connection Request Password	
Connection Request URL	http://10.0.10.114:30005/

Apply GetRPCMethods

Inform: select enable to let CPE be authorized to send Inform message to automatically connect to ACS.

Inform Interval: Specify the inform interval time (sec) which CPE used to periodically send inform message to automatically connect to ACS. When the inform interval time arrives, the CPE will send inform message to automatically connect to ACS.

ACS URL: Enter the ACS server login name.

ACS User Name: Specify the ACS User Name for ACS authentication to the connection from CPE.

ACS password: Enter the ACS server login password.

WAN interface used by TR-069: select the interface used by TR-069.

Display SOAP message on serial console: select whether to display SOAP message on serial console.

Connection Request Authentication: Check to enable connection request authentication feature.

Connection Request User Name: Enter the username for ACS server to make connection request.

Connection Request User Password: Enter the password for ACS server to make connection request.

Connection Request URL: Automatically match the URL for ACS server to make connection request.

GetRPCMethods: Supported by both CPE and ACS, display the supported RFC listing methods.

Click **Apply** to apply your settings.

HTTP Port

The device equips user to change the embedded web server accessing port. Default is 80.



The screenshot shows a web-based configuration interface titled "Advanced Setup". Inside, there is a section for "HTTP Port" with a "Parameters" label. Below this, the "HTTP Port" is set to "80" in a text box, with "(Default: 80)" displayed to its right. At the bottom of the configuration area, there are two buttons: "Apply" and "Cancel".

Remote Access

It is to allow remote access to the router to view or configure.

The screenshot shows the 'Advanced Setup' page with the 'Remote Access' section expanded. Under 'Parameters', 'Remote Access' is checked 'Enable'. 'Enable Service' has checkboxes for HTTP (checked), SSH, FTP, TELNET, and SNMP. An 'Apply' button is below. The 'Allowed Access IP Address Range' section has a 'Valid' checkbox checked. Below it, 'IP Version' is set to 'IPv4' and 'IP Address Range' has two empty input fields separated by a tilde (~). 'Add' and 'Edit / Delete' buttons are at the bottom.

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.

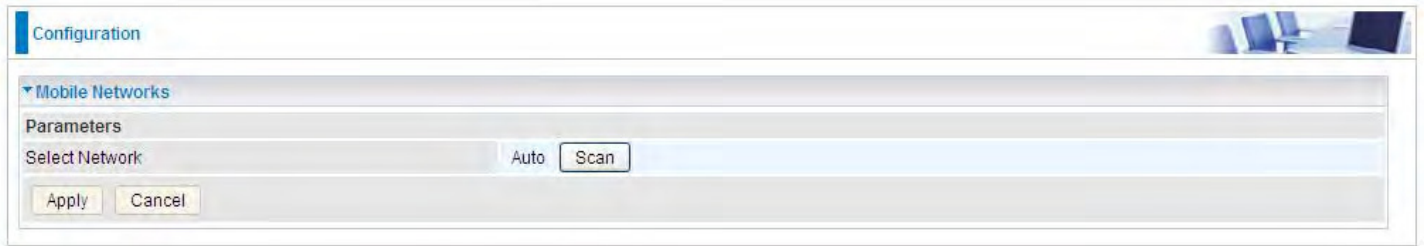
Note: 1. If user wants to grant remote access to IPs, first enable **Remote Access**.

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 a software window titled "Configuration" with a small icon of a laptop in the top right corner. Inside the window, there is a section titled "Mobile Networks" with a downward-pointing arrow. Below this, the word "Parameters" is displayed. A "Select Network" label is positioned to the left of a light blue button labeled "Auto". To the right of the "Auto" button is a smaller button labeled "Scan". At the bottom of the window, there are two buttons: "Apply" and "Cancel".

3G/LTE Usage Allowance

3G/LTE usage allowance is designated for users to monitor and control the 3G flow usage. 7820NZ's 3G/LTE usage allowance offers exact control settings for each SIM card.

Advanced Setup

3G/LTE Usage Allowance

Parameters

3G/LTE Usage Allowance ☒ Enable

SIM 1 (Current)

Mode

☒ Volume-based
Only Download MB data volume per month included

☐ Time-based
1 hours per month included

The billing period begins on day 1 of a month.

Over usage allowance action E-mail Alert

E-mail alert at percentage of bandwidth 80 %

Save the statistics to ROM Every one hours

SIM 2

Mode

☒ Volume-based
Only Download MB data volume per month included

☐ Time-based
1 hours per month included

The billing period begins on day 1 of a month.

Over usage allowance action E-mail Alert

E-mail alert at percentage of bandwidth 80 %

Save the statistics to ROM Every one hours

Apply Cancel

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.

Advanced Setup

Power Management

Parameters

Wait instruction when Idle	☒ Enable	Status	Enabled
DRAM Self Refresh	☒ Enable	Status	Enabled
Energy Efficient Ethernet	☒ Enable	Status	Enabled
Ethernet Auto Power Down and Sleep	☒ Enable	Status	Enabled
Adaptive Voltage Scaling	☒ Enable	Status	Enabled

Apply

Refresh

Number of ethernet interfaces in:
Powered up: 3
Powered down: 2

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.

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

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

BiPAC 7820NZ offers diagnostics tools including “Ping” and “Trace route test” tools to check for problems associated with network connections.

The screenshot shows the 'Advanced Setup' window with a 'Diagnostics Tools' section. It contains two main test configurations: 'Ping Test' and 'Trace route Test'. Each test has fields for 'Destination Host' and 'Source Address'. The 'Source Address' field includes a radio button to select between 'Interface' (with a dropdown menu) and 'IP Address' (with a text input). The 'Ping Test' section has a 'Ping Test' button. The 'Trace route Test' section has fields for 'Max TTL value' (set to 16, range [2-30]) and 'Wait time' (set to 3, range [2-999] seconds), along with a 'Trace route Test' button.

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

Advanced Setup

Diagnostics Tools

Ping Test

Destination Host:

Source Address: ☒ Interface ☐ IP Address

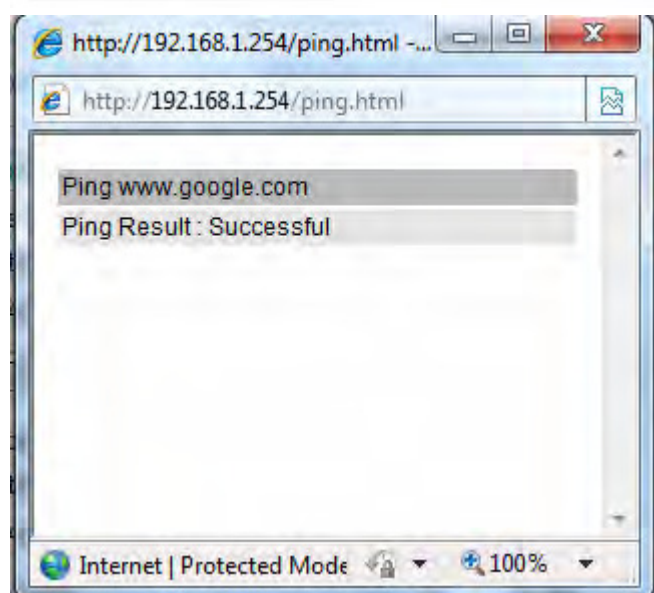
Trace route Test

Destination Host:

Source Address: ☒ Interface ☐ IP Address

Max TTL value: [2-30]

Wait time: seconds [2-999]



Example: “trace” www.google.com

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]

http://192.168.1.254/tracert.html - Windows Intern...

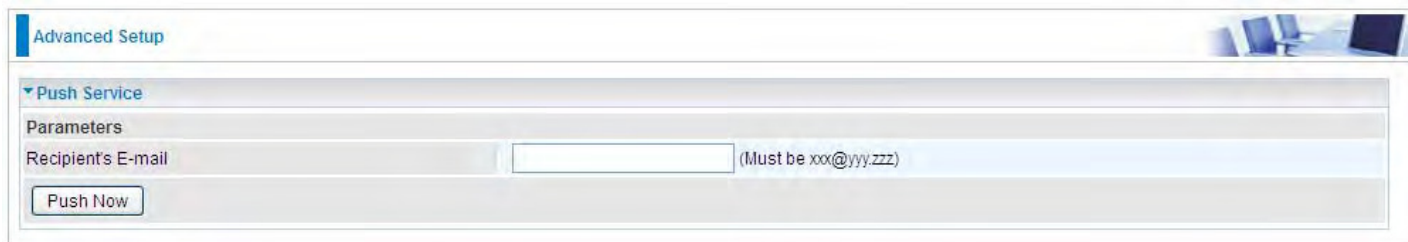
http://192.168.1.254/tracert.html

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.



The screenshot shows a web-based configuration interface titled "Advanced Setup". Under the "Push Service" section, there is a "Parameters" area. It includes a label "Recipient's E-mail" followed by a text input field. To the right of the input field is a validation hint: "(Must be xxx@yyy.zzz)". Below the input field is a button labeled "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](#).

Diagnostics

Check the connections, including Ethernet connection, Internet Connection and wireless connection. Click **Help** link that can lead you to the interpretation of the results and the possible, simply troubleshooting.

Diagnostics --- pppoe_0_8_35

▼ Test the connection to your local network

Test LAN Connection (P3)	FAIL	Help
Test LAN Connection (P2)	PASS	Help
Test LAN Connection (P1)	FAIL	Help
Test LAN Connection (P4/EWAN)	FAIL	Help
Test your Wireless Connection	PASSPASS	Help

▼ Test the connection to your DSL service provider

Test xDSL Synchronization	PASS	Help
Test ATM OAM F5 segment ping	PASS	Help
Test ATM OAM F5 end-to-end ping	PASS	Help

▼ Test the connection to your Internet service provider

Test PPP server connection	PASS	Help
Test authentication with ISP	PASS	Help
Test the assigned IP address	PASS	Help
Ping default gateway	PASS	Help
Ping primary Domain Name Server	FAIL	Help

Test

Test With OAM F4

Fault Management

IEEE 802.1ag Connectivity Fault Management (CFM) is a standard defined by IEEE. It defines protocols and practices for OAM (Operations, Administration, and Maintenance) for paths through 802.1 bridges and local area networks (LANs). Fault Management is to uniquely test the VDSL PTM connection; Push service

Advanced Setup

802.1ag Connectivity Fault Management

Parameters

This diagnostic is only used for xDSL PTM mode.

Maintenance Domain (MD) Level: 2

Destination MAC Address:

802.1Q VLAN ID: 0 [0-4095]

xDSL Traffic Type: Inactive

Test the connection to another Maintenance End Point (MEP)

Loopback Message (LBM):

Find Maintenance End Points (MEPs):

Linktrace Message (LTM):

Set MD Level Send Loopback Send Linktrace

Maintenance Domain (MD) Level: Maintenance Domains (MDs) are management spaces on a network, typically owned and operated by a single entity. MDs are configured with Names and Levels, where the eight levels range from 0 to 7. A hierarchal relationship exists between domains based on levels. The larger the domain, the higher the level value.

Maintenance End Point: Points at the edge of the domain, define the boundary for the domain. A MEP sends and receives CFM frames through the relay function, drops all CFM frames of its level or lower that come from the wire side.

Link Trace: Link Trace messages otherwise known as Mac Trace Route are Multicast frames that a MEP transmits to track the path (hop-by-hop) to a destination MEP which is similar in concept to User Datagram Protocol (UDP) Trace Route. Each receiving MEP sends a Trace route Reply directly to the Originating MEP, and regenerates the Trace Route Message.

Loop-back: Loop-back messages otherwise known as MaC ping are Unicast frames that a MEP transmits, they are similar in concept to an Internet Control Message Protocol (ICMP) Echo (Ping) messages, sending Loopback to successive MIPs can determine the location of a fault. Sending a high volume of Loopback Messages can test bandwidth, reliability, or jitter of a service, which is similar to flood ping. A MEP can send a Loopback to any MEP or MIP in the service. Unlike CCMs, Loop back messages are administratively initiated and stopped.

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%

Chapter 5: Troubleshooting

If your router is not functioning properly, please refer to the suggested solutions provided in this chapter. If your problems persist or the suggested solutions do not meet your needs, please kindly contact your service provider or Billion for support.

Problems with the router

Problem	Suggested Action
None of the LEDs is on when you turn on the router	Check the connection between the router and the adapter. If the problem persists, most likely it is due to the malfunction of your hardware. Please contact your service provider or Billion for technical support.
You have forgotten your login username or password	Try the default username "admin" and password "admin". If this fails, you can restore your router to its factory settings by pressing the reset button on the device rear side.

Problems with WAN interface

Problem	Suggested Action
Frequent loss of ADSL line sync (disconnections)	Ensure that all other devices connected to the same telephone line as your router (e.g. telephones, fax machines, analogue modems) have a line filter connected between them and the wall socket (unless you are using a Central Splitter or Central Filter installed by a qualified and licensed electrician), and ensure that all line filters are correctly installed and the right way around. Missing line filters or line filters installed the wrong way around can cause problems with your ADSL connection, including causing frequent disconnections. If you have a back-to-base alarm system you should contact your security provider for a technician to make any necessary changes.

Problem with LAN interface

Problem	Suggested Action
Cannot PING any PC on LAN	Check the Ethernet LEDs on the front panel. The LED should be on for the port that has a PC connected. If it does not lit, check to see if the cable between your router and the PC is properly connected. Make sure you have first uninstalled your firewall program before troubleshooting.
	Verify that the IP address and the subnet mask are consistent for both the router and the workstations.

Appendix: Product Support & Contact

If you come across any problems please contact the dealer from where you purchased your product.

Contact Billion

Worldwide:

<http://www.billion.com>

MAC OS is a registered Trademark of Apple Computer, Inc.

Windows 7/8, Windows XP and Windows Vista are registered Trademarks of Microsoft Corporation.

Federal Communication Commission Interference Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- ♦ Reorient or relocate the receiving antenna.
- ♦ Increase the separation between the equipment and receiver.
- ♦ Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- ♦ Consult the dealer or an experienced radio/TV technician for help.

FCC Caution:

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

(1) This device may not cause harmful interference

(2) This device must accept any interference received, including interference that may cause undesired operation.

Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment. . This device and its antenna(s) must not be co-located or operating in conjunction with any other antenna or transmitter.

FCC Radiation Exposure Statement

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

IC Warning:

This device complies with Industry Canada licence-exempt RSS standard(s). Operation is subject to the following two conditions:

- (1) this device may not cause interference, and
- (2) this device must accept any interference, including interference that may cause undesired operation of the device.

Le présent appareil est conforme aux CNR d'Industrie Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes :

- (1) l'appareil ne doit pas produire de brouillage, et
- (2) l'utilisateur de l'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.