

(8.) You can input <http://192.168.9.9> in IE browser to enter the GUI page of upper level device and make sure the connection.



### 5.2.6 WPS

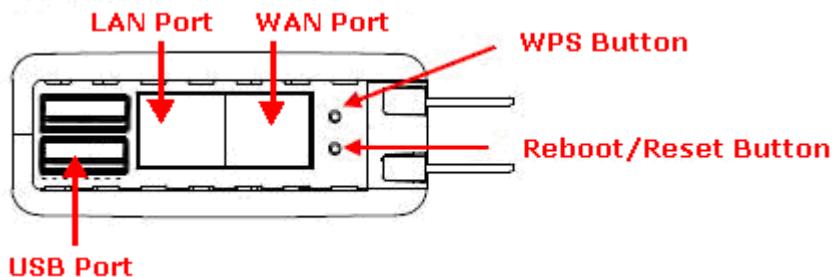
Wi-Fi Protected Setup, it can simplify the procedures of wireless encryption between Server Router and wireless network card. If the wireless network card also supports WPS function, users can activate WPS auto-encryption to speed up the procedures.

WPS supports 2 models: PIN (Personal Information Number) and PBC (Push Button Configuration). These models are approved by the Wi-Fi Alliance.

**PIN model**, in which a PIN has to be taken either from a sticker label or from the web interface of the WPS device. This PIN will then be entered in the AP or client WPS device to connect.

**PBC model**, in which the user simply has to push a button, either an actual or a virtual one, on both WPS devices to connect.

\*The following figure is the display of the front of Server Router.



When users select a specific model on wireless base station, the clients can connect to the base by selecting the same model.

The connection procedures of PIN and PBC are almost the same. The small difference between those two is:

Users input the PIN of wireless card in the base station first; it will limit the range of the clients. It is faster to establish a connection on PIN model.

On PBC model, users push the WPS button to activate the function, and then the wireless client must push the WPS button in 2 mins to enter the network. The client will search to see if there is any wireless base station which supports WPS is activating. If the client finds a matching base, the connection will be established. The speed of establishing a connection is slower than the PIN model because of this extra step.

On the other hand, users need to input the information of the wireless card into the register interface. It might lead to the failure of connection, if users make mistakes on inputting. On PBC model, users only need to click the WPS button on both sides to make a connection. It is easier to operate.

This page supports **Start PBC** and **Start PIN**; please follow the instructions to operate.

\* Start PBC:

(1.) Please click **Start PBC** to connect to the wireless network card.

## Wi-Fi Protected Setup

This page allows you to change the setting for WPS (Wi-Fi Protected Setup). Using this feature could let your wireless client automatically synchronize its setting and connect to the Access Point in a minute without any hassle.

**Disable WPS**

**WPS Status:**  Configured  UnConfigured

**Self-PIN Number:** 18864540

**Push Button Configuration:**  Start PBC

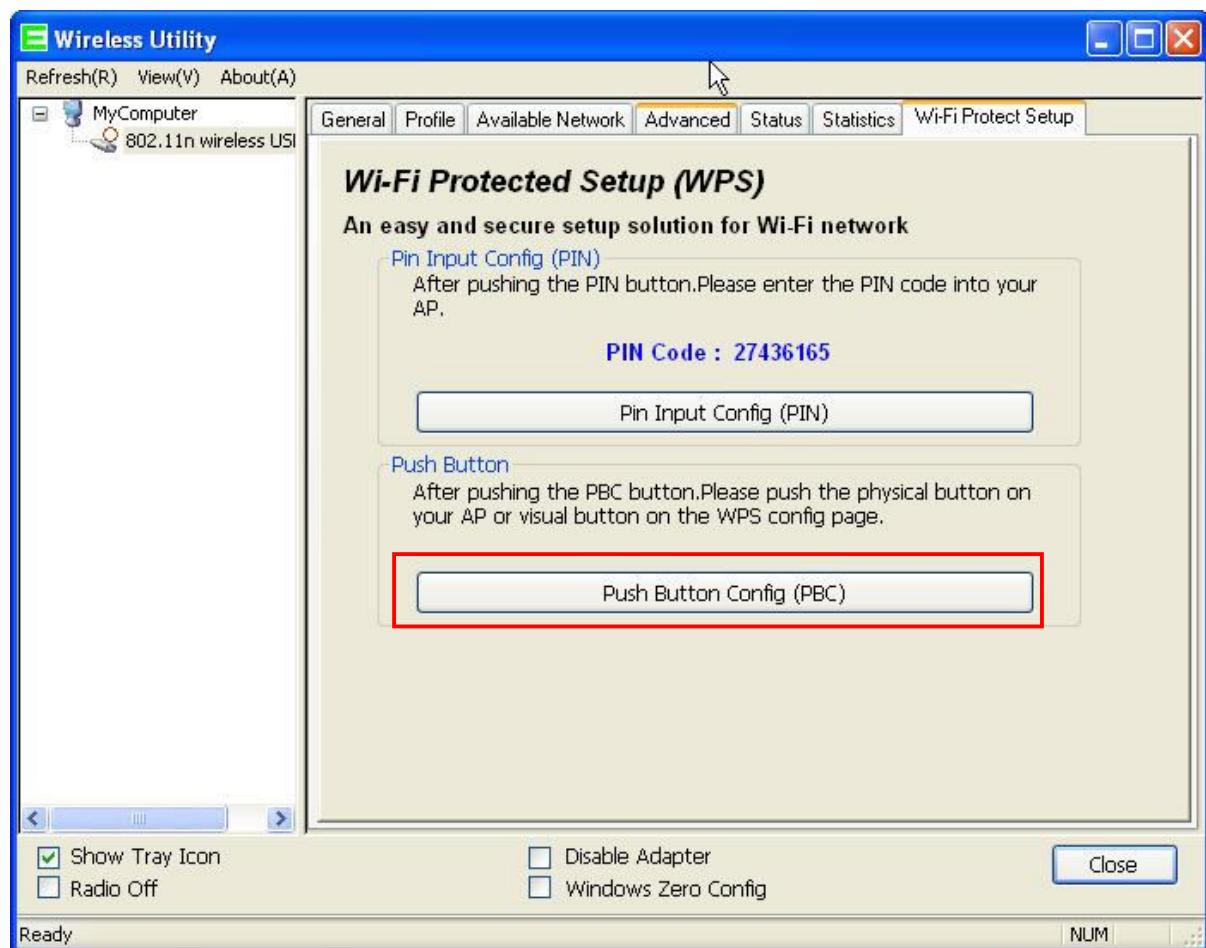
**Current Key Info:**

Authentication	Encryption	Key
Open	None	N/A

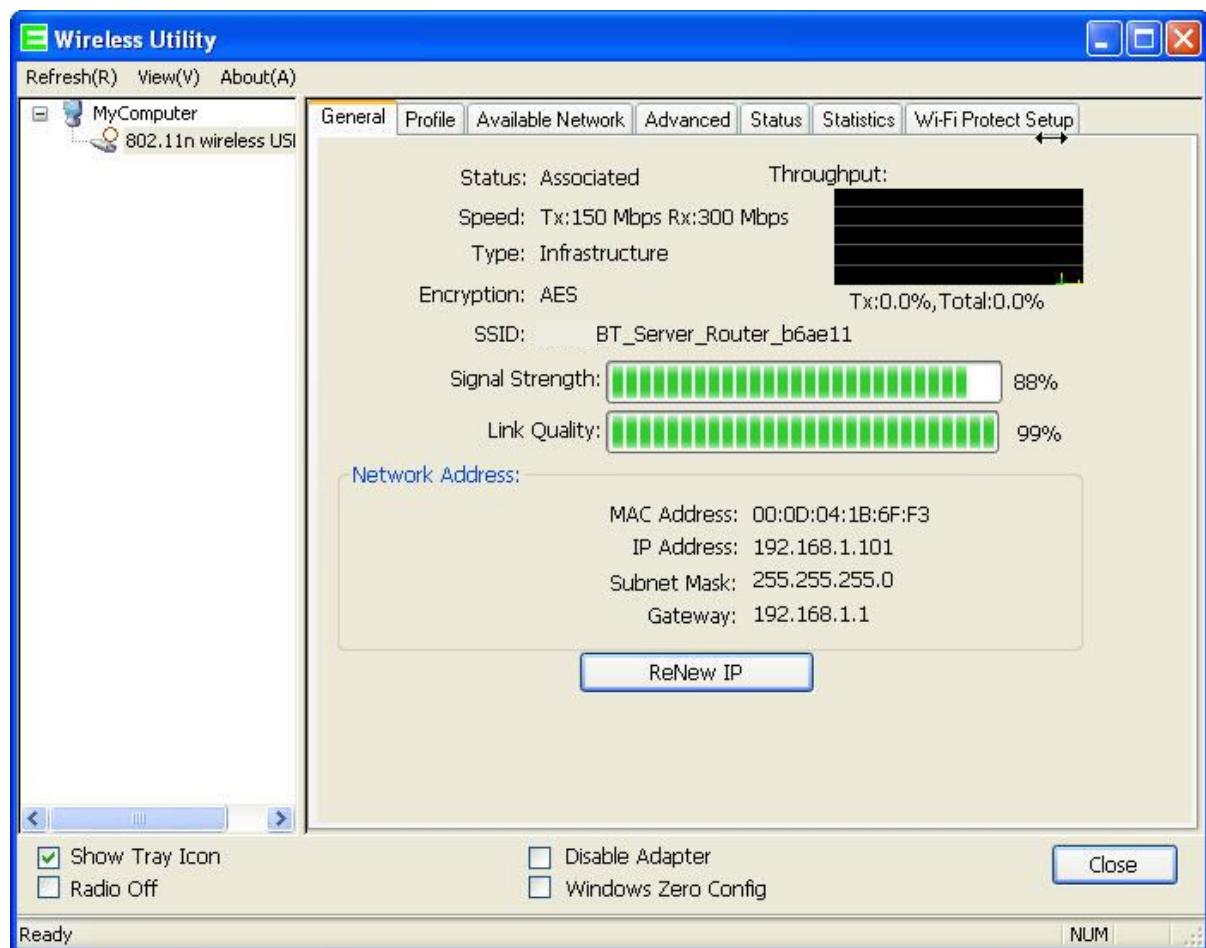
---

**Client PIN Number:**

(2.) Open the configuration page of the wireless card which supports WPS. Click the **WiFi Protect Setup**, and then click **PBC** to make a WPS connection with AP from the WPS AP list (PBC-Scanning AP).

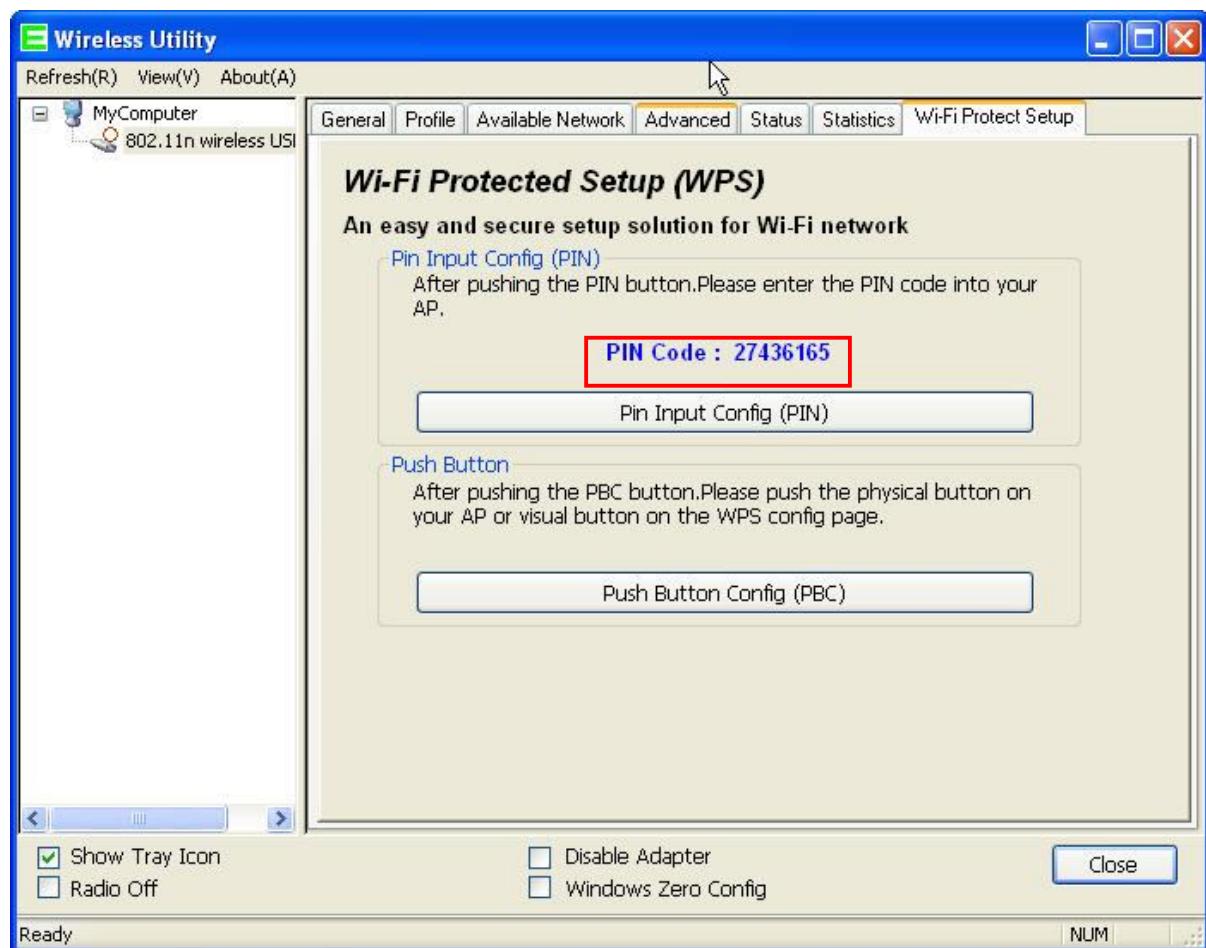


(3.) When you see **Network Address**, it means the WPS connection between wireless card and Server Router is established.



\* Start PIN:

(1.) Please open the configuration page of the wireless card, and write it down.



(2.) Open the Wi-Fi Protected Setup configuration page of Server Router, input the PIN number from the wireless card then click **Start PIN**.

## Wi-Fi Protected Setup

This page allows you to change the setting for WPS (Wi-Fi Protected Setup). Using this feature could let your wireless client automatically synchronize its setting and connect to the Access Point in a minute without any hassle.

---

**Disable WPS**

**WPS Status:**  Configured  Un-Configured

**Self-PIN Number:** 73220398

**Push Button Configuration:**

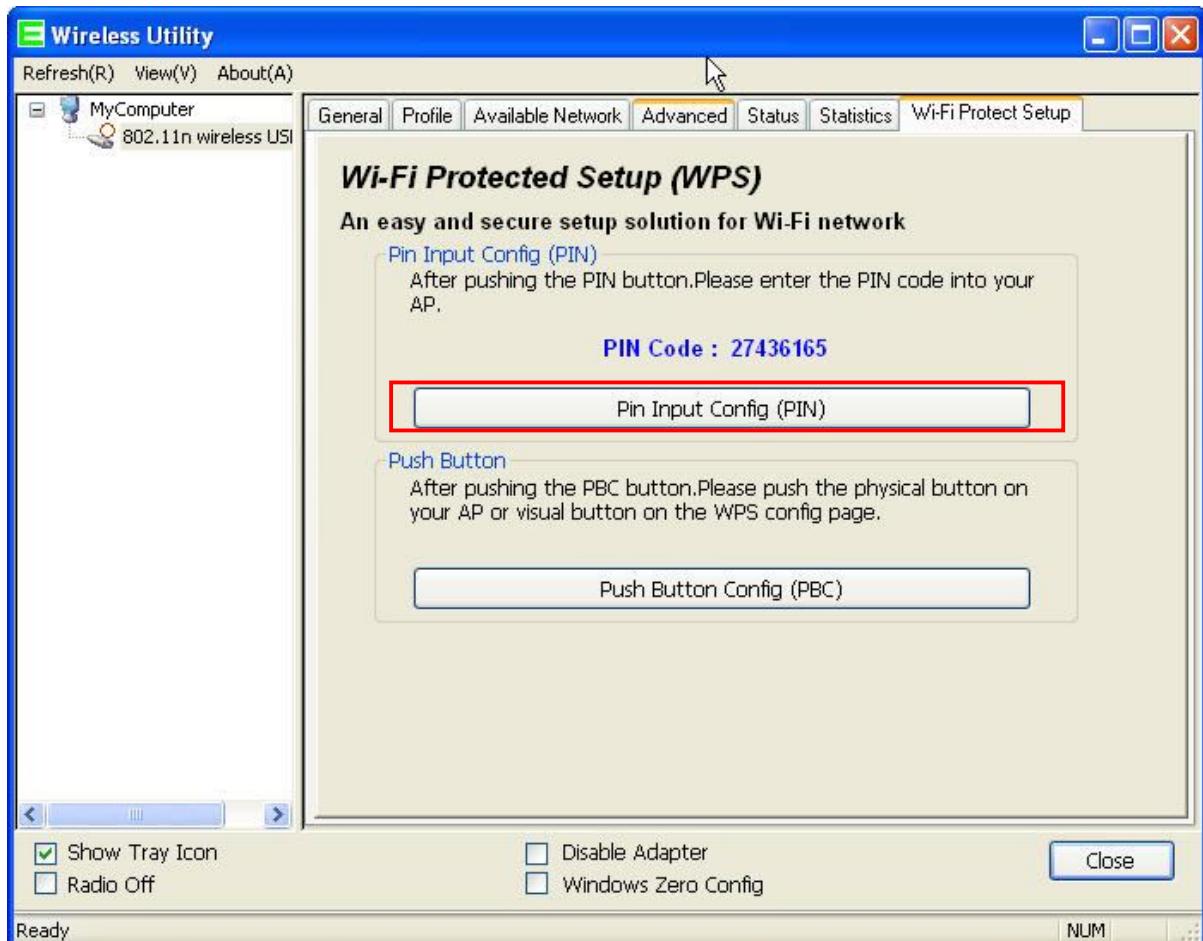
**Current Key Info:**

Authentication	Encryption	Key
WPA2 PSK	AES	65756575

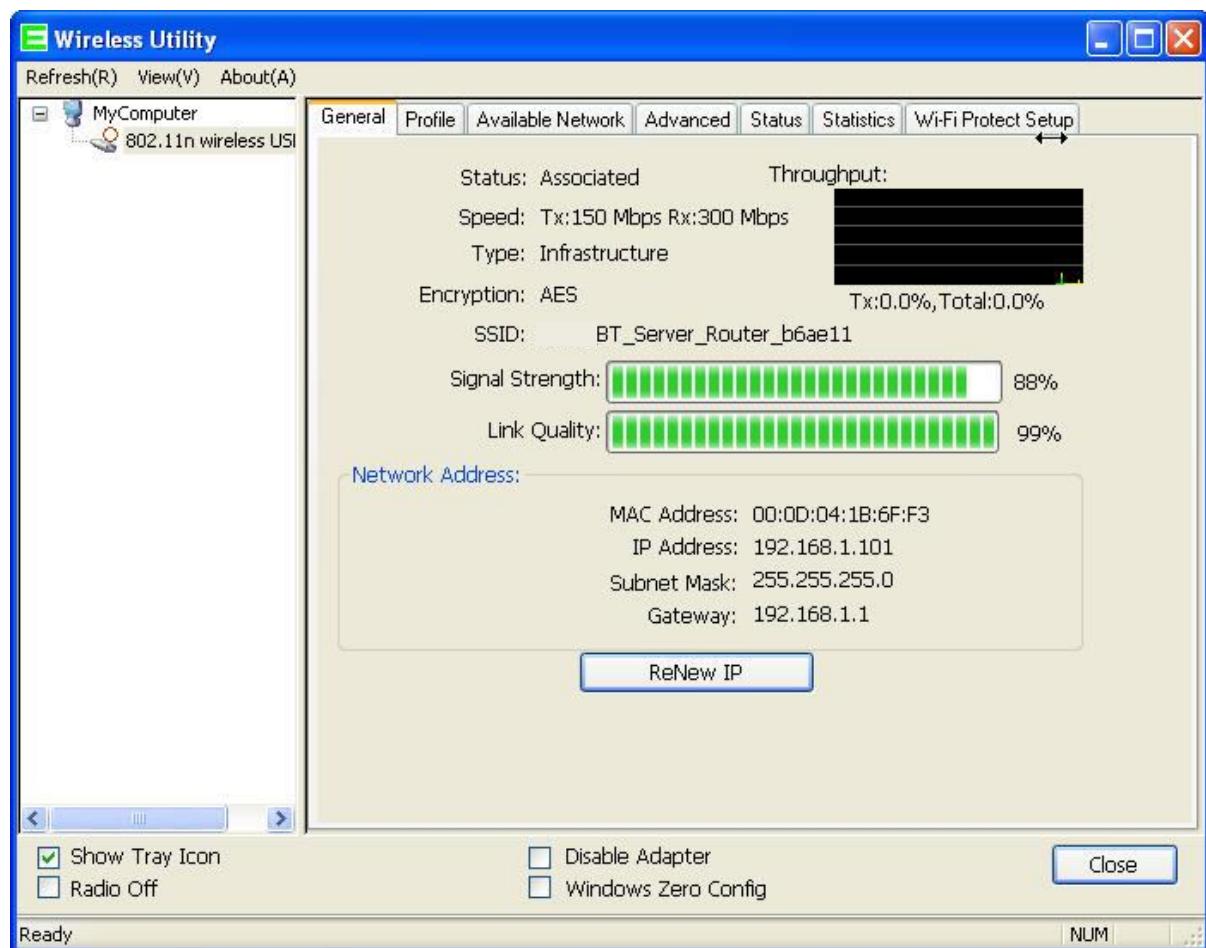
---

**Client PIN Number:**

(3.) Open the configuration page of the wireless card which supports WPS. Click the **WPS**, and then click **PIN** to make a WPS connection with AP from the WPS AP list (PIN-Begin associating to WPS AP).



(4.) When you see **Network Address**, it means the WPS connection between wireless card and Server Router is established.



## 5.3 NAT

### 5.3.1 Visual Server

Port forwarding service is to transfer packets from specific ports to corresponding IP address on local area network.

The screenshot shows the 'Visual Server' configuration interface with the following sections:

- Left Sidebar (Router):**
  - One Button Setup
  - Step Setup
  - IP Config
  - Wireless
  - NAT
    - Visual Server** (selected)
    - Visual DMZ
  - Firewall
  - Server
  - System Management
  - Log & Status
  - Logout
- Visual Server Section:**

Entries in this table allow you to automatically redirect common network services to a specific machine behind the NAT firewall. These settings are only necessary if you wish to host some sort of server like a web server or mail server on the private local network behind your Gateway's NAT firewall.

Enable Port Forwarding

IP Address:  Protocol:  Port Range:  -  Comment:
- Current Port Forwarding Table:**

Local IP Address	Protocol	Port Range	Comment	Select
<input type="button" value="Delete Selected"/>	<input type="button" value="Delete All"/>	<input type="button" value="Reset"/>		

## **1. Enable Port Forwarding**

Please select to enable Port Forwarding service or not.

## **2. IP Address**

Please specify the IP address which receives the incoming packets.

## **3. Protocol**

Please select the protocol type.

## **4. Port Range**

Please enter the port number, for example 80-80 or 20-22.

## **5. Comment**

You can add comments for this port forwarding rule.

## **6. Apply Changes & Reset**

Click on **Apply Changes** to save the setting data. Or you may click on **Reset** to clear all the input data.

## **7. Current Port Forwarding Table**

It will display all port forwarding regulation you made.

## **8. Delete Selected & Delete All**

Click **Delete Selected** will delete the selected item. Click **Delete All** will delete all items in this table.

## **9. Reset**

You can click **Reset** to cancel.

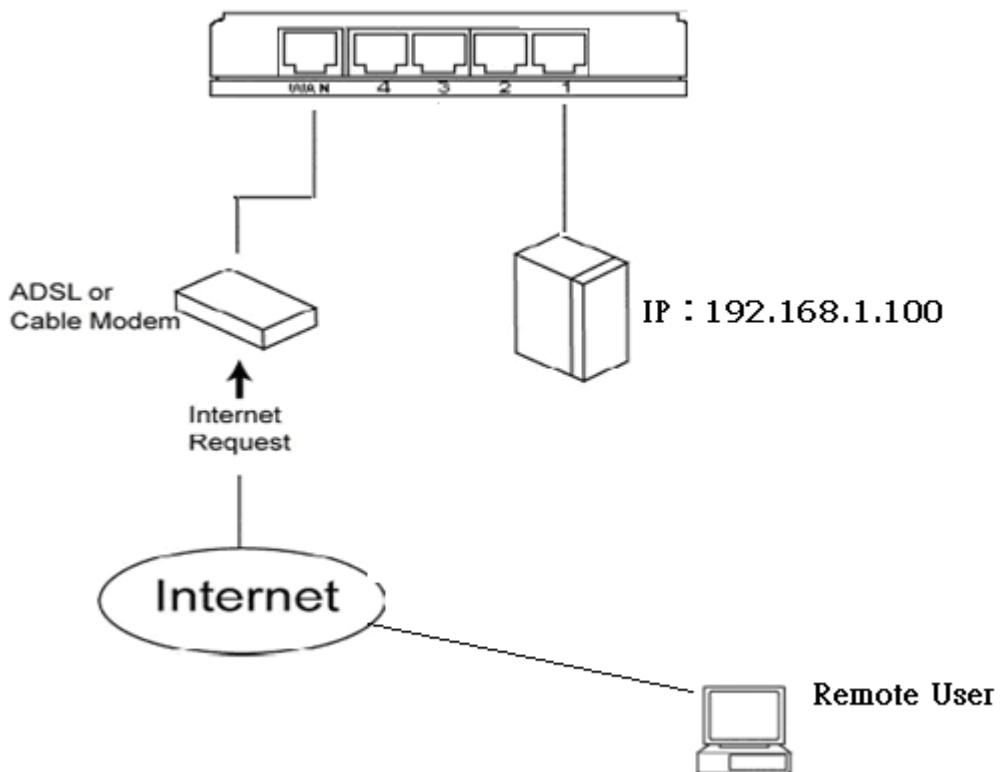
\*The following figure shows the ip forwarding configuration of your web on a local area network. The web server is located on 192.168.1.100, forwarding port is 80, and type is TCP+UDP.

Configuration:

Private IP: 192.168.1.100

Port: 80 - 80

Type: TCP+UDP

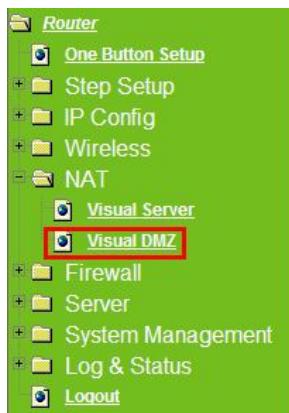


### 5.3.2 Visual DMZ

It will expose the computer which users enable the DMZ settings. All packets from the Internet will be forwarded to this computer. It is useful for specific applications, but please be careful to establish it.

DMZ (Demilitarized Zone) Host is a zone that is not limited by the firewall service.

DMZ allows you to redirect the packets from specific IP address to WAN IP address. An external attacker only has access to equipment in the DMZ, rather than the whole of the network, and internal users can access to this equipment.



#### 1. Enable DMZ

It will enable the DMZ service if you select it.

## 2. DMZ Host IP Address

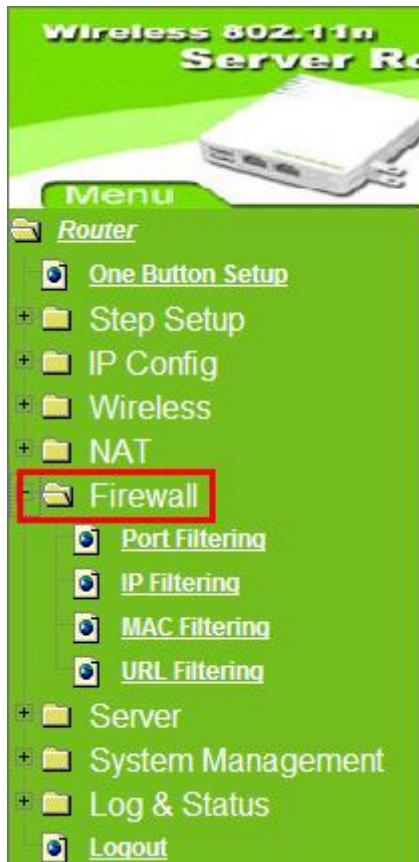
Please enter the specific IP address for DMZ host.

## 3. Apply Changes & Reset

Click on **Apply Changes** to save the setting data. Or you may click on **Reset** to clear all the input data.

## 5.4 Firewall

The Firewall service includes Port Filtering, IP Filtering, MAC Filtering, and URL Filtering.



### 5.4.1 Port Filtering

This function allows users to filter and manage specific ports; to limit the use of certain applications to transmit through a specific port. Port filtering helps users to improve the security of your network.

## 1. Enable Port Filtering

Please select **Enable Port Filtering** to filter ports.

## 2. Port Range

Please enter the port number that needs to be filtered.

## 3. Protocol

Please select the protocol type of the port.

## 4. Comment

You can add comments for this regulation.

## 5. Apply Changes & Reset

Click on **Apply Changes** to save the setting data. Or you may click on **Reset** to clear all the input data.

## 6. Current Filter Table

It will display all ports that are filtering now.

## 7. Delete Selected & Delete All

Click **Delete Selected** will delete the selected item. Click **Delete All** will delete all items in this table.

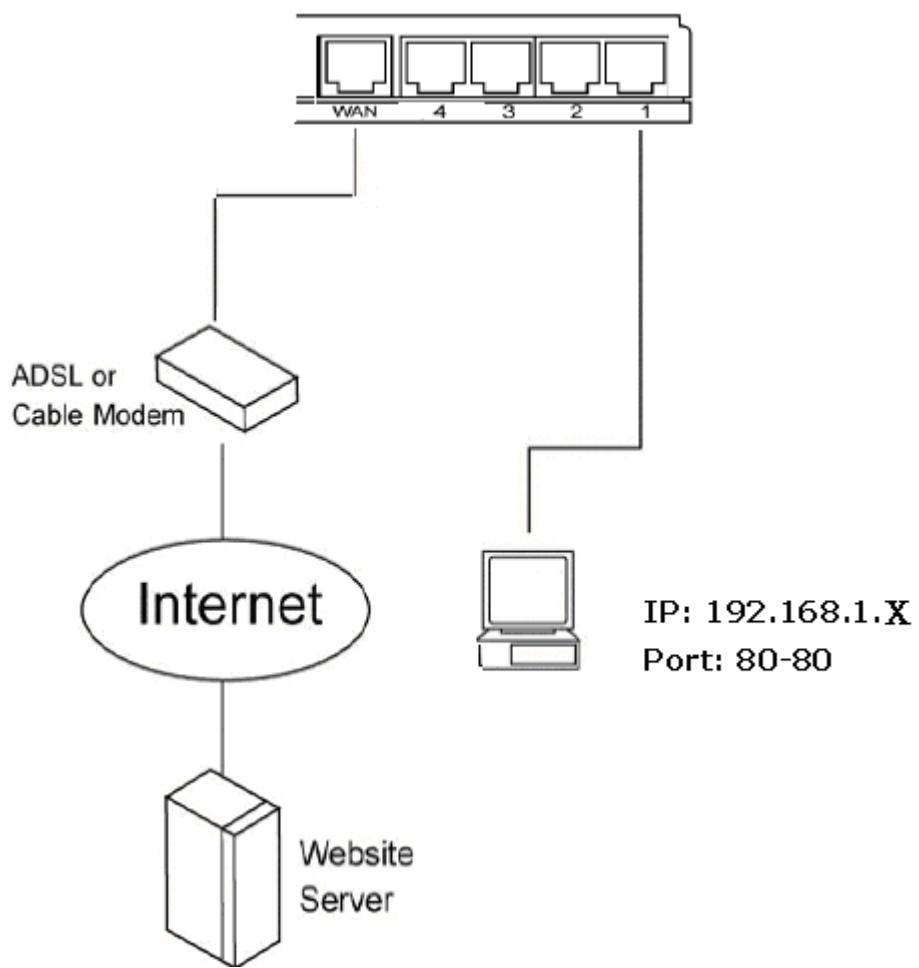
## 8. Reset

You can click **Reset** to cancel.

\* The following figure shows a user limits some applications to use the 80 port.

IP: 192.168.1.X

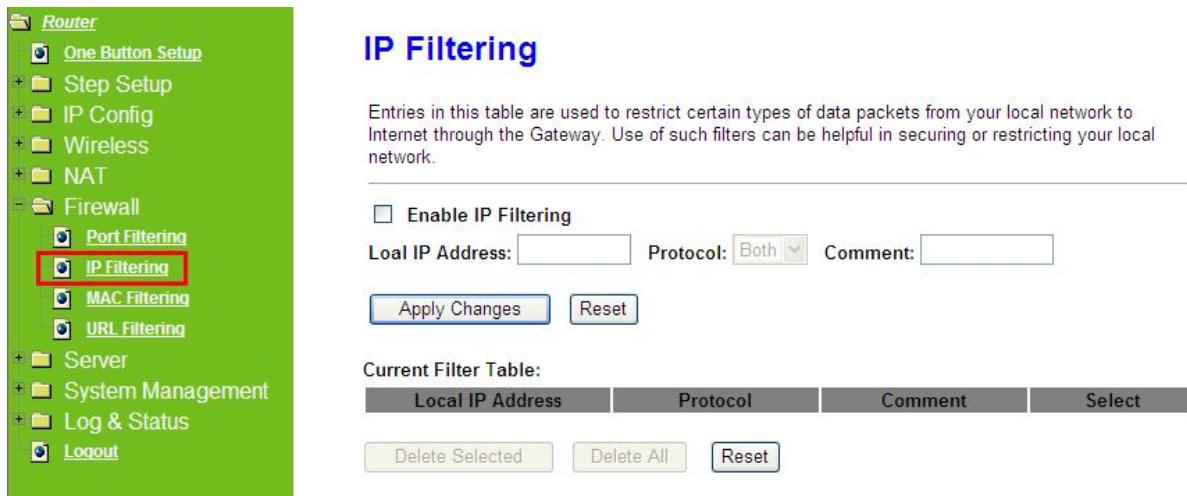
Port: 80-80



\*All clients inside the local area network can't open the 80 port through this router.

### 5.4.2 IP Filtering

This function can limit a specific ip address to access the Internet. The computer, whose ip address is listed on filter table, will be denied the access request by router. This protocol is made base on Internet Protocol and Transmission Control Protocol.



Router

- One Button Setup
- Step Setup
- IP Config
- Wireless
- NAT
- Firewall
  - Port Filtering
  - IP Filtering**
  - MAC Filtering
  - URL Filtering
- Server
- System Management
- Log & Status
- Logout

## IP Filtering

Entries in this table are used to restrict certain types of data packets from your local network to Internet through the Gateway. Use of such filters can be helpful in securing or restricting your local network.

Enable IP Filtering

Local IP Address:  Protocol:  Comment:

Current Filter Table:

Local IP Address	Protocol	Comment	Select

#### 1. Enable IP Filtering

Please select **Enable IP Filtering** to filter IP addresses.

#### 2. Local IP Address

Please enter the IP address that needs to be filtered.

#### 3. Protocol

Please select the protocol type of the IP address.

#### 4. Comment

You can add comments for this regulation.

#### 5. Apply Changes & Reset

Click on **Apply Changes** to save the setting data. Or you may click on **Reset** to clear all the input data.

#### 6. Current Filter Table

It will display all IP addresses that are filtering now.

#### 7. Delete Selected & Delete All

Click **Delete Selected** will delete the selected item. Click **Delete All** will delete all items in this table.

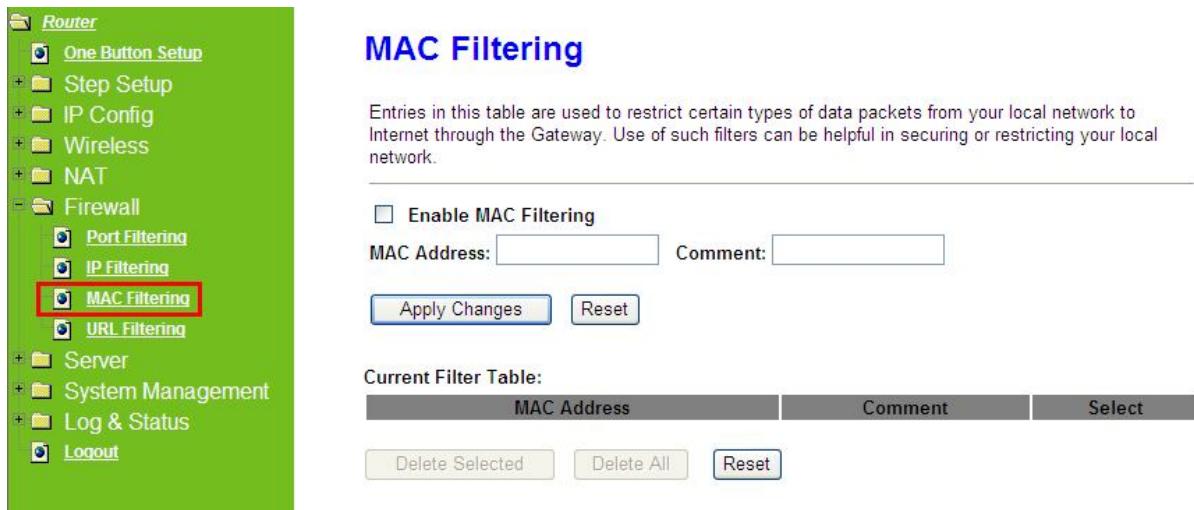
#### 8. Reset

You can click **Reset** to cancel.

---

### 5.4.3 MAC Filtering

This function can limit a specific MAC address to access the Internet. The network card, whose MAC address is listed on filter table, will be denied the access request by router.



## 1. Enable MAC Filtering

Please select **Enable MAC Filtering** to filter MAC addresses.

## 2. MAC Address

Please enter the MAC address that needs to be filtered.

## 3. Comment

You can add comments for this regulation.

## 4. Apply Changes & Reset

Click on **Apply Changes** to save the setting data. Or you may click on **Reset** to clear all the input data.

## 5. Current Filter Table

It will display all MAC addresses that are filtering now.

## 6. Delete Selected & Delete All

Click **Delete Selected** will delete the selected item. Click **Delete All** will delete all items in this table.

## 7. Reset

You can click **Reset** to cancel.

---

### 5.4.4 URL Filtering

This function is used to block users trying to access some webs with specific key words. Please enter the URL of the web in **URL Address** field.



## URL Filtering

URL filter is used to deny LAN users from accessing the internet. Block those URLs which contain keywords listed below.

**Enable URL Filtering**

URL Address:

Current Filter Table:

URL Address	Select
-------------	--------

### 1. Enable URL Filtering

Please select **Enable URL Filtering** to filter web pages.

### 2. URL Address

Please enter the URL of the web page. For example: www.google.com.

### 3. Apply Changes & Reset

Click on **Apply Changes** to save the setting data. Or you may click on **Reset** to clear all the input data.

### 4. Current Filter table

It will display all web pages that are filtering now.

### 5. Delete Selected & Delete All

Click **Delete Selected** will delete the selected item. Click **Delete All** will delete all items in this table.

### 6. Reset

You can click **Reset** to cancel.

**Caution:** This function is not in effect when the Visual Server is enabled. Please disable Visual Server before activate filter.

---

## 5.5 Server

Server Router provides Samba Server, FTP Server, Web Camera Server, and Printer Server Application.

### 5.5.1 Samba Server

Support NetBIOS Protocol, the consumer sharing file or printer which provides as the “**My Network Places**”. Please make sure storage devices and printers are connecting to USB ports on the router and already mounting.



## Samba Server

You can enable or disable samba server function in this page.

Enable Samba Server:  Enabled  Disabled

Workgroup Name:

Server Name:

Server Description:

### 1. Enable Samba Server

Enable or disable this function.

### 2. Workgroup Name

Input the workgroup name, default is “**WORKGROUP**”.

### 3. Server Name

Input the server name, default is “**Server Router**”.

### 4. Server Description

You can input description of the server.

### 5. Apply & Cancel

Click on **Apply** button to finish setting. Click on **Cancel** button to clean the setting on this page.

#### 5.5.1.1 How to enter the sharing folder

Please follow below steps.

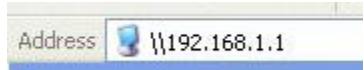
Step 1:

Please click the “**start**”, and select “**My Computer**”.



Step 2:

In the Address blank input the IP address: <\\192.168.1.1>.



Step 3:

Appear following menu, can open following to share internal data.



**Note :**

1. If connected USB flash or HDD, and then enable samba server function, it will appear a samba folder.
2. If connected USB printer, and then enable printer server function, it will appear a printer icon.

### 5.5.2 FTP Server

FTP Server utility allows both local and remote users to upload or download files, pictures or MP3 music form the same storage device. Before configure FTP Server, please make sure the storage device is properly plug into any USB port on the router and make sure this USB storage device is detected by the router.

#### 1. Enable FTP Server

Select to “**Enable**” or “**Disable**” FTP server.

#### 2. Enable Anonymous to Login

Allow anonymous to login after check on Enable.

#### 3. Enable FTP Access from WAN

Allow FTP access from WAN side by checking on Enable for this item.

#### 4. FTP Server Port

The default is 21. Define the FTP command transfer service port. If you want to change this port number, remember to change the service port setting of your FTP client, also.

## 5. Idle Connection Time-Out

When a specific time value is added, FTP Server will be de-activated if it has no activity within the time limit. The default is 300 seconds; the minimum is 60 seconds.

## 6. Apply & Cancel

Click on **Apply** button to continue. Click on **Cancel** button to clean the setting on this page.

## 7. User Account List

User Name, Status, and Opened Directory/File can be shown on the list.

**Note :** FTP server is compatible with FAT32 or EXT3 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 EXT3 standard.

### 5.5.3 Webcam Server

By connecting web camera to the router, it allows user to monitor their home or office from remote locations.

#### 5.5.3.1 Webcam Server Basic Setting



The screenshot shows the Router configuration menu. The 'WebCam Server' option is highlighted with a red box. The menu items include: Router, One Button Setup, Step Setup, IP Config, Wireless, NAT, Firewall, Server (with Samba Server, FTP Server, WebCam Server, and Print Server), System Management, Log & Status, and Logout.

**WebCam Server**

You can enable or disable WebCAM server function in this page.

**Enable Webcam:**  Enabled  Disabled

**Access from WAN:**  Enabled  Disabled

**Image format:** 320x240

Preview Record Setting Apply Changes Reset

##### 1. Enable Webcam Server

Select to “**Enable**” or “**Disable**” webcam server.

##### 2. Access from WAN

Allow webcam can access from WAN side by checking on Enable for this item.

### 3. Image format

The format is 320X240 pixels.

### 4. Preview

Click on this button, you can preview the image from webcam.

### 5. Record Setting

Please see the detail advance setting in "**5.5.3.2 Webcam Advanced Configuration**".

### 6. Apply & Cancel

Click on **Apply** button to continue. Click on **Cancel** button to clean the setting on this page.

## 5.5.3.2 Webcam Server Advanced Setting

Click on "**Record Setting**" button, and the screen will appear as below.

### Webcam Advanced Configuration

Snapshot Record Settings.

Save image interval:	<input type="text" value="5"/> sec (default: 5)
Save Location:	<input checked="" type="radio"/> <b>USB</b> <input type="radio"/> <b>Remote FTP</b>
Remote FTP URL:	<input type="text"/>
Remote FTP port:	<input type="text"/>
Remote FTP user:	<input type="text"/>
Remote FTP password:	<input type="text"/>
Remote FTP Directory:	<input type="text"/>

[Back](#) [Apply Changes](#) [Reset](#)

#### 1. Save image interval

For saving image, you can set the save interval time, the default value is 5 seconds.

#### 2. Save Location

Set the save location for webcam image, you may save into **USB HDD** or **Remote FTP**; if select save to **Remote FTP**, please continue following remote FTP setting.

#### 3. Remote FTP URL

Input the FTP URL for saving webcam image.

#### 4. Remote FTP port

Input the FTP port number under URL to save image.

## **5. Remote FTP user**

Input the users name you like and it will be used to save the webcam image into the FTP server.

## **6. Remote FTP password**

Input the remote password.

## **7. Remote FTP Directory**

To provide option of which folder should be used for saving webcam image.

## **8. Back**

Click on **Back** button for returning to Webcam Basic Setting screen.

## **9. Apply & Cancel**

Click on **Apply** button to continue. Click on **Cancel** button to clean the setting on this page.

### **5.5.3.3 Application for Web Camera**

#### **5.5.3.3.1 Web Camera Monitoring Application**

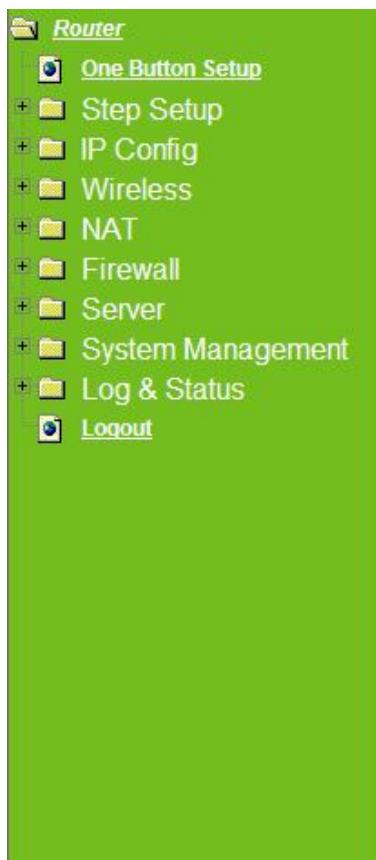
Monitor your home with a Webcam via Server Router. Take pictures via Server Router, also can do the monitoring or recording all images into the USB HDD for reviewing. Often marketed as surveillance tools for home or office security, network Webcams are now being employed by early adopters for more personal matters, such as watching kids and monitoring pets. The Webcam can be remotely accessed and controlled via a browser. Besides, to record and monitor live action with USB webcam, also can view the image through Internet browsers or mobile phones.

##### **5.5.3.3.1.1 Web Camera Monitoring via WAN connecting**

For viewing the image via webcam from WAN connecting, below is the diagram.

- How to check your WAN IP address**

To monitor the image via webcam from outside door, you need to know the WAN IP address. Select “**Network Configuration**” under **Log & Status** in main Menu after connection, and you will see the WAN IP Address which used to connect to webcam screen. Here use 192.168.2.51 as example.



## Network Config

This page shows the current status and some basic settings of the device.

System	
Uptime	0 day:0h:33m:7s
Firmware Version	2007/04/25 Ver1.0.7 B05
Wireless Configuration	
Mode	AP
Band	2.4 GHz (B+G)
SSID	Broadband_Router
Channel Number	11
Encryption	Disabled
MAC Address	00:e0:4c:81:86:21
Associated Clients	0
LAN Configuration	
Attain IP Protocol	Fixed IP
IP Address	192.168.1.1
Subnet Mask	255.255.255.0
Default Gateway	192.168.1.1
DHCP Server	Enabled
MAC Address	00:e0:4c:81:86:21
WAN Configuration	

### ● Monitor the image via webcam from WAN

Input the WAN IP Address (as you see in above screen) into browser blanks, and you will see the personal account login screen appear then input your own user account and password. After login by personal, your will see the personal control panel screen as below, please click on “**My Webcam**”.



Click on Personal Panel to enter.



There will be a pop-up screen showing the image from web camera as below example.



### **5.5.3.3.1.2 Web Camera Monitoring via mobile phone**

Also, you may view the monitor live action through mobile phones.

Please key in the WAN IP address plus “**/webcam.html**” e.g.  
**http://192.168.2.51/webcam.html** into the mobile phone’s browser blank and you will see the webcam user login screen appeared.



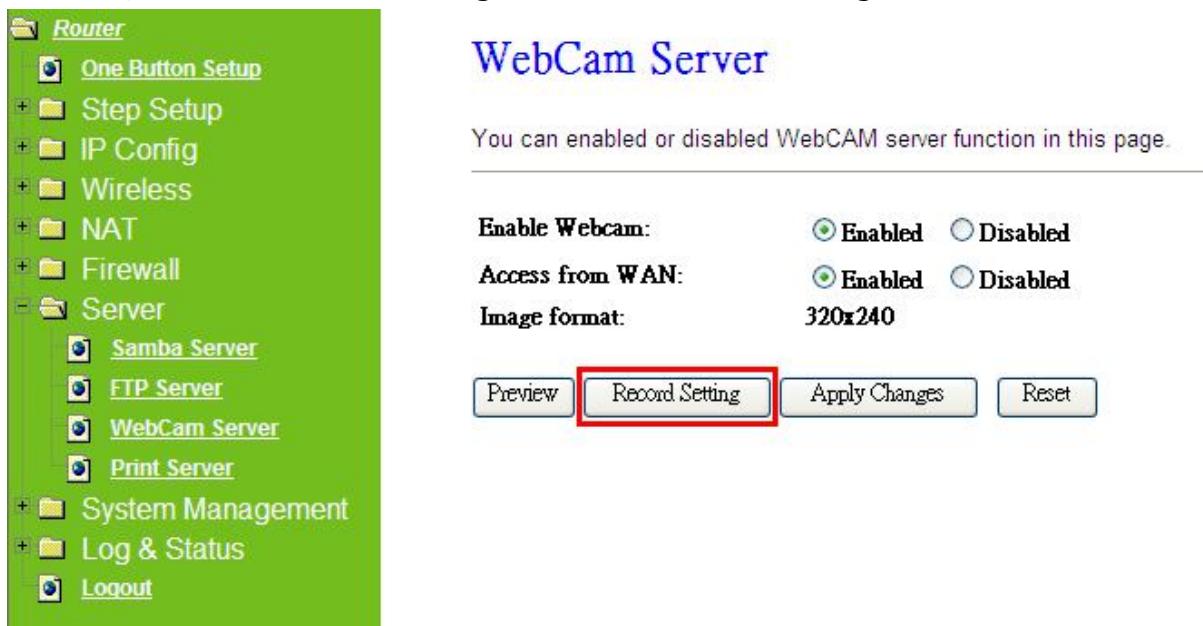
Input Username and Password of your own. You will see like as below monitor screen.



### 5.5.3.3.2 Web Camera Recording

#### 5.5.3.3.2.1 Administrator

Server Router also can record the pictures from Webcam; only Administrator can do the settings. Select **Web Camera Server** from main Menu and Enable this function, click on **Record** setting button for further setting.



The screenshot shows the Router configuration menu on the left with the 'WebCam Server' option selected. The main page title is 'WebCam Server' with the sub-instruction 'You can enabled or disabled WebCAM server function in this page.' Below are configuration options: 'Enable Webcam' (radio buttons for Enabled/Disabled, 'Enabled' is selected), 'Access from WAN' (radio buttons for Enabled/Disabled, 'Enabled' is selected), and 'Image format' (set to 320x240). At the bottom are buttons for 'Preview', 'Record Setting' (which is highlighted with a red box), 'Apply Changes', and 'Reset'.

To setup the Webcam Advanced Configuration for each blank and the image from webcam will be recorded into your USB HDD or Remote FTP.

### Webcam Advanced Configuration

Snapshot Record Settings.

Save image interval:	<input type="text" value="5"/> sec (default: 5)
Save Location:	<input checked="" type="radio"/> USB <input type="radio"/> Remote FTP
Remote FTP URL:	<input type="text"/>
Remote FTP port:	<input type="text"/>
Remote FTP user:	<input type="text"/>
Remote FTP password:	<input type="text"/>
Remote FTP Directory:	<input type="text"/>

[Back](#) [Apply Changes](#) [Reset](#)

For administrator, you may view all the images from webcam recording, please

select **Folder Management** and click on **Disk Explorer** to view entire folder inside the disk including webcam record files.

## Folder Management

You can specify which USB storage to be System Disk.

USB Device Name

SysDisk	Disk	TYPE	Capacity	Free Space	Function
	USB A	Unknown	63MB	39MB	<input type="button" value="Unplug"/>
<input type="button" value="Disk Explorer"/>					

## Partition / Format SysDisk

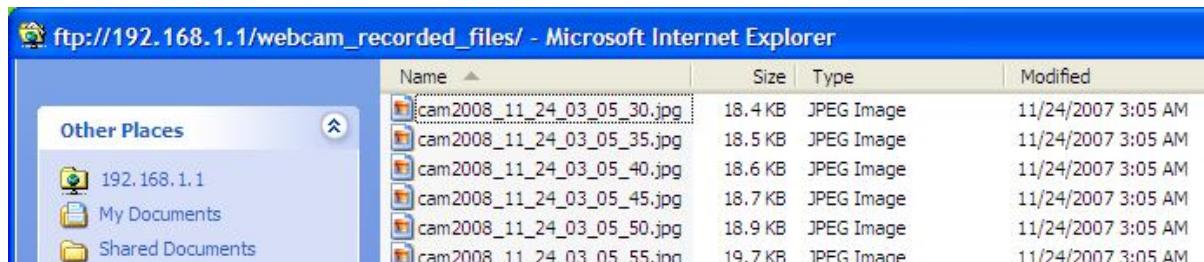
All existing data and partitions on the HDD will be DESTROYED ! Make sure you really need to do this !

TYPE:  FAT16/32  NTFS  EXT3

After click on **Disk Explorer**, you will see the folder screen appear including all the folders.



All the image files will be saved in the folder "**webcam\_recorded\_files**". Please open the file for checking.



### 5.5.3.3.2.2 Personal Application

All the users under administrator's setting can view entire webcam recording images from **My Document**. Please login by your own personal account. For viewing your own folder, please click on "**My Document**".



After click on "**My Document**", you will see below folder screen appeared. You can save files here.



**Note :** If you can't open the folder inside the FTP server, please check with administrator to setup your FTP & Webcam's privileges.

### 5.5.4 Printer Server

The two USB ports on Server Router are for connection with printers to be shared on the local area network. Follow the below steps to setup your PC to connect to a Printer server.



## 1. Enable Printer Server

Check **Enable** for applying printer server.

## 2. Enable Printer Access From WAN

Allow printer can access from WAN side by checking on **Enable** for this item.

## 3. Printer Model

The printer model will be shown when plug the USB printer.

## 4. Printer Name

Input the name of printer you like.

## 5. Printer Description

Input the description of printer as your demand.

## 6. Apply & Cancel

Click on **Apply** button to continue. Click on **Cancel** button to clean the setting on this page.

Besides above setting finished, the printer setting on PC also needs to be set as follows.

### 5.5.4.1 Printer Setting on PC

After Enable Printer Server in Quick Setup and Printer Server Configuration, please follow below steps to set the detail **LPR** settings in your PC. (Below example is for Windows XP platform.)

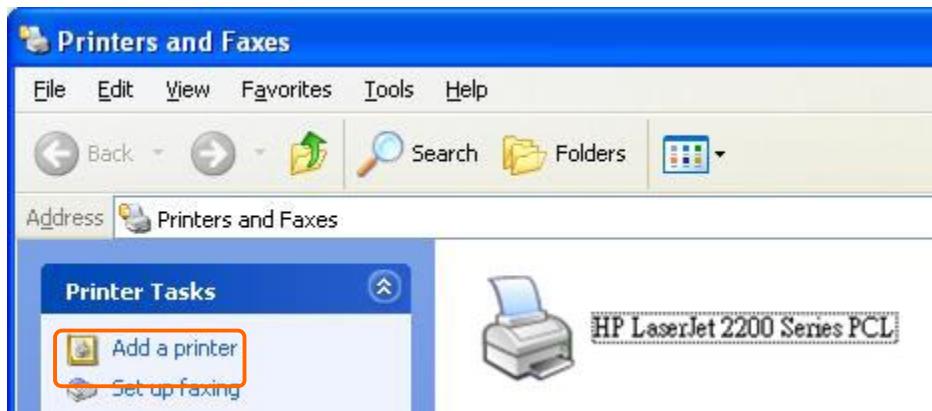
Step 1:

Please go to **Start > Printers and Faxes** to add a printer.



Step 2:

Click "**Add a printer**".



Step 3:

Click "**Next**".



Step 4:

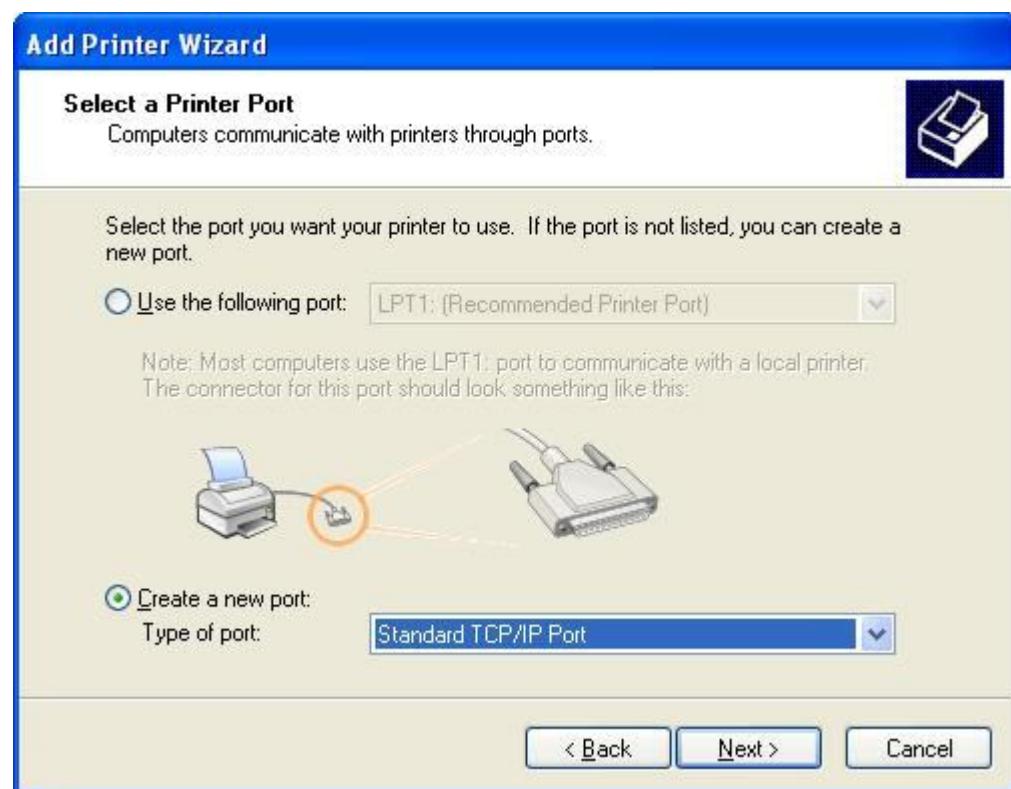
Click the **“Local printer attached to this computer”**, and then click **“Next”**.



Step 5:

Click the **“Create a new port”** and select the **“Standard TCP/IP Port”**, and

then click “**Next**”.



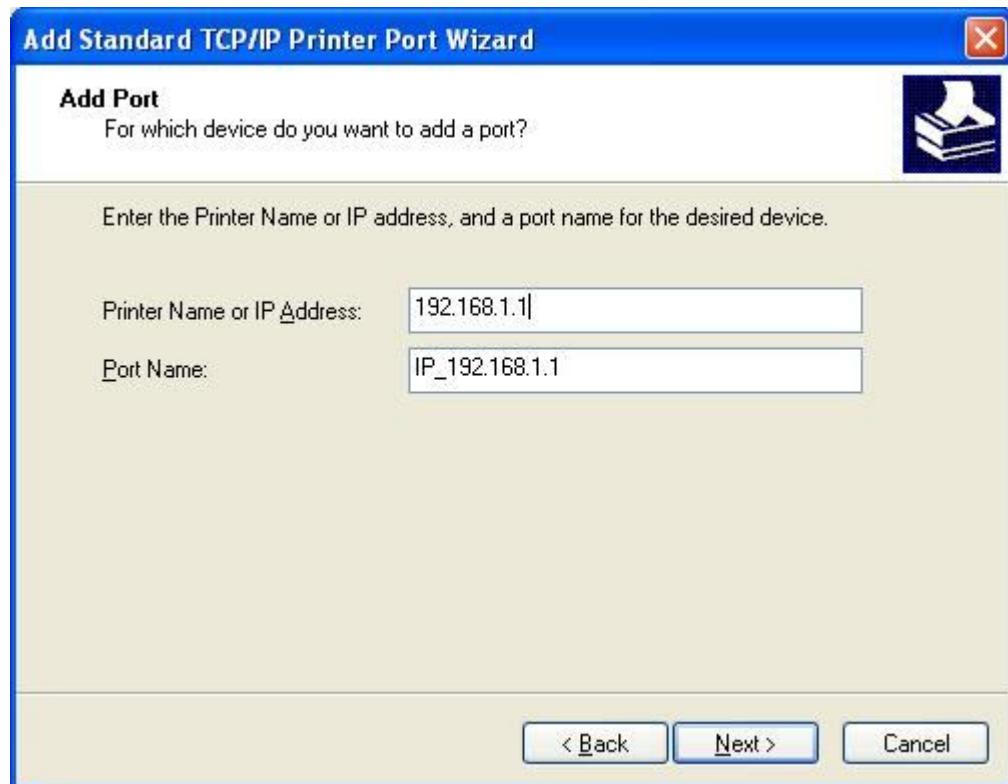
Step 6:

Click “**Next**”.



Step 7:

Input the IP address of Server Router: **192.168.1.1** (Router Mode), and then click “**Next**”.



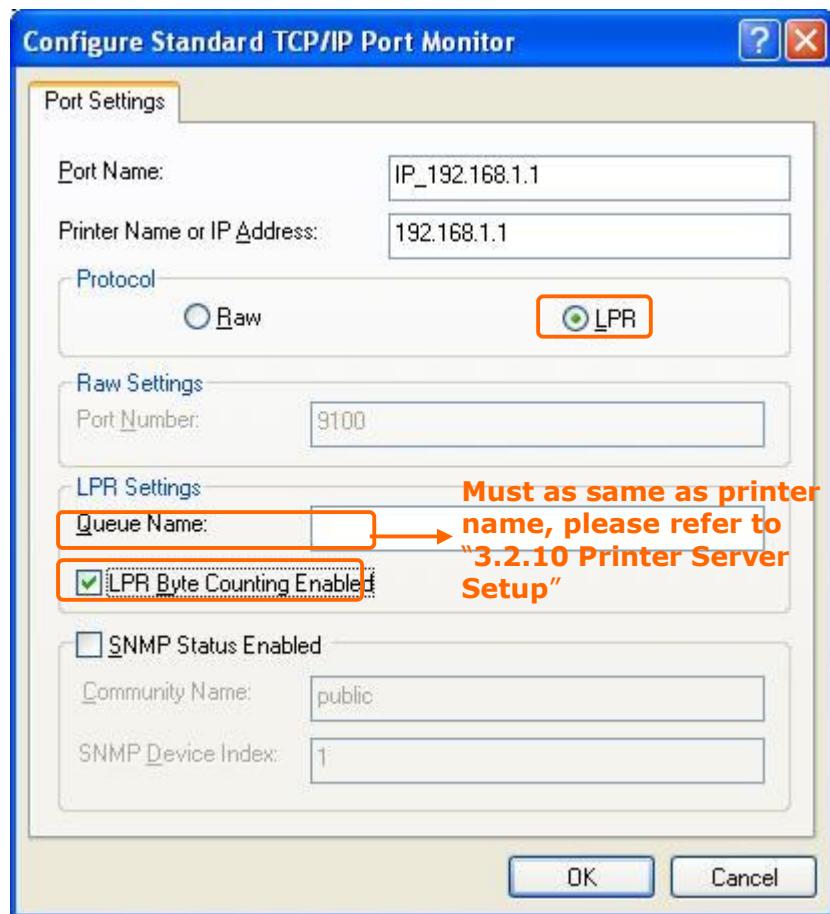
Step 8:

Select the “**Custom**” and click the “**Settings**”, and then click “**Next**”.



Step 9:

Select “**LPR**” and give it the same “**Queue Name**” as USB Printer Name as shown, and mark “**LPR Byte Counting Enabled**”. Finally, click on “**OK**” button.



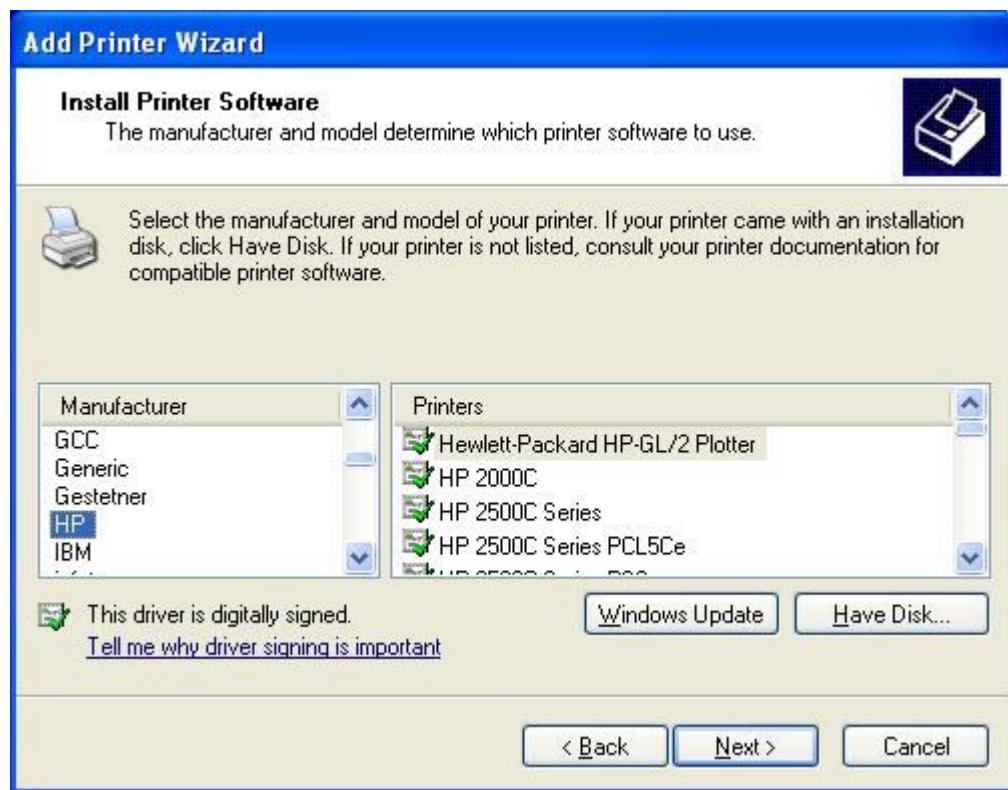
Step 10:

Click the **“Finish”**.



Step 11:

Select the **“Manufacturer”** and **“Printers”**. If your printer doesn’t listed in the table, please install its driver CD and then click on **“Have Disk...”** button for installation. Or click on **“Next”** button to finish the setting.



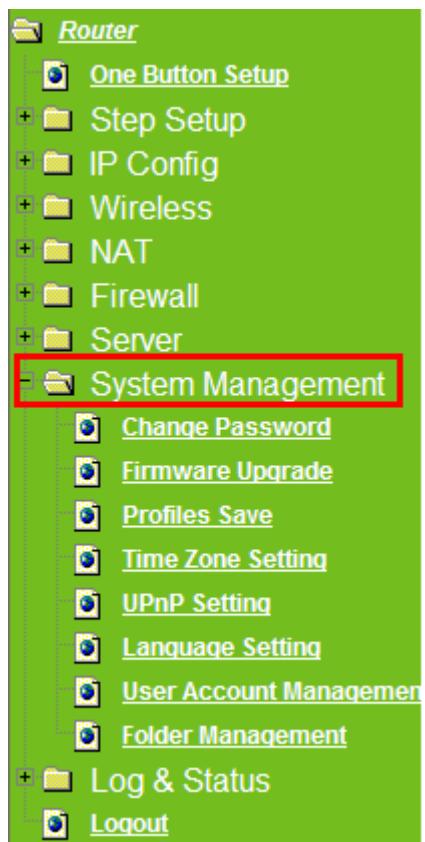
Step 12:

Click on **Finish** button and all steps of setting printer server are completely.



## 5.6 System Management

It has 6 sections: Change Password, Firmware Upgrade, Profiles Save, Time Zone Setting, UPnP Setting, and Language Setting. It is easy and helpful for users making more detailed settings.



---

### 5.6.1 Change Password

Users can set or change their password in this section.

The screenshot shows the Router's System Management menu on the left, with 'Change Password' selected. The main page title is 'Change Password'. It includes a note: 'This page is used to set the account to access the web server of Access Point. Empty user name and password will disable the protection.' There are three input fields: 'User Name', 'New Password', and 'Confirmed Password'. Below the fields are 'Apply Changes' and 'Reset' buttons. A red box highlights the 'Change Password' menu item, and another red box highlights the 'New Password' and 'Confirmed Password' fields. A red text overlay on the right reads: 'Please enter the password and confirm it.'

Click on **Apply Changes** to save the setting data. Or you may click on **Reset** to clear all the input data.

---

### 5.6.2 Firmware Upgrade

This function can upgrade the firmware of the router. There is certain risk while doing firmware upgrading. Firmware upgrade is not recommended unless the significant faulty is found and published on official website. If you feel the router has unusual behaviors and is not caused by the ISP and environment. You can check the website (<http://www.etopnetwork.com.tw>) to see if there is any later version of firmware. Download the firmware to your computer, click **Browser** and point to the new firmware file. Click **Upload** to upgrade the firmware. You can't make any move unless the machine reboot completely.

## Firmware Upgrade

This page allows you upgrade the Access Point firmware to new version. Please note, do not power off the device during the upload because it may crash the system.

Select File:

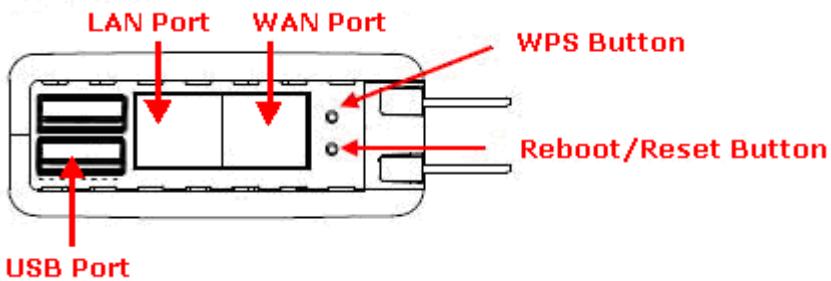
**Please download the firmware to the local computer first, and then browse it to upload.**

**Caution:** To prevent that firmware upgrading is interrupted by other wireless signals and causes failure. We recommend users to use wired connection during upgrading.

**Caution:** The firmware upgrade will not remove your previous settings.

**\*Reset button:**

On the back of this router, there is a reset button. If you can not login the administrator page by forgetting your password; or the router has problem you can't solve. You can push the reset button for 5 seconds with a stick. The router will reboot and all settings will be restored to factory default settings. If the problem still exists, you can visit our web site to see if there is any firmware for download to solve the problem.



### 5.6.3 Profiles Save

Users can save or restore the setting profile, and reset the setting to factory

default.



## Profiles Save

This page allows you save current settings to a file or reload the settings from the file which was saved previously. Besides, you could reset the current configuration to factory default.

Save Settings to File:

**Save it to a computer.**

Load Settings from File:

Reset Settings to Default:

**Upload the file from PC to router.**

**Reset to default.**

\*Please see the following instructions.

- Please click **Save...**, a prompt window will ask user to save config.dat file. (Figure 1), please select the location (Figure 2), for example: the desktop (Figure 3).



## Profiles Save

This page allows you save current settings to a file or reload the settings from the file which was saved previously. Besides, you could reset the current configuration to factory default.

Save Settings to File:

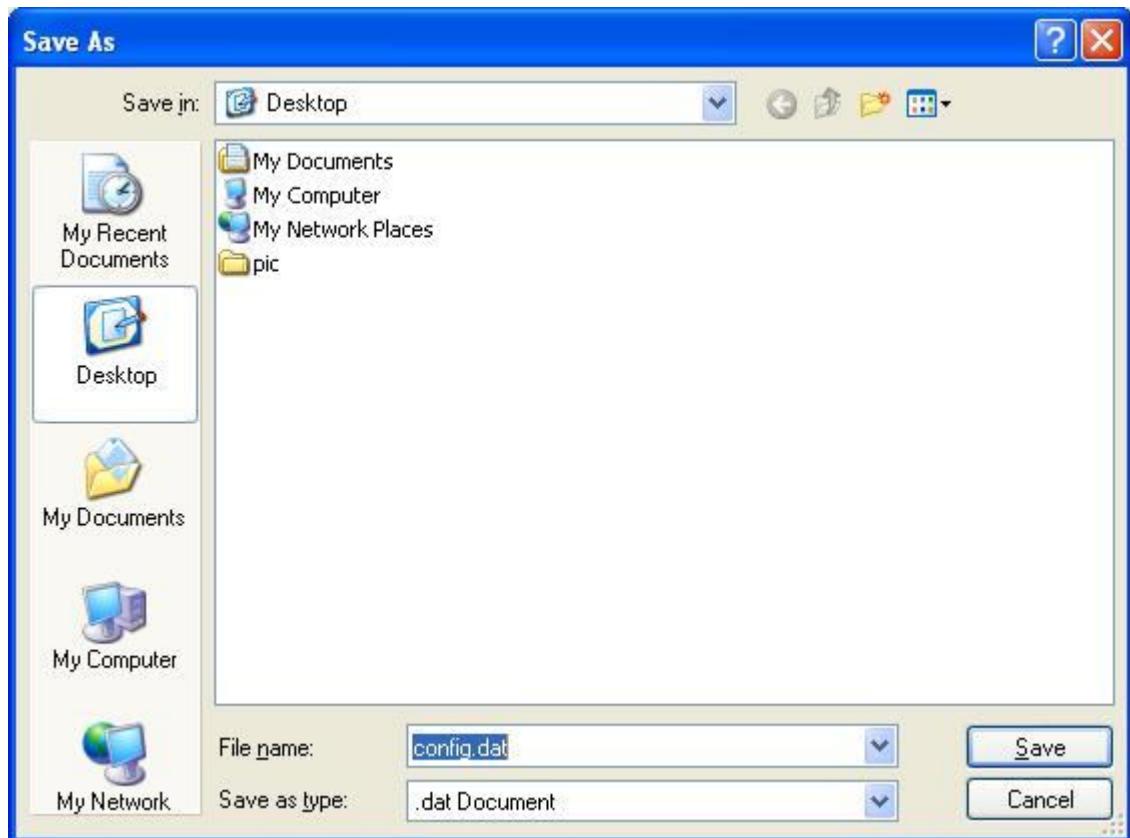
**Save it to a computer.**

Load Settings from File:

Reset Settings to Default:



(Figure 1)



(Figure 2)



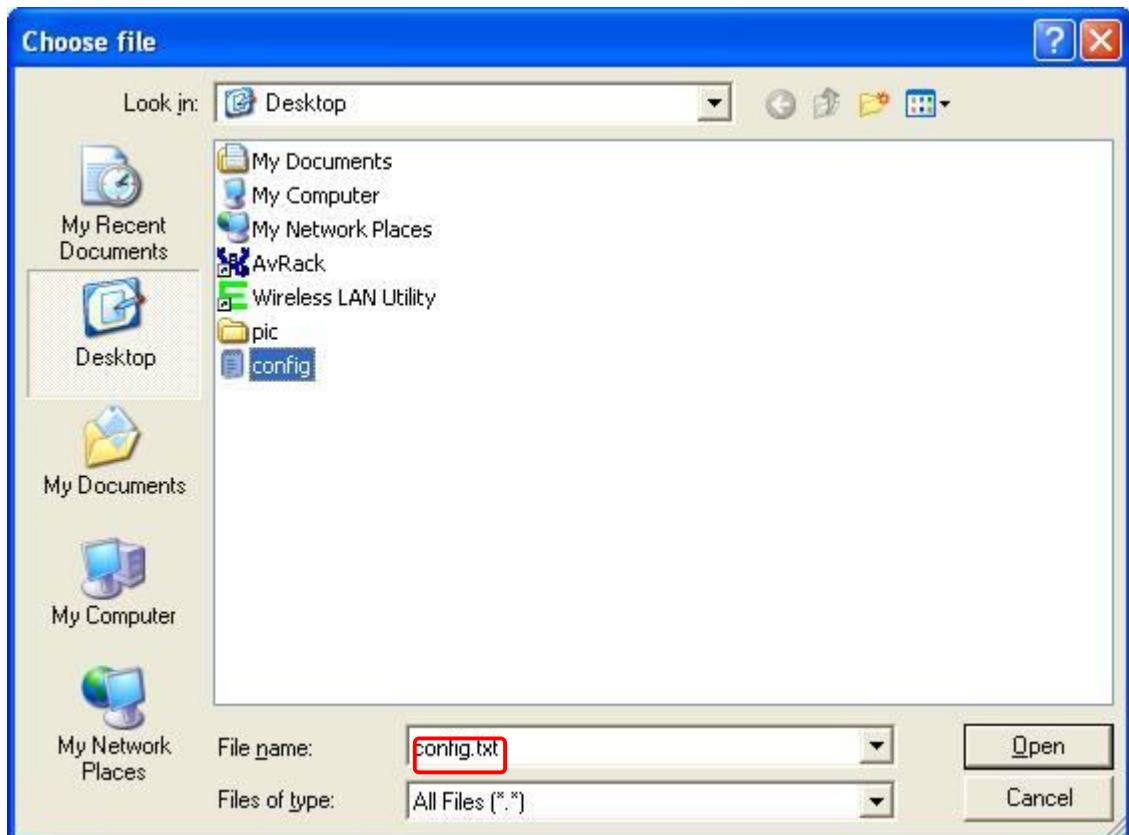
(Figure 3)

b. Please click **Browser...** (Figure 1) and select the config.dat file. (Figure 2), and then click **Upload** to retrieve (Figure 3).

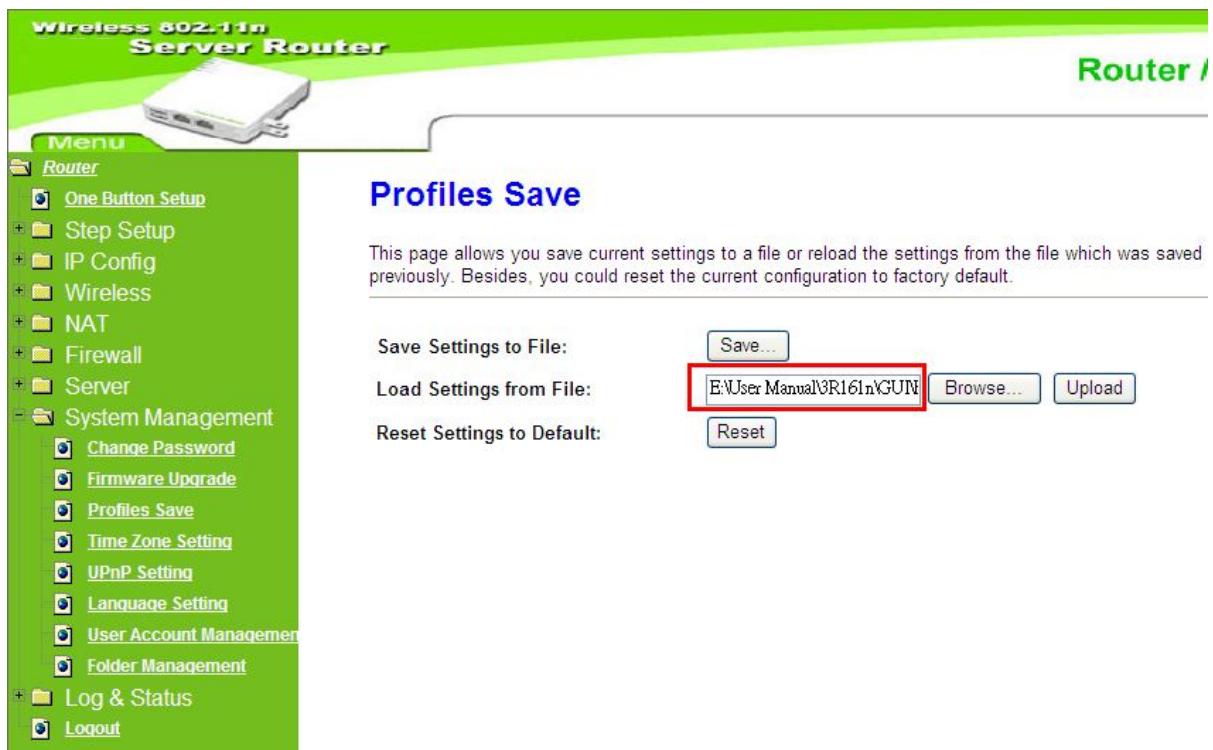


The image shows a screenshot of a router's configuration interface. The left sidebar has a green header 'Router' and a tree view of settings. Under 'System Management', the 'Profiles Save' option is highlighted with a blue box. The main content area is titled 'Profiles Save' and contains instructions: 'This page allows you save current settings to a file or reload the settings from the file which was saved previously. Besides, you could reset the current configuration to factory default.' It has three buttons: 'Save...', 'Load Settings from File:' with a 'Browse...' button (which is highlighted with a red box), and 'Upload'.

(Figure 1)



(Figure 2)

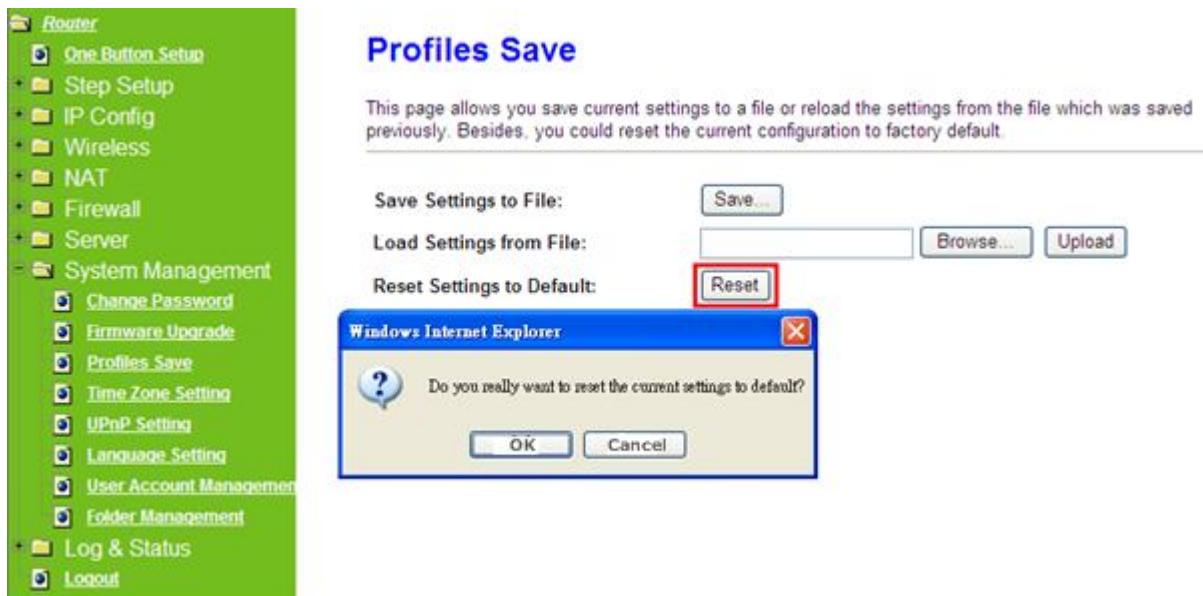


(Figure 3)

c. When you see the screen displaying like the following figure, it means update is completed. Please click **OK** to turn back to the configuration page.



d. if you want to reset the system back to factory default settings, please click **Reset** button.



e. When you see the screen displaying like the following figure, it means reset is completed. Please click **OK** to turn back to the configuration page.



#### 5.6.4 Time Zone Setting

This function allows users to select their time zone and NTP server. Users can adjust the time manually or through the NTP server.



## Time Zone Setting

You can maintain the system time by synchronizing with a public time server over the Internet.

Current Time : Yr 2000 Mon 1 Day 1 Hr 8 Mn 33 Sec 29

Time Zone Select : (GMT-08:00) Pacific Time Please select the time zone.

Enable NTP client update

Automatically Adjust Daylight Saving

NTP server :  192.5.41.41 - North America  (Manual IP Setting)

### 1. Current Time

Users can input the time manually.

### 2. Time Zone Select

Please select the time zone.

### 3. Enable NTP client update

Please select to enable NTP client update or not.

### 4. Automatically Adjust Daylight Saving

Please select to enable **Automatically Adjust Daylight Saving** or not.

### 5. NTP server

Please select the NTP server from the pull-down list, or you can enter the NTP server IP address manually.

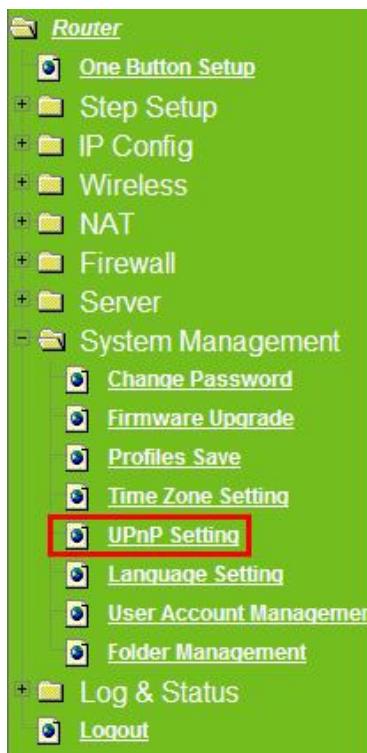
### 6. Apply Changes & Reset & Refresh

Please click on **Apply Changes** to save the setting data. Or you may click on **Reset** to clear all the input data. Or you may click on **Refresh** to update the system time on the screen.

## 5.6.5 UPnP Setting

**Universal Plug and Play (UPnP)** is a set of networking protocols promulgated by the UPnP Forum. The goals of UPnP are to allow devices to connect seamlessly and to simplify the implementation of networks in the home (data sharing, communications, and entertainment) and in corporate environments for simplified installation of computer components. Server Router supports UPnP function, and can cooperate with other UPnP devices. When you activate UPnP, please click **My**

**Network Places.** Users will see an **Internet Gateway Device** icon. By click the icon, users can enter the GUI of Server Router. If you do not wish to use UPnP, you can disable it.



## UPnP Setting

In this page, you can turn on or turn off the UPNP feature of your router.

Enable/Disable UPNP:  Enabled  Disabled

[Apply Changes](#)

[Reset](#)



### 5.5.6 Language Setting

Server Router provides users with 12 languages to choose. Users can change the language of the interface configuration. Please click **Apply Changes** after selecting a language.



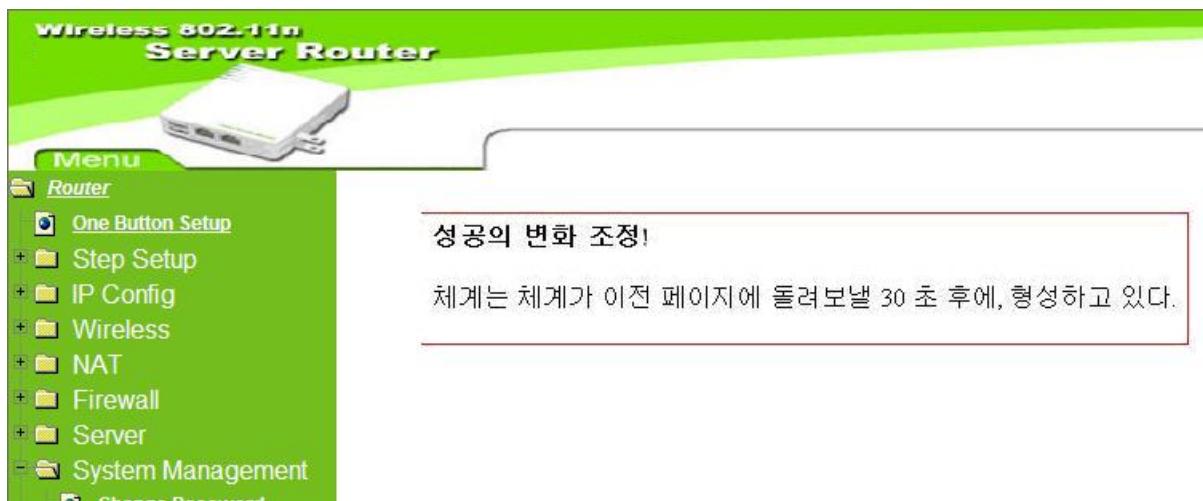
## Language Setting

This page allows you setup the gui language.

Select language:

English	<input type="button" value="▼"/>
English	
Traditional Chinese	
Simplified Chinese	
Japanese	
Russian	
German	
French	
Arabic	
Spanish	
Portuguese	
Italian	
Korean	

Using Korean as an example, the screen will display on the chosen language after the countdown is finished.



Caution: After countdown, you can press **Ctrl+F5** forcing the page to refresh. This can avoid any translation uncompleted situation.

### 5.5.7 User Account Management

Personal users can use each individual application such as My Status, My Webcam and My Document. This section is to set the user's right. Also, all the users right will be showed in User Account List and can do the edit or delete by clicking the meaning text.

## 1. User Name

Create the user name in this blank.

## 2. Password

Setup the user's password.

## 3. User Right

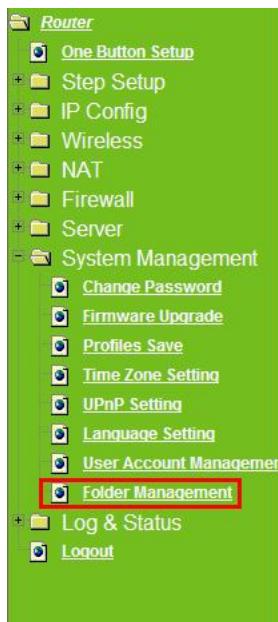
Enable the use to Webcam, FTP server.

## 4. Apply & Cancel

Click on **Apply** button to add the settings into the list table. Click on **Cancel** button to clean the setting on this page.

## 5.5.8 Folder Management

Easy to check all the USB storage devices connected to your Server Router, view the entire data folder inside each storage devices, and you can do the disk formatting/partition via click on the button in this page.



## Folder Management

You can specify which USB storage to be System Disk.

USB Device Name

SysDisk	Disk	TYPE	Capacity	Free Space	Function
<input checked="" type="radio"/>	USB A	Unknown	63MB	39MB	<input type="button" value="Unplug"/>

## Partition / Format SysDisk

All existing data and partitions on the HDD will be DESTROYED ! Make sure you really need to do this !

TYPE:

FAT16/32  NTFS  EXT3

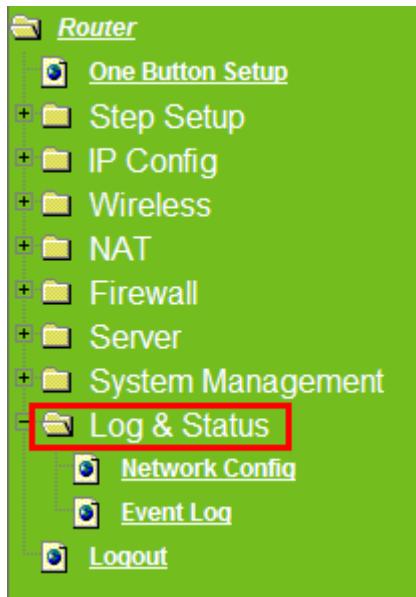
1. Select the USB Disk and click on **Mount** button for refresh all disks before you do disk partition, and the **Unplug** button will appear.
2. To partition/format the disk, please select the disk and click on **Format** button.
3. If you want to view the data inside the disk, please click on "**Disk Explorer**" to view all the disks folders inside the device.

**Note : You have to click on "Unplug" button before remove the USB devices.**

---

## 5.6 Log & Status

The category provides **Network Config** and **Event Log** status for users to know the operation status.



---

### 5.6.1 Network Config

Users can check the Internet status under this category, including Firmware version, Wireless setting, Connecting Time, WAN, TCP/IP ...information.

Router  
One Button Setup  
Step Setup  
IP Config  
Wireless  
NAT  
Firewall  
Server  
System Management  
Log & Status  
Network Config  
Event Log  
Logout

## Network Config

This page shows the current status and some basic settings of the device.

System	
Uptime	0day:0h:33m:7s
Firmware Version	2007/04/25 Ver1.0.7 B05
Wireless Configuration	
Mode	AP
Band	2.4 GHz (B+G)
SSID	Broadband_Router
Channel Number	11
Encryption	Disabled
MAC Address	00:e0:4c:81:86:21
Associated Clients	0
LAN Configuration	
Attain IP Protocol	Fixed IP
IP Address	192.168.1.1
Subnet Mask	255.255.255.0
Default Gateway	192.168.1.1
DHCP Server	Enabled
MAC Address	00:e0:4c:81:86:21

### 5.6.2 Event Log

You may enable the event log feature here.

Router  
One Button Setup  
Step Setup  
IP Config  
Wireless  
NAT  
Firewall  
Server  
System Management  
Log & Status  
Network Config  
Event Log  
Logout

## Event Log

This page can be used to set remote log server and show the system log.

<input type="checkbox"/> Enable Log	<input type="checkbox"/> system all	<input type="checkbox"/> Wireless	<input type="checkbox"/> DoS
<input type="checkbox"/> Enable Remote Log	Log Server IP Address: <input type="text"/>		

→ Please select to enable log function.

#### 1. Enable Log

You may choose to enable Event Log or not.

## 2. system all、wireless & DoS

Please select the event you want to record.

## 3. Enable Remote Log

You may choose to enable the remote event log or not.

## 4. Log Server IP Address

Please input the log server IP Address.

## 5. Apply Changes & Refresh & Clear

Click on **Apply Changes** to save the setting data. Click on **Refresh** to renew the system time, or on **Clear** to clear all the record.

\*The following figure is an example when users click **Apply Changes** to record the event log.

**Enable Log**

**system all**       **wireless**       **DoS**

**Enable Remote Log**      **Log Server IP Address:**

**Apply Changes**

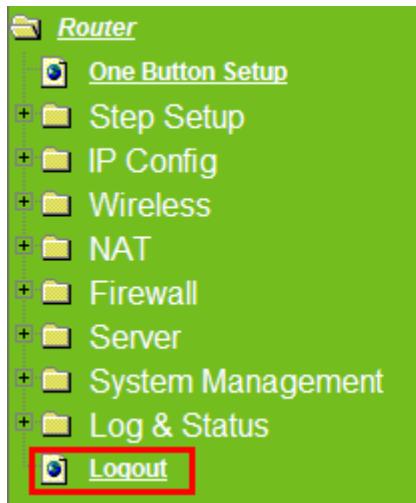
```
conntrack
Oday 00:00:17 PPTP netfilter connection tracking: registered
Oday 00:00:17 PPTP netfilter NAT helper: registered
Oday 00:00:17 ip_tables: (C) 2000-2002 Netfilter core team
Oday 00:00:17 NET4: Unix domain sockets 1.0/SMP for Linux NET4.0.
Oday 00:00:17 NET4: Ethernet Bridge 008 for NET4.0
Oday 00:00:17 VFS: Mounted root (squashfs filesystem) readonly.
Oday 00:00:17 Freeing unused kernel memory: 64k freed
Oday 00:00:17 mount /proc file system ok!
Oday 00:00:17 mount /var file system ok!
Oday 00:00:17 device eth0 entered promiscuous mode
Oday 00:00:17 device wlan0 entered promiscuous mode
Oday 00:00:17 TPT: unreasonable target TSSI 0
Oday 00:00:17 br0: port 2(wlan0) entering listening state
Oday 00:00:17 br0: port 1(eth0) entering listening state
Oday 00:00:17 br0: port 2(wlan0) entering learning state
```

**Refresh**   **Clear**

---

## 5.7 Logout

This function provides users to logout.



## Logout

This page is used to logout.

Do you want to logout ?

# Chapter 6 Advanced Configuration for AP Mode

---

## 6.1 IP Config

In this category, you can setup the IP rules under AP Mode.

---

### 6.1.1 LAN Setup

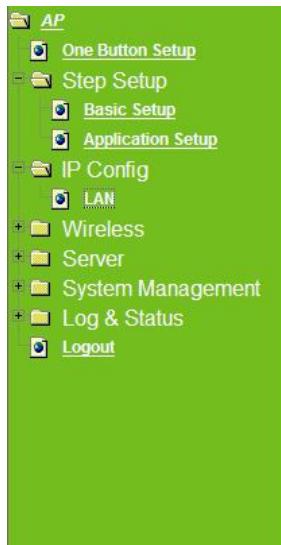


Please click on **LAN** of **IP Config** and follow the below setting.

---

### 6.1.2 LAN Interface Setup

This page is used to configure for local area network which connects to the LAN port of your Access Point. Here users may change the setting for IP address, Subnet Mask, DHCP, etc.



## LAN Interface Setup

This page is used to configure the parameters for local area network which connects to the LAN port of your Access Point. Here you may change the setting for IP address, subnet mask, DHCP, etc..

Device Name:	Server_Router
IP Address:	192.168.1.254
Subnet Mask:	255.255.255.0
Default Gateway:	0.0.0.0
DHCP:	Disable
DHCP Client Range:	192.168.1.100 - 192.168.1.200
802.1d Spanning Tree:	Disabled
Clone MAC Address:	000000000000

### 1. IP Address

The default IP address is **192.168.1.254** (recommend).

### 2. Subnet Mask

Please enter the Subnet Mask address; it should be **255.255.255.0** for the most time.

### 3. Default Gateway

Please enter the Default Gateway address. If you don't know the address, please contact your ISP.

### 4. DHCP

Users can choose to enable DHCP service or not. The DHCP server will give an unused IP address to a computer which is requesting for one. That computer must be a DHCP client, and then it can obtain an IP address automatically.

### 5. DHCP Client Range

The default value is 192.168.1.100 - 192.168.1.200. The DHCP server will assign an IP to a computer from this range. The **Show Client** will display every assigned IP address, MAC address, and expired time.

### 6. 802.1d Spanning Tree

IEEE 802.1d **Spanning Tree Protocol (STP)** is a link layer network protocol that ensures a loop-free topology for any bridged LAN. This function is optional.

### 7. Clone MAC Address

If your ISP asks you to enter a specific MAC Address, please input the correct info at the column.

### 8. Apply Changes & Reset

Click on **Apply Changes** to save the setting data. Or you may click on **Reset** to clear all the input data.

## 6.2 Wireless Setup

The category includes **Basic Settings**, **Advanced Settings**, **Security**, **Access Control**, **WDS settings**, and **WPS**. Please read below for the setting instruction.



### 6.2.1 Wireless Basic Settings

The basic settings related to the wireless are specified as following.

## Wireless Basic Settings

This page is used to configure the parameters for wireless LAN clients which may connect to your Access Point. Here you may change wireless encryption settings as well as wireless network parameters.

### Disable Wireless LAN Interface

Band:

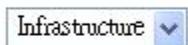


Mode:



Multiple AP

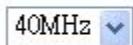
Network Type:



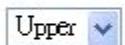
SSID:

Server\_Router

Channel Width:



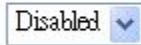
Control Sideband:



Channel Number:



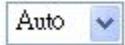
Broadcast SSID:



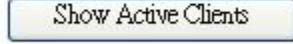
WMM:



Data Rate:



Associated Clients:



### Enable Mac Clone (Single Ethernet Client)

### Enable Universal Repeater Mode (Acting as AP and client simultaneously)

SSID of Extended Interface:



### 1. Disable Wireless LAN Interface

Turn off the wireless function.

### 2. Band

Please select the frequency. It has 6 options:

2.4 GHz (B/G/N/B+G/G+N/B+G+N).

### 3. Mode

Please select the mode. It has 3 modes to select:

(AP, WDS, AP+WDS).

**Multiple APs** can provide users another 4 different SSID for connection.

Users can add or limit the properties for each connection.

## Multiple APs

This page shows and updates the wireless setting for multiple APs.

No.	Enable	Band	SSID	Data Rate	Broadcast SSID	WMM	Access	Active Client List
AP1	<input type="checkbox"/>	2.4 GHz (B+G+N)	MultipeAP_1	Auto	Enabled	Enabled	LAN+WAN	Show
AP2	<input type="checkbox"/>	2.4 GHz (B+G+N)	MultipeAP_2	Auto	Enabled	Enabled	LAN+WAN	Show
AP3	<input type="checkbox"/>	2.4 GHz (B+G+N)	MultipeAP_3	Auto	Enabled	Enabled	LAN+WAN	Show
AP4	<input type="checkbox"/>	2.4 GHz (B+G+N)	MultipeAP_4	Auto	Enabled	Enabled	LAN+WAN	Show

**Apply Changes**

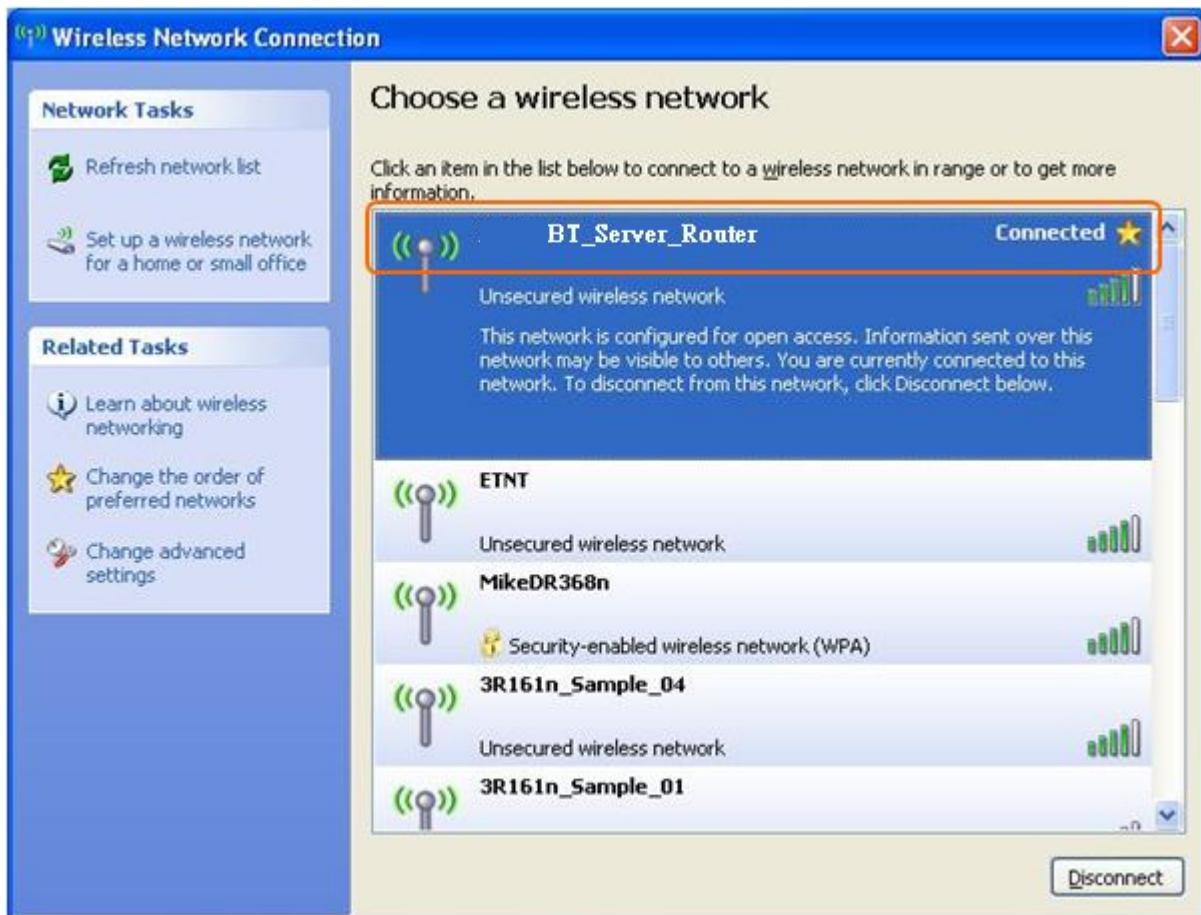
**Reset**

**Close**

- (1.) Enable: please choose to enable it or not.
- (2.) Band: please select the frequency.
- (3.) SSID: please enter the SSID.
- (4.) Data Rate: please select the data transmission rate.
- (5.) Access: enable this function can let clients use 2 access types: a. LAN+WAN: the client can access to the Internet and connect to Server Router's GUI to setup. b. WAN: the client can only access to the Internet.
- (6.) Active Client List: display the properties of the client which is connecting successfully.
- (7.) Apply Changes: Please click **Apply Changes** to initiate or click **Reset** to cancel.

Take the client side of wireless network card as an example:

The Client can search for Server Router\_AP1 (LAN+WAN) and connect to it. If the client connects to it successfully, it will display message to notify users.



#### 4. Network Type

Please select the network type, it has 2 options: **Infrastructure** or **Ad hoc**.  
If the wireless mode is set to AP mode, this section is disabled.

#### 5. SSID

Service Set identifier, the default SSID is **Server\_Router**, users can define to any.

#### 6. Channel Width

Please select the channel width, it has 2 options: 20MHZ, and 40MHZ.

#### 7. Control Sideband

Enable this function will control your router use lower or upper channel.

#### 8. Channel Number

Please select the channel; it has Auto, 1, 2~11 options.

#### 9. Broadcast SSID

User may choose to enable **Broadcast SSID** or not.

#### 10. Data Rate

Please select the data transmission rate.

#### 11. Associated Clients

Check the AP connectors and the Wireless connecting status.

## 12. Enable Mac Clone (Single Ethernet Client)

Clone the MAC address for ISP to identify.

## 13. Enable Universal Repeater Mode (Acting as AP and Client simultaneously)

Allow to equip with the wireless way conjunction upper level, provide the bottom layer user link in wireless and wired way in the meantime. (The IP that bottom layer obtains is from upper level.)

Ex: When users enable the Universal Repeater to connect to the upper level device, please input the channel and SSID of the upper level device on router's GUI. Click on **Apply Changes** to save the settings. (The DHCP in IP config needs to be disabled.)

---

Channel Number:	<input type="button" value="▼"/>
Broadcast SSID:	Disabled <input type="button" value="▼"/>
WMM:	Enabled <input type="button" value="▼"/>
Data Rate:	Auto <input type="button" value="▼"/>
Associated Clients:	<input type="button" value="Show Active Clients"/>
<input type="checkbox"/> <b>Enable Mac Clone (Single Ethernet Client)</b>	
<input type="checkbox"/> <b>Enable Universal Repeater Mode (Acting as AP and client simultaneously)</b>	
SSID of Extended Interface:	ESSID_Server_Router_0d21ff
<input type="button" value="Apply Changes"/>	<input type="button" value="Reset"/>

---

Users can go to the network Config section and check the information of upper level in Wireless Repeater Interface Configuration.

The screenshot shows the AP configuration interface. On the left, a sidebar lists various configuration options: One Button Setup, Step Setup, IP Config, Wireless, NAT, Firewall, Server, System Management, Log & Status, Network Config (which is highlighted with a red box), Event Log, and Logout. The main content area is divided into several sections:

- DNS** (with fields for DNS 1, DNS 2, and DNS 3, and buttons for Connect and Disconnect).
- Wireless Repeater Interface Configuration** (with fields for Mode (Infrastructure Client), SSID (Server\_Router\_0d21ff), Encryption (Disabled), BSSID (00:0e:68:ff:05:d8), and Status (Connected)).
- USB A Configuration** (with fields for USB Type (Storage), Name (PQI), and Model (3100)).
- USB B Configuration** (with fields for USB Type (Print), Name (EPSON), and Model (2100)).

If the bottom layer device is trying to make a connection, users must input the SSID of this router as a relay station. The IP that the bottom layer device gets is from the upper level device.

#### 14. SSID of Extended Interface

While linking the upper level device in wireless way, you can set SSID to give the bottom layer user search.

#### 15. Apply Changes & Reset

Click on **Apply Changes** to save the setting data. Or you may click on **Reset** to clear all the input data.

---

#### 6.2.2 Wireless Advanced Settings

Please complete the wireless advanced settings as following instructions.

# Wireless Advanced Settings

These settings are only for more technically advanced users who have a sufficient knowledge about wireless LAN. These settings should not be changed unless you know what effect the changes will have on your Access Point.

<b>Fragment Threshold:</b>	<input type="text" value="2346"/> (256-2346)
<b>RTS Threshold:</b>	<input type="text" value="2347"/> (0-2347)
<b>Beacon Interval:</b>	<input type="text" value="100"/> (20-1024 ms)
<b>Preamble Type:</b>	<input checked="" type="radio"/> Long Preamble <input type="radio"/> Short Preamble
<b>IAPP:</b>	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
<b>Protection:</b>	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
<b>Aggregation:</b>	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
<b>Short GI:</b>	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
<b>RF Output Power:</b>	<input checked="" type="radio"/> 100% <input type="radio"/> 70% <input type="radio"/> 50% <input type="radio"/> 35% <input type="radio"/> 15%

[Apply Changes](#)

[Reset](#)

## 1. Fragment Threshold

To identify the maxima length of packet, the over length packet will be fragmentized. The allowed range is 256-2346, and default length is 2346 Bytes.

## 2. RTS Threshold

This value should remain at its default setting of 2347. The range is 0~2347. 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. Fill the range from 0 to 2347 into this blank.

## 3. Beacon Interval

Beacons are packets sent by an access point to synchronize a wireless network. Specify a beacon interval value. The allowed setting range is 20-1024 ms.

## 4. Preamble Type

Preamble is the first subfield of PPDU, which is the appropriate frame format

form transmission to PHY (Physical layer). There are two options, Short Preamble and Long Preamble. The Short Preamble option improves throughput performance. Select the suit Preamble as Short or Long Preamble.

## **5. IAPP**

Inter Access Point Protocol. Allow seamless roaming between Access Points in your wireless network.

## **6. Protection**

Please select to enable wireless protection or not.

## **7. Aggregation**

Enable this function will combine several packets to one and transmit it. It can reduce the problem when mass packets are transmitting.

## **8. Short GI**

Users can get better wireless transmission efficiency when they enable this function.

## **9. RF Output Power**

Users can adjust the RF output power to get the best wireless connection.

Users can choose from 100%, 70%, 50%, 35%, and 15%.

## **10. Apply Changes & Reset**

Click on **Apply Changes** to save the setting data. Or you may click on **Reset** to clear all the input data.

---

### 6.2.3 Wireless Security Setup

4 encryption types could be selected here, please follow below instruction for the setting.

## Wireless Security Setup

This page allows you setup the wireless security. Turn on WEP or WPA by using Encryption Keys could prevent any unauthorized access to your wireless network.

Select SSID:

Encryption:

#### 1. Encryption – WEP

##### 1.1 Set WEP Key

This section provides 64bit and 128bit WEP encryptions for wireless network. Users can also choose ASCII and Hex shared Key format to protect data.

## Wireless Security Setup

This page allows you setup the wireless security. Turn on WEP or WPA by using Encryption Keys could prevent any unauthorized access to your wireless network.

Select SSID:

Encryption:

802.1x Authentication:

Authentication:  Open System  Shared Key  Auto

Key Length:

Key Format:

Encryption Key:

## 1.2 802.1x Authentication

It is a safety system by using authentication to protect your wireless network. Please choose between WEP 64bits and WEP 128bits.

### 4. Encryption – WPA (WPA, WPA2, and WPA2 Mixed)

#### WPA Authentication Mode

##### 2.1 Enterprise (RADIUS)

Please input the Port, IP Address, and Password of Authentication RADIUS Server.

## Wireless Security Setup

This page allows you setup the wireless security. Turn on WEP or WPA by using Encryption Keys could prevent any unauthorized access to your wireless network.

Select SSID:

Server\_Router

Encryption:

WPA

Authentication Mode:  Enterprise (RADIUS)  Personal (Pre-Shared Key)

WPA Cipher Suite:  TKIP  AES

RADIUS Server IP Address: 0.0.0.0

RADIUS Server Port: 1812

RADIUS Server Password:

##### 2.2 Personal (Pre-Shared Key)

Pre-Shared Key type is ASCII Code; the length is between 8 to 63 characters.

If the key type is Hex, the key length is 64 characters.

## Wireless Security Setup

This page allows you setup the wireless security. Turn on WEP or WPA by using Encryption Keys could prevent any unauthorized access to your wireless network.

Select SSID:

Encryption:

**Authentication Mode:**  Enterprise (RADIUS)  Personal (Pre-Shared Key)

**WPA Cipher Suite:**  TKIP  AES

**Pre-Shared Key Format:**

**Pre-Shared Key:**

### 2. Apply Changes & Reset

Click on **Apply Changes** to save the setting data. Or you may click on **Reset** to clear all the input data.

#### 6.2.4 Wireless Access Control

The function of access control is to allow or deny users to access Server Router by according MAC address, it is optional. If you select **Allowed Listed**, then only those clients whose MAC address is listed on access control can connect to your base station. If you select **Deny Listed**, those clients whose MAC address is listed on access control can't connect to your base station.

#### Wireless Access Control

If you choose 'Allowed Listed', only those clients whose wireless MAC addresses are in the access control list will be able to connect to your Access Point. When 'Deny Listed' is selected, these wireless clients on the list will not be able to connect the Access Point.

Wireless Access Control Mode:	<input style="border: 1px solid #ccc; padding: 2px 10px;" type="button" value="Disable"/> <span style="color: red;">→ Users may enable or disable this function.</span>
MAC Address:	<input style="width: 150px; border: 1px solid #ccc; padding: 2px;" type="text"/> Comment: <input style="width: 150px; border: 1px solid #ccc; padding: 2px;" type="text"/>
<input style="border: 1px solid #ccc; padding: 2px 10px;" type="button" value="Apply Changes"/> <input style="border: 1px solid #ccc; padding: 2px 10px;" type="button" value="Reset"/>	

Current Access Control List:

MAC Address	Comment	Select

Take the wireless card as the example.

(1.) We will use **Deny Listed** as an example. Please select **Deny Listed** in **Wireless Access Control Mode** first, and then input the MAC address of wireless card in MAC Address field. Click **Apply Changes** to save the setting data.

## Wireless Access Control

If you choose 'Allowed Listed', only those clients whose wireless MAC addresses are in the access control list will be able to connect to your Access Point. When 'Deny Listed' is selected, these wireless clients on the list will not be able to connect the Access Point.

Wireless Access Control Mode:	Deny Listed	
MAC Address:	00D041B0D117	Comment:
<input type="button" value="Apply Changes"/> <input type="button" value="Reset"/>		

Current Access Control List:

MAC Address	Comment	Select

(2.) You will find out that the MAC address appears on **Current Access Control List**, it means the initiation is completed.

## Wireless Access Control

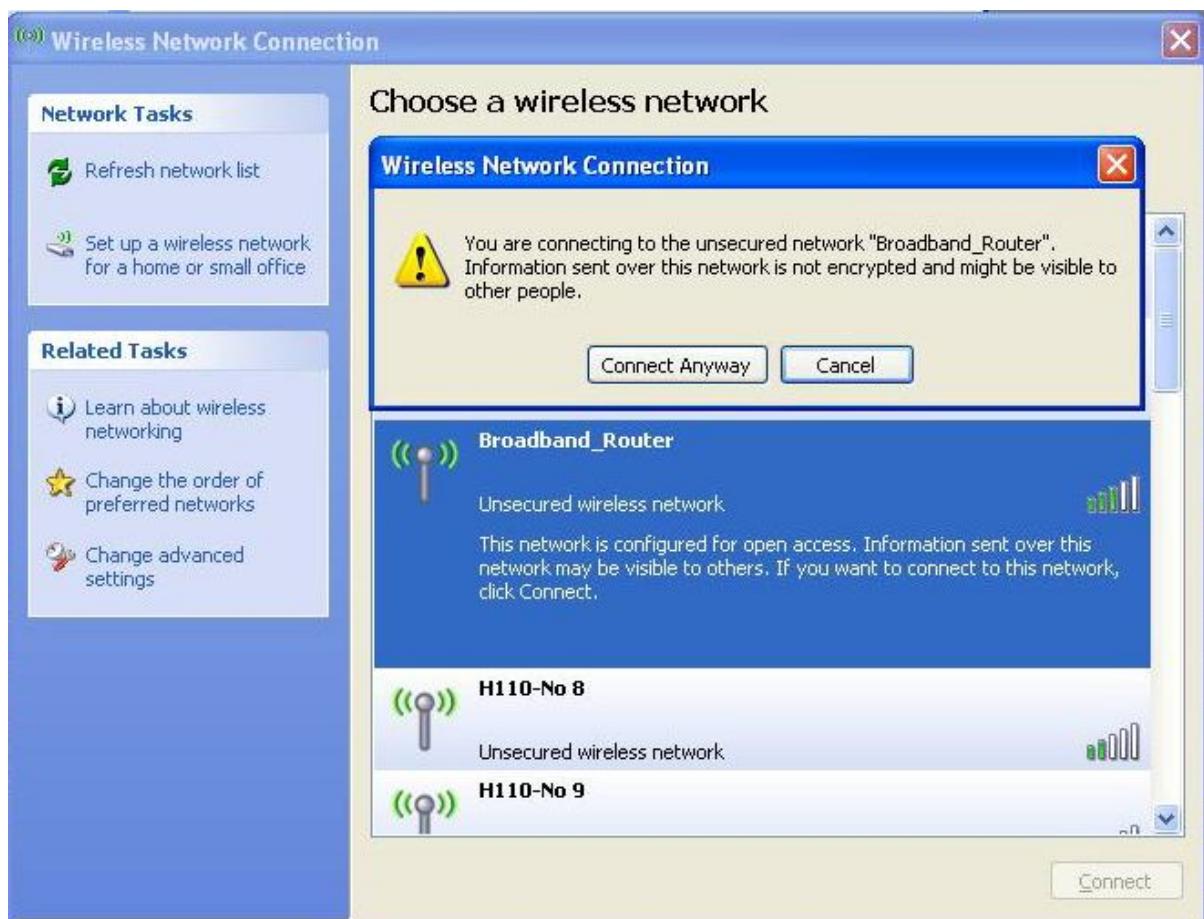
If you choose 'Allowed Listed', only those clients whose wireless MAC addresses are in the access control list will be able to connect to your Access Point. When 'Deny Listed' is selected, these wireless clients on the list will not be able to connect the Access Point.

Wireless Access Control Mode:	Deny Listed
MAC Address:	Comment:
<input type="button" value="Apply Changes"/> <input type="button" value="Reset"/>	

Current Access Control List:

MAC Address	Comment	Select
00:d0:41:b0:d1:17		<input type="checkbox"/>

(3.) Please open wireless card UI and try to connect to this router. You will find out that the connection request will be denied.



### 6.2.5 WDS Settings

Wireless basic settings must enable WDS first. This function can communicate with other APs by adding MAC address into the same channel.

## WDS Settings

Wireless Distribution System uses wireless media to communicate with other APs, like the Ethernet does. To do this, you must set these APs in the same channel and set MAC address of other APs which you want to communicate with in the table and then enable the WDS.

### Enable WDS

**MAC Address:**

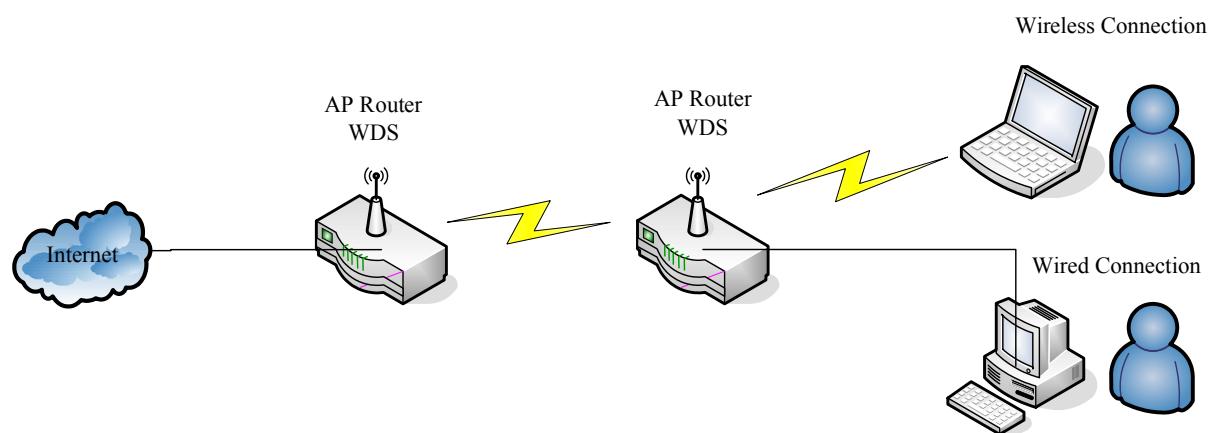
**Data Rate:**

**Comment:**

### Current WDS AP List:

MAC Address	Tx Rate (Mbps)	Comment	Select
-------------	----------------	---------	--------

\* The following figure is the explanation.



\* Please follow the instructions to setup the connection.

- (1.) Please check the MAC address and Channel number of the upper level device.

Wireless Configuration	
Mode	AP
Band	2.4 GHz (B+G)
SSID	Server_Router
Channel Number	9
Encryption	Disabled
MAC Address	00:e0:4c:81:86:21
Associated Clients	0
LAN Configuration	
Attain IP Protocol	Fixed IP
IP Address	192.168.1.1
Subnet Mask	255.255.255.0
Default Gateway	192.168.1.1
DHCP Server	Enabled
MAC Address	00:e0:4c:81:86:21

(2.) Enter the **Wireless Basic Settings** page, select **AP+WDS** mode, and then select the **Channel Number**. Click **Apply Changes** to save the setting data.

(3.) Enter the **WDS Settings** page, select **Enable WDS**, and then input the MAC address of the upper level device. Click **Apply Changes** to save the setting data.

## WDS Settings

Wireless Distribution System uses wireless media to communicate with other APs, like the Ethernet does. To do this, you must set these APs in the same channel and set MAC address of other APs which you want to communicate with in the table and then enable the WDS.

**Enable WDS**

**MAC Address:** 00:0e:68:ff:05:c8

**Data Rate:** Auto

**Comment:**

**Apply Changes** **Reset** **Set Security** **Show Statistics**

### Current WDS AP List:

MAC Address	Tx Rate (Mbps)	Comment	Select
00:0e:68:ff:05:c8	Auto		<input type="checkbox"/>

**Delete Selected** **Delete All** **Reset**

(4.) When the time counts down to 0, you will see the MAC address of the upper level device displaying on **Current WDS AP List**.

## WDS Settings

Wireless Distribution System uses wireless media to communicate with other APs, like the Ethernet does. To do this, you must set these APs in the same channel and set MAC address of other APs which you want to communicate with in the table and then enable the WDS.

**Enable WDS**

**MAC Address:**

**Data Rate:** Auto

**Comment:**

**Apply Changes** **Reset** **Set Security** **Show Statistics**

### Current WDS AP List:

MAC Address	Tx Rate (Mbps)	Comment	Select
00:0e:68:ff:05:c8	Auto		<input type="checkbox"/>

**Delete Selected** **Delete All** **Reset**

(5.) Head back to **LAN Interface**, disable **DHCP** option, and then click **Apply Changes** to save the setting data.

(6.) The MAC address of the upper level device is going to setup like the MAC address of the router. Enter the upper level device's **WDS settings** page, and input router's MAC address. Click **Apply Changes** to save the setting data.

## WDS Settings

Wireless Distribution System uses wireless media to communicate with other APs, like the Ethernet does. To do this, you must set these APs in the same channel and set MAC address of other APs which you want to communicate with in the table and then enable the WDS.

**Enable WDS**

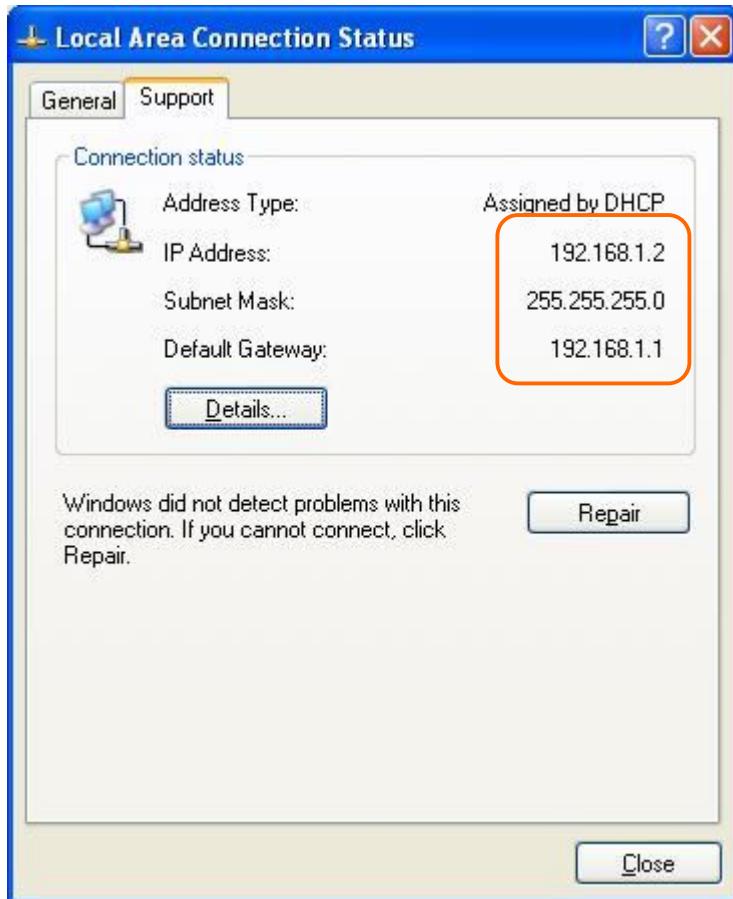
<b>MAC Address:</b>	000e68ff05d0	<b>Please input the MAC address.</b>
<b>Data Rate:</b>	Auto	
<b>Comment:</b>		
<input type="button" value="Apply Changes"/> <input type="button" value="Reset"/> <input type="button" value="Set Security"/> <input type="button" value="Show Statistics"/>		

### Current WDS AP List:

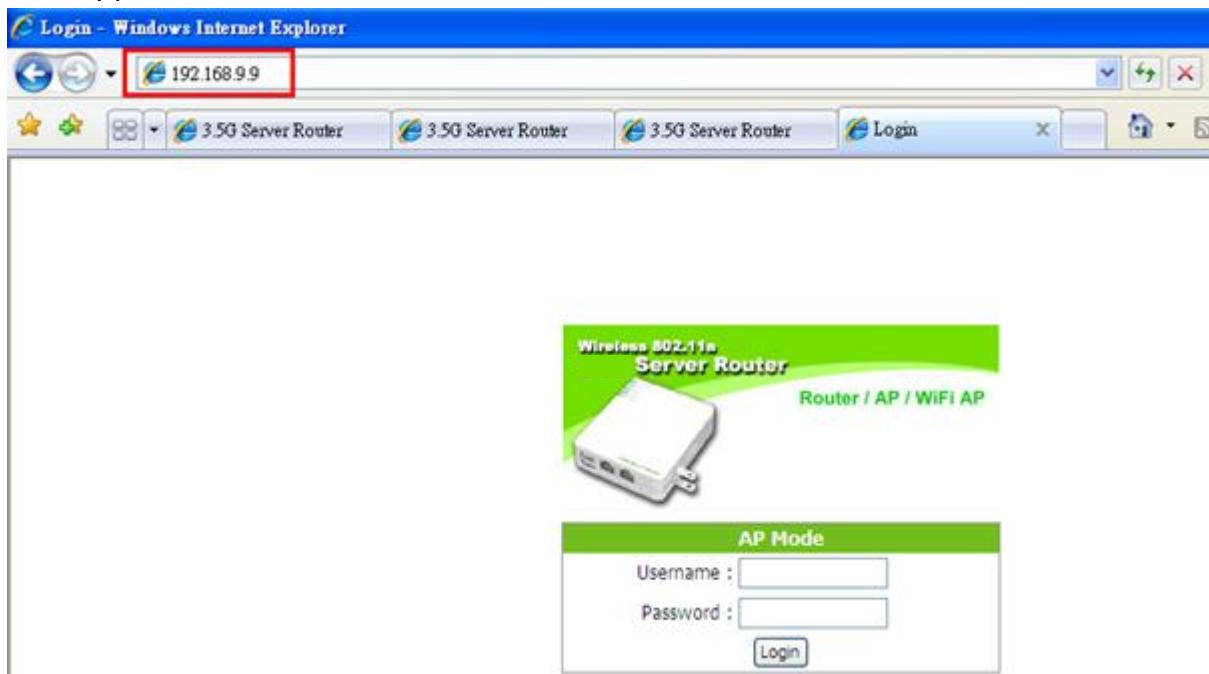
MAC Address	Tx Rate (Mbps)	Comment	Select
			<input type="button" value="Delete Selected"/>
			<input type="button" value="Delete All"/> <input type="button" value="Reset"/>

(7.) After initiating the upper level device, please check Local Area Connections.

Click Supports to check out the IP address which is assigned by upper level device.



(8.) You can input <http://192.168.9.9> in IE browser to enter the GUI page of the upper level device and make sure the connection.



### 6.2.6 WPS

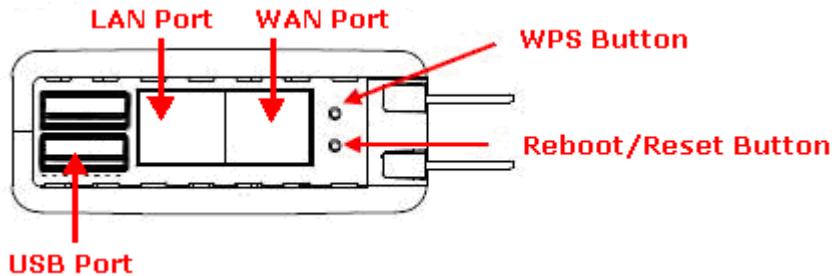
Wi-Fi Protected Setup, it can simplify the procedures of wireless encryption between Server Router and wireless network card. If the wireless network card also supports WPS function, users can activate WPS auto-encryption to speed up the procedures.

WPS supports 2 models: PIN (Personal Information Number) and PBC (Push Button Configuration). These models are approved by the Wi-Fi Alliance.

**PIN model**, in which a PIN has to be taken either from a sticker label or from the web interface of the WPS device. This PIN will then be entered in the AP or client WPS device to connect.

**PBC model**, in which the user simply has to push a button, either an actual or a virtual one, on both WPS devices to connect.

\*The following figure is the display of the front of Server Router.



When users select a specific model on wireless base station, the clients can connect to the base by selecting the same model.

The connection procedures of PIN and PBC are almost the same. The small difference between those two is:

Users input the PIN of wireless card in the base station first; it will limit the range of the clients. It is faster to establish a connection on PIN model.

On PBC model, users push the WPS button to activate the function, and then the wireless client must push the WPS button in 2 mins to enter the network. The client will search to see if there is any wireless base station which supports WPS is activating. If the client finds a matching base, the connection will be established. The speed of establishing a connection is slower than the PIN model because of this extra step.

On the other hand, users need to input the information of the wireless card into the register interface. It might lead to the failure of connection, if users make mistakes on inputting. On PBC model, users only need to click the WPS button on both sides to make a connection. It is easier to operate.

This page supports **Start PBC** and **Start PIN**; please follow the instructions to operate.

\* Start PBC:

(1.) Please click **Start PBC** to connect to the wireless network card.

## Wi-Fi Protected Setup

This page allows you to change the setting for WPS (Wi-Fi Protected Setup). Using this feature could let your wireless client automatically synchronize its setting and connect to the Access Point in a minute without any hassle.

**Disable WPS**

**WPS Status:**

Configured  UnConfigured

**Self-PIN Number:**

18864540

**Push Button Configuration:**

**Start PBC**

**Apply Changes**

**Reset**

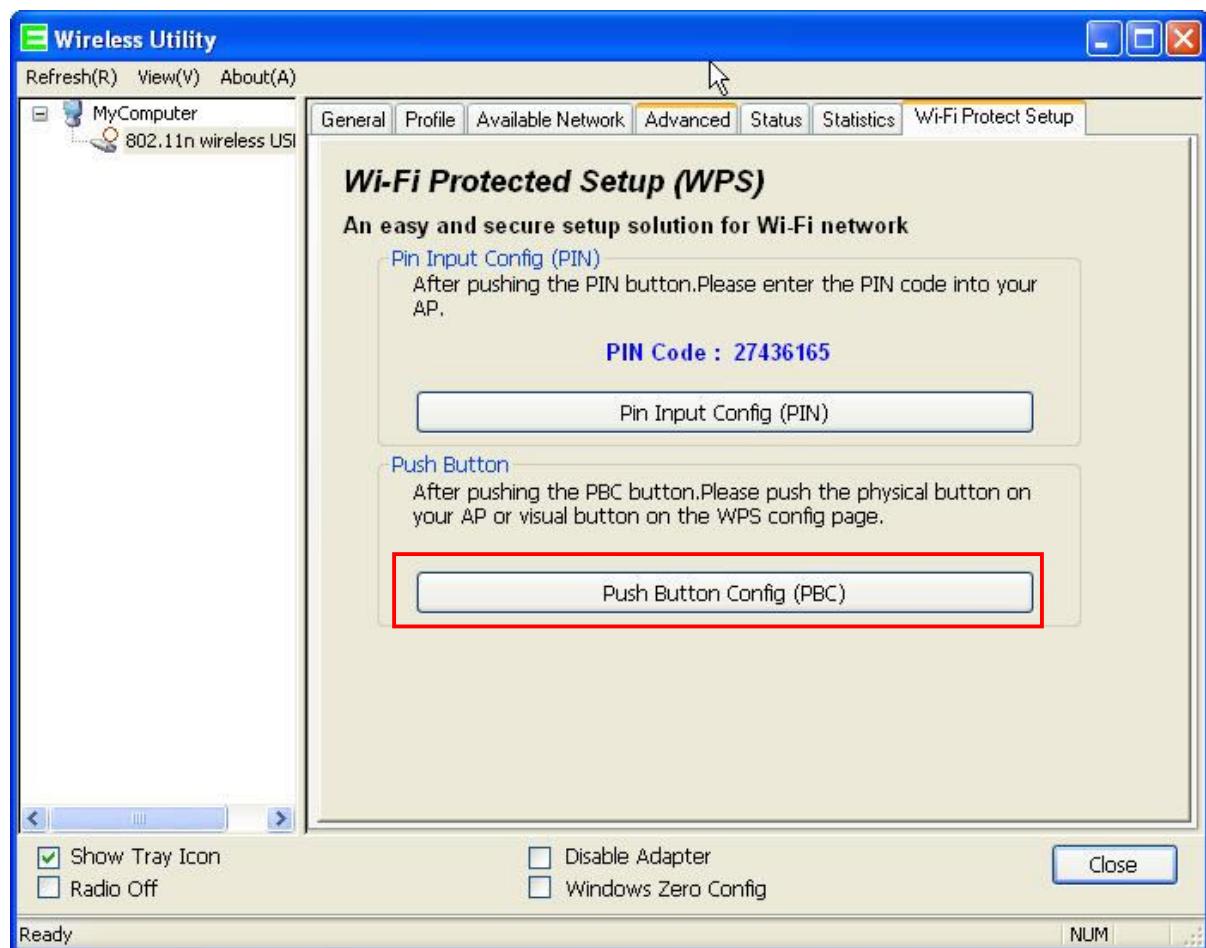
**Current Key Info:**

Authentication	Encryption	Key
Open	None	N/A

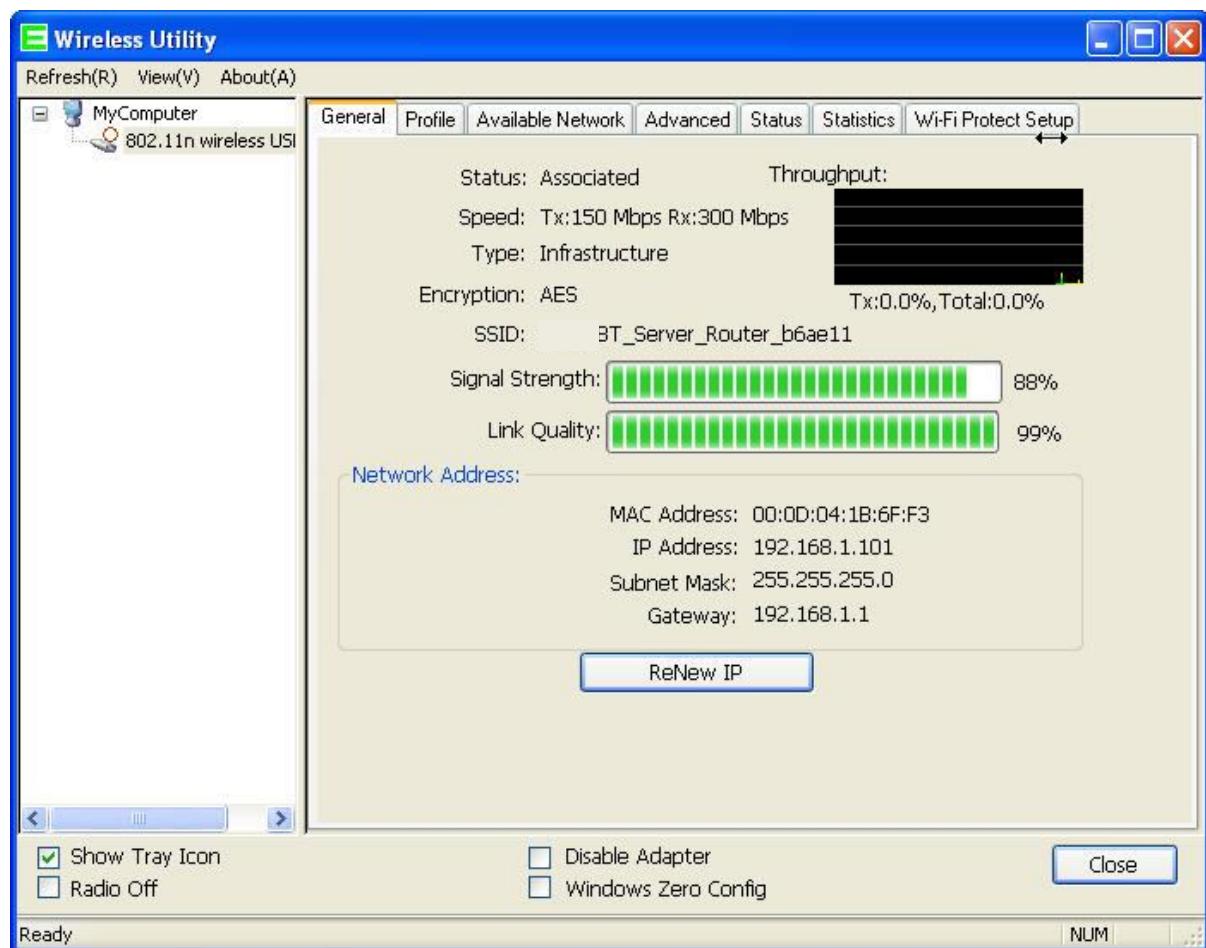
**Client PIN Number:**

**Start PIN**

(2.) Open the configuration page of the wireless card which supports WPS. Click the **WiFi Protect Setup**, and then click **PBC** to make a WPS connection with AP from the WPS AP list (PBC-Scanning AP).

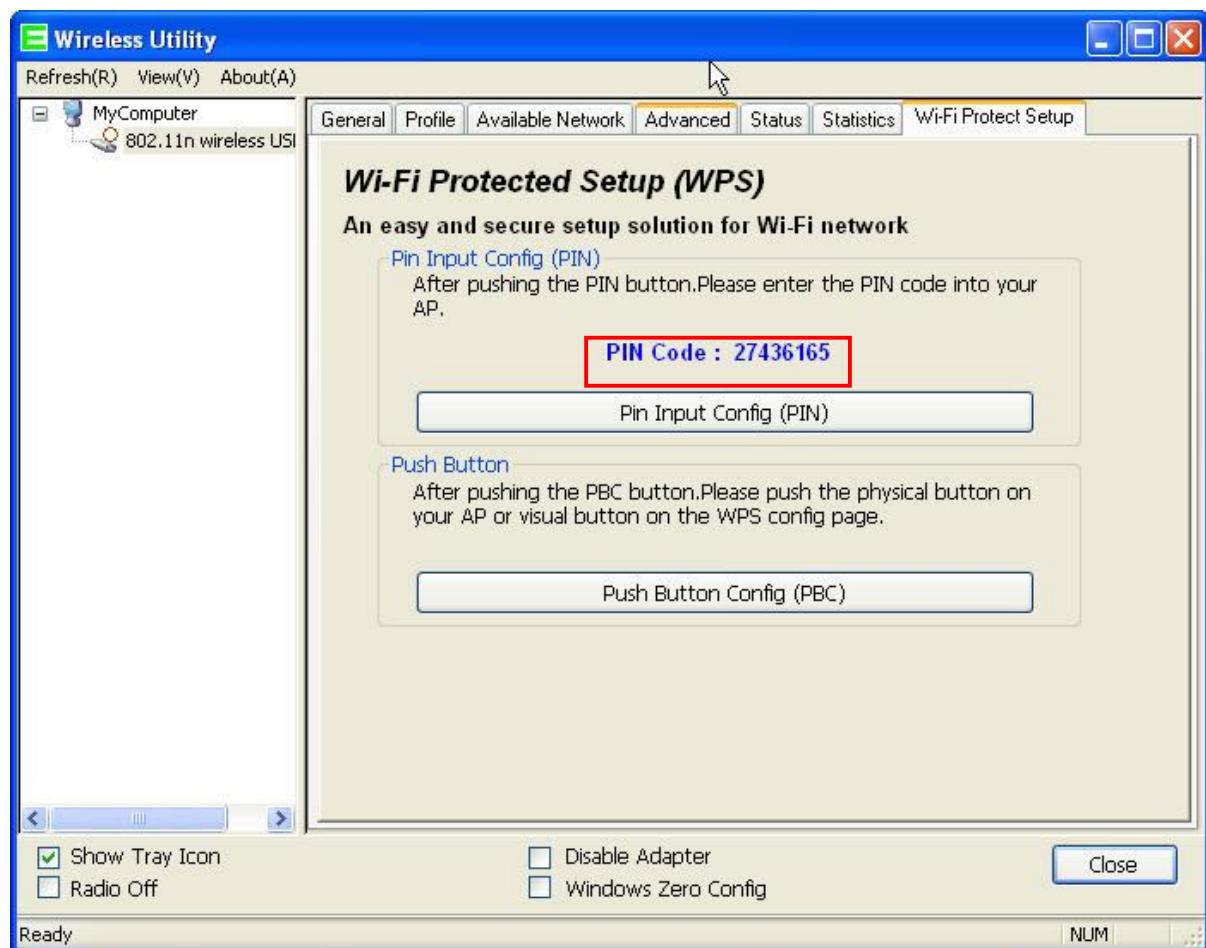


(3.) When you see **Network Address**, it means the WPS connection between wireless card and Server Router is established.



\* Start PIN:

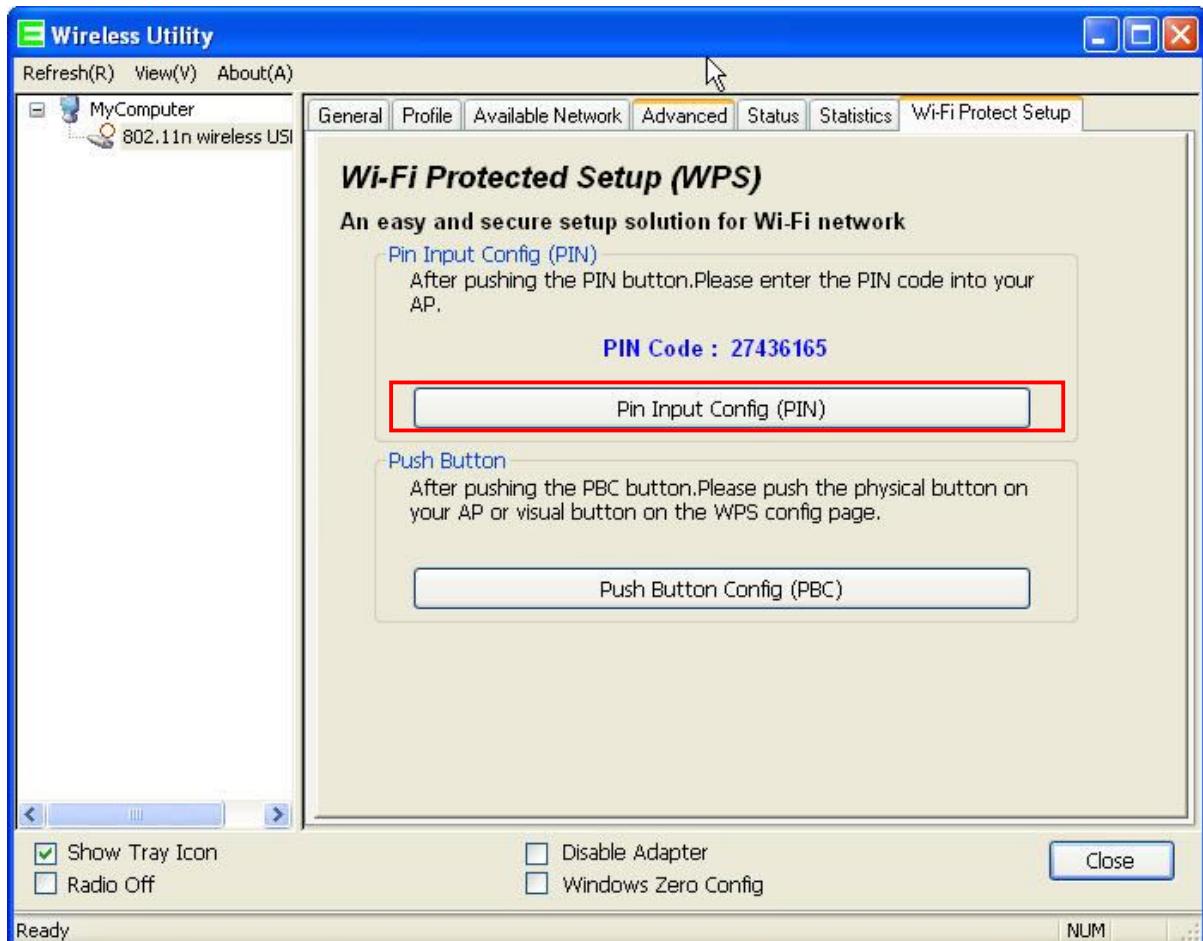
(1.) Please open the configuration page of the wireless card, and write it down.



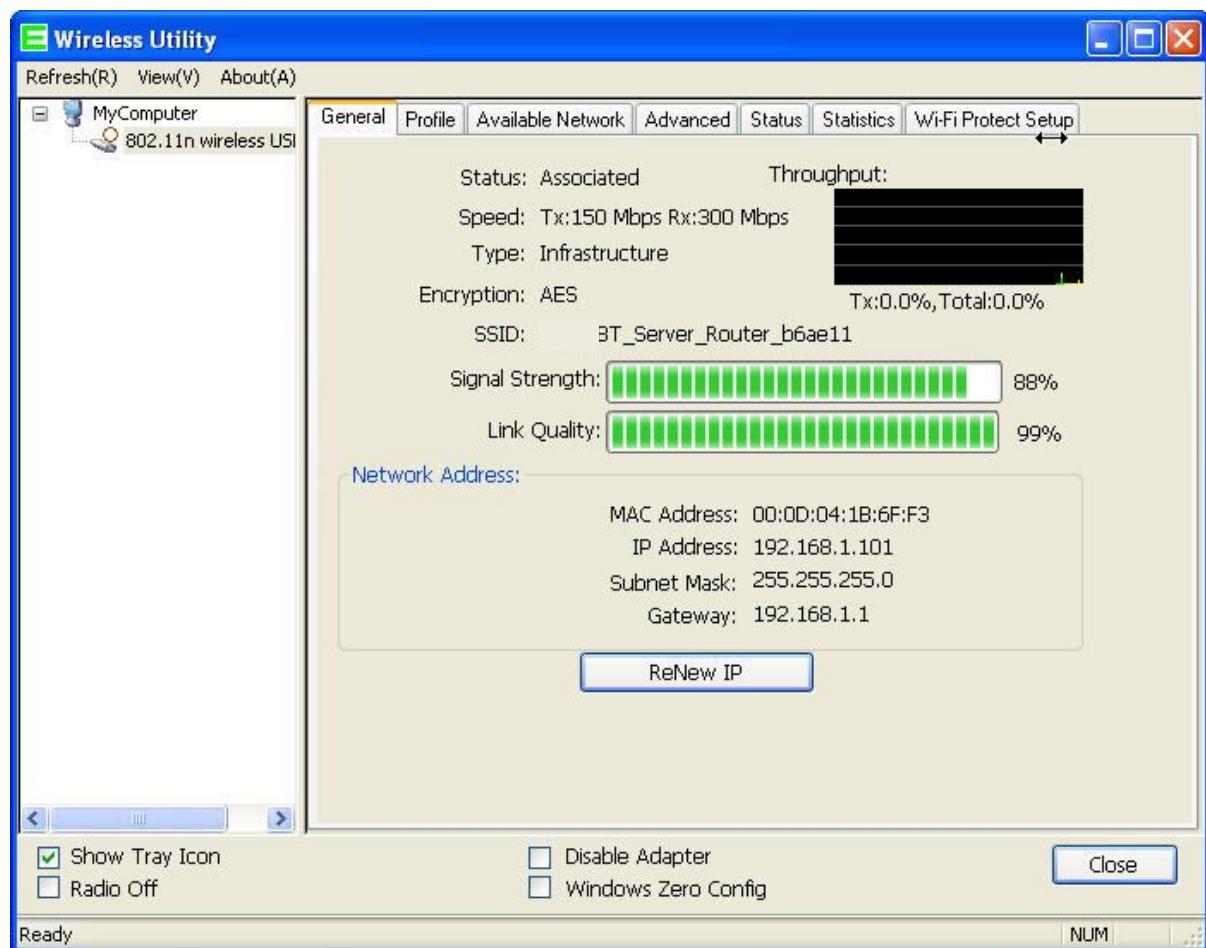
(2.) Open the Wi-Fi Protected Setup configuration page of Server Router, input the PIN number from the wireless card then click **Start PIN**.

A screenshot of a web-based 'Wi-Fi Protected Setup' configuration page. The title is 'Wi-Fi Protected Setup'. A descriptive text says: 'This page allows you to change the setting for WPS (Wi-Fi Protected Setup). Using this feature could let your wireless client automatically synchronize its setting and connect to the Access Point in a minute without any hassle.' There are several configuration options: a checkbox for 'Disable WPS', radio buttons for 'WPS Status' (Configured is selected), a text field for 'Self-PIN Number' (73220398), and a button for 'Push Button Configuration' (Start PBC). At the bottom, there are 'Apply Change' and 'Reset' buttons. A section titled 'Current Key Info:' shows a table with three columns: Authentication, Encryption, and Key. The table has one row: WPA2 PSK, AES, and 65756575. At the very bottom, there is a 'Client PIN Number:' field containing '27436165' and a 'Start PIN' button, both of which are highlighted with a red box.

(3.) Open the configuration page of the wireless card which supports WPS. Click the **WPS**, and then click **PIN** to make a WPS connection with AP from the WPS AP list (PIN-Begin associating to WPS AP).



(4.) When you see **Network Address**, it means the WPS connection between wireless card and Server Router is established.

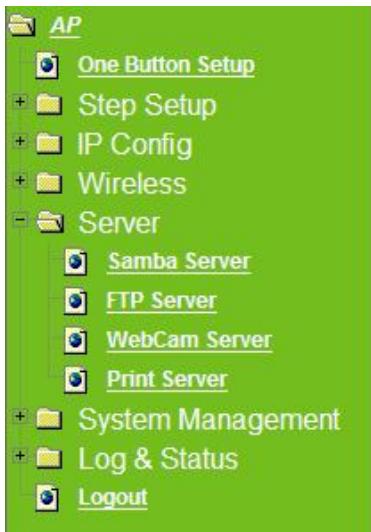


## 6.3 Server

Server Router provides Samba Server, FTP Server, Web Camera Server, and Printer Server Application.

### 6.3.1 Samba Server

Support NetBIOS Protocol, the consumer sharing file or printer which provides as the "**My Network Places**". Please make sure storage devices and printers are connecting to USB ports on the router and already mounting.



## Samba Server

You can enable or disable samba server function in this page.

Enable Samba Server:  Enabled  Disabled

Workgroup Name:

Server Name:  Server\_Router\_0d21ff

Server Description:

### 1. Enable Samba Server

Enable or disable this function.

### 2. Workgroup Name

Input the workgroup name, default is "WORKGROUP".

### 3. Server Name

Input the server name, default is "Server Router".

### 4. Server Description

You can input description of the server.

### 5. Apply & Cancel

Click on **Apply** button to finish setting. Click on **Cancel** button to clean the setting on this page.

#### 6.3.1.1 How to Enter The Sharing Folder

Please follow below steps.

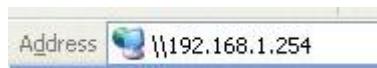
Step 1:

Please click the "start", and select "My Computer".



Step 2:

In the Address blank input the IP address: <\\192.168.1.254>.



Step 3:

Appear following menu, can open following to share internal data.



**Note :**

3. If connected USB flash or HDD, and then enable samba server function, it will appear a samba folder.
4. If connected USB printer, and then enable printer server function, it will appear a printer icon.

### 6.3.2 FTP Server

FTP Server utility allows both local and remote users to upload or download files, pictures or MP3 music form the same storage device. Before configure FTP Server, please make sure the storage device is properly plug into any USB port on the router and make sure this USB storage device is detected by the router.

#### 1. Enable FTP Server

Select to “**Enable**” or “**Disable**” FTP server.

#### 2. Enable Anonymous to Login

Allow anonymous to login after check on Enable.

#### 3. FTP Server Port

The default is 21. Define the FTP command transfer service port. If you want to change this port number, remember to change the service port setting of your FTP client, also.

#### 4. Idle Connection Time-Out

When a specific time value is added, FTP Server will be de-activated if it has no activity within the time limit. The default is 300 seconds; the minimum is 60 seconds.

#### 5. Apply & Cancel

Click on **Apply** button to continue. Click on **Cancel** button to clean the setting on this page.

#### 6. User Account List

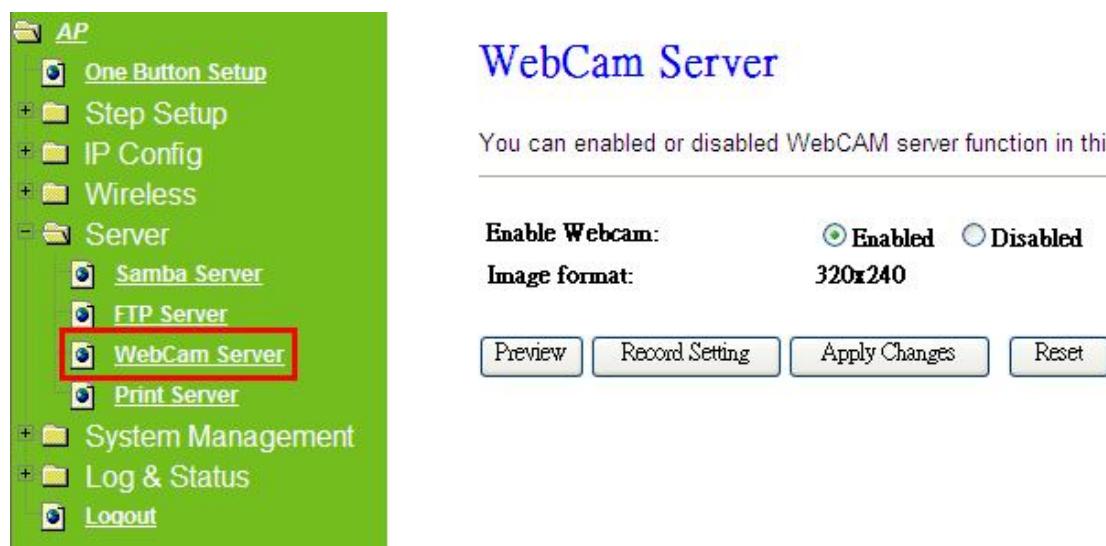
User Name, Status, and Opened Directory/File can be shown on the list.

**Note :** FTP server is compatible with FAT32 or EXT3 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 EXT3 standard.

### 6.3.3 Webcam Server

By connecting web camera to the router, it allows user to monitor their home or office from remote locations.

#### 6.3.3.1 Webcam Server Basic Setting



##### 1. Enable webcam server

Select to “**Enable**” or “**Disable**” webcam server.

##### 2. Image format

The format is 320X240 pixels.

### 3. Preview

Click on this button, you can preview the image from webcam.

### 4. Record Setting

Please see the detail advance setting in "**6.3.3.2 Webcam Advanced Configuration**".

### 5. Apply & Cancel

Click on **Apply** button to continue. Click on **Cancel** button to clean the setting on this page.

## 6.3.3.2 Webcam Server Advanced Setting

Click on "**Record Setting**" button, and the screen will appear as below.

### Webcam Advanced Configuration

Snapshot Record Settings.

Save image interval:	<input type="text" value="5"/> sec (default: 5)
Save Location:	<input checked="" type="radio"/> <b>USB</b> <input type="radio"/> <b>Remote FTP</b>
Remote FTP URL:	<input type="text"/>
Remote FTP port:	<input type="text"/>
Remote FTP user:	<input type="text"/>
Remote FTP password:	<input type="text"/>
Remote FTP Directory:	<input type="text"/>
 <input type="button" value="Back"/> <input type="button" value="Apply Changes"/> <input type="button" value="Reset"/>	

#### 1. Save image interval

For saving image, you can set the save interval time, the default value is 5 seconds.

#### 2. Save Location

Set the save location for webcam image, you may save into **USB HDD** or **Remote FTP**; if select save to **Remote FTP**, please continue following remote FTP setting.

#### 3. Remote FTP URL

Input the FTP URL for saving webcam image.

#### 4. Remote FTP port

Input the FTP port number under URL to save image.

#### 5. Remote FTP user

Input the users name you like and it will be used to save the webcam image

into the FTP server.

**6. Remote FTP password**

Input the remote password.

**7. Remote FTP Directory**

To provide option of which folder should be used for saving webcam image.

**8. Back**

Click on **Back** button for returning to Webcam Basic Setting screen.

**9. Apply & Cancel**

Click on **Apply** button to continue. Click on **Cancel** button to clean the setting on this page.

### **6.3.3.3 Application for Webcam**

#### **6.3.3.3.1 Web Camera Monitoring Application**

Monitor your home with a Webcam via Server Router. Take pictures via Server Router, also can do the monitoring or recording all images into the USB HDD for reviewing. Often marketed as surveillance tools for home or office security, network Webcams are now being employed by early adopters for more personal matters, such as watching kids and monitoring pets. The Webcam can be remotely accessed and controlled via a browser. Besides, to record and monitor live action with USB webcam, also can view the image through Internet browsers or mobile phones.

##### **6.3.3.3.1.1 Web Camera Monitoring via WAN connecting**

Users must config with Visual Server or DMZ settings. Input 192.168.1.254 into browser blanks, and you will see the personal account login screen appear then input your own user account and password. After login by personal, your will see the personal control panel screen as below, please click on "**My Webcam**".

## Wireless 802.11n Server Router



Router / AP / WiFi AP

*Administrator*

*Personal Panel*

Click on Personal Panel to enter.



There will be a pop-up screen showing the image from web camera as below example.



### 6.3.3.1.2 Web Camera Monitoring via Mobile Phone

Also, you may view the monitor live action through mobile phones.

Please key in the WAN IP address plus “**/webcam.html**” e.g.  
**http://192.168.1.254/webcam.html** into the mobile phone’s browser blank and you will see the webcam user login screen appeared.



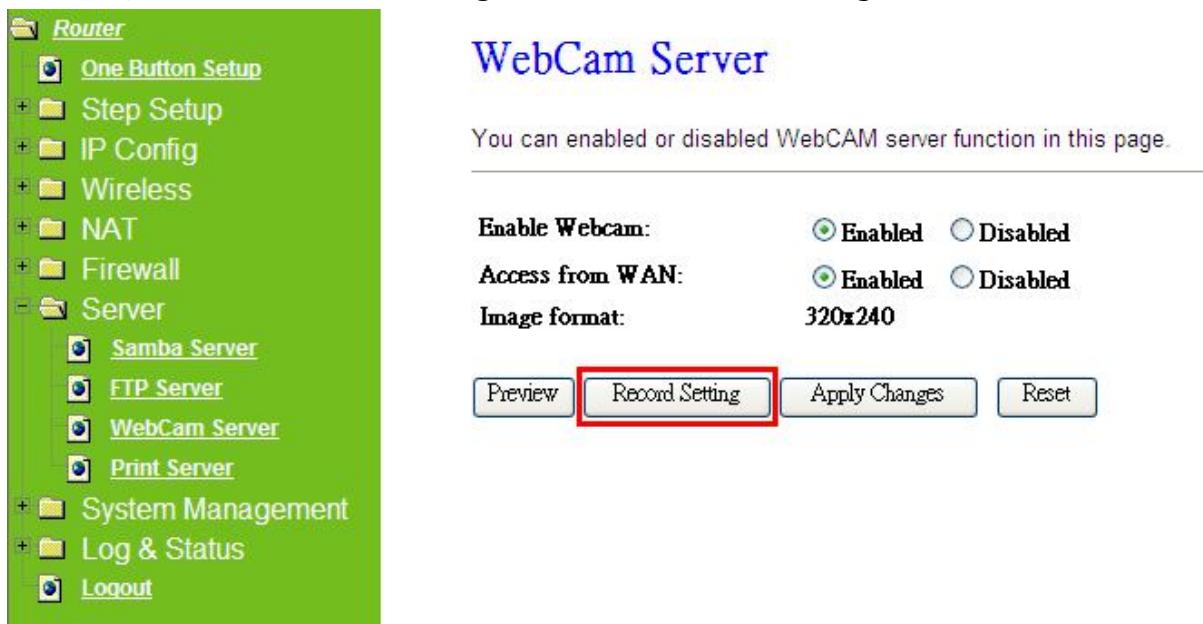
Input Username and Password of your own. You will see like as below monitor screen.



### 6.3.3.3.2 Web Camera Recording

#### 6.3.3.3.2.1 Administrator

Server Router also can record the pictures from Webcam; only Administrator can do the settings. Select **Web Camera Server** from main Menu and Enable this function, click on **Record** setting button for further setting.



The screenshot shows the left sidebar of the Router configuration interface. Under the 'Server' category, the 'WebCam Server' option is selected. The main content area is titled 'WebCam Server' and contains the following text: 'You can enable or disable WebCAM server function in this page.' Below this, there are three settings with radio buttons: 'Enable Webcam' (Enabled is selected), 'Access from WAN' (Enabled is selected), and 'Image format' (320x240). At the bottom are four buttons: 'Preview', 'Record Setting' (which is highlighted with a red box), 'Apply Changes', and 'Reset'.

To setup the Webcam Advanced Configuration for each blank and the image from webcam will be recorded into your USB HDD or Remote FTP.

#### Webcam Advanced Configuration

Snapshot Record Settings.

Save image interval:	<input type="text" value="5"/> sec (default: 5)
Save Location:	<input checked="" type="radio"/> USB <input type="radio"/> Remote FTP
Remote FTP URL:	<input type="text"/>
Remote FTP port:	<input type="text"/>
Remote FTP user:	<input type="text"/>
Remote FTP password:	<input type="text"/>
Remote FTP Directory:	<input type="text"/>

[Back](#) [Apply Changes](#) [Reset](#)

For administrator, you may view all the images from webcam recording, please

select **Folder Management** and click on **Disk Explorer** to view entire folder inside the disk including webcam record files.

## Folder Management

You can specify which USB storage to be System Disk.

USB Device Name

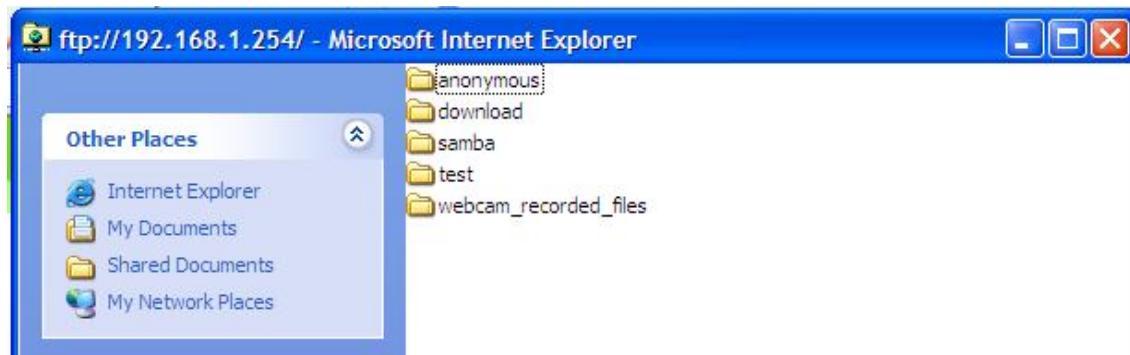
SysDisk	Disk	TYPE	Capacity	Free Space	Function
	USB A	Unknown	63MB	39MB	<input type="button" value="Unplug"/>
<input type="button" value="Disk Explorer"/>					

## Partition / Format SysDisk

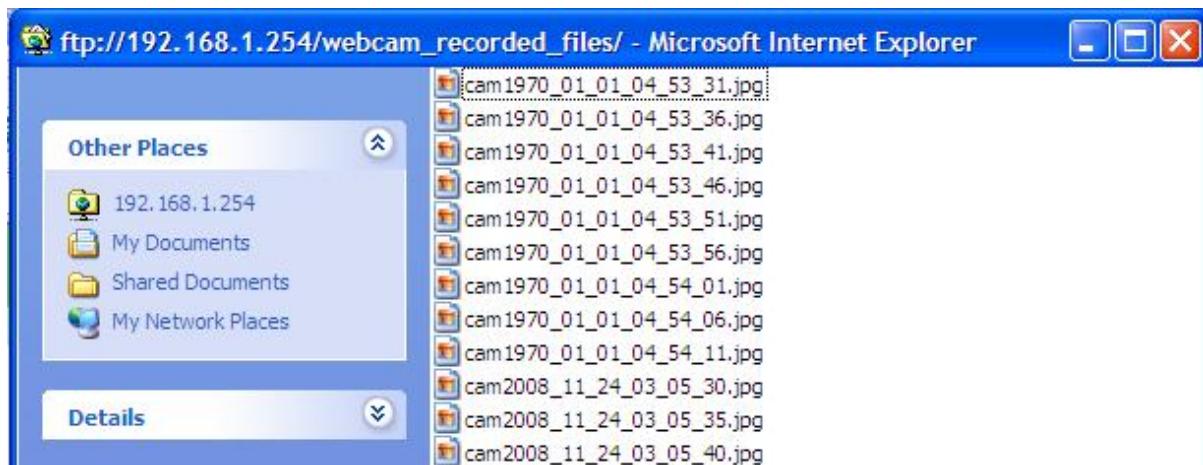
All existing data and partitions on the HDD will be DESTROYED ! Make sure you really need to do this !

TYPE:  FAT16/32  NTFS  EXT3

After click on **Disk Explorer**, you will see the folder screen appear including all the folders.



All the image files will be saved in the folder "**webcam\_recorded\_files**". Please open the file for checking.



### 6.3.3.3.2.2 Personal Application

All the users under administrator's setting can view entire webcam recording images from **My Document**. Please login by your own personal account. For viewing your own folder, please click on "**My Document**".



After click on "**My Document**", you will see below folder screen appeared. You can save files here.



**Note :** If you can't open the folder inside the FTP server, please check with administrator to setup your FTP & Webcam's privileges.

### 6.3.4 Printer Server

The two USB ports on Server Router are for connection with printers to be shared on the local area network. Follow the below steps to setup your PC to connect to a Printer server.



**Print Server**

You can enable or disable print server function in this page.

Enable Printer Server:  Enabled  Disabled

Printer Model: hp deskjet 1180c

Printer Name:

Printer Description:

**Apply Changes** **Reset**

#### 1. Enable Printer Server

Check **Enable** for applying printer server.

#### 2. Printer Model

The printer model will be shown when plug the USB printer.

#### 3. Printer Name

Input the name of printer you like.

#### 4. Printer Description

Input the description of printer as your demand.

#### 5. Apply & Cancel

Click on **Apply** button to continue. Click on **Cancel** button to clean the setting on this page.

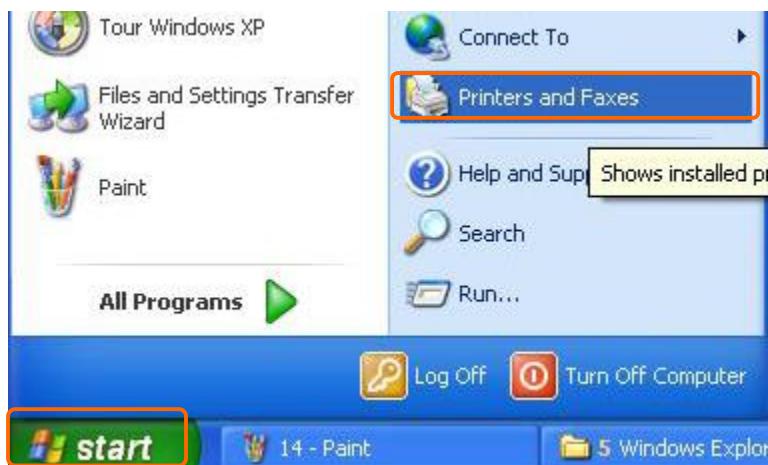
Besides above setting finished, the printer setting on PC also needs to be set as follows.

### 6.3.4.1 Printer Setting for PC

After Enable Printer Server in Quick Setup and Printer Server Configuration, please follow below steps to set the detail **LPR** settings in your PC. (Below example is for Windows XP platform.)

Step 1:

Please go to **Start > Printers and Faxes** to add a printer.



Step 2:

Click "**Add a printer**".



Step 3:

Click "**Next**".



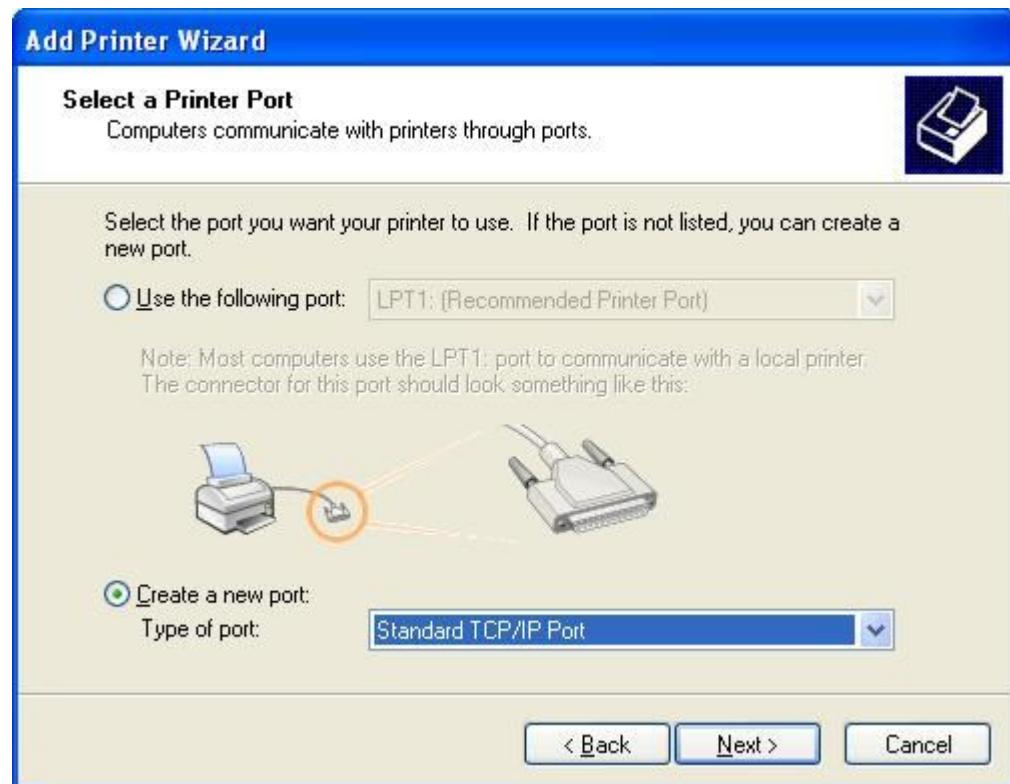
Step 4:

Click the **“Local printer attached to this computer”**, and then click **“Next”**.



Step 5:

Click the “**Create a new port**” and select the “**Standard TCP/IP Port**”, and then click “**Next**”.

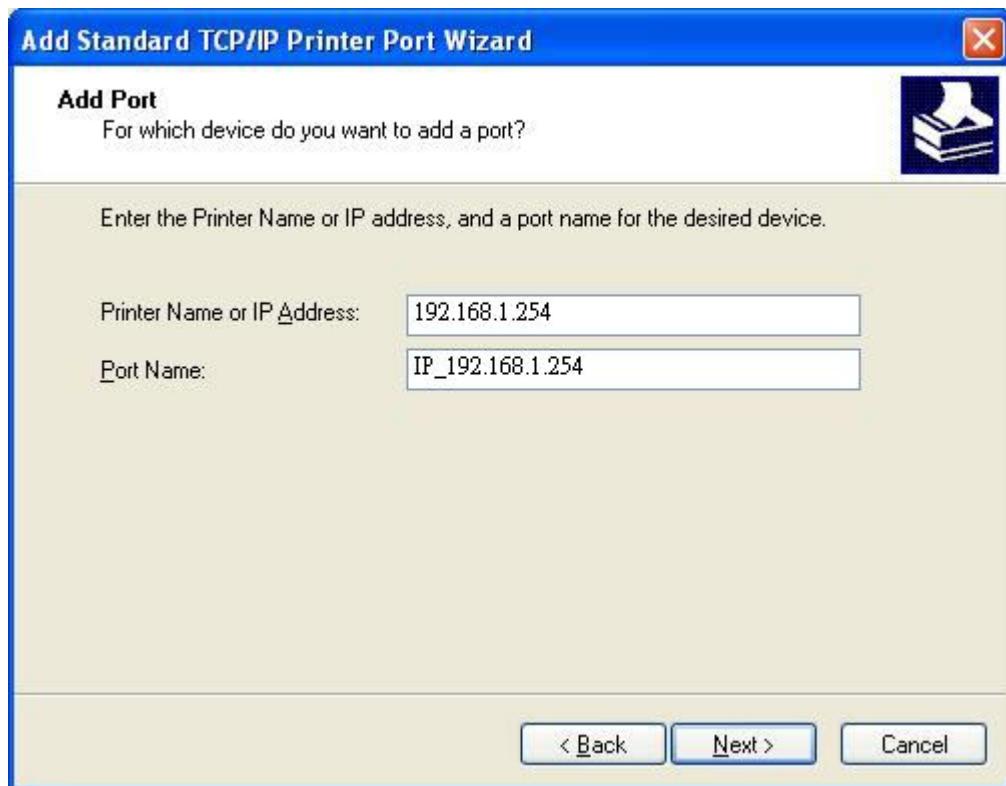


Step 6:  
Click “**Next**”.



Step 7:

Input the IP address of Server Router: **192.168.1.254**, and then click “**Next**”.



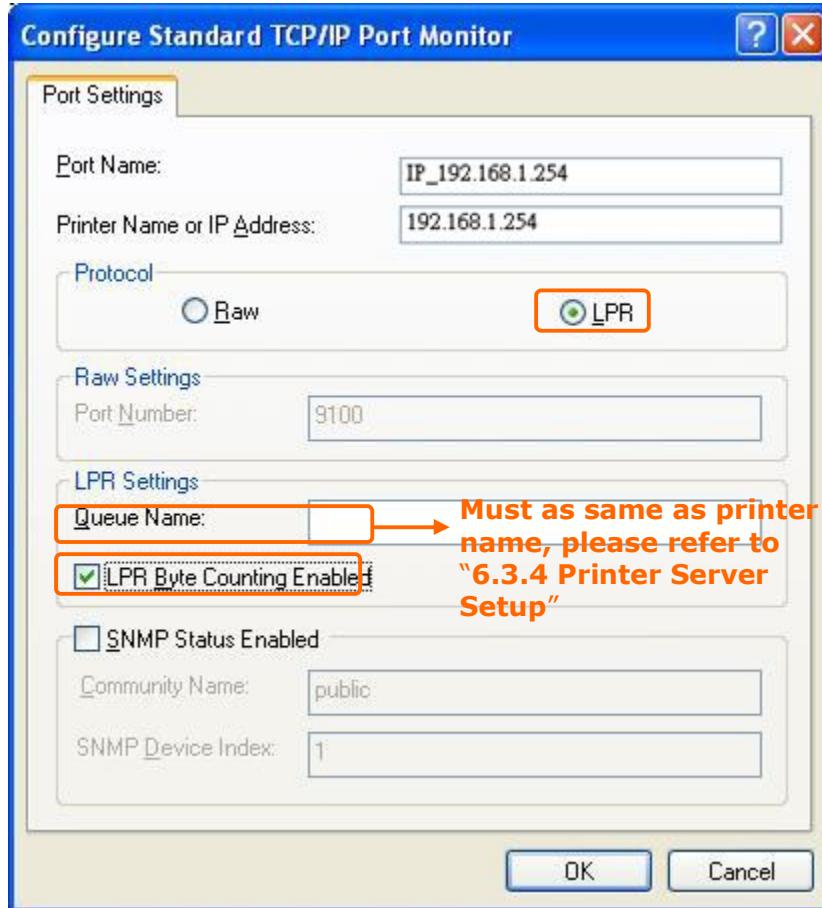
Step 8:

Select the “**Custom**” and click the “**Settings**”, and then click “**Next**”.



Step 9:

Select “**LPR**” and give it the same “**Queue Name**” as USB Printer Name as shown, and mark “**LPR Byte Counting Enabled**”. Finally, click on “**OK**” button.



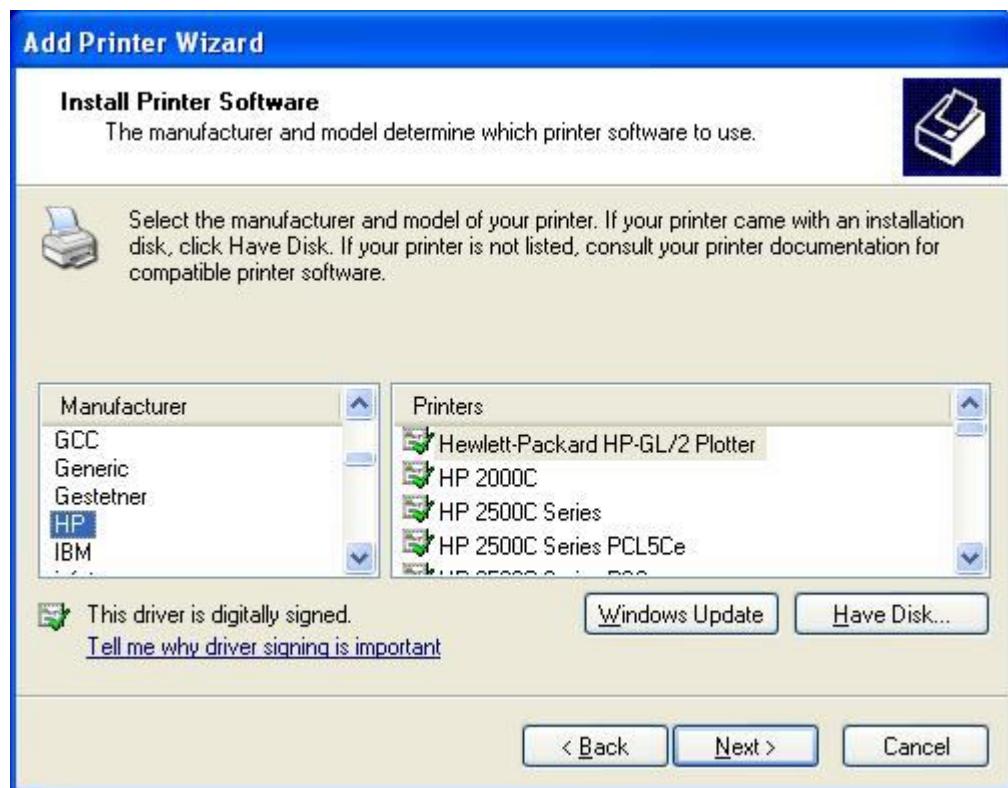
Step 10:

Click the “**Finish**”.



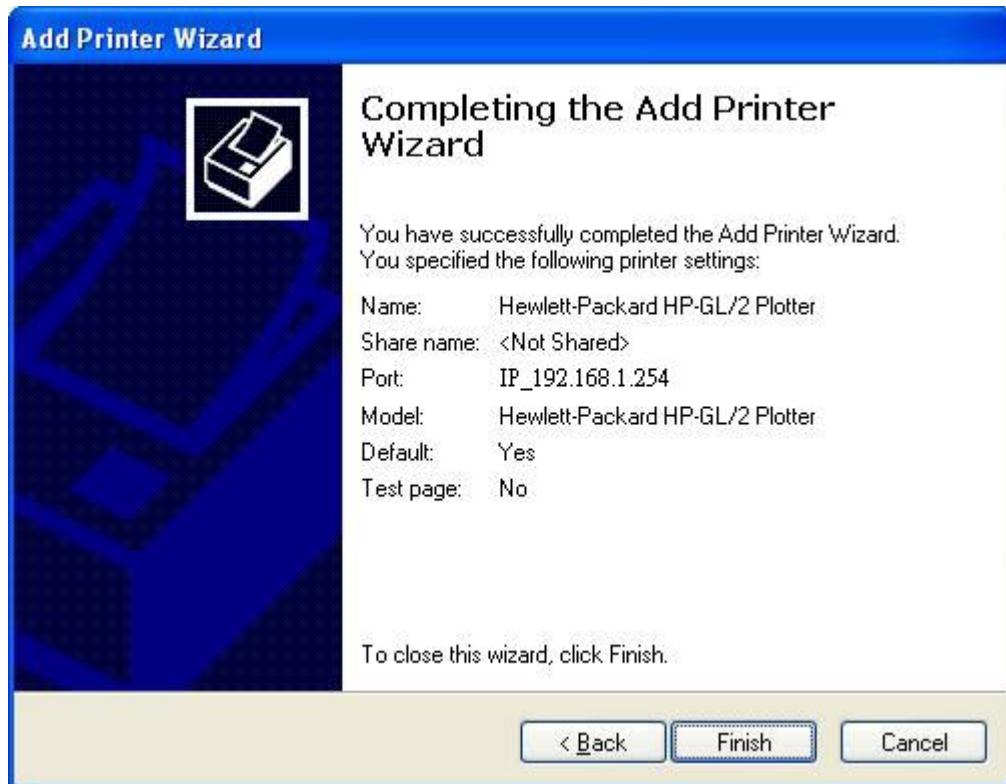
Step 11:

Select the **“Manufacturer”** and **“Printers”**. If your printer doesn’t listed in the table, please install its driver CD and then click on **“Have Disk...”** button for installation. Or click on **“Next”** button to finish the setting.



Step 12:

Click on **Finish** button and all steps of setting printer server are completely.



## 6.4 System Management

It has 6 sections: Change Password, Firmware Upgrade, Profiles Save, Time Zone Setting, UPnP Setting, and Language Setting. It is easy and helpful for users making more detailed settings.