FOSCAM
www.foscam.us

User Guide

Wireless N300 High Power Router

Copyright Statement

Technical Support

Website: http://www.foscam..us
Email: support@foscam.us
Toll Free:1-800-930-0949

Contents

Chapter 1 Product Overview

1 Package Contents

Unpack the box and verify that the package contains the following:

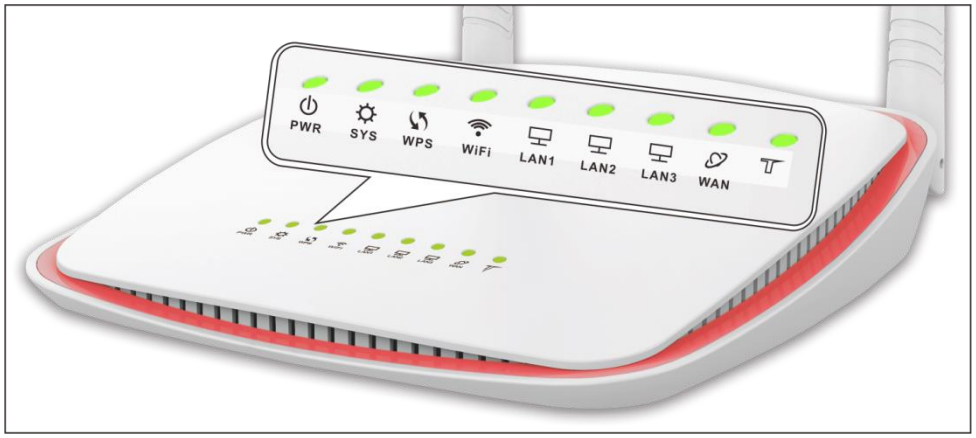
- Wireless N300 High Power Router
- Power Adapter
- Install Guide
- Ethernet Cable
- Resource CD

If any of the above items is incorrect, missing, or damaged, please contact your reseller for immediate replacement.

2 Getting to Know Your Router

Before you cable your router, take a moment to become familiar with the front and back panels and the label. Pay particular attention to the LEDs on the front panel.

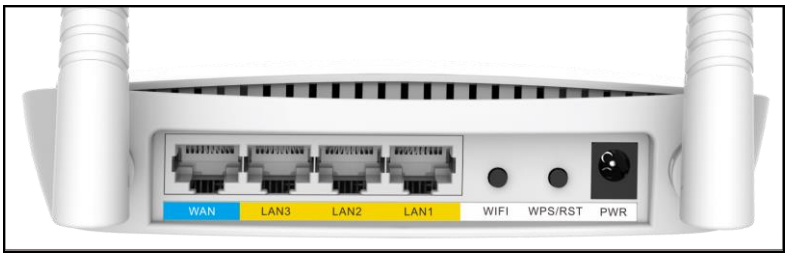
◈ Front Panel



LED Overview:

LED	Status	Description
LAN（1/2/3）	Solid	LAN port connected correctly
	Blinking	LAN port is transferring data.
	Off	LAN port connected incorrectly
WAN	Solid	WAN port connected correctly
	Blinking	WAN port is transferring data.
	Off	WAN port connected incorrectly
SYS	Blinking	Indicates system is functioning properly
	Solid/Off	Indicates system is functioning improperly
PWR	Solid	Indicates a proper connection to the power supply
	Off	Indicates an improper connection to the power supply
WPS	Blinking	Device is performing WPS authentication on a client device.
	Solid	WPS is enabled.
	Off	WPS is disabled or WPS authentication finished.
WiFi	Blinking	Transferring data
	Solid	WiFi is enabled.
	Off	WiFi is disabled.

◈ Back Panel



Button & Interface:

Port	Function Description
PWR	The power adapter is connected and you can use the provided adapter to supply power.
WAN	Usually for connecting Ethernet cable
LAN 1/2/3	Usually for connecting computers, switches, etc.
WPS/RST	When you press this button for over 7 seconds, files set by the router will be deleted and restored to default factory; for 1 second, WPS-PBC will be enabled and the WPS LED will be blinking accordingly.
WiFi	When WiFi is disabled, the WiFi LED will be off.

3 Position Your Router

For best performance, please keep your router:

- Near the center of the area where your computers and other devices operate, and preferably within line of sight to your wireless devices.
- Accessible to an AC power outlet and near Ethernet cables for wired computers.
- In an elevated location such as a high shelf, keeping the number of walls and ceilings between the router and your other devices to a minimum.
- Away from electrical devices that are potential sources of interference, such as ceiling fans, home security systems, microwaves, PCs, the base of a cordless phone, or a 2.4-GHz cordless phone.
- Away from any large metal surfaces, such as a solid metal door or aluminum studs. Large expanses of other materials such as glass, insulated walls, fish tanks, mirrors, brick, and concrete can also affect your wireless signal.

Chapter 2 Installation and Quick Setup Guide

1 Physical Installation

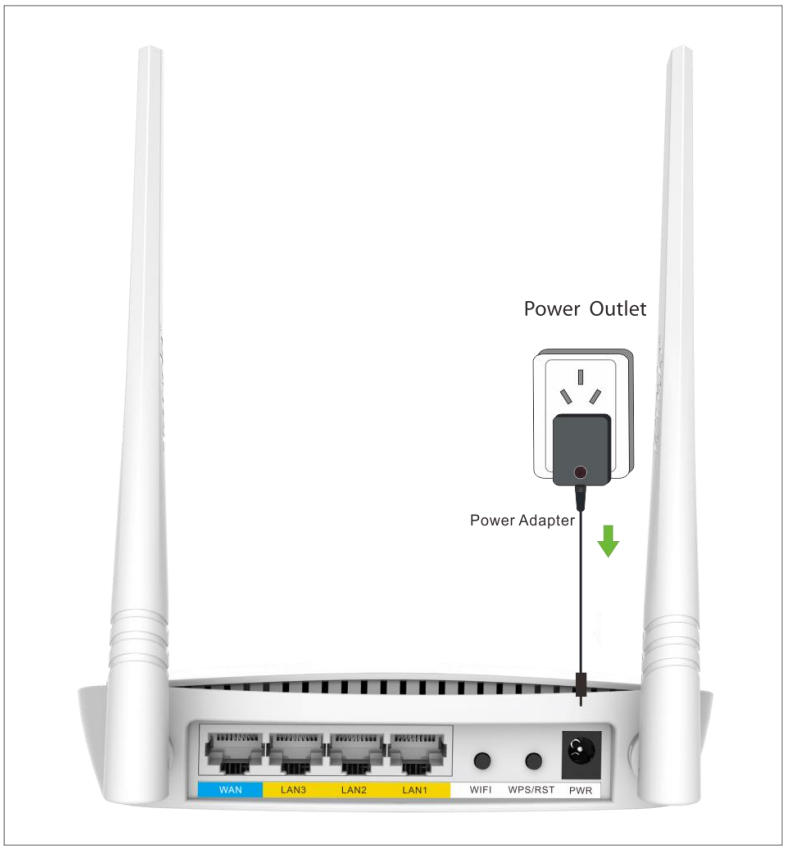
1.1 Preparation

Before connecting Ethernet cables, please verify the following items:

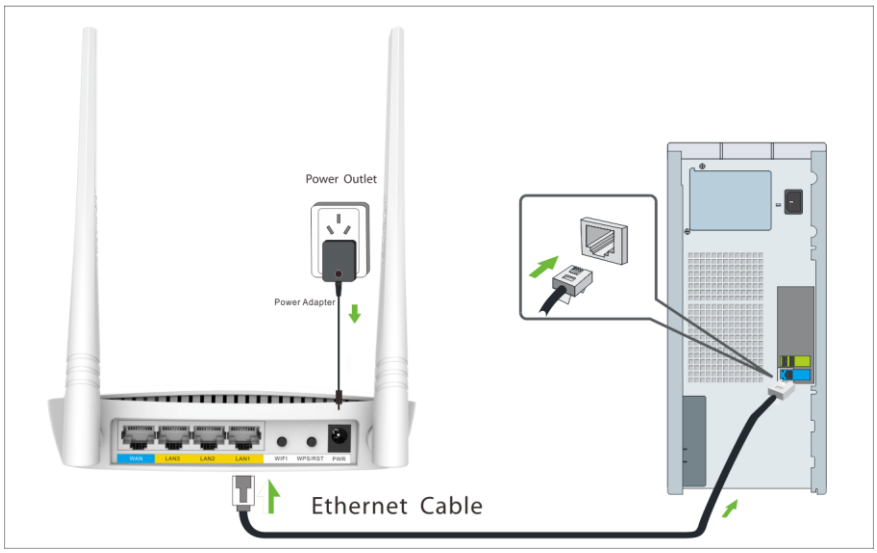
Item	Description
Wireless N300 High Power Router	Used with the provided power adapter
PC	Installed with IE8 or other better web browsers.
Ethernet Cable	Used for linking the PC to the router
Broadband Service	Provided by network service corporation
Internet Connection Setup	✧ If you connect to the Internet using a broadband connection that requires a username and a password provided by your ISP, please select PPPoE; ✧ If your ISP provides all the needed information: IP address, subnet mask, gateway address, and DNS address(es), please select Static IP; ✧ If you can access the Internet as soon as your computer directly connects to an Internet-enabled ADSL/Cable modem, please select DHCP; ✧ If your ISP uses a PPTP connection, please select PPTP; ✧ If your ISP uses an L2TP connection, please select L2TP; PPPoE Dual Access (only supported in special Area e.g. Russia.).

1.2 Physical installation

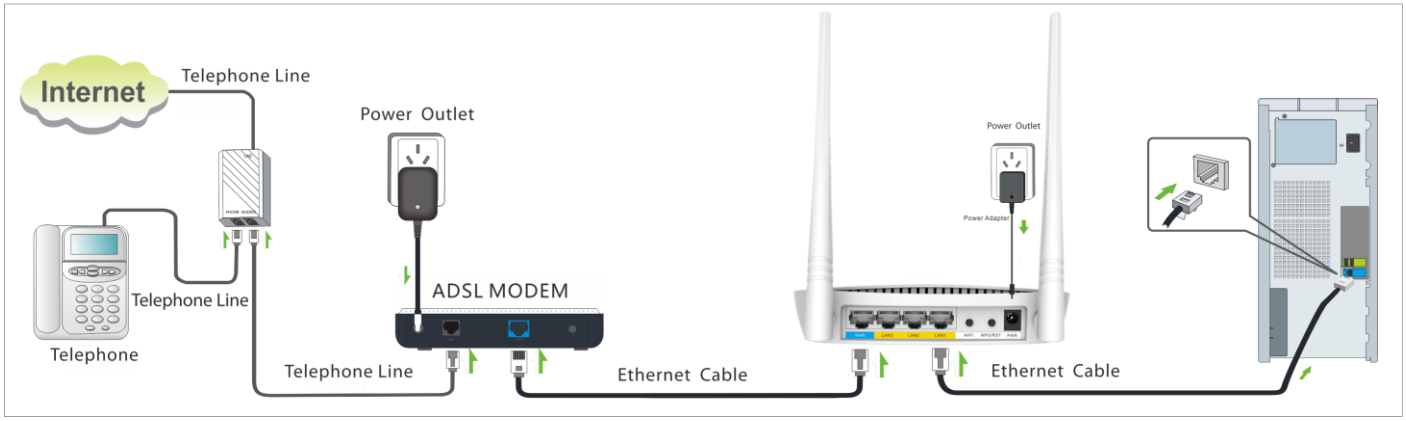
1. Connect one end of the included power adapter to the device and plug the other end into a wall outlet nearby (Using a power adapter with a different voltage rating than the one included with the device will cause damage to the device).



2. Connect one of the LAN ports on the Device to the NIC port on your PC using an Ethernet cable.



3. Connect your router's WAN port to the existing modem's RJ45 port (usually blue) with an Ethernet cable.



4. Log in to Web manager to set up Internet connection.

2 Internet Connection Setup

2.1 Configure PC

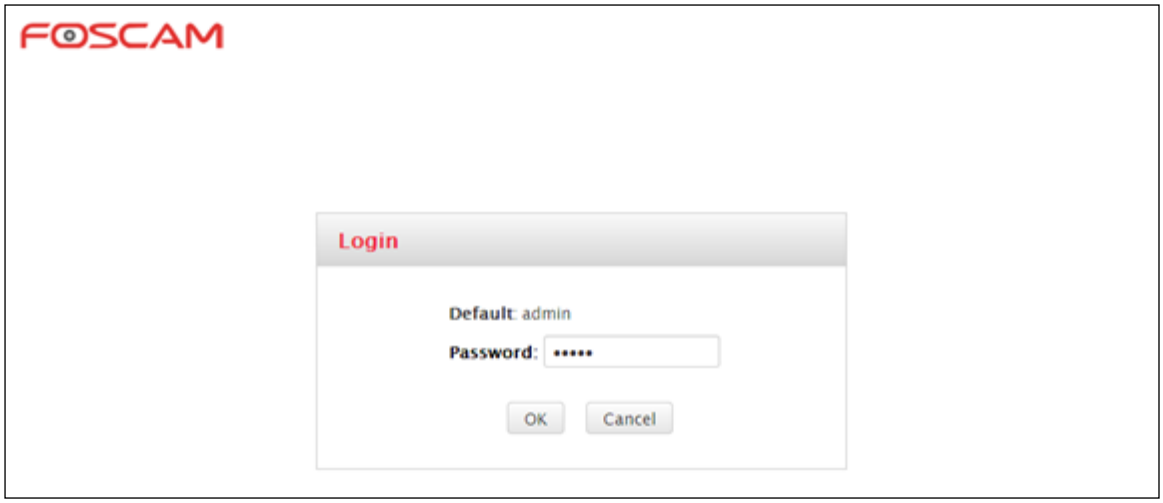
Configure your PC obtain IP address automatically. If you are not clear about this, please refer to Appendix 1 Configure PC.

2.2 Log in to Web Manager

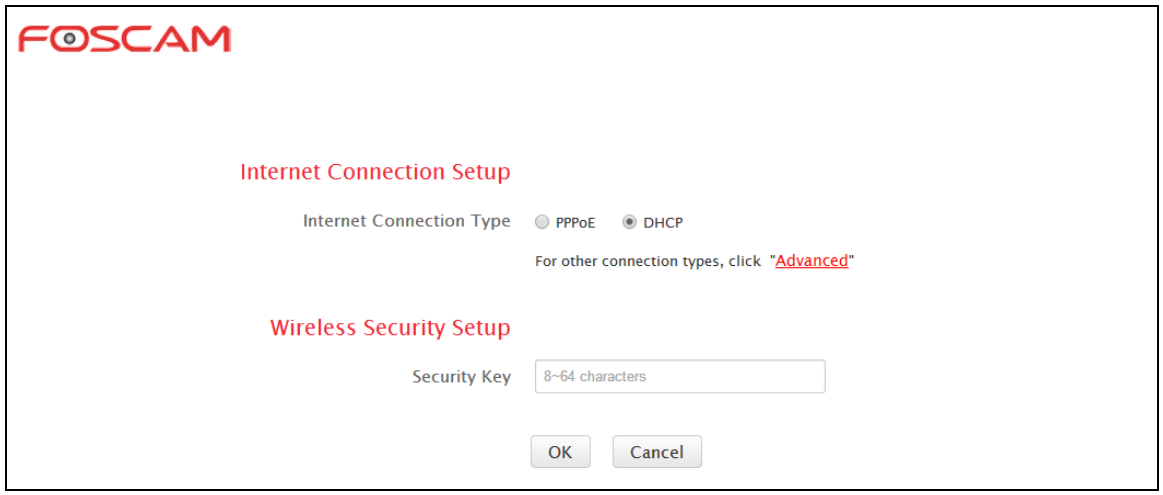
1. Launch a web browser, such as IE Web browser;

2. In the address bar, input 192.168.0.1 and press **Enter**;

3. Enter **admin** in the password field on the appearing login window and then click **OK.**



4. Now you may access the device's home page for quickly setting up Internet connection and wireless security.



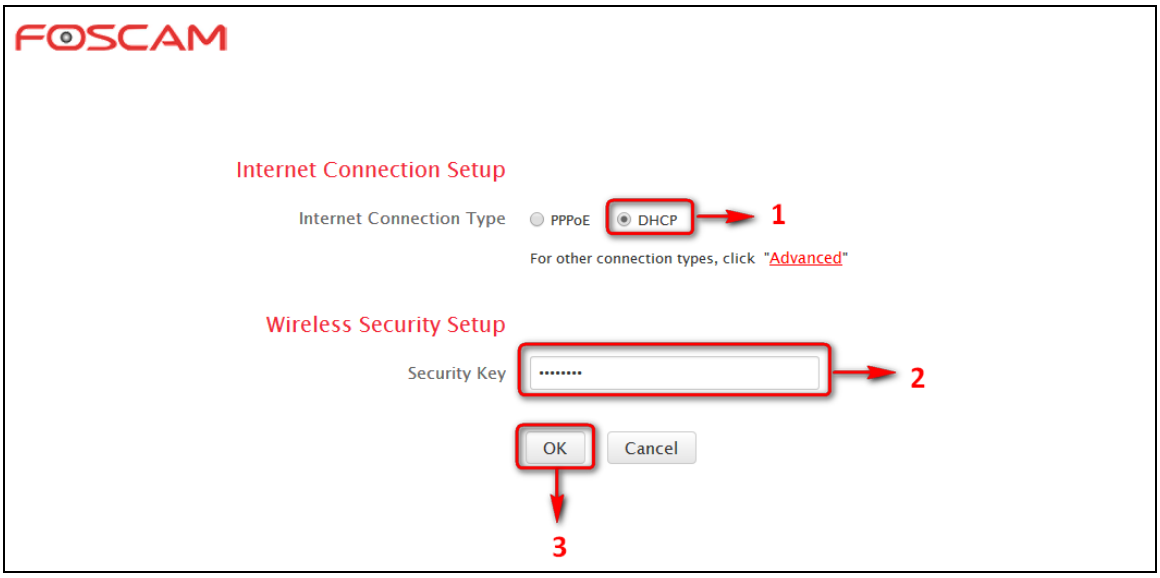
5. If you fail to log in to it, please refer to Appendix 2 FAQs.

2.3 Internet Connection Setup

Common Internet connection types are available on the home page: PPPoE and DHCP.

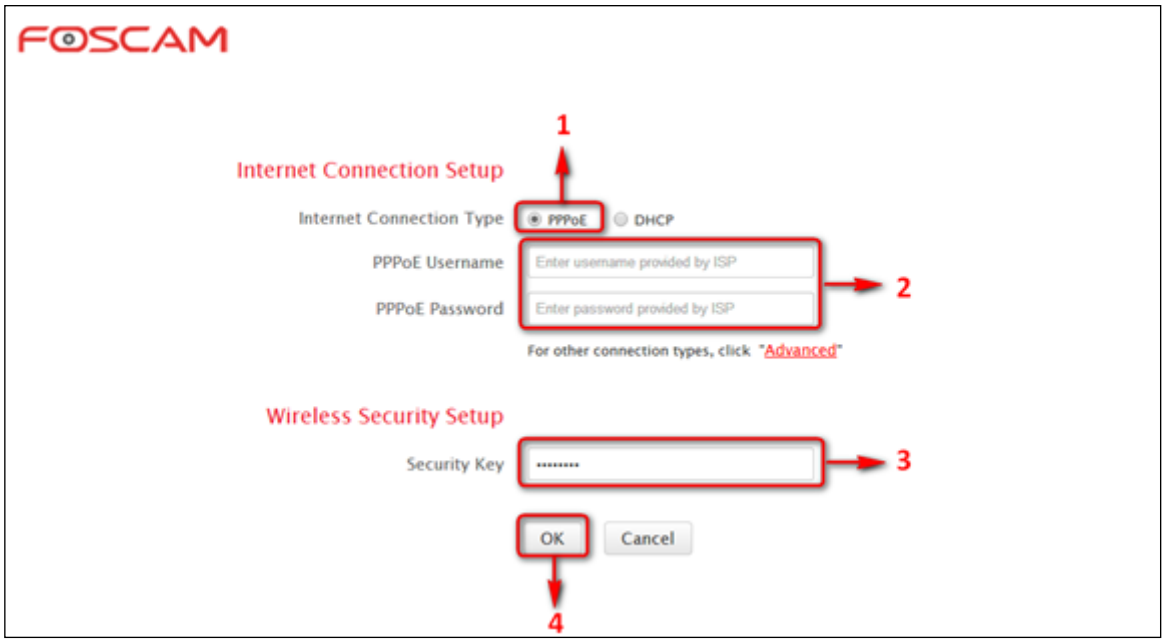
DHCP

Select DHCP (Dynamic IP) if you can access the Internet as soon as your computer directly connects to an Internet-enabled ADSL/Cable modem; configure a security key (8-63 characters) to secure your wireless network and then click OK.



PPPoE

Select PPPoE (Point to Point Protocol over Ethernet) if you used to connect to the Internet using a broadband connection that requires a username and a password. Enter the user name and password provided by your ISP; configure a security key to secure your wireless network and then click **OK**.



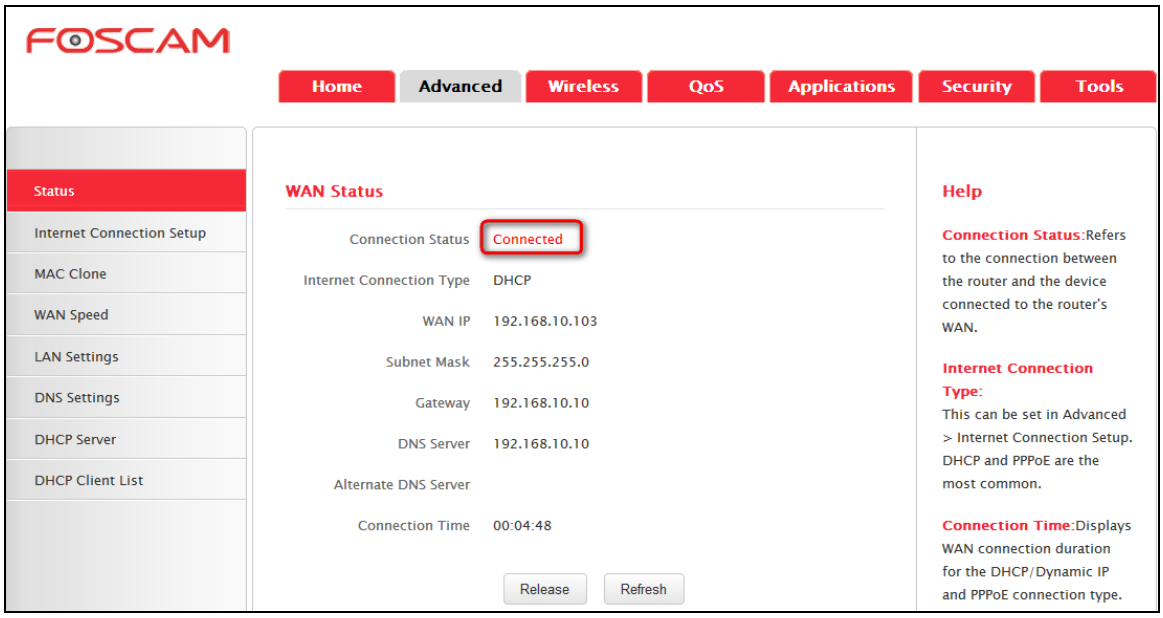
⚠Note:

1. DHCP is the default Internet connection type;
2. If you are not sure about your PPPoE username and password, contact your Internet service provider (ISP) for help. For other Internet connection types, please go to section 1.2: Internet Connection Setup.

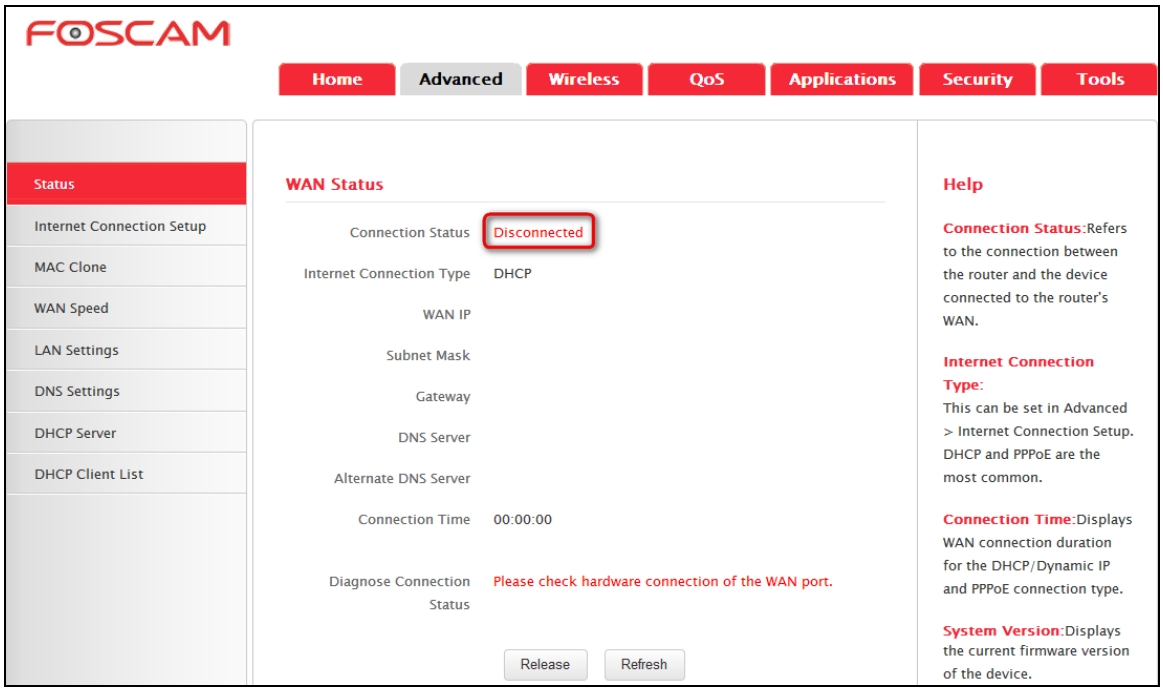
3 Verify Internet Connection Settings

System automatically skips to the status page when you finish all needed settings on the home page. Here you can see the system status and WAN connection status of the device.

1. If you find "**Connected**" and a WAN IP address displayed there (as shown below), you have got a wired internet access now.



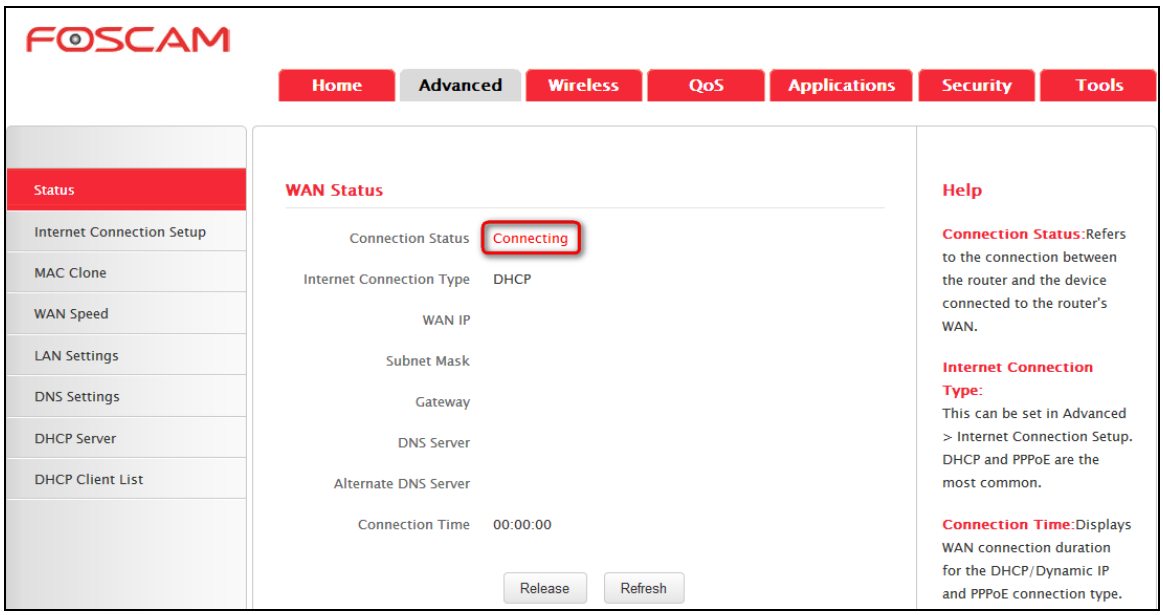
2. If connection status displays "Disconnected" and there is no WAN IP address displayed (as seen below), connection between the Internet-enabled modem and your device may have failed. Please double check or re-connect all involved devices and cables properly and then refresh the page. If nothing is wrong, "Connecting" or "Connected" will be displayed.



3. If "**Connecting**" is displayed and no WAN IP address is seen, try refreshing the page five times. And if it still displays "**Connecting**" try steps below:

1). Contact your ISP for assistance if you are using the DHCP connection type.

2). Read the connection diagnostic info on WAN status.



⚠**Note:**

Below diagnostic info will be displayed on particular occasions for your reference:

- You have connected to the Internet successfully.
- You might have entered a wrong user name and/or a wrong password. Please contact your ISP for the correct user name and password and enter them again.
- Ethernet cable is not connected or not properly connected to the WAN port on the device. Please reconnect it properly.
- No response is received from your ISP. Please verify that you can access the Internet when you directly connect your PC to an Internet-enabled modem. If not, contact your local ISP for help.

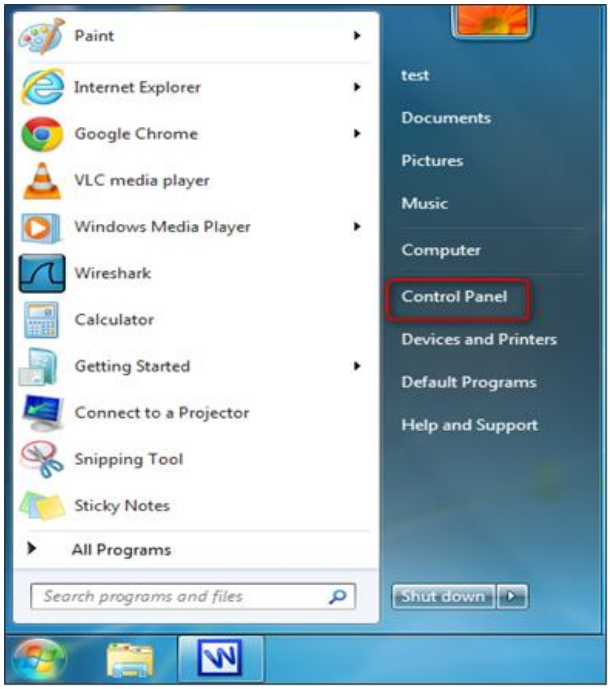
4 Connect to Device Wirelessly

Having finished above settings, you can search the device's wireless network (SSID) from your wireless devices (notebook, iPad, iPhone, etc) and enter a security key to connect to it wirelessly.

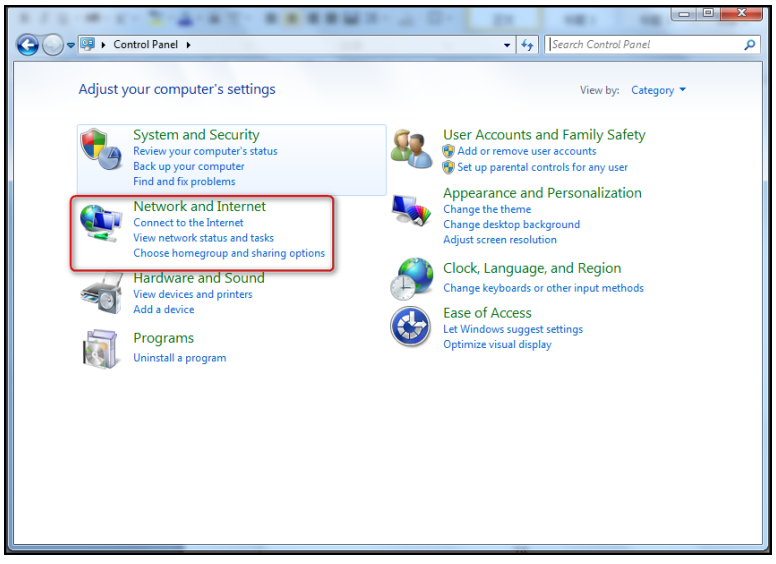
Windows 7

1. If you are using Windows 7 OS, do as follows:

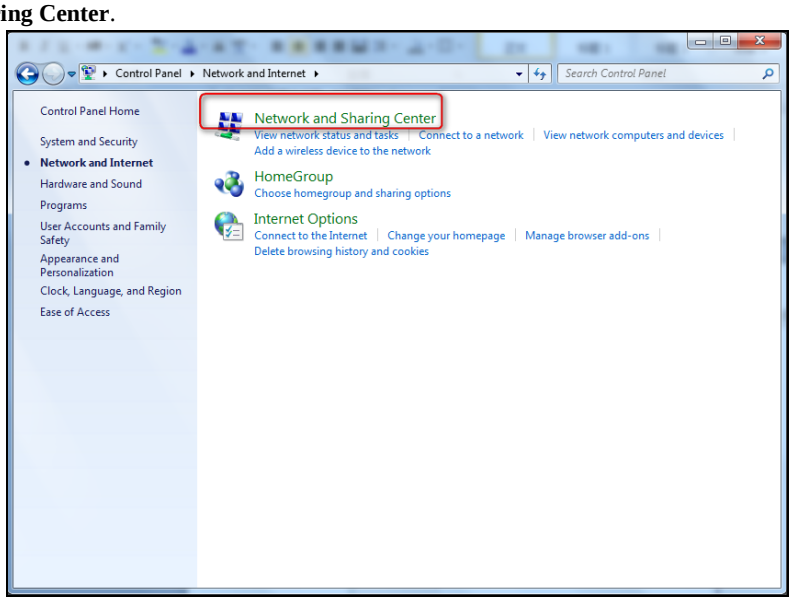
1) Click **Start** and select **Control Panel**.



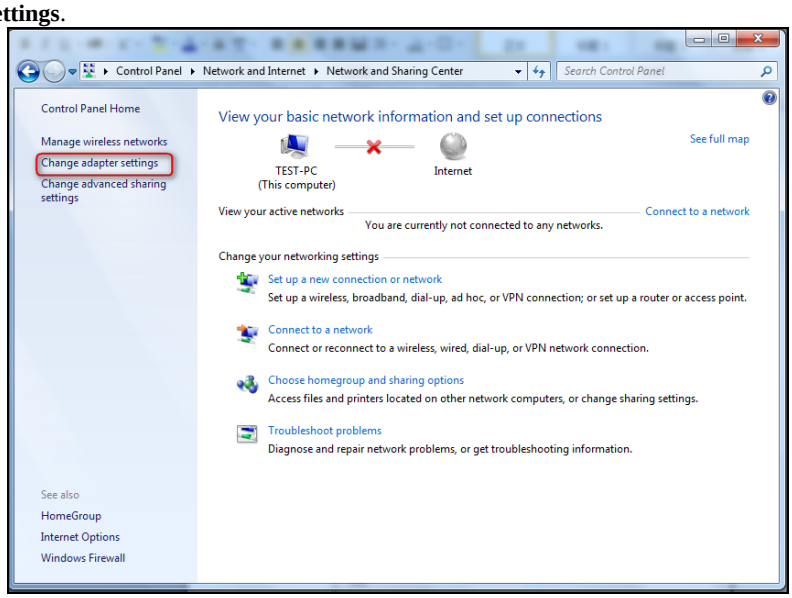
2) Click **Network and Internet**.



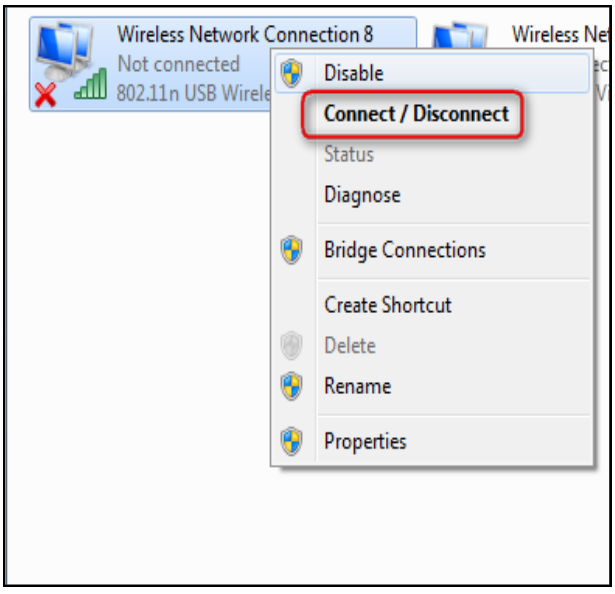
3) Click **Network and Sharing Center**.



4) Click **Change adapter settings**.

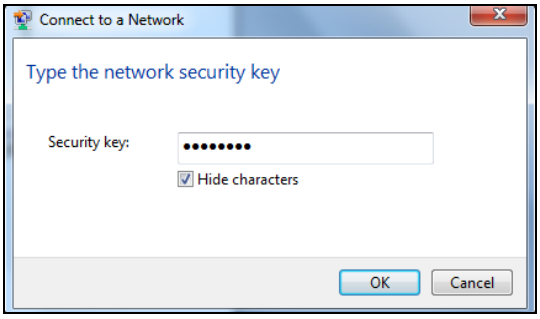


5) Select a desired wireless connection and click **Connect/Disconnect**.



6) Select the wireless network you wish to connect and click **Connect**.

7) Enter the security key and click **OK**.

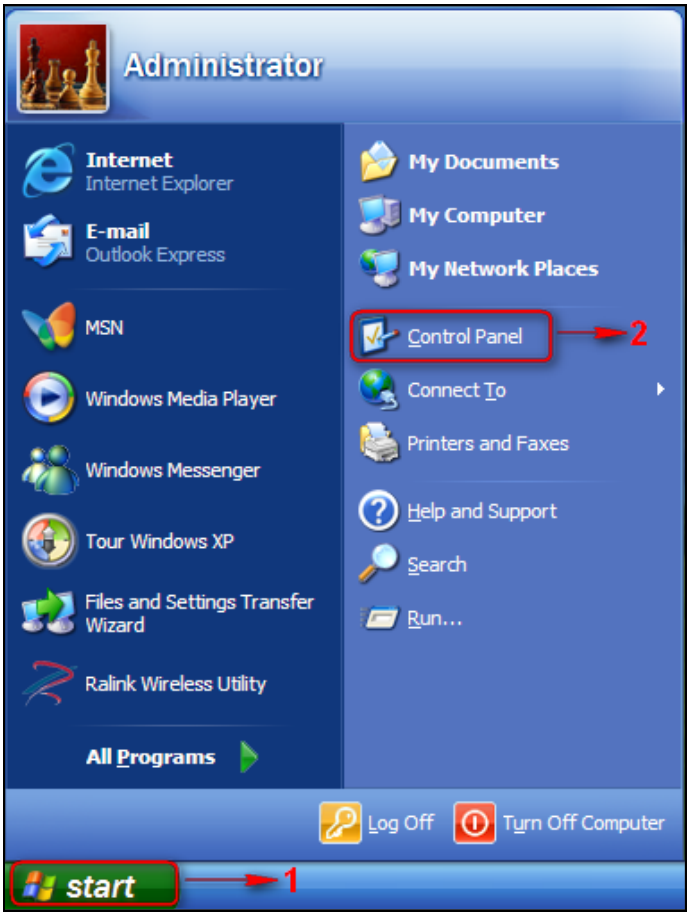


8) You can access the Internet via the device when "**Connected**" appears next to the wireless network name you have selected.

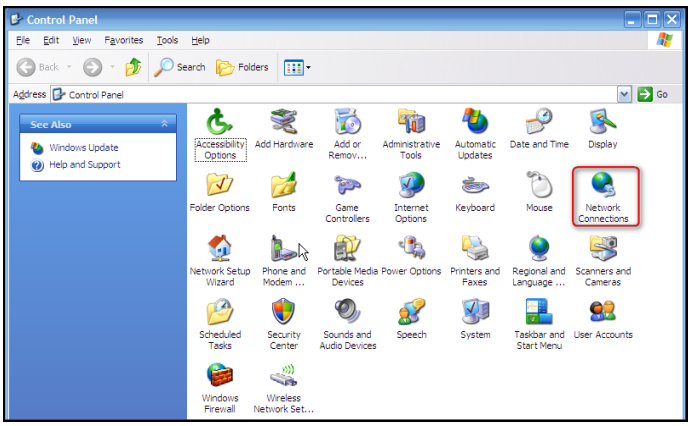
Windows XP

2. If you are using Windows XP OS, do as follows:

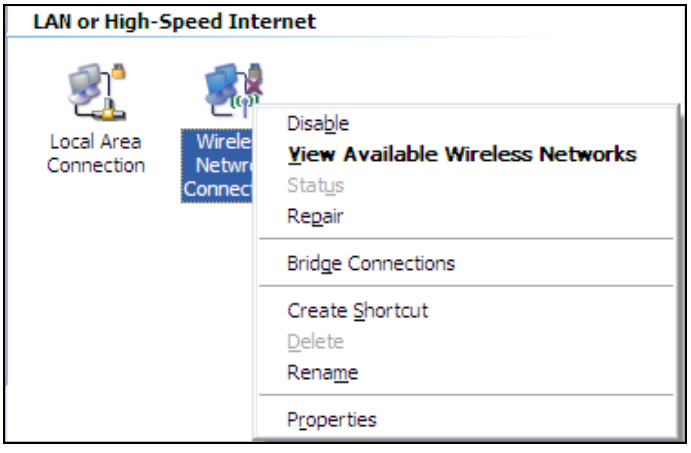
1) Click **Start** and select **Control Panel**.



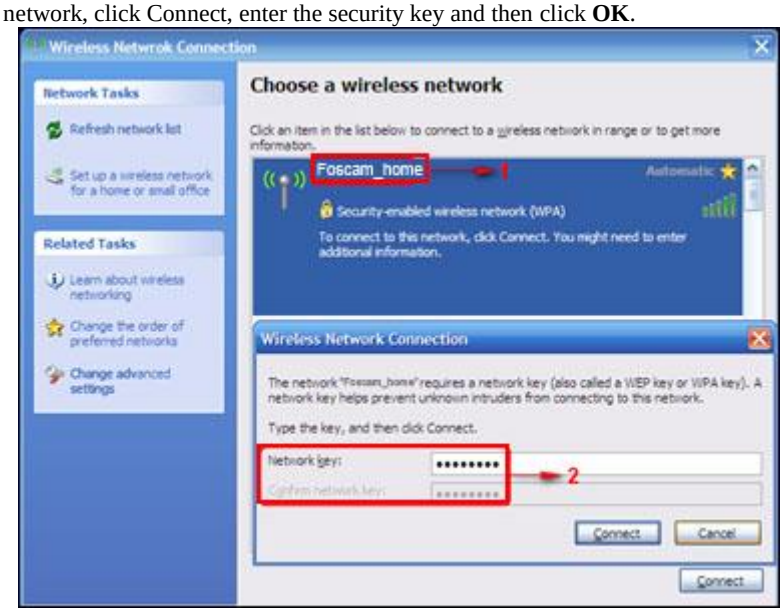
2) Click **Network Connections**.



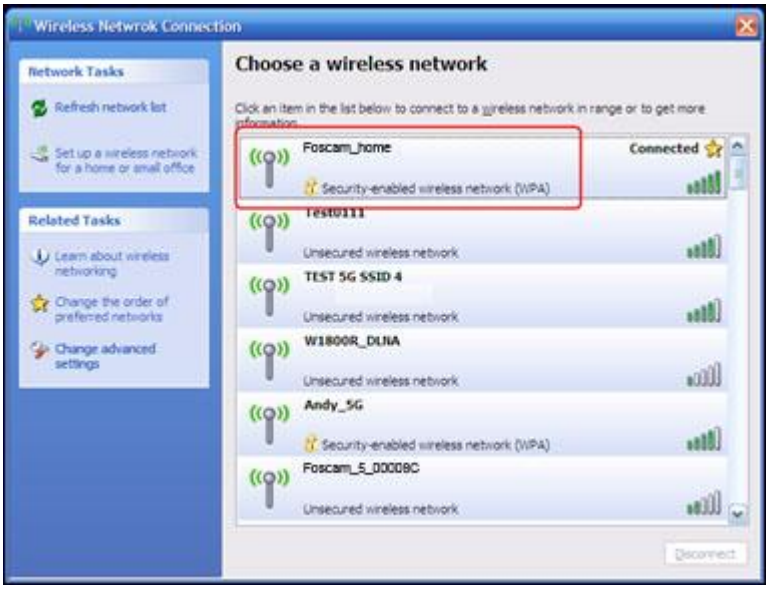
3) Right click **Wireless Network Connection** and then select **View Available Wireless Networks**.



4) Select the desired wireless network, click Connect, enter the security key and then click **OK**.



5) You can access the Internet via the device when "**Connected**" appears next to the wireless network name you selected.

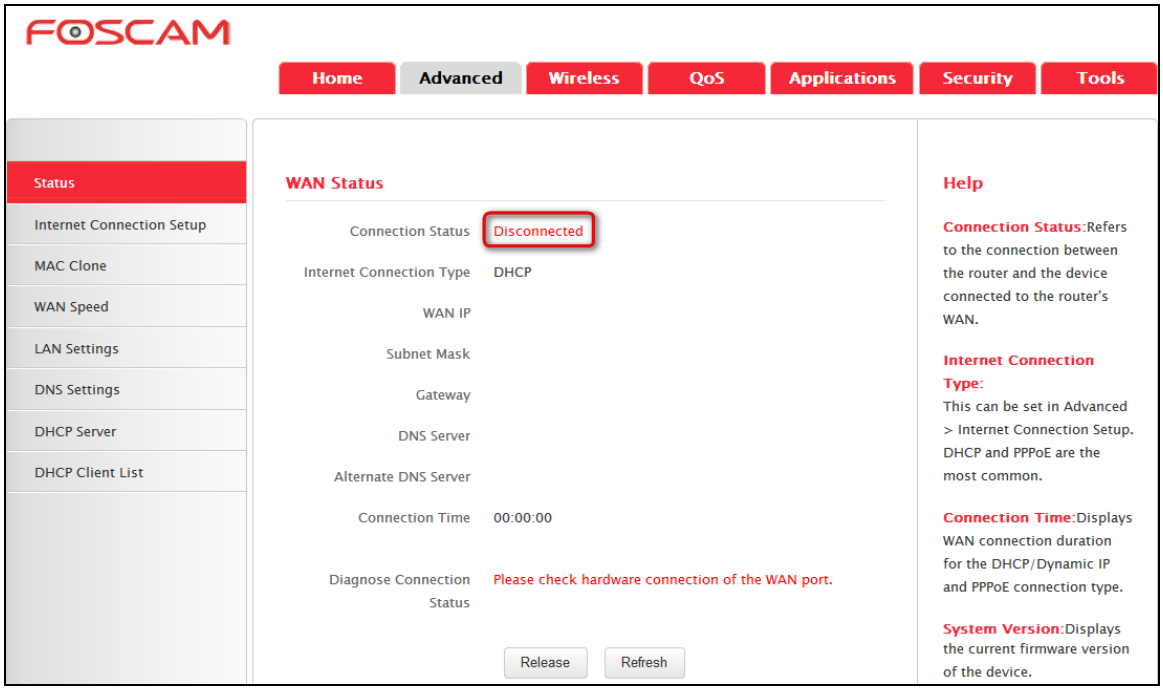


Chapter 3 Advanced Settings

1 Advanced

1.1 Status

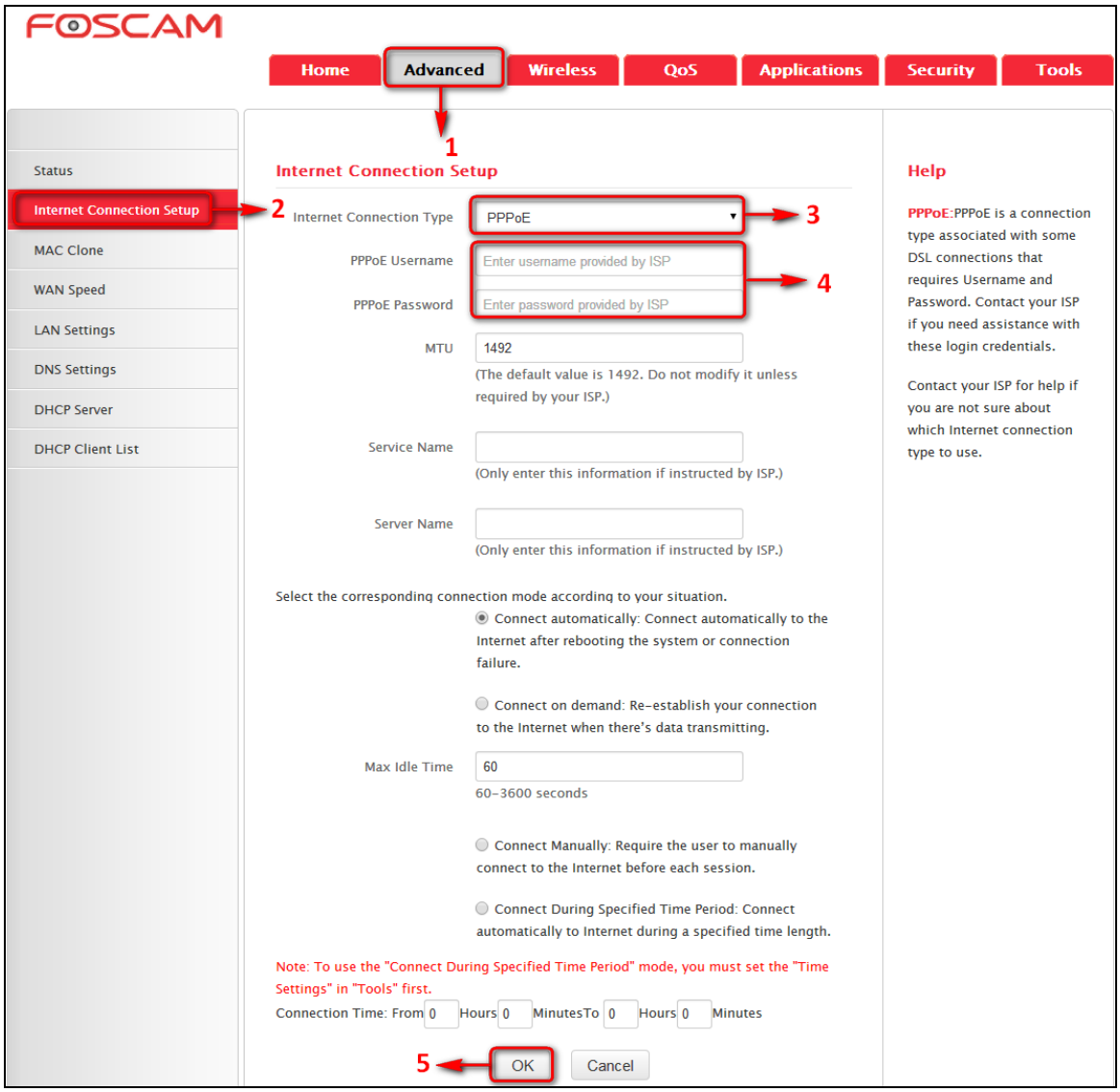
Here you can see at a glance the operating status of the device. If WAN port displays **Disconnected**, please refer to 3 Verify Internet Connection Settings.



1.2 Internet Connection Setup

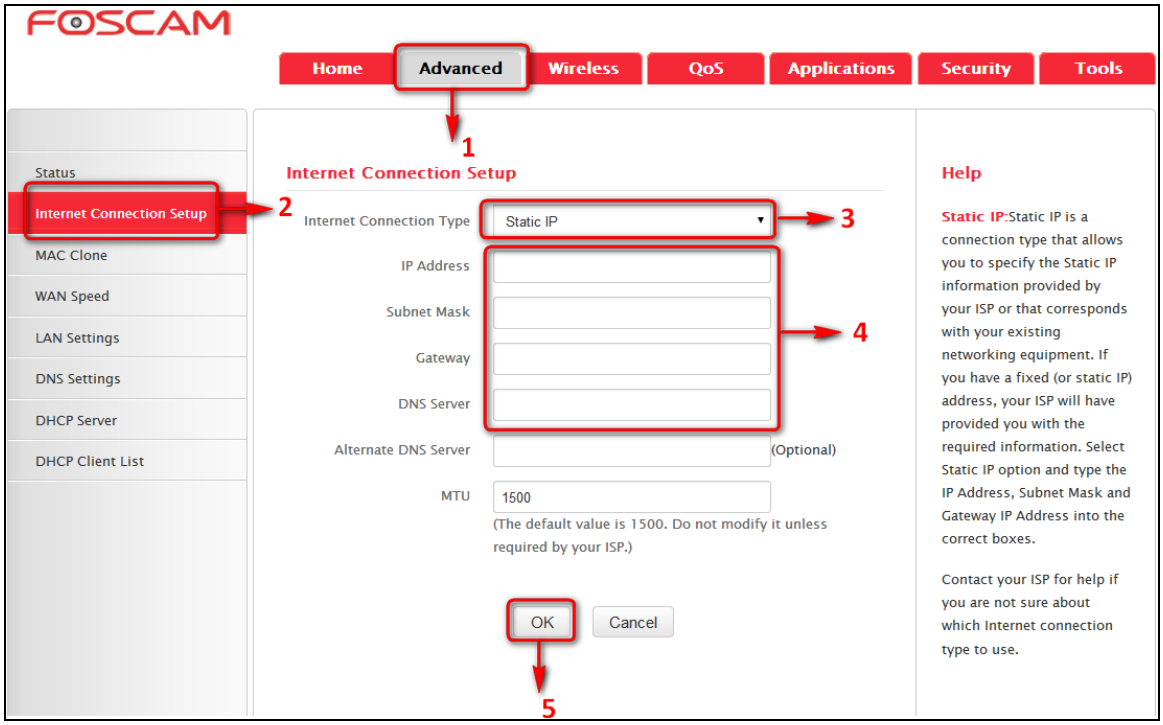
PPPoE

Select PPPoE (Point to Point Protocol over Ethernet) if you used to connect to the Internet using a broadband connection that requires a username and a password and enter the user name and password provided by your ISP.



Static IP

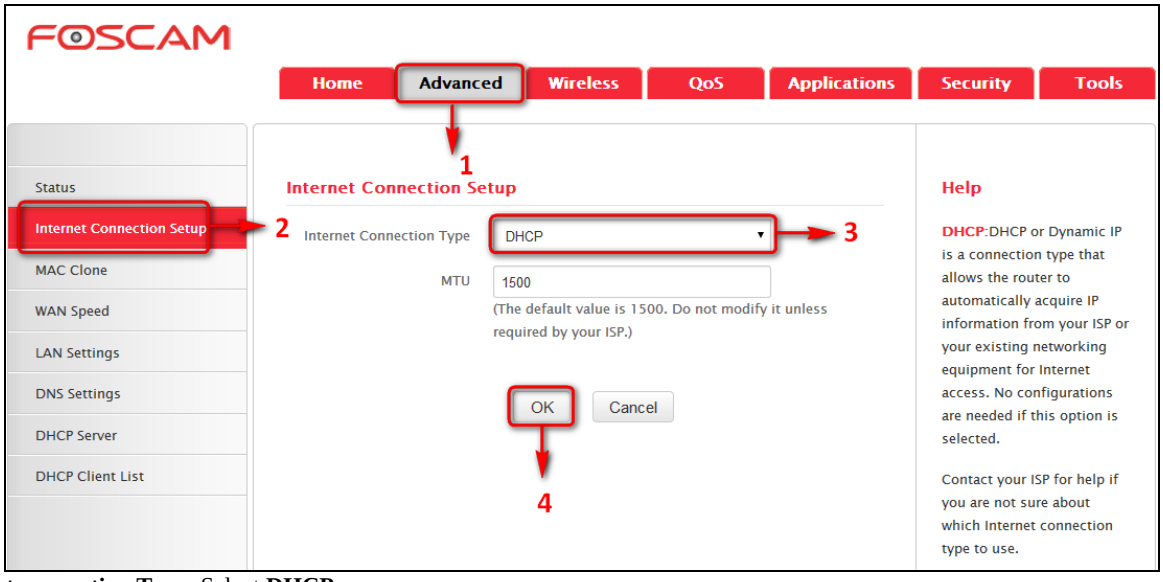
Select Static IP if your ISP provides all the needed info. You will need to enter the provided IP address, subnet mask, gateway address, and DNS address(es) in corresponding fields.



- **Internet connection Type:** Select **Static IP**.
- **IP Address:** Enter the IP address provided by your ISP. Consult your ISP if you are not clear. Consult your ISP if you are not clear.
- **Subnet mask:** Enter the subnet mask provided by your ISP.
- **Gateway:** Enter the WAN Gateway provided by your ISP.
- **DNS Server:** Enter the DNS address provided by your ISP.
- **OK:** Click it to save all your settings.

DHCP

Select **DHCP** (Dynamic IP) if you can access the Internet as soon as your computer directly connects to an Internet-enabled ADSL/Cable modem.



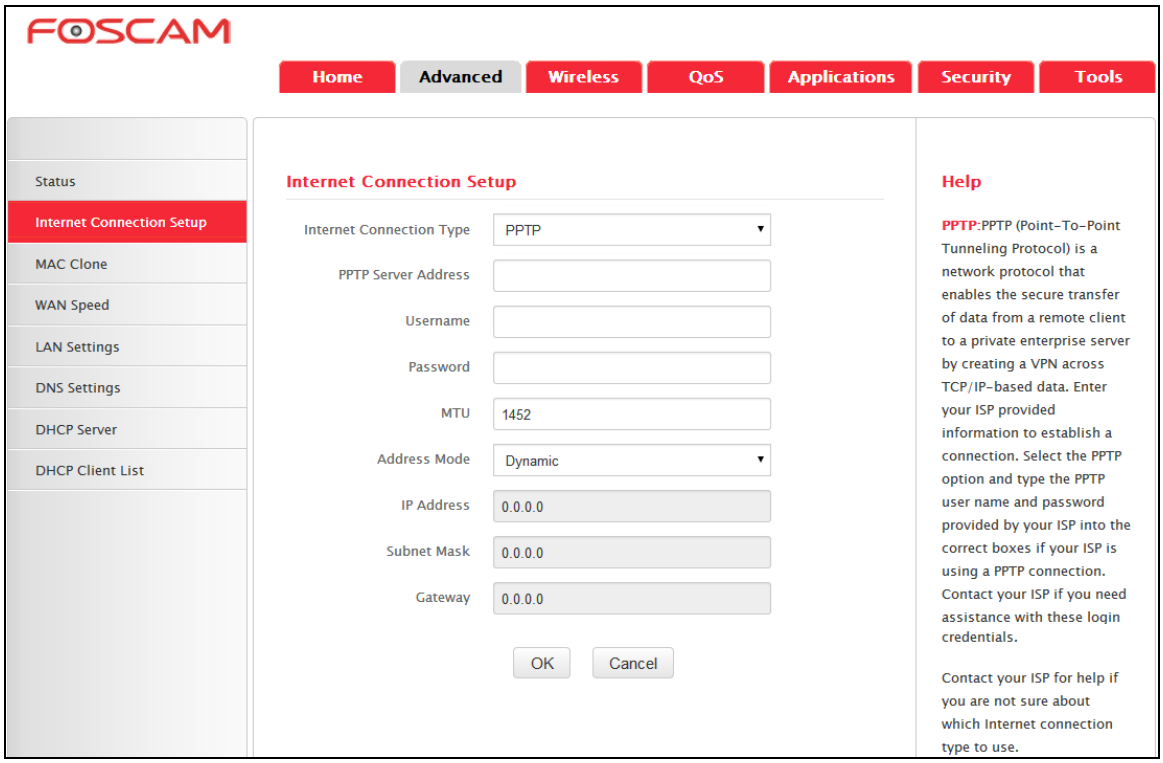
- **Internet connection Type:** Select **DHCP.**
- **MTU:** Maximum Transmission Unit. DO NOT change it from the factory default of 1500 unless instructed by your ISP. You may need to change it for optimal performance with some specific websites or application software that cannot be opened or enabled; in this case, try 1450, 1400, etc.
- **OK:** Click it to save your settings.

PPTP

Select PPTP (Point-to-Point-Tunneling Protocol) if your ISP uses a PPTP connection. The PPTP allows you to connect a router to a VPN server.

For example:

A corporate branch and headquarter can use this connection type to implement mutual and secure access to each other's resources.



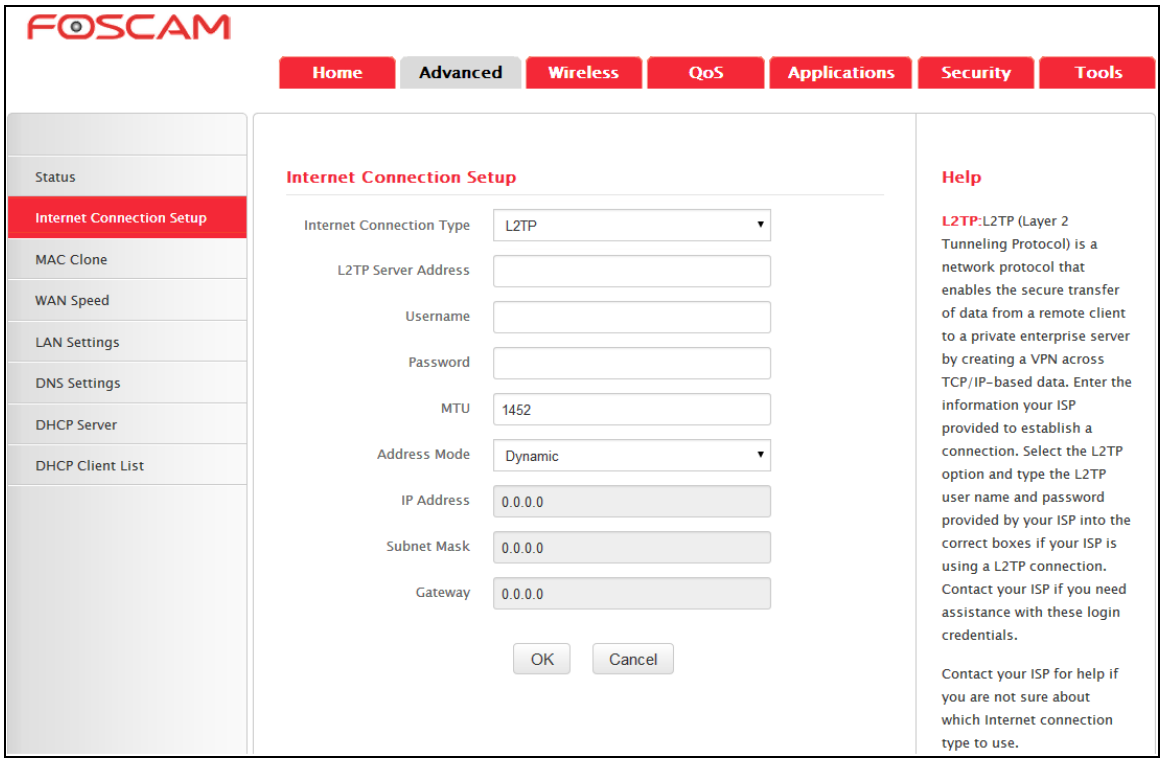
- **Internet connection Type:** Displays the current Internet connection type.
- **PPTP Server Address:** Enter the IP address of a PPTP server.
- **User Name:** Enter your PPTP User Name.
- **Password:** Enter the password.
- **MTU:** Maximum Transmission Unit. DO NOT change it from the factory default of 1492 unless instructed by your ISP. You may need to change it for optimal performance with some specific websites or application software that cannot be opened or enabled; in this case, try 1450, 1400, etc.
- **Address Mode**: Select "Dynamic" if you don't get any IP info from your ISP, otherwise select "Static". Consult your ISP if you are not clear.
- **IP Address**: Enter the IP address provided by your ISP. Consult your ISP if you are not clear.
- **Subnet mask**: Enter the subnet mask provided by your ISP.
- **Gateway**: Enter the WAN Gateway provided by your ISP. Consult your ISP if you are not clear.

L2TP

Select L2TP (Layer 2 Tunneling Protocol) if your ISP uses an L2TP connection. The L2TP connects your router to a L2TP server.

For Example:

A corporate branch and headquarter can use this connection type to implement mutual and secure access to each other's resources.



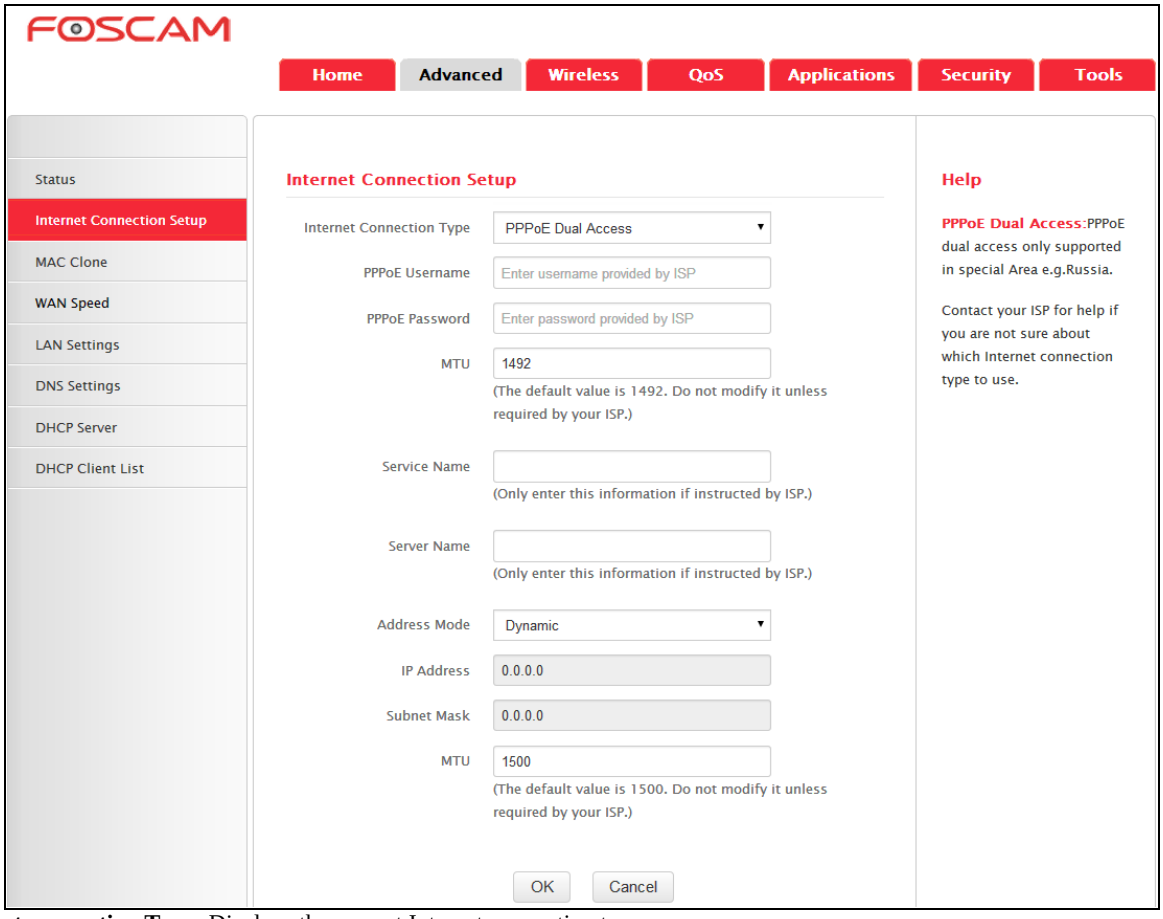
- **Internet connection Type:** Displays the current Internet connection type.
- **L2TP Server Address**: Enter the IP address of a L2TP server.
- **User Name**: Enter your L2TP username.
- **Password:** Enter the password.
- **MTU:** Maximum Transmission Unit. DO NOT change it from the factory default of 1492 unless instructed by your ISP. You may need to change it for optimal performance with some specific websites or application software that cannot be opened or enabled; in this case, try 1450, 1400, etc.
- **Address Mode:** Select "Dynamic" if you don't get any IP info from your ISP, otherwise select "Static". Consult your ISP if you are not clear.
- **IP Address:** Enter the IP address provided by your ISP. Consult your ISP if you are not clear.
- **Subnet mask:** Enter the subnet mask provided by your ISP.
- **Gateway:** Enter the WAN Gateway provided by your ISP. Consult your ISP if you are not clear.

⚠ **Note:**

- PPPOE, PPTP and L2TP cannot be used simultaneously!
- For PPTP and L2TP Internet connections, only Static IP or Dynamic IP is available.
- Note that PPTP and L2TP may not be available on some products.

PPPoE Dual Access

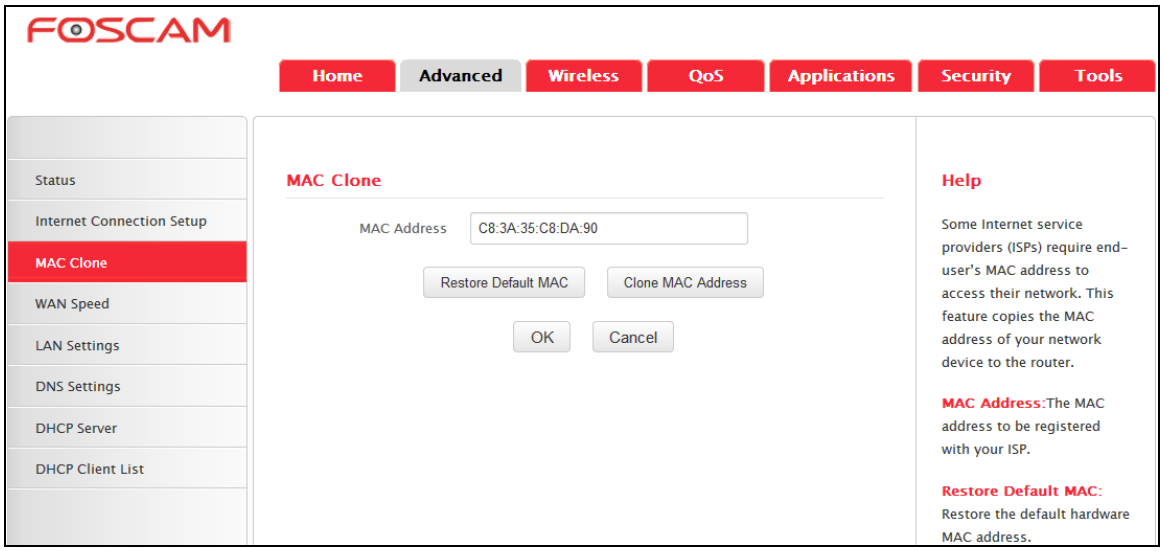
PPPoE dual access only supported in special Area e.g. Russia.



- **Internet connection Type:** Displays the current Internet connection type.
- **PPPoE User Name:** Enter the User Name provided by your ISP.
- **PPPoE Password:** Enter the password provided by your ISP.
- **MTU:** Maximum Transmission Unit. DO NOT change it from the factory default value unless necessary.
- **Service Name:** Description of PPPoE connection. Leave blank unless otherwise required.
- **Server Name:** Description of server. Leave blank unless otherwise required.
- **Address Mode:** Select "Dynamic" if you don't get any IP info from your ISP, otherwise select "Static". Consult your ISP if you are not clear.
- **IP Address:** Enter the IP address provided by your ISP. Consult your ISP if you are not clear.
- **Subnet mask:** Enter the subnet mask provided by your ISP.

1.3 MAC Clone

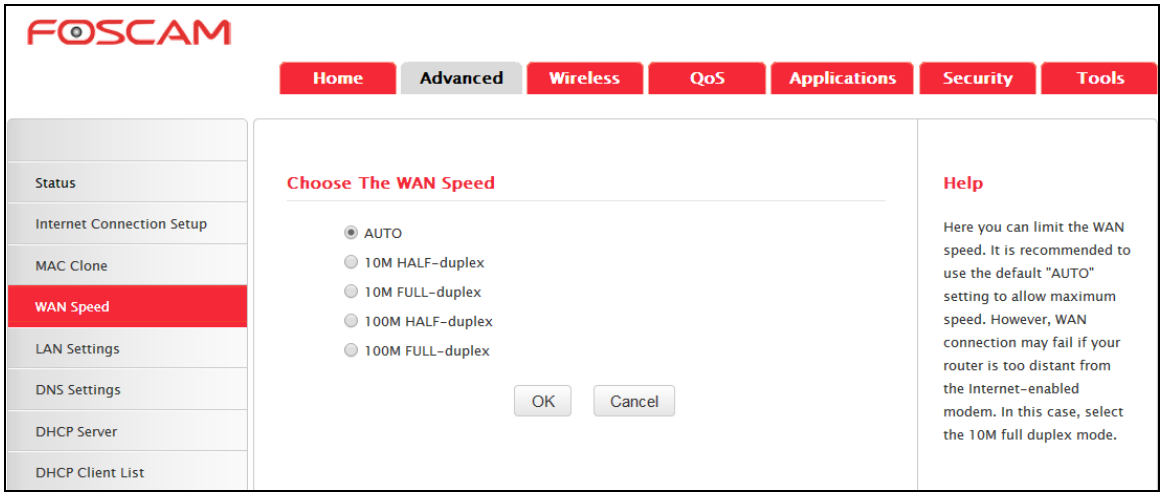
Some Internet service providers (ISPs) require end-user's MAC address to access their network. This feature copies the MAC address of your network device to the router.



- **MAC Address:** Configure device's WAN MAC address.
- **Clone MAC Address:** Click to copy your PC's MAC address to the device as a new WAN MAC address.
- **Restore Default MAC:** Reset device's WAN MAC to factory default.

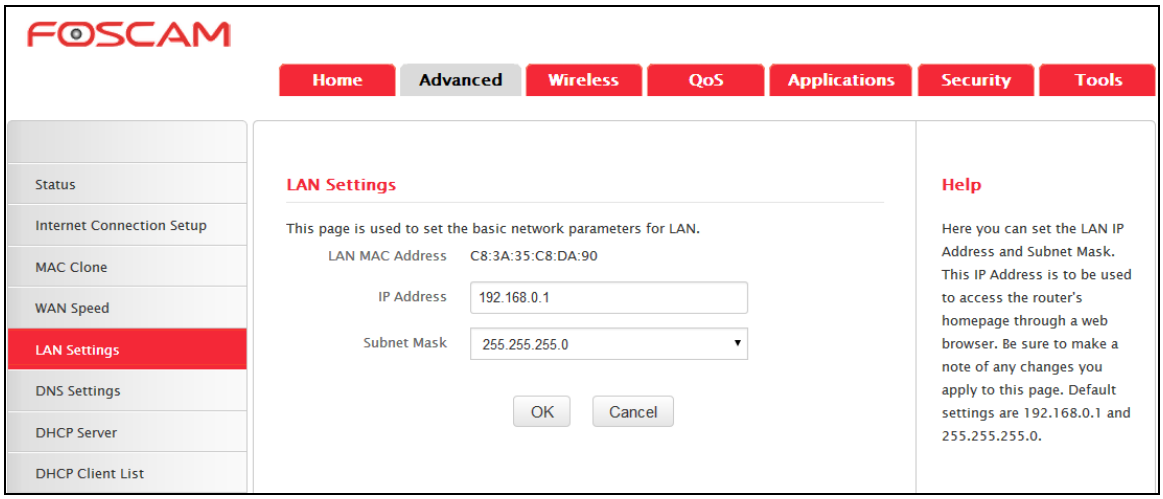
1.4 WAN Speed

Here you can set the speed and duplex mode for WAN port. It is advisable to keep the default **AUTO** setting to get the best speed.



1.5 LAN Settings

Click **Advanced** > **LAN Settings** to enter the screen below:



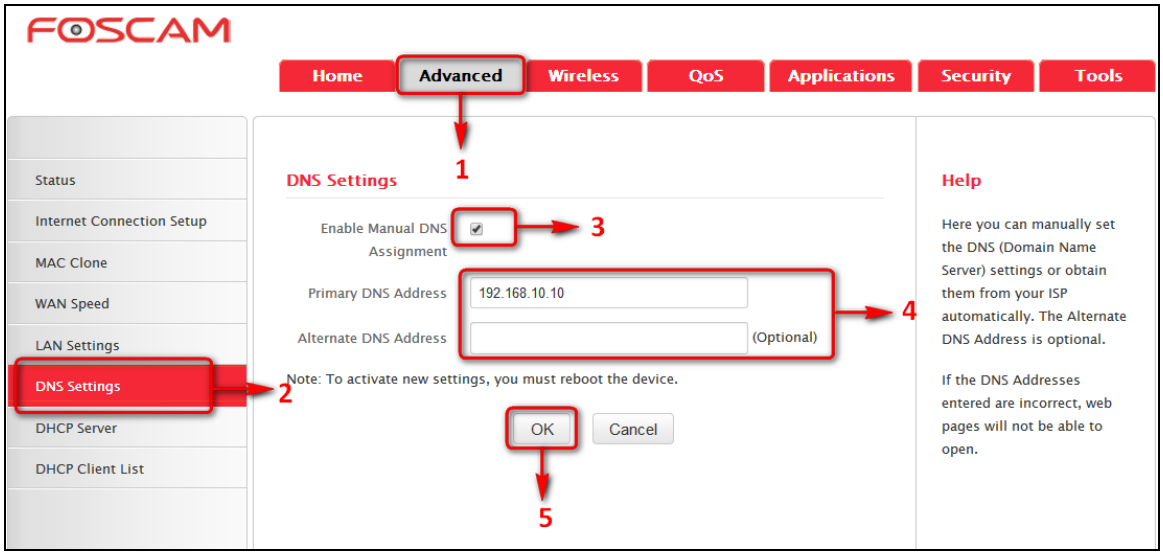
- **LAN MAC Address:** Displays device's LAN MAC address, which is NOT changeable.
- **IP Address:** Device's LAN IP address. The default is 192.168.0.1. You can change it according to your need.
- **Subnet Mask:** Device's LAN subnet mask, 255.255.255.0 by default.
- **OK:** Click to save your settings.

⚠**Note：**

If the default IP address is changed, you must enter the new IP address to log in.

1.6 DNS Settings

DNS is short for Domain Name System or Domain Name Service.



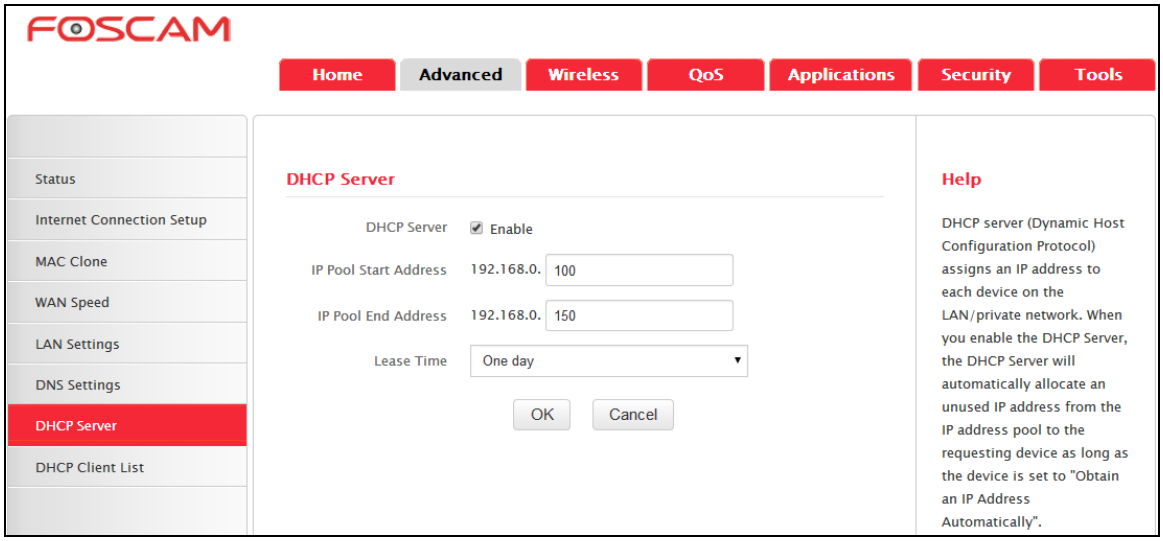
- **Enable Manual DNS Assignment:** Check to activate DNS settings.
- **Primary DNS Server：** Enter the primary DNS address provided by your IPS.
- **Alternate DNS Server：** Enter the other DNS address if your ISP provides such addresses (optional).
- **OK:** Click to save your settings.

⚠**Note:**

- Web pages are not able to open if DNS server addresses are entered incorrectly.
- Do remember to reboot the device to activate new settings when you finish all settings.

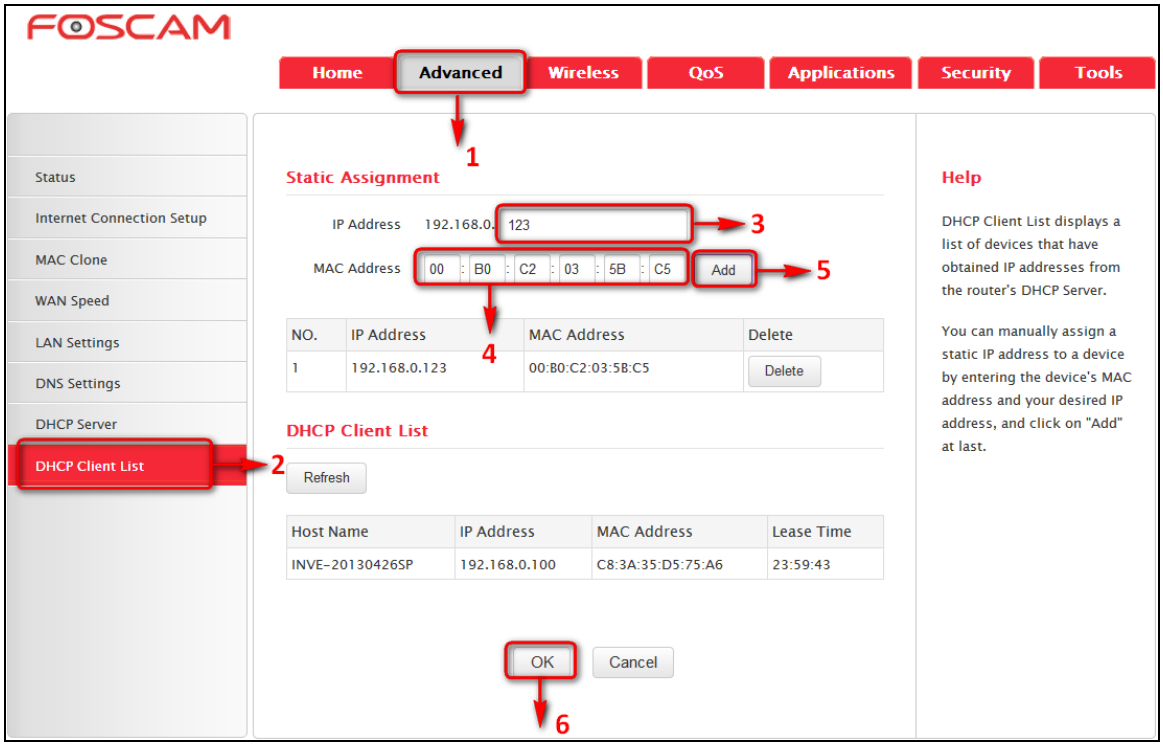
1.7 DHCP Server

The Dynamic Host Configuration Protocol (DHCP) is an automatic configuration protocol used on IP networks. If you enable the built-in DHCP server on the device, it will automatically configure the TCP/IP settings for all your LAN computers (including IP address, subnet mask, gateway and DNS etc), eliminating the need of manual intervention. Just be sure to set all computers on your LAN to be DHCP clients by selecting "Obtain an IP Address Automatically" respectively on each such PC. When turned on, these PCs will automatically load IP information from the DHCP server. (This feature is enabled by default. Do NOT disable it unless necessary).



1.8 DHCP Client List

DHCP Client List displays information of devices that have obtained IP addresses from the device's DHCP Server. If you would like some devices on your network to always get the same IP addresses, you can manually add a static DHCP reservation entry for each such device.



- **IP Address:** Enter the IP address for static DHCP reservation.
- **MAC Address:** Enter the MAC address of a computer to always receive the same IP address (the IP you just specified).
- **Add:** Click to add the entry to the MAC address reservation list.
- **OK:** Click to save your settings.

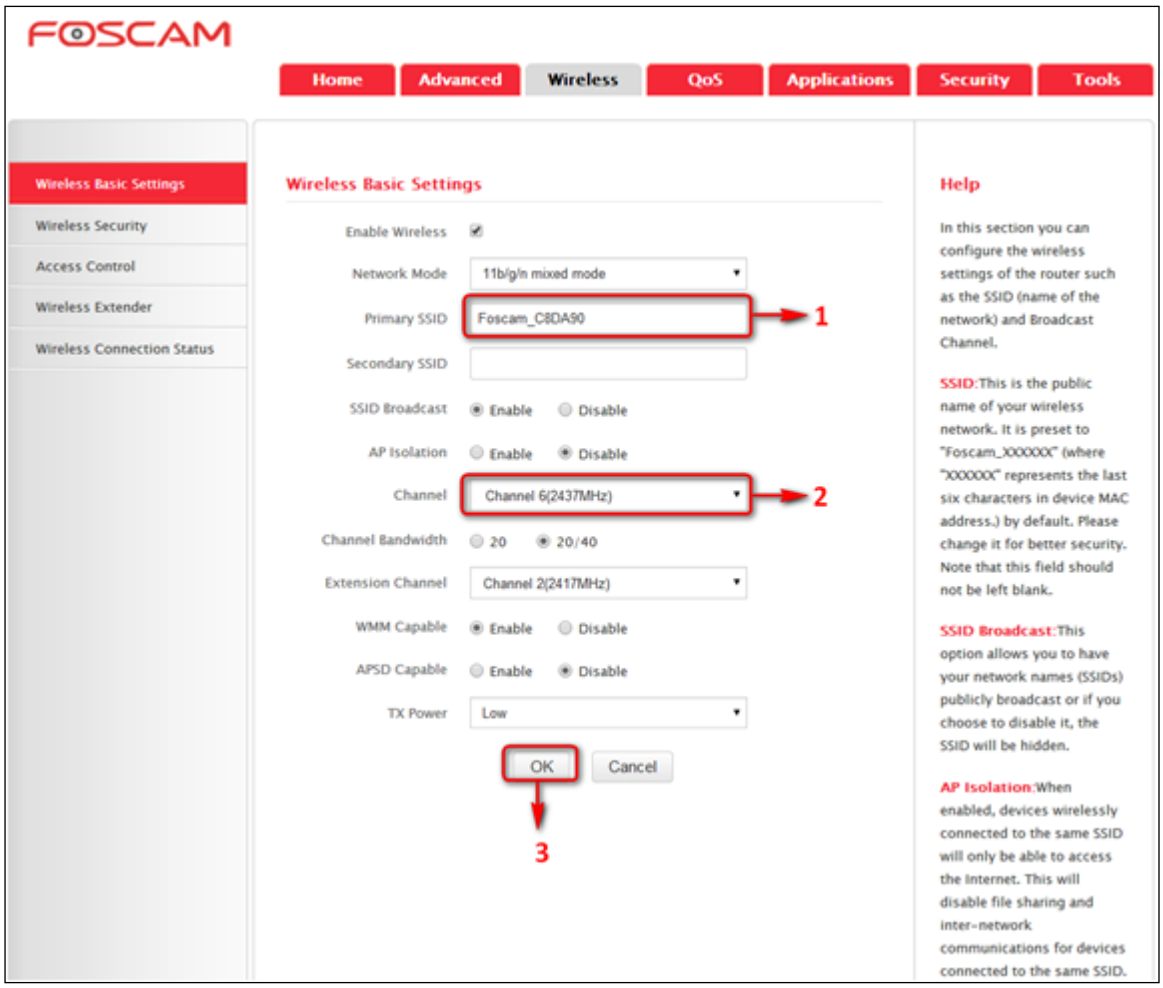
⚠Note:

If the IP address you have reserved for your PC is currently used by another client, then you will not be able to obtain a new IP address from the device's DHCP server, instead, you must manually specify a different IP address for your PC to access the Internet.

2 Wireless Settings

2.1 Wireless Basic Settings

If you want to create a WLAN for sharing Internet connection, simply click **Wireless-> Wireless Basic Settings**. Change the SSID, you can name it whatever you like. For example, select 2437MHz (channel 6) and leave other options unchanged and then click **OK**.



- **SSID:** This is the public name of your wireless network. The default is Foscam_XXXXXX. XXXXXX is the last six characters in the device's MAC address. It is recommended that you change it for better security and identification.
- **Channel:** Select a channel that is the least used by neighboring networks from the drop-down list or Auto. Channels 1, 6 and 11 are recommended.
- **OK:** Click to save your settings.

2.2 Wireless Security

Wireless Security Setup

This section allows you to secure your wireless network and block unauthorized accesses and malicious packet sniffing. To encrypt your wireless network, do as follows:

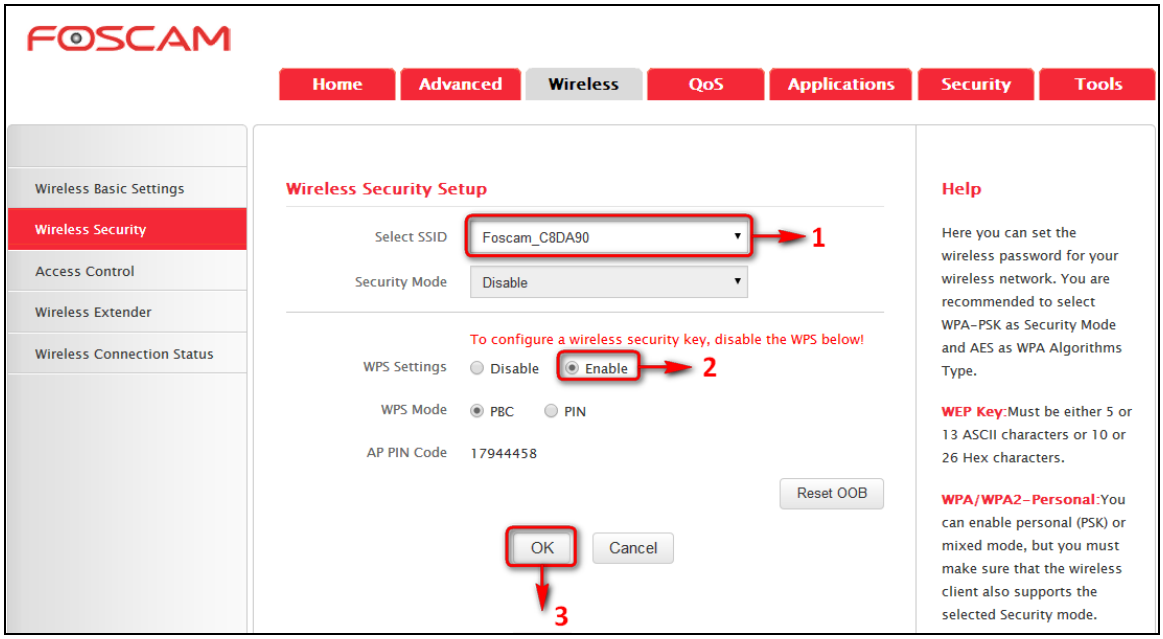
1. Select the wireless network (SSID) you wish to encrypt.
2. Disable WPS. (WPS is enabled on the router by default. If you want to use other security modes, you must first disable the WPS.)
3. Select a proper security mode and cipher type (also known as WPA Algorithm or WPA Encryption Type). WPA-PSK and AES are recommended by system default (5 security modes are available for your selection. Among them, WPA-PSK outstands with greater compatibility and security. For more information of other security modes, see appendix 2). Specify a security key that includes at least 8 characters.
4. Click **OK** to complete your settings.

Note:
You can also select other security modes as you need.

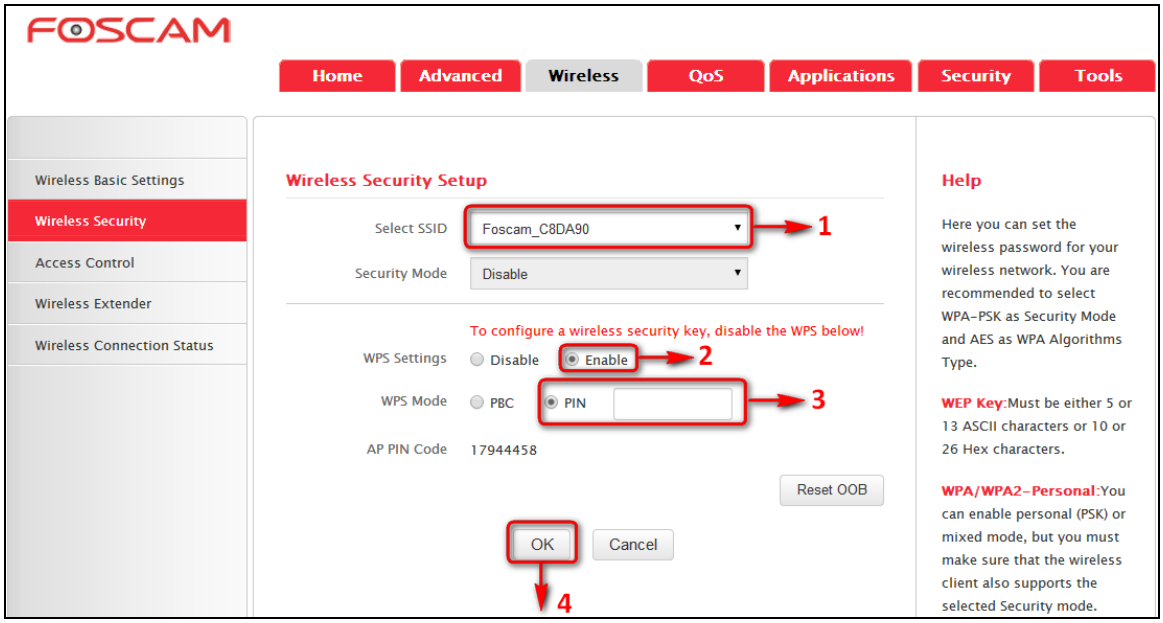
WPS

Wi-Fi Protected Setup makes it easy for home users who know little of wireless security to establish a home network, as well as to add new devices to an existing network without entering long passphrases or configuring complicated settings. Simply enter a PIN code or press the software PBC button or hardware WPS button (if any) and a secure wireless connection is established.

Operation Instructions:
PBC: To use WPS-PBC, try the way below:
Press the hardware WPS button on the router for about 1 second and then enable WPS/PBC on the client device within 2 minutes.

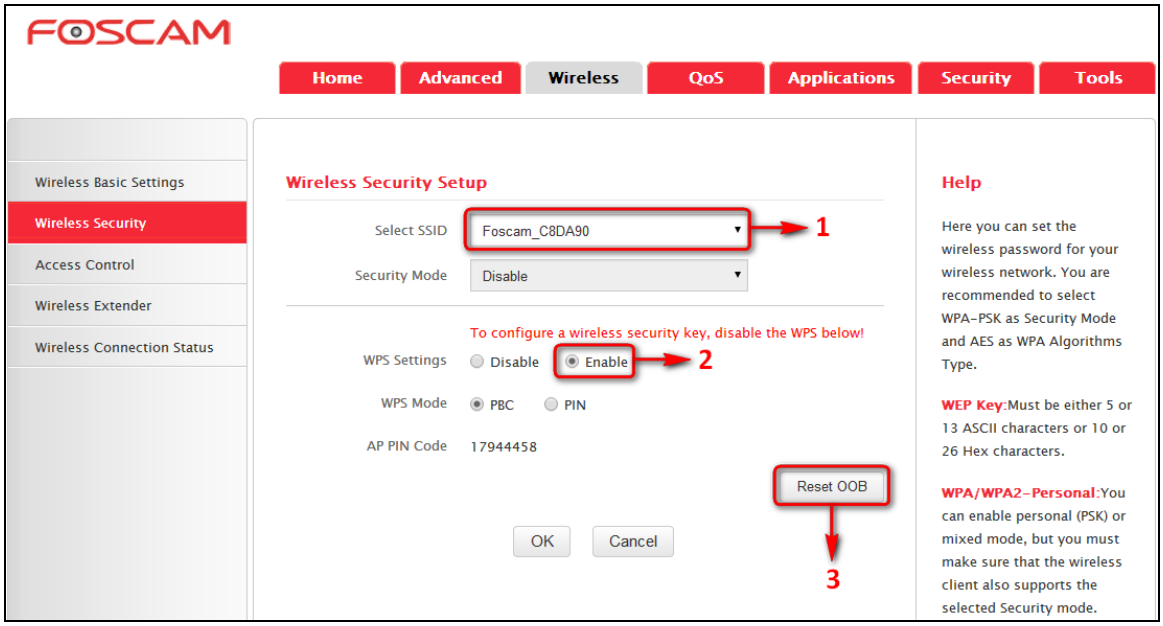


PIN: On the wireless security page, enable **WPS**, select **PIN** and enter the 8-digit PIN code from network adapter; then, within 2 minutes, enable **WPS/PIN** on the client device.



⚠Note：

- With WPS successfully enabled, the WPS LED on the router keeps blinking for about 2 minutes, and during this time, you can enable WPS on a wireless adapter; if the adapter successfully joins the wireless network, the WPS LED will display a solid light. Repeat steps above if you want to add more wireless adapters to the router.
- **Reset OOB:** Clicking this button will reset SSID to factory default and disable security mode.
- Existing wireless settings will still be maintained by default after a successful WPS connection. Namely security settings and SSID on the router will still be the same. If you want to generate a random wireless key via WPS, click **Reset OOB** and then follow WPS setup instructions above.



⚠Note:

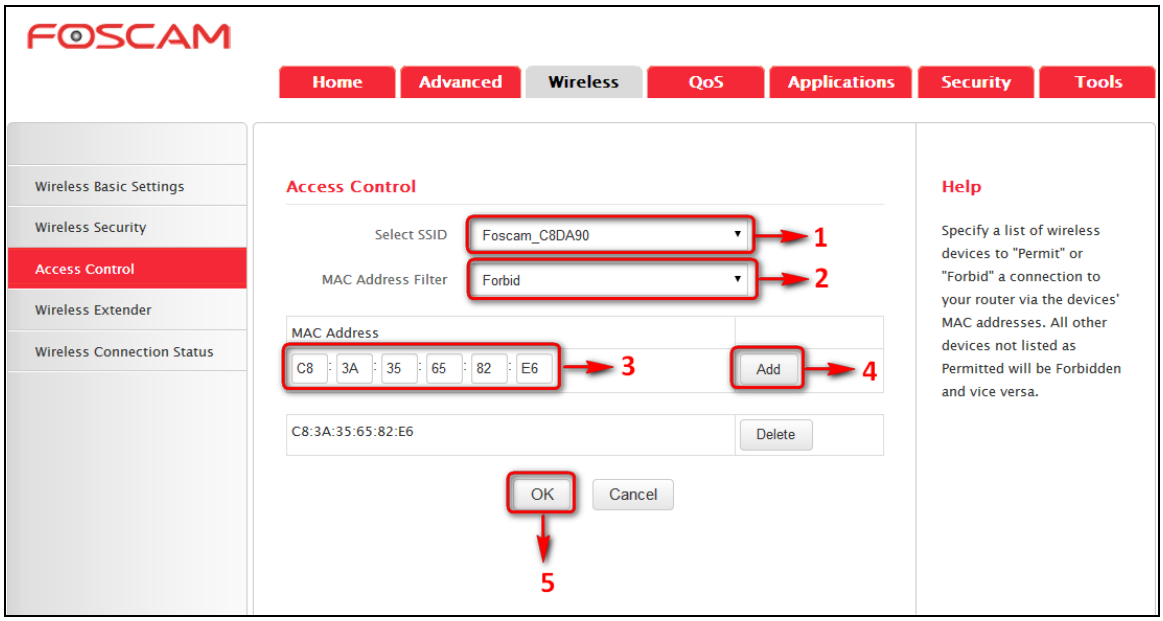
- To use the WPS security, the wireless client must be also WPS-capable.
- Before you press the hardware WPS button on the device for WPS/PBC connection, making sure the WPS feature has been enabled on the device.

2.3 Access Control

The Access Control feature allows you to specify a list of devices to Permit or Forbid a connection to your wireless network via the devices' MAC addresses. All other devices not listed as Permitted will be Forbidden and vice versa.

1. Select the wireless network (SSID) you wish to enable Access Control on.
2. **MAC Address Filter:** Select Permit or Forbid from the drop-down list.
3. To permit a wireless device to connect to your wireless network, select Permit, enter its MAC address, click Add and then OK. Then only this device listed as "Permitted" will be able to connect to your wireless network; all other wireless devices will forbidden.

Example: To forbid the PC at the MAC address of C8:3A:35:65:82:E6 from connecting to your wireless network, do as follows:



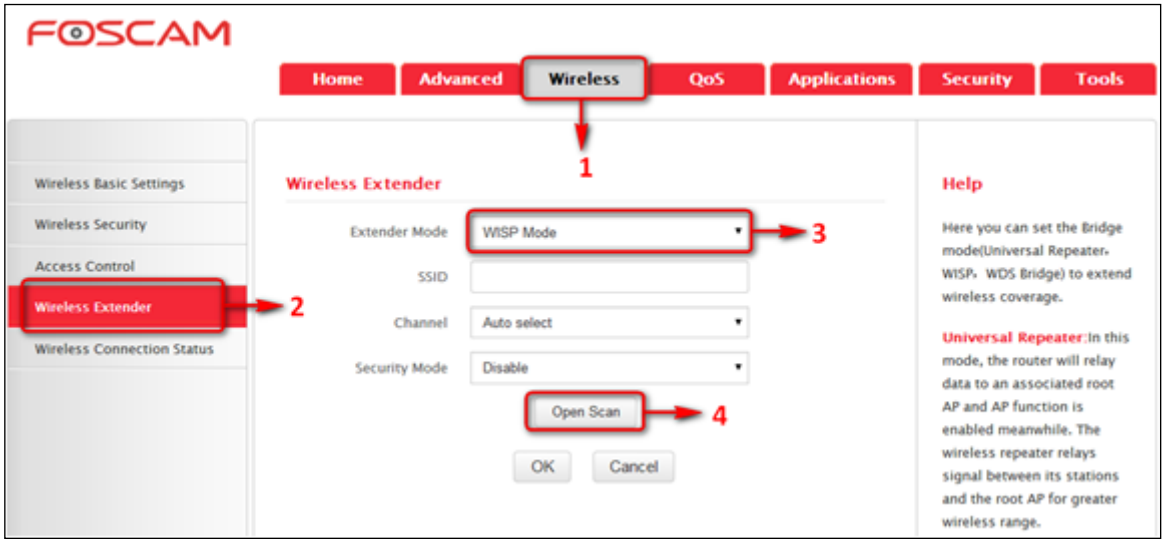
Step1. Select an SSID, say, **Foscam_C8DA90**.
Step2. Select **Forbid** from the corresponding drop-down menu.
Step3. Enter C8:3A:35:65:82:E6 in the MAC address box and click **Add**.
Step4. Click **OK** to save your settings. You can add more wireless MAC addresses you wish to forbid.

2.4 Wireless Extender

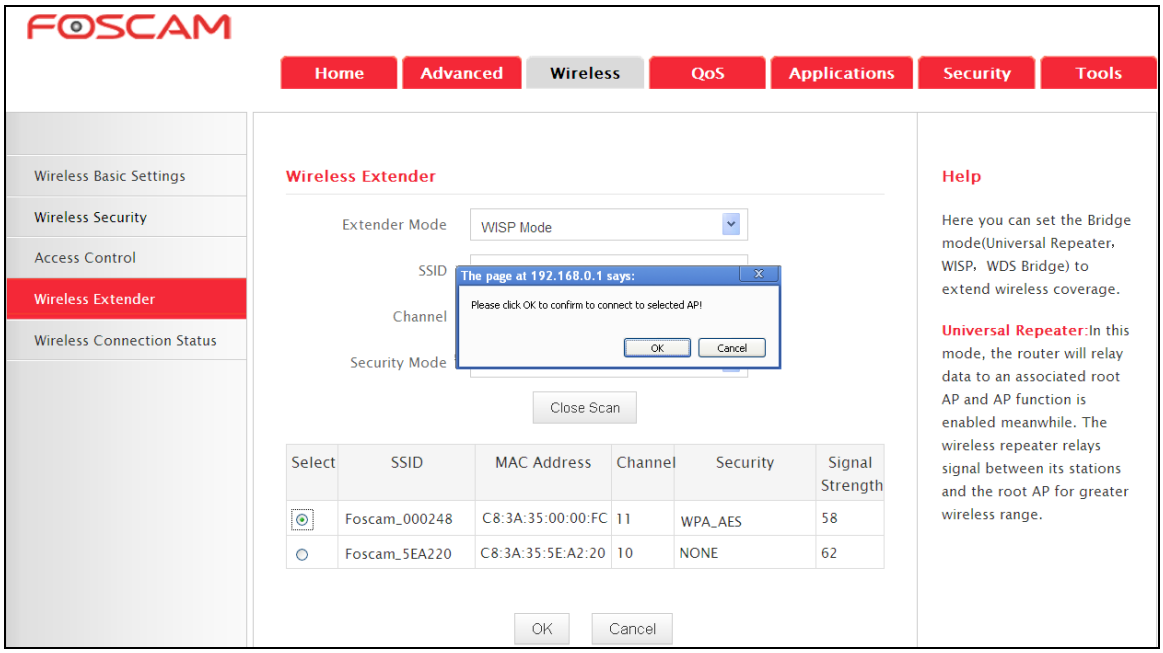
WISP Mode

If your router acquires Internet access from a wireless Access Point, please select WISP mode. Specific steps are as follows:

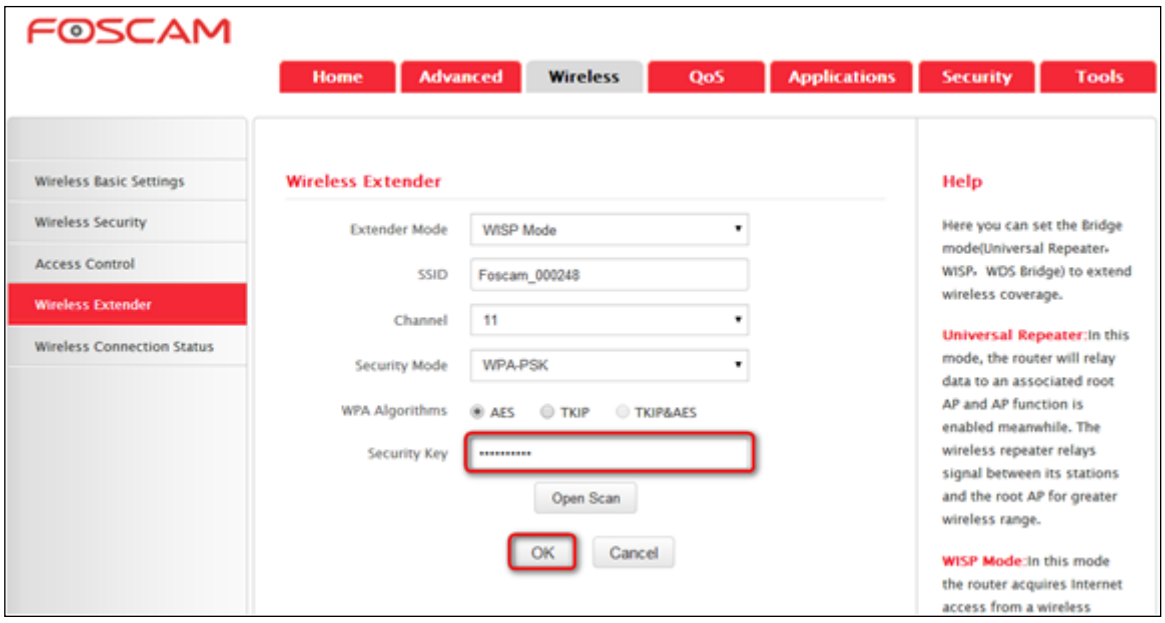
1. Click **Wireless**>**Wireless Extender**, select **WISP mode** and click **Open Scan**.



2. Select the AP you wish to connect, such as Foscam-000248, click **OK**, and click **Close Scan** ;

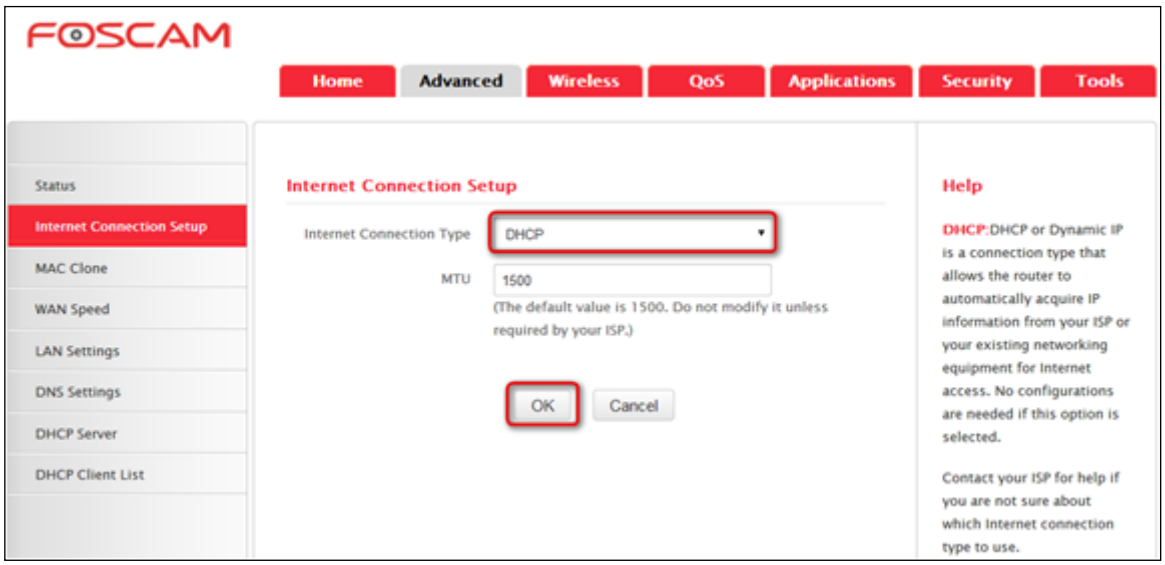


3. Enter the wireless security key of the selected SSID , and click **OK.**

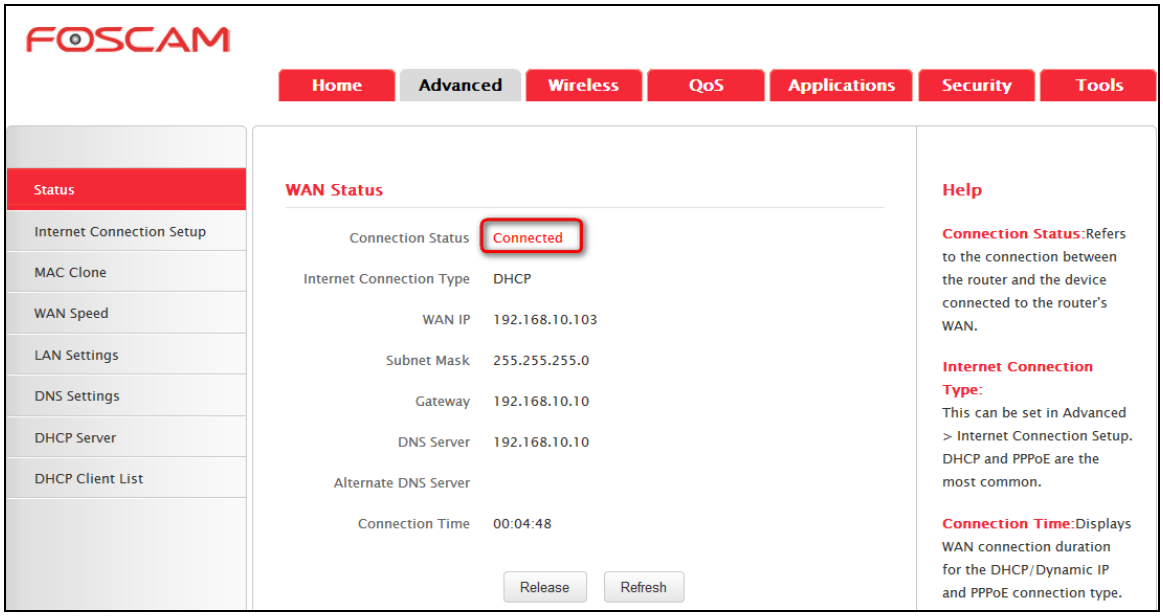


4. Save the settings and the router will reboot automatically.

5. Internet Connection Setup: Click **Advanced**>**Internet Connection Setup**, select Internet Connection Setup, such as DHCP, and click **OK**.



6. Click **Advanced**>**Status** and the connection status displays **Connected**.



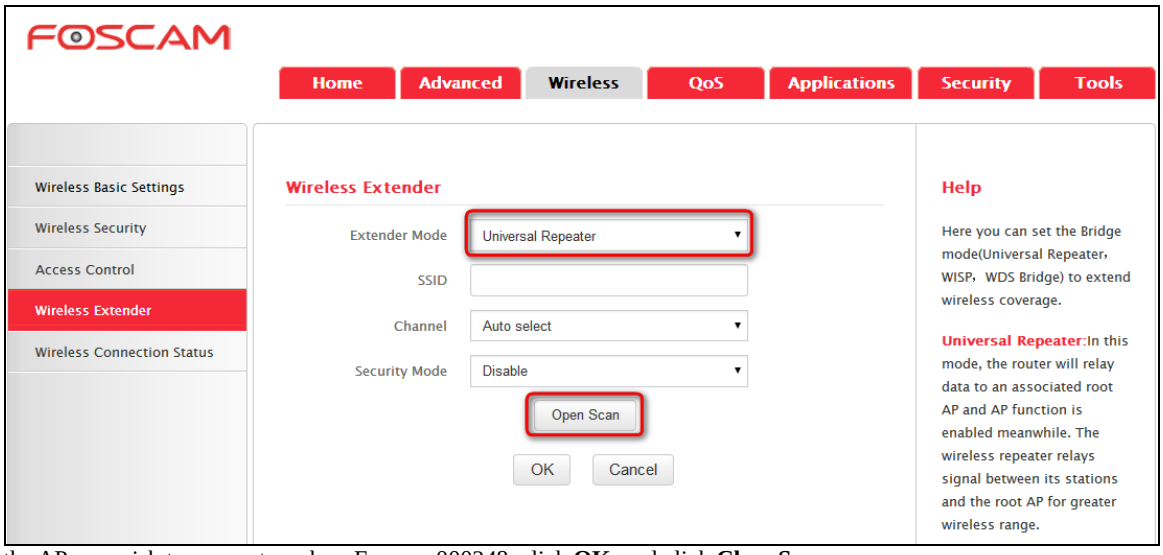
⚠Note :

- When the settings finished, remember to enter **Internet Connection Setup** to set up Internet connection.
- Verify that the SSID, channel, and security mode on the page match those of the added wireless network. If not, manually correct them.
- For the normal wireless connection between two routers, do not change this router's SSID settings, including SSID, channel, security mode and security key.

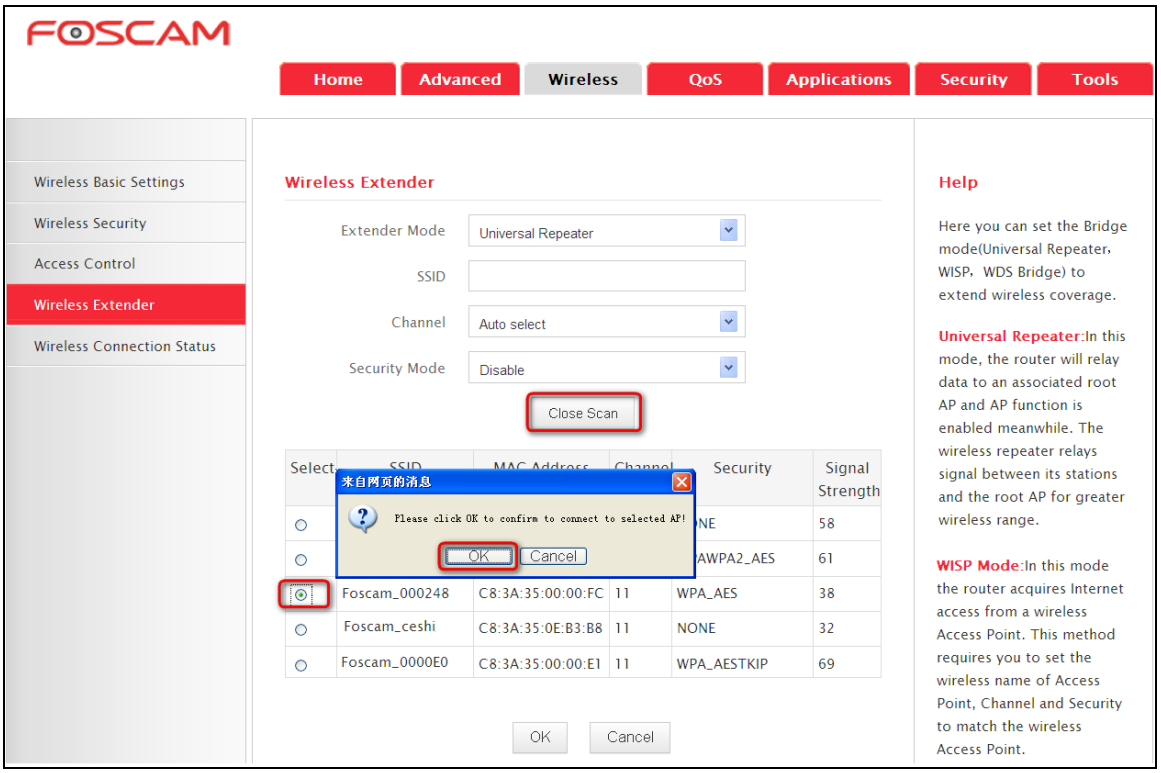
Universal Repeater Mode

In this mode, the router will relay data to an associated root AP and AP function is enabled meanwhile. The wireless repeater relays signal between its stations and the root AP for greater wireless range. Steps are shown as below:

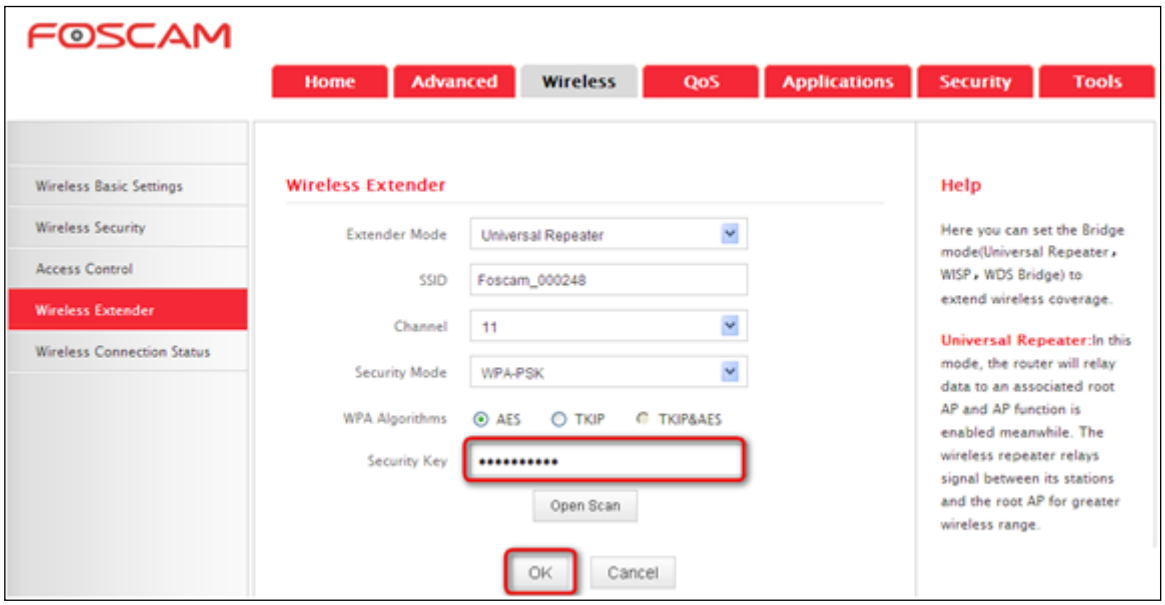
1. Click **Wireless**>**Wireless Extender**, select **Universal Repeater** in the extender mode and click **Open Scan**.



2. Select the AP you wish to connect, such as Foscam-000248, click **OK**, and click **Close Scan**;



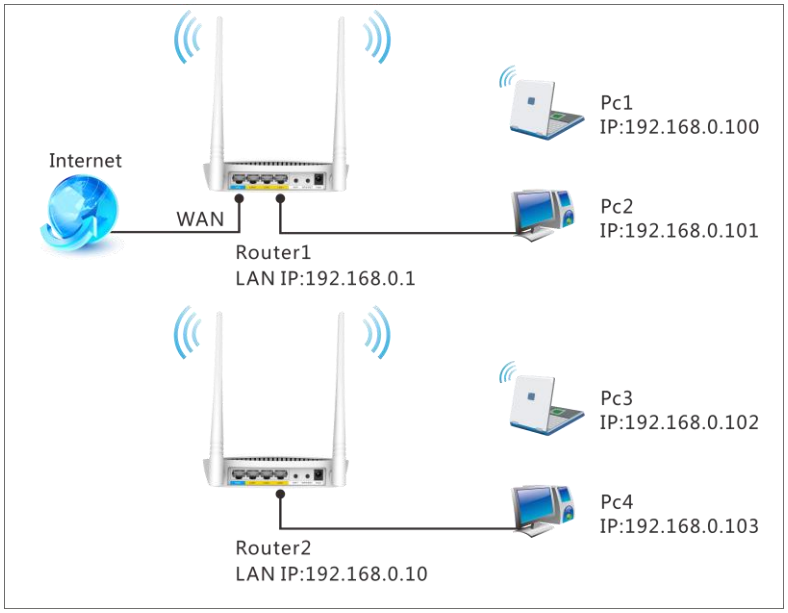
7. Enter the wireless security key of the selected SSID ,and click **OK.**



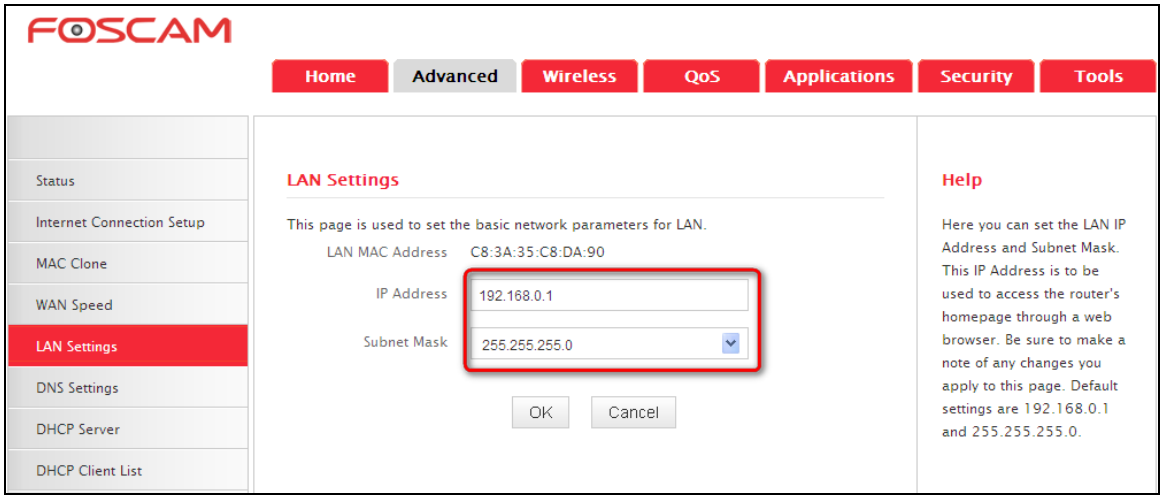
8. Save the settings and the router will restart automatically.

WDS Bridge Mode

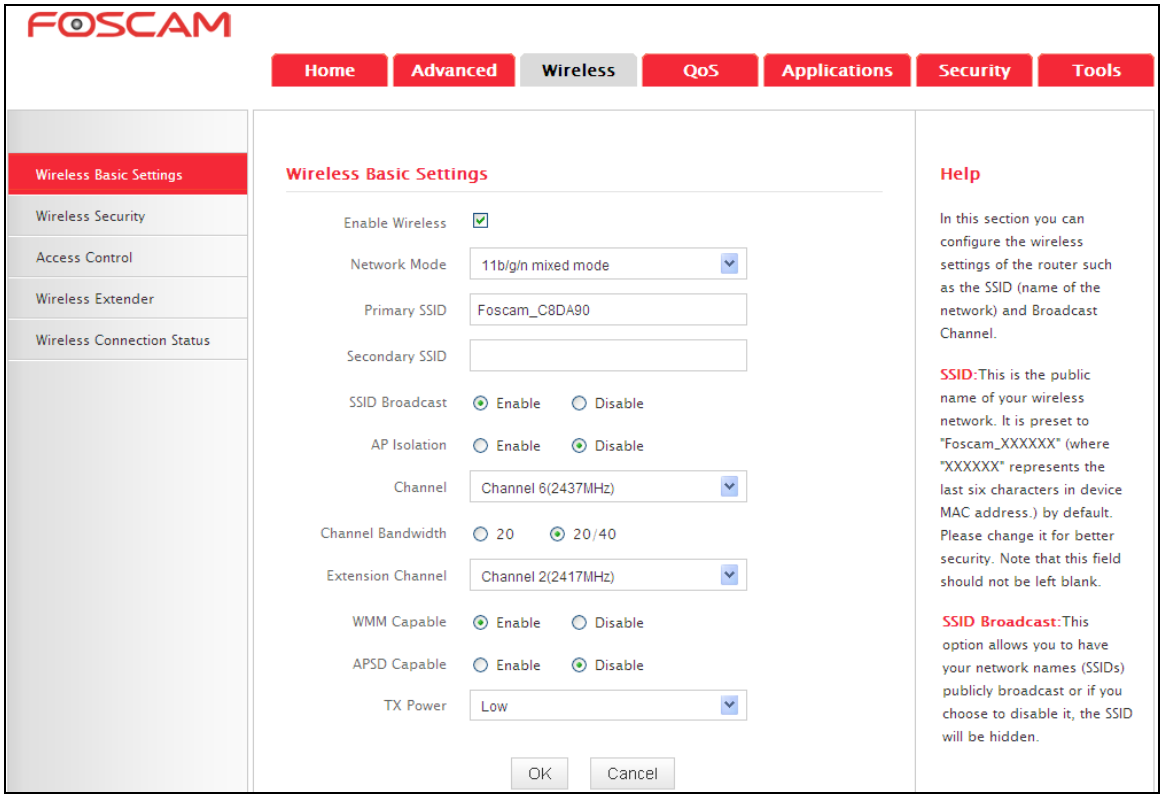
Wireless distribution system (WDS) is a system enabling the wireless interconnection of access points in an IEEE 802.11 network. It allows a wireless network to be expanded using multiple access points without the traditional requirement for a wired backbone to link them. Note: The Access Points you select must support WDS.



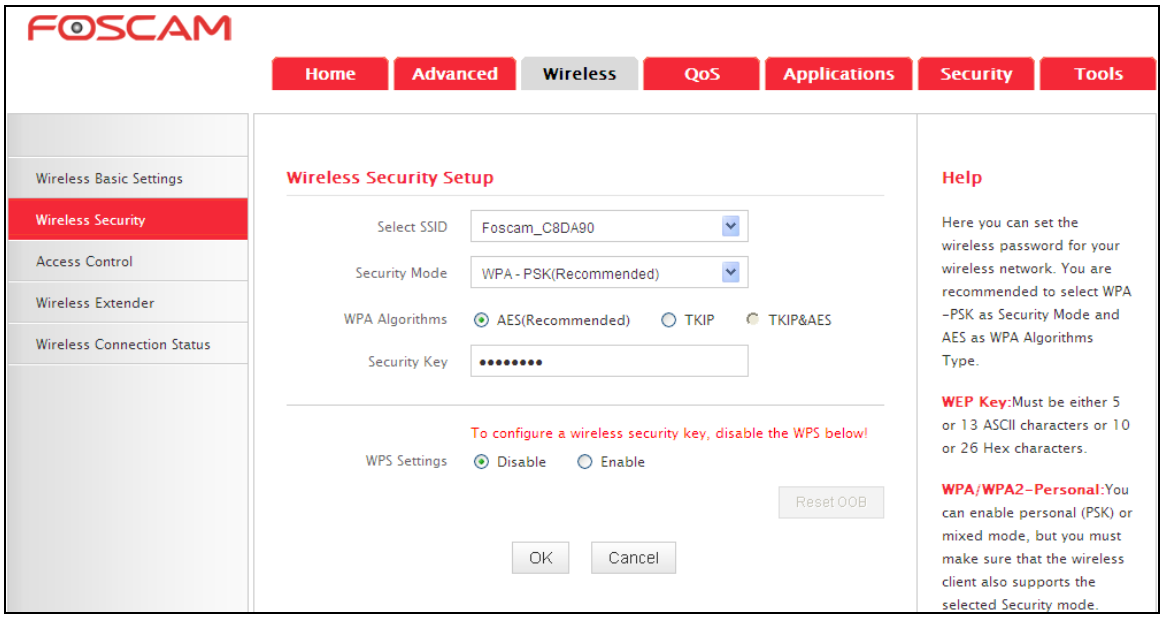
For example:
As seen in the figure above, PC1 and PC2 access the Internet via a wireless connection to Router 1. While PC3 and PC4 are too far to directly connect to Router 1 for Internet access. Now you can use the WDS bridge feature to let PC3 and PC4 access the Internet.
Before you get started:
1. View and note down the wireless security settings: security mode, cipher type, security key, etc. on Router 1; Click **Status**>**LAN Settings** and check the IP address.



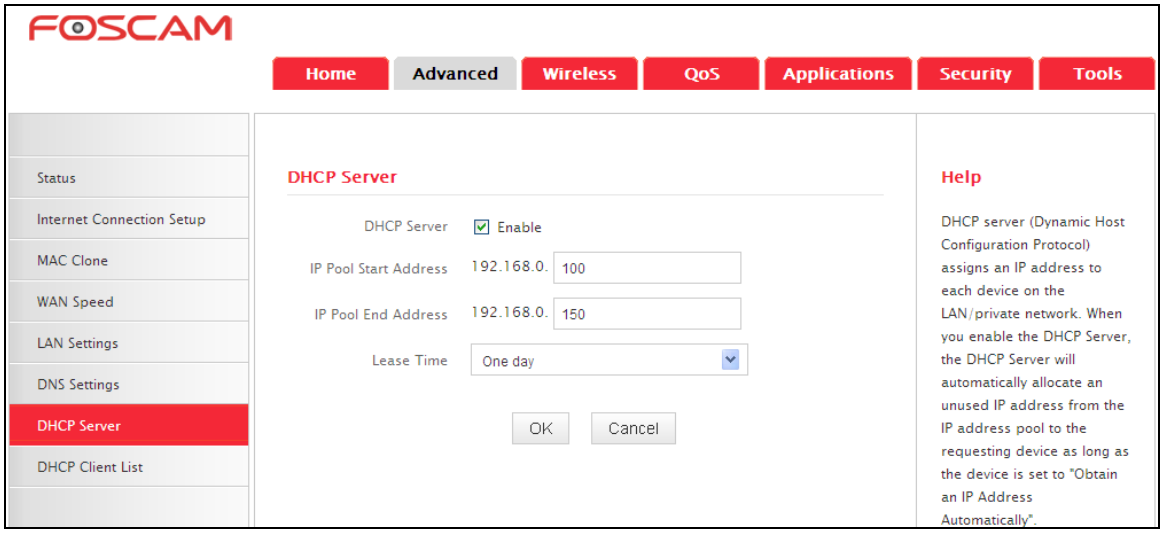
2. Click **Wireless**>**Wireless Basic Settings** to check router one's wireless basic settings.



3. Click W**ireless>Wireless Security** to check router one's wireless security settings.



4. Verify that DHCP server is enabled on Router 1: Click **Advanced**>**DHCP Server**.



5. Set the LAN IP address of Router 2 to a different address yet on the same net segment as Router 1.

As shown below:

Router 1:

LAN IP: 192.168.0.1;

Subnet Mask: 255.255.255.0;

Router 2:

LAN IP：192.168.0.10;

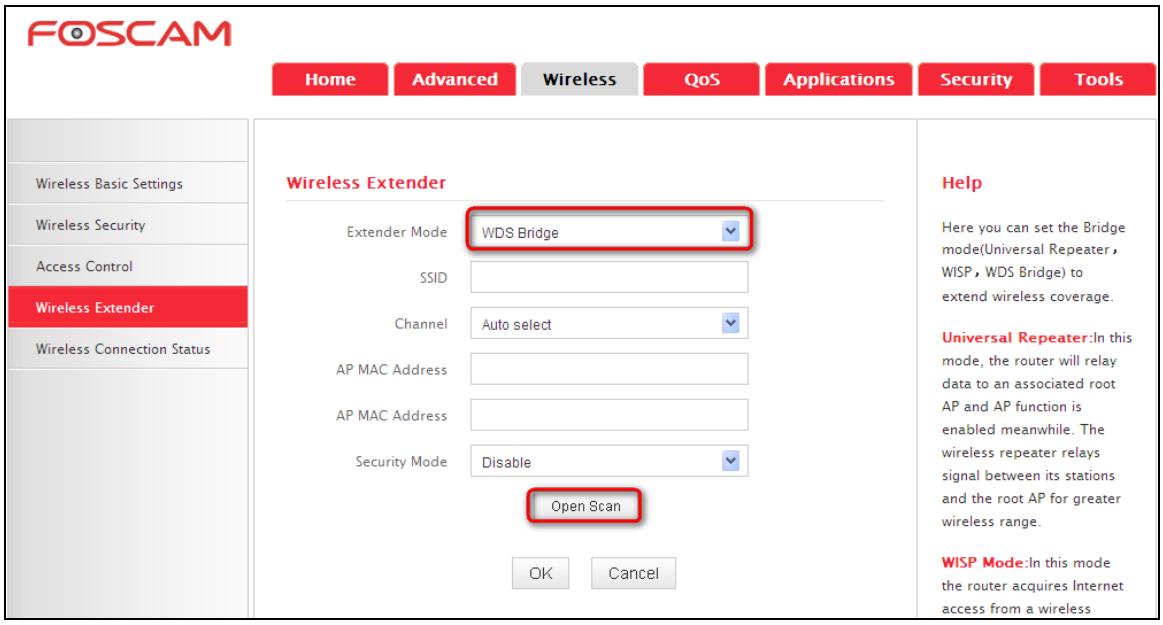
Subnet Mask: 255.255.255.0;

Then do as follows:

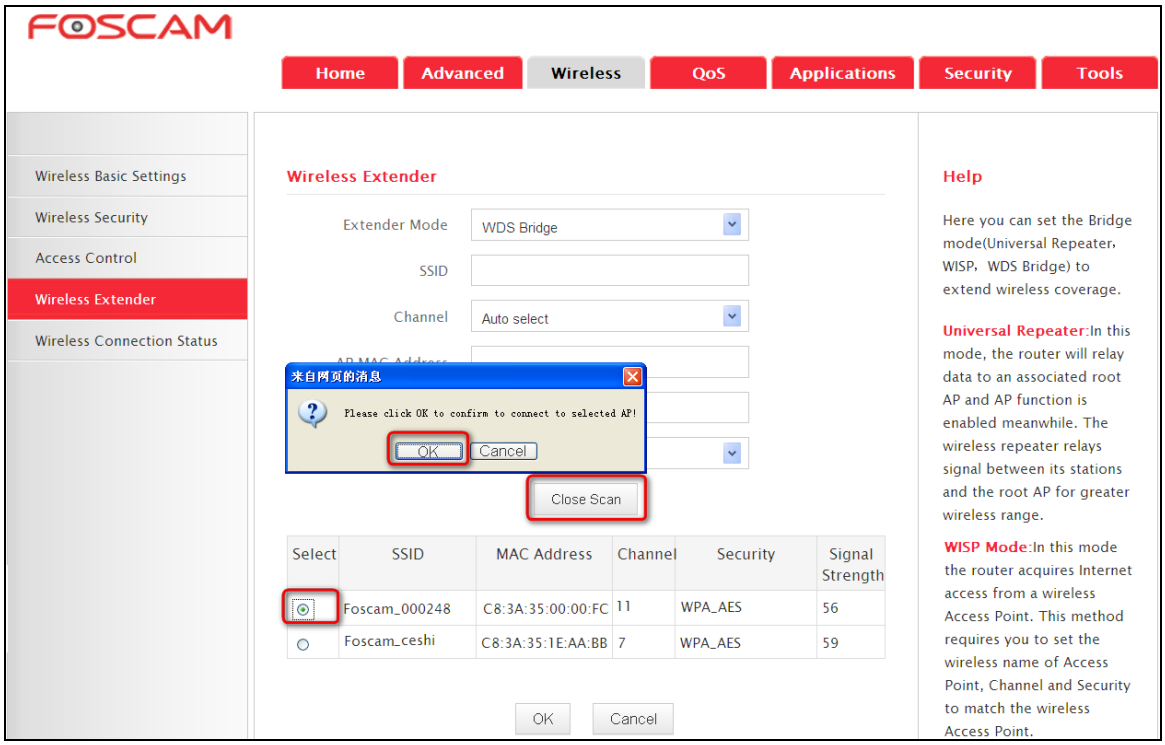
1. Configure Router 2:

1) Wireless Working Mode: Select WDS Bridge Mode.

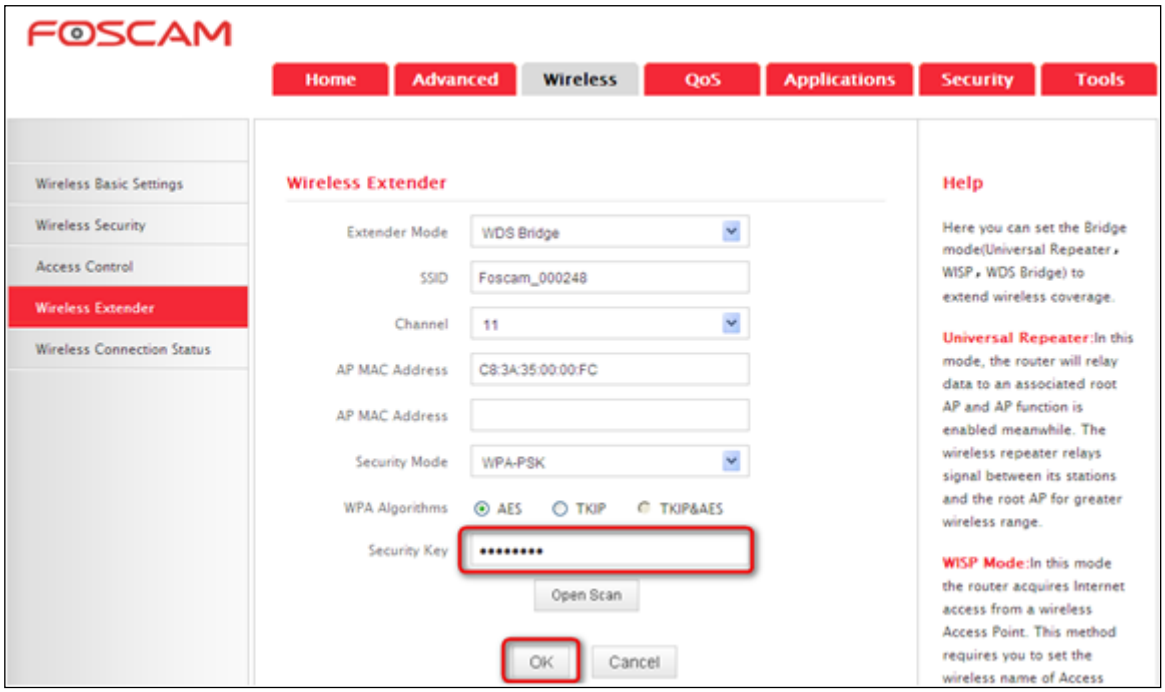
2) Click **Open Scan** to search for Router 1.



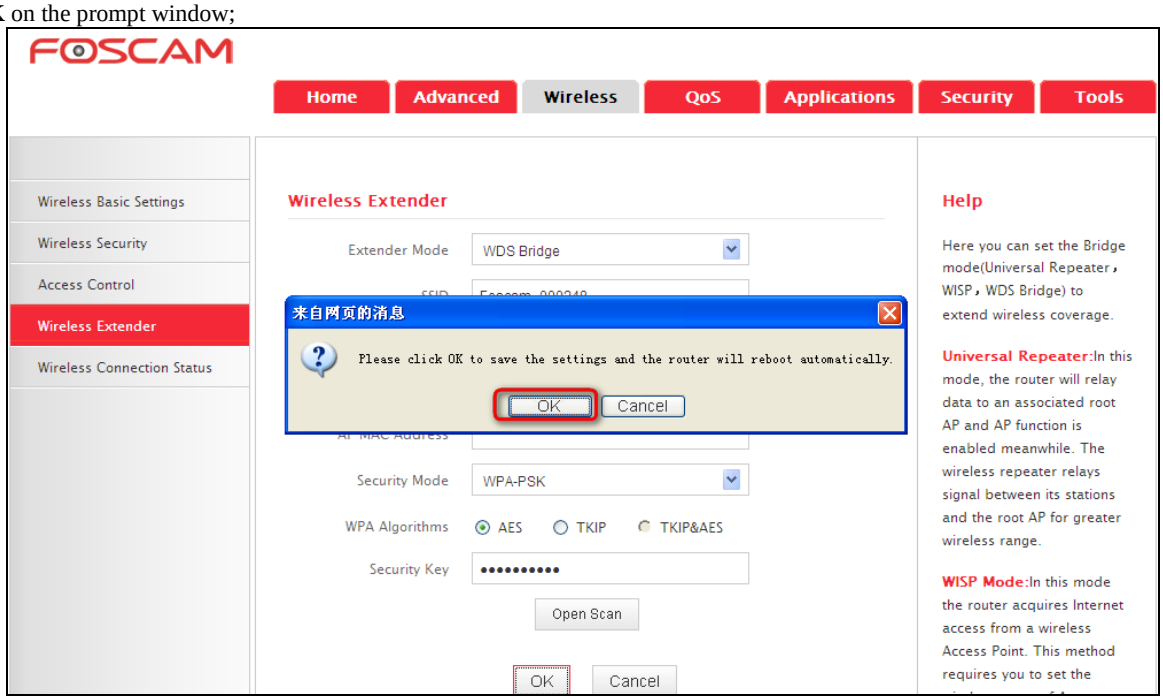
3) Select the wireless network to connect click **OK**, and click **Close Scan**;



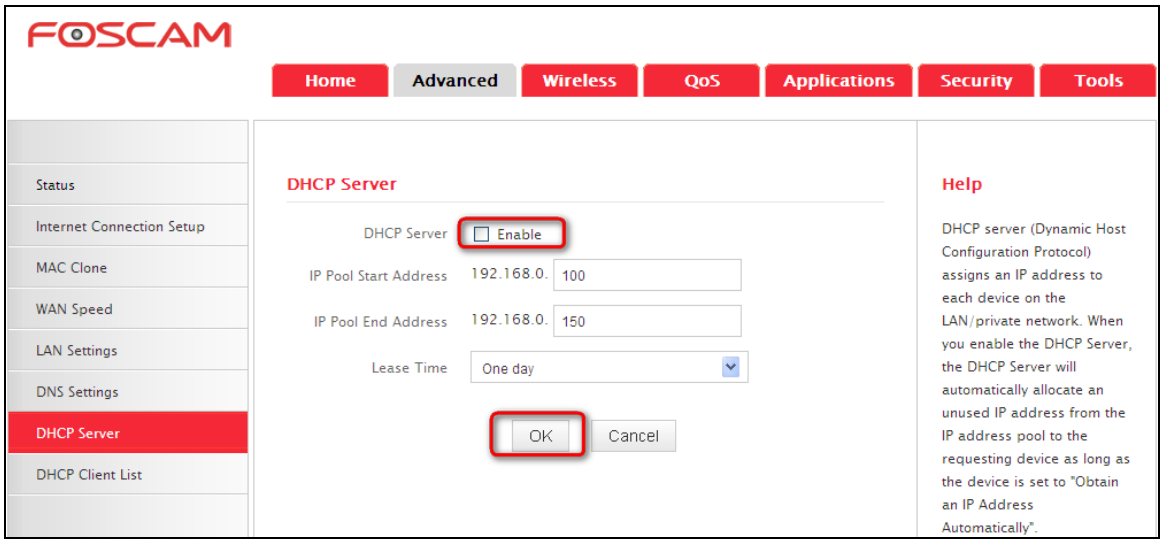
4) Enter the wireless security key of the selected SSID ,and click **OK.**



6) Click **OK** on the prompt window;

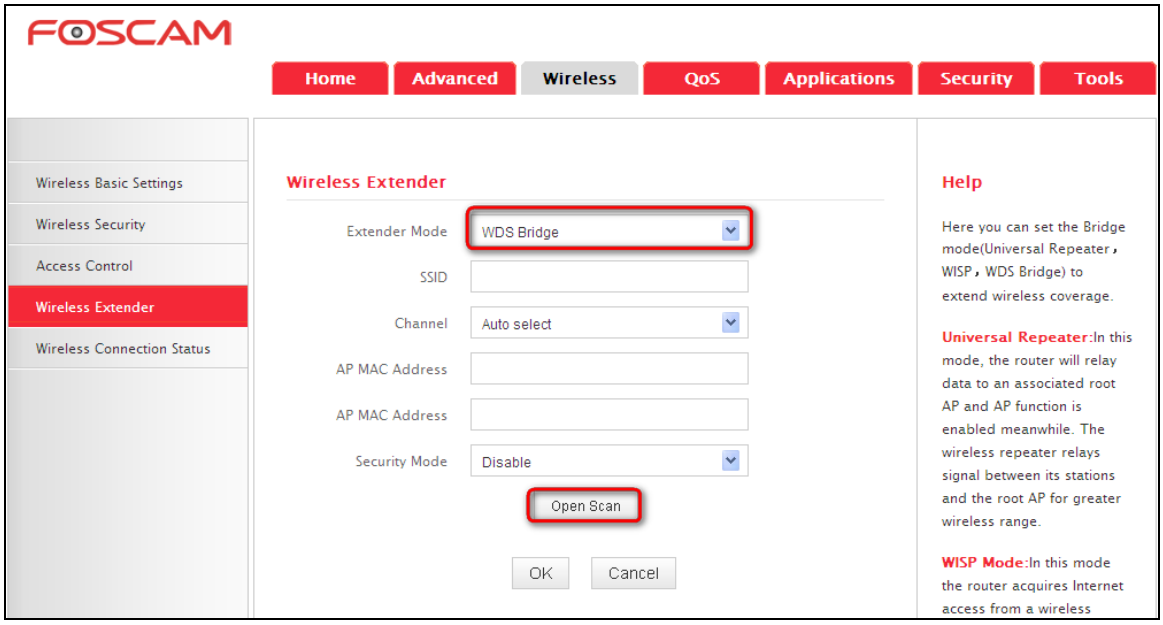


7) Go to **DHCP Server** to disable the DHCP on Router 2. Now you have finished all settings on Router 2 required for WDS.



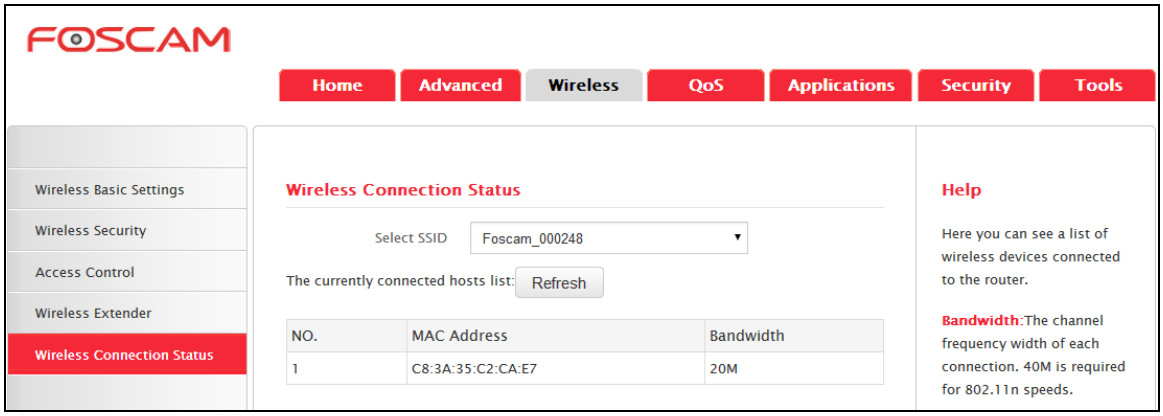
2. Configure Router 1:

1. Go to wireless section on Router 1 and specify **WDS (**or **WDS Bridge)** as its wireless working mode.
2. Manually enter Router 2's MAC address (Also, you can use the **Scan** option as mentioned above) and click **OK** to finish your settings.



2.5 Wireless Connection Status

Here you can see a list of wireless devices connected to the router, including their MAC addresses and bandwidth



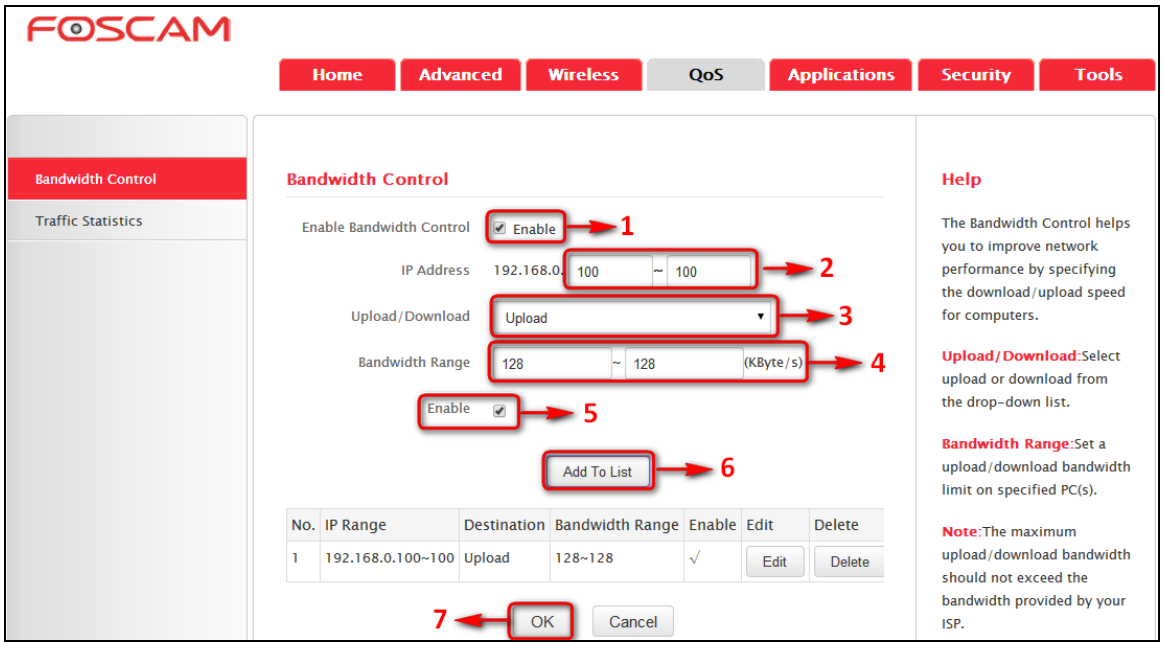
⚠**Note:**

The bandwidth here refers to the channel bandwidth instead of wireless connection rate.

3 QoS

3.1 Bandwidth Control

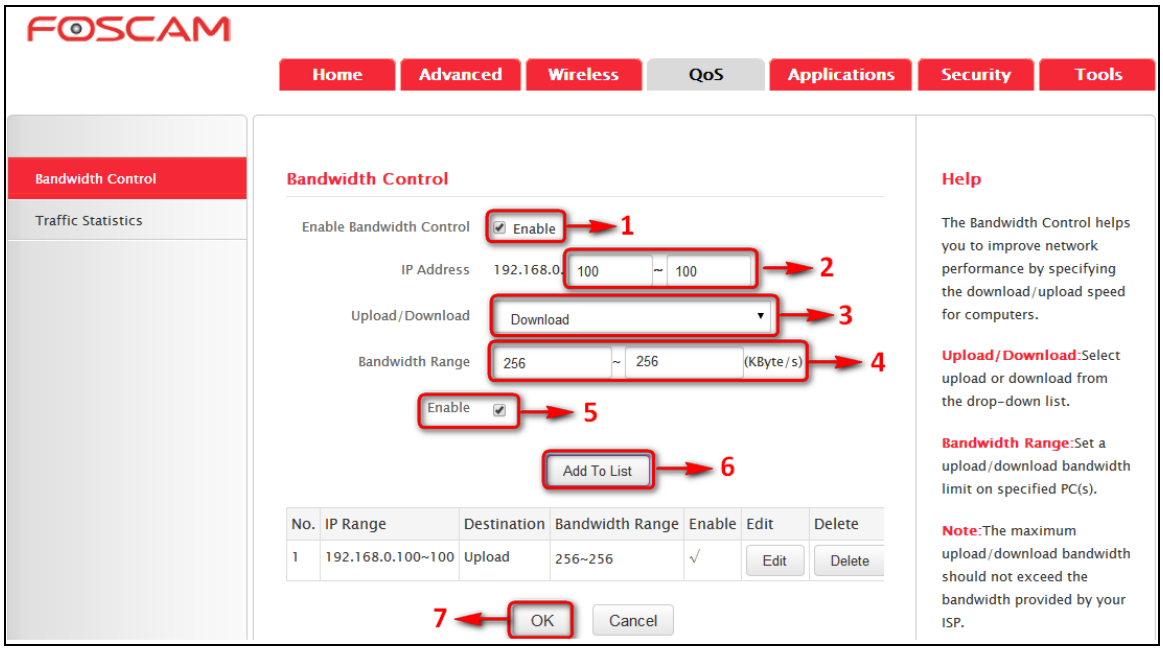
Use this section to manage bandwidth allocation to devices on your LAN. If there are multiple PCs behind your router competing for limited bandwidth resource, then you can use this feature to specify a reasonable amount of bandwidth for each such PC, so that no one will be over stuffed or starved to death.



- **Enable Bandwidth Control:** Check or uncheck the box to Enable or disable the bandwidth control feature.
- **IP Address:** Specify the same IP address (say, 100, 100) or two different IP addresses (say, 100, 110) in both boxes to specify a single IP address or an IP range to which the current bandwidth control rule will apply.
- **Upload/Download:** Select to control bandwidth over data upload or download.
- **Bandwidth Range:** Specify an upload/download bandwidth range limit on specified PC(s). The unit is KByte/s. 1M=128KByte/s. Note that maximum upload/download bandwidth should not exceed your router's WAN bandwidth limit. (Consult your ISP if you are not clear.).
- **Enable:** Check to enable current rule. (When disabled, corresponding entry will not take effect though existing in fact.)
- **Add to List:** Click to add current rule to the rule list.
- **OK:** Click to activate your settings.

For example:

If you are sharing a 4M broadband connection with a neighbor, who always exhausts the bandwidth resource downloading data, this feature will help. Simply specify half of the 4M bandwidth for your neighbor's PC (say, 192.168.0.100) and you will no longer need to struggle for bandwidth and your neighbor will only get up to 2M bandwidth. To do so, follow instructions below:

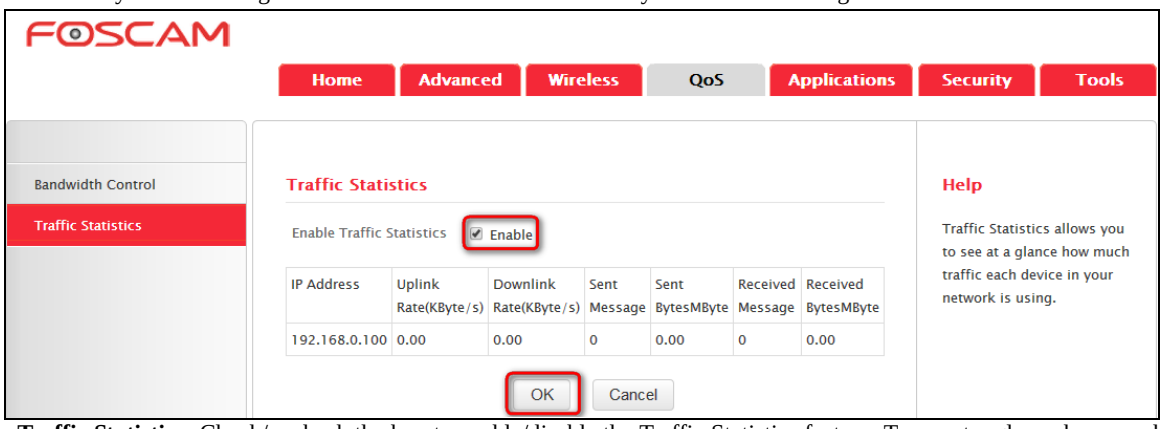


1. Check **Enable.**
2. Input "192.168.0.100" in both IP address boxes.
3. Select **Download.**
4. Enter "256" in both bandwidth range fields.

5. Check Enable.
6. Click **Add To List**
7. Click **OK.**

3.2 Traffic Statistics

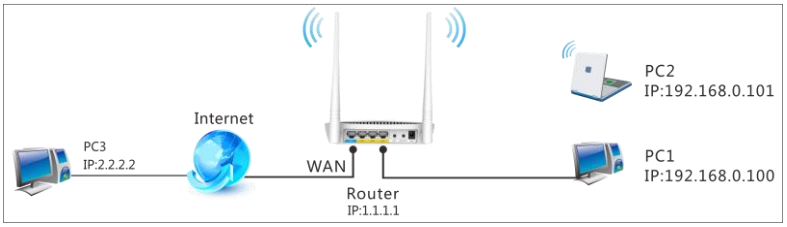
Traffic Statistics allows you to see at a glance how much traffic each device in your network is using.



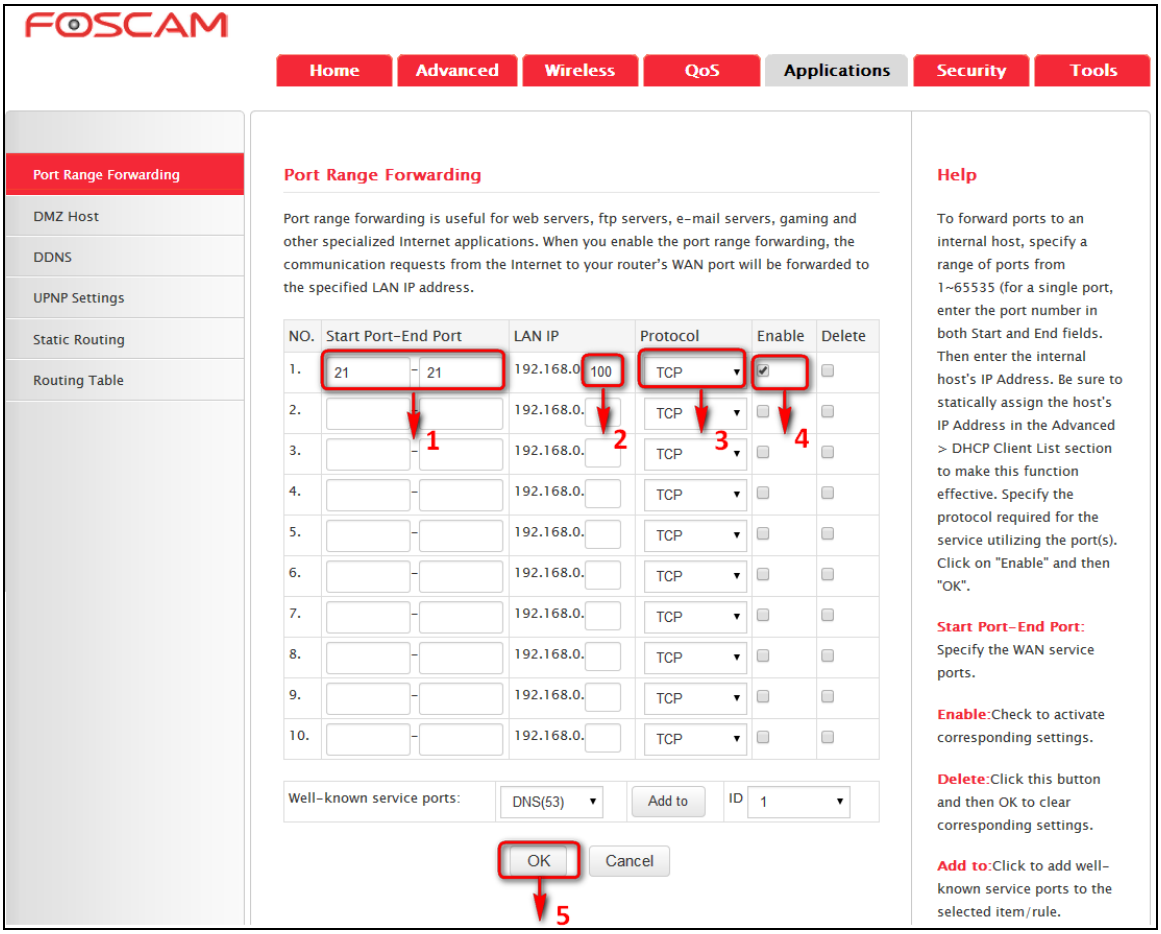
- **Enable Traffic Statistics:** Check/uncheck the box to enable/disable the Traffic Statistics feature. To see at a glance how much traffic each device in your network is using, enable this option. However usually, disabling it may boost your network performance. This option is disabled by default. However, once enabled the page refreshes every five minutes.
- **OK:** Click to activate corresponding settings.
- **IP Address:** Displays IP addresses of PCs connected to the device.
- **Uplink Rate:** Displays the upload speed (KByte/s) of a corresponding PC.
- **Downlink Rate:** Displays the download speed (KByte/s) of a corresponding PC.
- **Sent Message:** Displays the number of packets sent by a corresponding PC via the device since Statistics is enabled.
- **Sent Bytes:** Displays the number of Bytes sent by a corresponding PC via the device since Statistics is enabled. The unit is MByte.
- **Received Message:** Displays the number of packets received by a corresponding PC via the device since Statistics is enabled.
- **Received Bytes:** Displays the number of Bytes received by a corresponding PC via the device since Statistics is enabled. The unit is MByte.

4 Applications

4.1 Port Range Forwarding



Port range forwarding is useful for web servers, ftp servers, e-mail servers, gaming and other specialized Internet applications. When you enable port forwarding, the communication requests from the Internet to your router's WAN port will be forwarded to the specified LAN IP address. As seen in the figure above, to let PC3 access service ports on PC1, you must first configure port forwarding settings on the router to which PC1 is uplinked.

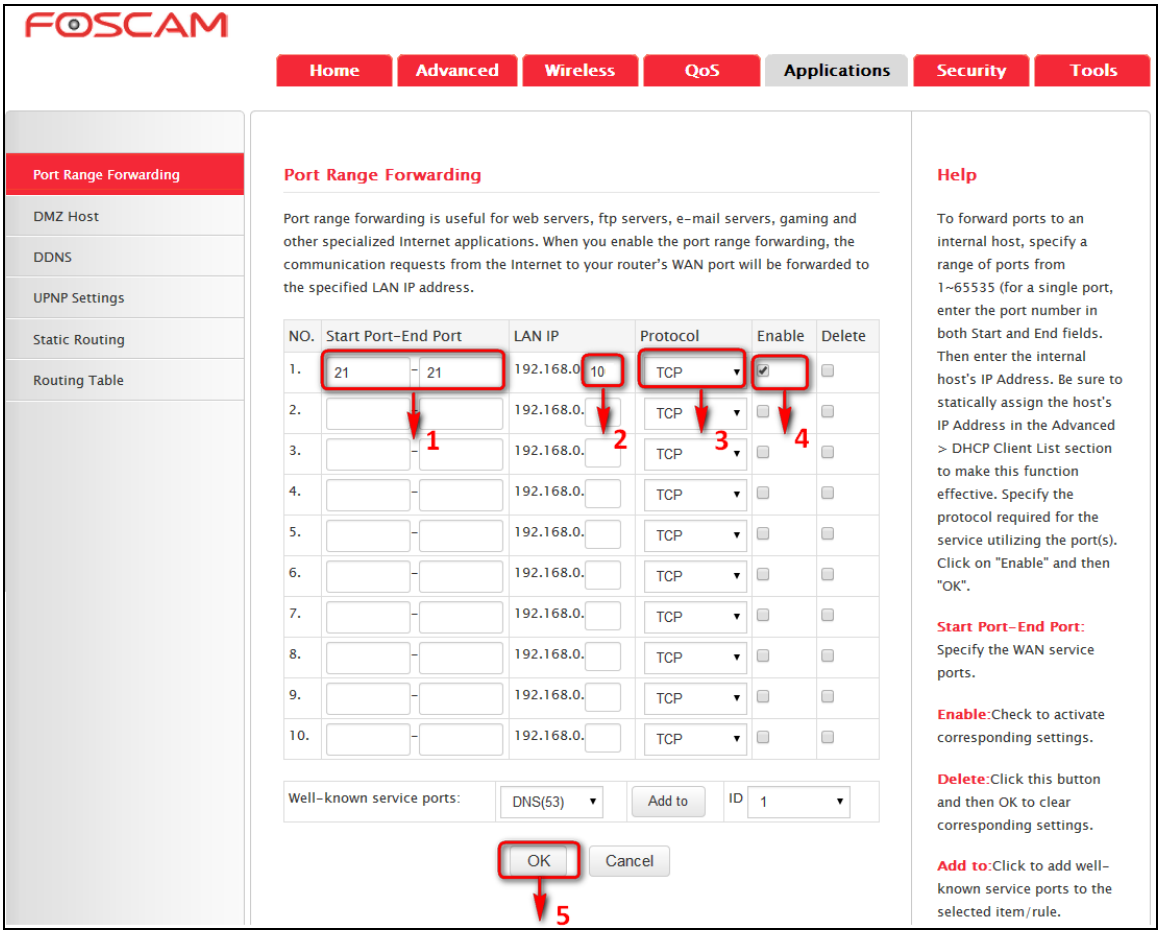


- **Start/End Port:** Specify a range of ports between 1~65535 (for a single port, enter the port number in both Start and End fields, say, 21 for FTP). Contact corresponding service provider if you don't know the port number of the service to use.
- **LAN IP:** Specify the internal host's IP address. Be sure to statically assign the host's IP address to make this function constant.
- **Protocol:** Specify the protocol required for the service utilizing the port(s).
- **Enable:** Check to enable current settings.
- **OK:** Click to activate your settings.

Now, your friends only need to enter ftp://xxx.xxx.xxx.xxx:21 in their browsers to access your FTP server xxx.xxx.xxx.xxx is the router's WAN IP address. Assuming it is 172.16.102.89, and then your friends need to enter ftp://172.16.102.89：21 in their browsers.

For example: You want to share some large files with your friends who are not in your LAN; however it is not convenient to transfer such large files across network. Then, you can set up your own PC as a FTP server and use the Port (Range) Forwarding feature to let your friends access these files. Assuming that the static IP address of the FTP server (Namely, your PC) is 192.168.0.10, you want your friends to access this FTP server through default port of 21 using the TCP protocol, then do as follows:

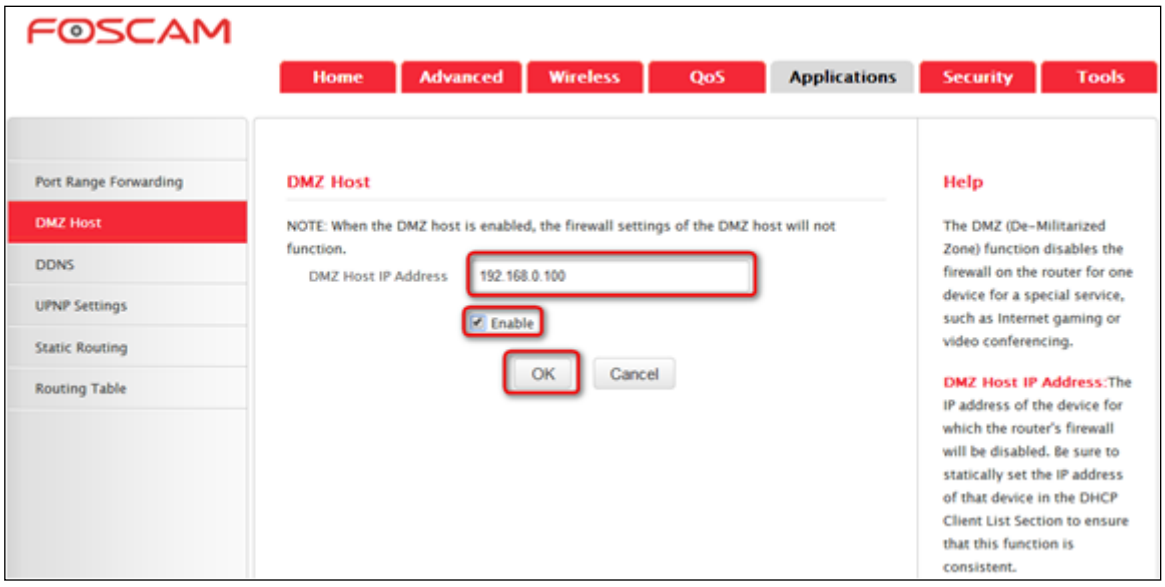
- **Start/End Port:** Enter 21 in both Start Port and End Port fields.
- **LAN IP:** Enter 192.168.0.10.
- **Protocol:** Select TCP.
- **Enable:** Check to enable current settings.
- **OK:** Click to activate your settings.



⚠**Note:**
If you include port 80 on this section, you must set the port for remote (web-based) management to a different number than 80, such as 8080, otherwise the virtual server feature may not take effect.

4.2 DMZ Host

The DMZ (De-Militarized Zone) function disables the firewall on the router for one device for a special purpose service such as Internet gaming or video conferencing. Enabling DMZ host may expose your local network to potential attacks. So it is advisable to use this feature with caution.



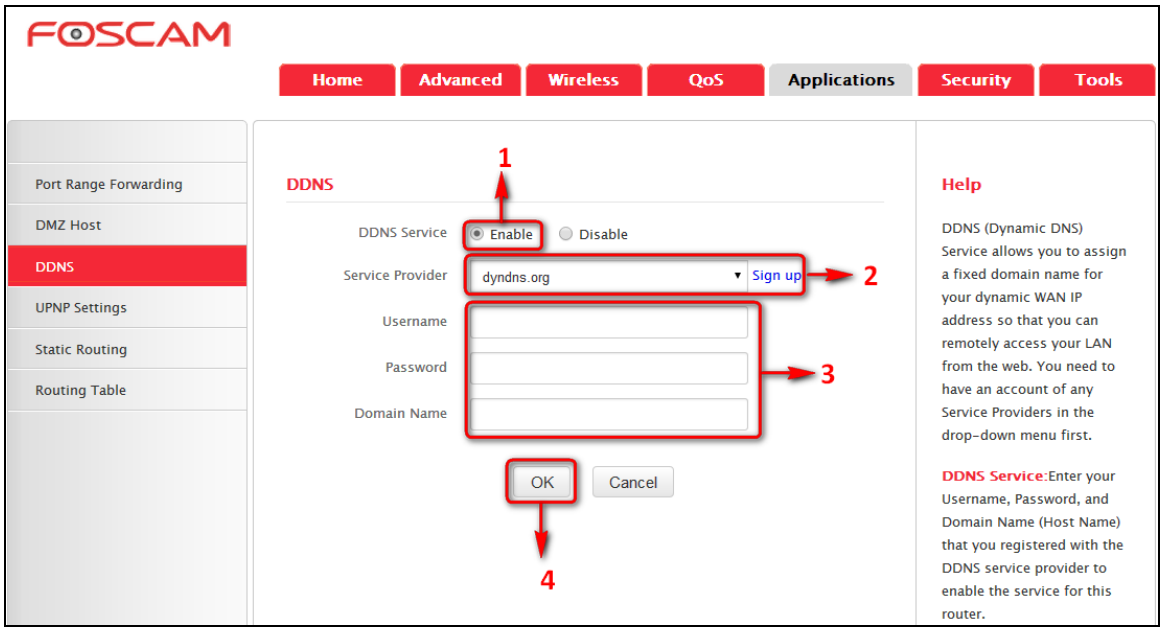
DMZ Host IP Address: The IP Address of the device for which the router's firewall will be disabled. Be sure to statically set the IP Address of that device for this function to be consistent.
Enable: Check/uncheck to enable/disable the DMZ host feature.
OK: Click to enable your settings.

Note:

Once enabled, the DMZ host loses protection from device's firewall and becomes vulnerable to attacks.

4.3 DDNS

Dynamic DNS or DDNS is a term used for the updating in real time of Internet Domain Name System (DNS) name servers. Dynamic DNS or DDNS is a term used for the updating in real time of Internet Domain Name System (DNS) name servers. We use a numeric IP address allocated by Internet Service Provider (ISP) to connect to the Internet; the address may either be stable ("static"), or may change from one session on the Internet to the next ("dynamic"). However, a numeric address is inconvenient to remember; an address which changes unpredictably makes connection impossible. The DDNS provider allocates a static host name to the user; whenever the user is allocated a new IP address this is communicated to the DDNS provider by software running on a computer or network device at that address; the provider distributes the association between the host name and the address to the Internet's DNS servers so that they may resolve DNS queries. Thus, uninterrupted access to devices and services whose numeric IP address may change is maintained. (You need to have an account with one of the Service Providers in the drop-down menu first.)



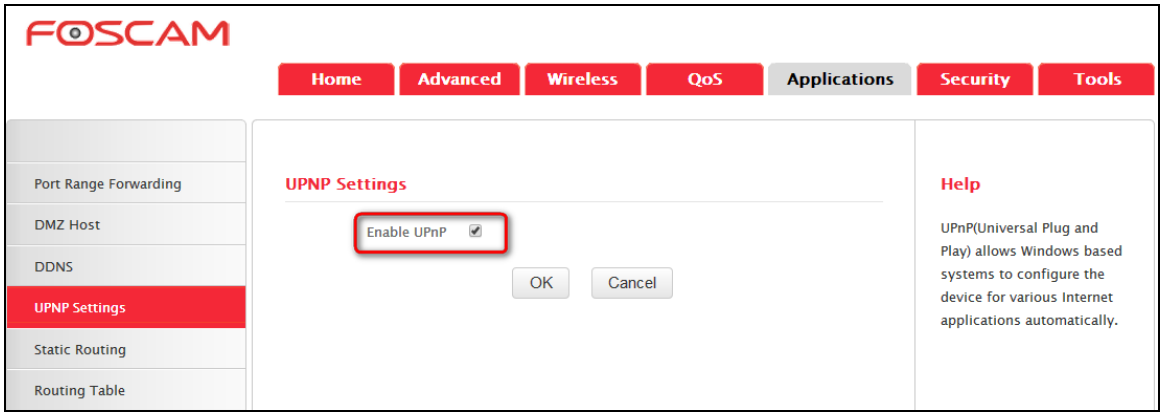
- **DDNS Service:** Select to enable/disable the DDNS feature.
- **Service Provider:** Select your DDNS service provider from the drop-down menu. (Here you can see a list of available service providers. Note that service providers not listed here are not available for use.)
- **User Name:** Enter the registered user name.
- **Password:** Enter the registered password.
- **Domain Name:** Enter the domain name you register.
- **OK:** Click to activate your settings.

Note:

This feature is usually used together with virtual server and is disabled by default. Configure necessary settings on port forwarding interface and enter the information provided by your DDNS service provider on the DDNS screen. If your domain name is foscam.dyndns.org, others can access your web server by simply entering http://foscam.dyndns.org in their browser address bar.

4.4 UPNP Settings

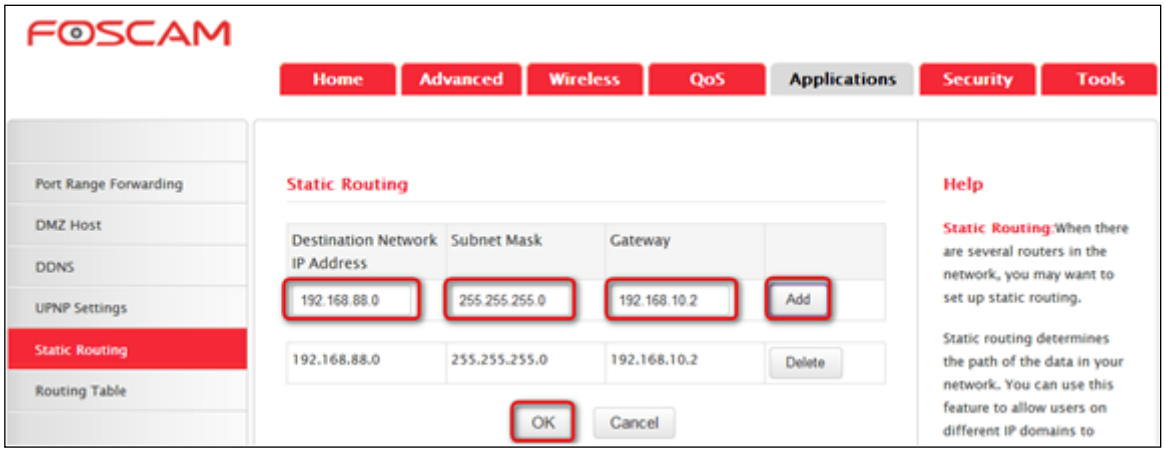
The Universal Plug and Play (UPnP) feature allows network devices, such as computers from the Internet, to access resources on local host or devices as needed. UPnP-enabled devices can be discovered automatically by the UPnP service application on the LAN. This feature is enabled by default. No settings are required.



- **Enable UPnP:** Check/uncheck to enable/disable the UPnP feature.
- **OK:** Click to complete your settings.

4.5 Static Routing

When there are several routers in the network, you may want to set up static routing. Static routing determines the path of the data in your network. You can use this feature to allow users on different IP domains to access the Internet via this device. It is not recommended to use this setting unless you are familiar with static routing. In most cases, dynamic routing is recommended, because this feature allows the router to detect the physical changes of the network layout automatically. If you want to use static routing, make sure the router's DHCP function is disabled.



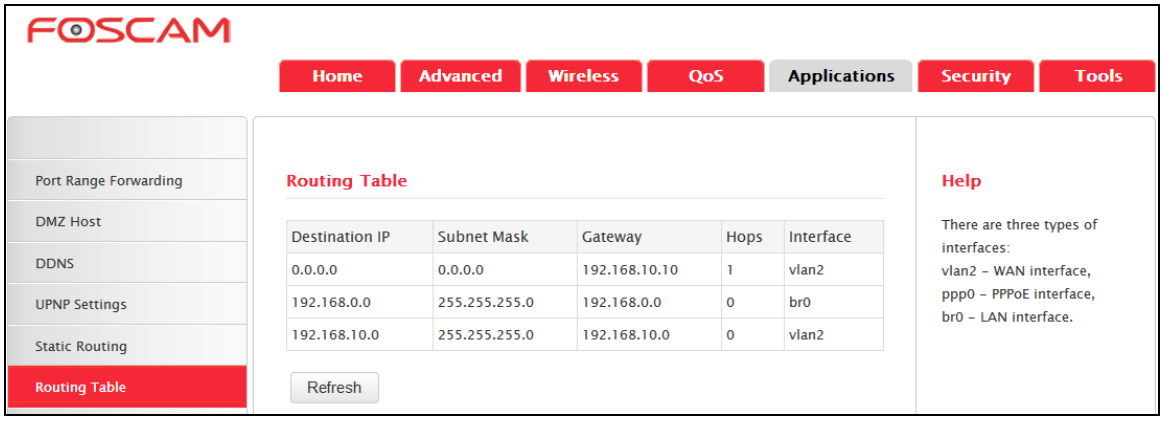
- **Destination Network IP Address:** Specify a single IP address, say, 172.17.0.100, or an IP net segment, .say, 192.168.88.0.
- **Subnet Mask:** Specify a Subnet Mask that corresponds to the specified destination IP.
- **Gateway:** Specify the IP address for next hop.
- **OK:** Click to activate your settings.

⚠**Note:**

- Gateway must be on the same IP net segment as device's LAN/WAN IP address.
- Subnet Mask must be entered 255.255.255.255 if destination IP address is a host.
- Subnet Mask must be entered accordingly if destination IP address represents an IP network segment. It must correspond to the specified IP address. For example, for IP address of 10.0.0.0, you may enter a subnet mask of 255.0.0.0.

4.6 Routing Table

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

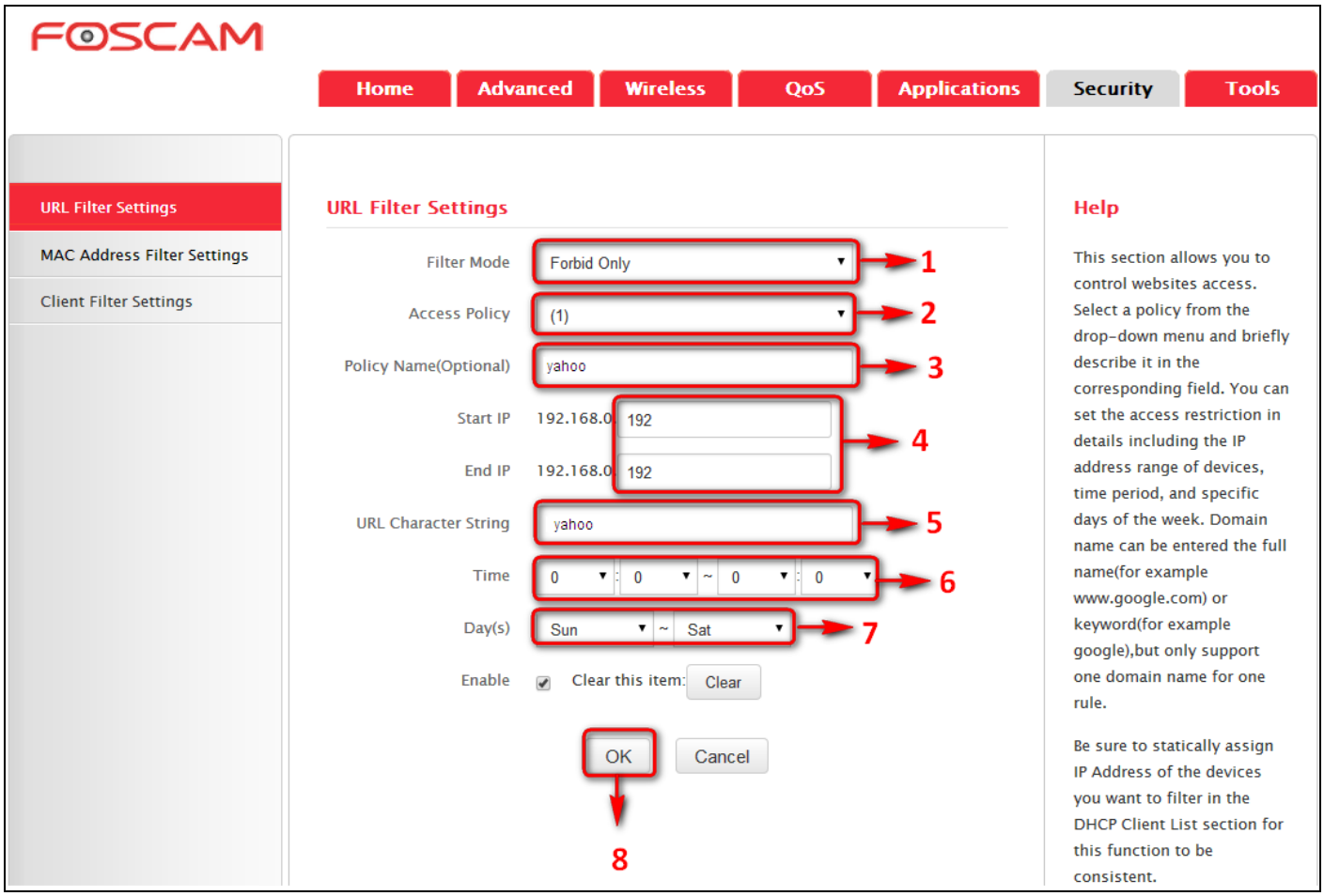


The principal task for a router is to look for an optimal transfer path for each data packet passing through it, and transfer it to the specified destination. To complete this work, the router stores and maintains related data of various transfer paths, i.e. establishing a routing table, for future route selection.

5 Security

5.1 URL Filter Settings

To better control LAN PCs, you can use the URL filter functionality to allow or disallow such PCs to access certain websites within a specified time range.



- **Filter Mode:** Select a proper filter mode, say, Forbid Only.
- **Access Policy:** Select an access policy number, say, 1, from the drop-down list.
- **Policy Name:** Briefly describe the current rule, say, yahoo, (It can only consist of numbers, letters, or underscore).
- Start IP/End IP: Enter the same IP address or 2 different IP addresses in both boxes to specify a single PC or a range of PCs for the current rule to apply to.
- **URL Character String:** Enter the domain name you wish to filter out, say, yahoo.

- **Time:** Specify a time period for a current rule to take effect. If the field is set to 0:00-0:00, the rule will be applied 24hrs/day.
- **Day(s):** Select a day or several days for a current rule to take effect. If Sun-Sat is selected, the rule will apply 7days/week.
- **Enable:** Check/uncheck to enable/disable the feature.
- **OK:** Click to activate your settings.

Example:

If you want to disallow all computers on your LAN to access youtube.com from 8 :00 to 18 :00 during working days: Monday- Friday, then do as follows:

1) **Filter Mode:** Select **Forbid Only.**
2) **Access Policy:** Select an access policy number, say, 1, from the drop-down list.
3) **Policy Name:** Briefly describe the current rule, say, yahoo, (It can only consist of numbers, letters, or underscore).
4) **Start IP/End IP:** Enter 2-254.
5) **URL Character String:** Enter yahoo.
6) **Time:** Select 8:00-18:00.
7) **Day(s):** Select Monday to Friday.
8) **Enable:** Check the **Enable** box.
9) **OK:** Click to save your settings.

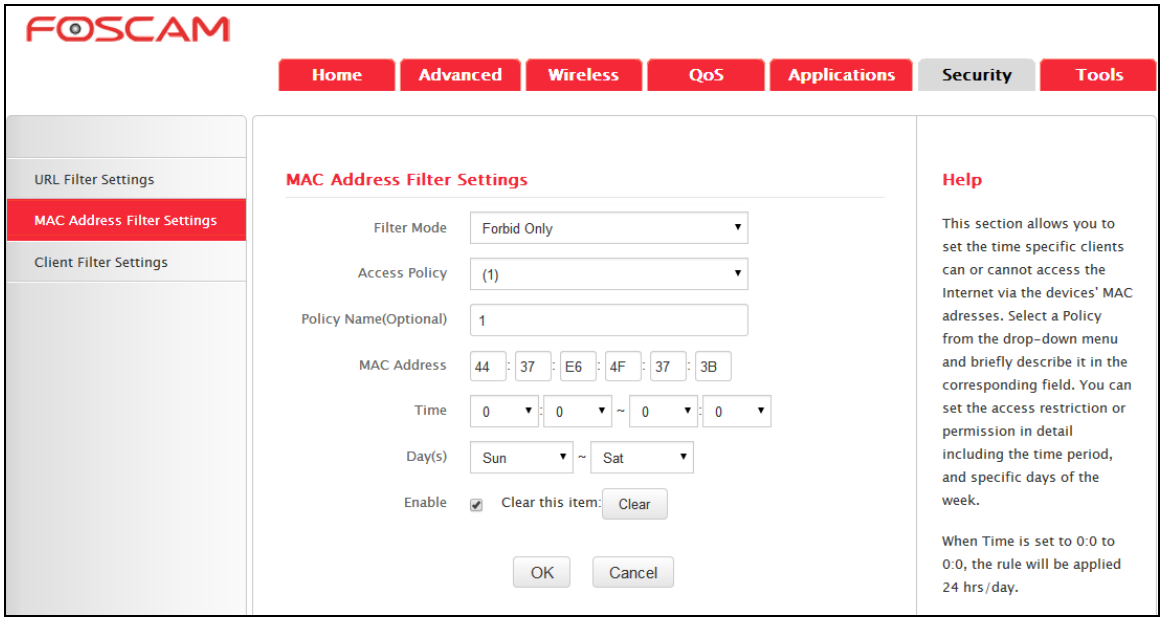
⚠**Note:**

Each rule can only include one domain name. Simply add more rules accordingly, if you want to filter multiple domain names.

5.2 MAC Address Filter Settings

This section allows you to set the times specific clients can or cannot access the Internet via the devices' MAC Addresses.

- **Forbid Only:** Specify a list of devices to Forbid access to the Internet. All other devices not listed as Forbidden will be permitted.
- **Permit Only:** Specify a list of devices to Permit access to the Internet. All other devices not listed as "Permitted" will be forbidden.



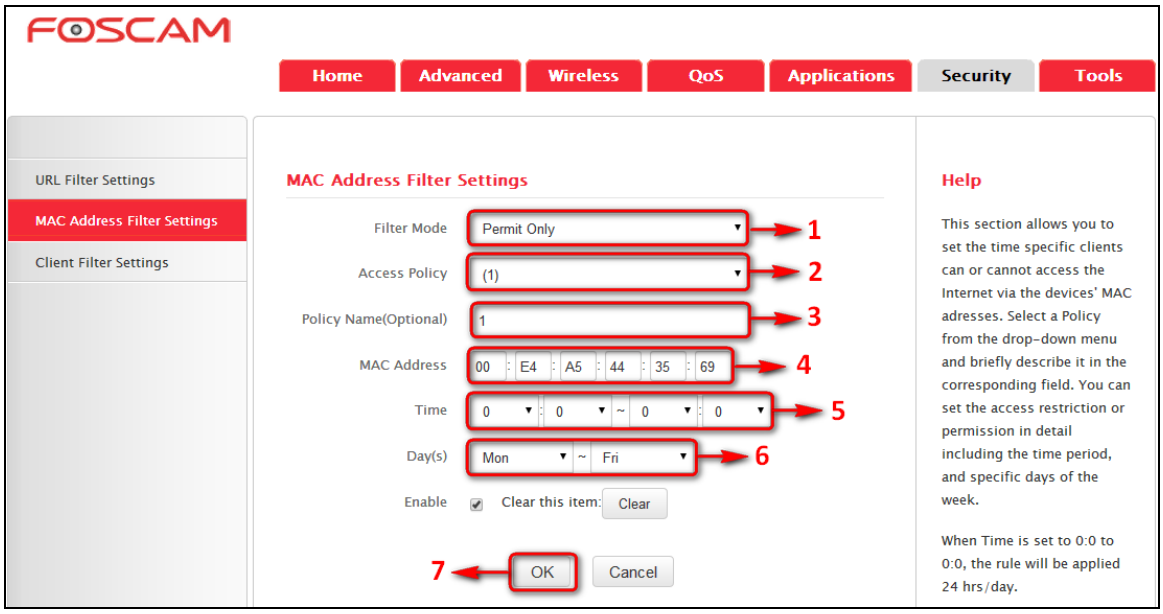
- **Filter Mode:** Select a proper filter mode, say, **Forbid Only**.
- **Access Policy:** Select an access policy number, say, 1, from the drop-down list.
- **Policy Name:** Briefly describe the current rule (It can only consist of numbers, letters, or underscore).
- **MAC Address:** Specify a MAC address for a corresponding MAC filter rule to apply to.
- **Time:** Specify a time period for a current rule to take effect. If the field is set to 0:00-0:00, the rule will be applied 24hrs/day.
- **Day(s):** Select a day or several days for a current rule to take effect. If Sun-Sat is selected, the rule will apply 7days/week.
- **Enable:** Check/uncheck to enable/disable the feature.
- **OK:** Click to activate your settings.

For Example:

To allow a PC at the MAC address of 00:E4:A5:44:35:69 to access the Internet from Monday to Friday.

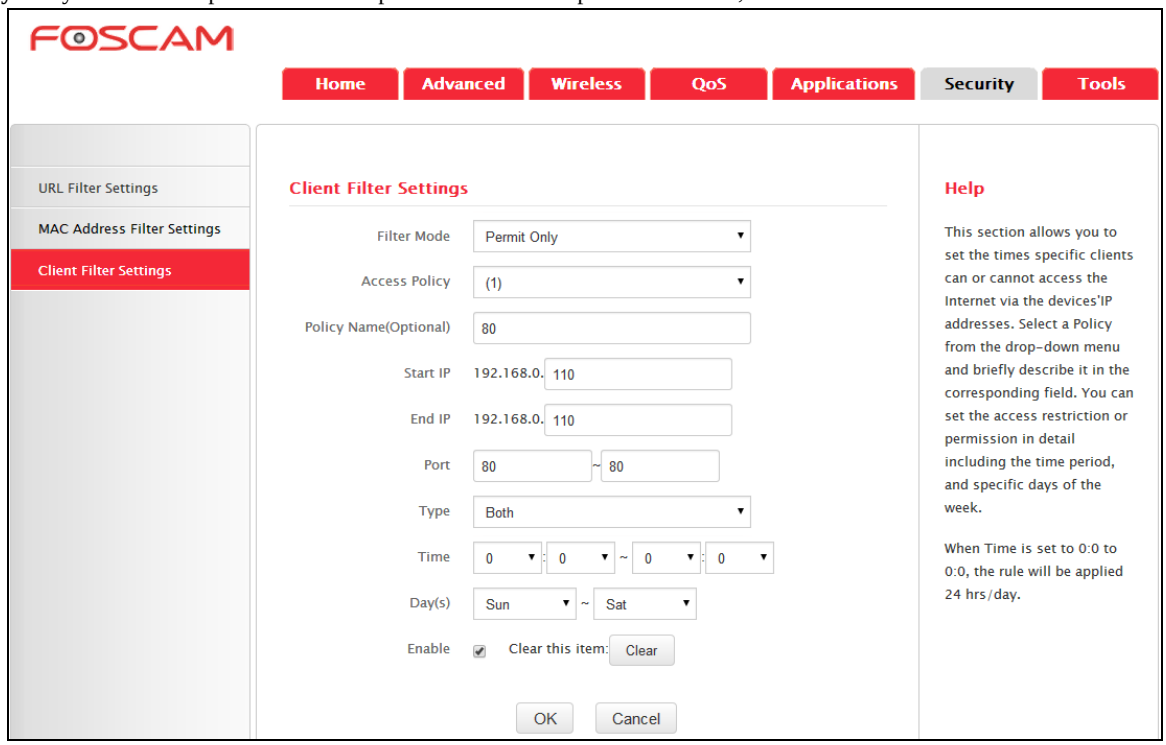
1) **Filter Mode**: Select **Permit Only**.
2) **Access Policy:** Select an access policy number, say, 1, from the drop-down list.
3) **Policy Name:** Briefly describe the current rule, say, **Permit_only**, (It can only consist of numbers, letters, or underscore).
4) **MAC Address:** Enter 00:E4:A5:44:35:69.
5) **Time:** Select 0 for all fields to apply the rule 24hrs/day.
6) **Day(s):** Select Monday to Friday.
7) **Enable:** Check the **Enable** box.

8) OK: Click to save your settings.



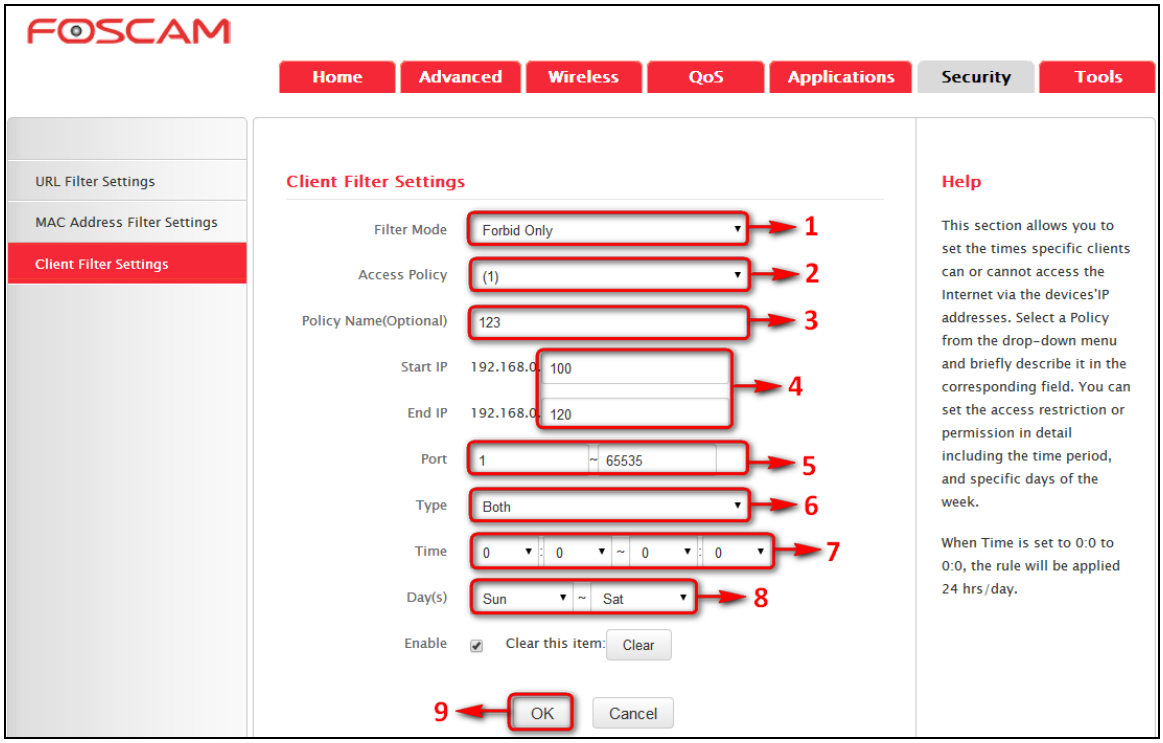
5.3 Client Filter Settings

This section allows you to set the times specific clients can or cannot access the Internet via the devices' assigned IP addresses and service port.
Forbid Only: Only PCs listed as Forbidden will be forbidden from accessing specified services; others are not restricted;
Permit Only: Only PCs listed as permitted will be permitted to access specified services; others will be forbidden.



- **Filter Mode:** Select **Permit Only.**
- **Access Policy:** Select an access policy number, say, 1, from the drop-down list.
- **Policy Name:** Briefly describe the current rule, say, 80.
- **Start IP/End IP:** Enter the same IP address, say, 110, or 2 different IP addresses, say, 110 and 120 in both boxes to specify a single PC or a range of PCs for the current rule to apply to.
- **Port:** Specify TCP/UDP protocol port number (s), say, 80.
- **Type:** Select **Both.**
- **Time:** Specify a time period for a current rule to take effect. If the field is set to 0:00-0:00, the rule will be applied 24hrs/day.
- **Day(s):** Specify a day or several days for a current rule to take effect.
- **Enable:** Check/uncheck to enable/disable the feature.
- **OK:** Click to activate your settings.

For example:
If you want to prohibit PCs within the IP address range of 192.168.0.100--192.168.0.120 from accessing the Internet, do as follows:

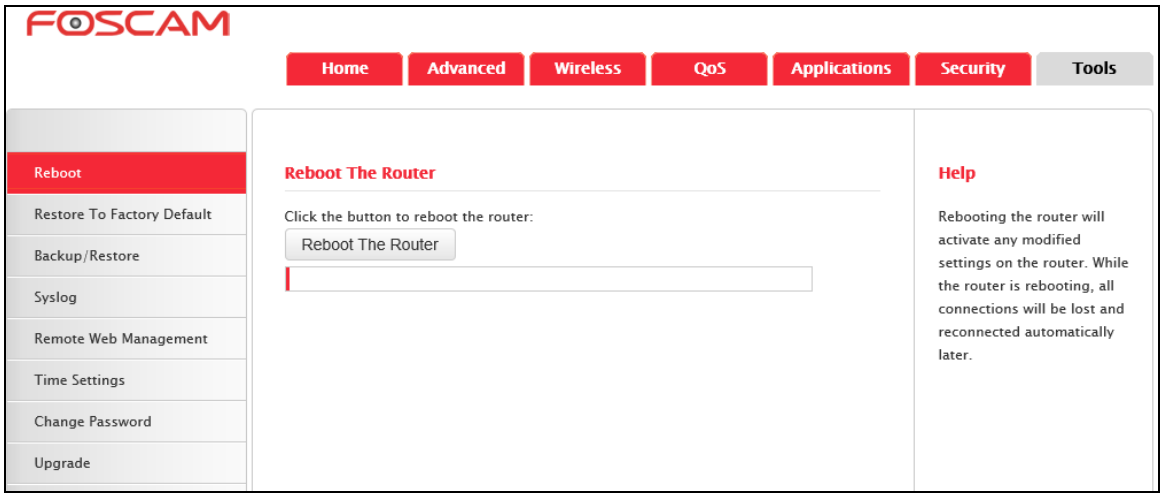


1) **Filter Mode:** Select **Forbid Only.**
2) **Access Policy:** Select an access policy number, say, 1, from the drop-down list.
3) **Policy Name:** Briefly describe the current rule, say, 123.
4) **Start IP:** Enter 100.
5) **End IP:** Enter 120.
6) **Port:** Enter 1-65535 to forbid all Internet services and applications.
7) **Type (or Protocol):** Select **Both**.
8) **Time:** Select 0 for all fields to apply the rule 24hrs/day.
9) **Day(s):** Select **Sun-Sa**t to apply the rule 7days/week.
10) **Enable:** Check the **Enable** box.
11) **OK:** Click to activate your settings.

6 Tools

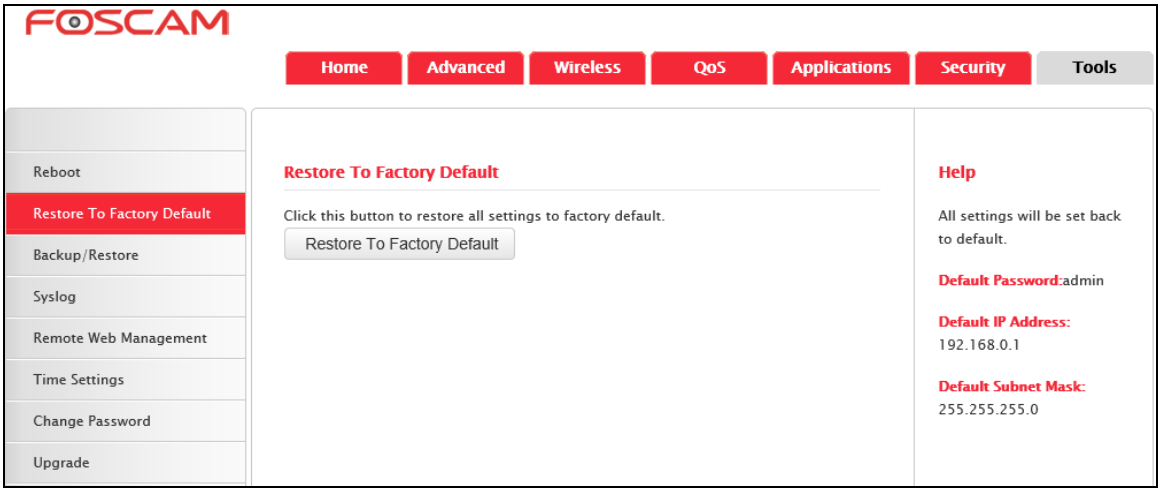
6.1 Reboot

Reboot the device to activate your settings. WAN connection will be disconnected during reboot.



6.2 Restore to Factory Default

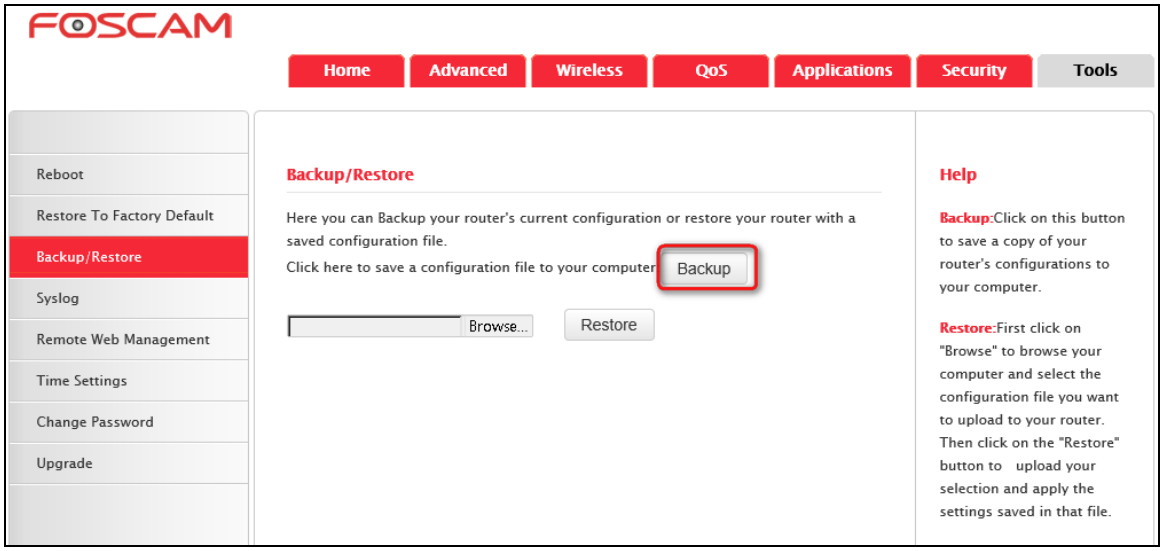
Click the **Restore To Factory Default** button to reset your device to factory default settings. You need to reconfigure parameters on the device (such as wireless settings) for Internet access, and reboot the device to activate your new settings.



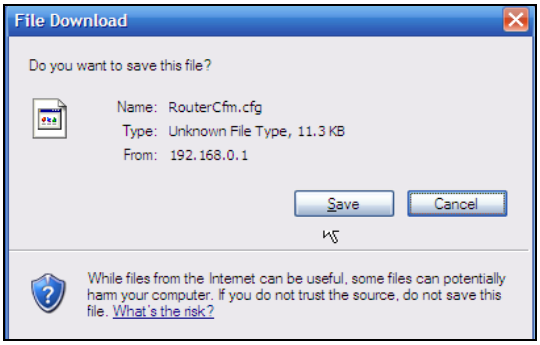
The factory default settings are listed below:
IP Address: 192.168.0.1
Subnet mask: 255.255.255.0

6.3 Backup/Restore

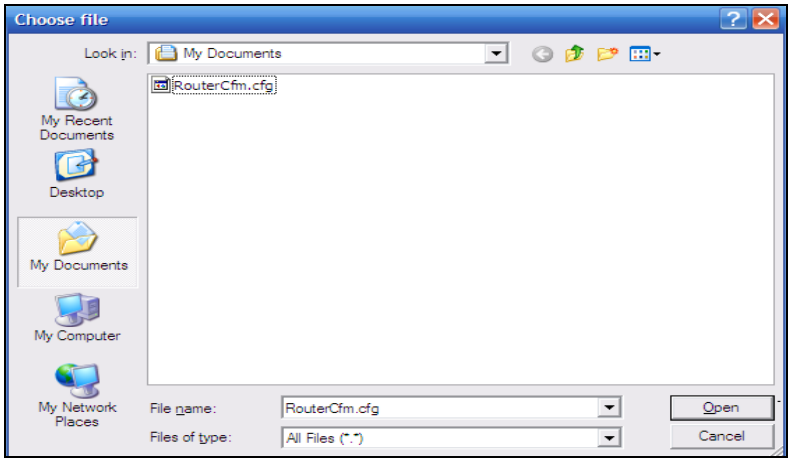
Backup: Once you have configured the device the way you want, you can save these settings to a configuration file on your local hard drive that can be later imported to your device in case that the device is restored to factory default settings. To do so, follow instructions below:
1. Click the **Backup** button and specify a directory to save settings on your local hardware.



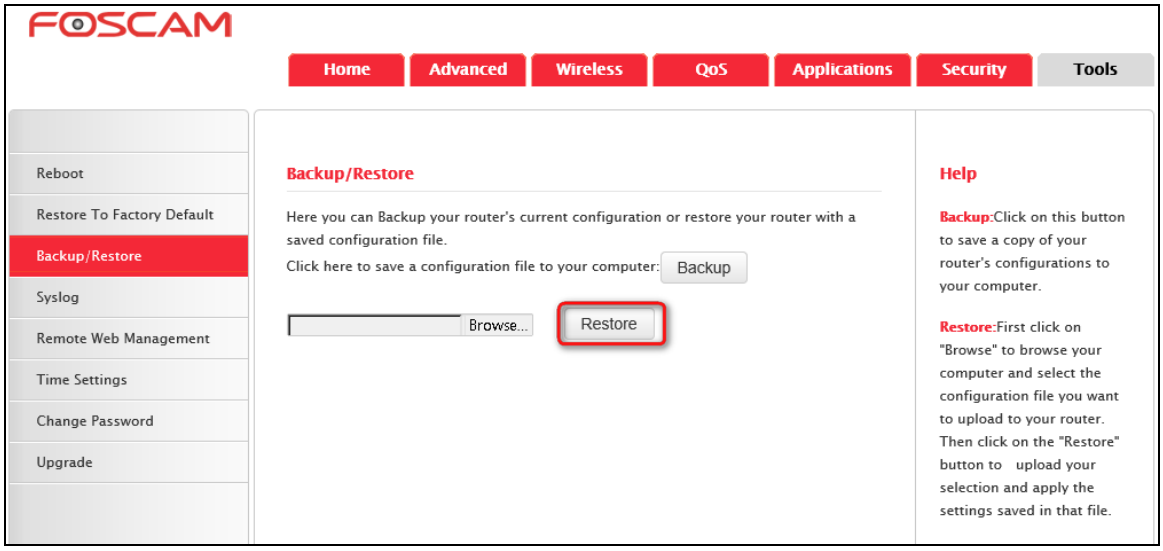
2. Click **Save** to download the configuration file.



To restore previous settings, do as follows:
Click the **Browse** button to locate and select a configuration file that is saved previously to your local hard drive.

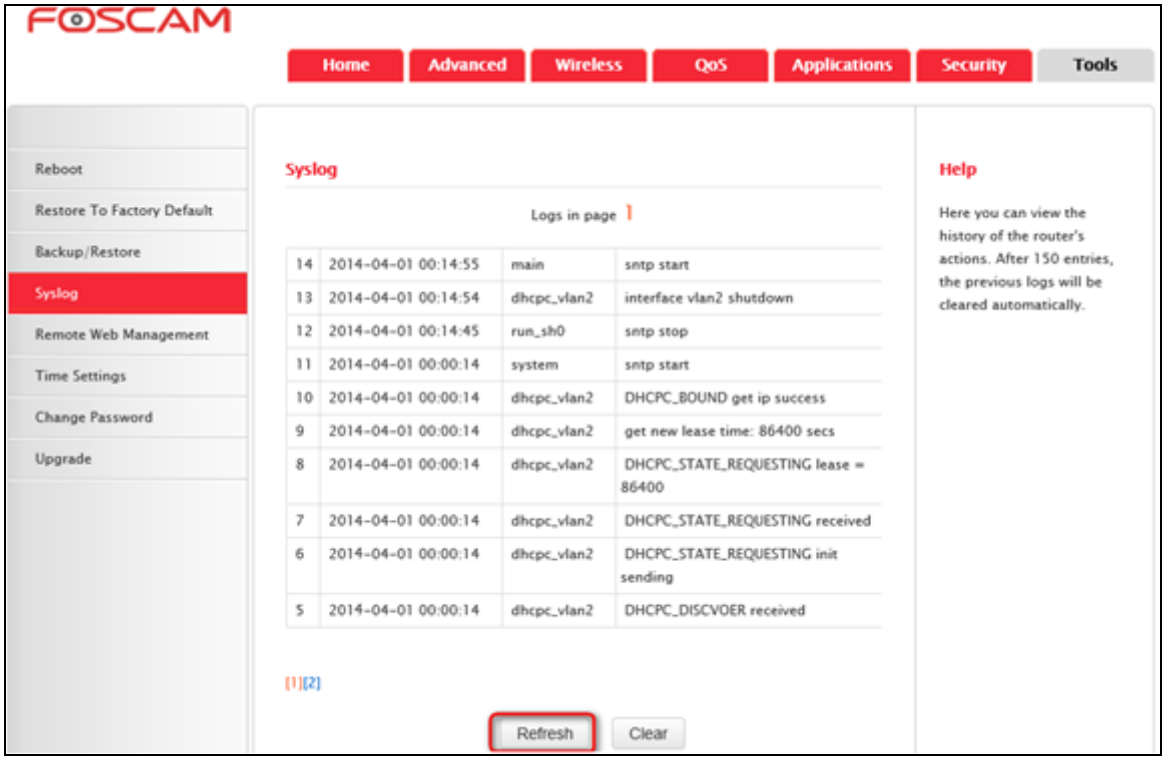


Click the **Restore** button to reset your device to previous settings.



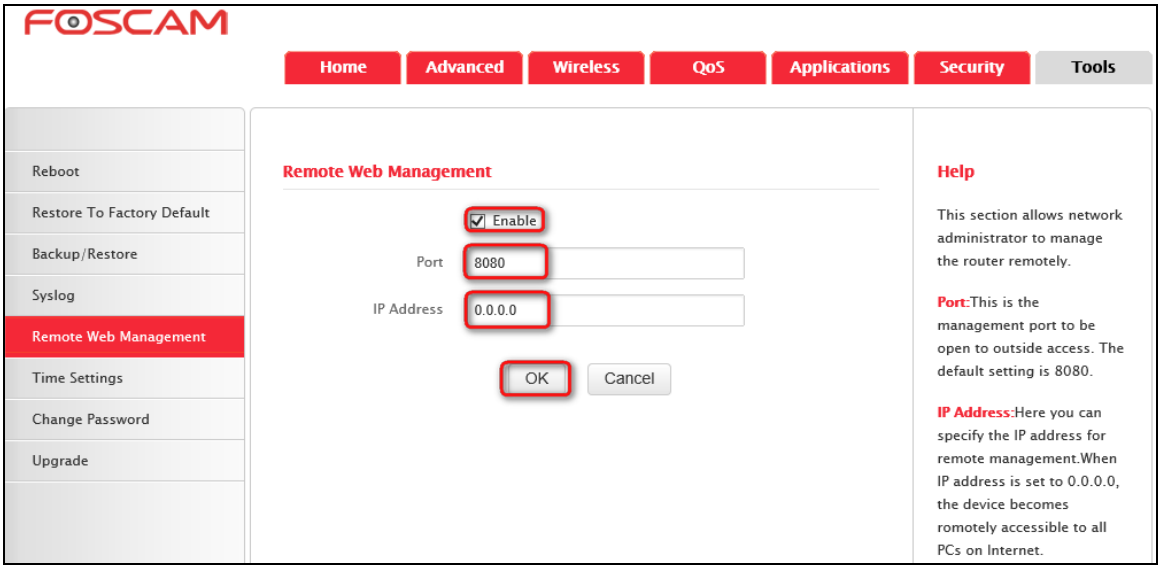
6.4 Syslog

Here you can view the record of the device's operations. After 150 records, the earliest log(s) will be cleared automatically.



6.5 Remote Web Management

This allows the device to be configured and managed remotely from the Internet via a web browser.



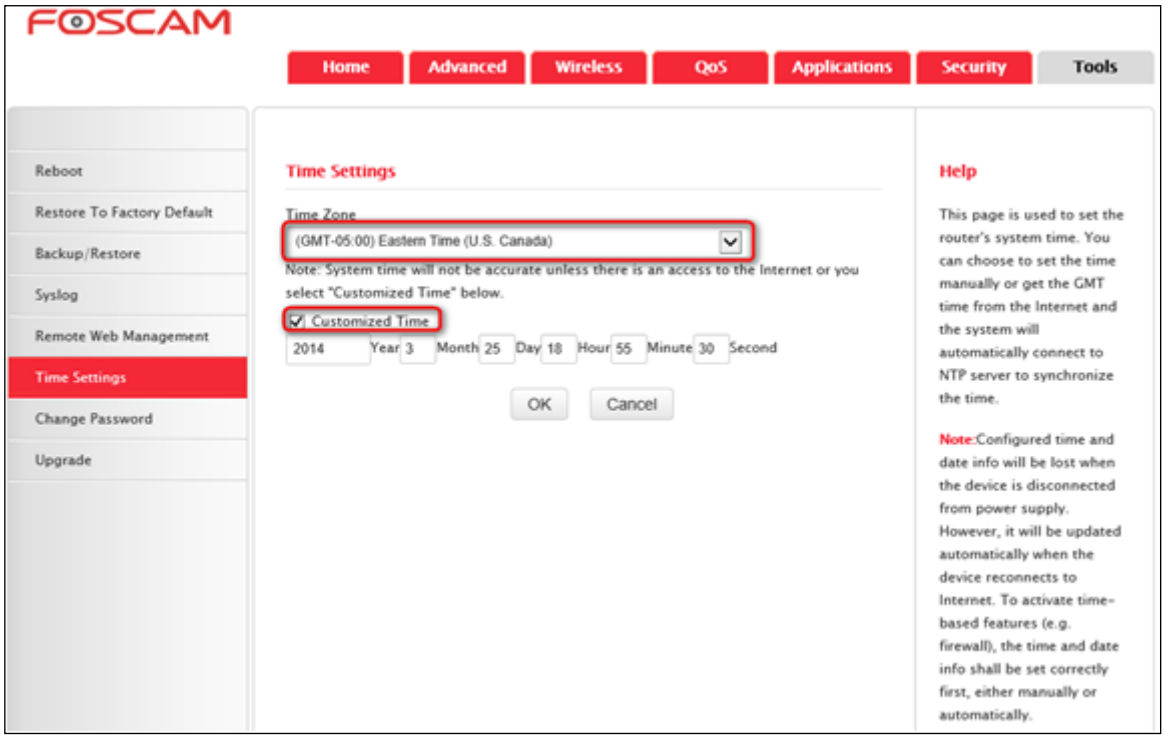
- **Enable:** Check/uncheck to enable/disable the DMZ host feature.
- **Port:** This is the management port to be open to external access. The default setting is 8080. Do NOT change it unless instructed by your ISP.
- **IP Address:** Here you can specify the IP Address Range for remote management (When set to 0.0.0.0, the device becomes remotely accessible to all the PCs on the Internet or other external networks).
- **OK:** Click **OK** to activate your settings.

⚠**Note:**

- To access the device via port 8080, enter http://x.x.x.x:8080.
  Here, "x.x.x.x" represents the device's Internet IP address; 8080 is the remote admin port.
  Assuming the device's Internet IP address is 220.135.211.56, then, simply replace the "x.x.x.x" with "220.135.211.56" (namely, http://220.135.211.56:8080).
- Leaving the IP address field at "0.0.0.0" makes the device remotely accessible to all the PCs on the Internet or other external networks; populating it with a specific IP address, say, 218.88.93.33, makes the device only remotely accessible to the PC at the specified IP address.

6.6 Time Settings

This page is used to set the router's system time. You can get the GMT time from the Internet, for the system will automatically connect to NTP server to synchronize the time. Also you can choose to set the time manually.

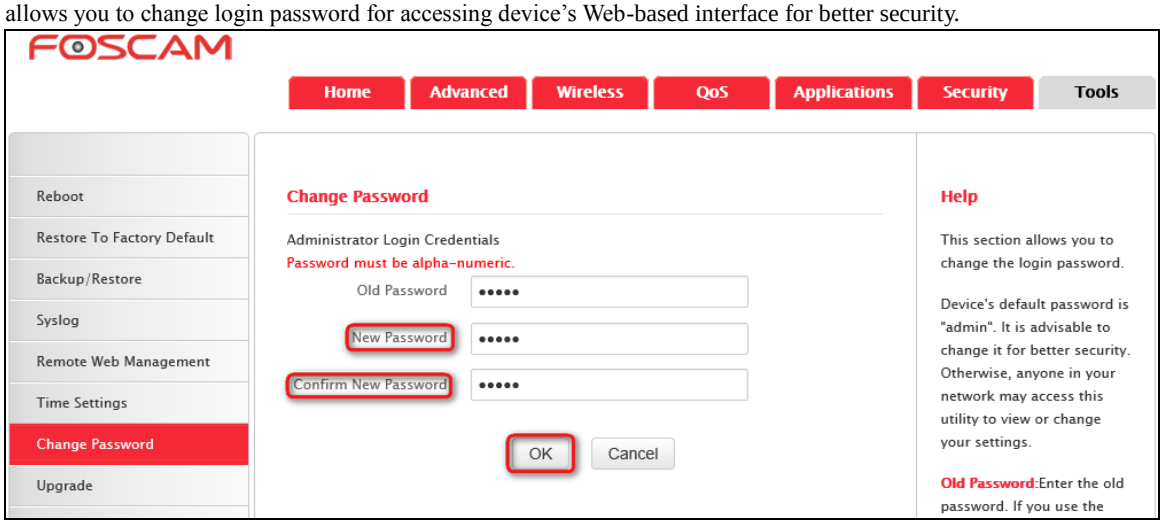


Note:

Configured time and date info will be lost when the device gets disconnected from power supply. However, it will be updated automatically when the device reconnects to the Internet. To activate time-based features (e.g. firewall), the time and date info shall be set correctly, either manually or automatically.

6.7 Change Password

This section allows you to change login password for accessing device's Web-based interface for better security.



- **New Password:** Enter a new password, say, 12345 (Note that the password can only be alphanumeric).
- **Confirm New Password:** Re-enter the new password for confirmation.
- **OK:** Click to activate your settings.

Note:

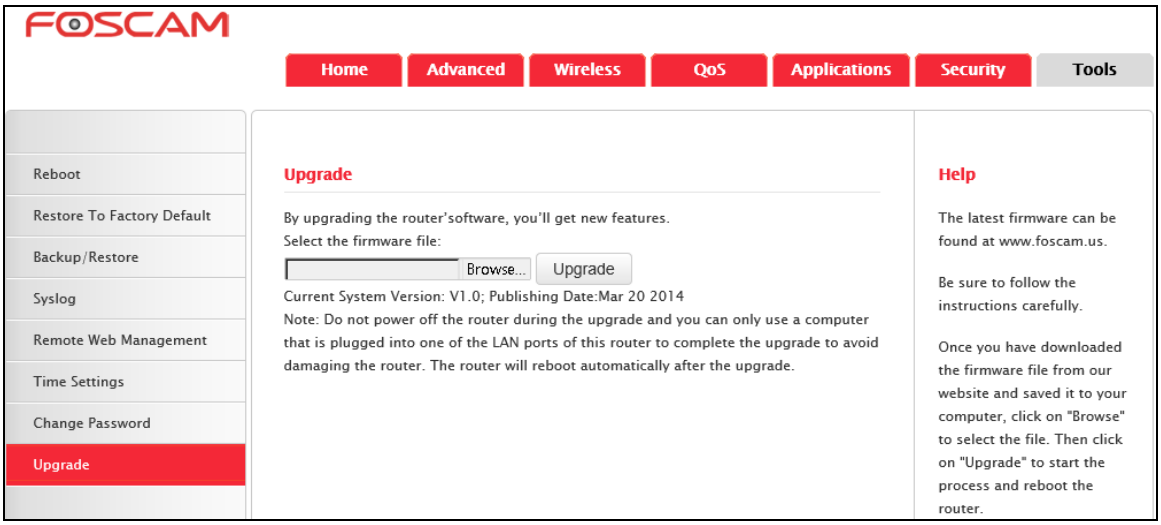
For better security, it is highly recommended that you should change your device's default login password.

6.8 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 about a specific feature of the device, log on to our website (www.foscam.us) to download the latest firmware to update your device.

Note:

- Before you upgrade the firmware, make sure you have a correct firmware. A wrong firmware may damage the device.
- Do NOT upgrade the firmware wirelessly or disconnect the device from power supply while firmware update is in process. Note that you need to update the device's firmware via a wired connection.



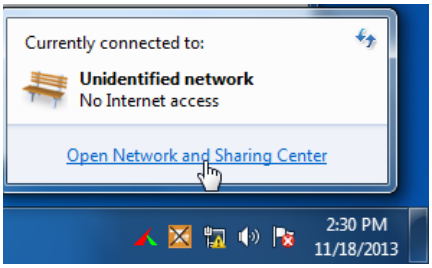
- **Browse:** Click to locate and select the firmware.
- **Upgrade:** Click to update firmware. Your device will restart automatically when its update completes.

Appendix 1 Configure PC

In this section we explain how to configure your PC's TCP/IP settings.

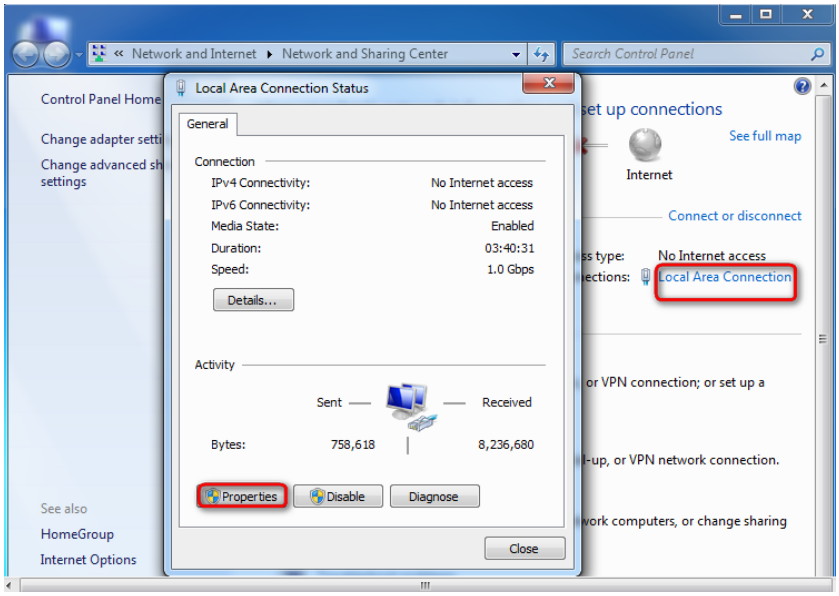
Windows 7

Step 1: Click the icon  on the bottom right corner of your desktop.
Step 2: Click **Open Network and Sharing Center**.

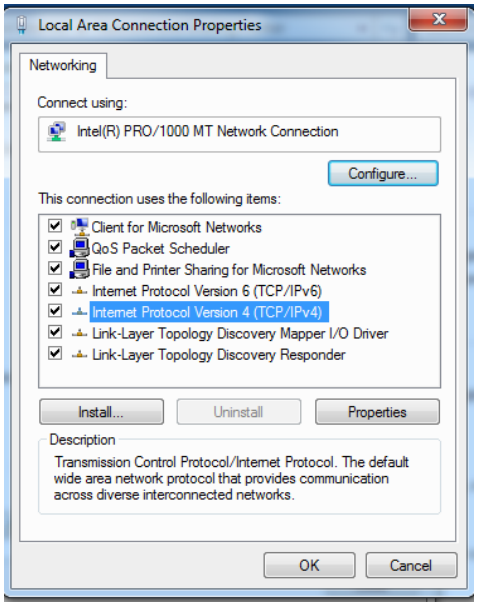


Tip: If you cannot find the icon  on the bottom right corner of your desktop, follow steps below: Click **Start** -> **Control Panel** -> **Network and Internet** -> **Network and Sharing Center**.

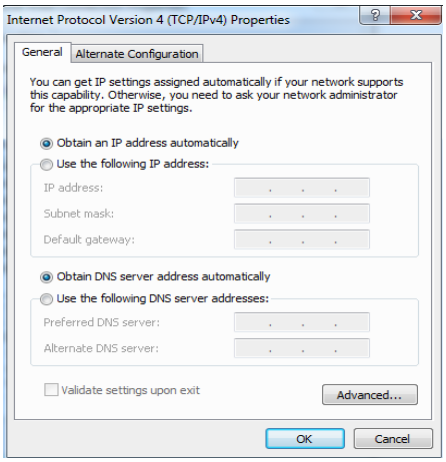
Step 3: Click **Local Area Connection** -> **Properties**.



Step 4: Find and double click **Internet Protocol Version 4 (TCP/IPv4)**.



Step 5: Select **Obtain an IP address automatically** and **Obtain DNS server address automatically** and click **OK**.

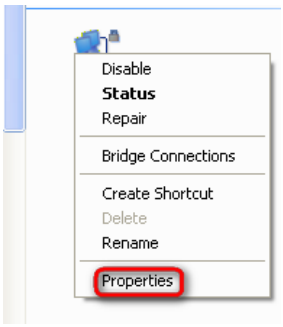


Step 6: Click **OK** on the **Local Area Connection Properties** window (see **Step 4** for the screenshot).

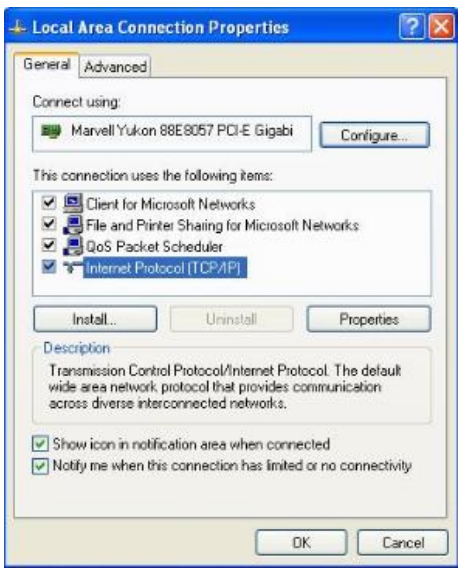
Windows XP

Step 1: Right click **My Network Places** on your desktop and select Properties.

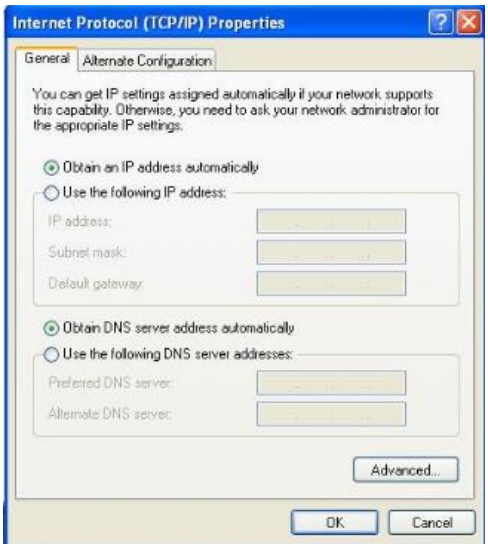
Step 2: Right click **Local Area Connection** and select **Properties**.



Step 3: Scroll down to find and double click **Internet Protocol (TCP/IP)**.



Step 4: Select **Obtain an IP address automatically** and **Obtain DNS server address automatically** and click **OK**.



Step 5: Click **OK** on the **Local Area Connection Properties** window (see **Step 3** for the screenshot).

Appendix 2 FAQs

This section provides solutions to problems that may occur during installation and operation of the device. If your problem is not covered here, please feel free to go to www.foscam.us to find a solution or email your problems to: support@foscam.us. We will be more than happy to help you out as soon as possible.

1. Q: I entered the device's LAN IP address in the web browser but cannot access the utility. What should I do?

a.Check whether device is functioning correctly. The SYS LED should blink a few seconds after device is powered up. If it does not light up, then some internal faults may have occurred.

b.Verify physical connectivity by checking whether a corresponding port's link LED lights up. If not, try a different cable. Note that an illuminated light does NOT ALWAYS indicate successful connectivity.

c. Run the "ping 192.168.0.1" command. If you get replies from 192.168.0.1, open your browser and verify that Proxy server is disabled. In case that ping fails, press and hold the "WPS/RST" button on your device for over 7 seconds to restore factory default settings, and then run "ping192.168.0.1" again.

d. Contact our technical support for help if the problem still exists after you tried all the above.

2. Q: What should I do if I forget the login password to my device?

Reset your device by pressing the WPS/RST button for over 7 seconds.

⚠**Note:**

All settings will be deleted and restored to factory defaults once you pressed the WPS/RST button.

3. Q: My computer shows an IP address conflict error after having connected to the device. What should I do?

a. Check if there are other DHCP servers present in your LAN. If there are other DHCP servers except your router, disable them immediately.

b. The default IP address of the device is 192.168.0.1; make sure this address is not used by another PC or device. In case that two computers or devices share the same IP addresses, change either to a different address.

4.Q: I cannot access Internet and send/receive emails; what should I do?

This problem mainly happens to users who use the PPPoE or Dynamic IP Internet connection type. You need to change the MTU size (1492 by default). In this case, go to "**Internet Connection Setup**" to change the MTU value from default 1480 to 1450 or 1400, etc.

5. Q: How do I share resources on my computer with users on the Internet through the device?

To let Internet users access internal servers on your LAN such as e-mail server, Web, FTP, via the device, use the " Port Range Forwarding r" feature. To do so, follow steps below:

Step 1: Create your internal server, make sure the LAN users can access these servers and you need to know related service ports, for example, port number for Web server is 80; FTP is 21; SMTP is 25 and POP3 is 110.

Step 2: Enter Port Range Forwarding screen from device web UI.

Step 3: Complete the Start Port (also called External/Ext Port on some products) and End Port (also known as Internal Port on some products) fields, say, 80-80.

Step 4: Input the internal server's IP address. For example, assuming that your Web server's IP address is 192.168. 0.10, then simply input it.

Step 5: Select a proper protocol type: TCP, UDP, or Both depending on which protocol(s) your internal host is using.

Step 6: Click **Enable** and save your settings.

For your reference, we collected a list of some well-known service ports as follows:

Server	Protocol	Service Port
Web Server	TCP	80
FTP Server	TCP	21
Telnet	TCP	23
Net Meeting	TCP	1503、1720
MSN Messenger	TCP/UDP	File Send:6891-6900(TCP) Voice:1863, 6901(TCP) Voice:1863, 5190(UDP)
PPTP VPN	TCP	1723
Iphone5.0	TCP	22555
SMTP	TCP	25
POP3	TCP	110

Appendix 3 Safety and Emission Statement

CE Mark Warning

This is a Class B product. In a domestic environment, this product may cause radio interference, in which case the user may be required to take adequate measures. This device complies with EU 1999/5/EC.

NOTE: (1) The manufacturer is not responsible for any radio or TV interference caused by unauthorized modifications to this equipment. (2) To avoid unnecessary radiation interference, it is recommended to use a shielded RJ45 cable.

FCC Statement

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

FCC Caution: Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

The manufacturer is not responsible for any radio or TV interference caused by unauthorized modifications to this equipment.

Radiation Exposure Statement

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

NOTE:

(1) The manufacturer is not responsible for any radio or TV interference caused by unauthorized modifications to this equipment.

(2) To avoid unnecessary radiation interference, it is recommended to use a shielded RJ45 cable.