

NEXXT[®]

S O L U T I O N S



NetGate

WIRELESS-G ACCESS POINT | *User Manual*

Copyright Statement

Nexxt Solutions™ is a registered trademark. Other trademarks or brand names contained herein are the trademarks or registered brand names of their respective owners. Copyright of the whole product as integration, including its accessories and software, belongs to Nexxt Solutions Ltd. No individual or third party is allowed to copy, plagiarize, reproduce, or translate it into other languages, without express consent from Nexxt Solutions, Ltd. All of the photos and product specifications mentioned in this manual are used as reference only. Upgrades of software and hardware may occur, and should there be any changes, Nexxt Solutions shall not be responsible for notifying about any such modifications in advance. If you would like to know more about our products, please visit our website at www.NexxtSolutions.com.

FCC STATEMENT

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

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

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions:

1. This device may not cause harmful interference.
2. This device must accept any interference received, including interference that may cause undesired operation.

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

Note: The manufacturer is not responsible for any radio or TV interference caused by unauthorized modifications to this equipment. Such modifications could void the user's authority to operate the equipment.

FCC RF Radiation Exposure Statement

This equipment complies with FCC RF radiation exposure limits set forth for an uncontrolled environment. This device and its antenna must not be co-located or operating in conjunction with any other antenna or transmitter.

“To comply with FCC RF exposure compliance requirements, this grant is applicable to only Mobile Configurations. The antennas used for this transmitter must be installed to provide a separation distance of at least 30 cm from all persons and must not be co-located or operating in conjunction with any other antenna or transmitter.”

CONTENTS

Chapter 1

Introduction

- 1.1 Product overview
- 1.2 Features

Chapter 2

Device layout

- 2.1 LED definition
- 2.2 Rear panel layout and connectos
- 2.3 System requirements
- 2.4 Environment requirements
- 2.5 Connecting the device

Chapter 3

Quick installation guide

- 3.1 Checking the LEDs
- 3.2 Initial configuration
- 3.3 Quick setup wizard

Chapter 4

AP Client Router & AP Router Operation Mode

- 4.1 Login
- 4.2 Status
- 4.3 Quick setup
- 4.4 Operation mode
- 4.5 Network
 - 4.5.1 LAN
 - 4.5.2 WAN
 - 4.5.3 MAC clone
- 4.6 Wireless
 - 4.6.1 Basic settings
 - 4.6.2 Wireless mode
 - 4.6.3 Security settings
 - 4.6.4 MAC filtering
 - 4.6.5 Wireless statistics
 - 4.6.6 Distance setting
 - 4.6.7 Antenna alignment
 - 4.6.8 Throughput monitor
- 4.7 DHCP
 - 4.7.1 DHCP settings
 - 4.7.2 DHCP clients list
 - 4.7.3 Address reservation
- 4.8 Wireless settings
- 4.9 Forwarding
 - 4.9.1 Virtual servers
 - 4.9.2 Port triggering
 - 4.9.3 DMZ
 - 4.9.4 UPnP
- 4.10 Security
 - 4.10.1 Firewall
 - 4.10.2 IP address filtering
 - 4.10.3 Domain filtering

- 4.10.4 MAC address filtering
- 4.10.5 Remote management
- 4.10.6 Advanced security
- 4.11 Static routing
- 4.12 IP & MAC binding
 - 4.12.1 Binding setting
 - 4.12.2 ARP list
- 4.13 Dynamic DNS
 - 4.13.1 Dyn dns.org DDNS
 - 4.13.2 Oray.net DDNS
 - 4.13.3 Comexe.cn DDNS
- 4.14 SNMP
 - 4.14.1 Community setting
 - 4.14.2 SNMP system setting
- 4.15 System tools
 - 4.15.1 Time
 - 4.15.2 Firmware
 - 4.15.3 Factory defaults
 - 4.15.4 Backup & restore
 - 4.15.5 Ping Watch Dog
 - 4.15.6 Speed test
 - 4.15.7 Reboot
 - 4.15.8 Password
 - 4.15.9 Syslog
 - 4.15.10 Statistics

Appendix A: FAQ

Appendix B: Configuring the PC

Appendix C: Specifications

Appendix D: Glossary

Package Contents

Upon opening the box, make sure that the following items are included:

- High Power Wireless Access Point
- Power adapter
- PSE module
- Mounting kit
- Quick installation guide
- Resource CD

Note:

If any of the listed items is missing, mismatched, damaged or broken, contact your local dealer immediately for replacement.

Chapter 1 Introduction

Thank you for purchasing the AELPLDR4U1 High Power Wireless Outdoor Access Point from Nexxt Solutions.

1.1 Product overview

The 2.4 GHz High Power Wireless Outdoor Access Point is a dedicated Wireless Internet Service Provider Customer-Premises Equipment (WISP CPE) device, providing the functions of a Wireless Access Point (WAP), WISP Client, and a high-gain antenna in one weatherproof device designed for outdoor use. The high power design extends transmission range and delivers a more reliable wireless connection. Equipped with a Power over Ethernet Port known as PoE, this device can be installed in locations where AC power is not readily available. It also features a web-based management utility for easy configuration and hassle-free network connection. Convenient power, LAN and signal strength LED indicators allow users to monitor the status of the network.

Three operation modes are provided in the access point to meet each user's needs.

AP Client Router: choose this mode to enable users to share the internet as a WISP client router.

AP Router: choose this mode to enable users to share internet via ADSL/Cable modem, in a wireless broadband router configuration.

AP: choose this mode to enable wireless devices to access a network using, in an access point configuration.

1.2 Features

- Complies with IEEE 802.11g, IEEE 802.11b, IEEE 802.3, IEEE 802.3u standards.
- Wireless Data transfer rates up to 54Mbps.
- The access point serves as the connection point between wireless and wired networks or as the center point of a stand-alone wireless network.
- High output power for extended range and reliability
- 12 dBi, dual-polarized antenna easily builds up to 9.3-mile wireless.
- Strong 24 dBm output power rating.
- Easy to set up and manage with Ppoe option. Ping Watch Dog feature automatically reboots device when necessary
- Controlled access and WEP, WPA/WPA2, WPA-PSK/WPA2-PSK encryption methods ensure data integrity and privacy.
- 3 year full warranty, with a 2 year extension with online registration
- Supports AP Client Router, AP Router and AP operation mode.
- Supports Client Router Mode for WISP CPE
- Supports passive power over Ethernet.
- Supports Wireless Distribution System (WDS).
- Up to 50Km.
- Supports Antenna Alignment.
- Throughput monitor detailed information about the current wireless data throughput.
- Supports Layer 2 User Isolation.
- Supports Ping Watch Dog.
- Supports link speed test.
- Supports Remote Management

- The device complies with 15.247(c)(1)(iii).
The installer is responsible for ensuring that the system is used exclusively for fixed, point-to-point operations. The instruction manual furnished with the intentional radiator shall contain language in the installation instructions informing the operator and the installer of this responsibility.
- Supports PPPoE, Dynamic IP, Static IP Internet Access.
- Built-in NAT and DHCP server supporting static IP address distributing.
Supports UPnP, Dynamic DNS, Static Routing, VPN Pass-through.
- Supports Virtual Server, Special Application and DMZ host.
- Built-in Firewall supporting IP address filtering, Domain Name filtering, and MAC address filtering.
- Provides WLAN ACL (Access Control List).
- Supports configuration backup/restore and firmware upgrade.
- Supports Web management.

IMPORTANT STATEMENT

This device is equipped with a high gain directional dual-Polarized directional antenna and designed with high output power, only long distance point-to-point using is allowed to comply with FCC Rules. The antenna's beam width is "Horizontal:60° Vertical: 30°", which can not be used for wireless network coverage. Anyone who privately replaces the antenna with an omni-directional antenna for point-to-multiply point using is illegal!

Chapter 2 Device layout

2.1 LED

The AELPLDR4U1 access point features LED indicators, designed to display the connection status and the strength of the wireless signal.

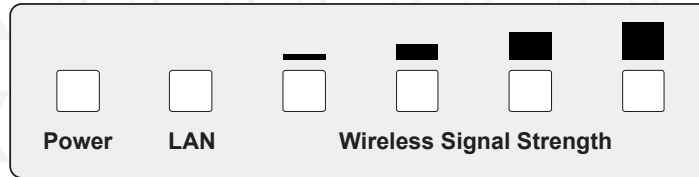


Figure 2-1 Front Panel sketch

Name	Status	Indication	
Power	Off	No power	
	On	Power on	
LAN	Off	There is no device linked to the corresponding port	
	On	There is a device linked to the corresponding port but no activity is being detected	
	Blinking	There is an active device linked to the corresponding port	
Wireless Signal Strength	Off	There is no remote wireless signal	Client or Repeater mode
	On	Indicates the wireless signal strength of a remote AP	

Table 2-1

Note:

Wireless Signal Strength Indicators:

- In AP or Bridge mode, all the four LEDs will light up.
- In Client or Repeater mode, the corresponding LED(s) will light up when the RSSI value (wireless signal strength value) reaches the RSSI threshold. The value of RSSI threshold can be set on the Wireless Advanced Settings page, as shown in Figure 4-26. For example, if the RSSI value you set is 30, while RSSI threshold of the four LEDs are 15, 25, 35, 45 respectively, then the LEDs having RSSI thresholds of 15 and 25 will light up.

2.2 Rear panel layout and connectors

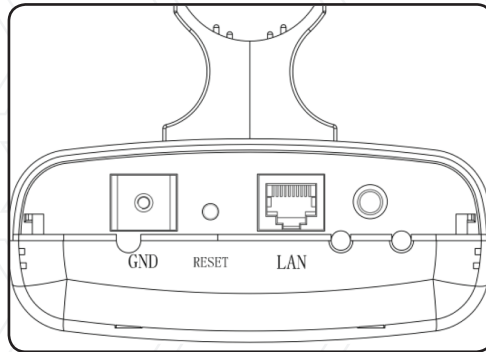



Figure 2-2 Rear panel sketch

- **Ground**
- **RESET button:** use it to reset device to its factory default values
- **LAN:** this port is used to connect to the PoE port of the PSE (Power Sourcing Equipment) module.
- : antenna jack to connect an additional high-power external antenna. Since the unit comes with a built in antenna, usually it is not required to connect another one outside.

2.3 System requirements

- Each PC in the LAN needs a working Ethernet Adapter and an Ethernet cable with RJ45 connectors
- TCP/IP protocol must be installed on each PC
- Web browser, such as Microsoft Internet Explorer 5.0 or later, Netscape Navigator 6.0 or later
- If the device is configured in the AP client router mode, you will also need: Wireless Internet Access Service (WISP).
- If the device is configured in the AP router mode, you will also need: Broadband Internet Access Service (DSL/Cable/Ethernet)
- One DSL/Cable Modem that has an RJ45 connector (you do not need it if you connect the router to the Ethernet)

2.4 Environment requirements

- Operating temperature: -30°C~70°C
- Operating Humidity: 10%~90% RH, non-condensing

2.5 Connecting the device

To establish an infrastructure network in AP Client Router mode as Figure 2-3, please take the following steps:

1. Make sure you are provided with wireless Internet service by your WISP (Wireless Internet Service Provider).
2. Locate an optimum location for the AP. Try to place your AP in an appropriate position where it can well receive the signal from WISP.
3. Connect the AP to the desktop PC.
4. Adjust the direction of the AP to get the best signal.
5. Power on the AP before configuring the AP on the web-based page on your computer.

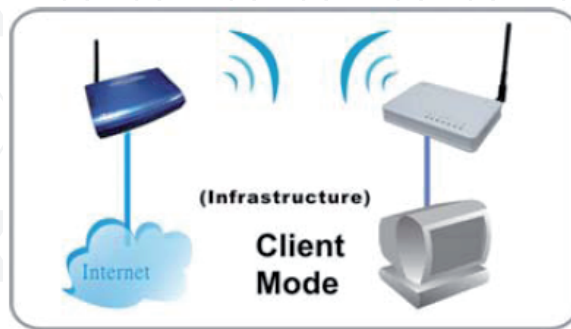


Figure 2-3

Chapter 3 Quick installation guide

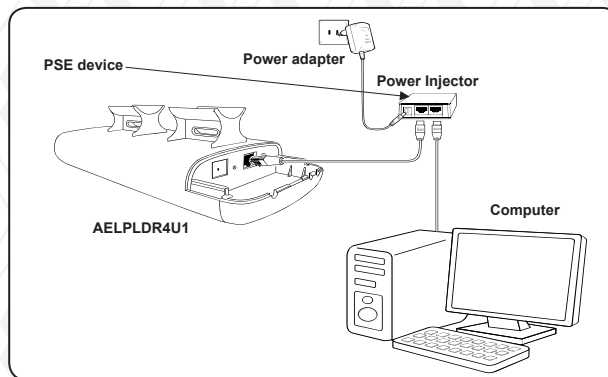
This Chapter will guide you to configure the AP to function in your network and gain access to the internet through your ISP immediately after successful configuration. A more detailed description of the AP's webbased utility and its functions can be found in "Chapter 4: Configuring the AP"

Note: only a wired network connection can be used for the initial configuration of the access point.

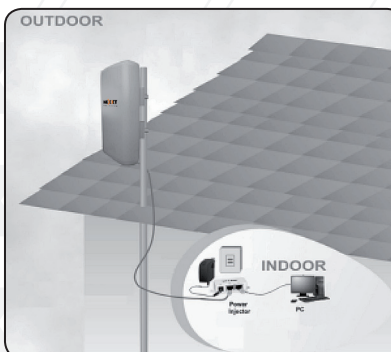
Before making any hardware connections, find a suitable location to place the access point. The best spot is usually at the center of the wireless network, with unobstructed line-of-sight to all wireless clients operating in the coverage area.

Also consider that the higher the antenna is placed, the better the device can perform. Do not forget to make sure that the pole or structure you use to install the device is stable and firmly secured in place.

1. In order to integrate your new wireless access point into your installation, start by plugging one end of an Ethernet cable to the PoE port of the supplied PSE, and the other end of the cable to the LAN port on the access point.
2. Use a second Ethernet cable to make the connection between the LAN port of the PSE module and your computer.
3. Power the device by plugging the included AC power adapter to DC jack on the PSE device, and the other end into a standard wall outlet.

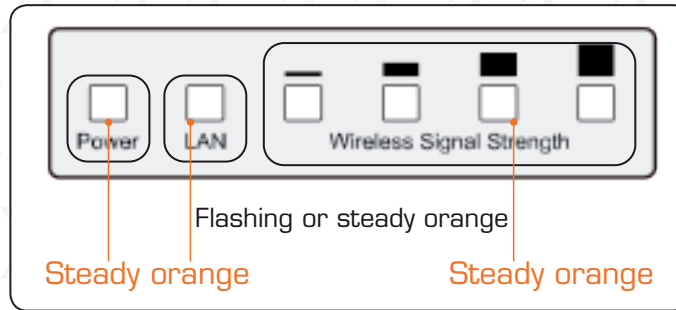


4. If setting up the device in an outdoor location, the connection will be similar to the figure below, once the above steps have been successfully completed.



3.1 Checking the LEDs

Upon powering on all your network devices, check the status of the access point by verifying that all the LEDs light up normally, as shown in the diagram below.

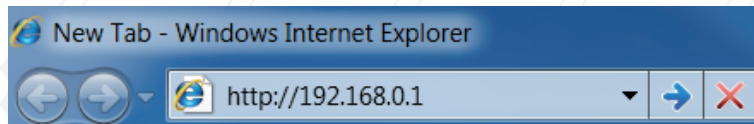


3.2 Initial configuration of the access point

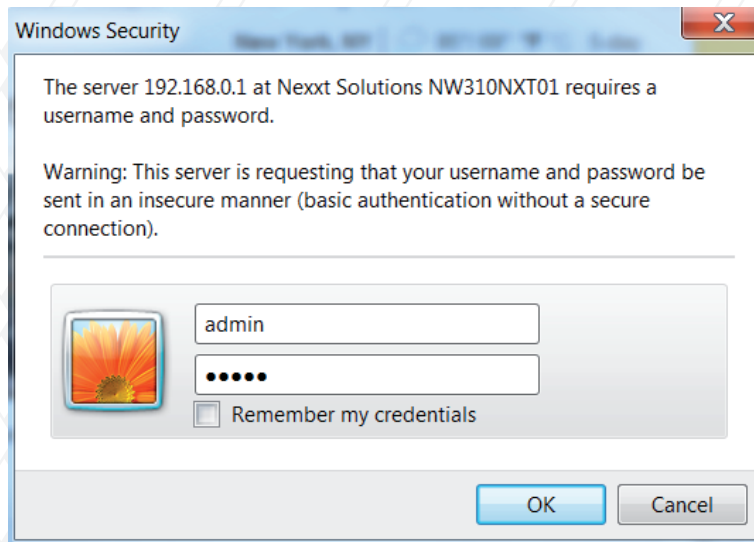
Note: first make sure your wired station Static IP address is set within the same range as the Wireless Access Point.

3.2.1 Login

1. Start your WEB browser. Type `http://192.168.0.1` in the address field of the browser. Press enter to continue.



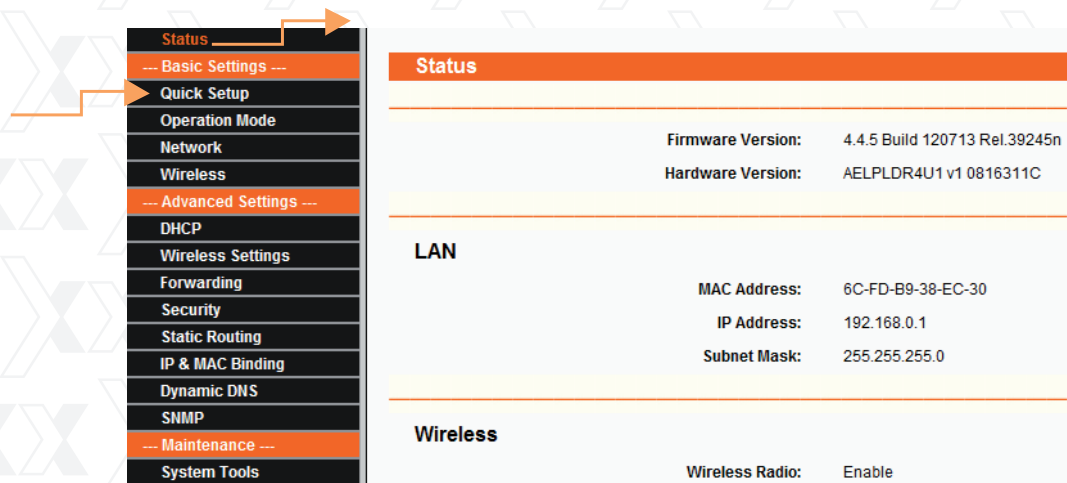
2. A dialog box will prompt you to enter the User name and Password. Enter the default values, both in lower case, and then click OK to complete the logging procedure.



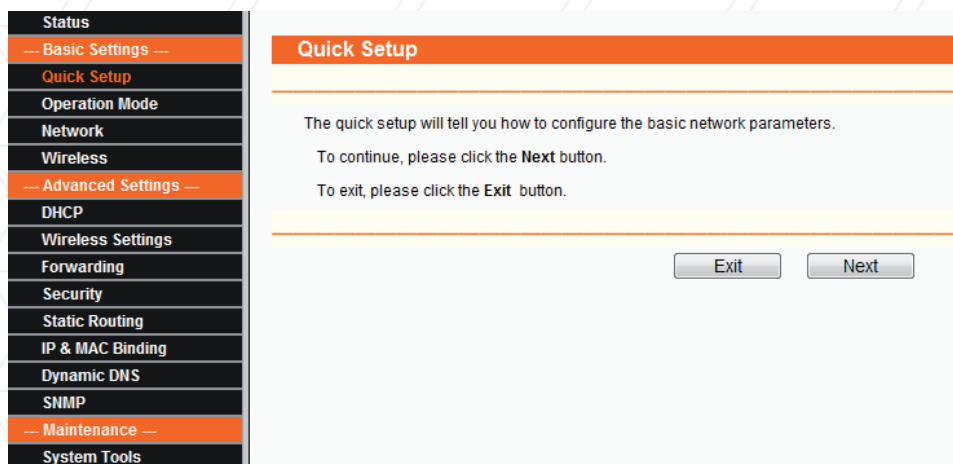
3. Afterwards, you can assign a new password for security purposes without necessarily modifying the default user name.
4. If the login window fails to appear, it means that your Web-browser has been set to a proxy. Verify that your parameters and passwords are correct, before making another attempt.
5. After successfully logging in, the main navigation page will appear on the screen.

3.3 Quick setup wizard

1. From the main menu on the left column of the screen, select the option Quick Setup.

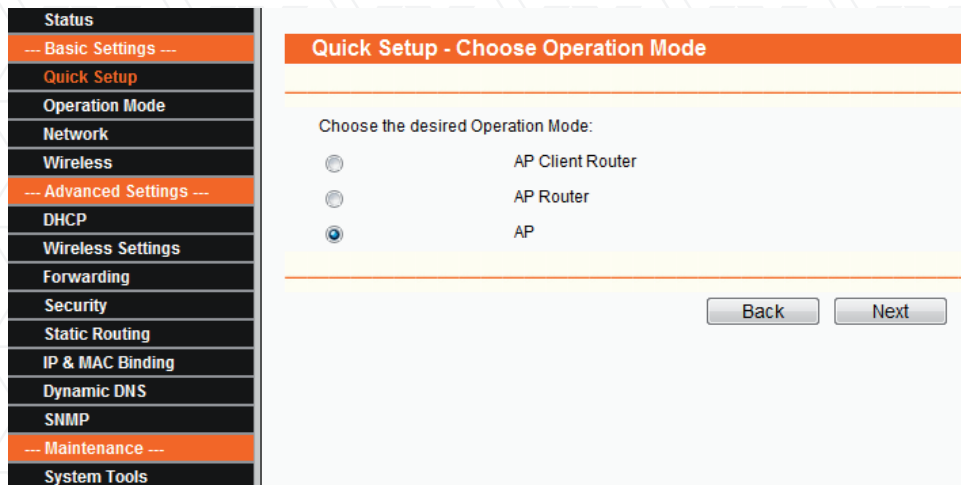


2. The Quick Setup window will pop up on the screen, as shown below. Click Next to open the following window.



3. Three operation modes are provided in the access point to meet each user's needs.

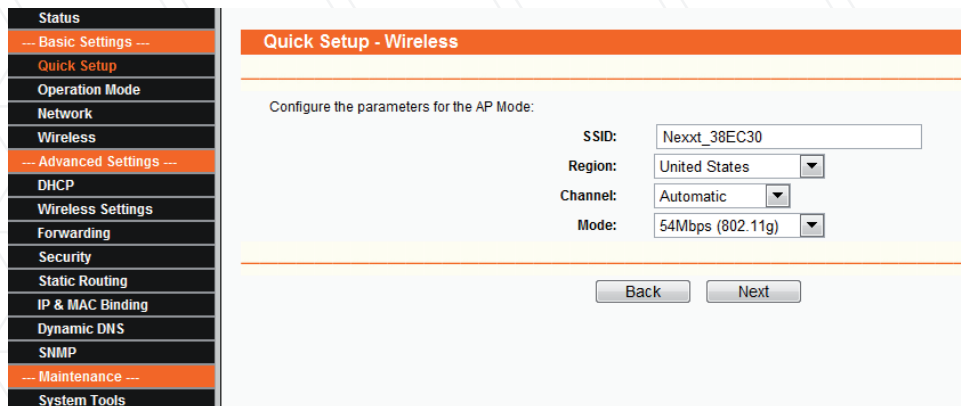
- **AP Client Router:** choose this mode to enable users to share the internet as a WISP client router.
- **AP Router:** choose this mode to enable users to share internet via ADSL/Cable modem, in a wireless broadband router configuration.
- **AP:** choose this mode to enable wireless devices to access a network using Wi-Fi, in an access point configuration.



4. For illustration purposes only, we will walk you through the AP option.

3.4 AP mode setting

1. Select AP on the Quick setup dialog box, as shown in the above illustration.
2. Click **Next** to open the wireless configuration window.



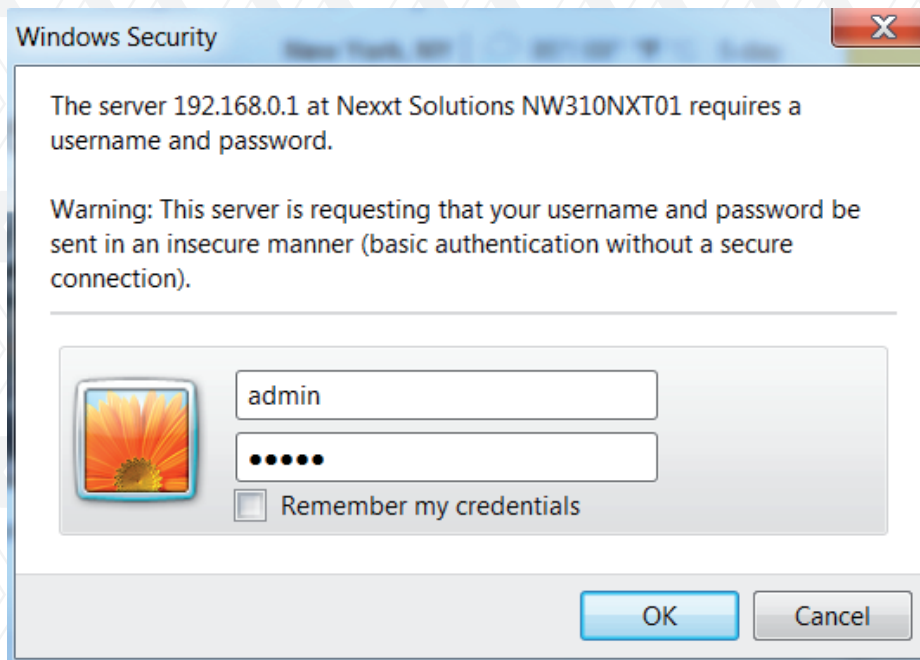
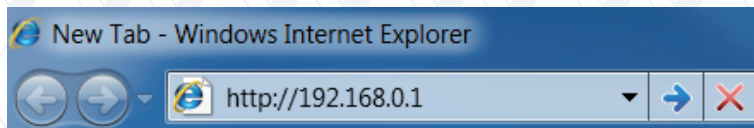
3. Enter a unique name to identify your wireless network. However, choose a name that is easily remembered by network users. In this example, we are using Nexxt_XXXXXX as the SSID identifier.
4. Select your region from the drop-down list, followed by **next**.



5. Click **Finish** to exit the Quick Setup wizard and wait until the AP finishes rebooting automatically. Changes will take effect only after the reboot is complete.
6. Remove the LAN cable from your computer and the PSE module. Now, insert your internet cable into the port labeled LAN located in the PSE device.
7. From now on, you can refer to the manual for any customized settings such as security, encryption, network modes, antenna alignment and more.

```
Pinging 192.168.0.1 with 32 bytes of data:  
Reply from 192.168.0.1: bytes=32 time=1ms TTL=64  
Reply from 192.168.0.1: bytes=32 time<1ms TTL=64  
Reply from 192.168.0.1: bytes=32 time=1ms TTL=64  
Reply from 192.168.0.1: bytes=32 time=1ms TTL=64  
  
Ping statistics for 192.168.0.1:  
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),  
    Approximate round trip times in milli-seconds:  
        Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

```
Pinging 192.168.0.1 with 32 bytes of data:  
  
Request timed out.  
Request timed out.  
Request timed out.  
Request timed out.
```



Quick Setup

The quick setup will tell you how to configure the basic network parameters.

To continue, please click the **Next** button.

To exit, please click the **Exit** button.

Exit

Next

Quick Setup - Choose Operation Mode

Choose the desired Operation Mode:

- AP Client Router
- AP Router
- AP

Back

Next

Quick Setup - Choose WAN Connection Type

Please choose WAN Connection Type:

- PPPoE
- Dynamic IP
- Static IP

Back

Next

Quick Setup - PPPoE

User Name:

Password:

Back

Next

Quick Setup - Static IP

IP Address:

Subnet Mask:

Default Gateway: (Optional)

Primary DNS: (Optional)

Secondary DNS: (Optional)

Back

Next

Quick Setup - Wireless

Please config parameters of APC Mode:

SSID:

Quick Setup - Wireless

Configure the parameters for the AP Mode:

SSID:

Region: ▼

Channel: ▼

Mode: ▼

(Note: If the device are prduced for selling in US, the Region will be unselectable.)

Quick Setup - Finish

Congratulations! The device is now connecting you to the Internet. For detailed settings, click on the corresponding menus if necessary.

Chapter 4 AP client router & AP router operation mode

This Chapter describes how to configure some advanced settings for your Access Point through the web-based management page. In the following sections, we will use the device in AP Client Router operation mode as example.

4.1 Login

After your successful login, you can configure and manage the Access Point. There are fourteen main menus on the left of the Web-based management page. Submenu will be available after you click one of the main menus. The fourteen main menus are: **Status, Quick Setup, Operation Mode, Network, Wireless, DHCP, Wireless Settings, Forwarding, Security, Static Routing, IP & MAC Binding, Dynamic DNS, SNMP** and **System Tools**. On the right of the Web-based management page, you will find detailed descriptions and instructions for the corresponding page. To apply any settings you have altered on the page, please click **Save**.

For a description of each Web page key functions, please refer to the sections below.

4.2 Status

In this screen, you will be able to view the AP's current status and configuration settings, all of which are read-only.

Status		
Firmware Version:	4.4.5 Build 120713 Rel.39245n	
Hardware Version:	AELPLDR4U1 v1 0816311C	
Wired		
MAC Address:	6C-FD-B9-38-EC-30	
IP Address:	192.168.0.1	
Subnet Mask:	255.255.255.0	
Wireless		
Operating Mode:	Access Point	
SSID:	Nexxt_38EC30_AP	
Channel:	11	
Mode:	54Mbps (802.11g)	
MAC Address:	6C-FD-B9-38-EC-30	
Traffic Statistics		
	Received	Sent
Bytes:	0	175574
Packets:	0	1033
System Up Time:	0 day(s) 00:10:09	
		<input type="button" value="Refresh"/>

Figure 4-1 Status

1. LAN

This field displays the current settings or information belonging to the LAN, including the MAC address, IP address and Subnet Mask.

2. Wireless

This field displays basic information or status belonging to the wireless function, including Wireless Radio, SSID, Channel, Mode, and Wireless MAC address.

3. WAN

These parameters apply to the WAN port of the router, including MAC address, IP address, Subnet Mask, Default Gateway and DNS server. If PPPoE is chosen as the WAN connection type, the Disconnect button will be shown here while you are accessing the Internet. You can also cut the connection by clicking the button. If you have not connected to the Internet, just click Connect to establish the connection.

4. Traffic Statistics

This field displays the router's traffic statistics.

5. System Up Time

The length of time since the system was last powered on or reset.

4.3 Quick setup

Please refer to Section 3.2: "Quick Setup".

4.4 Operation mode

The Operation Mode window will allow you to choose the operational application for your AP. The AP supports three mode types: AP Client Router, AP Router and AP. Please select the one you prefer, as shown in Figure 4-2. Click **Save** to confirm your choice.

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

Save

Figure 4-2 Operation Mode

- **AP Client Router** - In this mode, the device enables multiple computers to share the Internet from WISP. All LAN ports share the same IP from WISP through Wireless port. While connecting to WISP, the Wireless port works as a WAN port when in AP Client mode. The Ethernet port acts as a LAN port.
- **AP Router** - In this mode, the device enables multiple computers to share the Internet via ADSL/Cable Modem. The wireless port share the same IP to ISP through an ethernet WAN port. The Wireless port acts like a LAN port when in the AP mode.
- **AP** - In this mode, the device allows wireless communication devices to access a wireless network using WIFI. Both, the ethernet port and the wireless port work as LAN ports.

4.5 Network

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

There are three submenus under the Network menu (shown in Figure 4-3): **LAN**, **WAN** and **MAC Clone**. Click any of them in order to configure the corresponding function. Please refer to the sections below for a detailed description of each submenu.

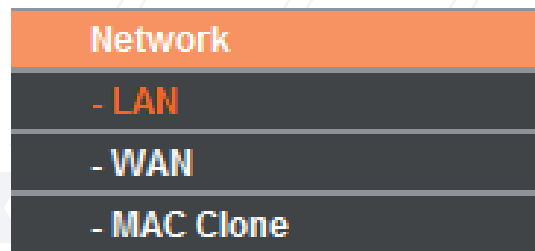


Figure 4-3 Network menu

4.5.1 LAN

Go to **Network > LAN** to enable the configuration of IP parameters of the LAN port on this page.

The image shows a screenshot of the 'LAN' configuration page. The page has an orange header with the word 'LAN'. Below the header, there are three rows of configuration fields. The first row is 'MAC Address:' with the value '6C-FD-B9-38-EC-30'. The second row is 'IP Address:' with a text input field containing '192.168.0.1'. The third row is 'Subnet Mask:' with a text input field containing '255.255.255.0'. At the bottom of the form, there is a 'Save' button.

Figure 4-4 LAN

- **MAC Address** - The physical address of the router, as seen from the LAN. This value cannot be changed.
- **IP Address** - Enter the IP address of your router in dotted-decimal notation (factory default: 192.168.0.1).
- **Subnet Mask** - An address code that determines the size of the network. Normally use 255.255.255.0 as the subnet mask.

Note:

1. If you change the IP Address of the LAN, you must use the new IP Address to login to the Router.
2. If the new LAN IP Address you set is not in the same subnet, the IP Address pool of the DHCP server will not take effect until they are re-configured.
3. If the new LAN IP Address you set is not in the same subnet, the Virtual Server and DMZ Host will change accordingly at the same time.

4.5.2 WAN

Go to **Network > WAN** to enable the configuration IP parameters of the WAN port on this page. First, please choose the WAN Connection Type (Dynamic IP/Static IP/PPPoE) for the Internet. The default type is Dynamic IP. If you are not given any login parameters (fixed IP Address, logging ID, etc), please select Dynamic IP. If you are given a fixed IP (static IP), please select Static IP. If you are given a user name and a password, please select the type of your ISP provided (PPPoE). If you are not sure which connection type you are currently using, please contact your ISP to obtain the correct information.

1. If you choose Dynamic IP, the router will automatically get IP parameters from your ISP. Please refer to Figure 4-5 below.

The screenshot shows the WAN configuration interface. At the top, there is an orange header with the text "WAN". Below this, the "WAN Connection Type" is set to "Dynamic IP" in a dropdown menu. The "Host Name" field is empty. The "IP Address", "Subnet Mask", and "Default Gateway" fields all contain "0.0.0.0". Below these fields are three buttons: "Renew", "Release", and "Obtaining network parameters...". The "MTU Size (in bytes)" is set to "1500" with a note: "(The default is 1500. Do not change it unless necessary.)". There are two checkboxes: "Use These DNS Servers" (unchecked) and "Get IP with Unicast DHCP (It is usually not required.)" (unchecked). The "Primary DNS" field contains "0.0.0.0" and the "Secondary DNS" field contains "0.0.0.0" with "(Optional)" next to it. At the bottom, there is a "Save" button.

Figure 4-5 WAN – Dynamic IP

This page displays the WAN IP parameters assigned dynamically by your ISP, including IP address, Subnet Mask, Default Gateway, etc. Click **Renew** to obtain new IP parameters from your ISP. Click the **Release** button to release the assigned IP parameters.

- **MTU Size** - The normal MTU (Maximum Transmission Unit) value for most ethernet networks is 1500 bytes. For some ISPs you need to reduce the MTU. But this is rarely required, and should not be done unless you are sure it is necessary for your ISP connection.

If your ISP gives you one or two DNS addresses, select Use These DNS Servers and enter the primary and secondary addresses into the correct fields. Otherwise, the DNS servers will be assigned dynamically from your ISP.

Note:

If you get address and find error when you go to a Web site, it is likely that your DNS servers are set up improperly. You should contact your ISP to get DNS server addresses.

- **Get IP with Unicast DHCP** - A few ISPs' DHCP servers do not support the broadcast applications. If you cannot get the IP Address normally, you can choose this option. (This is rarely required.)

2. If you choose Static IP, you should have fixed IP Parameters specified by your ISP. The Static IP settings page will appear as shown in Figure 4-6.

Figure 4-6 WAN - Static IP

In this case, you need to enter the following parameters into the spaces provided:

- **IP Address** - Enter the IP address in dotted-decimal notation provided by your ISP.
- **Subnet Mask** - Enter the subnet Mask in dotted-decimal notation provided by your ISP. Usually 255.255.255.0 is used as the subnet mask.
- **Default Gateway** - (Optional) Enter the gateway IP address in dotted-decimal notation provided by your ISP.
- **MTU Size** - The normal MTU (Maximum Transmission Unit) value for most ethernet networks is 1500 Bytes. For some ISPs you may need to modify the MTU. But this is rarely required, and should not be done unless you are sure it is necessary for your ISP connection.
- **Primary DNS** - (Optional) Enter the DNS address in dotted-decimal notation provided by your ISP.
- **Secondary DNS** - (Optional) Type another DNS address in dotted-decimal notation provided by your ISP if provided.

3. If you choose PPPoE, you should enter the following parameters as shown in Figure 4-7.

The screenshot shows the WAN configuration interface for a NetGate Wireless Access Point. The interface is titled "WAN" in an orange header. The configuration is for a PPPoE connection. The "WAN Connection Type" is set to "PPPoE". The "User Name" field contains "username" and the "Password" field is masked with dots. Under "WAN Connection Mode", the "Connect on Demand" radio button is selected. The "Max Idle Time" for this mode is set to 15 minutes. The "Connect Automatically" and "Connect Manually" options are unselected. The "Time-based Connecting" option is also unselected, and its "Period of Time" is set from 00:00 to 23:59. At the bottom of the configuration area, there are buttons for "Connect", "Disconnect", and "Disconnected" (which is highlighted in blue). Below the configuration area, there are "Save" and "Advanced" buttons.

Figure 4-7 WAN - PPPoE

- **User Name/Password** - Enter the User Name and Password provided by your ISP. These fields are case-sensitive.
- **Connect on Demand** - You can configure the router to disconnect 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 router to automatically re-establish your connection as soon as you attempt to access the Internet again. If you wish to activate Connect on Demand, 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 of minutes you want to have elapsed before your Internet connection terminates.
- **Caution:** Sometimes the connection cannot be terminated despite your setting of the "Max Idle Time" interval. This is due to some applications are continually linked to the internet in the background.
- **Connect Automatically:** The connection can be re-established automatically after being disabled.
- **Time-based Connection** - The connection will only be established within the period ranging from the start time to the end time (both are in HH:MM format) you specify in the Period of Time field.

Note:

Only when you have configured the system time on the **System Tools** -> **Time page**, the Time-based Connection will take effect.

- **Connect Manually** - You can set up the router so as to connect or disconnect it manually. After a specified period of inactivity (Max Idle Time), the router will cancel your Internet connection, in which case 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 of minutes that you wish to keep the connected status active unless a new link is requested.

Caution: Sometimes the connection cannot be terminated despite your setting of the "Max Idle Time" interval. This is due to some applications are continually linked to the internet in the background.

Click the **Connect** button to connect immediately. Click the **Disconnect** button to disconnect immediately.

If you want to do some advanced configurations, please click the **Advanced** button, and the page shown in Figure 4-8 will appear.

PPPoE Advanced Settings

MTU Size (in bytes): (The default is 1480, do not change unless necessary.)

Service Name:

AC Name:

Use IP address specified by ISP

ISP Specified IP Address:

Detect Online Interval: Seconds (0 ~ 120 seconds, the default is 0, 0 means not detecting.)

Use the following DNS Servers

Primary DNS:

Secondary DNS: (Optional)

Figure 4-8 PPPoE Advanced Settings

4.5.3 MAC clone

MAC Clone allows you to clone the MAC address of the managing PC's adapter to the WAN port. This is because some ISPs require that you register the MAC address of your adapter. Usually, no changes are required here.

Go to **Network > MAC Clone** in order to configure the MAC address of the WAN port on the current, page as shown in Figure 4-9.

Figure 4-9 MAC Address Clone

Some ISPs require that you register the MAC Address of your adapter, which is connected to your cable/DSL Modem or Ethernet during installation. Changes are rarely needed here.

- **WAN MAC Address** - This field displays the current MAC address of the WAN port. If your ISP requires that you register the MAC address, please enter the correct MAC address into this field. 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 router. If the MAC address is required, you can click the Clone MAC Address To button and this MAC address will be copied in the WAN MAC Address field.

Click **Restore Factory MAC** to restore the MAC address of the WAN port to its factory default value. Click **Save** to store your settings.

Note:

- 1) Only the PC on your LAN can use the Clone MAC Address To feature.
- 2) If you click **Save**, the Router will prompt you to reboot.

4.6 Wireless

The Wireless option, designed to improve functionality and performance of the wireless network, can help you to make the AP the ideal solution for your wireless network.

This menu allows users to create a wireless local area network through a few simple settings. Basic Settings are used for the configuration of some basic parameters of the AP. Wireless Mode allows you to select the mode that the AP works on. Security Settings provides three different security methods to protect your data and better safeguard 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 installations. Antenna Alignment shows the signal strength variation of the remote AP while changing the antenna's direction. Throughput Monitor provides information about the wireless data throughput. Wireless statistics enables you to get detailed information about the wireless stations currently connected.

There are eight submenus under the Wireless menu (shown in Figure 4-10): **Basic Settings, Wireless Mode, Security Settings, MAC Filtering, Wireless Statistics, Distance Setting, Antenna Alignment, Throughput Monitor, and Speed Test**. Click any of them, and you will be able to configure the corresponding function. A detailed description of each submenu is provided below.

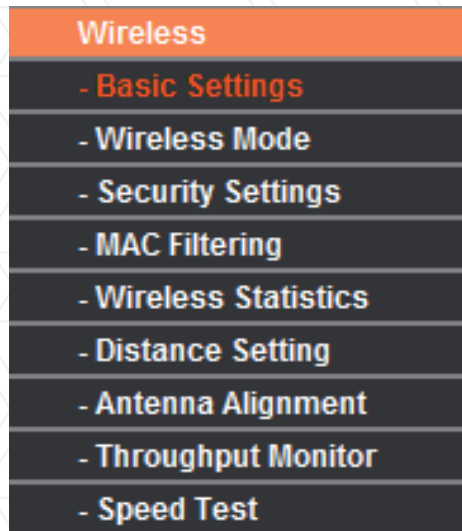


Figure 4-10 Wireless menu

4.6.1 Basic settings

Go to **Wireless > Basic Settings** in order to configure the basic parameters of your wireless network, as illustrated below (Figure 4-11).

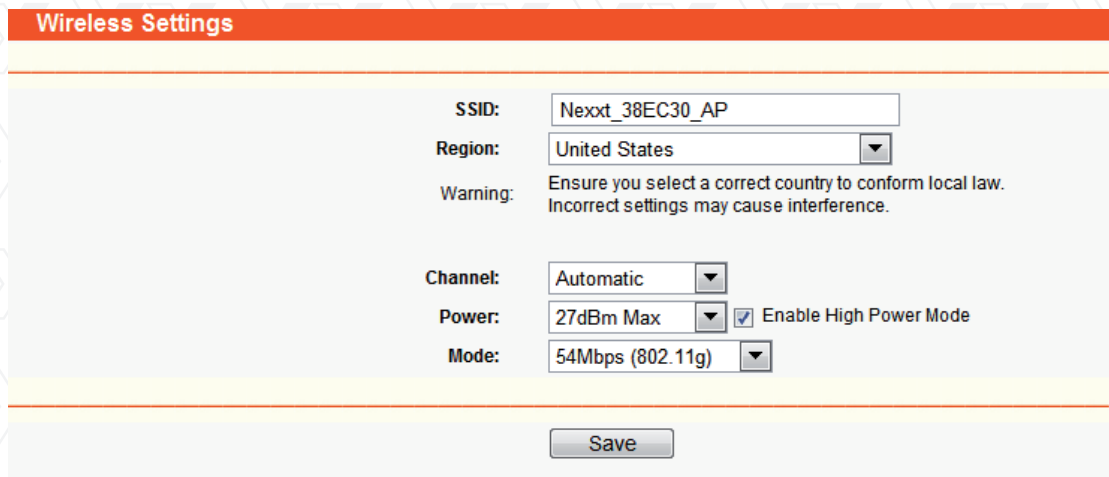
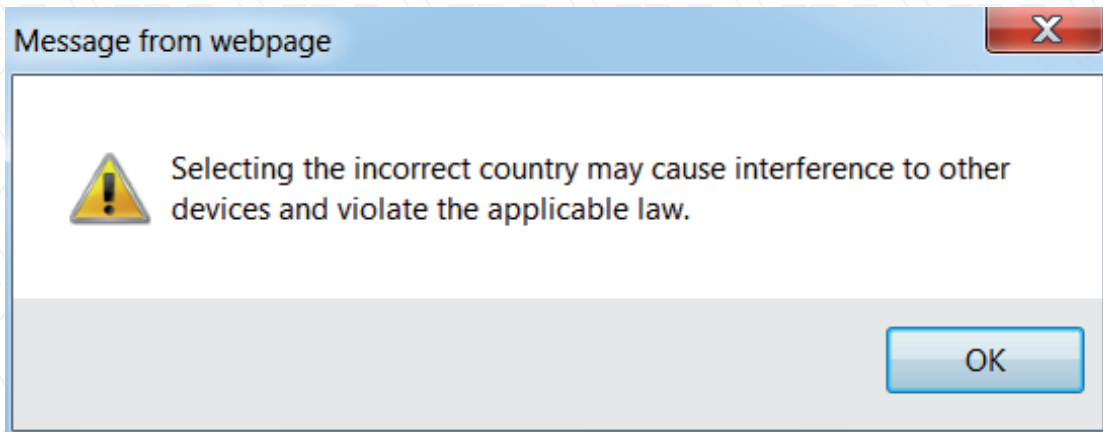


Figure 4-11 Wireless Settings in AP Client Router mode

- **SSID** - Enter a string of up to 32 characters. The same name or SSID (Service Set Identification) must be assigned to all wireless devices in your network. Considering your wireless network security, the default SSID is set to be NEXXT_XXXXXX (in which xxxxxx represent the last six unique characters of each router's MAC address). But it is strongly recommended that you change your network name (SSID) to a different value. 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 router in a region different from 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. The dialog box with this note will be displayed. Click **OK** to continue.
(Note: If the device are produced for selling in US, the Region will be unselectable.)



Dialog box

Note:

Based on local regulations, the North America version does not have the region selection option available.

- **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.
- **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.
- **Region** - Specifies the region where the wireless function of the AP can be used. Select your region from the drop-down list. If your country or region is not listed, please contact your local government agency for assistance.

Make sure to click the **Save** button to store your settings on this page.

Note:

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

4.6.2 Wireless mode

Go to **Wireless > Wireless Mode** in order to configure the wireless mode to be used by your device, as illustrated on this page (Figure 4-12).

Wireless Mode Settings

Access Point

Enable SSID Broadcast

Client

Enable WDS

SSID:

MAC of AP:

Repeater

MAC of AP:

Universal Repeater

MAC of AP:

Bridge (Point to Point)

With AP Mode

MAC of AP:

Bridge (Point to Multi-Point)

With AP Mode

MAC of AP1:

MAC of AP2:

MAC of AP3:

MAC of AP4:

MAC of AP5:

MAC of AP6:

Note: The current security method may be invalid after changing the wireless mode.

Figure 4-12 Wireless Mode

Note:

When AP Client Router is selected, only the Client mode will be available, as shown as Figure 4-12. However, when AP Router is selected, only the Access Point mode will be available.

- **Access Point** - Access Point mode allows wireless stations, including AP clients, to access the router. Enable SSID Broadcast - If you select the Enable SSID Broadcast checkbox, the Wireless AP will start broadcasting its name (SSID) on the air.
- **Client** - In Client mode, the access point will act as a wireless station to enable wired host(s) to access the wireless AP.
- **SSID** - Enter the SSID of AP that you want to access. If you check the radio button next to SSID, the AP client will connect to the AP using its SSID. MAC of AP - Enter the MAC address of AP that you want to access. If you check the radio button next to MAC of AP, the AP client will connect to the AP using its MAC address.

Note:

To apply any settings you have changed on the page, you must click the **Save** button. In this case, the AP will reboot automatically.

Click Survey to display the available access points within range after performing a scan. Choose from the list any of the access points to connect to, as shown in Figure 4-13.

AP List					
AP Count: 6					
ID	BSSID	SSID	Signal	Channel	Security
1	C4-0A-CB-5D-4B-D4	Nextt_3G_5FC706	21 dB	11	ON
2	C4-0A-CB-5D-4B-D1	Nextt_3G_5FC739	13 dB	4	ON
3	C4-0A-CB-5D-4B-D3	Nextt_0C749B	12 dB	8	OFF
4	C4-0A-CB-5D-4B-D5	Nextt_0CD0B8	20 dB	5	OFF
5	C8-3A-35-0C-74-B8	Nextt_0C65F4	69 dB	9	ON
6	00-15-70-23-1B-39	Nextt_0C74F1	0 dB	10	OFF

Figure 4-13 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** - Choose one AP from list to connect to.

If you click **Connect**, the values you selected will be filled in the SSID and MAC of AP fields, as shown in Figure 4-12.

Note:

If you want to configure other wireless mode settings, you can change your AP to AP operation mode on the Operation Mode page, as shown in Figure 4-2.

4.6.3 Security settings

Go to **Wireless > Security Settings** in order to configure the security parameters of the wireless network for your device, as illustrated on this page (Figure 4-14).

Wireless Security

Disable Security

WEP

Type: Automatic

WEP Key Format: Hexadecimal

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

WPA/WPA2

Version: Automatic

Encryption: Automatic

Radius Server IP:

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

Radius Password:

Group Key Update Period: 86400 (in seconds, minimum is 30, 0 means no update)

WPA-PSK/WPA2-PSK

Version: Automatic

Encryption: Automatic

PSK Passphrase:

(The Passphrase is between 8 and 63 characters long)

Group Key Update Period: 86400 (in seconds, minimum is 30, 0 means no update, valid only in AP mode.)

Save

Note: Some security methods cannot be selected, since they might not be supported by the current wireless mode.

Figure 4-14 Wireless Security

- **Disable Security** - The wireless security function can be enabled or disabled. If disabled, the wireless stations will be able to connect to the device without encryption. It is strongly recommended to opt for one of the following encryption methods, to better protect your network traffic.
- **WEP** - Selects the 802.11 WEP security.
 - **Type** - Choose the type for the WEP security from the pull-down list. The available options are:
 - 1) **Automatic** - Selects Shared Key or Open System authentication form automatically based on the wireless station's capability and request.
 - 2) **Shared Key** - Selects the 802.11 Shared Key authentication.
 - 3) **Open System** - Selects the 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 next to the key radio button you checked. 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 supported) 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 supported) 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 supported) or 16 ASCII characters.

Note:

If you do not set a passkey, the wireless encryption feature remains disabled even if you have selected Shared Key, as your Authentication Mode.

- **WPA/WPA2** - Selects WPA/WPA2 based on the radius server.
 - **Version** - Choose the WPA encryption method from the pull-down list.
The available options are:
 1. **Automatic** - It automatically sets WPA or WPA2 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 used by the radius server
 - **Radius Password** - Enter the password for the radius server.
 - **Group Key Update Period** - Specifies the group key update interval in seconds. The value should be 30 or higher. Enter 0 to disable the update.
- **WPA-PSK/ WPA2-PSK** - Selects WPA based on pre-shared passphrase.
 - **Version:** The user can choose any of the options below:
 1. **Automatic** - It automatically sets WPA-PSK or WPA2-PSK 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 **WPA-PSK** or WPA is set as the Authentication Mode, you can either select **Automatic**, or **TKIP** or **AES** as your Encryption type.
 - **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 should be 30 or higher. Enter 0 to disable the update.

Make sure to click the **Save** button to store your settings on this page.

Note:

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

4.6.4 MAC filtering

Go to **Wireless > MAC Filtering** in order to set up filtering rules designed to control the wireless access to the device, as shown in Figure 4-15.

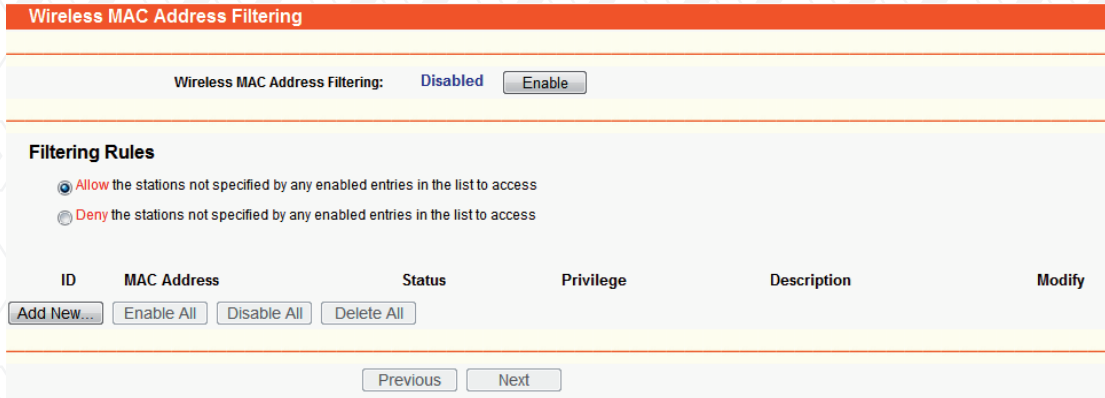


Figure 4-15 Wireless MAC address Filtering

The Wireless MAC Address Filtering feature allows you to control the wireless stations accessing the AP, based on the station’s MAC address.

- **MAC Address** - The wireless station’s MAC address that you want to access.
- **Status** - The status of this entry, either Enabled or Disabled.
- **Privilege** - Select the privileges for this entry. You may select one of the following Allow / Deny.
- **Description** - A short description of the wireless station.

To set up an entry, follow these instructions:

First, you must decide whether the unspecified wireless stations can access the router or not. If you desire that the unspecified wireless stations can access the router, please select the radio button Allow the stations not specified by any enabled entries in the list to access, otherwise, select the radio button Deny the stations not specified by any enabled entries in the list to access.

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, as shown in Figure 4-16.

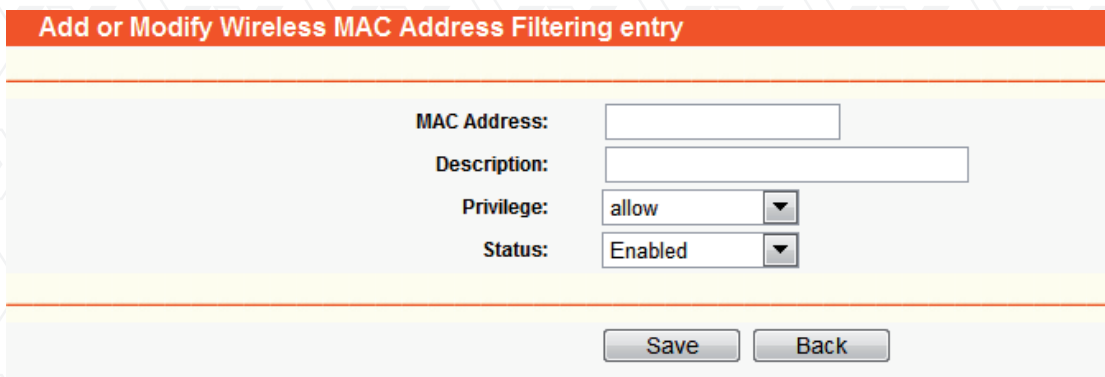


Figure 4-16 Add or Modify Wireless MAC Address Filtering entry

To add or modify a MAC Address Filtering entry, follow the instructions below:

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-00-07-0B.
2. Enter a short description of the wireless station in the Description field. For example: Wireless station A.
3. **Privilege** - Select the privileges for this entry, either **Allow** or **Deny**.
4. **Status** - Select **Enabled** or **Disabled** as the status for this entry, from the **Status** pull-down list.
5. Click the **Save** button to confirm this entry.

To add additional entries, repeat steps 1-5.
To modify or delete an existing entry:

1. Click the **Modify** button next to the entry you want to change. If you want to erase the entry, click on the **Delete** in this step.
2. Proceed with the changes you want to make.
3. Click the **Save** button.

Click the **Enable All** button to activate all entries enabled.
Click the **Disabled All** button to cancel all entries disabled.
Click the **Delete All** button to erase all entries.
Click the **Next** button to go to the following page and click the Previous button to return to the previous page.

For example: If you want to grant access to wireless station A with MAC address 00-0A-EB-00-07-BE, but deny access to wireless station B with MAC address 00-0A-EB-00-07-5F, while all other wireless stations cannot access the router, you should 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 and enter the MAC address 00-0A-EB-00-07-BE in the MAC Address field, enter wireless station A in the Description field, select **Allow** in the Privilege pull-down list and select **Enabled** in the **Status** pull-down list. Click the **Save** and the **Return** button at the end.
5. Click the **Add New...** button and enter the MAC address 00-0A-EB-00-07-5F in the MAC Address field, enter wireless station B in the Description field, select **Deny** in the Privilege pull-down list and select **Enabled** in the **Status** pull-down list. Click the **Save** and the **Return** button to complete this procedure.

The filtering rules just configured should look similar to the following list:

ID	MAC Address	Status	Privilege	Description	Modify
1	00-0A-EB-00-07-BE	Enabled	allow	Wireless Station A	Modify Delete
2	00-0A-EB-00-07-5F	Enabled	deny	Wireless Station B	Modify Delete

Note:

1. If you select the radio button **Allow the stations not specified by any enabled entries in the list to access** for Filtering Rules, the wireless station B will still not be able to access the router, however, other wireless stations that are not in the list will be able to access the router.
2. If you enable the function and select the **Deny the stations not specified by any enabled entries in the list to access** for Filtering Rules, and there are not any enabled entries in the list, thus, no wireless stations can access the router.

4.6.5 Wireless statistics

Selecting **Wireless > Wireless Statistics** will allow you to see the wireless transmission information in the following screen, as shown in Figure 4-17.

Wireless Statistics				
Currently Connected Wireless Stations numbers: 1 <input type="button" value="Refresh"/>				
ID	MAC Address	Current Status	Received Packets	Sent Packets
1	6C-FD-B9-38-EC-31	AP-DOWN	0	221866

Figure 4-17 Wireless stations linked to the router

- **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.
- **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.

4.6.6 Distance setting

Go to **Wireless > Distance Setting** in order to adjust the wireless range in outdoor settings, as shown in Figure 4-18. This parameter is critical for ensuring the stability of the link. Enter the distance of your wireless link, and the software will optimize the frame ACK timeout value automatically.

Distance Setting

Adjust option:

Distance: (0-52.6km)

Note: Use this command to specify the distance expressed in kilometers, rounded up to the nearest decimal place. If the distance is set too short or too long, it will result in a poor connection and degraded throughput performance. It is best to set the value at 110% of the real distance. If the AP is being used in an indoor installation, please select the indoor option.

Figure 4-18 Distance Setting

- **Adjust option** - Keep the default setting if the access point is mounted outdoors. You can also choose to set up this parameter manually.
- **Distance:** Use this command to specify the distance expressed in kilometers, rounded up to the nearest decimal place. If the distance is set too short or too long, it will result in a poor connection and degraded throughput performance. It is best to set the value at 110% of the real distance. If the AP is being used in an indoor installation, please select the indoor option. Click **Save** to confirm your settings.

4.6.7 Antenna alignment

Go to **Wireless > Antenna Alignment** in order to visualize how the signal strength of the remote AP varies when changing the antenna's direction.

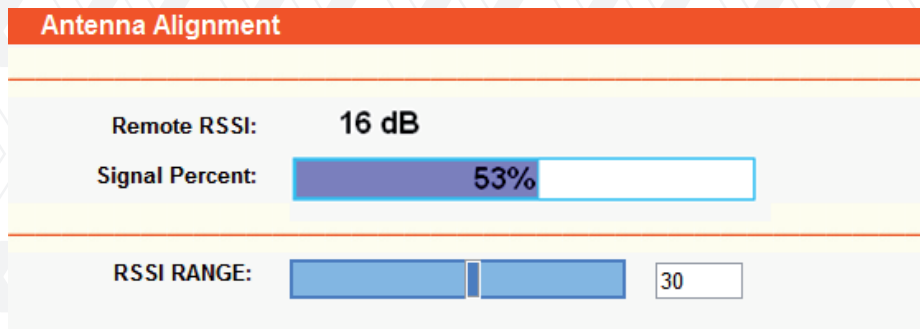


Figure 4-19 Antenna Alignment

- **Remote AP RSSI** - Remote AP signal strength value.
- **Signal percent** - The ratio of RSSI to RSSI RANGE (in percentage points).
- **RSSI RANGE** - You can drag the slider bar to configure it 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 can be used to change an offset of the maximum indicator value.

Note:

1. This works only after the connection to the remote access point has been established in client mode.
2. There is no other way to change the antennas direction except to adjust the devices direction manually.

4.6.8 Throughput monitor

Go to **Wireless > Throughput Monitor** in order to visualize the wireless throughput information in the screen as illustrated in Figure 4-20.

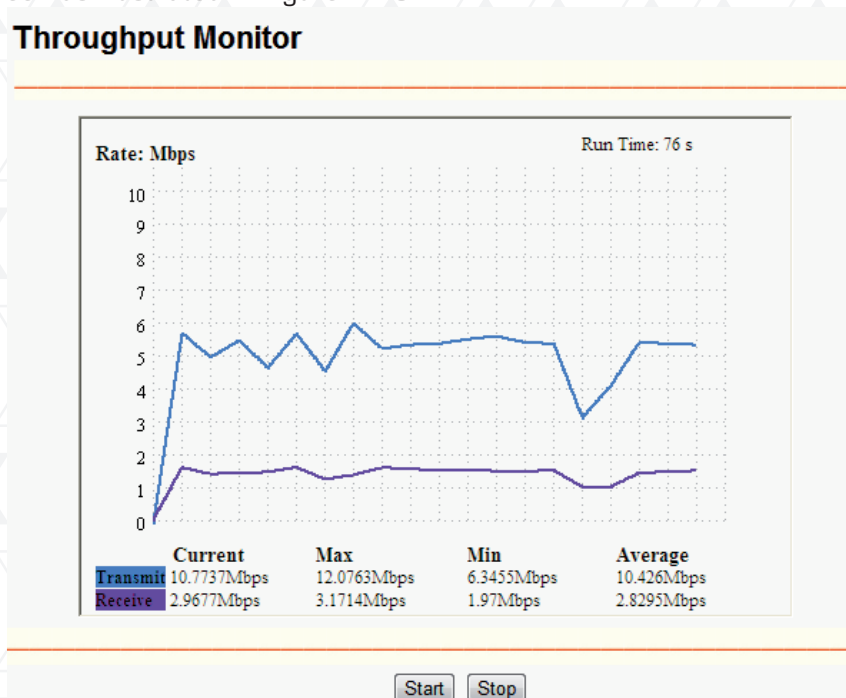


Figure 4-20 Wireless Throughput

- Rate** - The unit used to measure throughput.
- Run Time** - How long this function has been running.
- Transmit** - Wireless transmit rate.
- Receive** - Wireless receive rate.

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

4.7 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 (as shown in Figure 4-21): DHCP Settings, DHCP Clients List and Address Reservation. Clicking any of them will enable you to configure the corresponding function. Detailed descriptions for each submenu are provided below.

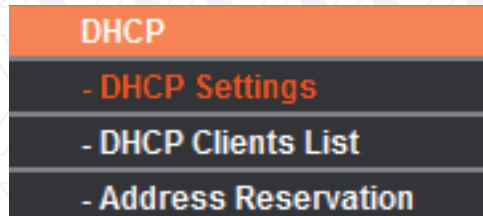


Figure 4-21 DHCP menu

4.7.1 DHCP settings

Go to **DHCP > DHCP Settings** in order 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 this page (Figure 4-22).

 A screenshot of the "DHCP Settings" configuration page. The page has a dark orange header with "DHCP Settings" in white. Below the header is a light grey form area. The form contains several settings:

- DHCP Server:** Radio buttons for "Disable" (selected) and "Enable".
- Start IP Address:** Text input field containing "192.168.0.100".
- End IP Address:** Text input field containing "192.168.0.199".
- Address Lease Time:** Text input field containing "120" followed by "minutes (1~2880 minutes, the default value is 120)".
- Default Gateway:** Text input field containing "192.168.0.1" with "(optional)" to its right.
- Default Domain:** Text input field with "(optional)" to its right.
- Primary DNS:** Text input field containing "0.0.0.0" with "(optional)" to its right.
- Secondary DNS:** Text input field containing "0.0.0.0" with "(optional)" to its right.

 At the bottom of the form is a "Save" button.

Figure 4-22 DHCP Settings

- **DHCP Server** - Selecting the radio button next to Disable/Enable will switch the DHCP server off or on in your AP. The default setting is Disable. If you disable the Server, you must have another DHCP server within your network. Otherwise, you will have to configure the IP address of the computer manually.
- **Start IP Address** - This field specifies the first address in the IP Address pool. 192.168.0.100 is the default start IP address.
- **End IP Address** - This field specifies the last address in the IP Address pool. 192.168.0.199 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 time range is 1 ~ 2880 minutes. The default value is 120 minutes.
- **Default Gateway (optional)** - This field is used to enter the IP address of the gateway for your LAN. The factory default setting is 0.0.0.0.
- **Default Domain (optional)** - This field is used to enter the domain name of the your DHCP server. You can leave the field blank.
- **Primary DNS (optional)** - This field is used to 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)** - This field is used to 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:

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 only after the device reboots.

4.7.2 DHCP clients list

Go to **DHCP > DHCP Clients List** in order to visualize the Client Name, MAC Address, Assigned IP and Lease Time for each DHCP Client attached to the device (Figure 4-23).

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 4-23 DHCP Clients List

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

No values on this page can be modified. To update this page and to show the devices currently attached, click on the Refresh button.

4.7.3 Address reservation

Go to **DHCP > Address Reservation** in order 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 4-24).

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 4-24 Address Reservation

- **MAC Address** - In this field the MAC address of the PC for which you want to reserve an IP address for is displayed.
- **Reserved IP Address** - In this field, the IP address that the AP reserved is displayed.
- **Status** - It shows whether the entry is enabled or not.
- **Modify** - Use it to either modify or delete an existing entry.

To reserve IP addresses:

1. Click the **Add New** button on the Address Reservation page. The following window will be displayed (Figure 4-25).
2. Enter the MAC address (using the XX-XX-XX-XX-XX-XX format) and the IP address in dotted-decimal notation of the computer you want to add.
3. Click the **Save** button when finished.

Add or Modify an Address Reservation Entry

MAC Address:
Reserved IP Address:
Status: ▼

Figure 4-25 Add or Modify an Address Reservation Entry

To modify a reserved IP address:

1. Select the reserved address entry you need and click Modify. If you wish to erase 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 following page, and Click **Previous** to return the last page.

Note:

Changes will take effect only after the device reboots.

4.8 Wireless settings

Go to **Wireless Settings** in order to enable the configuration of some advanced settings for the device in the following screen, as shown in Figure 4-26.

Figure 4-26 Wireless settings

- **Enable WMM** - WMM function guarantees that packets with high- priority messages to be transmitted preferentially. It is strongly recommended to have this feature enabled.
- **Enable AP Isolation** - This function can isolate wireless stations on your network from each other. Wireless devices will not be able to communicate with each other through the WLAN. This option is available only on Access Point mode.
- **Disable short preamble** - Check this box to disable the short preamble and use the long preamble only.. It is recommended not to modify these settings.
- **RTS threshold** - Here you can specify the RTS/CTS (Request to Send/Clear to send) threshold, which is the packet maximum size defining whether RTS/CTS frames should be sent.
- **Fragmentation Threshold** - The maximum packet size used for fragmentation.
- **Beacon Interval** - The time interval between two successive beacons.
- **Power** - The transmit power of the access point. The checkbox determines whether the transmit power conforms to regulatory levels or not. Un-checking the Obey Regulatory Power option may cause interference to other devices and also violate applicable laws in some areas.
- **Antenna Settings** - The polarization of an antenna.
- **Signal LED Thresholds** - The RSSI thresholds of the signal LEDs.

4.9 Forwarding

There are four submenus under the **Forwarding** menu (shown in Figure 4-27): **Virtual Servers**, **Port Triggering**, **DMZ** and **UPnP**. Click any of them to be able to configure the corresponding function. Detailed descriptions of each submenu are provided in the sections below.

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 as a virtual server must have a static or reserved IP Address because its IP Address may change when using the DHCP function. Port Triggering is used for some applications that cannot work with a pure NAT router, like Internet games, video conferencing, Internet calling and so on, which require multiple connections. The DMZ host feature allows one local host to be exposed to the Internet to gain access to certain applications such as Internet gaming or videoconferencing. DMZ host forwards all the ports at the same time. Any PC with a port 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 change when using the DHCP function. The Universal Plug and Play (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.

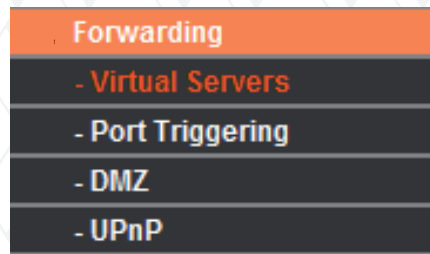


Figure 4-27 The Forwarding menu

4.9.1 Virtual servers

Go to **Forwarding > Virtual Servers** in order to set up virtual servers on this page, as shown in Figure 4-28.

Virtual Servers						
ID	Service Ports	IP Address	Protocol	Status	Modify	
1	21	192.168.0.101	TCP	Enabled	Modify Delete	

Figure 4-28 Virtual Servers

- **Service Port** - The numbers of External Ports. You can enter a service port or a range of service ports (in XXX – YYY format, whereby XXX is the start port number, and YYY is the end port number).
- **IP Address** - The IP Address of the PC providing the service application.