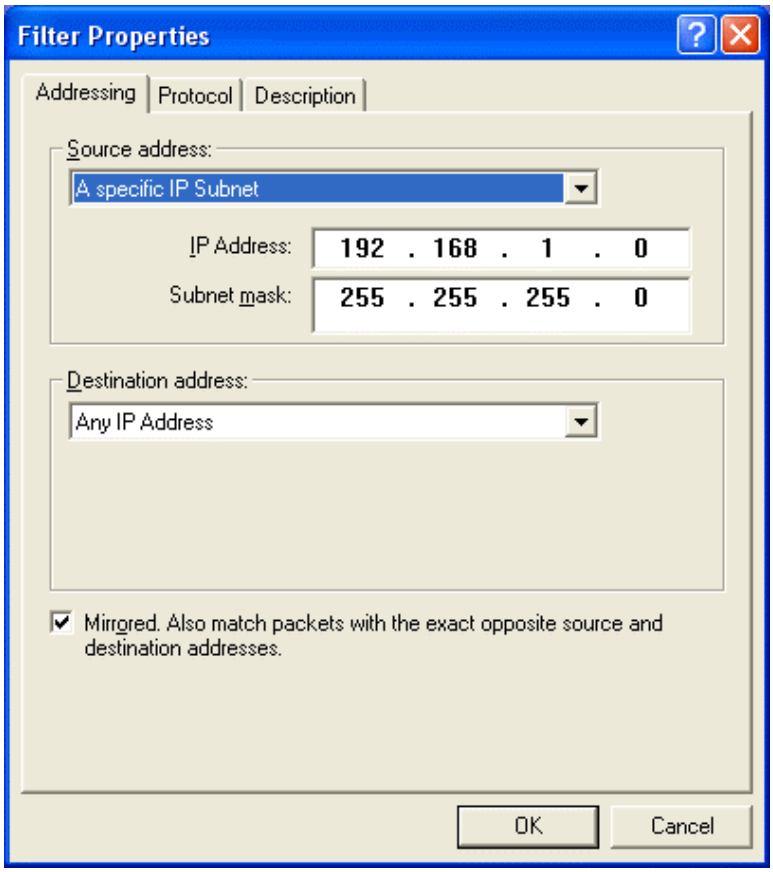
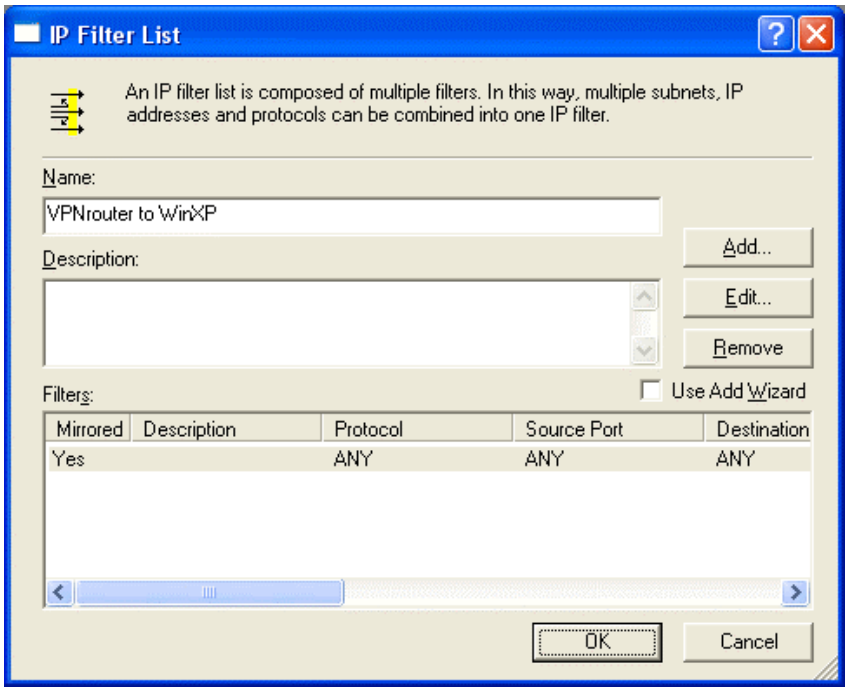
Wireless 1 WAN 4 LAN Multimedia Security VPN Router

User's Manual

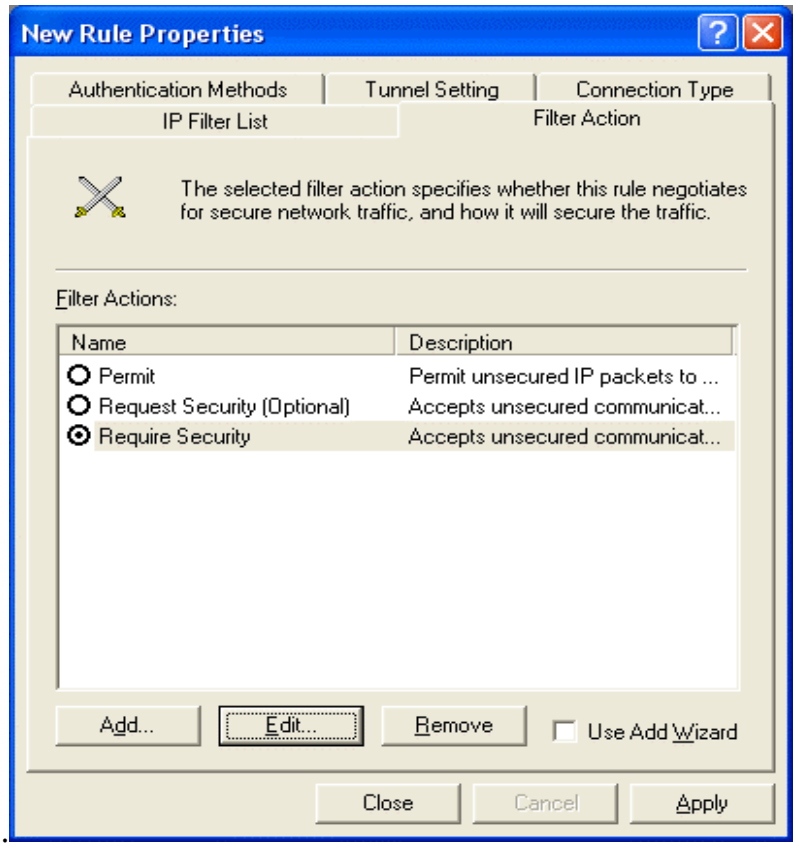
Model name: FL 1911G,Matrix 21,FL 1920



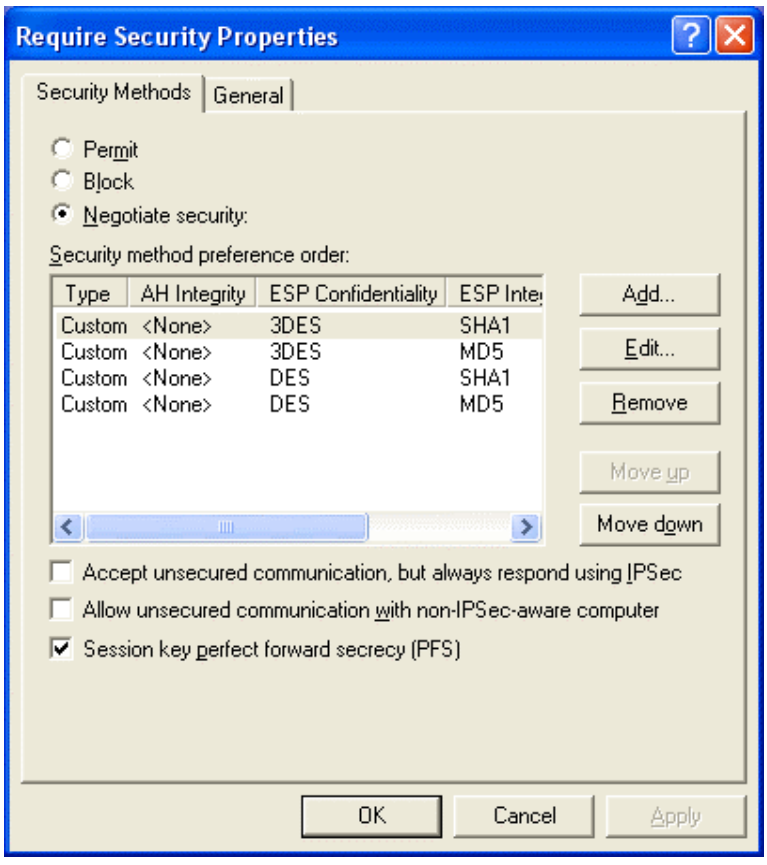
54. From **Source address** pull-down window, select **A specific IP Subnet**
55. Enter destination IP address and its subnet mask. (in this case, the destination IP is 192.168.1.0/255.255. 255.0) 。
56. From **Destination address** pull-down window, select **Any IP Address**.
57. Check the box of **Mirrored. Also match packets with the exact opposite source and destination addresses.**
58. Click on **OK** button



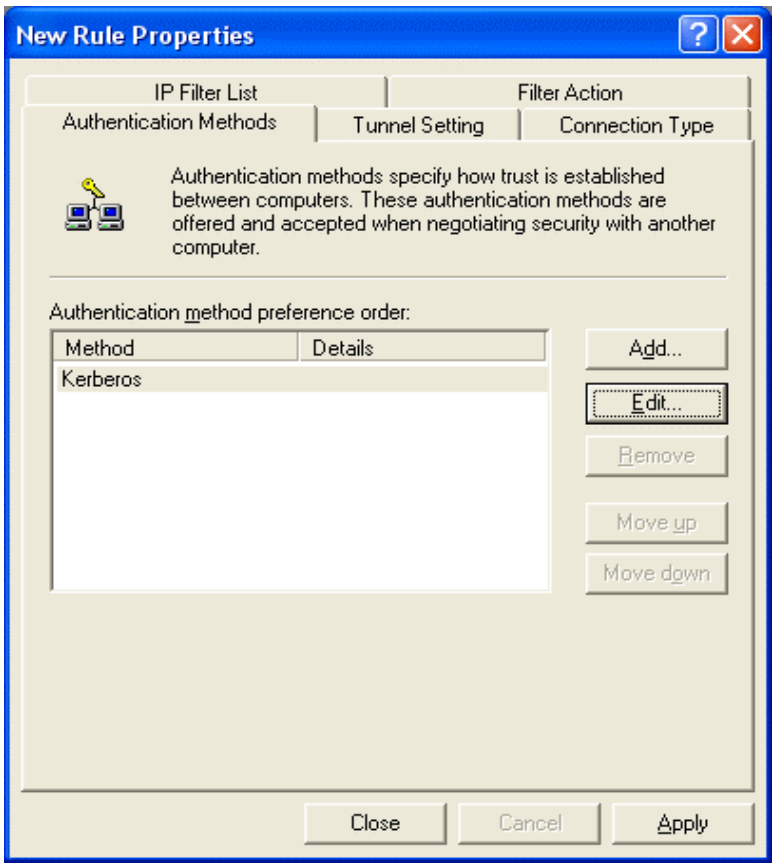
59. Click on **OK** button



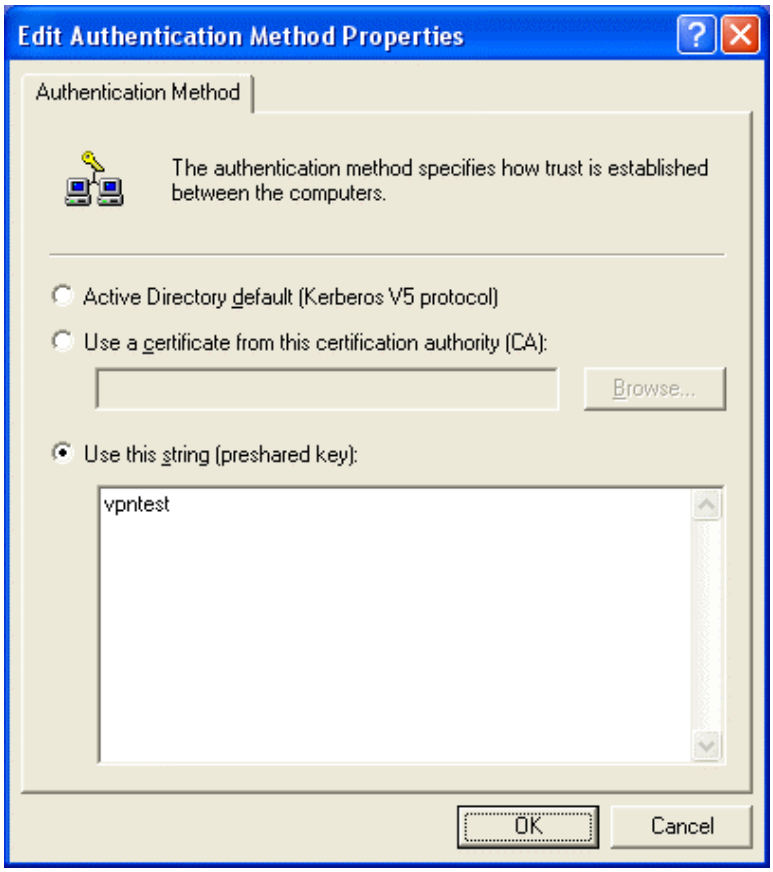
60. Click on **Require Security**
61. Click on **Edit** button



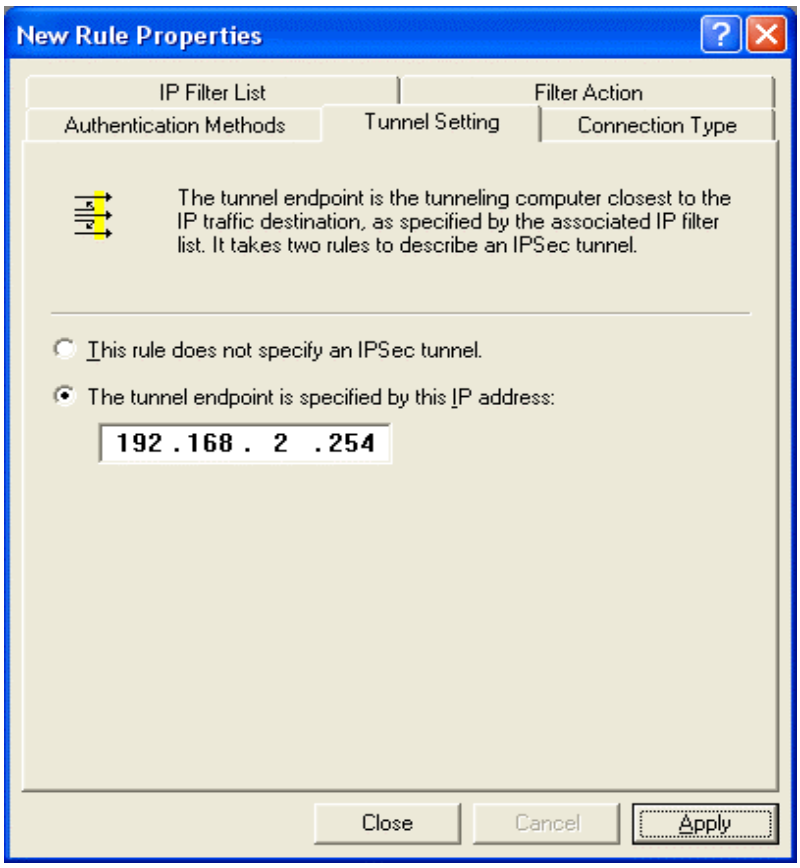
62. Click on **Negotiate security**
63. Cancel the check box of **Accept unsecured communication, but always respond using IPSec**
64. Tick the box of **session key perfect forward secrecy (PFS).**
65. Click on **OK** button



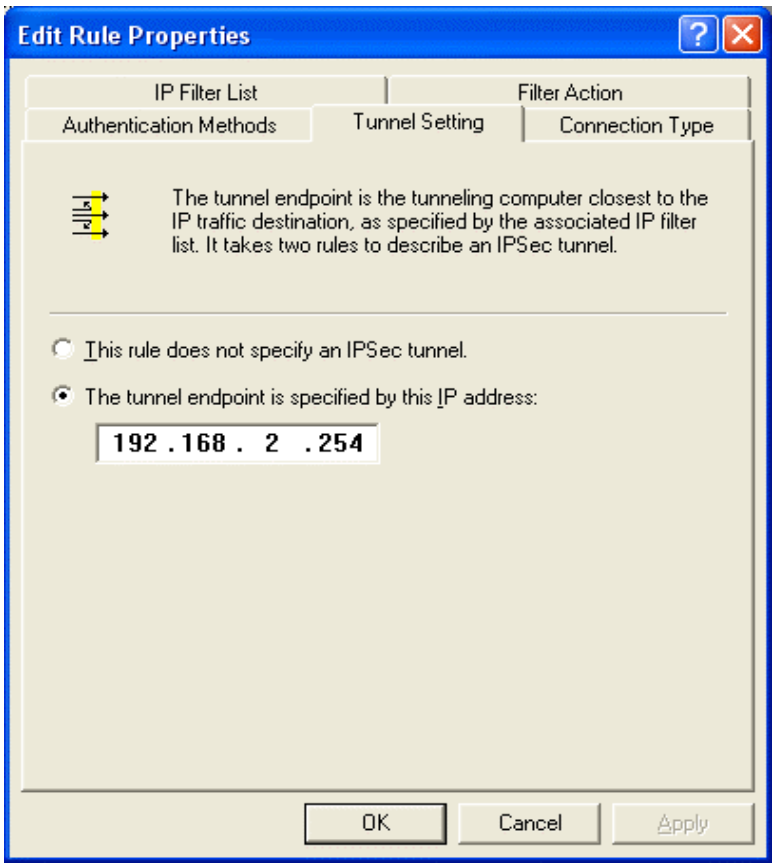
66. Click on **Edit** button



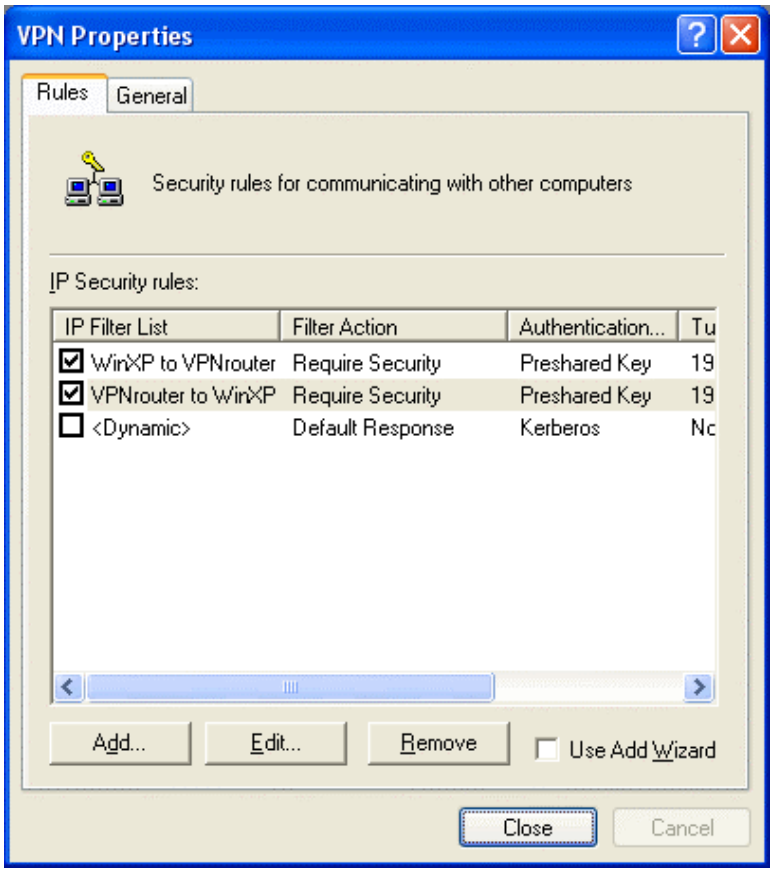
67. Click on **Use this string** (preshared key)
68. From the bottom blank area, enter the name of preshared key defined in web-based management from previous setting.
69. Click on **OK** buton



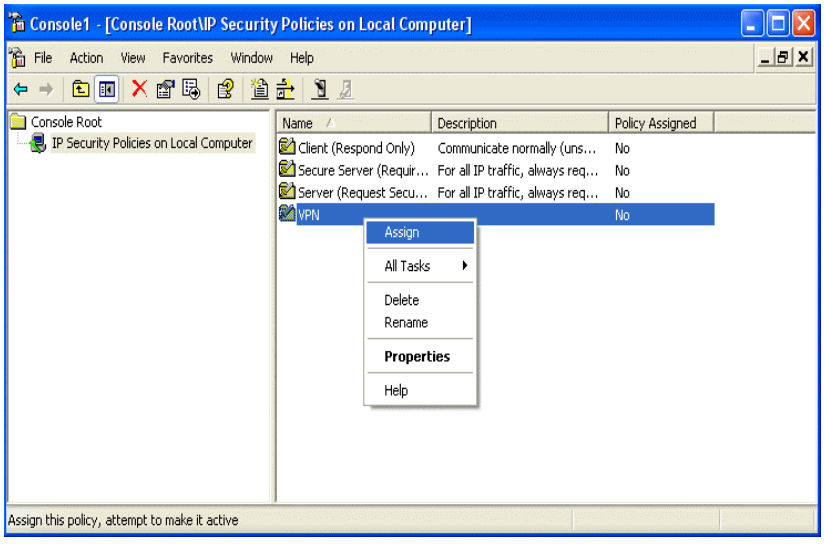
70. Click on **The tunnel endpoint is specified by this IP address**
71. Enter the **WAN IP** address of your WINXP PC (in this case, it's 192.168.2.254)
72. Click on **Apply** button



73. Click on **OK** button



74. Make sure you have checked the box of both IP Security rules you configured in previous section. In this case, they are WinXP to VPNrouter and VPNrouter to WinXP.
75. Click on **Close** button

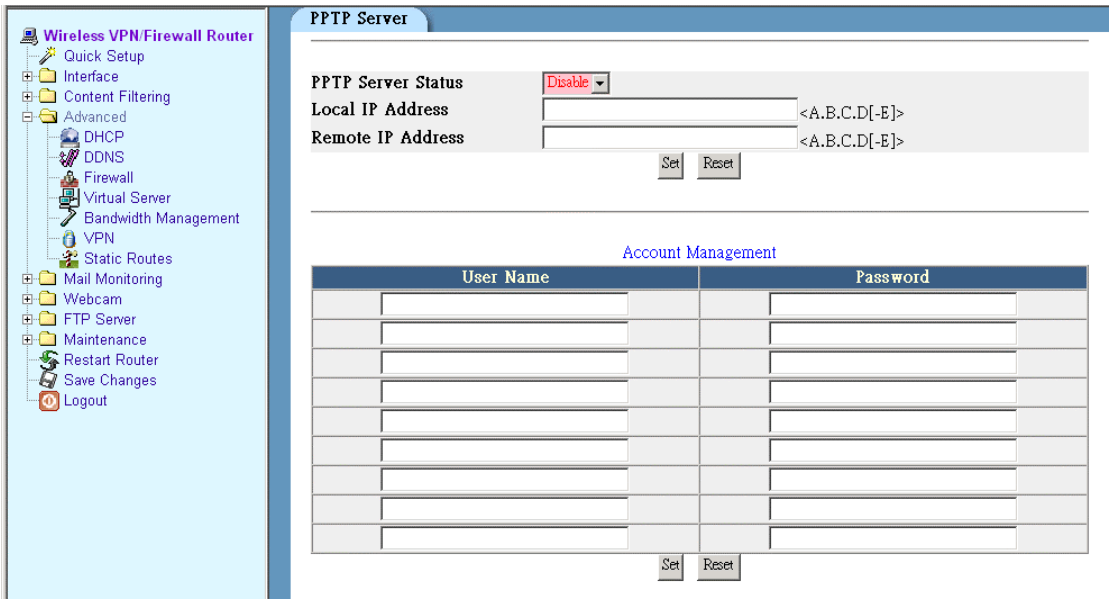


76. From IP Security Policy, click on the name of your VPN tunnel setting and click on the right hand button of your mouse.
77. Click on **Assign** from pull-down window.

Now, you have successfully established the VPN tunnel. In Web-Based management page of your router, go to **VPN** > **Show IPSEC SPI information**. The information page will appear and show all relevant information regards to your VPN connection.

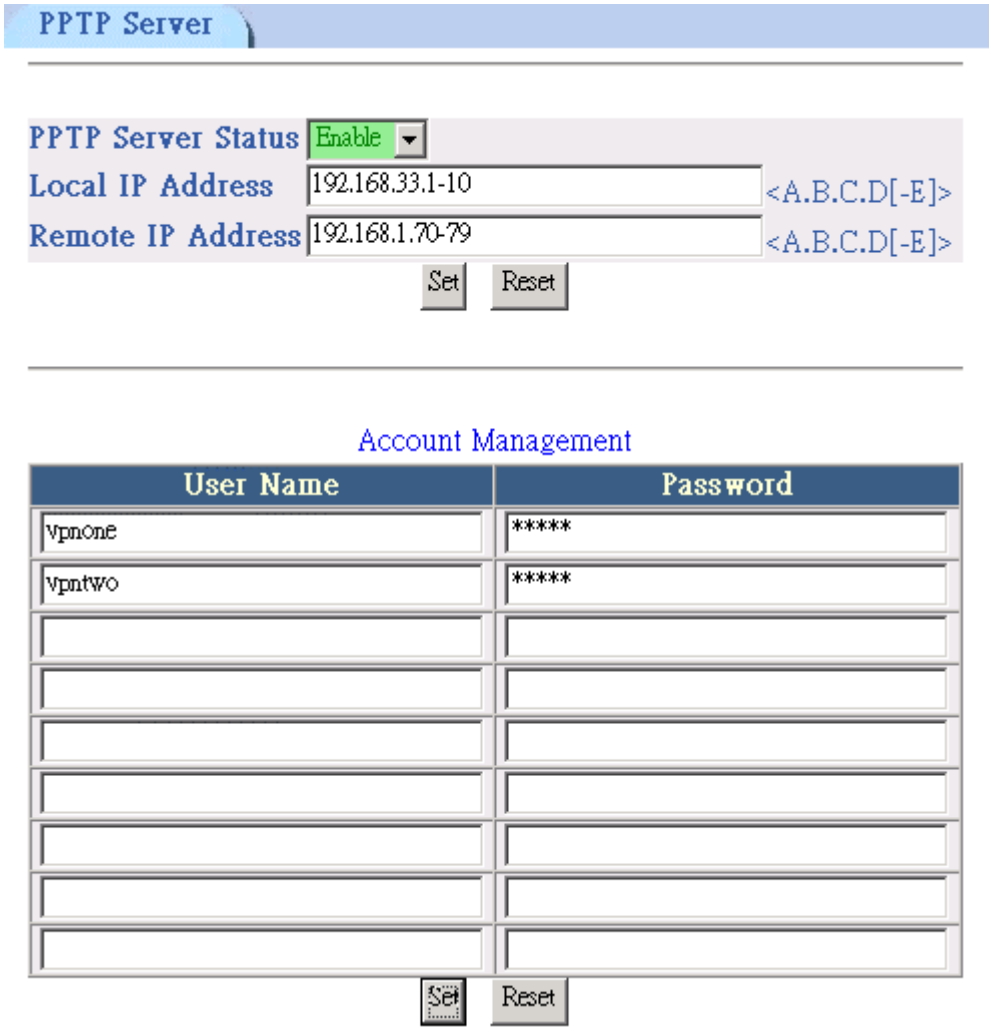
VPN PPTP Server

This router also supports PPTP tunneling protocol. Users can remotely login to the office via PPTP with supports up to 10 PPTP connections. To configure PPTP server, please click **VPN** from the left menu bar and click **PPTP Server Setting** button on the bottom of the page.



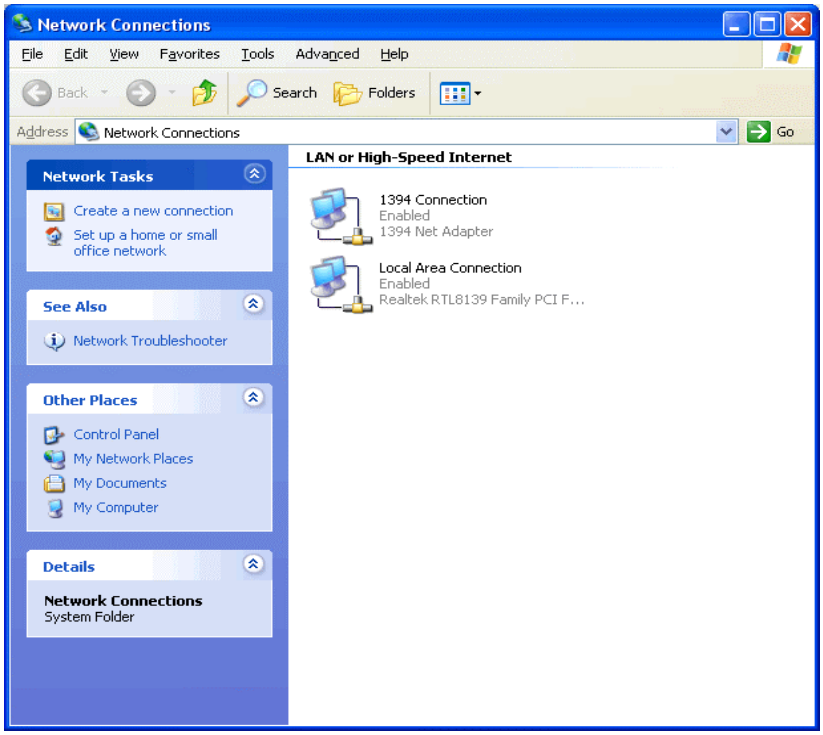
There are three major sections related to PPTP Server setting. There are **PPTP Server** setting, **Account Management** and **Client Management**.

In this case, if your VPN router's LAN IP address is 192.168.1.254/24 and its WAN IP address is 192.168.2.1/24. PPTP client's remote IP address is 192.168.1.70 – 192.168.1.79 and its local IP address is 192.168.33.1 – 192.168.33.10. Also create two user name accounts of vpnone (password: test1) and vpntwo (password: test2). Then the configuration should look like the following diagram:



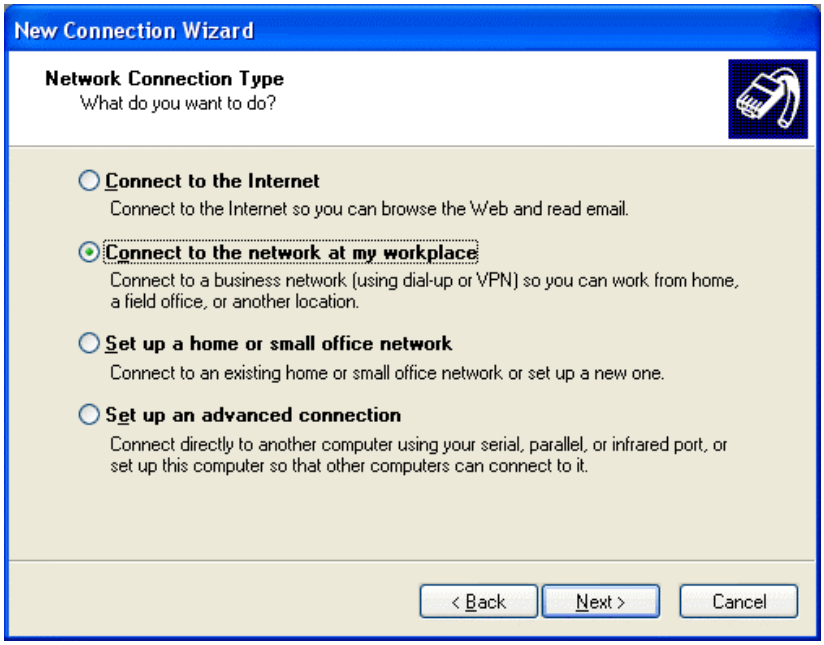
1. Firstly, please check the **PPTP Server Status** pull-down window and select **Enable**.
2. Please enter Local IP Address and Remote IP Address into their related column.
3. After complete your entries, please click on **Set** to confirm your setting.
4. In **Account Management** section, please enter **Account name** and **password** of both local user and remote user for VPN connection.
5. Please click on **Set** button to confirm after complete the entries.

In case of WINXP, the following steps shows PPTP client setting.



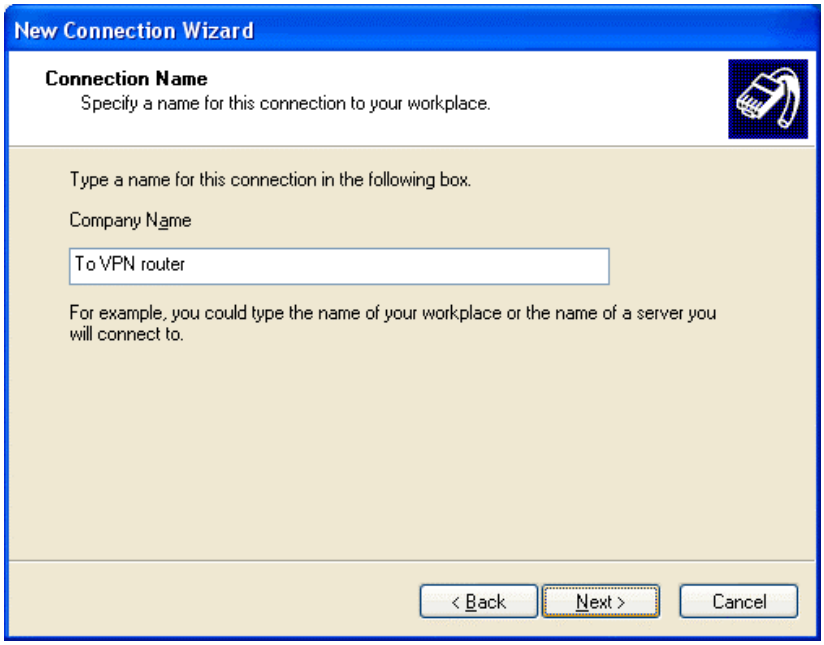
78. Go to **Network Connection** on Control Panel
79. Click on **Create a new connection.**

80. Click on **Next** button



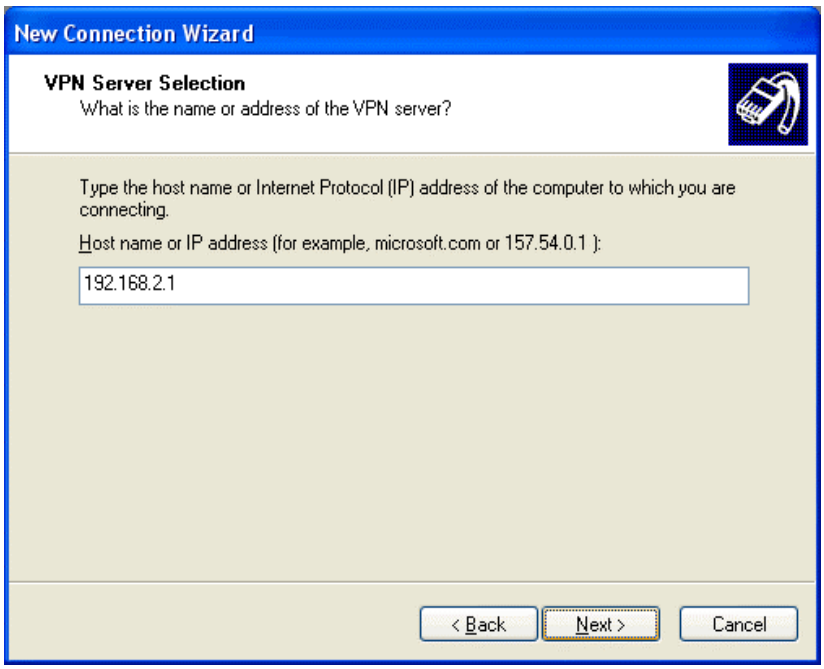
81. Click on **Connect to the network at my workplace**.
82. Click on **Next** button

83. Click on **Virtual Private Network connection**
84. Click on **Next** button



85. Enter the name of this VPN connection. In this case, the name is To VPN router.
86. Click on **Next**

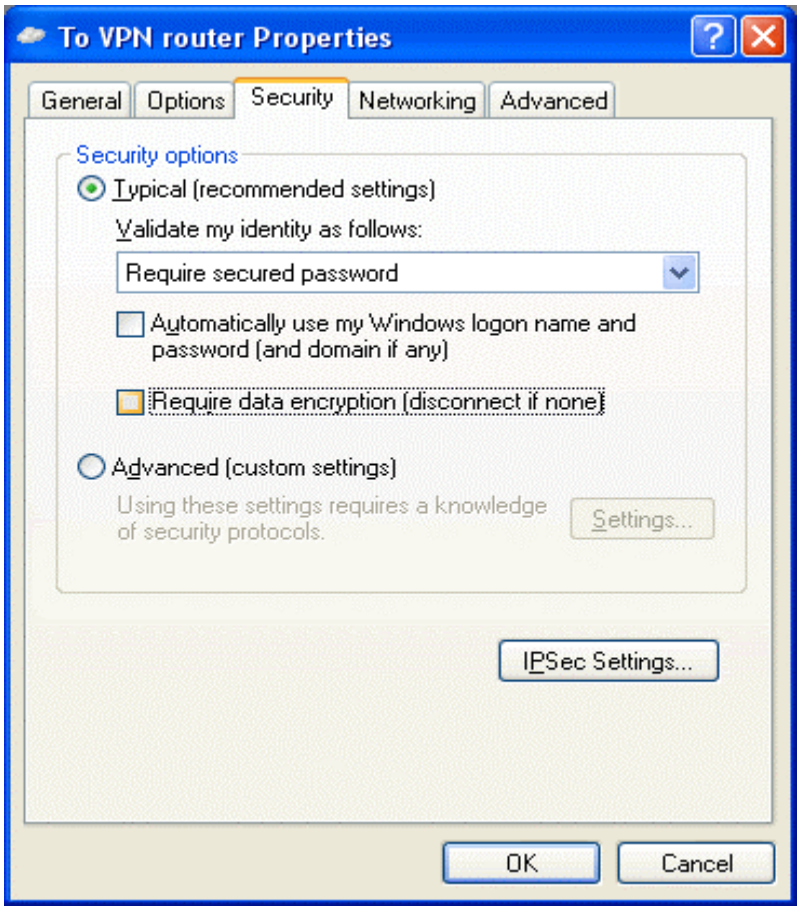
Then, enter Matrix's domain IP address. If you're using static IP and already applied for a domain name, or if you are using dynamic IP with DDNS domain name applied and activated built-in DDNS function in this router. Then you can enter the domain name in this section.



87. Enter the WAN IP address or domain name of your VPN router.
88. Click on **Next**

89. If you would like this connection to appear on your desktop. Please do so by ticking the check box of **Add a shortcut to the connection to my desktop.**
90. Click on **Finish** button.

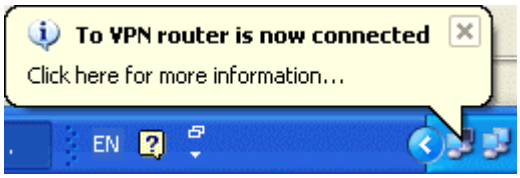
91. Click on **Properties** button



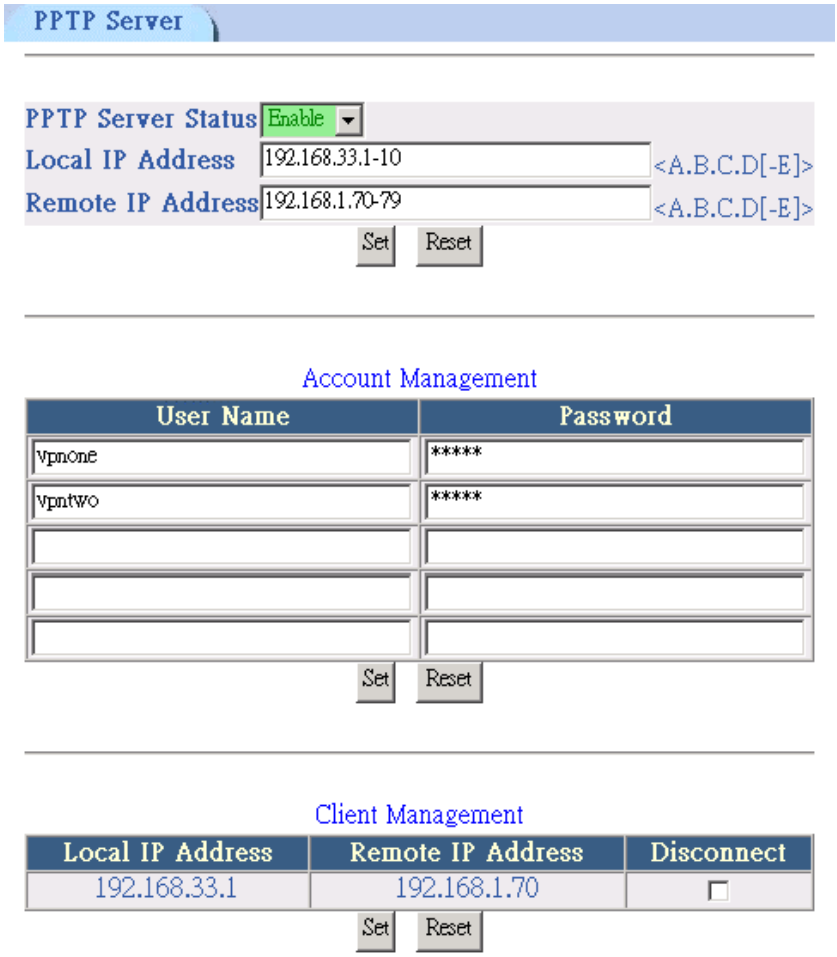
92. Un-tick or cancel the check box of **Require data encryption** (disconnect if none)
93. Click on **OK**

94. Enter your **User name** and **Password**
95. Click on **Connect** button.

Once the successful connection is made, your WINXP connection logo will appear on the bottom of your Window to confirm the successful connection.

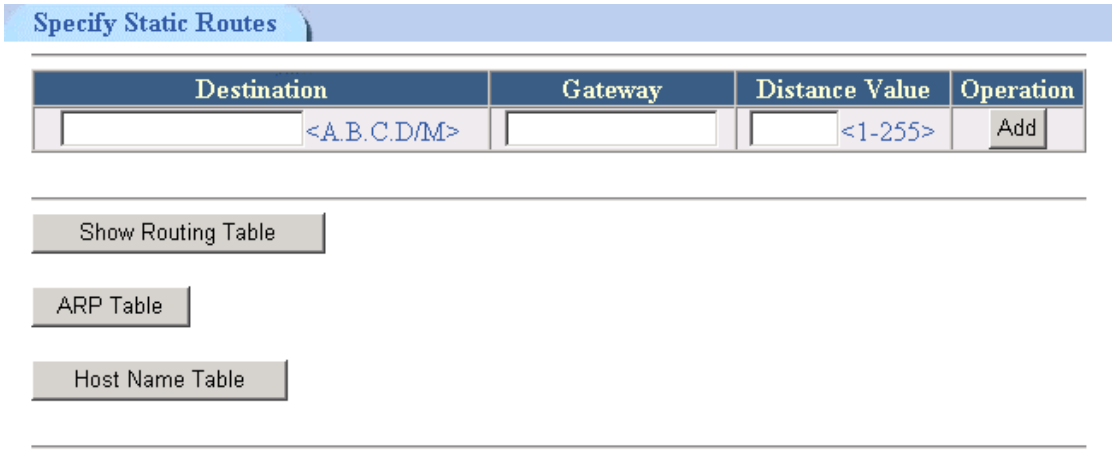


You can also access to your web-based management page from your router and go to PPTP server setting page. From the bottom of the page, you will see the current PPTP VPN connection status from **Client Management** section.



On **Client Management** section, if Disconnect check box is ticked and click on Set, it will allow PPTP disconnection. If the Reset button is clicked, PPTP disconnection will be cancelled and the PPTP will be reconnected again.

Static Route

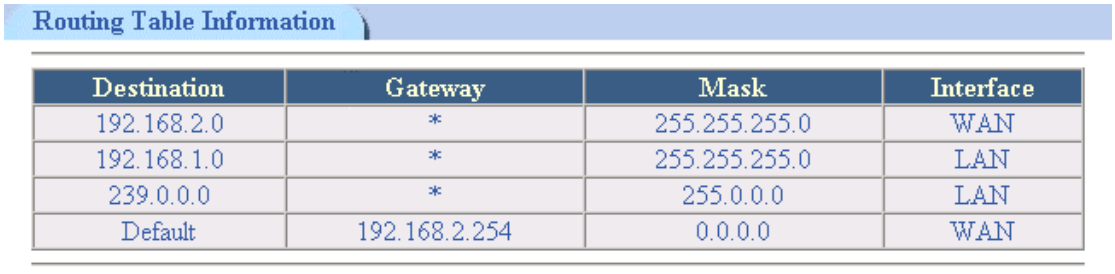


If the router is connected to more than one network, it may be necessary to set up a static route between them. A static route is a pre-determined pathway that network information must travel to reach a specific host or network. Click on Static Route from main menu to view the current static routing information.

Enter **Destination IP address** of the remote network or host which you wish to assign a static route. Enter the **Gateway IP** address of the gateway device that allows for contact between the router and the remote network or host. Enter **Distance Value** from 1 ~ 255 and click on **Add** to confirm your setting.

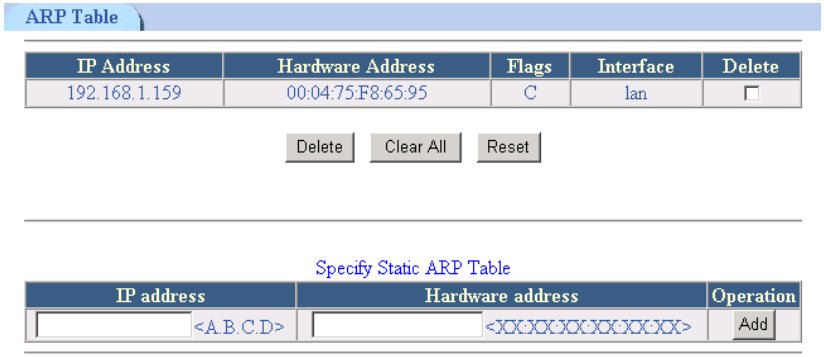
Show Routing Table

Click on **Show Routing Table** to check your new static route information.



Show ARP Table

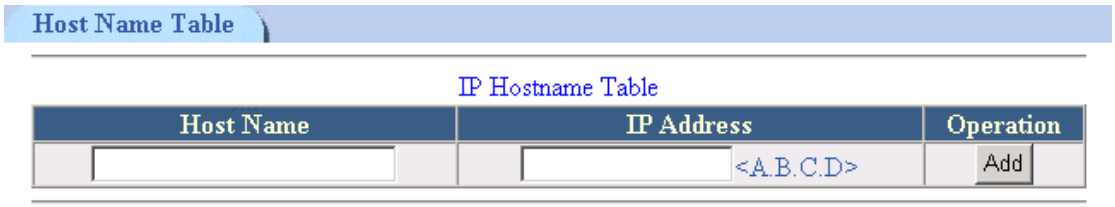
Before all packets are transmitted, the MAC address of the receiving host should be identified. Therefore, Matrix can auto learn the MAC address and the mapping IP. See below for the translation table.



Host Name Table

It is the mapping of host name and its IP address respectively.

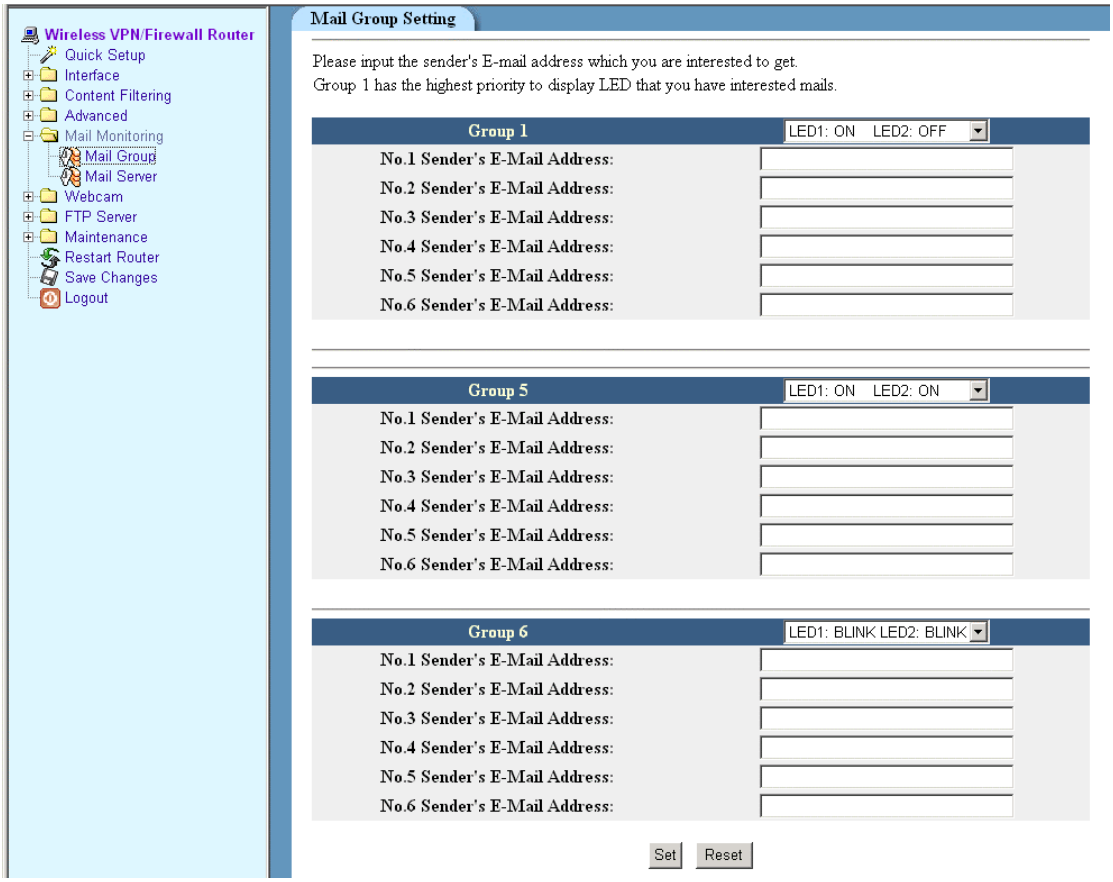
The default is blank.



Chapter 7: Mail Monitoring

In this section, Mail Monitor is used to monitor the incoming mails. Users can pre-define Mail Group and Mail Server for some specific people in advance. When these senders sent mail to you, the E-mail LED at the front panel will flash in accordance of your setting. You DO NOT need to open Outlook or your email system in order to know who has sent you E-mails.

To set up E-mail of your friends or customers who you wish to monitor, please take the following steps:

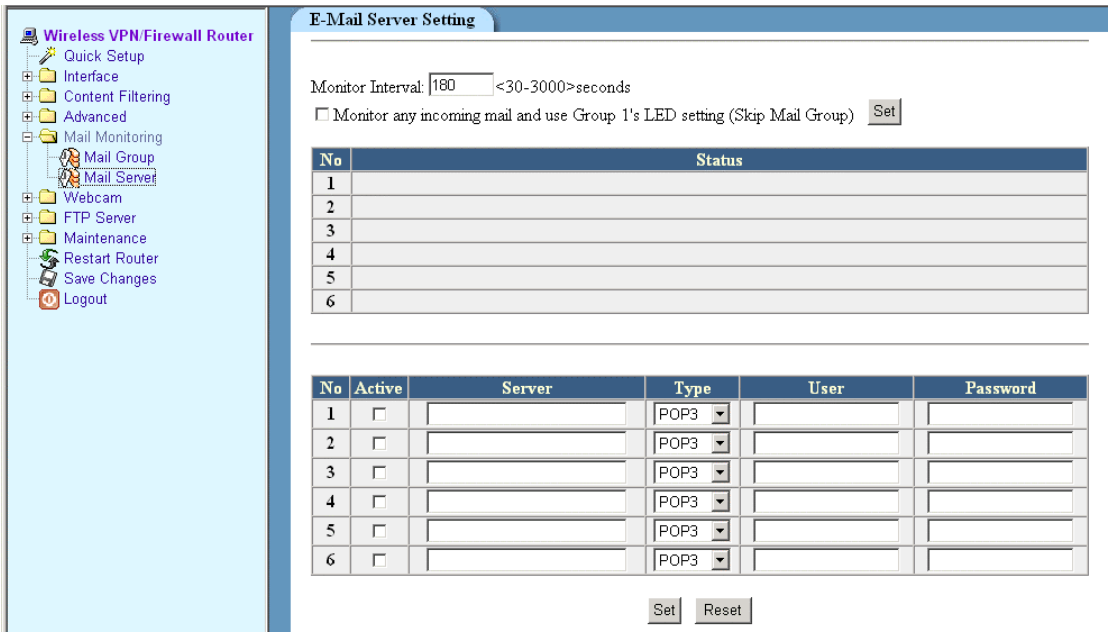


1. Select **Mail Monitor** utility from main menu and click on **Mail Group**.

2. In Mail Group setting, you have option to configure up to six different Email Server groups with six people in one group.

NOTE: Two email addresses from different Email Server must not exist in the same Mail Group.

3. After enter sender's email address, please select LED display for this sender. Click on **Set** to confirm the setting.
4. Go to **Mail Server** to configure Email Server Settings.

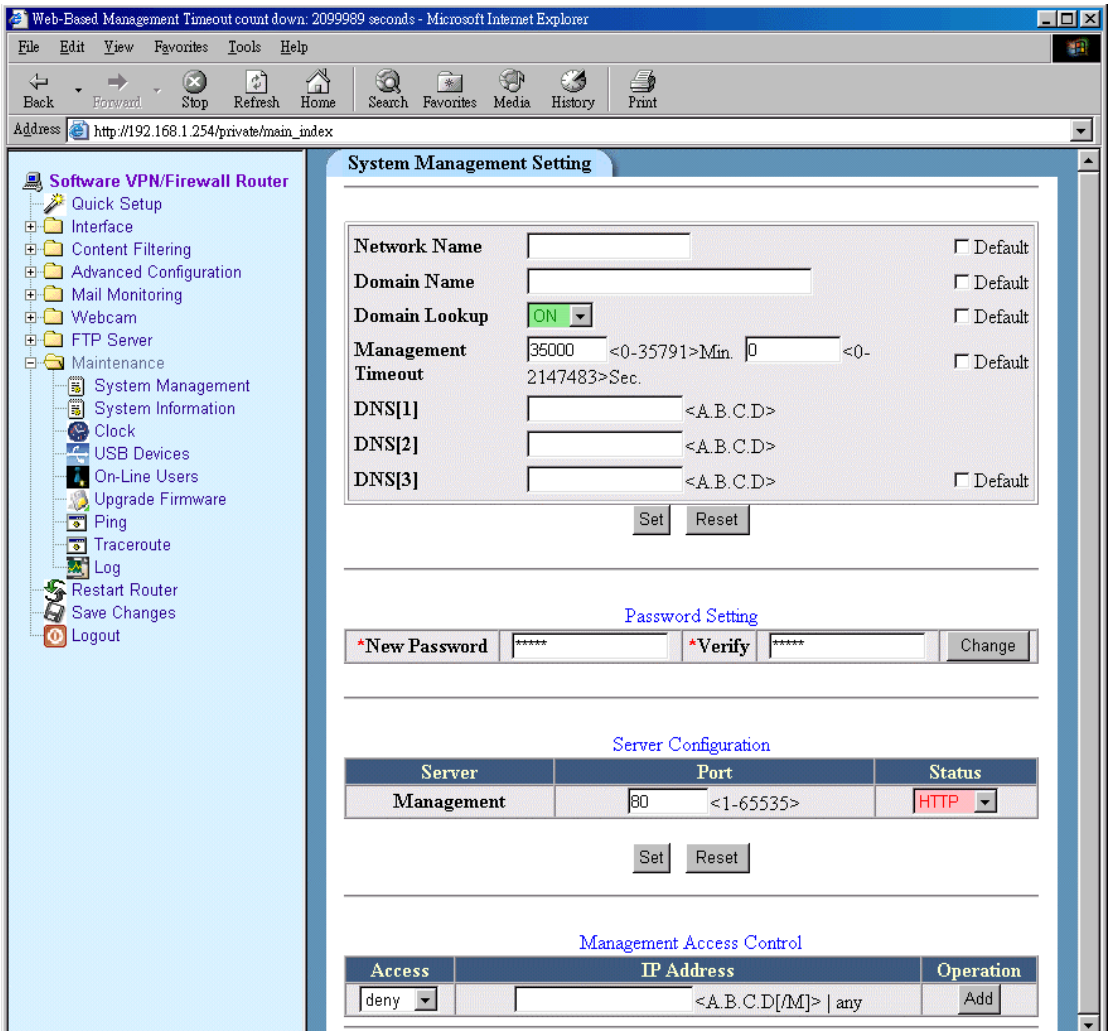


5. Define the value for **Monitor Interval.** The router will check the specific Email server based on this pre-defined time interval.
6. You have option to monitor any incoming mails and use Group 1's LED settings. If you wish to do that, please check the box and click **Set**.
7. Enter Email server IP address or domain name, user name and password.
8. Select Mail Server type and tick on **Active**.
9. Click on **Set** to confirm the setting.

Chapter 8: Maintenance

System Management

System management Utility provide user to configure router's system settings.



System Settings

Network Name — You can set up a name for your router in this field.

Domain Name — You can set domain name of where your router is located here. If you did not apply the domain name from your ISP, please leave it blank.

Domain Lookup This utility provides the function of searching domain from DNS Server you configured. Default is **ON**.

Management Timeout

This section allows you to set the time interval of when Web-Based Management should logout automatically when it is not in use. The default value is 5 minutes.

DNS Server When the domain name is defined, this is where the router should search for DNS Server. Please input the DNS Server IP address provided by your ISP.

Password Setting Here is where you set your password when login into Web-Based Management. Default password is **admin**

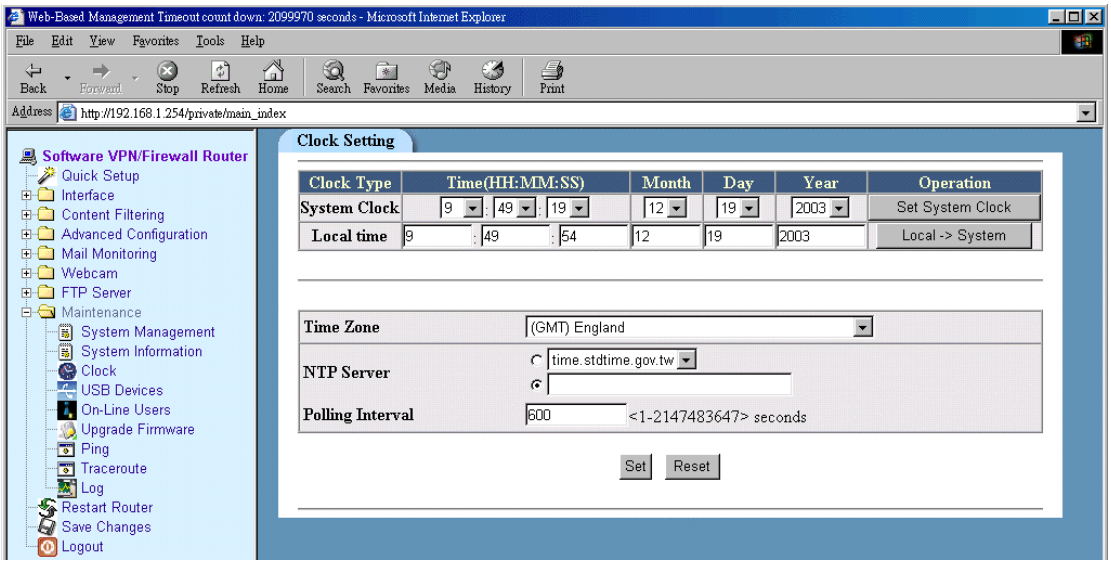
Server Configuration Here is where you can set the connection port for Web-Based Management. Based on security concern, it is recommended to set the port number between 5000 ~ 65535 in order to prevent intrusion attack. You can also select HTTPS from Status field in order to increase the security.

Management Access Control

You can define Accept or Deny for specific IP or domain where the Web-Based Management is login. Default is **Accept.**

Clock

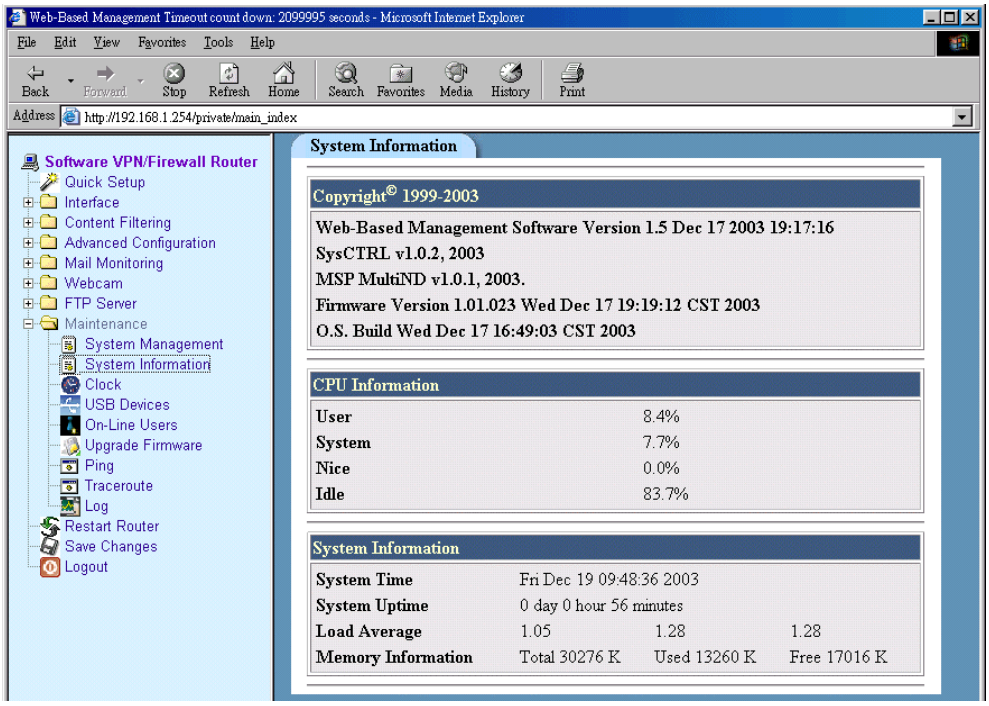
In this section, you can set Local Time and System Clock for your router. Select time values in every time fields by scrolling down the time menu. Click on **Set System Clock** or **Local -> System** to confirm your time settings.



NTP Server allows you to set IP address of NTP server to synchronize your system time. Select **Time Zone** at your region and appropriate NTP Server. Click on **Set** to confirm the settings.

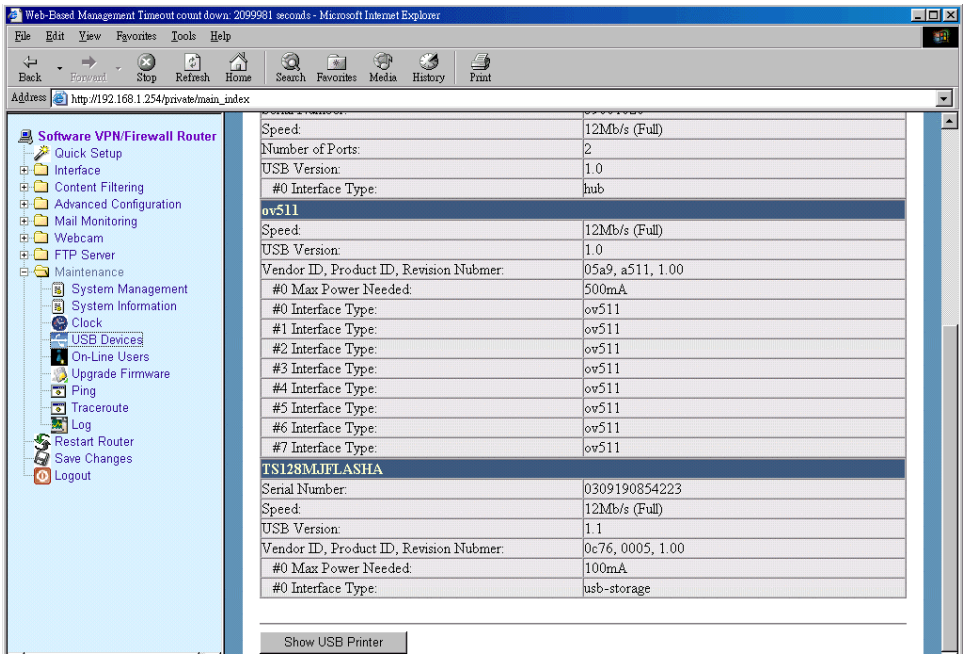
System Information

In this section, you are able to view the current status of **Firmware version**, **CPU information** and **System information** of the router.



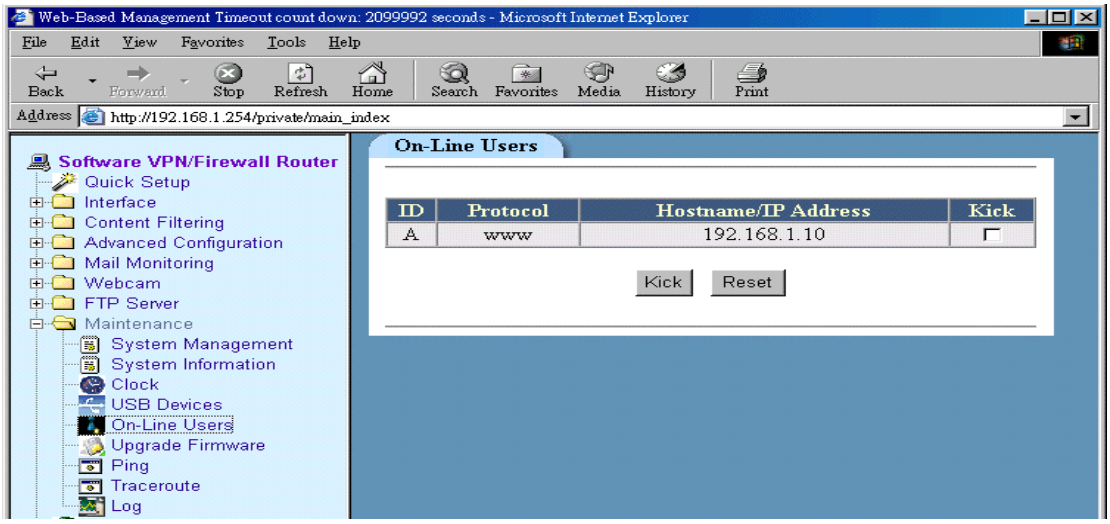
USB Devices

In the section, you are able to view and check the status of any USB device connected to the router. If an USB device is connected to the router and it does not show on this section, it means the USB device is not recognize by the router or it has compatibility problem.



On-Line Users

In this section, you are able to view and check all online users within your network group. You can force disconnection for some particular users by ticking on **Kick** box and click on **Kick** to confirm your setting.

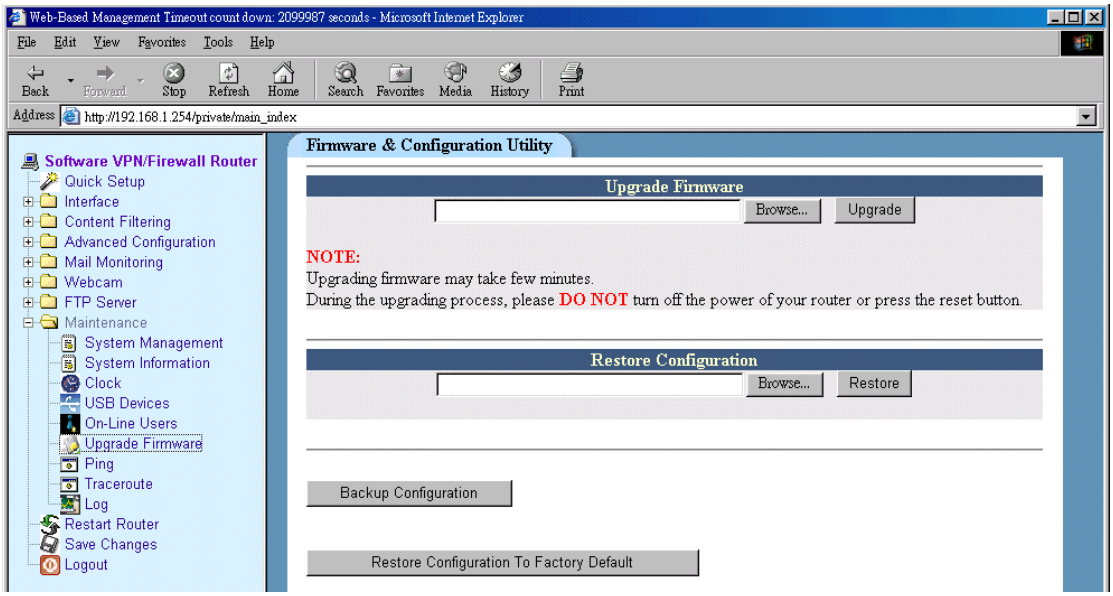


Firmware Upgrade

New firmware can be upgraded anytime through this utility. Please make sure you had obtained new firmware from your supplier and save it in your hard disk.

Important:

Before upgrading new firmware, please REMOVE all USB devices that connected to your router and reset your router to factory hardware default by press down the reset button for 5 seconds. Re-login the web-based management page and start the firmware upgrade from the following instructions.



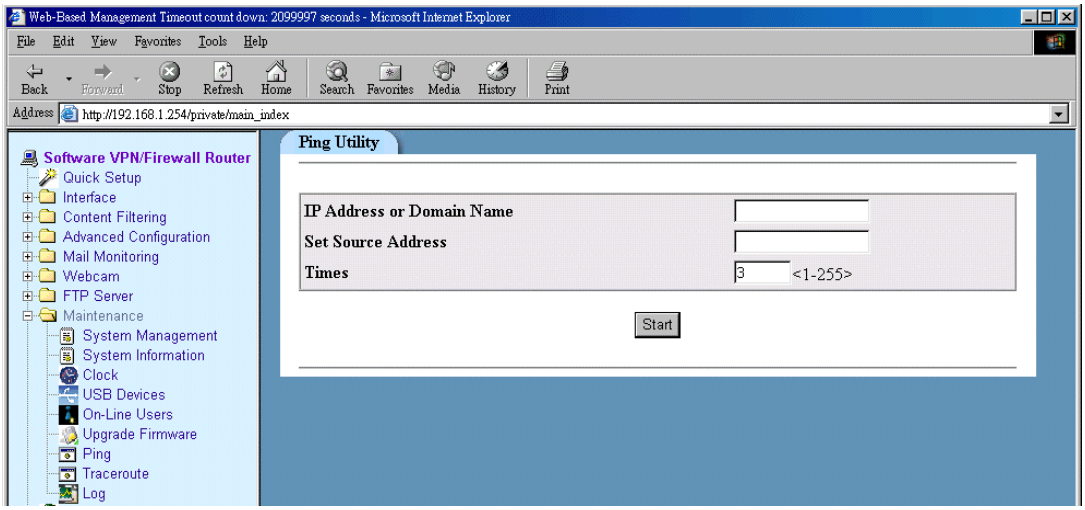
1. Select **Maintenance** from main menu and click on **Upgrade Firmware**.
2. Before upgrading new firmware, if you would like to back up the configuration, please do so by click on **Back-up configuration**.
3. Click on **Browse** to obtain the new firmware from your hard disk.
4. Click on **Upgrade** to start firmware upgrade.
5. Firmware upgrading may take few minute, wait until the pop-up window appear for the next instruction.
6. After the firmware has successfully upgraded, please use paper clip to press **Reset Button** for 5 seconds in order to clear old configurations.
7. Re-login Web-Based Management to reconfigure your network.

Restore Configuration

1. From Restore configuration section, Click on **browse** to search your back-up file from your hard disk.
2. Click on **Restore** to restore your previous configurations.

Ping

You can use this utility to determine whether a particular IP address or domain is online. It is used to test or debug a network by sending out a packet and waiting for a response.

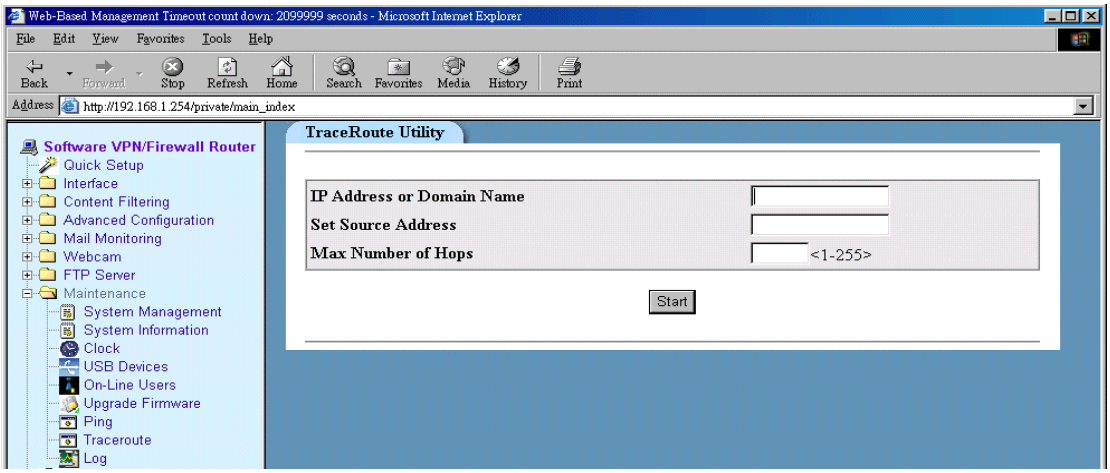


IP Address or Domain Name	In this field, enter the IP you wish to Ping
Set Source Address	Enter the source address
Times	Enter the value of how many times you wish to Ping

Click on Start to Ping

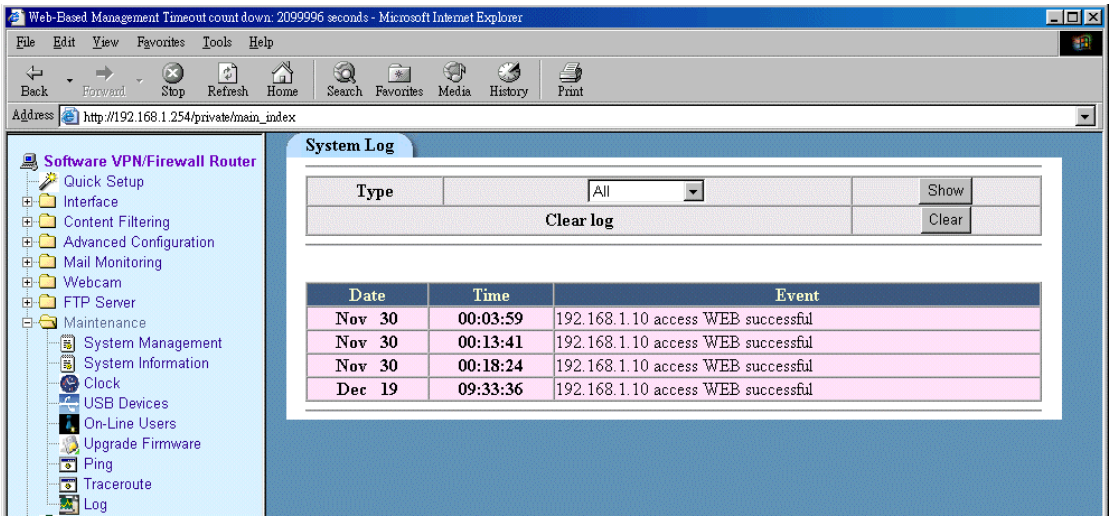
Trace route

You can use this utility to trace the routing path for a particular IP address or domain.



Enter IP address or domain name you wish to trace.
After enter Source Address, please enter maximum number of Hops should be carry out. Click on **Start** to begin.

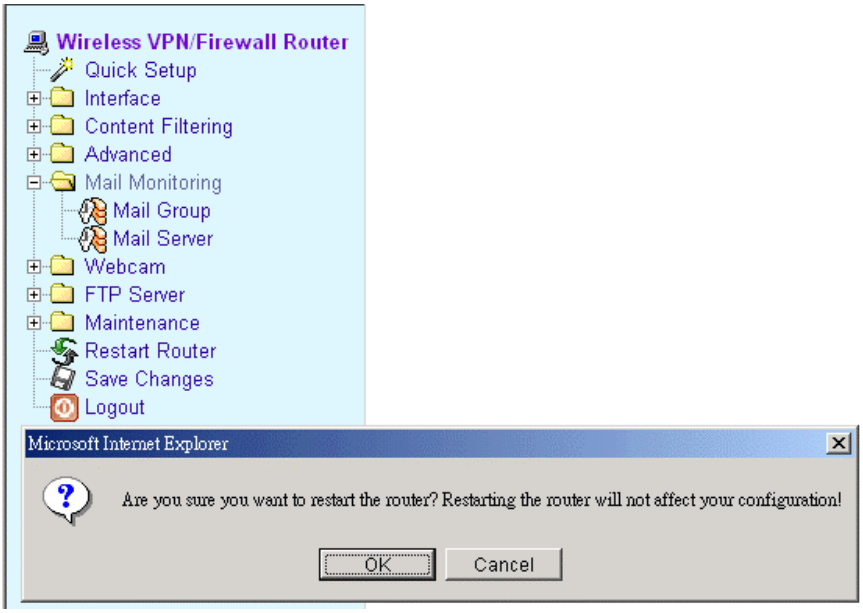
Log



The log feature provides you with a log of all information regards to firewall, system, incoming/outgoing IP address and content filtering of the router. Please select what type of log file you want to view and click on **Show** to view all log files. Click on **clear** if you wish to delete the log.

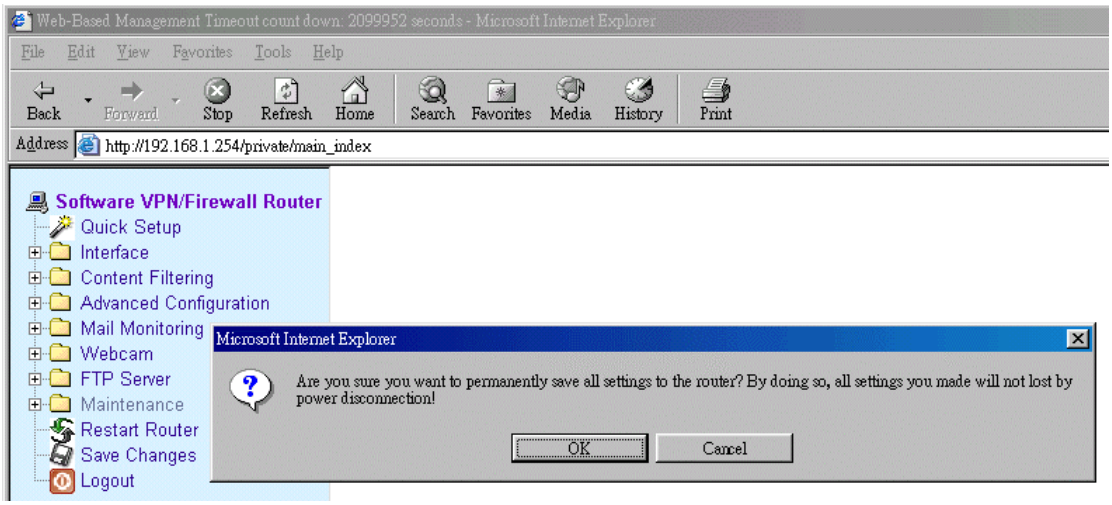
Restart Router

If you had entered the wrong configuration while setting up your router or other utilities, you can always reboot your router by clicking Restart Router icon.



Save Changes

It is strongly recommended to click on **Save Changes** when every time the Web-Based Management is logged out after configuration. By performing this action, the router will ensure all configurations and settings will not lost even when the router is not powered.



Logout

Clicking on **Logout** to exit Web-Based Management page.

Chapter 9: USB 2.0 Utilities

Multimedia VPN/Firewall Router has built-in 4 USB 2.0 ports for easy plug and share with wide range of USB devices. There is no need to install driver for these USB devices. Simply plug and Share to enjoy the fun and benefits from the following utilities.

1. **Printer** Up to four printers can be shared to your network at the same time

2. **USB Web Cam** The router has built-in Web Cam Server. By connecting web camera to the router, it allows user to monitor their home or office from remote locations. Motion Detection function also been built-in and allows user to use web cam to detect any motion at their home or office and send email alert with captured images.

3. **FTP Server** By connecting USB HDD, USB Flash, MP3 Player, USB Media Reader or Digital camera to the router, user can easily set up a FTP Server to share or download files for local or remote users.

The following table shows the MAXIMUM number of each USB device you can connect to the router in any combination of up to 4 ports:

Printer	WebCam	USB HDD	Flash Drive	MP3 Player	Card Reader	Digital Camera
4	1	1	2	2	2	2

Printer Server

Follow the following steps to how to setup your PC to connect to a print server.

When installing print server, you need to know its IP Address and Port Number. IP Address is the LAN IP address (IP Address of the printer). Port Number is 9100. If you are installing more than one print server, the second Port Number will be 9101, and so on.

Please have the appropriate “printer driver” ready, either on a floppy, or a network shared drive. If your printer is not included in the default list, use the “have disk” method after you’ve gone through the steps below. In some situations, you may have to install the printer driver first as if it were hooked up directly to LPT1.

For Windows 98/ME, AXIS monitor (or any other similar products) has to be installed. The reason is that Windows 98/ME does not support TCP/IP printing. You can download AXIS monitor from the following site:
ftp://ftp.axis.com/pub_soft/prt_srv/utility/printmon/latest/setup.exe

The general setup steps are summarized below and the details are at the later pages.

If you are running Windows XP

Start -> Control Panel -> Printers and Faxes -> Add Printer -> Local Printer (check off Auto Detect PnP) -> Next -> Create New Port -> Standard TCP/IP Port
IP Address = IP Address of the Printer
Port Name = PrintSrv (or any name you wish)
Custom Settings -> Raw Port
Raw Port = 9100

If you are running Windows 2000

Method A

Start -> Settings -> Printers -> Add Printers -> Local Printer -> Create New Port ->Choose Standard TCP/IP Port
IP Address = IP Address of the Printer
Port Name = PrintSrv (or any name you wish)
Port Number = 9100
Custom Settings -> Raw Port
Raw Port = 9100

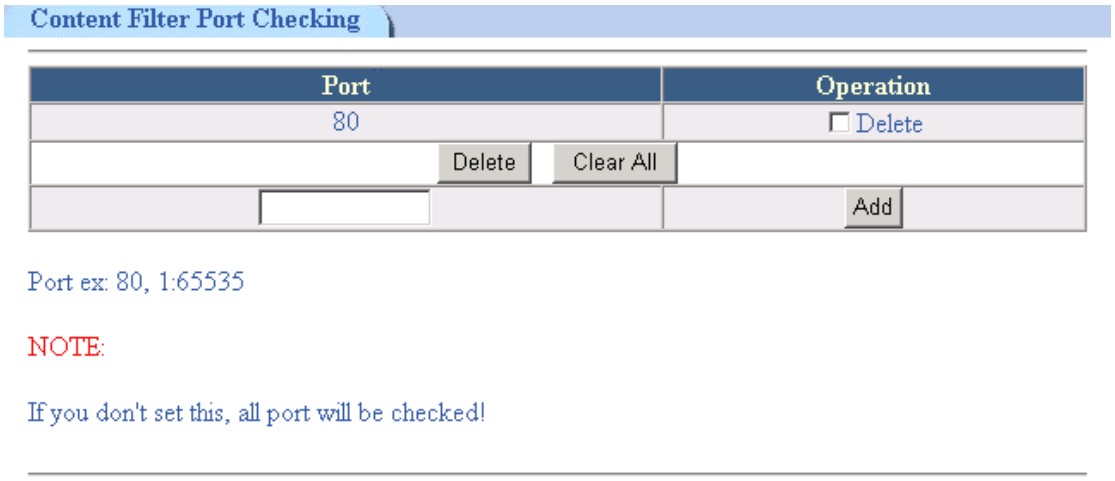
Method B

Start -> Settings -> Printers -> Add Printers -> Local Printer -> Create New Port -> Choose AXIS Port -> Choose RAW TCP/IP Port
IP Address = IP Address of the Printer
Port Number = 9100

any damage to you. Enter the range of **IP addresses** and the **Port Number** in the fields. Click **Add**.

Trusted IP has the highest priority. That means if there is a conflict between the rules in Trusted IP and URL Blocking (or Keyword Filtering or Port Checking), the rules under Trusted IP takes precedence of others.

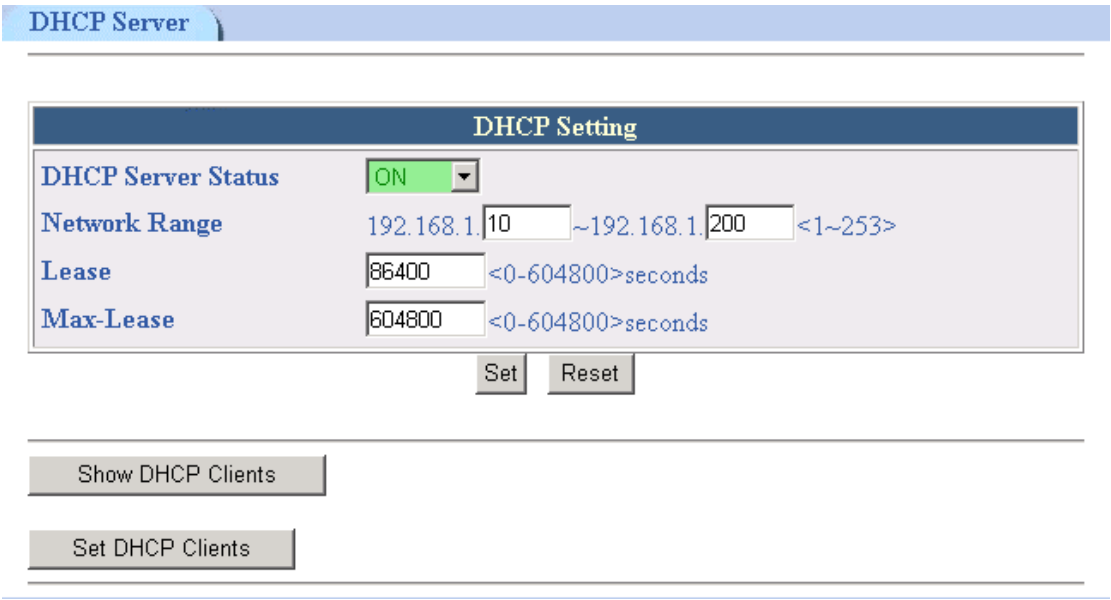
Port Checking



Enter the **port number** in the field and click **Add**. Ports entered will be scanned and checked for security measures. If nothing is entered here, all ports will be checked.

Chapter 6: Advanced Configurations

DHCP



A DHCP (Dynamic Host Configuration Protocol) Server automatically assigns IP addresses to each computer on your network. Unless you already have one, it is highly recommended that the router set up as a DHCP Server.

- **DHCP Server Status**

  Click ON to activate DHCP server; OFF to disable and Restart to restart the DHCP server. If the DHCP server status is OFF, click the Set button for it to be effective after changes. IF the DHCP server status is ON, click the Restart button and the new changes will be effective.

- **Network Range**

  Define IP range for DHCP server when issuing IP.

- **Lease Time**

  This is the default time duration that a DHCP client is able to keep the IP if the time duration is not specified.

- **Maximum Lease Time**

  DHCP clients can only request lease time smaller than this value. If the requested lease time is greater than Maximum Lease Time, this

is the default value taken by the system.

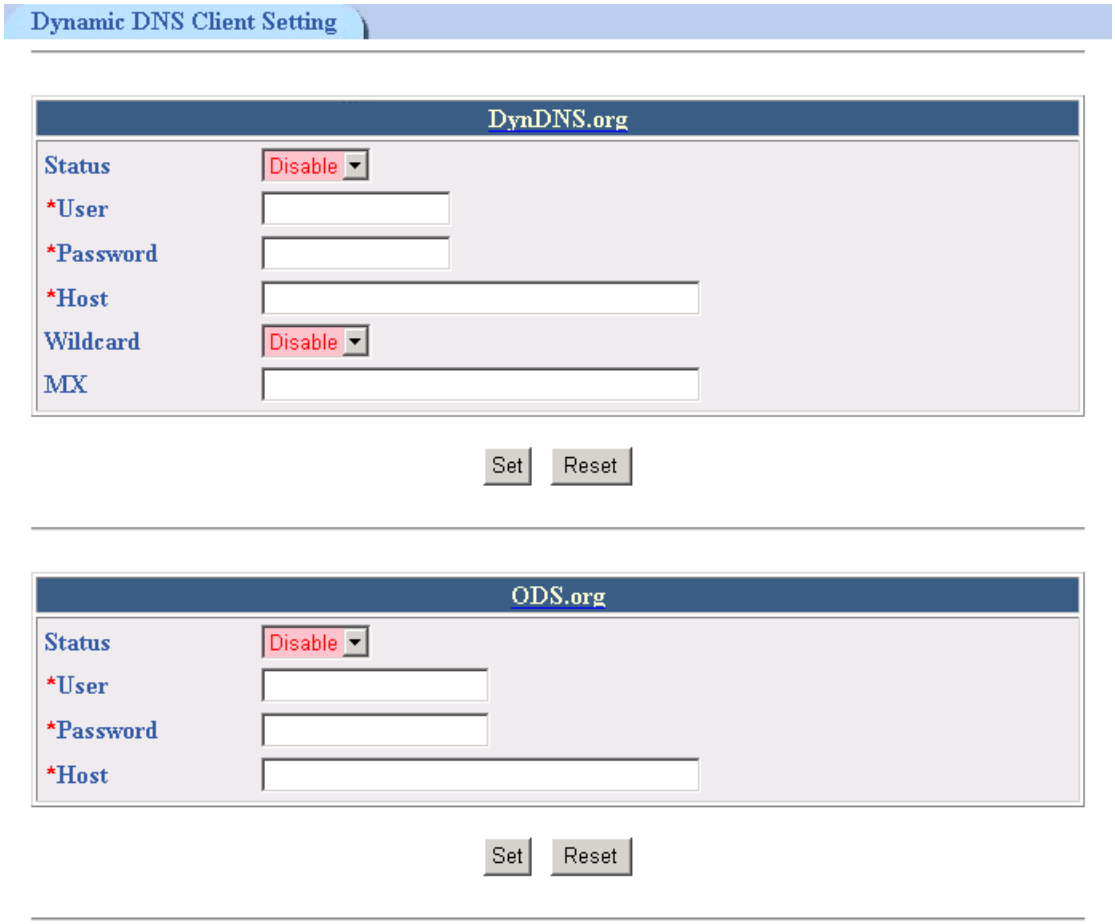
- **Show DHCP Clients**

  Click on this button to show the current DHCP client information

- **Set DHCP Clients**

  This function allows user to instruct DHCP server to assign IP address to a particular Mac ID in your network. Apart from assigning IP automatically, you can assign IP to specific device manually. Please enter the name of the device, its IP address, and the MAC address accordingly. The first three columns are mandatory. You can leave the last two empty. For servers that requires booting files from some other servers, make sure you enter its booting file and the TFTP IP address accordingly. After all the parameters are completed, click Add. To delete the rule, select Delete and then click the Delete box. Click Reset to undo the delete action

DDNS

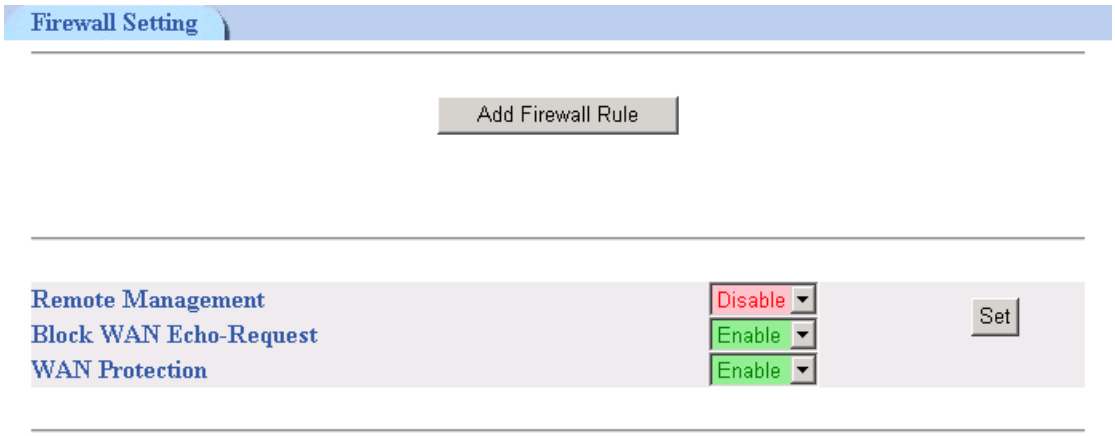


DDNS allows user to export host name to Internet through DDNS service provider. Each time the router is connect to Internet and get an IP address from ISP, this function will update your IP address to DDNS service provider automatically, so that any user on Internet can get access to Server behind it through a predefined name registered in DDNS service provider.

Multimedia VPN/Firewall router support the URL links to DynDNS.org and ODS.org. Move your mouse pointer on **DynDNS.org** or **ODS.org** and click. You can get access to free trail link to start with a free trail account.

After complete registration, please fill in all information in the fields such as **user**, **password** and **host name**. Select **Enable** from **Status** field and click on Set to confirm your settings. If you have an Email Server, please enter its IP address into **MX** field. Enable **Wildcard** to determines of domain name with wildcard is also redirected to your IP address.

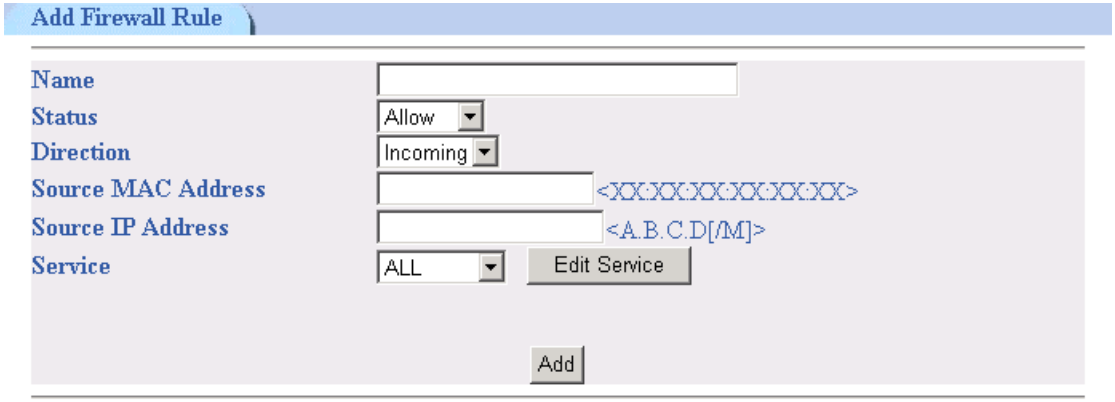
Firewall



A Firewall is a set of related programs, located at a network gateway server that protects the resources of a network from users from other networks. (The term also implies the security policy that is used with programs.) An enterprise with an intranet that allows its workers access to the wider Internet installs a firewall to prevent outsiders from accessing its own private data resources and for controlling what outside resources to which its own users have access.

In this Firewall section, it divides into three parts. There are **Add Firewall Rule**, **Remote Management**, **Block WAN Echo-Request** and **WAN Protection**.

Add Firewall Rule

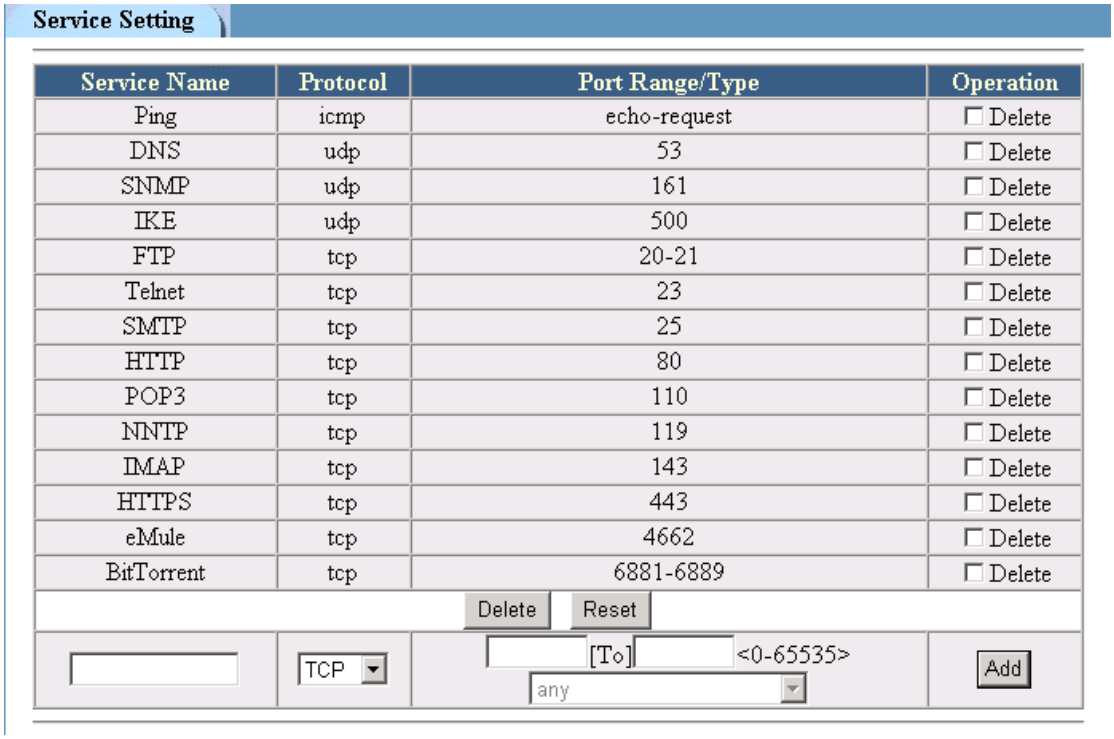


1. To configure Firewall, please select Firewall from main menu
2. To set a new firewall rule, please click on **Add Firewall Rule** button.

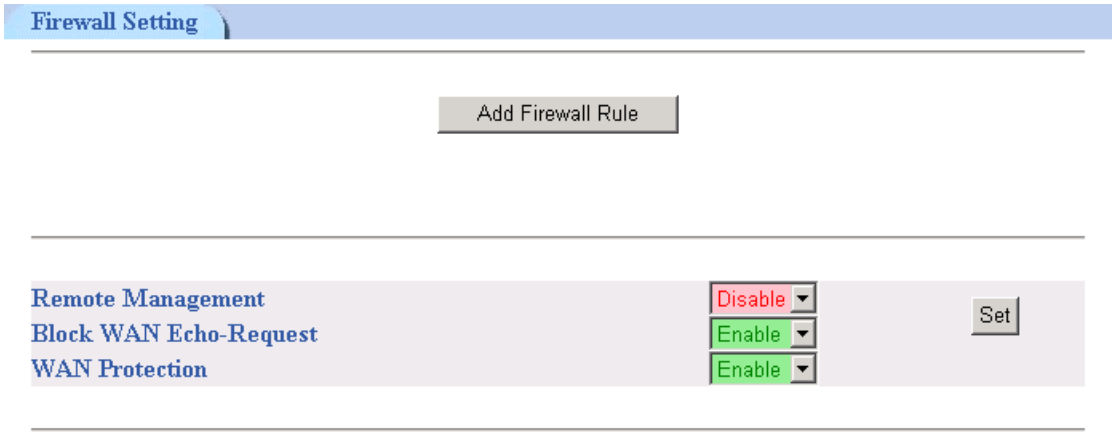
3. Enter **Name** for new firewall rule. The name can be anything as long it's can be identified by user who set the rule.
4. Pulling down **Status** window and select **Accept**, **Deny** or **Disable**.
5. Pulling down **Direction** window to select whether Firewall rule should apply to **Incoming** or **Outgoing** packets.
6. If you want to set Firewall rule to a particular MAC ID. You can enter MAC ID address into **Source MAC Address** window. This function is optional.
7. If you want to set Firewall rule to a particular IP address. You can enter IP address into **Source IP Address** window. This function is optional.
8. You can select a particular service to be activated with Firewall. You can find the range of services by pulling down **Service** window. Or you can customize your own firewall rule by click on **Edit Service** button.
9. Click on Add to confirm your firewall settings.

Edit Firewall Rules

Firewall Rules and policies can be customized depends on each individual's requirement. Simply click on **Edit Service** to access the page. Enter information such as **Service Name, Protocol** and **Port range / Type**. Your own firewall rules can be created upon your demand.



Remote Management



This Router is able to managed by WAN IP. When Remote Management is set on enable, user can enter Web-Based Management page by typing the router's WAN IP on web browser to manage the router.
Please take caution that once the Remote Management is enabled, the router may face the possibility of being attack by Internet hackers. You can reduce the risk of being attack by change connection PORT or use SSL for your connection. Also, make sure you frequently check the LOG records from LOG function in Web-Based Management.

To activate Remote Management, please select **Enable** and click on **Set** to confirm the setting.

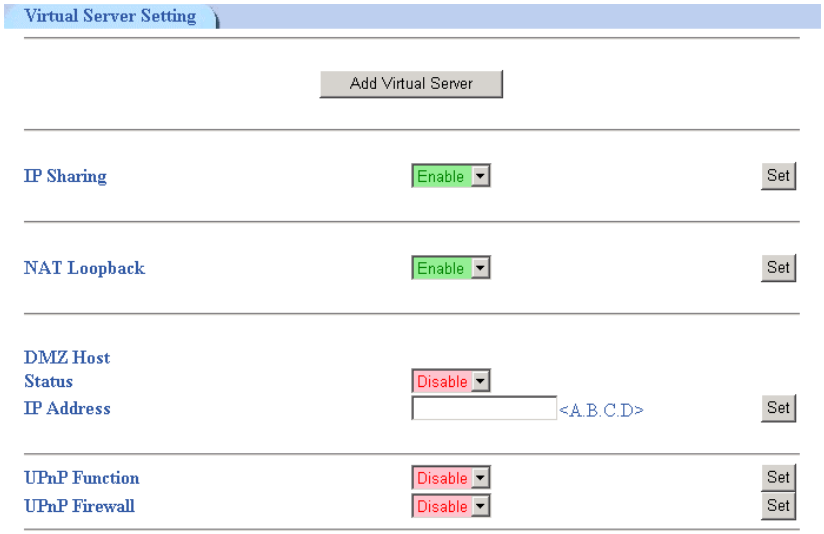
Block WAN Echo-Request

This Function allows user to set its WAN IP to stop giving response to outside request. When this function is enable, outsider will not get any response when they trying to PING the WAN IP. By doing this, you can avoid your router to be detected by hacker and prevent intrusion. The Default setting is **Enable**.

WAN Protection

When this option is enabled, the router will discard WAN packets that do not match the IP address specified. When IP Sharing is enabled, it is recommended to enable this option as well.

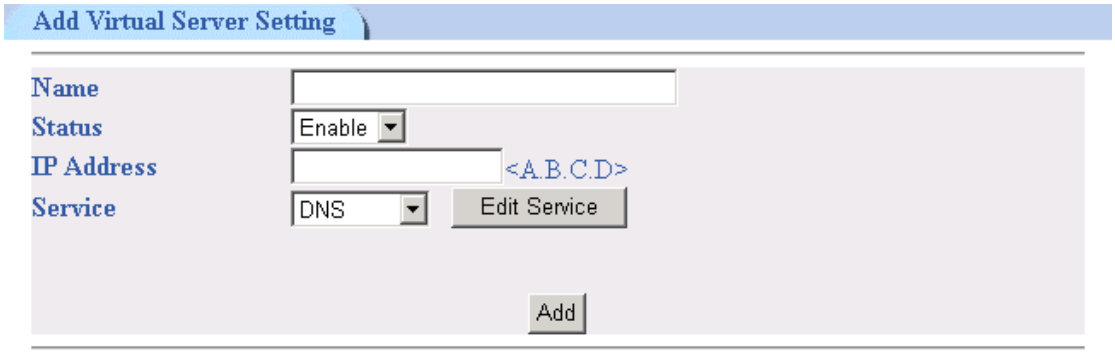
Virtual Server



Virtual Server

To make services, like WWW, FTP, provided by a server in your local network accessible for outside users, you should specify a local IP address to the server.

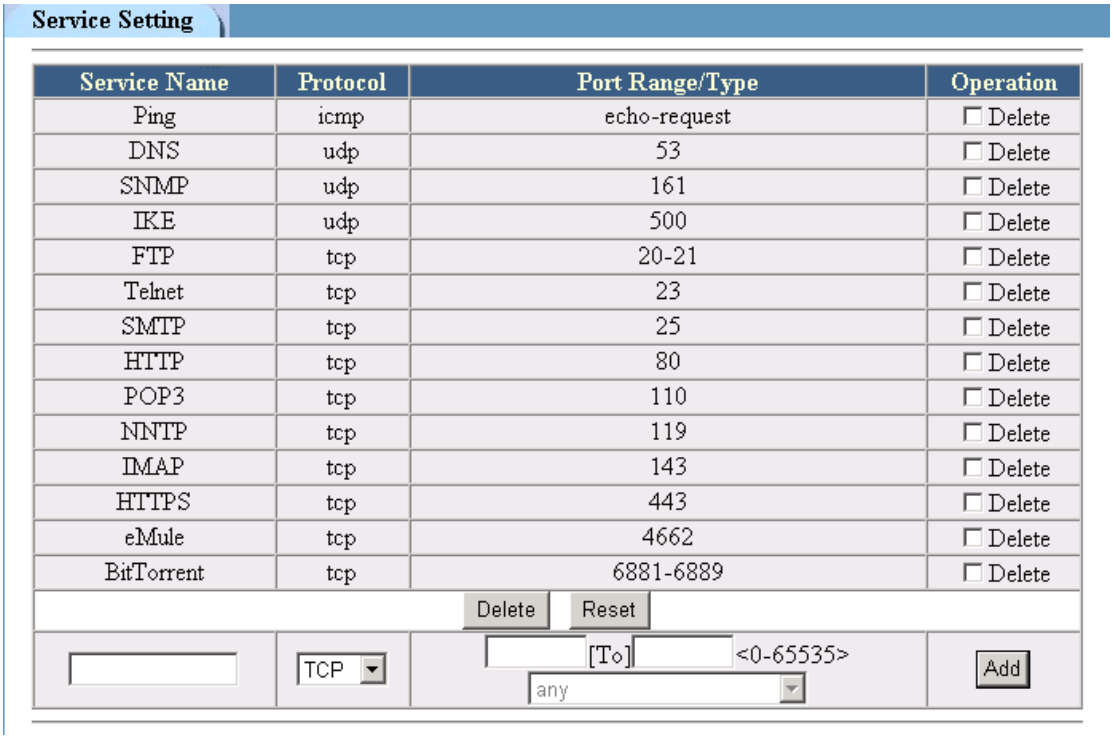
Please take the following steps to set up a Virtual Server for your router.



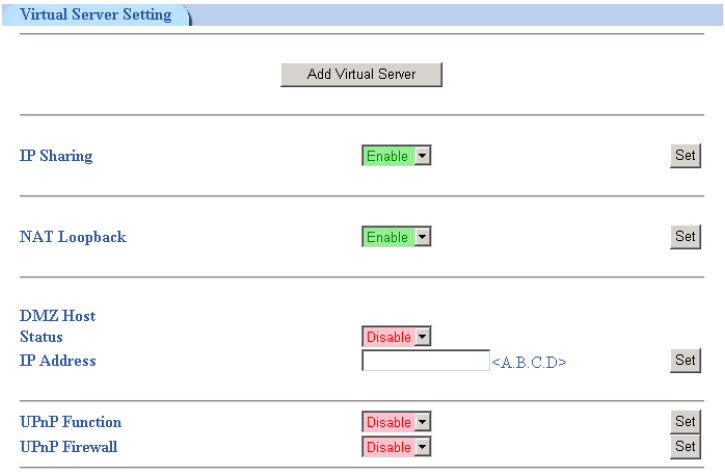
1. Select **Virtual Server** from the main menu and then click on **Add Virtual Server** button
2. Type in **Server** name. It can be anything as long as it is recognized by user
3. To activate Virtual Server function, click on **Enable** from Status box
4. **IP Address** – enter destination IP address that you like to redirect the matched packet to.
5. From **Service** window, select desired service of your demand.

If you could not find the desired service, please click on **Edit Service** button to customize your own settings. The screen will appear as below.

Edit Service



1. Enter your desired **Service Name**.
2. Select **Protocol** of your choice from pull-down window
3. Select port number or range of ports. Once the destination port of incoming packets matches the port within the port range, the incoming packets will be redirect to IP address specified in previous setting.
4. Click **Add** to confirm your Virtual Server Settings



IP Sharing

The host has to have a public IP in order to communicate with others on the Internet. Because of the fact of insufficient IP addresses, ISP provides dynamic IP address intead of static IP address. Dynamic IP address means that the IP address is different every time you log in. For those who needs a static IP, higher price has to be paid. Most home users or SOHOs use either one of them.

Since a public IP address is required to communicate with others on the Internet, IP sharing capability is required if there are more than one servers that wish to connect to the Internet. NAT (Network Address Translation) will do the address translation between LAN and WAN. Please enable IP sharing capability for situation described above.

NAT Loopback

This function allows the redirection of packets back to the virtual server when the request is initiated from the LAN side. To enable this function, please select **Enable** and click on **Set** to confirm your setting.

DMZ Host

The DMZ Host feature allows one local user to be exposed to the Internet to use a special-purpose service such as Internet gaming or video conferencing

1. Select **Enable** from **Status** window
2. Enter the **IP address** of PC which you would like to expose to Internet
3. Click on **Set** to confirm the setting

UPnP

UPnP allows users to connect their UPnP-enabled broadband router, print server and other devices right to the network with zero-configuration, meaning easier setup for installing the device on the network. The automatic discovery feature enables the device to obtain an IP address, present and describe itself to other devices and PCs on the network without having to install drivers, and then configure and use those devices.

UPnP Function	Select **Enable** and click **Set** to activate this service
UPnP Pass Through Firewall	Select **Enable** and click **Set** to allow UPnP pass through firewall

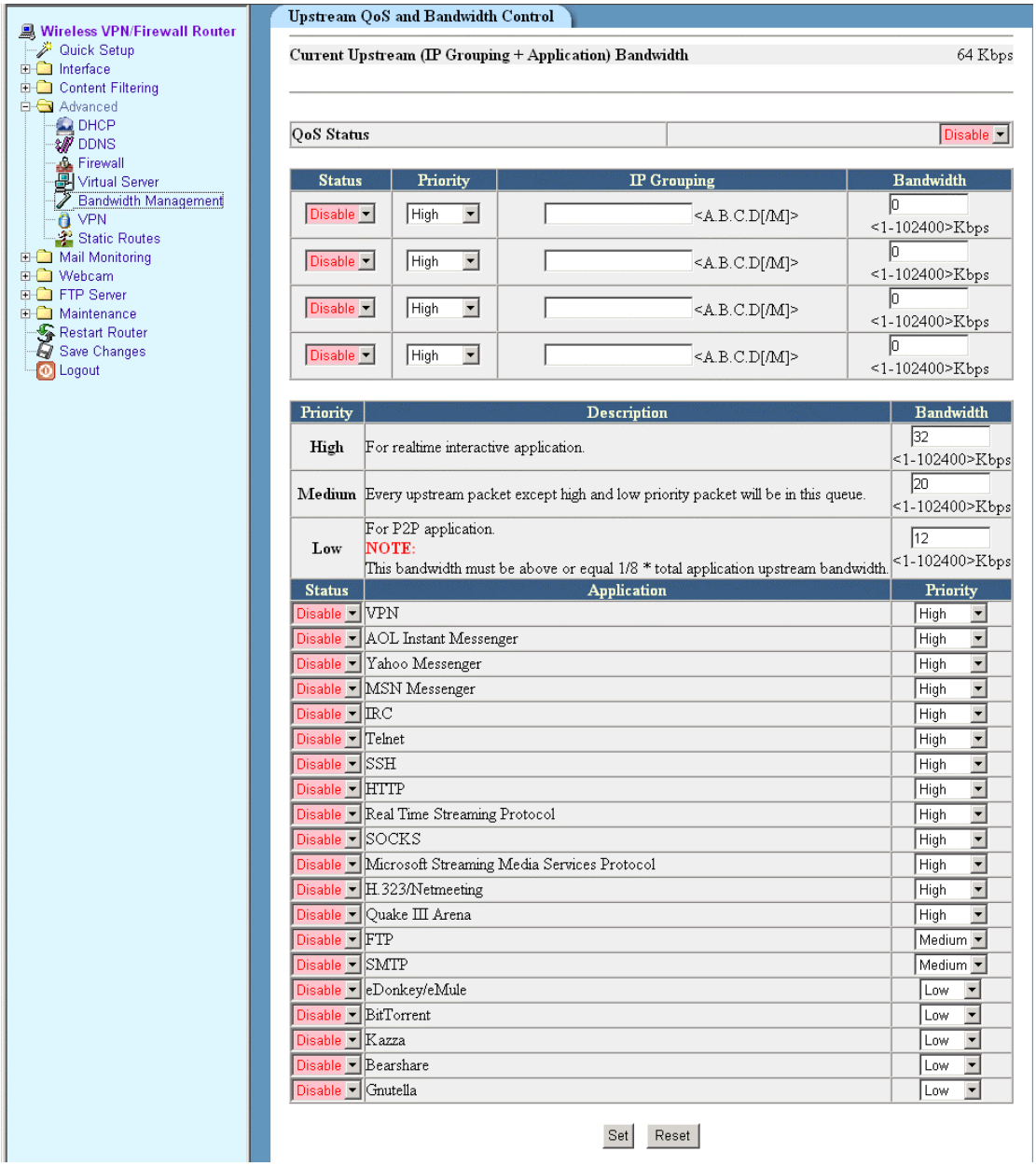
Bandwidth Management

QoS Bandwidth Management

Today, millions of people around the world share their MP3 music, Movies or other image files through freeware Peer-to-Peer platform such as E-Donkey, eMule, Kazza and so on. P2P application provides public platform of linking people around the world and share MP3, or movie files from each other's hard disk. When you're online and downloading music from other people's computer, at the same time, you are also sharing your music archive to other users on P2P network. When other online user downloading the MP3 from your hard disk, your Internet's upstream bandwidth will be eat up and that cause other user on your LAN network to have extreme difficult time to access Internet at very low speed due to lack of upstream bandwidth. With QoS Bandwidth management, this problem can be solved by pre-define the maximum upstream bandwidth allowed to each Internet application and set upstream packets in priority upon its importance.

Moreover, you are allowed to customize your own upstream QoS bandwidth management control depends on your bandwidth requirements. You are free to set what bandwidth priority you wish to give for each Internet application in respect of high, medium and low priority. With this outstanding bandwidth management feature, all users from LAN network will never have to worry about limited upstream bandwidth in broadband Internet environment.

There are two different solutions of efficiently managing the bandwidth. You can either managing the bandwidth by IP or IP group of your LAN network. Also, you can manage the bandwidth by giving priority queue according to its importance on each particular application of your choice.



Managing bandwidth by IP / IP group

In order to manage your network bandwidth more efficiently and to avoid some particular users on the LAN network is taking too much bandwidth by running heavy loaded applications, you're allowed to assign bandwidth priority to one or more users on your LAN network according to its importance.

To configure the settings, please take the following steps:

1. Go to **QoS Status** pull-down window and select **Enable**.
2. Enter IP address or IP group of LAN user you wish to manage and assign their priority of importance.
3. In each section of IP group QoS setting, you are required to enter bandwidth value in each section. **Please note the sum of total bandwidth in each section should not excess the total upstream bandwidth provided by your broadband service provider.**
4. Click on **Set** to confirm the settings.

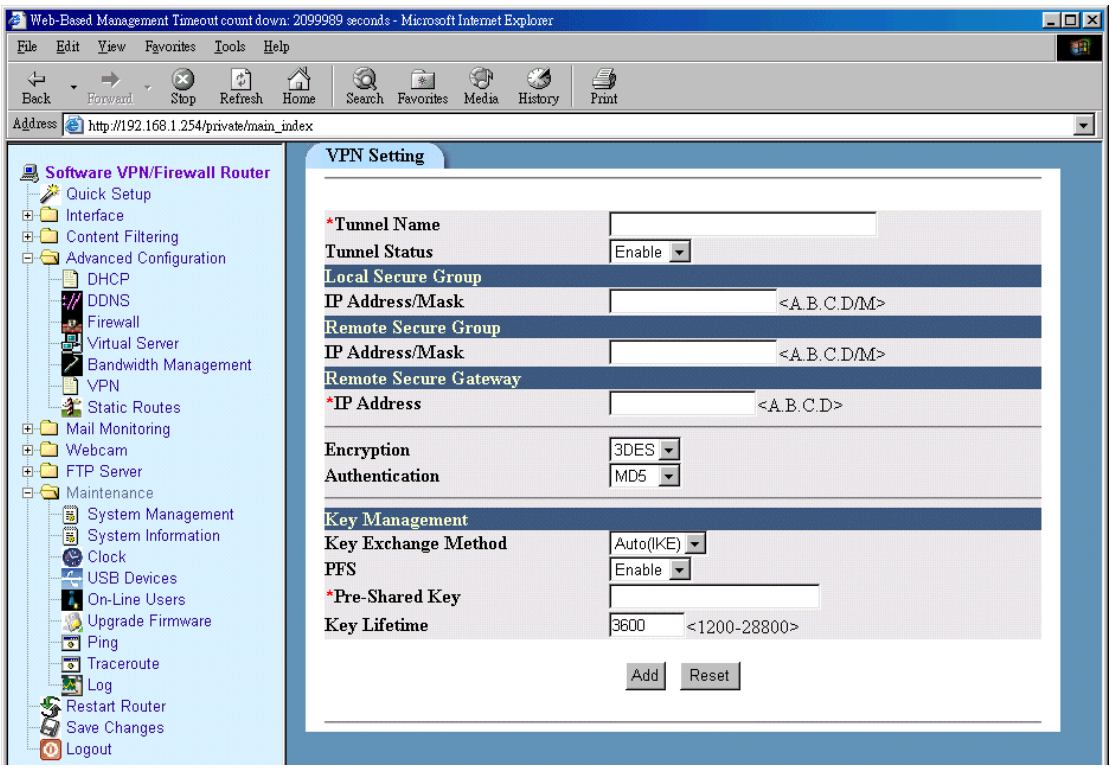
Manage bandwidth by applications

To manage your network bandwidth by particular application, please take the following steps

1. Select **enable** from **QoS status** pull-down window.
2. You need to know the maximum upstream bandwidth is allowed for your Internet connection provided by your ISP.
3. For each priority queue, you need to assign the upstream bandwidth value into each priority queue according to its importance from high to low. Please make sure all values sum up from each priority queue is equal to the total upstream bandwidth provided by your ISP.
4. From each priority queue, you need to select what applications you wish to include into QoS bandwidth management. You can do it by select enable or disable from the pull-down box beside each application.
5. After the selection, you need to decide what priority should be given to the application you selected. All P2P applications has been given the lowest priority and fixed as default.
6. Click on **Set** to confirm your settings.

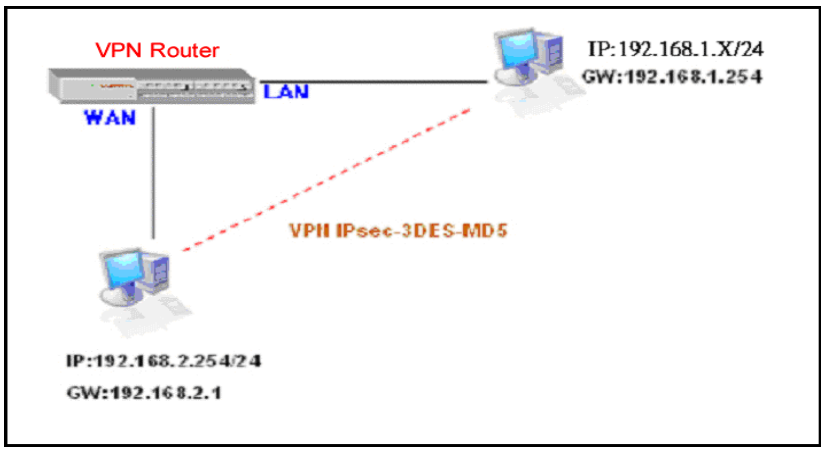
VPN

Virtual Private Networking (VPN) is a security measure that basically creates a secure connection (tunnel) between two remote locations on public Internet environment. This router unit has provided you with two kinds of VPN techniques. One is IPSec (IP Security Protocol) VPN and the other is PPTP (Point-to-Point tunneling) VPN. PPTP VPN provides Tunneling technique and IPSec provides tunneling, authentication, and encryption technique.

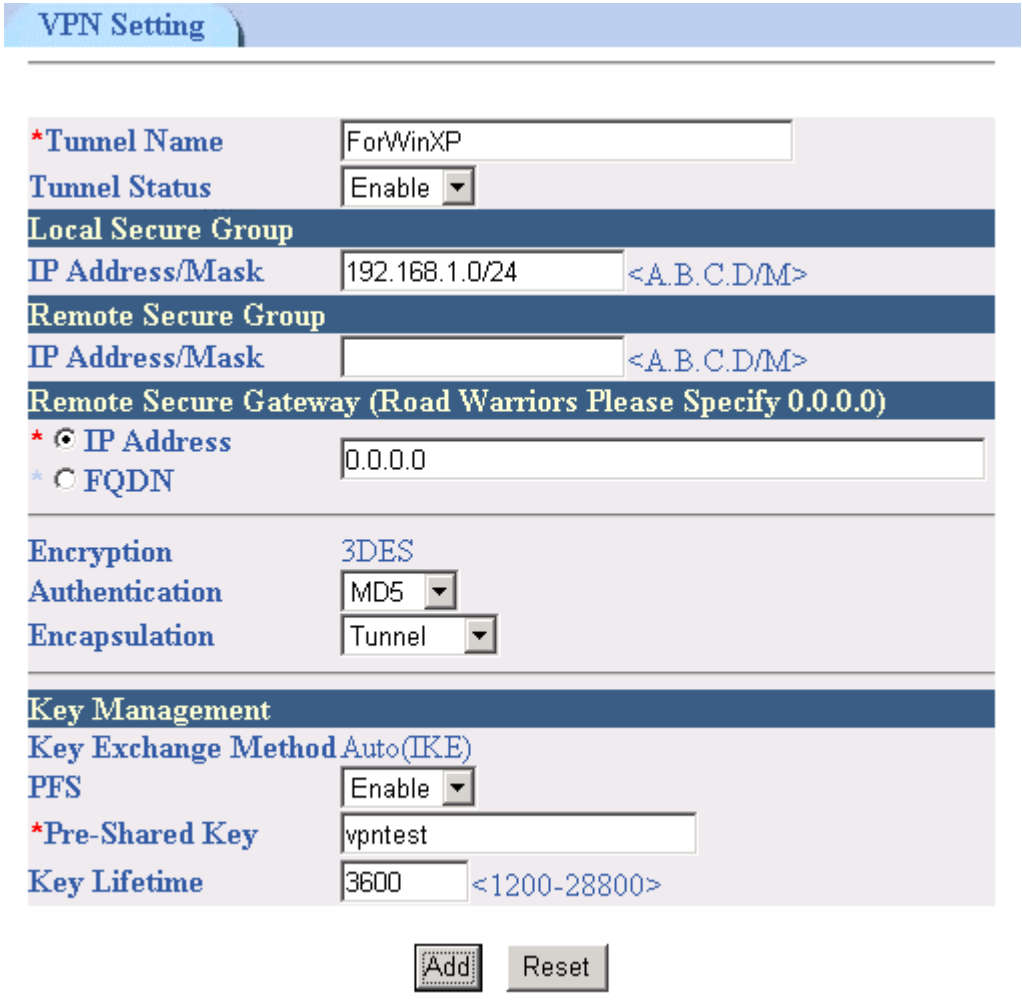


IPSEC

IPSec provide tunneling, authentication, and encryption technique so it ensure your data is safely transmitted on Internet without been attack by hackers. In order to create a secure VPN tunnel or channel between two endpoints by IPSEC, please take the following steps.

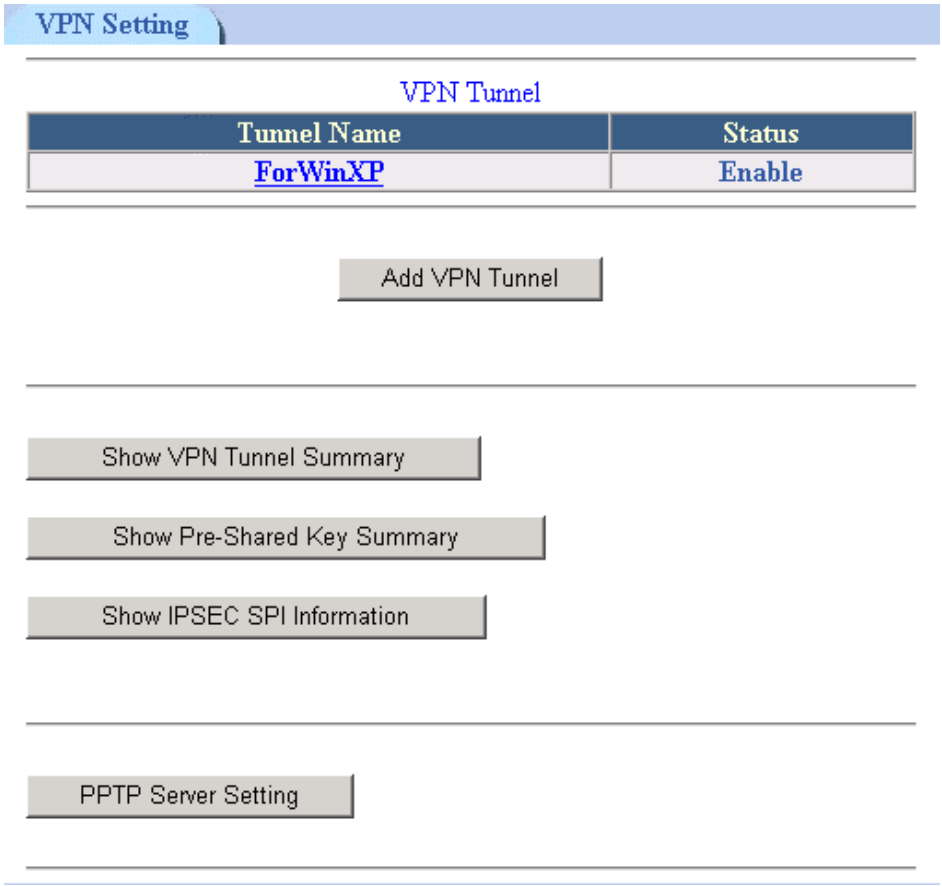


The above diagram provides simple illustration of how to connect two end points via your router by VPN technique. In this case, a PC with IP address of 192.168.2.254/24 is trying to connect with another PC with its IP address of 192.168.1.x/24 via your VPN router with it's IP address of 192.168.1.254/24.



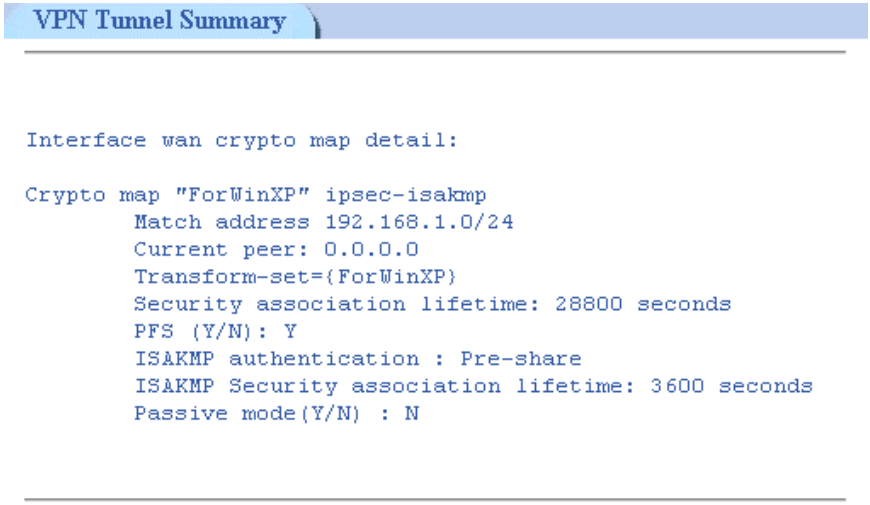
1. Click on **VPN** button on left manual bar from **Advanced** section**.**
2. Click on **Add VPN Tunnel**.
3. Enter the name of the tunnel in the **Tunnel name** field. It allows you to identify multiple tunnels from your tunnel group. It does not have to match the name used at the other end of the tunnel.
4. Select **Enable** from Tunnel Status field to activate the tunnel.
5. The **Local Secure Group** is the computer (s) on your LAN that can access the tunnel. Enter the IP address and subnet mask of your local VPN router in the field.
6. The **Remote Secure group** is the computer (s) on the remote end of the tunnel that can access the tunnel. Enter the IP address and subnet mask of the computer at the other end of the tunnel in this field.
7. The Remote Security Gateway is the VPN device, such as a second VPN router on the remote end of the VPN tunnel. Enter the IP address of the VPN device at the other end of the tunnel. The remote VPN device can be another VPN router, a VPN server, or a computer with VPN client software that supports IPSec. The IP address may either be static or dynamic, depending on the settings of the remote VPN device. Make sure that you have entered the IP address correctly, or the connection cannot be made.
8. Currently you have only one option to select one type of **Encryption** as **3DES**. This is the most secure type of encryption and it is set as the default value.
9. From **Authentication**, you have option to select either **MD5** or **SHA1**. It is recommended to select SHA1 as it is more secure than MD5.
10. From **Key Management** section, select Auto (IKE) as default value and select PFS (Perfect Forward Secrecy) and enter a series of numbers or letters in the **Pre-Shared Key** field. Based on this word, which must be entered at both ends of the tunnel. You may use any combination of up to 24 numbers or letters in this field. No special characters or spaces are allowed. In the **Key Lifetime** field, you may optionally select to have the key expire at the end of a time period of your choosing. Enter the number of seconds you like the key to be useful. The default value if Key Lifetime is 3600 seconds.
11. Click on **add** to confirm your VPN tunnel settings..

After the VPN tunnel has been established, you should see the name of VPN tunnel and status from the first page as following:



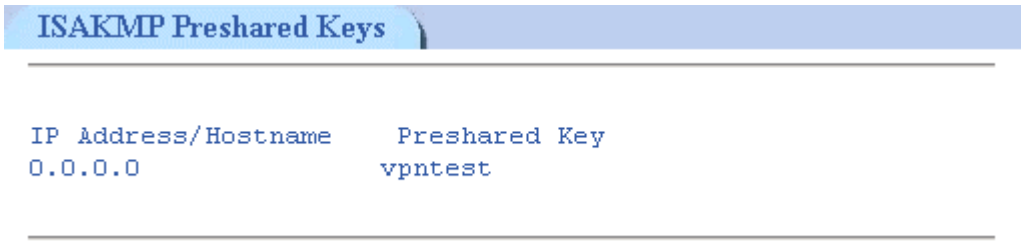
Show VPN Tunnel Summary

To view IPSec VPN tunnel setting values, please click on **Show VPN Tunnel Summary** button to access the information.



Show Pre-Shared Key Summary

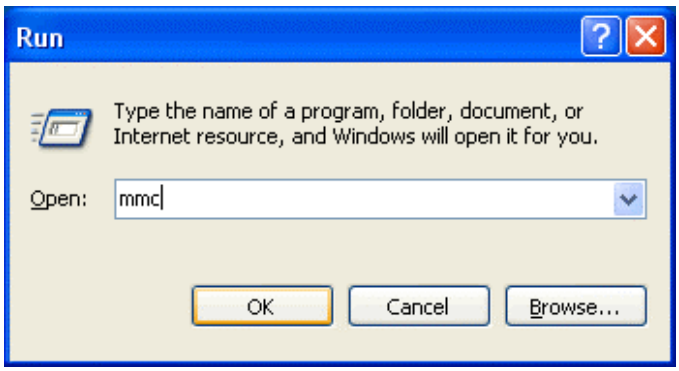
To view all Pre-shared Key configuration information, please click on Show Pre-Shared Key Summary button.



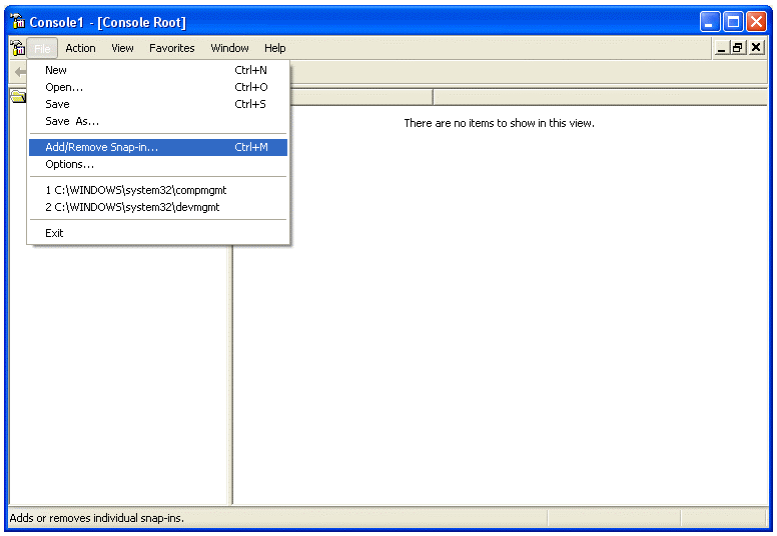
Since the VPN has not yet established, therefore if you click on "**Show IPSec SPI Information**" then it will show no values.

Configuring IPSEC between a WINXP PC and the router

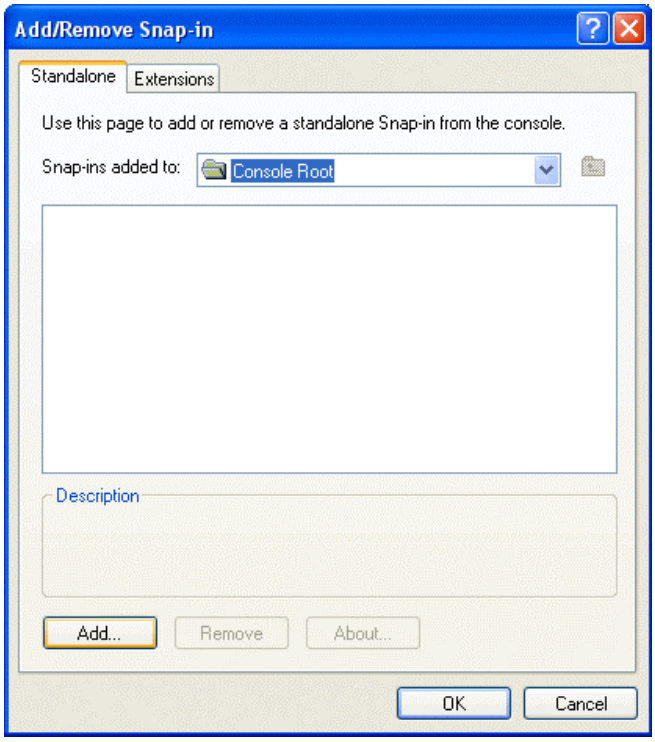
The following section will explain the configuration steps on how to connection VPN tunnels between your PC (WinXP) with your VPN router.



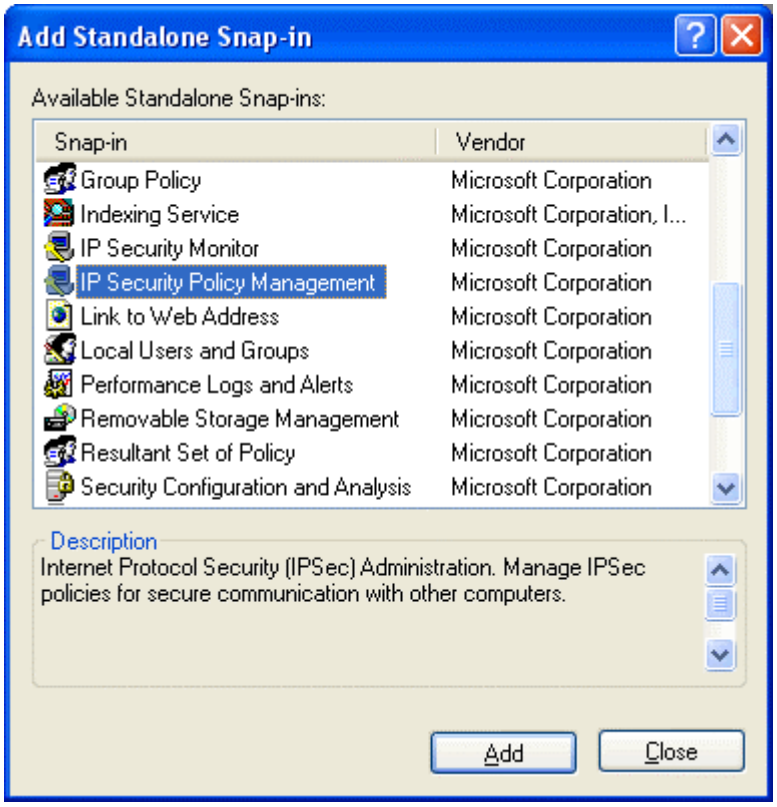
5. Go to **Start** button and select **Run**
6. Type **mmc** in **open** field
7. Click **Ok**.



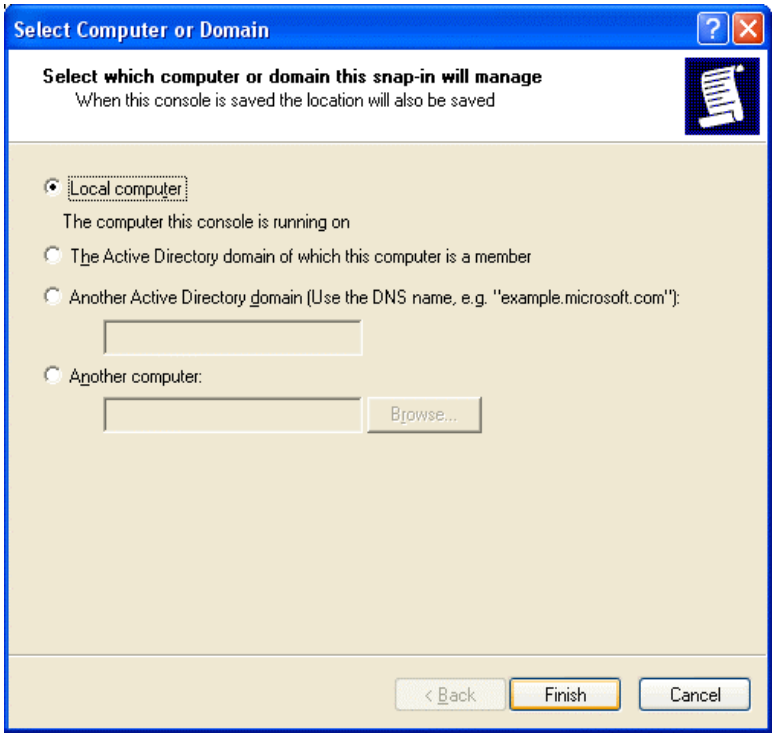
8. From **File** pull-down window, select **Add/Remove Snap-in**



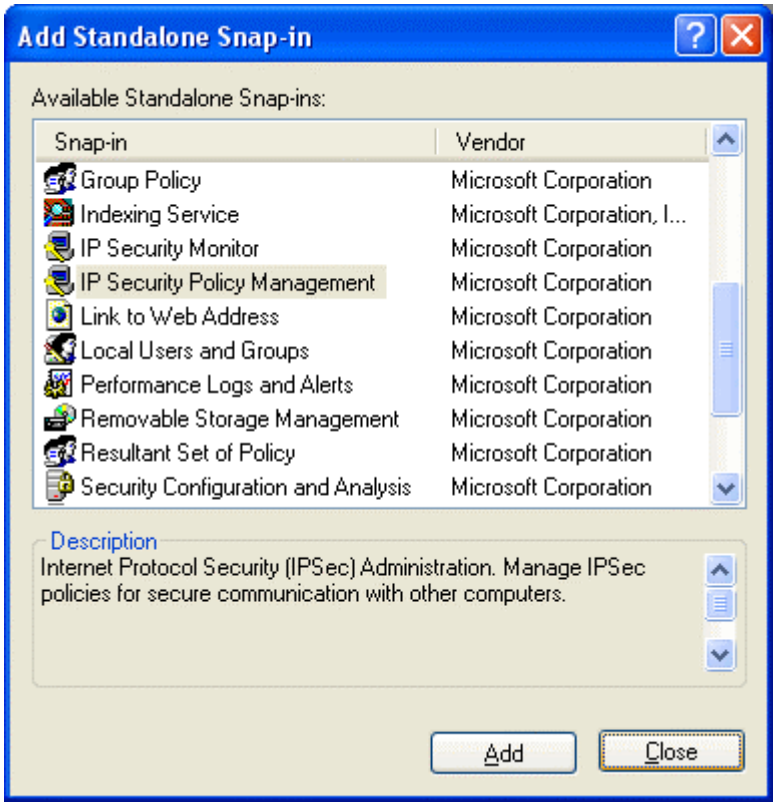
9. Click on **Add** button



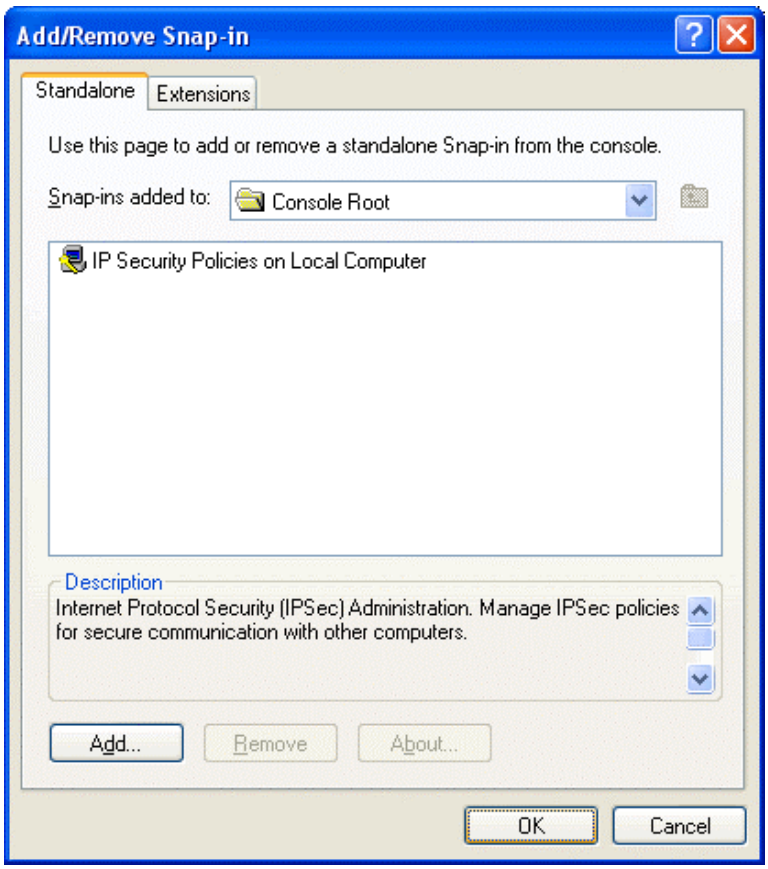
10. Click on **IP Security policy management**
11. Click on **Add** button



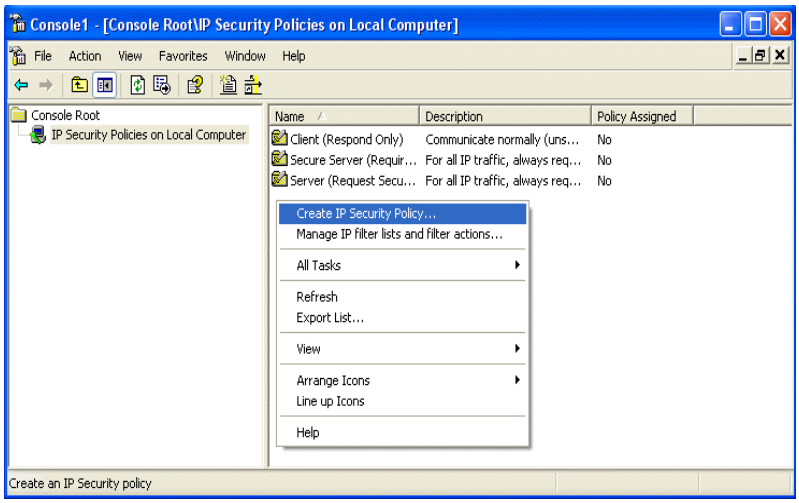
12. Select **Local Computer**
13. Click on **Finish** button



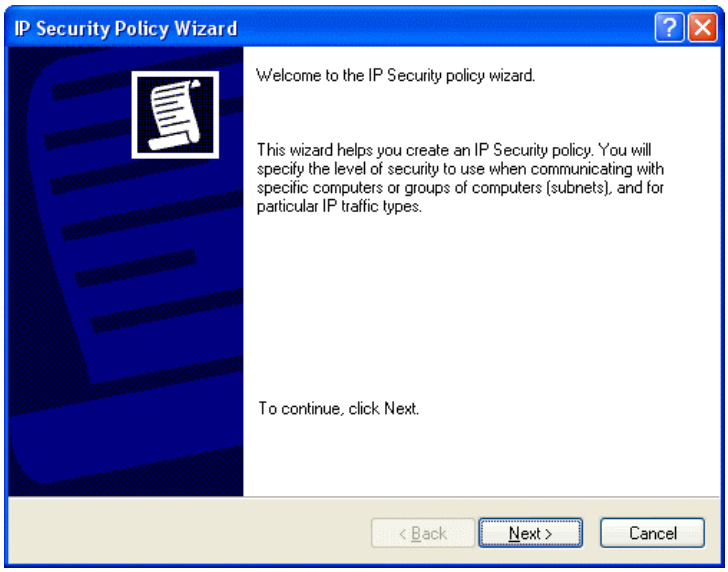
14. Click on **Close** button



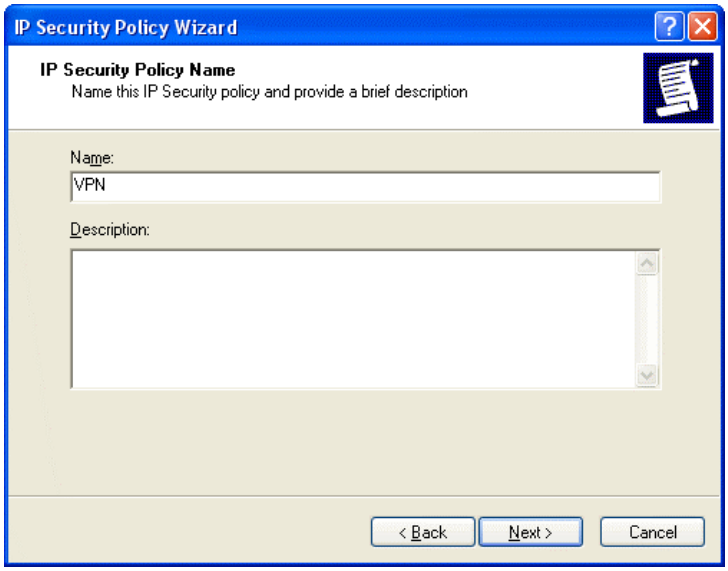
15. Click on **OK** button



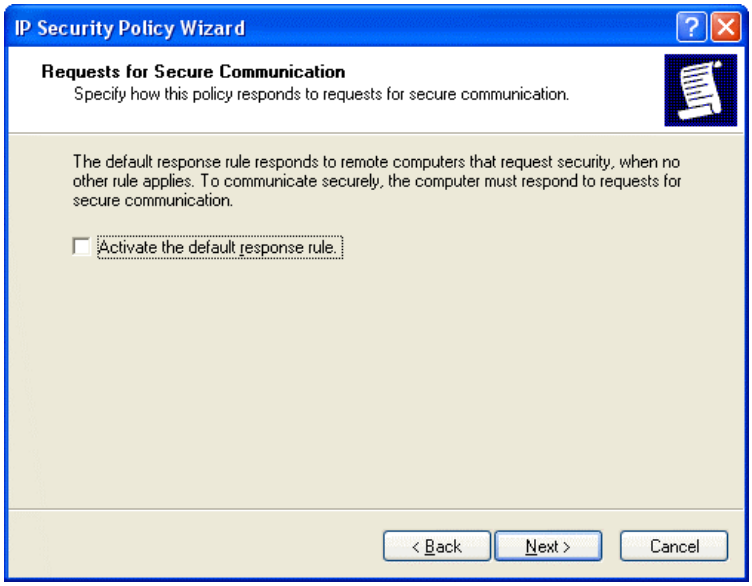
16. Click on **IP Security Policies on Local Computer** on the left screen
17. On the right screen, move you mouse cursor to the blank area and hit a single click on the right hand button of your mouse.
18. Select **Create IP Security Policy** from the pull-down window.



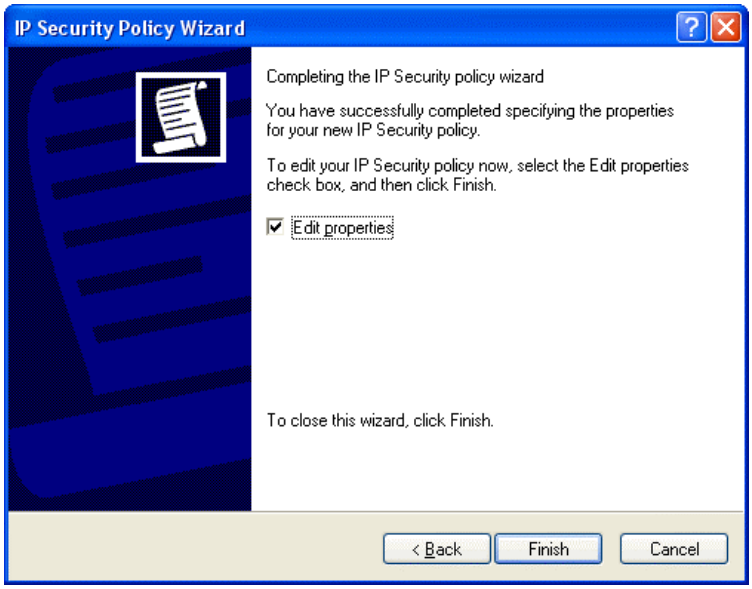
19. Click on **Next** button



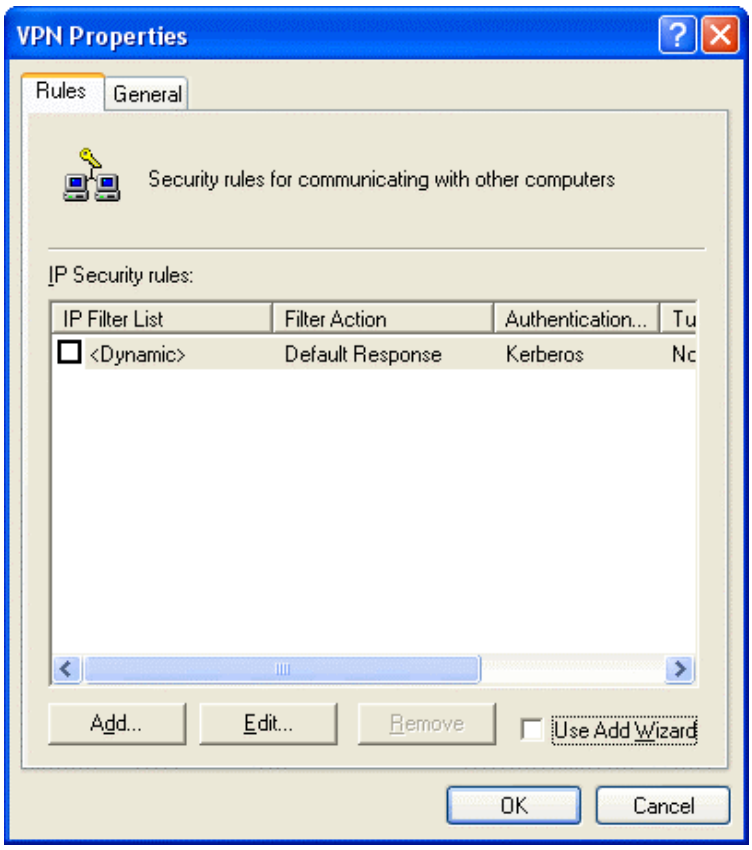
20. From the **Name** field, enter the name of VPN tunnel. (in this case, the name is called VPN)



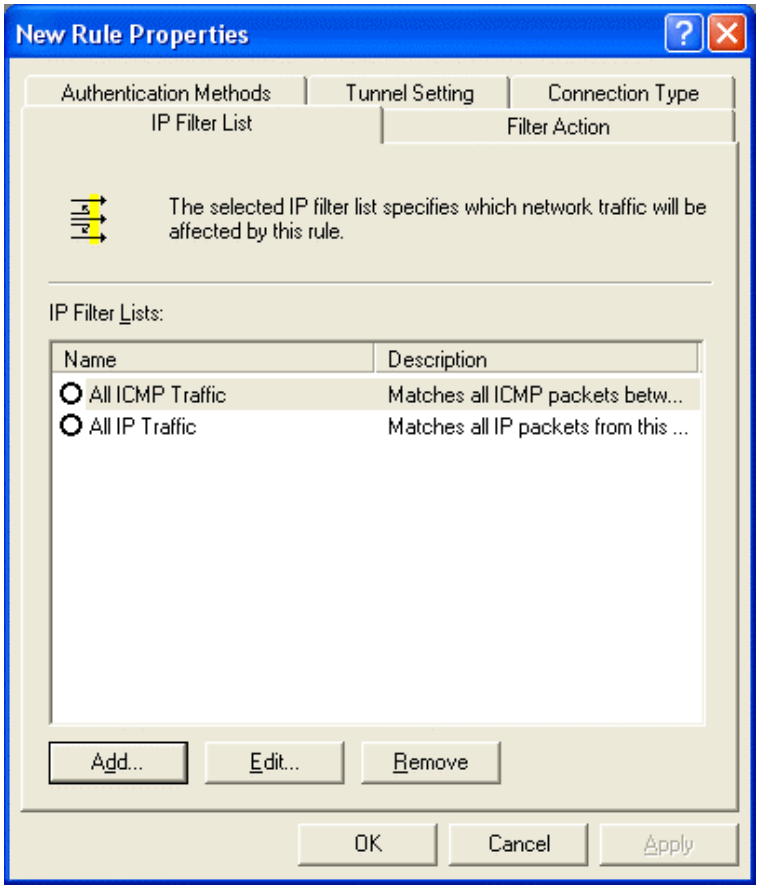
21. Un-check or cancel the square box next to **Activate the default response rule**.
22. Click on **Next** button



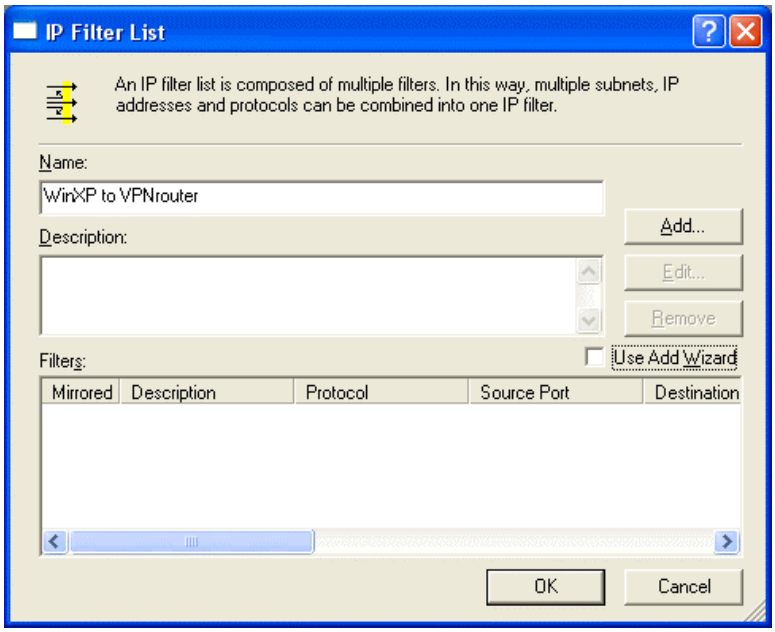
23. Tick on the square box next to **Edit properties**
24. Click on **Finish** button



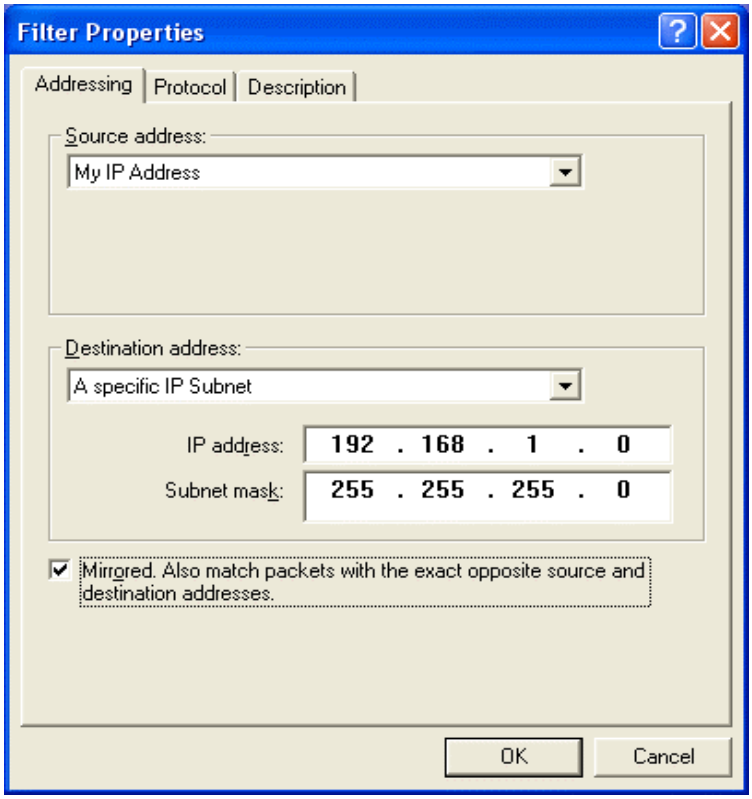
25. Un-tick or cancel **Use Add Wizard**
26. Click on **Add** button



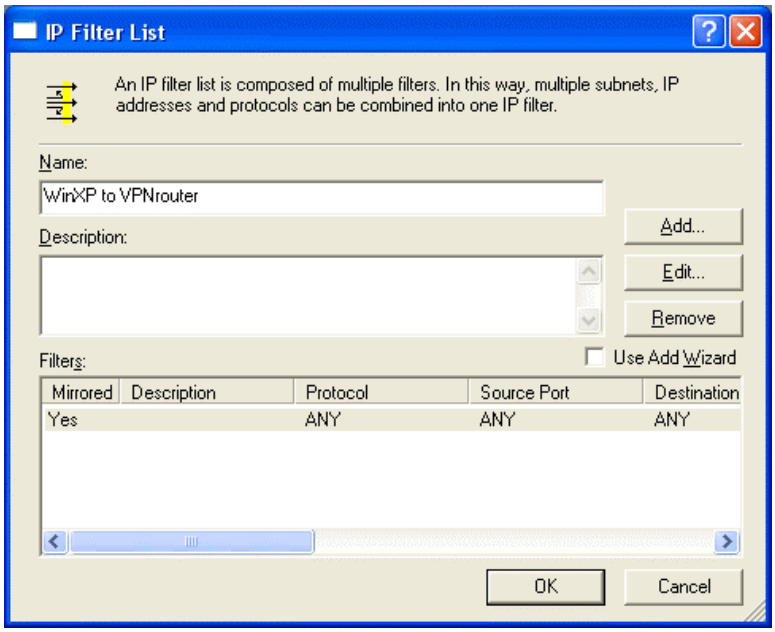
27. Click on **Add** button



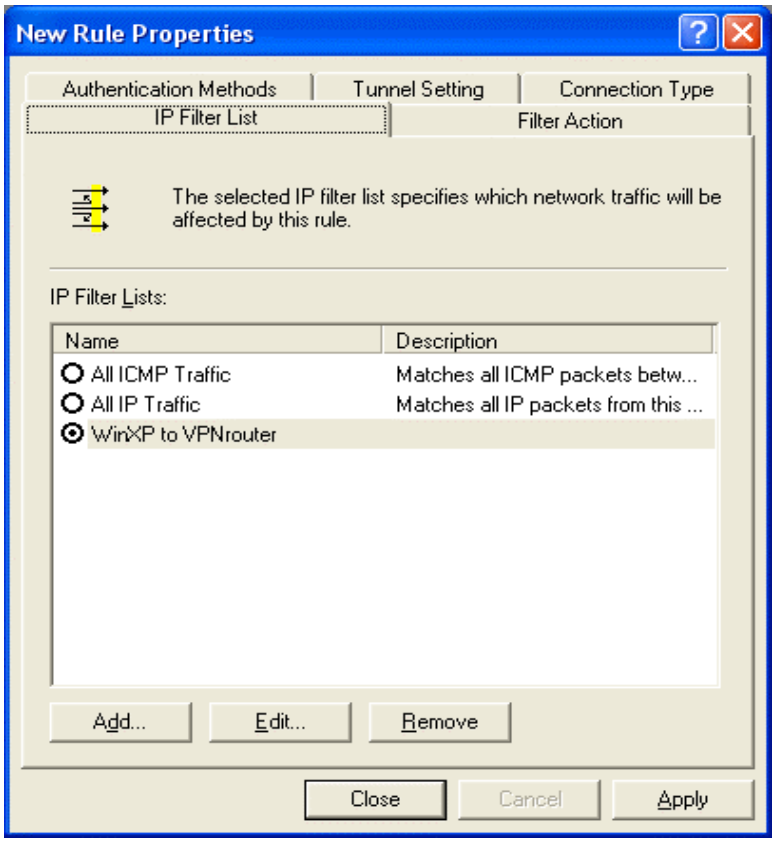
28. Enter the **name** of the **IP Filter List**. (In this case, the name is WinXP to VPNrouter)



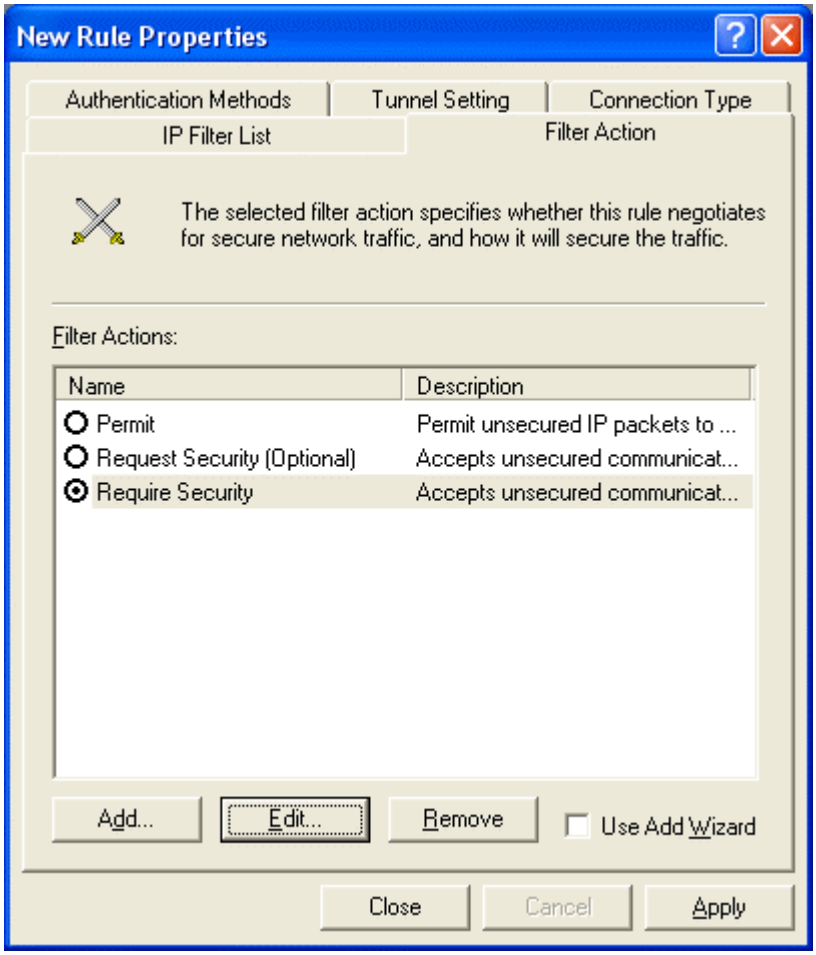
29. From **Source address** pull-down window, select **My IP Address**
30. From **Destination address** pull-down window, select **A specific IP Subnet**. Enter destination IP address and its subnet mask. (in this case, the destination IP is 192.168.1.0/255.255. 255.0) 。
31. Check the box of **Mirrored. Also match packets with the exact opposite source and destination addresses.**
32. Click on **OK** button



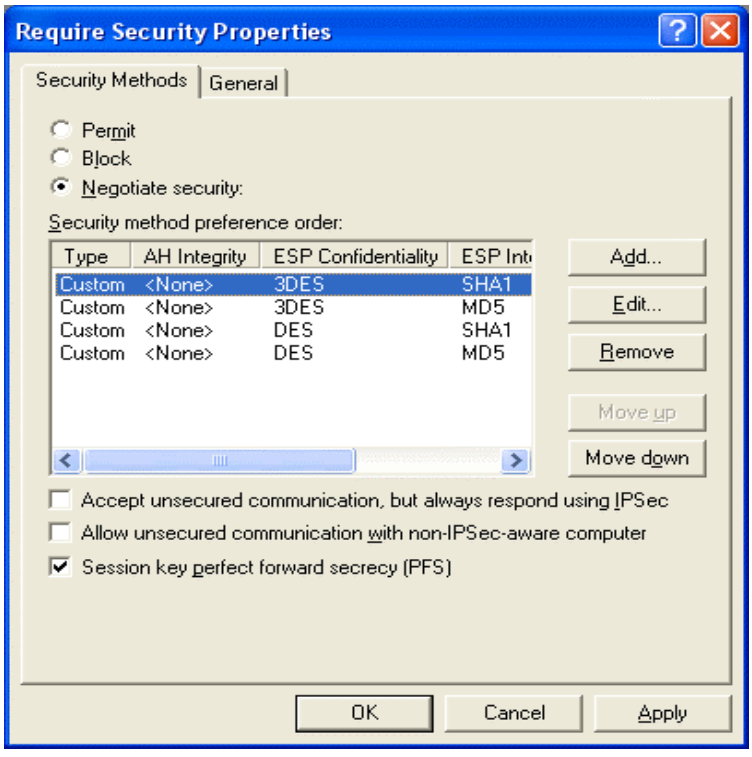
33. Click on **OK** button



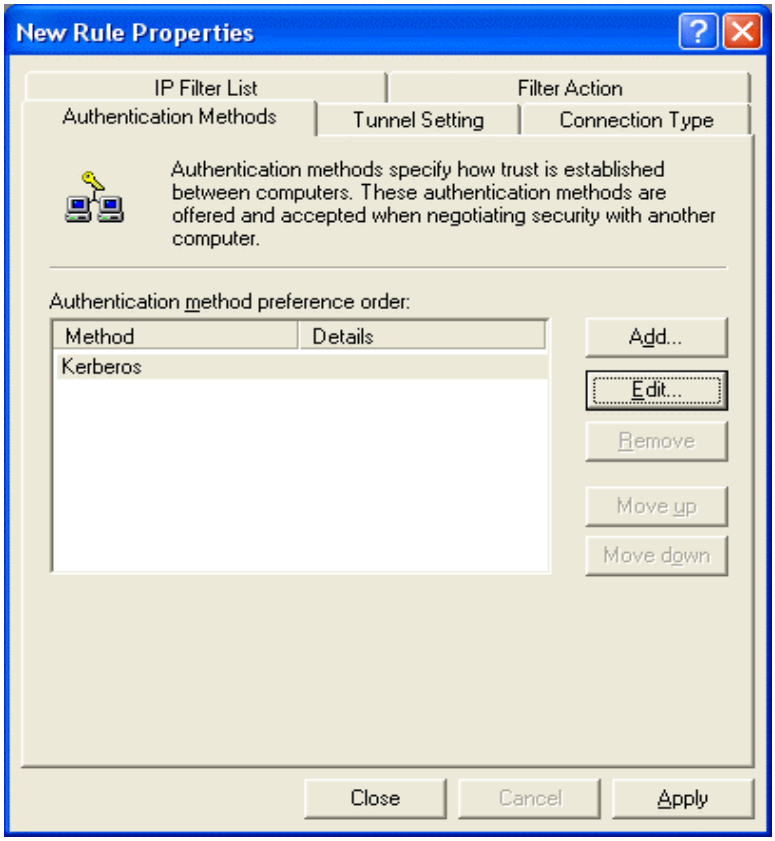
34. Click on IP Filter name of your previous setting. (in this case, it's WinXP to VPNrouter)
35. Click on **Filter Action** tab from the top.



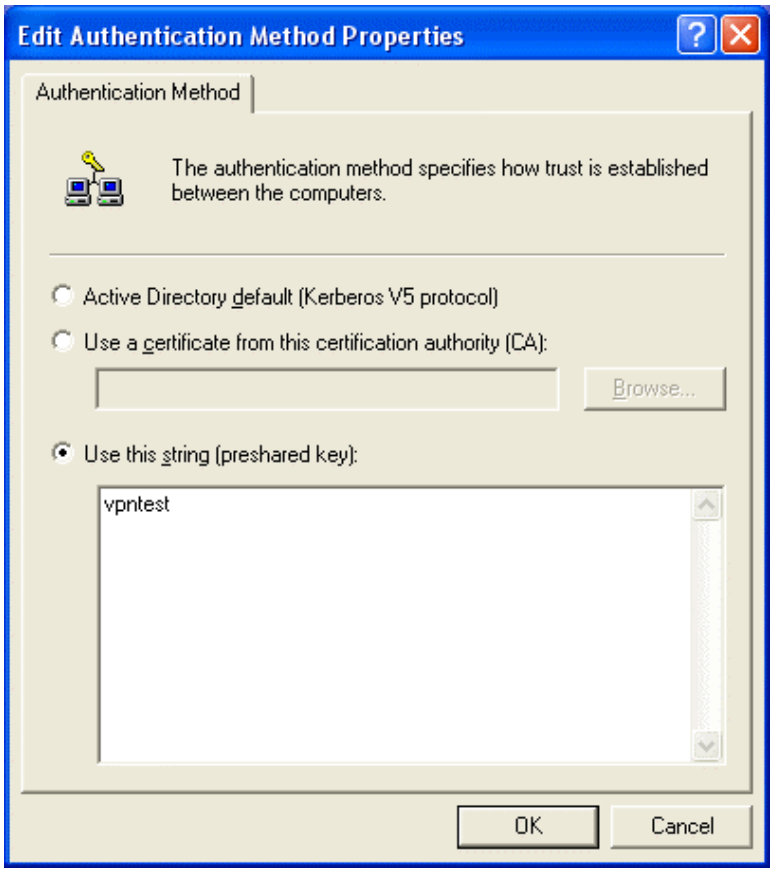
36. Click on **Require Security**
37. Click on **Edit** button



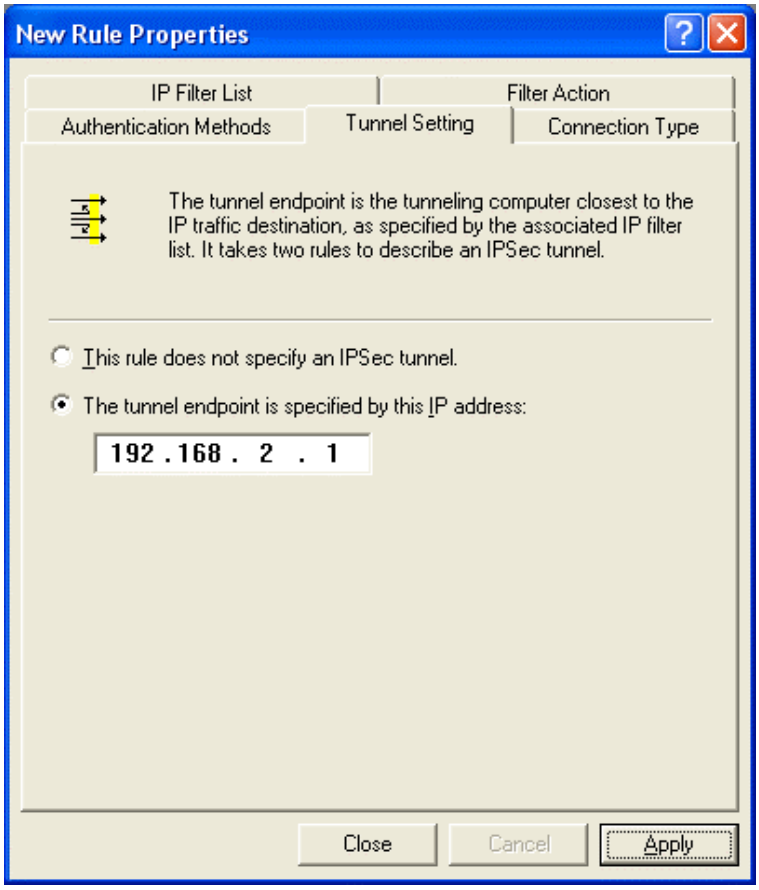
38. Click on **Negotiate security**
39. Cancel the check box of **Accept unsecured communication, but always respond using IPSec**
40. Tick the box of **session key perfect forward secrecy (PFS).**
41. Click on **OK** button



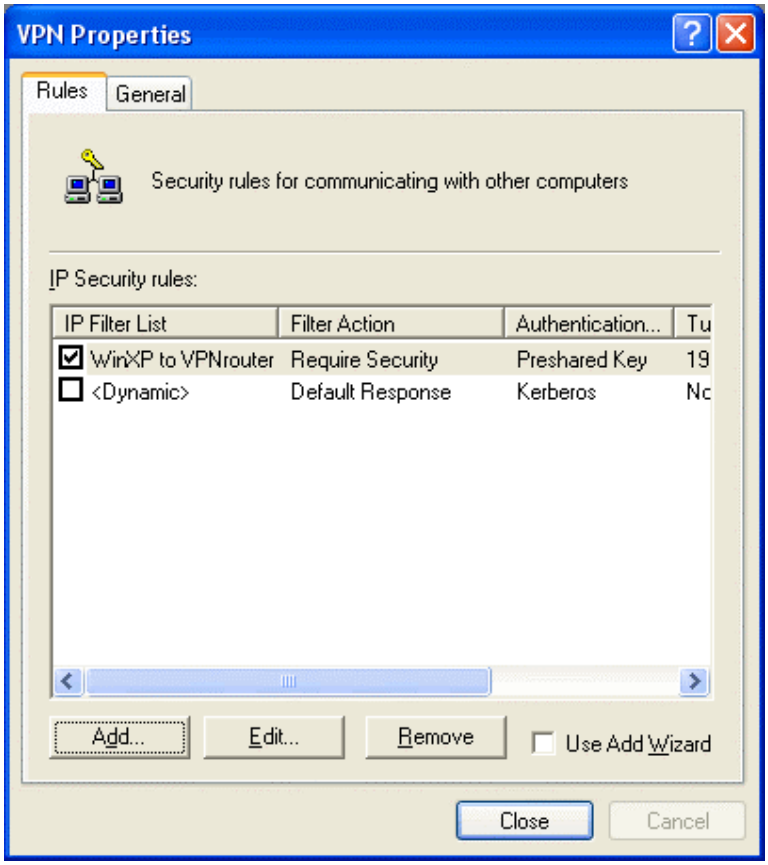
42. Click on **Edit** button



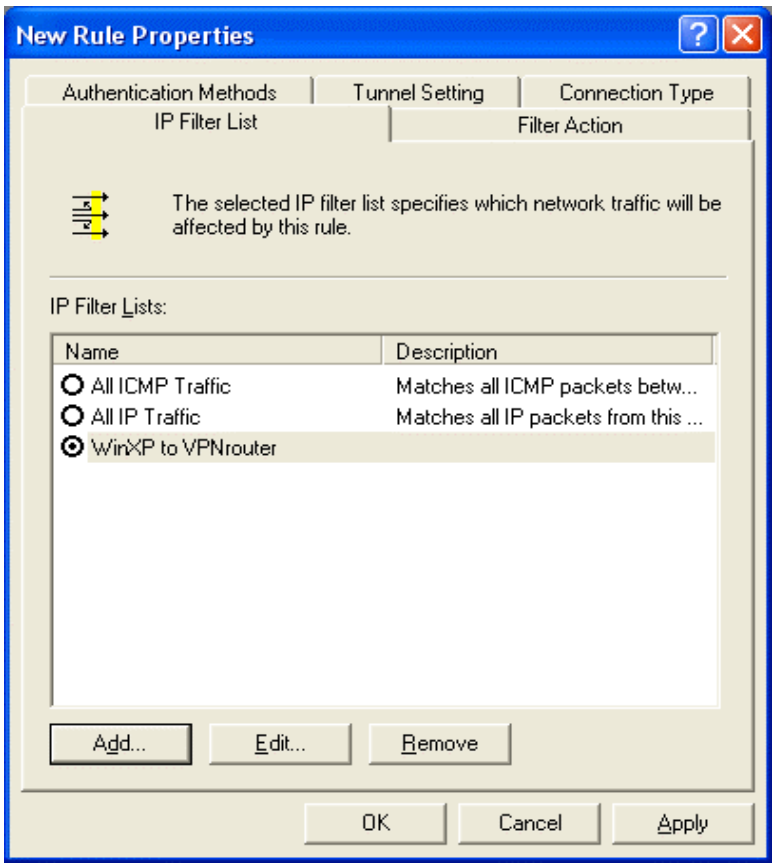
43. Click on **Use this string** (preshared key)
44. From the bottom blank area, enter the name of preshared key defined in web-based management from previous setting.
45. Click on **OK** buton



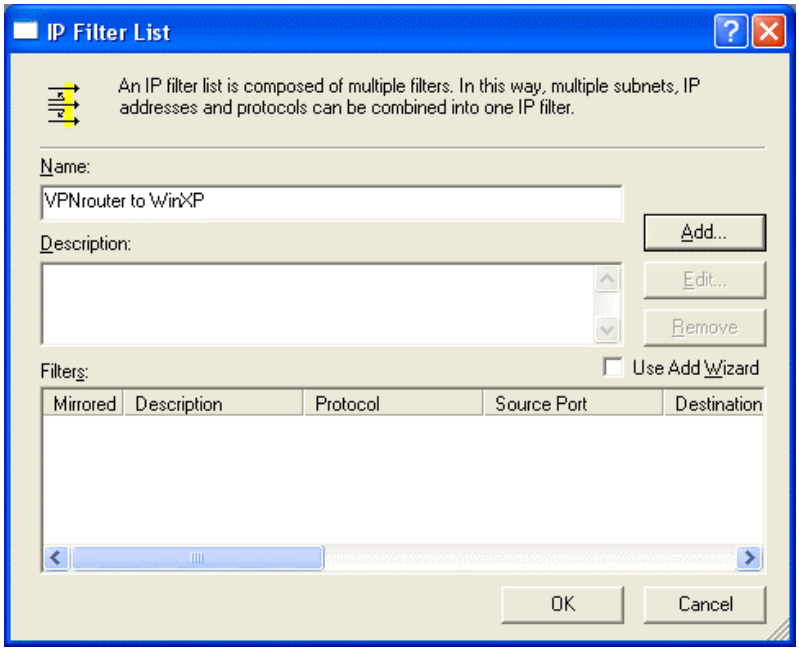
46. Click on **The tunnel endpoint is specified by this IP address**
47. Enter the **WAN IP** address of destination endpoint of VPN tunnel. (in this case, it's 192.168.2.1)
48. Click on **Apply** button



49. Click on pre-defined IP Security rules. (in this case it's WinXP to VPNtunnel)
50. Click on **Add** button



51. Click on **Add** button



52. Enter the name of IP filter list in opposite direction. In this case, it's VPNrouter to WinXP.
53. Click on **Add** button

Table of Contents

Chapter 1: Introduction

Overview

A true heart of your home/office network, Multimedia Security Gateway simplifies your network complexity by combining a multitude of functions into a single device.

Utilizing 56-bit DES and 168-bit 3DES encryption, header authentication, and IKE key exchange access control, Multimedia Security Gateway's full IPSec Virtual Private Network (VPN) capability provides complete data privacy.

Functions supported are IP sharing, PPPoE, DHCP, DDNS, Firewall, VPN, content filtering, four USB 2.0 ports, a four-port switch hub, printer server, FTP server, web cam server, motion detection, a 802.11g access point, USB Storage, UPnP and many more.

Equipped with the most advanced technology available today, this router is the only TOTAL SOLUTION for your networking needs.

Key Features

- High Performance CPU MIPS 170MHz
- Enterprise-Class Firewall
  - * SPI Firewall
  - * DoS
  - * True Content Filtering
- Full IPSec VPN capability
  - * Support (168-Bit) 3 DES Encryption Algorithms
  - * Support MD5 and SHA Authentication Algorithms
  - * Support IKE Key Management
  - * Support 100 VPN tunnels for S/W VPN and 200 Tunnels for H/W VPN
- Compatible with other IPSec VPN products
- Support QoS Bandwidth management
- 4 * USB 2.0 Port for Plug and Share Utilities
- Print Server, Web Cam Server and FTP Server built-in

Package content

- One Multimedia VPN/Firewall Router with 4*USB 2.0 Interfaces
- One Power Supply
- One User's manual in CD
- One RJ45 Ethernet cable
- One Antenna (for wireless product only)

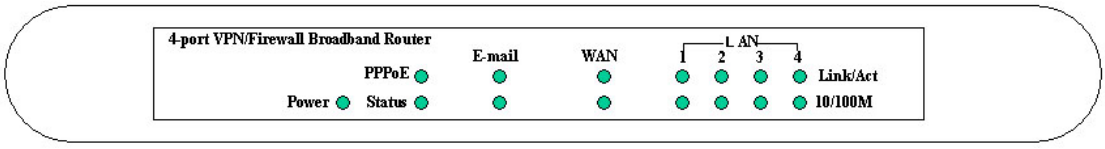
System Requirements

- One RJ-45 Broadband Internet connection
- One PC with 10/100Mbps Network card installed
- TCP/IP network protocol for each PC which connect to the router
- Internet Browser installed in PC
- RJ-45 Cat.5 network cables

Chapter 2: Get to know your Multimedia Router

Hardware Features

Front Panel LEDs



LAN indicators

Power

On Green The Power LED illuminates when the router is powered on.

Off The router is not power on.

E-mail Green & Orange

The two LED are used for E-mail notification indicators and will describe at later chapter

Link/Act

Green The Link/Act LED serves two purposes. If the LED continuously illuminated, the router is then successfully connected to a device through the corresponding port (1-4). If the LED is flashing, it means the router is actively sending or receiving date through that specific port.

10/100M

Orange The LED illuminates when a successful 100Mbps connection is made through the corresponding port.

WAN Indicators

PPPoE

Red The LED illuminates when successful broadband Internet connection is made via PPPoE connection type

Status

Red The LED illuminates when router is boot-up after connected to power or the router has connection failure. It is necessary to reset the router by pressing the reset button at rear panel of router

WAN

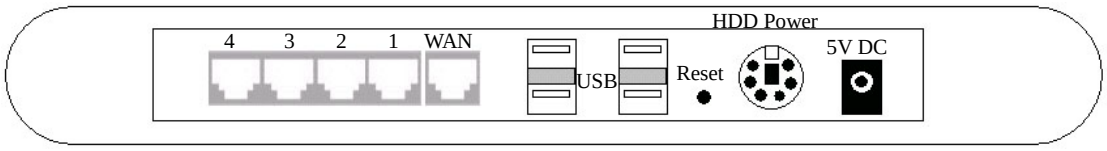
Green The LED illuminates when successful connection is made between router and your broadband device or network

Orange The LED illuminates when a successful 100Mbps connection is made through the corresponding port

Air (Wireless LAN)

Green The LED flashes when successful wireless connection is made between your PC and router.

Rear Panel Interfaces



WAN The WAN port is where you will connect your Cable or DSL modem.

LAN 1-4 These four LAN ports are where you will connect PC/Notebook

USB These four USB 2.0 ports are where you connect to other USB devices such as Printers, Web Cameras, USB HDD, Flash drive, MP3 player, Digital Camera and USB Media Reader

Reset
1. Press Reset button with pencil tip to re-boot the router when the router is having problem connecting to Internet
2. Press on the Reset button for 3 seconds until Status LED is flashing to clear all configurations.

HDD Power

Attach PS/2 cable from USB HDD to HDD Power Connector for additional power support when the router is connected to USB HDD. When USB HDD is equipped with PS/2 cable, it means the power needed for HDD is greater than the power provided by USB port. It is necessary to connect its PS/2 cable for stable power management.

Power Power Port is where you connect power supply

Chapter 3: Connecting the router to the Internet

Hardware Installation

1. Power down your PC, Cable/DSL modem and the Router

2. Connect a cable from one of your PC's Ethernet port to one of the LAN ports on the rear panel of the router. Do the same with all the PC you wish to connect to the router.

3. Connect the network cable from your Cable/DSL modem to the WAN port on the router's rear panel.

4. Connect antenna to the antenna connector of your router. (for wireless product only)

5. Connect the power supply to the power port on the rear panel of the router, and then plug the power supply to the power outlet. The **power** LED on the front panel will light up green as soon as the power supply is connected properly. The **Status** LED will light up red for few seconds when the router goes through its self-diagnostic test. The LED will turn after the self-test is completed.

6. Power on your Cable/DSL modem

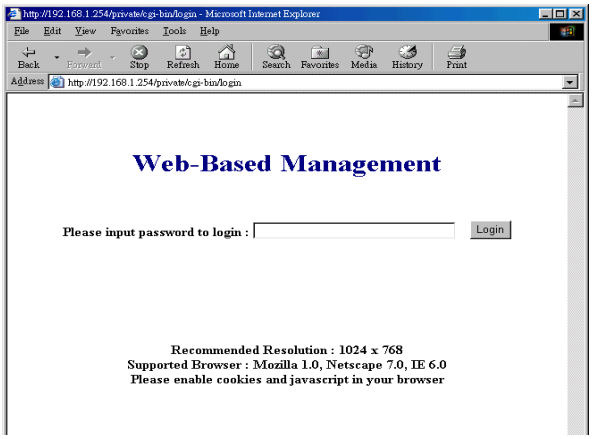
7. Press the **Reset Button** on the router's rear panel with paper clip. Hold the button until the **Status** LED flashing. This will restore the router's factory default settings.

Login to Web-Based Management Tool

Once the hardware installation is completed and the router is properly wired into your network, the software configuration of the router can begin.

The default IP address of the router is **192.168.1.254**
The default password is **admin**

1. Open a web browser and type 192.168.1.254 in the browser's address box. Press Enter. The following **Web-Based Management** Screen will appear.



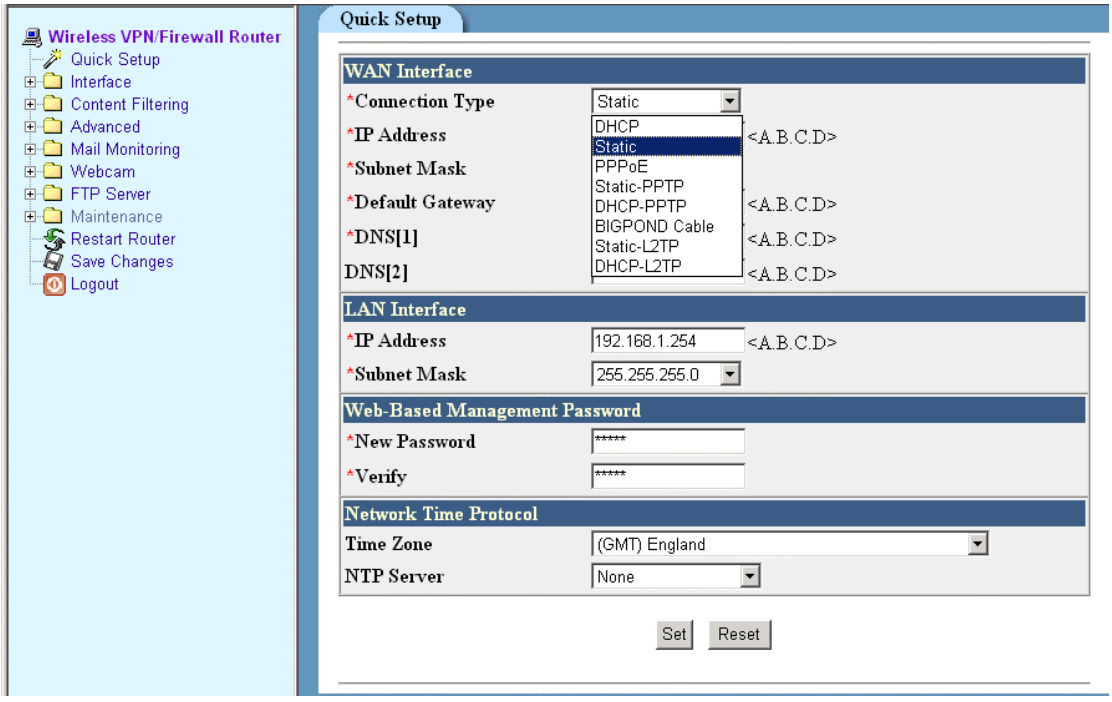
2. Enter **admin** in the password field and click on **Login** to enter Web-Based Management page. After successfully login to the system, the following screen will appear.

3. Click on **Quick Setup** from the main menu on the left side of the screen to begin connecting your network to Internet.

Quick Setup

There are four connection types in Quick Setup menu. Please select the most suitable connection type provided by your ISP. You can choose the connection type by pressing the check box on **Connection type** field.

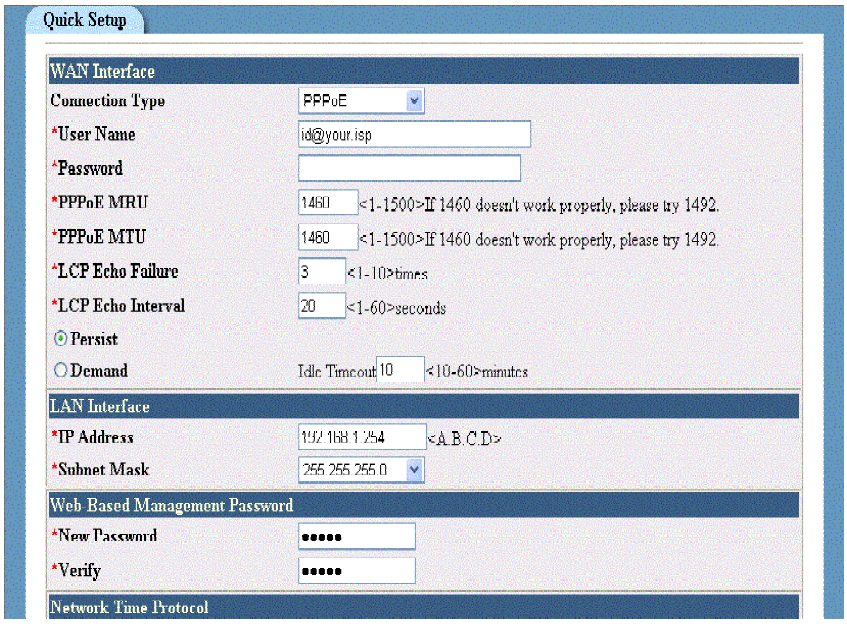
There are four major sections associated with each of connection type when configuring Quick Setup. There are WAN Interface, LAN Interface, Web-Based Management Password and Network Time Protocol (NTP).



WAN Interface

PPPoE

If your ISP provided PPPoE service for Internet connection, please take the following Setup steps:

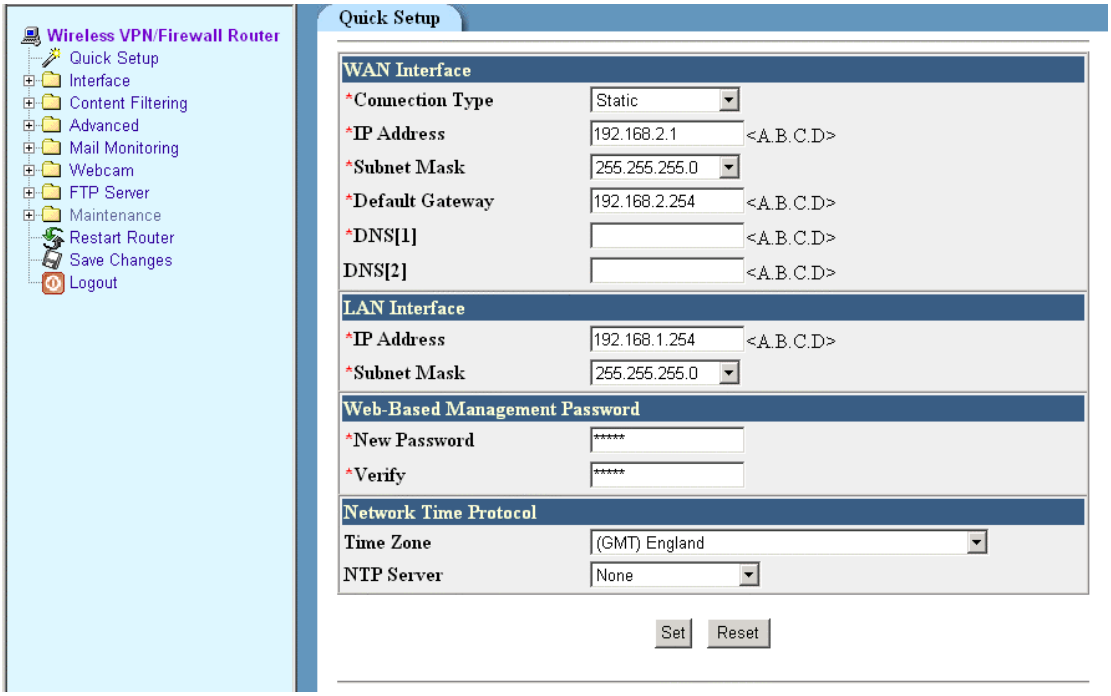


1. Select **PPPoE** from **Connection Type**
2. Enter the **User Name** you use to log onto your Internet connection. Some ISP may require the format of **User Name** to be id@isp.net. Please check double check with your ISP for this information.
3. Enter your corresponding **password.**
4. Click on **Set** to activate the connection.
5. When the **PPPoE** LED on front panel of the router illuminates, it means the router is successfully connected to Internet. To check the connection status or IP address information, please go to **Interface > WAN > Show WAN Information.**

6. If you wish to automatically disconnect your Broadband connection after the service has not been used for a period of time. Please click on **Demand** check box and set the **idle timeout** value. Your Broadband connection will automatically restart when the router receive any request or packet that need to send to Internet. For example, the Internet connection will resume by opening a web page or clicking on specific URL on your existing web page.

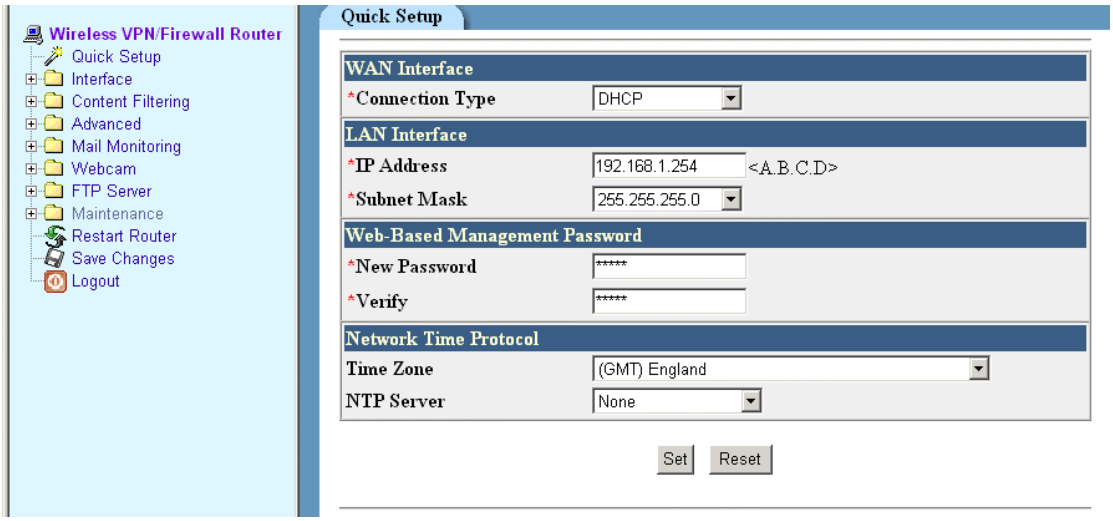
Static

If your ISP provides fixed IP for Internet connection, please take the following Setup steps:



1. Choose **Static** from **Connection type** pull-down box.
2. Enter **IP address**, **Subnet mask** and **Default gateway** as provided by your ISP.
3. Enter at least one **DNS Server** IP address as provided by your ISP.
4. Click on **Set** to activate the connection.

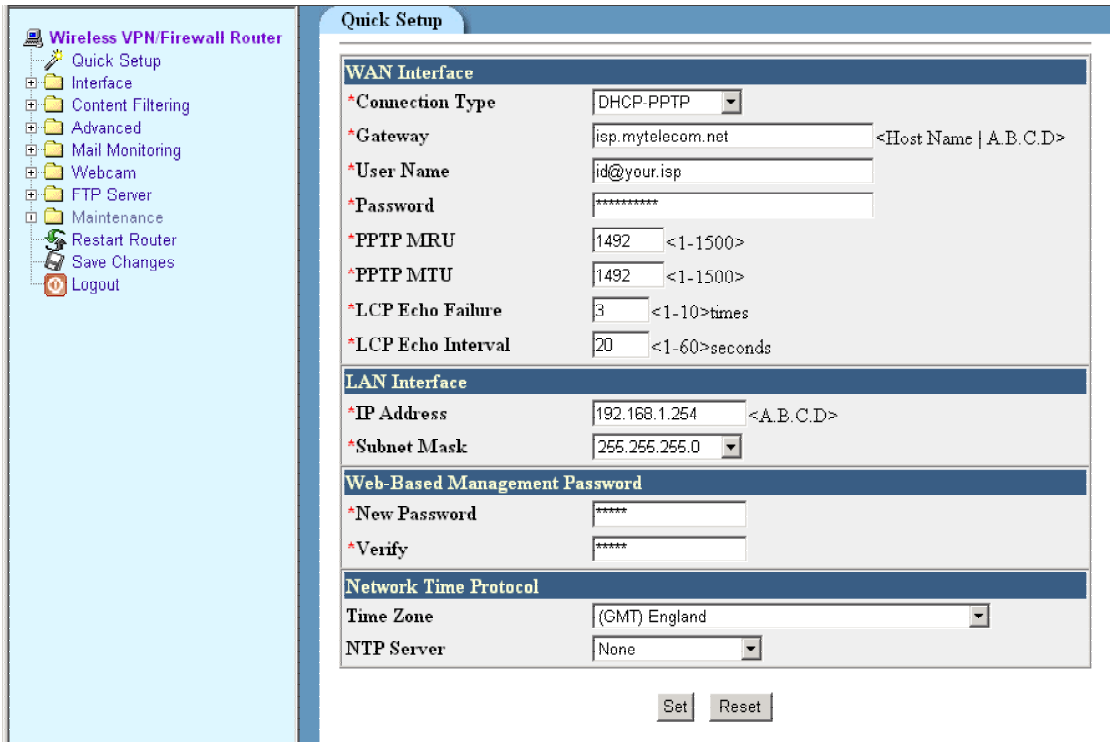
DHCP



If your ISP provides DHCP service for Internet connection then all you need to do is to select **DHCP** and click on **Set**. In order to make sure the WAN connection is made, you can go **Interface > WAN > Show WAN Information** to check the connection status.

PPTP-DHCP

If your ISP provides PPTP-Static service for Internet connection, please take the following Setup steps:



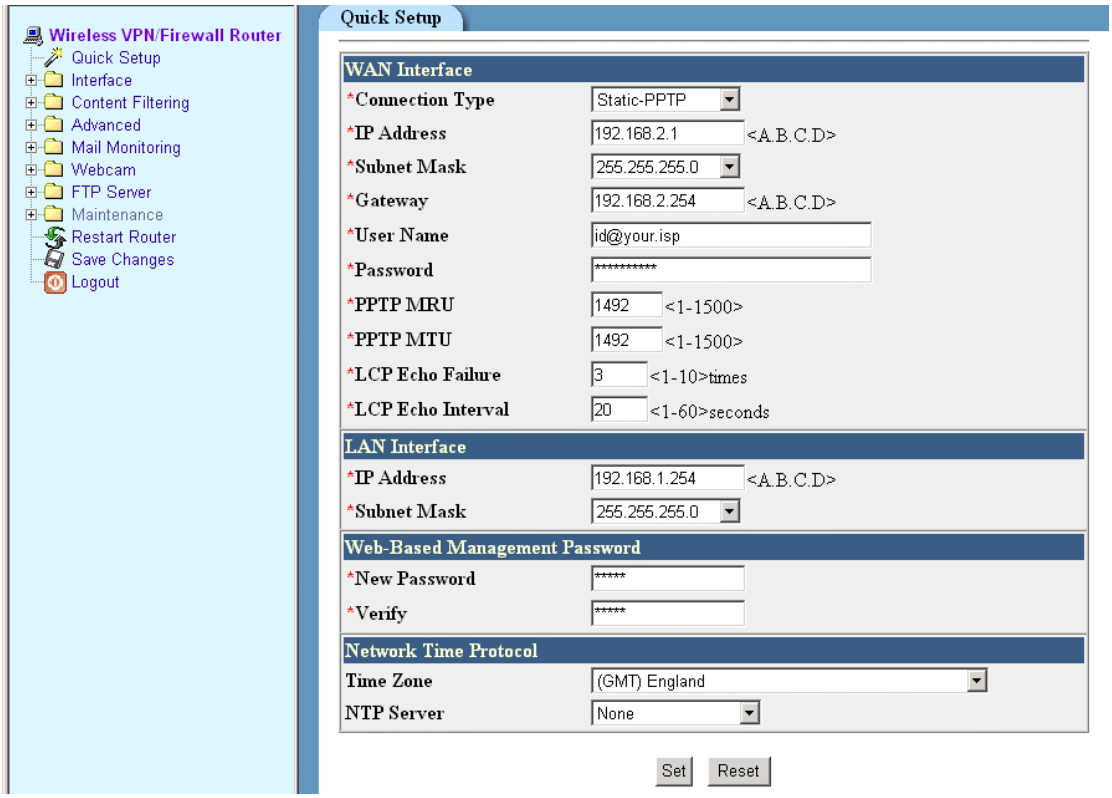
1. Select DHCP-PPTP from Connection type pull-down box
2. Enter **Gateway host name** as provided by your ISP.
3. Enter the **User Name** you use to log onto your Internet connection. Some ISP may require the format of **User Name** to be id@isp.net. Please check double check with your ISP for this information.
4. Enter your corresponding Password
5. Click on **Set** to confirm the settings.

NOTE:

Please **DO NOT** change the value of PPPoE MRU, PPPoE MTU, LCP Echo Failure and LCP Echo Interval unless it is request by your ISP. Please remain the values as factory default.

PPTP-Static

If your ISP provides PPTP-Static service for Internet connection, please take the following Setup steps:



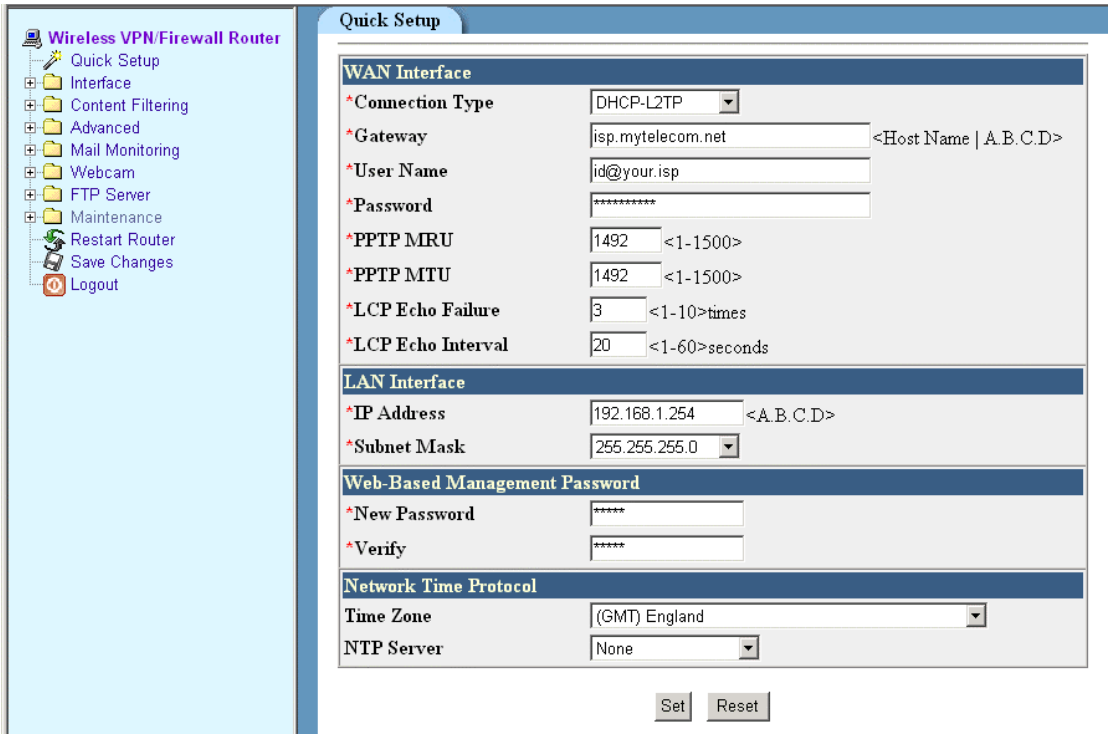
1. Select PPTP from Connection type box
2. Enter **IP address**, **Subnet mask** and **Default gateway** as provided by your ISP.
3. Enter the **User Name** you use to log onto your Internet connection. Some ISP may require the format of **User Name** to be id@isp.net. Please check double check with your ISP for this information.
4. Enter your corresponding Password

NOTE:

Please **DO NOT** change the value of PPTP MRU, PPTP MTU, LCP Echo Failure and LCP Echo Interval unless it is request by your ISP. Please remain the values as factory default.

L2TP-DHCP

If your ISP provides DHCP-L2TP service for Internet connection, please take the following Setup steps:



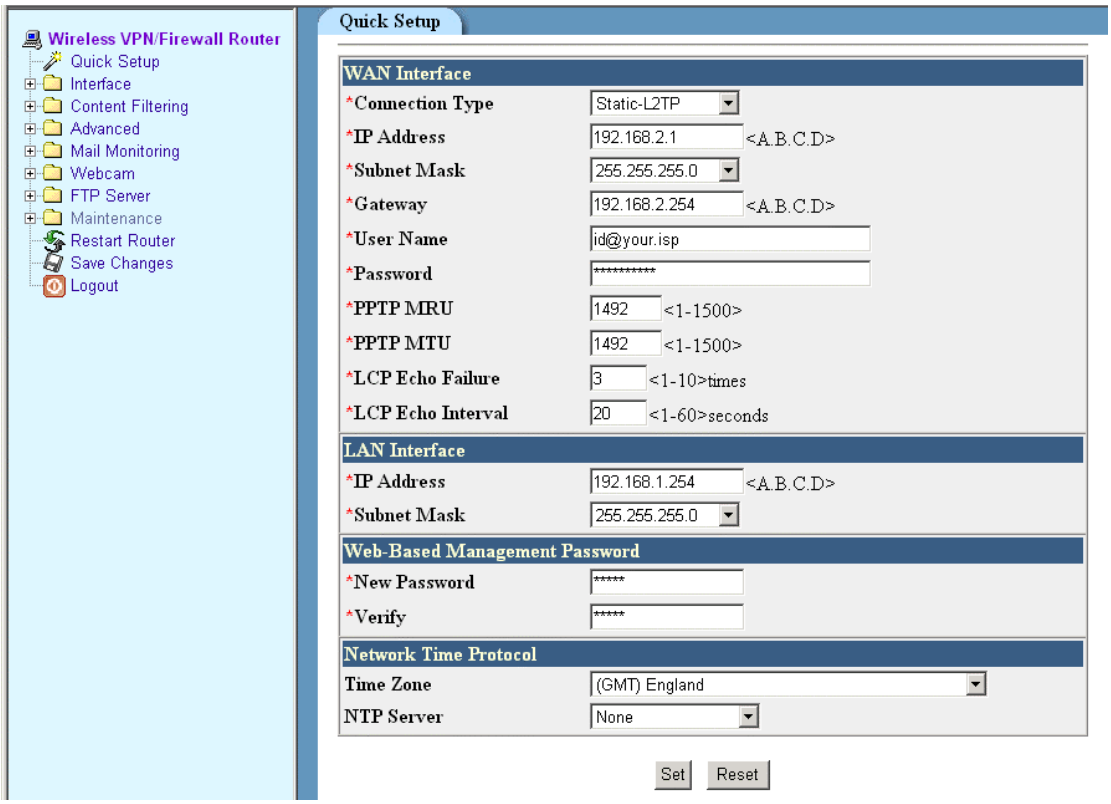
1. Select **DHCP-L2TP** from Connection type pull-down window.
2. Enter **Gateway, User name** and **Password** into their columns.
3. Click on **Set** to confirm the settings.

NOTE:

Please **DO NOT** change the value of PPPoE MRU, PPPoE MTU, LCP Echo Failure and LCP Echo Interval unless it is request by your ISP. Please remain the values as factory default.

L2TP-Static

If your ISP provides Static-L2TP service for Internet connection, please take the following Setup steps:



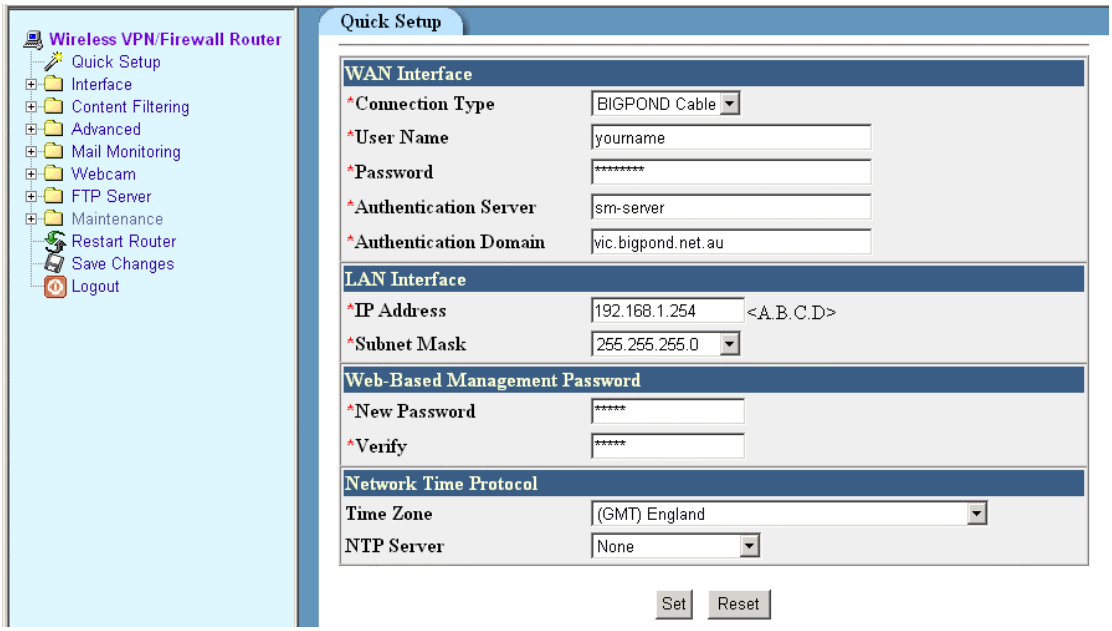
1. Select **Static-L2TP** from Connection type pull-down window.
2. Enter **IP address, Subnet Mask, Gateway, User name** and **Password** into their columns.
3. Click on **Set** to confirm the settings.

NOTE:

Please **DO NOT** change the value of PPPoE MRU, PPPoE MTU, LCP Echo Failure and LCP Echo Interval unless it is request by your ISP. Please remain the values as factory default.

BIGPOND Cable (Australia only)

This broadband connection service is only available for Australian users. If you're located in Australia, please take the following steps:



1. Select **BIGPOND Cable** from Connection type pull-down window.
2. Enter **User name** and **Password** into the related column.
3. Enter the **Authentication Server** and **Authentication Domain**.
4. Click on Set to confirm the settings.

LAN Interface

This Section allows users to modify Router's LAN IP address and subnet mask. When these values are modified, it is necessary to modify your IP and DHCP setting otherwise Web-Based Management could not be accessed.

Web-Based Management Password

This section allows you to change Web-Based Management Login password. Enter the new password and verify it again. The new password will activate the next time you login.

Network Time Protocol

Time Zone – This field indicates time zone where you are locating in.

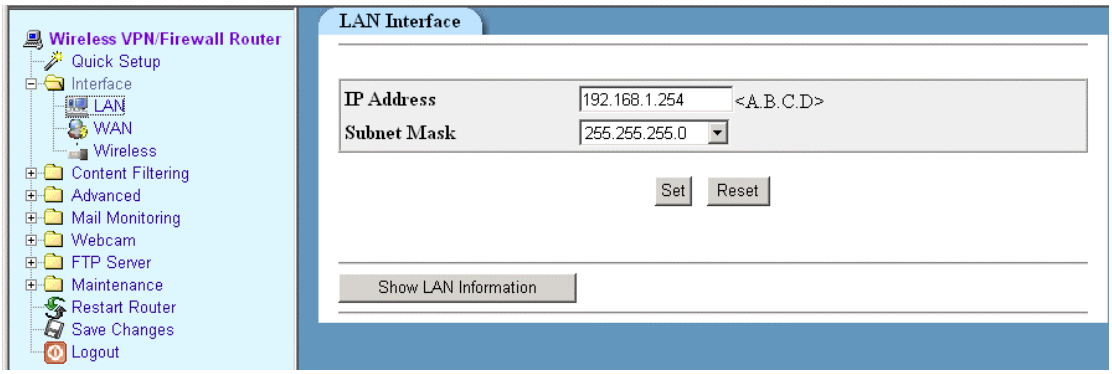
NTP Server - This field allows you to set IP address of NTP Server to synchronize your system time.

Chapter 4: Interface Configuration

Interface

This is to where LAN, WAN and Wireless interface relevant parameters can be configured. If you've already gone through the Quick Setup first, the fields should have values in it. If that is the case, you can skip the Interface configuration of LAN and WAN.

LAN Interface



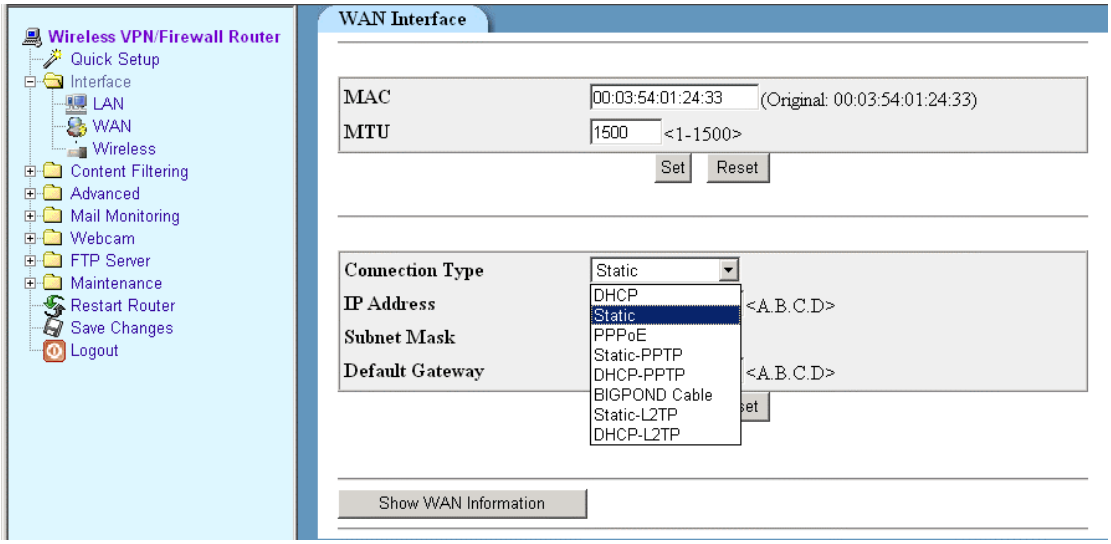
IP address — Enter the IP address. This field should be filled-in automatically already. The value is 192.168.1.254 unless you've changed it.

Subnet Mask — Enter the subnet mask. This field should be filled-in already.

Show LAN Information

Click on **Show LAN Information** in order to access to LAN interface in details.

WAN Interface



Mac — Your router's MAC address is a 12-digit code assigned to a unique piece of hardware for identification. Some ISPs require that you register the MAC address of your network card/adapter, which was connected to your cable or DSL modem during installation. If your ISPs require MAC address registration, find your adapter's MAC address by doing the following:

1. Click the Start button, and select Run. Run winipcfg, and then click more info. Or at the command prompt, run ipconfig/all, and look at your adapter's physical address.
2. Enter 12-digits into the fields and click on Set button. This "clones" your network adapter's MAC address onto your router, and prevents you from having call your ISP to change the registered MAC address to the router's MAC address.

MTU — It stands for maximum transmission unit. Usually it is set as 576 or 1500.

Connection Type — This shows the connection type where the router was connected to Internet. Please refer to the previous section for connection details.

IP address — this field indicates WAN IP address.

Subnet Mask this field indicates subnet mask address

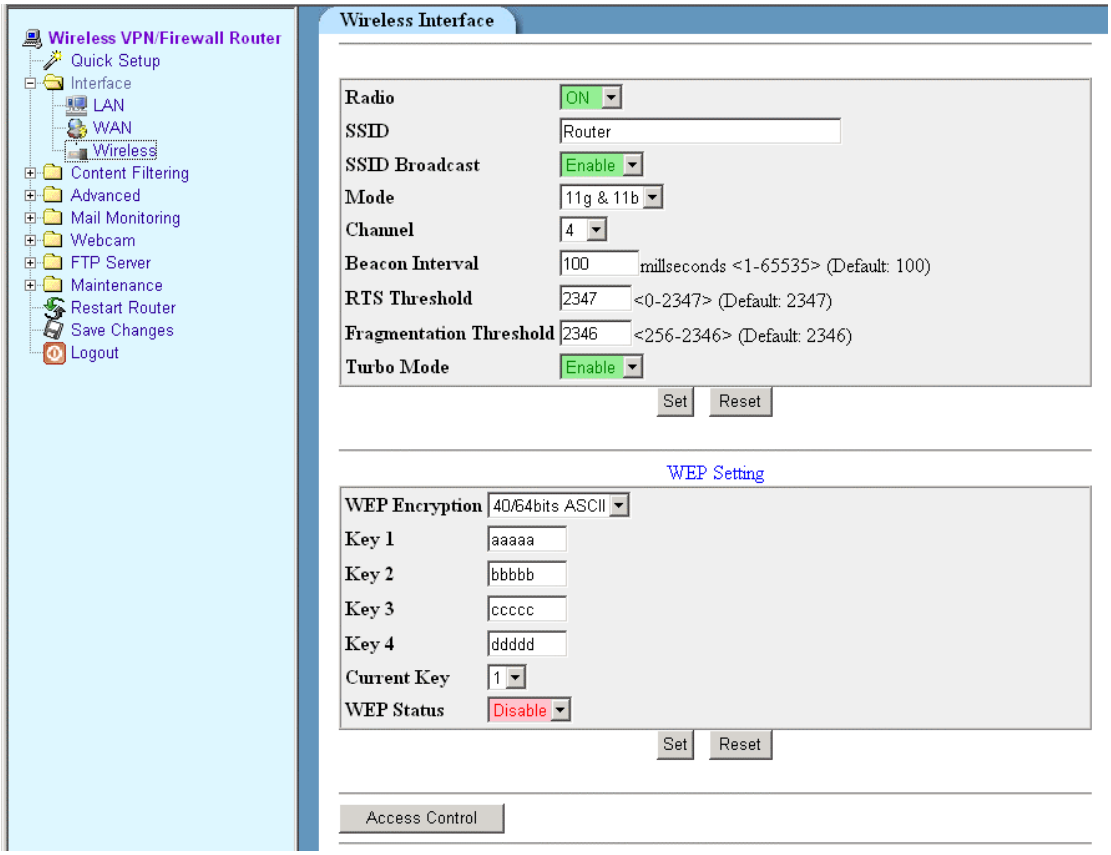
Default Gateway this field indicates Default Gateway address.

Show WAN Information

Click on this button to get access to WAN interface detailed information.

Wireless Interface (Only available to Wireless Router)

In this Wireless section, it lets you make changes to the wireless network settings. You can make changes to the wireless name (SSID), operating channel, encryption security settings, and configure router to be used as an access point.



Radio

The default setting is **on**. When Radio setting is **off**, the wireless function will be disabled and wireless radio signal will not be transmitted and distributed from the router.

SSID (Service Set Identifier)

The SSID is an identification string of up to 32 ASCII characters that differentiate one wireless Access Point router or Access Point from other manufacturers. You can use default SSID or create your own and radio channel unless more than one Wireless Router or Access Point is deployed in the same area. In that case, you should use a different SSID and radio channel for each Wireless Router and Access Point. All Wireless Router and

802.11g/802.11b WLAN client adapters must have the same SSID to allow a wireless mobile client to roam between the wireless routers. By default, the SSID is set to "**Router**".

SSID Broadcast

When wireless clients searching the local area of wireless networks to associate with, they will detect the SSID broadcast by the router. To broadcast the router's SSID, please keep the default setting "enable". If you do not wish to broadcast router's SSID, please select "Disable".

Mode

Your Wireless Router is compatible with both WLAN 11g/11b Client Adapters. In this field, you are able to choose connection mode with both 11g/11b clients or 11g only or 11b only. The default setting is **11g/11b**.

Channel

IEEE 802.11g and 802.11b devices are direct sequence spread spectrum devices that spread a radio signal over a range of frequencies. The range of frequencies used by a direct sequence device is called Channels.
Make sure that all nodes on the same wireless LAN network use the same channel, or the channel usage is automatic when a connection between WLAN clients and your wireless multimedia router are made

Authentication Type

Using "**Shared Key Only**" is recommended for greater security. If "**Both**" is selected, the wireless multimedia router may accept connection requests from unauthorized wireless clients.

Beacon Interval

The default value is 100. Enter a value between 1 and 65,535 milliseconds. The beacon interval value indicates the frequency interval of the beacon. A beacon is a packet broadcast by the router to synchronize the wireless network.

RTS Threshold

This value should remain at its default setting of 2347. The range is 0-2347 bytes. Should you encounter inconsistent data flow, only minor modifications are recommended. If a network packet is smaller than the

present RTS threshold size, the RTS/CTS mechanism will not be enabled. The router sends Request to Send (RTS) frames to a particular receiving station and negotiates the sending of a data frame. After receiving an RTS, the wireless station responds with a Clear to Send (CTS) frame to acknowledge the right to begin transmission.

Fragmentation Threshold

If the length of data frame needing transmission exceeds the fragmentation threshold you set in the column, the data frame will be fragmented. If there is significant interference or high utilization in your wireless network, the smaller fragmentation value can increase the reliability of transmission. However, it is more efficient to set the large fragment size.

Turbo Mode

When Turbo mode is enabled, it allows the router or access point to use frame bursting to deliver the maximum throughput of 2 times faster than any standard 802.11g equipment to 802.11g clients. This measurement is based on aggregate throughput in a mixed 802.11g and 802.11b environment. 802.11g clients also need to support turbo mode in order to make this utility work. Clients that do not support turbo mode will operate normally when it enabled.

WEP Setting

WEP (Wired Equivalent Privacy) is a method of encrypting data transmitted on a wireless network for greater security. If WEP security is enabled, data is encrypted before being transmitted, making communication more secure.

WEP Encryption

Current encryption technology offers 64-bit and 128-bit WEP encryption. Where encryption is concerned, 128-bit has greater security than 64-bit. A WEP key is a string of hexadecimal characters that your wireless network uses in two ways. First, all nodes in your wireless network are identified with a common key. Second, these WEP keys encrypted and decrypted data sent over your wireless network. So, a higher security ensures that hacker have a harder time breaking into your network.

In this field, you are able to select what type of data encryption you wish to use for WEP security. Select the encryption type from drop-down menu by clicking on the options. It is recommended to use 128-bit encryption for higher security. From this drop-down menu, you have option to decide the character format for WEP key entries.

Hex Set WEP key entries with the range of 0-9 and A-F.

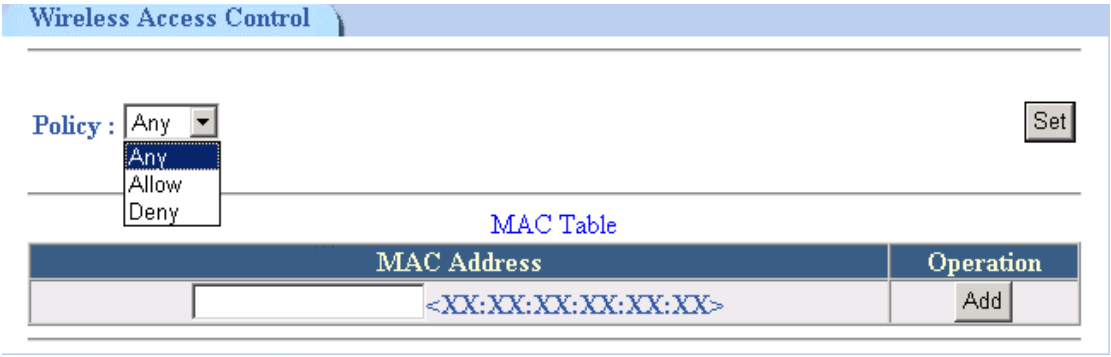
ASCII Set WEP key entries with any character or symbol button on your keyboard.

After selected WEP encryption type, you will require to put WEP key entries. Select which WEP key (1-4) will be used when the router send data, then select that number from the **Current Key** field. Type in the values in the field by following to Hex and ASCII entry rules indicated above. Keep typing the values until the letters or digits stop appearing on KEY field.

Select **Enable** from **WEP** field after you had completed the WEP key value entries. Click on **SET** to confirm your WEB settings.

Access Control

As the figure, the wireless network access control is devided to two parts. The upper part is the access policy; the lower part is the MAC table.



There are three value options of access policy:

Any	the MAC table does not work, and all the wireless equipments will be accepted
Allow	only accept the wireless equipments set in MAC table
Deny	deny the the wireless equipments set in MAC table

After the access policy is selected, you have to click Set button to make the new setting work.

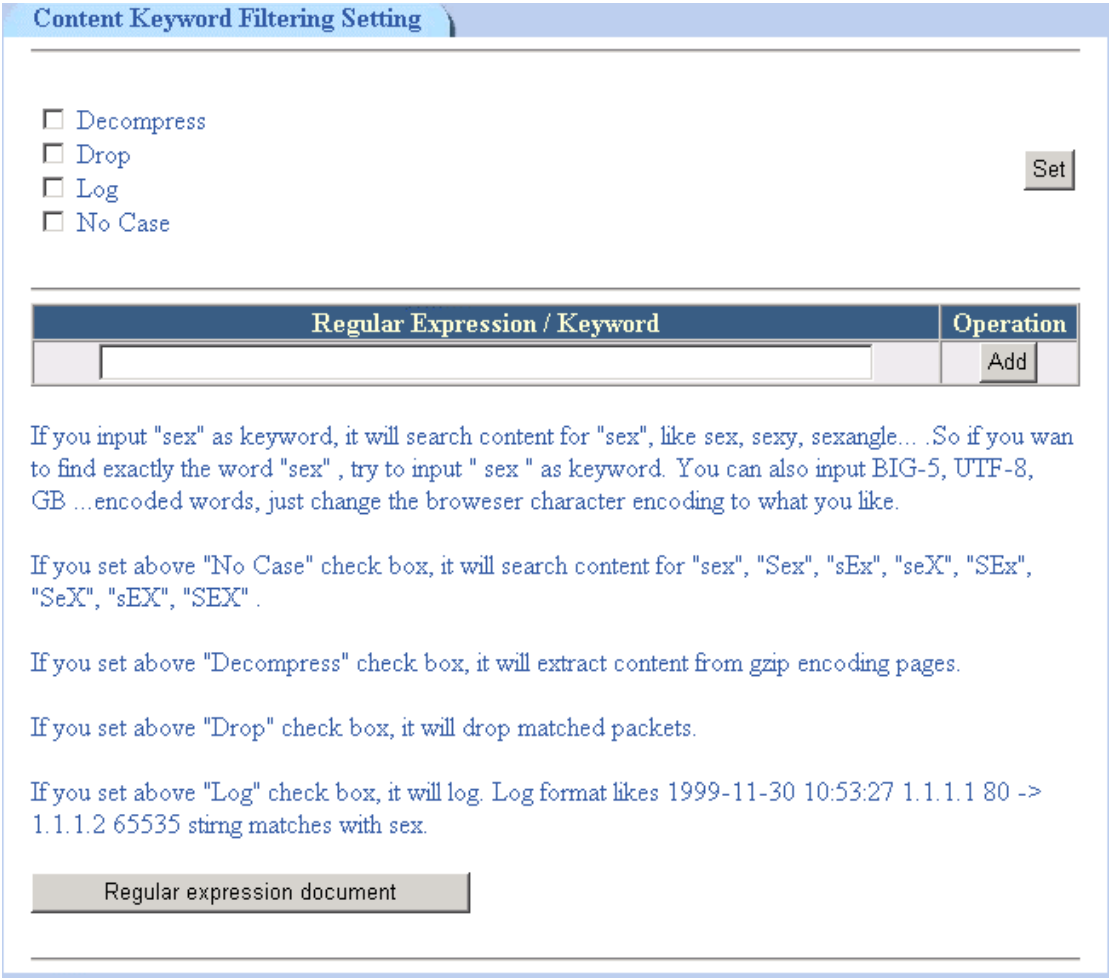
If you want to add wireless equipment to MAC table, enter the hardware address of the lower left field, and then press Add button to add it. If you want to delete equipment from MAC table, please check the corresponding Delete block on the right, and then press Delete button to delete the selected equipment. Reset button can be used to cancel the selection.

Chapter 5: Content Filtering

There are four selections under Content Filter: **Keyword Filtering, URL Blocking, Trusted IP** and **Port Checking.**

Trusted IP has the highest priority. In other words, if certain URL or keyword is being blocked, but the IP address is in the Trusted IP range, it is considered safe.

Keyword Filtering



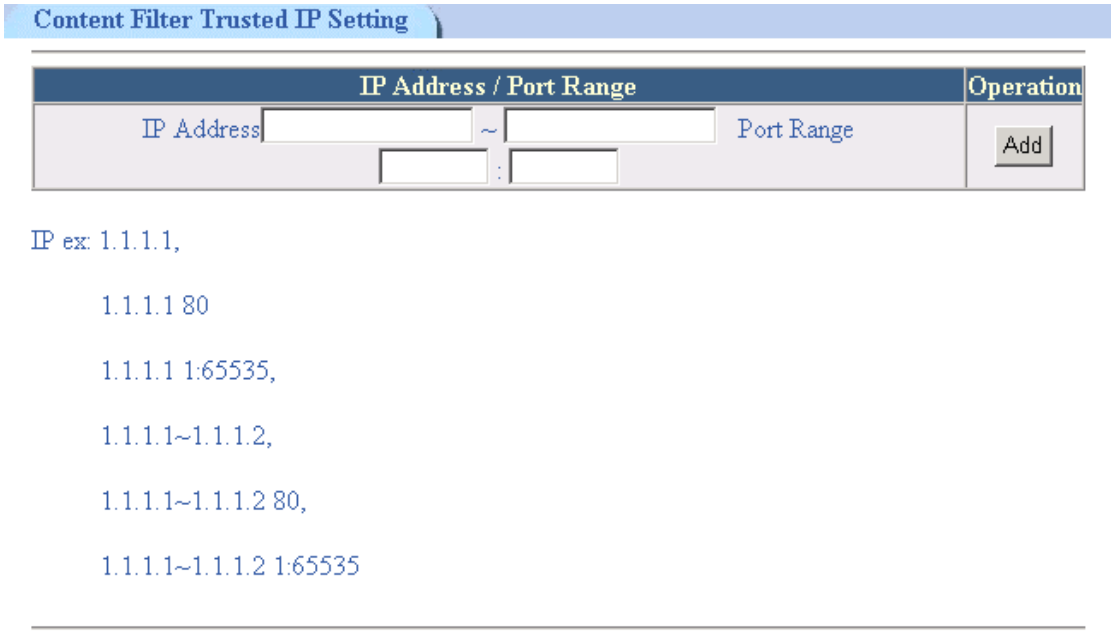
1. Determine first what action would be applied to the keyword. Check off the appropriate box and click Set.
2. Enter the expression that wishes to be blocked. For example, you can enter the word “violence” in the field. Click Add to add it to the expression list. The action chosen in Step 1 will be applied to the

situation when the keyword appears. For example, if **DROP** is chosen; then web pages contain the word, violence, will be dropped and will not be available.

URL Blocking

Enter the URLs that are considered inappropriate and wish to be blocked. Click **Add** for it to be effective.

Trusted IP



Trusted IP means that the IP addresses are considered safe and will not pose