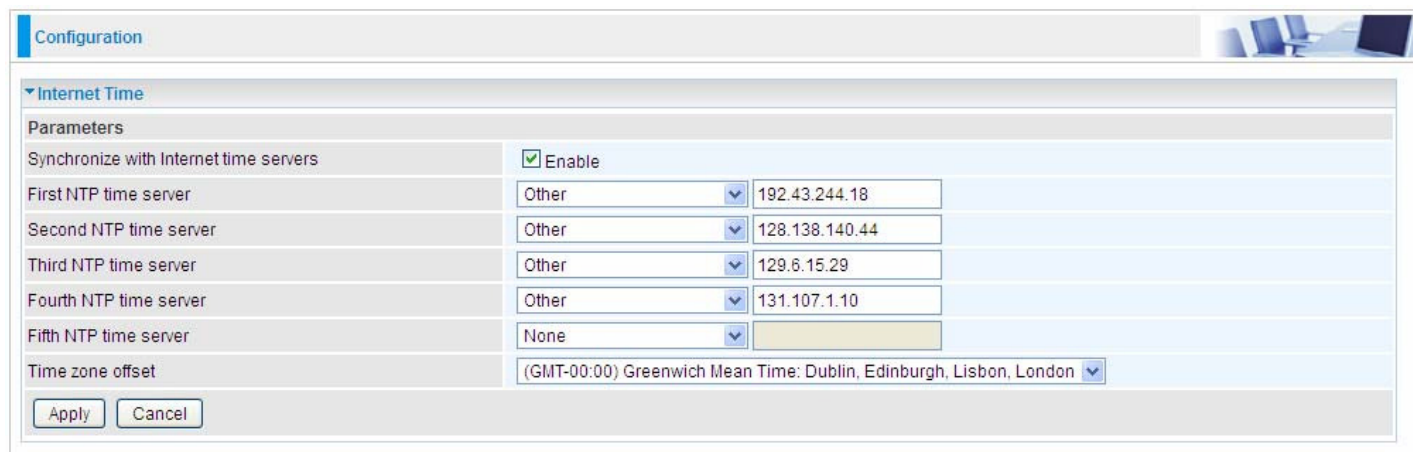


System

Internet Time

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

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



The screenshot shows the 'Configuration' page of a router, specifically the 'Internet Time' section. The 'Parameters' are as follows:

Parameters	
Synchronize with Internet time servers	☒ Enable
First NTP time server	Other [v] 192.43.244.18
Second NTP time server	Other [v] 128.138.140.44
Third NTP time server	Other [v] 129.6.15.29
Fourth NTP time server	Other [v] 131.107.1.10
Fifth NTP time server	None [v]
Time zone offset	(GMT-00:00) Greenwich Mean Time: Dublin, Edinburgh, Lisbon, London [v]

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

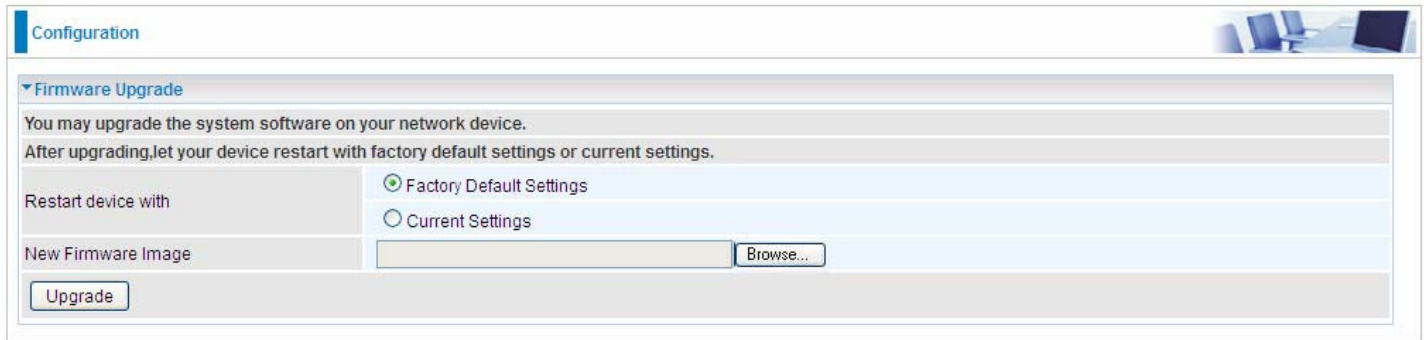
Choose the NTP time server from the drop-down menu, if you prefer to specify an NTP server other than those in the drop-down list, simply enter its IP address in their appropriate blanks provided as shown above. Your ISP may also provide an SNTP server for you to use.

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

Click **Apply** to apply your settings.

Firmware Upgrade

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



The screenshot shows the 'Configuration' page of a router, specifically the 'Firmware Upgrade' section. It includes instructions on upgrading the system software and restarting the device with either factory default or current settings. There are radio buttons for 'Factory Default Settings' (selected) and 'Current Settings'. A text field for 'New Firmware Image' is followed by a 'Browse...' button. An 'Upgrade' button is at the bottom left of the section.

Restart device with:

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

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

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

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



Warning

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

Backup / Update

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

Configuration

Backup / Update

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

Backup Configuration

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

Backup Settings

Restore Configuration

Configuration File

Browse...

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

Update Settings

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

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

progress

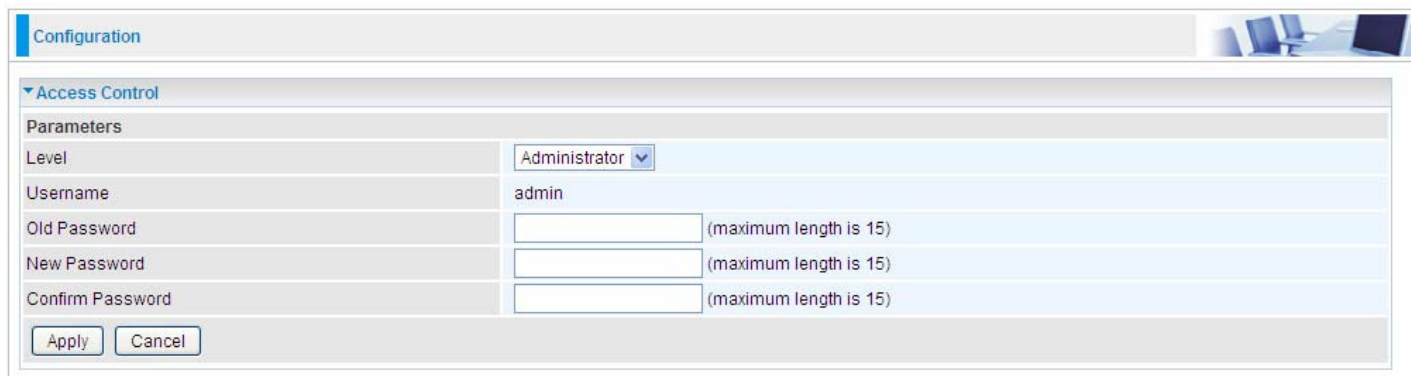
progress...

Do not switch off device during flash update or rebooting.

total :6%

Access Control

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



The screenshot shows the 'Configuration' page with the 'Access Control' section expanded. Under 'Parameters', the 'Level' is set to 'Administrator'. The 'Username' is 'admin'. There are three password fields: 'Old Password', 'New Password', and 'Confirm Password', each with a note '(maximum length is 15)'. At the bottom are 'Apply' and 'Cancel' buttons.

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

- ① **Administrator:** the root user, corresponding default username and password are admin and admin respectively.
- ① **Advanced:** username for the remote user to login, corresponding default username and password are support and support respectively.
- ① **User:** username for the general user, when logon to the web page, only few items would be listed for common user, corresponding default username password are user and user respectively.

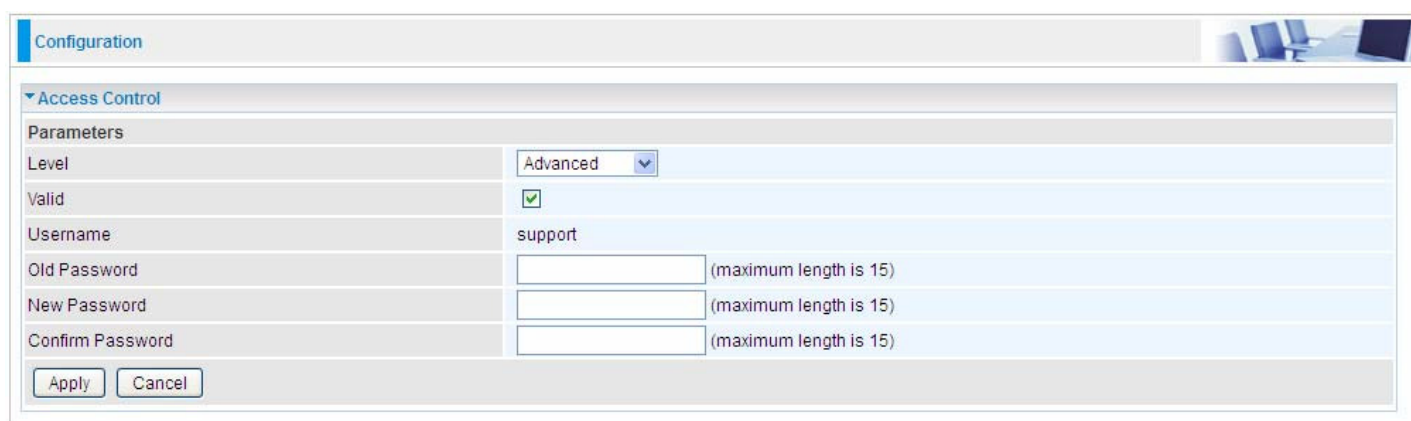
Username: The default username for each user level.

Old Password: Enter the old password.

New Password: Enter the new password.

Confirm Password: Enter again the new password to confirm.

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



The screenshot shows the 'Configuration' page with the 'Access Control' section expanded. Under 'Parameters', the 'Level' is set to 'Advanced'. The 'Valid' checkbox is checked. The 'Username' is 'support'. There are three password fields: 'Old Password', 'New Password', and 'Confirm Password', each with a note '(maximum length is 15)'. At the bottom are 'Apply' and 'Cancel' buttons.

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

Mail Alert

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

Configuration

▼ Mail Alert

Server Information

WAN Port: DSL

Apply all the settings to: ☐ Ethernet ☐ 3G/LTE

SMTP Server:

Username:

Password:

Sender's E-mail: (Must be xxx@yyy.zzz)

SSL / TLS: ☐ Enable

Port: 25

Account Test

Failover / Failback

Recipient's E-mail: (Must be xxx@yyy.zzz)

WAN IP Change Alert

Recipient's E-mail: (Must be xxx@yyy.zzz)

3G/4G LTE Usage Allowance

Recipient's E-mail: (Must be xxx@yyy.zzz)

SIM lost

Recipient's E-mail: (Must be xxx@yyy.zzz)

Apply Cancel

WAN Port: Mail Alert feature can be applicable to every WAN mode: Ethernet, DSL and 3G/4G LTE. Select the port you want to use Mail Alert.

For example DSL, then when the WAN connection is in DSL mode and when there is any unexpected event, the alert message will be sent to your specified E-mail.

Apply all settings to: check whether you want to have a copy of the settings to apply to other WAN port, suppose the above Main port is DSL, then if you enable this function, then Ethernet port will have the same configuration.

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

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

Password: Enter the password of your email account.

Sender's Email: Enter your email address.

SSL/TLS: Check to whether to enable SSL/TLS encryption feature.

Port: the port, default is 25.

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

Recipient's Email (Failover / Failback): Enter the email address that will receive the alert message once the WAN-interface failover or failback occurs.

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

Recipient's Email (3G/4G LTE Usage Allowance): Enter the email address that will receive the alert message once the 3G over Usage Allowance occurs.

Recipient's Email (SIM lost): Enter the email address that will receive the alert message once the

SIM card loss has been detected.

SMS Alert

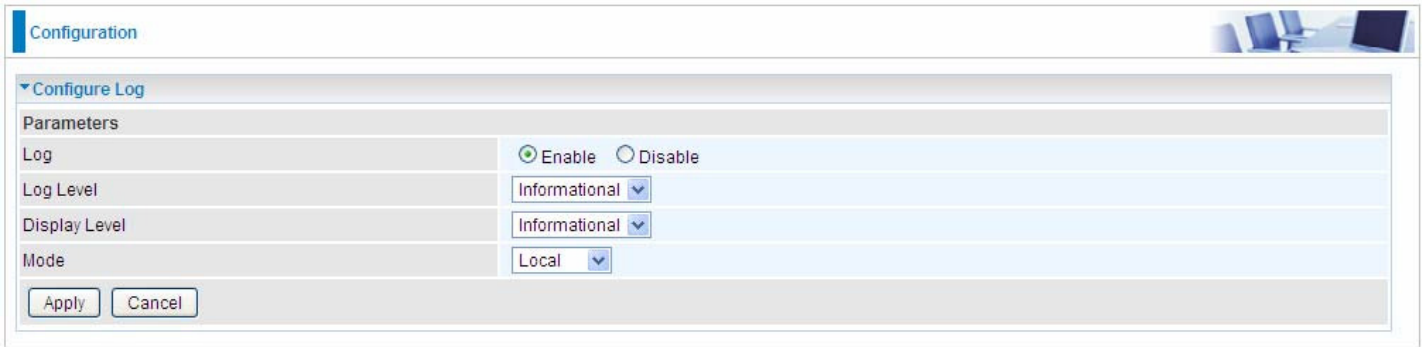
SMS, Short Message Service, is to inform clients the information clients subscribe. The BiPAC 8920NXL-600 offers SMS alert sending clients alert messages when a WAN IP change is detected.



The screenshot shows a web-based configuration interface. At the top, there is a 'Configuration' tab. Below it, a section titled 'SMS Alert' is expanded, showing a 'WAN IP Change Alert' configuration. Under this, there is a label 'Recipient's Number' followed by a text input field. At the bottom of this section is an 'Apply' button.

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

Configure Log



Log: Enable or disable this function.

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

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

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

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

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

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

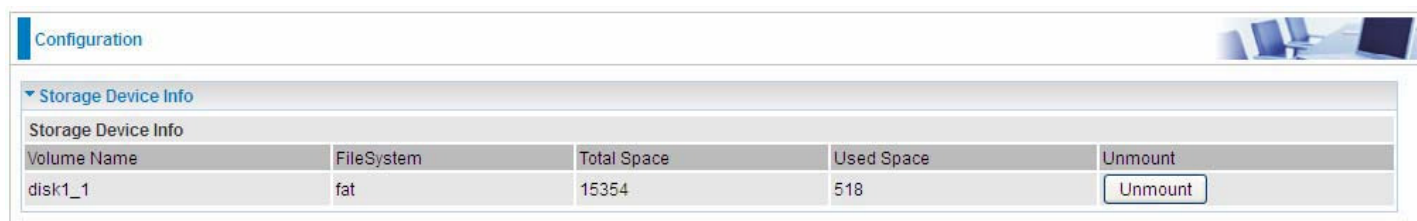
Click **Apply** to save your settings.

USB

Storage here refers to network sharing in the network environment, USB devices act as the storage carrier for DLNA, common file sharing.

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.



The screenshot shows a web interface with a 'Configuration' tab. Under the 'Storage Device Info' section, there is a table with the following data:

Volume Name	FileSystem	Total Space	Used Space	Unmount
disk1_1	fat	15354	518	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 Accounts

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.
Default user admin.

Configuration

▼ User Accounts

User Accounts

A maximum accounts can be configured: 16

Username	Home Directory	Remove	Edit
admin	/		

Add

Remove

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

Configuration

▼ User Accounts

Parameters

Username

Password

Confirm Password

Volume Name

disk1_1

Apply

Cancel

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 disk1_1.

Configuration

▼ User Accounts

User Accounts

A maximum accounts can be configured: 16

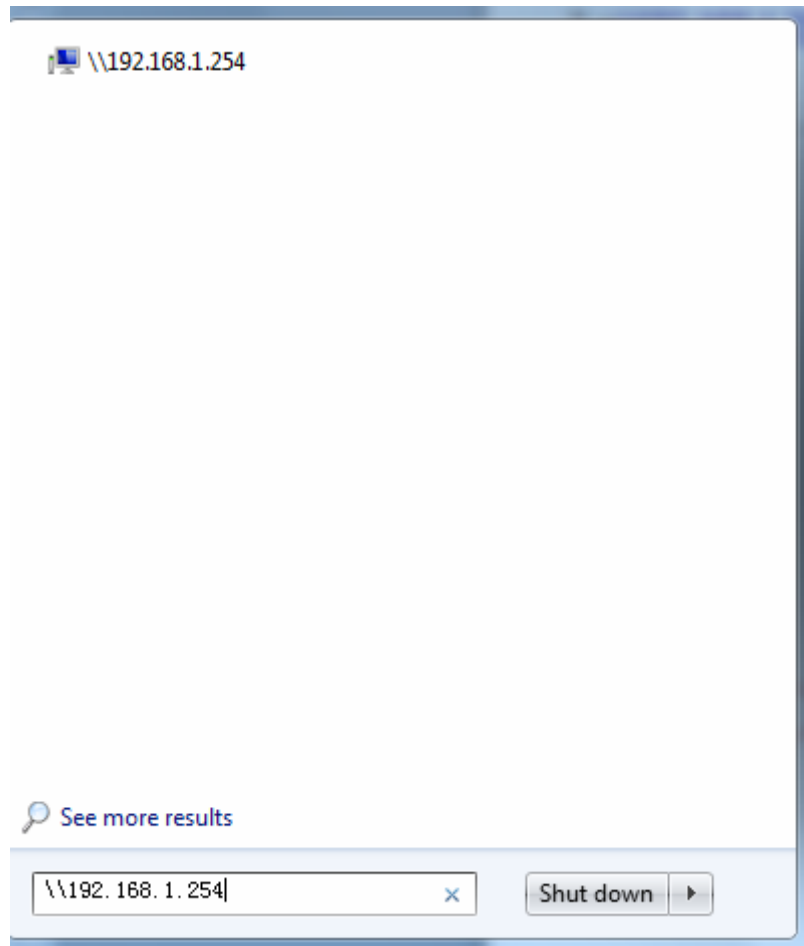
Username	Home Directory	Remove	Edit
admin	/		
test	disk1_1/test	☐	Edit

Add

Remove

Accessing mechanism of Storage:

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

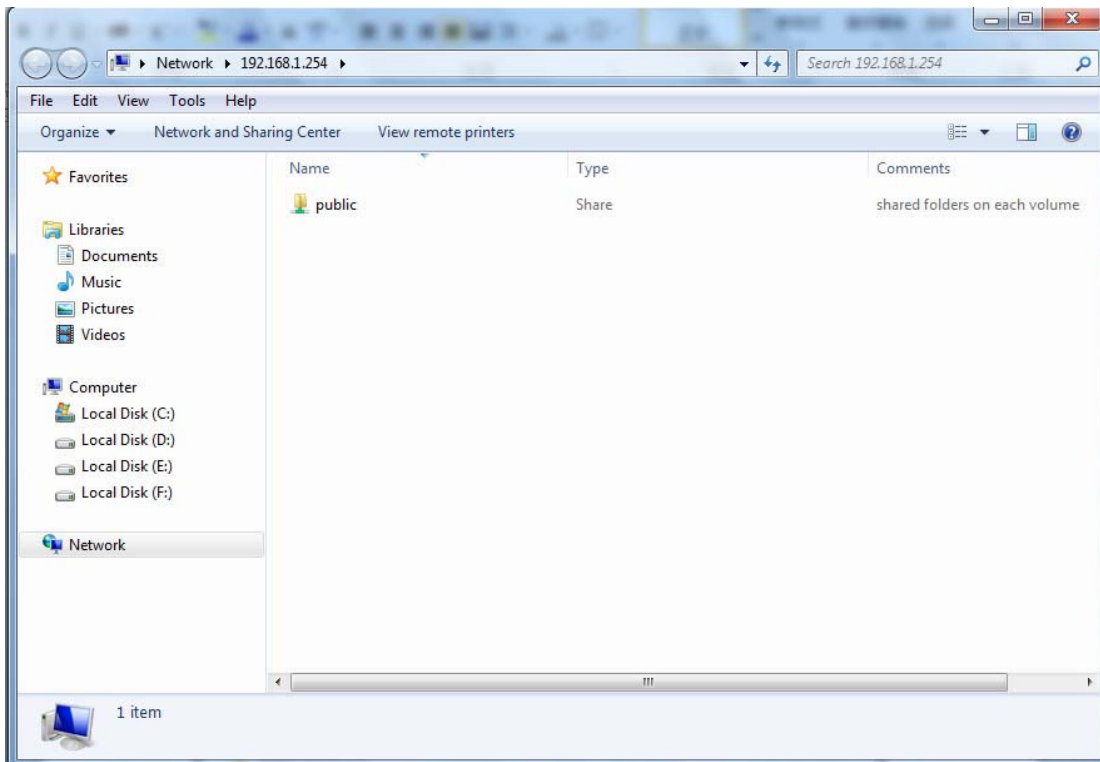


When accessing the network storage, you can see a folder named “**public**”, users should have the account to enter, and the account can be set at the User Accounts section.

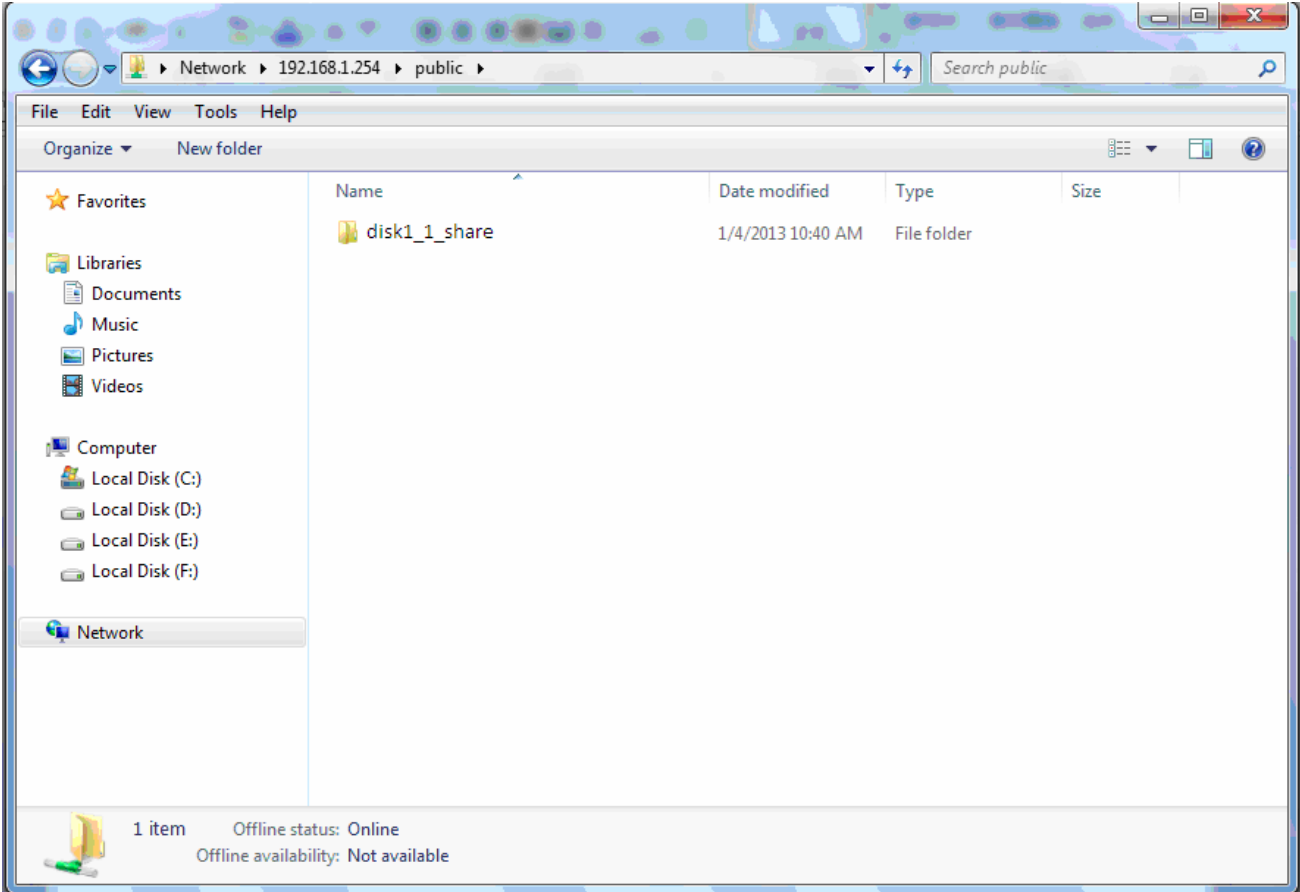
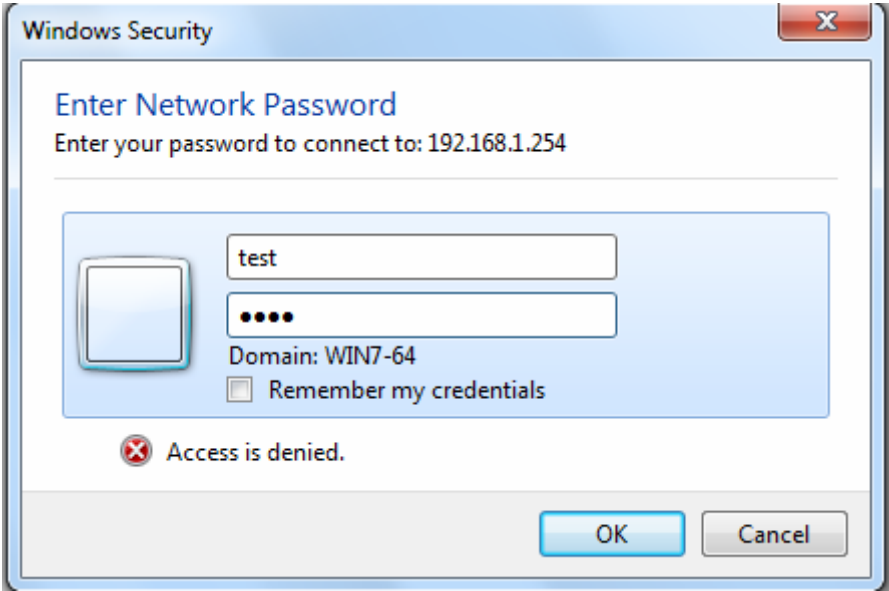
When first logged on to the network folder, you will see the “**public**” folder.

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

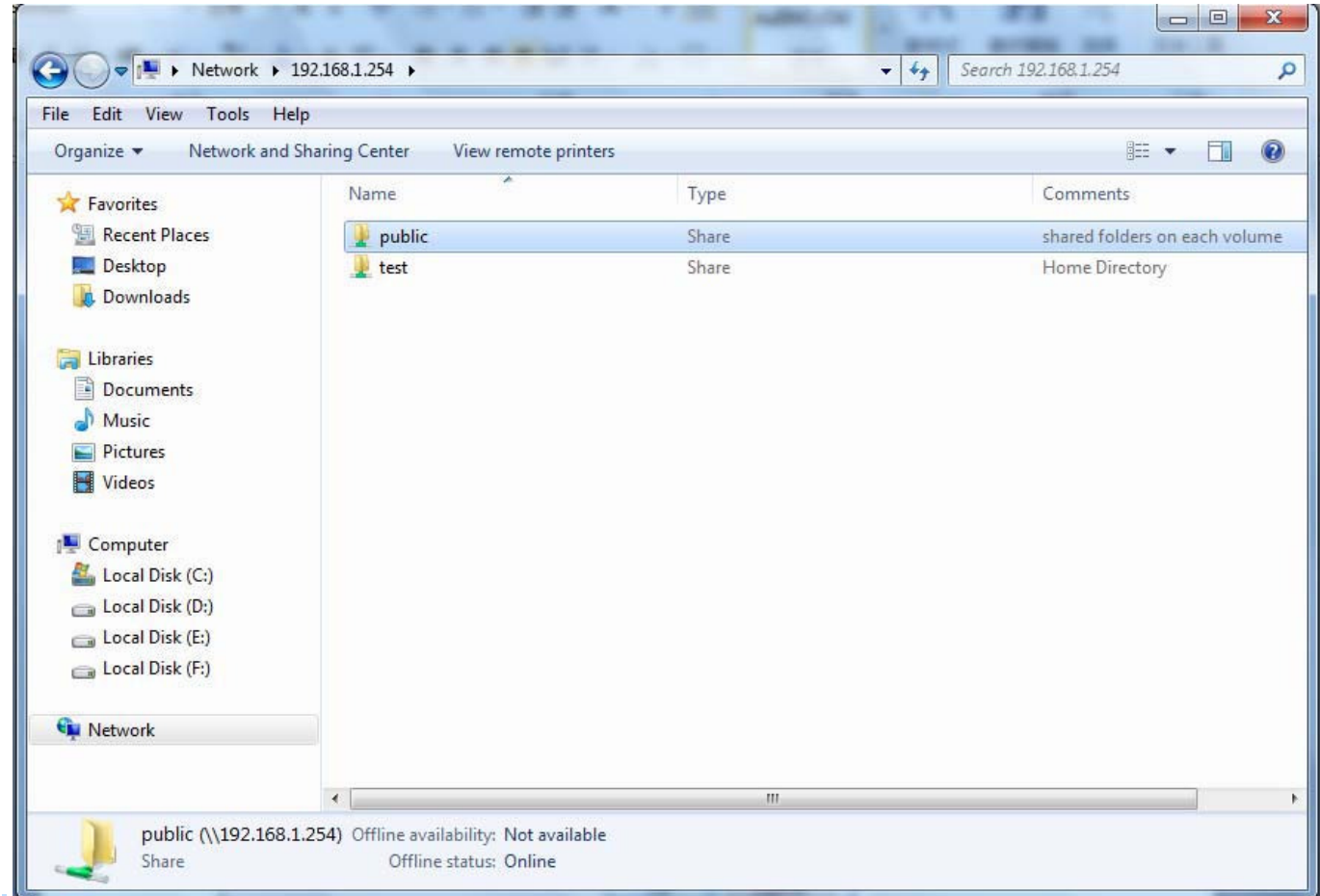
When user register a USB account and log successfully, a private folder (the same name as the user account registered) exclusive for each user is established. Go on to see the details.



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.



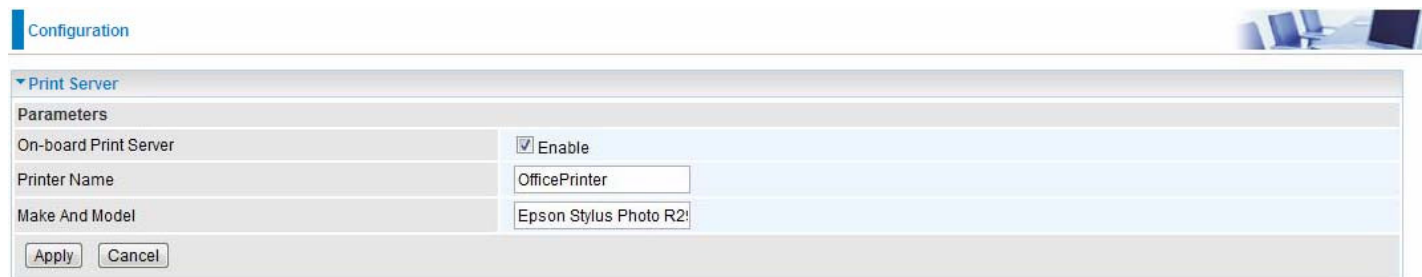
Print Server

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 BiPAC 8920NX(L)-600. This allows you to print from any location on your network.

Note: Only USB printers are supported.

Setup of the printer is a 3 -step process

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



The screenshot shows the 'Configuration' page of the BiPAC 8920NX(L)-600 router. The 'Print Server' section is expanded, showing the 'Parameters' tab. The 'On-board Print Server' is checked and set to 'Enable'. The 'Printer Name' is set to 'OfficePrinter' and the 'Make And Model' is set to 'Epson Stylus Photo R2!'. There are 'Apply' and 'Cancel' buttons at the bottom of the section.

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*

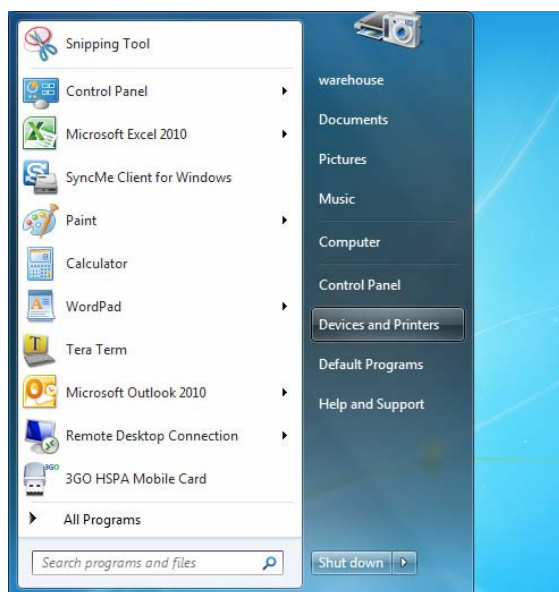
Note:

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)

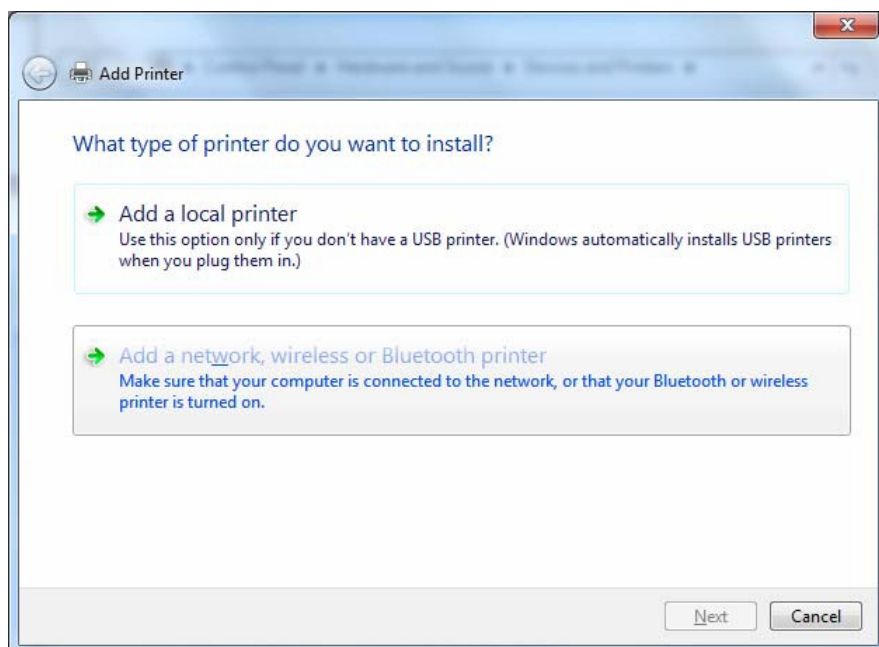
Step 1: Click **Start** and select "Devices and Printers"



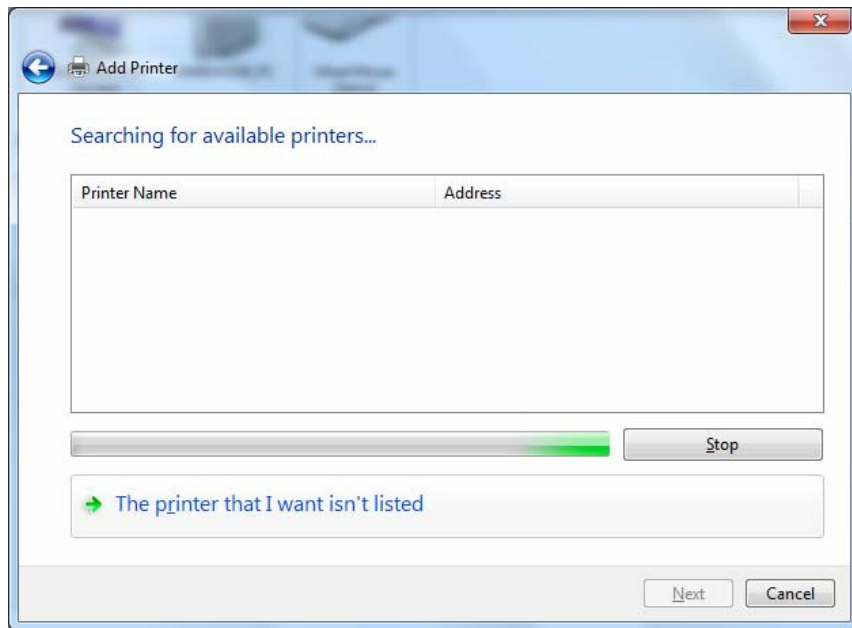
Step 2: Click "Add a Printer".



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



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

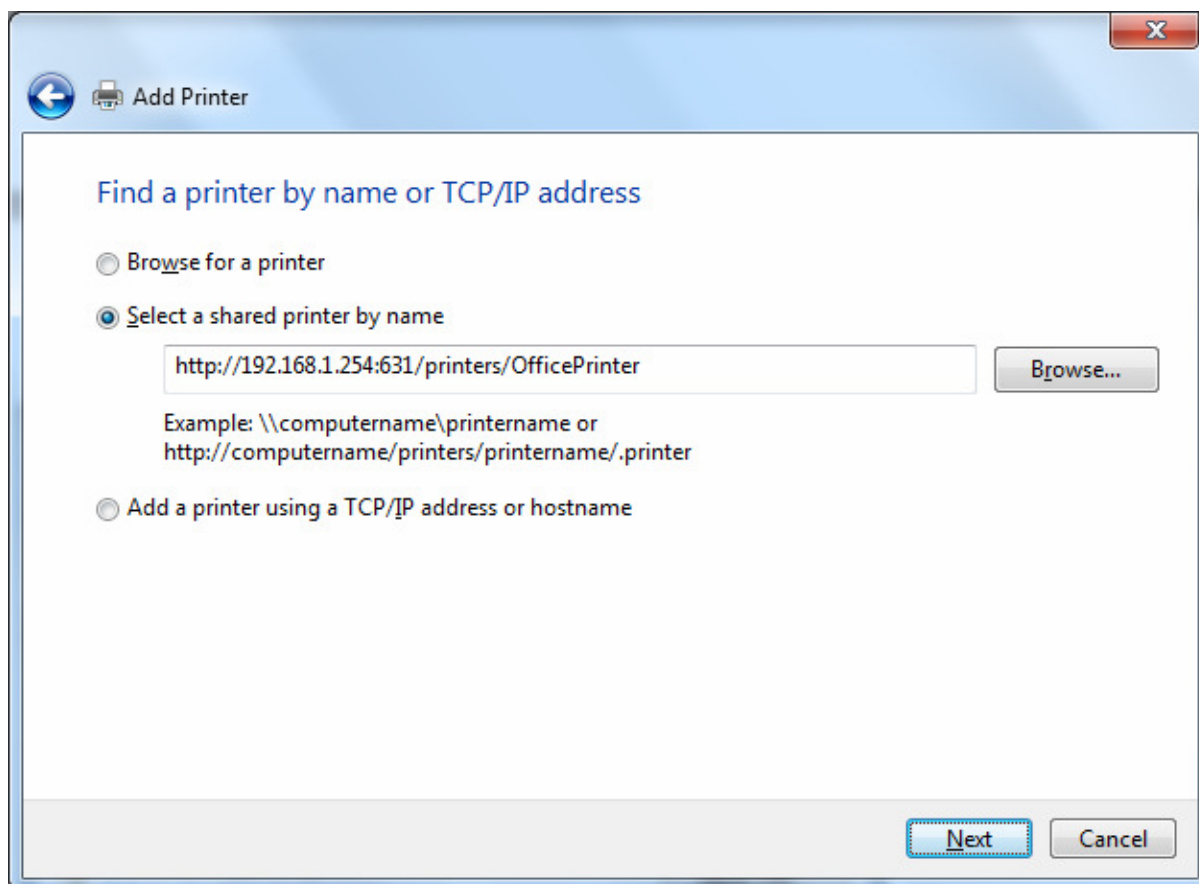


Step 5: Select “Select a shared printer by name”

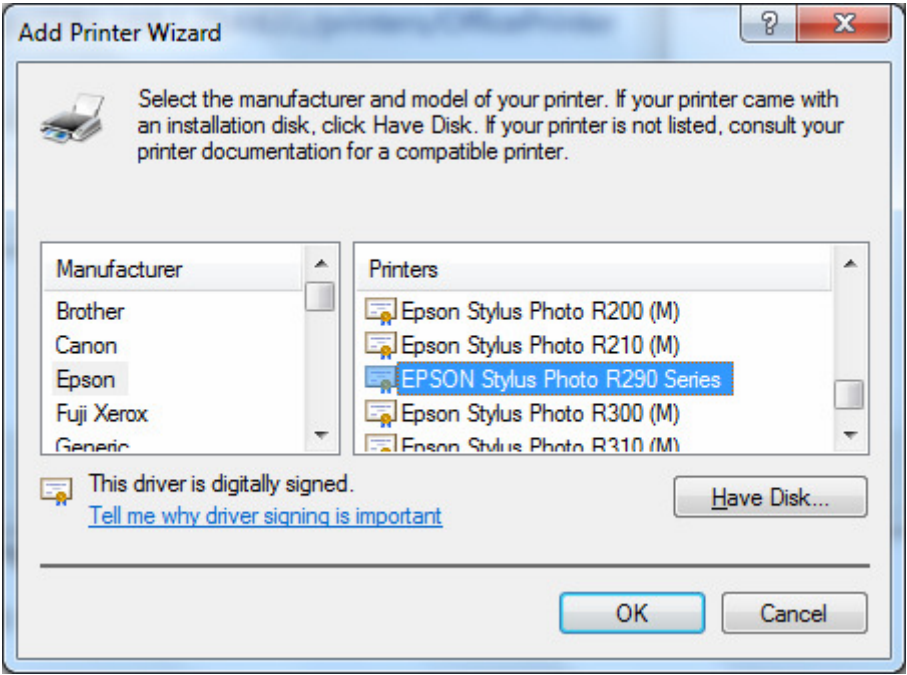
Enter `http://8920NXL600-LAN-IP:631/printers/printer-name` or. Make sure printer’s name is the same as what you set in the router earlier

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

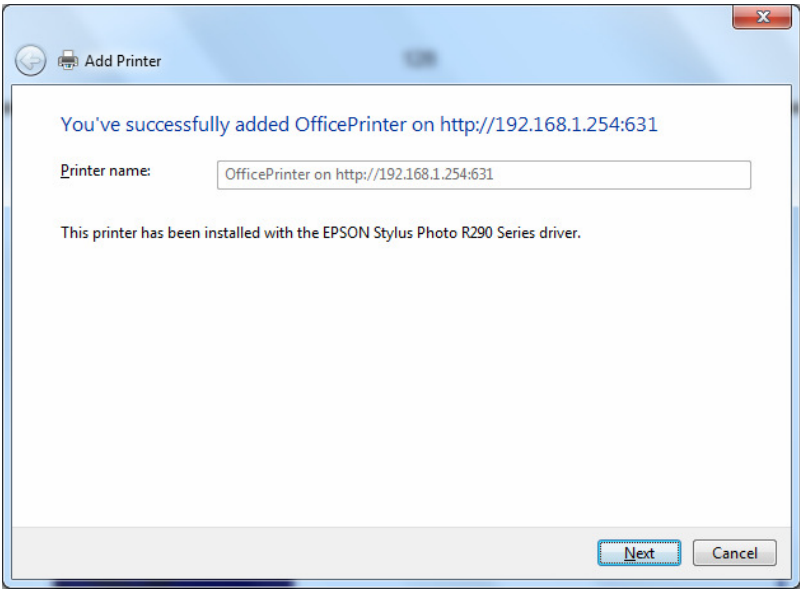
OfficePrinter is the Printer Name we setup earlier



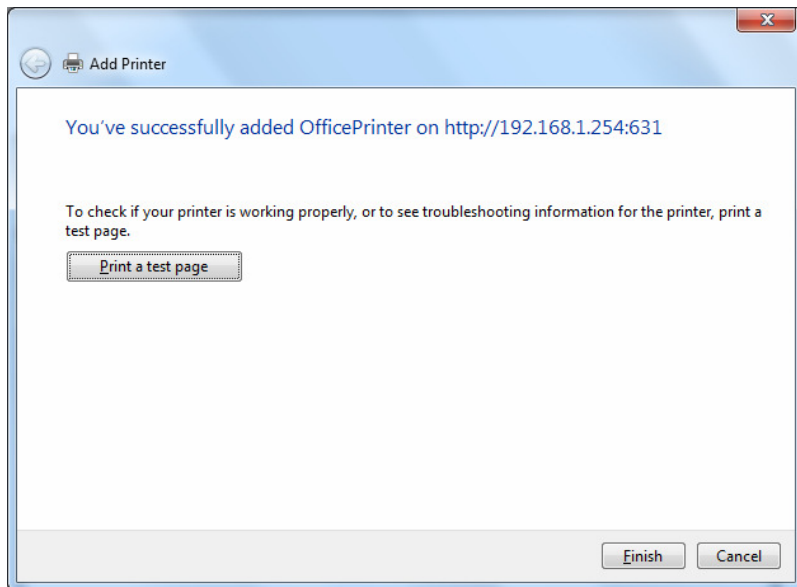
Step 6: Click “Next” to add the printer driver. If your printer is not listed and your printer came with an installation disk, click “Have Disk” find it and install the driver.



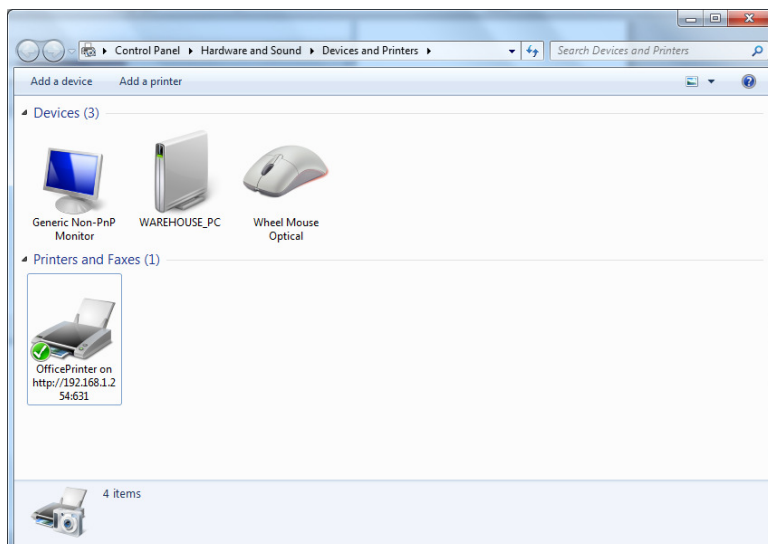
Step 7: Click “Next”



Step 8: Click “Next” and you are done



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



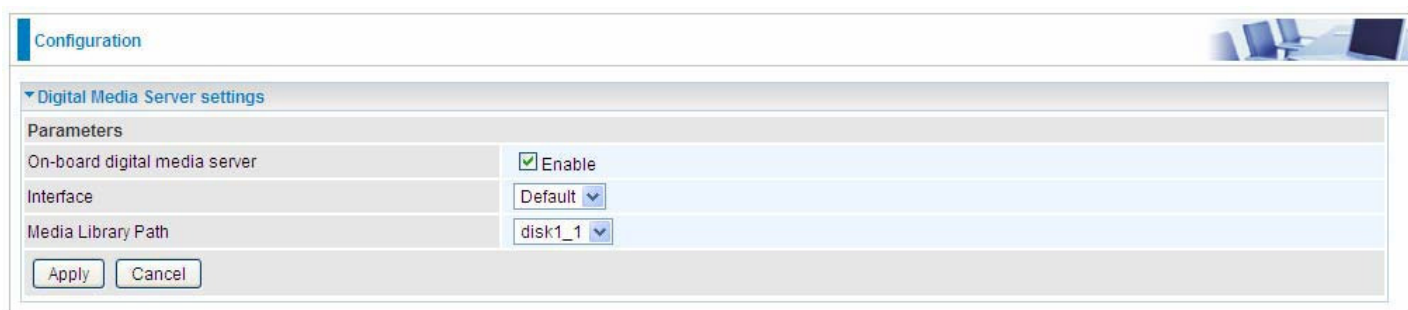
DLNA

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

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

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

With USB storage, 8920NXL-600 can serve as a DLNA server.



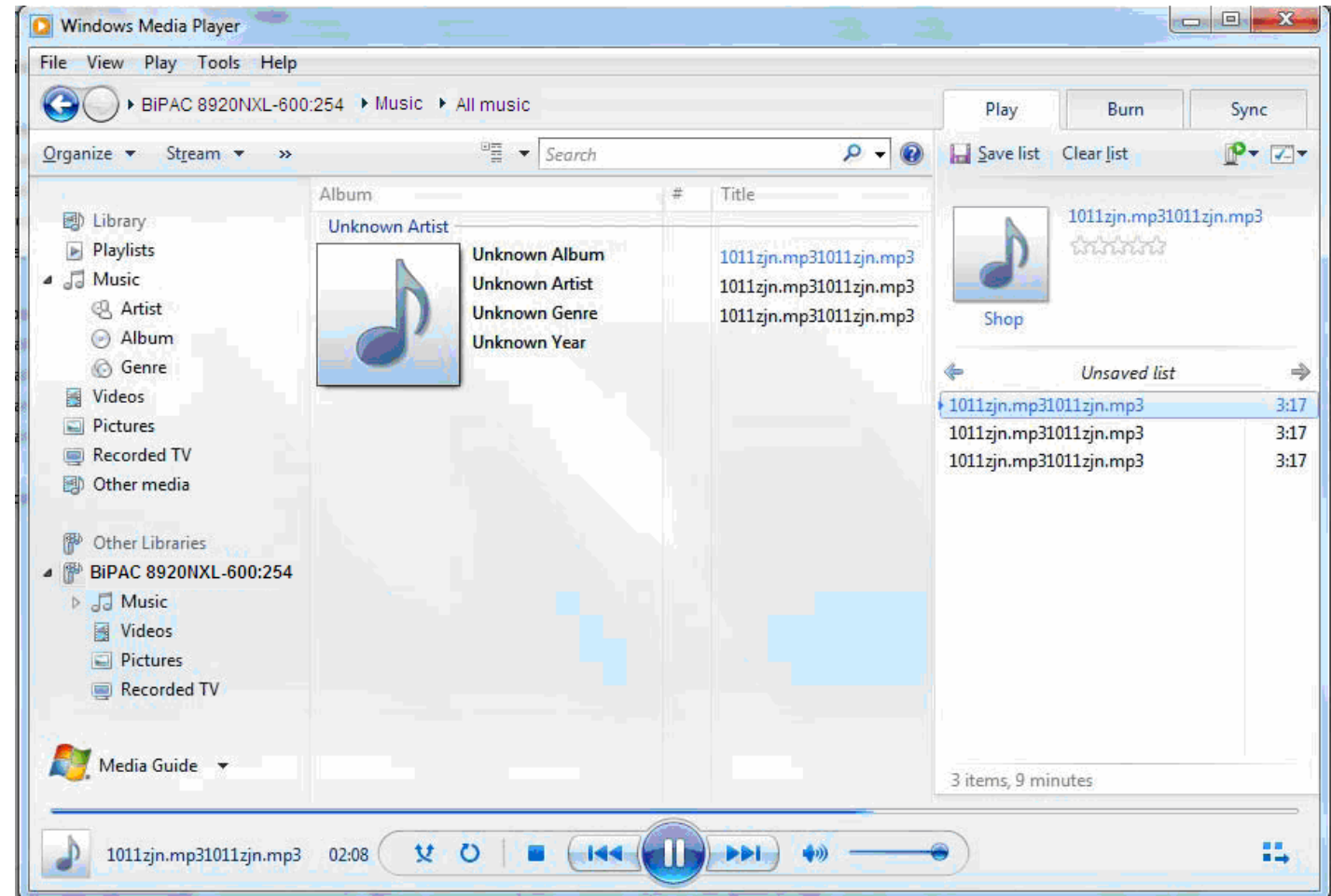
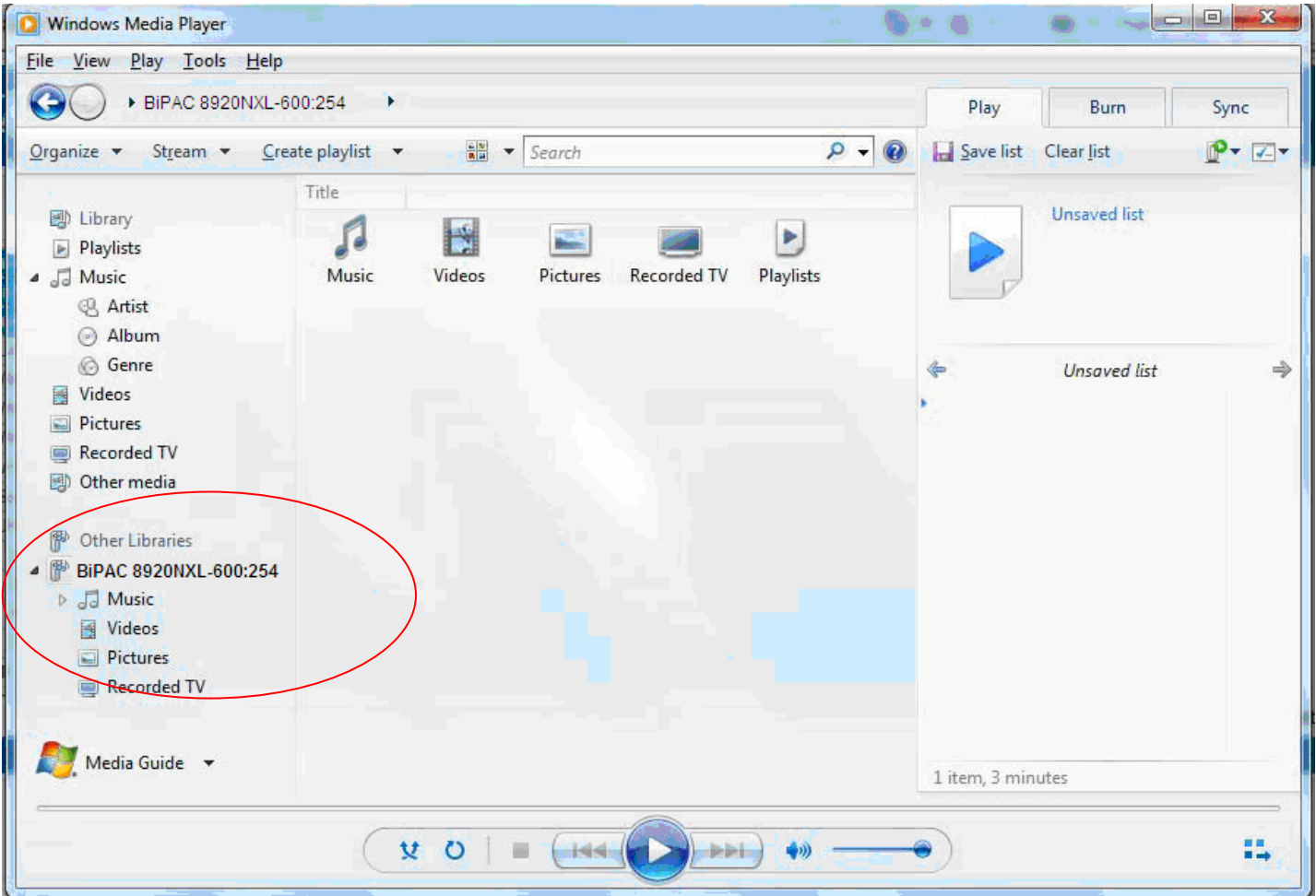
The screenshot shows a web-based configuration interface. At the top, there is a 'Configuration' tab. Below it, the 'Digital Media Server settings' section is expanded. Under the 'Parameters' heading, there are three settings: 'On-board digital media server' with a checked 'Enable' checkbox, 'Interface' with a dropdown menu set to 'Default', and 'Media Library Path' with a dropdown menu set to 'disk1_1'. At the bottom of this section are 'Apply' and 'Cancel' buttons.

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

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

Media Library Path: Default is disk1_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. The windows media player lists the resources (music, videos, etc) stored by the router's DLNA-based library under file "BiPAC 8920NXL-600, for example".



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

IPv4inIPv6

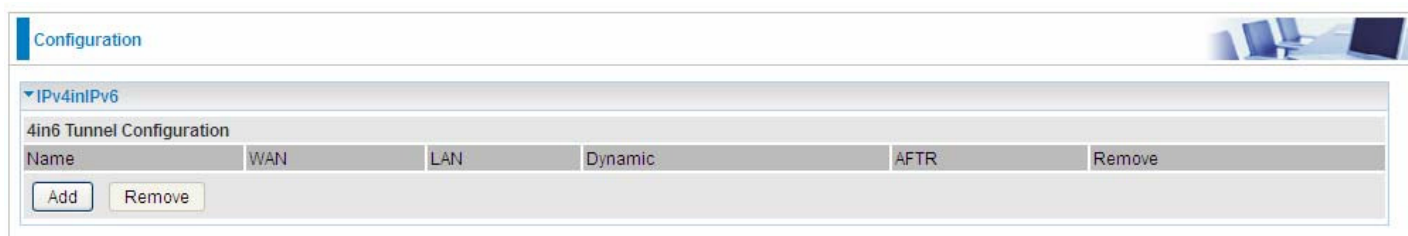
4in6 refers to tunneling of IPv4 in IPv6. It is an inherent internet interoperation mechanism allowing IPv4 to be used in an IPv6 only network.

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).

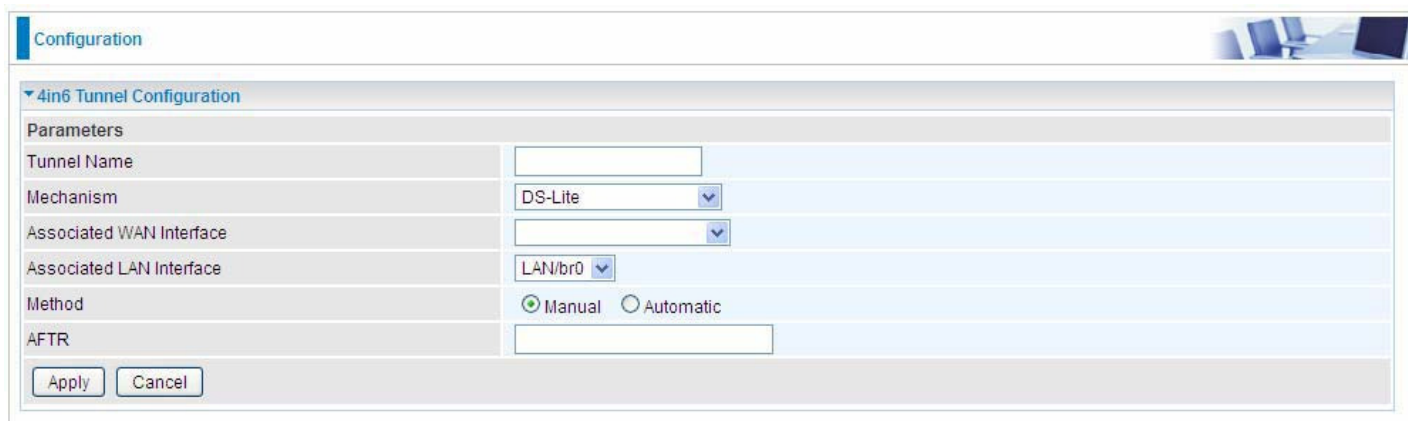
The CPE distributes private IPv4 addresses for the LAN clients, the same as a NAT device. The subnet information is chosen by the customer, identically to the NAT model. However, instead of performing the NAT itself, the CPE encapsulates the IPv4 packet inside an IPv6 packet.



The screenshot shows a web interface titled "Configuration" with a sub-section "IPv4inIPv6". Below this is a "4in6 Tunnel Configuration" table. The table has columns for Name, WAN, LAN, Dynamic, AFTR, and Remove. There is an "Add" button and a "Remove" button below the table.

Name	WAN	LAN	Dynamic	AFTR	Remove
------	-----	-----	---------	------	--------

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



The screenshot shows a web interface titled "Configuration" with a sub-section "4in6 Tunnel Configuration". Below this is a "Parameters" section with the following fields:

- Tunnel Name:
- Mechanism:
- Associated WAN Interface:
- Associated LAN Interface:
- Method: ☒ Manual ☐ Automatic
- AFTR:

At the bottom 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.

Note: The maximum number of entries: 32.

Configuration

IP Filtering

Outgoing IP Filtering Setup

A maximum entries can be configured: 32

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

Add

Remove

Reorder

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

Configuration

Outgoing IP Filtering Setup

Parameters

Filter Name

<< --type or select from listbox--

IP Version

IPv4

Protocol

TCP/UDP

Protocol Number

[0 - 254]

Source IP address

~

Source Port

[port or port:port]

Destination IP address

~

Destination Port

[port or port:port]

Time Schedule

Always On

Sun

Mon

Tue

Wed

Thu

Fri

Sat

From

00

:

00

To

00

:

00

Action

drop

Log

Apply

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

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

Protocol: Set the traffic type (TCP/UDP, TCP, UDP, ICMP, RAW, Any) 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.

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 blocked. Or exactly in the rule below, all traffic trying to access FTP will be forwarded.

Configuration

Outgoing IP Filtering Setup

Parameters

Filter Name

FTP

<< FTP(TCP 21)

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

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

Order	Filter Name	IP Version	Protocol	Source IP address	Source Port	Action	Log	Disable	Remove	Edit
	FTP	4	TCP	Any	Any	forward	Enable	☐	☐	Edit
				Any	21					

Add

Remove

Reorder

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

Add another Outgoing IP Filtering rule, users will find the “arrow” icon to change the IP outgoing filter rule working orders.

Configuration

IP Filtering

Outgoing IP Filtering Setup

A maximum entries can be configured: 32

Order	Filter Name	IP Version	Protocol	Source IP address	Source Port	Action	Log	Disable	Remove	Edit
↓	FTP	4	TCP	Any	Any	forward	Enable	☐	☐	Edit
↑	HTTP	4	TCP	Any	Any	forward	Enable	☐	☐	Edit
				Any	80					

Add

Remove

Reorder

How to disable set rule.

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

Order	Filter Name	IP Version	Protocol	Source IP address	Source Port	Action	Log	Disable	Remove	Edit
	FTP	4	TCP	Any	Any	forward	Enable	☒	☐	Edit
				Any	21					

Add

Remove

Reorder

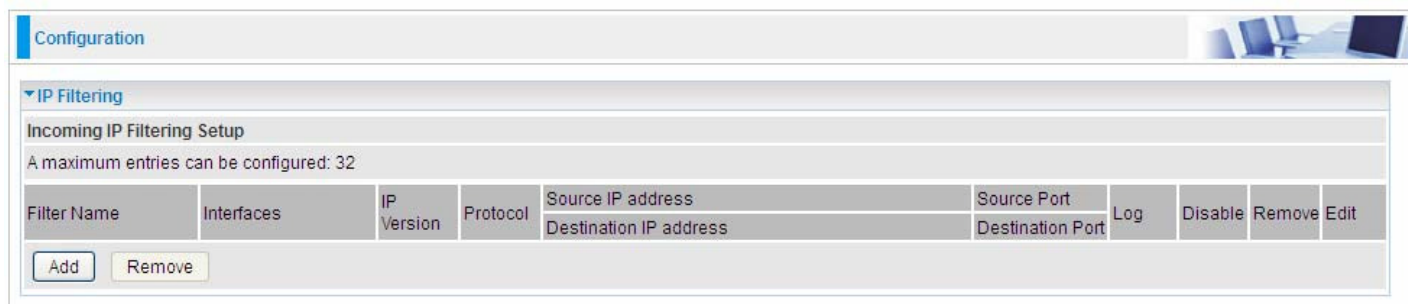
(Rule inactive)

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.

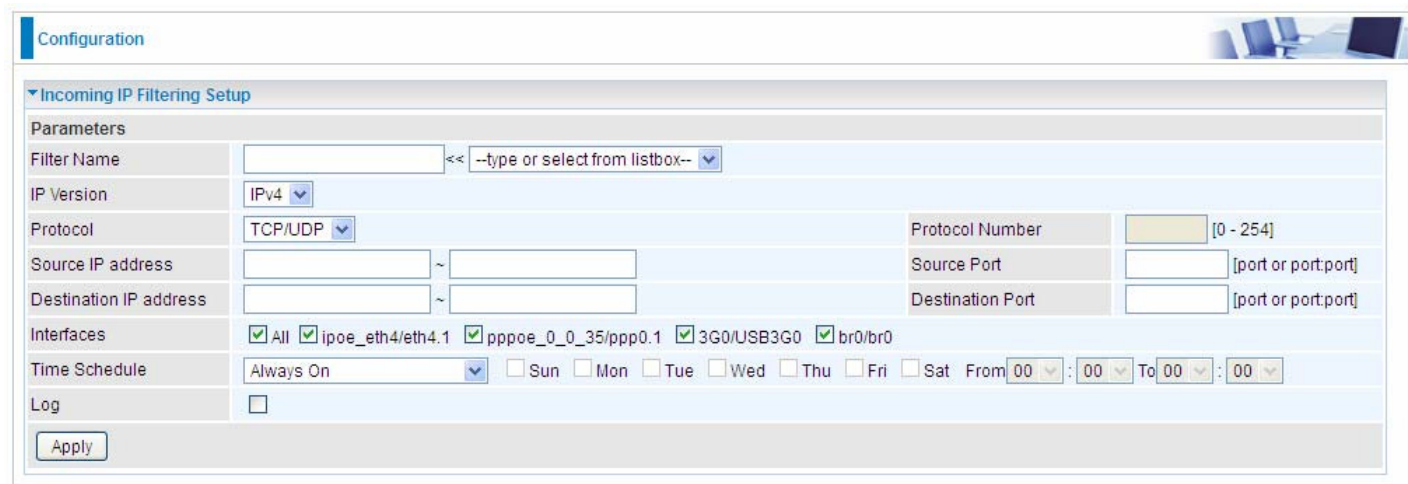
Note:

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. There are 'Add' and 'Remove' buttons below the table.

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, IP Version (IPv4), Protocol (TCP/UDP), Source IP address, Destination IP address, Source Port, Destination Port, Interfaces (All, ipoe_eth4/eth4.1, pppoe_0_0_35/ppp0.1, 3G0/USB3G0, br0/br0), Time Schedule (Always On), and Log. There are 'Apply' and 'Remove' buttons.

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, RAW, Any) 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](#).

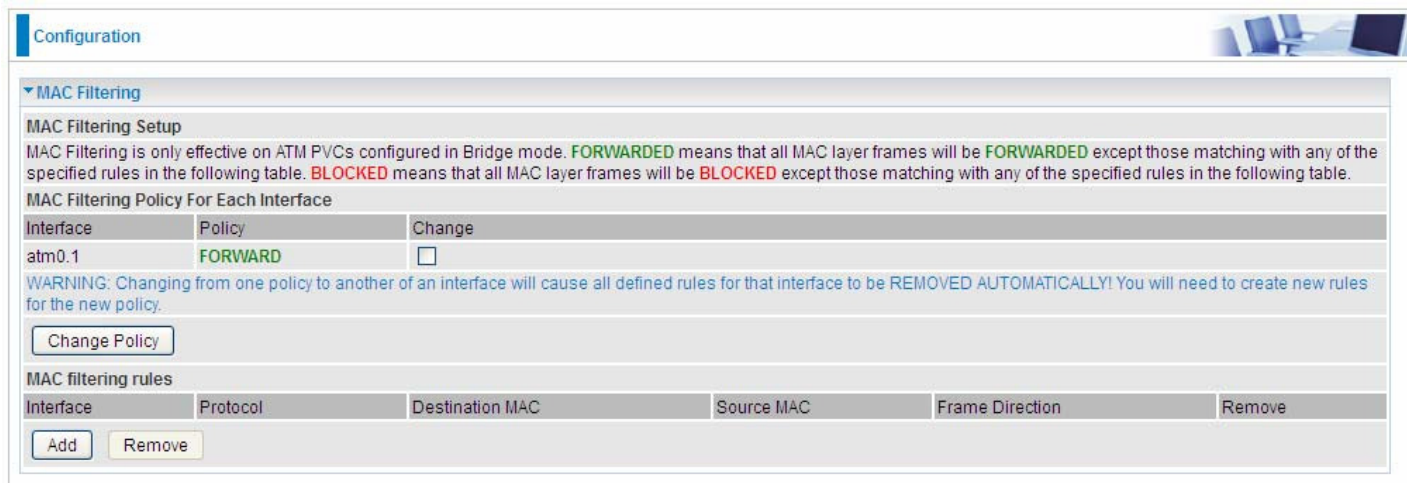
Log: check the check-box to record the security log. To check the log, users can turn to [Security Log](#).

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

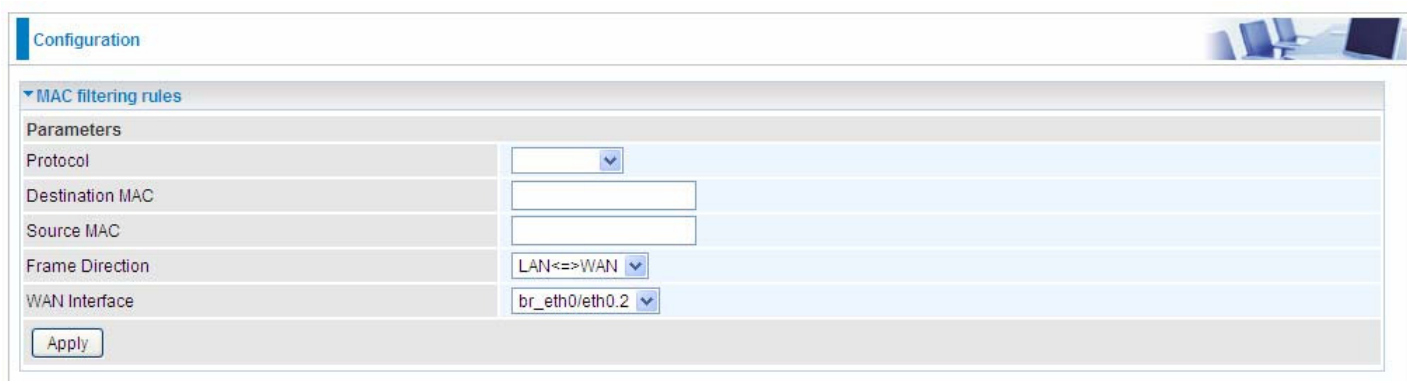
Interface	Protocol	Destination MAC	Source MAC	Frame Direction	Remove
-----------	----------	-----------------	------------	-----------------	--------

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

WAN Interface

Apply

Protocol: 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.

Block 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. Please click Add button to add the device(s) to be subject to Time Restriction rules (forward or drop connection to internet). Devices Not added will not comply with the rules and access internet and router willingly.

To find out the MAC address of a window based PC, go to command window, and type "ipconfig/all".

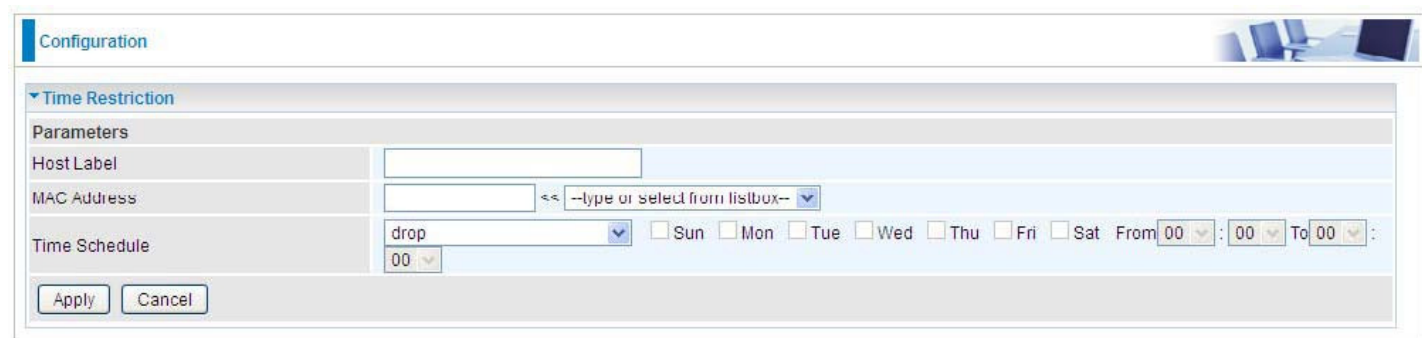
Note: The maximum entries configured: 32.



The screenshot shows the 'Configuration' page with the 'Time Restriction' section expanded. It displays a table of existing rules. The table has columns for Host Label, MAC Address, and days of the week (Sun, Mon, Tue, Wed, Thu, Fri, Sat). The Start Time and End Time columns are also present. There are 'Add' and 'Remove' buttons at the bottom left of the table.

Host Label	MAC Address	Sun	Mon	Tue	Wed	Thu	Fri	Sat	Start Time	End Time	Remove	Edit
A maximum entries can be configured: 32												

Click **Add** to add the rules.



The screenshot shows the 'Add' dialog box for the Time Restriction configuration. It has fields for Host Label, MAC Address, and Time Schedule. The Time Schedule section includes a dropdown for the action (drop, forward, or select from listbox) and checkboxes for the days of the week. There are also fields for the start and end times. The 'Apply' and 'Cancel' buttons are at the bottom.

Host Label: User-defined name.

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

Time Schedule: Configure to control the PC from accessing router and internet.

- 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.

Configuration

URL Filter

Parameters

Keywords Filtering ☐ Enable [Detail ▶](#)

Domains Filtering ☐ Enable [Detail ▶](#)

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

Except IP Address [Detail ▶](#)

Log ☐

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

Apply Cancel

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

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

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

Except 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

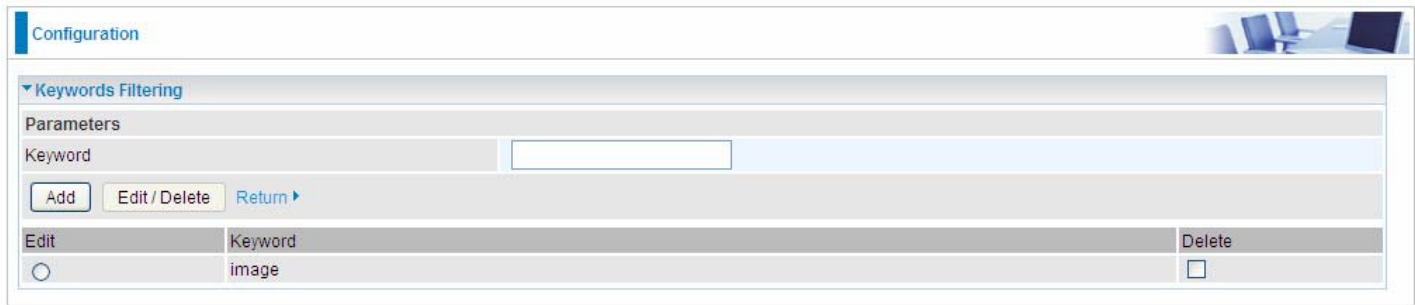
Note: Maximum number of entries: 32.

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



The screenshot shows the 'Configuration' window with the 'Keywords Filtering' section expanded. Under 'Parameters', there is a 'Keyword' text field and three buttons: 'Add', 'Edit / Delete', and 'Return ▶'.

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



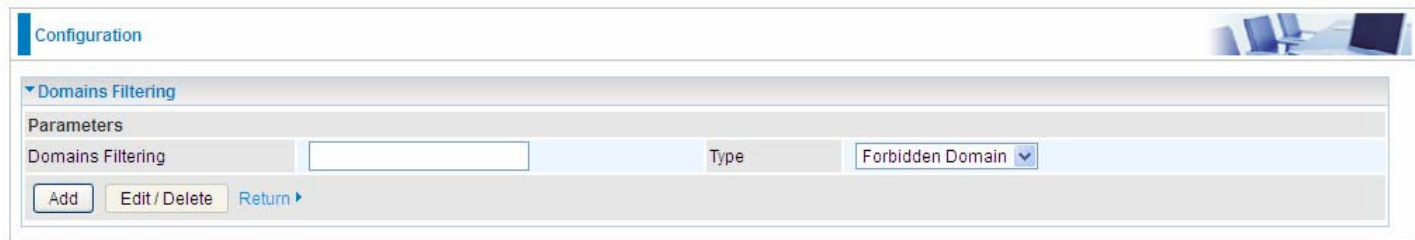
The screenshot shows the 'Keywords Filtering' section with a list of keywords. The list has three columns: 'Edit', 'Keyword', and 'Delete'. The first row shows a radio button in the 'Edit' column, the word 'image' in the 'Keyword' column, and a checkbox in the 'Delete' column.

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.

Domains Filtering

Note: Maximum number of entries: 32.

Click [Detail ▶](#) to add Domains.



The screenshot shows the 'Configuration' window with the 'Domains Filtering' section expanded. Under 'Parameters', there is a 'Domains Filtering' text field, a 'Type' dropdown menu set to 'Forbidden Domain', and three buttons: 'Add', 'Edit / Delete', and '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.

Except IP Address

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

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



Configuration

▼ Except IP Address

Parameters

IP Version: IPv4 ▼

Internal IP Address: [] ~ []

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

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

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

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

Parental Control Provider

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

Configuration

▼ Parental Control Provider

Parameters

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

Provider	www.opendns.com
Host Name	
Username	
Password	

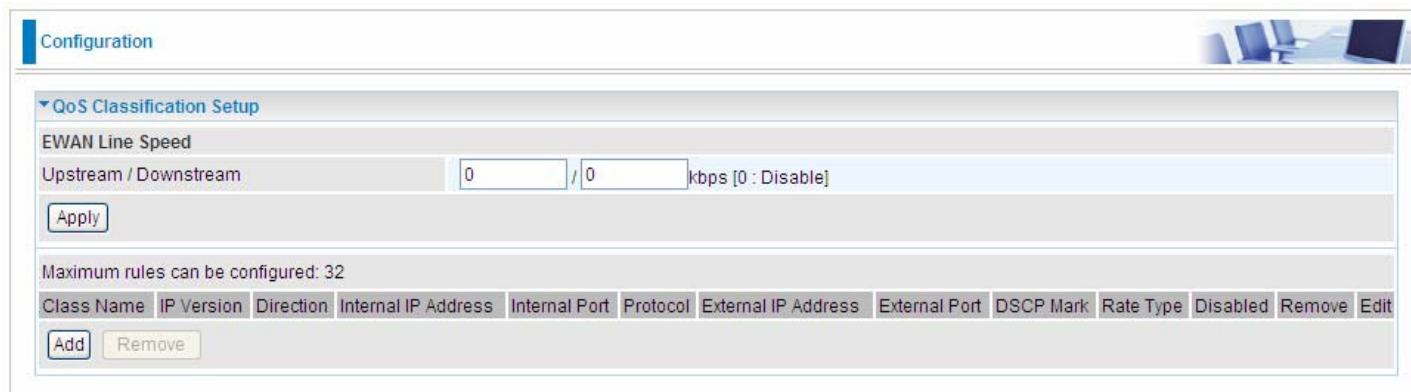
Host Name, Username and Password: Enter your registered domain name and your username and password at the provider website www.opendns.com.

QoS - Quality of Service

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: VDSL/ADSL line speed is based on the VDSL/ADSL sync rate. But there is no QoS on 3G/4G LTE as the 3G/4G LTE line speed is various and can not be known exactly.

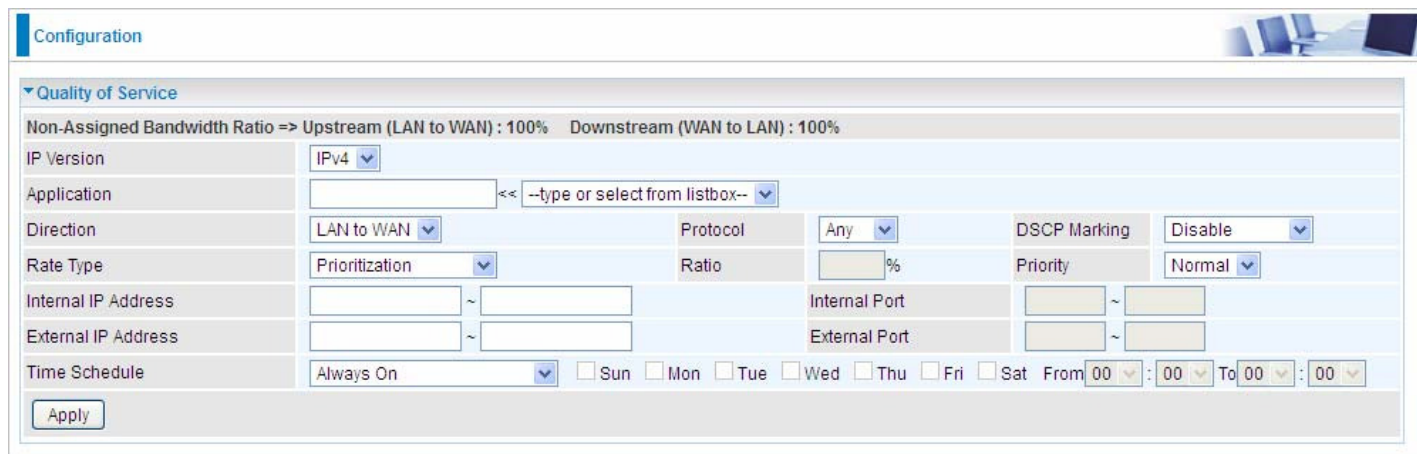


The screenshot shows the 'Configuration' page with the 'QoS Classification Setup' section expanded. It includes a 'QoS Classification Setup' header, a 'EWAN Line Speed' section with 'Upstream / Downstream' rate inputs (0 / 0 kbps) and an 'Apply' button. Below this, it states 'Maximum rules can be configured: 32' and shows 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 at the bottom of 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 includes a 'Quality of Service' header, a 'Non-Assigned Bandwidth Ratio' section showing 'Upstream (LAN to WAN) : 100%' and 'Downstream (WAN to LAN) : 100%'. Below this, there are various configuration fields: 'IP Version' (IPv4), 'Application' (a text box and a dropdown), 'Direction' (LAN to WAN), 'Protocol' (Any), 'DSCP Marking' (Disable), 'Rate Type' (Prioritization), 'Ratio' (a text box and a percentage dropdown), 'Priority' (Normal), 'Internal IP Address' (a text box and a range dropdown), 'Internal Port' (a text box and a range dropdown), 'External IP Address' (a text box and a range dropdown), 'External Port' (a text box and a range dropdown), and 'Time Schedule' (Always On, with checkboxes for days of the week and a time range dropdown). There is an 'Apply' button 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 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.

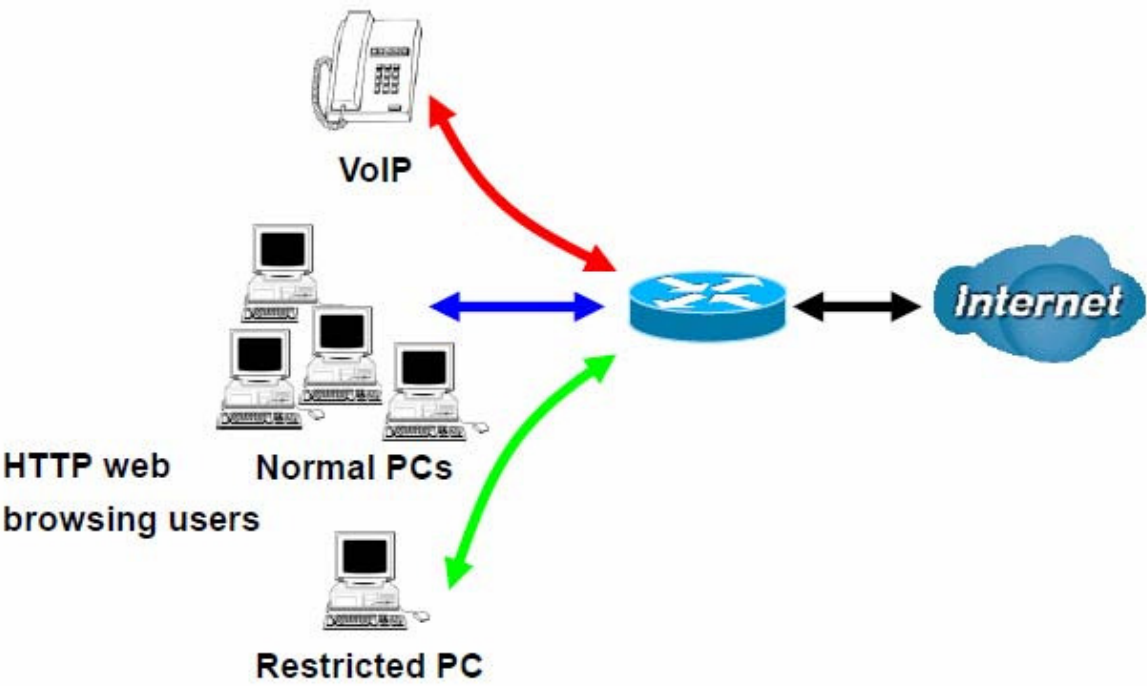
External IP Address: The IP address on remote / WAN side.

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.

Configuration

Quality of Service

Non-Assigned Bandwidth Ratio => Upstream (LAN to WAN) : 80% Downstream (WAN to LAN) : 100%

IP Version	IPv4		
Application	P2P << --type or select from listbox--		
Direction	LAN to WAN	Protocol	Any
Rate Type	Prioritization	Ratio	%
Internal IP Address		Internal Port	
External IP Address		External Port	
Time Schedule	timeslot1 ☐ Sun ☒ Mon ☒ Tue ☒ Wed ☒ Thu ☒ Fri ☐ Sat From 00 : 00 To 09 : 19		
Apply			

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.

Configuration

QoS Port Shaping

Parameters

QoS port shaping supports traffic shaping of Ethernet interface. If “Shaping Rate” is set to “-1”, it means no shaping and “Burst Size” will be ignored.

Interface	Type	QoS Shaping Rate (kbps)	Burst Size (Byte)
P5/EWAN	WAN	-1	0
P1	LAN	-1	0
P2	LAN	-1	0
P3	LAN	-1	0
P4	LAN	-1	0

Apply

Cancel

Interface: P1-P5. P5 used as EWAN also covered.

Type: All LAN when P5 is LAN port; P5 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

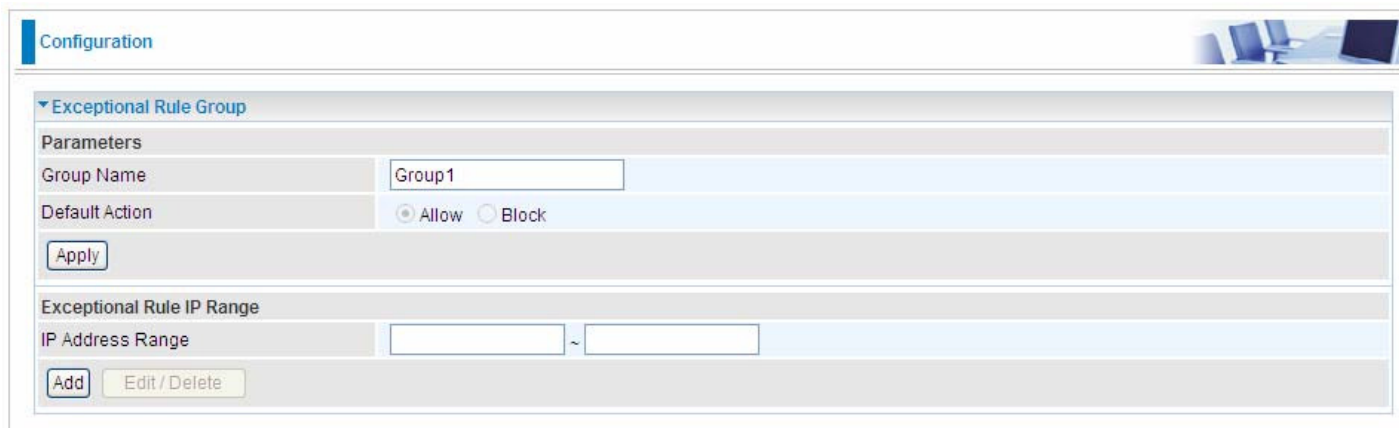
Exceptional Rule is dedicated to giving or blocking NAT/DMZ access to some specific IP or IPs(range). Users are allowed to set 8 different exceptional rule groups at most. In each group, user can add specific IP or IP range.



The screenshot shows the 'Configuration' page for 'Exceptional Rule Group'. It contains a table with 8 groups. Each group has a 'Group Index', 'Group Name', 'Default Action', 'Exceptional Rule IP Range', and an 'Edit' button.

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 for 'Exceptional Rule Group' with the 'Edit' form for Group1. The form includes fields for 'Group Name' (Group1), 'Default Action' (radio buttons for Allow and Block), 'Exceptional Rule IP Range' (IP Address Range), and buttons for 'Apply', 'Add', and 'Edit / Delete'.

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. Select “Allow” to grant access to the listed IP or IPs to Virtual Server and DMZ Host.

While choose “Block” to ban the listed IP or IPs to access the 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 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:

Default Action: ☐ Allow ☒ Block

Exceptional Rule IP Range

IP Address Range: ~

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

Virtual Servers

In TCP/IP and UDP networks a port is a 16-bit number used to identify which application program (usually a server) incoming connections should be delivered to. Some ports have numbers that are pre-assigned to them by the IANA (the Internet Assigned Numbers Authority), and these are referred to as “well-known ports”. Servers follow the well-known port assignments so clients can locate them.

If you wish to run a server on your network that can be accessed from the WAN (i.e. from other machines on the Internet that are outside your local network), or any application that can accept incoming connections (e.g. Peer-to-peer/P2P software such as instant messaging applications and P2P file-sharing applications) and are using NAT (Network Address Translation), then you will usually need to configure your router to forward these incoming connection attempts using specific ports to the PC on your network running the application. You will also need to use port forwarding if you want to host an online game server.

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

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

This part is only available when NAT is enabled.

Note: The maximum number of entries: 64.

Configuration

▼ **Virtual Servers**

Virtual Servers Setup

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

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

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				

Apply

Cancel

WAN IP: To specify the exact WAN IP address. It can be flexible while there are multiple WAN IPs on one interface. If the WAN IP field is empty, 8920NXL-600 uses the current WAN IP of this interface.

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.

External Port

- ## Internal Port

- Protocol:** select the protocol this service used: TCP/UDP, TCP, UDP, ICMP, etc.

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

Exceptional Rule Group

None

External Port

Start

End

Protocol

TCP

Protocol Number

Internal Port

Start

End

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

<< --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

Apply

Cancel

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 rule 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.

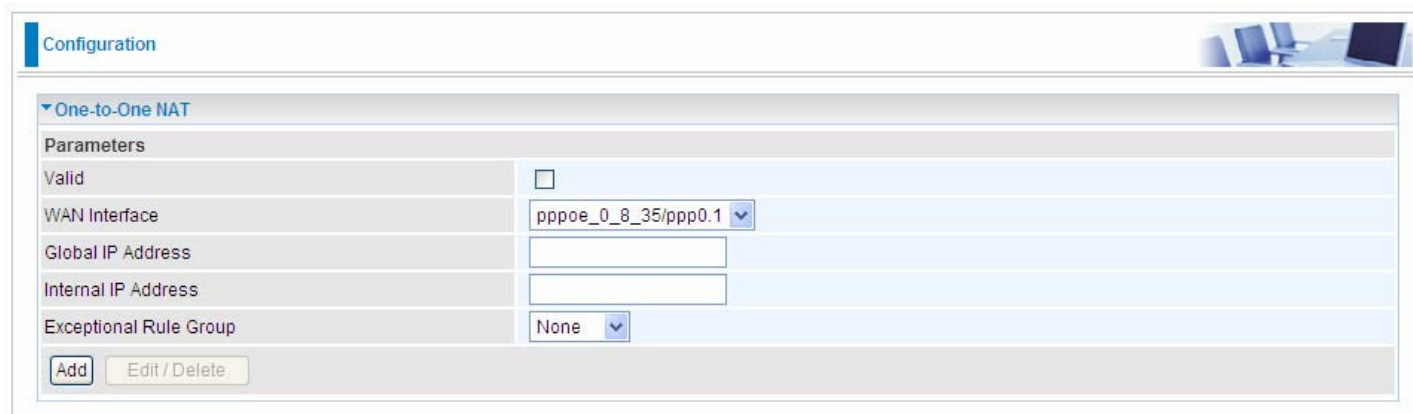


Attention

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". At the top, there is a "Configuration" tab and a small graphic of a computer. Below the tab, the "One-to-One NAT" section is expanded, showing a "Parameters" table. The table has five rows: "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 table, there are two buttons: "Add" and "Edit / Delete".

Parameters	
Valid	☐
WAN Interface	pppoe_0_8_35/ppp0.1
Global IP Address	
Internal IP Address	
Exceptional Rule Group	None

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

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

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

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

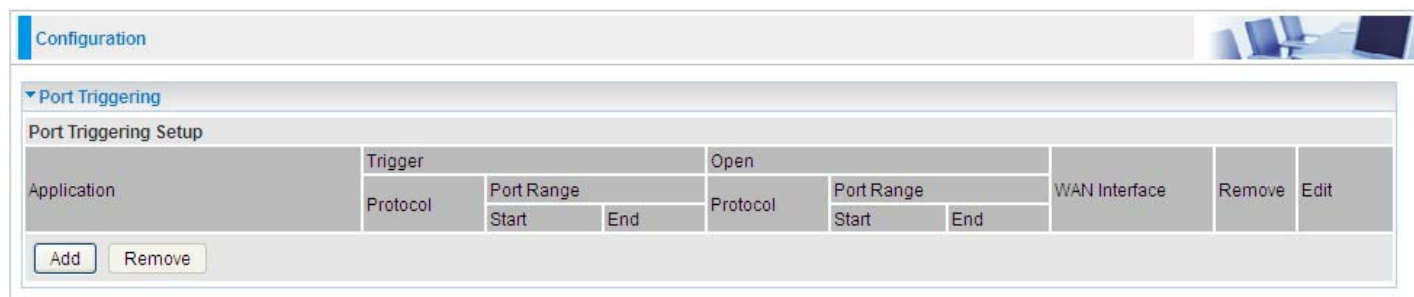
Exceptional Rule Group: Select the exceptional group listed. It is to give or block access to a group of IPs to the server after One-to-One NAT. For example, a server with 192.168.1.3 is mapped to 123.1.1.2 by One-to-One NAT, then the exceptional group can be designated to have or have not access to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

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.

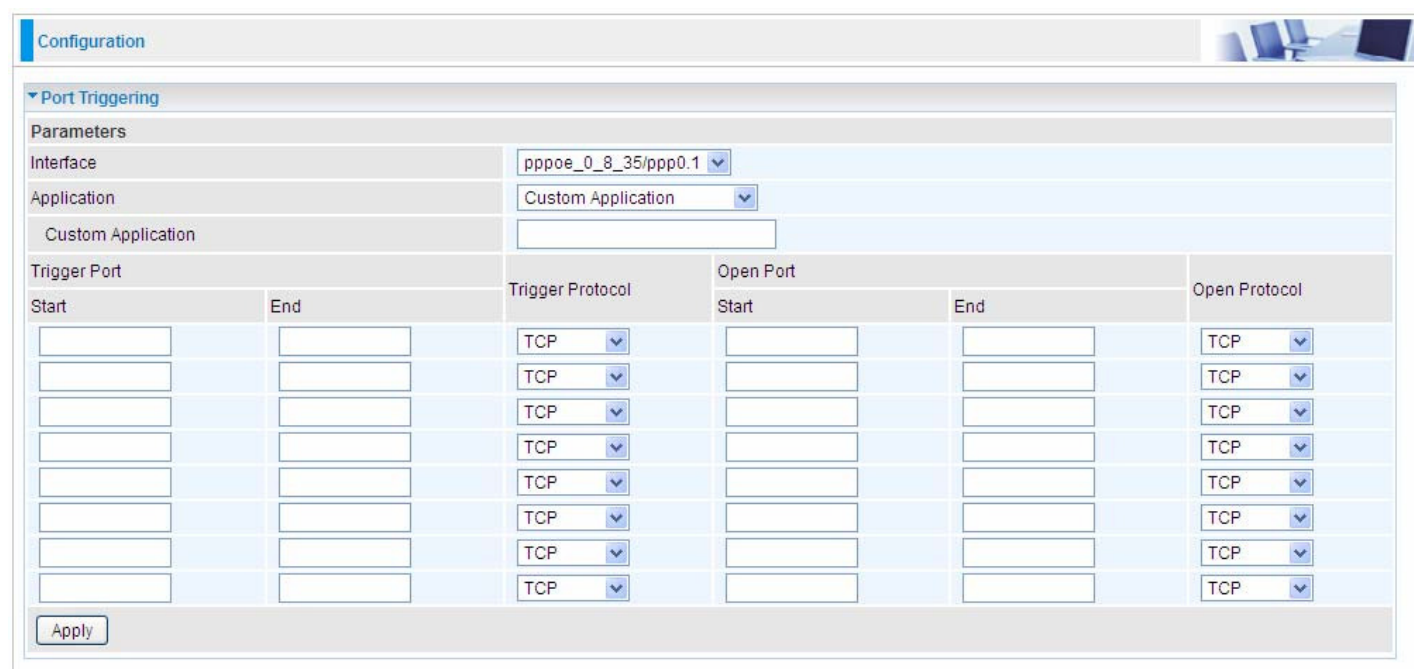


The screenshot shows the 'Port Triggering Setup' section of a configuration interface. It features a table with columns for 'Application', 'Trigger' (Protocol, Port Range), 'Open' (Protocol, Port Range), 'WAN Interface', 'Remove', and 'Edit'. Below the table are 'Add' and 'Remove' buttons.

Application	Trigger		Open			WAN Interface	Remove	Edit
	Protocol	Port Range (Start, End)	Protocol	Port Range (Start, End)				

Buttons: Add, Remove

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



The screenshot shows the 'Port Triggering Parameters' section. It includes dropdown menus for 'Interface' (pppoe_0_8_35/ppp0.1) and 'Application' (Custom Application). Below is a text field for 'Custom Application'. The main part is a table for defining trigger and open ports, with columns for Start, End, and Protocol. An 'Apply' button is at the bottom.

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

Buttons: 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.

Port Triggering						
Parameters						
Interface		pppoe_0_8_35/ppp0.1				
Application		Aim Talk				
Custom Application						
Trigger Port			Open Port			
Start	End	Trigger Protocol	Start	End	Open Protocol	
4099	4099	TCP	5191	5191	TCP	
		TCP			TCP	
		TCP			TCP	
		TCP			TCP	
		TCP			TCP	
		TCP			TCP	
		TCP			TCP	
		TCP			TCP	

Apply

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

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

Add Remove

 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**.

Configuration

Port Triggering

Port Triggering Setup

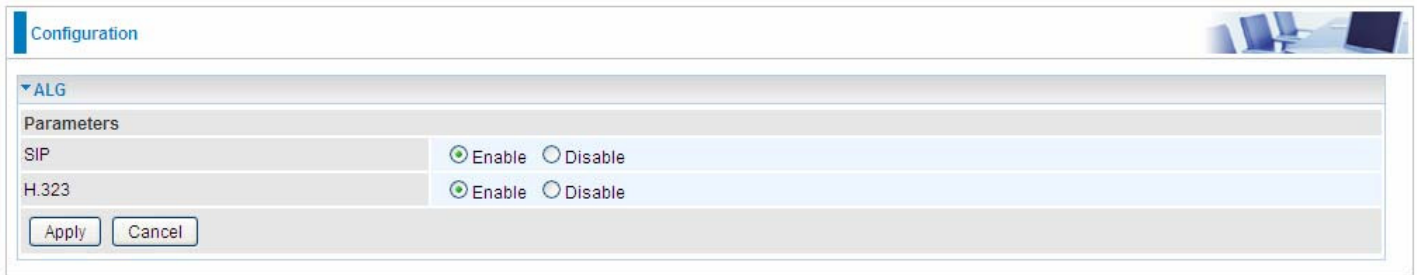
Application	Trigger			Open			WAN Interface	Remove	Edit			
	Protocol	Port Range		Protocol	Port Range							
		Start	End		Start	End						
Aim Talk	TCP	4099	4099	TCP	5191	5191	ppp0.1	☐	Edit			

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 two rows: 'SIP' and 'H.323'. Each row has two radio buttons: 'Enable' (selected) and 'Disable'. At the bottom of the window, there are 'Apply' and 'Cancel' buttons.

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

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.

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.

MAC Address: 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	Sun	Mon	Tue	Wed	Thu	Fri	Sat	Time	Delete
☐	11		x	x	x	x	x		09:00	☐

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.

Configuration

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(BiPAC 8920NX-600 only)

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.

▶ Status
• Quick Start
▶ Configuration
▼ VPN
• IPsec
• VPN Account
• Exceptional Rule Group
▶ PPTP
▶ L2TP
• GRE
▶ Advanced Setup

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 page with the 'IPSec' tab selected. The 'IPSec Settings' section includes a checkbox for 'L2TP over IPsec' (unchecked). Below this are fields for 'Connection Name', 'WAN Interface' (set to 'Default'), 'IP Version' (set to 'IPv4'), 'Local Network' (set to 'Single Address'), 'IP Address', 'Netmask', 'Remote Security Gateway', 'Anonymous' checkbox (unchecked), 'Remote Network' (set to 'Single Address'), 'IP Address', 'Netmask', 'Key Exchange Method' (set to 'IKE'), 'IPsec Protocol' (set to 'ESP'), 'Pre-Shared Key', 'Local ID Type' (set to 'Default'), 'ID Content', 'Remote ID Type' (set to 'Default'), and 'ID Content'. The 'Phase 1' section includes 'Mode' (set to 'Main'), 'Encryption Algorithm' (set to '3DES'), 'Integrity Algorithm' (set to 'MD5'), 'DH Group' (set to 'MODP1024(DH2)'), 'SA Lifetime' (set to '480 Minute(s) [60-1440]'), 'Phase 2' (set to 'Main'), 'Encryption Algorithm' (set to '3DES'), 'Integrity Algorithm' (set to 'MD5'), 'DH Group' (set to 'None'), 'IPsec Lifetime' (set to '60 Minute(s) [60-1440]'), 'Keep Alive' (set to 'None'), and 'MTU' (set to '0 (0 : Default)'). An 'Apply' button is at the bottom.

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 Security 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.

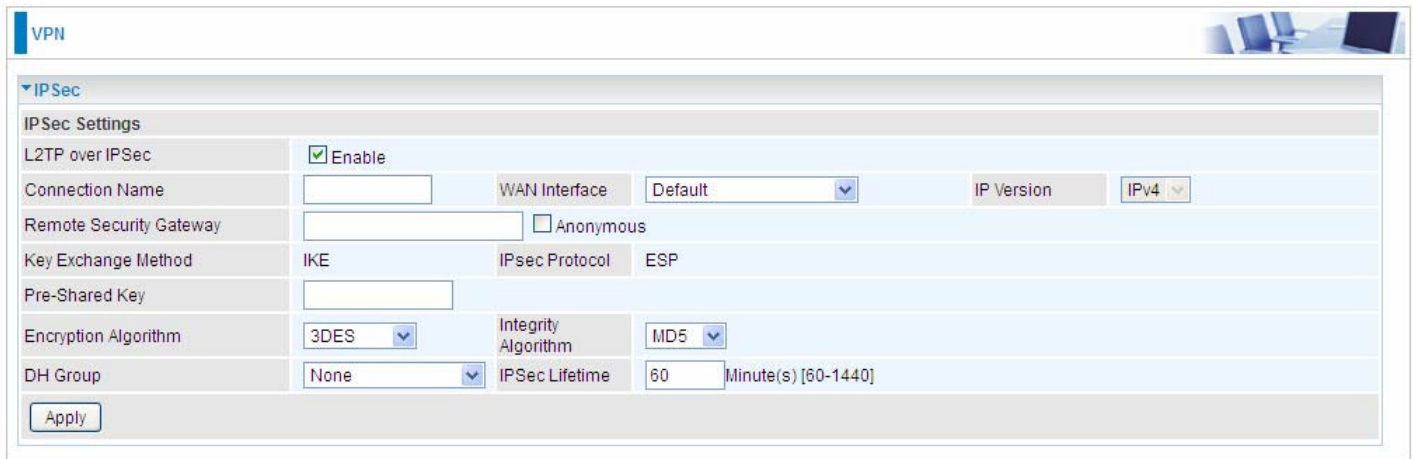
Ping IP (0.0.0.0 : NEVER)	0.0.0.0	Interval	10	Second(s) [0-3600, 0 : NEVER]
---------------------------	---------	----------	----	-------------------------------

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. At the top, there is a 'VPN' tab. Below it, the 'IPSec' section is expanded, showing 'IPSec Settings'. The settings are as follows:

Setting	Value
L2TP over IPSec	☒ Enable
Connection Name	[Empty text box]
WAN Interface	Default
IP Version	IPv4
Remote Security Gateway	[Empty text box] ☐ Anonymous
Key Exchange Method	IKE
IPsec Protocol	ESP
Pre-Shared Key	[Empty text box]
Encryption Algorithm	3DES
Integrity Algorithm	MD5
DH Group	None
IPsec Lifetime	60 Minute(s) [60-1440]

At the bottom of the settings section is an 'Apply' button.

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 **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.

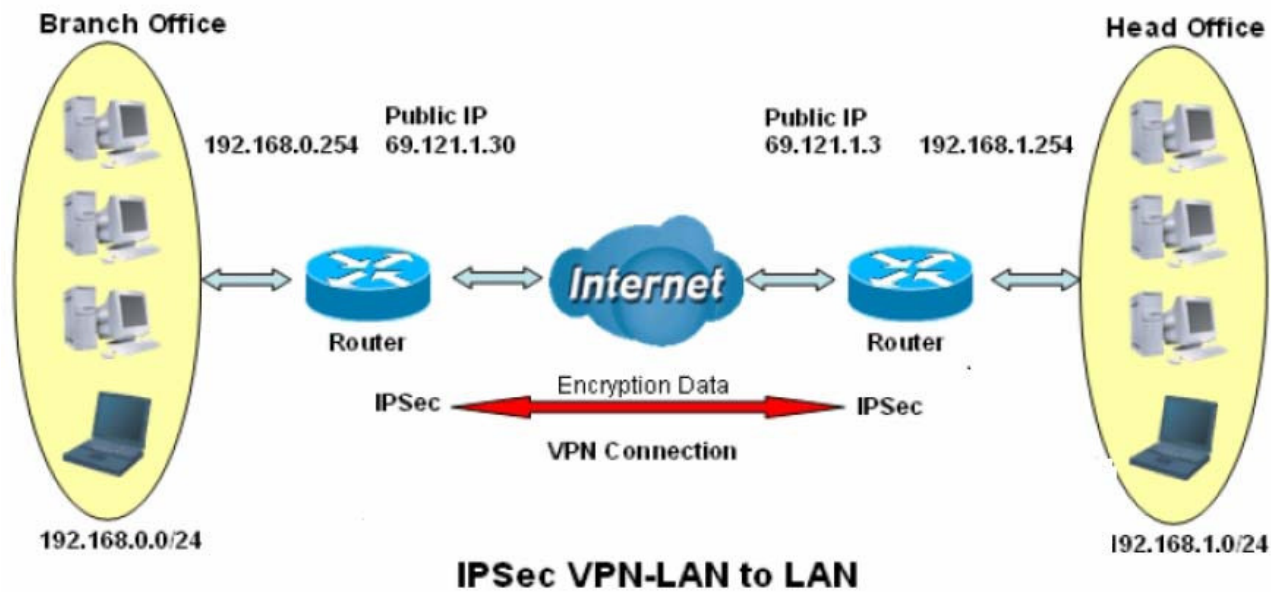
IPsec Lifetime: Specify the number of minutes that IPsec will stay active before new encryption and authentication key will be exchanged. Enter a value to negotiate and establish secure authentication. Default is 60 minutes (3600 seconds). A short time increases security by forcing the two parties to 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 89200NX-600s 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

☐

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

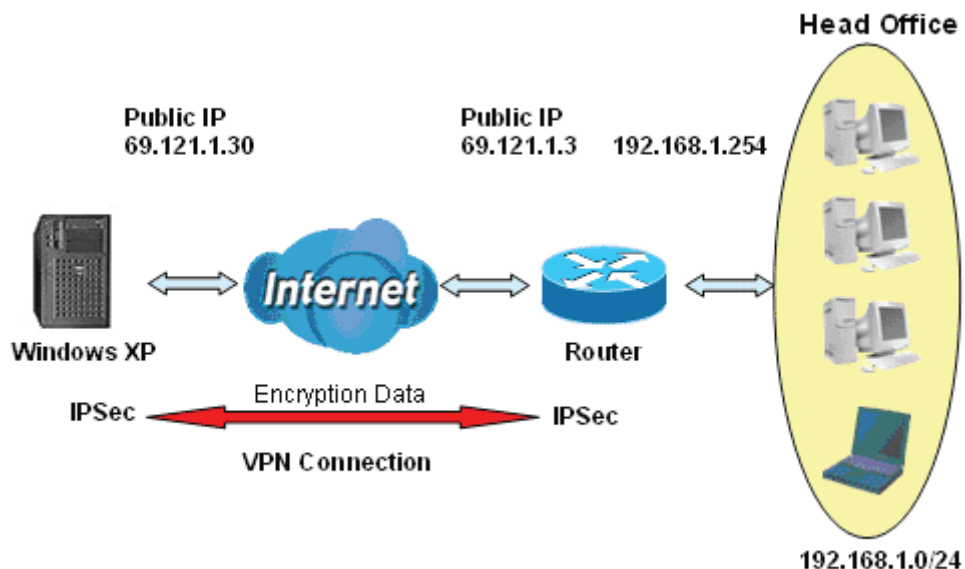
1500

(0 : Default)

Apply

1. 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	IP Version	IPv4
Local Network	Subnet	IP Address	192.168.1.0	Netmask	255.255.255.0
Remote Security Gateway	69.121.1.30	☐ Anonymous			
Remote Network	Single Address	IP Address	69.121.1.30	Netmask	255.255.255.0
Key Exchange Method	IKE	IPsec Protocol	ESP		
Pre-Shared Key	123456				
Local ID Type	Default	ID Content			
Remote ID Type	Default	ID Content			

Phase 1

Mode	Main
Encryption Algorithm	3DES
Integrity Algorithm	MD5
DH Group	MODP1024(DH2)
SA Lifetime	480 Minute(s) [60-1440]

Phase 2

Encryption Algorithm	3DES
Integrity Algorithm	MD5
DH Group	None
IPsec Lifetime	60 Minute(s) [60-1440]
Keep Alive	DPD
Detection Interval	180 Second(s) [180-86400]
Idle Timeout	5 Consecutive times [5-99]
MTU	1500 (0 : Default)

VPN Account

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



VPN

VPN Account

VPN Account: applied to PPTP Server and L2TP Server.

Parameters

Name		Tunnel	☒ Enable ☐ Disable
Username		Password	
Connection Type	☒ Remote Access ☐ LAN to LAN		
Peer Network IP		Peer Netmask	

Name: A user-defined name for the connection.

Tunnel: Select **Enable** to activate the account. PPTP(L2TP) server is waiting for the client to connect to this account.

Username: Please input the username for this account.

Password: Please input the password for this account.

Connection Type: Select Remote Access for single user, Select LAN to LAN for remote gateway.

Peer Network IP: Please input the subnet IP for remote network.

Peer Netmask: Please input the Netmask for remote network.

Exceptional Rule Group

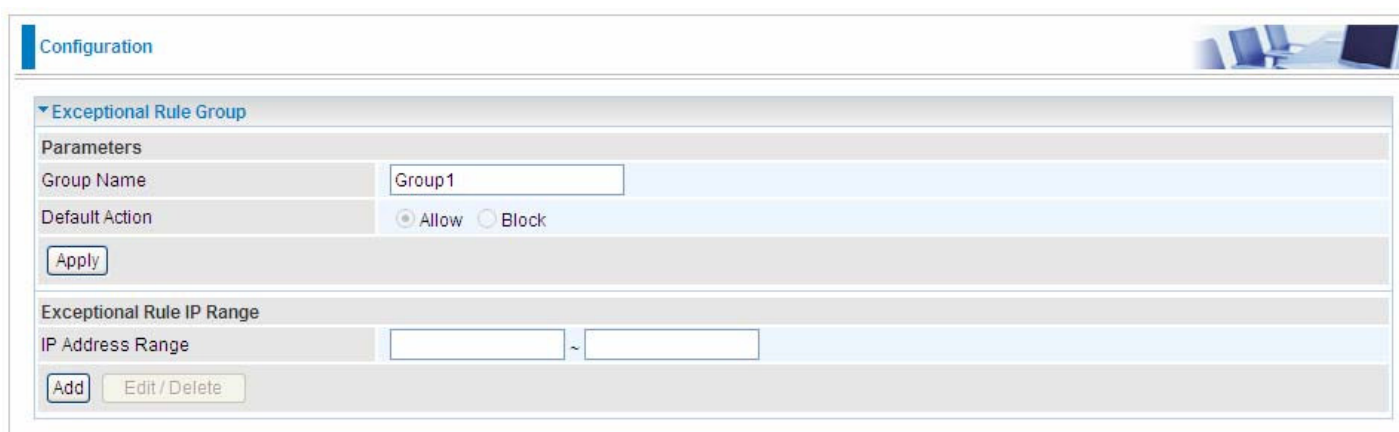
Exceptional Rule is dedicated to giving or blocking PPTP/L2TP server access to some specific IP or IPs(range). Users are allowed to set 8 different exceptional rule groups at most. In each group, user can add specific IP or IP range.



The 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 Actions are set to 'Allow'. Each row has an 'Edit' button in the last 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 'Add' and 'Edit / Delete' buttons.

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	☐

189

PPTP

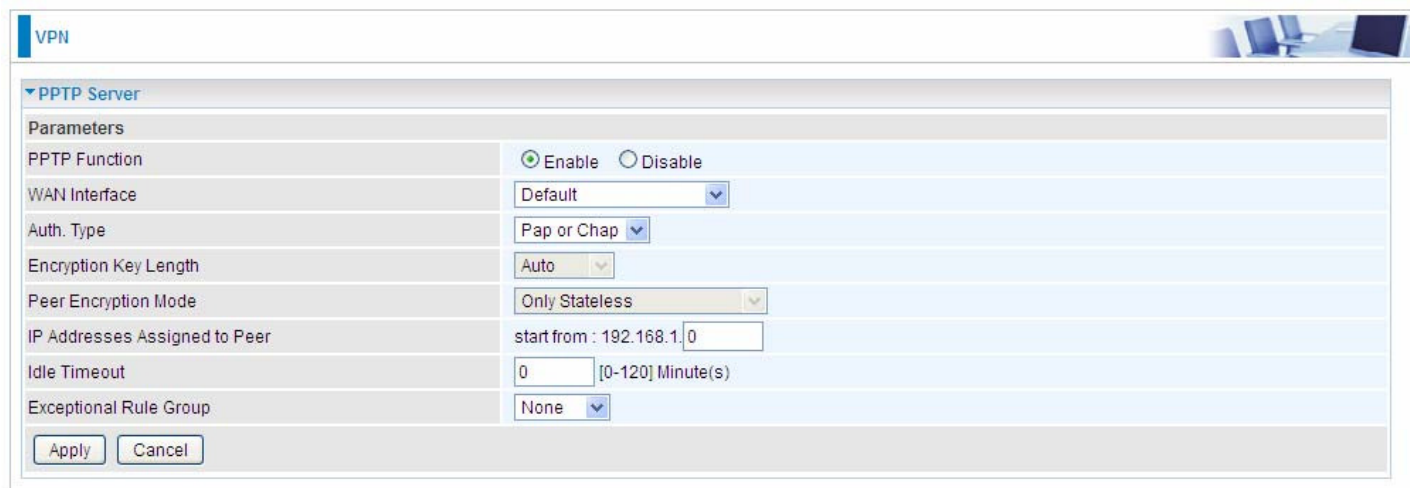
The **Point-to-Point Tunneling Protocol** (PPTP) is a Layer2 tunneling protocol for implementing virtual private networks through IP network. PPTP uses an enhanced GRE (Generic Routing Encapsulation) mechanism to provide a flow- and congestion-controlled encapsulated datagram service for carrying PPP 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 'VPN' management interface with the 'PPTP Server' configuration window open. The window has a 'Parameters' section with the following settings:

Parameter	Value
PPTP Function	☒ Enable ☐ Disable
WAN Interface	Default
Auth. Type	Pap or Chap
Encryption Key Length	Auto
Peer Encryption Mode	Only Stateless
IP Addresses Assigned to Peer	start from : 192.168.1.0
Idle Timeout	0 [0-120] Minute(s)
Exceptional Rule Group	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

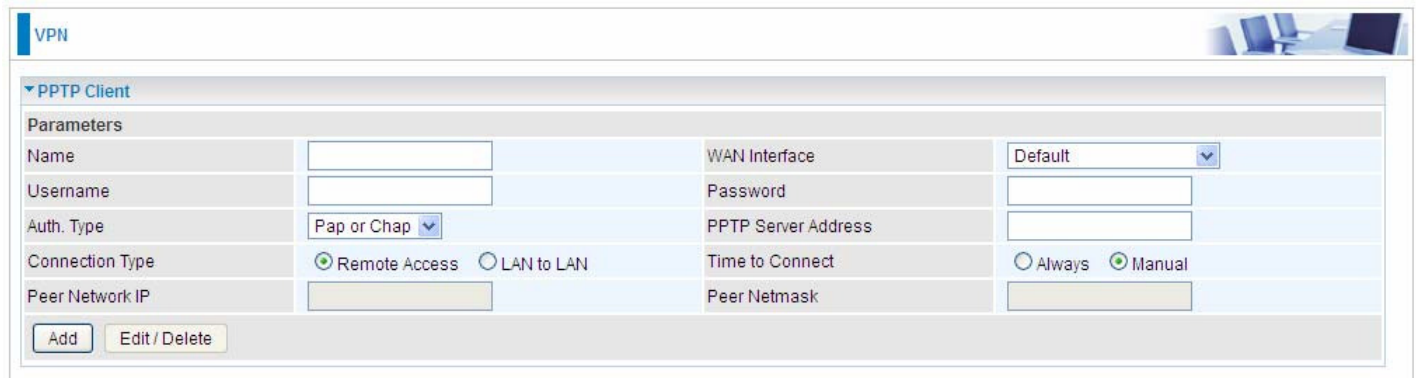
minutes.

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. The 'Parameters' section contains the following fields:

Parameters	
Name	
Username	
Auth. Type	Pap or Chap
Connection Type	☒ Remote Access ☐ LAN to LAN
Peer Network IP	
WAN Interface	Default
Password	
PPTP Server Address	
Time to Connect	☐ Always ☒ Manual
Peer Netmask	

At the bottom 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.

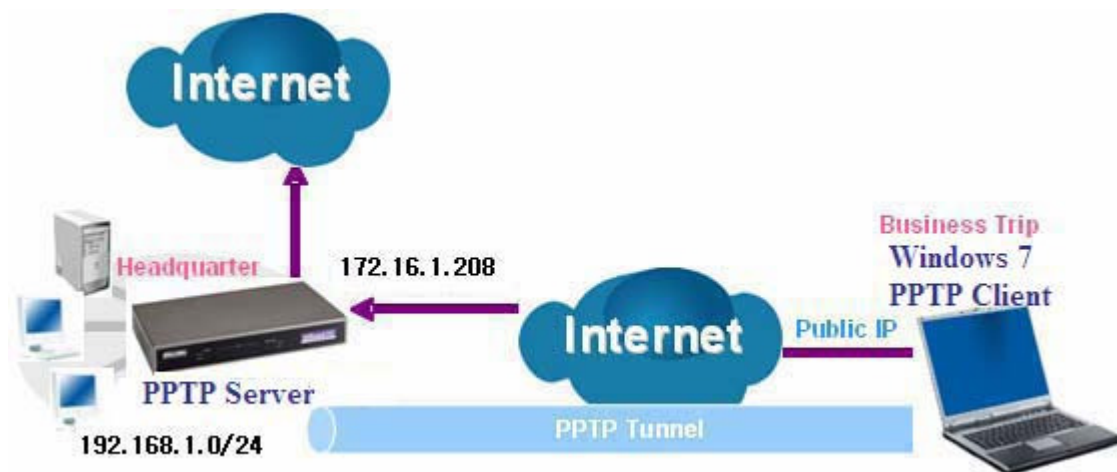
Peer Network IP: Please input the subnet IP for Server peer.

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 page 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.

2. Create a PPTP Account "test".

The screenshot shows the 'VPN Account' configuration page. The 'Parameters' section includes the following settings:

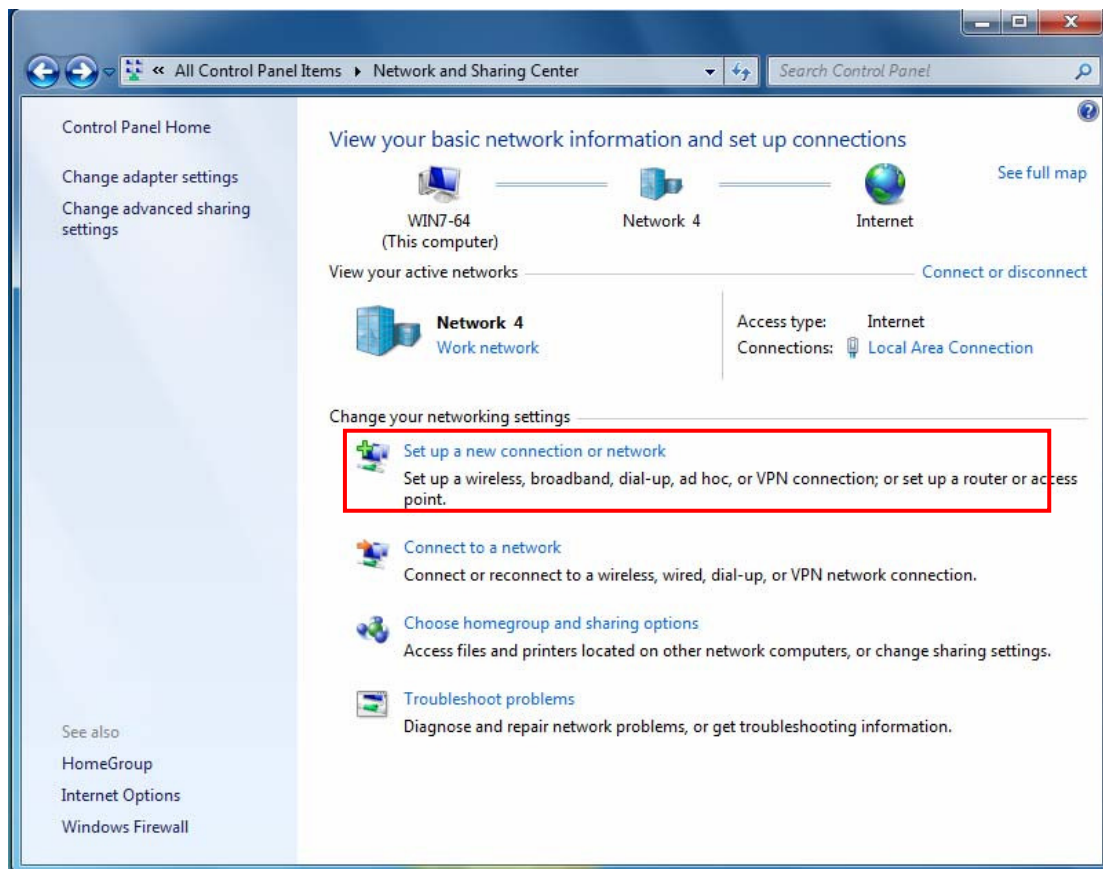
- Name: test
- Username:
- Connection Type: ☒ Remote Access ☐ LAN to LAN
- Peer Network IP:
- Peer Netmask:
- Tunnel: ☒ Enable ☐ Disable
- Password:

Buttons for 'Add' and 'Edit / Delete' are at the bottom. Below the form is a table listing the configured accounts:

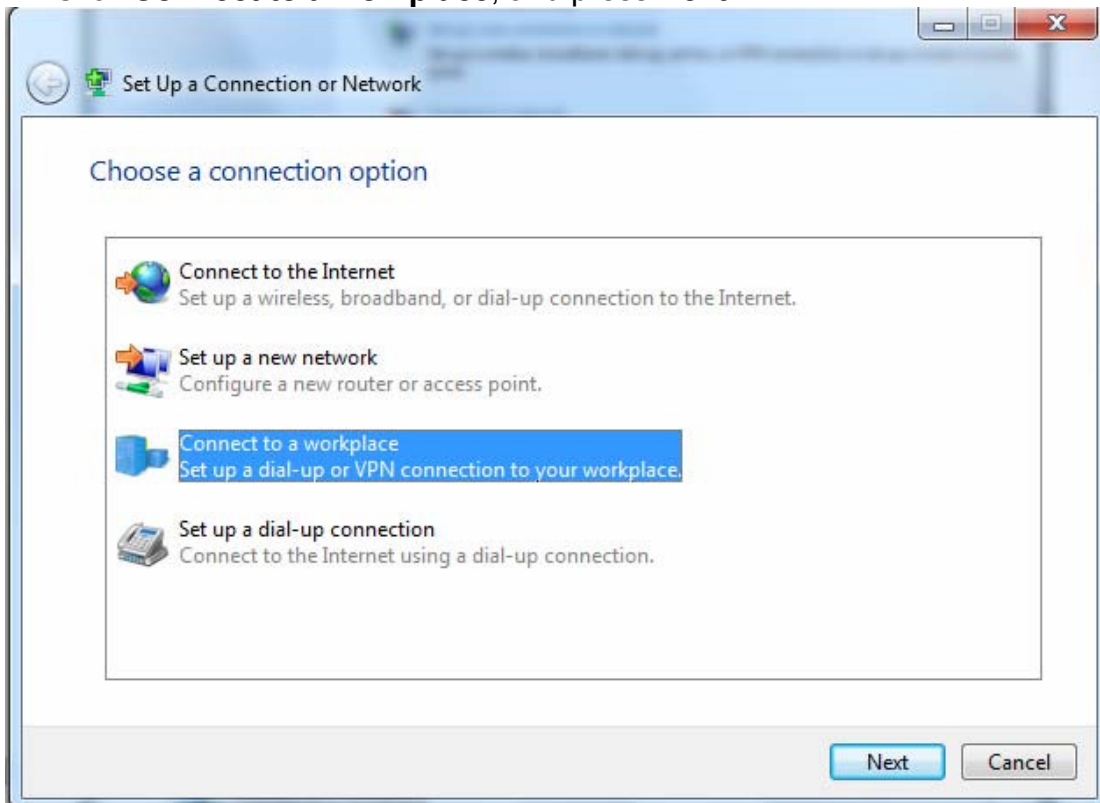
Edit	Name	Tunnel	Connection Type	Peer Network IP	Peer Netmask	Delete
☐	test	Enable	Remote Access			☐

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: [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: 172.16.1.208

Destination name: test

☐ 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

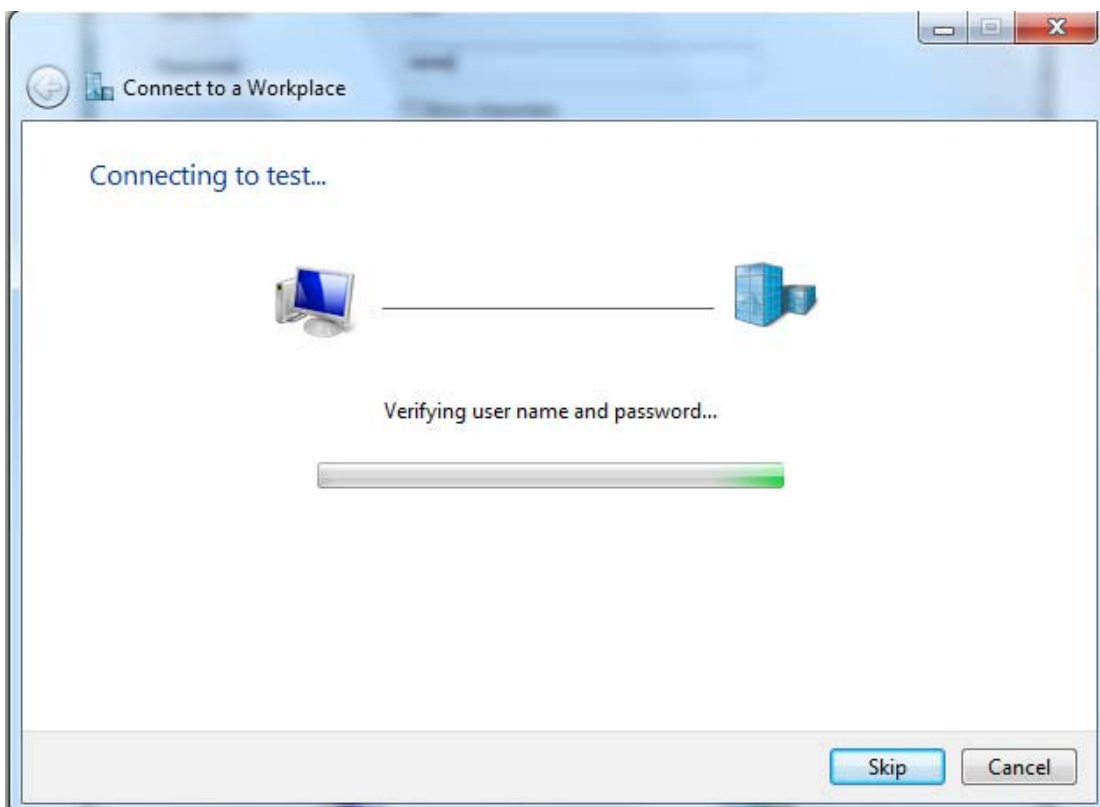
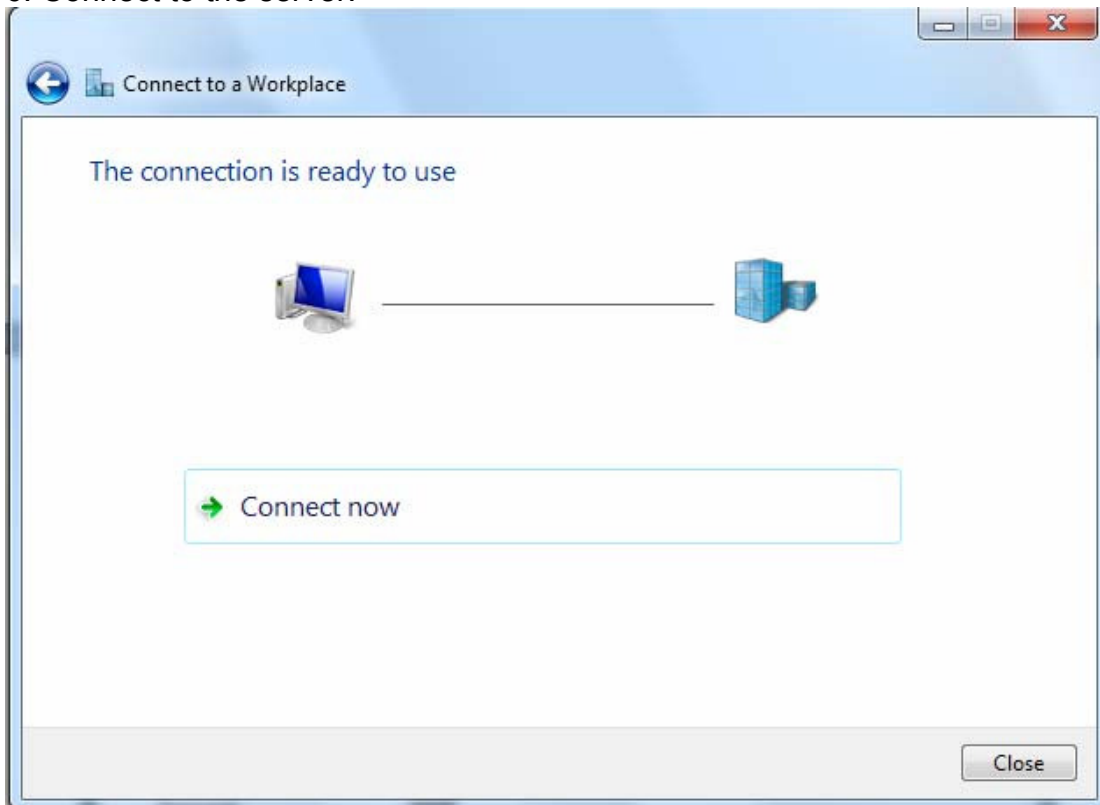
5. Input the account (**user name** and **password**) and press **Create**.

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

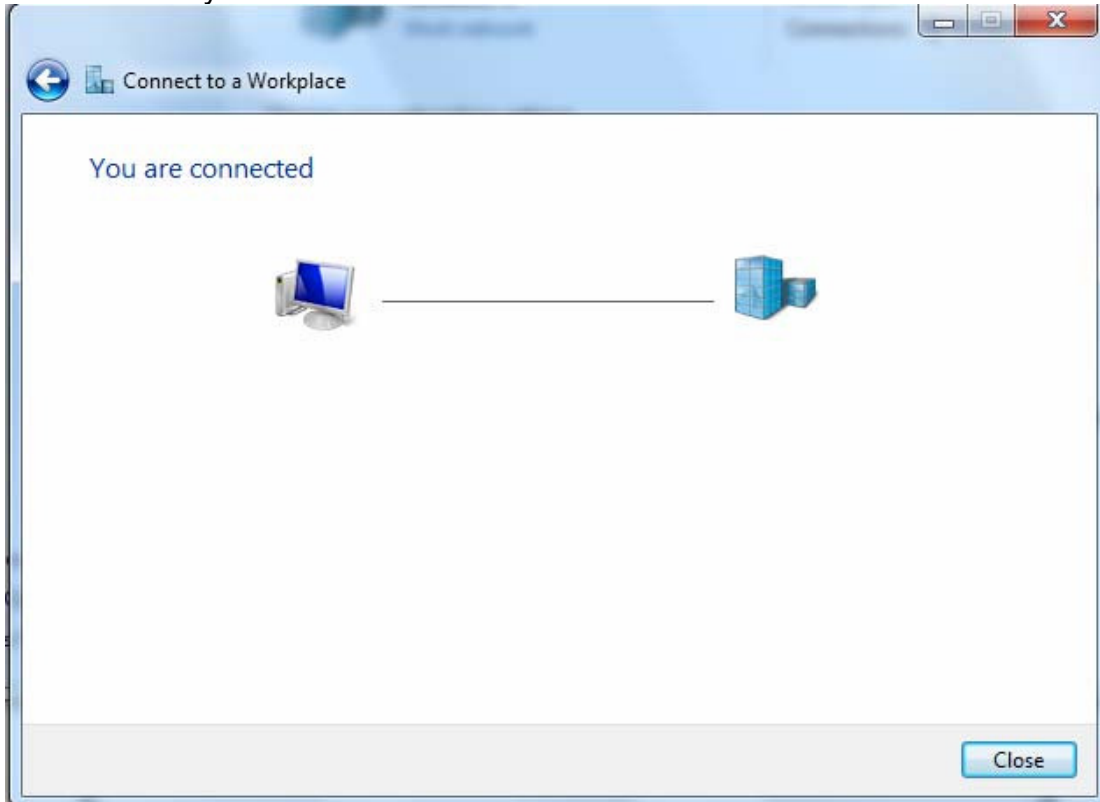
Top Screenshot: The dialog box contains the instruction "Type your user name and password". It features three input fields: "User name:", "Password:", and "Domain (optional):". The "Password:" field has two checkboxes below it: "Show characters" and "Remember this password", both of which are currently 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 black dots, indicating a masked password. 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.

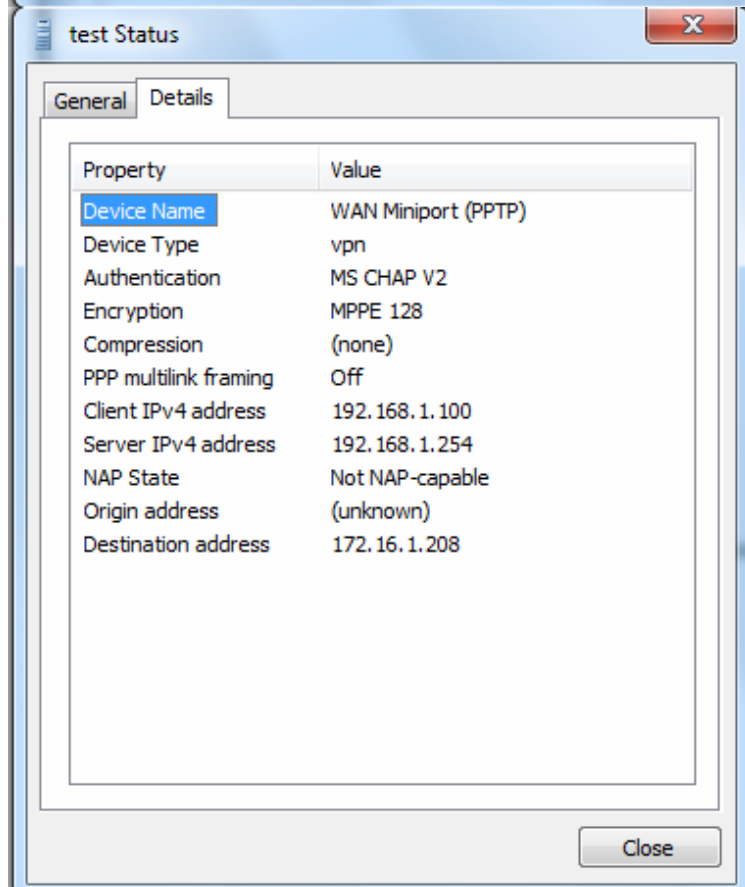
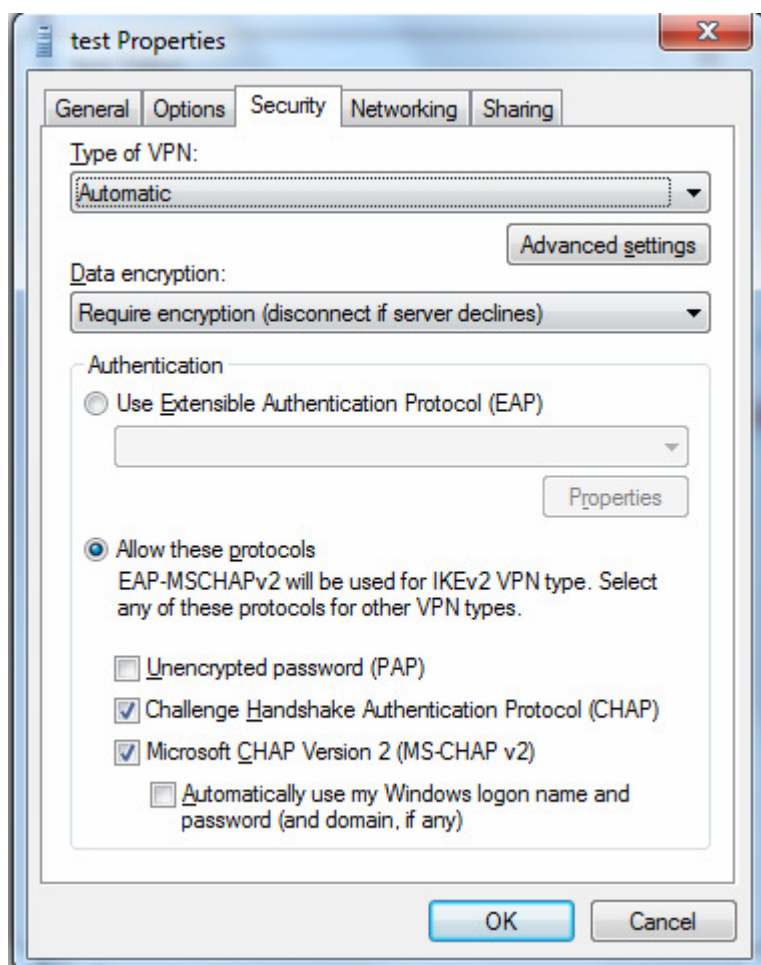


7. Successfully connected.



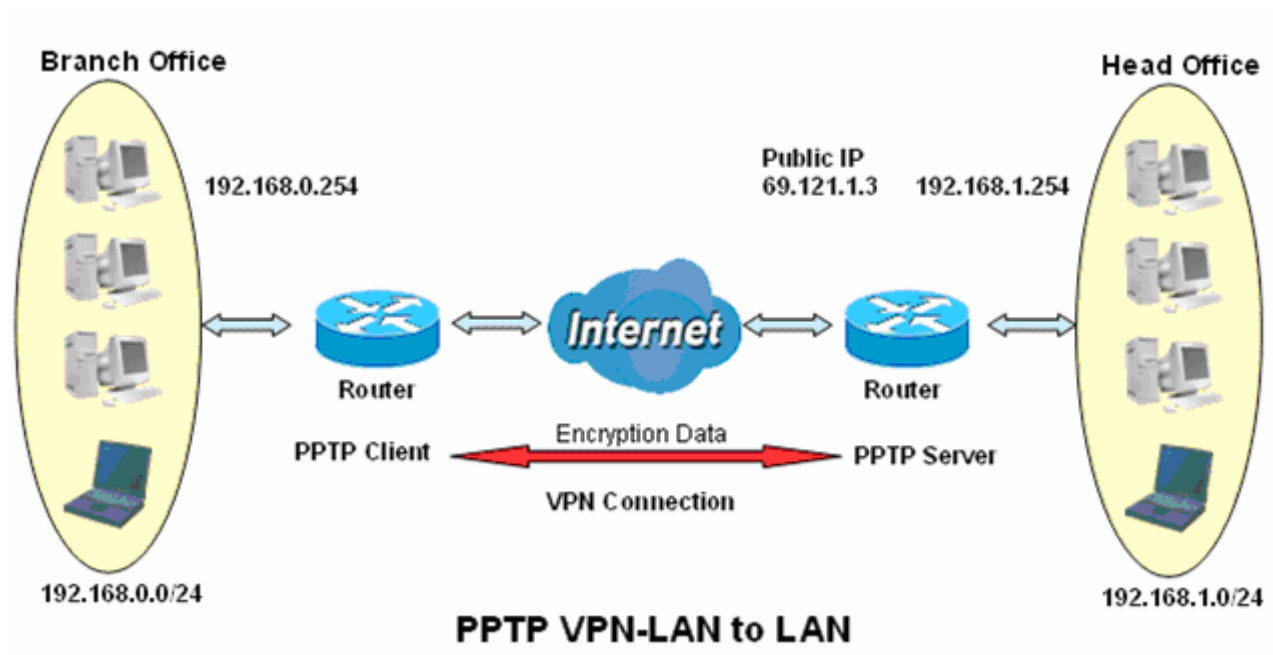
PS: You can also go to **Network Connections** shown below to check the detail of the connection. Right click "test" icon, and select "Properties" to change the security parameters (if the connection fails, users can go here to change the settings)





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

VPN

▼ PPTP Server

Parameters	
PPTP Function	☒ Enable ☐ Disable
WAN Interface	Default
Auth. Type	MS-CHAPv2
Encryption Key Length	Auto
Peer Encryption Mode	Only Stateless
IP Addresses Assigned to Peer	start from : 192.168.1.00
Idle Timeout	10 [0-120] Minute(s)
Exceptional Rule Group	None

Apply Cancel

The above is the common setting for PPTP Server, set as you like for authentication and encryption. The settings in Client side should be in accordance with settings in Server side.

Then the PPTP Account.

VPN Account

VPN Account applied to PPTP Server and L2TP 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

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.

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		
Peer Network IP	192.168.1.0	Peer Netmask	255.255.255.0

Edit	Enable	Default Gateway	Name	Time to Connect	PPTP Server Address	Connection Type	Peer Network IP	Peer Netmask	Delete
☒	☐	☐	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.

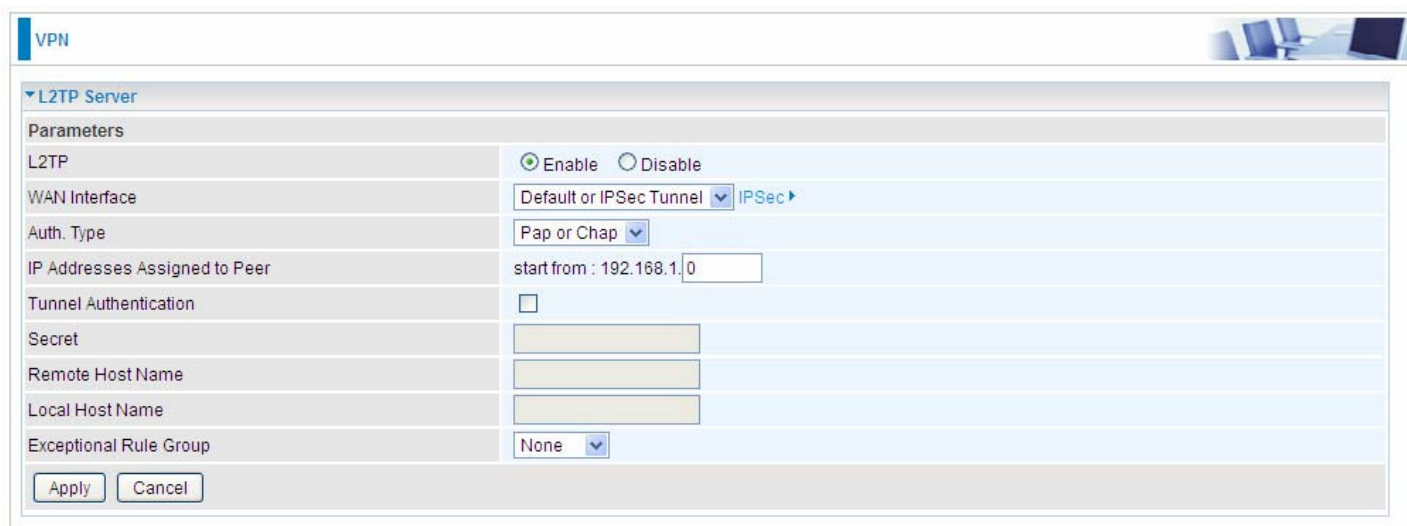
L2TP does not provide confidentiality or strong authentication by itself. IPsec is often used to secure L2TP packets by providing confidentiality, authentication and integrity. The combination of these two protocols is generally known as L2TP/IPsec.

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.



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		L2TP over IPsec	☐ Enable
WAN Interface	Default		
Username		Password	
Auth. Type	Pap or Chap	L2TP Server Address	
Connection Type	☒ Remote Access ☐ LAN to LAN		
Peer Network IP		Peer Netmask	
Tunnel Authentication	☐	Secret	
Remote Host Name		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		L2TP over IPsec	☒ Enable
IPSec Tunnel	test2	IPSec	
Username		Password	
Auth. Type	Pap or Chap	L2TP Server Address	
Connection Type	☒ Remote Access ☐ LAN to LAN		
Peer Network IP		Peer Netmask	
Tunnel Authentication	☐	Secret	
Remote Host Name		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 a sub-tab for 'L2TP Client'. Under the 'Parameters' section, there is a table of configuration fields:

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

At the bottom of the form are two buttons: 'Add' and 'Edit / 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.

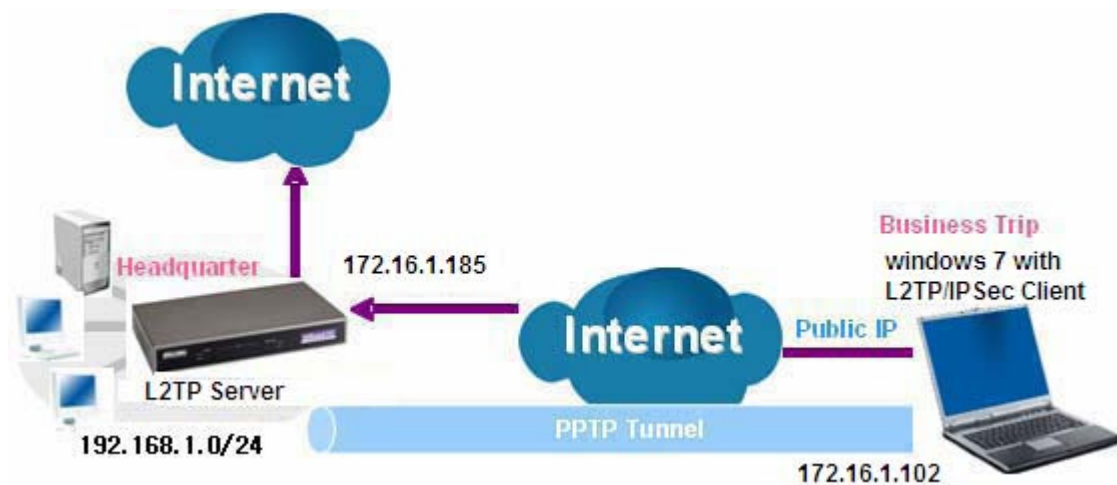
Secret: Enter the set secret password in the server side.

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**.

VPN

L2TP Server

Parameters

L2TP ☒ Enable ☐ Disable

WAN Interface

IP Addresses Assigned to Peer start from :

Tunnel Authentication ☐

Secret

Remote Host Name

Local Host Name

Exceptional Rule Group

The IPSec for L2TP rule

VPN

IPSec

IPSec Settings

L2TP over IPSec ☒ Enable

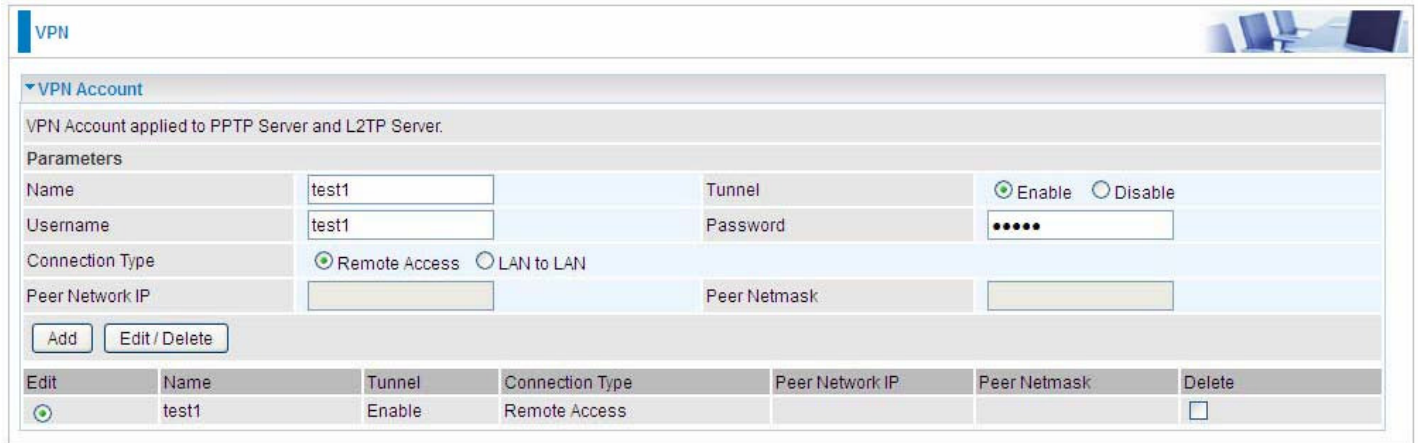
Connection Name WAN Interface IP Version

Remote Security Gateway ☒ Anonymous

Key Exchange Method IPsec Protocol

Pre-Shared Key

2. Create a L2TP Account “test1”.



VPN

VPN Account

VPN Account applied to PPTP Server and L2TP Server.

Parameters

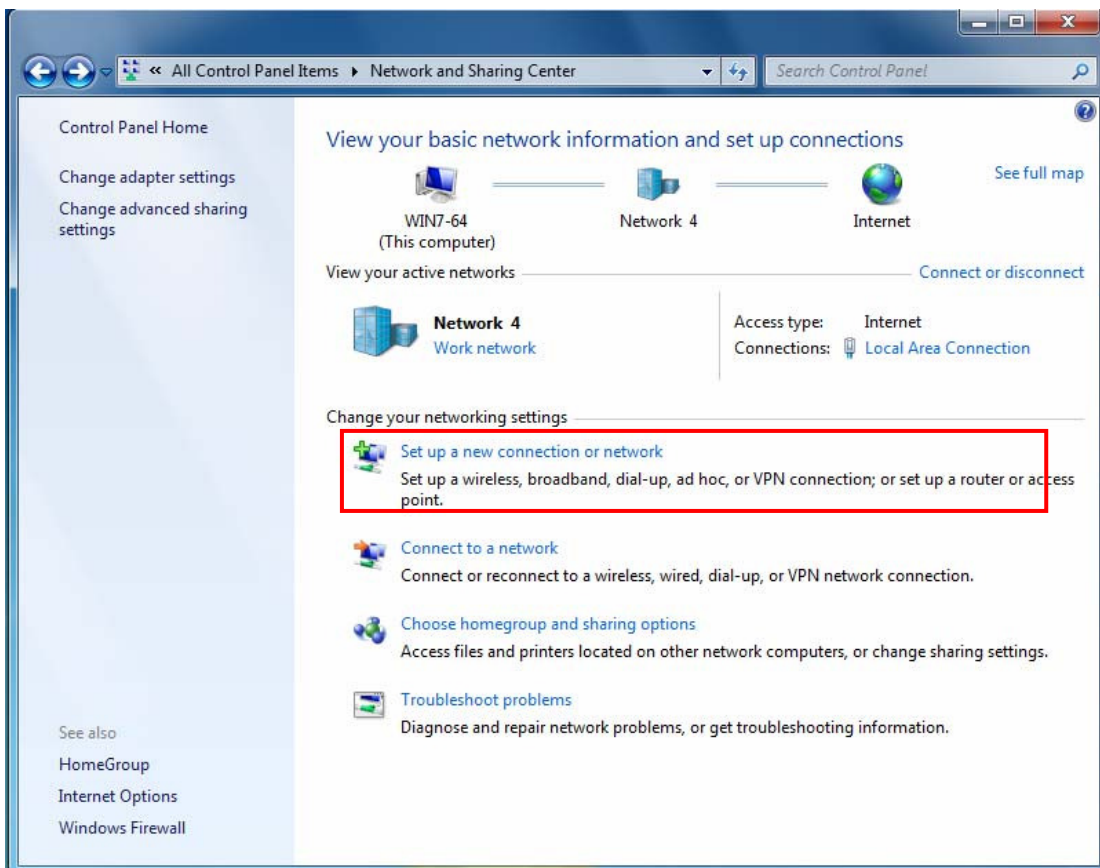
Name	test1	Tunnel	☒ Enable ☐ Disable
Username	test1	Password	
Connection Type	☒ Remote Access ☐ LAN to LAN		
Peer Network IP		Peer Netmask	

Add Edit / Delete

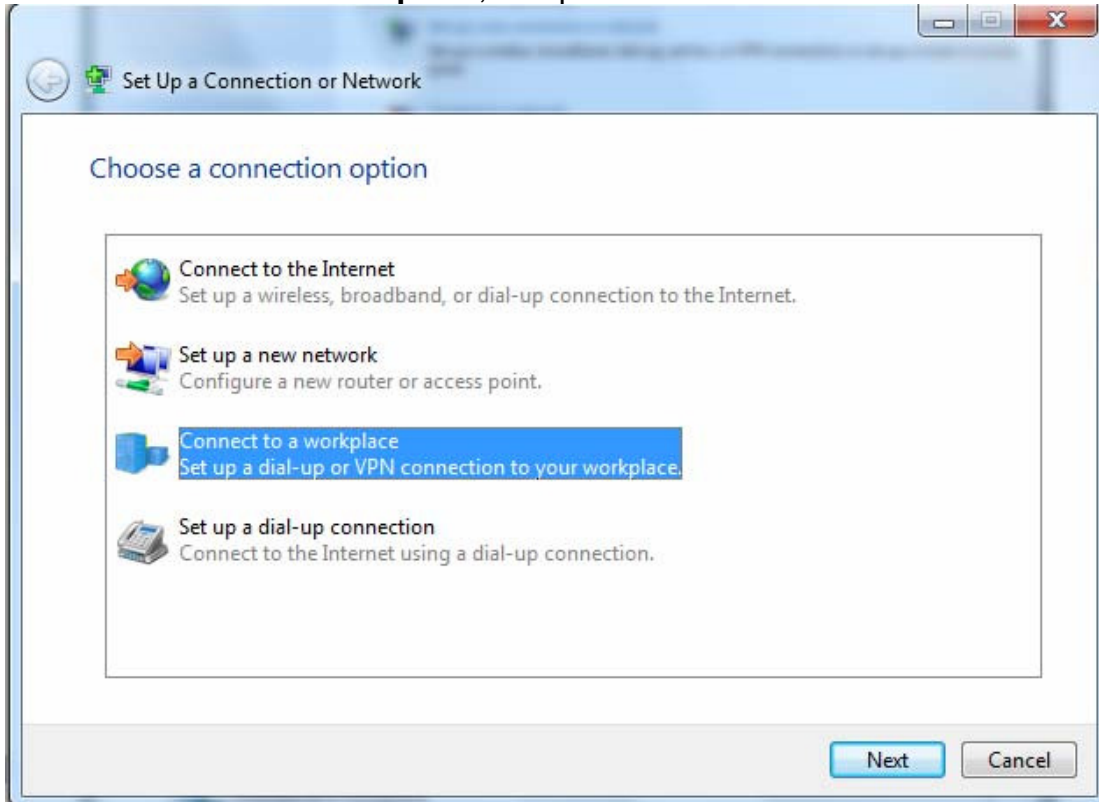
Edit	Name	Tunnel	Connection Type	Peer Network IP	Peer Netmask	Delete
☒	test1	Enable	Remote Access			☐

Client Side:

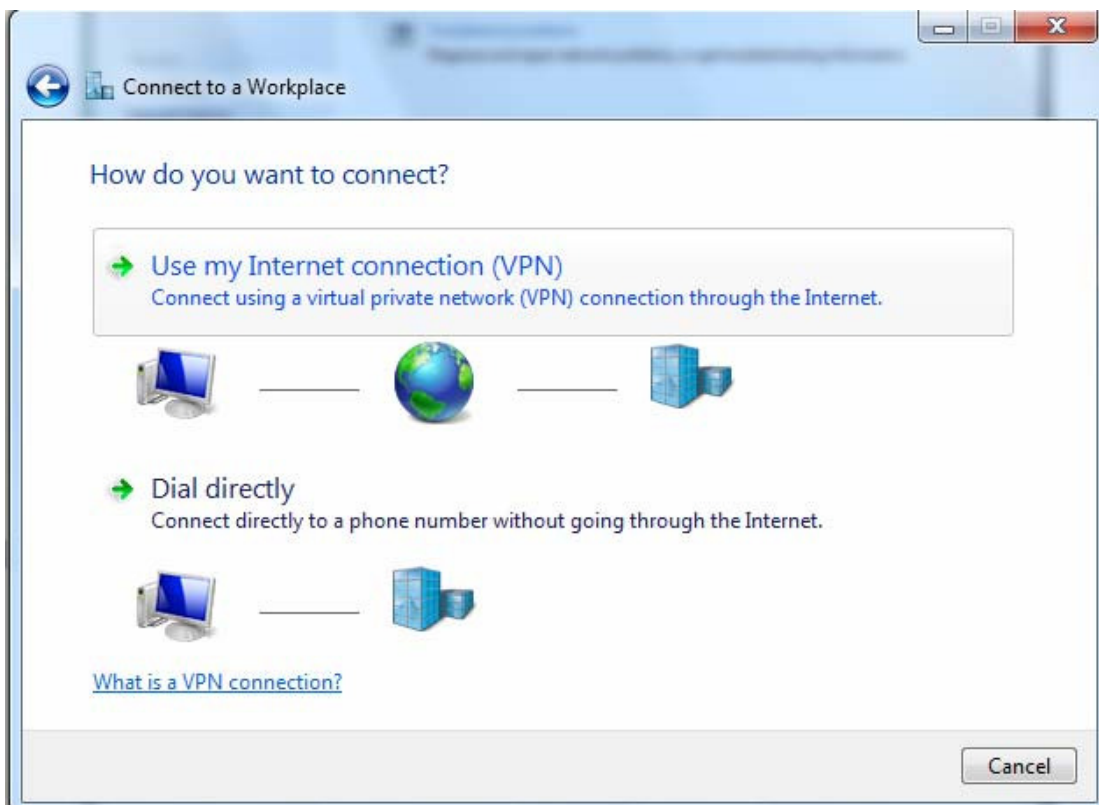
1. In Windows7 click **Start > Control Panel> Network and Sharing Center**, Click **Set up a new connection network**.



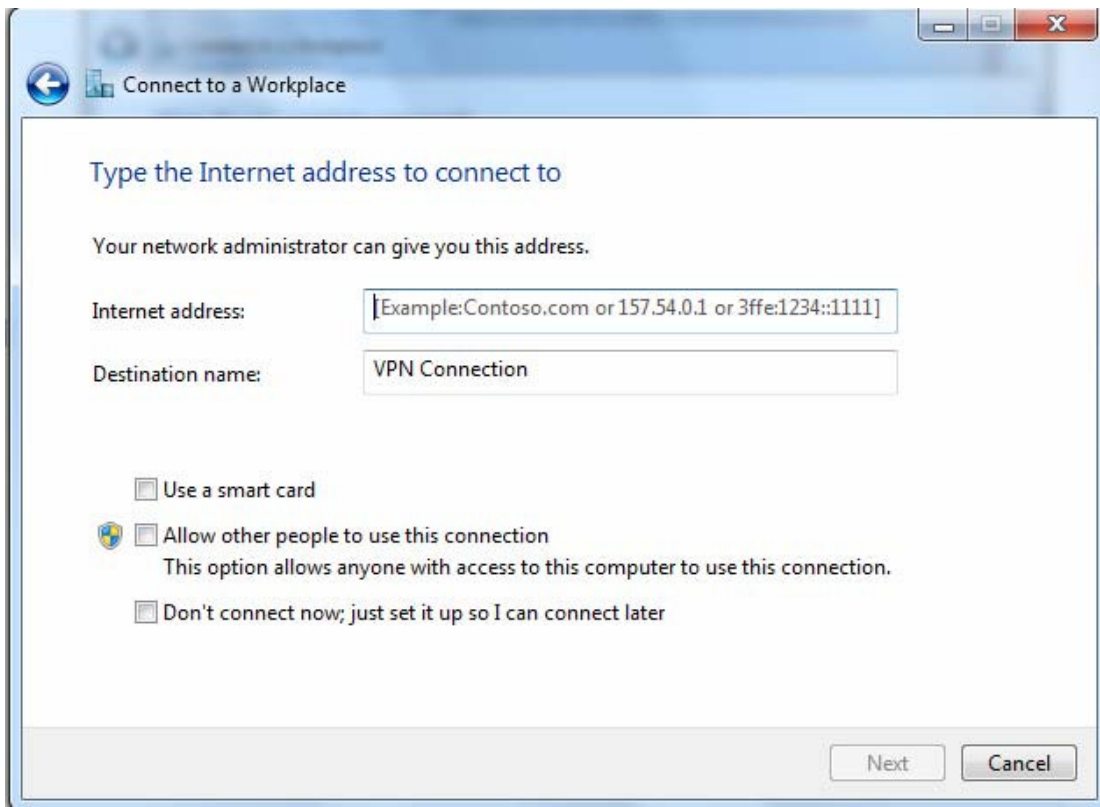
2. Click **Connect to a workplace**, and press **Next**.



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]

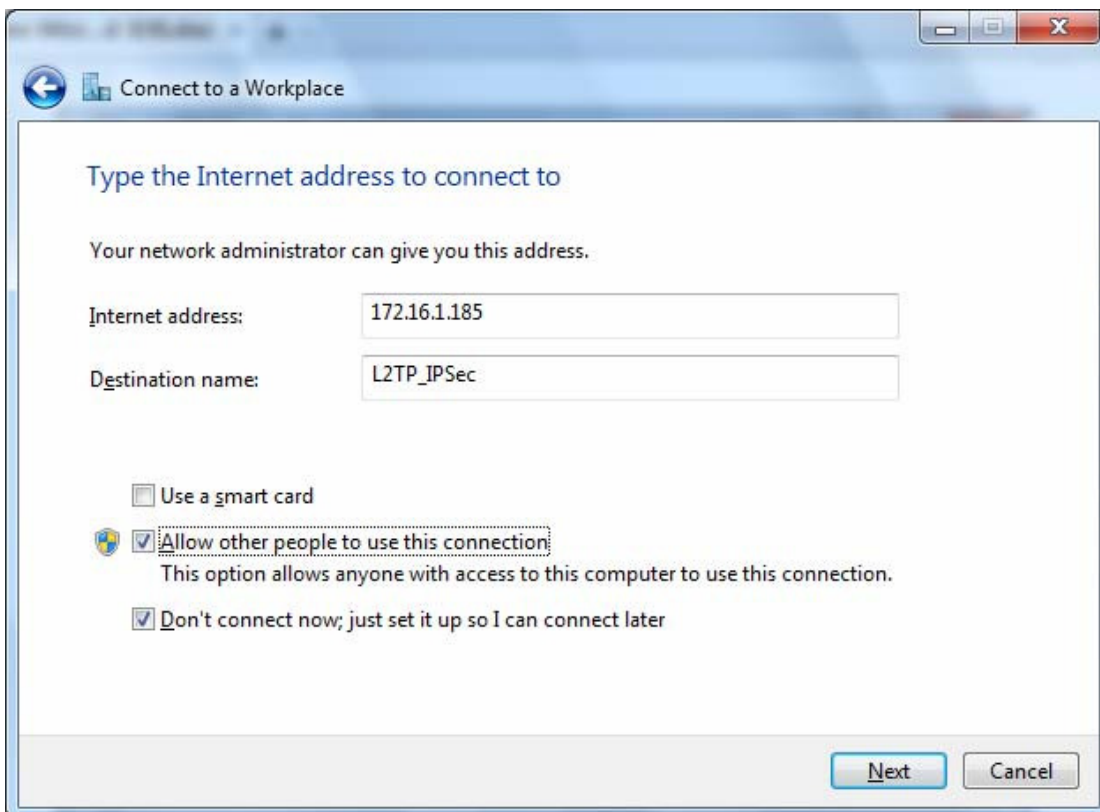
Destination name: VPN Connection

☐ 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**.

 Connect to a Workplace

Type your user name and password

User name:

Password:

☐ Show characters

☐ Remember this password

Domain (optional):

Create

Cancel

 Connect to a Workplace

Type your user name and password

User name:

test1

Password:

•••••

☐ Show characters

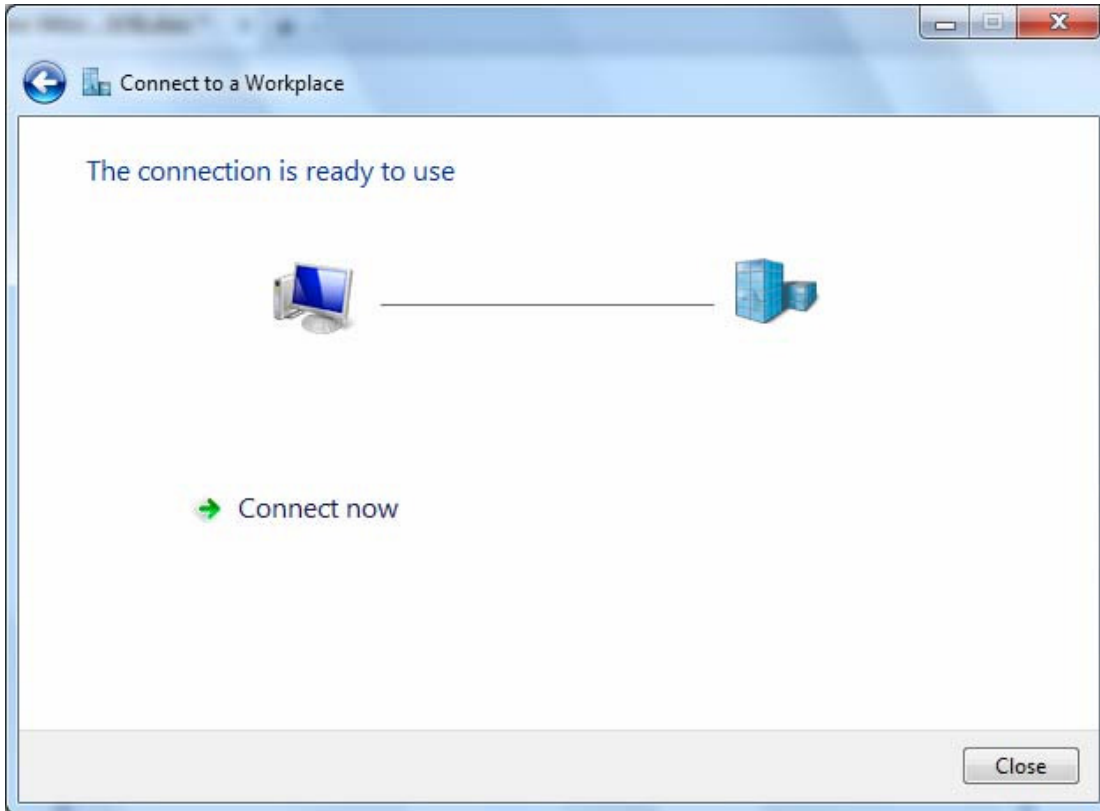
☐ Remember this password

Domain (optional):

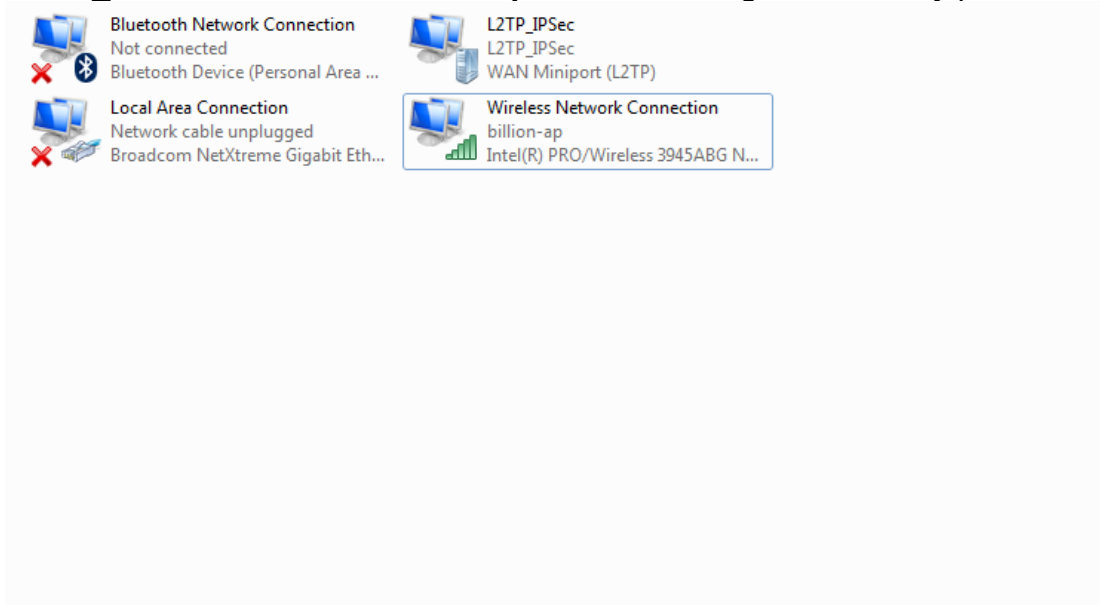
Create

Cancel

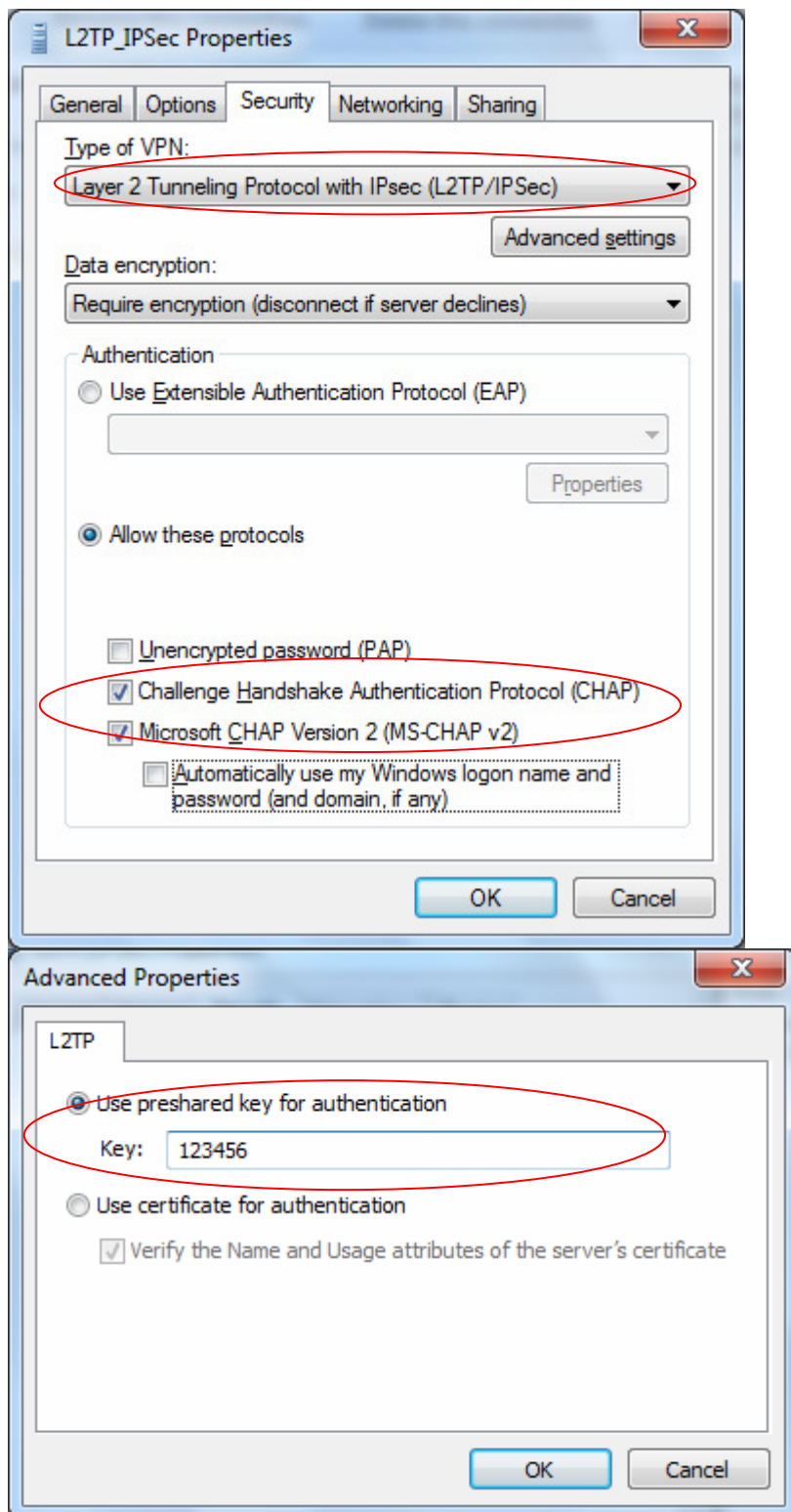
6. Connection created. Press **Close**.



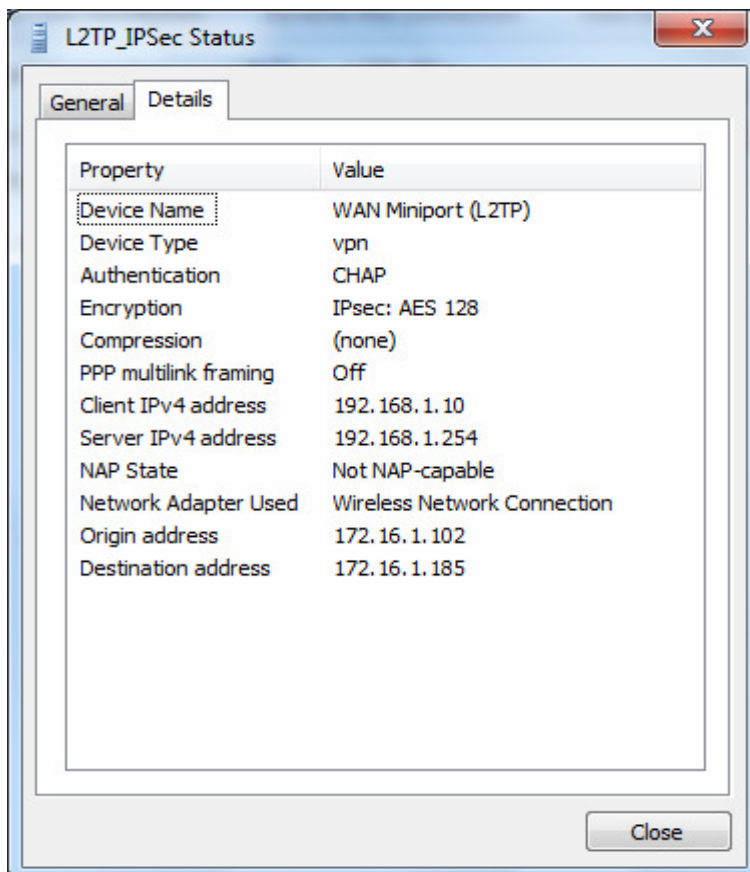
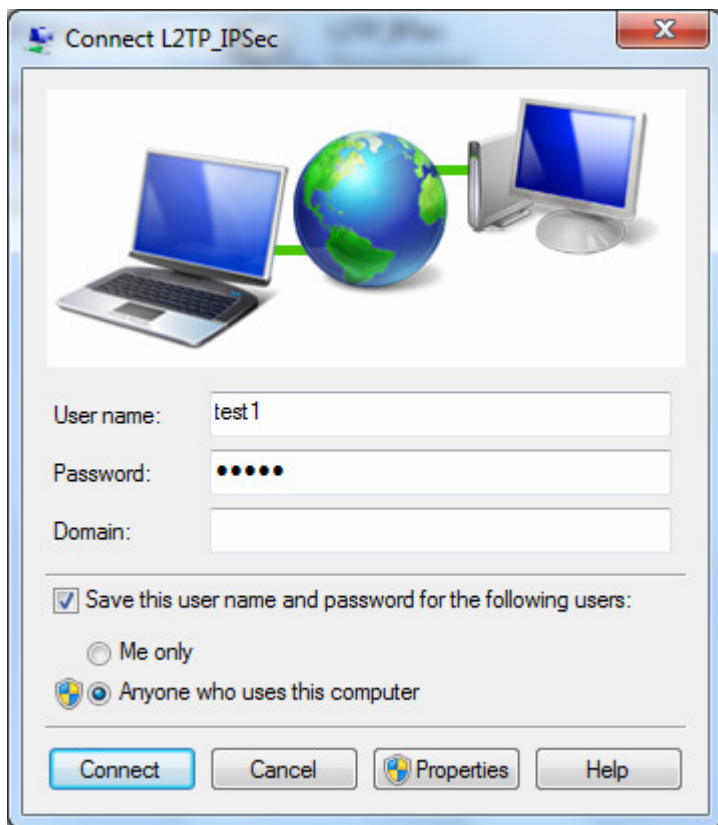
7. Go to **Network Connections** shown below to check the detail of the connection. Right click "L2TP_IPSec" icon, and select "**Properties**" to change the security parameters.



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.



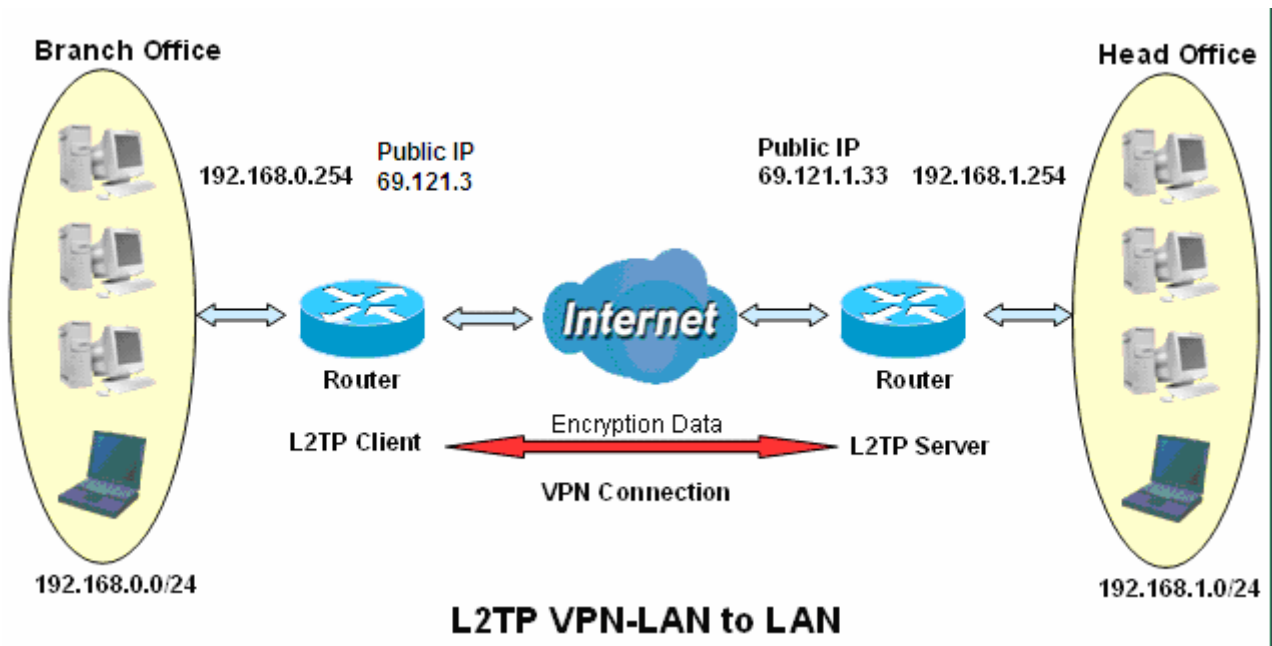
9. Go to **Network connections**, enter username and password to connect L2TP_IPSec and check the connection status.



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 commonly 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 Server and L2TP 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 L2TP server, and can also set the tunnel as the default route for all outgoing traffic.

VPN

L2TP Client

Parameters

Name

BO

L2TP over IPSec

☒ Enable

IPSec Tunnel

test2

IPSec

Username

test2

Password

.....

Auth. Type

Chap

L2TP Server Address

69.121.1.33

Connection Type

☐ Remote Access

☒ LAN to LAN

Peer Network IP

192.168.1.0

Peer Netmask

255.255.255.0

Tunnel Authentication

☐

Secret

Remote Host Name

Local Host Name

Add

Edit / Delete

Edit

Enable

Default Gateway

Name

L2TP Server Address

Connection Type

Peer Network IP

Peer Netmask

Delete

☒

☐

☐

BO

69.121.1.33

LAN to LAN

192.168.1.0

255.255.255.0

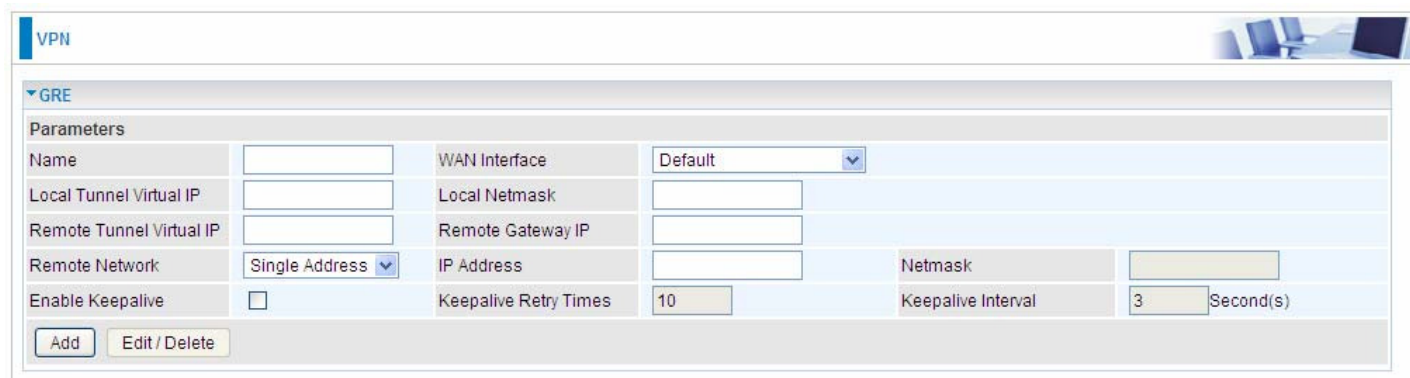
☐

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.

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.

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 and a small graphic of a laptop. Below this, a 'GRE' section is expanded, showing a 'Parameters' table. The table has two columns for configuration fields. The fields include: Name (text input), WAN Interface (dropdown menu set to 'Default'), Local Tunnel Virtual IP (text input), Local Netmask (text input), Remote Tunnel Virtual IP (text input), Remote Gateway IP (text input), Remote Network (dropdown menu set to 'Single Address'), IP Address (text input), Netmask (text input), Enable Keepalive (checkbox), Keepalive Retry Times (text input set to '10'), and Keepalive Interval (text input set to '3' with a unit of 'Second(s)'). At the bottom of the table, there are two buttons: 'Add' and 'Edit / Delete'.

Parameters	
Name	
WAN Interface	Default
Local Tunnel Virtual IP	
Local Netmask	
Remote Tunnel Virtual IP	
Remote Gateway IP	
Remote Network	Single Address
IP Address	
Netmask	
Enable Keepalive	☐
Keepalive Retry Times	10
Keepalive Interval	3 Second(s)

[Add](#) [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.

Local Netmask: Input the netmask for the local tunnel.

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

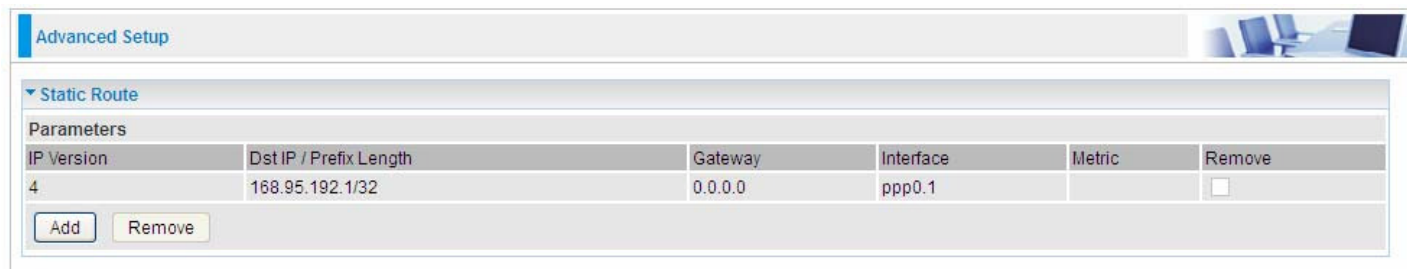
Cancel

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.

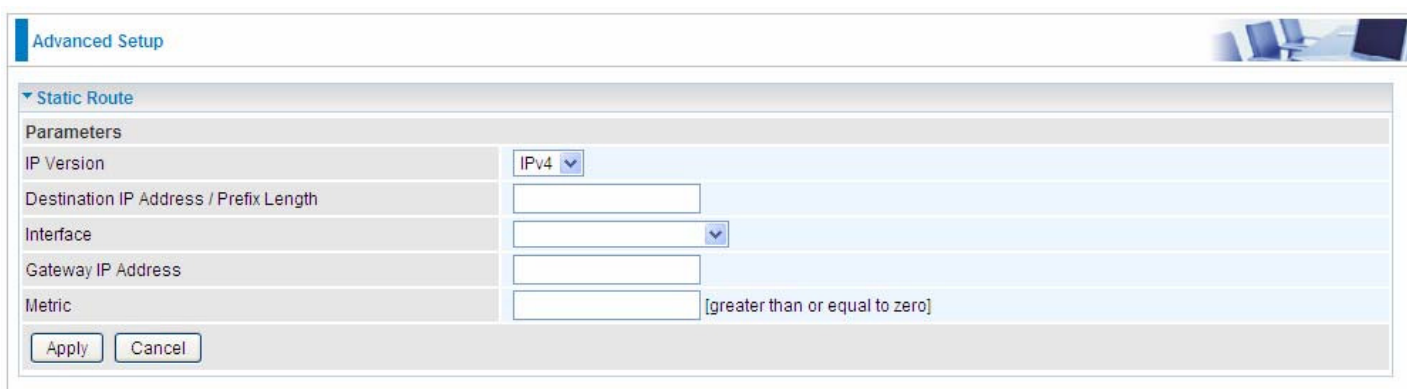


The screenshot shows the 'Advanced Setup' window with the 'Static Route' tab selected. Below the tab is a table with the following data:

IP Version	Dst IP / Prefix Length	Gateway	Interface	Metric	Remove
4	168.95.192.1/32	0.0.0.0	ppp0.1		☐

Below the table are two buttons: 'Add' and 'Remove'.

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 has the following fields:

- IP Version:** A dropdown menu set to 'IPv4'.
- Destination IP Address / Prefix Length:** A text input field.
- Interface:** A dropdown menu.
- Gateway IP Address:** A text input field.
- Metric:** A text input field with a hint '[greater than or equal to zero]'.

At the bottom of the form are two buttons: 'Apply' and 'Cancel'.

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

Destination IP Address / Prefix Length: Enter the destination IP address and the prefix length. For IPv4, the prefix length means the number of '1' in the submask, it is another mode of presenting submask. One IPv4 address, 192.168.1.0/24, submask is 255.255.255.0. While in IPv6, IPv6 address composes of two parts, thus, the prefix and the interface ID, the prefix is like the net ID in IPv4, and the interface ID is like the host ID in IPv4. The prefix length is to identify the net ID in the address. One IPv6 address, 3FFE:FFFF:0:CD30:0:0:0:0 / 64, the prefix is 3FFE:FFFF:0:CD3.

Interface: Select an interface this route associated.

Gateway IP Address: Enter the gateway IP address.

Metric: Metric is a policy for router to commit router, to determine the optimal route. Enter one number greater than or equal to 0.

Click **Apply** to apply this route and it will be listed in the route listing table.

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	pppoe_0_8_35/ppp0.1 ▼
Default Gateway	
Apply Cancel	

Policy Name: User-defined name.

Physical LAN Port: Select the LAN port.

Source IP: Enter the Host Source IP.

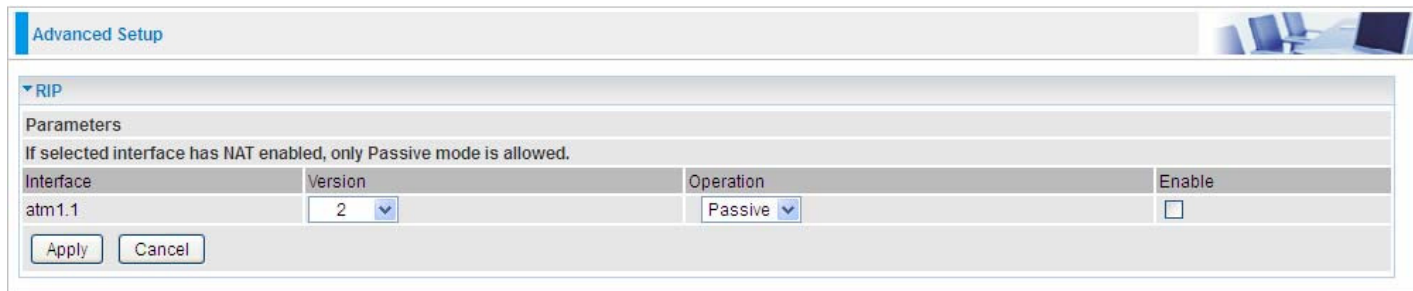
Interface: Select the WAN interface which you want the Source IP to access outside through.

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 the 'Advanced Setup' window for configuring RIP. The 'RIP' section is expanded, showing a table with columns: Interface, Version, Operation, and Enable. The first row shows 'atm1.1' for the interface, '2' for the version, 'Passive' for the operation, and an unchecked checkbox for the enable status. Below the table are 'Apply' and 'Cancel' buttons.

Interface	Version	Operation	Enable
atm1.1	2	Passive	☐

Interface: the interface the rule applies to.

Version: select the RIP version, RIP-1, RIP-2 and both.

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.