

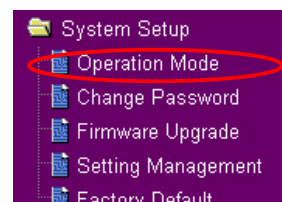


4. Wireless router features

This chapter provides setup examples of some frequently used router features. You can setup these features via your Web browser.

1) Choosing an appropriate operation mode

ASUS WL-500gP Wireless Router supports three operation modes: home gateway, router, and access point. Click **System Setup -> Operation mode** to open the configuration page.



Home gateway mode is for home or SOHO users who want to connect to their ISPs for Internet services. In this operation mode, NAT, WAN connection, Internet firewall functions are supported.

Router mode is for office use where multiple routers and switches co-exist. You can set up routing policies in this mode; however, NAT function is disabled.

Access point mode works when you setup WL-500gP as a wireless bridge. In this mode, all Ethernet ports on WL-500gP (4 LAN ports and 1 WAN port) are recognized as LAN ports. WAN connection, NAT, and Internet firewall functions are disabled in access point mode.

Select a proper mode which complies to your network scenario and press **Apply** button, and then you can continue to setup advanced features for your WL-500gP.

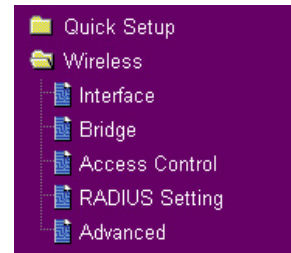
System Setup - Operation Mode	
ASUS Wireless Router supports three operation modes to meet different requirements from different group of people. Please select the mode that match your situation.	
☒ Home Gateway	In this mode, we suppose you use ASUS Wireless Router to connect to Internet through ADSL or Cable Modem. And, there are many people in your environment share the same IP to ISP. Explaining with technical terms, gateway mode is , NAT is enabled, WAN connection is allowed by using PPPoE, or DHCP client, or static IP. In addition, some features which are useful for home user, such as UPnP and DDNS, are supported.
☐ Router	In Router mode, we suppose you use ASUS Wireless Router to connect to LAN in your company. So, you can set up routing protocol to meet your requirement in office. Explaining with technical terms, router mode is, NAT is disabled, static routing protocol are allowed to set.
☐ Access Point	In Access Point mode, all 5 Ethernet ports and wireless devices are set to locate in the same local area network. Those WAN related functions are not supported here. Explaining with technical terms, access point mode is, NAT is disabled, one wan port and four lan ports of ASUS Wireless Router are bridged together.
Apply	



2) Setting up wireless encryption

WL-500gP provides a set of encryption and authentication methods to meet the different demands of home, SOHO, and enterprise users. Before setting up encryption and authentication for WL-500gP, contact your network administrator for advice.

Click **Wireless -> Interface** to open the configuration page.



Wireless - Interface	
SSID:	WL500gP
Channel:	Auto
Wireless Mode:	Auto ☐ 54g Protection
Authentication Method:	WPA
WPA Encryption:	TKIP
WPA Pre-Shared Key:	*****
WEP Encryption:	WEP-64bits
Passphrase:	
WEP Key 1 (10 or 26 hex digits):	*****
WEP Key 2 (10 or 26 hex digits):	*****
WEP Key 3 (10 or 26 hex digits):	*****
WEP Key 4 (10 or 26 hex digits):	*****
Key Index:	2
Network Key Rotation Interval:	0
Restore Finish Apply	

Encryption

The encryption modes supported by WL-500gP are: WEP (64bits), WEP (128bits), TKIP, AES, and TKIP+AES.

WEP stands for Wired Equivalent Privacy, it uses 64bits or 128bits static keys to encrypt the data for wireless transmission. To setup WEP keys, set **WEP Encryption** to **WEP-64bits** or **WEP-128bits**, then manually type in four sets **WEP Keys** (10 hexadecimal digits for 64-bit key or 26 hexadecimal digits for 128-bit key). You can also let the system generate the keys by entering a **Passphrase**.

TKIP stands for Temporal Key Integrity Protocol. TKIP dynamically generates unique keys to encrypt every data packet in a wireless session.

AES stands for Advanced Encryption Standard. This solution offers stronger protection and increases the complexity of wireless encryption.

TKIP+AES is used when both WPA and WPA2 clients co-exist in the wireless network.



Authentication

The authentication methods supported by WL-500gP include: Open, shared key, WPA-PSK, WPA, and Radius with 80.211x.

Open: This option disables authentication protection for wireless network. Under Open mode, any IEEE802.11b/g client can connect to your wireless network.

Shared: This mode uses the the WEP keys currently in use for authentication.

WPA and WPA-PSK: WPA stands for WiFi-Protected Access. WPA provides two security modes: WPA for enterprise network, and WPA-PSK for home and SOHO users. For enterprise network, WPA uses the already existing RADIUS server for authentication; for home and SOHO user, it provides Pre-Shared Key (PSK) for user identification. The Pre-Shared Key consists of 8 to 64 characters.

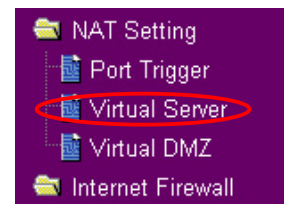
Radius with 802.11x: Similar with WPA, this solution also uses RADIUS server for authentication. The difference lays on the encryption methods: WPA adopts TKIP or AES encryption methods, while Radius with 802.11x does not provide encryption.

When authentication and encryption are set, click **Finish** to save the settings and restart the wireless router.

3) Setting up virtual server in your LAN

Virtual server is a Network Address Translation (NAT) function which turns a computer within a LAN into a server by allowing data packets of certain service, such as HTTP, from Internet.

1. Click **Virtual Server** in NAT Setting folder to open the NAT configuration page.



2. Select **Yes** to enable virtual server. For example, if host 192.168.1.100 is FTP server which is to be accessed by Internet user, it means all packets from Internet with destination port as 21 are to be directed to the host. Set Well-known Application to FTP. Port range to 21, Local IP to the host IP, Local Port to 21, Protocol to TCP.

NAT Setting - Virtual Server

To make services, like WWW, FTP, provided by a server in your local network accessible for outside users, you should specify a local IP address to the server. Then, add the IP address and network protocol type, port number, and name of the service in the following list. Based on the list, the gateway will forward service request from outside users to the corresponding local server.

Enable Virtual Server? ☒ Yes ☐ No

Virtual Server List Add Del

Well-Known Applications: FTP

Port Range	Local IP	Local Port	Protocol	Description
21	192.168.1.100	21	TCP	FTP Server (21)

3. Click **Finish**.

Restore Finish Apply

4. Click **Save & Restart** to restart the wireless router and activate the settings.

Save & Restart

Save&Restart will save all setting you have changed to ASUS Wireless Router and restart it. Please click **SaveRestart** button to continue.

Save&Restart



4) Setting up virtual DMZ in your LAN

To expose an internal host to Internet and make all services provided by this host available to outside users, enable Virtual DMZ function to open all ports of the host. This function is useful when the host plays multiple roles such as HTTP server and FTP server. However, in doing this, your network becomes less secure.

1. Click **Virtual DMZ** in the NAT Setting menu.



2. Enter the IP address of the host and click **Finish**.

NAT Setting - Virtual DMZ	
Virtual DMZ allows you to expose one computer to Internet, so that all the inbounds packets will be redirected to the computer you set. It is useful while you run some applications that use uncertain incoming ports. Please use it carefully.	
IP Address of Exposed Station:	192.168.1.100

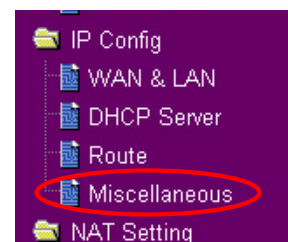
3. Click **Save & Restart** to restart the wireless router and activate the settings.

Save & Restart
Save&Restart will save all setting you have changed to ASUS Wireless Router and restart it. Please click SaveRestart button to continue.
Save&Restart

5) Setting up DDNS

DNS enables host who uses static IP address to associate with a domain name; for dynamic IP user, they can also associate with a domain name via dynamic DNS (DDNS). DDNS requires registering and account-creating at DDNS service providers' website. The DDNS server updates your IP address information once you are assigned to a new IP address. Therefore, Internet user can always access your network.

1. Click **Miscellaneous** from IP Config folder.



2. Select **Yes** to enable the DDNS service. If you do not have a DDNS account, click **Free Trial** to register for a trial account.

DDNS Setting	
Dynamic-DNS (DDNS) allows you to export your server to Internet with an unique name, even though you have no static IP address. Currently, several DDNS clients are embedded in WL566gM. You can click Free Trial below to start with a free trial account.	
Enable the DDNS Client?	☒ Yes ☐ No
Server:	WWW.DYNDNS.ORG Free Trial



- After clicking Free Trial, you are directed to the homepage of www.DynDNS.org, where you can register and apply for DDNS service.

Read the policy and select "I have read..."

- Enter your user name, e-mail address, password, then click **Create Account**.

- A message prompts out informing that your account has been created. An E-mail is sent to your mailbox. Open your mailbox and read the mail.

- You can find the activation letter in your E-mail box. Click the hyperlink.

- The link directs you to a login page. Click **login**.

- Enter the user name and password then click **Login**.