

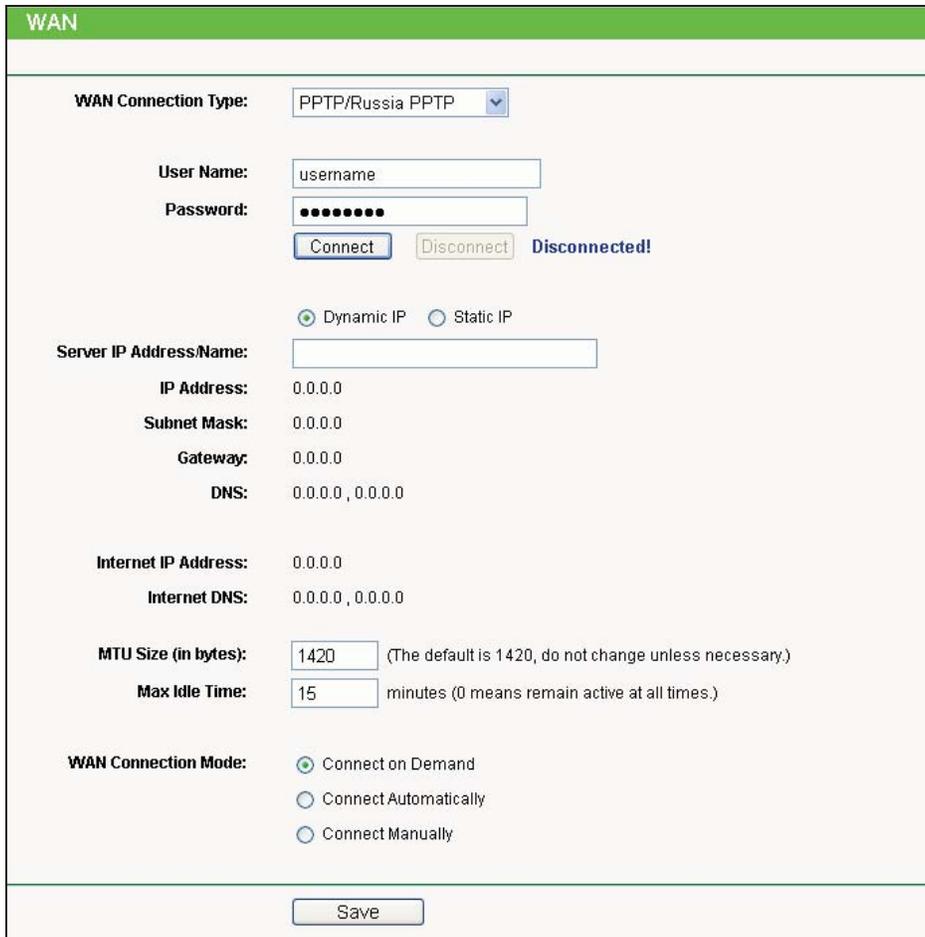
- **Connect Manually** - You can configure the Device to make it connect or disconnect manually. After a specified period of inactivity (**Max Idle Time**), the Device will disconnect from your Internet connection, and you will not be able to re-establish your connection automatically as soon as you attempt to access the Internet again. To use this option, check the radio button. If you want your Internet connection to remain active at all time, enter "0" in the **Max Idle Time** field. Otherwise, enter the number of minutes that you wish to have the Internet connecting last unless a new link is requested.

 **Note:**

Sometimes the connection cannot be disconnected although you specify a time to **Max Idle Time**, because some applications are visiting the Internet continually in the background.

Click the **Save** button to save your settings.

5. If your ISP provides PPTP connection, please select **PPTP/Russia PPTP** option. And you should enter the following parameters (Figure 5-21):



The screenshot shows the WAN configuration interface for PPTP/Russia PPTP. The 'WAN Connection Type' is set to 'PPTP/Russia PPTP'. The 'User Name' field contains 'username' and the 'Password' field is masked with dots. Below the password field are 'Connect' and 'Disconnect' buttons, with the status 'Disconnected!' displayed. The 'Server IP Address/Name' field is empty, and radio buttons for 'Dynamic IP' (selected) and 'Static IP' are present. Below are fields for 'IP Address', 'Subnet Mask', 'Gateway', and 'DNS', all set to '0.0.0.0'. Further down are 'Internet IP Address' and 'Internet DNS' fields, also set to '0.0.0.0'. The 'MTU Size (in bytes)' is set to '1420' with a note '(The default is 1420, do not change unless necessary.)'. The 'Max Idle Time' is set to '15' minutes, with a note '(0 means remain active at all times.)'. At the bottom, the 'WAN Connection Mode' has radio buttons for 'Connect on Demand' (selected), 'Connect Automatically', and 'Connect Manually'. A 'Save' button is located at the very bottom of the form.

Figure 5-21 WAN – PPTP/Russia PPTP

- **User Name/Password** - Enter the User Name and Password provided by your ISP. These fields are case-sensitive.
- **Dynamic IP/ Static IP** - Choose either as you are given by your ISP and enter the ISP's IP address or the domain name.
  - If you choose static IP and enter the domain name, you should also enter the DNS assigned by your ISP. And click the **Save** button.
  - Click the **Connect** button to connect immediately. Click the **Disconnect** button to disconnect immediately.
- **Connect on Demand** - You can configure the Device to disconnect from your Internet connection after a specified period of inactivity (**Max Idle Time**). If your Internet connection has been terminated due to inactivity, **Connect on Demand** enables the Device to automatically re-establish your connection as soon as you attempt to access the Internet again. If you wish to activate **Connect on Demand**, check the radio button. If you want your Internet connection to remain active at all times, enter "0" in the **Max Idle Time** field. Otherwise, enter the number of minutes you want to have elapsed before your Internet connection terminates.
- **Connect Automatically** - Connect automatically after the Device is disconnected. To use this option, check the radio button.
- **Connect Manually** - You can configure the Device to make it connect or disconnect manually. After a specified period of inactivity (**Max Idle Time**), the Device will disconnect from your Internet connection, and you will not be able to re-establish your connection automatically as soon as you attempt to access the Internet again. To use this option, click the radio button. If you want your Internet connection to remain active at all times, enter "0" in the **Max Idle Time** field. Otherwise, enter the number in minutes that you wish to have the Internet connecting last unless a new link is requested.

 **Note:**

Sometimes the connection cannot be disconnected although you specify a time to **Max Idle Time** because some applications are visiting the Internet continually in the background.

Click the **Save** button to save your settings.

6. If your ISP provides BigPond Cable (or Heart Beat Signal) connection, please select **BigPond Cable** option. And then you should enter the following parameters as in Figure 5-22.

 **Note:**

This type of WAN Connection is only available in AP Router mode, but not in AP Client Router Mode.

Figure 5-22 WAN – BigPond Cable

- **User Name/Password** - Enter the User Name and Password provided by your ISP. These fields are case-sensitive.
- **Auth Server** - Enter the authenticating server IP address or host name.
- **Auth Domain** - Type in the domain suffix server name based on your location.  
 NSW / ACT - [nsw.bigpond.net.au](http://nsw.bigpond.net.au)  
 VIC / TAS / WA / SA / NT - [vic.bigpond.net.au](http://vic.bigpond.net.au)  
 QLD - [qld.bigpond.net.au](http://qld.bigpond.net.au)
- **MTU Size** - The normal **MTU** (Maximum Transmission Unit) value for most Ethernet networks is 1500 Bytes. It is not recommended that you change the default **MTU Size** unless required by your ISP.
- **Connect on Demand** - In this mode, the Internet connection can be terminated automatically after a specified inactivity period (**Max Idle Time**) and be re-established when you attempt to access the Internet again. If you want your Internet connection keeps active all the time, please enter “0” in the **Max Idle Time** field. Otherwise, enter the number of minutes you want to have elapsed before your Internet access disconnects.
- **Connect Automatically** - The connection can be re-established automatically when it was down.

- **Connect Manually** - You can click the **Connect/Disconnect** button to connect/disconnect immediately. This mode also supports the **Max Idle Time** function as **Connect on Demand** mode. The Internet connection can be disconnected automatically after a specified inactivity period and re-established when you attempt to access the Internet again.
- Click the **Connect** button to connect immediately. Click the **Disconnect** button to disconnect immediately.

**Note:**

Sometimes the connection cannot be terminated although you specify a time to Max Idle Time because some applications are visiting the Internet continually in the background.

Click the **Save** button to save your settings.

### 5.6.3 MAC Clone

Choose menu “**Network > MAC Clone**”, and then you can configure the **WAN MAC Address** on the screen below, as shown in Figure 5-23:

Figure 5-23 MAC Address Clone

- **WAN MAC Address** - This field displays the current MAC address of the WAN port. If your ISP requires that you register the MAC address of your adapter, please enter the correct MAC address into this field. Usually, you do not need to change anything here. The format for the MAC Address is XX-XX-XX-XX-XX-XX (X is any hexadecimal digit).
- **Your PC's MAC Address** - This field displays the MAC address of the PC that is managing the Device. If the MAC address of your adapter is registered, you can click the **Clone MAC Address** button, and then it will be filled into the **WAN MAC Address** field.

Click **Restore Factory MAC** to restore the MAC address of WAN port to the factory default value.

Click the **Save** button to save your settings.

**Note:**

1. Only the PC(s) in your LAN can use the **MAC Address Clone** feature.
2. If you change **WAN MAC Address** when the WAN connection type is PPPoE, it will not take effect until the connection is re-established.

## 5.7 Wireless



Figure 5-24 Wireless menu in AP Router Mode

In AP Router mode, there are seven submenus under the Wireless menu (shown in Figure 5-24): **Wireless Settings**, **Wireless Security**, **Wireless MAC Filtering**, **Wireless Advanced**, **Distance Setting**, **Throughput Monitor** and **Wireless Statistics**. Click any of them, and you will be able to configure the corresponding function.

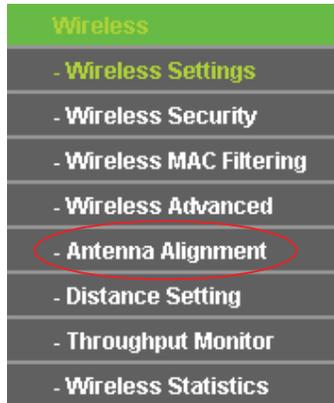


Figure 5-25 Wireless menu in AP Client Router Mode

In AP Client Router mode, there are eight submenus under the Wireless menu (shown in Figure 5-25): **Wireless Settings**, **Wireless Security**, **Wireless MAC Filtering**, **Wireless Advanced**, **Antenna Alignment**, **Distance Setting**, **Throughput Monitor** and **Wireless Statistics**. Click any of them, and you will be able to configure the corresponding function.

 **Note:**

Notably, there is one more submenu in AP Client Router mode, which is **Antenna Alignment**.

### 5.7.1 Wireless Settings

Choose menu “**Wireless > Wireless Settings**”, and then you can configure the basic settings for the wireless network on the **Wireless Settings** page (Figure 5-26 & Figure 5-27) .

**Note:**

There are differences between the Wireless Settings page in AP Router mode and that in AP Client Router mode, as shown in Figure 5-26 & Figure 5-27.

**1. Wireless settings in AP Router mode**

Figure 5-26 Wireless Settings in AP Router mode

- **Wireless Radio-** Enable or disable the wireless radio.
- **SSID-** Enter a string of up to 32 characters. The same Name (SSID) must be assigned to all wireless devices in your network. The default SSID is set to be **TP-LINK\_XXXXXX** (XXXXXX indicates the last unique six characters of each Device's MAC address), which can ensure your wireless network security. But it is recommended strongly that you change your networks name (SSID) to a different value. This value is case-sensitive. For example, **MYSSID** is NOT the same as **MySSID**.
- **Region-** Select your region from the pull-down list. This field specifies the region where the wireless function of the Device can be used. It may be illegal to use the wireless function of the Device in a region other than one of those specified in this filed. If your country or region is not listed, please contact your local government agency for assistance.
- **Channel-** This field determines which operating frequency will be used. It is not necessary to change the wireless channel unless you notice interference problems with another nearby access point. If you select auto, then the Device will select the best channel automatically.
- **Mode-** This field determines the wireless mode which the Device works on.
- **Max Tx Rate-** You can limit the maximum tx rate of the Device through this field. You can select one of security options listed as the below items.

- **Disable Security**- The wireless security function can be enabled or disabled. If disabled, the wireless stations will be able to connect the Device without encryption. It is recommended strongly that you choose one of the following options to enable security.
- **WPA-PSK/WPA2-PSK**- Select WPA based on pre-shared passphrase.
- **PSK Password**- You can enter **ASCII** or **Hexadecimal** characters.  
For **ASCII**, the length should be between 8 and 63 characters.  
For **Hexadecimal**, the length should be between 8 and 64 characters.  
Please note that the key is case sensitive.
- **Not Change**- If you chose this option, wireless security configuration will not change.

## 2. Wireless settings in AP Client Router mode

The screenshot shows the 'Wireless Settings' configuration page. It has a green header with the title 'Wireless Settings'. Below the header, there are two main sections: 'Client Setting' and 'AP Setting'.  
**Client Setting** includes:  
 - SSID: An empty text input field.  
 - BSSID: A text input field with an example '00-1D-0F-11-22-33' to its right.  
 - Region: A dropdown menu currently showing 'United States'.  
 - Warning: A text block stating: 'First at all, you should select your location, save it and reboot, or you may not search any APs. Ensure you select a correct country to conform local law. Incorrect settings may cause interference.'  
 - Search: A button labeled 'Search'.  
 - Key type: A dropdown menu currently showing 'None'.  
 - WEP Index: A dropdown menu currently showing '1'.  
 - Auth type: A dropdown menu currently showing 'open'.  
 - Password: An empty text input field.  
**AP Setting** includes:  
 - Local SSID: A text input field containing 'TP-LINK\_050500'.  
 - Three checkboxes:  
   - 'Enable Wireless Router Radio' (checked).  
   - 'Enable SSID Broadcast' (checked).  
   - 'Disable Local Wireless Access' (unchecked).  
 At the bottom center of the page is a 'Save' button.

Figure 5-27 Wireless Settings in AP Client Router mode

- **SSID** - The SSID of the AP your Device is going to connect to as a client. You can also use the search function to select a SSID to join.
- **BSSID** - The BSSID of the AP your Device is going to connect to as a client. You can also use the search function to select a BSSID to join.
- **Region** - Select your region from the pull-down list. This field specifies the region where the wireless function of the Device can be used. It may be illegal to use the wireless function of

the Device in a region other than one of those specified in this filed. If your country or region is not listed, please contact your local government agency for assistance.

- **Search** - Click this button, you can search the AP which runs in the current channel.
- **Key type** - This option should be chosen according to the AP's security configuration. It is recommended that the security type is the same as your AP's security type.
- **WEP Index** - This option should be chosen if the key type is WEP (ASCII) or WEP (HEX). It indicates the index of the WEP key.
- **Auth Type** - This option should be chosen if the key type is WEP (ASCII) or WEP (HEX). It indicates the authorization type of the Root AP.
- **Password** - If the AP your Device is going to connect needs password, you need to fill the password in this blank.
- **Local SSID** - Enter a value of up to 32 characters. The same Name (SSID) must be assigned to all wireless devices in your network.
- **Enable Wireless Router Radio** - The wireless radio of the Device can be enabled or disabled to allow wireless stations access. If enabled, the wireless stations will be able to access the Device; otherwise, wireless stations will not be able to access the Device.
- **Enable SSID Broadcast** - If you select the **Enable SSID Broadcast** checkbox, the wireless Router will broadcast its name (SSID) on the air.
- **Disable Local Wireless Access** - If you select the **Disable Local Wireless Access** checkbox, the wireless Device will disable local wireless access; other stations will not be able to access the Device by wireless.

Click **Search** button on the Wireless page shown as Figure 5-27, and then AP List page will appear, as shown in Figure 5-28. Find the SSID of the Access Point you want to access, and click **Connect** in the corresponding row. For example, the desired item is selected. The target network's SSID will be automatically filled into the corresponding box which is shown as the Figure 5-29.

AP List						
AP Count: 18						
ID	BSSID	SSID	Signal	Channel	Security	Choose
1	74-EA-3A-51-F9-38	TP-LINK_51F938	11dB	1	OFF	<a href="#">Connect</a>
2	94-0C-6D-EB-BE-5B	TP-LINK_EBBE5B	9dB	1	OFF	<a href="#">Connect</a>
3	AE-D5-A1-99-BB-5E	WepAP	26dB	1	ON	<a href="#">Connect</a>
4	00-0A-EB-CE-1E-2F	CE1E2F	28dB	2	OFF	<a href="#">Connect</a>
5	D8-5D-4C-BF-13-4C	chendeyu	24dB	2	ON	<a href="#">Connect</a>
6	94-0C-6D-2F-3C-BE	TP-LINK	16dB	4	ON	<a href="#">Connect</a>
7	D8-5D-4C-BF-14-2C	TP-LINK_BF142C	17dB	5	OFF	<a href="#">Connect</a>
8	00-27-19-C4-B9-84	1234567	37dB	6	ON	<a href="#">Connect</a>
9	00-0A-EB-01-53-01	015301	1dB	6	OFF	<a href="#">Connect</a>
10	00-25-86-1E-EE-CC	1EEEECC	255dB	6	ON	<a href="#">Connect</a>
11	F4-EC-38-2B-38-48	TP-LINK_2B3848	29dB	6	ON	<a href="#">Connect</a>
12	F4-EC-38-2B-F7-5E	TP-LINK_2BF75E	22dB	6	OFF	<a href="#">Connect</a>
13	D8-5D-4C-BA-43-E6	zora	34dB	6	OFF	<a href="#">Connect</a>
14	00-1D-0F-FB-E2-D2	2581	15dB	8	OFF	<a href="#">Connect</a>
15	D8-5D-4C-10-FF-16	TP-LINK_10FF16	6dB	9	ON	<a href="#">Connect</a>
16	00-0A-EB-13-09-19	TP-LINK_fake_WISP	6dB	10	OFF	<a href="#">Connect</a>
17	00-D2-4C-81-98-97	RTK 11n AP	3dB	11	OFF	<a href="#">Connect</a>
18	00-22-44-38-38-39	TP-LINK_383839	19dB	11	ON	<a href="#">Connect</a>

Figure 5-28 AP List

The screenshot shows the 'Wireless Settings' configuration page. It is divided into two main sections: 'Client Setting' and 'AP Setting'.  
**Client Setting:**  
 - SSID: TP-LINK\_51F938  
 - BSSID: 74-EA-3A-51-F9-38 (with an example: 00-1D-0F-11-22-33)  
 - Region: United States (dropdown menu)  
 - Warning: First at all, you should select your location, save it and reboot, or you may not search any APs. Ensure you select a correct country to conform local law. Incorrect settings may cause interference.  
 - Search: A button labeled 'Search'.  
 - Key type: None (dropdown menu)  
 - WEP Index: 1 (dropdown menu)  
 - Auth type: open (dropdown menu)  
 - Password: An empty text field.  
**AP Setting:**  
 - Local SSID: TP-LINK\_050500  
 - Enable Wireless Router Radio:   
 - Enable SSID Broadcast:   
 - Disable Local Wireless Access:   
 At the bottom of the page is a 'Save' button.

Figure 5-29

**Note:**

If you know the SSID of the desired AP, you can also input it to the field "SSID" manually.

Be sure to click the **Save** button to save your settings on this page.

**Note:**

The operating distance or range of your wireless connection varies significantly based on the physical placement of the Device. For best results, place your Device:

- Near the center of the area in which your wireless stations will operate;
- In an elevated location such as a high shelf;
- Away from the potential sources of interference, such as PCs, microwaves, and cordless phones;
- With the Antenna in the upright position;
- Away from large metal surfaces.

**Note:**

Failure to follow these guidelines can result in significant performance degradation or inability to wirelessly connect to the Device.

### 5.7.2 Wireless Security

Choose menu “**Wireless > Wireless Security**”, and then you can configure the security settings of your wireless network.

There are three wireless security modes supported by the Device: **WEP** (Wired Equivalent Privacy), **WPA/WPA2** (Wi-Fi Protected Access/ Wi-Fi Protected Access 2), and **WPA-PSK/WPA2-PSK** (Pre-Shared Key).

Figure 5-30 Wireless Security

**Note:**

Only in Standard AP mode, the current operation mode is shown at the top. Besides, if Multi-SSID, a sub mode of Standard AP, is selected, you can choose one of the 4 SSIDs from the pull-down list.

You can select one of the following security options:

- **Disable Security** - The wireless security function can be enabled or disabled. If disabled, the wireless stations will be able to connect the AP without encryption. It is recommended strongly that you choose one of following options to enable security.

- **WEP** - Select 802.11 WEP security.
- **WPA-PSK** - Select WPA based on pre-shared passphrase.
- **WPA** - Select WPA based on Radius Server.

Each security option has its own settings as described follows:

➤ **WEP**

- **Type** - You can select one of following types:

**Automatic** - Select **Shared Key** or **Open System** authentication type automatically based on the wireless station's capability and request.

**Shared Key** - Select 802.11 Shared Key authentication.

**Open System** - Select 802.11 Open System authentication.

- **WEP Key Format** - You can select **ASCII** or **Hexadecimal** format. ASCII Format stands for any combination of keyboard characters in the specified length. Hexadecimal format stands for any combination of hexadecimal digits (0-9, a-f, A-F) in the specified length.
- **WEP Key settings** - Select which of the four keys will be used and enter the matching WEP key information for your network in the selected key radio button. These values must be identical on all wireless stations in your network.
- **Key Type** - You can select the WEP key length (64-bit, or 128-bit, or 152-bit) for encryption. "Disabled" means this WEP key entry is invalid.

**For 64-bit encryption** - You can enter 10 hexadecimal digits (any combination of 0-9, a-f, A-F, and null key is not permitted) or 5 ASCII characters.

**For 128-bit encryption** - You can enter 26 hexadecimal digits (any combination of 0-9, a-f, A-F, and null key is not permitted) or 13 ASCII characters.

**For 152-bit encryption** - You can enter 32 hexadecimal digits (any combination of 0-9, a-f, A-F, and null key is not permitted) or 16 ASCII characters.

 **Note:**

If you do not set the key, the wireless security function is still disabled even if you have selected Shared Key as Authentication Type.

➤ **WPA/WPA2**

- **Version** - You can select one of following versions:

**Automatic** - Select **WPA** or **WPA2** automatically based on the wireless station's capability and request.

**WPA** - Wi-Fi Protected Access.

**WPA2** - WPA version 2.

- **Encryption** - You can select either **Automatic**, or **TKIP** or **AES**.
- **Radius Server IP** - Enter the IP address of the Radius Server.
- **Radius Port** - Enter the port that radius service uses.
- **Radius Password** - Enter the password for the Radius Server.
- **Group Key Update Period** - Specify the group key update interval in seconds. The value can be either 0 or at least 30. Enter 0 to disable the update.

➤ **WPA-PSK/WPA2-PSK**

- **Version** - You can select one of following versions:
  - Automatic** - Select **WPA-PSK** or **WPA2-PSK** automatically based on the wireless station's capability and request.
  - WPA-PSK** - Pre-shared key of WPA
  - WPA2-PSK** - Pre-shared key of WPA2
- **Encryption** - You can select either **Automatic**, or **TKIP** or **AES**.
- **PSK Password** - You can enter **ASCII** or **Hexadecimal** characters. For **Hexadecimal**, the length should be between 8 and 64 characters; for **ASCII**, the length should be between 8 and 63 characters.
- **Group Key Update Period** - Specify the group key update interval in seconds. The value can be either 0 or at least 30. Enter 0 to disable the update.

Be sure to click the **Save** button to save your settings on this page.

### 5.7.3 Wireless MAC Filtering

Choose menu "**Wireless > MAC Filtering**", and then you can control the wireless access by configuring the **Wireless MAC Filtering** function, as shown in Figure 5-31.

Figure 5-31 Wireless MAC Filtering

- To filter wireless users by MAC Address, click **Enable**. The default setting is **Disable**.
  - **MAC Address** - The wireless station's MAC address that you want to filter.
  - **Description** - A simple description of the wireless station.
  - **Status** - The status of this entry, either **Enabled** or **Disabled**.
- To Add a Wireless MAC Address filtering entry, click the **Add New...** button. The "**Add or Modify Wireless MAC Address Filtering entry**" page will appear, shown in Figure 5-32:

Figure 5-32 Add or Modify Wireless MAC Address Filtering entry

- **To add or modify a MAC Address Filtering entry, follow these instructions:**
  1. Enter the appropriate MAC Address into the **MAC Address** field. The format of the MAC Address is XX-XX-XX-XX-XX-XX(X is any hexadecimal digit). For example: 00-0A-EB-B0-00-0B.
  2. Give a simple description for the wireless station in the **Description** field. For example: Wireless station A.

3. Select **Enabled** or **Disabled** for this entry on the **Status** pull-down list.
4. Click the **Save** button to save this entry.

➤ **To modify or delete an existing entry:**

1. Click the **Modify** in the entry you want to modify. If you want to delete the entry, click the **Delete**.
2. Modify the information.
3. Click the **Save** button.

Click the **Enable All** button to make all entries enabled

Click the **Disabled All** button to make all entries disabled.

Click the **Delete All** button to delete all entries.

Click the **Next** button to go to the next page.

Click the **Previous** button to return to the previous page.

➤ **For example:** If you desire that the wireless station A with MAC address 00-0A-EB-B0-00-0B and the wireless station B with MAC address 00-0A-EB-00-07-5F are able to access the Device, but all the other wireless stations cannot access the Device, you can configure the **Wireless MAC Address Filtering** list by following these steps:

1. Click the **Enable** button to enable this function.
2. Select the radio button "**Deny the stations not specified by any enabled entries in the list to access**" for **Filtering Rules**.
3. Delete all or disable all entries if there are any entries already.
4. Click the **Add New...** button.
  - 1) Enter the MAC address 00-0A-EB-B0-00-0B/00-0A-EB-00-07-5F in the **MAC Address** field.
  - 2) Enter wireless station A/B in the **Description** field.
  - 3) Select **Enabled** in the **Status** pull-down list.
  - 4) Click the **Save** button.
  - 5) Click the **Back** button.

The filtering rules that are configured should be similar to the following list:

**Filtering Rules**

Allow the stations not specified by any enabled entries in the list to access.  
 Deny the stations not specified by any enabled entries in the list to access.

ID	MAC Address	Status	Description	Modify
1	00-0A-EB-B0-00-0B	Enabled	wireless station A	<a href="#">Modify</a> <a href="#">Delete</a>
2	00-0A-EB-00-07-5F	Enabled	wireless station A	<a href="#">Modify</a> <a href="#">Delete</a>

Figure 5-33

### 5.7.4 Wireless Advanced

Choose menu “**Wireless > Wireless Advanced**”, and then you can configure the advanced settings of your wireless network.

**Wireless Advanced**

**Antenna Setting:** Vertical Antenna   
**Transmit Power:** High   Enable High Power Mode  
**Beacon Interval :** 100 (20-1000)  
**RTS Threshold:** 2346 (1-2346)  
**Fragmentation Threshold:** 2346 (256-2346)  
**DTIM Interval:** 1 (1-255)  
 Enable WMM  
 Enable Short GI  
 Enable AP Isolation

Figure 5-34 Wireless Advanced

- **Antenna Settings** - The polarization of an antenna. You can select Vertical Antenna, Horizontal Antenna, or External Antenna.
- **Transmit Power** - Here you can specify the transmit power of the Device. You can select High, Middle or Low whichever you would like. High is the default setting and is recommended.
- **Beacon Interval** - The beacons are the packets sent by the Device to synchronize a wireless network. Beacon Interval value determines the time interval of the beacons. You can specify a value between 20-1000 milliseconds. The default value is 100.

- **RTS Threshold** - Here you can specify the RTS (Request to Send) Threshold. If the packet is larger than the specified RTS Threshold size, the Device will send RTS frames to a particular receiving station and negotiate the sending of a data frame. The default value is 2346.
- **Fragmentation Threshold** - This value is the maximum size determining whether packets will be fragmented. Setting the Fragmentation Threshold too low may result in poor network performance since excessive packets. 2346 is the default setting and is recommended.
- **DTIM Interval** - This value determines the interval of the Delivery Traffic Indication Message (DTIM). You can specify the value between 1-255 Beacon Intervals. The default value is 1, which indicates the DTIM Interval is the same as Beacon Interval.
- **Enable WMM** - WMM function can guarantee the packets with high-priority messages being transmitted preferentially. It is strongly recommended enabled.
- **Enable Short GI** - This function is recommended for it will increase the data capacity by reducing the guard interval time.
- **Enable AP Isolation** - Isolate all connected wireless stations so that wireless stations cannot access each other through WLAN. This function will be disabled if WDS/Bridge is enabled.

**Note:**

If you are not familiar with the setting items in this page, it's strongly recommended to keep the provided default values; otherwise, it may result in lower wireless network performance.

### 5.7.5 Antenna Alignment

**Note:**

This function is not available in AP Router mode, but in both Standard AP mode and AP Client Router mode.

Choose menu **"Wireless > Antenna Alignment"**, and then you can know how remote the Device's signal strength changes while changing the antenna's direction.

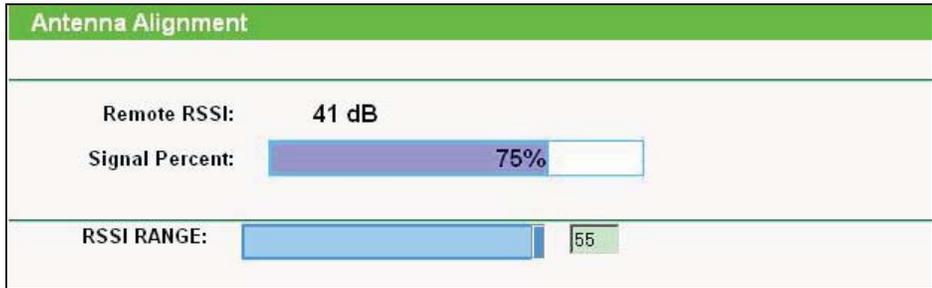


Figure 5-35 Antenna Alignment

- **Remote RSSI** - Remote AP's signal strength value.
- **Signal Percent** - The ratio of RSSI to RSSI RANGE in percentage.
- **RSSI RANGE** - You can drag the Slider to set or input the RSSI RANGE value.

**Note:**

It only works after you have established connection to remote AP in client mode.

### 5.7.6 Distance Settings

Choose menu “**Wireless > Distance Settings**”, and then you can adjust the wireless range in outdoor conditions.

Figure 5-36

This is a critical feature required for stabilizing outdoor links. Enter the distance of your wireless link, and then the software will optimize the frame ACK timeout value automatically.

**Note:**

One hundred-meter is the smallest unit of this setting.

### 5.7.7 Throughput Monitor

Selecting **Wireless > Throughput Monitor** will help to watch wireless throughput information in the following screen shown in Figure 5-37.

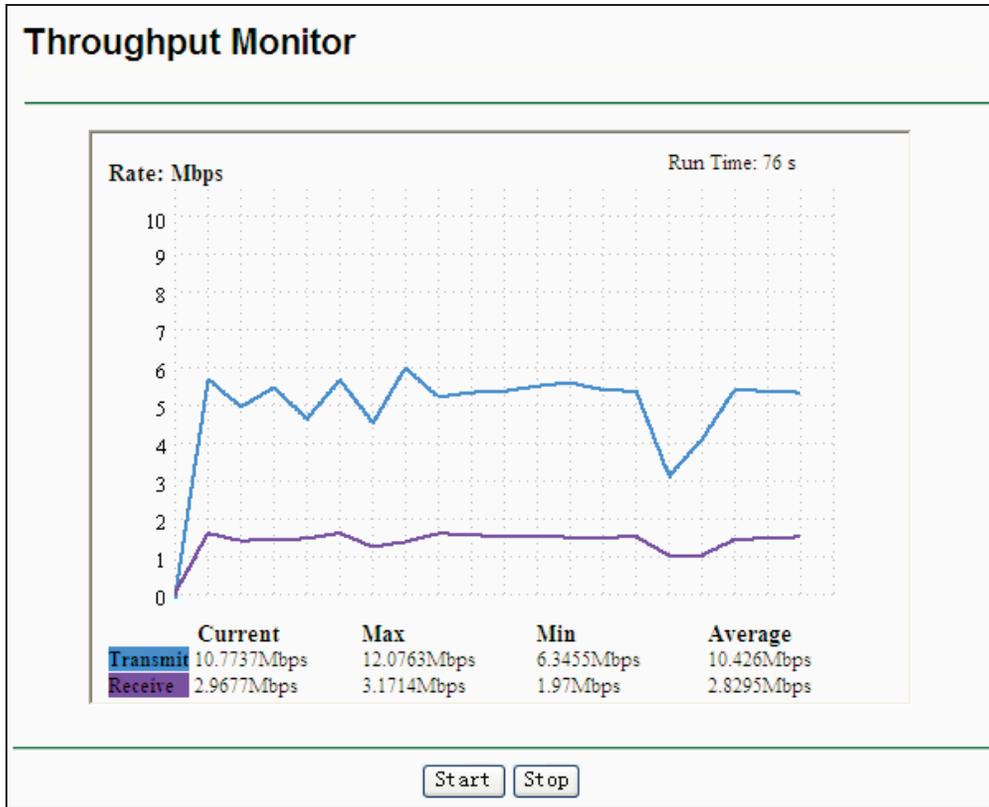


Figure 5-37 Throughput Monitor

- **Rate** - The Throughput unit.
- **Run Time** - How long this function is running.
- **Transmit** - Wireless transmit rate information.
- **Receive** - Wireless receive rate information.

Click the **Start** button to start wireless throughput monitor.

Click the **Stop** button to stop wireless throughput monitor.

### 5.7.8 Wireless Statistics

Choose menu “**Wireless > Wireless Statistics**”, and then you can see the MAC Address, Current Status, Received Packets and Sent Packets for each connected wireless station.

Wireless Statistics					
Current Connected Wireless Stations numbers:				1	<input type="button" value="Refresh"/>
ID	MAC Address	Current Status	Received Packets	Sent Packets	
1	00-0A-EB-88-34-75	STA-ASSOC	416	2	
<input type="button" value="Previous"/>		<input type="button" value="Next"/>			

Figure 5-38 Wireless Statistics

- **MAC Address** - the connected wireless station's MAC address.
- **Current Status** - the connected wireless station's running status, one of STA-AUTH / STA-ASSOC / STA-JOINED / WPA / WPA-PSK / WPA2 / WPA2-PSK / AP-UP / AP-DOWN / Disconnected.
- **Received Packets** - packets received by the station.
- **Sent Packets** - packets sent by the station.
- **Belong To** - the SSID that station belong to.

You cannot change any of the values on this page. To update this page and to show the current connected wireless stations, click on the **Refresh** button.

If the numbers of connected wireless stations go beyond one page, click the **Next** button to go to the next page and click the **Previous** button to return to the previous page.

 **Note:**

This page will be refreshed automatically every 5 seconds.

## 5.8 DHCP



Figure 5-39 The DHCP menu

The DHCP (Dynamic Host Configuration Protocol) server function, which provides the TCP/IP configuration for all the PCs that are connected to the device in the LAN, is **Disable** by default.

There are three submenus under the DHCP menu (shown in Figure 5-39), **DHCP Settings**, **DHCP Clients List** and **Address Reservation**. Click any of them, and you will be able to configure the corresponding function.

### 5.8.1 DHCP Settings

Choose menu “**DHCP > DHCP Settings**”, and then you can configure the DHCP Server on the page as shown in Figure 5-40. The Device is set up by default as a DHCP server.

Figure 5-40 DHCP Settings

- **DHCP Server - Enable** or **Disable** the server. If you disable the Server, you must have another DHCP server within your network, or else you must configure the IP address of the computer manually.
- **Start IP Address** - This field specifies the first address in the IP Address pool. 192.168.1.100 is the default start IP address.
- **End IP Address** - This field specifies the last address in the IP Address pool. 192.168.1.199 is the default end IP address.
- **Address Lease Time** – It is the length of time a network user will be allowed to keep connecting to the device with the current DHCP Address. Enter the amount of time, in minutes, that the DHCP address will be "leased". The time range is 1~2880 minutes. The default value is 120 minutes.
- **Default Gateway** - (Optional) Input the IP Address of the gateway.
- **Default Domain** - (Optional) Input the domain name of your network.
- **Primary DNS** - (Optional) Input the DNS IP address provided by your ISP.
- **Secondary DNS** - (Optional) You can input the IP Address of another DNS server if your ISP provides two DNS servers.

**Note:**

To use the DHCP server function of the device, you should configure all computers in the LAN as "Obtain an IP Address automatically" mode. This function will take effect until the device reboots.

### 5.8.2 DHCP Clients List

Choose menu "DHCP > DHCP Clients List", and then you can view the information about the clients attached to the Device in the screen as shown in Figure 5-41.

DHCP Clients List				
ID	Client Name	MAC Address	Assigned IP	Lease Time
1	Anthea	00-13-8F-AA-6D-77	192.168.1.100	01:59:29

Refresh

Figure 5-41 DHCP Clients List

- **Client Name** - The name of the DHCP client.
- **MAC Address** - The MAC address of the DHCP client.
- **Assigned IP** - The IP address that the device has allocated to the DHCP client.
- **Lease Time** - The time of the DHCP client leased.

You cannot change any of the values on this page.

To update this page and to show the current attached devices, click the **Refresh** button.

### 5.8.3 Address Reservation

Choose menu "DHCP > Address Reservation", and then you can view or add a reserved address for clients via the next screen (shown in Figure 5-42).

Address Reservation				
ID	MAC Address	Reserved IP Address	Status	Modify
1	00-0A-EB-00-23-11	192.168.1.100	Enabled	<a href="#">Modify</a> <a href="#">Delete</a>

Figure 5-42 Address Reservation

When you specify a reserved IP address for a PC on the LAN, the PC will always receive the same IP address each time when it accesses the DHCP server. Reserved IP addresses should be assigned to the servers that require permanent IP settings.

- **MAC Address** - The MAC Address of the PC that you want to reserve an IP address for.
- **Reserved IP Address** - The IP address that the device reserved.
- **Status** - It shows whether the entry is enabled or not.
- **Modify** - To modify or delete an existing entry.
- **To Reserve IP Addresses, you can follow these steps:**
  1. Click **Add New...** button in Figure 5-42, then the **Add or Modify an Address Reservation Entry** page will appear as shown in Figure 5-43.
  2. Enter the MAC Address (The format for the MAC Address is XX-XX-XX-XX-XX-XX) and the IP address in dotted-decimal notation of the computer you wish to add.
  3. Click the **Save** button.

Add or Modify an Address Reservation Entry	
<b>MAC Address:</b>	<input type="text"/>
<b>Reserved IP Address:</b>	<input type="text"/>
<b>Status:</b>	Enabled <input type="button" value="v"/>

Figure 5-43 Add or Modify an Address Reservation Entry

➤ To modify a Reserved IP Address, you can follow these steps:

1. Select the reserved address entry as you desired, **Modify** it. If you wish to delete the entry, click the **Delete** link of the entry.
2. Click the **Save** button.

Click the **Add New...** button to add a new Address Reservation entry.

Click the **Enable All** button to enable all the entries in the table.

Click the **Disable All** button to disable all the entries in the table.

Click the **Delete All** button to delete all the entries in the table.

Click the **Next** button to go to the next page, or click the **Previous** button return to the previous page.

## 5.9 Forwarding

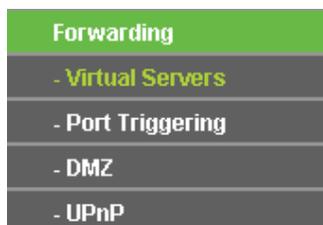


Figure 5-44 The Forwarding menu

There are four submenus under the Forwarding menu (shown in Figure 5-44): **Virtual Servers**, **Port Triggering**, **DMZ** and **UPnP**. Click any of them, and you will be able to configure the corresponding function.

### 5.9.1 Virtual Servers

Choose menu "**Forwarding > Virtual Servers**", and then you can view and add virtual servers in the screen as shown in Figure 5-45.

Virtual servers can be used for setting up public services on your LAN, such as DNS, Email and FTP. A virtual server is defined as a service port, and all requests from the Internet to this service port will be redirected to the computer specified by the server IP. Any PC that is used for a virtual server must have a static or reserved IP Address because its IP Address may be changed when using the DHCP function.

Virtual Servers					
ID	Service Port	IP Address	Protocol	Status	Modify
1	21	192.168.1.101	ALL	Enabled	<a href="#">Modify</a> <a href="#">Delete</a>

Figure 5-45 Virtual Servers

- **Service Port** - The numbers of External Ports. You can enter a service port or a range of service ports (the format is XXX - YYY, XXX is Start port, YYY is End port).
- **IP Address** - The IP address of the PC running the service application.
- **Protocol** - The protocol used for this application, either **TCP**, **UDP**, or **All** (all protocols are supported by the Device.).
- **Status** - The status of this entry. "Enabled" means the virtual server entry is enabled.
- **Common Service Port** - Some common services already exist in the pull-down list.
- **Modify** - To modify or delete an existing entry.
- **To setup a virtual server entry, you can follow these steps:**
  1. Click the **Add New...** button.
  2. Select the service you want to use from the **Common Service Port** list. If the **Common Service Port** menu does not list the service that you want to use, enter the number of the service port or service port range in the **Service Port** box.
  3. Enter the IP address of the computer running the service application in the **IP Address** box.
  4. Select the protocol used for this application in the **Protocol** box: **TCP**, **UDP**, or **All**.
  5. Select the **Enabled** option in the **Status** pull-down list.
  6. Click the **Save** button.

The screenshot shows a web form titled "Add or Modify a Virtual Server Entry". The form contains the following fields and controls:

- Service Port:** A text input field with a hint "(XX-XX or XX)".
- IP Address:** A text input field.
- Protocol:** A dropdown menu currently set to "ALL".
- Status:** A dropdown menu currently set to "Enabled".
- Common Service Port:** A dropdown menu currently set to "--Select One--".

At the bottom of the form are two buttons: "Save" and "Back".

Figure 5-46 Add or Modify a Virtual Server Entry

**Note:**

If your computer or server has more than one type of available service, please select another service, and enter the same IP Address for that computer or server.

**To modify or delete an existing entry:**

1. Click the **Modify** in the entry you want to modify. If you want to delete the entry, click the **Delete**.
2. Modify the information.
3. Click the **Save** button.

Click the **Enable/Disabled All** button to make all entries enabled/disabled.

Click the **Delete All** button to delete all entries.

Click the **Next** button to go to the next page and click the **Previous** button to return the previous page.

## 5.9.2 Port Triggering

Choose menu "**Forwarding > Port Triggering**", and then you can view and add port triggering in the screen as shown in Figure 5-47.

Some applications require multiple connections, like Internet games, video conferencing, Internet calling and so on. These applications cannot work with a pure NAT Router. Port Triggering is used for some of these applications that can work with an NAT Router.

Port Triggering						
ID	Trigger Port	Trigger Protocol	Incoming Port	Incoming Protocol	Status	Modify
1	554	ALL	8970-8999	ALL	Enabled	<a href="#">Modify</a> <a href="#">Delete</a>

Figure 5-47 Port Triggering

➤ **Once configured, operation is as follows:**

1. A local host makes an outgoing connection to an external host using a destination port number defined in the **Trigger Port** field.
2. The Device records this connection, opens the incoming port or ports associated with this entry in the **Port Triggering** table, and associates them with the local host.
3. When necessary, the external host will be able to connect to the local host using one of the ports defined in the **Incoming Ports** field.

➤ **Rules:**

- **Trigger Port** - The port for outgoing traffic. An outgoing connection using this port will Trigger this rule.
- **Trigger Protocol** - The protocol used for Trigger Ports, either **TCP**, **UDP**, or **All** (all protocols are supported by the Device.).
- **Incoming Port** - The port or port range used by the remote system when it responds to the outgoing request. A response using one of these ports will be forwarded to the PC which triggered this rule. You can input at most 5 groups of ports (or port sections). Every group of ports must be separated with ",". For example, 2000-2038, 2046, 2050-2051, 2085, 3010-3030.
- **Incoming Protocol** - The protocol used for Incoming Port, either TCP, UDP, or ALL (all protocols are supported by the Device.).
- **Status** - The status of this entry. Enabled means the Port Triggering entry is enabled.
- **Modify** - To modify or delete an existing entry.
- **Common Applications** - Some popular applications already listed in the from the pull-down list of Incoming Protocol.

➤ **To add a new rule do the following on the Port Triggering screen:**

1. Click the **Add New...** button.
2. Enter a port number used by the application to send an outgoing request in the Trigger Port box.
3. Select the protocol used for the **Trigger Port** from the pull-down list of Trigger Protocol, either TCP, UDP, or All.
4. Enter the range of port numbers used by the remote system when it responds to the PC's request in the Incoming Ports box.
5. Select the protocol used for **Incoming Ports** range from the pull-down list, either TCP, UDP, or All.
6. Select the **Enabled** option in the **Status** pull-down list.
7. Click the **Save** button to save the new rule.

Figure 5-48 Add or Modify a Port Triggering Entry

There are many popular applications in the **Common Application** list. You can select an application and then the boxes of Trigger Port and Incoming Ports will be automatically filled in. This has the same effect as adding a new rule.

➤ **To modify or delete an existing entry:**

1. Find the desired entry in the table.
2. Click **Modify** or **Delete** as desired on the **Modify** column.

Click the **Enable All** button to enable all entries.

Click the **Disable All** button to disable all entries.

Click the **Delete All** button to delete all entries.

Click the **Next** button to go to the next page and Click the **Previous** button to return to the previous page.

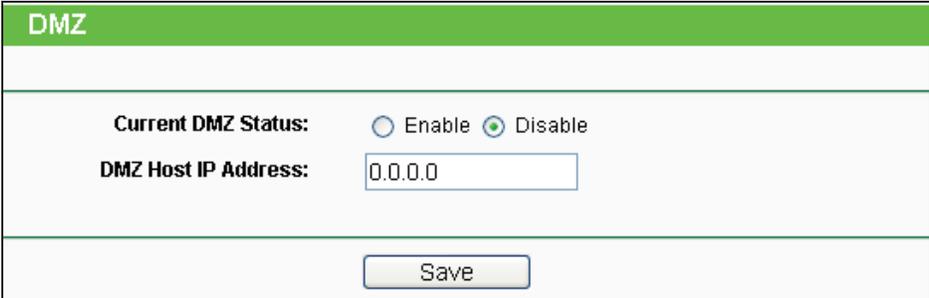
**Note:**

1. When the trigger connection is released, the corresponding opened ports will be closed.
2. Each rule can only be used by one host on the LAN at a time. The trigger connection of other hosts on the LAN will be refused.
3. **Incoming Ports** ranges cannot overlap each other.

### 5.9.3 DMZ

Choose menu "**Forwarding > DMZ**", and then you can view and configure DMZ host in the screen as shown in Figure 5-49.

The DMZ host feature allows one local host to be exposed to the Internet for a special-purpose service such as Internet gaming or video-conferencing. DMZ host forwards all the ports at the same time. Any PC whose port is being forwarded must have its DHCP client function disabled and should have a new static IP Address assigned to it because its IP Address may be changed when using the DHCP function.



DMZ	
Current DMZ Status:	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
DMZ Host IP Address:	<input type="text" value="0.0.0.0"/>
<input type="button" value="Save"/>	

Figure 5-49 DMZ

➤ **To assign a computer or server to be a DMZ server:**

1. Click the **Enable** button.
2. Enter the IP address of a local PC that is set to be DMZ host in the **DMZ Host IP Address** field.
3. Click the **Save** button.

### 5.9.4 UPnP

Choose menu “**Forwarding > UPnP**”, and then you can view the information about **UPnP** (Universal Plug and Play) in the screen as shown in Figure 5-50.

The UPnP feature allows the devices, such as Internet computers, to access the local host resources or devices as needed. UPnP devices can be automatically discovered by the UPnP service application on the LAN.

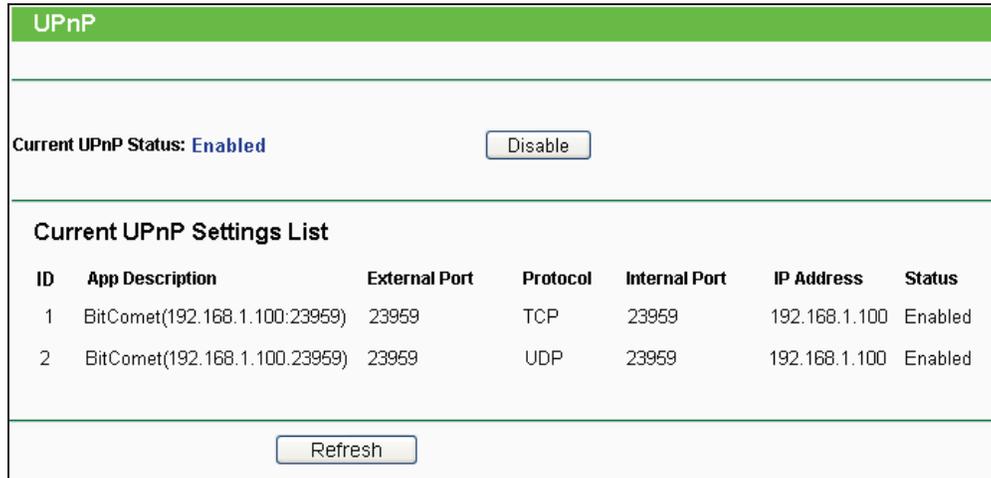


Figure 5-50 UPnP

- **Enable UPnP** - UPnP can be enabled or disabled by clicking the **Enable** or **Disable** button. This feature is enabled by default.
- **Current UPnP Settings List** - Displays the current UPnP information.
  - **App Description** - Description about the application which initiates the UPnP request.
  - **External Port** - Port that the Device opened for the application.
  - **Protocol** - Type of protocol that is opened.
  - **Internal Port** - Port that the Device opened for local host.
  - **IP Address** - IP address of the local host which initiates the UPnP request.
  - **Status** - Either Enabled or Disabled. "Enabled" means that port is still active; otherwise, the port is inactive.

Click the **Enable** button to enable UPnP.

Click the **Disable** button to disable UPnP.

Click the **Refresh** button to update the Current UPnP Settings List.

## 5.10 Security



Figure 5-51 The Security menu

There are four submenus under the Security menu as shown in Figure 5-51: **Basic Security**, **Advanced Security**, **Local Management** and **Remote Management**. Click any of them, and you will be able to configure the corresponding function.

### 5.10.1 Basic Security

Choose menu “**Security > Basic Security**”, and then you can configure the basic security in the screen as shown in Figure 5-52.

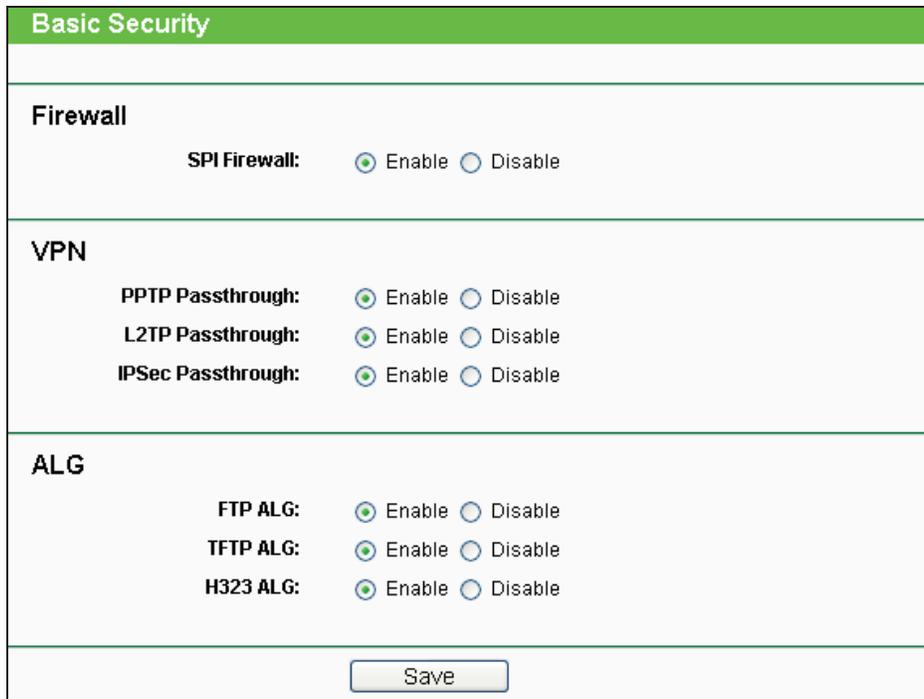


Figure 5-52 Basic Security

- **Firewall** - Here you can enable or disable the Device's firewall.
  - **SPI Firewall** - Stateful Packet Inspection (SPI) helps to prevent cyber attacks by tracking more state per session. It validates that the traffic passing through the session conforms

to the protocol. SPI Firewall is enabled by factory default. If you want all the computers on the LAN exposed to the outside world, you can disable it.

- **VPN** - VPN Passthrough must be enabled if you want to allow VPN tunnels using VPN protocols to pass through the Device.
  - **PPTP Passthrough** - PPTP (Point-to-Point Tunneling Protocol) allows the Point-to-Point Protocol (PPP) to be tunneled through an IP network. To allow PPTP tunnels to pass through the Device, click Enable.
  - **L2TP Passthrough** - L2TP (Layer Two Tunneling Protocol) is the method used to enable Point-to-Point sessions via the Internet on the Layer Two level. To allow L2TP tunnels to pass through the Device, click Enable.
  - **IPSec Passthrough** - IPSec (Internet Protocol security) is a suite of protocols for ensuring private, secure communications over IP (Internet Protocol) networks, through the use of cryptographic security services. To allow IPSec tunnels to pass through the Device, click **Enable**.
  
- **ALG** - It is recommended to enable Application Layer Gateway (ALG) because ALG allows customized Network Address Translation (NAT) traversal filters to be plugged into the gateway to support address and port translation for certain application layer "control/data" protocols such as FTP, TFTP, H323 etc.
  - **FTP ALG** - To allow FTP clients and servers to transfer data across NAT, click Enable.
  - **TFTP ALG** - To allow TFTP clients and servers to transfer data across NAT, click Enable.
  - **H323 ALG** - To allow Microsoft NetMeeting clients to communicate across NAT, click Enable.

Click the **Save** button to save your settings.

### 5.10.2 Advanced Security

Choose menu "**Security > Advanced Security**", and then you can protect the Device from being attacked by ICMP-Flood, UDP Flood and TCP-SYN Flood in the screen as shown in Figure 5-53.

Figure 5-53 Advanced Security

**Note:**

FLOOD Filtering will take effect only when the **Traffic Statistics** in **System Tools** is enabled.

- **Packets Statistics interval (5~60)** - The default value is 10. Select a value between 5 and 60 seconds in the pull-down list. The Packets Statistic interval value indicates the time section of the packets statistic. The result of the statistic used for analysis by ICMP-Flood, UDP Flood and TCP-SYN Flood.
- **DoS Protection** - Enable or Disable the DoS protection function. Only when it is enabled, will the flood filters be enabled.
- **Enable ICMP-FLOOD Attack Filtering** - Enable or Disable the ICMP-FLOOD Attack Filtering.
- **ICMP-FLOOD Packets Threshold (5~3600)** - The default value is 50. Enter a value between 5 ~ 3600. When the current ICMP-FLOOD Packets number is beyond the set value, the Device will start up the blocking function immediately.
- **Enable UDP-FLOOD Filtering** - Enable or Disable the UDP-FLOOD Filtering.
- **UDP-FLOOD Packets Threshold (5~3600)** - The default value is 500. Enter a value between 5 ~ 3600. When the current UPD-FLOOD Packets number is beyond the set value, the Device will start up the blocking function immediately.

- **Enable TCP-SYN-FLOOD Attack Filtering** - Enable or Disable the TCP-SYN-FLOOD Attack Filtering.
- **TCP-SYN-FLOOD Packets Threshold (5~3600)** - The default value is 50. Enter a value between 5 ~ 3600. When the current TCP-SYN-FLOOD Packets numbers is beyond the set value, the Device will start up the blocking function immediately.
- **Ignore Ping Packet From WAN Port** - Enable or Disable Ignore Ping Packet From WAN Port. The default setting is Disabled. If enabled, the ping packet from Internet cannot access the Device.
- **Forbid Ping Packet From LAN Port** - Enable or Disable Forbid Ping Packet From LAN Port. The default setting is Disabled. If enabled, the ping packet from LAN cannot access the Device and defend against some viruses.

Click the **Save** button to save the settings.

Click the **Blocked DoS Host List** button to display the DoS host table by blocking.

### 5.10.3 Local Management

Choose menu “**Security > Local Management**”, and then you can configure the management rule in the screen as shown in Figure 5-54. The management feature allows you to deny computers in LAN from accessing the Device.

Figure 5-54 Local Management

By default, the radio button **All the PCs on the LAN are allowed to access the Router's Web-Based Utility** is selected. If you want to allow PCs with specific MAC Addresses to access the Setup page of the Device's Web-Based Utility locally, from inside the network, click the radio button **Only the PCs listed can browse the built-in web pages to perform Administrator tasks**, and then enter each MAC Address in a separate field. The format for the MAC Address is XX-XX-XX-XX-XX-XX (X is any hexadecimal digit). Only the PCs with the MAC address listed can

use the password to browse the built-in web pages to perform Administrator tasks and all the others will be blocked.

After click the **Add** button, your PC's MAC Address will be placed in the Control List above.

Click the **Save** button to save your settings.

**Note:**

If your PC is blocked and you want to access the Device again, use a pin to press and hold the **Reset Button** on the back panel about 5 seconds to reset the Device's factory defaults in the Device's Web-Based Utility.

### 5.10.4 Remote Management

Choose menu "**Security > Remote Management**", and then you can configure the Remote Management function in the screen as shown in Figure 5-55. This feature allows you to manage your Device from a remote location via the Internet.

Figure 5-55 Remote Management

- **Web Management Port** - Web browser access normally uses the standard HTTP service port 80. This Device's default remote management web port number is 80. For greater security, you can change the remote management web port to a custom port by entering that number in the box provided. Choose a number between 1 and 65535 but do not use the number of any common service port.
- **Remote Management IP Address** - This is the current address you will use when accessing your Device from the Internet. This function is disabled when the IP address is set to the default value of 0.0.0.0. To enable this function you should change 0.0.0.0 to a valid IP address. If set to be 255.255.255.255, then all the hosts can access the Device from Internet.

To access the Device, you should enter your Device's WAN IP address into your browser's address (in IE) or location (in Netscape) box, followed by a colon and the custom port number you set in the Web Management Port box.

- For example, if your Device's WAN address is 202.96.12.8 and you use port number 8080, enter http://202.96.12.8:8080 in your browser. You will be asked for the Device's password.

After successfully entering the password, you will be able to access the Device's web-based utility.

**Note:**

Be sure to change the Device's default password to a secure password.

### 5.11 Parental Control

Choose menu **“Parental Control”**, and then you can configure the parental control in the screen as shown in Figure 5-56. The Parental Control function can be used to control the Internet activities of the children, their access to certain websites, as well as the time of surfing.

Figure 5-56 Parental Control Settings

- **Parental Control** - Check **Enable** if you want this function to take effect; otherwise check **Disable**.
- **MAC Address of Parental PC** - In this field, enter the MAC address of the controlling PC, or you can make use of the **Copy To Above** button below.
- **MAC Address of Your PC** - This field displays the MAC address of the PC that is managing this Device. If the MAC Address of your adapter is registered, you can click the **Copy To Above** button to fill this address to the MAC Address of Parental PC field above.
- **Website Description** - Description of the allowed website for the PC controlled.
- **Schedule** - The time period allowed for the PC controlled to access the Internet. For detailed information, please go to **Access Control > Schedule**.
- **Modify** - Here you can edit or delete an existing entry.

- **For example:** If you desire that the children’s PC with MAC address 00-11-22-33-44-AA can access www.google.com on Saturday only while the parent PC with MAC address 00-11-22-33-44-BB is without any restriction, you should follow the settings below:
  1. Click **Parental Control** menu on the left to enter the Parental Control Settings page. Check **Enable** and enter the MAC address 00-11-22-33-44-BB in the MAC Address of Parental PC field.
  2. Click **Access Control > Schedule** on the left to enter the **Schedule** Settings page. Click **Add New...** button to create a new schedule with Schedule Description is **Schedule\_1**, Day is **Sat** and Time is "**all day-24 hours**".
  3. Click **Parental Control** menu on the left to go back to the Parental Control Settings page, and then follow the instructions below.
    - 1) Click **Add New...** button.
    - 2) Enter 00-11-22-33-44-AA in the **MAC Address of Child PC** field.
    - 3) Enter **Allow Google** in the **Website Description** field.
    - 4) Enter **www.google.com** in the **Allowed Domain Name** field.
    - 5) Select **Schedule\_1** you create just now from the **Effective Time** drop-down list.
    - 6) In **Status** field, select **Enable**.
    - 7) Click **Save** to complete the settings.
  4. Then you will go back to the **Parental Control** Settings page and see the following list.

ID	MAC address	Website Description	Schedule	Status	Modify
1	00-11-22-33-44-AA	Allow Google	Schedule_1	Enabled	<a href="#">Edit</a> <a href="#">Delete</a>

Page

Figure 5-57 Parental Control List

- Click the **Add New...** button to add a new Parental Control entry.
- Click the **Enable All** button to enable all the rules in the list.
- Click the **Disable All** button to disable all the rules in the list.
- Click the **Delete All** button to delete all the entries in the table.
- Click the **Next** button to go to the next page.
- Click the **Previous** button return to the previous page.

## 5.12 Access Control



Figure 5-58 Access Control

There are four submenus under the Access Control menu as shown in Figure 5-58: **Rule**, **Host**, **Target** and **Schedule**. Click any of them, and you will be able to configure the corresponding function.

The Device, providing convenient and strong **Internet access control** function, can control the Internet activities of hosts in the LAN. Moreover, you can flexibly combine the **Host List**, **Target List** and **Schedule** to restrict the Internet surfing of these hosts.

### 5.12.1 Rule

Choose menu “**Access Control > Rule**”, and then you can view and set Access Control rules in the screen as shown in Figure 5-59.

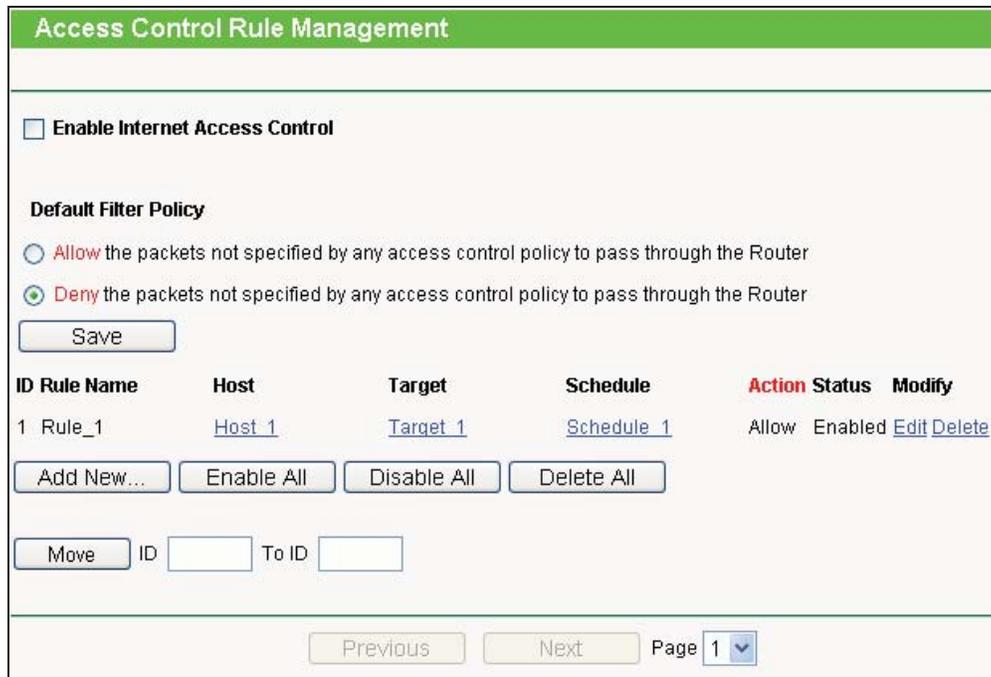


Figure 5-59 Access Control Rule Management

- **Enable Internet Access Control** - Select the check box to enable the Internet Access Control function, and then the **Default Filter Policy** can take effect.
  - **Rule Name** - Here displays the name of the rule and this name is unique.
  - **Host** - Here displays the host selected in the corresponding rule.
  - **Target** - Here displays the target selected in the corresponding rule.
  - **Schedule** - Here displays the schedule selected in the corresponding rule.
  - **Action** - Here displays the action the Device takes to deal with the packets. It could be **Allow** or **Deny**. **Allow** means that the Device permits the packets to go through the Device. **Deny** means that the Device rejects the packets to go through the Device.
  - **Status** - This field displays the status of the rule. **Enabled** means the rule will take effect, **Disabled** means the rule will not take effect.
  - **Modify** - Here you can edit or delete an existing rule.
- **For example:** If you desire to allow the host with MAC address 00-11-22-33-44-AA to access www.google.com only from 18:00 to 20:00 on Saturday and Sunday, and forbid other hosts in the LAN to access the Internet, you should follow the settings below:
1. Click the submenu **Host** of **Access Control** on the left to enter the **Host Setting** page. Add a new entry with the Host Description as Host\_1 and MAC Address as 00-11-22-33-44-AA.
  2. Click the submenu **Target** of **Access Control** on the left to enter the **Target Settings** page. Add a new entry with the Target Description as Target\_1 and Domain Name as www.google.com.
  3. Click the submenu **Schedule** of **Access Control** on the left to enter the **Schedule Settings** page. Add a new entry with the Schedule Description as Schedule\_1, Day as Sat and Sun, Start Time as 1800 and Stop Time as 2000.
  4. Click the submenu **Rule** of **Access Control** on the left to return to the **Rule Management** page. Select **Enable Internet Access Control** and choose "**Deny the packets not specified by any Internet access control rule to pass through the Router**".
  5. Click **Add New...** button to add a new rule as follows:
    - 1) In Rule Name field, create a name for the rule. Note that this name should be unique, for example Rule\_1.
    - 2) In Host field, select Host\_1.
    - 3) In Target field, select Target\_1.

- 4) In Schedule field, select Schedule\_1.
  - 5) In Action field, select Allow.
  - 6) In Status field, select Enable.
  - 7) Click **Save** to complete the settings.
6. Then you will go back to the **Access Control Rule Management** page and see the following list.

ID	Rule Name	Host	Target	Schedule	Action	Status	Modify
1	Rule_1	<a href="#">Host_1</a>	<a href="#">Target_1</a>	<a href="#">Schedule_1</a>	Allow	Enabled	<a href="#">Edit</a> <a href="#">Delete</a>

ID  To ID

Page

Figure 5-60 Access Control List

Click the **Add New...** button to add a new host list entry.

Click the **Enable All** button to enable all the rules in the list.

Click the **Disable All** button to disable all the rules in the list.

Click the **Delete All** button to delete all the entries in the table.

Click the **Next** button to go to the next page.

Click the **Previous** button return to the previous page.

### 5.12.2 Host

Choose menu “**Access Control > Host**”, and then you can view and set a Host list in the screen as shown in Figure 5-61. The host list is necessary for the Access Control Rule.

Host Settings			
ID	Host Description	Information	Modify
1	Host_1	IP: 192.168.1.1 - 192.168.1.23	<a href="#">Edit</a> <a href="#">Delete</a>

Page

Figure 5-61 Host Settings

- **Host Description** - Here displays the description of the host and this description is **unique**.
- **Information** - Here displays the information about the host. It can be IP or MAC.

- **Modify** - To modify or delete an existing entry.
- **For example:** If you desire to restrict the Internet activities of host with MAC address 00-11-22-33-44-AA, you should follow the settings below:
  1. Click **Add New...** button to enter the **Add or Modify a Host Entry** page.
  2. In Mode field, select MAC Address from the drop-down list.
  3. In Host Name field, create a unique description for the host, for example Host\_1.
  4. In MAC Address field, enter 00-11-22-33-44-AA.
  5. Click **Save** to complete the settings.
  6. Go back to the **Host Settings** page and you will see the following list.

ID	Host Description	Information	Modify
1	Host_1	MAC: 00-11-22-33-44-AA	<a href="#">Edit</a> <a href="#">Delete</a>

---

Page 1

Figure 5-62 Host List

Click the **Add New...** button to add a new host list entry.

Click the **Delete All** button to delete all the entries in the table.

Click the **Next** button to go to the next page.

Click the **Previous** button return to the previous page.

### 5.12.3 Target

Choose menu “**Access Control > Target**”, and then you can view and set a Target list in the screen as shown in Figure 5-63. The target list is necessary for the Access Control Rule.

Target Settings			
ID	Target Description	Information	Modify
1	Target_1	192.168.1.2 - 192.168.1.23/21/TCP	<a href="#">Edit</a> <a href="#">Delete</a>

---

Page 1

Figure 5-63 Target Settings

- **Target Description** - Here displays the description about the target and this description is unique.
- **Information** - The target can be IP address, port, or domain name.
- **Modify** - To modify or delete an existing entry.
- **For example:** If you desire to restrict the Internet activities of host with MAC address 00-11-22-33-44-AA in the LAN to access www.google.com only, you should first follow the settings below:
  1. Click **Add New...** button to enter **Add or Modify an Access Target Entry** page.
  2. In Mode field, select Domain Name from the drop-down list.
  3. In Target Description field, create a unique description for the target, for example Target\_1.
  4. In Domain Name field, enter www.google.com.
  5. Click **Save** to complete the settings.
  6. Go back to the **Target Settings** page and see the following list

ID	Target Description	Information	Modify
1	Target_1	www.ggoogle.com	<a href="#">Edit</a> <a href="#">Delete</a>

Page

Figure 5-64 Access Target List

Click the **Add New...** button to add a new target entry.

Click the **Delete All** button to delete all the entries in the table.

Click the **Next** button to go to the next page.

Click the **Previous** button return to the previous page.

#### 5.12.4 Schedule

Choose menu “**Access Control > Schedule**”, you can view and set a Schedule list in the next screen as shown in Figure 5-65. The Schedule list is necessary for the Access Control Rule.

Schedule Settings				
ID	Schedule Description	Day	Time	Modify
1	Schedule_1	Sat	00:00 - 24:00	<a href="#">Edit</a> <a href="#">Delete</a>
<input type="button" value="Add New..."/> <input type="button" value="Delete All"/>				
<input type="button" value="Previous"/> <input type="button" value="Next"/> Page <input type="text" value="1"/>				

Figure 5-65 Schedule Settings

- **Schedule Description** - Here displays the description of the schedule and this description is **unique**.
- **Day** - Here displays the day(s) in a week.
- **Time** - Here displays the time period in a day.
- **Modify** - Here you can edit or delete an existing schedule.
- **For example:** If you desire to restrict the Internet activities of host with MAC address 00-11-22-33-44-AA to access www.google.com only from 18:00 to 20:00 on Saturday and Sunday, you should first follow the settings below:
  1. Click **Add New...** button to enter the **Advance Schedule Settings** page.
  2. In Schedule Description field, create a unique description for the schedule, for example Schedule\_1.
  3. In Day field, choose **Select Days** and select Sat and Sun.
  4. In Time field, enter 1800 in Start Time and 2000 in Stop Time.
  5. Click **Save** to complete the settings.
  6. Go back to the **Schedule Settings** page and see the following list

Schedule Settings				
ID	Schedule Description	Day	Time	Modify
1	Schedule_1	Sat Sun	18:00 - 20:00	<a href="#">Edit</a> <a href="#">Delete</a>
<input type="button" value="Add New..."/> <input type="button" value="Delete All"/>				
<input type="button" value="Previous"/> <input type="button" value="Next"/> Page <input type="text" value="1"/>				

Figure 5-66 Schedule List

Click the **Add New...** button to add a new target entry.

Click the **Delete All** button to delete all the entries in the table.

Click the **Next** button to go to the next page.

Click the **Previous** button return to the previous page.

### 5.13 Static Routing



Figure 5-67 Static Routing

There is only one submenu under the Static Routing menu as shown in Figure 5-67: **Static Routing List**. Click it, and you will be able to configure the corresponding function.

Choose menu “**Static Routing > Static Routing List**”, and then you can configure the static route in the next screen (shown in Figure 5-68).

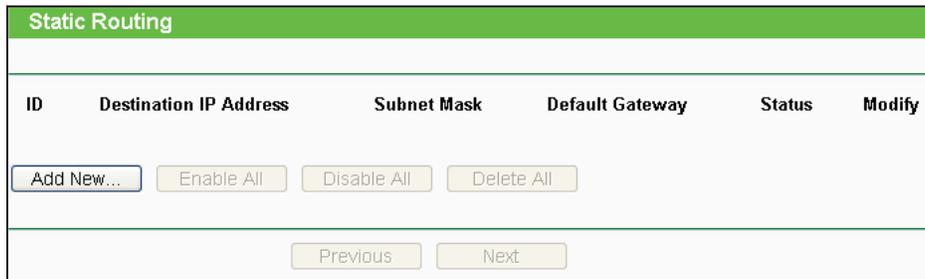


Figure 5-68

A static route is a pre-determined path that network information must follow to reach a specific host or network. Use the **Static Routing** page to add or delete a route.

➤ **To add static routing entries:**

1. Click the **Add New...** button.
2. Enter the following data:

**Destination IP Address** - The address of the network or host that you want to assign to a static route

**Subnet Mask** - Determines which portion of an IP address is the network portion, and which portion is the host portion.

**Default Gateway** - The IP address of the default gateway device that allows for the contact between the Device and the network or host

3. Select the **Enabled** in the **Status** pull-down list.
4. Click the **Save** button to save the changes.

➤ **To modify or delete an existing entry:**

1. Find the desired entry in the table.
2. Click **Modify** or **Delete** as desired on the **Modify** column.

Click the **Enable All** button to enable all entries.

Click the **Disable All** button to disable all entries.

Click the **Delete All** button to delete all entries.

## 5.14 Bandwidth Control



Figure 5-69 Bandwidth Control

There are two submenus under the Bandwidth Control menu as shown in Figure 5-69: **Control Settings** and **Rules List**. Click any of them, and you will be able to configure the corresponding function. The detailed explanations for each submenu are provided below.

### 5.14.1 Control Settings

Choose menu “**Bandwidth Control > Control Settings**”, and then you can configure the Egress Bandwidth and Ingress Bandwidth in the next screen (shown in Figure 5-70). Their values should be configured less than 1000000Kbps.

Figure 5-70 Bandwidth Control Settings

- **Enable Bandwidth Control** - If enabled, the Bandwidth Control rules will take effect.
- **Egress Bandwidth** - The upload speed through the WAN port.
- **Ingress Bandwidth** - The download speed through the WAN port.

### 5.14.2 Rules List

Choose menu “**Bandwidth Control > Rules List**”, and then you can view and configure the Bandwidth Control rules in the screen below.

Bandwidth Control Rules List							
ID	Description	Egress Bandwidth(Kbps)		Ingress Bandwidth(Kbps)		Enable	Modify
		Min	Max	Min	Max		
1	192.168.1.2 - 192.168.1.23/21	0	1000	0	4000	<input checked="" type="checkbox"/>	<a href="#">Modify</a> <a href="#">Delete</a>

Now is the  page

Figure 5-71 Bandwidth Control Rules List

- **ID** - The sequence of entry.
- **Description** - The information of description include address range, the port range and protocol of transport layer.
- **Egress Bandwidth** - The max upload speed which through the WAN port. The default number is 0.
- **Ingress Bandwidth** - The max download speed which through the WAN port. The default number is 0.
- **Enable** - Rule status, which shows whether the rule takes effect.
- **Modify** - Choose to modify or delete an existing entry.

### 5.15 IP& MAC Binding



Figure 5-72 the IP & MAC Binding menu

There are two submenus under the IP &MAC Binding menu (shown in Figure 5-72): **Binding Settings** and **ARP List**. Click either of them, and you will be able to view or configure the corresponding function. The detailed explanations for each submenu are provided below.

### 5.15.1 Binding Settings

Choose menu “**IP&MAC Binding > Binding Settings**”, and then you can view and configure the IP&MAC Binding in the screen below.

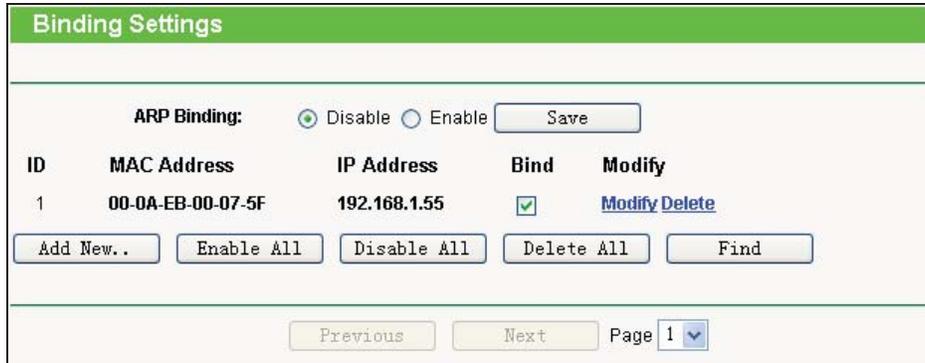


Figure 5-73 Binding Settings

- **MAC Address** - The MAC address of the controlled computer in the LAN.
- **IP Address** - The assigned IP address of the controlled computer in the LAN.
- **Bind** - Check this option to enable ARP binding for a specific device.
- **Modify** -To modify or delete an existing entry.
  
- **Add New...** - Click the **Add New...** button to add a new entry to the table.
- **Enable All** - Click the **Enable All** button to enable all entries.
- **Disable All** - Click the **Disable All** button to disable all entries.
- **Delete All** - Click the **Delete All** button to delete all entries.
- **Find** - To find existed entry you want.

### 5.15.2 ARP List

Choose menu "IP&MAC Binding > ARP List", and then you can view and configure the ARP List in the screen below shown in Figure 5-74.

ARP List				
ID	MAC Address	IP Address	Status	Configure
1	00-0A-EB-00-07-5F	192.168.1.55	Bound	<a href="#">Load</a> <a href="#">Delete</a>
2	00-14-5E-91-19-E3	192.168.1.56	Bound	<a href="#">Load</a> <a href="#">Delete</a>
3	00-19-66-80-54-2B	192.168.1.92	Unbound	<a href="#">Load</a> <a href="#">Delete</a>

Figure 5-74 ARP List

- **MAC Address** - The MAC address of a controlled computer in the LAN.
- **IP Address** - The assigned IP address of a controlled computer in the LAN.
- **Status** - Indicates whether or not the MAC and IP addresses are bound.
- **Configure** - These buttons are for loading or deleting an item.
  - **Load** - Load the item to the IP & MAC Binding list.
  - **Delete** - Delete the item from the list.
- **Bind All** - Bind all current items. This option is only available when ARP Binding is enabled and saved in the Binding Setting page.
- **Load All** - Load all items into the IP & MAC Binding list.

 **Note:**

An item can not be loaded to the IP & MAC Binding list if the IP address of the item has been loaded before. Error warning will prompt as well. Likewise, "Load All" only loads the items have no interference with the IP & MAC Binding list.

## 5.16 Dynamic DNS

The Device offers a Dynamic Domain Name System (**DDNS**) feature. DDNS lets you assign a fixed host and domain name to a dynamic Internet IP address. It is useful when you are hosting your own website, FTP server, or other server behind the Device. Before using this feature, you

need to sign up for DDNS service providers such as [www.comexe.cn](http://www.comexe.cn), [www.dyndns.org](http://www.dyndns.org), or [www.no-ip.com](http://www.no-ip.com). The Dynamic DNS client service provider will give you a password or key.

1. If the dynamic DNS **Service Provider** you select is [www.comexe.cn](http://www.comexe.cn), the page will appear as shown in Figure 5-75.

Figure 5-75 Comexe.cn DDNS Settings

➤ **To set up for DDNS, follow these instructions:**

- 1) Enter the **Domain Names** your dynamic DNS service provider gave.
- 2) Enter the **User Name** for your DDNS account.
- 3) Enter the **Password** for your DDNS account.
- 4) Click the **Login** button to login the DDNS service.

➤ **Connection Status** - The status of the DDNS service connection is displayed here.

Click **Logout** to logout the DDNS service.

 **Note:**

If you want to login again with another account after a successful login, please click the Logout button, then input your new username and password and click the Login button.

- If the dynamic DNS **Service Provider** you select is [www.dyndns.org](http://www.dyndns.org), the page will appear as shown in Figure 5-76.

Figure 5-76 DynDNS.org DDNS Settings

- **To set up for DDNS, follow these instructions:**
  - 1) Enter the User Name for your DDNS account.
  - 2) Enter the Password for your DDNS account.
  - 3) Enter the Domain Name you received from dynamic DNS service provider.
  - 4) Click the Login button to login to the DDNS service.
- **Connection Status** - The status of the DDNS service connection is displayed here.

Click **Logout** to logout of the DDNS service.

**Note:**

If you want to login again with another account after a successful login, please click the Logout button, then input your new username and password and click the Login button.

- If the dynamic DNS **Service Provider** you select is [www.no-ip.com](http://www.no-ip.com), the page will appear as shown in Figure 5-77.

**DDNS**

**Service Provider:** No-IP ( www.no-ip.com ) [Go to register...](#)

**User Name:** username

**Password:** ●●●●●●●●

**Domain Name:**

Enable DDNS

**Connection Status:** DDNS not launching!

Login Logout

Save

Figure 5-77 No-ip.com DDNS Settings

➤ **To set up for DDNS, follow these instructions:**

1. Enter the User Name for your DDNS account.
2. Enter the Password for your DDNS account.
3. Enter the Domain Name you received from dynamic DNS service provider.
4. Click the Login button to login to the DDNS service.

➤ **Connection Status** - The status of the DDNS service connection is displayed here.

Click **Logout** to logout of the DDNS service.

**Note:**

If you want to login again with another account after a successful login, please click the Logout button, then input your new username and password and click the Login button.

## 5.17 System Tools



Figure 5-78 The System Tools menu

There are nine submenus under the **System Tools** main menu (as shown in Figure 5-78): **Time Settings**, **Diagnostic**, **Firmware Upgrade**, **Factory Defaults**, **Backup & Restore**, **Reboot**, **Password**, **System Log** and **Statistics**. Click any of them, and you will be able to configure the corresponding function. The detailed explanations for each submenu are provided below.

### 5.17.1 Time Settings

Choose menu "**System Tools > Time Settings**", and then you can configure the time on the following screen.

 A configuration page titled "Time Settings" with a green header. The page contains the following fields and controls:
 

- Time zone:** A dropdown menu showing "(GMT+08:00) Beijing, Hong Kong, Perth, Singapore".
- Date:** Three input boxes for month (1), day (1), and year (2000), with "(MM/DD/YY)" to the right.
- Time:** Three input boxes for hour (2), minute (25), and second (31), with "(HH/MM/SS)" to the right.
- NTP Server Prior:** Two input boxes, both containing "0.0.0.0".
- A button labeled "Get GMT" with the text "(Get GMT when connected to Internet)" below it.
- A "Save" button at the bottom center.

Figure 5-79 Time settings

- **Time Zone** - Select your local time zone from this pull down list.
- **To set time manually:**
  1. Select your local time zone.
  2. Enter the **Date** in Month/Day/Year format.

3. Enter the **Time** in Hour/Minute/Second format.
4. Click **Save**.

➤ **For automatic time synchronization:**

1. Enter the address of the **NTP Server Prior**.
2. Click the **Get GMT** button to get GMT from the Internet.

👉 **Note:**

1. This setting will be used for some time-based functions such as firewall functions. These time-dependant functions will not work if time is not set. So, it is important to specify time settings as soon as you successfully login to the Device.
2. The time will be lost if the Device is turned off.
3. The Device will automatically obtain GMT from the Internet if it is configured accordingly.

### **5.17.2 Diagnostic**

Choose menu “**System Tools > Diagnostic**”, and then you can transact Ping or Traceroute function to check connectivity of your network in the following screen.

**Diagnostic Tools**

**Diagnostic Parameters**

Diagnostic Tool:  Ping  Traceroute

IP Address/ Domain Name:

Ping Count:  (1-50)

Ping Packet Size:  (4-1472 Bytes)

Ping Timeout:  (100-2000 Milliseconds)

Traceroute Max TTL:  (1-30)

**Diagnostic Results**

The Router is ready.

Figure 5-80 Diagnostic Tools

- **Diagnostic Tool** - Click the radio button to select one diagnostic tool:
  - **Ping** - This diagnostic tool troubleshoots connectivity, reachability, and name resolution to a given host or gateway.
  - **Traceroute** - This diagnostic tool tests the performance of a connection.

 **Note:**

You can use ping/traceroute to test both numeric IP address or domain name. If pinging/tracerouting the IP address is successful, but pinging/tracerouting the domain name is not, you might have a name resolution problem. In this case, ensure that the domain name you are specifying can be resolved by using Domain Name System (DNS) queries.

- **IP Address/ Domain Name** - Enter the IP Address or Domain Name of the PC whose connection you wish to diagnose.
- **Ping Count** - Specifies the number of Echo Request messages sent. The default is 4.
- **Ping Packet Size** - Specifies the number of data bytes to be sent. The default is 64.
- **Ping Timeout** - Time to wait for a response, in milliseconds. The default is 800.

- **Traceroute Max TTL** - Set the maximum number of hops (max TTL to be reached) in the path to search for the target (destination). The default is 20.

Click the **Start** button to start the diagnostic procedure.

The **Diagnostic Results** page (as shown in Figure 5-81) displays the result of diagnosis.

If the result is similar to the following screen, the connectivity of the Internet is fine.

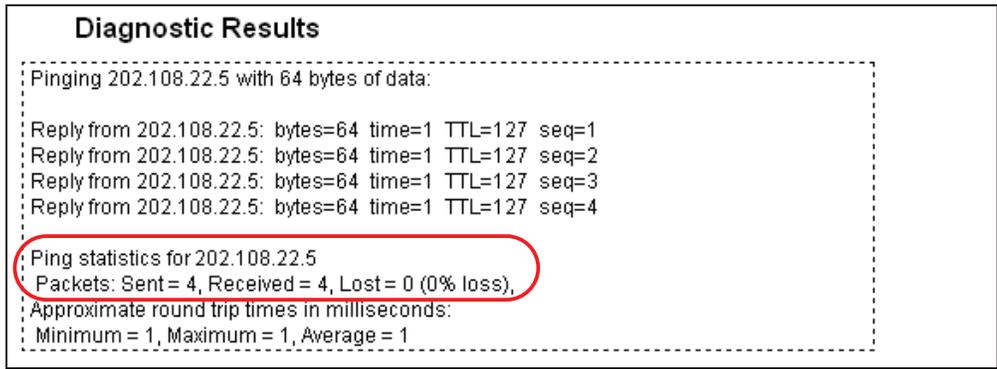


Figure 5-81 Diagnostic Results

**Note:**

1. Only one user can use the diagnostic tools at one time.
2. "Ping Count", "Ping Packet Size" and "Ping Timeout" are Ping Parameters, and "Traceroute Max TTL" is Traceroute Parameter.

### 5.17.3 Firmware Upgrade

Choose menu **"System Tools > Firmware Upgrade"**, and then you can update the latest version of firmware for the Device on the following screen.

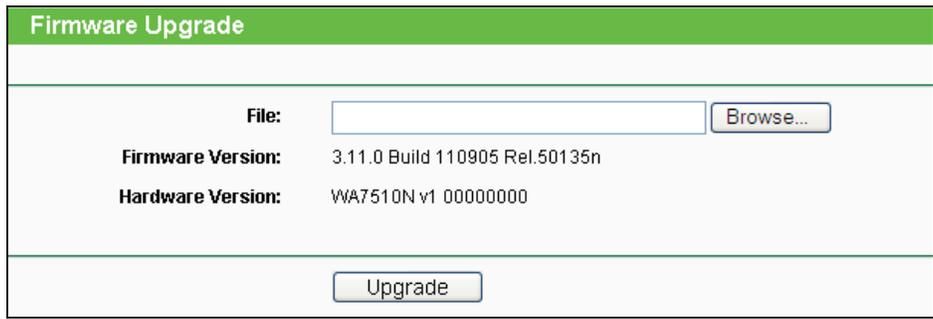


Figure 5-82 Firmware Upgrade

- **To upgrade the Device's firmware, follow these instructions:**

1. Download a most recent firmware upgrade file from our website ([www.tp-link.com](http://www.tp-link.com)).

2. Enter or select the path name where you save the downloaded file on the computer into the **File Name** blank.
  3. Click the **Upgrade** button.
  4. The Device will reboot while the upgrading has been finished.
- **Firmware Version** - Displays the current firmware version.
  - **Hardware Version** - Displays the current hardware version. The hardware version of the upgrade file must accord with the current hardware version.

 **Note:**

The firmware version must correspond to the hardware. The upgrade process takes a few moments and the Device restarts automatically when the upgrade is complete. It is important to keep power applied during the entire process. Loss of power during the upgrade could damage the Device.

#### 5.17.4 Factory Defaults

Choose menu “**System Tools > Factory Defaults**”, and you can restore the configurations of the Device to factory defaults on the following screen.



Figure 5-83 Restore Factory Default

Click the **Restore** button to reset all configuration settings to their default values.

- Default User Name - **admin**.
- Default Password - **admin**.
- Default IP Address - **192.168.1.254**.
- Default Subnet Mask - **255.255.255.0**.

 **Note:**

All changed settings will be lost when defaults are restored.

### 5.17.5 Backup & Restore

Choose menu “**System Tools > Backup & Restore**”, and then you can save the current configuration of the Device as a backup file and restore the configuration via a backup file as shown in Figure 5-84.



Figure 5-84 Backup & Restore

Click the **Backup** button to save all configuration settings to your local computer as a file.

- To restore the AP's configuration, follow these instructions:
  1. Click the **Browse** button to find the configuration file which you want to restore.
  2. Click the **Restore** button to update the configuration with the file whose path is the one you have input or selected in the blank.

#### **Note:**

The current configuration will be covered with the uploading configuration file. Wrong process will lead the device unmanaged. The restoring process lasts for 20 seconds and the AP will restart automatically then. Keep the power of the AP on during the process, in case of any damage.

### 5.17.6 Reboot

Choose menu “**System Tools > Reboot**”, and then you can click the **Reboot** button to reboot the Device via the next screen.



Figure 5-85 Reboot the Device

Click the **Reboot** button to reboot the Device.

- Some settings of the Device will take effect only after rebooting, including:

- Change the LAN IP Address (system will reboot automatically).
- Change the DHCP Settings.
- Change the Wireless configurations.
- Change the Web Management Port.
- Upgrade the firmware of the Device (system will reboot automatically.).
- Restore the Device's settings to the factory defaults (system will reboot automatically.).
- Update the configuration with the file (system will reboot automatically.).

### 5.17.7 Password

Choose menu “**System Tools > Password**”, and then you can change the factory default user name and password of the Device in the next screen as shown in Figure 5-86.

The screenshot shows a web interface for changing the password. It features a green header bar with the text 'Password'. Below this, there are five text input fields arranged in two columns. The first column contains 'Old User Name:', 'Old Password:', and 'Confirm New Password:'. The second column contains 'New User Name:', 'New Password:', and another empty input field. At the bottom of the form, there are two buttons: 'Save' and 'Clear All'.

Figure 5-86 Password

It is strongly recommended that you change the factory default user name and password of the AP. All users who try to access the AP's web-based utility will be prompted for the AP's user name and password.

**Note:**

The new user name and password must not exceed 14 characters in length and must not include any spaces. Enter the new Password twice to confirm it.

Click the **Save** button when finished.

Click the **Clear All** button to clear all.

### 5.17.8 System log

Choose menu “System Tools > System Log”, and then you can view the logs of the Device.

The screenshot shows the 'System Log' interface. At the top, there is a green header with the text 'System Log'. Below the header, there are several controls: 'Auto Mail Feature: Disabled' with a 'Mail Settings' button, 'Log Type: All' with a dropdown arrow, and 'Log Level: ALL' with a dropdown arrow. The main part of the interface is a table with the following data:

Index	Time	Type	Level	Log Content
7	1st day 00:00:07	SECURITY	INFO	H323 ALG enabled
6	1st day 00:00:07	SECURITY	INFO	TFTP ALG enabled
5	1st day 00:00:07	SECURITY	INFO	FTP ALG enabled
4	1st day 00:00:06	SECURITY	INFO	IPSEC Passthrough enabled
3	1st day 00:00:06	SECURITY	INFO	L2TP Passthrough enabled
2	1st day 00:00:06	SECURITY	INFO	PPTP Passthrough enabled
1	1st day 00:00:03	OTHER	INFO	System started

Below the table, there is system status information: 'Time = 2000-01-01 0:03:42 223s', 'H-Ver = WA7510N v1 00000000 : S-Ver = 3.11.0 Build 110905 Rel.50135n', 'L = 192.168.1.254 : M = 255.255.255.0', and 'W1 = DHCP : W = 0.0.0.0 : M = 0.0.0.0 : G = 0.0.0.0'. At the bottom, there are four buttons: 'Refresh', 'Save Log', 'Mail Log', and 'Clear Log'. At the very bottom, there are navigation buttons: 'Previous', 'Next', 'Current No. 1' (with a dropdown arrow), and 'Page'.

Figure 5-87 System Log

- **Auto Mail Feature** - Indicates whether auto mail feature is enabled or not.
- **Mail Settings** - Set the receiving and sending mailbox address, server address, validation information as well as the timetable for Auto Mail Feature.

Figure 5-88 Mail Account Settings

- **From** - Your mail box address.
- **To** - Recipient's address.
- **SMTP Server** - Your SMTP server.
- **Authentication** - Most SMTP Server requires Authentication.

 **Note:**

Only when you select **Authentication**, do you have to enter the User Name and Password in the following fields.

- **User Name** - Your mail account name.
- **Password** - Your mail account password.
- **Auto Mail Feature** will help you monitor how your Device is running.

Everyday, at specified time, the Device will automatically send the log to specified mailbox.

Every few hours, such as 2 hours, the Device will automatically send the log to specified mailbox.

- **Log Type** - By selecting the log type, only logs of this type will be shown.
- **Log Level** - By selecting the log level, only logs of this level will be shown.
- **Refresh** - Refresh the page to show the latest log list.

- **Save Log** - Click to save all the logs in a txt file.
- **Mail Log** - Click to send an email of current logs manually according to the address and validation information set in Mail Settings. The result will be shown in the later log soon.
- **Clear Log** - All the logs will be deleted from the Device permanently, not just from the page.

Click the **Next** button to go to the next page.

Click the **Previous** button return to the previous page.

### 5.17.9 Statistics

Choose menu “**System Tools > Statistics**”, and then you can view the statistics of the Device, including total traffic and current traffic of the last Packets Statistic Interval.

Figure 5-89 Statistics

The Statistics page shows the network traffic of each PC on the LAN, including total traffic and the value of the last **Packets Statistic interval** in seconds.

- **Current Statistics Status** - Enabled or Disabled. The default value is disabled. To enable, click the Enable button. If disabled, the function of DoS protection in Security settings will be disabled.
- **Packets Statistics Interval** - The default value is 10. Select a value between 5 and 60 seconds in the pull-down list. The Packets Statistic interval value indicates the time section of the packets statistic.
- **Sorted Rules** - Choose how displayed statistics are sorted.

Click the **Auto-refresh** checkbox to refresh automatically.

Click the **Refresh** button to refresh the page.

Click the **Reset All** button to reset the values of all entries to zero.

Click the **Delete All** button to delete all entries in the table.

➤ **Statistics Table**

IP Address/ MAC Address	Total		Current				Modify
	Packets	Bytes	Packets	Bytes	ICMP Tx	UDP Tx	
The current list is empty.							
Per page <input type="text" value="5"/> entries Current No. <input type="text" value="1"/> page							
<input type="button" value="Previous"/> <input type="button" value="Next"/>							

Figure 5-90 Statistics Table

➤ **IP Address/MAC Address** - The IP Address and MAC address are displayed with related statistics.

➤ **Total**

- **Packets** - The total number of packets received and transmitted by the Device.
- **Bytes** - The total number of bytes received and transmitted by the Device.

➤ **Current**

- **Packets** - The total number of packets received and transmitted in the last Packets Statistics interval seconds.
- **Bytes** - The total number of bytes received and transmitted in the last Packets Statistics interval seconds.
- **ICMP Tx** - The number of ICMP packets transmitted to the WAN per second at the specified Packets Statistics interval. It is shown like "current transmitting rate / Max transmitting rate".
- **UDP Tx** - The number of UDP packets transmitted to the WAN per second at the specified Packets Statistics interval. It is shown like "current transmitting rate / Max transmitting rate".
- **TCP SYN Tx** - The number of TCP SYN packets transmitted to the WAN per second at the specified Packets Statistics interval. It is shown like "current transmitting rate / Max transmitting rate".

➤ **Modify**

- **Reset** - Reset the values of the entry to zero.
- **Delete** - Delete the existing entry in the table.

## Appendix A: FAQ

### 1. How do I configure the Device to access the Internet by ADSL users?

- 1) First, configure the ADSL Modem configured in RFC1483 bridge model.
- 2) Connect the Ethernet cable from your ADSL Modem to the WAN port on the Device. The telephone cord plugs into the Line port of the ADSL Modem.
- 3) Login to the Device, click the “Network” menu on the left of your browser, and click "WAN" submenu. On the WAN page, select “PPPoE” for WAN Connection Type. Type user name in the “User Name” field and password in the “Password” field, finish by clicking “Connect”.

The screenshot shows the WAN Connection Type configuration interface. At the top, 'WAN Connection Type:' is set to 'PPPoE' with a dropdown arrow and a 'Detect' button. Below this, the 'PPPoE Connection:' section contains two input fields: 'User Name:' with the text 'username' and 'Password:' with a masked field of ten dots.

Figure A-1 PPPoE Connection Type

- 4) If your ADSL lease is in “pay-according-time” mode, select “Connect on Demand” or “Connect Manually” for the Internet connection mode. Type in an appropriate number for “Max Idle Time” to avoid wasting paid time. Otherwise, you can select “Auto-connecting” for the Internet connection mode.

The screenshot shows the Wan Connection Mode configuration interface. Under 'Wan Connection Mode:', there are four radio button options: 'Connect on Demand' (selected), 'Connect Automatically', 'Time-based Connecting', and 'Connect Manually'. Below 'Connect on Demand', there is a 'Max Idle Time:' field set to '15' minutes. Below 'Time-based Connecting', there is a 'Period of Time:' field set from '0 : 0 (HH:MM)' to '23 : 59 (HH:MM)'. At the bottom, there are 'Connect' and 'Disconnect' buttons, and the status 'Disconnected!' is displayed.

Figure A-2 PPPoE Connection Mode

**Note:**

1. Sometimes the connection cannot be disconnected although you specify a time to Max Idle Time, since some applications is visiting the Internet continually in the background.
2. If you are a Cable user, please configure the Device following the above steps.

**2. How do I configure the Device to access the Internet by Ethernet users?**

- 1) Login to the Device, click the “Network” menu on the left of your browser, and click "WAN" submenu. On the WAN page, select “Dynamic IP” for "WAN Connection Type", finish by clicking “Save”.
- 2) Some ISPs require that you register the MAC Address of your adapter, which is connected to your cable/DSL Modem during installation. If your ISP requires MAC register, login to the Device and click the "Network" menu link on the left of your browser, and then click "MAC Clone" submenu link. On the "MAC Clone" page, if your PC’s MAC address is proper MAC address, click the "Clone MAC Address" button and your PC’s MAC address will fill in the "WAN MAC Address" field. Or else, type the MAC Address into the "WAN MAC Address" field. The format for the MAC Address is XX-XX-XX-XX-XX-XX. Then click the "Save" button. It will take effect after rebooting.

Figure A-3 MAC Clone

**3. If I want to use Net meeting, what do I need to do?**

- 1) If you start Net meeting as a sponsor, you don’t need to do anything with the Device.
- 2) If you start as a response, you need to configure Virtual Server or DMZ Host.
- 3) How to configure Virtual Server: Login to the Device, click the “Forwarding” menu on the left of your browser, and click "Virtual Servers" submenu. On the "Virtual Server" page, click **Add New**, then on the “Add or Modify a Virtual Server” page, enter “1720” into the blank behind the “Service Port”, and your IP address behind the IP Address, assuming 192.168.1.169 for an example, remember to “Enable” and “Save”.

Figure A-4 Virtual Servers

The screenshot shows a web interface titled "Add or Modify a Virtual Server Entry". It contains the following fields and controls:

- Service Port:** A text input field containing "1720" with a help icon and the text "(XX-XX or XX)".
- IP Address:** A text input field containing "192.168.1.169".
- Protocol:** A dropdown menu currently set to "ALL".
- Status:** A dropdown menu currently set to "Enabled".
- Common Service Port:** A dropdown menu currently set to "--Select One--".
- Buttons:** "Save" and "Back" buttons are located at the bottom of the form.

Figure A-5 Add or Modify a Virtual server Entry

**Note:**

Your opposite side should call your WAN IP, which is displayed on the "Status" page.

- 4) How to enable DMZ Host: Login to the Device, click the "Forwarding" menu on the left of your browser, and click "DMZ" submenu. On the "DMZ" page, click "Enable" radio and type your IP address into the "DMZ Host IP Address" field, using 192.168.1.169 as an example, remember to click the **Save** button.

The screenshot shows a web interface titled "DMZ". It contains the following fields and controls:

- Current DMZ Status:** Two radio buttons, "Enable" (which is selected) and "Disable".
- DMZ Host IP Address:** A text input field containing "192.168.1.169".
- Buttons:** A "Save" button is located at the bottom of the form.

Figure A-6 DMZ

**4. If I want to build a Web Server on the LAN, what should I do?**

- 1) Because the Web Server port 80 will interfere with the Web management port 80 on the Device, you must change the Web management port number to avoid interference.
- 2) To change the Web management port number: Login to the Device, click the "Security" menu on the left of your browser, and click "Remote Management" submenu. On the "Remote Management" page, type a port number except 80, such as 88, into the "Web Management Port" field. Click "Save" and reboot the Device.

Figure A-7 Remote Management

**Note:**

If the above configuration takes effect, to configure to the Device by typing <http://192.168.1.254:88/> (the Device's LAN IP address: Web Management Port) in the address field of the Web browser.

- 3) Login to the Device, click the “Forwarding” menu on the left of your browser, and click the “Virtual Servers” submenu. On the “Virtual Server” page, click **Add New**, then on the “Add or Modify a Virtual Server” page, enter “80” into the blank behind the “Service Port”, and your IP address behind the IP Address, assuming 192.168.1.188 for an example, remember to “Enable” and “Save”.

Figure A-8 Virtual Servers

A-9 Add or Modify a Virtual server Entry

**5. Why is it that the wireless stations cannot connect to the Device?**

- 1) Make sure the "Wireless Router Radio" is enabled.
- 2) Make sure that the wireless stations' SSID accord with the Device's SSID.
- 3) Make sure the wireless stations have the right KEY for encryption when the Device is encrypted.
- 4) If the wireless connection is ready, but you can't access the Device, check the IP Address of your wireless stations.

## Appendix B: Factory Defaults

Item	Default Value
<b>Common Default Settings</b>	
Username	admin
Password	admin
IP Address	192.168.1.254
Subnet Mask	255.255.255.0
<b>Wireless</b>	
SSID	TP-LINK_XXXXXX
Wireless Security	Disable
Wireless MAC Address Filtering	Disable
<b>DHCP</b>	
DHCP Server	Disable
Start IP Address	192.168.1.100
End IP Address	192.168.1.199
Address Lease Time	120 minutes (Range:1 ~ 2880 minutes)
Default Gateway (optional)	0.0.0.0
Primary DNS (optional)	0.0.0.0
Secondary DNS (optional)	0.0.0.0

 **Note:**

The default SSID is TP-LINK\_XXXXXX (XXXXXX indicates the last unique six characters of each device's MAC address). This value is case-sensitive.

## Appendix C: Specifications

<b>General</b>	
Standards and Protocols	IEEE 802.11a, IEEE 802.11n, IEEE 802.3, IEEE 802.3u, IEEE 802.1x, IEEE 802.3x, IEEE 802.11i, IEEE 802.11e
Safety & Emission	FCC, CE
Ports	One 10/100M Auto-Negotiation LAN RJ45 port, supporting passive MDI/MDIX
LEDs	PWR, LAN, four RRSI
<b>Wireless</b>	
Channel	36, 40, 44, 48, 149, 153, 157, 161, 165
Frequency Band	5.180 ~ 5.240GHz ( Indoor Use ); 5.745 ~ 5.825GHz
Antenna	Type: External Antenna
	Gain: 15dBi
Wireless Data Rates	11a: 54/48/36/24/18/12/9/6Mbps 11n: up to 150 Mbps
Data Modulation	11a: OFDM; 11n: QPSK,BPSK,16-QAM,64-QAM
Wireless Encryptions	WPA/WPA2; 64/128/152-bit WEP; TKIP/AES
<b>Physical and Environment</b>	
Temperature	Operating: -30°C ~ 40°C
	Storage: -40°C ~ 40°C
Humidity	Operating: 10% ~ 90% RH, Non-condensing
	Storage: 5% ~ 90% RH, Non-condensing
Output Voltage	12V/1A
<b>Power adapter Info</b>	
Brand	LEADER ELECTRONICS INC.
Model	MU12-S120100-XX("XX"means different pin type)
Rating	Input: 100~240VAC,50/60Hz,0.5A Output: 12VDC1A

## Appendix D: Glossary

- **802.11n** - 802.11n builds upon previous 802.11 standards by adding MIMO (multiple-input multiple-output). MIMO uses multiple transmitter and receiver antennas to allow for increased data throughput via spatial multiplexing and increased range by exploiting the spatial diversity, perhaps through coding schemes like Alamouti coding. The Enhanced Wireless Consortium (EWC) was formed to help accelerate the IEEE 802.11n development process and promote a technology specification for interoperability of next-generation wireless local area networking (WLAN) products.
- **DDNS (Dynamic Domain Name System)** - The capability of assigning a fixed host and domain name to a dynamic Internet IP Address.
- **DHCP (Dynamic Host Configuration Protocol)** - A protocol that automatically configure the TCP/IP parameters for the all the PC(s) that are connected to a DHCP server.
- **DMZ (Demilitarized Zone)** - A Demilitarized Zone allows one local host to be exposed to the Internet for a special-purpose service such as Internet gaming or videoconferencing.
- **DNS (Domain Name System)** - An Internet Service that translates the names of websites into IP addresses.
- **Domain Name** - A descriptive name for an address or group of addresses on the Internet.
- **DoS (Denial of Service)** - A hacker attack designed to prevent your computer or network from operating or communicating.
- **DSL (Digital Subscriber Line)** - A technology that allows data to be sent or received over existing traditional phone lines.
- **ISP (Internet Service Provider)** - A company that provides access to the Internet.
- **MTU (Maximum Transmission Unit)** - The size in bytes of the largest packet that can be transmitted.
- **NAT (Network Address Translation)** - NAT technology translates IP addresses of a local area network to a different IP address for the Internet.
- **PPPoE (Point to Point Protocol over Ethernet)** - PPPoE is a protocol for connecting remote hosts to the Internet over an always-on connection by simulating a dial-up connection.
- **SSID** - A **S**ervice **S**et **I**dentification is a thirty-two character (maximum) alphanumeric key identifying a wireless local area network. For the wireless devices in a network to communicate with each other, all devices must be configured with the same SSID. This is typically the configuration parameter for a wireless PC card. It corresponds to the ESSID in the wireless Access Point and to the wireless network name.

- **WEP (Wired Equivalent Privacy)** - A data privacy mechanism based on a 64-bit or 128-bit or 152-bit shared key algorithm, as described in the IEEE 802.11 standard.
- **Wi-Fi** - is a trademark of the Wi-Fi Alliance, founded in 1999 as Wireless Internet Compatibility Alliance (WICA), comprising more than 300 companies, whose products are certified by the Wi-Fi Alliance, based on the IEEE 802.11 standards (also called Wireless LAN (WLAN) and Wi-Fi). This certification warrants interoperability between different wireless devices.
- **WISP - Wireless Internet Service Providers (WISPs)** are Internet service providers with networks built around wireless networking. The technology used ranges from commonplace Wi-Fi mesh networking or proprietary equipment designed to operate over open 900MHz, 2.4GHz, 4.9, 5.2, 5.4, and 5.8GHz bands or licensed frequencies in the UHF or MMDS bands.
- **WLAN (Wireless Local Area Network)** - A group of computers and associated devices communicate with each other wirelessly, which network serving users are limited in a local area.