

Figure 4-42 Add or Modify a Static Route 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.

4.12 IP & MAC Binding

ARP Binding is useful for controlling access of specific computers in the LAN. This page displays the **IP & MAC Binding Setting** table; you can operate it in accord with your desire.

There are two submenus under the IP & MAC Binding menu (shown in Figure 4-43): **Binding Setting** and **ARP List**. Click any of them, and you will be able to configure the corresponding function. The detailed explanations for each submenu are provided below.



Figure 4-43 the IP & MAC Binding menu

4.12.1 Binding Setting

Selecting **IP & MAC Binding > Binding Setting** will allow you to configure the binding entries, as shown in Figure 4-44.



Figure 4-44 Binding Setting

- **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.

When you want to add or modify an IP & MAC Binding entry, you can click the **Add New** button or **Modify** button, and then you will go to the next page. This page is used for adding or modifying an IP & MAC Binding entry (shown in Figure 4-45).

IP & MAC Binding Settings

Bind:

MAC Address:

IP Address:

Figure 4-45 IP & MAC Binding Setting (Add & Modify)

To add IP & MAC Binding entries, follow the steps below.

1. Click the **Add New...** button as shown in Figure 4-62.
2. Enter the MAC Address and IP Address.
3. Select the Bind checkbox.
4. Click the **Save** button to save it.

To modify or delete an existing entry, follow the steps below.

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

To find an existing entry, follow the steps below.

1. Click the **Find** button as shown in Figure 4-62.
2. Enter the MAC Address or IP Address.
3. Click the **Find** button in the page as shown in Figure 4-46.

Find IP & MAC Binding Entry

MAC Address:

IP Address:

ID	MAC Address	IP Address	Bind	Link
1	00-0A-EB-00-07-BE	192.168.1.101	<input checked="" type="checkbox"/>	To page

Figure 4-46 Find IP & MAC Binding Entry

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

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

4.12.2 ARP List

Selecting **IP & MAC Binding > ARP List** will enable you to observe the computers in the LAN by checking the relationship of MAC address and IP address on the ARP list, and you could configure the items on the ARP list also. This page displays the ARP List; it shows all the existing IP & MAC Binding entries (shown in Figure 4-47).

ARP List				
ID	MAC Address	IP Address	Status	Configure
1	00-19-66-CB-45-66	192.168.1.93	Unbound	Load Delete
2	00-0A-EB-00-07-BE	192.168.1.101	Bound	Load Delete

Figure 4-47 ARP List

- **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.
- **Status** - Indicates whether or not the MAC and IP addresses are bound.
- **Configure** - Load or delete an item.
 - **Load** - Load the item to the IP & MAC Binding list.
 - **Delete** - Delete the item.

Click the **Bind All** button to bind all the current items, available after enable.

Click the **Load All** button to load all items to the IP & MAC Binding list.

Click the **Refresh** button to refresh all items.

 **Note:**

An item could 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 without interference to the IP & MAC Binding list.

4.13 Dynamic DNS

The router 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 router. Before using this feature, you need to sign up for DDNS service providers such as www.dyndns.org, www.oray.net or www.comexe.cn. The Dynamic DNS client service provider will give you a password or key.

4.13.1 Dyndns.org DDNS

If your selected dynamic DNS **Service Provider** is www.dyndns.org , the page will appear as shown in Figure 4-48.

DDNS

Service Provider: DynDNS (www.dyndns.org) [Go to register...](#)

User Name:

Password:

Domain Name:

Enable DDNS

Connection Status: DDNS not launching!

Figure 4-48 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 log in to the DDNS service.
- **Connection Status** - The status of the DDNS service connection is displayed here.

Click **Logout** to log out the DDNS service.

4.13.2 Oray.net DDNS

If your selected dynamic DNS **Service Provider** is www.oray.net, the page will appear as shown in Figure 4-49.

Figure 4-49 Oray.net 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. Click the **Login** button to log in to the DDNS service.
- **Connection Status** - The status of the DDNS service connection is displayed here.
 - **Domain Name** - The domain names are displayed here.

Click **Logout** to log out the DDNS service.

4.13.3 Comexe.cn DDNS

If your selected dynamic DNS **Service Provider** is www.comexe.cn, the page will appear as shown in Figure 4-50.

Figure 4-50 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 log in to the DDNS service.
- **Connection Status** -The status of the DDNS service connection is displayed here.
- Click **Logout** to log out the DDNS service.

4.14 SNMP

SNMP will allow the network management station to retrieve statistics and status from the SNMP agent in this device. Simple Network Management Protocol (SNMP) is a popular network monitoring and management protocol, used to refer to a collection of specifications for network management that include the protocol itself. To use this function, select Enable and enter the following parameters in Figure 4-51.



Figure 4-51 SNMP Settings

4.14.1 Community Setting

Selecting **SNMP > Community Setting** will allow you to configure the SNMP community as

shown in Figure 4-52, which is helpful for managing the access authority.

Community List				
Num	Community	Access Mode	Status	Status
1	public	Read Only	Disable	Modify
2	public	Read Only	Disable	Modify
3	public	Read Only	Disable	Modify
4	public	Read Only	Disable	Modify

Figure 4-52 Community Setting

- **Num** - Displays the entry number of the community.
- **Community** - Defines the password used to authenticate the management station to the device.
- **Access Mode** - This field allows you to specify the authority of the community. Read Only means the community is only permitted to read the device configuration. Read&Write means the community has the authority to read and change the device configuration.
- **Status** - This field allows you to enable/disable the corresponding entry.
- **Modify** - This field allows you to modify an entry.

To modify a community setting entry:

1. Find the desired entry in the table.
2. Click **Modify** as desired on the **Modify** column.
3. Modify the contact of **community**
4. Select the **Read Only** or **Read&Write** option in the **Access Mode** pull-down list.
5. Select the **Enabled** option in the **Status** pull-down list.
6. Click the **Save** button.

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

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

4.14.2 SNMP System Setting

Selecting **SNMP > SNMP Setting** will allow you to configure some parameters for System (iso.org.dod.internet.mgmt.mib-2.system) as shown in Figure 4-53.

The image shows a web form titled "SNMP System Settings". It has a green header bar with the title. Below the header, there are three input fields: "System Contact:", "System Name:", and "System Location:". Each field is followed by a rectangular text box. At the bottom of the form, there is a "Save" button.

Figure 4-53 SNMP System Setting

- **System Contact** - The textual identification of the contact person for this managed node, together with information on how to contact this person.
- **System Name** - An administratively-assigned name for this managed node. By convention, this is the node's fully-qualified domain name.
- **System Location** - The physical location of this node.

Click the **Save** button to save configuration in current page.

4.15 System Tools

System Tools option helps you to optimize the configuration of your device. You can upgrade the AP to the latest version of firmware as well as backup or restore the AP's configuration files. Ping Watch Dog can help to continuously monitor a particular connection to a remote host. Speed Test helps to test the connection speed to and from any reachable IP address on current network, especially when we are building wireless network between devices which are far away from each other. It's suggested that you change the default password to a more secure one because it controls access to the device's web-based management page. Besides, you can find out what happened to the system in System Log.

There are ten submenus under the **System Tools** menu (shown as Figure 4-54): **Time**, **Firmware**, **Factory Defaults**, **Backup & Restore**, **Ping Watch Dog**, **Speed Test**, **Reboot**, **Password**, **Syslog** and **Statistics**. Clicking any of them will enable you to configure the corresponding function. The detailed explanations for each submenu are provided below.



Figure 4-54 The System Tools menu

4.15.1 Time

Selecting **System Tools > Time** will allow you to set time manually or get GMT from the Internet for the router on the page as shown in Figure 4-55.

Figure 4-55 Time settings

- **Time Zone** - Select your local time zone from this drop-down list.
- **Date** - Enter your local date in MM/DD/YY into the right blanks.
- **Time** - Enter your local time in HH/MM/SS into the right blanks.

To configure Time settings, please follow these steps below:

1. Select your local time zone.
2. Enter date and time in the right blanks
3. Click **Save**.

Click the **Get GMT** button to get GMT time from the Internet if you have connected to the Internet.

If you're using Daylight saving time, please follow the steps below.

1. Select **Using Daylight Saving Time**.
2. Enter daylight saving begin time and end time in the right blanks.

 **Note:**

- 1) This setting will be used for some time-based functions such as firewall. You must specify your time zone once you log in to the router successfully, if not, the time limited on these functions will not take effect.
- 2) The time will be lost if the router is turned off.

The router will obtain GMT automatically from the Internet When it connects to Internet.

4.15.2 Firmware

Selecting **System Tools > Firmware** allows you to upgrade the latest version of firmware for the device on the screen shown in Figure 4-56.

Figure 4-56 Firmware Upgrade

New firmware versions are posted at <http://www.tp-link.com> and can be downloaded for free. There is no need to upgrade the firmware unless the new firmware has a new feature you want to use. However, when experiencing problems caused by the AP itself, you can try to upgrade the firmware.

Note:

Before upgrading the AP's firmware, you should write down some of your customized settings to avoid losing important configuration settings of AP.

To upgrade the AP's firmware, please take the following steps:

1. Download a more recent firmware upgrade file from the TP-LINK website (<http://www.tp-link.com>).
 2. Click **Browse** to view the folders and select the downloaded file.
 3. Click **Upgrade**.
- **Firmware Version** - Displays the current firmware version.
 - **Hardware Version** - Displays the current hardware version. The upgrade file must accord with the current hardware version.

Note:

Do not turn off the AP or press the **Reset** button while the firmware is being upgraded. The AP will reboot after the Upgrading has been finished.

4.15.3 Factory Defaults

Selecting **System Tools > Factory Default** allows you to restore the factory default settings for the device on the screen shown in Figure 4-57).

Figure 4-57 Restore Factory Default

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

- The default **User Name**: admin
- The default **Password**: admin

- The default **IP Address**: 192.168.1.254
- The default **Subnet Mask**: 255.255.255.0

 **Note:**

All settings you have saved will be lost when the default settings are restored.

4.15.4 Backup & Restore

Selecting **System Tools > Backup & Restore** allows you to save all configuration settings to your local computer as a file or restore the device's configuration on the screen shown in Figure 4-58.



Figure 4-58 Save or Restore the Configuration

Click **Backup** to save a backup configuration file to your local computer.

To restore the AP's configuration, please take the following steps:

- Click **Browse** to find the location of configuration file which you want to restore.
- Click **Restore** to update the configuration with the file whose path is the one you have input or selected in the blank.

 **Note:**

- 1) The current configuration will be covered by the uploading configuration file.
- 2) Wrong process will lead the device unmanaged.
- 3) The restoring process will last for 20 seconds and the AP will restart automatically. Do not power off the device during the process to avoid any damage.

4.15.5 Ping Watch Dog

Selecting **System Tools > Ping Watch Dog** allows you to continuously monitor the particular connection between the device to a remote host. It makes this device continuously ping a user defined IP address (it can be the internet gateway for example). If it is unable to ping under the user defined constraints, this device will automatically reboot.

Ping Watch Dog Utility

Enable:

IP Address:

Interval: seconds

Delay: seconds

Fail Count:

Figure 4-59 Ping Watch Dog Utility

- **Enable** - Turn on/off Ping Watch Dog.
- **IP Address** - The IP address of the target host where the Ping Watch Dog Utility is sending ping packets.
- **Interval** - Time interval between two ping packets which are sent out continuously.
- **Delay** - Time delay before first ping packet is sent out when the device is restarted.
- **Fail Count** - Upper limit of the ping packet the device can drop continuously. If this value is overrun, the device will restart automatically.

Be sure to click the **Submit** button to make your settings in operation.

4.15.6 Speed Test

Selecting **System > Speed Test** allows you to test the connection speed to and from any reachable IP address on current network on the page as shown in Figure 4-60. The speed test is especially used when you are building wireless network between devices which are far away from each other. It should be used for the preliminary throughput estimation between two network devices. The estimation is rough. You can input the remote device's administrator Username and Password under **Advance options** to get a precise estimation if the remote device is **TL-WA5210G** too.

Figure 4-60 Speed Test

- **Destination IP** - The Remote device's IP address.
- **User** - Administrator password of the remote device. It should be filled correctly if you want to get a precise estimation. Otherwise, keep it clean.
- **Advanced options** - This is a switch to show advanced test options which are used only for precise estimation.

Note:

If either User or Password is incorrect, we will take a basic test instead. In other words, none of the advance options you set will take effect.

- **Direction** - There are 3 options available for the traffic direction while estimating the throughput.
 - **transmit** - Estimate the outgoing throughput (TX).
 - **receive** - Estimate the ingoing throughput (RX).
 - **both** - Estimate the incoming (RX) first and then the outgoing (TX) afterwards.
- **Duration** - The value you specify here indicate how much time the test should last.
- **Data amount** - The maximal data amount to be sent out during the whole test.

Note:

If both Duration and Data amount are specified, the test will stop after any of them is met.

Be sure to click the **Run Test** button to start a new test after you filled enough information. You can also stop a running test by click Stop Test button at any time.

4.15.7 Reboot

Selecting **System Tools > Reboot** allows you to reboot the device on the screen shown in Figure 4-61.



Figure 4-61 Reboot the AP

Click **Reboot** to reboot the AP.

Some settings of the AP will take effect only after rebooting, which include:

- Change LAN IP Address. (System will reboot automatically)
- Upgrade the firmware of the AP (system will reboot automatically).
- Restore the AP's settings to factory default (system will reboot automatically).
- DHCP service function.
- Static address assignment of DHCP server.

4.15.8 Password

Selecting **System Tools** > **Password** allows you to change the factory default user name and password of the device on the screen shown in Figure 4-62.

Figure 4-62 Password

It is strongly recommended that you change the factory default user name and password of the AP to more secure ones because they control access to the AP's web-based utility. All users who try to access the AP's web-based utility or Quick Setup 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 space. Enter the new Password twice to confirm it.

Click **Save** when finished.

Click **Clear All** to clear all.

4.15.9 Syslog

Selecting **System Tools** > **System Log** allows you to query the Logs of the device on the screen

shown in Figure 4-63.

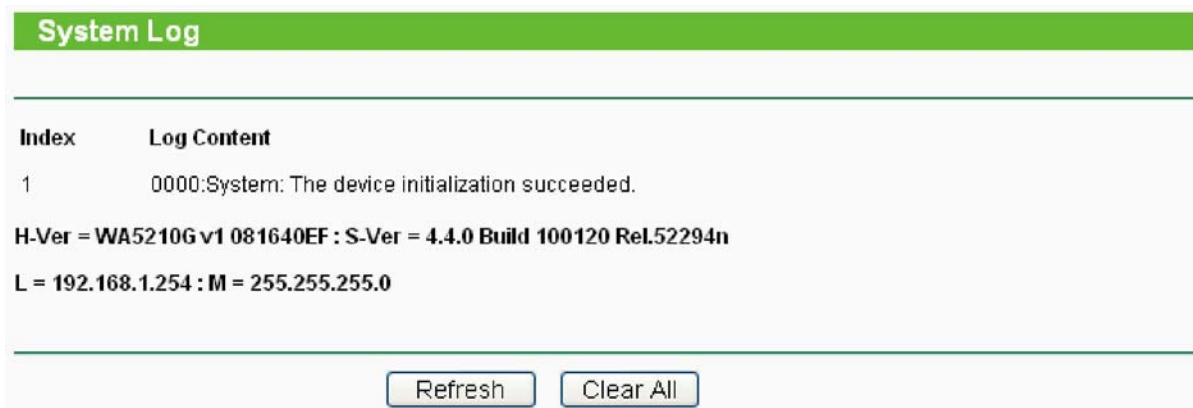


Figure 4-63 System Log

The AP can keep logs of all traffic. You can query the logs to find out what happened to the AP. Click **Refresh** to refresh the logs.

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

4.15.10 Statistics

The Statistics page (shown in Figure 4-64) displays the network traffic of each PC on the LAN, including total traffic and traffic of the last **Packets Statistic interval** seconds.

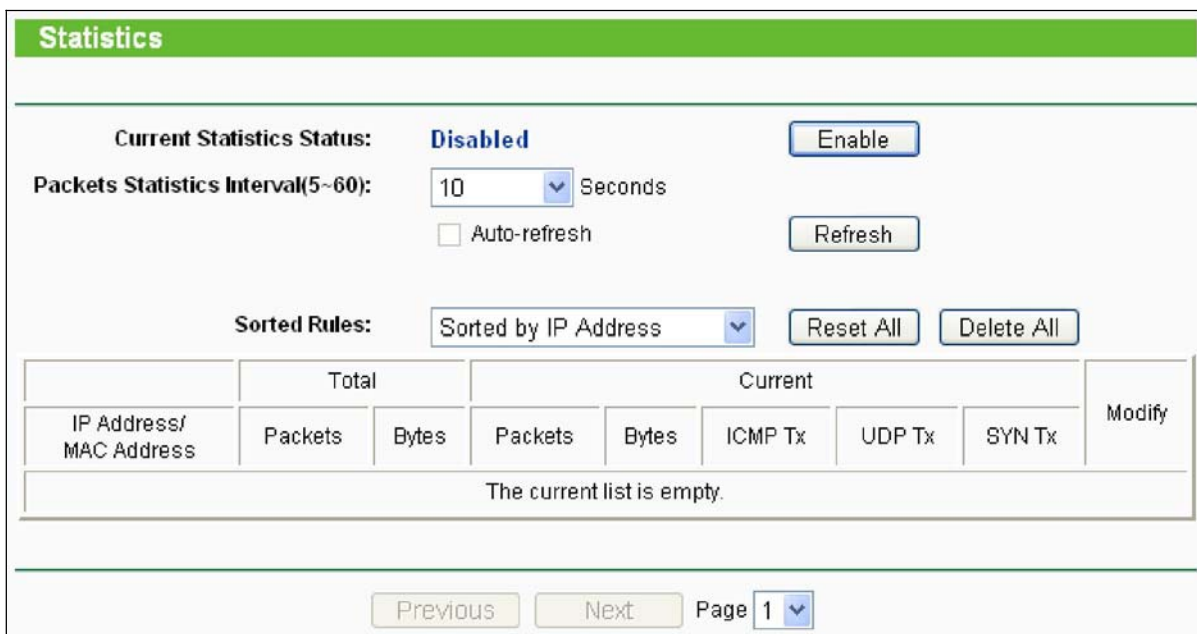


Figure 4-64 Statistics

- **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 ineffective.
- **Packets Statistics Interval** - The default value is 10. Select a value between 5 and 60 seconds from the pull-down list. The Packets Statistic interval indicates the time section of the packets statistic.
- **Sorted Rules** - Here displays sort as desired

Statistics Table:

IP Address		The IP Address displayed with statistics
Total	Packets	The total amount of packets received and transmitted by the router.
	Bytes	The total amount of bytes received and transmitted by the router.
Current	Packets	The total amount of packets received and transmitted in the last Packets Statistic interval seconds.
	Bytes	The total amount of bytes received and transmitted in the last Packets Statistic interval seconds.
	ICMP Tx	The total amount of the ICMP packets transmitted to WAN in the last Packets Statistic interval seconds.
	UDP Tx	The total amount of the UDP packets transmitted to WAN in the last Packets Statistic interval seconds.
	TCP SYN Tx	The total amount of the TCP SYN packets transmitted to WAN in the last Packets Statistic interval seconds.

Click the **Save** button to save the **Packets Statistic interval** value.

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

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

Chapter 5 AP Operation Mode

This Chapter describes how to configure some advanced settings for your Access Point through the web-based management page in AP operation mode.

5.1 Login

After your successful login, you can configure and manage the Access Point. There are eight main menus on the left of the Web-based management page. Submenus will be available after you click one of the main menus. The eight main menus are: **Status**, **Quick Setup**, **Operation Mode**, **Network**, **Wireless**, **DHCP**, **Wireless Settings**, **SNMP** and **System Tools**. On the right of the Web-based management page, there are the detailed explanations and instructions for the corresponding page. To apply any settings you have altered on the page, please click **Save**.

The detailed explanations for each Web page key's function are listed below.

5.2 Status

Selecting **Status** will enable you to view the AP's current status and configuration, all of which is read-only



Figure 5-1

- **Wired** - This field displays the current settings or information for the Network, including the **MAC address**, **IP address** and **Subnet Mask**.
- **Wireless** - This field displays basic information or status for wireless function, including **Operating Mode**, **Signal**, **SSID**, **Channel**, **Mode**, and **MAC Address**.
- **Traffic Statistics** - This field displays the AP's traffic statistics.
- **System Up Time** - The time of the AP running from it's powered on or reset.

5.3 Quick Setup

Please refer to Section [3.2: "Quick Setup"](#).

5.4 Operation Mode

The AP supports three operation modes, **AP Client Router**, **AP Router** and **AP**. Please select one you want. Click **Save** to save your choice. Figure 5-2.



<input type="radio"/>	AP Client Router:	WISP Client Router
<input type="radio"/>	AP Router:	Wireless Broadband Router
<input checked="" type="radio"/>	AP:	Access Point

Save

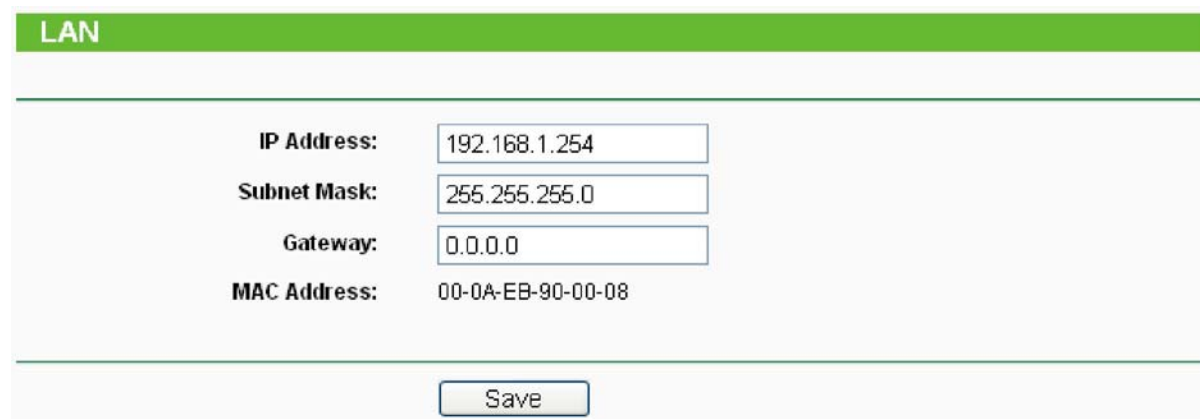
Figure 5-2 Operation Mode

- **AP Client Router:** In this mode, the device enables users to access Internet from WISP. The LAN port devices share the same IP from WISP through Wireless port. While connecting to WISP, the Wireless port works as a WAN port at AP Client Router mode. The Ethernet port acts as a LAN port.
- **AP Router** - In this mode, the device can establish a long distance connection between two LANs in different segments. Because the data transmit between different segments need Router's IP Address Translation.
- **AP** - In this mode, the device can establish a long distance connection between two LANs in same segments.

5.5 Network

The **Network** option allows you to customize your local network manually by changing the default settings of the AP.

Selecting **Network** will enable you to configure the IP parameters of Network on this page.



IP Address:	192.168.1.254
Subnet Mask:	255.255.255.0
Gateway:	0.0.0.0
MAC Address:	00-0A-EB-90-00-08

Save

Figure 5-3 Network

- **IP Address** - Enter the IP address of your AP in dotted-decimal notation (factory default: 192.168.1.254).
- **Subnet Mask** - An address code that determines the size of the network. Normally use 255.255.255.0 as the subnet mask.

- **Gateway** - The gateway should be in the same subnet as your IP address.
- **MAC Address** - the physical address of the AP, as seen from the LAN. This value can't be changed.

Note:

- 1) If you change the IP Address, you must use the new IP Address to log in the AP.
- 2) If the new LAN IP Address you set is not in the same subnet, the IP Address pool in the DHCP sever will not take effect unless they are re-configured.
- 3) The device will reboot automatically after clicking **Save**.

5.6 Wireless

The **Wireless** option, improving functionality and performance for wireless network, can help you make the AP an ideal solution for your wireless network.

Here you can create a wireless local area network just through a few settings. Basic Settings is used for the configuration of some basic parameters of the AP. Wireless Mode allows you to select the mode that AP works on. Security Settings provides three different security types to secure your data and thus provide greater security for your wireless network. MAC filtering allows you to control the access of wireless stations to the AP. Wireless Statistics shows you the statistics of current connected Wireless stations. Distance Setting is used to adjust the wireless range in outdoor conditions. Antenna Alignment shows how remote AP's signal strength changes while changes the antenna's direction. Throughput Monitor helps to watch wireless throughput information Wireless statistics enables you to get detailed information about the current connected wireless stations.

There are eight submenus under the Wireless menu (shown in Figure 5-4): **Basic Settings**, **Wireless Mode**, **Security Settings**, **MAC Filtering**, **Wireless Statistics**, **Distance Setting**, **Antenna Alignment** and **Throughput Monitor**. Click any of them, and you will be able to configure the corresponding function. The detailed explanations for each submenu are provided below.

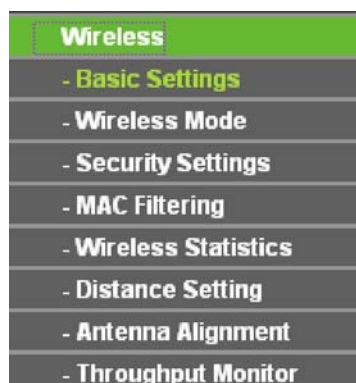


Figure 5-4 Wireless menu

5.6.1 Basic Settings

Selecting **Wireless > Basic Settings** will enable you to configure the basic settings for your wireless network on the screen below (Figure 5-5).

Figure 5-5 Wireless Settings in AP mode

- **SSID** (Set Service Identifier) - Identifies your wireless network name. Create a name up to 32 characters and make sure all wireless points in the wireless network with the same SSID. 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. For example, *TEST* is NOT the same as *test*.
- **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 field. If your country or region is not listed, please contact your local government agency for assistance.

When you select your local region from the pull-down list, click the **Save** button, then the Note Dialog appears. Click **OK**.



Note Dialog

Note:

Limited by local law regulations, version for North America does not have region selection option.

- **Channel** - Determines the operating frequency to be used. It is not necessary to change the wireless channel unless you notice interference problems with another nearby access point.
- **Mode** - Select the desired wireless mode. The options are:
 - **54Mbps (802.11g)** - Both 802.11g and 802.11b wireless stations can connect to the router.
 - **11Mbps (802.11b)** - Only 802.11b wireless stations can connect to the router.

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

Note:

The device will reboot automatically after you click the **Save** button.

5.6.2 Wireless Mode

Selecting **Wireless > Wireless Mode** will enable you to configure the wireless mode for your device.

- **Access Point** – Pair with another TL-WA5210G in Client Router or Client mode to establish a long distance point to point connection.
 - **Enable SSID Broadcast** - If you select the **Enable SSID Broadcast** checkbox, the Wireless AP will broadcast its name (SSID) on the air.
- **Client** - In **Client** mode, AP will act as a wireless station to enable wired host(s) to access wireless AP. Pair with another TL-WA5210G in AP or AP Router mode to establish a long distance point to point connection.
 - **Enable WDS** - The AP client can connect to AP with WDS enabled or disabled. If WDS is enabled, all traffic from wired networks will be forwarded in the format of WDS frames consist of four address fields. If WDS is disabled, three address frames are used. If your AP supports WDS well, please select the option.
 - **SSID** - Enter the SSID of AP that you want to access. If you select the radio before **SSID**, the AP client will connect to AP according SSID.
 - **MAC of AP** - Enter the MAC address of AP that you want to access. If you select the radio before **MAC of AP**, the AP client will connect to AP according MAC address.
- **Repeater** - The **Repeater** mode is the AP with its own BSS and with WDS enabled that relays data, to which it is associated. The wireless repeater relays signal for greater wireless range. Please input the MAC address of root AP in the field of **MAC of AP**.
- **Universal Repeater** - The **Universal Repeater** mode is the AP with its own BSS and with WDS disabled that relays data to a root AP, to which it is associated. The wireless repeater relays signal between its stations and the root AP for greater wireless range. Please input the MAC address of root AP in the field of **MAC of AP**.

Note:

If the available AP can't support with WDS, you may select [Client mode without WDS](#) or [Universal Repeater mode](#) to associate with the AP.

Here is an example of how to configure wireless repeater. Please do the following:

1. Configure the Operating Mode of the TL-WA5210G.
 - Configure AP1 on LAN Segment 1 in Access Point mode.
 - Configure AP2 in Repeater mode with the MAC address of its root AP (AP1).
2. Verify the wireless security parameters for all access points, if any.
3. Verify connectivity across the LANs. A computer on any LAN segment should be able to connect to the Internet or share files and printers with any other PCs or servers connected to any of the two WLAN segments.

Note:

You can extend this repeating by adding up to 2 additional TL-WA5210G configured in repeater mode. However, since Repeater configurations communicate in half-duplex mode, the bandwidth decreases as you add Repeaters to the network. Also, you can extend the range of the wireless network with wireless antenna accessories.

- **Bridge (Point to Point)** - This mode bridges the AP and another AP also in bridge mode to connect two wired LANs. Please input the MAC address of the other AP in the field of **MAC of AP**. AP function can startup also.
 - **With AP mode:** If you select this option, you AP will also support AP mode when it is in Bridge (Point to Point) mode.

Here is an example of how to configure Point-to-Point Bridge. Please do the following:

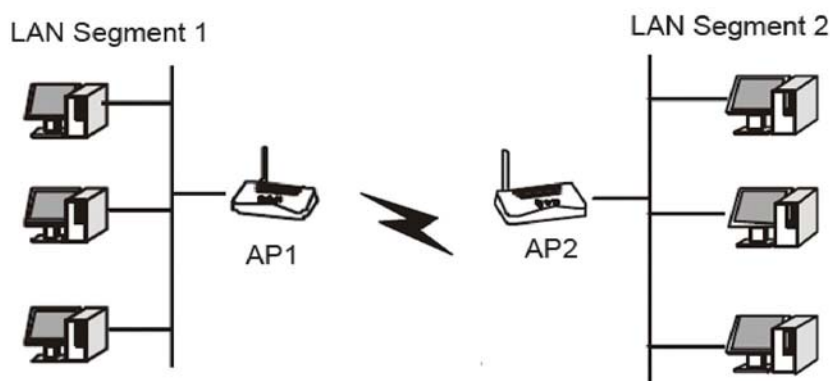


Figure 5-6 Point to Point Bridge

1. Configure the TL-WA5210G (AP1) on LAN Segment 1 in Point-to-Point Bridge mode.
2. Configure the TL-WA5210G (AP2) on LAN Segment 2 in Point-to-Point Bridge mode. AP1 must have AP2's MAC address in its MAC Address field and AP2 must have AP1's MAC address in its MAC Address field.
3. Configure and verify the following parameters for both access points:
 - Both use the same Channel and security settings if security is in use.

Verify connectivity across the LAN 1 and LAN 2. A computer on either LAN segment should be able to connect to the Internet or share files and printers of any other PCs or servers connected to LAN Segment 1 or LAN Segment 2.

Note:

- 1) To apply any settings you have altered on the page, please click the **Save** button, and wait the AP reboot automatically.

Click **Survey** will show the site list of scanning result shown as Figure 5-7.

AP List						
AP Count: 53						
ID	BSSID	SSID	Signal	Channel	Security	Choose
1	00-21-27-4B-23-78	TP-LINK_4B2378	28 dB	11	OFF	Connect
2	00-1D-0F-98-2B-08	TP-LINK	25 dB	11	ON	Connect
3	00-08-01-00-00-80	AKING	18 dB	11	OFF	Connect
<input type="button" value="Refresh"/>						

Figure 5-7 AP List

- **BSSID** -The BSSID of the AP, usually also the MAC address of the AP.

- **SSID** -The SSID of the AP.
- **Signal** -The signal received from the AP.
- **Channel** -The channel the AP works in.
- **Security** -The AP communicates in privacy.
- **Choose** - Click to connect to the corresponding AP.

5.6.3 Security Settings

Selecting **Wireless > Security Settings** will enable you to configure the security of the wireless network for your device as shown in Figure 5-8.

Wireless Security

Disable Security

WEP

Type:

WEP Key Format:

Key Selected	WEP Key	Key Type
Key 1: <input checked="" type="radio"/>	<input type="text"/>	Disabled <input type="text" value="Disabled"/>
Key 2: <input type="radio"/>	<input type="text"/>	Disabled <input type="text" value="Disabled"/>
Key 3: <input type="radio"/>	<input type="text"/>	Disabled <input type="text" value="Disabled"/>
Key 4: <input type="radio"/>	<input type="text"/>	Disabled <input type="text" value="Disabled"/>

WPA/WPA2

Version:

Encryption:

Radius Server IP:

Radius Port: (1-65535, 0 stands for default port 1812)

Radius Password:

Group Key Update Period: (in second, minimum is 30, 0 means no update)

WPA-PSK/WPA2-PSK

Version:

Encryption:

PSK Passphrase:

(The Passphrase is between 8 and 63 characters long)

Group Key Update Period: (in second, minimum is 30, 0 means no update, only be valid in AP mode.)

Note: Some security mode can not be selected since it can not be supported by the current wireless mode.

Figure 5-8 Wireless Security

- **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 following options to enable security.
- **WEP** - Select 802.11 WEP security.
 - **Type** - You can select one of following types,
 - 1) **Automatic** - Select **Shared Key** or **Open System** authentication type automatically based on the wireless station's capability and request.
 - 2) **Shared Key** - Select 802.11 Shared Key authentication.
 - 3) **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** - 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.
 - 1) For **64-bit** encryption - You can enter 10 hexadecimal digits (any combination of 0-9, a-f, A-F, zero key is not permitted) or 5 ASCII characters.
 - 2) For **128-bit** encryption - You can enter 26 hexadecimal digits (any combination of 0-9, a-f, A-F, zero key is not permitted) or 13 ASCII characters.
 - 3) For **152-bit** encryption - You can enter 32 hexadecimal digits (any combination of 0-9, a-f, A-F, zero 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** - Select WPA/WPA2 based on Radius Server.
 - **Version** - You can select one of following versions,
 - 1) **Automatic** - Select **WPA** or **WPA2** automatically based on the wireless station's capability and request.
 - 2) **WPA** - Wi-Fi Protected Access.
 - 3) **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 used.
 - **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** - Select WPA based on pre-shared passphrase.
 - **Version** - You can select one of following versions,

- 1) **Automatic** - Select **WPA-PSK** or **WPA2-PSK** automatically based on the wireless station's capability and request.
- 2) **WPA-PSK** - Pre-shared key of WPA.
- 3) **WPA2-PSK** - Pre-shared key of WPA2.
 - **Encryption** - When you select **WPA-PSK** or **WPA2-PSK** for **Authentication Type** you can select either **Automatic**, or **TKIP** or **AES** as **Encryption**.
 - **PSK Passphrase** - You can enter a passphrase between 8 and 63 characters long.
 - **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.

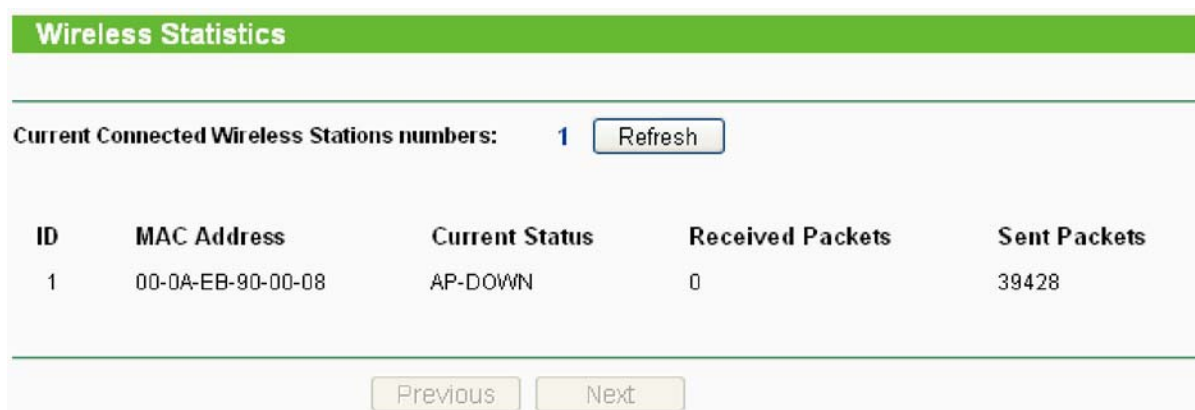
Be sure to click the **Save** button to save your settings on this page.

 **Note:**

The device will reboot automatically after you click the **Save** button.

5.6.4 Wireless Statistics

Selecting **Wireless > Wireless Statistics** will allow you to see the wireless transmission information in the following screen shown in Figure 5-9.



ID	MAC Address	Current Status	Received Packets	Sent Packets
1	00-0A-EB-90-00-08	AP-DOWN	0	39428

Figure 5-9 The router attached wireless stations

- **MAC Address** - The connected wireless station's MAC address
- **Current Status** - The connected wireless station's running status, one of STA-AUTH / STA-ASSOC / AP-UP / WPA / WPA-PSK / WPA2/WPA2-PSK/None
- **Received Packets** - Packets received by the station
- **Sent Packets** - Packets sent by the station

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 the previous page.

 **Note:**

This page will be refreshed automatically every 5 seconds.

5.6.5 Distance Setting

Selecting **Wireless > Distance Setting** will allow you to adjust the wireless range in outdoor conditions as shown in Figure 5-10. This is a critical feature required for stabilizing outdoor links.

Enter the distance of your wireless link and the software will optimize the frame ACK timeout value automatically.

Distance Setting

Adjust option: Automatic

Distance: (0-52.6km)

Note: Specify the distance value in kilometers, accurate to the first decimal place. If the distance is set too short or too long, it will result poor connection and throughput performance, it is best to set the value at 110% of the real distance. If the AP is being used in an indoor setting, please use the default setting.

Save

Figure 5-10 Distance Setting

- **Adjust option** - Keep the default setting if the AP is used for indoor environment. Or you can change the distance.
- **Distance:** Specify the distance value in kilometers, accurate to the first decimal place. If the distance is set too short or too long, it will result poor connection and throughput performance, it is best to set the value at 110% of the real distance. If the AP is being used in an indoor setting, please use the default setting.

Click **Save** to keep your settings.

5.6.6 Antenna Alignment

Selecting **Wireless > Antenna Alignment** will allow you to view how remote AP's signal strength changes while changing the antenna's direction.

Antenna Alignment

Remote RSSI: 14 dB

Signal Percent: 47%

RSSI RANGE: 30

Figure 5-11 Antenna Alignment

- **Remote AP 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 bar to set or input the RSSI RANGE value. The slider bar allows the range of the meter to be either increased or reduced. If the range is reduced, the color change will be more sensitive to signal fluctuations. The slider bar actually changes an offset of the maximum indicator value scale.

Note:

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

5.6.7 Throughput Monitor

Selecting **Wireless > Throughput Monitor** will help to watch wireless throughput information in the following screen shown in Figure 5-12.

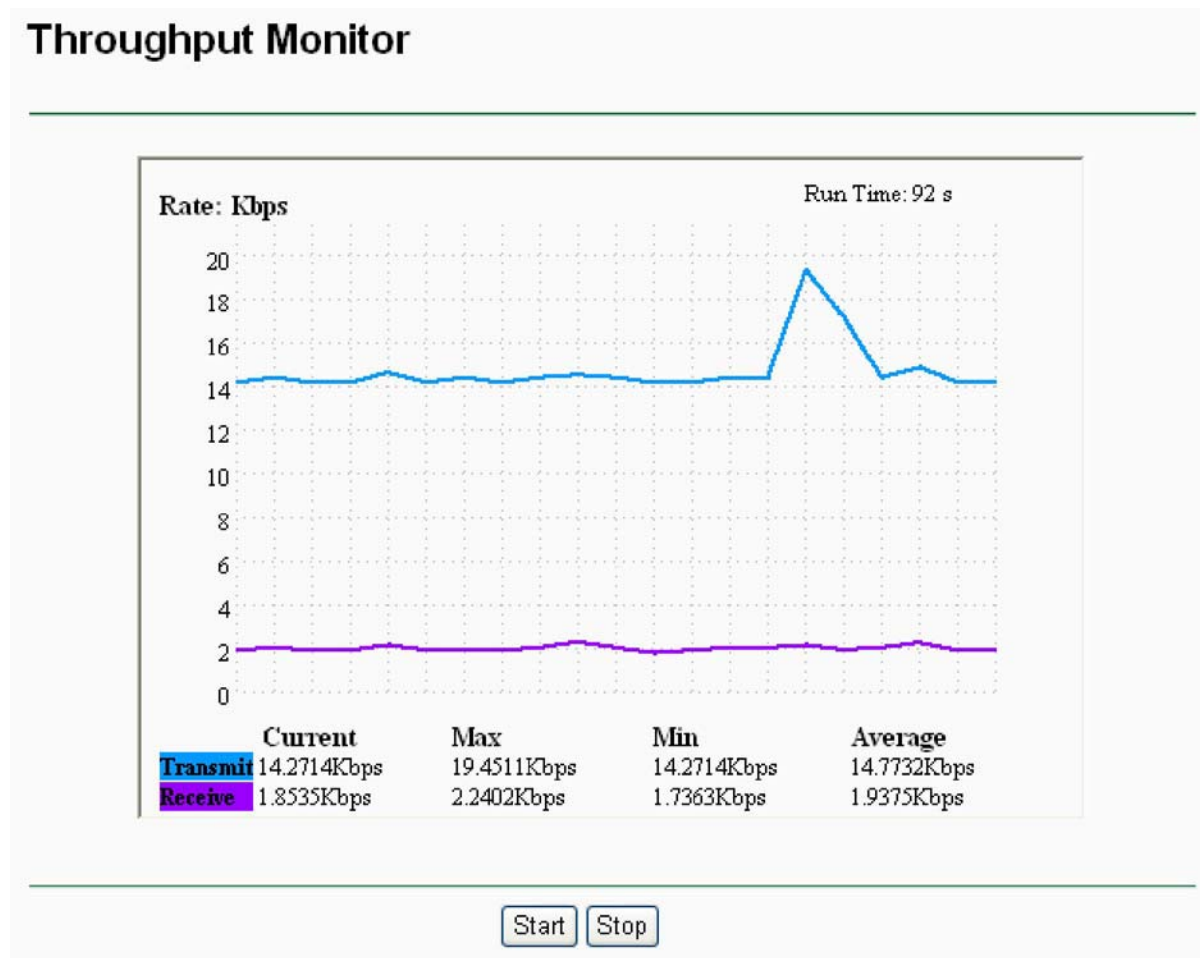


Figure 5-12 Wireless Throughput

- **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 DHCP

DHCP stands for Dynamic Host Configuration Protocol. The DHCP Server will automatically assign dynamic IP addresses to the computers on the network. This protocol simplifies network management and allows new wireless devices to receive IP addresses automatically without the need to manually assign new IP addresses.

There are three submenus under the DHCP menu (shown as Figure 5-13): **DHCP Settings**, **DHCP Clients List** and **Address Reservation**. Clicking any of them will enable you to configure the corresponding function. The detailed explanations for each submenu are provided below.

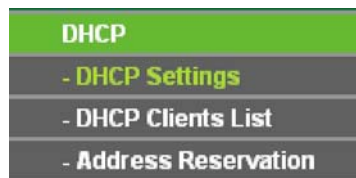


Figure 5-13 The DHCP menu

5.7.1 DHCP Settings

Selecting **DHCP > DHCP Settings** will enable you to set up the AP as a DHCP (Dynamic Host Configuration Protocol) server, which provides the TCP/IP configuration for all the PCs that are connected to the system on the LAN. The DHCP Server can be configured on the page (shown as Figure 5-14).

Figure 5-14 DHCP Settings

- **DHCP Server** - Selecting the radio button before **Disable/Enable** will disable/enable the DHCP server on your AP. The default setting is **Disable**. If you disable the Server, you must have another DHCP server within your network or else you must manually configure the computer.
- **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** - Enter the amount of time for the PC to connect to the AP with its current assigned dynamic IP address. The time is measured in minutes. After the time is up, the PC will be automatically assigned a new dynamic IP address. The range of the time is 1 ~ 2880 minutes. The default value is 120 minutes.
- **Default Gateway (optional)** - Enter the IP address of the gateway for your LAN. The factory default setting is 0.0.0.0.
- **Default Domain (optional)** - Enter the domain name of the your DHCP server. You can leave the field blank.
- **Primary DNS (optional)** - Enter the DNS IP address provided by your ISP. Consult your ISP if you don't know the DNS value. The factory default setting is 0.0.0.0.

- **Secondary DNS (optional)** - Enter the IP address of another DNS server if your ISP provides two DNS servers. The factory default setting is 0.0.0.0.

Click **Save** to save the changes.

Note:

- 1) When the device is working on Dynamic IP mode, the DHCP Server function will be disabled.
- 2) 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 not take effect until the device reboots.

5.7.2 DHCP Clients List

Selecting **DHCP > DHCP Clients List** will enable you to view the Client Name, MAC Address, Assigned IP and Lease Time for each DHCP Client attached to the device (Figure 5-15).

DHCP Clients List				
ID	Client Name	MAC Address	Assigned IP	Lease Time
1	microsoft	00-19-66-CB-45-66	192.168.1.100	01:56:59

Figure 5-15 DHCP Clients List

- **ID** - Here displays the index of the DHCP client.
- **Client Name** - Here displays the name of the DHCP client.
- **MAC Address** - Here displays the MAC address of the DHCP client.
- **Assigned IP** - Here displays the IP address that the AP has allocated to the DHCP client.
- **Lease Time** - Here displays the time of the DHCP client leased. Before the time is up, DHCP client will request to renew the lease automatically.

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

5.7.3 Address Reservation

Selecting **DHCP > Address Reservation** will enable you to specify a reserved IP address for a PC on the LAN, so the PC will always obtain the same IP address each time when it accesses the AP. Reserved IP addresses should be assigned to servers that require permanent IP settings. The screen below is used for address reservation (shown in Figure 5-16).

Address Reservation				
ID	MAC Address	Reserved IP Address	Status	Modify
<input type="button" value="Add New..."/> <input type="button" value="Enable All"/> <input type="button" value="Disable All"/> <input type="button" value="Delete All"/>				
<input type="button" value="Previous"/> <input type="button" value="Next"/>				

Figure 5-16 Address Reservation

- **MAC Address** - Here displays the MAC address of the PC for which you want to reserve an IP address.
- **Reserved IP Address** - Here displays the IP address that the AP is reserved.
- **Status** - Here shows whether the entry is enabled or not
- **Modify** - To modify or delete an existing entry.

To Reserve IP addresses:

1. Click the **Add New button** in the page of **Address Reservation**, the following page (Figure 5-17) will display.
2. Enter the MAC address (the format for the MAC Address is XX-XX-XX-XX-XX-XX) and IP address in dotted-decimal notation of the computer you want to add.
3. Click the **Save** button after finish configuring.



Add or Modify an Address Reservation Entry

MAC Address: 00-0A-EB-00-07-5F

Reserved IP Address: 192.168.1.23

Status: Enabled

Save Back

Figure 5-17 Add or Modify an Address Reservation Entry

To modify A Reserved IP address:

1. Select the reserved address entry to your needs and click **Modify**. If you wish to delete the entry, click **Delete**.
2. Click **Save** to keep your changes.

To delete all Reserved IP addresses:

1. Click **Clear All**.

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

Note:

The changes won't take effect until the device reboots.

5.8 Wireless settings

Selecting **Wireless Settings** will allow you to do some advanced settings for the device in the following screen shown in Figure 5-18.

Wireless Advanced Settings

Enable WMM

Enable AP Isolation

Disable short preamble

RTS Threshold: (1-2346)

Fragmentation Threshold: (256-2346)

Beacon Interval: (20-1000ms)

Power: Obey Regulatory Power

Antenna Settings:

LED1 LED2 LED3 LED4

Signal LED Thresholds: (0-99dB)

Figure 5-18 Wireless settings

- **Enable WMM** - WMM function can guarantee the packets with high- priority messages being transmitted preferentially. It is strongly recommended enabled.
- **Enable AP Isolation** - Isolate all connected wireless stations so that wireless stations can not access each other through WLAN. This option is available only for AP mode.
- **Disable short preamble** - Disable short preamble and use long preamble only. 802.11b mode supports only long preamble and this parameter will be ignored. It is recommended that you do not change these settings.
- **RTS threshold** - RTS/CTS Threshold, the packet size that is used to determine if RTS/CTS should be sent.
- **Fragmentation Threshold** - The maximum packet size used for fragmentation.
- **Beacon Interval** - The interval time between two successive beacons.
- **Power** - The transmit power of the access point. The checkbox determines the transmit power that whether it obeys regulatory power or not. Un-checking the **Obey Regulatory Power** option may cause interference to other devices and violate the applicable law.
- **Antenna Settings** -The polarization of an antenna.
- **Signal LED Thresholds** - The RSSI thresholds of the signal LEDs.

5.9 SNMP

SNMP will allow the network management station to retrieve statistics and status from the SNMP agent in this device. Simple Network Management Protocol (SNMP) is a popular network monitoring and management protocol, used to refer to a collection of specifications for network management that include the protocol itself. To use this function, select Enable and enter the following parameters in Figure 5-19.



Figure 5-19 SNMP Settings

5.9.1 Community Setting

Selecting **SNMP > Community Setting** will allow you to configure the SNMP community as shown in Figure 5-20, which is helpful for managing the access authority.

Community List				
Num	Community	Access Mode	Status	Status
1	public	Read Only	Disable	Modify
2	public	Read Only	Disable	Modify
3	public	Read Only	Disable	Modify
4	public	Read Only	Disable	Modify

Figure 5-20 Community Setting

- **Num** - Displays the entry number of the community.
- **Community** - Defines the password used to authenticate the management station to the device.
- **Access Mode** - This field allows you to specify the authority of the community. Read Only means the community is only permitted to read the device configuration. Read&Write means the community has the authority to read and change the device configuration.
- **Status** - This field allows you to enable/disable the corresponding entry.
- **Modify** - This field allows you to modify an entry.

To modify a community setting entry:

1. Find the desired entry in the table.
2. Click **Modify** as desired on the **Modify** column.
3. Modify the contact of **community**
4. Select the **Read Only** or **Read&Write** option in the **Access Mode** pull-down list.
5. Select the **Enabled** option in the **Status** pull-down list.
6. Click the **Save** button.

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

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

5.9.2 SNMP System Setting

Selecting **SNMP > SNMP Setting** will allow you to configure some parameters for System (iso.org.dod.internet.mgmt.mib-2.system) as shown in Figure 5-21.



The image shows a web form titled "SNMP System Settings" with a green header. Below the header, there are three input fields: "System Contact:", "System Name:", and "System Location:". Each field is followed by a text input box. At the bottom of the form, there is a "Save" button.

Figure 5-21 SNMP System Setting

- **System Contact** - The textual identification of the contact person for this managed node, together with information on how to contact this person.
- **System Name** - An administratively-assigned name for this managed node. By convention, this is the node's fully-qualified domain name.
- **System Location** - The physical location of this node.

Click the **Save** button to save configuration in current page.

5.10 System Tools

System Tools option helps you to optimize the configuration of your device. You can upgrade the AP to the latest version of firmware as well as backup or restore the AP's configuration files. Ping Watch Dog can help to continuously monitor a particular connection to a remote host. Speed Test helps to test the connection speed to and from any reachable IP address on current network, especially when we are building wireless network between devices which are far away from each other. It's suggested that you change the default password to a more secure one because it controls access to the device's web-based management page. Besides, you can find out what happened to the system in System Log.

There are eight submenus under the **System Tools** menu (shown as Figure 5-22): **Firmware**, **Factory Defaults**, **Backup & Restore**, **Ping Watch Dog**, **Speed Test**, **Reboot**, **Password** and **Syslog**. Clicking any of them will enable you to configure the corresponding function. The detailed explanations for each submenu are provided below.



Figure 5-22 The System Tools menu

5.10.1 Firmware

Selecting **System Tools > Firmware** allows you to upgrade the latest version of firmware for the device on the screen shown in Figure 5-23.



Figure 5-23 Firmware Upgrade

New firmware versions are posted at <http://www.tp-link.com> and can be downloaded for free. There is no need to upgrade the firmware unless the new firmware has a new feature you want to use. However, when experiencing problems caused by the AP itself, you can try to upgrade the firmware.

 **Note:**

Before upgrading the AP's firmware, you should write down some of your customized settings to avoid losing important configuration settings of AP.

To upgrade the AP's firmware, please take the following steps:

1. Download a more recent firmware upgrade file from the TP-LINK website (<http://www.tp-link.com>).
 2. Click **Browse** to view the folders and select the downloaded file.
 3. Click **Upgrade**.
- **Firmware Version** - Displays the current firmware version.
 - **Hardware Version** - Displays the current hardware version. The upgrade file must accord with the current hardware version.

 **Note:**

Do not turn off the AP or press the Reset button while the firmware is being upgraded. The AP will reboot after the Upgrading has been finished.

5.10.2 Factory Defaults

Selecting **System Tools > Factory Default** allows you to restore the factory default settings for the device on the screen shown in Figure 5-24.

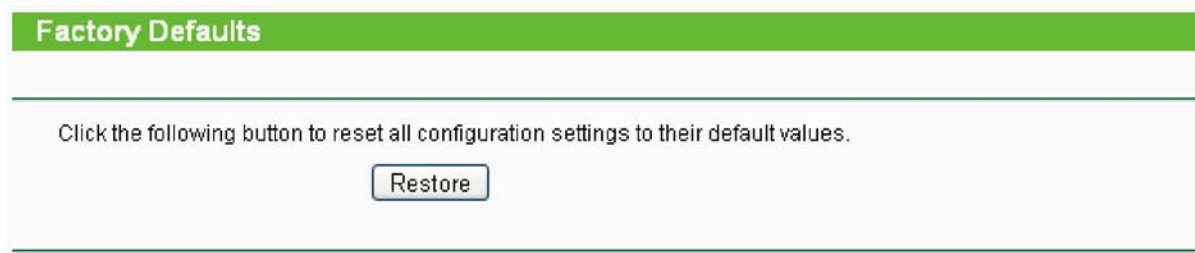


Figure 5-24 Restore Factory Default

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

- The default **User Name**: admin
- The default **Password**: admin
- The default **IP Address**: 192.168.1.254
- The default **Subnet Mask**: 255.255.255.0

 **Note:**

All settings you have saved will be lost when the default settings are restored.

5.10.3 Backup & Restore

Selecting **System Tools > Backup & Restore** allows you to save all configuration settings to your local computer as a file or restore the device's configuration on the screen shown in Figure 5-25.



Figure 5-25 Save or Restore the Configuration

Click **Backup** to save a backup configuration file to your local computer.

To restore the AP's configuration, please take the following steps:

- Click **Browse** to find the location of configuration file which you want to restore.
- Click **Restore** to update the configuration with the file whose path is the one you have input or selected in the blank.

 **Note:**

- 1) The current configuration will be covered by the uploading configuration file.
- 2) Wrong process will lead the device unmanaged.
- 3) The restoring process will last for 20 seconds and the AP will restart automatically. Do not power off the device during the process to avoid any damage.

5.10.4 Ping Watch Dog

Selecting **System Tools > Ping Watch Dog** allows you to continuously monitor the particular connection between the device to a remote host. It makes this device continuously ping a user defined IP address (it can be the internet gateway for example). If it is unable to ping under the user defined constraints, this device will automatically reboot.

Ping Watch Dog Utility

Enable:

IP Address:

Interval: seconds

Delay: seconds

Fail Count:

Figure 5-26 Ping Watch Dog Utility

- **Enable** - Turn on/off Ping Watch Dog.
- **IP Address** - The IP address of the target host where the Ping Watch Dog Utility is sending ping packets.
- **Interval** - Time interval between two ping packets which are sent out continuously.
- **Delay** - Time delay before first ping packet is sent out when the device is restarted.
- **Fail Count** - Upper limit of the ping packet the device can drop continuously. If this value is overrun, the device will restart automatically.

Be sure to click the **Submit** button to make your settings in operation.

5.10.5 Speed Test

Selecting **System > Speed Test** allows you to test the connection speed to and from any reachable IP address on current network on the page as shown in Figure 5-27. The speed test is especially used when you are building wireless network between devices which are far away from each other. It should be used for the preliminary throughput estimation between two network devices. The estimation is rough. You can input the remote device's administrator Username and Password under **Advance options** to get a precise estimation if the remote, too.

Simple Network Speed Test Utility

Destination IP:

User:

Password:

Advanced options:

Direction:

transmit ▼

Duration:

10

seconds

Data amount:

bytes

Test Results

Tx:

N/A

Rx:

N/A

Figure 5-27 Speed Test

- **Destination IP** - The Remote device's IP address.
- **User** - Administrator password of the remote device. It should be filled correctly if you want to get a precise estimation. Otherwise, keep it clean.
- **Advanced options** - This is a switch to show advanced test options which are used only for precise estimation.

Note:

If either User or Password is incorrect, we will take a basic test instead. In other words, none of the advance options you set will take effect.

- **Direction** - There are 3 options available for the traffic direction while estimating the throughput.
 - **transmit** - Estimate the outgoing throughput (TX).
 - **receive** - Estimate the ingoing throughput (RX).
 - **both** - Estimate the incoming (RX) first and then the outgoing (TX) afterwards.
- **Duration** - The value you specify here indicate how much time the test should last.
- **Data amount** - The maximal data amount to be sent out during the whole test.

Note:

If both Duration and Data amount are specified, the test will stop after any of them is met.

Be sure to click the **Run Test** button to start a new test after you filled enough information. You can also stop a running test by click Stop Test button at any time.

5.10.6 Reboot

Selecting **System Tools > Reboot** allows you to reboot the device on the screen shown in Figure 5-28.



Figure 5-28 Reboot the AP

Click **Reboot** to reboot the AP.

Some settings of the AP will take effect only after rebooting, which include:

- Change LAN IP Address. (System will reboot automatically)
- Upgrade the firmware of the AP (system will reboot automatically).
- Restore the AP's settings to factory default (system will reboot automatically).
- DHCP service function.
- Static address assignment of DHCP server.

5.10.7 Password

Selecting **System Tools > Password** allows you to change the factory default user name and password of the device on the screen shown in Figure 5-29.

Figure 5-29 Password

It is strongly recommended that you change the factory default user name and password of the AP to more secure ones because they control access to the AP's web-based utility. All users who try to access the AP's web-based utility or Quick Setup 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 space. Enter the new Password twice to confirm it.


Click **Save** when finished.

Click **Clear All** to clear all.

5.10.8 Syslog

Selecting **System Tools > System Log** allows you to query the Logs of the device on the screen

shown in Figure 5-30.



The screenshot displays a web interface for viewing system logs. At the top, there is a green header bar with the text "System Log". Below this, a table with two columns, "Index" and "Log Content", contains one entry with index "1" and content "0000:System: The device initialization succeeded.". Underneath the table, there is a line of system information: "H-Ver = WA5210G v1 081640EF : S-Ver = 4.4.0 Build 100120 Rel.52294n" and another line: "L = 192.168.1.254 : M = 255.255.255.0". At the bottom of the interface, there are two buttons: "Refresh" and "Clear All".

Index	Log Content
1	0000:System: The device initialization succeeded.

H-Ver = WA5210G v1 081640EF : S-Ver = 4.4.0 Build 100120 Rel.52294n
L = 192.168.1.254 : M = 255.255.255.0

Refresh Clear All

Figure 5-30 System Log

The AP can keep logs of all traffic. You can query the logs to find out what happened to the AP.

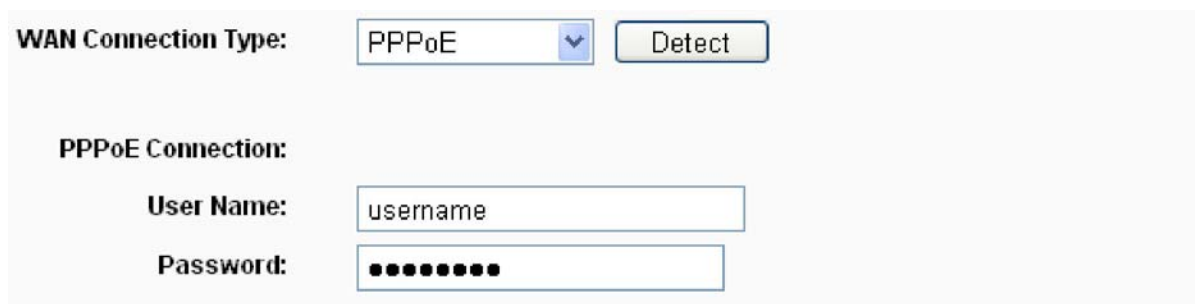
Click **Refresh** to refresh the logs.

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

Appendix A: FAQ

1. How do I configure the router 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 router. The telephone cord plugs into the Line port of the ADSL Modem.
- 3) Login to the router, 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".



WAN Connection Type:

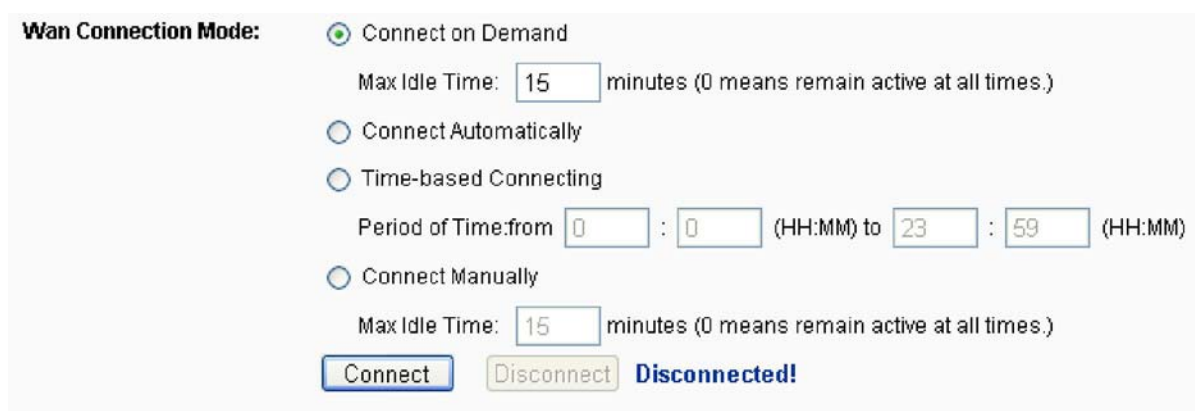
PPPoE Connection:

User Name:

Password:

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 an appropriate number for "Max Idle Time" to avoid wasting paid time. Otherwise, you can select "Auto-connecting" for the Internet connection mode.



Wan Connection Mode:

Connect on Demand
Max Idle Time: minutes (0 means remain active at all times.)

Connect Automatically

Time-based Connecting
Period of Time: from : (HH:MM) to : (HH:MM)

Connect Manually
Max Idle Time: minutes (0 means remain active at all times.)

Disconnected!

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 router following the above steps.

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

- 1) Login to the router, 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

router 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. I want to use Netmeeting, what do I need to do?

- 1) If you start Netmeeting as a sponsor, you don't need to do anything with the router.
- 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 router, 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

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 router, 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.



Figure A-6 DMZ

4. 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 router, you must change the Web management port number to avoid interference.
- 2) To change the Web management port number: Login to the router, 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 router.

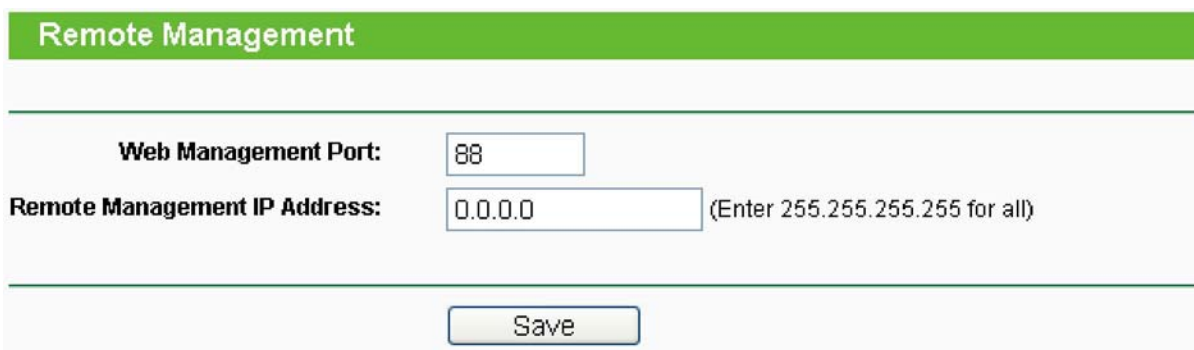


Figure A-7 Remote Management

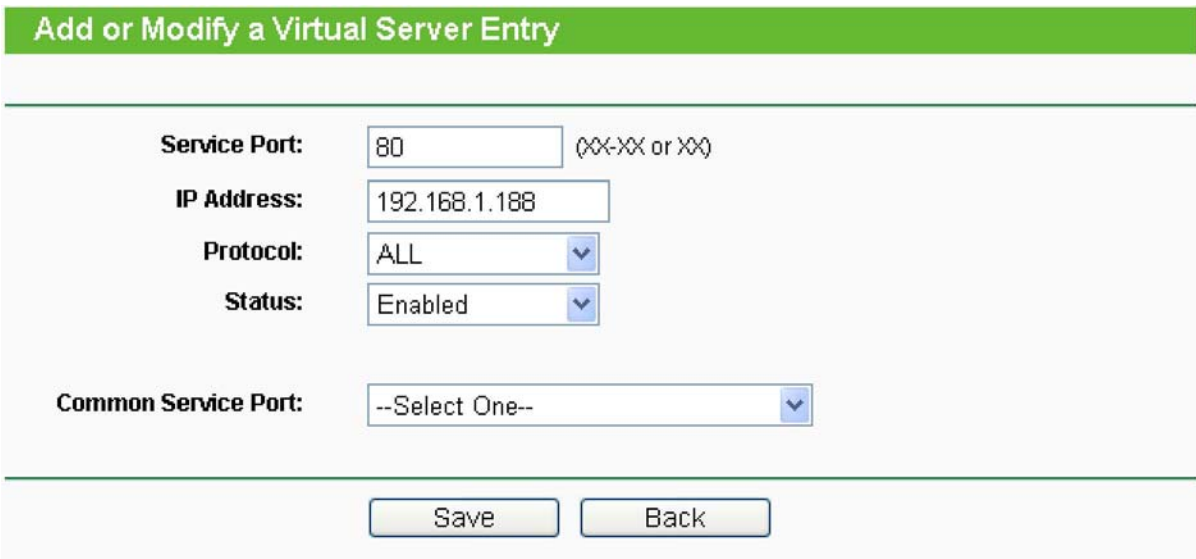
Note:

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

- 3) Login to the router, 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. The wireless stations cannot connect to the router.

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

Appendix B: Configuring the PC

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

1. Configure TCP/IP component

- 1) On the Windows taskbar, click the **Start** button, and then click **Control Panel**.
- 2) Click the **Network and Internet Connections** icon, and then click on the **Network Connections** tab in the appearing window.
- 3) Right click the icon that showed below, select Properties on the prompt page.

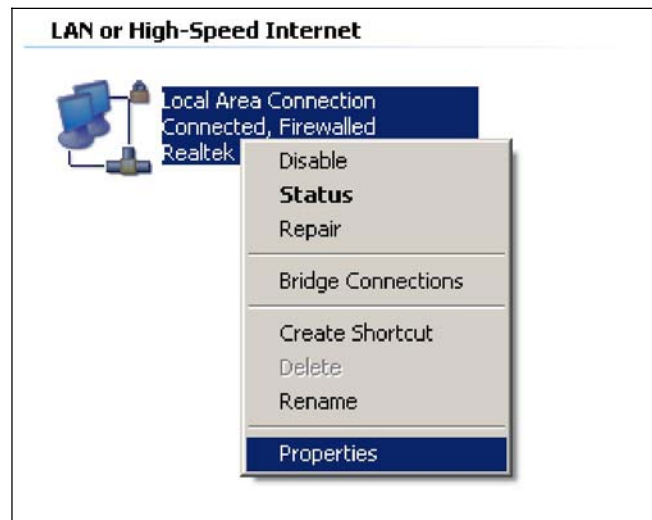


Figure B-1

- 4) In the prompt page that showed below, double click on the **Internet Protocol (TCP/IP)**.

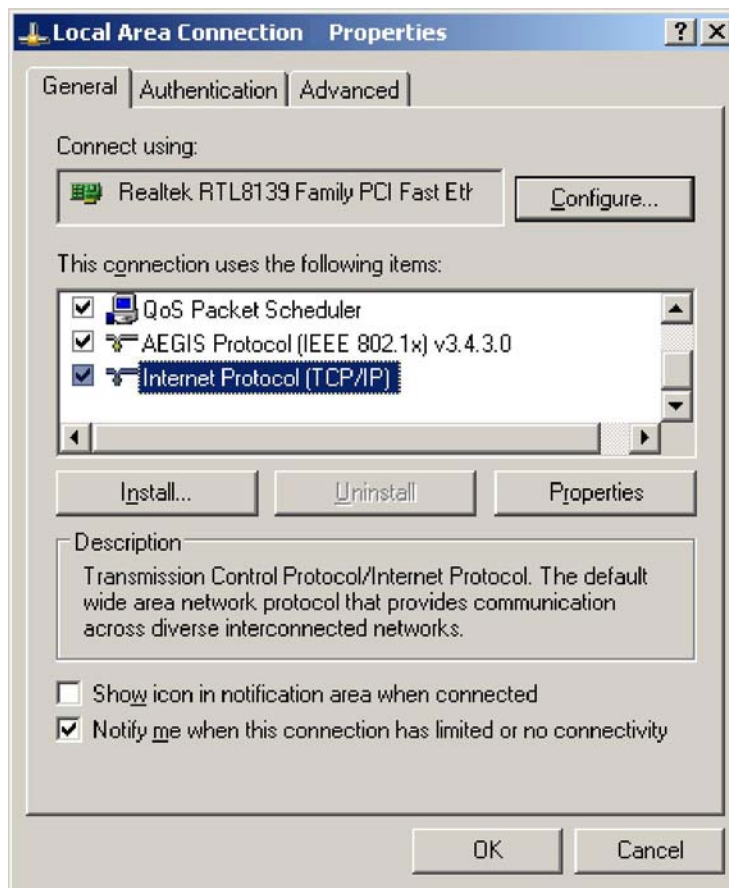


Figure B-2

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

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

➤ **Setting IP address automatically**

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

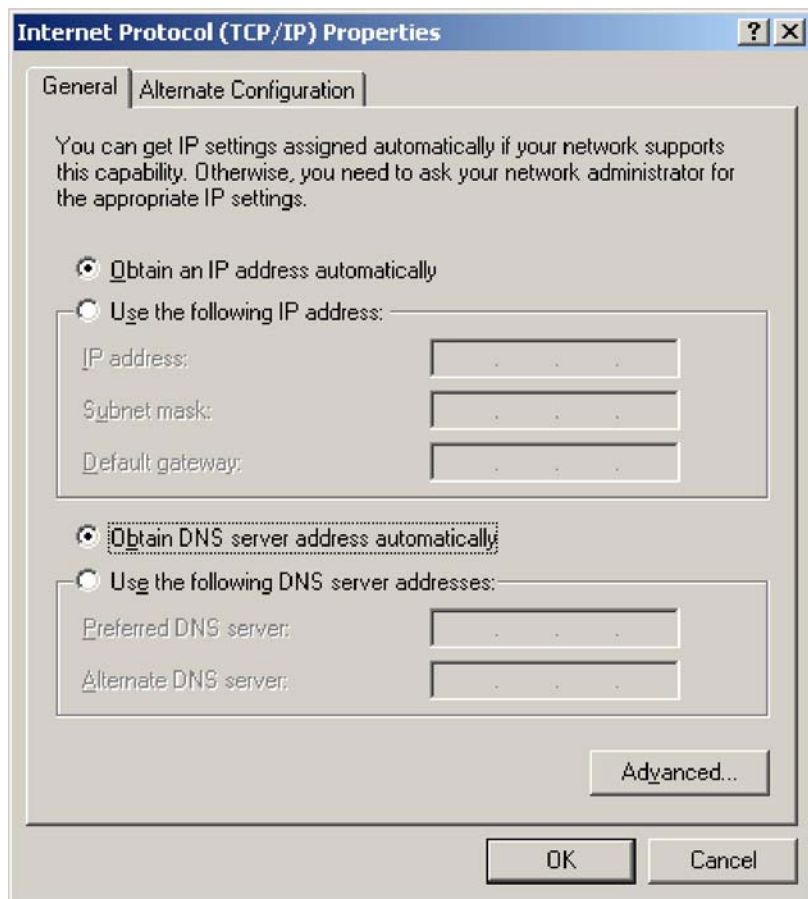


Figure B-3

Note: For Windows 98 OS or before, the PC and router may need to be restarted.

➤ **Setting IP address manually**

1. Select **Use the following IP address** radio button. And the following items available
2. If the router's LAN IP address is 192.168.1.254, specify the **IP address** as 192.168.1.x (x is from 1 to 253), and the **Subnet mask** as 255.255.255.0.
3. Type the router's LAN IP address (the default IP is 192.168.1.254) into the **Default gateway** field.
4. Select **Use the following DNS server addresses**. In the **Preferred DNS Server** field you can enter the same value as the **Default gateway** or type the local DNS server IP address.

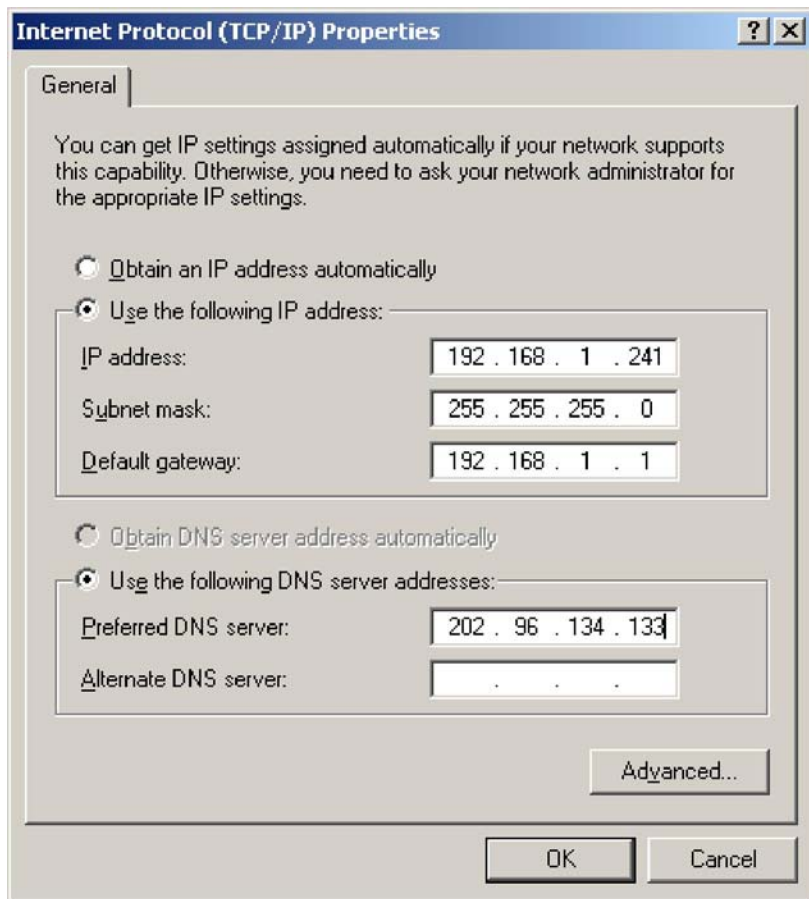


Figure B-4

Now:

Click **OK** to keep your settings.

Appendix C: Specifications

General	
Standards and Protocols	IEEE 802.3, 802.3u, 802.11b and 802.11g, TCP/IP, DHCP
Safety & Emission	FCC, CE
Ports	One 10/100M Auto-Negotiation LAN RJ45 port, supporting passive PoE
Cabling Type	10BASE-T: UTP category 3, 4, 5 cable (maximum 100m) EIA/TIA-568 100Ω STP (maximum 100m) 100BASE-TX: UTP category 5, 5e cable (maximum 100m) EIA/TIA-568 100Ω STP (maximum 100m)
Wireless	
Wireless Data Rates	54/48/36/24/18/12/9/6Mbps or 11/5.5/3/2/1Mbps
Wireless Encryptions	64/128/152-bit WEP, WPA/WPA2, WPA-PSK/WPA2-PSK
Physical and Environment	
Working Temperature	-30°C~70°C
Working Humidity	10% ~ 90% RH, Non-condensing
Storage Temperature	-40°C~70°C(-40°F~158°F)
Storage Humidity	5% ~ 90% RH, Non-condensing

Appendix D: Glossary

- **2x to 3x eXtended Range™ WLAN Transmission Technology** - The WLAN device with 2x to 3x eXtended Range™ WLAN transmission technology make its sensitivity up to 105 dB, which gives users the ability to have robust, longer-range wireless connections. With this range-enhancing technology, a 2x to 3x eXtended Range™ based client and access point can maintain a connection at as much as three times the transmission distance of traditional 802.11b and 802.11g products, for a coverage area that is up to nine times greater. A traditional 802.11b and 802.11g product transmission distance is about 300m, a 2x to 3x eXtended Range™ based client and access point can maintain a connection transmission distance may be up to 830m.
- **802.11b** - The 802.11b standard specifies a wireless networking at 11 Mbps using direct-sequence spread-spectrum (DSSS) technology and operating in the unlicensed radio spectrum at 2.4GHz, and WEP encryption for security. 802.11b networks are also referred to as Wi-Fi networks.
- **802.11g** - specification for wireless networking at 54 Mbps using direct-sequence spread-spectrum (DSSS) technology, using OFDM modulation and operating in the unlicensed radio spectrum at 2.4GHz, and backward compatibility with IEEE 802.11b devices, and WEP encryption for security.
- **DDNS (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.