

# **Multimedia VPN/Firewall Broadband Router**

## **User's Manual**

## Chapter 1: Introduction

### Overview

A true heart of your home/office network, MBIG-xx Multi-media 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, MBIG-xx 's full IPSec Virtual Private Network (VPN) capability provides complete data privacy.

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

Equipped with the most advanced technology available today, MBIG-XX 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 (only available to VPN equipped model)
  - \* Support (56-Bit) DES and (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
- 4 \* USB 2.0 Port for Plug and Share Utilities
- Print Server, Web Cam Server and FTP Server built-in

## Multimedia VPN/Firewall Broadband Router

### Package content

- One MBIG-XX Multimedia VPN/Firewall Router with 4\*USB 2.0 Interfaces
- One Power Supply
- One User's manual in CD

### System Requirements

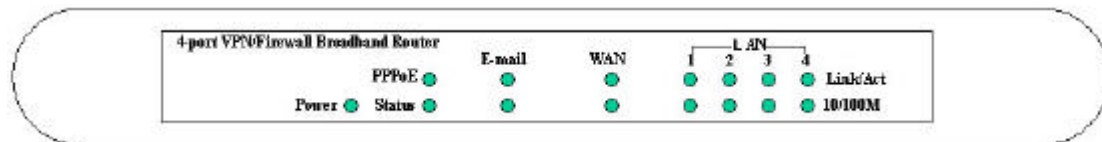
- One RJ-45 Broadband Internet connection
- One PC with 10/100Mbps Network card installed
- TCP/IP network protocol for each PC which connect to the router
- Internet Browser installed in PC
- RJ-45 Cat.5 network cables

## 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 data 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

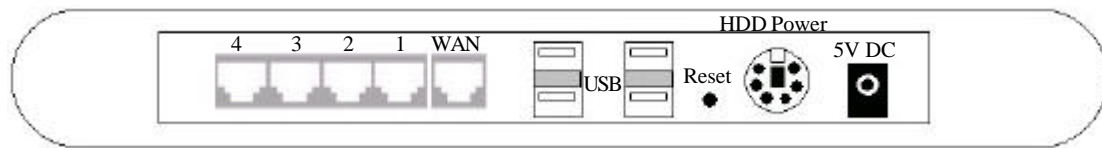
Red	The LED illuminates when router is boot-up after connected to power or the router has connection failure. It is necessary to reset the router by pressing the reset button at rear panel of router
-----	---------------------------------------------------------------------------------------------------------------------------------------------------------------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

### 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
--------	-------------------------------------------------------------------------------------------------

## 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 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.
5. Power on your Cable/DSL modem
6. 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.

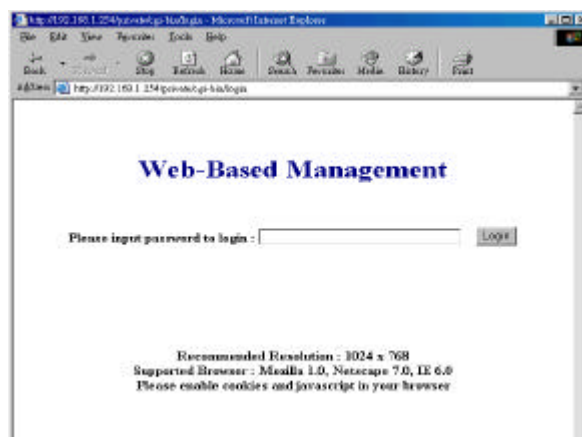
## Login to Web-Based Management page

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

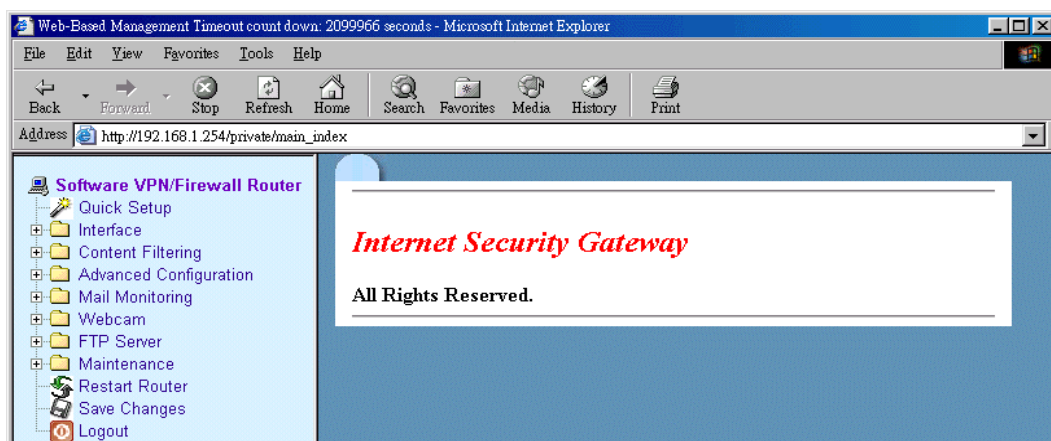
The default IP address of the router is 192.168.1.254

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

### DHCP

Web-Based Management Timeout count down: 2099981 seconds - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Refresh Home Search Favorites Media History Print

Address [http://192.168.1.254/private/main\\_index](http://192.168.1.254/private/main_index)

**Software VPN/Firewall Router**

- Quick Setup
- Interface
- Content Filtering
- Advanced Configuration
- Mail Monitoring
- Webcam
- FTP Server
- Maintenance
- Restart Router
- Save Changes
- Logout

### Quick Setup

<b>WAN Interface</b>	
*Connection Type	DHCP
<b>LAN Interface</b>	
*IP Address	192.168.1.254 <A.B.C.D>
*Subnet Mask	255.255.255.0
<b>Web-Based Management Password</b>	
*New Password	*****
*Verify	*****
<b>Network Time Protocol</b>	
Time Zone	(GMT) England
NTP Server	None

Set Reset

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.

## PPPoE

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

Web-Based Management Timeout count down: 2099997 seconds - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Refresh Home Search Favorites Media History Print

Address [http://192.168.1.254/private/main\\_index](http://192.168.1.254/private/main_index)

**Software VPN/Firewall Router**

- Quick Setup
- Interface
- Content Filtering
- Advanced Configuration
- Mail Monitoring
- Webcam
- FTP Server
- Maintenance
- Restart Router
- Save Changes
- Logout

**Quick Setup**

**WAN Interface**

\*Connection Type: PPPoE

\*User Name: id@your.isp

\*Password: \*\*\*\*\*

\*PPPoE MRU: 1492 <1-1500>

\*PPPoE MTU: 1492 <1-1500>

\*LCP Echo Failure: 3 <1-10>times

\*LCP Echo Interval: 20 <1-60>seconds

**LAN Interface**

\*IP Address: 192.168.1.254 <A.B.C.D>

\*Subnet Mask: 255.255.255.0

**Web-Based Management Password**

\*New Password: \*\*\*\*\*

\*Verify: \*\*\*\*\*

**Network Time Protocol**

Time Zone: (GMT) England

NTP Server: None

Set Reset

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](mailto: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.

## 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.

## 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.

Web-Based Management Timeout count down: 2099980 seconds - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Refresh Home Search Favorites Media History Print

Address [http://192.168.1.254/private/main\\_index](http://192.168.1.254/private/main_index)

**Software VPN/Firewall Router**

- Quick Setup
- Interface
- Content Filtering
- Advanced Configuration
- Mail Monitoring
- Webcam
- FTP Server
- Maintenance
- Restart Router
- Save Changes
- Logout

### Quick Setup

#### WAN Interface

\*Connection Type: Static

\*IP Address: <A.B.C.D>

\*Subnet Mask: 255.255.255.0

\*Default Gateway: <A.B.C.D>

\*DNS[1]: <A.B.C.D>

DNS[2]: <A.B.C.D>

#### LAN Interface

\*IP Address: 192.168.1.254 <A.B.C.D>

\*Subnet Mask: 255.255.255.0

#### Web-Based Management Password

\*New Password: \*\*\*\*\*

\*Verify: \*\*\*\*\*

#### Network Time Protocol

Time Zone: (GMT) England

NTP Server: None

Set Reset

## PPTP

If your ISP provides PPTP 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](mailto:id@isp.net).  
Please check double check with your ISP for this information.
4. Enter your corresponding Password
5. Enter at least one DNS Server IP address as provided by your ISP.

Web-Based Management Timeout count down: 2099988 seconds - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Refresh Home Search Favorites Media History Print

Address [http://192.168.1.254/private/main\\_index](http://192.168.1.254/private/main_index)

**Software VPN/Firewall Router**

- Quick Setup
- Interface
- Content Filtering
- Advanced Configuration
- Mail Monitoring
- Webcam
- FTP Server
- Maintenance
- Restart Router
- Save Changes
- Logout

**Quick Setup**

**WAN Interface**

\*Connection Type: PPTP

\*IP Address: 192.168.2.1 <A.B.C.D>

\*Subnet Mask: 255.255.255.0

\*Gateway: 192.168.2.254 <A.B.C.D>

\*User Name: id@your.isp

\*Password: \*\*\*\*\*

\*PPTP MRU: 1492 <1-1500>

\*PPTP MTU: 1492 <1-1500>

\*LCP Echo Failure: 3 <1-10>times

\*LCP Echo Interval: 20 <1-60>seconds

**LAN Interface**

\*IP Address: 192.168.1.254 <A.B.C.D>

\*Subnet Mask: 255.255.255.0

**Web-Based Management Password**

\*New Password: \*\*\*\*\*

\*Verify: \*\*\*\*\*

**Network Time Protocol**

Time Zone: (GMT) England

NTP Server: None

Set Reset

## 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.

### LAN I nterface

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.

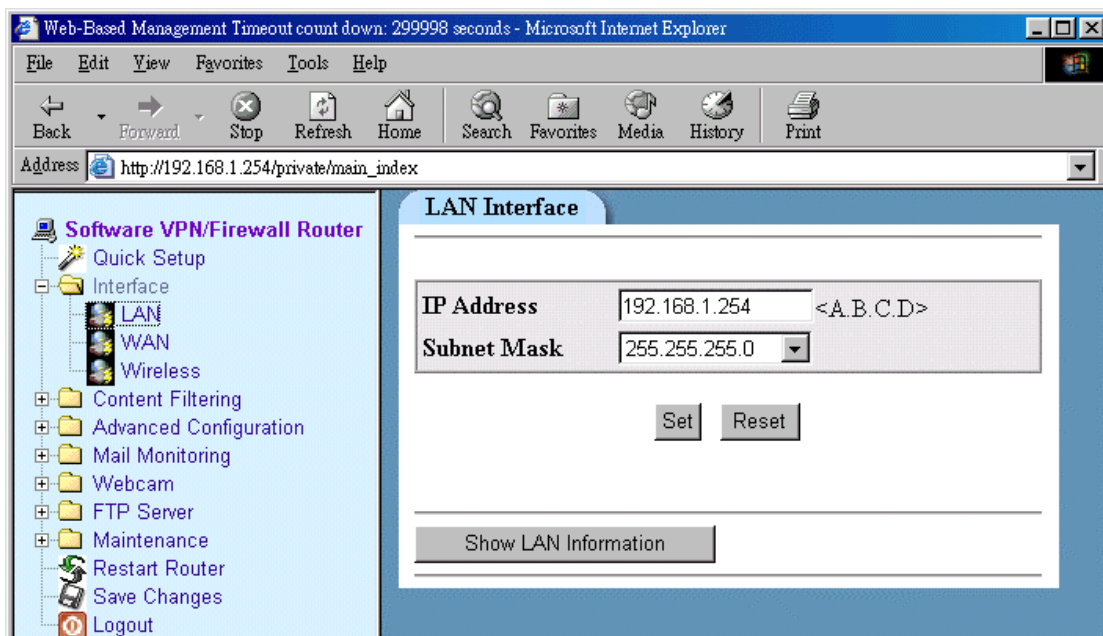
NTP Server - This field allows you to set IP address of NTP Server to synchronize your system time.

## 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

The screenshot shows a web browser window titled "Web-Based Management Timeout count down: 299991 seconds - Microsoft Internet Explorer". The address bar shows "http://192.168.1.254/private/main\_index". The left sidebar contains a tree view with the following items: "Software VPN/Firewall Router", "Quick Setup", "Interface" (expanded), "LAN", "WAN" (selected), "Wireless", "Content Filtering", "Advanced Configuration", "Mail Monitoring", "Webcam", "FTP Server", "Maintenance", "Restart Router", "Save Changes", and "Logout". The main content area is titled "WAN Interface" and contains the following configuration fields:

MAC	<input type="text" value="00:03:54:00:18:c4"/> (Original: 00:03:54:00:18:c4)
MTU	<input type="text" value="1500"/> <1-1500>
<input type="button" value="Set"/> <input type="button" value="Reset"/>	

---

Connection Type	<input type="text" value="Static"/>
IP Address	<input type="text" value="10.1.1.1"/> <A.B.C.D>
Subnet Mask	<input type="text" value="255.255.255.0"/>
Default Gateway	<input type="text" value="10.1.1.2"/> <A.B.C.D>
<input type="button" value="Set"/> <input type="button" value="Reset"/>	

Mac                      It shows Mac ID of WAN port

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

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 Access Point 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.

**Wireless Interface**

SSID

SSID Broadcast

Enable

Mode

11g & 11b

Channel

9

Authentication Type

Both

Beacon Interval

100

milliseconds <1-65535> (Default: 100)

RTS Threshold

2347

<0-2347> (Default: 2347)

Fragmentation Threshold

2346

<256-2346> (Default: 2346)

Turbo Mode

Disable

Set

Reset

WEPS Setting

WEP Encryption

40/64bits ASCII

Key 1

Key 2

Key 3

Key 4

Current Key

1

WEP Status

Enable

Set

Reset



### 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

It is the signal sent periodically by wireless access point to provide synchronization among the stations in wireless LAN.

### RTS Threshold

RTS packet is use to account for potential hidden stations. This feature allows you to set the size of RTS packet.

### 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.

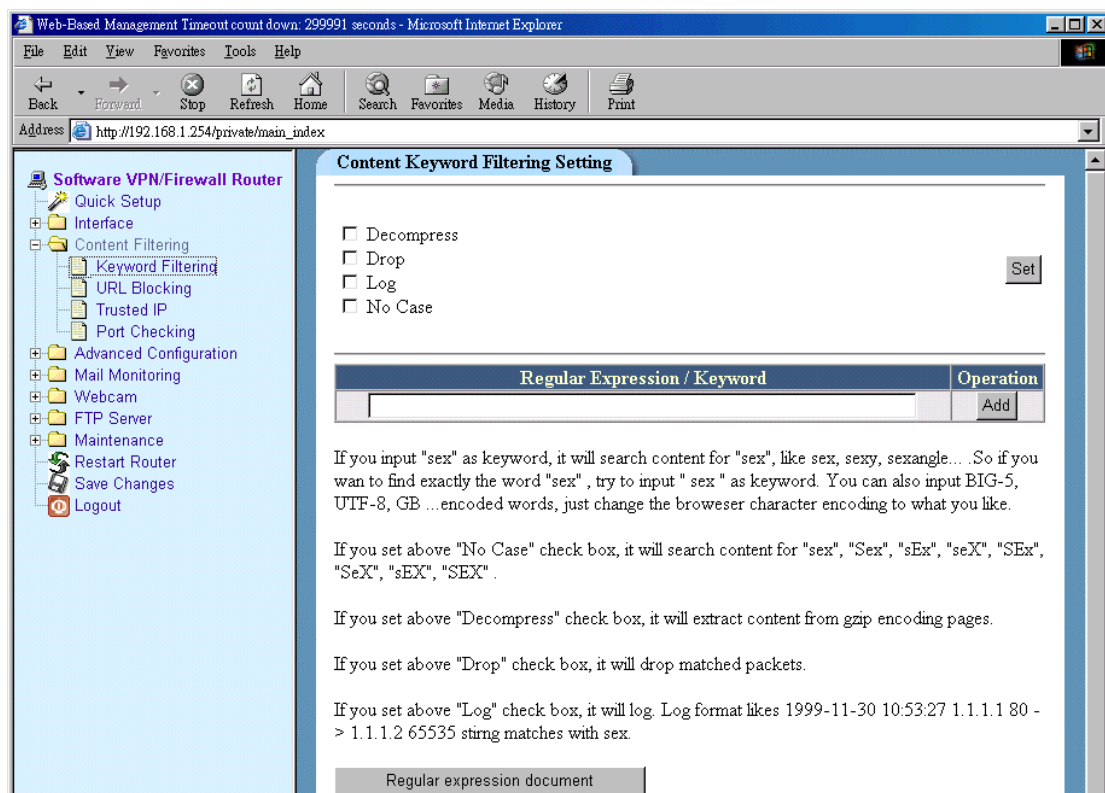
Select Enable from WEP field after you had completed the WEP key value entries. Click on SET to confirm your WEB settings.

## Chapter 4: 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.

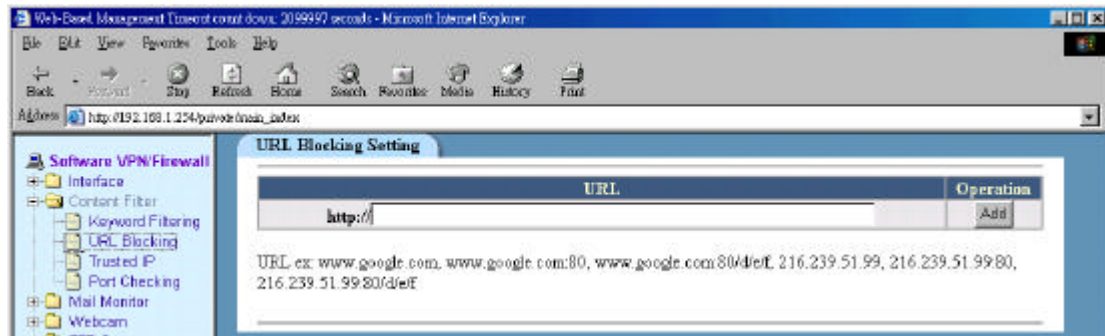
### Keyword Filtering



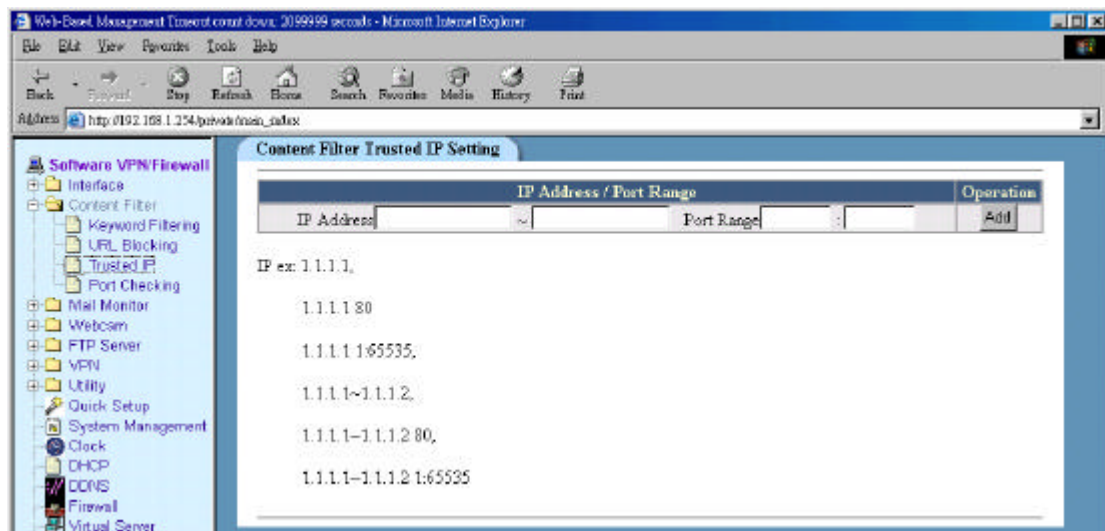
1. Determine first what action would be applied to the keyword. Check off the appropriate box and click Set.
2. Enter the expression that wishes to be blocked. For example, you can enter the word "violence" in the field. Click Add to add it to the expression list. The action chosen in Step 1 will be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



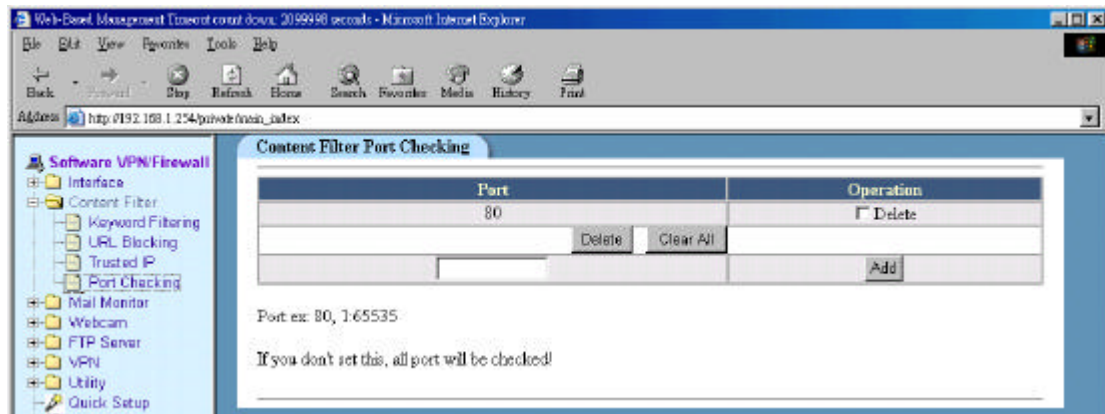
## Trusted IP



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

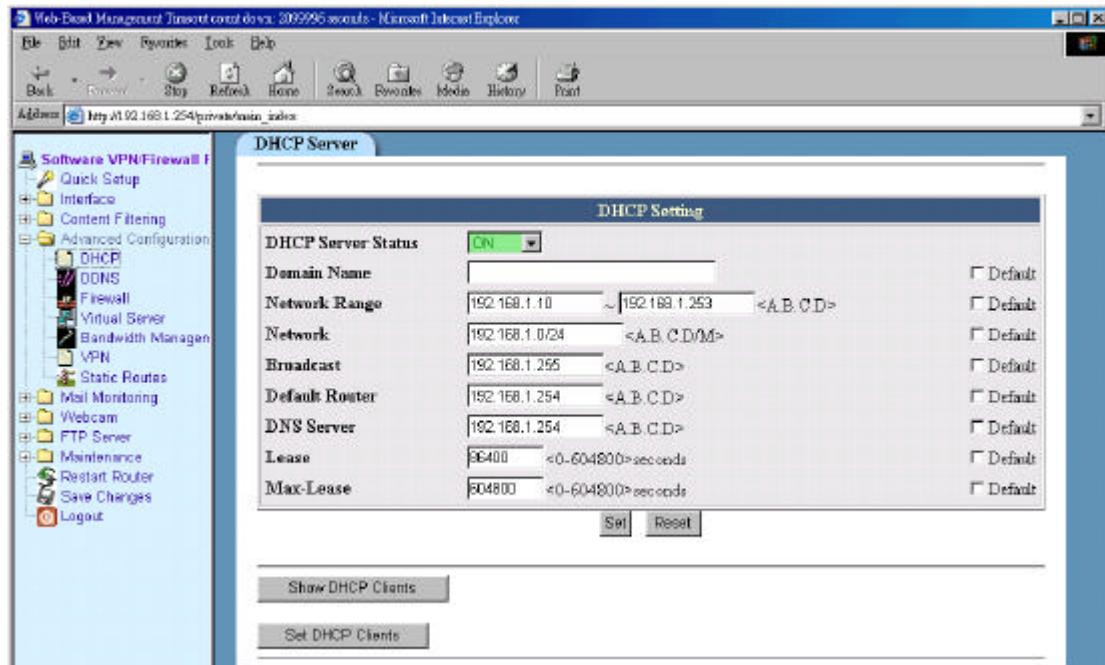
## Port Checking



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 5: Advanced Configurations

### DHCP

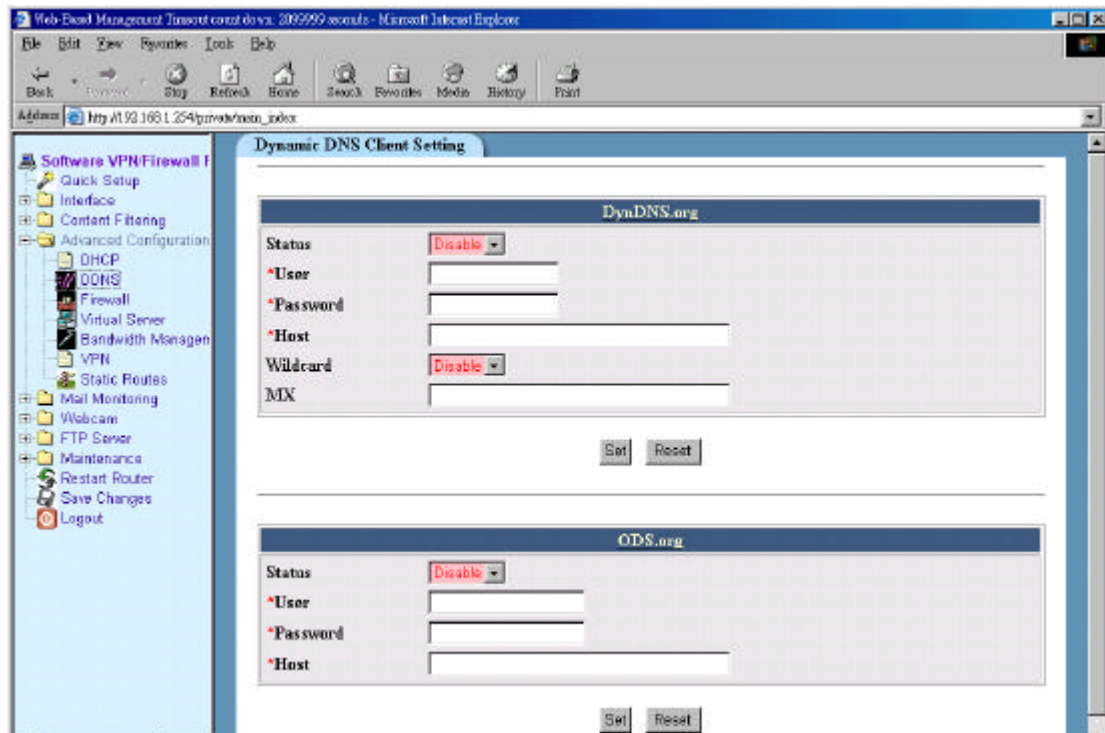


A DHCP (Dynamic Host Configuration Protocol) Server automatically assigns IP addresses to each computer on your network. Unless you already have one, it is highly recommended that the router set up as a DHCP Server.

DHCP Server Status	Click ON to activate DHCP Server
Domain Name	Type in the domain name if you have one
Network Range	Define IP range for DHCP Server when issuing IP
Network	You can change network domain if necessary
Broadcast	Modify Broadcast IP address if Network domain changed
Default Router	Modify default router's IP address here
DNS Server	Modify your DNS Server IP address here
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.

## 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.



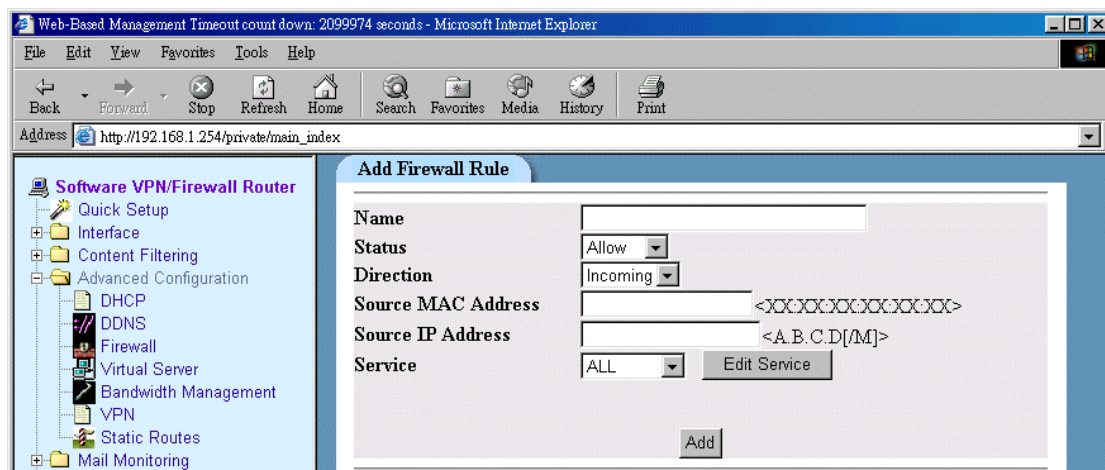
## Firewall

---

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.

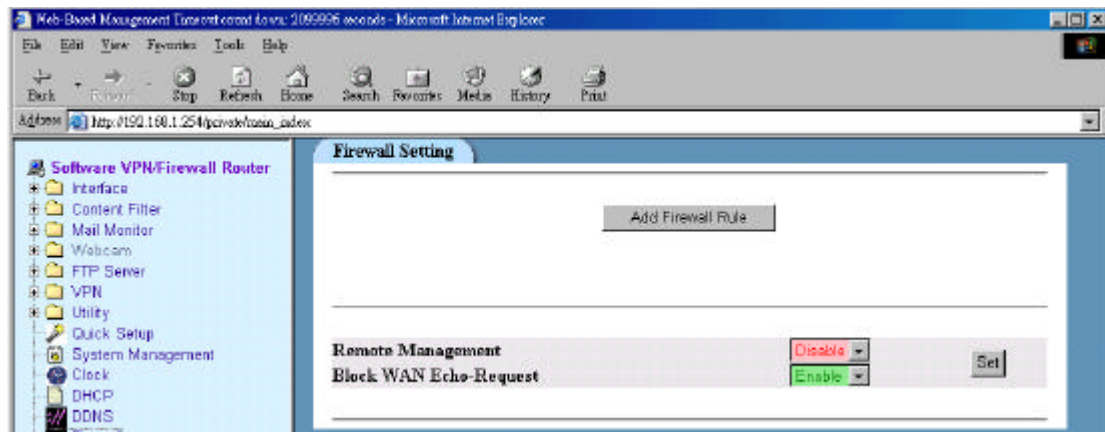
In this Firewall section, it divides into three parts. There are Add Firewall Rule, Remote Management and Block WAN Echo-Request.

### 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.

## 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.

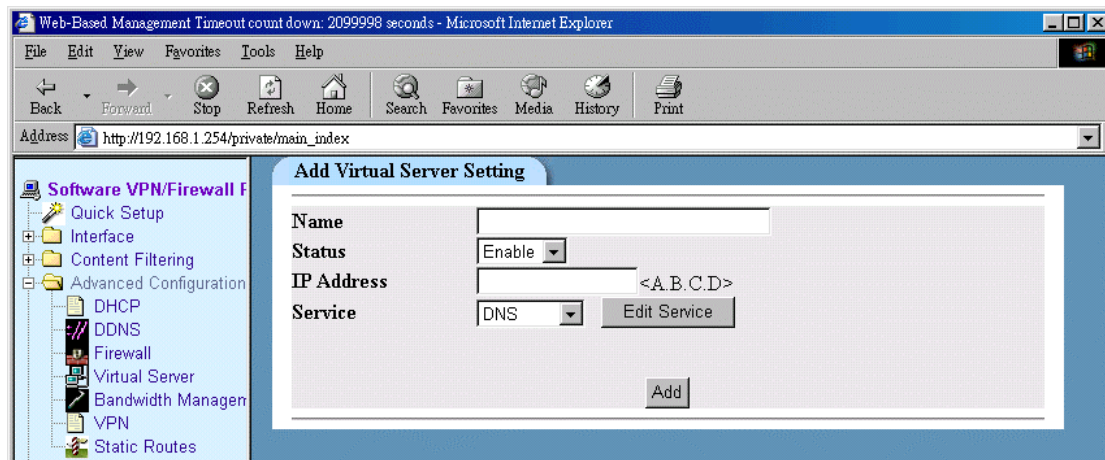
To activate Remote Management, please select Enable and click on Set to confirm the setting.

## 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.

## Virtual Server

---



### Virtual Server

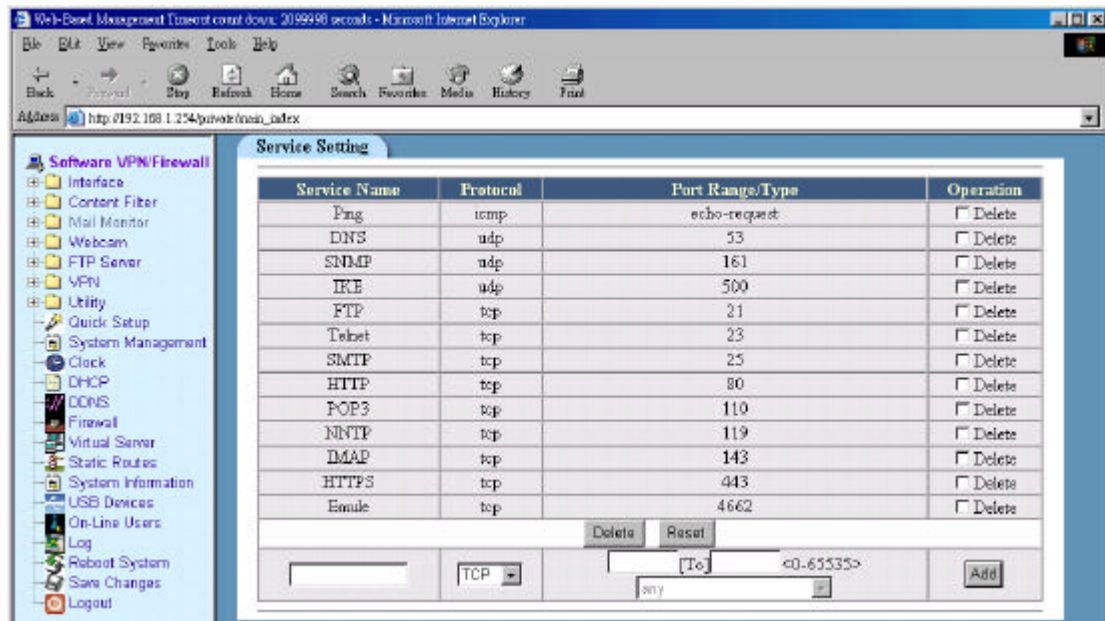
To make services, like WWW, FTP, provided by a server in your local network accessible for outside users, you should specify a local IP address to the server.

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

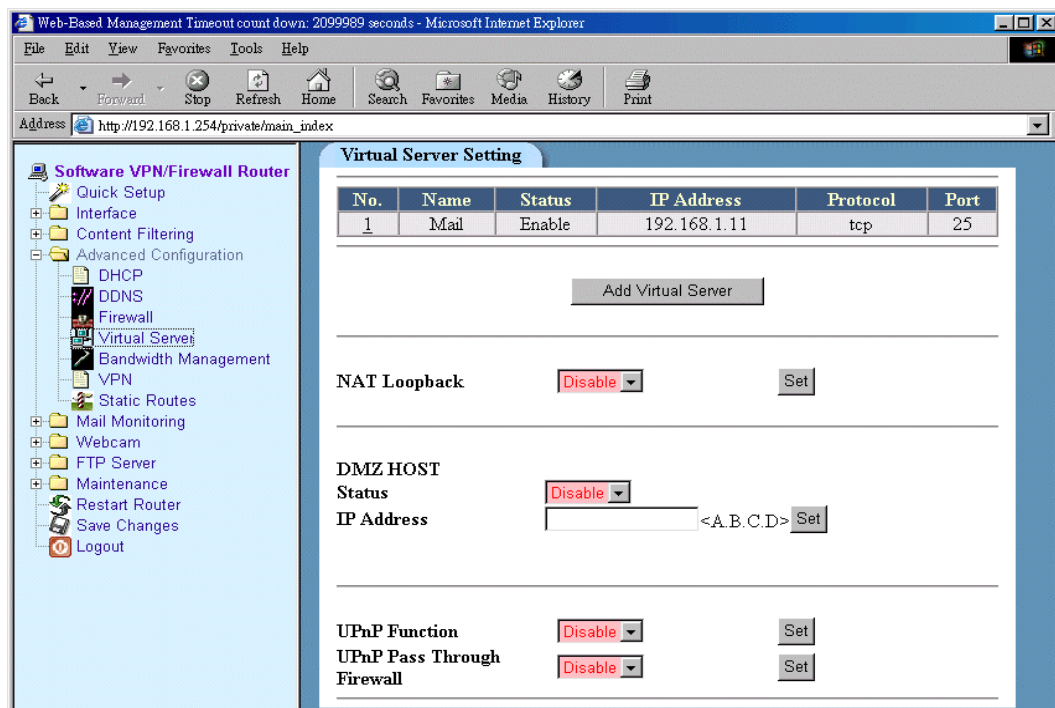
1. Select Virtual Server from the main menu and then click on Add Virtual Server button
2. Type in Server name. It can be anything as long as it is recognized by user
3. To activate Virtual Server function, click on Enable from Status box
4. IP Address – enter destination IP address that you like to 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



### 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. Basically, once you plug the hardware onto the network, it will take care of preparing itself for use.

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

---

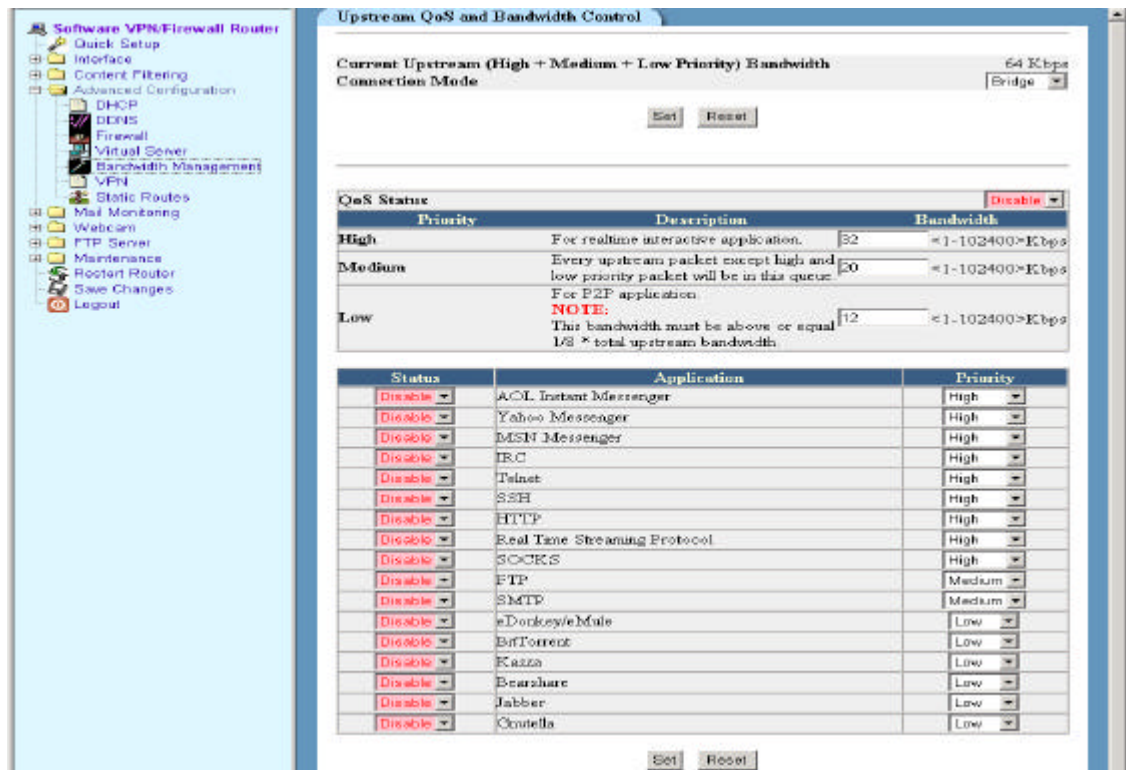
### QoS Bandwidth Management

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, WinMX and so on. Peer-to-Peer platform provides function of linking up all people who are online and share MP3, or movie files from each other's hard disk. When you're online and download music from other people's computer, at the same time, you are also sharing your music archive to other users on the network for them to download your files. When other online user downloading the MP3 from your hard disk, your Internet's upstream bandwidth will be eat up and the other user on your LAN network will 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.



## Multimedia VPN/Firewall Broadband Router

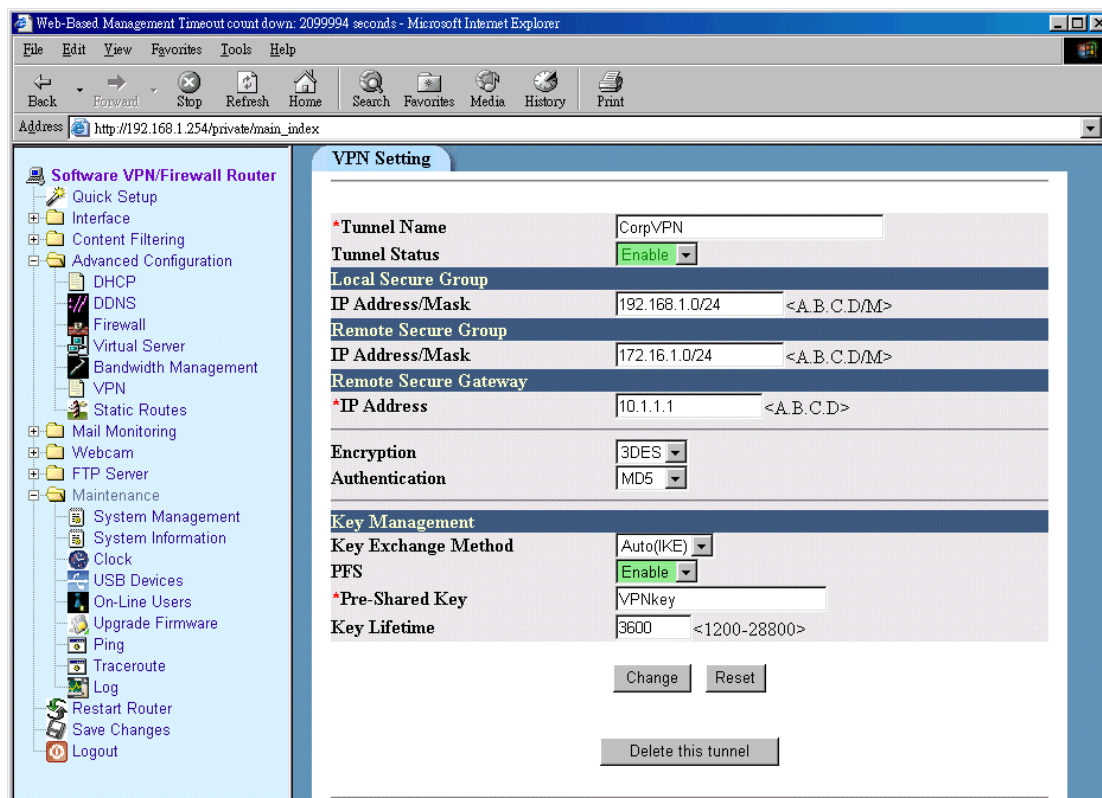


Please take the following instructions of how to configure QoS management:

1. In Connection Mode, you need to select Bridge mode or Routing mode. In most case, then you're using PPPoE or PPTP for your Internet connection, please select Bridge mode. If you're using Static for your Internet connection, please select Routing mode. The default value is Bridge Mode. Click on set to confirm the setting.
2. Select enable from QoS status field.
3. You need to know the maximum upstream bandwidth is allowed for your Internet connection provided by your ISP.
4. 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.
5. 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.
6. 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.
7. Click on Set to confirm your settings.

## VPN

Virtual Private Networking (VPN) is a security measure that basically creates a secure connection between two remote locations.



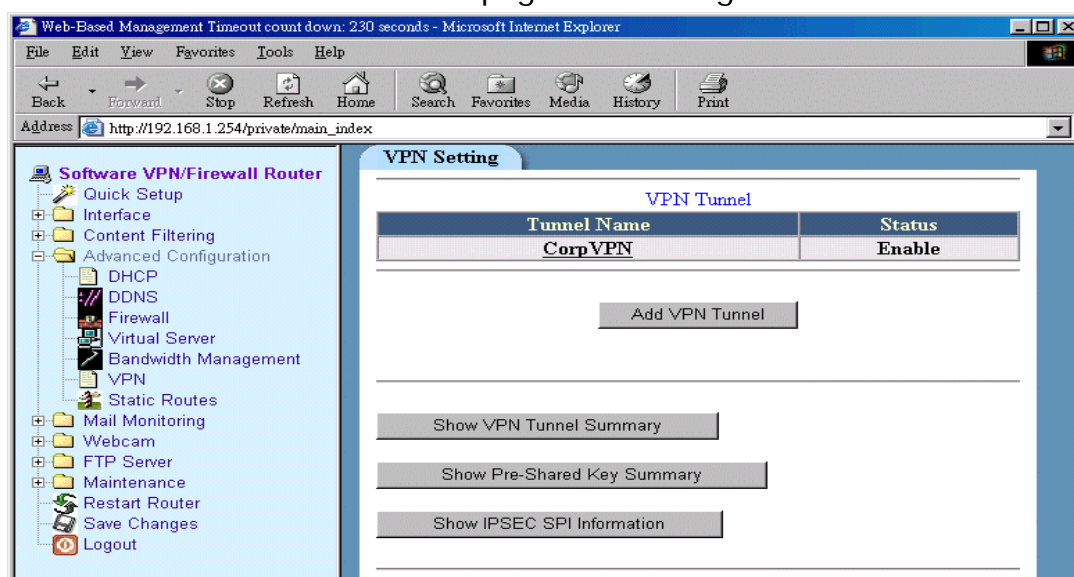
In order to create a secure VPN tunnel or channel between two endpoints, please take the following steps.

1. Go to Advanced Configuration in main menu and select VPN.
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.

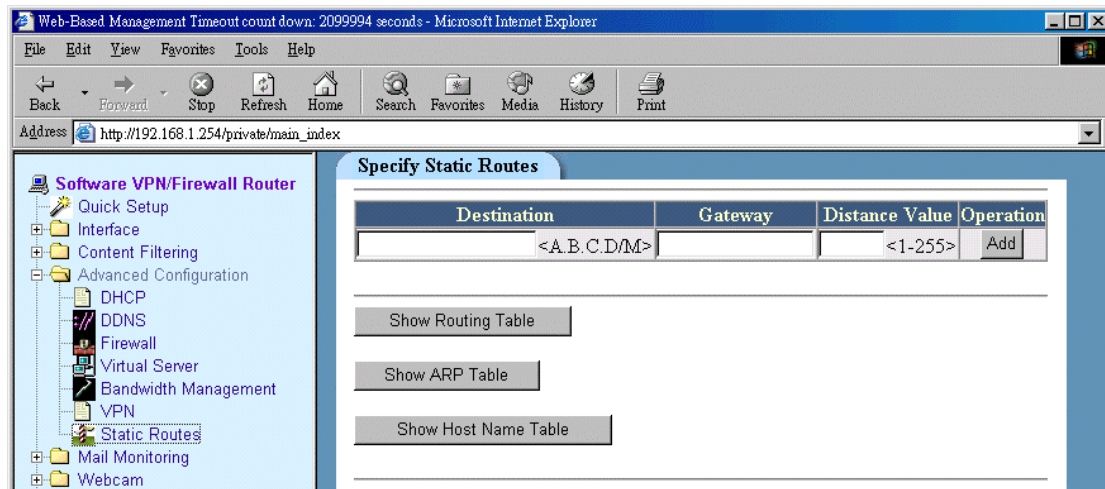


7. The Remote Security Gateway is the VPN device, such as a second VPN router on the remote end of the VPN tunnel. Enter the IP address of the VPN device at the other end of the tunnel. The remote VPN device can be another VPN router, a VPN server, or a computer with VPN client software that supports 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:



## 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.

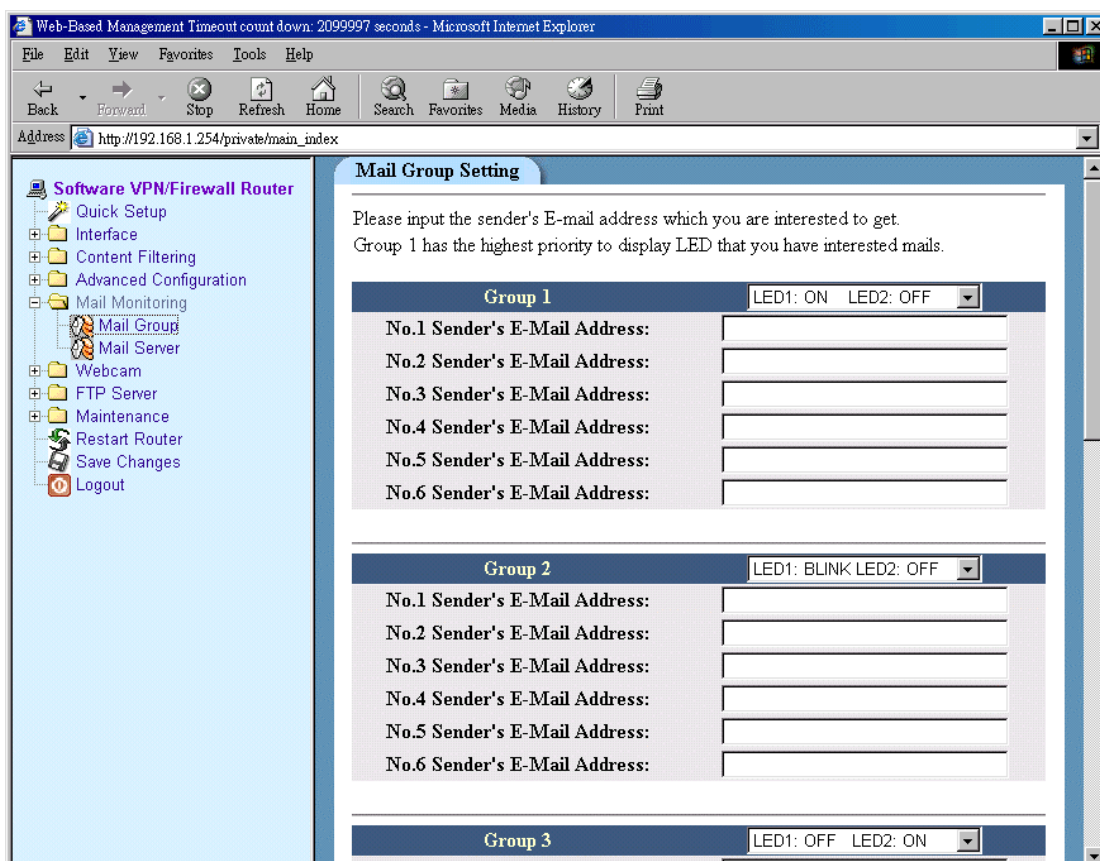
Click on Show Routing Table to check your new static route information.

## Chapter 6: 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.

Web-Based Management Timeout count down: 2099995 seconds - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Refresh Home Search Favorites Media History Print

Address [http://192.168.1.254/private/main\\_index](http://192.168.1.254/private/main_index)

**Software VPN/Firewall Router**

- Quick Setup
- Interface
- Content Filtering
- Advanced Configuration
- Mail Monitoring
  - Mail Group
  - Mail Server**
- Webcam
- FTP Server
- Maintenance
- Restart Router
- Save Changes
- Logout

### E-Mail Server Setting

Monitor Interval:  <30-3000>seconds

☐ Monitor any incoming mail and use Group 1's LED setting (Skip Mail Group)

No	Status
1	
2	
3	
4	
5	
6	

No	Active	Server	Type	User	Password
1	<input type="checkbox"/>		POP3		
2	<input type="checkbox"/>		POP3		
3	<input type="checkbox"/>		POP3		
4	<input type="checkbox"/>		POP3		
5	<input type="checkbox"/>		POP3		
6	<input type="checkbox"/>		POP3		

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 7: Maintenance

### System Management

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

Web-Based Management Timeout count down: 2099989 seconds - Microsoft Internet Explorer

Address: [http://192.168.1.254/private/main\\_index](http://192.168.1.254/private/main_index)

**Software VPN/Firewall Router**

- Quick Setup
- Interface
- Content Filtering
- Advanced Configuration
- Mail Monitoring
- Webcam
- FTP Server
- Maintenance
  - System Management**
  - System Information
  - Clock
  - USB Devices
  - On-Line Users
  - Upgrade Firmware
  - Ping
  - Traceroute
  - Log
  - Restart Router
  - Save Changes
  - Logout

### System Management Setting

Network Name:  ☐ Default

Domain Name:  ☐ Default

Domain Lookup:  ☐ Default

Management Timeout:  <0-35791>Min.  <0-2147483>Sec. ☐ Default

DNS[1]:  <A.B.C.D>

DNS[2]:  <A.B.C.D>

DNS[3]:  <A.B.C.D> ☐ Default

### Password Setting

\*New Password:  \*Verify:

### Server Configuration

Server	Port	Status
Management	<input type="text" value="80"/> <1-65535>	<input type="text" value="HTTP"/>

### Management Access Control

Access	IP Address	Operation
<input type="text" value="deny"/>	<input type="text"/> <A.B.C.D[/M]>   any	<input type="button" value="Add"/>

### System Settings

Network Name

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

Domain Name

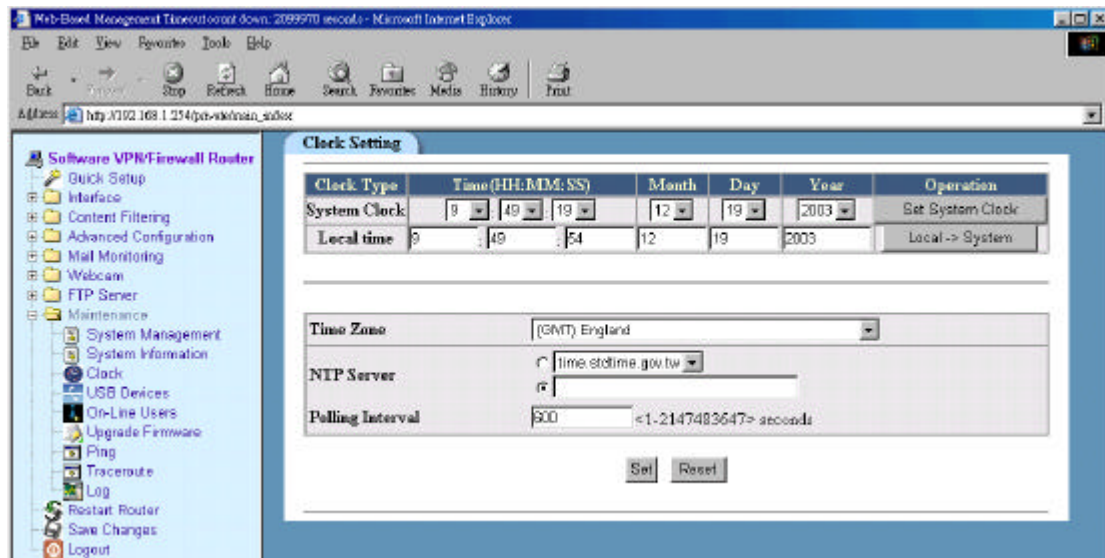
You can set domain name of where your router is located here. If you did not apply the domain name from your ISP, please leave it blank.

- 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.

The screenshot shows a web browser window titled "Web-Based Management Timeout count down: 2099995 seconds - Microsoft Internet Explorer". The address bar shows "http://192.168.1.254/private/main\_index". The left sidebar contains a tree view of the router's management options, including "Software VPN/Firewall Router", "Quick Setup", "Interface", "Content Filtering", "Advanced Configuration", "Mail Monitoring", "Webcam", "FTP Server", "Maintenance", "System Management", "System Information" (selected), "Clock", "USB Devices", "On-Line Users", "Upgrade Firmware", "Ping", "Traceroute", "Log", "Restart Router", "Save Changes", and "Logout".

The main content area displays the "System Information" page, which includes the following sections:

**Copyright© 1999-2003**

Web-Based Management Software Version 1.5 Dec 17 2003 19:17:16  
SysCTRL v1.0.2, 2003  
MSP MultiND v1.0.1, 2003.  
Firmware Version 1.01.023 Wed Dec 17 19:19:12 CST 2003  
O.S. Build Wed Dec 17 16:49:03 CST 2003

**CPU Information**

User	8.4%
System	7.7%
Nice	0.0%
Idle	83.7%

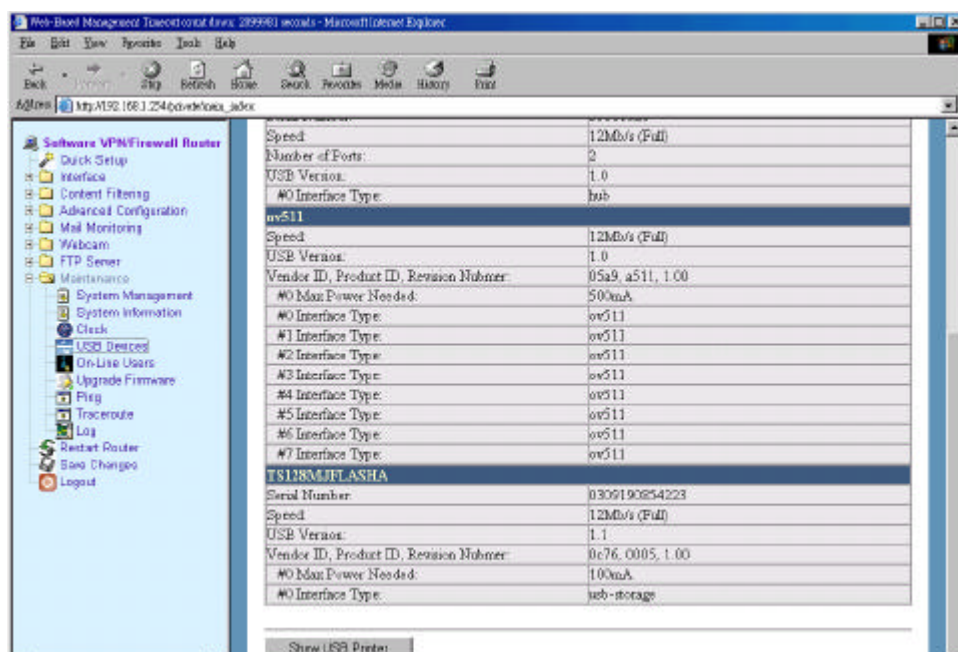
**System Information**

System Time	Fri Dec 19 09:48:36 2003		
System Uptime	0 day 0 hour 56 minutes		
Load Average	1.05	1.28	1.28
Memory Information	Total 30276 K	Used 13260 K	Free 17016 K



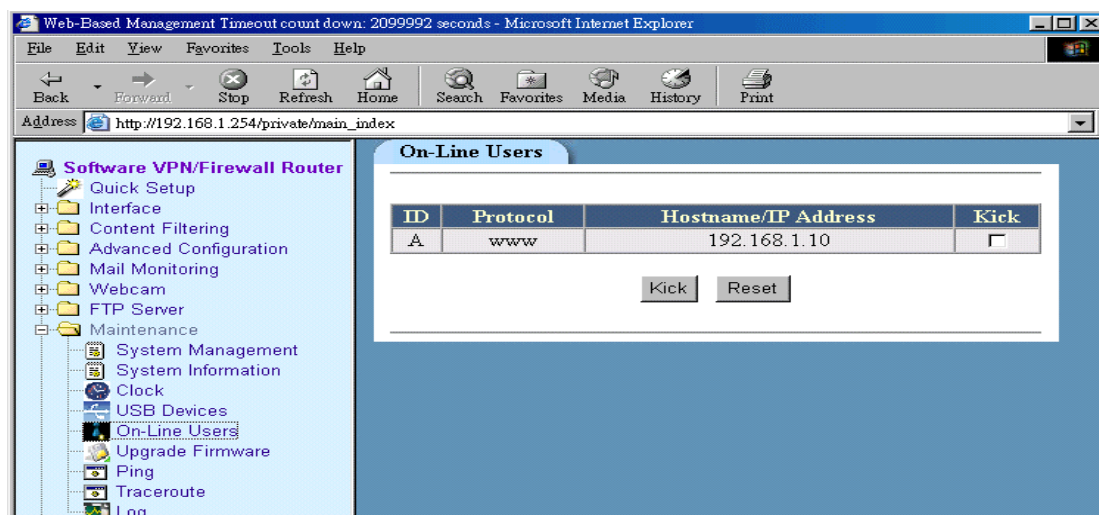
## USB Devices

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.



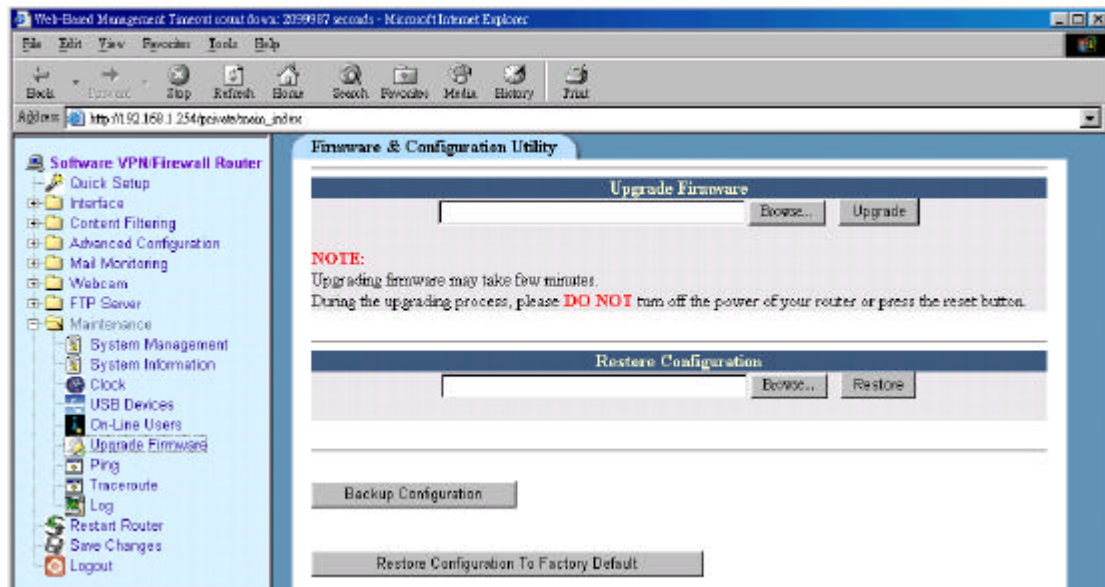
## On-Line Users

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

Updated firmware can be upgraded anytime through this utility. Before upgrading firmware, please make sure you had obtained new firmware from your supplier and save in your hard disk.



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.

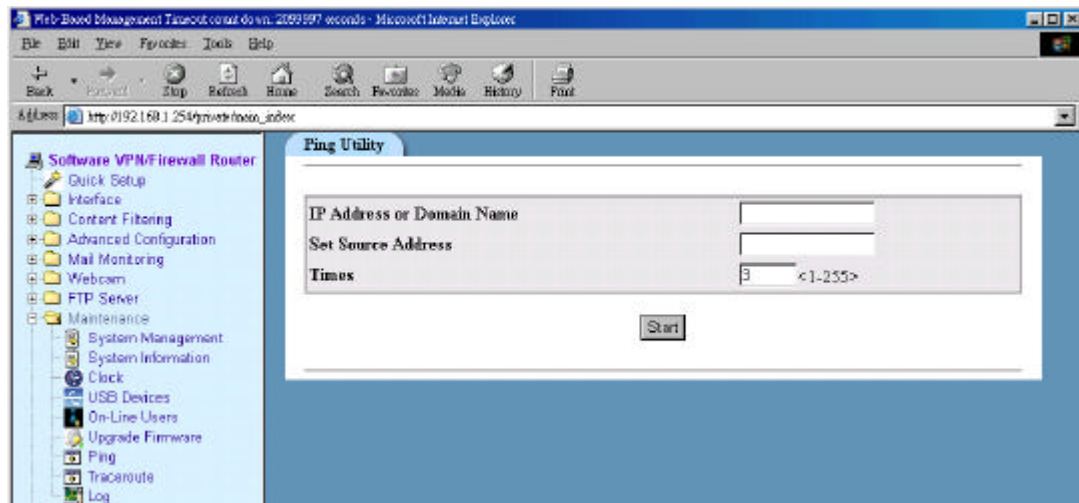
### Restore Configuration

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

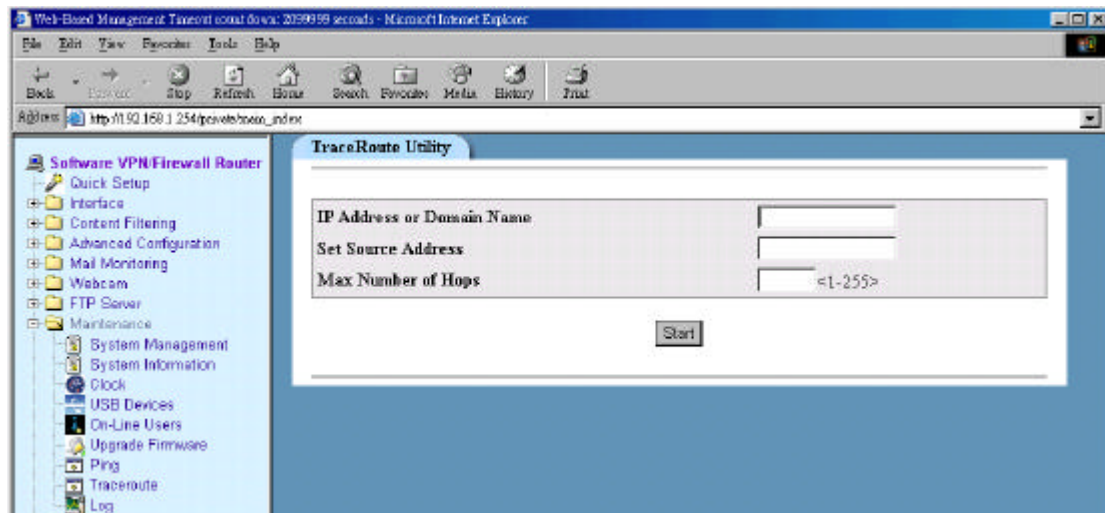
Enter the value of how many times you wish to Ping

Click on Start to Ping

## Trace route

---

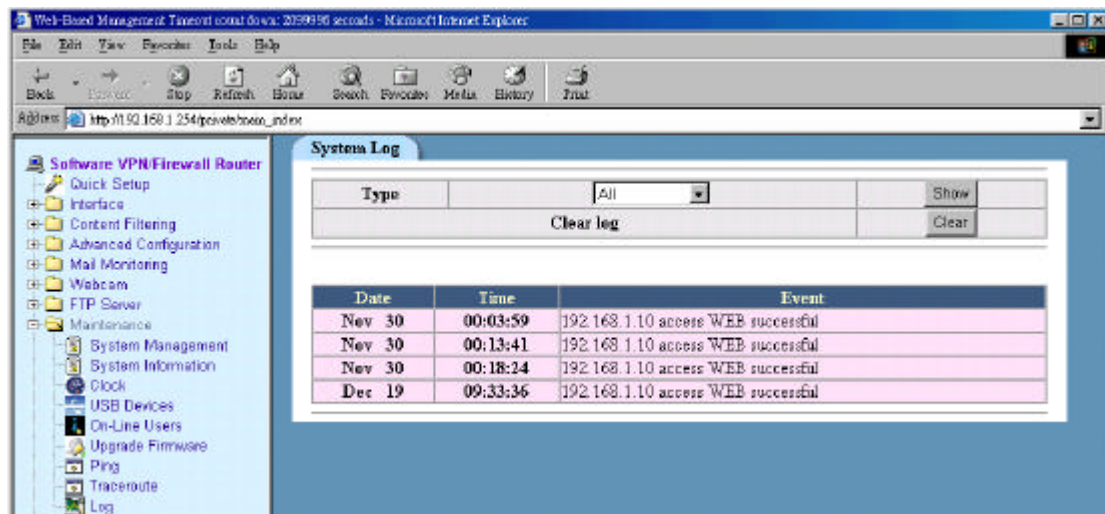
You can use this utility to trace the routing path for a particular IP address or domain.



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.

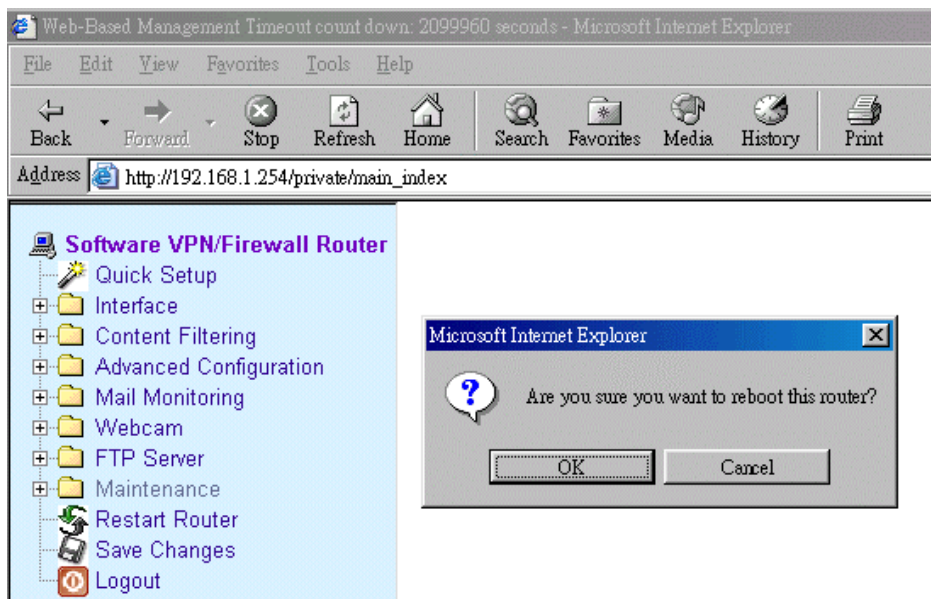
## Log



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

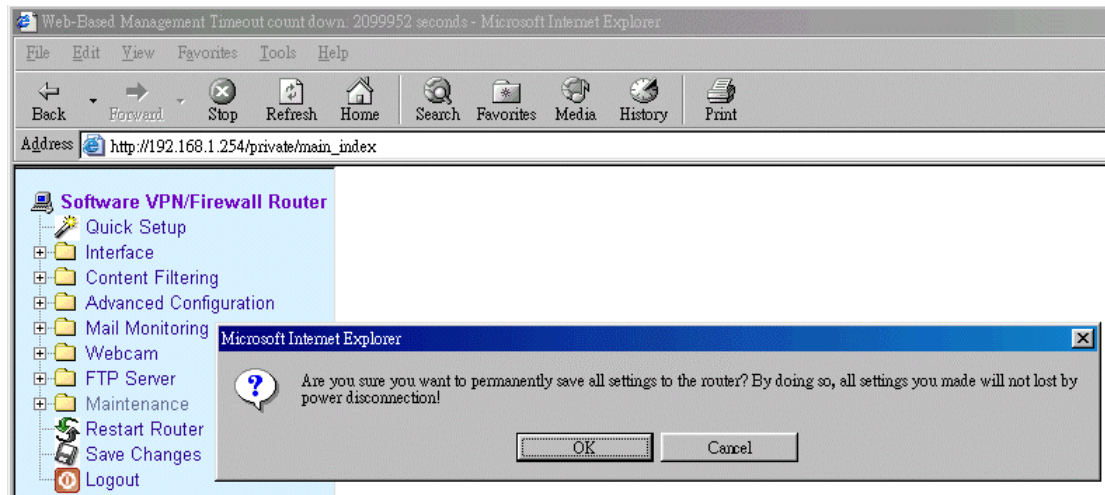
If you had entered the wrong configuration while setting up your router or other utilities, you can always reboot your router by clicking Restart Router icon.



## 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 8: 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	2	1	2	2	2	2



## Print 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](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

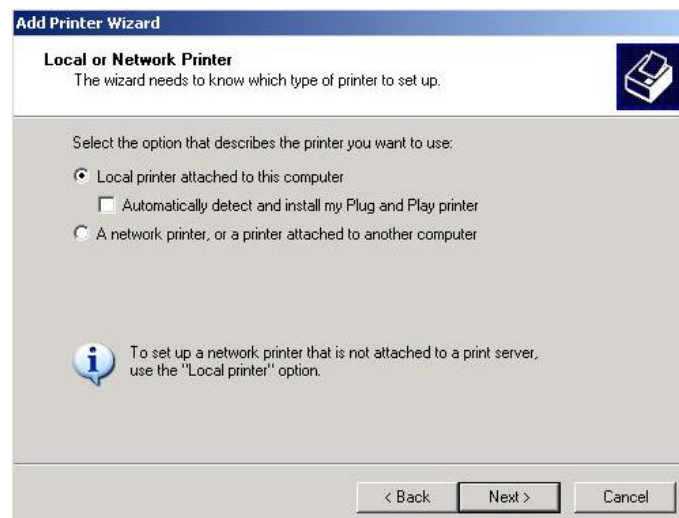
If you are running:

Windows 2000 and XP

Please note that the installation screen (Method A and Method B) looks a little bit different under different operating system, differing from step 4.

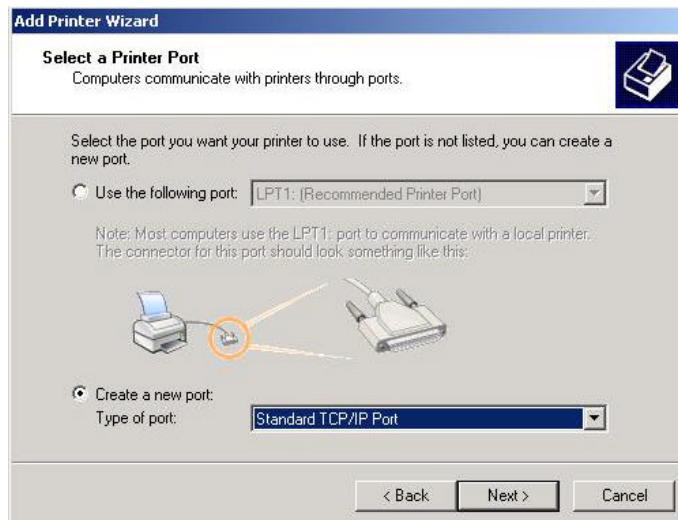
**Method A**

1. Click Start, Settings, Control Panel, and then Printers and Faxes. Click Add Printer.
2. Click Next. Choose Local Printer. Next.



## Multimedia VPN/Firewall Broadband Router

3. Choose New Port.
4. Select Standard TCP/IP Port. Click Next.




**Add Printer Wizard**

**Select a Printer Port**  
Computers communicate with printers through ports.

Select the port you want your printer to use. If the port is not listed, you can create a new port.

☐ Use the following port: LPT1: (Recommended Printer Port)

Note: Most computers use the LPT1: port to communicate with a local printer. The connector for this port should look something like this:



☒ Create a new port:  
Type of port: Standard TCP/IP Port

< Back Next > Cancel



**Add Standard TCP/IP Printer Port Wizard**

**Welcome to the Add Standard TCP/IP Printer Port Wizard**

You use this wizard to add a port for a network printer.

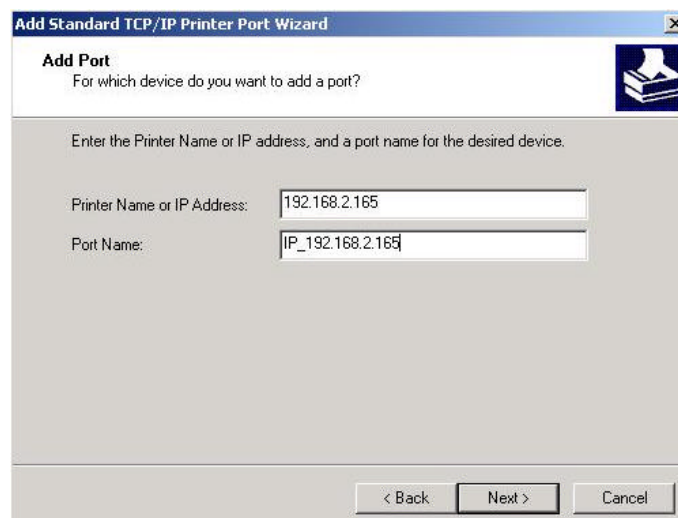
Before continuing be sure that:

1. The device is turned on.
2. The network is connected and configured.

To continue, click Next.

< Back Next > Cancel

5. IP Address: Please enter the LAN IP Address that the server is connected.
6. Port Name: PrintSrv or any name you wish. Click Next.
7. Click Custom Settings.
8. Click the Raw button. Enter 9100 as Raw Port Number. Click OK.



**Add Standard TCP/IP Printer Port Wizard**

**Add Port**  
For which device do you want to add a port?

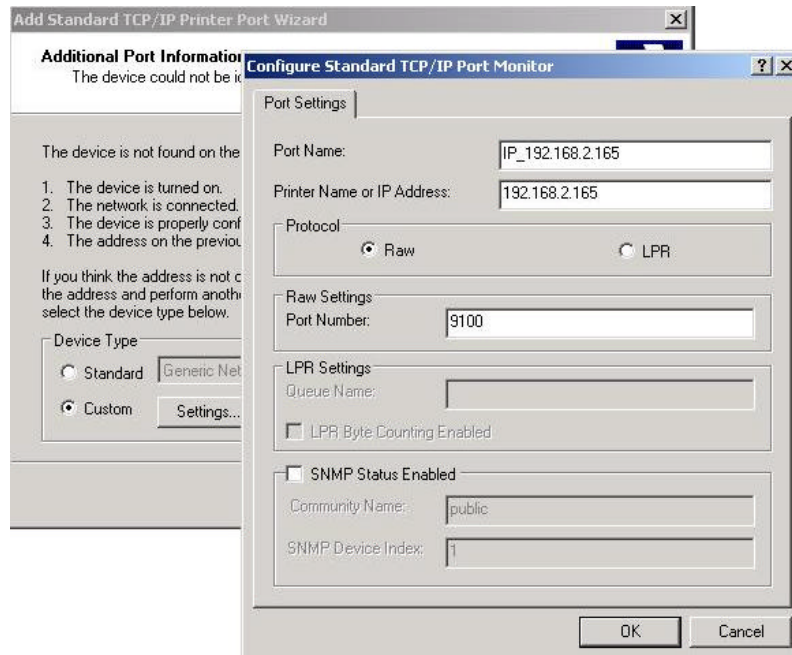
Enter the Printer Name or IP address, and a port name for the desired device.

Printer Name or IP Address: 192.168.2.165

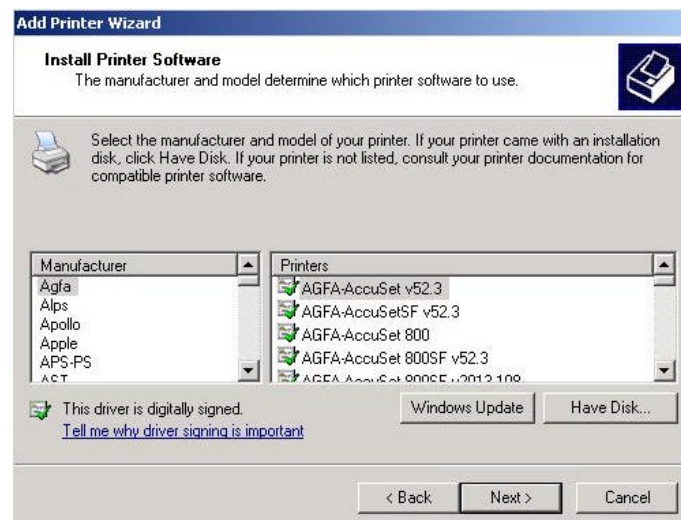
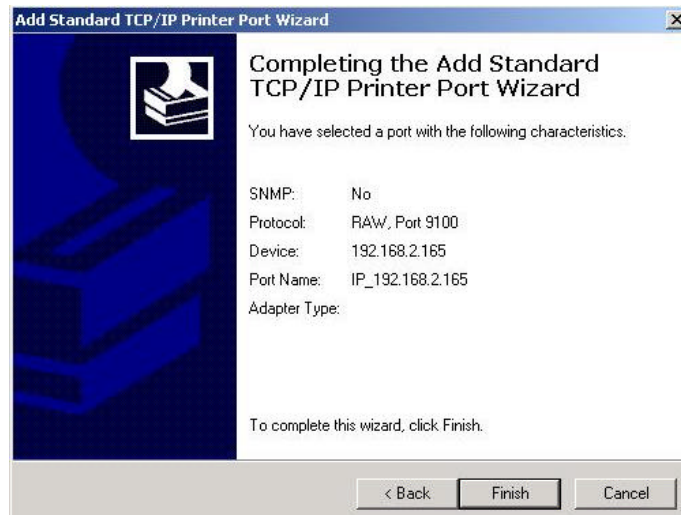
Port Name: IP\_192.168.2.165

< Back Next > Cancel

## Multimedia VPN/Firewall Broadband Router



9. You can see your settings here. Click Back if you want to change anything. Click Finish if everything is right.
10. Choose your printer from the list of printers. Click Next.
11. Congratulations! Now you've successfully installed the print server.



## Multimedia VPN/Firewall Broadband Router

### Method B

1~3

The installing screen looks different starting from step four, where you have to specify using TCP/IP protocol. But the underlying principle is the same.

Start -> Control Panel->

Printer and Faxes -> Add

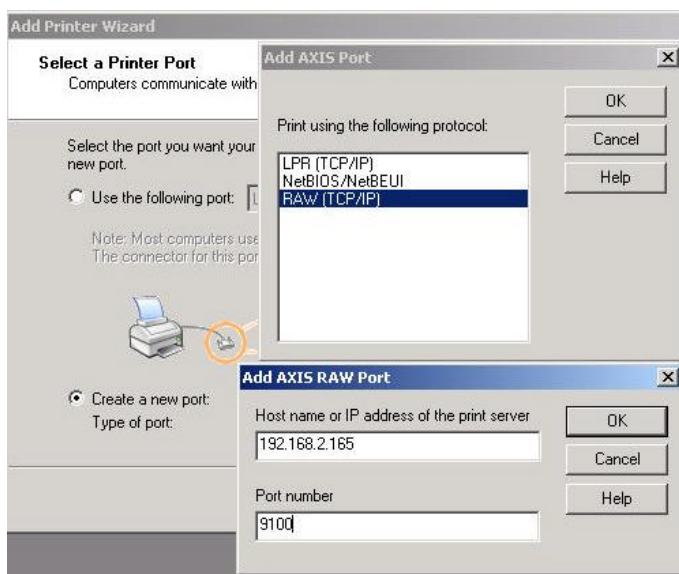
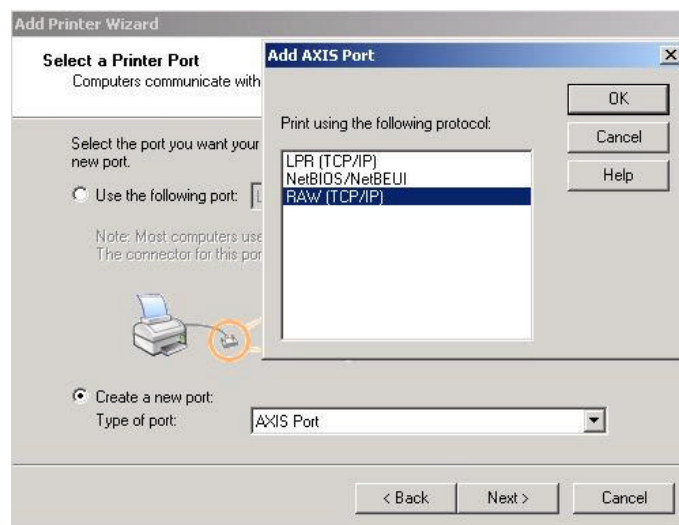
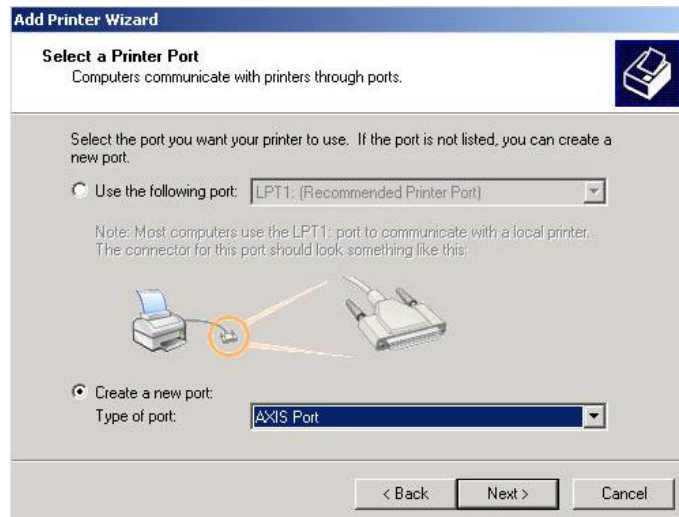
Printer -> Local Printer ->

Next -> Create New Port

-> Choose AXIS Port

4. Click NEXT after  
AXIS Port.

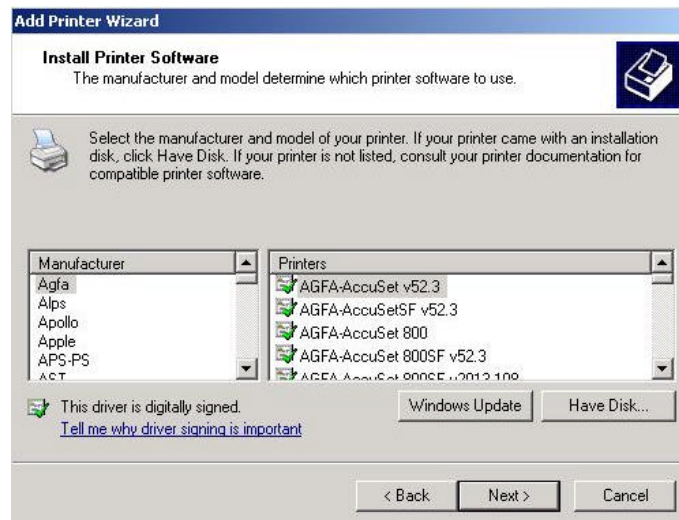
5. Click RAW TCP/IP.  
Click OK.



### Method B

6. Enter LAN IP address.
7. Enter Port Number, which is 9100. Click OK.
8. Select your printer from the list.

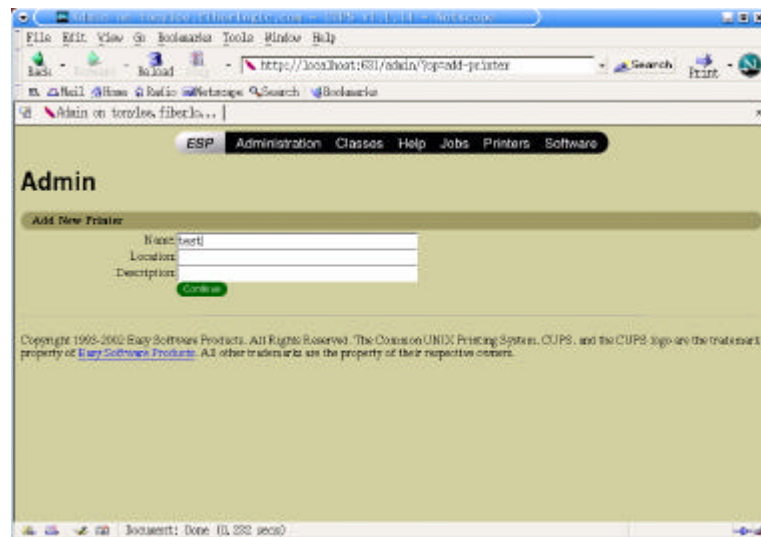
## Multimedia VPN/Firewall Broadband Router



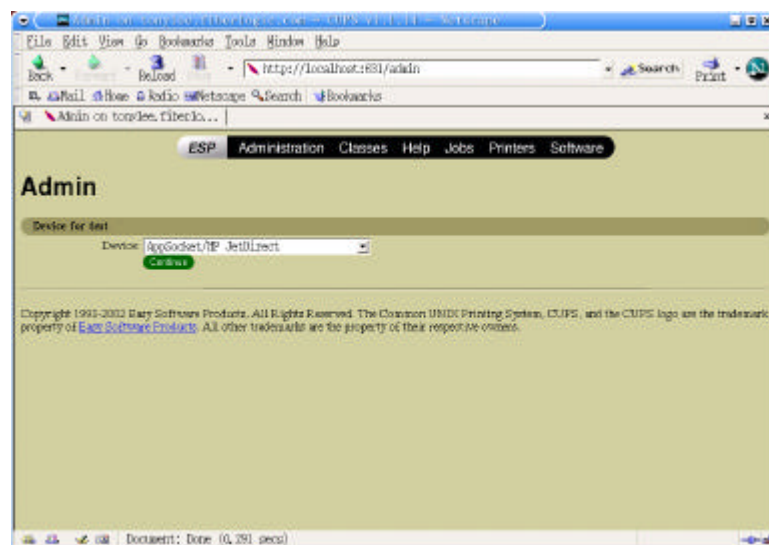


If you are running Linux

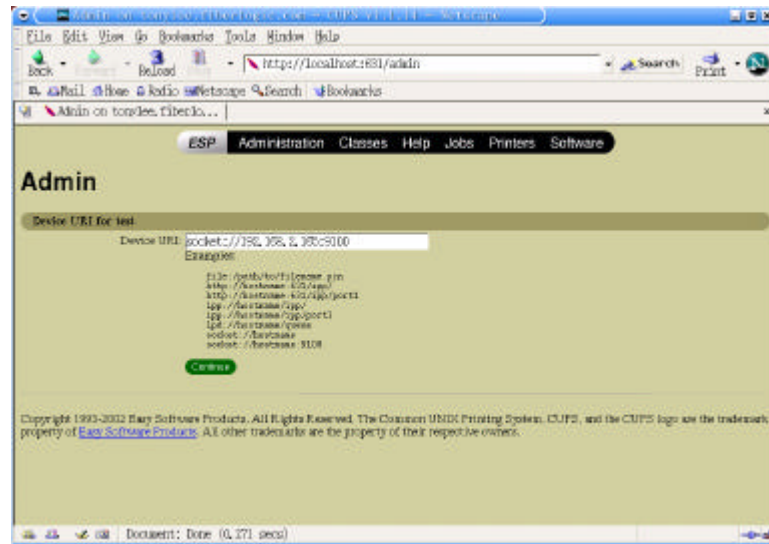
1. Enable CUPS.
2. Enter the default of URL:  
<http://localhost:631/printers>.
3. Click ADD PRINTER.
4. Give your printer a name.



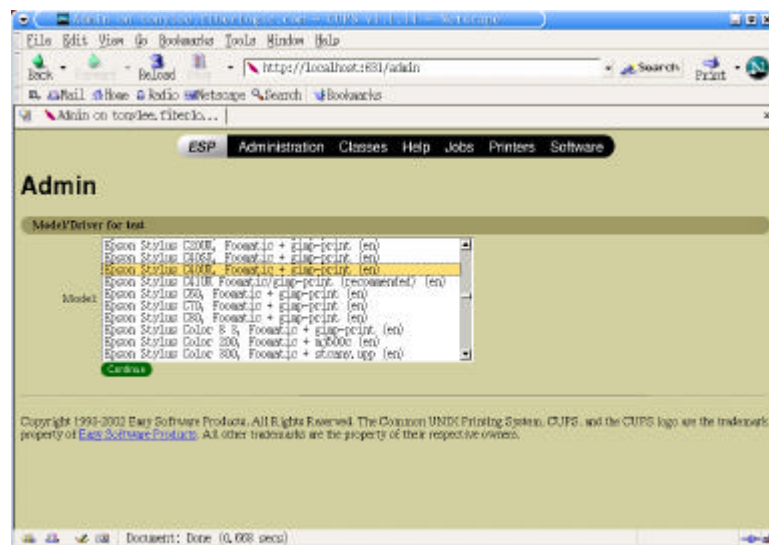
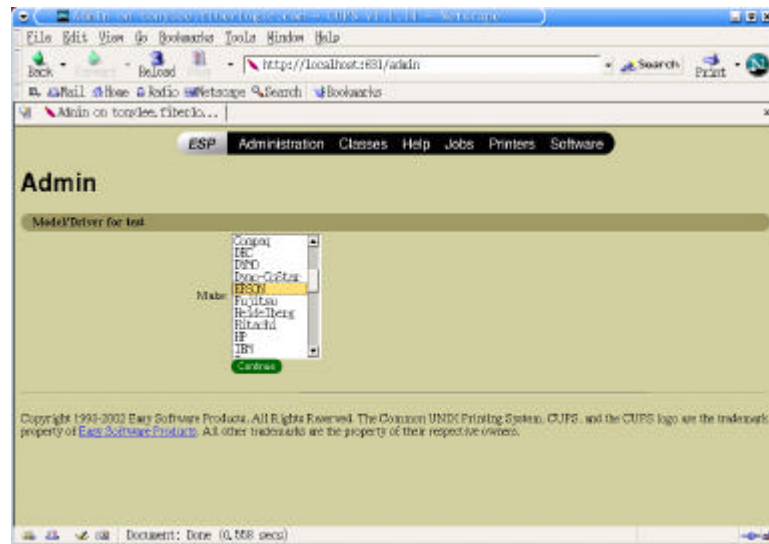
5. Select your printer from the list of device. Click CONTINUE.
6. Device URI is the LAN IP Address and the port number.
7. Click CONTINUE.



## Multimedia VPN/Firewall Broadband Router



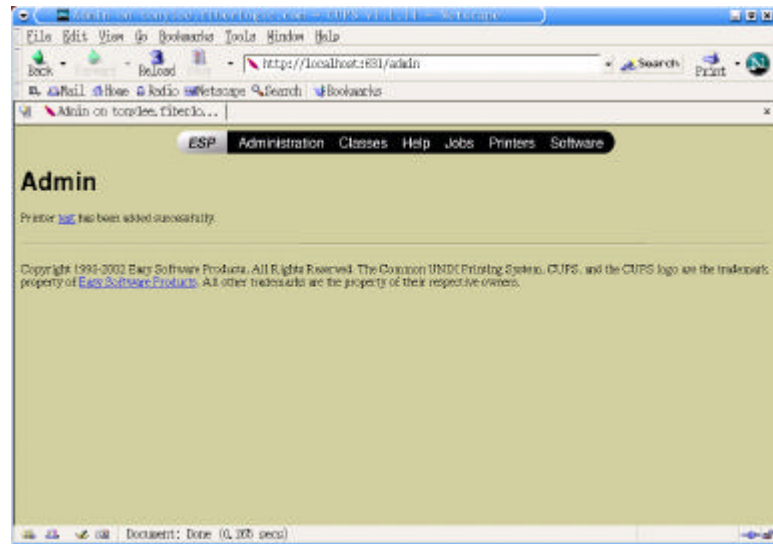
8. Choose the printer model, click CONTINUE.
9. Choose the Driver for the Model selected. Click





## Multimedia VPN/Firewall Broadband Router

10. The screen shows that you've successfully added a new printer. In this case, it's called "test".
11. Click "test" and



## Web Camera Server

---

By directly connecting USB Web Camera to any port of USB 2.0, the router can act as Web CAM server and perform the following functions

### 1. Digital Home/Office Surveillance Security system

Simply connecting a Web Camera to the router, users can surveillance their home or office through the web page from any remote or local location wherever Internet connection is available. This is the cheapest way to help users to keep close eyes on their office and home or other properties.

### 2. Motion Detection Security Alert System

This function allows movement from any unauthorized intruders to be detected at home or office. Once the router detected the movement, it will automatically send alert emails to pre-defined email address with captured images.

**Caution:** Web Cam server is compatible with limited web cameras. Please find the Compatible list from the Appendix 1 in this manual.

The surveillance image resolution may be affected by the quality of the web cam you purchased. Only use the high-resolution web cam from the compatible list. It is recommended to use "Logitech QuickCam 4000 Pro" or "Logitech QuickCam Zoom" for high quality resolution.

### **Important:**

In order to view live images from "Web Cam Live", you must install Java Plug-in software into your PC. If you don't have Java Plug-in software, please go to the following websites to get free download.

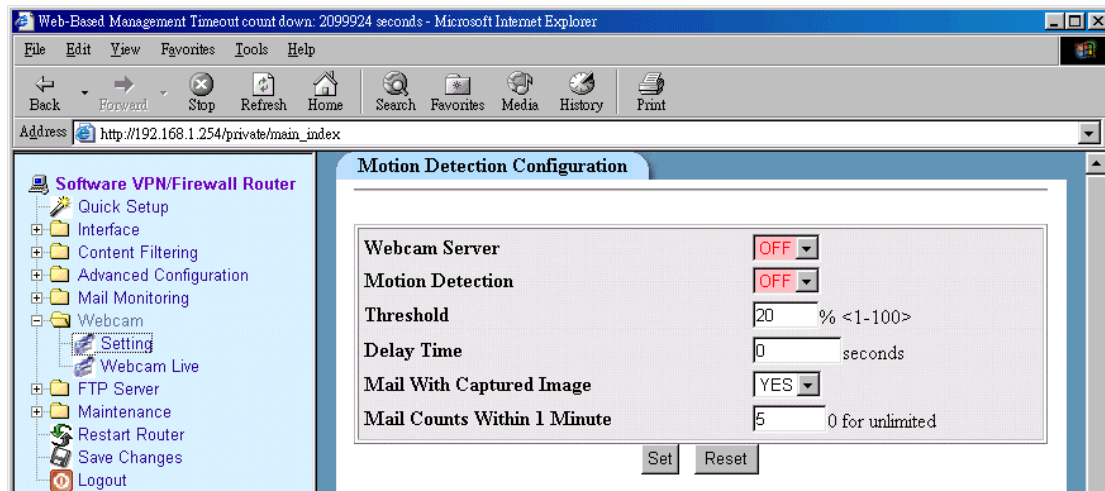
<http://java.sun.com/j2se/1.4.2/download.html>

or

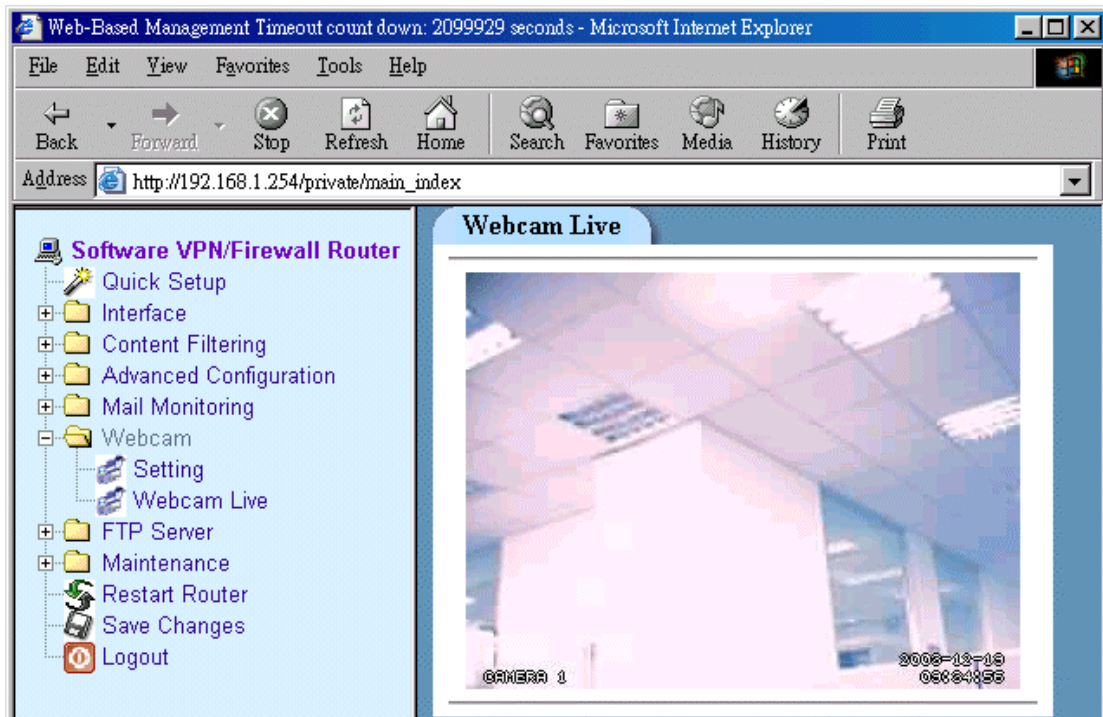
[www.java.com/en/download/windows\\_automatic.jsp](http://www.java.com/en/download/windows_automatic.jsp)

## Home/Office Surveillance function

To activate Home/Office Surveillance function, please take the following steps:



- Before activate surveillance function, please make sure Web Cam is properly plug into any USB port on the router and make sure web cam is detected by the router. You can check it at "USB Devices" function in maintenance menu.
- Go to "Web Cam" in main menu and click on Setting.
- Web Cam Server – To activate web cam server, please select "ON".
- Click on "Set" to activate the service.
- Click on "Web Cam Live" from main menu to get access to live motion.
- Only two Web Cameras can be connected and viewed at the same time.



To view web cam live images from remote locations  
You can access to live images from any remote location where Internet access is allowed. Please take the following instructions:

1. Make sure the web camera is properly connected to the any USB port of the router.
2. Make sure Remote Management from Firewall Section is set to enable.
3. Open a web browser and type in your router's WAN IP address. (WAN IP can be obtained from main menu on Interface -> WAN)
4. After type in WAN IP in your web browser, it will then lead you to Web-Based Management utility page. Type in your password to login into Web-Based Management page. Select Web cam live to view the live images.

## Motion Detection System

To activate Motion Detection System, please take the following steps:

**Schedule Setting**

Start Hour	Start Minutes	Stop Hour	Stop Minutes	Mon	Tue	Wed	Thu	Fri	Sat	Sun
0-2										
3-5										
6-8										
9-11										
12-14										
15-17										
18-20										
21-23										

Set Reset

**Mail Address Setting**

Mail Server	Mail Address	User Name	Password

Set Reset

- Go to Mail Address Setting and enter all mail server information of where alert e-mail should be sent. Click on Set after complete information has been entered.
- Go to Motion Detection Configuration and make sure both Web Cam Server and Motion Detection are enable.
- Click on Set to activate Motion Detection function.

## Schedule Setting

Motion Detection System can be activated through pre-set time schedule on dairy or weekly basis. To set time schedule,, go to Schedule Setting and enter the desired time schedule in related time box. Click on Set after completion.

## Advanced Setting

- Threshold - Enter a threshold value. This value works in conjunction with the noise level. Ignore this field if motion detection is OFF.
- Delay Time - This feature allows the router to automatically enabling the Motion Detection function after a period of time set in this field. This function allows you to have enough time to leave your home/office without been detected after configured the motion detection function to your router.
- Mail With Captured Image - Choose No to mail the motion detection alert message with just words. Choose YES to mail the motion detection alert message with pictures taken.
- Mail Counts within 1 minute - Enter the maximum alert emails mailed out within one minute. 0 is for unlimited emails mailed out if detected. The default value is 5.

## FTP Server

---

By directly connecting USB storage devices to any USB 2.0 port, FTP server can be created with simple configuration. FTP Server utility allows both local and remote users to upload or download files, pictures or MP3 music from the same storage device in most easy and timely fashion. It is also cost effective where users do not need to purchase a dedicated PC to set up a 24 hours FTP service.

Before configure FTP Server, please make sure one of the following storage devices is properly plug into any USB port on the router and make sure this USB storage device is detected by the router. You can check it at "USB Devices" function in main menu.

1. USB Hard Disk Drive

(Only use USB HDD that equipped with its own Power supply)

2. USB Flash Drive

3. Digital Camera

4. MP3 Player

5. USB Media Reader

**Caution:**

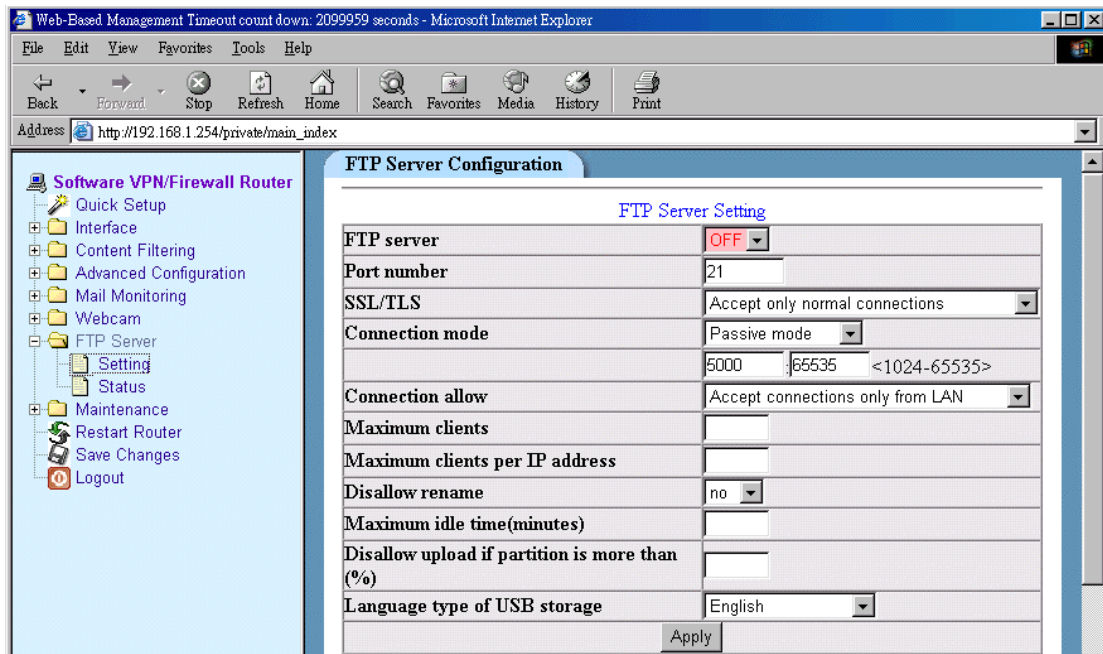
FTP server is compatible with FAT32 or EXT2 format USB storage device. In case you need to format your USB storage device. Please always make sure the device is formatted with FAT32 or EXT2 standard.



- ## Set Up a FTP Server



To activate FTP server, please go to “FTP Server Setting” and take the following steps:



- FTP Server – Select “On” to activate FTP server function.
- Connection Allow – Both WAN and LAN IP of router can be used to identify FTP Server. Select “Accept Connections only from LAN” will activate FTP server within local LAN group. Select “Accept Connections from LAN and WAN” will activate FTP Server for remote users.
- Click “Change” after above information is given.

How to create a FTP Server I P address??

After completed the configuration steps listed above, FTP server can be accessed through web page by keying its unique FTP IP address. The formula of creating FTP IP address is listed below:

ftp://Account-name@WAN IP Address  
(Need to type in password when log in)

ftp://Account-name:Password@WAN IP Address  
(Do not need to type password when log in)

For example: If the account name of the FTP server you configured is "Fiber" and your WAN IP address is 192.168.1.254, Password is 1234.

Then, Your FTP IP address should be

ftp://fiber@192.168.1.254

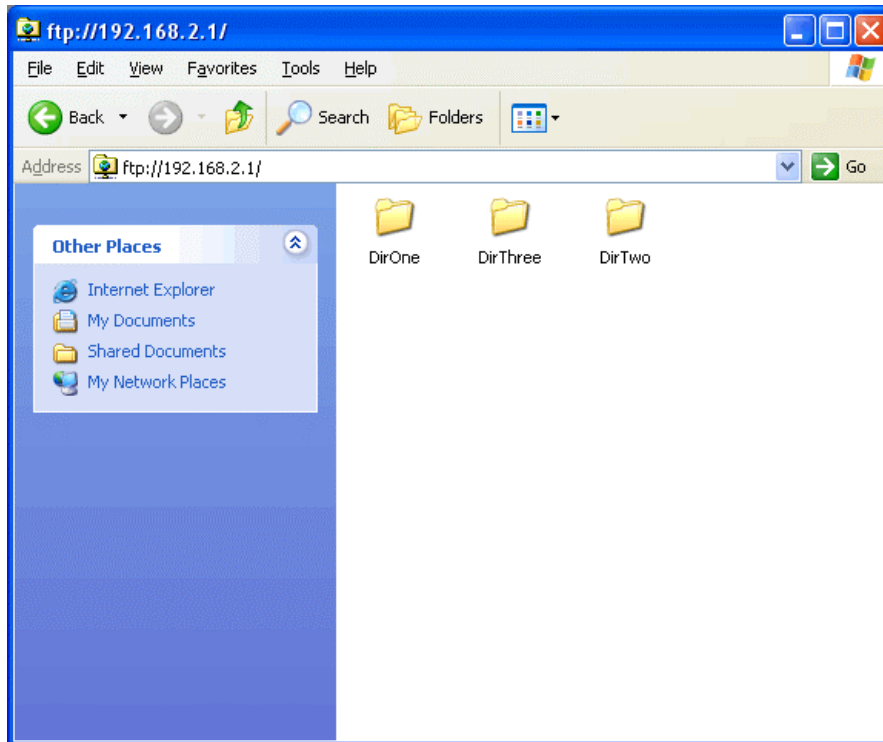
Or

ftp://fiber:1234@192.168.1.254

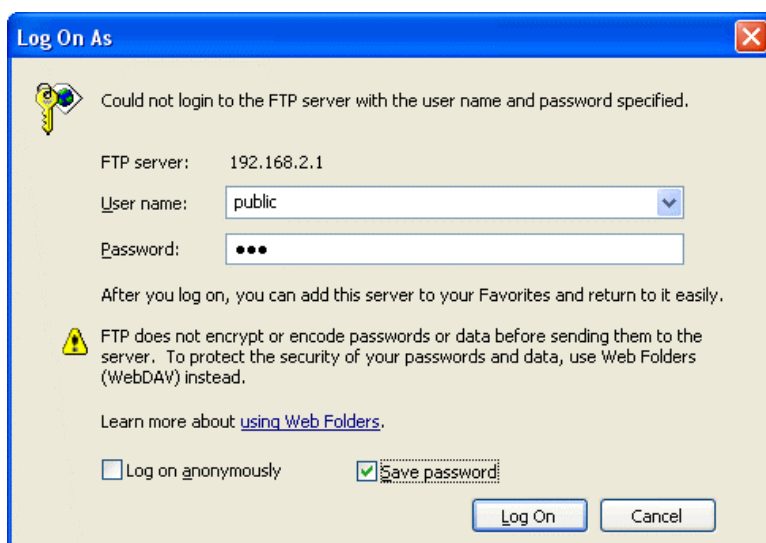
How to access your FTP server??

After the FTP server is set up, it is open for access from both local and remote network via web page.

1. Open a web page and type in FTP IP address



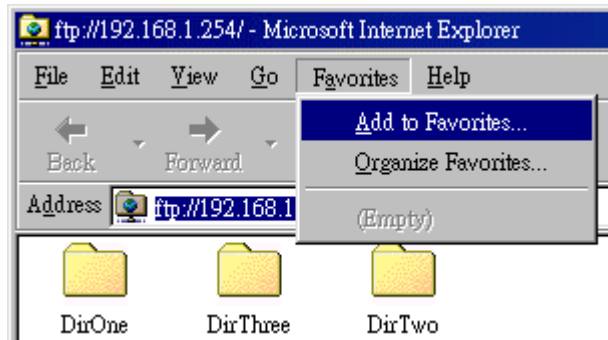
2. Once the FTP IP address is entered, the screen will pop up and required to enter Account name and Password. Please enter the information and click ok.



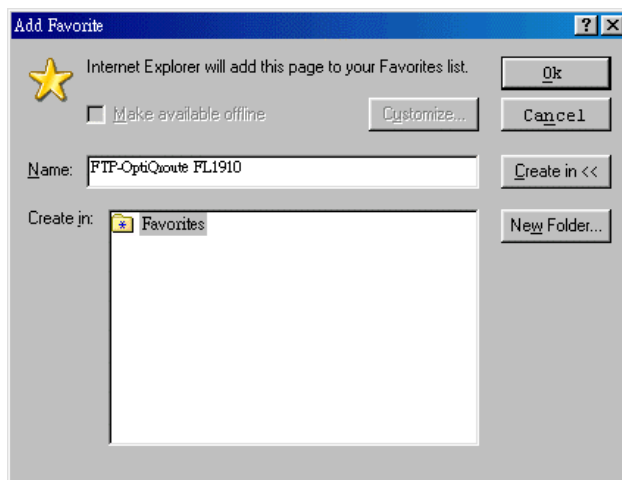
To create "Network Neighborhood" by using FTP Server (WIN 98)

After successfully set up a FTP server, you can also use this FTP server to act as one of your "Network Neighborhood" within your LAN network.

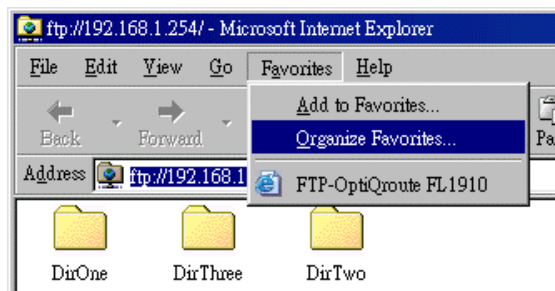
1. After log onto FTP Server web page, please go to "Favorites" and click on "Add to favorites".



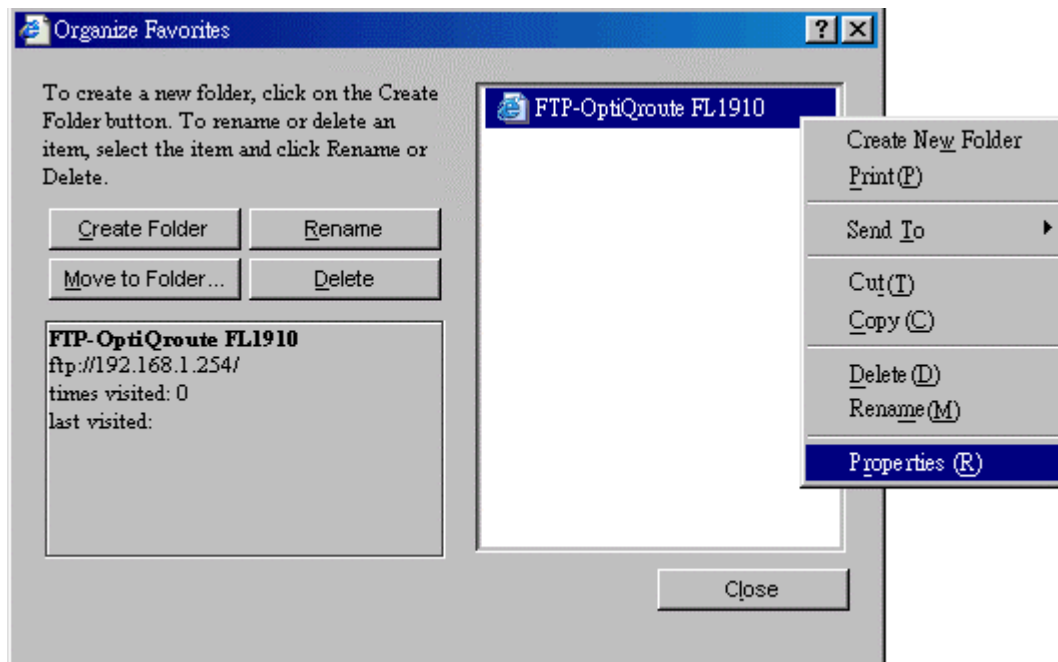
2. Please change the name if necessary and click on OK.



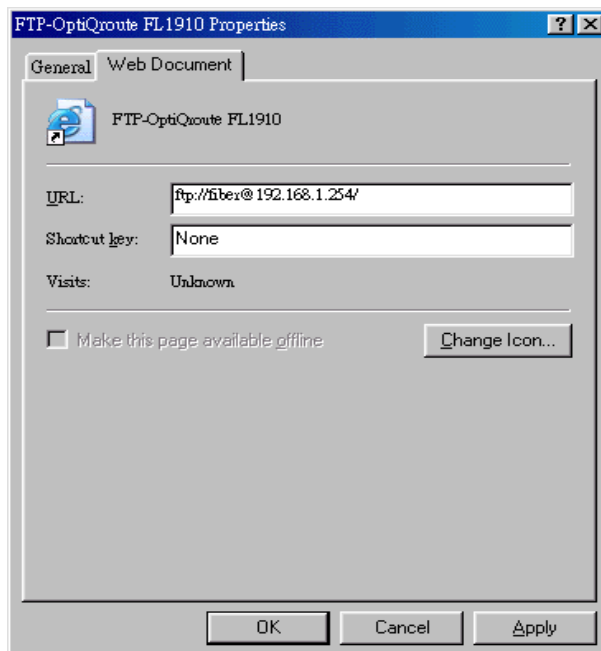
3. Please select "Organize Favorites" from "Favorites" menu.



4. Please find the name of your FTP server which you added to “favorites” and hit single click on the name. Click on the right button of your mouse in order to find “properties” function.



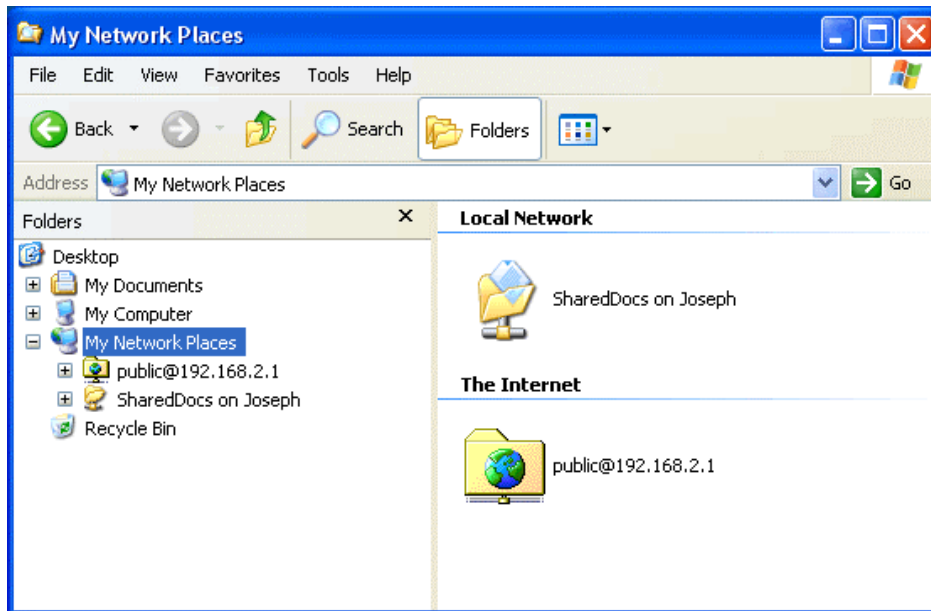
6. After click on “properties”, the following screen will appear.



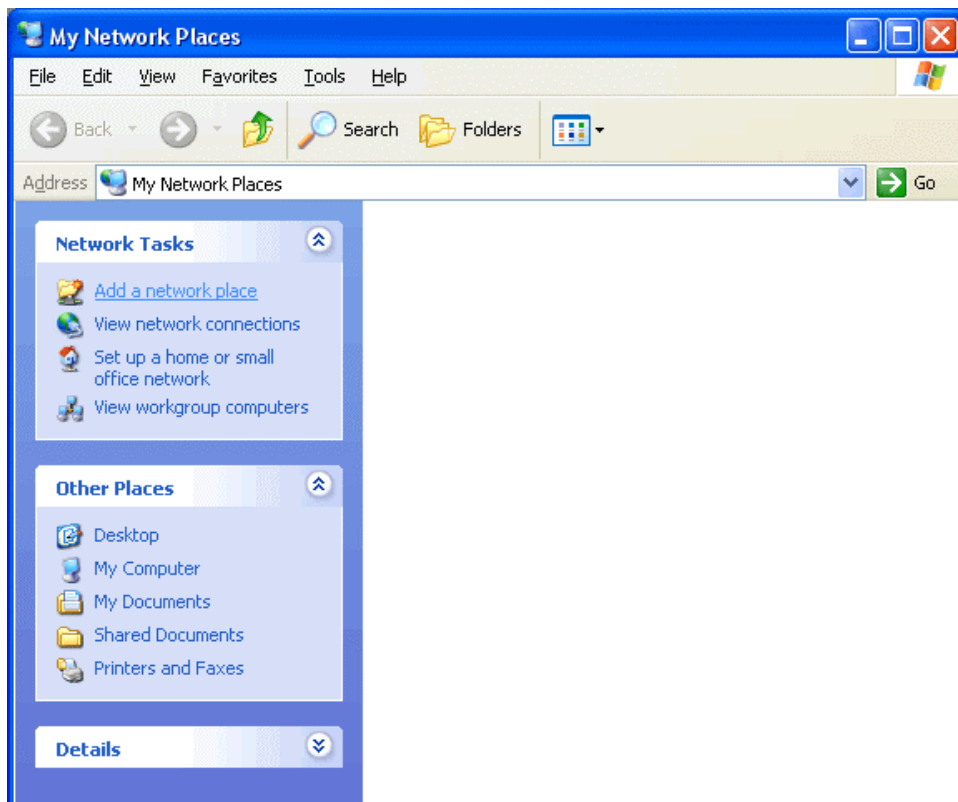
7. Click on OK to finish the setting. Now you can find the FTP folder appear in your Network Neighborhood from File Manager.

To create "Network Neighborhood" by using FTP Server (Win 2000/XP)

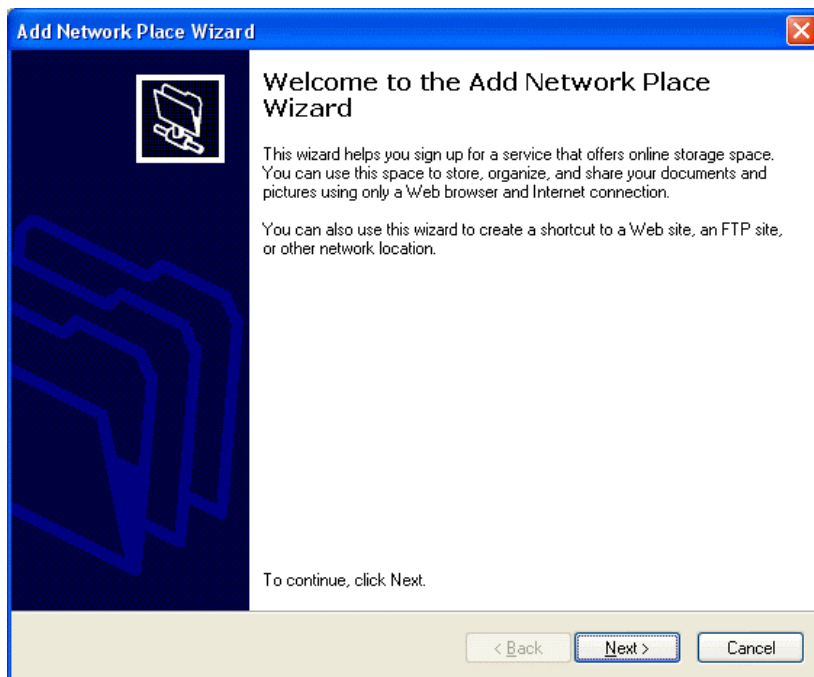
1. Open "Window Explorer" and click on "Network Neighborhood" or "My Network Places".



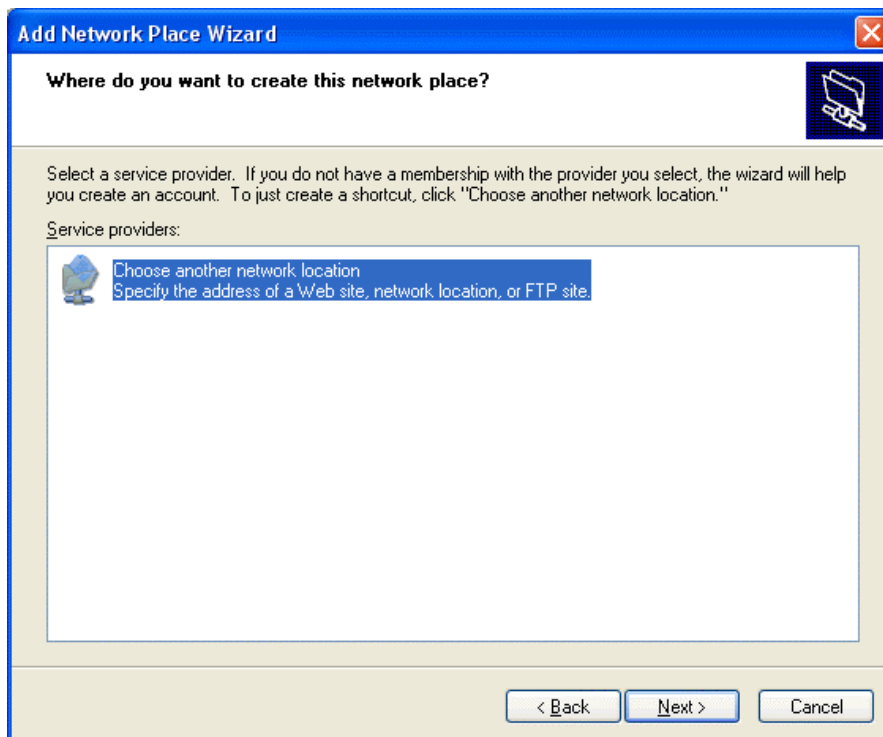
2. You will then find a utility called "Add a Network Place".



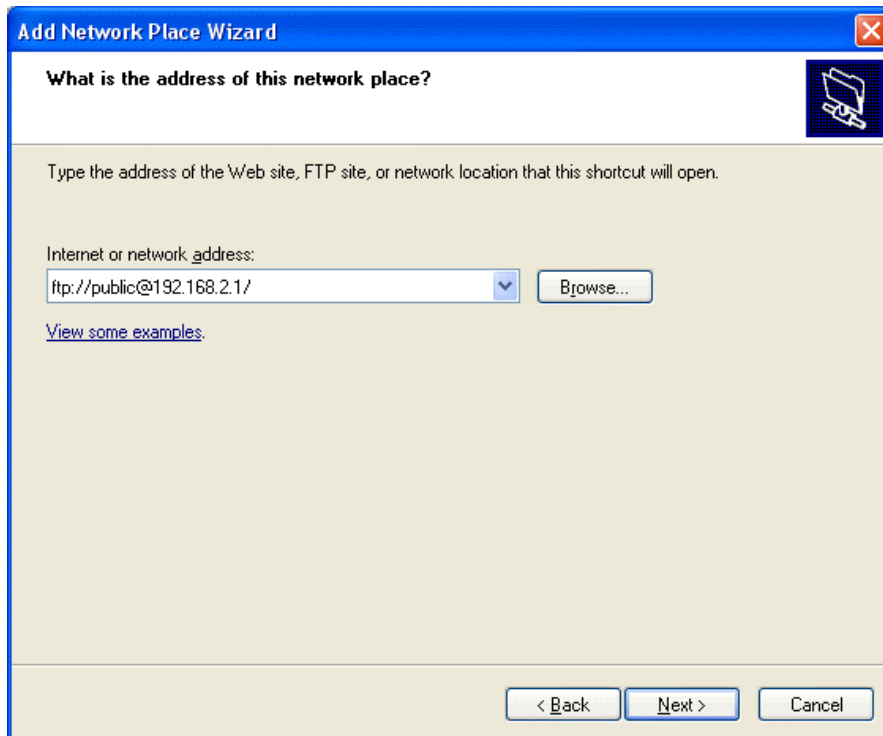
3. After click on "Add a Network Place", a welcome page of setup wizard will appear. Click next to begin the setup.



4. Click on next again to continue the set up of creating Network Neighborhood from FTP location.



5. Type in FTP address where you need to set up for Network Neighborhood.  
Tip: If you do not wish to enter password every time when you access the FTP server from "My Network Places", it is recommended to add password into FTP IP address so other users do not need to enter the password again if they need to access it within your LAN network. The FTP address should be in the following format.  
ftp://Account-name:Password@WAN IP Address



**Add Network Place Wizard**

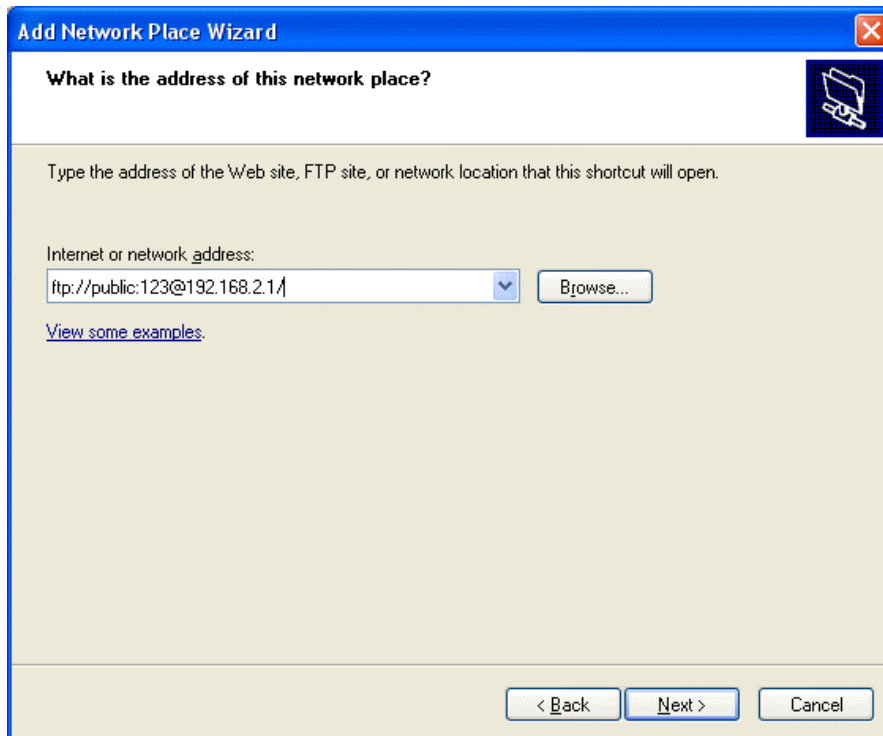
**What is the address of this network place?**

Type the address of the Web site, FTP site, or network location that this shortcut will open.

Internet or network address:  
ftp://public@192.168.2.1/

[View some examples.](#)





**Add Network Place Wizard**

**What is the address of this network place?**

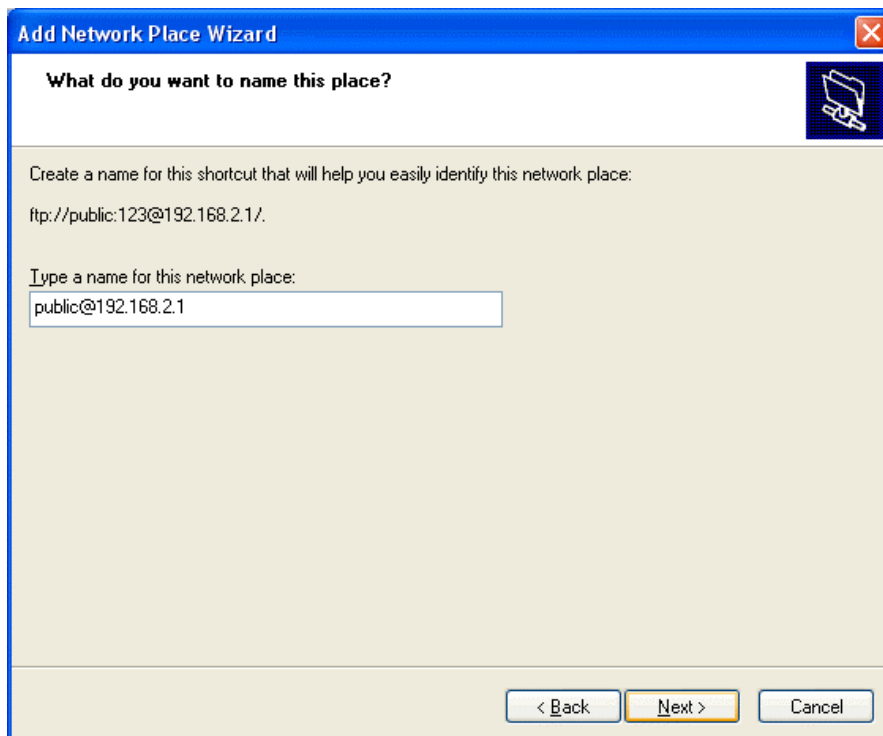
Type the address of the Web site, FTP site, or network location that this shortcut will open.

Internet or network address:

[View some examples.](#)

< Back   Next >   Cancel

6. In this section, you need to type the name of FTP server in "Network Neighborhood". Click next to continue.



**Add Network Place Wizard**

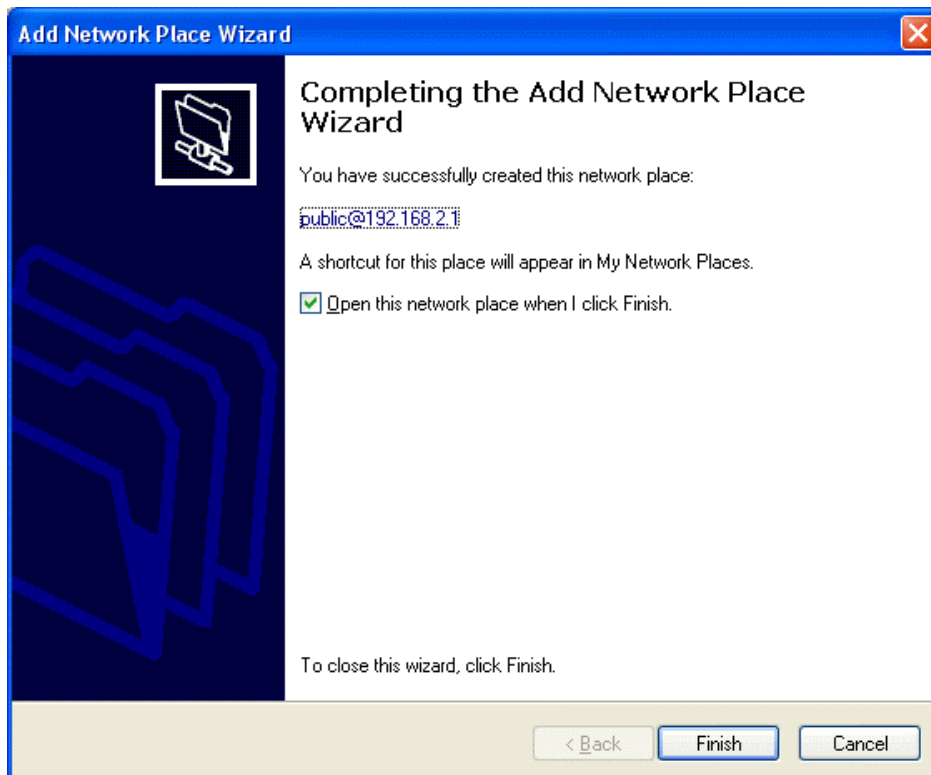
**What do you want to name this place?**

Create a name for this shortcut that will help you easily identify this network place:  
ftp://public:123@192.168.2.1/.

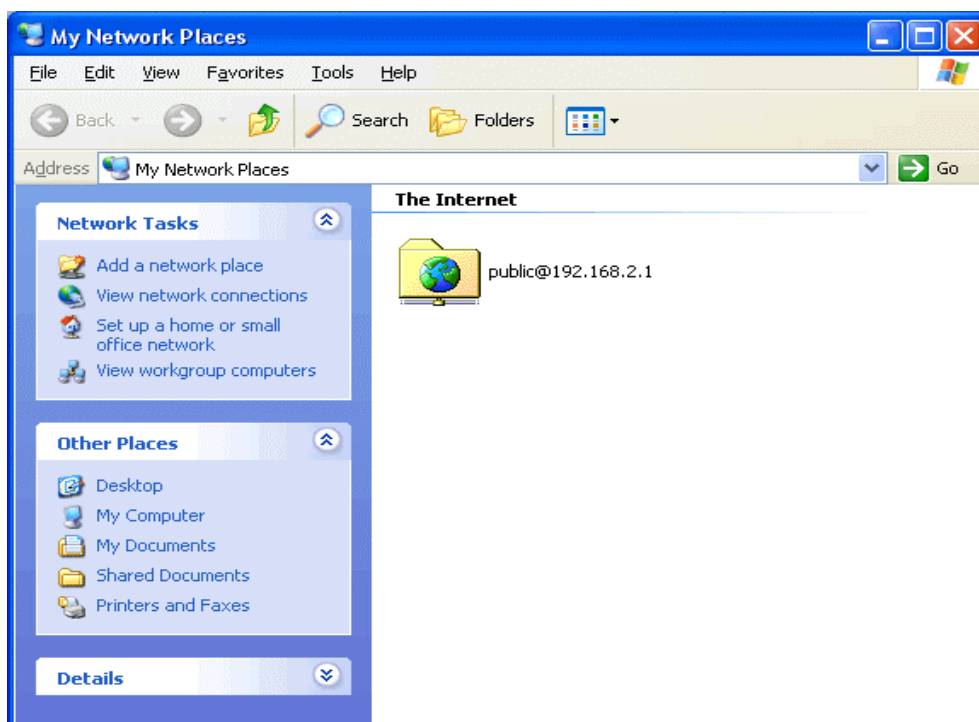
Type a name for this network place:

< Back   Next >   Cancel

7. Now you had completed the setup. Click finish to exit Setup Wizard.



8. Now go back to "File management" and then go to Network Neighborhood, you should find the folder of FTP Server appear in this section.



## Advanced Settings

### FTP Server Setting

- Port number – Port number - Define the FTP command transfer service port. Default value is 21. If you have changed this, remember to change the service port setting of your FTP client.
- SSL/TLS –Enable/Disable the SSL transfer of the FTP command. There are three choices of this option, you can use only normal connections, only SSL/TLS connections, or accept both of them at the same time. Enable the SSL/TLS connections only when you have the security concern. The default value of this option is <Accept only normal connections>.
- Connection mode – Passive mode served as default value. The data can be transmitted through Port 5000 ~ 65535. When select Active mode, the data transmitted through standard Port 20.
- Maximum clients – You can restrict limited number of clients access FTP at the same time. Leave it blank for unlimited access.
- Maximum clients per IP – You can restrict limited number of clients access FTP at the same time with same IP. Leave it blank for unlimited access.
- Disallow rename – Default value is “No”. Select “Yes” if do not allow rename the files.
- Maximum idle time (minutes) – When a specific time value is added, FTP Server will be de-activated if it has no activity within the time limit.
- Disallow upload if partition is more than (%) – This function allows users to limiting storage capacity in their storage device so storage device will not fully occupy with uploaded files.
- Language type of USB storage – The function allows the file name to be viewed in different languages from FTP web page.

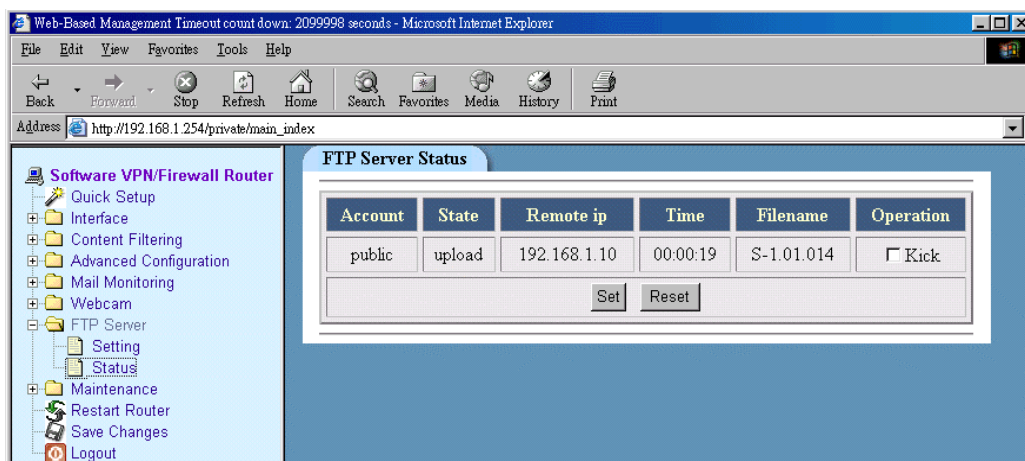
## FTP Account Setting

- Download throttling (kb/s) – Download speed can be limited by a given value.
- Upload throttling (kb/s) – Upload speed can be limited by a given value.
- Download/Upload ratio – When the value is set, you are able to download and upload according to desired ratio.
- Allow client domain name/IP < A.B.C.D./M>:

## FTP Server Status

In this section, all FTP server activity can be monitored or forced disconnection when the file is uploading or downloading.

- Account – this section indicate the account name of FTP Server which currently transmitting the data.
- State – this section indicate the connection status.
- Remote IP – this section indicate Remote IP when it connect to FTP Server.
- Time – this section indicate the connection time
- Filename – this section indicate the file name when downloading or uploading are in processing.
- Operation – Downloading or uploading transmission can be discounted at any time if “Kick” box is checked and “Set” button is pressed.



## Appendix 1

## Web Camera Compatible List

Manufacturer	Model
Aiptek	HyperVcam Home
Amitech	AWK-300
Askey	Askey VC010
Alpha Vision Tech.	AlphaCam SE (model AC-520)
Avaks	AvCam USB-600
AverMedia	InterCam Elite
BestBuy	EasyCam U
Creative Labs	WebCam (model PD1001, alternate version)
Creative Labs	WebCam 3
Creative Labs	WebCam 5 (PID=400c)
Creative Labs	WebCam Plus (Model CT6840)
Creative Labs	WebCam Plus ("WebCam Mini"; model PD0040)
Creative Labs	WebCam Pro (model PD1030)
Creative Labs	Webcam Pro Ex
D-Link	DSB-C100
D-Link	DSB-C310
D-Link	DU-C300
Elecom	UCAM-C1C30
Elta	WEBCam 8211 PCC
Ezonics	EZPhone Cam
Hawking Tech.	UC-110
Hawking Tech.	UC-300
Hawking Tech.	UC-310
I-View	NetView NV300M
Intel	Me2Cam
LG Electronics	LPC-UM10

## Multimedia VPN/Firewall Broadband Router

LG Electronics	LPC-UM15
Liferview	USB CapView
Liferview	RoboCam
Lifetec	LT 9388
Logitech	QuickCam 3000 Pro
Logitech	QuickCam 4000 Pro
Logitech	QuickCam Notebook Pro
Logitech	QuickCam Zoom
Logitech	QuickCam Orbit/Sphere
Maxxtro	CAM22U
Maxell	Maxcam (MPCC-1)
Medion	MD9388
MediaForte	MV300
MediaForte	PC Vision 300
Mustek	WCam 3X
Mtekvision	Zeca MV402
OmniVision	OV7110 Eval Board
OmniVision	OV511+/OV7120 Eval Board
OmniVision	OV511+/OV7620 Eval Board
Pretec	PCC-600
Prochips	PCA-3100
Puretek	PT-6007
Philips	PCA645VC
Philips	PCA646VC
Philips	PCVC675K "Vesta"
Philips	PCVC680K "Vesta Pro"
Philips	PCVC690K "Vesta Scan"
Philips	PCVC720K/40 "ToUCam XS"
Philips	PCVC730K "ToUCam Fun"
Philips	PCVC740K "ToUCam Pro"

## Multimedia VPN/Firewall Broadband Router

Philips	PCVC750K "ToUCam Scan"
Sotec	Sotec Afina Eye
Suma	EON
Samsung	MPC-C10
Samsung	MPC-C30
Samsung	Anycam MPC-M10
TRENDNet	TV-PC100
TRENDNet	TV-PC300
TRENDNet	TV-PC301
Trust	Sp@ceC@m USB
Trust	Sp@ceC@m 200
Trust	Sp@ceC@m 300
Typhoon	WebShot 350
TEVion	MD 9308
TCE	NetCam 310u
Terratec	TerraCam PRO
Visionite	Visionite VCS UM100
Visionite	Visionite VCS UC300
Waytech	I-Pac VIC-30
Webeye	2000B