## 2) Setting up wireless encryption

WL-500W 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-500W, contact your network administrator for advice.

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

📁 Quick Setup
📁 Wireless
　📄 Interface
　📄 Bridge
　📄 Access Control
　📄 RADIUS Setting
　📄 Advanced
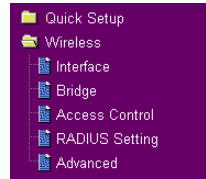
Wireless - Interface

SSID:	default
Channel:	Auto
Wireless Mode:	Auto ☐ Protection
Bandwidth:	40MHz
Authentication Method:	Open System or Shared Key
WPA Encryption:	TKIP
WPA Pre-Shared Key:	
WEP Encryption:	None
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):	

Note: For 802.11n performance, select 40MHz bandwidth. Channel option will depend on the bandwidth that you select.

Encryption

The encryption modes supported by WL-500W 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-500W 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 WEP keys currently in use for authentication.

WPA/WPA2 and WPA-PSK/WPA2-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 802.1X: 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 802.1X 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.
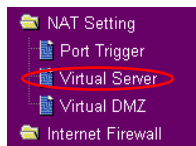
1. Click **Virtual Server** in NAT Setting folder to open the NAT configuration page.

2. Select **Yes** to enable virtual server. For example, if host 192.168.1.100 is the FTP server that the user will access, 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.

3. Click **Finish**.

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

4) Setting up virtual DMZ in your LAN

To expose an internal host to the 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.
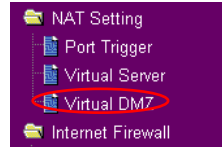
2. Enter the IP address of the host and click **Finish**.

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

5) Setting up DDNS

DNS enables host who uses static IP address to associate with a domain name; for dynamic IP users, 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. Thus, the Internet user can always access your network.

1. Click **Miscellaneous** from IP Config folder.
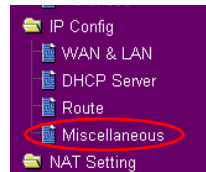
2. Select **Yes** to enable the DDNS service. If you do not have a DDNS account, click **Free Trial** to register for a trial account.

3. 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...**".

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

5. 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.

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

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

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

9. After logging in, you can see this welcome message.

Logged In

You are currently logged in as: account (Logout)

10. Select **Services** tab.

11. Click **Add Dynamic DNS Host** .

12. Enter the host name then click **Add Host**.

13. You can see this message when your hostname is successfully created.

14. Fill the account information into the DDNS setting fields of your wireless router.

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, serveral 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**
User Name or E-mail Address:	account	
Password or DDNS Key:	••••••••	
Host Name:	account.dyndns.org	
Enable wildcard?	○ Yes ⦿ No	
Update Manually:	Update	

15. Click **Finish**.

| Restore | Finish | Apply |

16. 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

17. Verify whether DDNS is working. Click **Start** menu and select **Run.** Type **cmd** and click **OK** to open the CLI console.
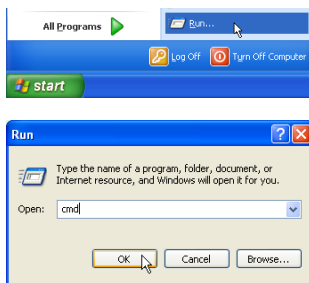
18. Type **ping account.dyndns.org** (your DDNS domain name). If you can see the reply like what is shown in the right picture, DDNS is working correctly.
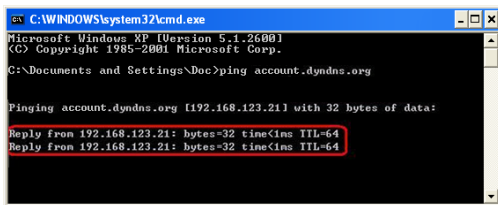
6) Setting up Bandwidth Management

Bandwidth Management provides a mechanism to set up download and upload bandwidth based on IP address and port range. You can define the minimum bandwidth and the maximum bandwidth for host within your LAN, and thus control the traffic of you network. To set up upload bandwidth management, you need to set up the virtual server to allow the incoming packets of the specified services.
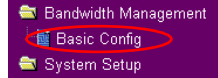
1. Click **Basic Config** page in Bandwidth Management folder.

2. Select **Yes** to enable Bandwidth Management function.

3. **Download bandwidth**

If you want to limit the download bandwidth of a host within a speed range (for example, between 100 to 200kbps), you need to fill in the host IP address, and the speeds (maximum: 200kbps; minimum: 100kbps). When the minimum speed is defined, the host can transmit data at the minimum speed regardless of the traffic conditions.

a. To apply on all host an **FTP** download speed policy, leave the IP address field blank, input "**20**" in the **Port** field and define the speeds, then click **Add**.

b. To set up **Web** access download policy, input "**80**" in the **Port** field, define the speeds and click **Add**.

c. To set up download bandwidth policy of a certain service for a host, input the host IP address and the port number of the service, define the speeds and click **Add**.

d. To set up the download bandwidth policy for all hosts in your LAN, leave the IP addresses and the port fields blank; and define the speeds (the speeds are higher than download policies). Click **Add** to add the rule.

Download Policy List — Add — Del

IP Address	Port	Max.(kbps)	Min.(kbps)
		500	200
192.168.1.6		200	100
	20	100	50
	80	300	100
192.168.1.100	3702	10	

4. **Upload stream**

If you want to set up the upload traffic control policy (for example, to limit the upload bandwidth of port 2100 of 192.168.1.2 between 10 to 80kbps), you need to first set up the NAT policy to allow incoming packets.

- NAT Setting
  - Port Trigger
  - Virtual Server
  - Virtual DMZ
- Internet Firewall
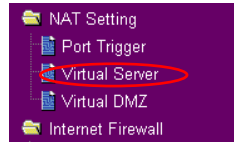
a. Select **Yes** to enable Virtual Server function. In the Virtual Server List field, fill the port, and the IP address into the fields and press **Add**.

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.
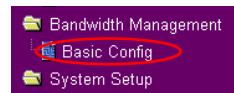
Enable Virtual Server?   ⊙ Yes ○ No

Virtual Server List   Add — Del

Well-Known Applications:		User Defined ▼		
Port Range	**Local IP**	**Local Port**	**Protocol**	**Description**
2100	192.168.1.2	2100	TCP ▼	

b. Press **Apply** button.

Restore   Finish   Apply

c. Return to the Upload Policy List in Bandwidth Management setting page.

- Bandwidth Management
  - Basic Config
- System Setup

d. Set the **Port** as "2100", **Max (kbps)** as "80", **Min.(kbps)** as "10", then click **Add**.

Upload Policy List   Add — Del

Port	Max.(kbps)	Min.(kbps)
2100	80	10

e. When the settings are complete, press **Finish**.

Restore   Finish   Apply

f. 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