



N.MINI

300Mbps 11/b/g/n Mini-AP

User's Manual





Copyright & Disclaimer

No part of this publication may be reproduced in any form or by any means, whether electronic, mechanical, photocopying, or recording without the written consent of OvisLink Corp.

OvisLink Corp. has made the best effort to ensure the accuracy of the information in this user's guide. However, we are not liable for the inaccuracies or errors in this guide. Please use with caution. All information is subject to change without notice

All Trademarks are properties of their respective holders.



FCC Statement

Federal Communication Commission Interference 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 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.

FCC Caution

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

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, and (2) this device must accept any interference received, including interference that may cause undesired operation. For product available in the USA/Canada market, only channel 1~11 can be operated. Selection of other channels is not possible.

This device and its antenna(s) must not be co-located or operation in conjunction with any other antenna or transmitter.

IMPORTANT NOTE

FCC Radiation Exposure Statement:

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.



© 2009 OvisLink Corporation, All Rights Reserved



Table of Contents

1. Introduction	1
1.1 Overview	1
1.2 Features	2
1.3 Features	2
1.4 Physical Details	3
1.4.1 Top LED	3
1.4.2 Bottom Switch	4
1.4.3 Side Panel	5
2. Operation Modes	6
2.1 Router Mode	6
2.2 Access Point Mode	7
2.3 Client Mode	8
3. Installation	9
3.1 Hardware Connection	9
3.1.1 AP/ Client Mode	9
3.1.2 Router Mode	9
3.1.3 Bridging the Network	10
3.2 Login	11
3.3 Default Settings	13
3.4 Common Connection Types	14
3.3.1 Cable Modems	14
3.3.2 DSL Modems	14
3.3.3 Other Modems (e.g. Broadband Wireless)	15
4. Web Configuration	16
4.1 Setup Wizard	16
4.1.1 Router Mode	17
4.1.2 AP/Client Mode	18
4.2 Wireless	20
4.2.1 Basic Settings	20
4.2.2 Advanced Settings	23
4.2.3 Security	25
4.2.4 Access Control	28
4.2.5 WDS Settings	28
4.2.6 Site Survey	34



4.2.7	WPS	35
4.2.8	Schedule	36
4.3	TCP/IP Settings	37
4.3.1	LAN Interface	37
4.3.2	WAN Interface	40
4.4	Firewall	45
4.4.1	Port Filtering	45
4.4.2	IP Filtering	46
4.4.3	MAC Filtering	47
4.4.4	Port Forwarding	48
4.4.5	URL Filtering	49
4.4.6	DMZ	50
4.4.7	VLAN	51
4.5	QoS	52
4.6	Route Setup	54
4.7	Management	55
4.7.1	Status	55
4.7.2	Statistics	56
4.7.3	Dynamic DNS	57
4.7.4	Time Zone Setting	58
4.7.5	Denial of Service	59
4.7.6	Logs	60
4.7.7	Upgrade Firmware	61
4.7.8	Save /Reload Settings	62
4.7.9	Password	62
4.8	Log out	63
5. PC Configuration		64
5.1	Overview	64
5.2	Windows Clients	64
5.2.1	TCP/IP Settings – Overview	64
5.2.2	Checking TCP/IP Settings - Windows 2000	64
5.2.3	Checking TCP/IP Settings - Windows XP	66
5.2.4	Checking TCP/IP Settings - Windows Vista	68
5.2.5	Checking TCP/IP Settings - Windows 7	69
5.2.6	Internet Access	71
5.2.7	Macintosh Clients	73
5.2.8	Linux Clients	73
5.2.9	Other Unix Systems	74
5.2.10	Wireless Station Configuration	74



Appendix A: Troubleshooting.....75

- Overview75
- General Problems75
- Internet Access75
- Wireless Access.....76

Appendix B: About Wireless LANs78

- BSS78
- Channels.....78
- Security78
- Wireless LAN Configuration.....79



1

Introduction



1.1 Overview

N.MINI is a pocket size IEEE802.11b/g/n router with 1 fast Ethernet ports, which provides a powerful high-speed wireless connection for compatible wireless-enabled devices into the network with the freedom to roam. With web-based UI, this wireless router is easy to be setup and maintained. All functions can be configured within the easy and friendly user interface via web browser. Via the fast wireless network speed up to 300 Mbps, you can be very comfortable to have experience of high speed web surfing, files downloading, online game playing, and video conference session and streaming high quality multimedia materials. The wireless router provides WPA/WPA2, 64/128 bit WEP encryption and IEEE802.1x which ensures a high level of security to protect users' data and privacy when you are traveling.

If not specify, "Wireless Router" means N.MINI in the following paragraph.



1.2 Features

If you encounter a technical issue that can not be resolved by information on this guide, we recommend that you visit our comprehensive website support at www.airlive.com. The tech support FAQ are frequently updated with latest information.

In addition, you might find new firmwares that either increase software functions or provide bug fixes for N.MINI. You can reach our on-line support center at the following link: http://www.airlive.com/support/support_2.jsp

Since 2009, AirLive has added the “Newsletter Instant Support System” on our website. AirLive Newsletter subscribers receives instant email notifications when there are new download or tech support FAQ updates for their subscribed airlive models. To become an AirLive newsletter member, please visit: http://www.airlive.com/member/member_3.jsp

Instant Support : Subscribe Language :

All Products

Product Main Category	Product Secondary Category	Model NO
Print Server	11 b/g/n Indoor	N.MINI
Router	11a/b/g Outdoor	
Security Gateway	11b/g Indoor	
Skype	11b/g Outdoor	
Switches	PCBA	
VoIP		
Wireless Indoor		
Wireless Accessory		
Wireless Outdoor		
WISP		

Figure 1.4: AirLive Newsletter Support System

1.3 Features


- Create temporary, personal, wireless access in your hotel room or a coffee shop hotspot
- High security with build-in: WEP 64/128, WPA, WPA2 mixed, 802.1x and 802.11i
- Support AP, Router and Client Mode
- Wireless Quality of Service (QoS) - 802.11e, WMM
- Support WPS (Push button/ Pin code)
- Slide switch to change mode (Router/AP(Bridge + Repeater)/Client) easily



1.4 Physical Details

1.4.1 Top LED



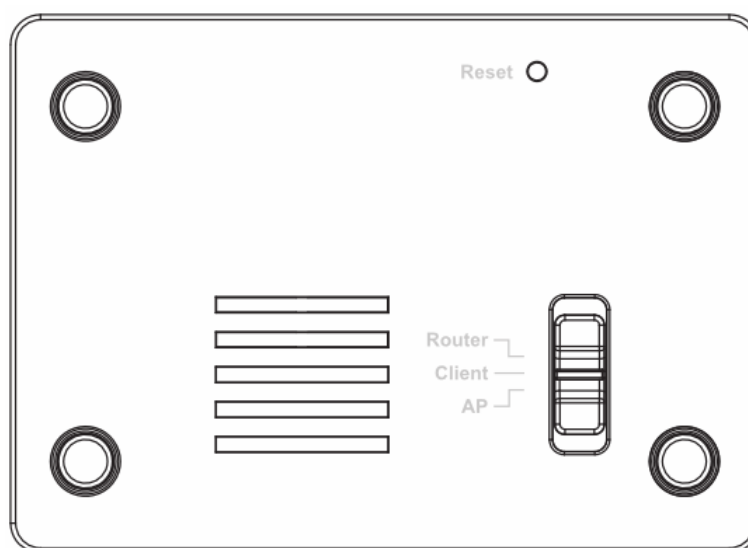
WPS button	
	Press the physical WPS button on the Wireless Router once, or go to enable the WPS function via web configuration (Go to Wireless > WPS page), then the LED will start to flash. Please make a connection with other WPS supported device within 2 minutes.

LED Behavior				
LED	Printed	Color	Behavior	Indication
POWER	PWR	Green	Off	Power off
			On	Power on
			Blinking	Power saving mode starting
System	SYS	Green	On	Press reset button two seconds the LED will on, keep on pressing more than 3-5 seconds, the LED will start to flash
			Blinking	System CPU is busy



Wireless LAN	WLAN	Green	Off	WLAN function off
			On	WLAN link / active
			Blinking	WLAN traffic transmitting
WPS	WPS	Green	Off	WPS Off
			Blinking	WPS is enabled to make a connection
Ethernet	Ethernet	Green	Off	No Ethernet cable connecting
			On	Ethernet cable connected
			Blinking	Receiving/ sending data

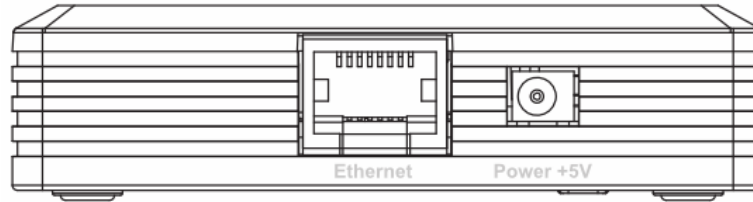
1.4.2 Bottom Switch



Reset button and switch bar	
Reset	Keep on pressing the Reset button more than 3 seconds, the Wireless Router will set all setting back to factory default values.
Switch	User need to MANUALLY switch the bar into the mode preferred, Router, AP or Client mode, then the device will reboot automatically into the mode selected.



1.4.3 Side Panel



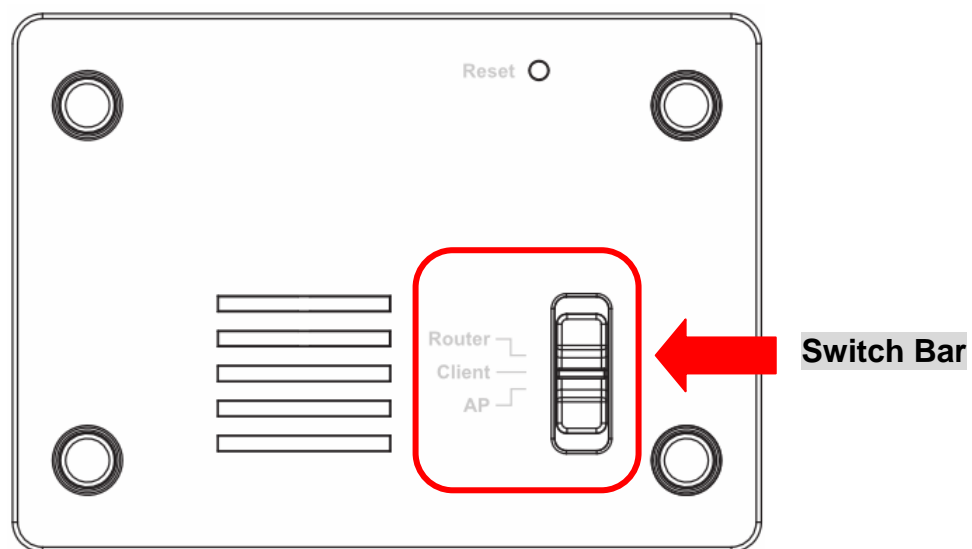
Ethernet and power ports	
Ethernet	When the mode be set to AP or Client modes, use standard LAN cables (RJ45 connectors) to connect your PCs to this port. If required, any port can be connected to another hub. Any LAN port will automatically function as an "Uplink" port when necessary. When the mode be set to Router mode, connect the ADSL or Cable Modem here with RJ45 cable. If your modem came with a cable, use the supplied cable, otherwise, use a standard LAN cable (RJ45 connectors).
Power (5V)	Connect the supplied power adapter here.



2

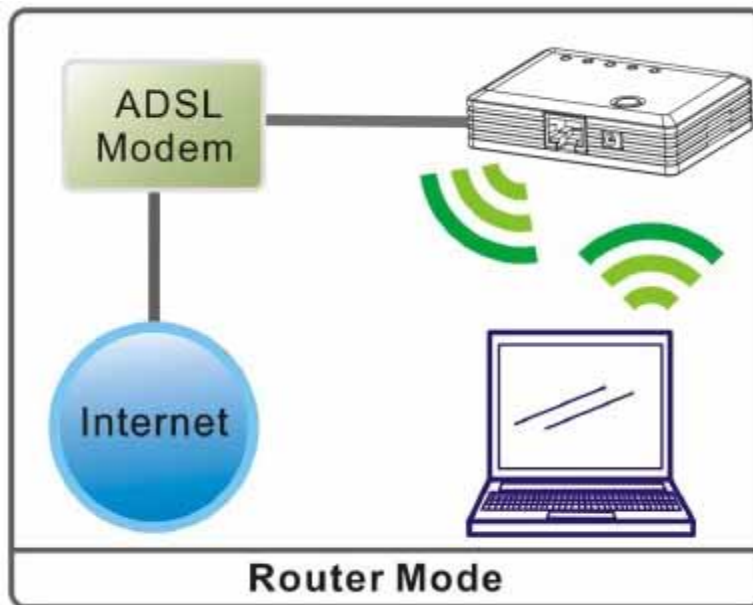
Operation Modes

This device provides operational applications with Router, AP and Client modes, which are mutually exclusive. This device is shipped with configuration that is functional right out of the box. If you want to change the settings in order to perform more advanced configuration or even change the mode of operation, you can manually switch to the mode you desire by the manufacturer as described in the following sections. The default setting mode is AP mode.



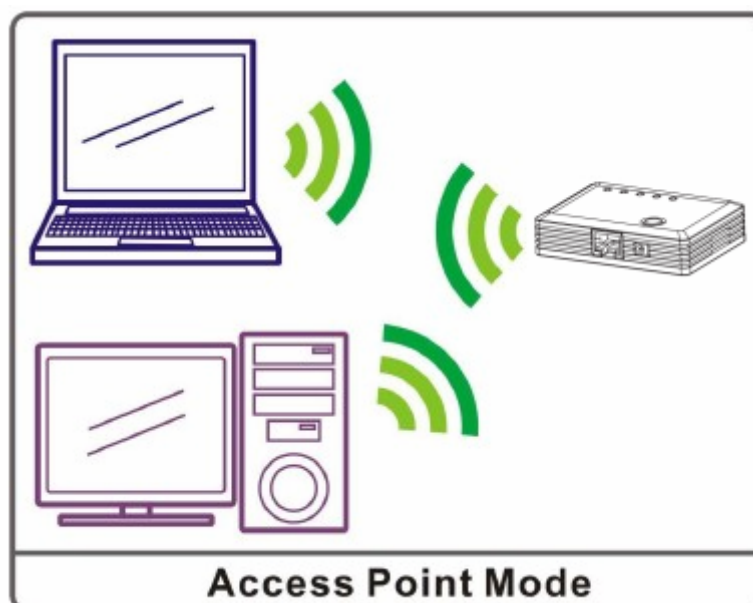
2.1 Router Mode

When set to Router mode, ensure you are using the wireless LAN interface, connect the Wireless Router with computer via radio frequency. In this mode, the device is supposed to connect to internet via ADSL/Cable Modem. Connect the ADSL modem to the Ethernet port of the Wireless Router by Ethernet cable. After connected successfully, user can login the web page of the Wireless Router to set up the Internet connection by using PPPoE, DHCP client, PPTP client, L2TP client or static IP.



2.2 Access Point Mode

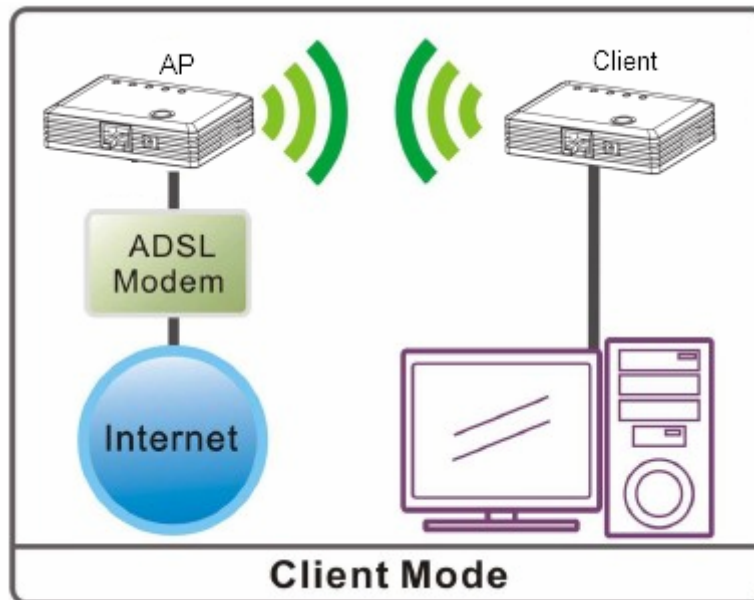
When acting as an Access Point (AP), this device connects all the stations (PC/notebook with wireless network adapter) to a wireless network.





2.3 Client Mode

If set to Client (Infrastructure) mode, this device can work like a wireless station when it's connected to a computer so that the computer can send packets from wired end to wireless interface.





3

Installation

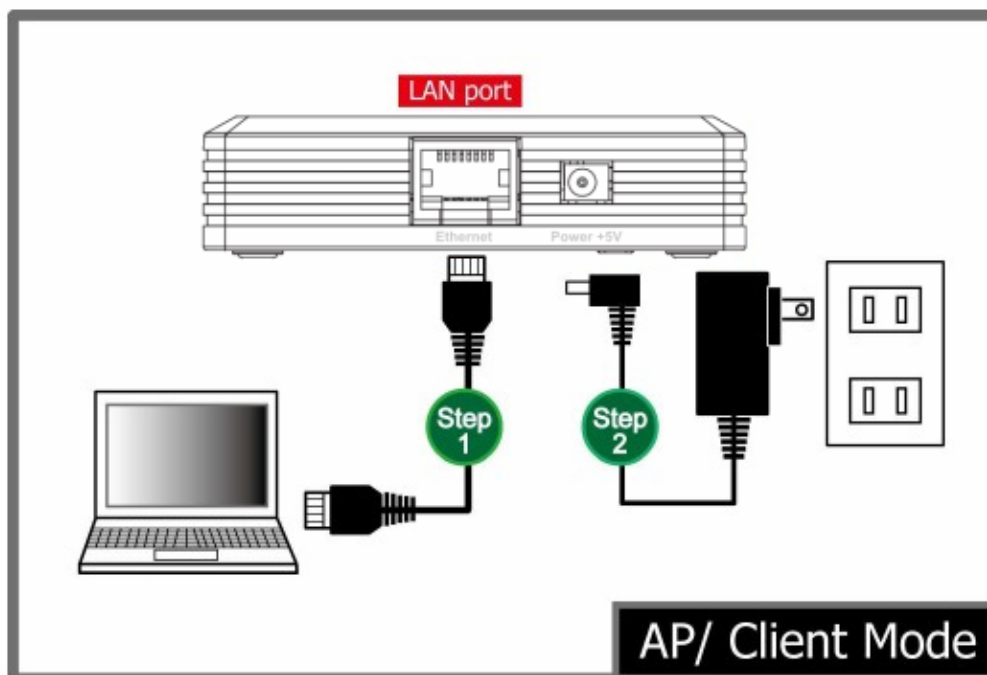
3.1 Hardware Connection

3.1.1 AP/ Client Mode

Connect via cable ...

Step1. Connect one end of the Ethernet cable to the Ethernet port(act as a LAN port here) of the Wireless Router, another end to your PC or notebook.

Step2. Then, connect the Wireless Router with a power to an outlet.



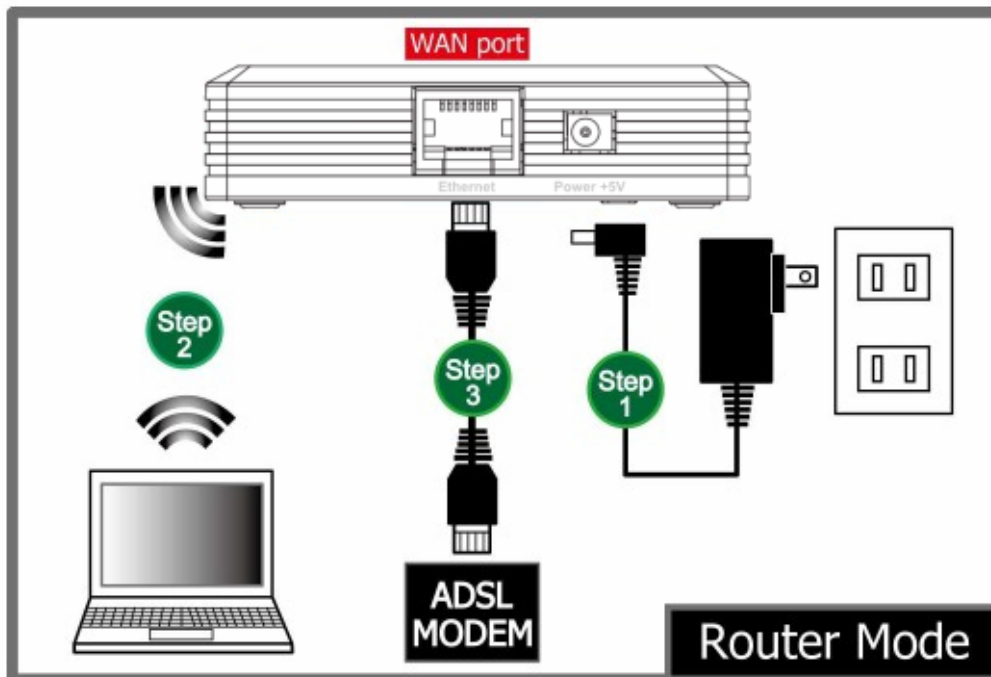
3.1.2 Router Mode

Connect via wireless...

Step1. Power on the wireless router first, connect the Wireless Router with a power to an outlet.

Step2. Then, connect the computer with the wireless router via wireless LAN interface.

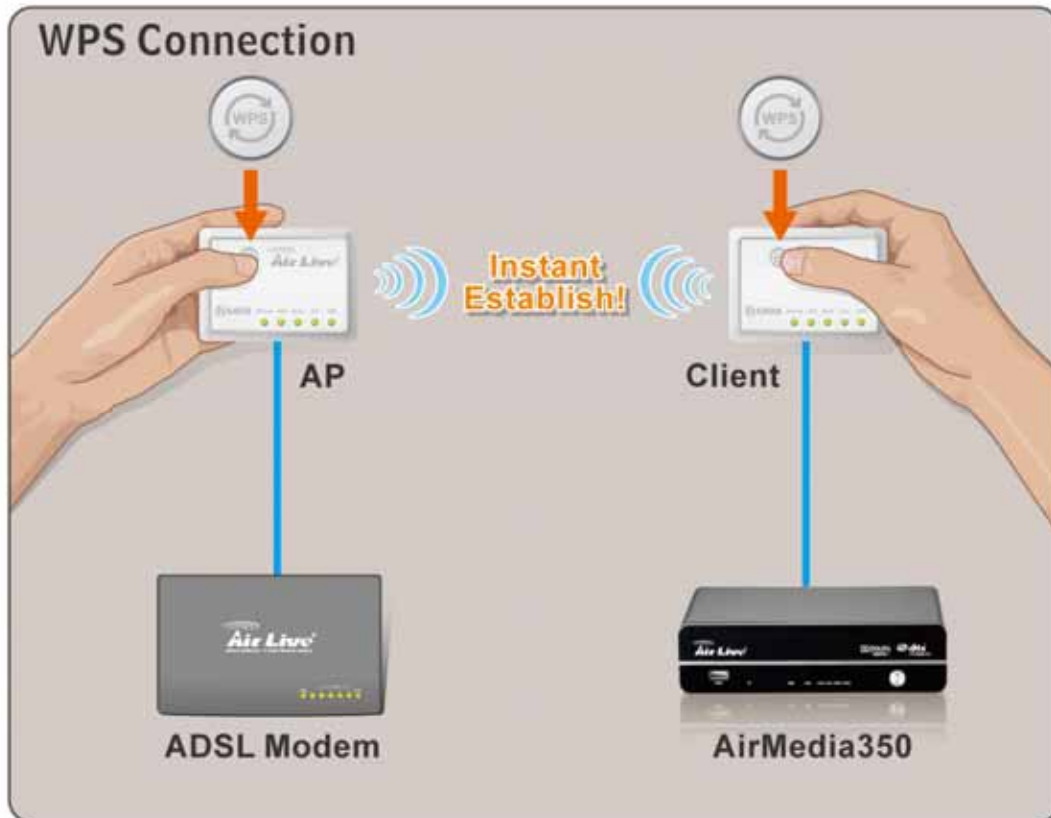
Step3. After make a connection and set up(please refer to TCP/IP Settings> WAN Interface Setup) successfully, connect the ADSL or cable modem with an cable to the Ethernet port(act as WAN port here). If your modem came with a cable, use the supplied cable.



3.1.3 Bridging the Network

Configure one N.MINI as AP and the other as Client...

- Step1. Please set one N.MINI to AP mode and the other N.MINI to Client mode. Using the hardware switch in the back of the APs.
- Step2. Wait for about 2 minutes for both AP to finish reboot
- Step3. Connect the "AP mode" N.MINI to the Internet by Ethernet cable
- Step4. Connect the "Client mode" N.MINI to an electronic device such as PC, game console, media player, or IP Set-top box.
- Step5. Press the WPS push button on the "AP mode" N.MINI until the WPS LED blinks.
- Step6. Then, press the WPS push button on the "Client mode" N.MINI until the WPS LED blinks
- Step7. Wait for 2 minutes for the connection to establish between 2 N.MINIs.



3.2 Login

Step1. Make sure the connection between your computer and Wireless Router setup successfully.

Step2. Start your Web Browser.

Step3. In the Address box, enter the IP address of the Wireless Router, as in this example, which uses the Wireless Router's default IP address:

AP or Router Mode IP	192.168.1.254
Client Mode IP:	192.168.1.253



Step4. After connected successfully, the following screen will show up. Simply enter the username "admin" without password to login(case-sensitive).



After login successfully, please click the Setup Wizard item that provides a primary configuration of this device. You may enter each screen to change the default settings step by step.



3.3 Default Settings

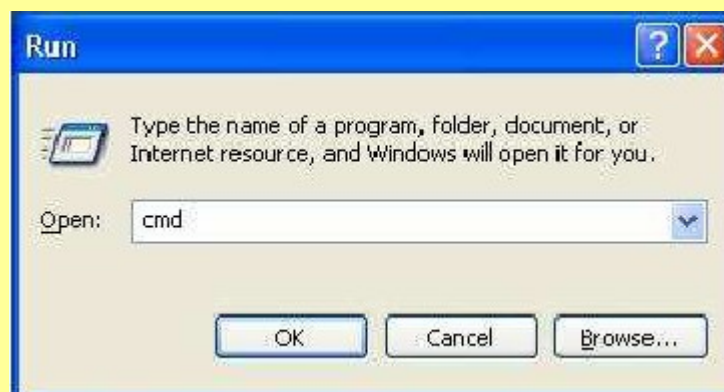
The default settings of N.MINI are listed below:

- AP or Router Mode IP: 192.168.1.254
- Client Mode IP: 192.168.1.253
- Username: admin
- Password: airlive
- SSID: airlive

If you cannot connect...

If the Wireless Router does not respond, please check following:

- Step1. The Wireless Router is properly installed and connection with computer is OK, and it is already powered ON. You can test the connection by using the "Ping" command:
- Step2. Please go to Start>Run...> Enter "cmd" command in the column to open the MS-DOS window.



Step3. Enter the command: ping 192.168.1.254

```

C:\WINDOWS\system32\cmd.exe
C:\Documents and Settings\al1787>ping 192.168.1.254

Pinging 192.168.1.254 with 32 bytes of data:

Reply from 192.168.1.254: bytes=32 time=1ms TTL=64
Reply from 192.168.1.254: bytes=32 time<1ms TTL=64
Reply from 192.168.1.254: bytes=32 time<1ms TTL=64
Reply from 192.168.1.254: bytes=32 time=1ms TTL=64

Ping statistics for 192.168.1.254:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms
  
```



- Step4. If no response is received, either the connection is not working, or your PC's IP address is not compatible with the Wireless Router's IP address. (See next item.)
- Step5. If your PC is using a fixed IP address, its IP address must be within the range 192.168.1.1 to 192.168.1.253 to be compatible with the Wireless Router's default IP Address of 192.168.1.254. Also, the Network Mask must be set to 255.255.255.0. See Chapter 4 - PC Configuration for details on checking your PC's TCP/IP settings.
- Step6. Ensure that your PC and the Wireless Router are on the same network segment. (If you don't have a router, this must be the case.)
- Step7. When set to AP/Client mode, ensure you are using the wired LAN interface, connect the computer by Ethernet cable to the Ethernet port of the Wireless Router.
- Step8. When set to Router mode, ensure you are using the wireless interface, connect the Wireless Router with computer via radio frequency. The Wireless interface can only be used if its configuration matches computer's wireless settings.

3.4 Common Connection Types

3.3.1 Cable Modems

Type	Details	ISP Data required
Dynamic IP Address	Your IP Address is allocated automatically, when you connect to you ISP.	Usually, none. However, some ISP's may require you to use a particular Hostname, Domain name, or MAC (physical) address.
Static (Fixed) IP Address	Your ISP allocates a permanent IP Address to you.	IP Address allocated to you. Some ISP's may also require you to use a particular Hostname, Domain name, or MAC (physical) address.

3.3.2 DSL Modems

Type	Details	ISP Data required
Dynamic IP Address	Your IP Address is allocated automatically, when you connect to you ISP.	None.
Static (Fixed) IP	Your ISP allocates a	IP Address allocated to you.



Address	permanent IP Address to you.	
PPPoE	You connect to the ISP only when required. The IP address is usually allocated automatically.	User name and password.
PPTP	Mainly used in Europe. You connect to the ISP only when required. The IP address is usually allocated automatically, but may be Static (Fixed).	<ol style="list-style-type: none"> 1. PPTP Server IP Address. 2. User name and password. 3. IP Address allocated to you, if Static (Fixed).
L2TP	Mainly used in Europe. You connect to the ISP only when required. The IP address is usually allocated automatically, but may be Static (Fixed).	<ol style="list-style-type: none"> 1. L2TP Server IP Address. 2. User name and password. 3. IP Address allocated to you, if Static (Fixed).

3.3.3 Other Modems (e.g. Broadband Wireless)

Type	Details	ISP Data required
Dynamic IP Address	Your IP Address is allocated automatically, when you connect to you ISP.	None
Static (Fixed) IP Address	Your ISP allocates a permanent IP Address to you.	IP Address allocated to you.



4

Web Configuration

After login successfully, please click the Setup Wizard item that provides a primary configuration of this device. You may enter each screen to change the default settings step by step.

The screenshot shows the Air Live web configuration interface. The top navigation bar is blue and contains the Air Live logo, the website URL www.airlive.com, and the device model **N.MINI 11b/g/n Mini-AP**. A language dropdown menu is set to "English" with an "Apply" button next to it. On the left side, there is a vertical menu with the following items: Setup Wizard (selected), Wireless, TCP/IP Settings, Management, Logout, and Reboot. The main content area is titled "Setup Wizard" and contains the following text:

The setup wizard will guide you to configure access point for first time. Please follow the setup wizard step by step.

Welcome to Setup Wizard. The Wizard will guide you through the following steps. Begin by clicking on Next.

1. Set Wireless Network Name
2. Select Wireless Security Mode

At the bottom right of the main content area, there is a green button labeled "Next>>".

4.1 Setup Wizard

The setup wizard will guide you to configure access point for first time. Please follow the setup wizard step by step.



4.1.1 Router Mode

Setup Wizard

The setup wizard will guide you to configure access point for first time. Please follow the setup wizard step by step.

Welcome to Setup Wizard.

The Wizard will guide you the through following steps. Begin by clicking on Next.

1. WAN Interface Setup

Step 1- WAN Interface Setup

User can select the WAN access type here for internet connection.

1. WAN Interface Setup

This page is used to configure the parameters for Internet network which connects to the WAN port of your Access Point.

WAN Access Type:

User Name:

Password:

WAN Access Type	<p>If the PPPoE be selected, user have to set up the user name and password according to the ISP that provided the related information. User Name: Enter the username that provide by your ISP provider. Maximum input is 32 alphanumeric characters (case sensitive).</p> <p>Password: Enter the password that provide by your ISP provider. Maximum input is 32 alphanumeric characters (case sensitive).</p>
User Name	Enter the username that provide by your ISP provider. Maximum input is 32 alphanumeric characters (case-sensitive).
Password	Enter the password that provide by your ISP provider. Maximum input is 32 alphanumeric characters (case-sensitive).



4.1.2 AP/Client Mode

Setup Wizard

The setup wizard will guide you to configure access point for first time. Please follow the setup wizard step by step.

Welcome to Setup Wizard.

The Wizard will guide you the through following steps. Begin by clicking on Next.

1. Set Wireless Network Name
2. Select Wireless Security Mode

Step 1- Set Wireless Network Name

User can setup the network name of the Wireless Router here.

1. Set Wireless Network Name

You can enter the Wireless Network Name of AP.

Wireless Network Name(SSID):

Wireless Network Name (SSID)	A SSID is referred to a network name because essentially it is a name that identifies a wireless network (case-sensitive).
------------------------------	--

Step 2- Select Wireless Security Mode

User can setup the security here, it is strongly recommended to set up security mode to prevent any unauthorized accessing.

2. Select Wireless Security Mode

This page allows you setup the wireless security. Turn on WEP or WPA by using Encryption Keys could prevent any unauthorized access to your wireless network.

Encryption:

Encryption	<p>Select desired security type from the pull-down menu None, WEP, WPA, WPA2 and WPA2-Mixed. The default setting is None. It is strongly recommended to set up security mode (WEP, WPA, WPA2 and WPA2-Mixed) to prevent any unauthorized accessing.</p> <p>WEP</p> <p>Encryption: <input type="text" value="WEP"/></p> <p>Key Length: <input type="text" value="64-bit"/></p> <p>Key Format: <input type="text" value="Hex"/></p> <p>Key Setting: <input type="text" value="*****"/></p> <p>Key Length: Select key length 64-bit or 128-bit.</p> <p>Key Format:</p> <ul style="list-style-type: none"> Hexadecimal (WEP 64 bits): 10 Hex characters (0~9, a~f). Hexadecimal (WEP 128 bits): 26 Hex characters (0~9, a~f). ASCII (WEP 64 bits): 5 ASCII characters (case-sensitive). ASCII (WEP 128 bits): 13 ASCII characters (case-sensitive). <p>Key Setting: Enter the key in the key setting field.</p> <p>WPA/WPA2/WPA2 Mixed</p> <p>Encryption: <input type="text" value="WPA2 Mixed"/></p> <p>Pre-Shared Key Format: <input type="text" value="Passphrase"/></p> <p>Pre-Shared Key: <input type="text"/></p> <p>Key Length: Select key length 64-bit or 128-bit.</p>
------------	---



	<p>Key Format:</p> <p>Hexadecimal (WEP 64 bits): 10 Hex characters (0~9, a~f).</p> <p>Hexadecimal (WEP 128 bits): 26 Hex characters (0~9, a~f).</p> <p>ASCII (WEP 64 bits): 5 ASCII characters (case-sensitive).</p> <p>ASCII (WEP 128 bits): 13 ASCII characters (case-sensitive).</p> <p>Key Setting: Enter the key in the key setting field.</p>
--	---

4.2 Wireless

4.2.1 Basic Settings

Wireless Basic Settings

This page is used to configure the parameters for wireless LAN clients which may connect to your Access Point. Here you may change wireless encryption settings as well as wireless network parameters.

Disable Wireless LAN Interface

Band:

Mode:

Network Type:

SSID:

Channel Width:

Control Sideband:

Channel Number:

Broadcast SSID:

WMM:

Data Rate:

Associated Clients:

Enable Mac Clone (Single Ethernet Client)

Enable Universal Repeater Mode (Acting as AP and client simultaneously)

SSID of Extended Interface:

<p>Disable Wireless LAN Interface</p>	<p>Check to disable the wireless function. If the wireless LAN interface be disabled, the WLAN LED on the top will be off.</p>																																													
<p>Band</p>	<p>You can choose one mode of the following you need. The default is</p> <p>2.4GHz (B+G+N) mode.</p> <p>2.4GHz (B): 802.11b supported rate only.</p> <p>2.4GHz (G): 802.11g supported rate only.</p> <p>2.4GHz (N): 802.11n supported rate only.</p> <p>2.4GHz (B+G): 802.11b supported rate and 802.11g supported rate.</p> <p>2.4GHz (G+N): 802.11g supported rate and 802.11n supported rate.</p> <p>2.4GHz (B+G+N): 802.11b, 802.11g and 802.11n supported rate.</p>																																													
<p>Mode</p>	<p>Under Router operation mode, user can select AP, WDS, and AP+WDS from the pull-down list. For AP mode, user can select AP, Client, WDS and AP+WDS mode. Under Client mode, there is only Client mode can be selected.</p> <p>Multiple APs</p> <p>This page shows and updates the wireless setting for multiple APs</p> <p>Multiple APs</p> <p><small>This page shows and updates the wireless setting for multiple APs.</small></p> <table border="1" data-bbox="491 1400 1337 1594"> <thead> <tr> <th>No.</th> <th>Enable</th> <th>Band</th> <th>SSID</th> <th>Data Rate</th> <th>Broadcast SSID</th> <th>WMM</th> <th>Access</th> <th>Active Client List</th> </tr> </thead> <tbody> <tr> <td>AP1</td> <td><input type="checkbox"/></td> <td>2.4 GHz (B+G+N)</td> <td>11nRouter1</td> <td>Auto</td> <td>Enabled</td> <td>Enabled</td> <td>LAN+WAN</td> <td>Show</td> </tr> <tr> <td>AP2</td> <td><input type="checkbox"/></td> <td>2.4 GHz (B+G+N)</td> <td>11nRouter2</td> <td>Auto</td> <td>Enabled</td> <td>Enabled</td> <td>LAN+WAN</td> <td>Show</td> </tr> <tr> <td>AP3</td> <td><input type="checkbox"/></td> <td>2.4 GHz (B+G+N)</td> <td>11nRouter3</td> <td>Auto</td> <td>Enabled</td> <td>Enabled</td> <td>LAN+WAN</td> <td>Show</td> </tr> <tr> <td>AP4</td> <td><input type="checkbox"/></td> <td>2.4 GHz (B+G+N)</td> <td>11nRouter4</td> <td>Auto</td> <td>Enabled</td> <td>Enabled</td> <td>LAN+WAN</td> <td>Show</td> </tr> </tbody> </table> <p><input type="button" value="Apply Changes"/> <input type="button" value="Reset"/></p> <p>User can set up the multiple AP here. To enable one of the APs from 1~4, then setup the wireless settings from the pull-down list.</p>	No.	Enable	Band	SSID	Data Rate	Broadcast SSID	WMM	Access	Active Client List	AP1	<input type="checkbox"/>	2.4 GHz (B+G+N)	11nRouter1	Auto	Enabled	Enabled	LAN+WAN	Show	AP2	<input type="checkbox"/>	2.4 GHz (B+G+N)	11nRouter2	Auto	Enabled	Enabled	LAN+WAN	Show	AP3	<input type="checkbox"/>	2.4 GHz (B+G+N)	11nRouter3	Auto	Enabled	Enabled	LAN+WAN	Show	AP4	<input type="checkbox"/>	2.4 GHz (B+G+N)	11nRouter4	Auto	Enabled	Enabled	LAN+WAN	Show
No.	Enable	Band	SSID	Data Rate	Broadcast SSID	WMM	Access	Active Client List																																						
AP1	<input type="checkbox"/>	2.4 GHz (B+G+N)	11nRouter1	Auto	Enabled	Enabled	LAN+WAN	Show																																						
AP2	<input type="checkbox"/>	2.4 GHz (B+G+N)	11nRouter2	Auto	Enabled	Enabled	LAN+WAN	Show																																						
AP3	<input type="checkbox"/>	2.4 GHz (B+G+N)	11nRouter3	Auto	Enabled	Enabled	LAN+WAN	Show																																						
AP4	<input type="checkbox"/>	2.4 GHz (B+G+N)	11nRouter4	Auto	Enabled	Enabled	LAN+WAN	Show																																						
<p>Network Type</p>	<p>If the mode be set to Client mode that the network type can be set to Infrastructure or Ad hoc.</p>																																													
<p>Network Name (SSID)</p>	<p>A SSID is referred to a network name because essentially it is a name that identifies a wireless network(case-sensitive).</p>																																													
<p>Channel Width</p>	<p>This function will be available under 2.4GHz (N), 2.4GHz (G+N), 2.4GHz (B+G+N) mode. Select 20MHz the channel number will</p>																																													



	be form 5~11 and auto; Select 40MHz channel width the channel number will be form 1~11 and auto. Default is 40MHz.														
Control Sideband	This function will be available under 2.4GHz (N), 2.4GHz (G+N), 2.4GHz (B+G+N) mode. Select upper or lower form the pull-down list, default is upper.														
Channel Number	The channel number base on the channel width you select.														
Broadcast SSID	Enabled: This Wireless Router will show its network name(SSID) to stations. Disabled: This Wireless Router will hide the network name to stations. If stations want to connect to this Wireless Router, this Router's network name(SSID) should be known in advance to make a connection.														
WMM	The Wi-Fi Multiple Media function is available under 2.4GHz (B), 2.4GHz (G) and 2.4GHz (B+G) band, and it is disabled under 2.4GHz (N), 2.4GHz (G+N) and 2.4GHz (B+G+N) band.														
Data Rate	There are several data rate that you can select from the pull-down menu.														
Associated Clients	<p>Click Show Active Clients button to show all connected clients.</p> <p>Active Wireless Client Table</p> <p>This table shows the MAC address, transmission, reception packet counters and encrypted status for each associated wireless client.</p> <table border="1"> <thead> <tr> <th>MAC Address</th> <th>Mode</th> <th>Tx Packet</th> <th>Rx Packet</th> <th>Tx Rate (Mbps)</th> <th>Power Saving</th> <th>Expired Time (s)</th> </tr> </thead> <tbody> <tr> <td>00:4f:69:c4:9a:bd</td> <td>11g</td> <td>1153</td> <td>1767</td> <td>54</td> <td>no</td> <td>300</td> </tr> </tbody> </table> <p>Refresh Close</p>	MAC Address	Mode	Tx Packet	Rx Packet	Tx Rate (Mbps)	Power Saving	Expired Time (s)	00:4f:69:c4:9a:bd	11g	1153	1767	54	no	300
MAC Address	Mode	Tx Packet	Rx Packet	Tx Rate (Mbps)	Power Saving	Expired Time (s)									
00:4f:69:c4:9a:bd	11g	1153	1767	54	no	300									
Enable Mac Clone (Single Ethernet Client)	This function will be enabled under Client mode.														
Enable Universal Repeater Mode (Acting as AP and Client simultaneously)	This function will be enabled under AP mode.														



4.2.2 Advanced Settings

Wireless Advanced Settings

These settings are only for more technically advanced users who have a sufficient knowledge about wireless LAN. These settings should not be changed unless you know what effect the changes will have on your Access Point.

Fragment Threshold:	<input type="text" value="2346"/> (256-2346)
RTS Threshold:	<input type="text" value="2347"/> (0-2347)
Beacon Interval:	<input type="text" value="100"/> (20-1024 ms)
Preamble Type:	<input checked="" type="radio"/> Long Preamble <input type="radio"/> Short Preamble
IAPP:	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
Protection:	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
Aggregation:	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
Short GI:	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
WLAN Partition:	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
STBC:	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
20/40MHz Coexist:	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
RF Output Power:	<input checked="" type="radio"/> 100% <input type="radio"/> 70% <input type="radio"/> 50% <input type="radio"/> 35% <input type="radio"/> 15%

Fragment Threshold	Fragmentation mechanism is used for improving the efficiency when high traffic flows along in the wireless network. If the 802.11g MIMO Wireless Router often transmit large files in wireless network, you can enter new Fragment Threshold value to split the packet. The value can be set from 256 to 2346. The default value is 2346.
RTS Threshold	<p>RTS Threshold is a mechanism implemented to prevent the “Hidden Node” problem. If the “Hidden Node” problem is an issue, please specify the packet size. The RTS mechanism will be activated if the data size exceeds the value you set.</p> <p>Warning: Enabling RTS Threshold will cause redundant network overhead that could negatively affect the throughput performance instead of providing a remedy.</p> <p>This value should remain at its default setting of 2347. Should you encounter inconsistent data flow, only minor modifications of this value are recommended.</p>



Beacon Interval	Beacon Interval is the amount of time between beacon transmissions. Before a station enters power save mode, the station needs the beacon interval to know when to wake up to receive the beacon. Range 20-1024 ms, default is 100.
Preamble Type	A preamble is a signal used in wireless environment to synchronize the transmitting timing including Synchronization and Start frame delimiter. You can select Long or Short for the preamble type.
IAPP	Select Enabled or Disabled to execute this function.
Protection	Select Enabled or Disabled to execute the security function.
Aggregation	Select Enabled or Disabled to execute this function.
Short GI	Select Enabled or Disabled to execute this function.
WLAN Partition	Select Enabled or Disabled to execute this function.
STBC	Select Enabled or Disabled to execute this function. The default is Disabled.
20/40MHz Coexist	Select Enabled or Disabled to execute this function. The default is Disabled.
RF Output Power	Select the transmitting power rate 100%, 70%, 50%, 35%, 15%.

4.2.3 Security

Wireless Security Setup

This page allows you setup the wireless security. Turn on WEP or WPA by using Encryption Keys could prevent any unauthorized access to your wireless network.

Select SSID:

Encryption:

Authentication Mode: Enterprise (RADIUS) Personal (Pre-Shared Key)

WPA2 Cipher Suite: TKIP AES

Pre-Shared Key Format:

Pre-Shared Key:

Security Mode	<p>Select desired security type from the pull-down menu Disable, WEP, WPA, WPA2 and WPA2-Mixed. The default setting is Disable. It is strongly recommended to set up security mode (WEP, WPA, WPA2 and WPA2-Mixed) to prevent any unauthorized accessing.</p> <p>Note:</p> <p>WPA and WPA2 only support TKIP and AES as encryption method. Shared Key only supports WEP as encryption method. AUTO(Open/Shared) means AP can accept station connect to it using OPEN-WEP or SHARED-WEP</p> <p>WEP</p> <p>Encryption: <input type="text" value="WEP"/></p> <p>802.1x Authentication: <input type="checkbox"/></p> <p>Authentication: <input type="radio"/> Open System <input type="radio"/> Shared Key <input checked="" type="radio"/> Auto</p> <p>Key Length: <input type="text" value="64-bit"/></p> <p>Key Format: <input type="text" value="Hex (10 characters)"/></p> <p>Encryption Key: <input type="text" value="*****"/></p> <p>802.1x Authentication: Check the box to enable the 802.1x authentication.</p>
---------------	--

Authentication: Select Open System, Shared Key or Auto.

Key Length: select key length 64-bit or 128-bit.

Key Format:

Hexadecimal (WEP 64-bit): 10 Hex characters (0~9, a~f).

Hexadecimal (WEP 128-bit): 26 Hex characters (0~9, a~f).

ASCII (WEP 64-bit): 5 ASCII characters (case-sensitive).

ASCII (WEP 128-bit): 13 ASCII characters (case-sensitive).

Encryption Key: Enter the key in the key setting field.

802.1x Authentication

Encryption:

802.1x Authentication:

Authentication: Open System Shared Key Auto

Key Length: 64 Bits 128 Bits

RADIUS Server IP Address:

RADIUS Server Port:

RADIUS Server Password:

Key Length: select key length 64 Bits or 128 Bits.

RADIUS Server IP Address: Enter the RADIUS Server's IP Address provided by your ISP.

RADIUS Server Port: Enter the RADIUS Server's port number provided by your ISP. The default is 1812.

RADIUS Server Password: Enter the password that the AP shares with the RADIUS Server.

WPA/ WPA2/ WPA2-Mixed

Encryption:

Authentication Mode: Enterprise (RADIUS) Personal (Pre-Shared Key)

WPA Cipher Suite: TKIP AES

WPA2 Cipher Suite: TKIP AES

Pre-Shared Key Format:

Pre-Shared Key:



Personal (Pre-Shared Key)

Authentication Mode: Select Enterprise (RADIUS) or Personal (Pre-Shared Key) mode.

WPA Cipher Suite: Here supported AES only.

WPA2 Cipher Suite: Here supported AES only.

Pre-Shared Key Format: There are two formats for choice to set the Pre-shared key, Passphrase and Hex (64 characters). If Hex is selected, users will have to enter a 64 characters string. For easier configuration, the Passphrase (at least 8 characters) format is recommended.

Pre-Shared Key : Pre-Shared Key serves as a password. Users may key in 8 to 63 characters string if you selected passphrase. Pre-shared key format to set the passwords or leave it blank, in which the 802.1x Authentication will be activated.

Make sure the same password is used on client's end.

Enterprise (RADIUS)

Encryption:	<input type="text" value="WPA-Mixed"/>
Authentication Mode:	<input checked="" type="radio"/> Enterprise (RADIUS) <input type="radio"/> Personal (Pre-Shared Key)
WPA Cipher Suite:	<input type="checkbox"/> TKIP <input checked="" type="checkbox"/> AES
WPA2 Cipher Suite:	<input type="checkbox"/> TKIP <input checked="" type="checkbox"/> AES
RADIUS Server IP Address:	<input type="text"/>
RADIUS Server Port:	<input type="text" value="1812"/>
RADIUS Server Password:	<input type="text"/>

RADIUS Server IP Address: Enter the RADIUS Server's IP Address provided by your ISP.

RADIUS Server Port: Enter the RADIUS Server's port number provided by your ISP. The default is 1812.

RADIUS Server Password: Enter the password that the AP shares with the RADIUS Server.



4.2.4 Access Control

Wireless Access Control

If you choose 'Allowed Listed', only those clients whose wireless MAC addresses are in the access control list will be able to connect to your Access Point. When 'Deny Listed' is selected, these wireless clients on the list will not be able to connect the Access Point.

Wireless Access Control Mode:

MAC Address: Comment:

Current Access Control List:

MAC Address	Comment	Select
<input type="button" value="Delete Selected"/>	<input type="button" value="Delete All"/>	<input type="button" value="Reset"/>

Wireless Access Control Mode	Select Allow Listed or Deny Listed form the pull-down menu to enable access control function. Default setting is Disabled.
MAC Address	Enter the MAC address (12 characters) of a station that is allowed to access this Wireless Router.
Comment	You may enter up to 20 characters as a remark to the previous MAC address.
Current Access Control List	This table displays you the station MAC information.
Delete Selected	Click Delete Selected to delete items which are selected.
Delete All	Click Delete All to delete all the items.
Reset	Click Reset to rest.

4.2.5 WDS Settings

Wireless Distribution System uses wireless media to communicate with other APs, like the Ethernet does. To do this, you must set these APs in the same channel and set MAC address of other APs which you want to communicate with in the table and then enable the



WDS.

To use WDS function:

1. The APs must support WDS function.
2. To set the same SSID (Network name).
3. The channel must be set to the same on the APs.
4. To set the same Wireless MAC address (BSSID) on the APs.
5. To set same security (WEP or WPA) on the APs.

Note

To setup WDS must use the same wireless products (the same model will be better); due to different wireless products might support different WDS settings.

Thus, it is suggested that to use the same wireless products that support WDS function.

WDS Settings

Wireless Distribution System uses wireless media to communicate with other APs, like the Ethernet does. To do this, you must set these APs in the same channel and set MAC address of other APs which you want to communicate with in the table and then enable the WDS.

Enable WDS

MAC Address:

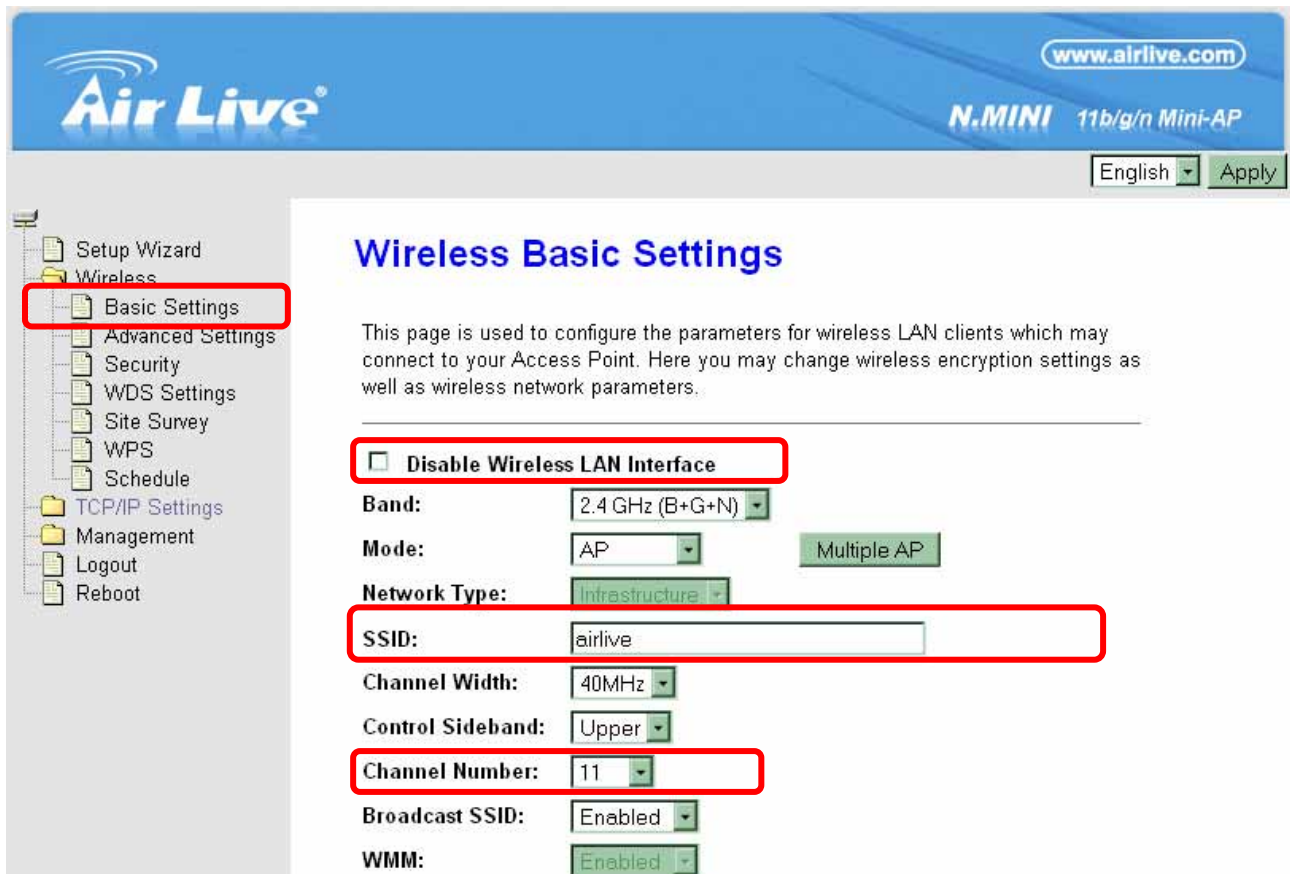
Data Rate:

Comment:

Current WDS AP List:

MAC Address	Tx Rate (Mbps)	Comment	Select
-------------	----------------	---------	--------

Step1. Users would like to set up the WDS function, please go to Wireless > Basic Settings page to set up the Mode into WDS or AP+ WDS (Repeater) mode, and set the APs into the same SSID (Network Name) and Channel Number (If set to WDS mode, the SSID do not need to change). After setting up, please click Apply Changes button to execute.



Wireless Basic Settings

This page is used to configure the parameters for wireless LAN clients which may connect to your Access Point. Here you may change wireless encryption settings as well as wireless network parameters.

Disable Wireless LAN Interface

Band: 2.4 GHz (B+G+N)

Mode: AP Multiple AP

Network Type: Infrastructure

SSID: airlive

Channel Width: 40MHz

Control Sideband: Upper

Channel Number: 11

Broadcast SSID: Enabled

WMM: Enabled

Step2. Then go back to Wireless > WDS Settings page to check Enable WDS box to enable WDS function and then enter Wireless MAC address (please make sure the BSSID of the other WDS supported AP) 12 characters to each other to make the WDS connection. Please click Apply Changes button to execute.



Enable WDS	Check the box to enable the WDS function.																
MAC Address	<p>MAC Address: Enter the Wireless BSSID (MAC) 12 characters of the other wireless AP that you want to connect with. To check your wireless router's MAC address, please go to Status > Wireless Configuration to find your BSSID (Wireless MAC address.)</p> <table border="1"> <thead> <tr> <th colspan="2">Wireless Configuration</th> </tr> </thead> <tbody> <tr> <td>Mode</td> <td>AP+WDS</td> </tr> <tr> <td>Band</td> <td>2.4 GHz (B+G+N)</td> </tr> <tr> <td>SSID</td> <td>LU-MINI</td> </tr> <tr> <td>Channel Number</td> <td>5</td> </tr> <tr> <td>Encryption</td> <td>Disabled(AP), Disabled(WDS)</td> </tr> <tr> <td>BSSID</td> <td>00:4f:69:c1:4f:c0</td> </tr> <tr> <td>Associated Clients</td> <td>1</td> </tr> </tbody> </table>	Wireless Configuration		Mode	AP+WDS	Band	2.4 GHz (B+G+N)	SSID	LU-MINI	Channel Number	5	Encryption	Disabled(AP), Disabled(WDS)	BSSID	00:4f:69:c1:4f:c0	Associated Clients	1
Wireless Configuration																	
Mode	AP+WDS																
Band	2.4 GHz (B+G+N)																
SSID	LU-MINI																
Channel Number	5																
Encryption	Disabled(AP), Disabled(WDS)																
BSSID	00:4f:69:c1:4f:c0																
Associated Clients	1																
Data Rate	Select the data rate form the pull-down list.																
Comment	Enter a description for the device.																
Apply Changes	After completing the settings on this page, click Apply changes button to save the settings.																

<p>Reset</p>	<p>After completing the settings on this page, click Apply changes button to save the settings.</p>
<p>Set Security</p>	<p>Enable the WDS function and then click Set Security button to set up the WDS security.</p> <p>WDS Security Setup</p> <p>This page allows you setup the wireless security for WDS. When enabled, you must make sure each WDS device has adopted the same encryption algorithm and Key.</p> <hr/> <p>Encryption: <input type="text" value="None"/></p> <p>WEP Key Format: <input type="text" value="ASCII (5 characters)"/></p> <p>WEP Key: <input type="text"/></p> <p>Pre-Shared Key Format: <input type="text" value="Passphrase"/></p> <p>Pre-Shared Key: <input type="text"/></p> <p><input type="button" value="Apply Changes"/> <input type="button" value="Reset"/></p> <p>Encryption: Select the encryption type None, WEP 64 bits, WEP 128 bits, and WPA2 from the pull-down menu.</p> <p>WEP</p> <p>WDS Security Setup</p> <p>This page allows you setup the wireless security for WDS. When enabled, you must make sure each WDS device has adopted the same encryption algorithm and Key.</p> <hr/> <p>Encryption: <input type="text" value="WEP 64bits"/></p> <p>WEP Key Format: <input type="text" value="ASCII (5 characters)"/></p> <p>WEP Key: <input type="text" value="*****"/></p> <p>Pre-Shared Key Format: <input type="text" value="Passphrase"/></p> <p>Pre-Shared Key: <input type="text"/></p> <p><input type="button" value="Apply Changes"/> <input type="button" value="Reset"/></p> <p>WEP Key Format: For WEP 64 bits and WEP 128 bits encryption type, the selection of WEP Key Format are Hex and ASCII.</p> <p>WEP Key: If select Hex if you are using hexadecimal numbers (0-9, or A-F).</p> <p>Select ASCII if you are using ASCII characters (case-sensitive).</p> <p>Hexadecimal (WEP 64 bits): 10 Hex characters (0~9, a~f).</p> <p>Hexadecimal (WEP 128 bits): 26 Hex characters (0~9, a~f).</p> <p>ASCII (WEP 64 bits): 5 ASCII characters (case-sensitive).</p>

	<p>ASCII (WEP 128 bits): 13 ASCII characters (case-sensitive).</p> <p>WPA2</p> <h3>WDS Security Setup</h3> <p>This page allows you setup the wireless security for WDS. When enabled, you must make sure each WDS device has adopted the same encryption algorithm and Key.</p> <hr/> <p>Encryption: <input type="text" value="WPA2 (AES)"/></p> <p>WEP Key Format: <input type="text" value="ASCII (5 characters)"/></p> <p>WEP Key: <input type="text" value="*****"/></p> <p>Pre-Shared Key Format: <input type="text" value="Passphrase"/></p> <p>Pre-Shared Key: <input type="text"/></p> <p><input type="button" value="Apply Changes"/> <input type="button" value="Reset"/></p> <p>Pre-Shared Key Format: The Pre-shared Key Format will be enabled when WPA (TKIP) and WPA2 (AES) encryption be selected. There are two formats for choice to set the Pre-shared key, Passphrase and Hex (64 characters). If Hex is selected, users will have to enter a 64 characters string. For easier configuration, the Passphrase (at least 8 characters) format is recommended.</p> <p>Pre-Shared Key: Pre-Shared-Key serves as a password. Users may key in 8 to 63 characters string to set the passwords or leave it blank, in which the 802.1x Authentication will be activated. Make sure the same password is used on client's end.</p>					
<p>Show Statistics</p>	<p>Click Show Statistics to show the current WDS AP table. This table shows the MAC address, transmission packets and errors, reception packets and Tx Rate (Mbps) counters for each configured WDS AP.</p> <h3>WDS AP Table</h3> <p>This table shows the MAC address, transmission, reception packet counters and state information for each configured WDS AP.</p> <table border="1" data-bbox="496 1675 1295 1744"> <thead> <tr> <th>MAC Address</th> <th>Tx Packets</th> <th>Tx Errors</th> <th>Rx Packets</th> <th>Tx Rate (Mbps)</th> </tr> </thead> </table> <p><input type="button" value="Refresh"/> <input type="button" value="Close"/></p> <p>Refresh: Click to renew the counters information. Close: Click to leave the screen.</p>	MAC Address	Tx Packets	Tx Errors	Rx Packets	Tx Rate (Mbps)
MAC Address	Tx Packets	Tx Errors	Rx Packets	Tx Rate (Mbps)		
<p>Current WDS AP List</p>	<p>Here shows the current WDS AP information.</p>					
<p>Delete Selected</p>	<p>Click Delete Selected to delete the selected AP information.</p>					

Delete All	Click Delete All to delete all the items.
Reset	Click Reset to restore the settings.

4.2.6 Site Survey

Wireless Site Survey

This page provides tool to scan the wireless network. If any Access Point or IBSS is found, you could choose to connect it manually when client mode is enabled.

List of APs:

SSID	BSSID	Channel	Type	Encrypt	Signal
LU-301R	00:4f:62:ff:c7:e4	4 (B+G+N)	AP	WPA2-PSK	78
AirMax2	00:4f:62:11:43:fc	3 (B+G)	AP	WPA2-PSK	44
WL-5460AP	00:4f:62:2b:73:cf	11 (B+G)	AP	no	40
WL-5470PoE	00:4f:62:d5:29:e1	6 (B+G)	AP	no	28
Air3G	00:4f:62:d5:29:e2	6 (B+G)	AP	WPA	26
Airlive2	00:4f:62:a4:bc:b6	6 (B+G+N)	AP	WEP	24
Airlive	00:4f:62:11:11:11	9 (B+G)	AP	WEP	20

Refresh	Check this button to renew all the listed access point.
Connect	Under the client mode and select a site that you would like to communicate, and then click the Connect button to make a connection.

4.2.7 WPS

Wi-Fi Protected Setup

This page allows you to change the setting for WPS (Wi-Fi Protected Setup). Using this feature could let your wireless client automatically synchronize its setting and connect to the Access Point in a minute without any hassle.

Disable WPS

ON Configured UnConfigured

[Reset to UnConfigured](#)

Self-PIN Number: 48704793

Push Button Configuration: [Start PBC](#)

[Apply Changes](#) [Reset](#)

Current Key Info:

Authentication	Encryption	Key
Open	None	N/A

Client PIN Number: [Start PIN](#)

Disable WPS	Check the box to disable the WPS function, default setting is enabled.
WPS Status	Here shows the current status of the WPS function. Default setting is Configured, click Reset to UnConfigured to re-configured the WPS connection.
Self-PIN Number	Here shows the 8-digit numbers PIN code of the router itself. Enter the Self-PIN Number to client (Registrar) end and click the PIN button at the client end to make a WPS connection. It will connect with the wireless router within two minutes and get IP address.
Push Button Configuration	Click Start PBC button (or press the physical WPS button on the Wireless Router once), meanwhile, the client should also click the PBC button simultaneously within 2 minutes.
Current Key Info	This table shows the security status of the Wireless Router. If user would like to set up the security, please go to Wireless > Security.
Client PIN Number	Enter the client (Enrollee) PIN code into the blank field then click



	the Start PIN button to make a WPS connection with client. Then, the wireless router will connect to client within 2 minutes and get IP address.
--	---

4.2.8 Schedule

Wireless Schedule

This page allows you setup the wireless schedule rule. Please do not forget to configure system time before enable this feature.

Enable Wireless Schedule

Days:

Everyday Sun Mon Tue Wed Thu Fri Sat

Time:

24 Hours From : To :

Enable Wireless Schedule	Check the box to enable the schedule function. Set up the time to schedule the wireless access rule. Select the day and time you want to enable the wireless function.
--------------------------	--



4.3 TCP/IP Settings

4.3.1 LAN Interface

LAN Interface Setup

This page is used to configure the parameters for local area network which connects to the LAN port of your Access Point. Here you may change the setting for IP address, subnet mask, DHCP, etc..

IP Address:
Subnet Mask:
Default Gateway:
DHCP:
DHCP Client Range: -
Static DHCP:
Domain Name:
802.1d Spanning Tree:
Clone MAC Address:

IP Address	Shows the IP address of the Wireless Router. Default IP address is 192.168.1.254 (Router/AP mode) or 192.168.1.253 (Client Mode).
Subnet Mask	The subnet mask of the Wireless Router (Default subnet mask is 255.255.255.0.)
Default Gateway	Enter the Gateway IP address here.
DHCP	<p>Disable: Select to disable this Wireless Router to distribute IP addresses to connected clients.</p> <p>Server: Select to enable this Wireless Router to distribute IP Addresses (DHCP Server) to connected clients. And the following field will be activated for you to enter the starting IP address.</p>
DHCP Client Range	The starting address of this local IP network address pool. The pool is a piece of continuous IP address segment, the device will distribute IP addresses from 192.168.1.100 to 192.168.1.200 to all the computers in the network that request IP addresses from

DHCP server (Router). The end IP address maximum is 253.

Note:

If “Continuous IP address pool starts” is set at 192.168.1.1 and the “ Number of IP address in pool end” is 253, the device will distribute IP addresses from 192.168.1.100 to 192.168.1.253 to all the computers in the network that request IP addresses from DHCP server (Router).

Click **Show Client** button to show Active DHCP Client Table. The table shows assigned IP address, MAC address and time expired for each client.

Active DHCP Client Table

This table shows the assigned IP address, MAC address and time expired for each DHCP leased client.

IP Address	MAC Address	Time Expired(s)
192.168.1.100	00:4f:69:c4:9a:bd	857482

Refresh: Click this button to refresh the table.
 Close: Click this button to close the window.

Static DHCP

Check the box to enable the Static DHCP function, default setting is disabled.

When set to enabled, user can click **Set Static DHCP** button to set the Static DHCP function.

Static DHCP Setup

This page allows you reserve IP addresses, and assign the same IP address to the network device with the specified MAC address any time it requests an IP address. This is almost the same as when a device has a static IP address except that the device must still request an IP address from the DHCP server.

Enable Static DHCP

IP Address:

MAC Address:

Comment:

Static DHCP List:

IP Address	MAC Address	Comment	Select

IP Address: Enter the fixed IP address that DHCP server assigned to a certain connected station.

MAC Address: Enter the MAC address of a certain station, and then the DHCP server will to distribute a fixed IP address to the



	<p>station automatically once they connected.</p> <p>Comment: You can enter a comment to description above IP address or MAC address.</p> <p>Apply Changes: After completing the settings on this page, click Apply changes button to save the settings.</p> <p>Reset: Click Reset to restore to default values.</p> <p>Static DHCP List: Here shows the static IP address that have been assigned according to the MAC address.</p> <p>Delete Selected: Click Delete Selected to delete items which are selected.</p> <p>Delete All: Click Delete All button to delete all the items.</p> <p>Reset: Click Reset button to rest.</p>
Domain Name	Enter the network area name here.
802.1d Spanning Tree	Select Disabled or Enabled form the pull-down list.
Clone MAC Address	Your ISP may require a particular MAC address in order for you to connect to the Internet. This MAC address is the PC's MAC address that your ISP had originally connected your Internet connection to. Type in the MAC address to replace the WAN MAC address with the MAC address of that PC.



4.3.2 WAN Interface

WAN Interface Setup

This page is used to configure the parameters for Internet network which connects to the WAN port of your Access Point. Here you may change the access method to static IP, DHCP, PPPoE, PPTP or L2TP by click the item value of WAN Access type.

WAN Access Type:

Host Name:

MTU Size: (1400-1492 bytes)

Attain DNS Automatically
 Set DNS Manually

DNS 1:

DNS 2:

DNS 3:

Clone MAC Address:

Enable UPnP
 Enable IGMP Proxy
 Enable Ping Access on WAN
 Enable Web Server Access on WAN
 Enable IPsec pass through on VPN connection
 Enable PPTP pass through on VPN connection
 Enable L2TP pass through on VPN connection

WAN Access Type	<p>DHCP Client</p> <p> WAN Access Type: <input type="text" value="DHCP Client"/> </p> <p> Host Name: <input type="text" value="11nRouter"/> </p> <p> MTU Size: <input type="text" value="1492"/> (1400-1492 bytes) </p> <p>If the DHCP Client connection be selected, the PC will obtain the IP address automatically.</p>
-----------------	--



Host Name: Enter the network area name in the column.

MTU Size: The most appropriate MTU (Maximum Transmission Unit) namely the maximum packet size, the default value is 1492 for your application. Reducing the packet size can help connecting to certain web sites or speeding up packet transfer rate. If the incorrect packet size is entered, you may not be able to open certain web sites.

Static IP

WAN Access Type:	<input type="text" value="Static IP"/>
IP Address:	<input type="text" value="192.168.0.19"/>
Subnet Mask:	<input type="text" value="255.255.255.0"/>
Default Gateway:	<input type="text" value="192.168.0.254"/>
MTU Size:	<input type="text" value="1500"/> (1400-1500 bytes)
DNS 1:	<input type="text" value="192.168.0.254"/>
DNS 2:	<input type="text" value="168.95.1.1"/>
DNS 3:	<input type="text"/>

If the Static IP be selected, user have to set up the IP address, subnet mask and default gateway according to the ISP (Internet Service Provider) that provided the related information.

IP Address: Enter the WAN IP address provided by your ISP here.

Subnet Mask: Enter the subnet mask here. Default Gateway: Enter the default gateway IP address provided by your ISP here.

MTU Size: The most appropriate MTU (Maximum Transmission Unit) namely the maximum packet size. Reducing the packet size can help connecting to certain web sites or speeding up packet transfer rate. If the incorrect packet size is entered, you may not be able to open certain web sites.

DNS 1: Enter the DNS server IP address(es) provided by your ISP, or you can specify your own preferred DNS server IP address(es).

DNS 2/ DNS 3: These servers are optional. You can enter another DNS server's IP address as a backup. DNS 2 and 3 servers will be used when the DNS 1 server fails.

PPPoE	
WAN Access Type:	<input type="text" value="PPPoE"/>
User Name:	<input type="text" value="12345678@hinet.net"/>
Password:	<input type="password" value="●●●●●●●●"/>
Service Name:	<input type="text" value="Hinet"/>
Connection Type:	<input type="text" value="Continuous"/> <input type="button" value="Connect"/> <input type="button" value="Disconnect"/>
Idle Time:	<input type="text" value="5"/> (1-1000 minutes)
MTU Size:	<input type="text" value="1452"/> (1360-1492 bytes)
<input type="radio"/> Attain DNS Automatically <input checked="" type="radio"/> Set DNS Manually	
DNS 1:	<input type="text" value="192.168.0.254"/>
DNS 2:	<input type="text" value="168.95.1.1"/>
DNS 3:	<input type="text"/>

If the PPPoE be selected, user has to set up the user name and password according to the ISP that provided the related information.

User Name: Enter the username that provide by your ISP provider. Maximum input is 32 alphanumeric characters (case sensitive).

Password: Enter the password that provide by your ISP provider. Maximum input is 32 alphanumeric characters (case sensitive).

Service Name: Enter the Internet service provider name in the column.

Connection Type: Select the connection type Continuous, Connect on Demand or Manual from the pull-down menu. If selected Manual user can click Connect button to make a connection.

Idle Time: It represents that the device will idle after the minutes you set. The time must be set between 1~1000 minutes. Default value of idle time is 5 minutes. This function will be available when the Connection Type is selected to Connect on Demand.

MTU Size: The most appropriate MTU (Maximum Transmission Unit) namely the maximum packet size, the default value is 1452 for your application. Reducing the packet size can help connecting to certain web sites or speeding up packet transfer rate. If the incorrect packet size is entered, you may not be able to open certain web sites.

	<p>PPTP</p> <p>WAN Access Type: <input type="text" value="PPTP"/></p> <p>IP Address: <input type="text" value="172.1.1.2"/></p> <p>Subnet Mask: <input type="text" value="255.255.255.0"/></p> <p>Server IP Address: <input type="text" value="172.1.1.1"/></p> <p>User Name: <input type="text"/></p> <p>Password: <input type="password"/></p> <p>Connection Type: <input type="text" value="Continuous"/> <input type="button" value="Connect"/> <input type="button" value="Disconnect"/></p> <p>Idle Time: <input type="text" value="5"/> (1-1000 minutes)</p> <p>MTU Size: <input type="text" value="1460"/> (1400-1460 bytes)</p> <p><input type="checkbox"/> Request MPPE Encryption <input type="checkbox"/> Request MPPC Compression</p> <p>If the PPTP be selected, user has to set up the server IP address, user name and password according to the ISP that provided the related information.</p> <p>IP Address: Enter the WAN IP address provided by your ISP here.</p> <p>Subnet Mask: Enter the subnet mask here.</p> <p>Server IP Address: Enter the PPTP Server IP Address in this column.</p> <p>User Name: Maximum input is 20 alphanumeric characters (case sensitive).</p> <p>Password: Maximum input is 32 alphanumeric characters (case sensitive).</p> <p>Connection Type: Select the connection type Continuous, Connect on Demand or Manual from the pull-down menu. If selected Manual user can click Connect button to make a connection.</p> <p>Idle Time: It represents that the device will idle after the minutes you set. The time must be set between 1~1000 minutes. Default value of idle time is 5 minutes. This function will be available when the Connection Type is selected to Connect on Demand.</p> <p>MTU Size: The most appropriate MTU (Maximum Transmission Unit) namely the maximum packet size, the default value is 1460 for your application. Reducing the packet size can help connecting to certain web sites or speeding up packet transfer rate. If the incorrect packet size is entered, you may not be able to open certain web sites.</p>
--	--



	<p>L2TP</p> <p>WAN Access Type: <input type="text" value="L2TP"/></p> <p>IP Address: <input type="text" value="172.1.1.2"/></p> <p>Subnet Mask: <input type="text" value="255.255.255.0"/></p> <p>Server IP Address: <input type="text" value="172.1.1.1"/></p> <p>User Name: <input type="text"/></p> <p>Password: <input type="text"/></p> <p>Connection Type: <input type="text" value="Continuous"/> <input type="button" value="Connect"/> <input type="button" value="Disconnect"/></p> <p>Idle Time: <input type="text" value="5"/> (1-1000 minutes)</p> <p>MTU Size: <input type="text" value="1460"/> (1400-1460 bytes)</p> <p>If the L2TP be selected, user has to set up the server IP address, user name and password according to the ISP that provided the related information.</p> <p>IP Address: Enter the WAN IP address provided by your ISP here.</p> <p>Subnet Mask: Enter the subnet mask here.</p> <p>Server IP Address: Enter the L2TP Server IP Address in this column.</p> <p>User Name: Maximum input is 20 alphanumeric characters (case sensitive).</p> <p>Password: Maximum input is 32 alphanumeric characters (case sensitive).</p> <p>Connection Type: Select the connection type Continuous, Connect on Demand or Manual from the pull-down menu. If selected Manual user can click Connect button to make a connection.</p> <p>Idle Time: It represents that the device will idle after the minutes you set. The time must be set between 1~1000 minutes. Default value of idle time is 5 minutes. This function will be available when the Connection Type is selected to Connect on Demand.</p> <p>MTU Size: The most appropriate MTU (Maximum Transmission Unit) namely the maximum packet size, the default value is 1460 for your application. Reducing the packet size can help connecting to certain web sites or speeding up packet transfer rate. If the incorrect packet size is entered, you may not be able to open certain web sites.</p>
<ul style="list-style-type: none"> ● Attain DNS Automatically 	<p>Select to Attain DNS Automatically or select Set DNS Manually to set the DNS server IP address at the following DNS 1~3</p>



<ul style="list-style-type: none"> ● Set DNS Manually ● DNS 1 ● DNS 2 ● DNS3 	<p>columns. Default setting is Attain DNS Automatically.</p> <p>Enter the DNS server IP address(es) provided by your ISP, or you can specify your own preferred DNS server IP address(es).</p> <p>DNS 2 server is optional. You can enter another DNS server's IP address as a backup. DNS 2 server will be used when the DNS 1 server fails.</p>
Clone MAC address	Your ISP may require a particular MAC address in order for you to connect to the Internet. This MAC address is the PC's MAC address that your ISP had originally connected your Internet connection to. Type in this Clone MAC address in this section to replace the WAN MAC address with the MAC address of that PC.
Enable uPNP...	Check to enable the listed functions.
Apply Changes	After completing the settings on this page, click Apply changes button to save the settings.
Reset	Click Reset to restore to default values.

4.4 Firewall

4.4.1 Port Filtering

Port Filter Settings

Entries in this table are used to restrict certain types of data packets from your local network to Internet through the Gateway. Use of such filters can be helpful in securing or restricting your local network.

Enable Port Filtering

Port Range: - Protocol: Comment:

Current Filter Table:

Port Range	Protocol	Comment	Select
------------	----------	---------	--------



Enable Port Filtering	Check to enable Port Filtering function.
Port Range	Enter the beginning of the range of port numbers used by the service. If the service uses a single port number, enter it in both the start and finish fields.
Protocol	Select the protocol (TCP, UDP or Both) used to the remote system or service.
Comment	You may key in a description MAC address.
Apply Changes	After completing the settings on this page, click Apply Changes button to save the settings.
Reset	Click Reset button to restore to default values.
Current Filter Table	Shows the current Port Forwarding information.
Delete Selected	Click Delete Selected button to delete items which are selected.
Delete All	Click Delete All button to delete all the items.
Reset	Click Reset button to rest.

4.4.2 IP Filtering

IP Filtering

Entries in this table are used to restrict certain types of data packets from your local network to Internet through the Gateway. Use of such filters can be helpful in securing or restricting your local network.

Enable IP Filtering

Local IP Address: Protocol: Comment:

Current Filter Table:

Local IP Address	Protocol	Comment	Select
------------------	----------	---------	--------

Enable IP Filtering	Check to enable IP filtering function.
---------------------	--



Local IP Address	Enter the local computer's IP address.
Protocol	Select the protocol (TCP, UDP or Both) used to the remote system or service.
Comment	You may key in a description for the port range.
Apply Changes	After completing the settings on this page, click Apply Changes button to save the settings.
Reset	Click Reset button to restore to default values.
Current Filter Table	Shows the current IP filter information.
Delete Selected	Click Delete Selected button to delete items which are selected.
Delete All	Click Delete All button to delete all the items.
Reset	Click Reset button to rest.

4.4.3 MAC Filtering

MAC Filtering

Entries in this table are used to restrict certain types of data packets from your local network to Internet through the Gateway. Use of such filters can be helpful in securing or restricting your local network.

Enable MAC Filtering

MAC Address: Comment:

Apply Changes

Reset

Current Filter Table:

MAC Address	Comment	Select
-------------	---------	--------

Delete Selected

Delete All

Reset

Enable MAC Filtering	Check to enable MAC filtering function.
MAC Address	Enter the client MAC address in the field.
Comment	You may key in a description MAC address.



Apply Changes	After completing the settings on this page, click Apply Changes button to save the settings.
Reset	Click Reset button to restore to default values.
Current Filter Table	Shows the current MAC filter information.
Delete Selected	Click Delete Selected button to delete items which are selected.
Delete All	Click Delete All button to delete all the items.
Reset	Click Reset button to rest.

4.4.4 Port Forwarding

Enable Port Forwarding

Entries in this table allow you to automatically redirect common network services to a specific machine behind the NAT firewall. These settings are only necessary if you wish to host some sort of server like a web server or mail server on the private local network behind your Gateway's NAT firewall.

Enable Port Forwarding

IP Address: Protocol: Port Range: -

Comment:

Current Port Forwarding Table:

Local IP Address	Protocol	Port Range	Comment	Select
------------------	----------	------------	---------	--------

Enable Port Forwarding	Check to enable Port Forwarding function.
IP Address	Enter the IP address in the field.
Protocol	Select the protocol (TCP, UDP or Both) used to the remote system or service.
Port Range	For TCP and UDP Services, enter the beginning of the range of port numbers used by the service. If the service uses a



	single port number, enter it in both the start and finish fields.
Comment	You may key in a description MAC address.
Apply Changes	After completing the settings on this page, click Apply Changes button to save the settings.
Reset	Click Reset button to restore to default values.
Current Port Forwarding Table	Shows the current Port Forwarding information.
Delete Selected	Click Delete Selected button to delete items which are selected.
Delete All	Click Delete All button to delete all the items.
Reset	Click Reset button to rest.

4.4.5 URL Filtering

URL Filtering

URL filter is used to deny LAN users from accessing the internet. Block those URLs which contain keywords listed below.

Enable URL Filtering

URL Address:

Current Filter Table:

URL Address	Select
-------------	--------

Enable URL Filtering	Check to enable URL filtering function.
URL Address	Enter the URL address in the field
Apply Changes	After completing the settings on this page, click Apply Changes button to save the settings.



Reset	Click Reset button to restore to default values.
Current Filter Table	Shows the current URL address filter information.
Delete Selected	Click Delete All button to delete all the items.
Reset	Click Reset button to rest.

4.4.6 DMZ

DMZ

A Demilitarized Zone is used to provide Internet services without sacrificing unauthorized access to its local private network. Typically, the DMZ host contains devices accessible to Internet traffic, such as Web (HTTP) servers, FTP servers, SMTP (e-mail) servers and DNS servers.

Enable DMZ

DMZ Host IP Address:

Enable DMZ	Check the box to enable DMZ function. If the DMZ Host Function is enabled, it means that you set up DMZ host at a particular computer to be exposed to the Internet so that some applications/software, especially Internet / online game can have two way connections.
DMZ Host IP Address	Enter the IP address of a particular host in your LAN which will receive all the packets originally going to the WAN port/Public IP address above. Note You need to give your LAN PC clients a fixed/static IP address for DMZ to work properly.
Apply Changes	After completing the settings on this page, click Apply Changes button to save the settings.
Reset	Click Reset button to restore to default values



4.4.7 VLAN

VLAN Settings

Entries in below table are used to config vlan settings. VLANs are created to provide the segmentation services traditionally provided by routers. VLANs address issues such as scalability, security, and network management.

Enable VLAN

Enable	Ethernet/Wireless	WAN/LAN	Tag	VID(1~4090)	Priority	CFI
<input type="checkbox"/>	Wireless Primary AP	LAN	<input type="checkbox"/>	1	0	<input checked="" type="checkbox"/>
<input type="checkbox"/>	Virtual AP1	LAN	<input type="checkbox"/>	1	0	<input checked="" type="checkbox"/>
<input type="checkbox"/>	Virtual AP2	LAN	<input type="checkbox"/>	1	0	<input checked="" type="checkbox"/>
<input type="checkbox"/>	Virtual AP3	LAN	<input type="checkbox"/>	1	0	<input checked="" type="checkbox"/>
<input type="checkbox"/>	Virtual AP4	LAN	<input type="checkbox"/>	1	0	<input checked="" type="checkbox"/>
<input type="checkbox"/>	Ethernet Port5	WAN	<input type="checkbox"/>	1	0	<input checked="" type="checkbox"/>

Apply Changes

Reset

Enable VLAN	<p>VLAN(Virtual Local Area Network) refers to a group of logically networked devices on one or more LANs that are configured so that they can communicate as if they were attached to the same wire, when in fact they are located on different LAN segments. Because VLANs are based on logical instead of physical connections, it is very flexible for user/host management.</p> <p>Enable this function to setup the virtual local area network.</p>
-------------	--



4.5 QoS

Use this section to configure QoS. The QoS settings improve your online gaming experience by ensuring that your game traffic is prioritized over other network traffic, such as FTP or Web.

QoS Setup

Entries in this table improve your online gaming experience by ensuring that your game traffic is prioritized over other network traffic, such as FTP or Web.

Enable QoS

Automatic Uplink Speed

Manual Uplink Speed (Kbps):

Automatic Downlink Speed

Manual Downlink Speed (Kbps):

QoS Rule Setting:

Address Type:

IP MAC

Local IP Address:

-

MAC Address:

Mode:

Uplink Bandwidth (Kbps):

Downlink Bandwidth (Kbps):

Comment:

Current

QoS Rules

Table:

Local IP Address	MAC Address	Mode	Uplink Bandwidth	Downlink Bandwidth	Comment	Select
------------------	-------------	------	------------------	--------------------	---------	--------



Enable QoS	This function improves online gaming experience by ensuring that game traffic is prioritized over other network traffic, such as FTP or Web.
Automatic Uplink/Download Speed	Check the box to enable the automatic uplink/ download speed function.
Manual Uplink/Download Speed	You can manually enter the uplink/ download transmission rate in the blank field.
Address Type	Select IP or MAC address type.
Local IP address MAC address	Depend on the address type that selected, user can enter the IP address or MAC address of client to set up the bandwidth of the transmission.
Mode	Select Guaranteed minimum bandwidth or Restricted maximum bandwidth modes.
Uplink Bandwidth (Kbps)	Enter the Uplink Bandwidth (Kbps) in the column.
Downlink Bandwidth (Kbps)	Enter the Downlink Bandwidth (Kbps) in the column.
Comment	Enter the note for the setting.



4.6 Route Setup

Routing Setup

This page is used to setup dynamic routing protocol or edit static route entry.

Enable Dynamic Route

NAT: Enabled Disabled

Transmit: Disabled RIP 1 RIP 2

Receive: Disabled RIP 1 RIP 2

Apply Changes

Reset

Enable Static Route

IP Address:

Subnet Mask:

Gateway:

Metric:

Interface:

Apply Changes

Reset

Show Route Table

Static Route Table:

Destination IP Address	Netmask	Gateway	Metric	Interface	Select
------------------------	---------	---------	--------	-----------	--------

Delete Selected

Delete All

Reset

Enable Dynamic Route	Dynamic routing performs the same function as static routing except it is steadier. Dynamic routing allows routing tables in routers to change as the possible routes change. There are several protocols used to support dynamic routing including RIP and OSPF.
NAT	Network Address Translation (NAT) selects to enable or disable this function.
Transmit	Select to enable or disable RIP protocol for transmit.
Receive	Select to enable or disable RIP protocol for receive.



Enable Static Route	<p>If you connect several routers with this Wireless Router, you may need to set up a predefined routing rule to have more effective network topology/traffic, this is called static route between those routers and the Wireless Router.</p> <p>To set static routers, enter the settings including route IP address, route mask, route gateway and the route Interface from LAN or WAN.</p>
IP Address	Set up the IP address that would like to send the packets pass through.
Subnet Mask	Set up the Subnet Mask that would like to send the packets pass through.
Gateway	Set up the gateway that would like to send the packets pass through.
Metric	<p>It is used by a router to make routing decisions.</p> <p>The metrics used by a router to make routing decisions. It is typically one of many fields in a routing table. Router metrics can contain any number of values that help the router determine the best route among multiple routes to a destination. A router metric typically based on information like path length, bandwidth, load, hop count, path cost, delay, Maximum Transmission Unit (MTU), reliability and communications cost.</p>
Interface	Select the interface of the setting path.

4.7 Management

4.7.1 Status

This page shows the current Wireless Router settings information.

Access Point Status

This page shows the current status and some basic settings of the device.

System	
Uptime	0day0h59m29s
Firmware Version	v71.11.0.0.1e_b1
Build Time	Jul 9 14:00:50 CST 2010
Wireless Configuration	
Mode	AP+WDS
Band	2.4 GHz (B+G+N)
SSID	LU-MINI
Channel Number	5
Encryption	Disabled(AP), Disabled(WDS)
BSSID	00:4f:69:c1:4f:c0
Associated Clients	1
WAN Configuration	
Attain IP Protocol	PPPoE Disconnected
IP Address	0.0.0.0
Subnet Mask	0.0.0.0
Default Gateway	0.0.0.0
MAC Address	00:4f:69:c1:4f:c5

4.7.2 Statistics

This page shows the packet counters for transmission and reception regarding to wireless and Ethernet networks.

Statistics

This page shows the packet counters for transmission and reception regarding to wireless and Ethernet networks.

Wireless LAN	<i>Sent Packets</i>	9127
	<i>Received Packets</i>	120095
Ethernet WAN	<i>Sent Packets</i>	285
	<i>Received Packets</i>	0

Refresh



4.7.3 Dynamic DNS

Dynamic DNS Setting

Dynamic DNS is a service, that provides you with a valid, unchanging, internet domain name (an URL) to go with that (possibly everchanging) IP-address.

Enable DDNS

Service Provider :

Domain Name :

User Name/Email:

Password/Key:

Note:

For TZO, you can have a 30 days free trial [here](#) or manage your TZO account in [control panel](#)

For DynDNS, you can create your DynDNS account [here](#)

Enable DDNS	Check to enable the DDNS function.
Service Provider	Select the desired DDNS Service Provider DynDNS or TZO from the pull-down list.
Domain Name	Here shows the domain name of the service provider.
User Name/Email	Enter your email that you registered in service provider website. (You can refer to below Note information to apply a account form the service provider website.)
Password/Key	Enter your passwords that you registered in service provider website. Maximum input is 30 alphanumeric characters (case sensitive).
Apply Changes	After completing the settings on this page, click Apply Changes button to save the settings.
Reset	Click Reset button to restore to default values.



4.7.4 Time Zone Setting

Time Zone Setting

You can maintain the system time by synchronizing with a public time server over the Internet.

Current Time : Yr Mon Day Hr Mn Sec

Time Zone Select :

Enable NTP client update

Automatically Adjust Daylight Saving

NTP server :

(Manual IP Setting)

Current Time	Enter the current time of this wireless router or click the Copy Computer Time button to synchronize the time with the connected computer automatically.
Time Zone Select	Select the local time zone from the pull-down menu.
Enable NTP client update	Check to enable NTP (Network Time Protocol Server) client update function.
Automatically Adjust Daylight Saving	Check the box to enable this function.
NTP server Manual IP Setting	You may choose to select NTP server from the pull-down menu or enter an IP address of a specific server manually.
Apply Changes	After completing the settings on this page, click Apply Changes button to save current settings.
Refresh	Click Refresh button to renew current time.

4.7.5 Denial of Service

Denial of Service

A denial-of-service (DoS) attack is characterized by an explicit attempt by hackers to prevent legitimate users of a service from using that service.

Enable DoS Prevention

- Whole System Flood: SYN Packets/Second
- Whole System Flood: FIN Packets/Second
- Whole System Flood: UDP Packets/Second
- Whole System Flood: ICMP Packets/Second
- Per-Source IP Flood: SYN Packets/Second
- Per-Source IP Flood: FIN Packets/Second
- Per-Source IP Flood: UDP Packets/Second
- Per-Source IP Flood: ICMP Packets/Second
- TCP/UDP PortScan Sensitivity
- ICMP Smurf
- IP Land
- IP Spoof
- IP TearDrop
- PingOfDeath
- TCP Scan
- TCP SynWithData
- UDP Bomb
- UDP EchoChargen

Select ALL

Clear ALL

Enable Source IP Blocking

Block time (sec)

Apply Changes

<p>Enable DoS Prevention</p>	<p>DoS (Denial of Service) attacks can flood your Internet connection with invalid packets and connection requests, using so much bandwidth and so many resources that Internet access becomes unavailable. The Wireless Router incorporates protection against DoS attacks. This screen allows you to configure DoS protection.</p>
------------------------------	--



	Check the box to enable the DoS settings.
Select All	After you enabled the DoS prevention, you can click to select all DoS preventions.
Clear All	After you enabled the DoS prevention, you can click to uncheck all DoS preventions.
Apply Changes	After completing the settings on this page, click Apply Changes button to save current settings.

4.7.6 Logs

System Log

This page can be used to set remote log server and show the system log.

Enable Log
 system all Wireless DoS
 Enable Remote Log Log Server IP Address:



Enable Log	Check to enable logging function.
System all	Activates all logging functions.
Wireless	Only logs related to the wireless LAN will be recorded.
DoS	Only logs related to the DoS protection will be recorded.
Enable Remote Log	Only logs related to the Remote control will be recorded.
Log Server IP address	Only logs related to the server will be recorded.
Apply Changes	After completing the settings on this page, click Apply Changes button to save current settings.
Refresh	Click Refresh button to renew the logs.
Clear	Click Clear button to delete the logs.

4.7.7 Upgrade Firmware

Upgrade Firmware

This page allows you upgrade the Access Point firmware to new version. Please note, do not power off the device during the upload because it may crash the system.

Firmware Version: v71.11.0.0.1e_b1

Select File:

Select File	Click the Browse button to find and open the firmware file (the browser will display to correct file path.)
Upload	Click the Upload button to perform.
Reset	Click Reset button to restore to default values.



4.7.8 Save /Reload Settings

Save/Reload Settings

This page allows you save current settings to a file or reload the settings from the file which was saved previously. Besides, you could reset the current configuration to factory default.

Save Settings to File:

Load Settings from File:

Reset Settings to Default:

Save Settings to File	Click the Save button to save the current settings file in the PC.
Load Settings form File	Click the Browse button to find and open the previous saved file (the browser will display to correct file path.) Then, click Upload button to upload the previous file.
Reset Settings to Default	Click Reset button to set the device back to default settings.

4.7.9 Password

Password Setup

This page is used to set the account to access the web server of Access Point. Empty user name and password will disable the protection.

User Name:

New Password:

Confirmed Password:



User Name	Key in a new login user name in the blank field. User can empty the user name and password columns to disable the access.
New Password	Maximum input is 30 alphanumeric characters (case sensitive.)
Confirmed Password	Key in the password again to confirm.

4.8 Log out

Click the Logout button to leave the web configuration page.

Logout

This page is used to logout

Do you want to logout

Apply change



5

PC Configuration

5.1 Overview

For each PC, the following may need to be configured:

- TCP/IP network settings
- Internet Access configuration
- Wireless configuration

5.2 Windows Clients

- This section describes how to configure Windows clients for Internet access via the Wireless Router.
- The first step is to check the PC's TCP/IP settings.
- The Wireless Router uses the TCP/IP network protocol for all functions, so it is essential that the TCP/IP protocol be installed and configured on each PC.

5.2.1 TCP/IP Settings – Overview

If using default Wireless Router settings, and default Windows TCP/IP settings, no changes need to be made.

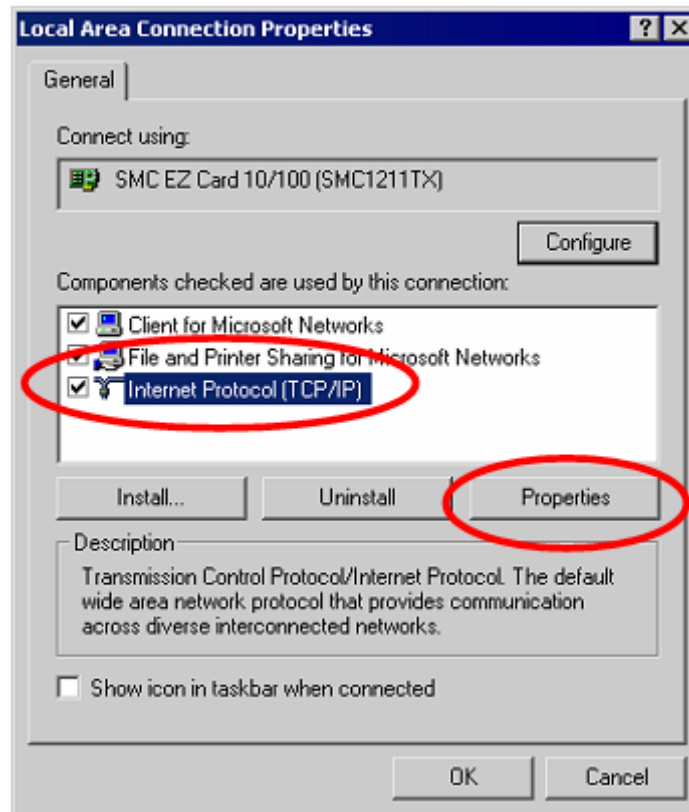
- By default, the Wireless Router will act as a DHCP Server, automatically providing a suitable IP address (and related information) to each PC when the PC boots.
- For all non-Server versions of Windows, the default TCP/IP setting is to act as a DHCP client.

If using a Fixed (specified) IP address, the following changes are required:

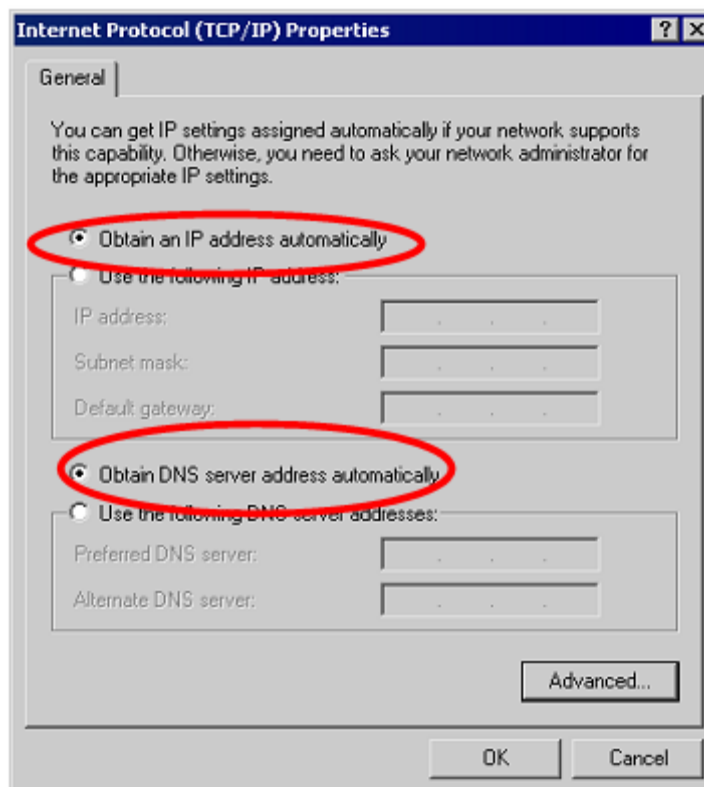
- The Gateway must be set to the IP address of the Wireless Router.
- The DNS should be set to the address provided by your ISP.

5.2.2 Checking TCP/IP Settings - Windows 2000

1. Select Control Panel - Network and Dial-up Connection.
2. Right - click the Local Area Connection icon and select Properties. You should see a screen like the following:



3. Select the TCP/IP protocol for your network card.
4. Click on the Properties button. You should then see a screen like the following.



Ensure your TCP/IP settings are correct, as described below.



Using DHCP

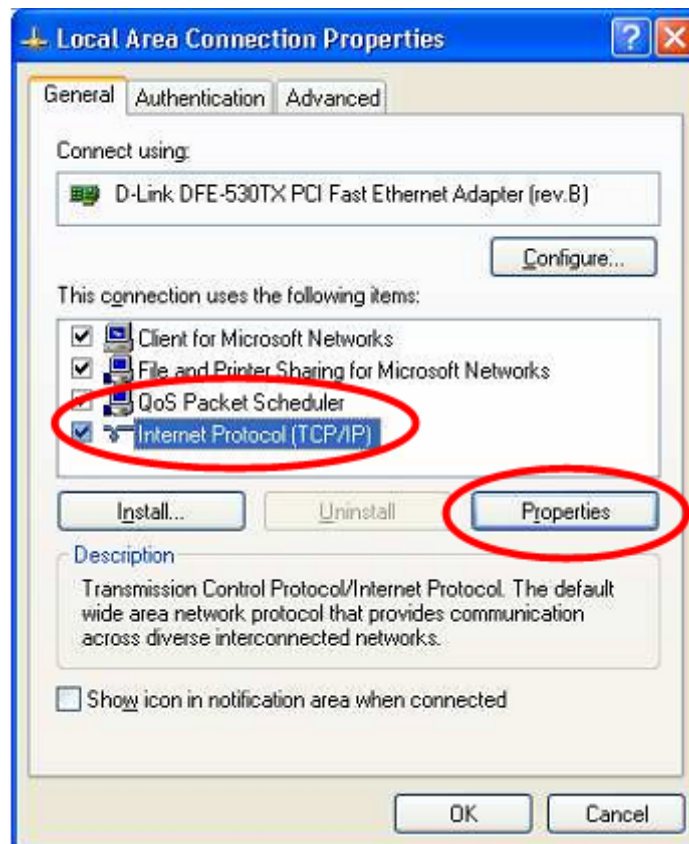
- To use DHCP, select the radio button Obtain an IP Address automatically. This is the default Windows setting. Using this is recommended. By default, the Wireless Router will act as a DHCP Server.
- Restart your PC to ensure it obtains an IP Address from the Wireless Router.

Using a fixed IP Address ("Use the following IP Address") If your PC is already configured, check with your network administrator before making the following changes.

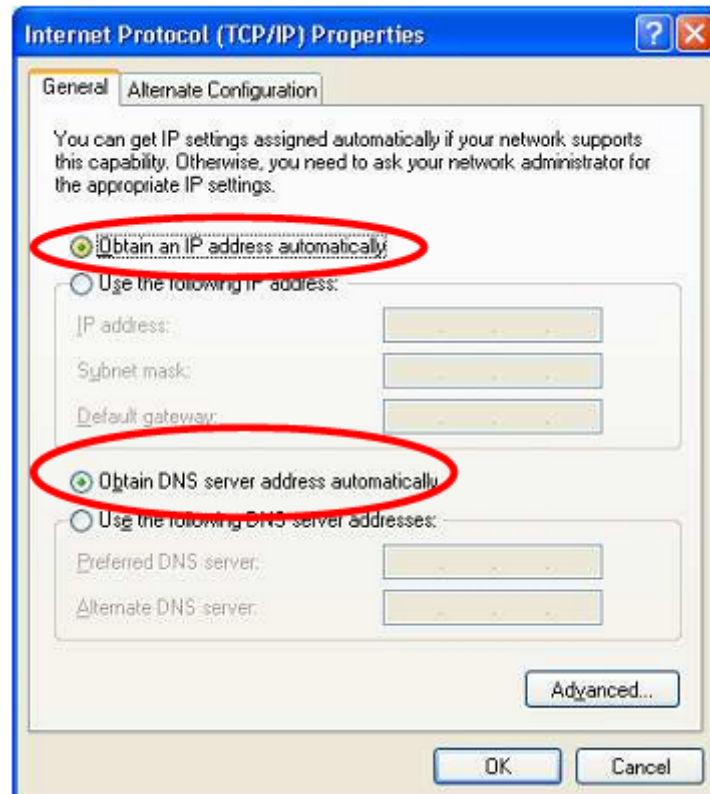
- Enter the Wireless Router 's IP address in the Default gateway field and click OK. (Your LAN administrator can advise you of the IP Address they assigned to the Wireless Router.)
- If the DNS Server fields are empty, select Use the following DNS server addresses, and enters the DNS address or addresses provided by your ISP, then click OK.

5.2.3 Checking TCP/IP Settings - Windows XP

1. Select Control Panel - Network Connection.
2. Right click the Local Area Connection and choose Properties. You should see a screen like the following:



3. Select the TCP/IP protocol for your network card.
4. Click on the Properties button. You should then see a screen like the following.



5. Ensure your TCP/IP settings are correct.

Using DHCP

- To use DHCP, select the radio button Obtain an IP Address automatically. This is the default Windows setting. Using this is recommended. By default, the Wireless Router will act as a DHCP Server.
- Restart your PC to ensure it obtains an IP address from the Wireless Router.

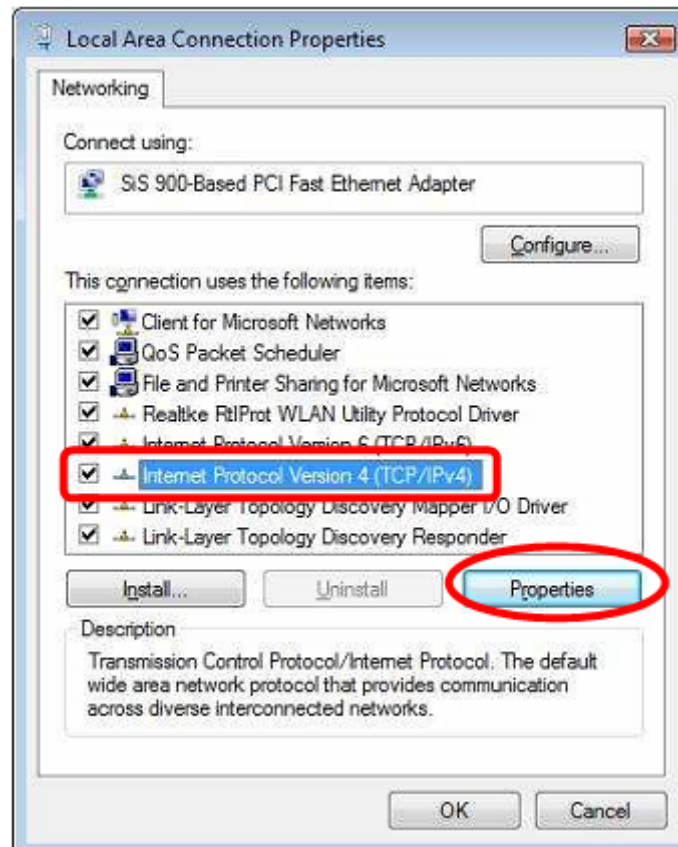
Using a fixed IP Address ("Use the following IP Address")

If your PC is already configured, check with your network administrator before making the following changes.

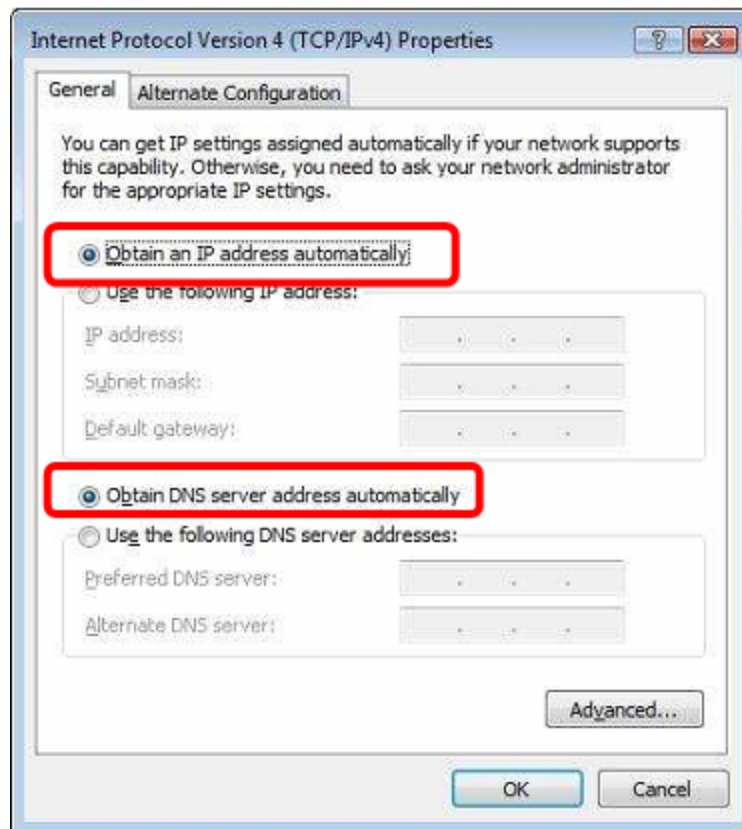
- In the Default gateway field, enter the Wireless Router's IP address and click OK. Your LAN administrator can advise you of the IP Address they assigned to the Wireless Router.
- If the DNS Server fields are empty, select Use the following DNS server addresses, and enters the DNS address or addresses provided by your ISP, then click OK.

5.2.4 Checking TCP/IP Settings - Windows Vista

1. Go to Start > Control Panel> Network and Internet> Network and Sharing Center> Manage Network Connections> Local Area Connection.
2. Right click the Local Area Connection icon and choose Properties. You should see a screen like the following:



3. Select the Internet Protocol Version 4(TCP/IPv4) or 6 (TCP/IPv6) for your network card.
4. Click on the Properties button. You should then see a screen like the following.



5. Ensure your TCP/IP settings are correct.

Using DHCP

- To use DHCP, select Obtain an IP address automatically and Obtain DNS server address automatically. This is the default Windows setting. Using this is recommended. By default, the Wireless Router will act as a DHCP Server.
- Restart your PC to ensure it obtains an IP address from the Wireless Router.

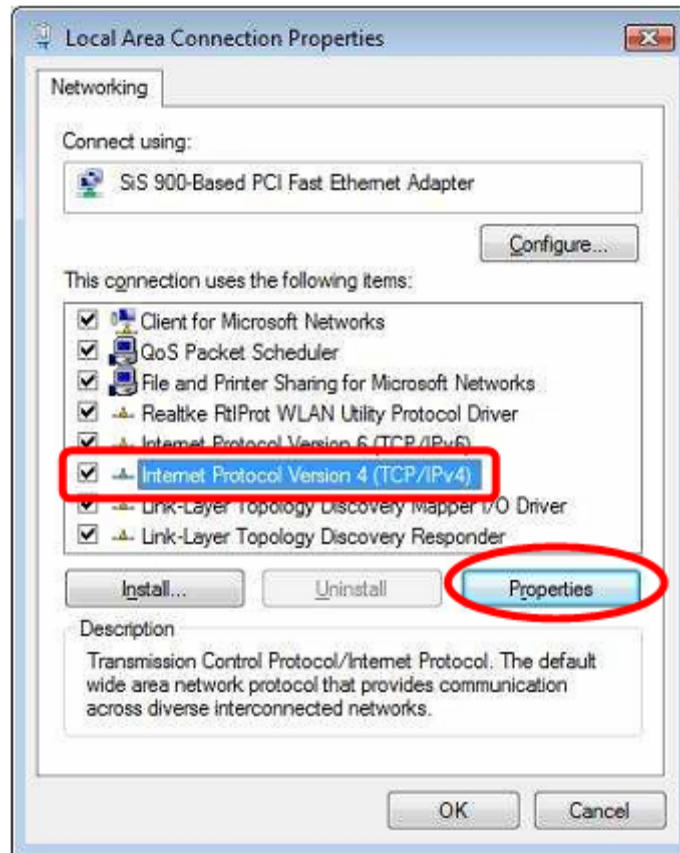
Using a fixed IP Address ("Use the following IP Address")

If your PC is already configured, check with your network administrator before making the following changes.

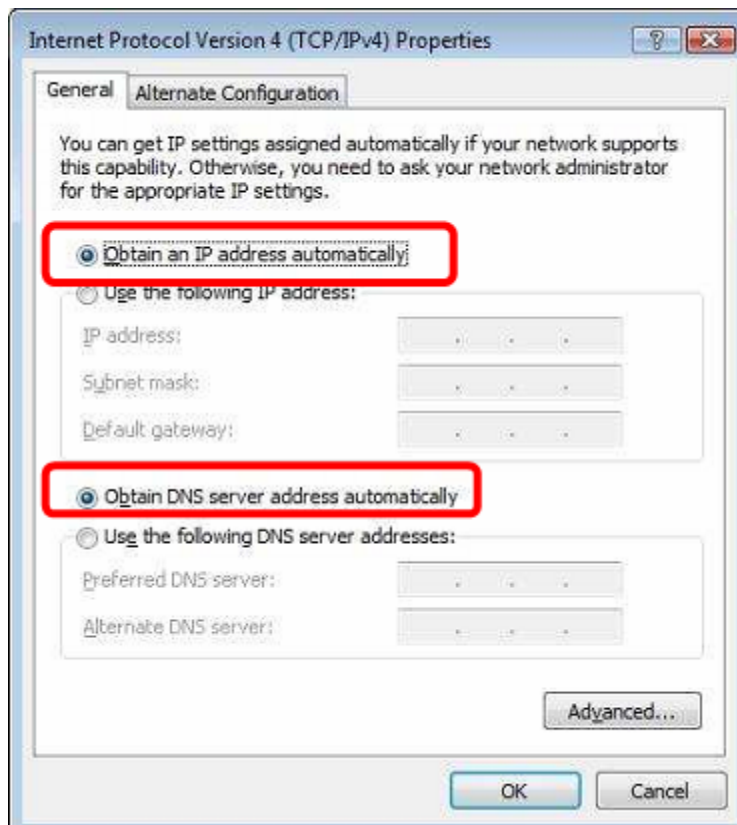
- In the Default gateway field, enter the Wireless Router 's IP address. Your LAN administrator can advise you of the IP address they assigned to the Wireless Router.
- If the DNS Server fields are empty, select Use the following DNS server addresses, and enters the DNS address or addresses provided by your ISP, then click OK.

5.2.5 Checking TCP/IP Settings - Windows 7

1. Go to Start > Control Panel> Network and Sharing Center> Manage Network Connections> Local Area Connection.
2. Right click the Local Area Connection icon and choose Properties. You should see a screen like the following:



3. Select the Internet Protocol Version 4(TCP/IPv4) or 6 (TCP/IPv6) for your network card.
4. Click on the Properties button. You should then see a screen like the following.





Using DHCP

- To use DHCP, select Obtain an IP address automatically and Obtain DNS server address automatically. This is the default Windows setting. Using this is recommended. By default, the Wireless Router will act as a DHCP Server.
- Restart your PC to ensure it obtains an IP address from the Wireless Router.

Using a fixed IP Address ("Use the following IP Address")

If your PC is already configured, check with your network administrator before making the following changes.

- In the Default gateway field, enter the Wireless Router 's IP address. Your LAN administrator can advise you of the IP address they assigned to the Wireless Router.
- If the DNS Server fields are empty, select Use the following DNS server addresses, and enters the DNS address or addresses provided by your ISP, then click OK.

5.2.6 Internet Access

To configure your PCs to use the Wireless Router for Internet access:

- Ensure that the ADSL modem, DSL modem, Cable modem, or other permanent connection is functional.
- Use the following procedure to configure your Browser to access the Internet via the LAN, rather than by a Dial-up connection.

For Windows 2000

1. Select Start menu - Settings - Control Panel - Internet Options.
2. Select the Connection tab, and click the Setup button.
3. Select "I want to set up my Internet connection manually, or I want to connect through a local area network (LAN)" and click Next.
4. Select "I connect through a local area network (LAN)" and click Next.
5. Ensure all of the boxes on the following Local area network Internet Configuration screen are unchecked.
6. Check the "No" option when prompted "Do you want to set up an Internet mail account now?"
7. Click Finish to close the Internet Connection Wizard. Setup is now completed.

For Windows XP

1. Select Start menu >Control Panel > Network and Internet Connections.
2. Select Set up or change your Internet Connection.
3. Select the Connection tab, and click the Setup button.
4. Cancel the pop-up "Location Information" screen.



5. Click Next on the "New Connection Wizard" screen.
6. Select "Connect to the Internet" and click Next.

For Windows Vista

1. Select Start menu > Control Panel > Network and Internet> Network and Sharing Center.
2. Select Set up a connection or network.
3. Select Connect to the Internet and click Next to continue.
4. Select Broadband (PPPoE).
5. Enter User name and Password that provided by the ISP, then click Connect to make a connection.

For Windows 7

1. Select Start menu > Control Panel > Network Sharing Center.
2. Select Set up a new connection or network.
3. Select Connect to the Internet and click Next to continue.
4. Select Broadband (PPPoE).
5. Enter User name and Password that provided by the ISP, then click Connect to make a connection.

Accessing AOL

To access AOL (America On Line) through the Wireless Router, the AOL for Windows software must be configured to use TCP/IP network access, rather than a dial-up connection. The configuration process is as follows:

1. Start the AOL for Windows communication software. Ensure that it is Version 2.5, 3.0 or later. This procedure will not work with earlier versions.
2. Click the Setup button.
3. Select Create Location, and change the location name from "New Locality" to "Wireless Router".
4. Click Edit Location. Select TCP/IP for the Network field. (Leave the Phone Number blank.)
5. Click Save, then OK.
6. Configuration is now complete.
7. Before clicking "Sign On", always ensure that you are using the "Wireless Router" location.



5.2.7 Macintosh Clients

From your Macintosh, you can access the Internet via the Wireless Router. The procedure is as follow

1. Open the TCP/IP Control Panel.
2. Select Ethernet from the Connect via pop-up menu.
3. Select Using DHCP Server from the Configure pop-up menu. The DHCP Client ID field can be left blank.
4. Close the TCP/IP panel, saving your settings.

Note

If using manually assigned IP addresses instead of DHCP, the required changes are:

- Set the Router Address field to the Wireless Router 's IP Address.
- Ensure your DNS settings are correct.

5.2.8 Linux Clients

To access the Internet via the Wireless Router, it is only necessary to set the Wireless Router as the "Gateway".

Ensure you are logged in as "root" before attempting any changes.

Fixed IP Address

By default, most Unix installations use a fixed IP Address. If you wish to continue using a fixed IP Address, make the following changes to your configuration.

- Set your "Default Gateway" to the IP Address of the Wireless Router.
- Ensure your DNS (Domain Name server) settings are correct.

To act as a DHCP Client (Recommended)

The procedure below may vary according to your version of Linux and X -windows shell.

1. Start your X Windows client.
2. Select Control Panel – Network.
3. Select the "Interface" entry for your Network card. Normally, this will be called "eth0".
4. Click the Edit button, set the "protocol" to "DHCP", and save this data.
5. To apply your changes:
 - Use the "Deactivate" and "Activate" buttons, if available.
 - OR, restart your system.



5.2.9 Other Unix Systems

To access the Internet via the Wireless Router:

- Ensure the "Gateway" field for your network card is set to the IP Address of the Wireless Router.
- Ensure your DNS (Name Server) settings are correct.

5.2.10 Wireless Station Configuration

- This section applies to all wireless stations wishing to use the Wireless Router 's access point, regardless of the operating system that is used on the client.
- To use the Wireless Router, each wireless station must have compatible settings, as following:

Mode	The mode must be set to Infrastructure.
SSID (ESSID)	The network name must match the value used on the Wireless Router. Note The SSID is case- sensitive.
Disable	If there is no security is enabled on the Wireless Router, the security of each station should be disabled as well. And, you can connect the Wireless Router without security, but it is NOT recommended.
WEP	By default, WEP on the Wireless Router is disabled. <ul style="list-style-type: none"> ● If WEP remains disabled on the Wireless Router, all stations must have WEP disabled. ● If WEP is enabled on the Wireless Router, each station must use the same settings as the Wireless Router.
WPA WPA2 WPA-Mixed 802.1x	RADIUS Server: RADIUS is an authentication, authorization and accounting client-server protocol. The client is a Network Access Server that desires to authenticate its links. The server is a server that has access to a user database with authentication information. Each station must set up the RADIUS Server's IP address, port and passwords that provided by your ISP.

Note

By default, the Wireless Router will allow 802.11b, 802.11g and 802.11n connections.



A

Appendix A: Troubleshooting

Overview

This chapter covers some common problems that may be encountered while using the Wireless Router and some possible solutions to them. If you follow the suggested steps and the Wireless Router still does not function properly, contact your dealer for further advice.

General Problems

Problem 1:	Can't connect to the Wireless Router to configure it.
Solution 1:	<p>Check the following:</p> <ul style="list-style-type: none"> ● Check the Wireless Router is properly installed, LAN connections are OK, and it is powered ON. ● Ensure that your PC and the Wireless Router are on the same network segment. ● If your PC is set to "Obtain an IP Address automatically" (DHCP client), please restart it. ● If your PC uses a Fixed (Static) IP address, ensure that it is using an IP Address within the range 192.168.1.1 to 192.168.1.252 and thus compatible with the Wireless Router's default IP Address. About the Router's default settings, please refer to 3.3 Default Settings in this manual. <p>Also, the Network Mask should be set to 255.255.255.0 to match the Wireless Router.</p> <p>In Windows, you can check these settings by using Control Panel-Network to check the Properties for the TCP/IP protocol.</p>

Internet Access

Problem 1:	When I enter a URL or IP address I get a time out error.
Solution 1:	<p>A number of things could be causing this. Try the following troubleshooting steps.</p> <ul style="list-style-type: none"> ● Check if other PCs work. If they do, ensure that your PCs IP



	<p>settings are correct. If using a Fixed (Static) IP Address, check the Network Mask, Default gateway and DNS as well as the IP Address.</p> <ul style="list-style-type: none"> ● If the PCs are configured correctly, but still not working, check the Wireless Router. Ensure that it is connected and ON. Connect to it and check its settings. (If you can't connect to it, check the LAN and power connections.) ● If the Wireless Router is configured correctly, check your Internet connection (DSL/Cable modem etc) to see that it is working correctly.
Problem 2:	Some applications do not run properly when using the Wireless Router.
Solution 2:	<p>The Wireless Router processes the data passing through it, so it is not transparent.</p> <p>Use the Content Filter Settings feature to allow the use of Internet applications, which do not function correctly.</p> <p>If this does solve the problem you can use the DMZ function. This should work with almost every application, but:</p> <ul style="list-style-type: none"> ● It is a security risk, since the firewall is disabled. ● Only one (1) PC can use this feature.

Wireless Access

Problem 1:	My PC can't locate the Wireless Router.
Solution 1:	<p>Check the following:</p> <ul style="list-style-type: none"> ● Your PC is set to Infrastructure Mode. (Access Points are always in Infrastructure Mode) ● The SSID on your PC and the Wireless Router are the same. ● Remember that the SSID is case-sensitive. So, for example "Workgroup" does NOT match "workgroup." ● Both your PC and the Wireless Router must have the same setting for security. The default setting for the Wireless Router security is disabled, so your wireless station should also have security disabled. ● If security is enabled on the Wireless Router, your PC must have security enabled, and the key must be matched. ● To see if radio interference is causing a problem, see if connection is possible when close to the Wireless Router.



	Remember that the connection range can be as little as 100 feet in poor environments.
Problem 2:	Wireless connection speed is very slow.
Solution 2:	<p>The wireless system will connect at the highest possible speed, depending on the distance and the environment. To obtain the highest possible connection speed, you can experiment with the following:</p> <ul style="list-style-type: none"> ● Wireless Router location <p>Try adjusting the location and orientation of the Wireless Router.</p> <ul style="list-style-type: none"> ● Wireless Channel <p>If interference is the problem, changing to another channel may show a marked improvement.</p> <ul style="list-style-type: none"> ● Radio Interference <p>Other devices may be causing interference. You can experiment by switching other devices off, and see if this helps. Any "noisy" devices should be shielded or relocated.</p> <ul style="list-style-type: none"> ● RF Shielding <p>Your environment may tend to block transmission between the wireless stations. This will mean high access speed is only possible when close to the Wireless Router.</p>



B

Appendix B: About Wireless LANs

BSS

BSS

A group of Wireless Stations and a single Access Point, all using the same ID (SSID), form a Basic Service Set (BSS).

Using the same SSID is essential. Devices with different SSIDs are unable to communicate with each other.

Channels

The Wireless Channel sets the radio frequency used for communication.

- Access Points use a fixed Channel. You can select the Channel used. This allows you to choose a Channel which provides the least interference and best performance. In the USA and Canada, 11 channels are available. If using multiple Access Points, it is better if adjacent Access Points use different Channels to reduce interference.
- In "Infrastructure" mode, Wireless Stations normally scan all Channels, looking for an Access Point. If more than one Access Point can be used, the one with the strongest signal is used. (This can only happen within an ESS.)

Note

To comply with US FCC regulation, the country selection function has been completely removed from all US models. The above function is for non-US models only.

Security

- WEP

WEP (Wired Equivalent Privacy) is a standard for encrypting data before it is transmitted. This is desirable because it is impossible to prevent snoopers from receiving any data which is transmitted by your Wireless Stations. But if the data is encrypted, then it is meaningless unless the receiver can decrypt it.

If WEP is used, the Wireless Stations and the Access Point must have the same security settings for each of the following:

WEP	64 Bits, 128 Bits.
Key	For 64 Bits encryption, the Key value must match. For 128 Bits encryption, the Key value must match.
WEP Authentication	Open System or Shared Key.



- WPA/WPA2/ WPA-Mixed

WPA/WPA2 (Wi-Fi Protected Access) is more secure than WEP. It uses a “Shared Key” which allows the encryption keys to be regenerated at a specified interval. There are several encryption options: TKIP, AES, TKIP-AES and additional setup for RADIUS is required in this method. The most important features beyond WPA to become standardized through 802.11i/WPA2 are: pre-authentication, which enables secure fast roaming without noticeable signal latency.

If WPA or WPA2 is used, the Wireless Stations and the Access Point must have the same security settings.

- 802.1x

With 802.1x authentication, a wireless PC can join any network and receive any messages that are not encrypted, however, additional setup for RADIUS to issue the WEP key dynamically will be required. RADIUS is an authentication, authorization, and accounting client-server protocol. The client is a Network Access Server that desires to authenticate its links. The server is a server that has access to a user database with authentication information.

Wireless LAN Configuration

To allow Wireless Stations to use the Access Point, the Wireless Stations and the Access Point must use the same settings, as follows:

Mode	The mode must be set to Infrastructure.
SSID (ESSID)	The network name must match the value used on the Wireless Router. Note The SSID is case- sensitive.
Disable	If there is no security is enabled on the Wireless Router, the security of each station should be disabled as well. And, you can connect the Wireless Router without security, but it is NOT recommended.
WEP Open System/ Shared Key/ Auto	By default, WEP on the Wireless Router is disabled. Shared Key only supports WEP as encryption method. AUTO(Open/Shared) means AP can accept STA connect to it using OPEN-WEP or SHARED-WEP. <ul style="list-style-type: none"> ● If WEP remains disabled on the Wireless Router, all stations must have WEP disabled. ● If WEP is enabled on the Wireless Router, each station must use the same settings as the Wireless Router.



<p>Personal (Pre-Shared Key)</p> <p>WPA</p> <p>WPA2</p> <p>WPA2-Mixed</p>	<p>WPA-PSK (TKIP/AES)/ WPA2-PSK (TKIP/AES):</p> <p>If one of these securities is enabled on the Wireless Router. To make a connection, each station must use the same algorithms and pass phrase as the Wireless Router.</p> <p>Pre-Shared Key Format:</p> <p>There are two formats for choice to set the Pre-shared key, Passphrase and Hex (64 characters). If Hex is selected, users will have to enter a 64 characters string. For easier configuration, the Passphrase (at least 8 characters) format is recommended.</p> <p>Pre-Shared Key :</p> <p>Pre-Shared Key serves as a password. Users may key in 8 to 63 characters string if you selected passphrase. Pre-shared key format to set the passwords or leave it blank, in which the 802.1x Authentication will be activated. Make sure the same password is used on client's end.</p>
<p>Enterprise (RADIUS)</p> <p>WPA</p> <p>WPA2</p> <p>WPA2-Mixed</p> <p>802.1x</p>	<p>RADIUS Server: RADIUS is an authentication, authorization and accounting client-server protocol. The client is a Network Access Server that desires to authenticate its links. The server is a server that has access to a user database with authentication information. Each station must set up the RADIUS Server's IP address, port and passwords that provided by your ISP.</p>