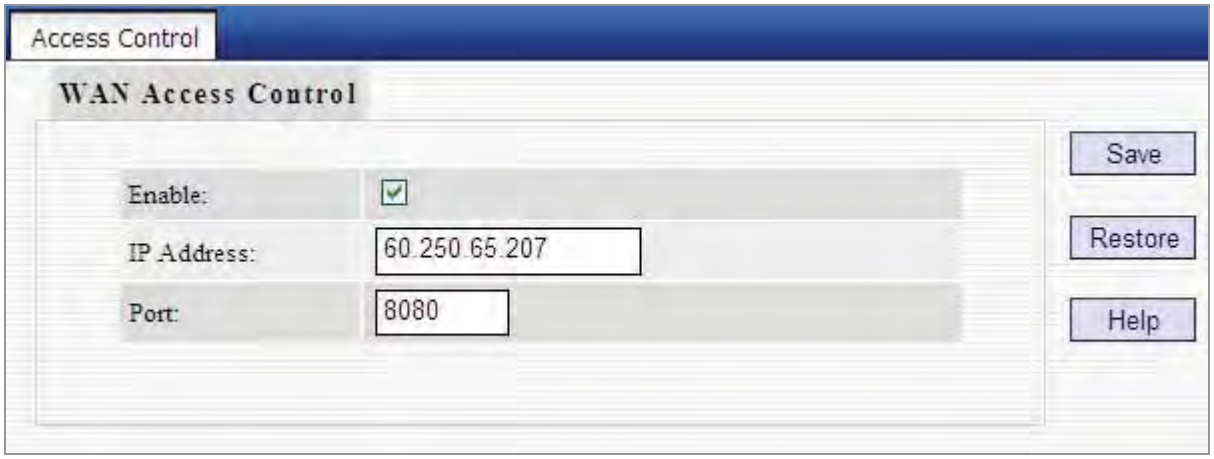

Access Control
WAN Access Control
Enable:
IP Address:
60.250.65.207
Port:
8080
Save
Restore
Help

Figure 5-3-22

5.4 Advanced Settings

“Advanced Settings” includes the following 6 submenus. Clicking any of them enters corresponding interface for configuration. Below explains, in details, each such feature.

5.4.1 Virtual Server

The Virtual Server feature grants Internet users access to services on your LAN. It is useful for hosting online services such as FTP, Web, or game servers. For each Virtual Server, you define a WAN port on your router for redirection to an internal LAN IP Address and LAN port.

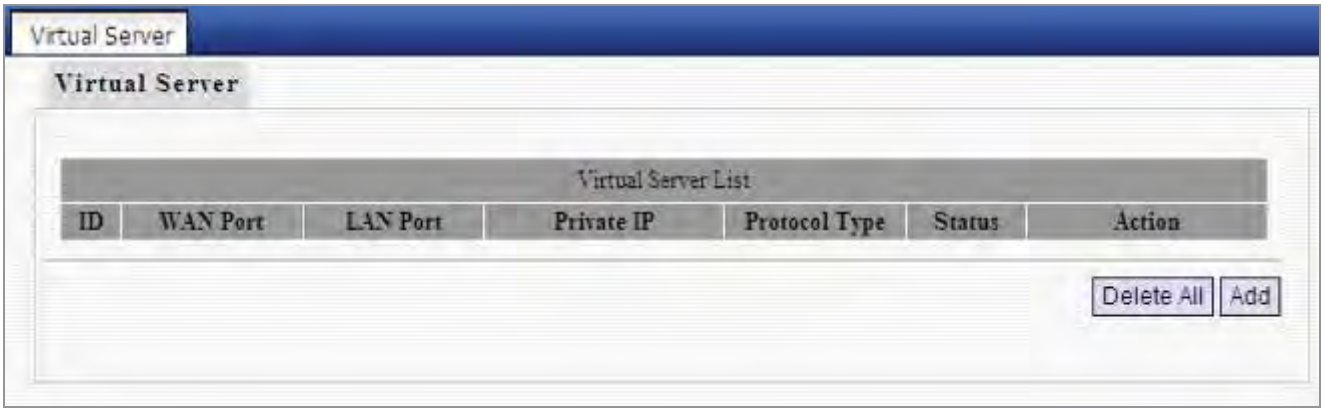


Figure 5-4-1

Click “**Add**” to display below page.

Figure 5-4-2

The page includes the following fields:

Object	Description
• **WAN Port:**	Enter the WAN service port.
• **Well-Known Service Ports:**	The “Well-Known Service Port” lists commonly used protocol ports such as: ■ Leviton S&A Controller (4369) ■ DNS (53） ■ FTP (21) ■ GOPHER (70) ■ HTTP (80) ■ NNTP (1190) ■ POP3 (110) ■ PPTP (1723) ■ SMTP (25) ■ SOCK (1080) ■ TELNET(23) In case that you don’t find the port ID you need, add it manually.
• **LAN Port:**	Enter LAN service port.
• **LAN IP:**	The IP address of a computer used as a server in LAN.
• **Protocol:**	Includes **TCP**, **UDP** and **Both**. Select “Both” if you are not sure about which protocol to use.
• **Enable:**	Check the “Enable” option to activate corresponding entry.

For example: If you create a web server using port 80 on a LAN PC at the IP address of 192.168.0.100, and you want WAN users to access such server via http://x.x.x.x:4000 (x.x.x.x represents router’s WAN IP address), then do as follows:

1) Enter “4000” in WAN Port field, 80 in LAN port field and 192.168.0.100 in Private IP field,
2) Select “Both” from protocol drop-down list.
3) Check the “Enable” box.
4) Click “Save” to save such settings.

Figure 5-4-3

Note

Setting WAN port hereon to the same value as that on WAN access control section will deactivate the virtual server feature.

5.4.2 DMZ Settings

In some cases, we need to set a computer to be completely exposed to extranet for implementation of a bidirectional communication. To do so, we set it as a DMZ host.

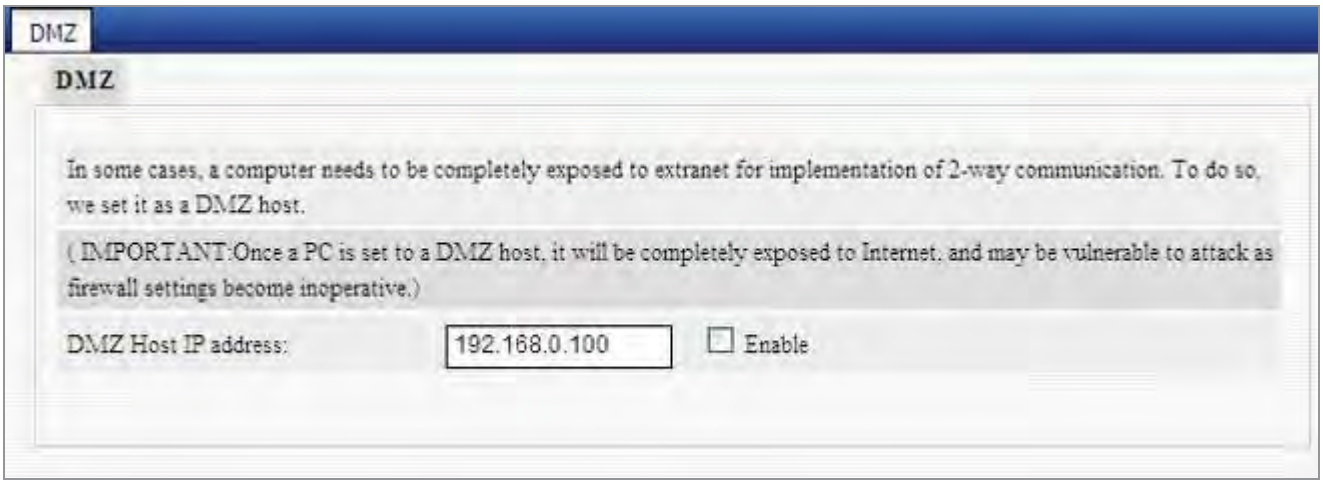


Figure 5-4-4

The page includes the following fields:

Object	Description
• **DMZ Host IP Address:**	Enter the IP address of a LAN computer which you want to set to a DMZ host.
• **Enable:**	Check/uncheck to enable/disable the DMZ host.

Note

1. If you set a PC to a DMZ host, it will be completely exposed to extranet and gains no more protection from the device firewall.
2. 2. A WAN user accesses the DMZ host through a corresponding WAN IP address.

5.4.3 UPnP Settings

UPnP (Universal Plug and Play) requires Windows ME/Windows XP or later or application softwares that support such UPnP feature.

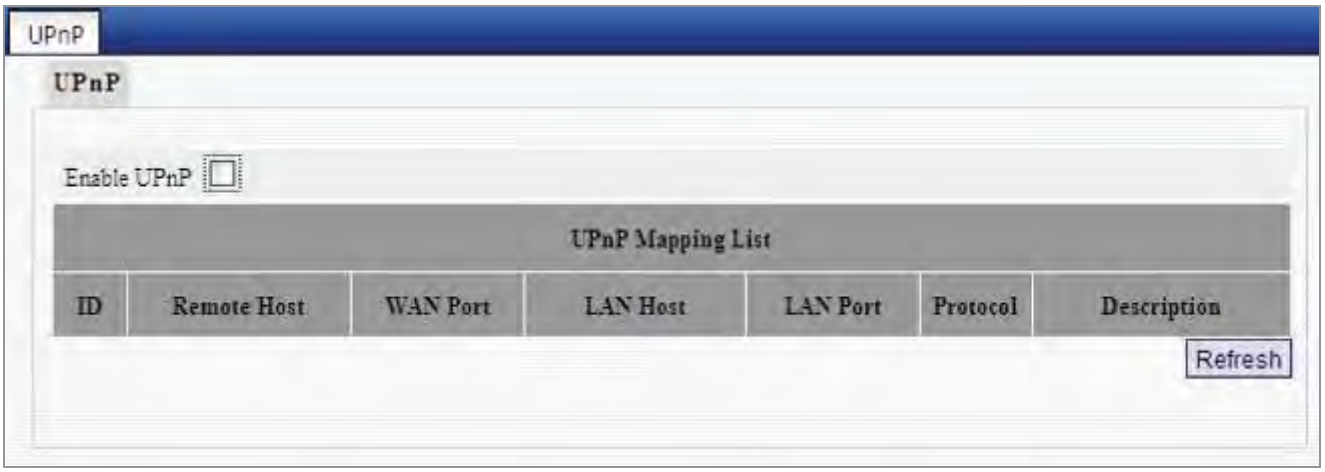


Figure 5-4-5

The page includes the following fields:

Object	Description
• **ID:**	Entry ID.
• **Remote Host:**	Description of a remote host that receives/sends responses.
• **WAN Port:**	Port on router side.
• **LAN Host:**	Description of an internal host that receives/sends responses.
• **LAN Port:**	Port on host side.
• **Protocol:**	Indicates whether to perform TCP or UDP port forwarding
• **Description:**	Software info of a mapped port.

5.4.4 Routing

This section talks about **Routing Table** and **Static Routing** features.

■ Routing Table

This page displays the router's core routing table which lists destination IP, subnet mask, gateway, hop count and interface.

Figure 5-4-6

■ Static Routing

You can use this section to set up router's static routing feature.

Figure 5-4-7

Click "**Add**" to add static routing entries.

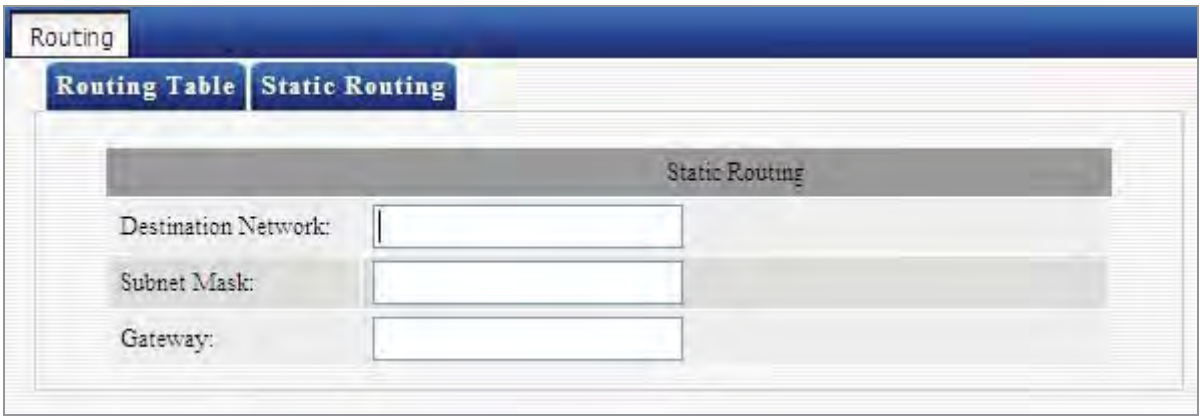


Figure 5-4-8

The page includes the following fields:

Object	Description
• **Destination Network:**	Enter a destination IP address.
• **Subnet Mask:**	Enter a Subnet Mask that corresponds to the destination IP address you entered.
• **Gateway:**	Next-hop IP address.

5.4.5 Bandwidth Control

To better manage bandwidth allocation and optimize network performance, use the Custom Bandwidth Allocation feature.

Figure 5-4-9

The page includes the following fields:

Object	Description
• **Custom Bandwidth Allocation:**	Select this option to customize a bandwidth allocation policy that best fits your network. You can set specific limits on uplink and downlink bandwidth of PCs within a specified IP range.

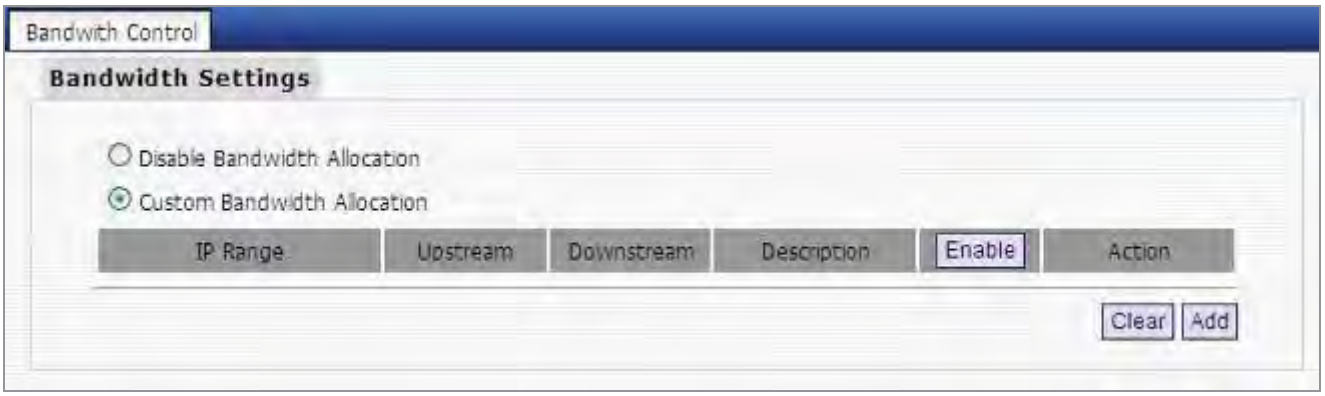


Figure 5-4-10

Click "**Add**" to display the page below:

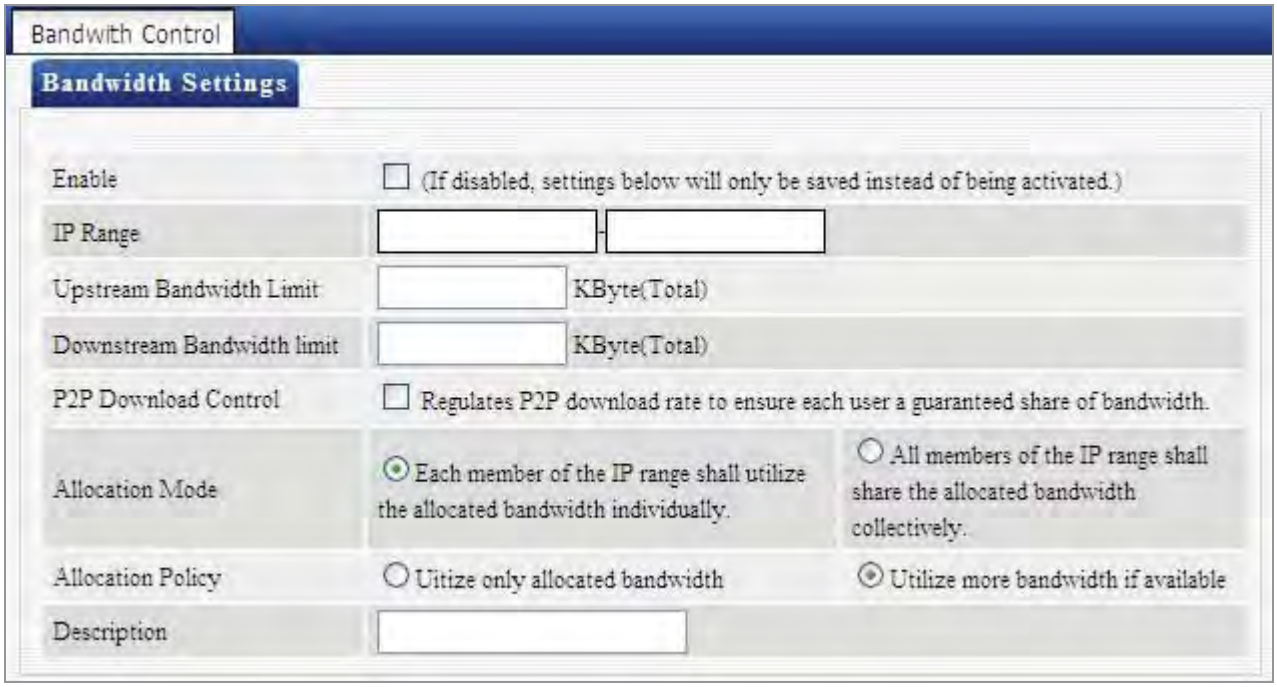


Figure 5-4-11

The page includes the following fields:

Object	Description
• **Enable:**	Check/uncheck to enable/disable current bandwidth entry
• **IP Range:**	Enter a single IP or an IP range.
• **Upstream Bandwidth Limit:**	Max total upload bandwidth for a specified PC or a range of PCs.
• **Downstream Bandwidth Limit:**	Max total download bandwidth for a specified PC or a range of PCs
• **P2P Download Control:**	Regulates P2P download rate to ensure each user a guaranteed share of bandwidth.
• **Allocation Mode:**	Select either- ■ "Individual (Each member of the IP range shall utilize the allocated bandwidth individually)" ■ "Collective (All members of the IP range shall share the allocated bandwidth collectively)"
• **Allocation Policy:**	Select either "Utilize only the allocated bandwidth" or "Utilize more bandwidth if available"
• **Description:**	Brief description of current entry.

1. Please note the bandwidth unit.
2. If you enable the P2P Download Control feature, it will limit P2P download rate (smaller than the specified value) to ensure other applications such as web browsing a reserved and guaranteed share of bandwidth.
3. If you select "**Utilize more bandwidth if available**", router will dynamically adjust uplink/downlink bandwidth allocation to ensure defined and additional bandwidth if available or only defined bandwidth.

For example:

If you want each PC within the IP range of 192.168.0.100-192.168.0.120 to have up to 2M uplink and 2M downlink bandwidth, and want to control P2P download bandwidth, then configure same settings as shown on the screen below on your router:

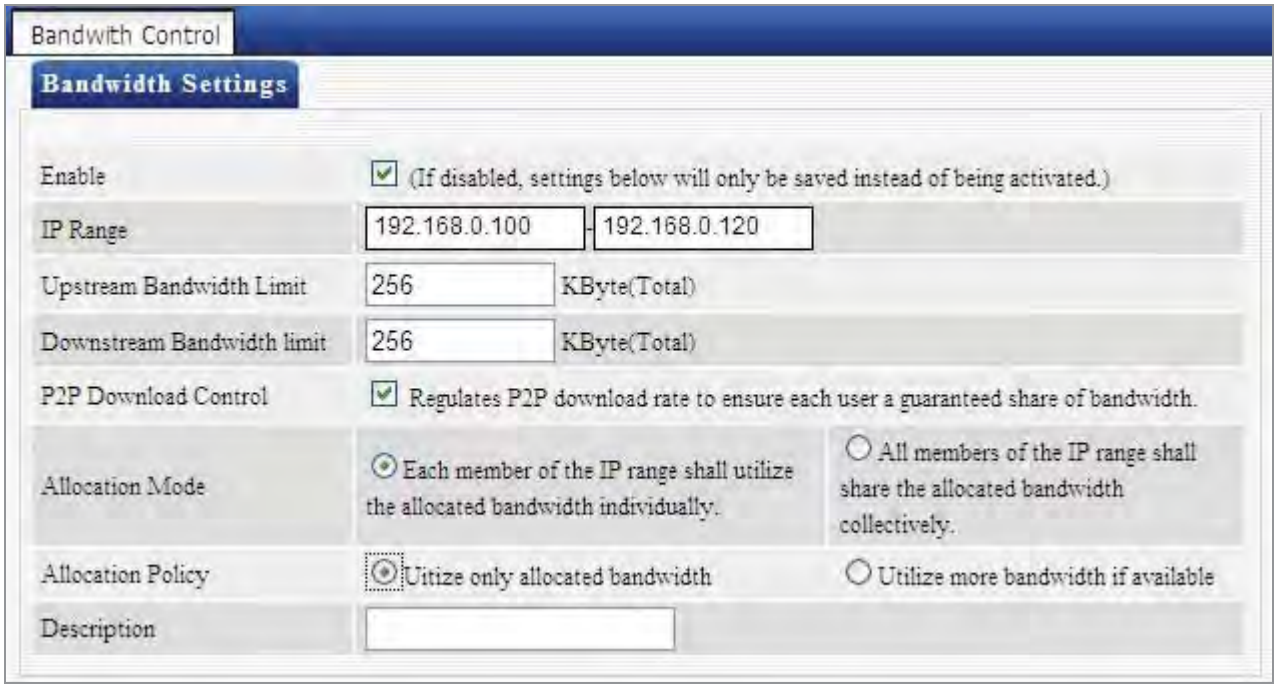


Figure 5-4-12

5.5 Wireless Settings

Wireless Settings includes 8 submenus as shown in the screenshot below. Clicking any tab enters corresponding interface for configuration.

5.5.1 Basic Settings

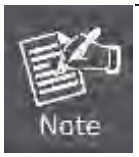
This section allows you to manage your wireless network (2.4G or 5G). You can config country code, wireless network name (SSID), network mode and channel settings, etc the way you want.

■ **Basic Settings-- 2.4G**

Figure 5-5-1

The page includes the following fields:

Object	Description
• **Country:**	Select your country code from the drop-down list. There are 11 options available.
• **2.4GHz Wireless Network:**	Check/uncheck to enable/disable the 2.4GHz wireless feature. If disabled, all 2.4GHz-based features will be disabled accordingly.
• **SSID Broadcast:**	Select "Enable"/"Disable" to make your wireless network visible/ invisible to any wireless clients within coverage when they perform a scan they perform a scan to see what's available. When disabled, such wireless clients will have to first know this SSID and manually enter it on their devices if they want to connect to the SSID. By default, it is **enabled**.
• **SSID:**	A SSID (Service Set Identifier) is the unique name of a wireless network.
• **802.11 Mode:**	Select a right mode according to your wireless client. The default mode is **11b/g/n mixed**.
• **Channel:**	For an optimal wireless performance, you may select the least interferential channel. It is advisable that you select an unused channel or "Auto" to let device detect and select the best possible channel for your wireless network to operate on from the drop-down list.
• **Channel Bandwidth:**	Select a proper channel bandwidth to enhance wireless performance. When there are 11b/g and 11n wireless clients, please select the 802.11n mode of **20/40M** frequency band.
• **Extension Channel:**	Working network frequency range for 11n mode
• **WMM-Capable:**	Enabling this option may boost transmission capacity of wireless multimedia data (such as online video play).
• **ASPD Capable:**	Select to enable/disable the auto power saving mode.



When there are only **non-11n wireless clients**, select **20M** frequency band mode; when the wireless network mode is **11n mode**, please select **20/40M** frequency band to boost its throughput.

■ Basic Settings-- 5G

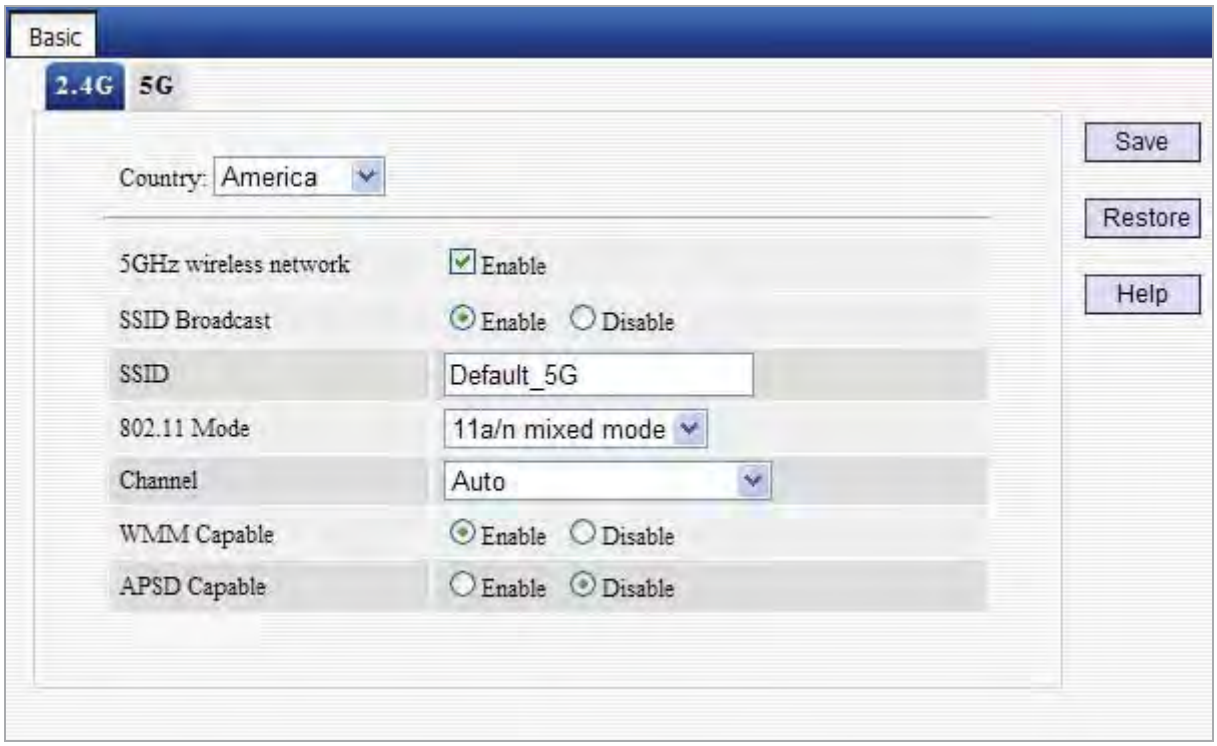


Figure 5-5-2

The page includes the following fields:

Object	Description
• **Country:**	Select your country code from the drop-down list. There are 10 options available.
• **5GHz Wireless Network:**	Check/uncheck to enable/disable the 5GHz wireless feature. If disabled, all 5GHz-based features will be disabled accordingly.
• **SSID Broadcast:**	Select “Disable” to hide your SSID. When disabled, no wireless clients will be able to see your wireless network when they perform a scan to see what’s available. If they want to connect to your router, they will have to first know this SSID and then manually enter it on their devices. By default, this option is **enabled**.
• **SSID:**	A SSID (Service Set Identifier) is the unique name of a wireless network (changeable).
• **802.11 Mode:**	Select a right mode according to your wireless client. The default mode is **11a/n**.
• **Channel:**	The Channel can be changed to fit the channel setting for an existing wireless network or to customize the wireless network. From the drop-down list, you can select a most effective channel. You can also select “**Auto Select**” to let system detect and choose one that best fits

	your network.
• **WMM-Capable:**	Enabling this option may boost transmission capacity of wireless multimedia data (such as online video play).
• **ASPD Capable:**	Select to enable/disable the auto power saving mode.

5.5.2 Wireless Security

This section allows you to encrypt both 2.4GHz wireless and 5GHz wireless networks to block unauthorized accesses and malicious packet sniffing.

To configure wireless security settings for 2.4GHz network, enter page below:

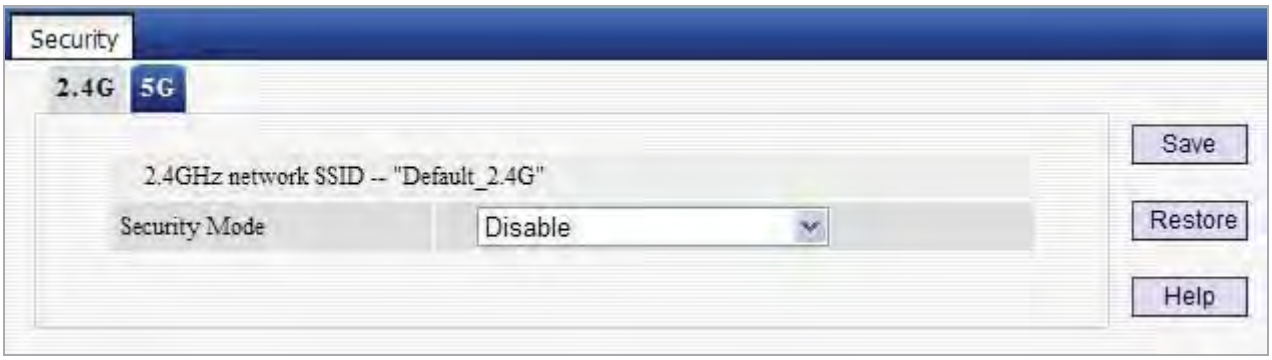


Figure 5-5-3

Available options for security mode include "**Open**", "**Shared**", "**WPA-PSK**", "**WPA2-PSK**", "**Mixed WPA/WPA2-PSK**". See below for details.

Figure 5-5-4

■ OPEN/SHARED

WEP is intended to provide data confidentiality comparable to that of a traditional wired network. Two methods of authentication can be used with WEP: **Open System** authentication and **Shared Key** authentication.

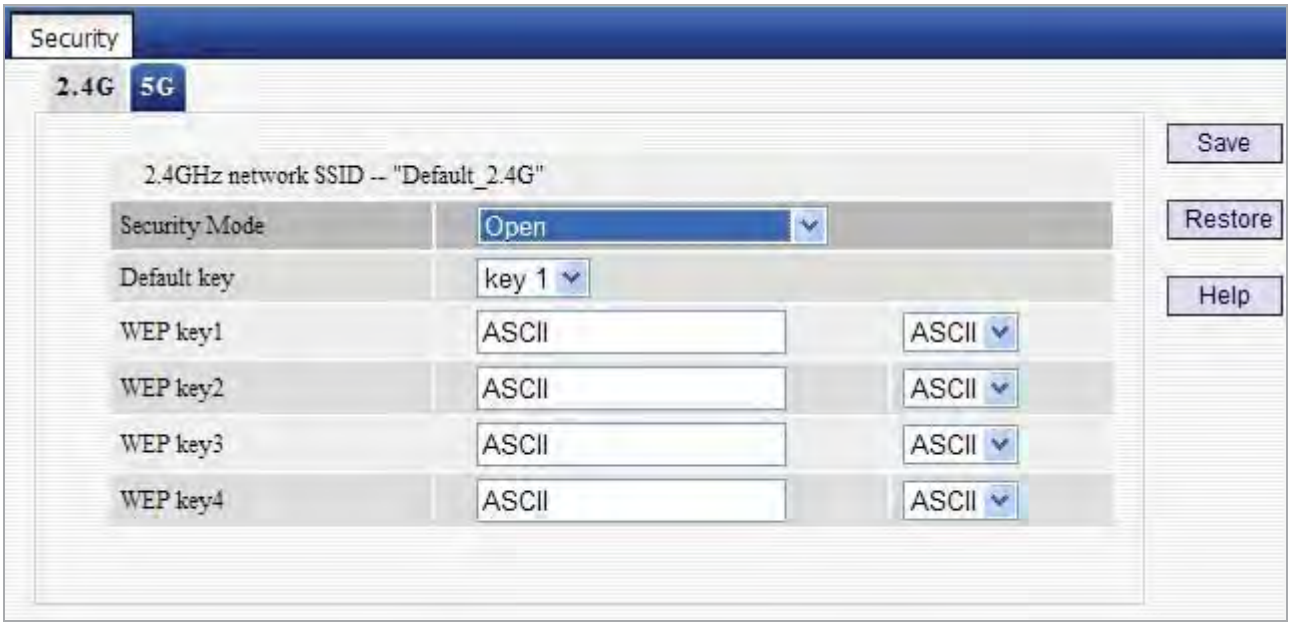


Figure 5-5-5

The page includes the following fields:

Object	Description
• **Security Mode:**	Select a proper security mode from the drop-down menu.
• **Default Key:**	Select one key from the 4 preset keys to encrypt wireless data on the network.

■ WPA-PSK

The WPA protocol implements the majority of the IEEE 802.11i standard. It enhances data encryption through the **Temporal Key Integrity Protocol (TKIP)** which is a 128-bit per-packet key, meaning that it dynamically generates a new key for each packet. WPA also includes a message integrity check feature to prevent data packets from being hampered with. Only authorized network users can access the wireless network.

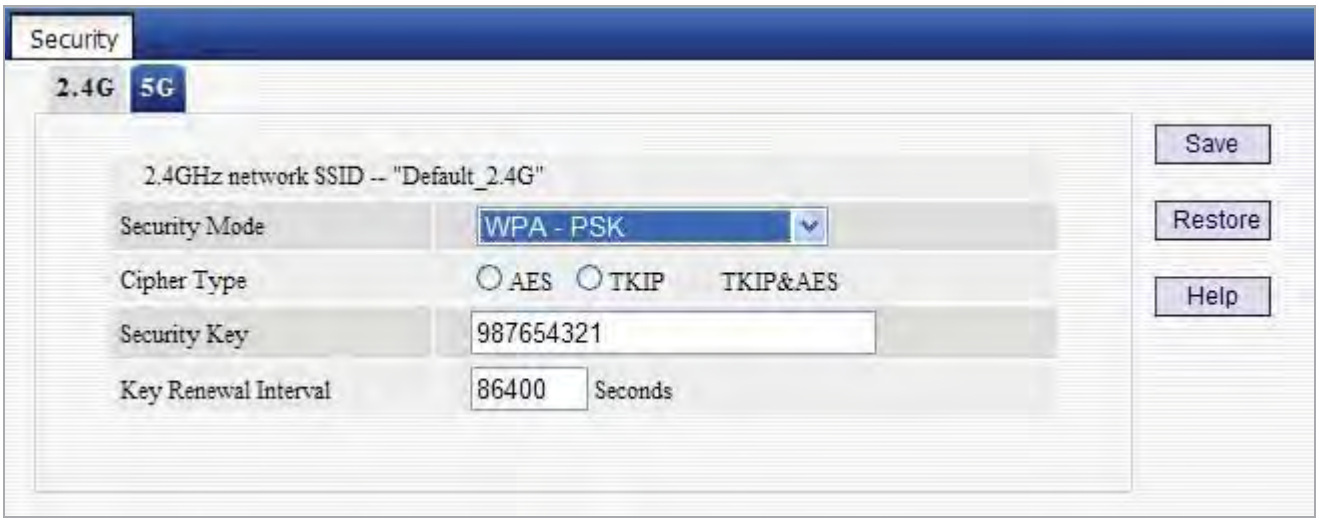


Figure 5-5-6

The page includes the following fields:

Object	Description
• **Cipher Type:**	Select one cipher type from: ■ **AES** (Advanced Encryption Standard) ■ **TKIP** (Temporary Key Integrity Protocol)
• **Security Key:**	Enter a security key, which must be between 8-63 ASCII characters.
• **Key Renewal Interval:**	Enter a valid time period for the key.

■ WPA2-PSK

The later WPA2 protocol features compliance with the full IEEE 802.11i standard and uses **Advanced Encryption Standard (AES)** in addition to TKIP encryption protocol to guarantee better security than that provided by WEP or WPA.

Figure 5-5-7

The page includes the following fields:

Object	Description
• **Cipher Type:**	Select one cipher type from: ■ **AES** (Advanced Encryption Standard) ■ **TKIP** (Temporary Key Integrity Protocol) ■ **TKIP&AES**.
• **Security Key:**	Enter a security key, which must be between 8-63 ASCII characters.
• **Key Renewal Interval:**	Enter a valid time period for the key.

5.5.3 WPS Settings

Wi-Fi Protected Setup makes it easy for home users who know little of wireless security to establish a secure wireless home network, as well as to add new devices to an existing network without entering long passphrases or configuring complicated settings.

Figure 5-5-8

Simply enter a PIN code or press the software PBC button or hardware WPS button (if any) and a secure wireless connection is established.

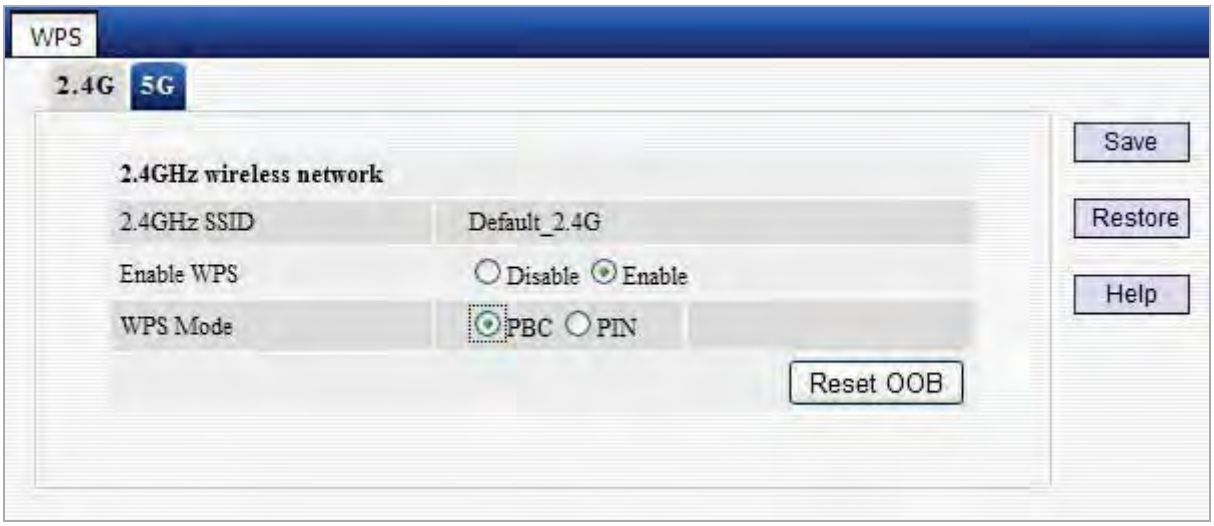


Figure 5-5-9

The page includes the following fields:

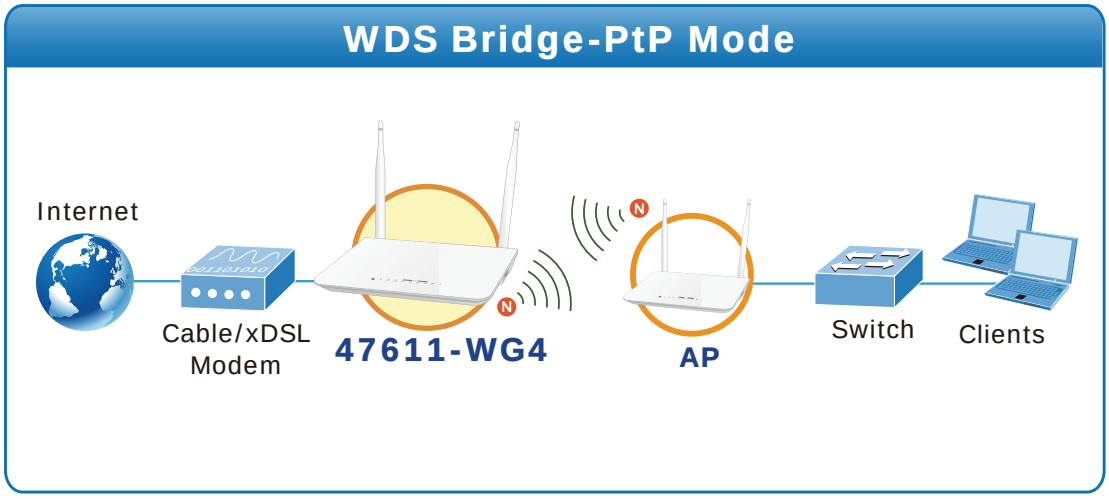
Object	Description
• **Enable WPS:**	Select to enable/disable the WPS encryption.
• **WPS Mode:**	Select PBC (Push-Button Configuration) or PIN. Operation Instructions ■ **PBC:** If you find the WPS LED blinking for 2 minutes after you press the hardware WPS button on the device, it means that PBC encryption method is successfully enabled. And an authentication will be performed between your router and the WPS/PBC-enabled

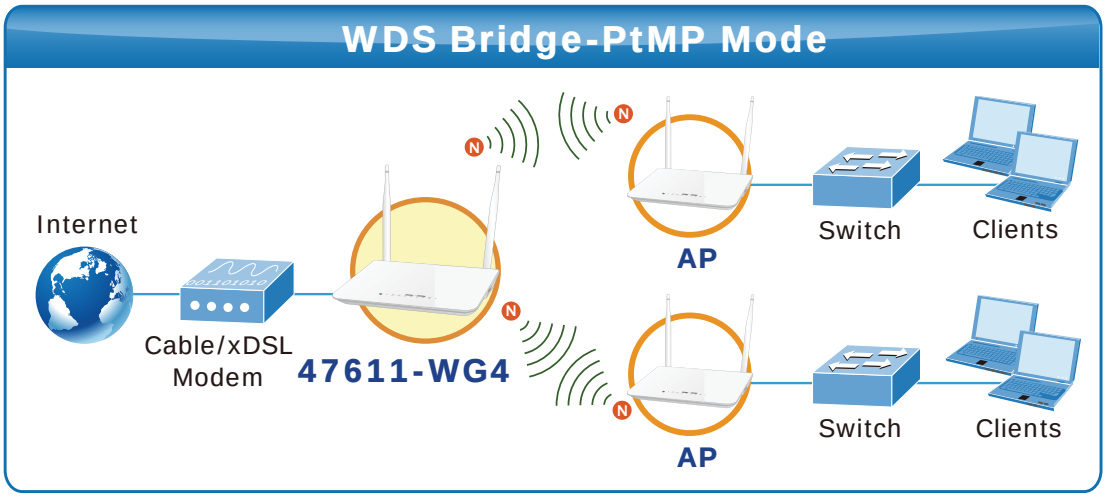
	wireless client device during this time; if it succeeds, the wireless client device connects to your device, and the WPS LED turns off. Repeat steps mentioned above if you want to connect more wireless client devices to the device. ■ **PIN**：To use this option, you must know the PIN code from the wireless client and enter it in corresponding field on your device while using the same PIN code on client side for such connection.
• **Reset OOB:**	When clicked, the WPS LED turns off; WPS function will be disabled automatically; WPS server on the Router enters idle mode and will not respond to client's WPS connection request

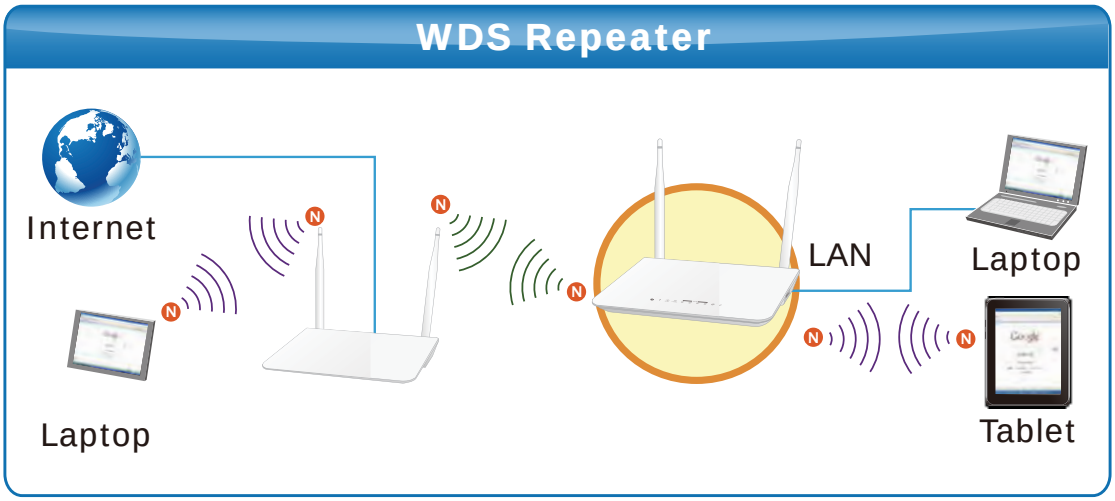
The WPS encryption can be implemented only between your Router and another WPS-capable device.

5.5.4 WDS Settings

WDS (Wireless Distribution System) feature can be used to extend your existing 2.4G or 5G wireless network coverage. Here we present you how to configure such feature in 2.4GHz, which also apply to 5GHz.







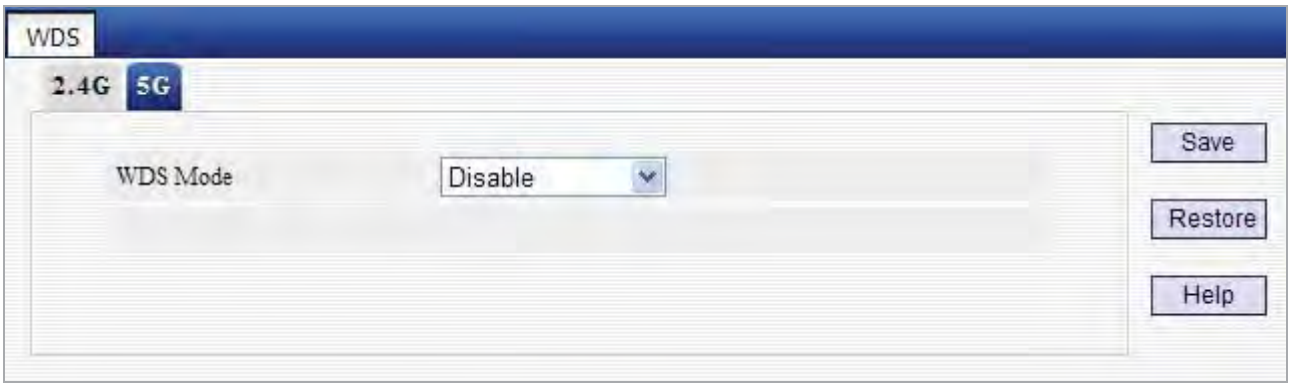


Figure 5-5-10

Select Repeater Mode to display below page:

Object	Description
• **AP MAC Address:**	Enter the MAC address of a wireless link partner or populate this field using the Open Scan option.
• **WDS Mode:**	Select **Disable** or **Repeater Mode**

For example: If you want to implement the WDS feature on 2 47611-WG4 routers labeled 47611-WG4-1 and 47611-WG4-2 respectively, then first select “Repeater Mode” and follow steps below:

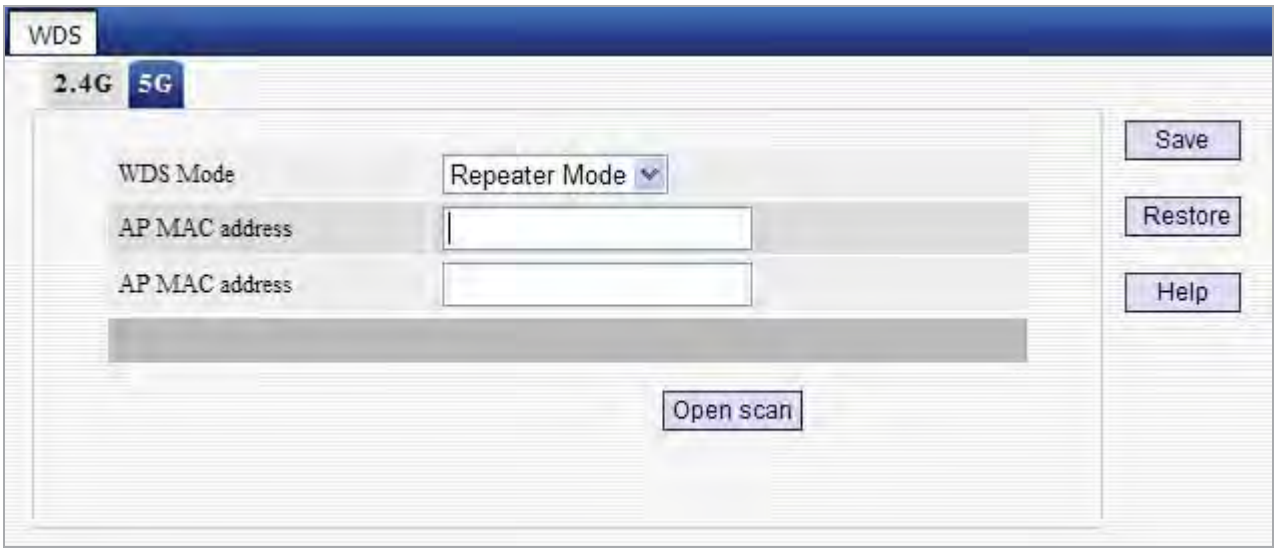


Figure 5-5-11

1. If you already know **47611-WG4-2’s** MAC address, then you can manually enter it on **47611-WG4-1** and click “**Save**”.

2. Or you can use the Open Scan option.

1) Click the “**Open Scan**” button to search and select **47611-WG4-2’s** SSID, confirm on the appearing dialogue

box and then click “Save”. **47611-WG4-2’s** MAC address will be added automatically.

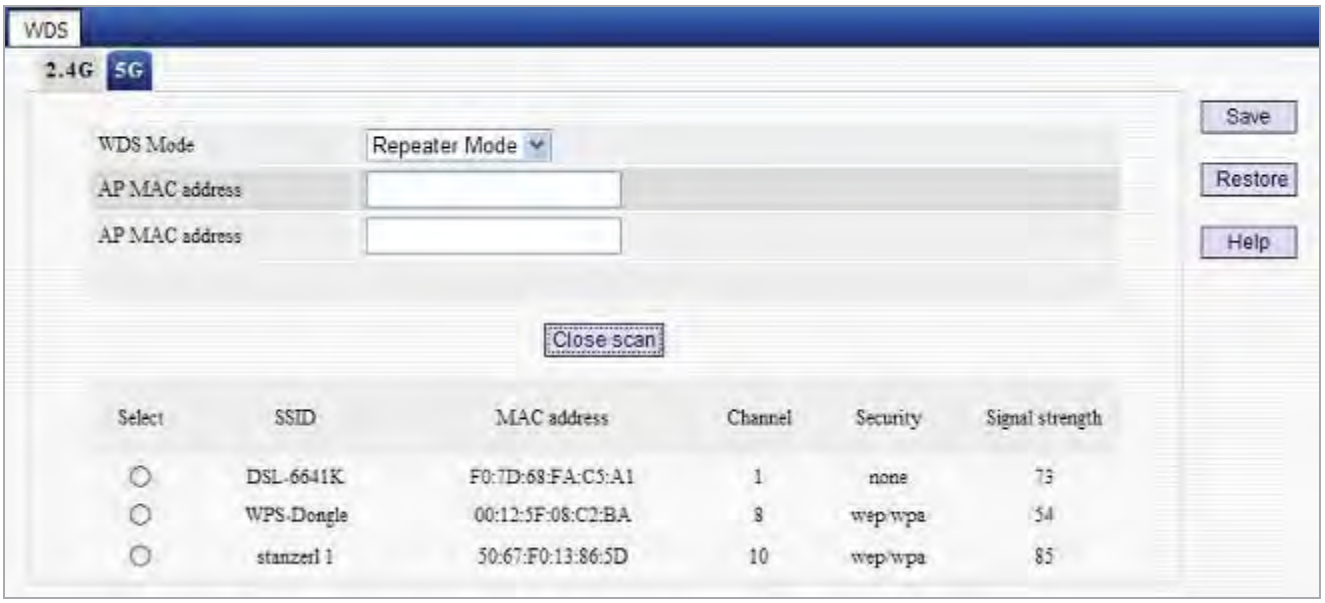


Figure 5-5-12

2) Save your settings.

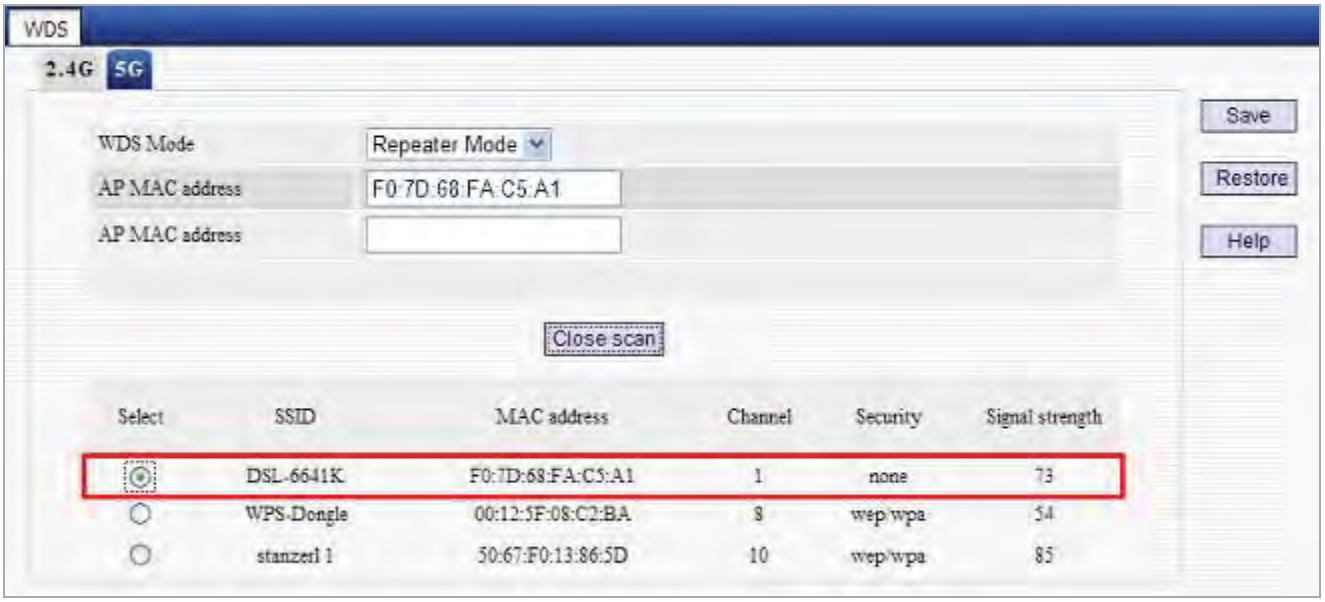


Figure 5-5-13

3. Repeat steps 1-2 on **47611-WG4-2.** After the 2 devices have added each other’s MAC address the WDS feature can be implemented.

Note

1. WDS feature can only be implemented between 2 wireless devices that both support the WDS feature. Plus, SSID, channel, security settings and security key must be the same on both such devices.
2. To encrypt your wireless network, see **sections 5.5.2-5.5.3**. Do remember to reboot the device after you saved your wireless security settings, otherwise the

WDS feature may not function.

5.5.5 Guest Network

The Guest Network feature allows guests to access Internet and other users on the guest network while disallowing them to access device web manager, users on primary network and clients behind the LAN ports.

You can find it available in both 2.4G and 5G network. Here we present you how to configure such feature in 2.4GHz, which also apply to 5GHz.

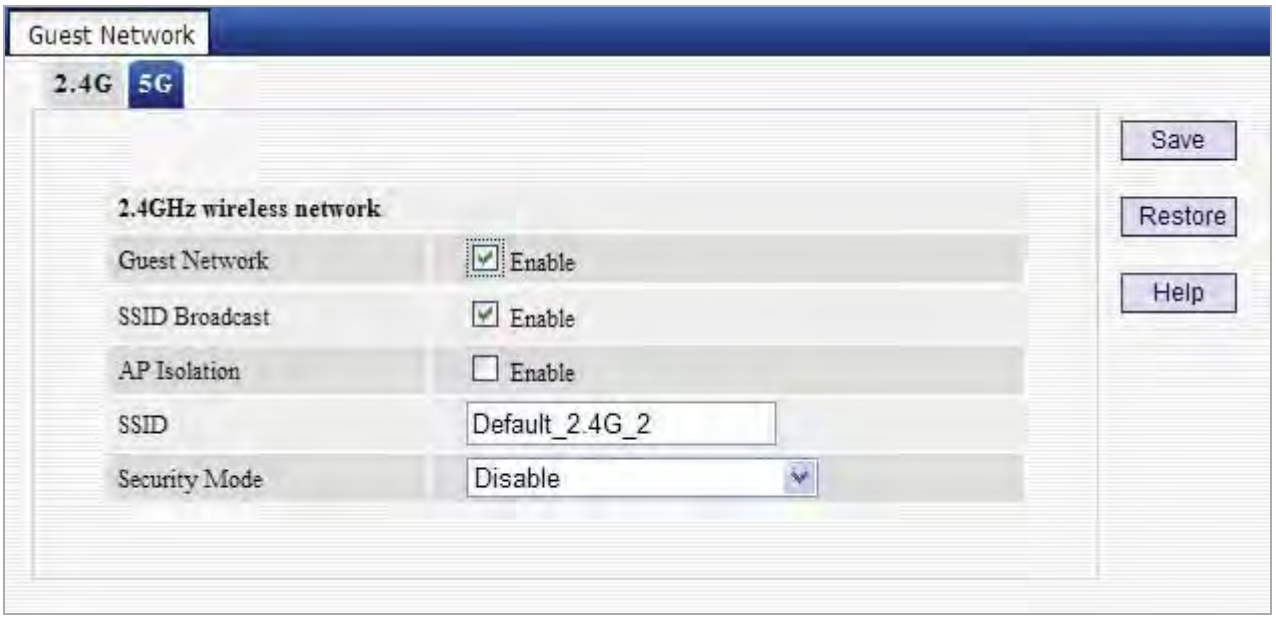


Figure 5-5-14

The page includes the following fields:

Object	Description
• **Guest Network:**	Check/uncheck to enable/disable the guest network feature.
• **SSID Broadcast:**	Select “Disable” to hide your SSID. When disabled, no wireless clients will be able to see your wireless network when they perform a scan to see what’s available. If they want to connect to your router, they will have to first know this SSID and then manually enter it on their devices. By default, it is enabled.
• **AP Isolation:**	If enabled, clients connecting to the guest network will be mutually inaccessible.
• **SSID:**	A SSID (Service Set Identifier) is the unique name of a wireless network.
• **Security Mode:**	Determine whether to require authentication on wireless clients. Select a proper mode from the drop-down menu.

5.5.6 Wireless Access Control

The **MAC-based Wireless Access Control** feature can be used to allow or disallow clients to connect to your 2.4G or 5G wireless network. Here we present you how to config such feature in 2.4GHz, which also apply to 5GHz.

Figure 5-5-15

The page includes the following fields:

Object	Description
• **MAC Address Filter:**	Selecting “Disable” means to deactivate the MAC address filter feature. ■ “**Allow**” means to only allow PCs at specified MAC addresses to connect to your wireless network while ■ “**Deny**” means to only block PCs at specified MAC addresses from connecting to your wireless network.
• **MAC Address:**	Enter the MAC addresses of a wireless client.
• **Add:**	Click it to add a new MAC to the MAC address list.
• **Delete:**	Click it to remove an existing entry.

To allow only a PC at the MAC address of 00:aa:bb:11:22:33 to connect to your wireless network, do as follows:

Step 1. Select “**Allow**” from MAC Address Filter drop-down menu.

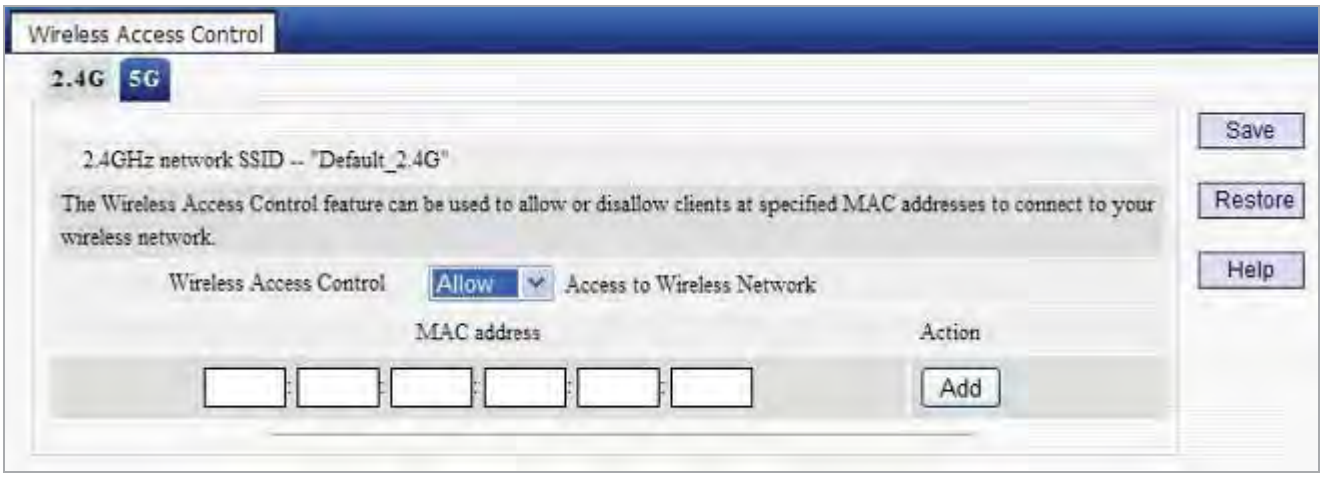


Figure 5-5-16

Step 2. Enter 00:aa:bb:11:22:33 in the MAC address box and click "**Add**".

Step 3. Click the "**Save**" button to save your settings and you can add more MAC addresses, if you like, simply repeating the above steps.

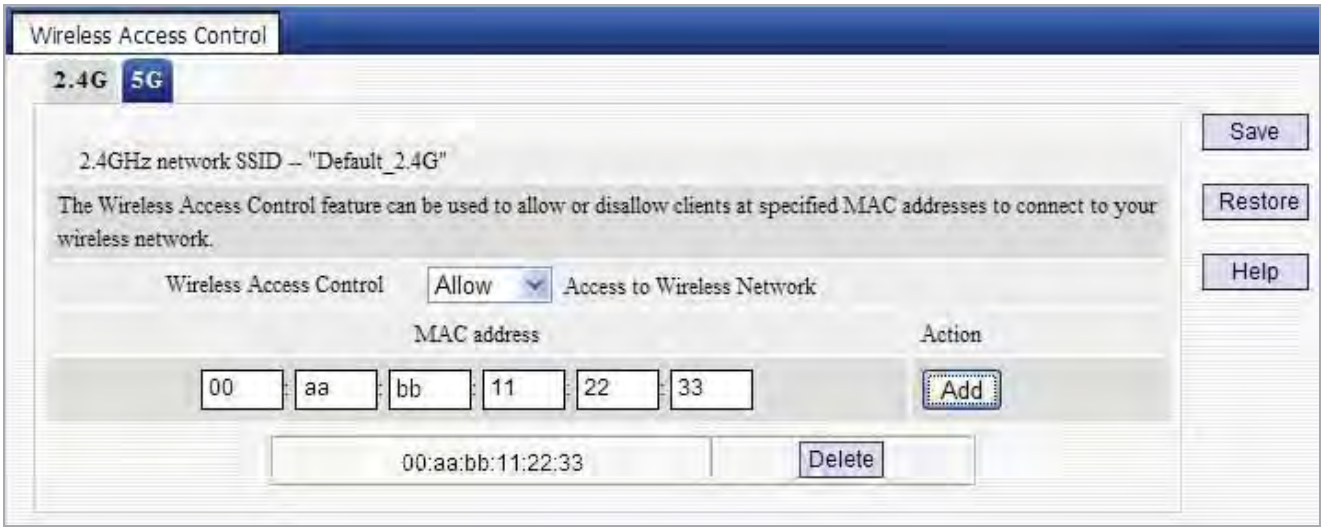


Figure 5-5-17

5.5.7 Connection Status

This interface displays the information of currently connected 2.4G and 5G wireless clients (if any).

Figure 5-5-18

Figure 5-5-19

5.5.8 Wireless –Advance Settings

This section allows you to configure advanced settings, including **Beacon interval, Fragment threshold, RTS threshold** and **DTIM interval**, etc, for both 2.4G and 5G wireless networks.

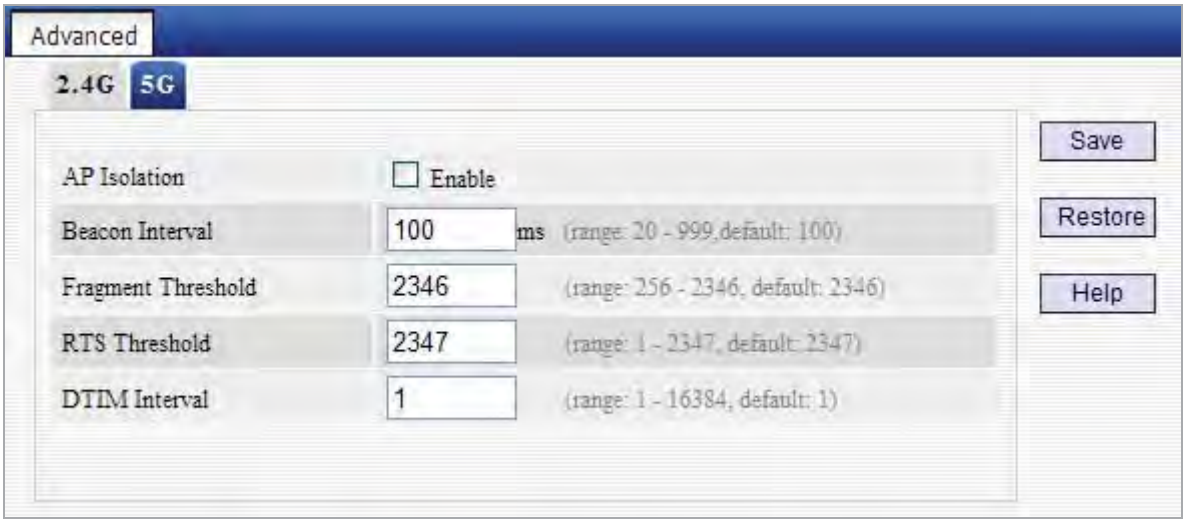


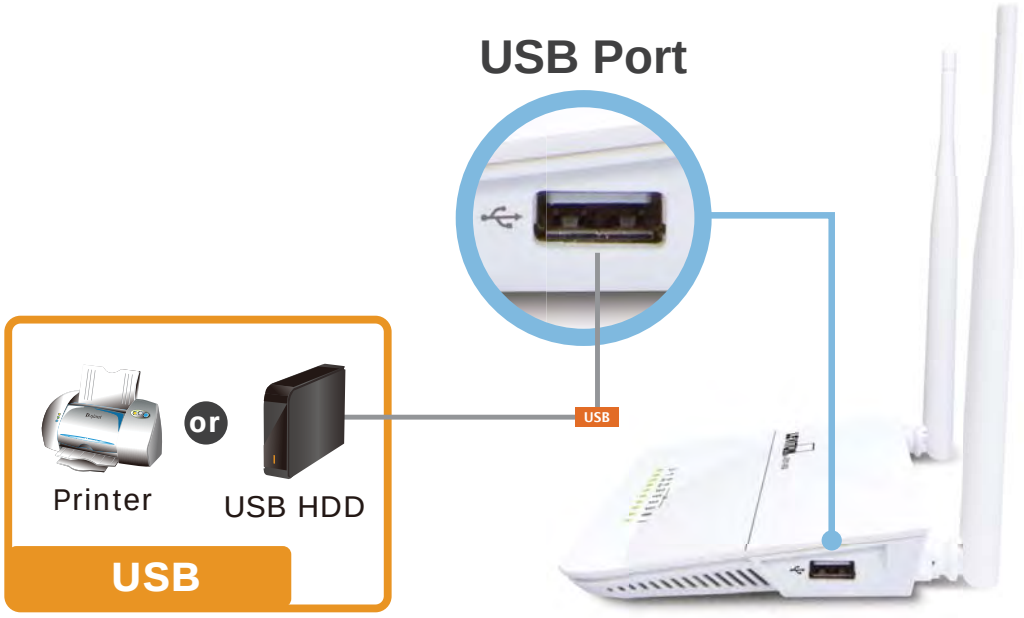
Figure 5-5-20

The page includes the following fields:

Object	Description
• **AP Isolation:**	Isolates clients connecting to the private SSID.
• **Beacon Interval:**	A time interval between any 2 consecutive Beacon packets sent by device. **Note:** Do NOT change the default value of 100 unless necessary.
• **Fragment Threshold:**	Enter a Fragment Threshold (256-2346). Any wireless packet exceeding such set value will be divided into several fragments. **Note:** DO NOT change the default value of 2346 unless necessary
• **RTS Threshold:**	If a packet exceeds such set value, RTS/CTS scheme will be used to reduce collisions. Set it to a smaller value provided that there are distant clients and interference. For normal SOHO, it is recommended to keep the default value unchanged; otherwise, device performance may be degraded
• **DTIM Interval:**	A time interval between any two consecutive broadcast and multicast packet messages sent by the device to clients. When such packets arrive at device's buffer, the device will send **DTIM (delivery traffic indication message)** and DTIM interval to wake clients up for receiving these packets.

5.6 USB Applications

47611-WG4 built-in with one USB 2.0 port can be connected to a **USB printer** or **storage for file sharing**.
It can auto recognized the USB printer or storage automatically without user experience. Thus all clients on the network can share printer or mass storage on 47611-WG4 without complicated network configuration. The USB port also output 5V DC power can charge any USB compliant devices.



* Sharing Printer and Mass Storage

5.6.1 USB Storage

Share a USB storage device with PC/Laptop on the local network of the 47611-WG4.
Insert a USB storage device, such as a flash drive or external hard drive, to the USB port on the right side of the 47611-WG4. The 47611-WG4 can automatically identify attached storage and load its root directory folder. Follow the directions below for your operating system.

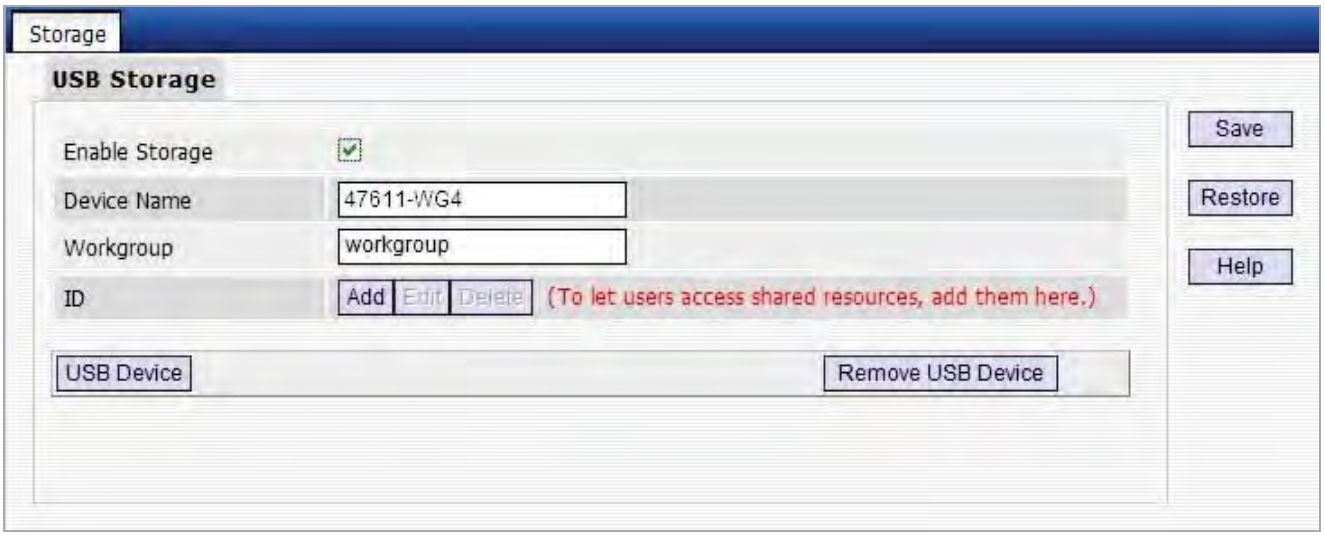


Figure 5-6-1

The page includes the following fields:

Object	Description
• **Enable:**	Check/uncheck to enable/disable file sharing feature.
• **Device Name:**	Define a meaningful name to you for the device.
• **Work Group:**	Define a work group name for the device.
• **Add:**	Click to add an account. Up to 5 accounts can be added.
• **Edit:**	Click to edit an existing account.
• **Delete:**	Click to delete an existing account.

Note: Up to 5 users are allowed for server sharing.

Operation Instructions:

Step 1. Create an account.

1). Click "**Add**" to display a dialogue box below:

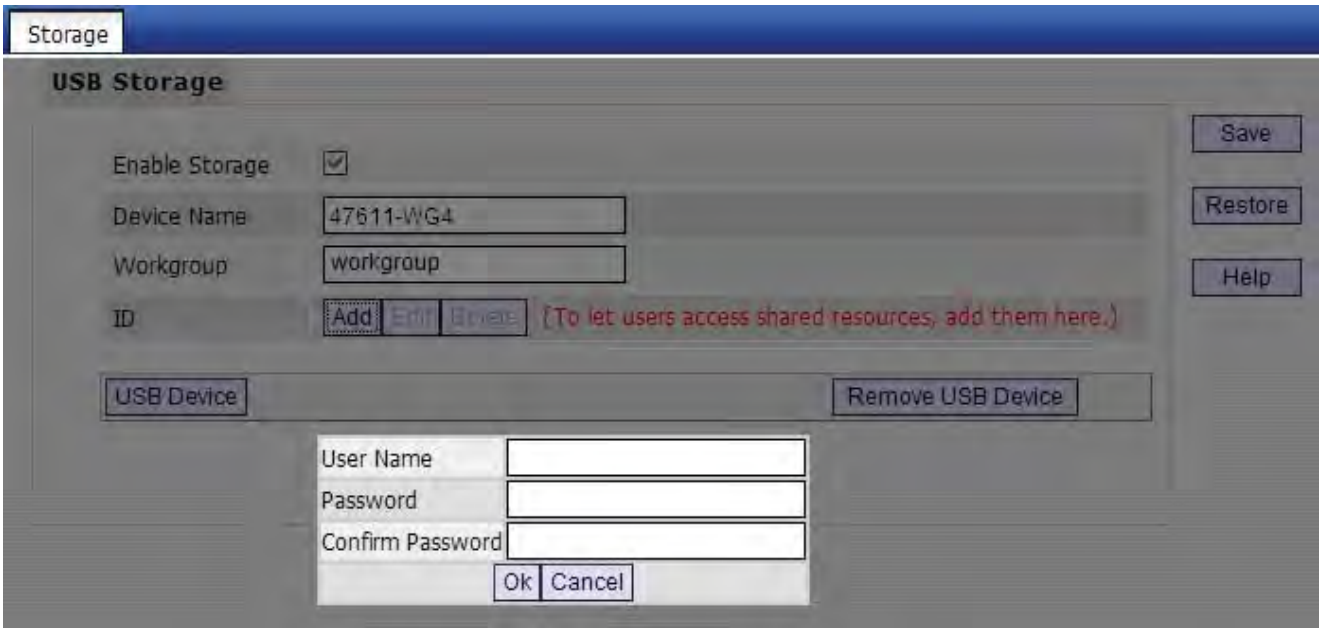


Figure 5-6-2

2) Enter a user name and a password, which will be used by clients when accessing the USB storage device for sharing files thereon.

3) Re-type to confirm password and then click the "OK" button.

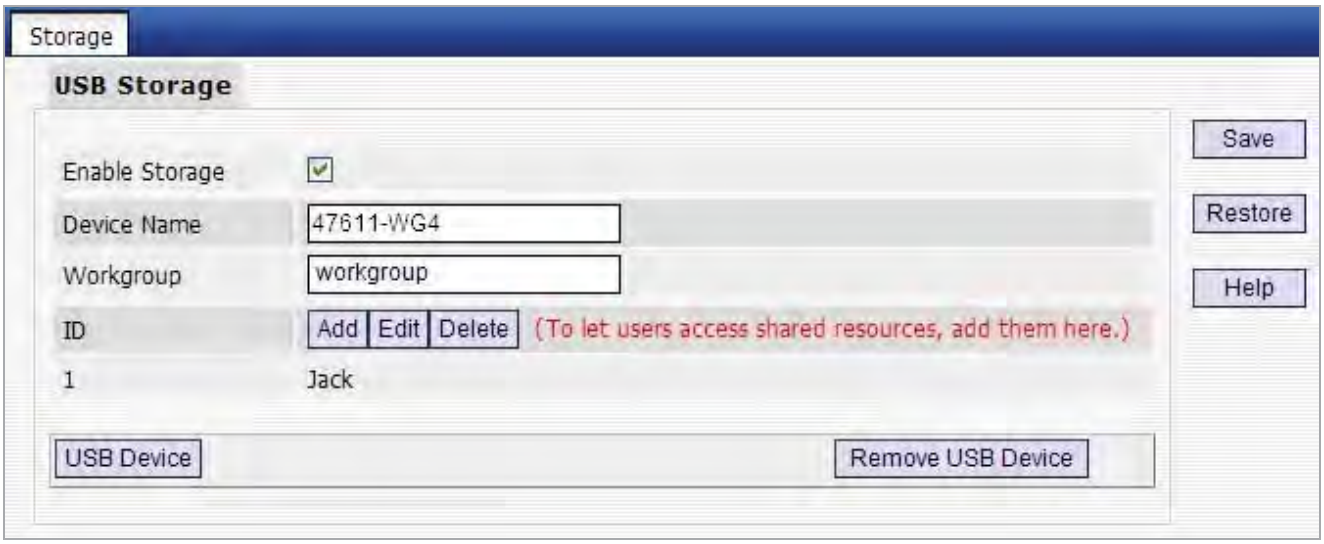


Figure 5-6-3

Step 2. Set Access Right

First select an account and click USB Device. And then select a proper access right from below for each entry. Access authority is classified into three levels: R/W, R, and N.

Figure 5-6-4

R/W:	Read and Write right.
R:	Read right.
N:	No right.

At last click "**Save**" to apply your settings.

Step 3. Access shared file

To access resources on such storage device, double click "**My Computer**" on your PC and enter \\192.168.0.1.

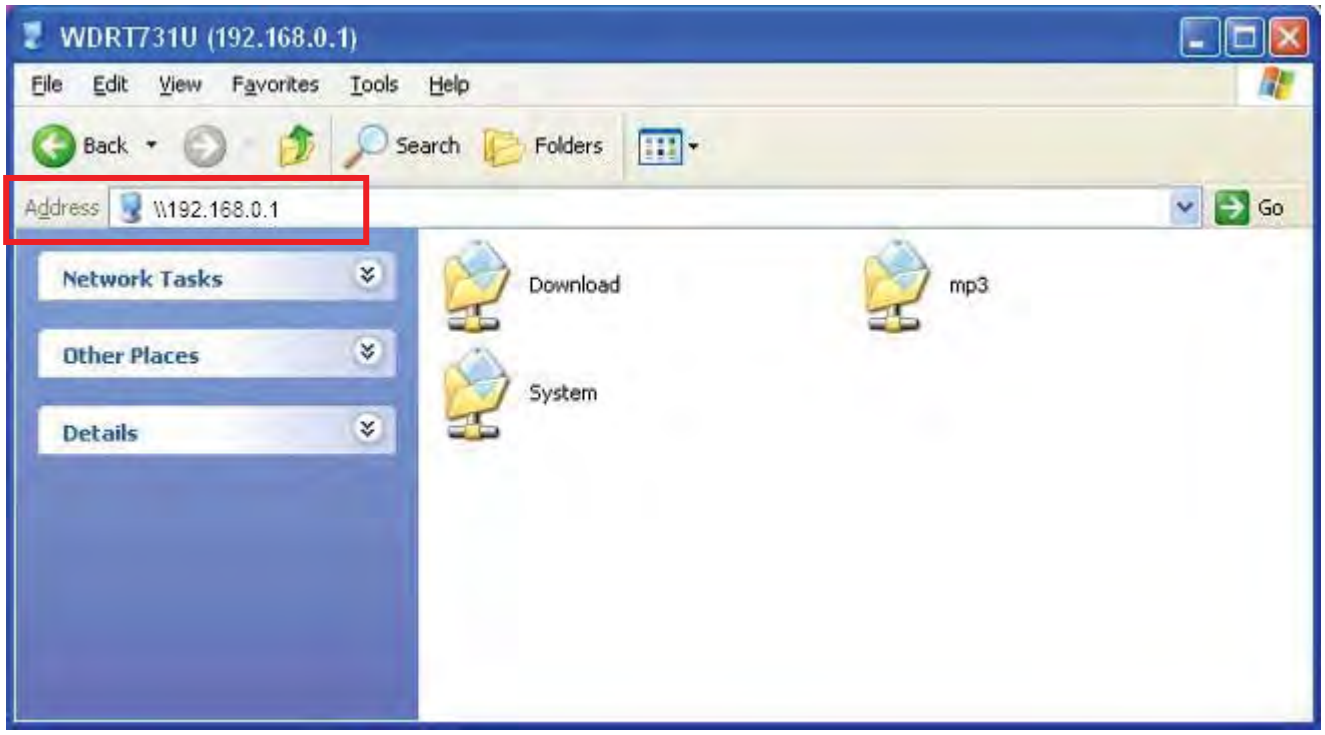


Figure 5-6-5

5.6.2 Printing Service

The USB printer service allows you to connect a USB printer to the device and thus all clients on your network can print anything they want on their PCs. The device can identify a printer automatically as long as it is successfully connected.

Figure 5-6-6

The page includes the following fields:

Object	Description
• **Enable Printer:**	Check/uncheck to enable/disable USB printer service.

1. GDI interface printers are not supported.
2. Multifunction printers are not supported.

Operation Instructions

Step 1. Correctly connect your USB printer to the USB port on the device.

Figure 5-6-7

Step 2. Enable printer service.

The printer will be detected automatically and the printer's information will be shown.

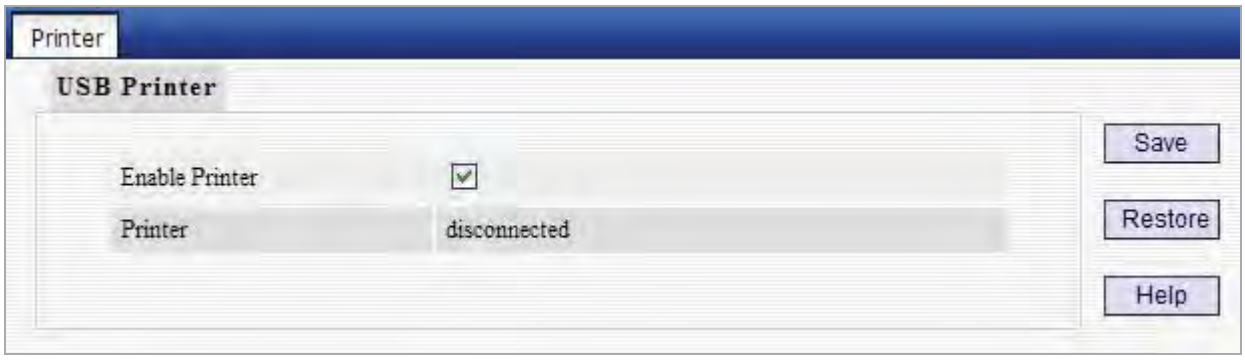


Figure 5-6-8

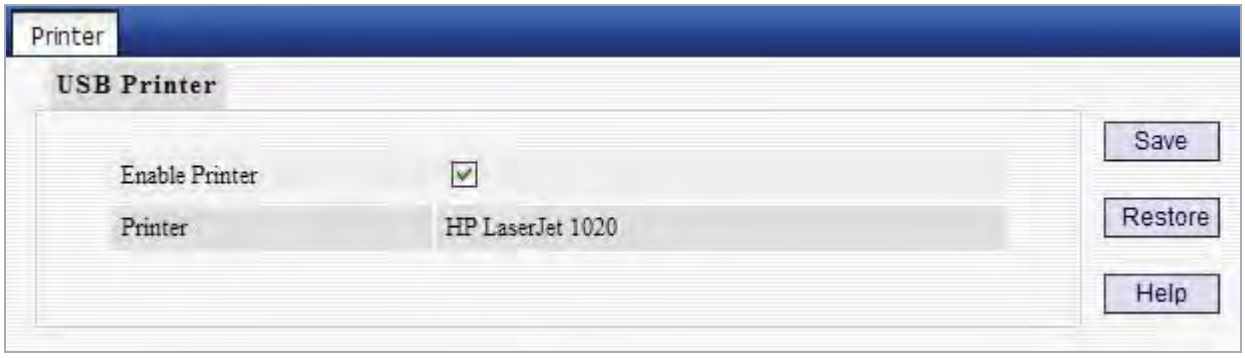


Figure 5-6-9

■ Windows XP Users

The following steps apply to Windows XP.

Step 3. On your PC (connected to the device), click "Start"——"Settings"——"Printers and Faxes"

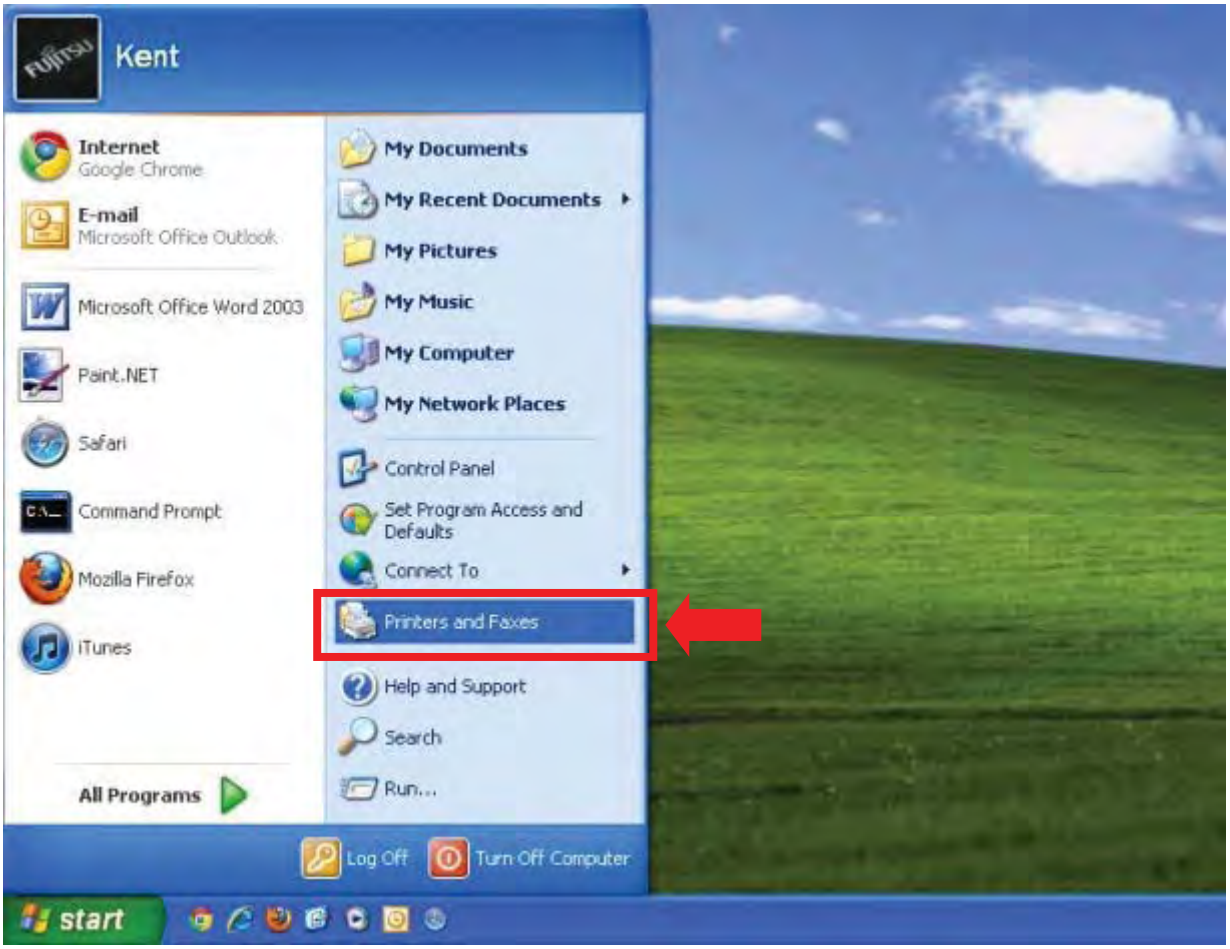

Kent
Internet
Google Chrome
E-mail
Microsoft Office Outlook
Microsoft Office Word 2003
Paint.NET
Safari
Command Prompt
Mozilla Firefox
iTunes
All Programs
My Documents
My Recent Documents
My Pictures
My Music
My Computer
My Network Places
Control Panel
Set Program Access and Defaults
Connect To
Printers and Faxes
Help and Support
Search
Run...
Log Off
Turn Off Computer
start

Figure 5-6-10

Step 4. Select "Add a printer" on appearing window.

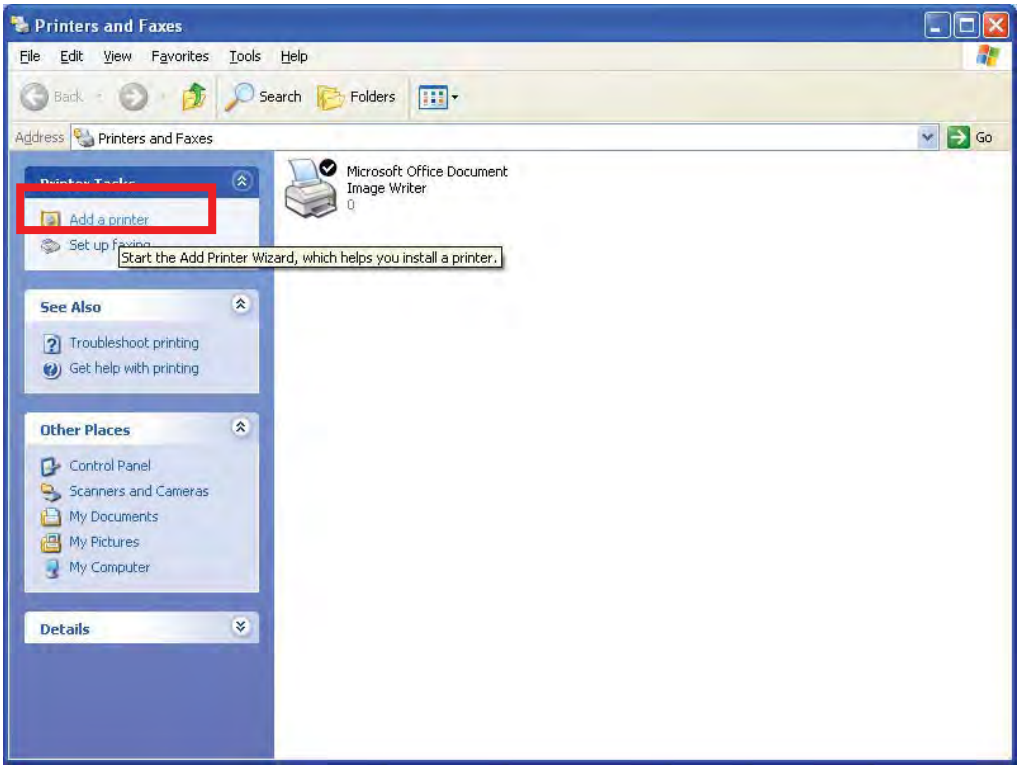


Figure 5-6-11

Step 5. Click "Next".

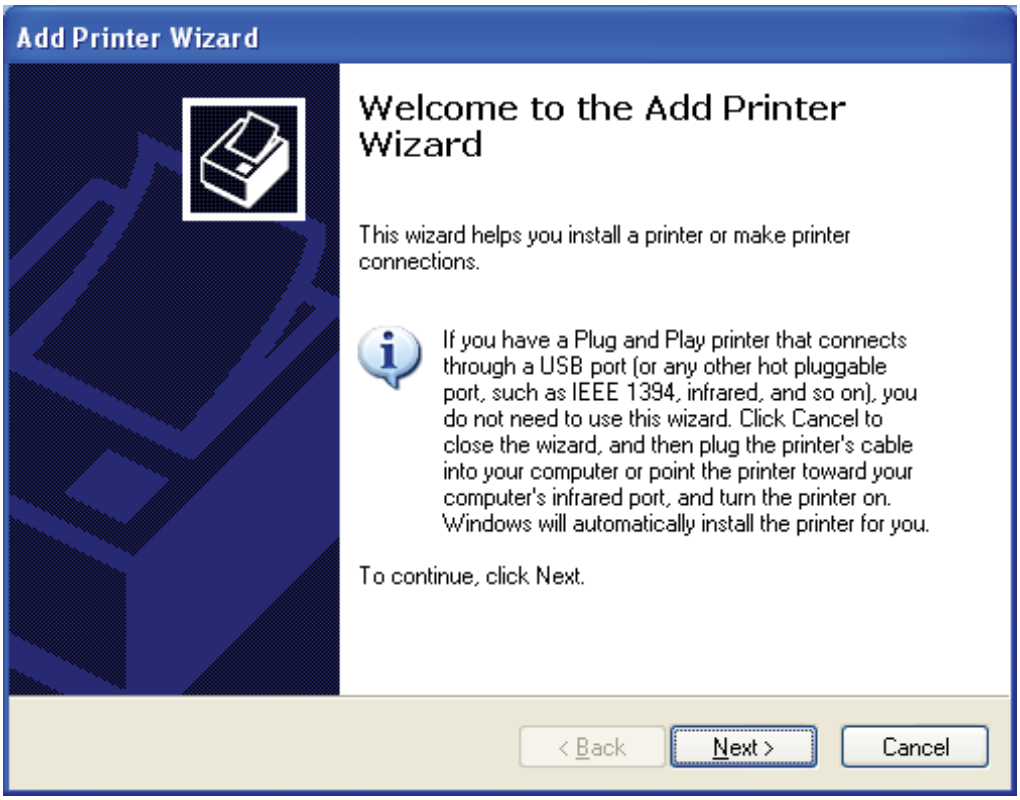


Figure 5-6-12

Step 6. Select “Local printer attached to this computer” and click “”Next.

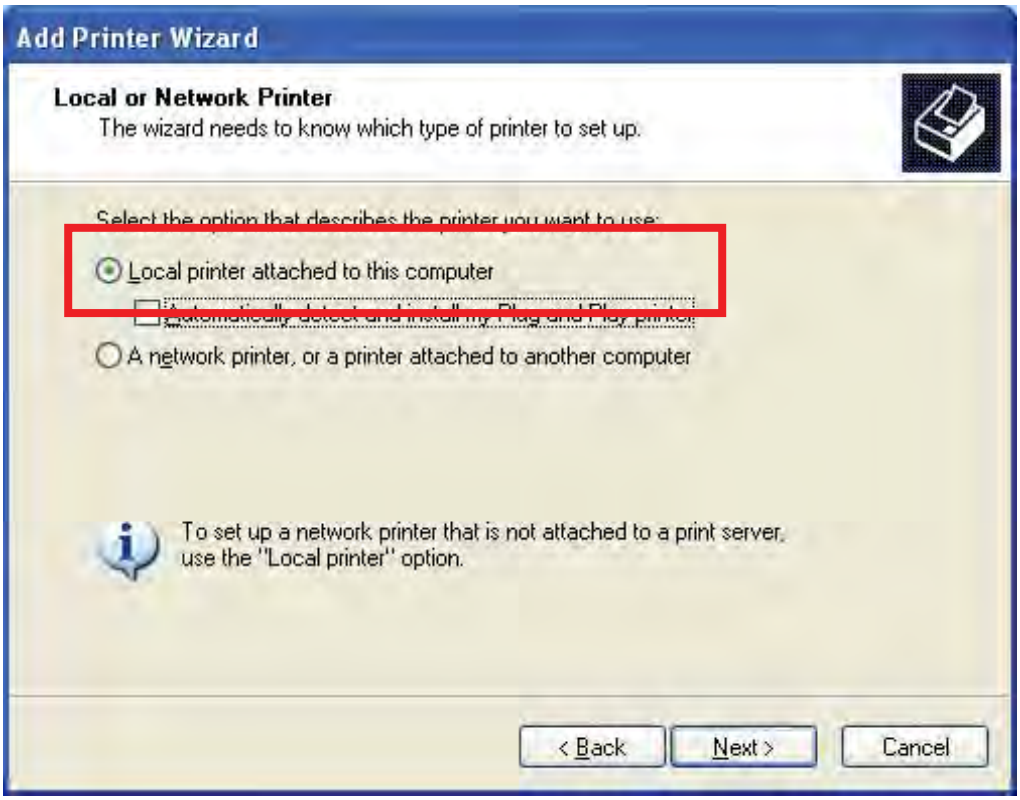


Figure 5-6-13

Step 7. Select “Create a new port”, Type of port: “Standard TCP/IP Port” and click “Next”.

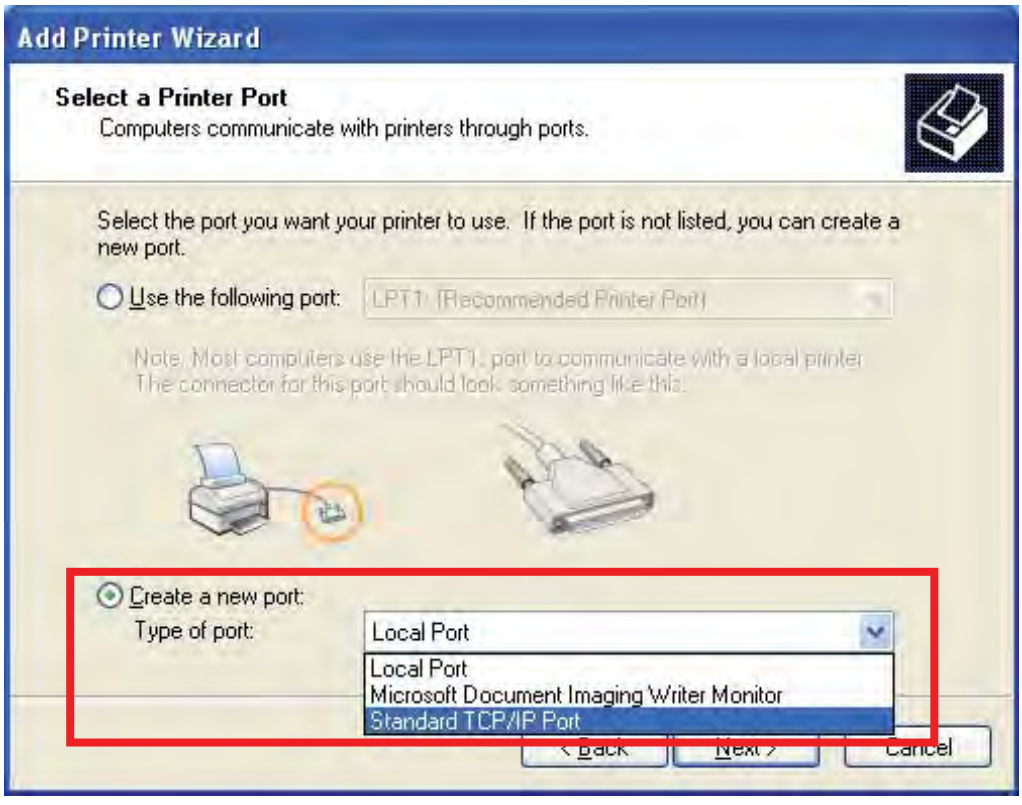


Figure 5-6-14

Step 8. Click "Next".

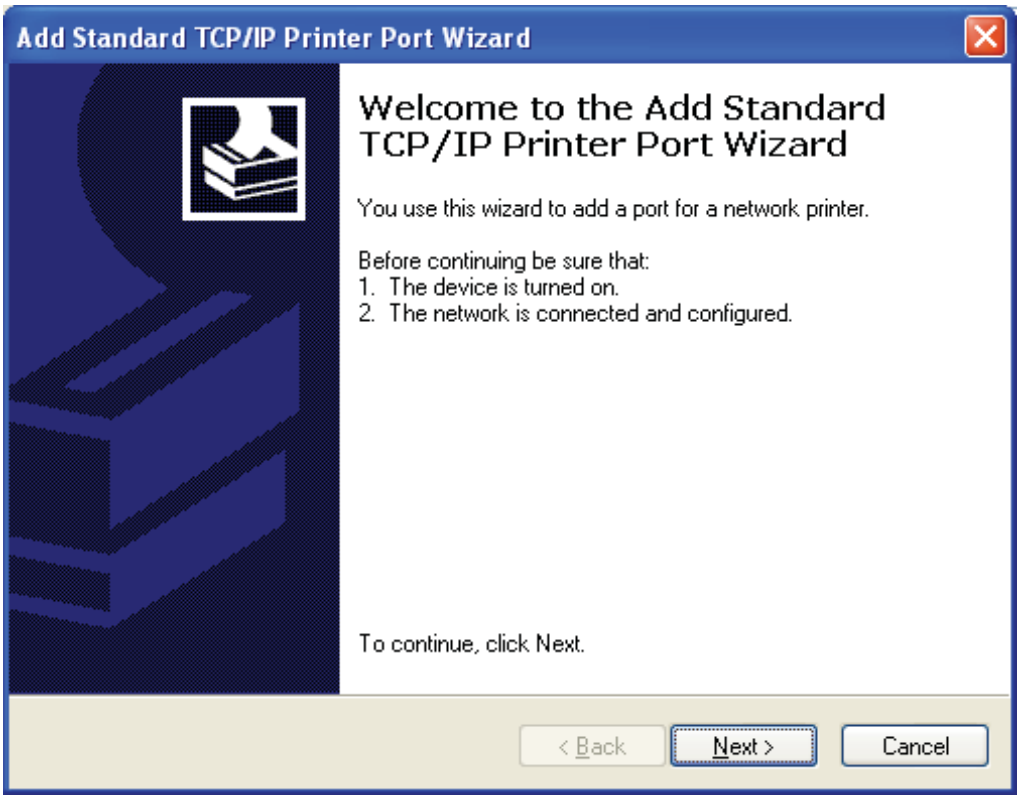


Figure 5-6-15

Step 9. Enter device's LAN IP address and click "Next". (The default IP address of 47611-WG4 is 192.168.0.1)

Figure 5-6-16

Step 10. Click “Standard” under Device Type and select “Generic Network Card”, then click “Next”.

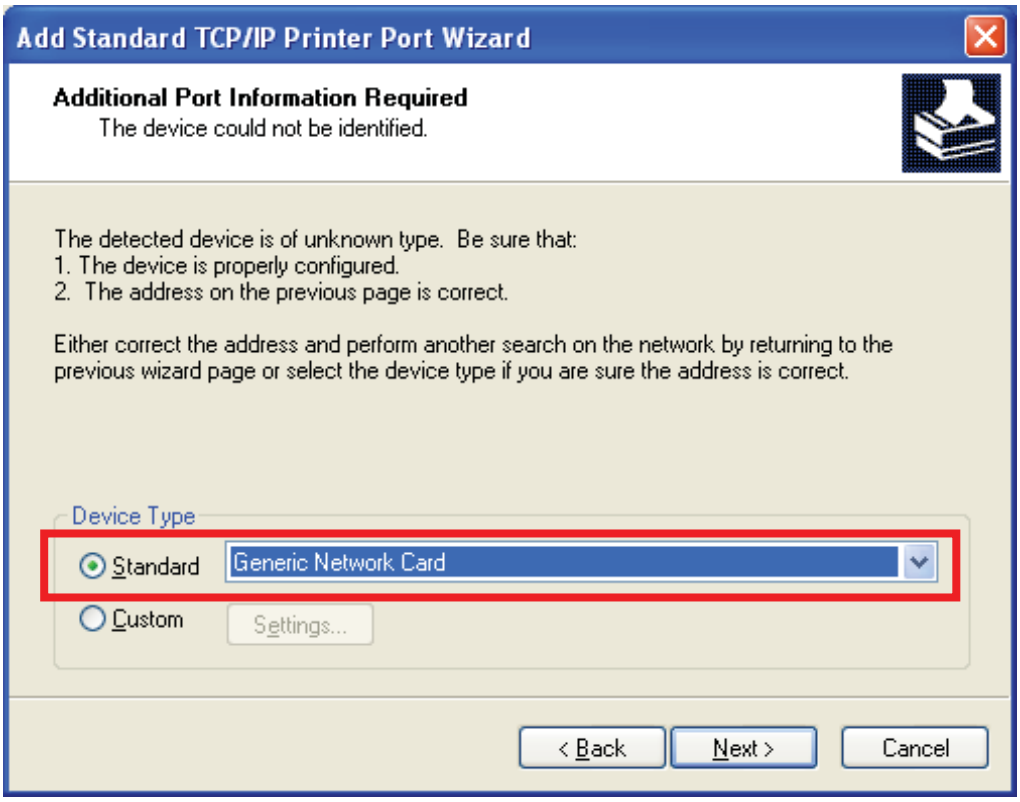


Figure 5-6-17

Step 11. Click “Finish”.

Figure 5-6-18

Step 12. Select "Have Disk".

Select a suitable printer manufacturer and the printer model and click "**Next**". If your printer is not in the list, click "**Have Disk…**" to install the driver of the printer.

Figure 5-6-19

Step 13. Click "Browse", select corresponding drive file and click "Open". At last click "OK".

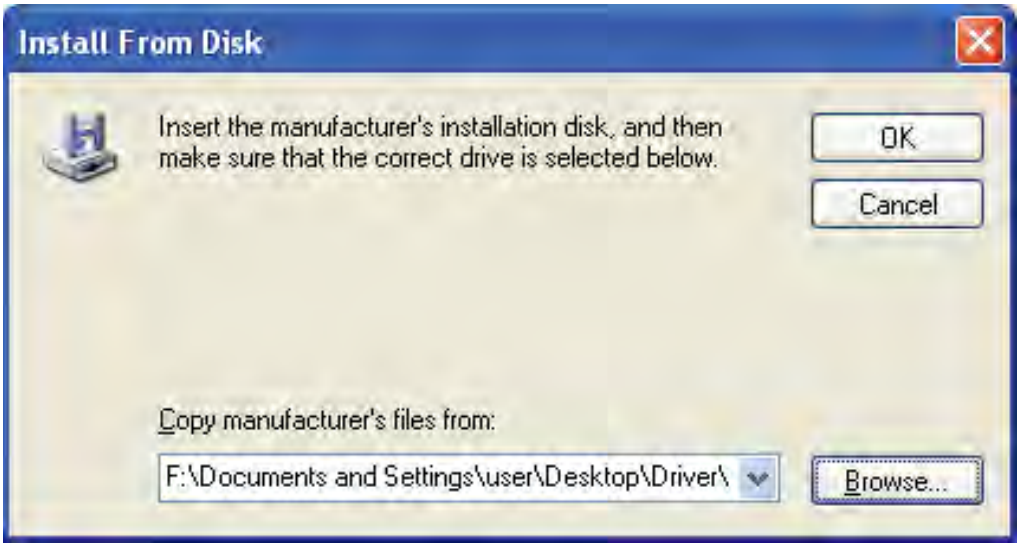


Figure 5-6-20

Step 14. Click “Next”.

After installation, the printer model will be added to the list.

Figure 5-6-21

Step 15. Define a name for the printer and click “Next”.

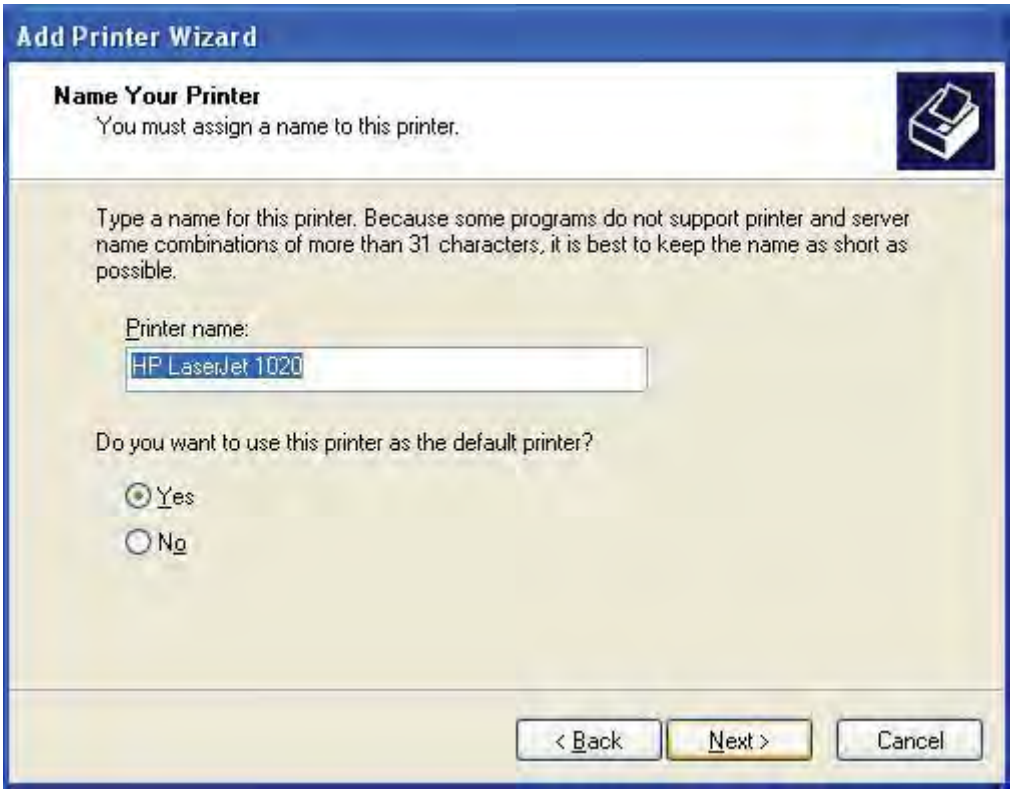


Figure 5-6-22

Step 16. Click “Finish".

Now you have added the network printer to the Windows XP PC successfully. The information of the printer is displayed in the following windows.

Figure 5-6-23

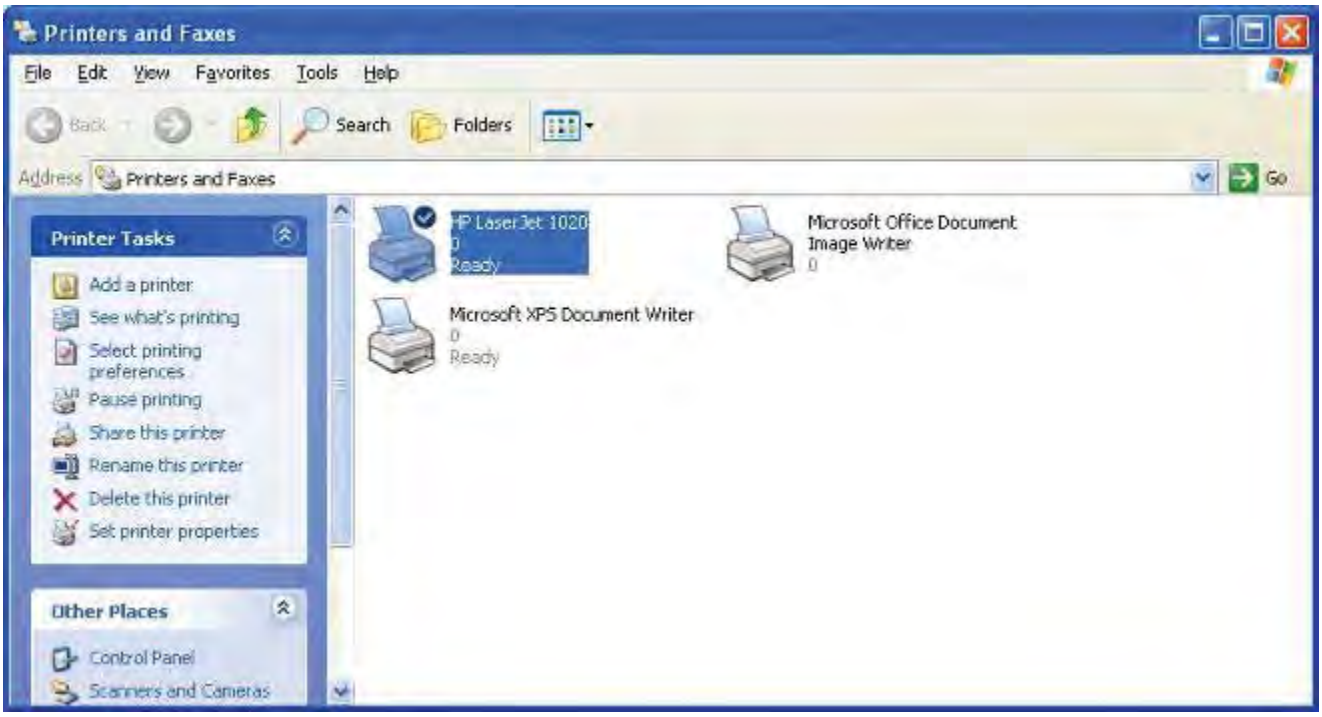


Figure 5-6-24

■ Windows 7 Users

The following steps apply to Windows 7.

Step 3. On your Windows 7 PC (connected to the device), click "**Start**"——"**Device and Printer**" and select "**Add a printer"** on appearing window.

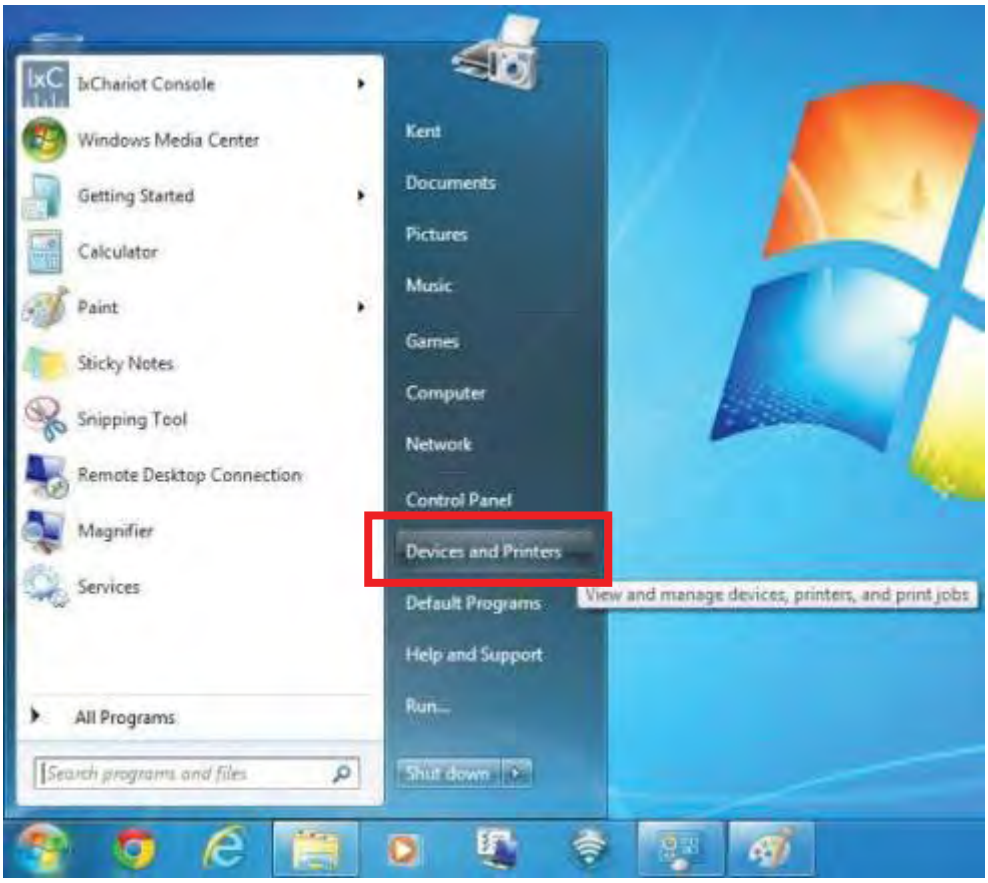


Figure 5-6-25

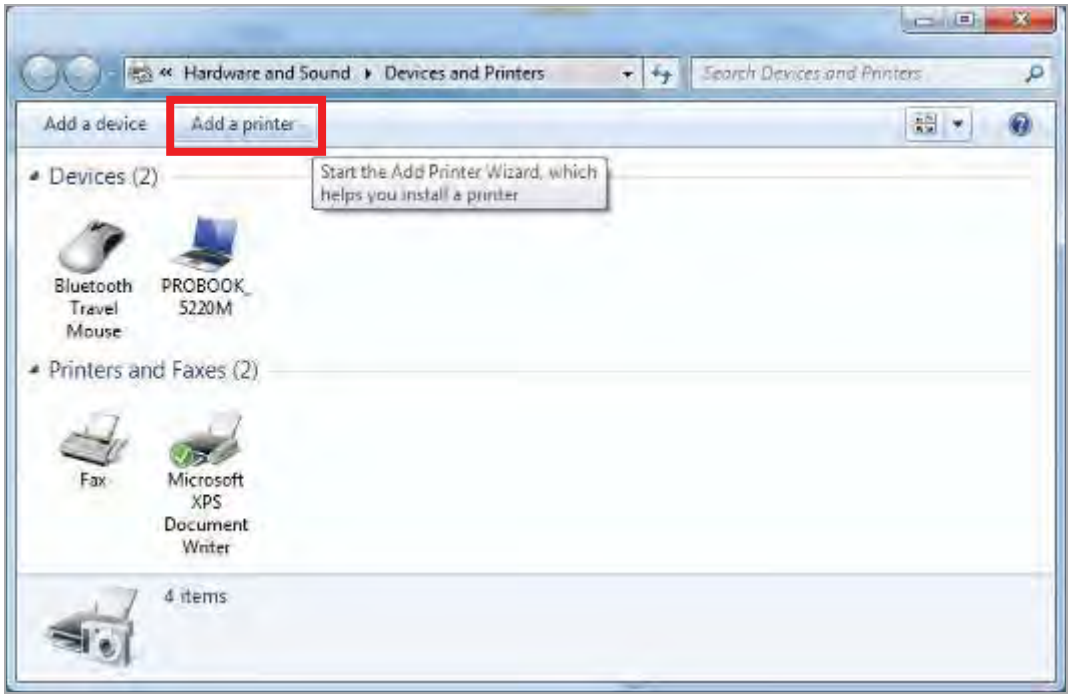


Figure 5-6-26

Step 4. Click "**Next**".

Step 5. Select "**Add a Local Printer**" and click ""Next.

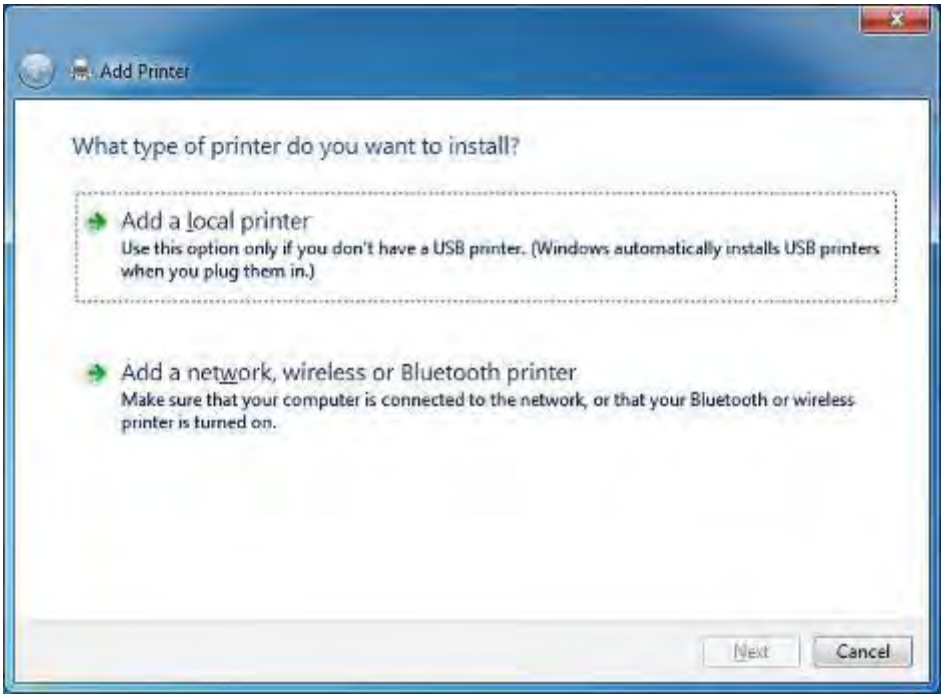


Figure 5-6-27

Step 6. Select "**Create a new port**", Type of port: "**Standard TCP/IP Port**" and click "**Next**".

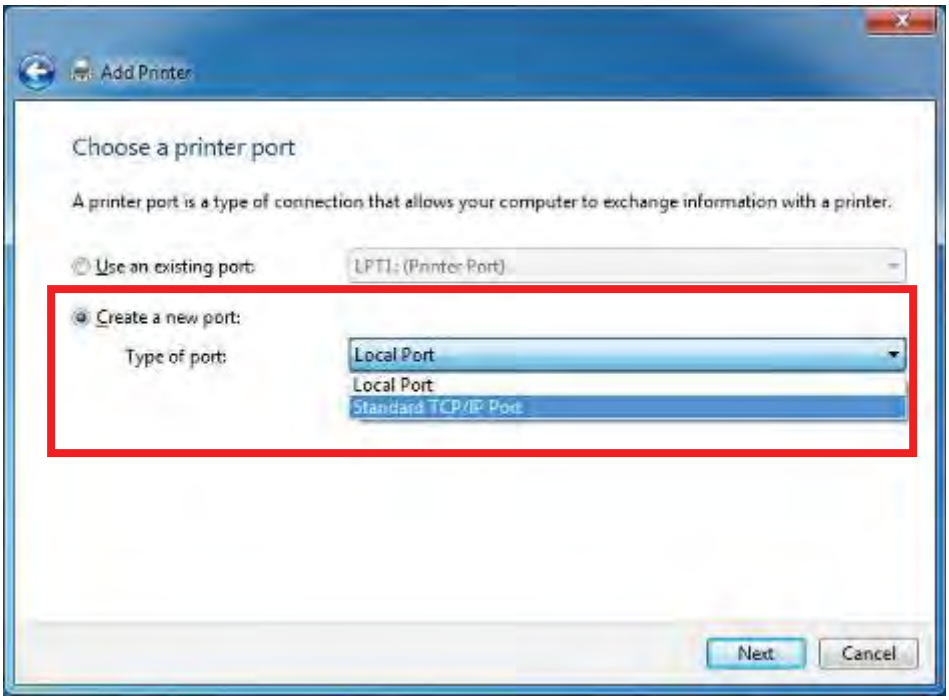


Figure 5-6-28

Step 7. Enter your 47611-WG4's LAN IP address and click "Next".

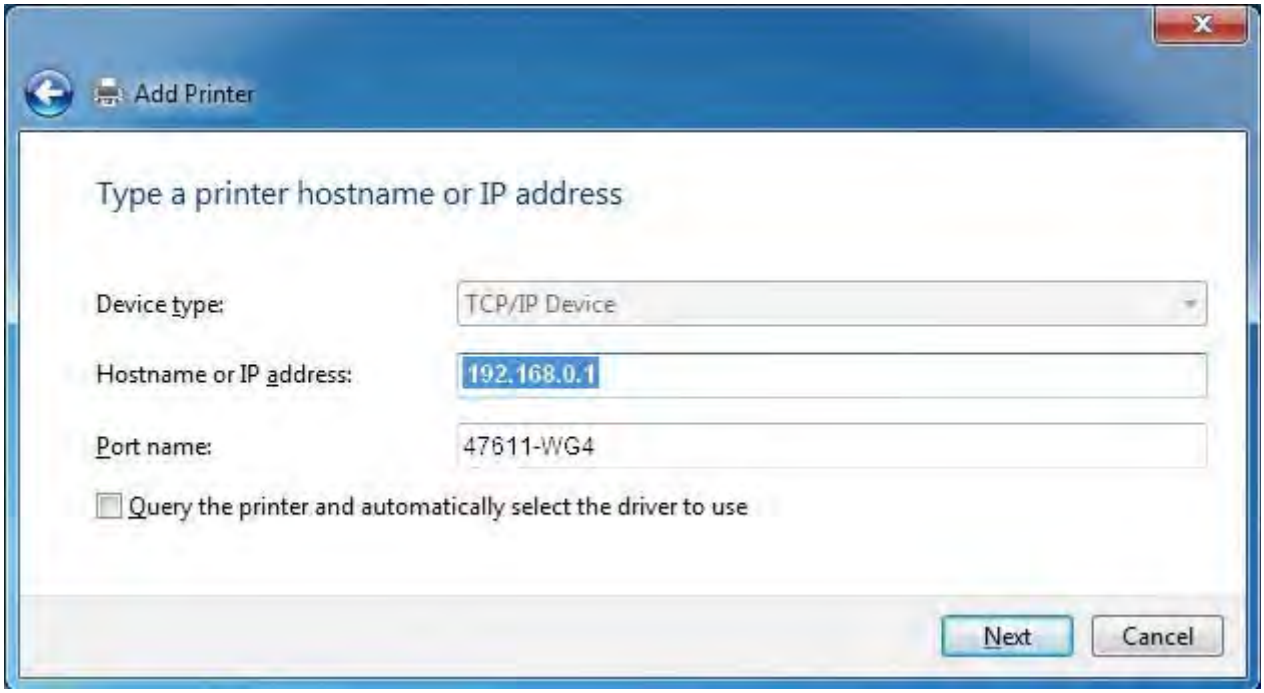


Figure 5-6-29

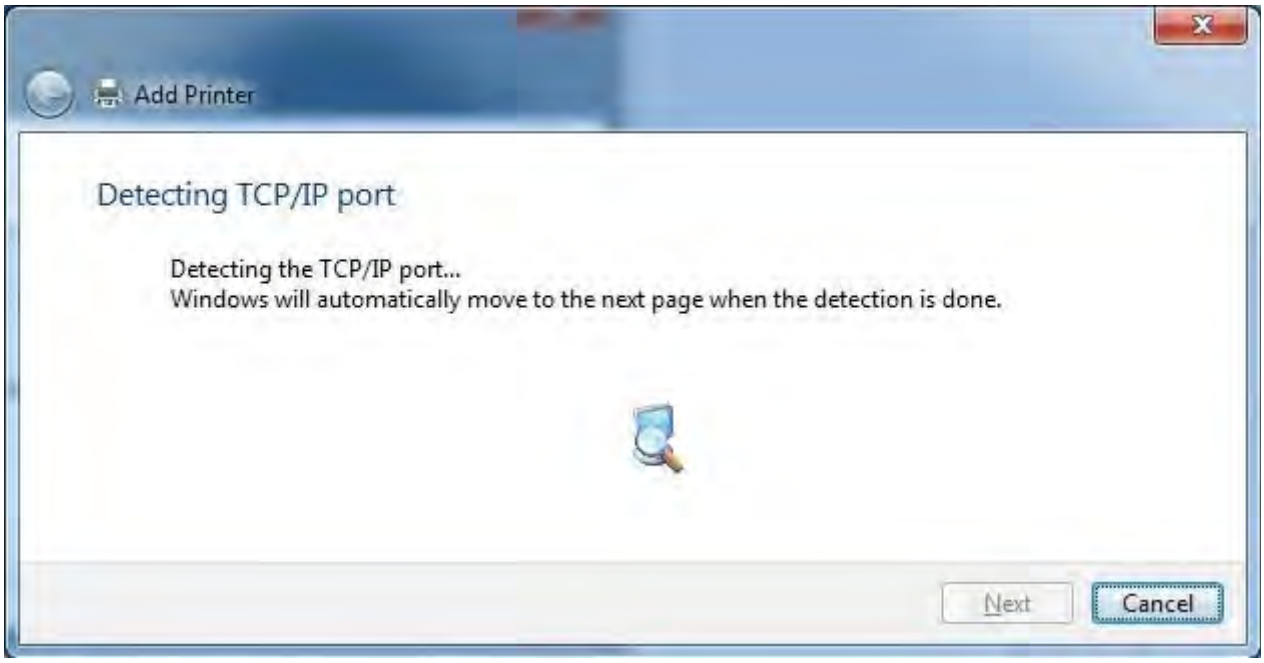


Figure 5-6-30

Step 8. Click "**Standard**" under Device Type and select "**Generic Network Card**", then click "**Next**".

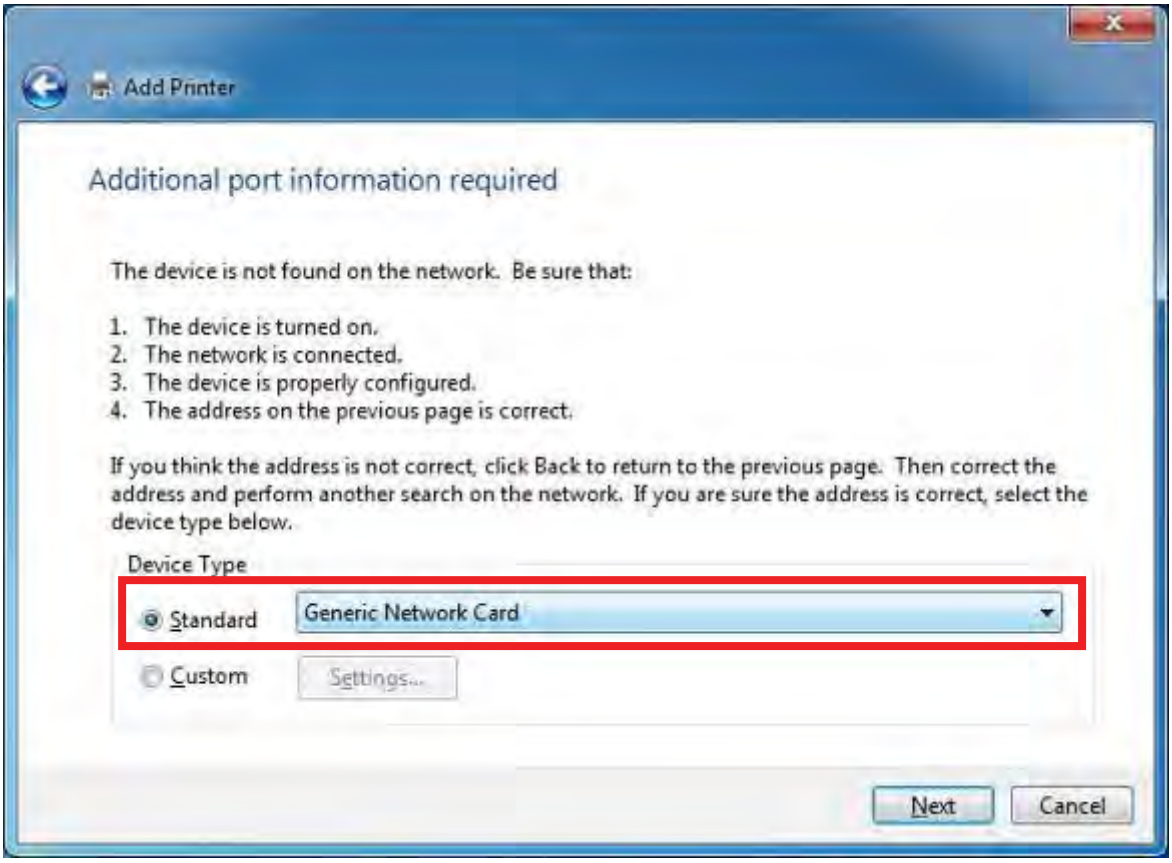


Figure 5-6-31

Step 9. Select "**Have Disk**".

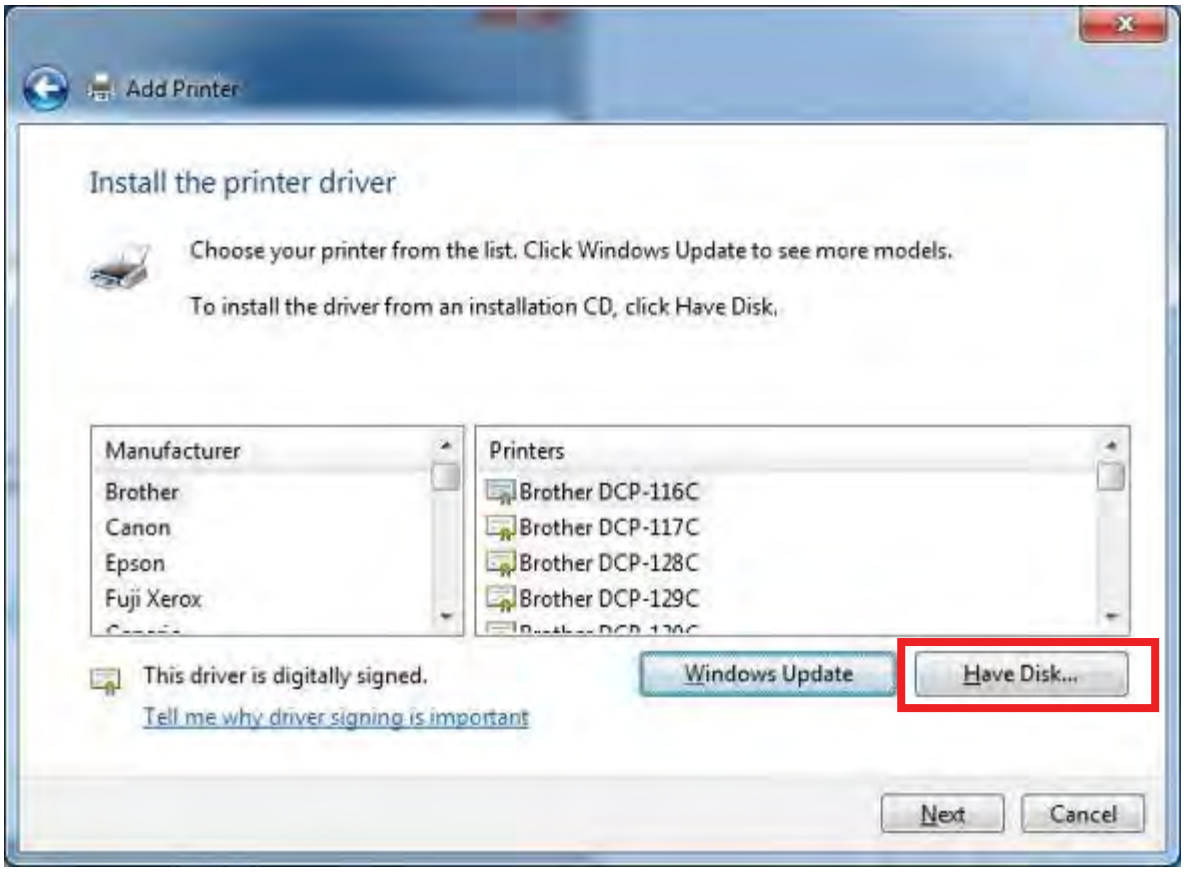


Figure 5-6-32

Step 10. Click “**Browse**”, select corresponding drive file and click “Open”. At last click “OK”.

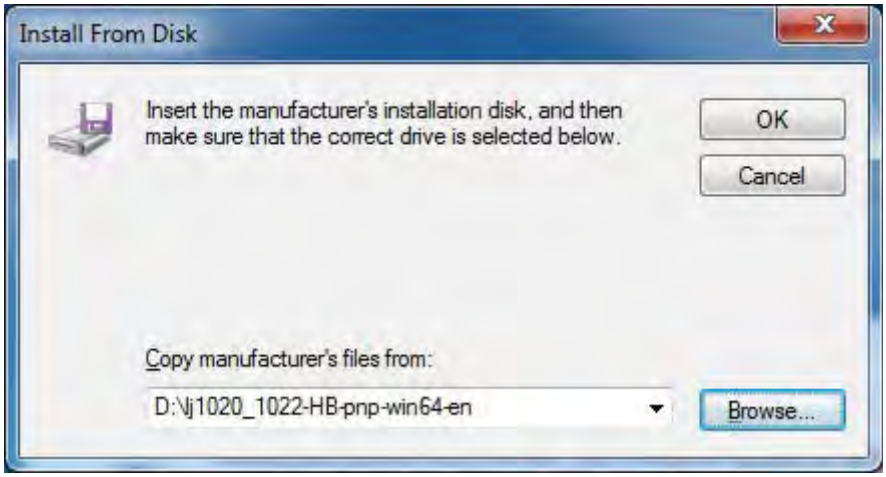


Figure 5-6-33

Step 11. Click “**Next**”.

After installation, the printer model will be added to the list. Choose the right printer and click “Next”.

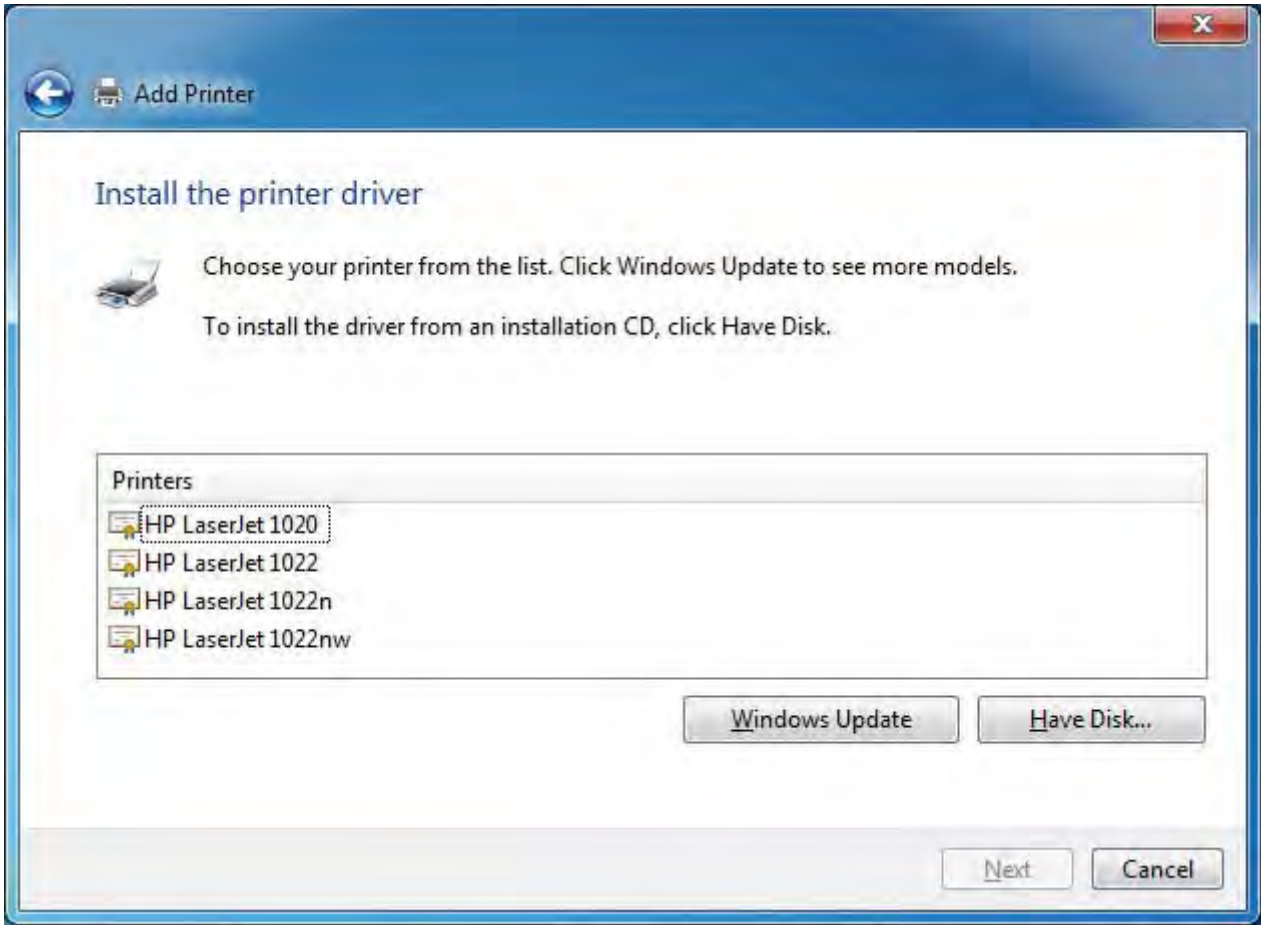


Figure 5-6-34

Step 12. Define a name for the printer and click "**Next**".

Figure 5-6-35

Step 13. You can choose to share the printer or not. Then click "**Next**".

Figure 5-6-36

Step 14. After installing the correct printer driver, the windows wizard shows the model name of the new network printer. You can choose to print a test page or click “Finish” to exit the wizard.

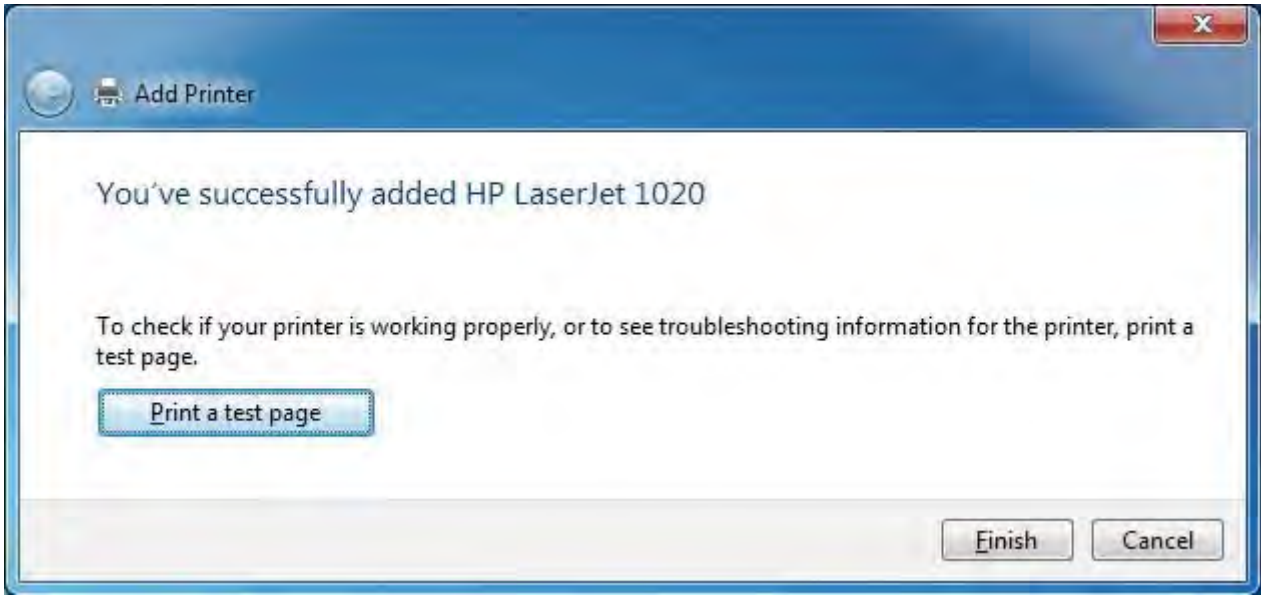


Figure 5-6-37

The new network printer that attached to the 47611-WG4 is now available for printing.

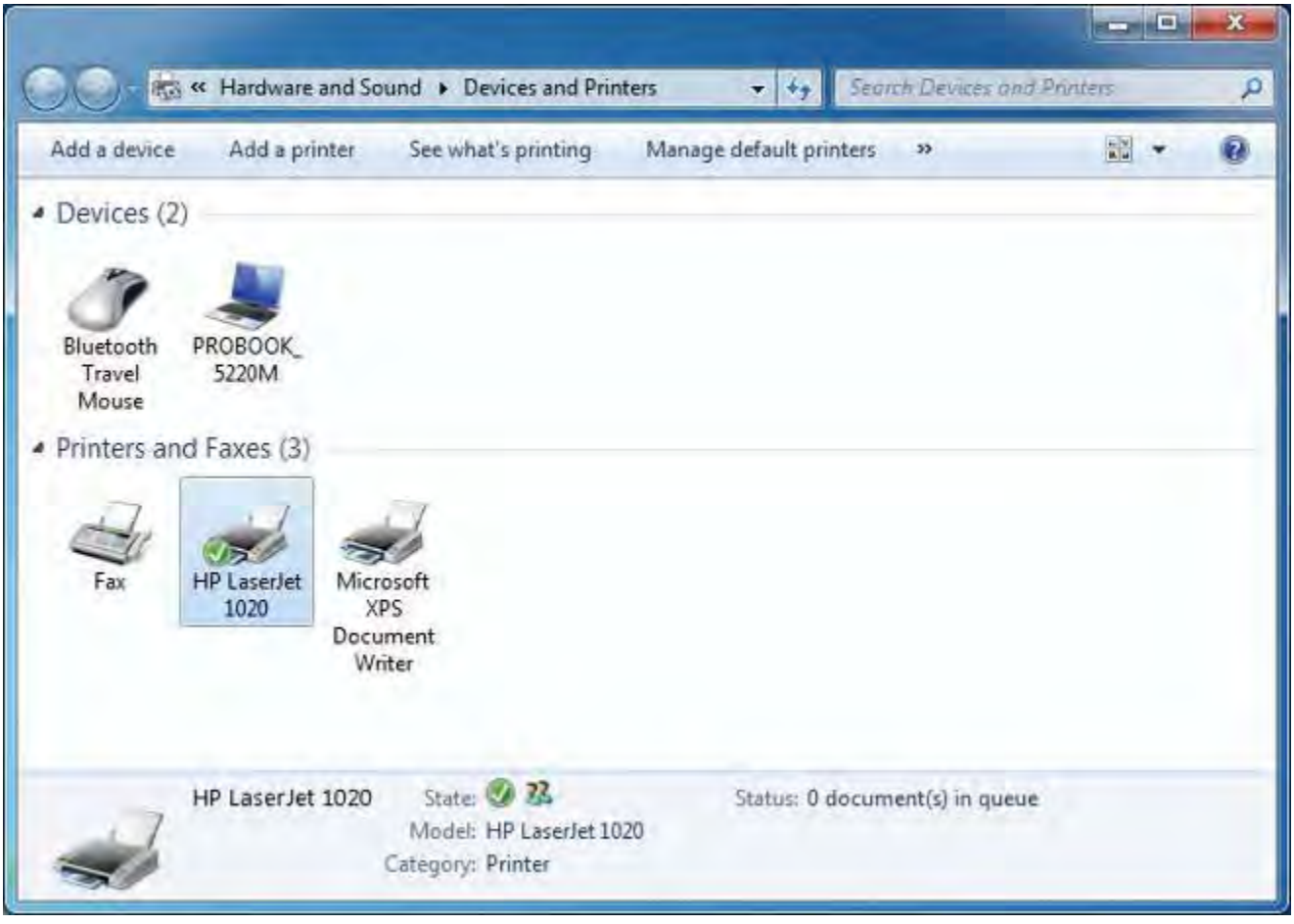
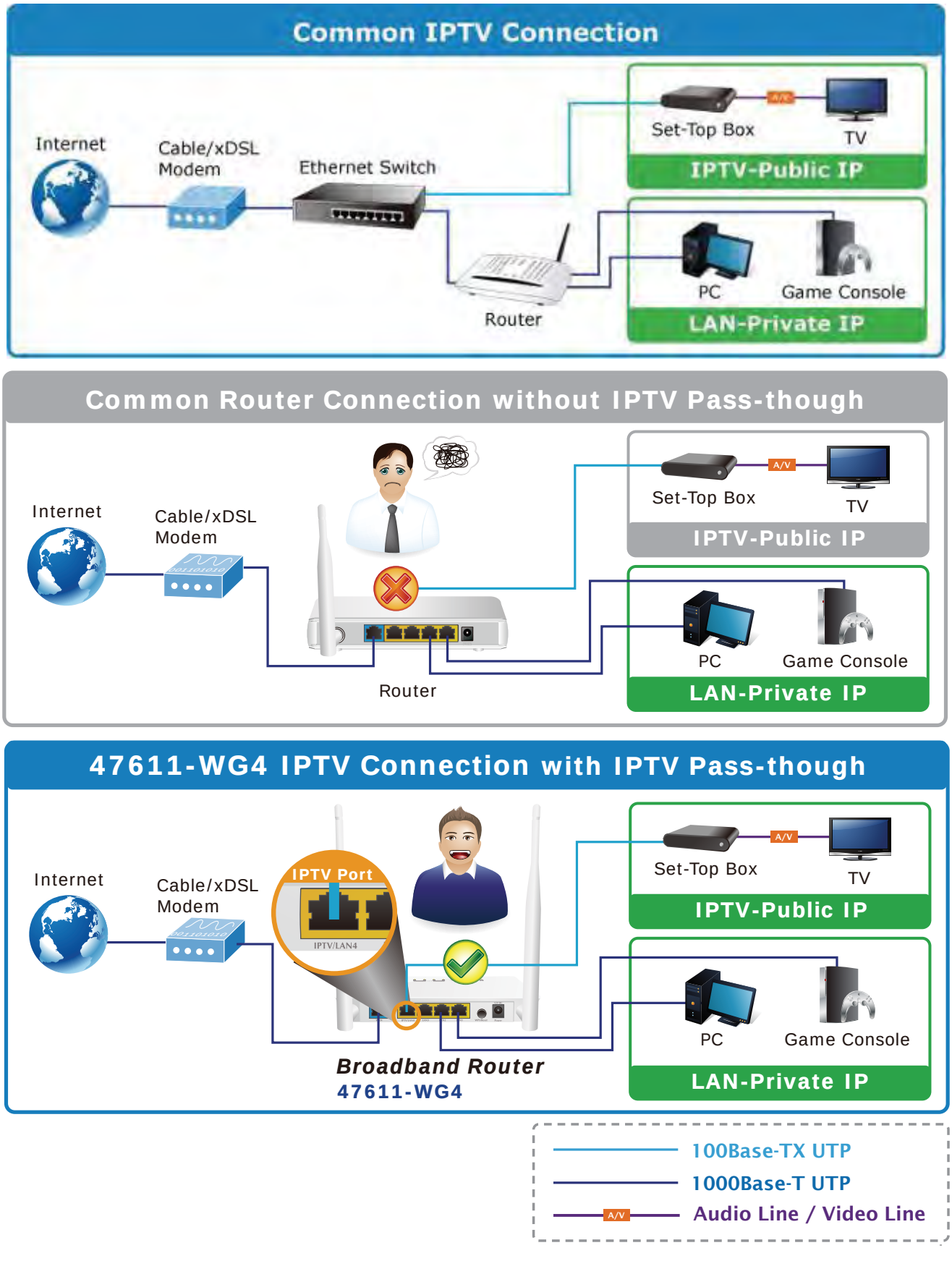


Figure 5-6-39

5.7 IPTV Settings

The IPTV feature makes it possible to enjoy online videos on your TV set via a set-top box while surfing Internet. See below for the topology:



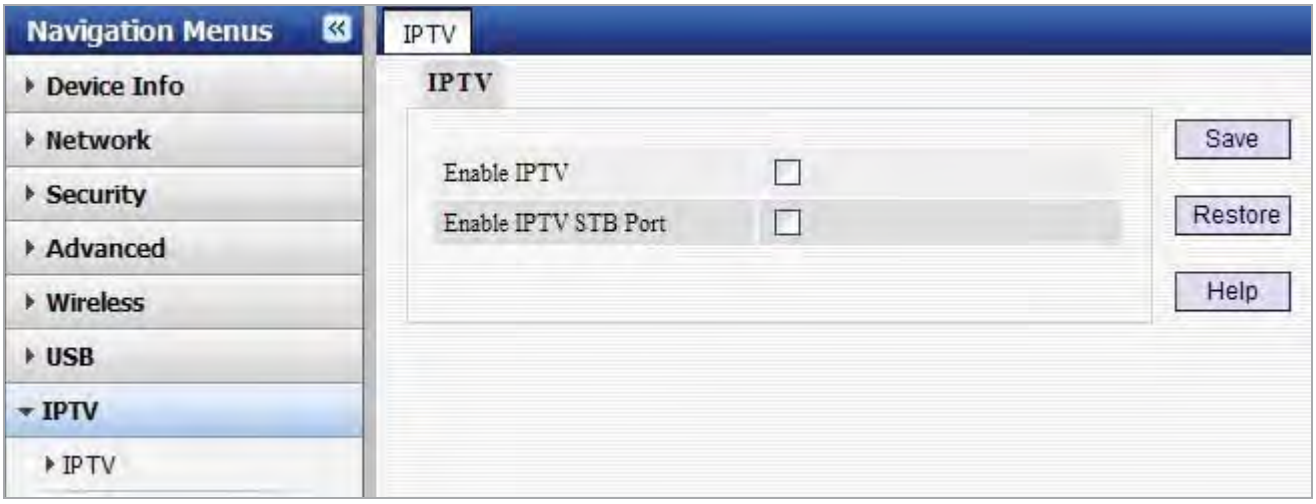


Figure 5-7-1

The page includes the following fields:

Object	Description
• **Enable IPTV:**	Check/uncheck to enable/disable the IPTV feature.
• **Enable IPTV STB Port:**	Check/uncheck to enable/disable the IPTV-specific port.

Note:

1. If you enabled both options mentioned above, then note below:

   (a). Set IPTV connection type to DHCP/dynamic IP or static IP if the set-top box is connected to any LAN port from 1-3.

   (b). Select the dial mode provided by your ISP if the set-top box is connected to the IPTV-specific port.

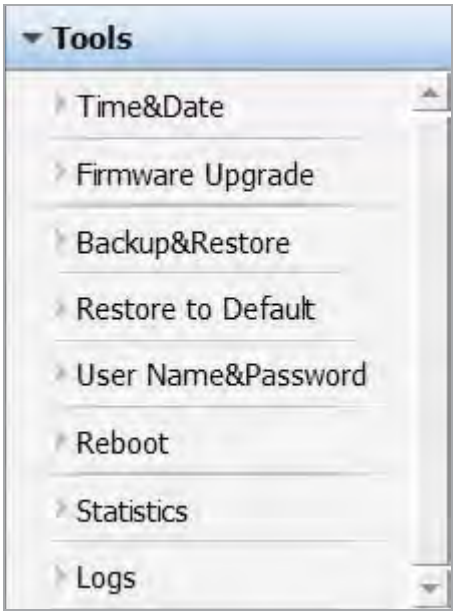
IMPORTANT	Note that the IP address of the set-top-box or smart TV should be on the same IP net segment as router's WAN IP.

2. After the IPTV port is set for IPTV purpose, PC that connects to such port will not be able to obtain an IP address or access Internet. So think twice before you start. Plus, LAN ports1-3 can only be used to connect PCs instead of an IPTV set-top box.

3. The IPTV feature does not support wireless access.

5.8 Tools

System tools include the following 8 submenus. Clicking any of them enters corresponding interface for configuration. Below explains, in details, each such feature.



5.8.1 Time Settings

This section assists you in setting the device's system time; you can either select to set the time and date manually or automatically obtain the GMT time from Internet.

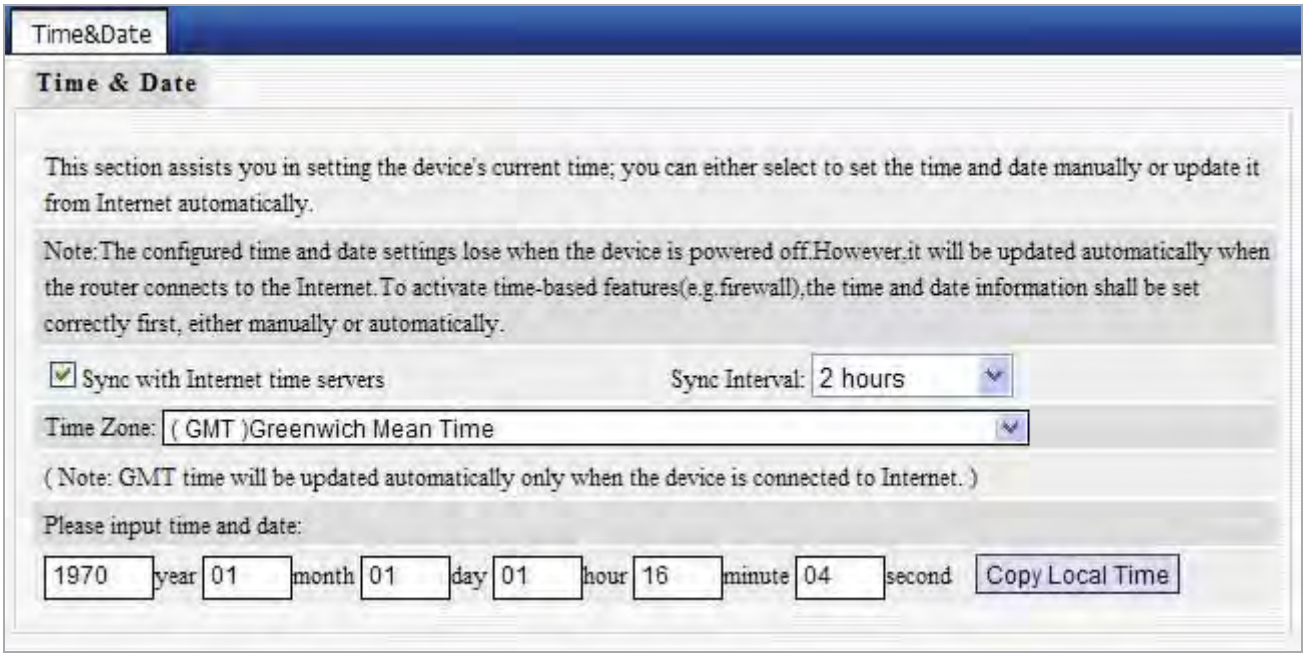


Figure 5-8-1

The page includes the following fields:

Object	Description
• **Sync with Internet time servers:**	Time and date will be updated automatically from Internet.
• **Sync Interval:**	Determines a time length when device periodically updates its time and date info from Internet. The default is 2 hours.
• **Time Zone:**	Select your current time zone.
• **Copy Local Time:**	Click it to copy your PC's time to the device.

5.8.2 Firmware Upgrade

Firmware upgrade is released periodically to improve the functionality of your device and also to add new features. If you run into a problem with a specific feature of the device, log on to our website www.leviton.com to download the latest firmware to update your device.

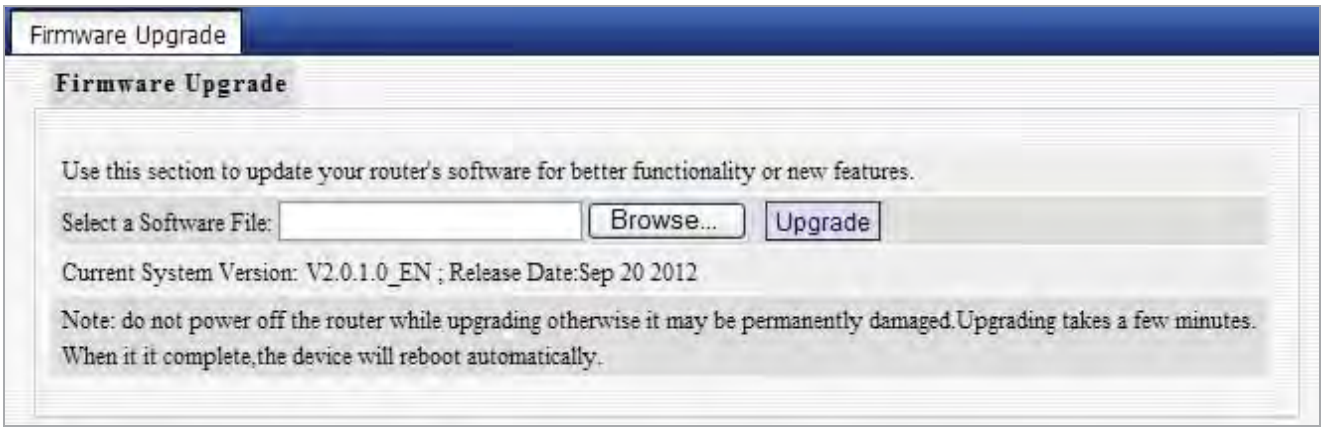


Figure 5-8-2

To update firmware, do as follows:

1. Click "**Browse**" to locate the firmware and "**Upgrade**" to update.
2. Router will reboot automatically when upgrade completes.

Note

Do not disconnect the device from your management PC (the PC you use to configure the device) or power off it during the upgrade process; otherwise, it may be permanently damaged. The device will restart automatically when the upgrade process, which takes several minutes, completes.

5.8.3 Backup/Restore Settings

This section allows you to backup current settings or to restore the previous settings configured on the device.

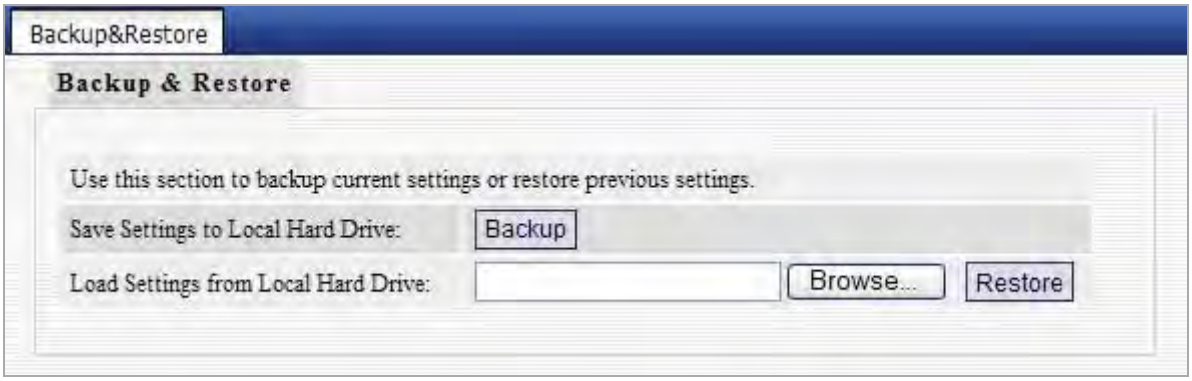


Figure 5-8-3

The page includes the following fields:

Object	Description
• **Backup Settings:**	Once you have configured the device the way you want it, you can save these settings to a configuration file on your local hard drive that can later be imported to your device in case that the device is restored to factory default settings. To do this, click the "**Backup**" button and specify a directory to save settings on your local hardware.
• **Restore Settings:**	Click the "Browse" button to locate and select a configuration file that is saved previously to your local hard drive. And then click the "Restore" button to reset your device to previous settings.

5.8.4 Restore to Factory Default Settings

To restore all settings to the device's factory default values, click the "**Restore to Factory Default**" button:

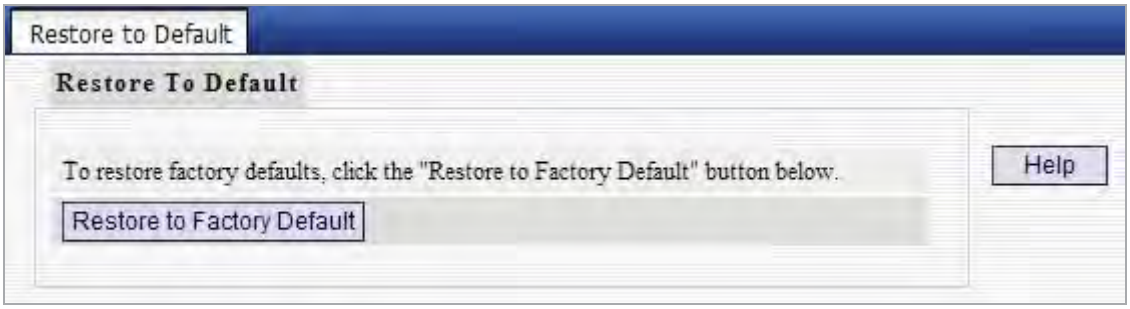


Figure 5-8-4

Factory Default Settings:

User Name: admin

Password: admin

IP Address: 192.168.0.1

Subnet Mask: 255.255.255.0

Note

To activate your settings, you need to reboot the device after you reset it.

5.8.5 Change Password/User Name

This section allows you to change login password and user name for accessing device's Web-based interface.

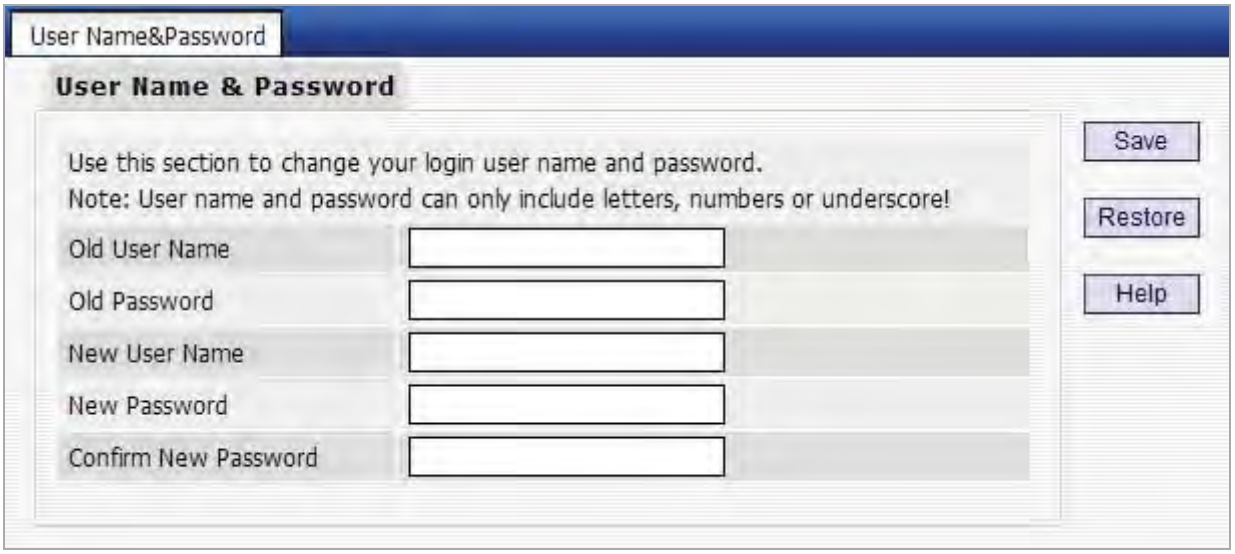
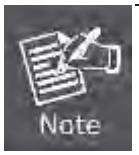


Figure 5-8-5

The page includes the following fields:

Object	Description
• **Old Password / User Name:**	Enter the old password/user name.
• **New Password / User Name:**	Enter a new password/user name.
• **Confirm New Password:**	Re-enter the new password for confirmation.
• **Save:**	Click it to save new settings.



For the sake of security, it is highly recommended that you change default login password and user name.

5.8.6 Reboot

This section allows you to reboot the device.

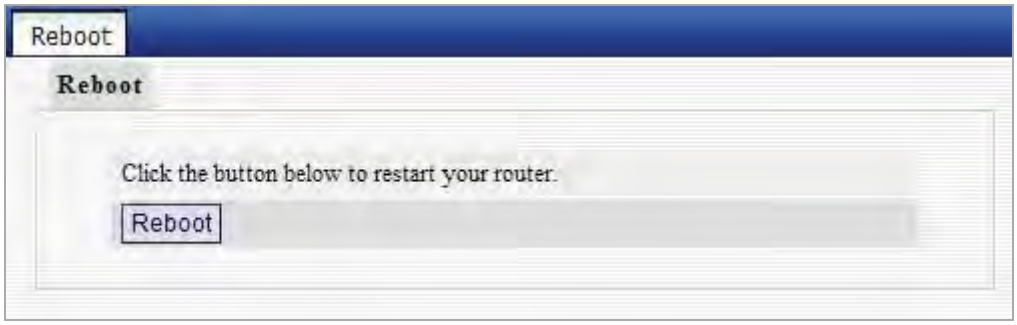


Figure 5-8-6

To restart your device, click the “Reboot” button.

Figure 5-8-7

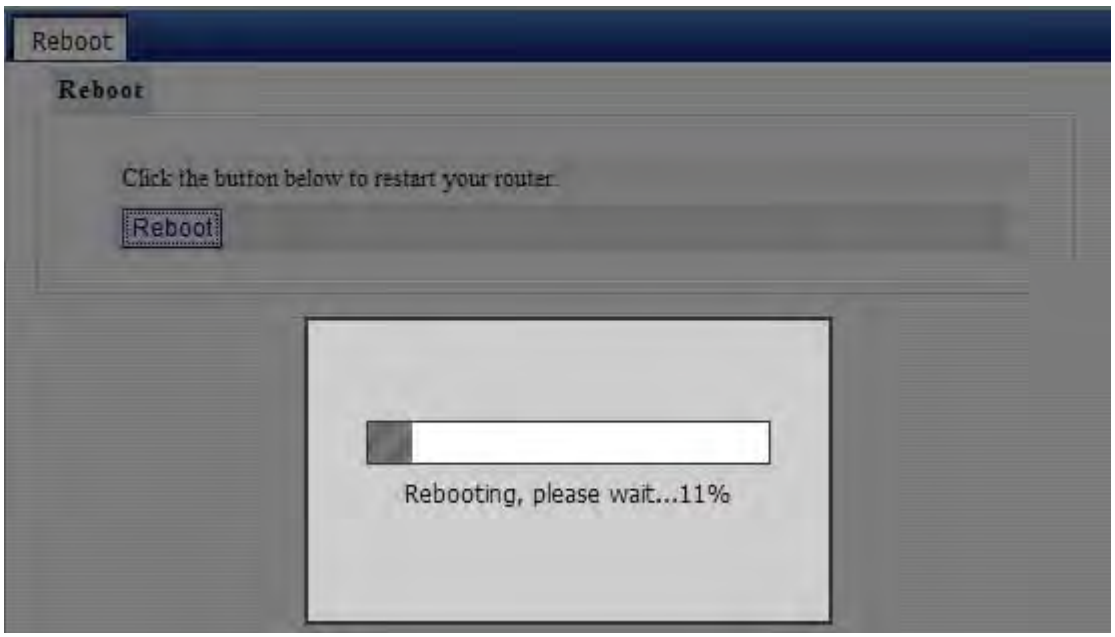


Figure 5-8-8

5.8.7 Statistics

Statistics displays current traffic of PCs on your LAN.

You can view the bandwidth usage on your LAN using the statistics feature, for better management of network resources.

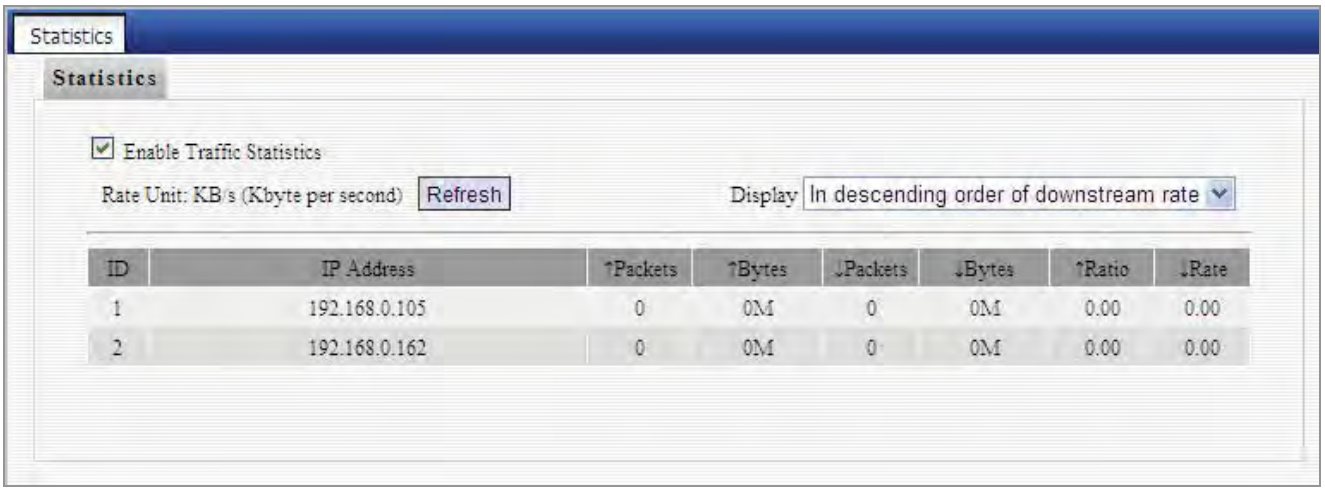


Figure 5-8-9

The page includes the following fields:

Object	Description
• **Enable Traffic Statistics:**	Check/uncheck the box to enable/disable the Traffic Statistics feature.
• **Refresh:**	Click to update statistic data.
• **Clear:**	Click to remove statistic data.
• **Ratio:**	The quantitative relation between broadcast packets and the forwarded packets. Normally, if this value exceeds 10%, there may be problems present in some PC on the network.

Note

Enabling the Traffic Statistics feature may degrade router's packet processing capacity. So, do not enable it unless necessary.

5.8.8 Syslog

The Syslog option allows you to view all events that occur upon system startup and check whether there is attack present in your network.

The logs are classified into 3 types: "**All**", "**System** "and "**WAN**".

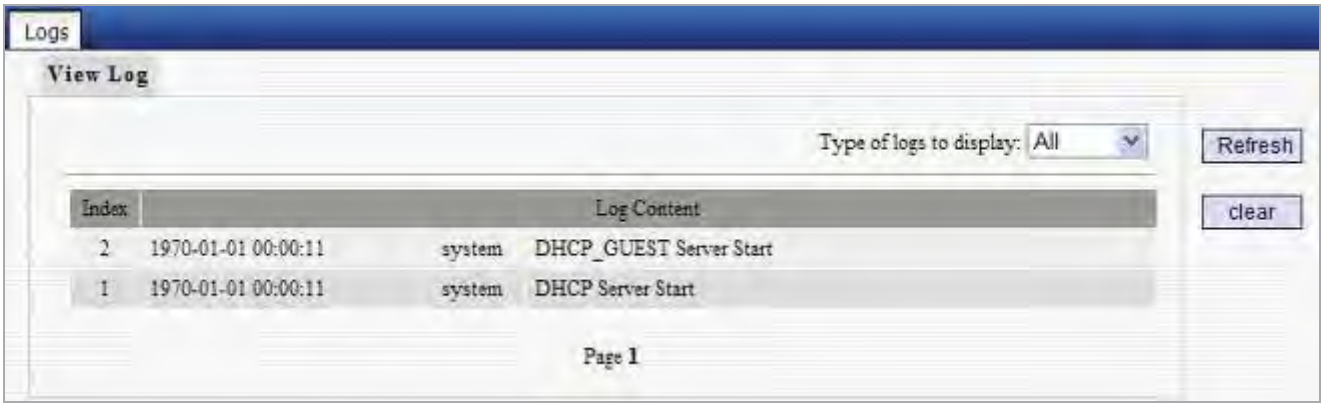

Logs
View Log
Type of logs to display: All
Refresh
clear
Index
Log Content
2 1970-01-01 00:00:11 system DHCP_GUEST Server Start
1 1970-01-01 00:00:11 system DHCP Server Start
Page 1

Figure 5-8-10

Chapter 6. Quick Connection to a Wireless Network

6.1 Windows XP (Wireless Zero Configuration)

Step 1: Right-Click on the **wireless network icon** displayed in the system tray

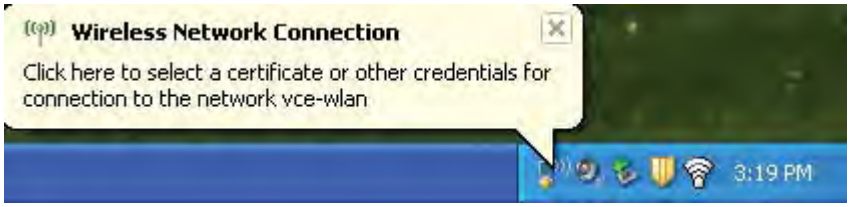


Figure 6-1

Step 2: Select [**View Available Wireless Networks**]

Figure 6-2

Step 3: Highlight and select the wireless network (SSID) to connect

(1) Select SSID [LEVITON]

(2) Click the [**Connect**] button

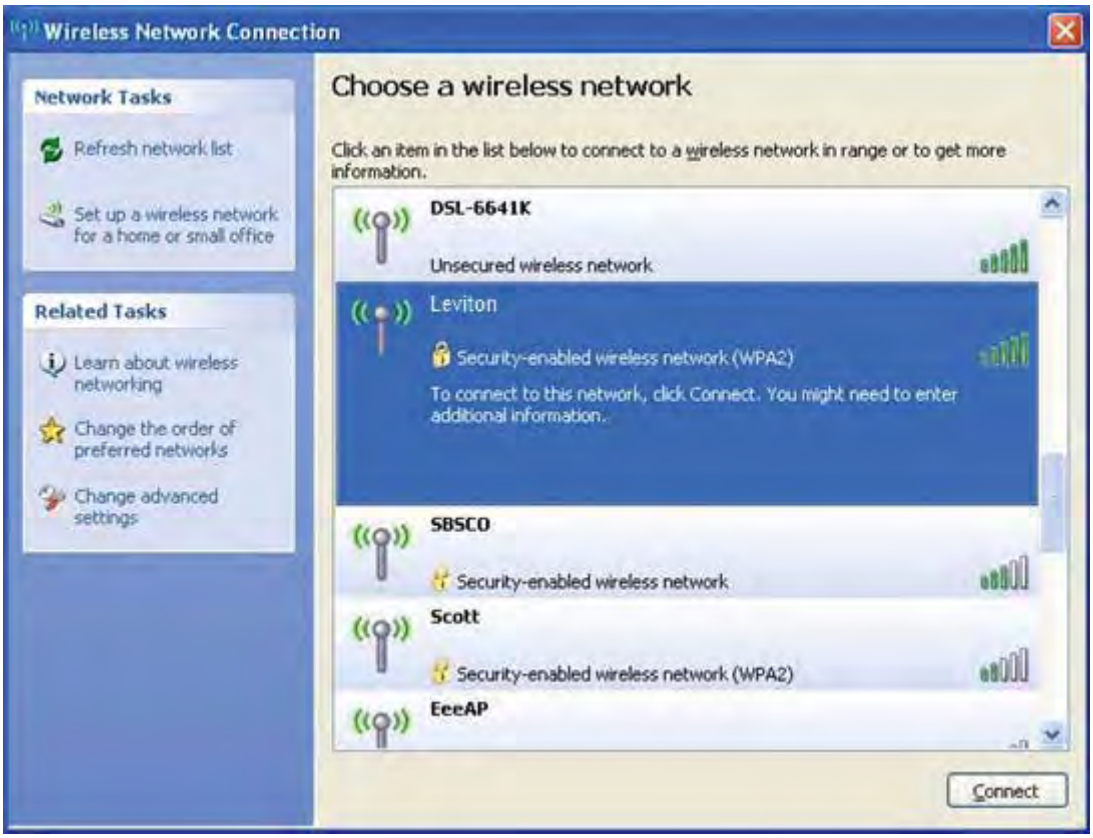


Figure 6-3

Step 4: Enter the **encryption key** of the Wireless Router

(1) The Wireless Network Connection box will appear

(2) Enter the encryption key that configured in section 5.6.2

(3) Click the [Connect] button

Figure 6-4

Step 5: Check if "**Connected**" is displayed

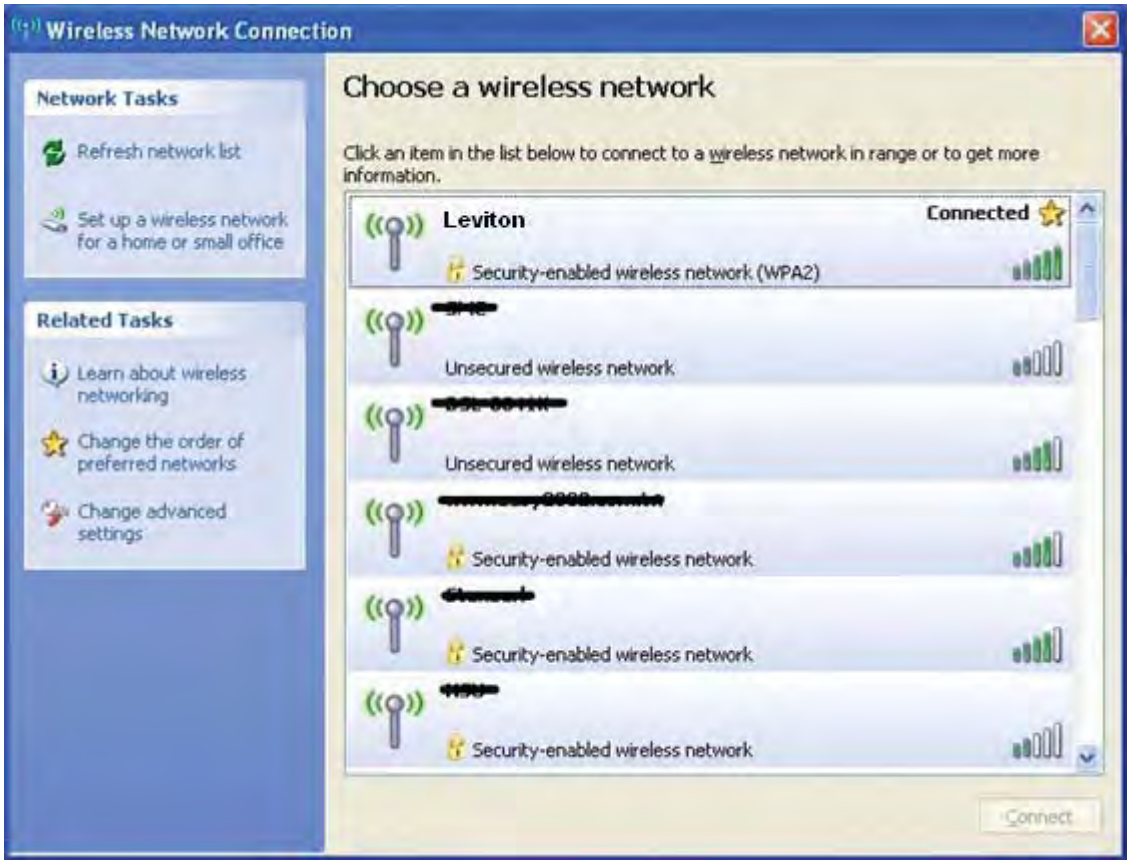


Figure 6-5

Note

Some laptops are equipped with an “Wireless ON/OFF” switch for the internal wireless LAN, make sure the hardware wireless switch is switch to “ON” position.

6.2 Windows 7 (WLAN AutoConfig)

WLAN AutoConfig service is built-in in Windows 7 that can be used to detect and connect to wireless network. This built-in wireless network connection tool is similar to wireless zero configuration tool in Windows XP.

Step 1: Right-Click on the **network icon** displayed in the system tray

Figure 6-6

Step 2: Highlight and select the wireless network (SSID) to connect

(1) Select SSID [defauld_2.4G]

(2) Click the [**Connect**] button

Figure 6-7

Note

If you will be connecting to this Wireless Router in the future, checking [**Connect automatically**].

Step 4: Enter the **encryption key** of the Wireless Router

(1) The Connect to a Network box will appear

(2) Enter the encryption key that configured in section 5.6.2

(3) Click the [OK] button

Figure 6-8

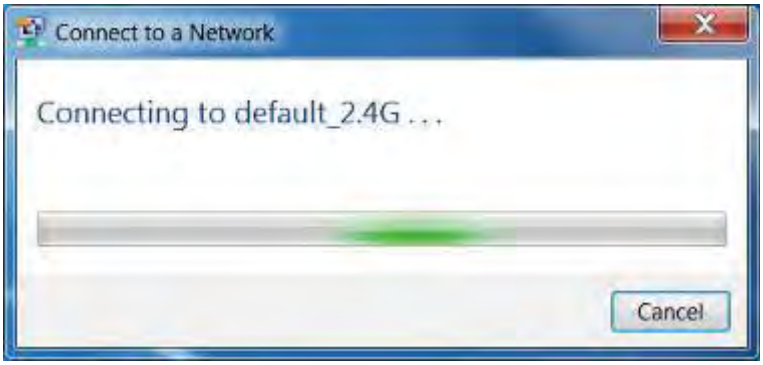


Figure 6-9

Step 5: Check if "**Connected**" is displayed

Figure 6-10

6.3 Mac OS X 10.x

Step 1: Right-Click on the **network icon** displayed in the system tray

The AirPort Network Connection menu will appear

Figure 6-11

Step 2: Highlight and select the wireless network (SSID) to connect

(1) Select and SSID [LEVITON]

(2) Double-click on the selected SSID

Figure 6-12

Step 4: Enter the **encryption key** of the Wireless Router

(1) Enter the encryption key that configured in section 5.6.2

(2) Click the [OK] button

Figure 6-13

Note

If you will connect this Wireless Router in the future, check [**Remember this network**].

Step 5: Check if the AirPort is connect to the selected wireless network.

If “Yes”, then there will be a “check” symbol in the front of the SSID.

Figure 6-14

6.4 iPhone / iPod Touch / iPad

Step 1: Tap the [**Settings**] icon displayed in the home screen

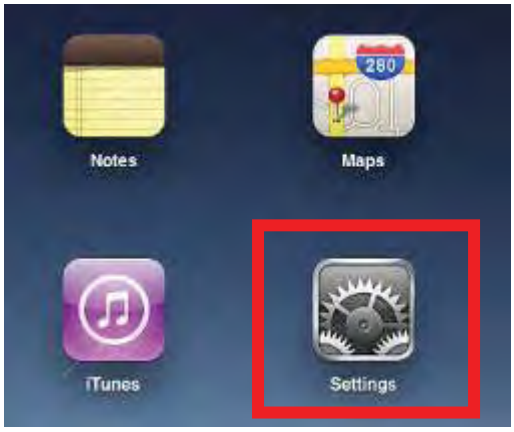


Figure 6-15

Step 2: Check Wi-Fi setting and select the available wireless network

(1) Tap [**General**] \ [**Network**]

(2) Tap [**Wi-Fi**]

If this is the first time to connect to the Wireless Router, it should shows “Not Connected”.

Figure 6-16

Figure 6-17

Step 3: Tap the target wireless network (SSID) in "**Choose a Network…**"

(1) Turn on Wi-Fi by tapping "**Wi-Fi**"

(2) Select SSID [LEVITON]

Figure 6-18

Step 4: Enter the **encryption key** of the Wireless Router

(1) The password input screen will be displayed

(2) Enter the encryption key that configured in section 5.6.2

(3) Tap the [**Join**] button

Figure 6-19

Step 5: Check if the iDevice is connect to the selected wireless network.

If “Yes”, then there will be a “check” symbol in the front of the SSID.

Figure 6-20

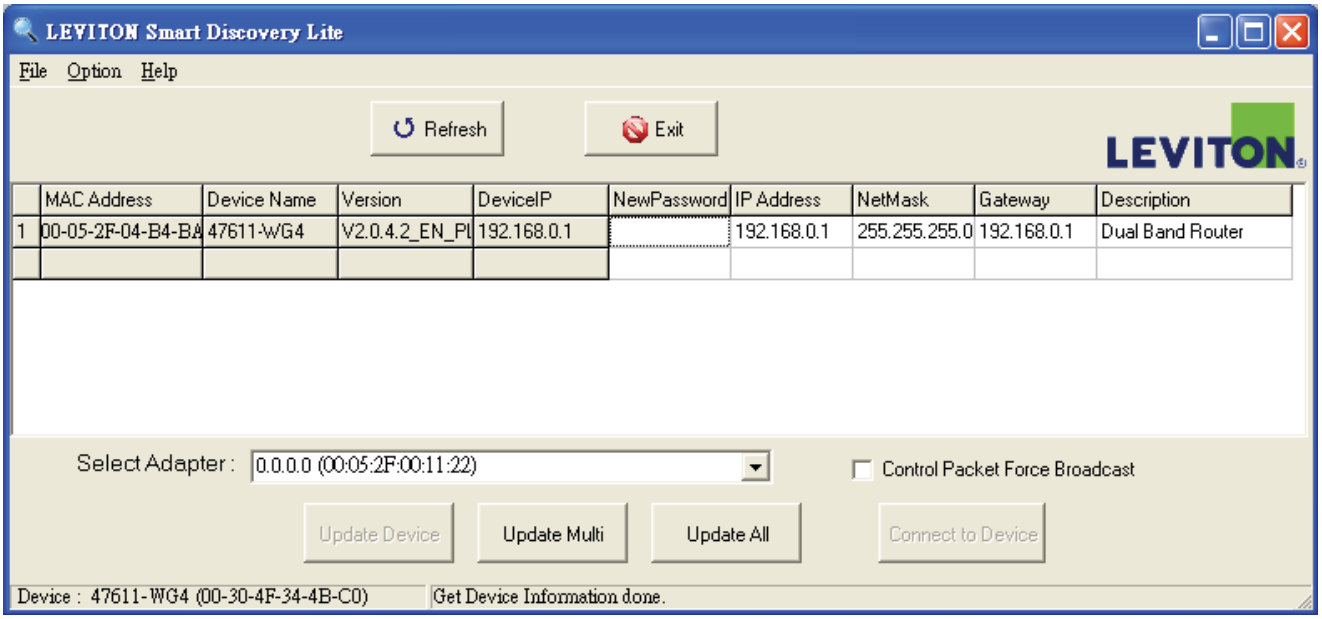
Appendix A: Leviton Smart Discovery Utility

To easily list the device in your Ethernet environment, the Smart Discovery Utility from user's manual CD-ROM is an ideal solution.

The following installation instructions guide you to running the Smart Discovery Utility.

Step 1: Deposit the **Leviton Smart Discovery Utility** in administrator PC.

Step 2: Run this utility and the following screen appears.



Step 3: Press **"Refresh"** button for current connected devices in the discovery list as shown in the following screen:

Step 4: Press **"Connect to Device"** button and then the Web login screen appears.

The fields in white background can be modified directly, and then you can apply the new setting by clicking the "**Update Device**" button.

Appendix B: Troubleshooting

If you found the router is working improperly or stop responding to you, please read this troubleshooting first before contacting the Leviton Tech Support for help,. Some problems can be solved by yourself within very short time.

Scenario	Solution
The router is not responding to me when I want to access it by web browser.	a. Please check the connection of the power cord and the Ethernet cable of this router. All cords and cables should be correctly and firmly inserted to the router. b. If all LEDs on this router are off, please check the status of power adapter, and make sure it is correctly powered. c. You must use the same IP address section which router uses. d. Are you using MAC or IP address filter? Try to connect the router by another computer and see if it works; if not, please reset the router to the factory default settings (pressing 'reset' button for over 10 seconds). e. Set your computer to obtain an IP address automatically (DHCP), and see if your computer can get an IP address. f. If you did a firmware upgrade and this happens, contact the Leviton Tech Support for help. g. If all the solutions above don't work, contact the Leviton Tech Support for help.
I can't get connected to the Internet.	a. Go to 'Status' -> 'Internet Connection' menu, and check Internet connection status. b. Please be patient, sometime Internet is just that slow. c. If you connect a computer to Internet directly before, try to do that again, and check if you can get connected to Internet with your computer directly attached to the device provided by your Internet service provider. d. Check PPPoE / L2TP / PPTP user ID and password again. e. Call your Internet service provide and check if there's something wrong with their service. f. If you just can't connect to one or more website, but you can still use other internet services, please check URL/Keyword filter. g. Try to reset the router and try again later. h. Reset the device provided by your Internet service provider too. i. Try to use IP address instead of hostname. If you can use IP address to communicate with a remote server,

	but can't use hostname, please check DNS setting.
I can't locate my router by my wireless device.	a. 'Broadcast ESSID' set to off? b. All two antennas are properly secured. c. Are you too far from your router? Try to get closer. d. Please remember that you have to input ESSID on your wireless client manually, if ESSID broadcast is disabled.
File download is very slow or breaks frequently.	a. Are you using QoS function? Try to disable it and try again. b. Internet is slow sometimes, being patient. c. Try to reset the router and see if it's better after that. d. Try to know what computers do on your local network. If someone's transferring big files, other people will think Internet is really slow. e. If this never happens before, call you Internet service provider to know if there is something wrong with their network.
I can't log into the web management interface; The password is wrong.	a. Make sure you're connecting to the correct IP address of the router! b. Password is case-sensitive. Make sure the 'Caps Lock' light is not illuminated. c. If you really forget the password, do a hard reset.
The router becomes hot	a. This is not a malfunction, if you can keep your hand on the router's case. b. If you smell something wrong or see the smoke coming out from router or A/C power adapter, please disconnect the router and A/C power adapter from utility power (make sure it's safe before you're doing this!), and call your dealer of purchase for help.

Appendix C: Configuring the PC in Windows 7

In this section, we'll introduce how to configure the TCP/IP correctly in Windows 7. First make sure your Network Adapter is working, refer to the adapter's manual if needed.

1) On the Windows taskbar, click the **Start** button, and then click **Control Panel**.

2) Click the **Network and Sharing Center** icon, and then click the **Change adapter settings** on the left side of the screen.

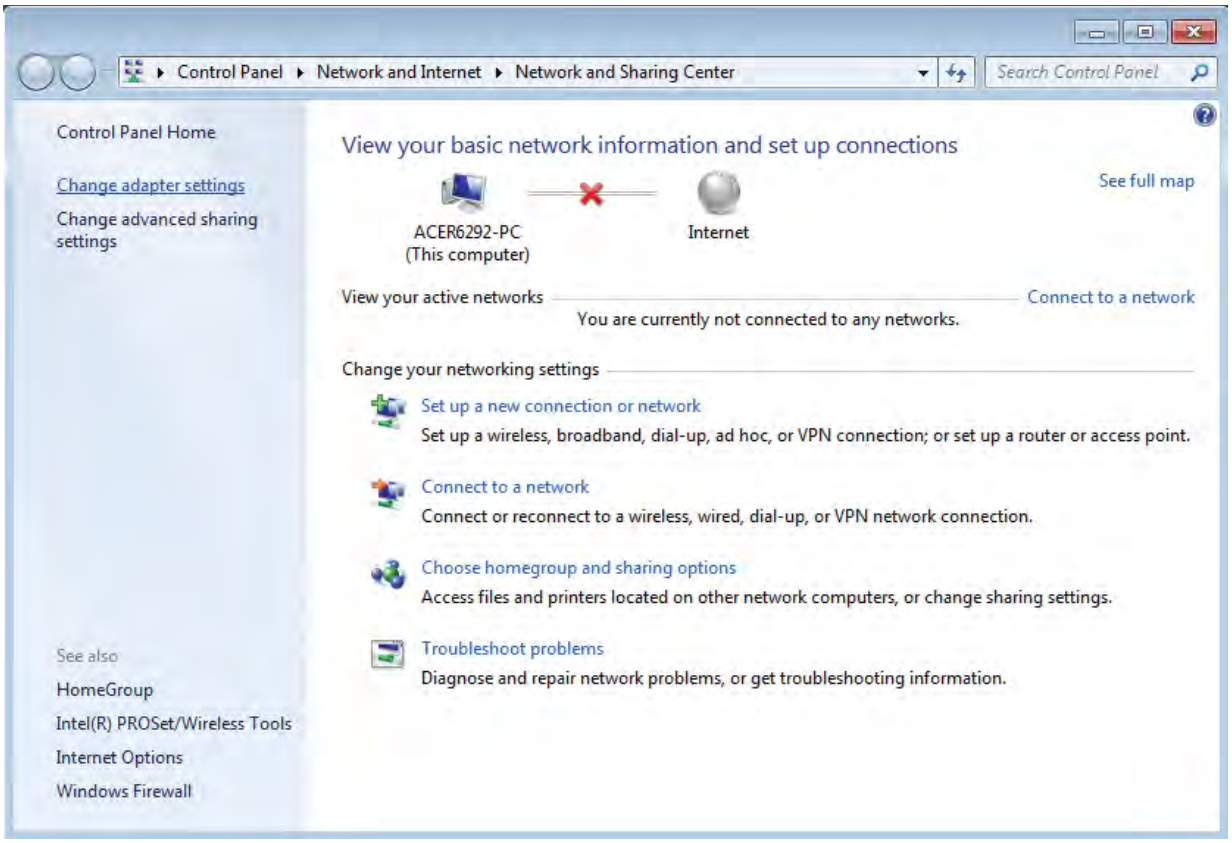


Figure B-1

3) Right click the icon of the network adapter shown in the figure below, and select Properties on the prompt window.

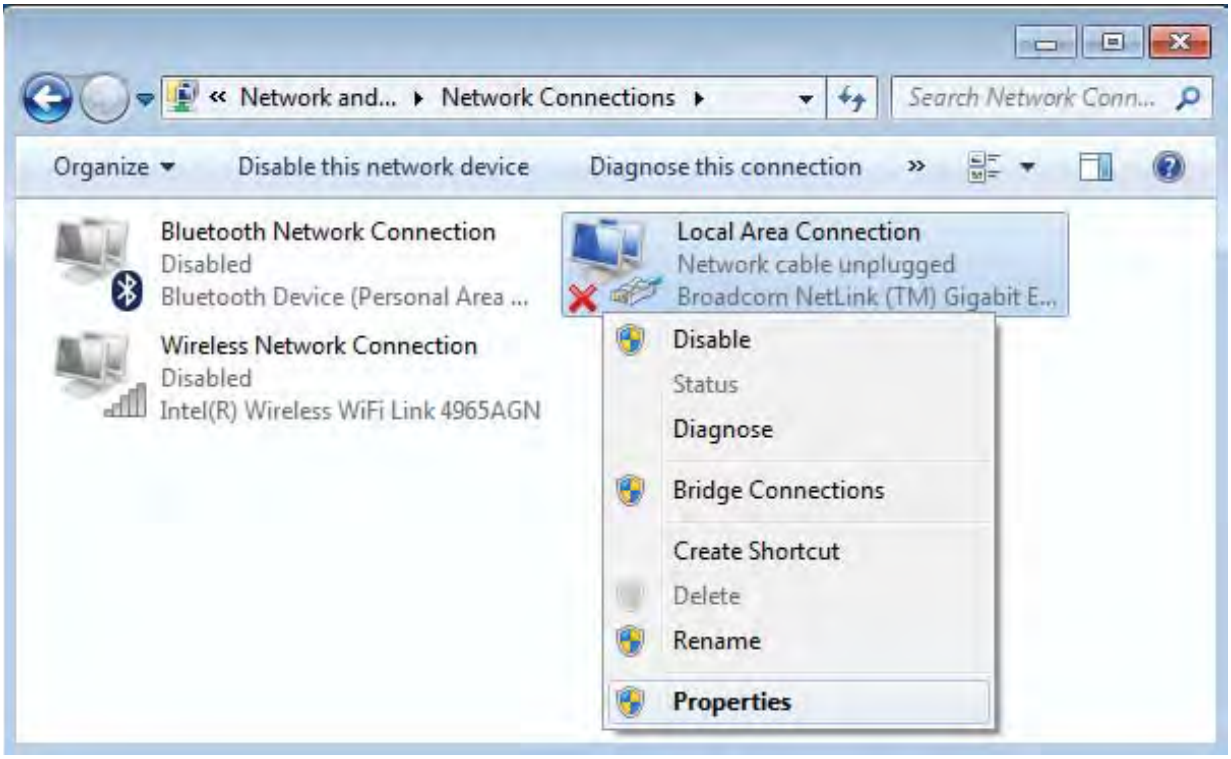


Figure B-2

4) In the prompt page shown below, double click on the **Internet Protocol Version 4 (TCP/IPv4)**.

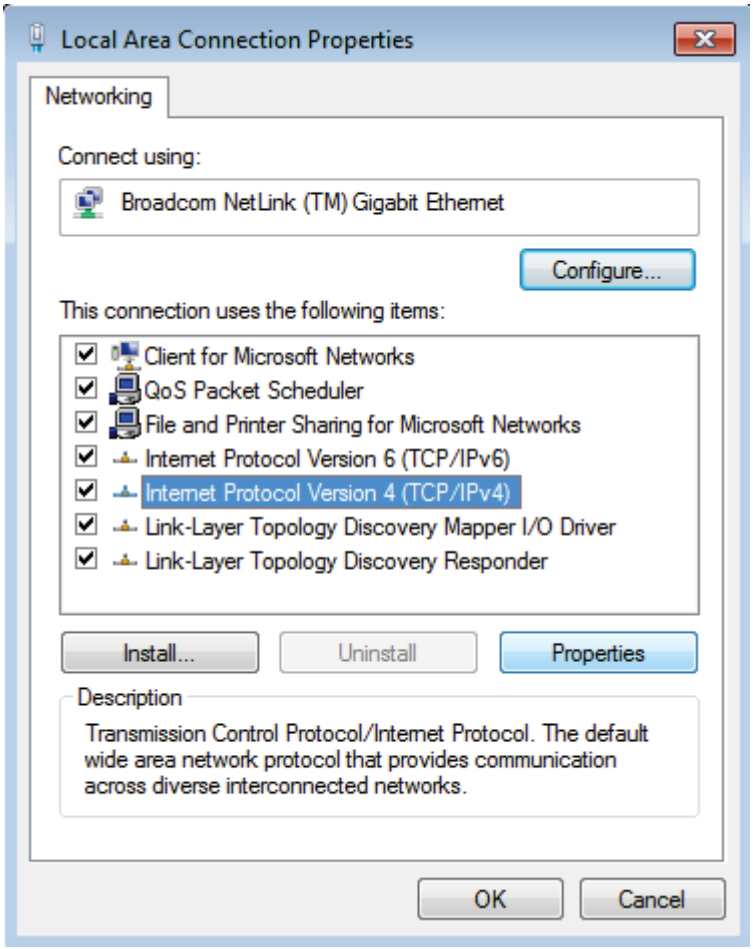


Figure B-3

5) The following **TCP/IP Properties** window will display and the **IP Address** tab is open on this window by default.

Now you have two ways to configure the **TCP/IP** protocol below:

➢ **Setting IP address automatically**

Select **Obtain an IP address automatically**, Choose **Obtain DNS server address automatically**, as shown in the Figure below:

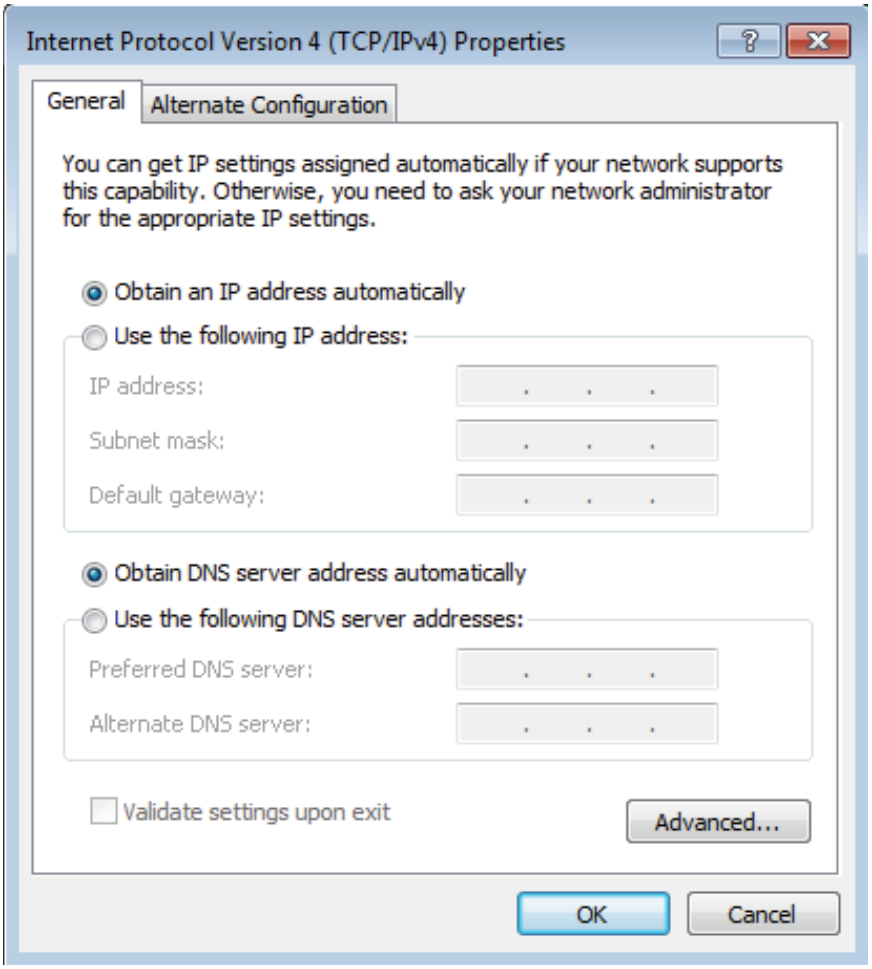


Figure B-4

➢ **Setting IP address manually**

1 Select **Use the following IP address** radio button.

2 If the Router's LAN IP address is 192.168.0.1, type in IP address 192.168.0.x (x is from 2 to 254), and **Subnet mask** 255.255.255.0.

3 Type the Router's LAN IP address (the default IP is 192.168.0.1) into the **Default gateway** field.

4 Select **Use the following DNS server addresses** radio button. In the **Preferred DNS Server** field you can

type the DNS server IP address which has been provided by your ISP

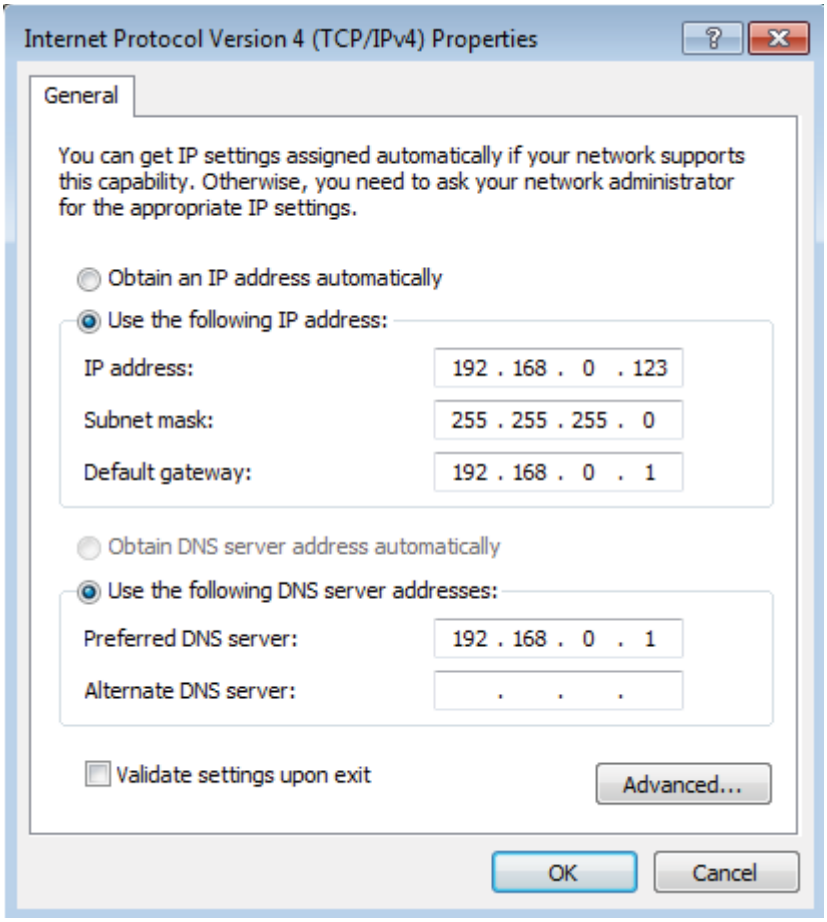


Figure B-5

Now click **OK** to keep your settings.

Appendix D: Specifications

Product	**47611-WG4** 300Mbps Dual-Band 802.11n Wireless Gigabit Router	
Hardware Specification		
Interface	WAN Port:	1 x 10/100/1000Mbps Auto MDI/MDI-X RJ45 port
	LAN Port:	3 x 10/100/1000Mbps Auto MDI/MDI-X RJ45 ports (LAN1~3)
	IPTV Port:	1 x 10/100/1000Mbps Auto MDI/MDI-X RJ45 port (LAN4)
	USB Port :	USB 2.0, Type-A, 5V DC/0.5A Output
Antenna	Gain:	2 x 5dBi fixed antenna
	Orientation:	Omni-directional
Reset / WPS Button	Reset / WPS button at rear panel ■ Press for about 7 seconds to reset the device to factory default. ■ Press for 1 second to activate WPS function.	
LED Indicators	PWR/SYS, WLAN (2.4G & 5G) x 2 WAN (Link & 1000Mbps) x 1 LAN (Link & 1000Mbps) x 3 IPTV (Link & 1000Mbps) x 1 USB, WPS	
Material	Plastic	
Dimension (WxDxH)	171.61 x 111.16 x 25.47 mm (W x D x H)	
Weight	8.81oz	
Power Requirement	12V DC, 1A	
Wireless interface Specification		
Standard	Compliance with IEEE 802.11a/b/g/n	
Frequency Band	Simultaneous 2.4 GHz and 5 GHz 2.4GHz: 2.412~2.484GHz 5GHz: 5.180~5.825GHz	
Transmission Distance	Indoor up to 100m	
RF Power (Intentional Radiator)	**2.4GHz:** 11b: 17±1dBm 11g: 14.5±1.5dBm 11n: 12.5±1.5dBm	**5GHz:** 11a: 12±1.5dBm 11n: 12±1.5dBm
Wireless Management Features		
Wireless Modes	■ AP ■ WDS PtP ■ WDS PtMP	
Encryption Security	■ WEP (64/128-bit) ■ WPA-PSK (TKIP) / WPA2-PSK (AES) ■ WPA (TKIP) / WPA2 (AES)	
Wireless Security	Provide Wireless LAN ACL (Access Control List) filtering	
	Wireless MAC address filtering	

	Support WPS (WIFI Protected Setup)
Wireless Advanced	Support Dual-SSID (2.4G & 5G)
	AP Isolation: Enable it to isolate each connected wireless client.
	Support 802.11e WMM (Wi-Fi Multimedia)
Max. Supported Clients	Wire: 15 Wireless: 10
Router Features	
Internet Connection Type	Shares data and Internet access for users, supporting following internet access: ■ Dynamic IP ■ Static IP ■ PPPoE ■ PPTP ■ L2TP ■ PPPoE Dual Access
Firewall	NAT firewall
	Built-in NAT server which supports Virtual Server, and DMZ
	Built-in firewall with IP address filtering, Port filtering, URL filtering, and MAC address filtering
Routing Protocol	Static Routing
LAN	Built-in DHCP server supporting static IP address distributing
	Support UPnP, Dynamic DNS
	Support Packets Statistics
	IP-based Bandwidth Control
	Session Number: Max. 8000
System Management	Web-based (HTTP) management interface
	Remote management (WAN Access Control)
	SNTP time synchronize
	System Log
OS Compatibility	Windows 7 Windows Vista Windows XP Mac OS X 10.4 and higher

Appendix E: Glossary

- **802.11n -** 802.11n builds upon previous 802.11 standards by adding MIMO (multiple-input multiple-output). MIMO uses multiple transmitter and receiver antennas to allow for increased data throughput via spatial multiplexing and increased range by exploiting the spatial diversity, perhaps through coding schemes like Alamouti coding. The Enhanced Wireless Consortium (EWC) [3] was formed to help accelerate the IEEE 802.11n development process and promote a technology specification for interoperability of next-generation wireless local area networking (WLAN) products.
- **802.11b -** The 802.11b standard specifies a wireless networking at 11 Mbps using direct-sequence spread-spectrum (DSSS) technology and operating in the unlicensed radio spectrum at 2.4GHz, and WEP encryption for security. 802.11b networks are also referred to as Wi-Fi networks.
- **802.11g -** specification for wireless networking at 54 Mbps using direct-sequence spread-spectrum (DSSS) technology, using OFDM modulation and operating in the unlicensed radio spectrum at 2.4GHz, and backward compatibility with IEEE 802.11b devices, and WEP encryption for security.
- **DDNS** (**D**ynamic **D**omain **N**ame **S**ystem) **-** The capability of assigning a fixed host and domain name to a dynamic Internet IP Address.
- **DHCP** (**D**ynamic **H**ost **C**onfiguration **P**rotocol) **-** A protocol that automatically configure the TCP/IP parameters for the all the PC(s) that are connected to a DHCP server.
- **DMZ** (**De**-**mi**litarized **Z**one) **-** A Demilitarized Zone allows one local host to be exposed to the Internet for a special-purpose service such as Internet gaming or videoconferencing.
- **DNS** (**D**omain **N**ame **S**ystem) **-** An Internet Service that translates the names of websites into IP addresses.
- **Domain Name -** A descriptive name for an address or group of addresses on the Internet.
- **DSL** (**D**igital **S**ubscriber **L**ine) **-** A technology that allows data to be sent or received over existing traditional phone lines.
- **ISP** (**I**nternet **S**ervice **P**rovider) **-** A company that provides access to the Internet.
- **MTU** (**Maximum Transmission Unit**) **-** The size in bytes of the largest packet that can be transmitted.
- **NAT** (**N**etwork **A**ddress **T**ranslation) **-** NAT technology translates IP addresses of a local area network to a different IP address for the Internet.
- **PPPoE** (**P**oint to **P**oint **P**rotocol **o**ver **E**thernet) **-** PPPoE is a protocol for connecting remote hosts to the Internet over an always-on connection by simulating a dial-up connection.

- **SSID -** A **S**ervice **S**et **Id**entification is a thirty-two character (maximum) alphanumeric key identifying a wireless local area network. For the wireless devices in a network to communicate with each other, all devices must be configured with the same SSID. This is typically the configuration parameter for a wireless PC card. It corresponds to the ESSID in the wireless Access Point and to the wireless network name.
- **WEP** (**W**ired **E**quivalent **P**rivacy) **-** A data privacy mechanism based on a 64-bit or 128-bit or 152-bit shared key algorithm, as described in the IEEE 802.11 standard.
- **Wi-Fi -** A trade name for the 802.11b wireless networking standard, given by the Wireless Ethernet Compatibility Alliance (WECA, see http://www.wi-fi.net), an industry standards group promoting interoperability among 802.11b devices.
- **WLAN** (**W**ireless **L**ocal **A**rea **N**etwork) **-** A group of computers and associated devices communicate with each other wirelessly, which network serving users are limited in a local area.