



WN-151ARM

Wireless 11b/g/n 150Mbps
ADSL2/2+ Router

User's Manual



www.airlive.com



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.



© 2009 OvisLink Corporation, All Rights Reserved



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

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

FCC Caution

This equipment must be installed and operated in accordance with provided instructions and a minimum 20 cm spacing must be provided between computer mounted antenna and person's body (excluding extremities of hands, wrist and feet) during wireless modes of operation.

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.

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



Federal Communication Commission (FCC) Radiation Exposure Statement

This equipment complies with FCC radiation exposure set forth for an uncontrolled environment. In order to avoid the possibility of exceeding the FCC radio frequency exposure limits, human proximity to the antenna shall not be less than 20cm (8 inches) during normal operation.

The antenna(s) used for this transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

R&TTE Compliance Statement

This equipment complies with all the requirements of DIRECTIVE 1999/5/EC OF THE EUROPEAN PARLIAMENT AND THE COUNCIL of March 9, 1999 on radio equipment and telecommunication terminal Equipment and the mutual recognition of their conformity (R&TTE)

The R&TTE Directive repeals and replaces in the directive 98/13/EEC (Telecommunications Terminal Equipment and Satellite Earth Station Equipment) As of April 8, 2000.

Safety

This equipment is designed with the utmost care for the safety of those who install and use it. However, special attention must be paid to the dangers of electric shock and static electricity when working with electrical equipment. All guidelines of this and of the computer manufacture must therefore be allowed at all times to ensure the safe use of the equipment.

EU Countries Intended for Use

The ETSI version of this device is intended for home and office use in Austria, Belgium, Denmark, Finland, France, Germany, Greece, Ireland, Italy, Luxembourg, the Netherlands, Portugal, Spain, Sweden, and the United Kingdom.

The ETSI version of this device is also authorized for use in EFTA member states: Iceland, Liechtenstein, Norway, and Switzerland.

EU Countries Not intended for use

None.

The specification is subject to change without notice.

Table of Contents

1. Introduction	6
1.1 Features	7
1.2 Front Panel and Rear Panel	12
1.3 Packing List	17
2. Installation	18
3. Setup	20
3.1 Setup Wizard	23
3.2 LAN Screen	27
3.3 Wireless Screen	29
3.4 Wireless Security	34
3.5 Password Screen	41
3.6 Mode Screen	42
4. Operation and Status	43
5. Advanced Features	51
5.1 Internet	52
5.2 Access Control	55
5.3 Dynamic DNS	58
5.4 Option	60
5.5 Schedule	61
5.6 Port Trigger	63
5.7 Port Forward	65
5.8 Port Range Forward	67
5.9 QoS	68
6. Administration	70
6.1 PC Database	71
6.2 Config File	76
6.3 Logs	77
6.4 Email	79
6.5 Diagnostics	81
6.6 Remote Administration	83
6.7 Routing	85
6.8 Upgrade Firmware	90
7. Modem Mode	91
Appendix A - Troubleshooting	97
Appendix B - Wireless LAN	100
Appendix C - Specifications	104
Appendix D - Wireless Network Glossary	107

1

Introduction

Congratulations on the purchase of your new AirLive WN-151ARM. This device is an all-in-one device that combines the function of high-speed DSL modem, wireless-N access point and a single port Ethernet router. It supports the latest ADSL2+ standard and allows you to access the Internet and surf the Web at double the speed previously available through ADSL2. With the combine of Wireless-N technology and WPS (Wi-Fi Protected Setup), it further enhanced the wireless transfer speed and coverage, also simplifies the security settings by push a button. AirLive WN-151ARM is an ideal cost-efficient all-in-one multi-function device which provides the following services to you.

- ***ADSL2/2+ Modem Router with downstream data rates up to 24Mbps***
- ***Shares Broadband Internet Access and creates your personal private Network***
- ***The latest Wireless N technology for enhanced transfer speed and coverage***
- ***WPS (Wi-Fi Protected Setup) for simple establishment of Wireless security***
- ***Integrated 1-Port 10/100Mbps LAN switch with auto MDI/MDI-X detection***



1.1 Features

Internet Access Features

Shared Internet Access:

- All users on the LAN or WLAN can access the Internet through the WN-151ARM, using only a single external IP Address. The local (invalid) IP Addresses are hidden from external sources. This process is called NAT (Network Address Translation).

Built-in ADSL2/2+ Modem:

- The WN-151ARM has a built-in ADSL modem; it supports all common ADSL2/2+ connections.

IPoA, PPPoE, PPPoA, Direct Connection Support:

- The WN-151ARM supports all common connection methods.

Auto-detect Internet Connection Method:

- In most situations, the WN-151ARM can test your ADSL and Internet connection to determine the connection method used by your ISP.

Fixed or Dynamic IP Address:

- On the Internet (ADSL port) connection, the WN-151ARM supports both Dynamic IP Address (IP Address is allocated on connection) and Fixed IP Address.

Advanced Internet Functions

Application Level Gateways (ALGs):

- Applications which use non-standard connections or port numbers are normally blocked by the Firewall. The ability to define and allow such applications is provided, to enable such applications to be used normally.

Firewall:

- As well as the built-in firewall to protect your LAN, you can define Firewall Rules to determine which incoming and outgoing traffic should be permitted.

**Port Triggering:**

- This feature, also called Special Applications, allows you to use Internet applications which normally do not function when used behind a firewall.

Port Forwarding:

- This feature allows Internet users to access Internet servers on your LAN. The required setup is quick and easy.

Dynamic DNS Support:

- DDNS, when used with the Virtual Servers feature, allows users to connect to Servers on your LAN using a Domain Name, even if you have a dynamic IP address which changes every time you connect.

URL Filter:

- Use the URL Filter to block access to undesirable Web sites by LAN users.

Scheduling:

- Both the URL Filter and Firewall rules can be scheduled to operate only at certain times. This provides great flexibility in controlling Internet -bound traffic.

QoS Support:

- Quality of Service can be used to handle packets so that more important connections receive priority over less important one.

Logs:

- Define what data is recorded in the Logs, and optionally send log data to a Syslog Server. Log data can also be E-mailed to you.

VPN Pass through Support:

- PCs with VPN (Virtual Private Networking) software using PPTP, L2TP and IPSec are transparently supported - no configuration is required.

Wireless Features

Wireless N technology:

- Advanced Wireless N technology for enhanced throughput and coverage. Complies with 2.4GHz IEEE 802.11n standard and is backward compatible with IEEE 802.11b/g standards.

WEP:

- WEP (Wired Equivalent Privacy) encryption key, the key sizes of 64 Bit and 128 Bit are supported. WEP encrypts any data before transmission, providing protection against snoopers.

WPA:

- Similar to WEP, WPA-PSK encrypts any data before transmission, providing protection against snoopers. The WPA-PSK is a newer standard than WEP which provides easier configuration and greater security than WEP.

WPA2-PSK:

- WPA2 encryption key uses the extremely secure AES encryption method which it is recommended for user who has security breach concern.

802.1x:

- The 802.1x mode is providing for the industrial-strength wireless security of 802.1x authentication and authorization.

Wireless MAC Access Control:

- This feature will check the MAC address (hardware address) of Wireless stations to ensure that only trusted Wireless Stations can be granted for access.

WPS:

- WPS (Wi-Fi Protected Setup) is the simplest way to build connections between wireless network clients and this router. Instead of selecting an encryption mode and entering a long encryption passphrase, just press client and router's WPS push button and the WPS will do the setup for you.

WDS:

- WDS (Wireless Distribution System) allows the Wireless Access Point to act as a Wireless Bridge. Both Point-to-Point and Multi-Point Bridge modes are supported.



LAN Features

Single Port Ethernet Router:

- The WN-151ARM integrated 1-port 10/100Mbps LAN switch with auto MDI-MID-X support.

DHCP Server Support:

- Dynamic Host Configuration Protocol provides a dynamic IP address to PCs and other devices upon request. The WN-151ARM can act as a **DHCP Server** for devices on your local LAN and WLAN.

Configuration & Management

Easy Setup:

- WEB user interface, open a browser for configuration.

Configuration File Upload/Download:

- Save (download) the configuration data from WN-151ARM to your personal computer for easy backup.

Restore (upload) a previously-saved configuration file from your personal computer to WN-151ARM.

Remote Management.

- The WN-151ARM can be managed from any PC on your LAN or Wireless LAN. And, if the Internet connection exists, it can also (optionally) be configured via the Internet.

Network Diagnostics:

- You can use the WN-151ARM to perform a **Ping** or **DNS lookup**.

Security Features

- **Password - protected Configuration:** Password protection is provided to prevent unauthorized users from modifying the configuration data and settings.
- **Wireless LAN Security:** WPA-802.1x, WPA2-802.1x and WEP and Wireless access control by MAC address are all supported. The MAC-level access control feature can be used to prevent unknown wireless stations from accessing your LAN.
- **NAT Protection:** An intrinsic side effect of NAT (Network Address Translation) technology is that by allowing all LAN users to share a single IP address, the location and even the existence of each PC is hidden. From the external viewpoint, there is no network, only a single device - the WN-151ARM.
- **Firewall:** All incoming data packets are monitored and all incoming server requests are filtered, thus protecting your network from malicious attacks from external sources.
- **Protection against DoS attacks:** 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 WN-151ARM incorporates protection against DoS attacks.

1.2 Front Panel and Rear Panel

Front-mounted LEDs



As listed below, the LEDs indicate the current status of the router.

<u>LED</u>	<u>Mode</u>	<u>Status</u>
Security (White)	ON	SSID1 wireless security is enabled
	OFF	SSID1 wireless security is disabled
	Blinking	When WPS button is pressed, the LED will blink for two minutes
Power (Orange)	ON	Ready for operation
	OFF	Power off
	Blinking	System in boot stage
LAN (Blue)	ON	The LAN port is active
	OFF	No Network connection
	Blinking	Network traffic is being transmitted/received
WLAN (Blue)	ON	Wireless client is connected
	OFF	The wireless LAN is disabled or no wireless client is connected
	Blinking	Wireless traffic is being transmitted/received
Internet (Blue)	ON	Internet connection established
	OFF	No Internet connection
	Blinking	Data is being transmitted/received



ADSL (Green)

ON

ADSL connection
established

OFF

No ADSL connection

Blinking

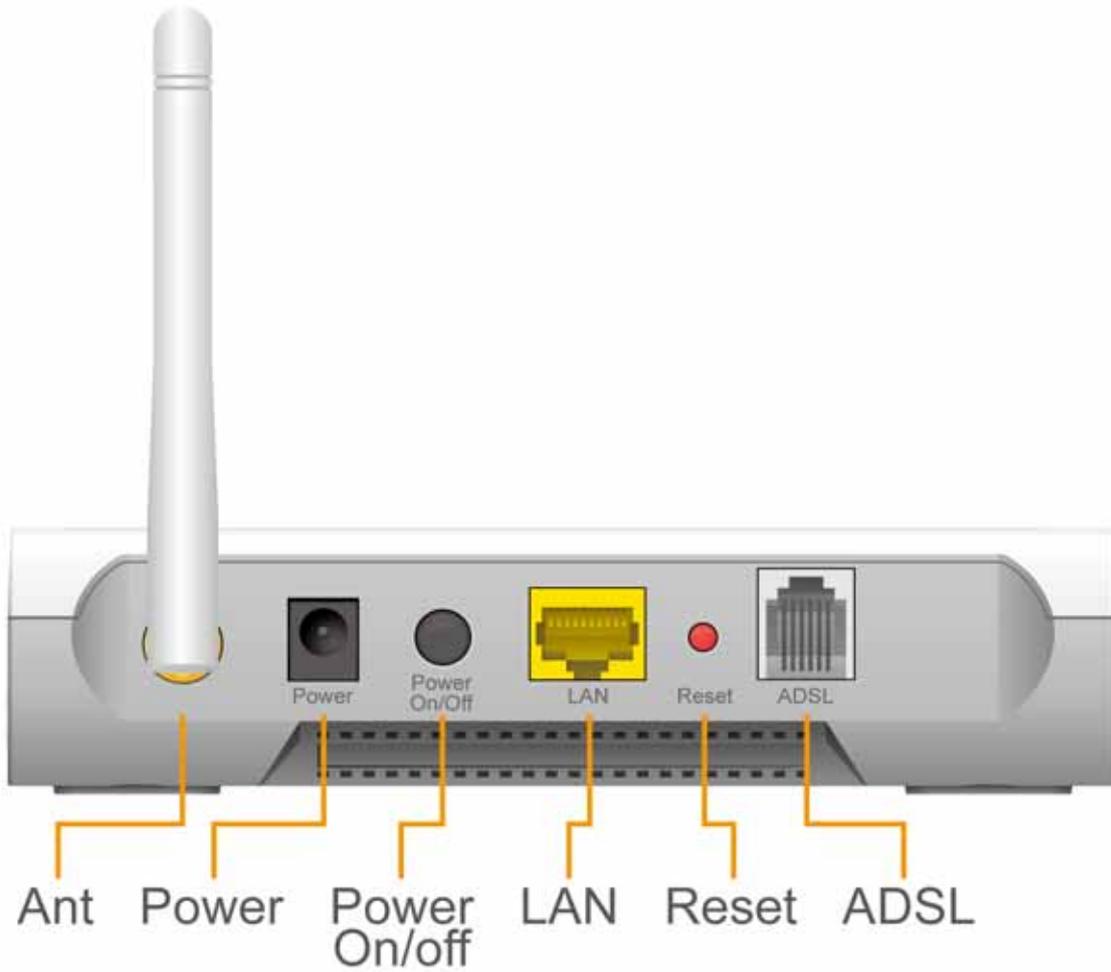
ADSL is synchronizing

Push Button

WPS

Push the WPS button on the device and your client device to perform WPS function which it can perform an easy way to create an encryption-secured wireless connection.

Rear Panel



<u>Port</u>	<u>Description</u>
ADSL	The included RJ-11 phone line connects this to an ADSL network
LAN	10/100 BaseT connection, use a standard LAN cable (RJ-45) to connect to your computer or a switch.
Power socket	The included 12V DC power adapter is connected here.
<u>Push Button</u>	
Reset	This can be used to reset the router or to restore the factory default settings. To restore the factory default value, press and hold the Reset Button for five (5) seconds, until the Status LED is lit, then release the Reset Button and wait for it to reboot. Press and release to reboot the device.
Power ON/OFF	Push the button to switch power ON/OFF

1.3 Packing List

The following items should be included:

- WN-151ARM
- Software CD
- Quick Setup Guide
- 1 x RJ-45 Cat.5e Cable
- 1 x RJ-11 Phone Cable
- 1 x 2dBi Dipole Antenna
- Power Adapter

When you open the package, make sure all of the above items are included. If there's anything missing in the package, please contact your dealer of purchase.

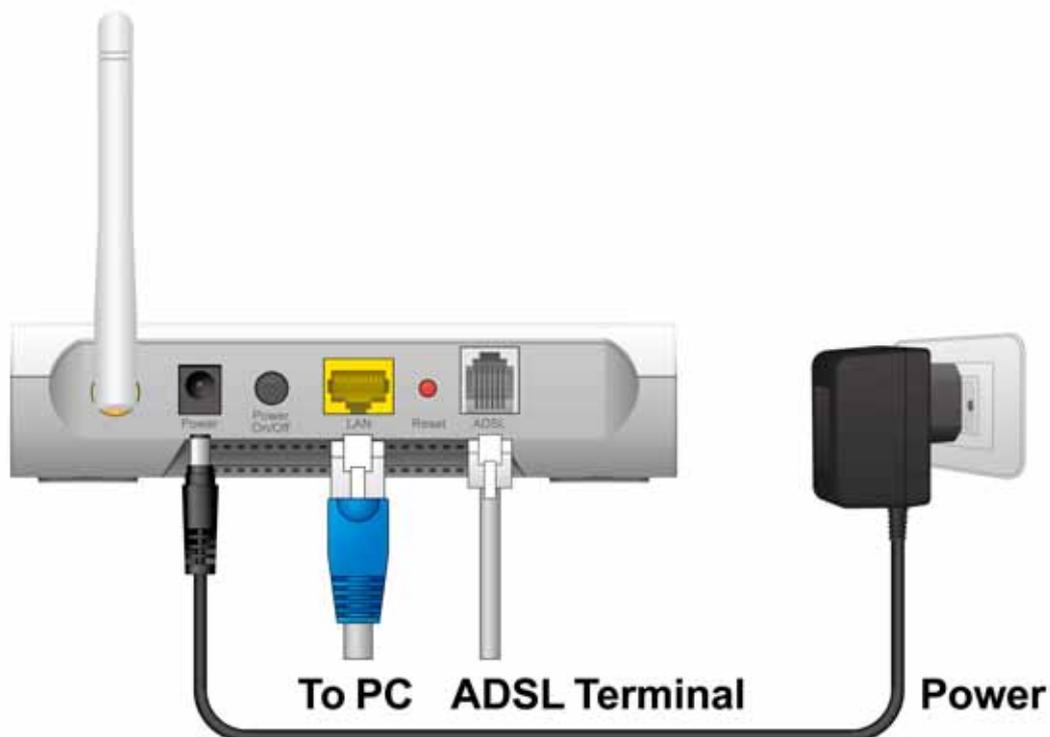
2

Installation

Requirement

- Network cables. Use standard 10/100BaseT network cables with RJ45 connectors.
- TCP/IP protocol must be installed on all PCs
- For Internet Access, an Internet Access account with an ISP, and a DSL connection.
- To use the Wireless Access Point, all Wireless devices must be compliant with the IEEE 802.11b/g/n standard.

Procedure



1. Choose an Installation Site

Select a suitable place on the network to install the WN-151ARM.

Notes:

For best Wireless reception and performance, the WN-151ARM should be positioned in a central location with minimum obstructions between the WN-151ARM and the PCs.

Also, if using multiple Access Points, adjacent Access Points should use different Channels.

2. Connect LAN Cables

Use standard LAN cables to connect PCs to the Switching ports on the WN-151ARM. Both 10BaseT and 100BaseT connections can be used simultaneously.

3. Connect ADSL Cable

Connect the supplied ADSL cable from to the ADSL port on the WN-151ARM (the RJ11 connector) to the ADSL terminator provided by your phone company.

4. Power Up

Connect the supplied power adapter to the WN-151ARM and plug into a power outlet.

Note: Use only the power adapter included with this device.

Using a different one may cause hardware damage.

5. Check the LEDs

- The **Power** (Orange) LED should be ON.
- For the LAN (PC) connection, the **LAN** LED should be ON
- The **Wireless** (Blue) LED will be turned ON once there's client connection established.
- The **Internet** (Blue) LED may be OFF. It will be ON after configuration.
- The **ADSL** (Green) LED should be ON if ADSL line is connected and available.

6. Router's default IP

- The default IP address of router's LAN port is:

IP Address: 192.168.1.254

Subnet Mask: 255.255.255.0

- For Web Management, please configure client PC as DHCP client to obtain IP address from WN-151ARM.
- After the IP assignment is assigned, please enter the router's IP address "192.168.1.254" in Web browser to manage the router, type the proper user name and password for authentication.

7. Default user name and password

- User's name: **admin**
- Password: **airlive**

3

Setup

Overview

This chapter describes the setup procedure for:

- Internet Access
- LAN configuration
- Wireless setup
- Assigning a Password to protect the configuration data.

Use the table below to locate detailed instructions for the required functions.

To Do this:	Refer to:
Check WN-151ARM operation and status.	Chapter 4: Operation and Status
Use any of the following Advanced features: <ul style="list-style-type: none">• Internet (DMZ, URL Filter)• Access Control• Dynamic DNS• Options• Schedule• Port Trigger• Port Forward• Port Range Forward• QoS	Chapter 5: Advanced Features

Use any of the following Administration
Configuration settings or features:

- PC Database
- Config File
- Logs
- E-mail
- Diagnostics
- Remote Admin
- Routing
- Upgrade Firmware

Chapter 6

Advanced Administration

Configuration Program

The WN-151ARM contains an HTTP server. This enables you to connect and configure WN-151ARM by using your Web Browser. **Note: the Web Browser must support JavaScript.**

The configuration program has been tested on the following browsers:

- Netscape 7.1 or later.
- Mozilla 1.6 or later
- Internet Explorer 5.5 or later

Preparation

Before attempting to configure the WN-151ARM, please ensure that:

- The computer must have at least one available network port so that it can establish a physical connection to the WN-151ARM by using a LAN cable.
- The WN-151ARM must be properly setup and powered ON.
- If the WN-151ARM's default IP Address (192.168.1.254) is already used by another device, the other device must be turned OFF until the WN-151ARM is allocated a new IP Address during configuration.



Using your Web Browser

To establish a connection from your computer to the WN-151ARM:

1. After installing the WN-151ARM in your LAN, start your computer. If your computer is already running, restart it.
2. Start your WEB browser.
3. In the **Address** box, enter "HTTP:///" and the IP Address of the WN-151ARM, as in this example, which uses the WN-151ARM's default IP Address:

http://192.168.1.254

4. When prompted for the User name and Password, enter values as follows:
 - User name **admin**
 - Password **airlive**

Note

If the WN-151ARM does not respond, check the following:

- The device is properly installed, LAN connection is OK, and it is powered ON. You can test the connection by using the "Ping" command:
 - Open the MS-DOS window or command prompt window.
 - Enter the command:

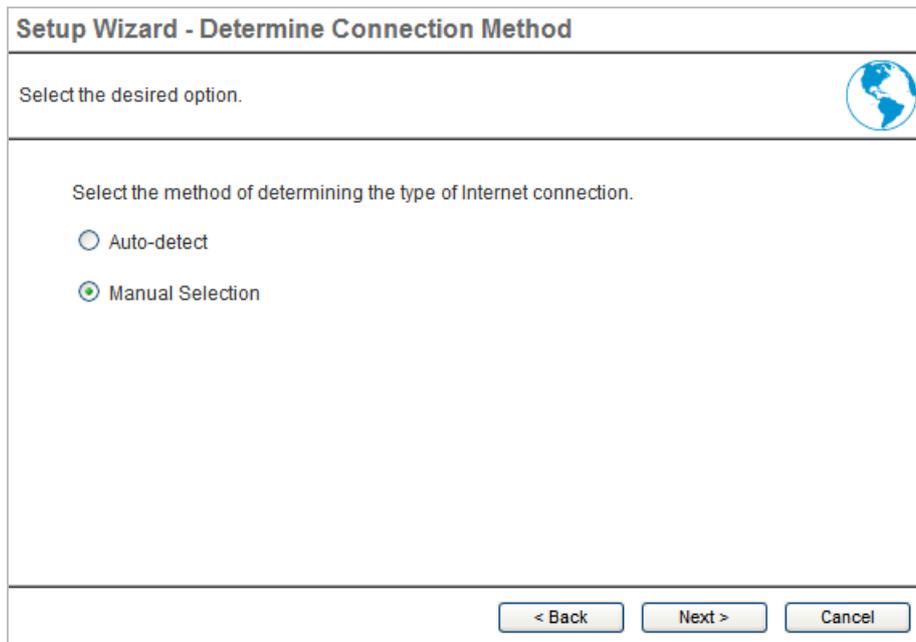
```
ping 192.168.1.254
```

if there's no respond, either the connection is not working, or your computer's IP address is not compatible with the WN-151ARM's IP Address. (See next item.)
- If your computer 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 WN-151ARM's default IP Address of 192.168.1.254. Also, the **Network Mask** must be set to 255.255.255.0.
- Ensure that your computer and the WN-151ARM are on the same network segment.
- For the first time, please make sure that you are using the wired LAN interface to configure the setting. The Wireless interface configuration can only be used after the establishment of the wireless setting.

3.1 Setup Wizard

If this is the first time you connect to the WN-151ARM, it is recommended to run the **Setup Wizard** to configure the ADSL and Internet Connection.

1. Click the **Setup Wizard** link on the main menu
2. On the first screen, select *Auto-detect* or *Manual Selection*, then click "Next"



Setup Wizard - Determine Connection Method

Select the desired option. 

Select the method of determining the type of Internet connection.

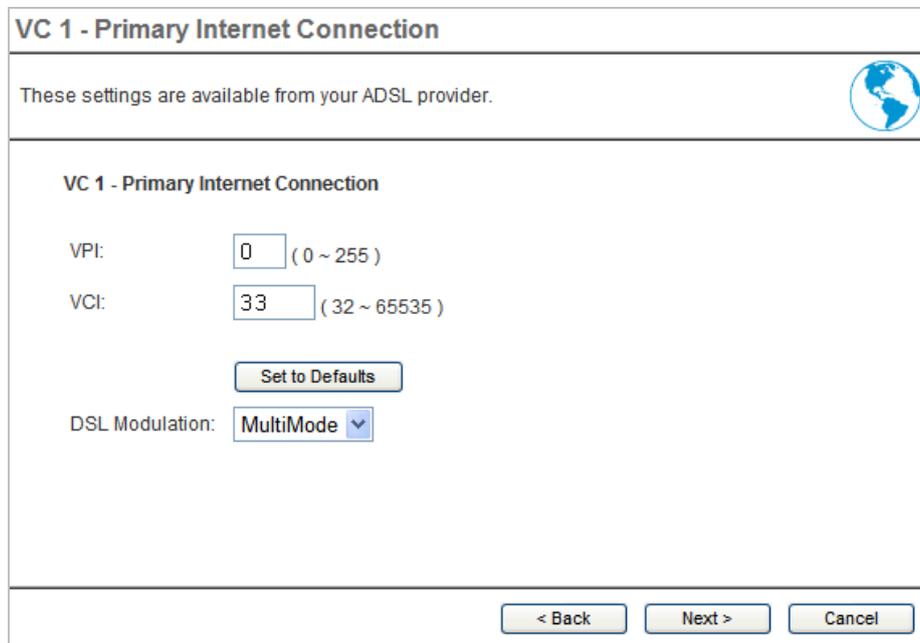
Auto-detect

Manual Selection

< Back Next > Cancel

Figure: Select desired option

3. If *Manual Selection* is selected, you will see the VC 1 screen shown below. Enter the VPI and VCI values provided by your ISP, then click "Next".



VC 1 - Primary Internet Connection

These settings are available from your ADSL provider.

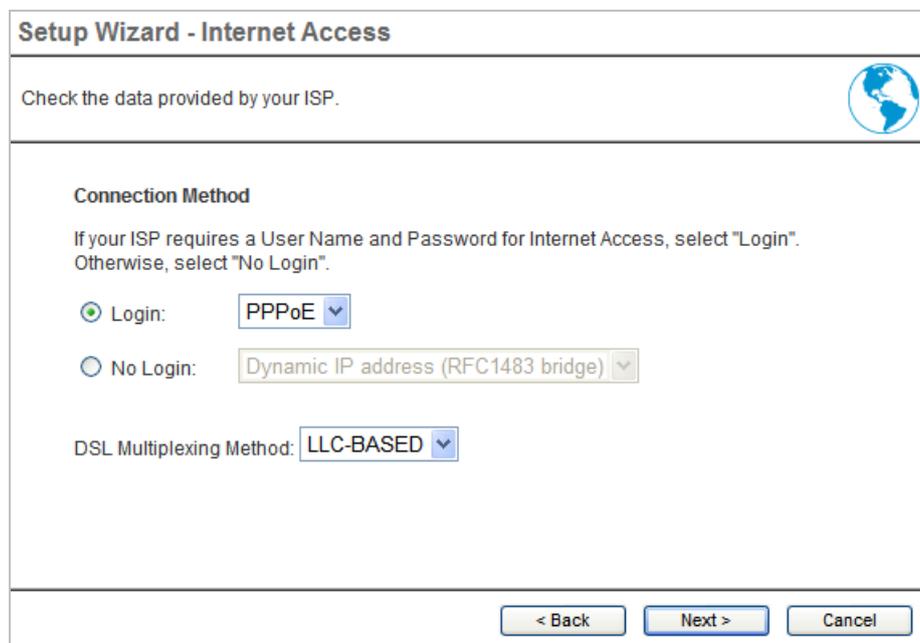
VC 1 - Primary Internet Connection

VPI: (0 ~ 255)

VCI: (32 ~ 65535)

DSL Modulation:

Figure: Setup Wizard - VC1



Setup Wizard - Internet Access

Check the data provided by your ISP.

Connection Method

If your ISP requires a User Name and Password for Internet Access, select "Login". Otherwise, select "No Login".

Login:

No Login:

DSL Multiplexing Method:

Figure: Setup Wizard - Internet Access

4. On the Internet Access Screen, shown above, select the correct connection type, as used by your ISP. Click "Next" and complete the configuration for your connection method.
 - You need the data supplied by your ISP. Your ISP's data will also have the **DSL Multiplexing Method** (LLC or VC)

The common connection types are explained in the following table.

Connection Type	Details	ISP Data required
Dynamic IP Address	Your IP Address is allocated automatically, when you connect to you ISP.	Often, none. Some ISP's may require you to use a particular Hostname or Domain name, or MAC (physical) address.
Static (Fixed) IP Address	Your ISP allocates a permanent IP Address to you. Usually, the connection is "Always on".	IP Address allocated to you, and related information, such as Network Mask, Gateway IP address, and DNS address.
PPPoE, PPPoA	You connect to the ISP only when required. The IP address is usually allocated automatically.	a) User name and password are always required. b) If using a Static (Fixed) IP address, you need the IP address and related information (Network Mask, Gateway IP address, and DNS address)
IPoA (IP over ATM)	Normally, the connection is "Always on".	IP Address allocated to you, and related information, such as Network Mask, Gateway IP address, and DNS address.

5. Step through the Wizard until finished.
6. On the final screen of the Wizard, run the test and check that an Internet connection can be established.
7. If the connection test fails:
 - Check all connections, and the front panel LEDs.
 - Make sure the data is input correctly.



Home Screen

After finishing the Setup Wizard, you will see the **Home** screen. An example screen is shown below.



Figure: Home Screen

Main Menu

The menu bar on the left of the screen contains the links to the setting pages.

The main menu page displays the current setting of this device and also contains a Log out button for administrator to log out after the configuration.

Navigation & Data Input

- Use the menu bar on the left of the screen, and the "Back" button on your Browser, for navigation.
- Changing to another screen without clicking "Save" does NOT save any changes you may have made. You must "Save" before changing screens or your data will be ignored.

3.2 LAN Screen

Use the **LAN** hyperlink on the main menu to reach the LAN screen. An example screen is shown below.

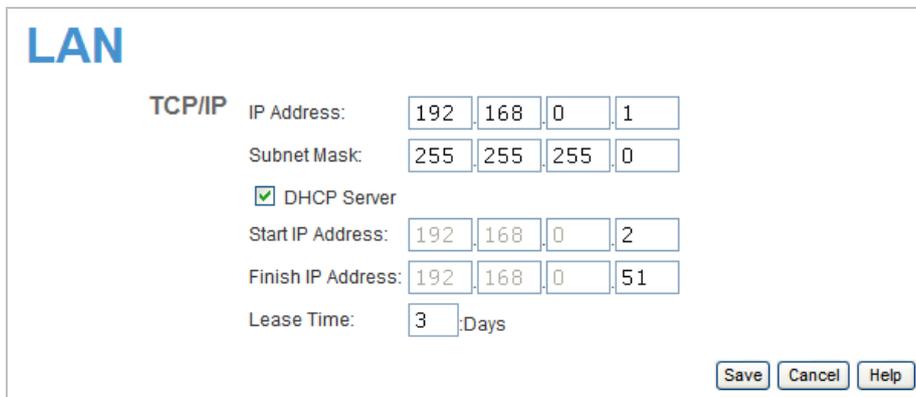


Figure 1: LAN Screen

LAN Screen

TCP/IP	
IP Address	IP address for the WN-151ARM, as seen from the local LAN. Use the default value unless the address is already in use or your LAN is using a different IP address range. In the latter case, enter an unused IP Address from within the range used by your LAN.
Subnet Mask	The default value 255.255.255.0 is standard for small (class "C") networks. For other networks, use the Subnet Mask for the LAN segment to which the WN-151ARM is attached (the same value as the PCs on that LAN segment).
DHCP Server	<ul style="list-style-type: none"> • If enabled, the WN-151ARM will allocate IP Addresses to PCs (DHCP clients) on your LAN when they start up. The default (and recommended) value is Enabled. • If you are already using a DHCP Server, this setting must be disabled, and the existing DHCP server must be re-configured to treat the WN-151ARM as the default Gateway. See the following section for further details. • The Start IP Address and Finish IP Address fields set the values used by the DHCP server when allocating IP Addresses to DHCP clients. This range also determines the number of DHCP clients supported. Enter the desired value for the Lease Time, which should be between 1 and 7. <p>See the following section for further details on using DHCP.</p>



DHCP

What DHCP Does

DHCP (Dynamic Host Configuration Protocol) **Server** allocates a valid IP address to a DHCP **Client** (PC or device) upon request.

- The client request is made when the client device starts up (boots).
- The DHCP Server provides the **Gateway** and **DNS** addresses to the client, as well as allocating an IP Address.
- The WN-151ARM can act as a **DHCP server**.
- Windows other non-Server versions of Windows will act as a DHCP **client**. This is the default Windows setting for the TCP/IP network protocol. However, Windows uses the term **Obtain an IP Address automatically** instead of "DHCP Client".
- You must NOT have two (2) or more DHCP Servers on the same LAN segment. (If your LAN does not have other Routers, this means there must only be one (1) DHCP Server on your LAN.)

Using the WN-151ARM's DHCP Server

This is the default setting. The DHCP Server settings are on the **LAN** screen. On this screen, you can:

- Enable or Disable the WN-151ARM's *DHCP Server* function.
- Set the range of IP Addresses allocated to PCs by the DHCP Server function.

Note: You can assign Fixed IP Addresses to some devices while using DHCP, provided that the Fixed IP Addresses are NOT within the range used by the DHCP Server.

Using another DHCP Server

You can only use one (1) DHCP Server per LAN segment. If you wish to use another DHCP Server, rather than the WN-151ARM's, the following procedure is required.

- Disable the DHCP Server feature in the WN-151ARM. This setting is on the LAN screen.
- Configure the DHCP Server to provide the WN-151ARM's IP Address as the **Default Gateway**.

To Configure your computer to use DHCP

This is the default setting for TCP/IP for all non-Server versions of Windows.

See **Chapter 4 - Client Configuration** for the procedure to check these settings.

3.3 Wireless Screen

The WN-151ARM will automatically accept 802.11b, 11g and 11n connections without complicated settings. To change the WN-151ARM's default settings for the Wireless Access Point feature, use the **Wireless** link on the main menu to reach the **Wireless** screen. An example screen is shown below.



Figure: Wireless Screen



Wireless Screen

Region	
Region	<p>Select the correct domain of your location. It is your responsibility to ensure:</p> <ul style="list-style-type: none"> • That the WN-151ARM is only used in domains for which is licensed. • That you select the correct domain, so that only the legal channels for that domain can be selected.
Multi SSID	
SSID	<p>With Multiple SSID, you can manage two SSID. For example, a Guest SSID without encryption for visitors to have Internet access only, and a Admin SSID with encryption for private use to secure your company resources.</p> <p>Select the desired SSID from the list to configure.</p>
SSID 1/2	<p>This is also called the "Network Name".</p> <ul style="list-style-type: none"> • If using an ESS (Extended Service Set, with multiple access points) this ID is called an ESSID (Extended Service Set Identifier). • To communicate, all Wireless stations should use the same SSID/ESSID.
Broadcast SSID	<p>If enabled, the WN-151ARM will broadcast its SSID. This allows your computer and other wireless stations to detect this Access Point and use the correct SSID for wireless connectivity.</p> <p>If disabled, computer users will have to manually enter the SSID and other details of the wireless interface before they can connect to this Access Point.</p>
Isolation within SSID	<p>If Enabled, the devices that have the same SSID will not be able to see each other.</p>
Security Setting	<p>It displays the current wireless security status. The default value is disabled.</p>
Configure SSID 1/2 Button	<p>Click this button to access the Wireless security sub-screen, and view or change the settings. See the following section for details.</p>

MAC Address Filter	
Allow access by ...	<p>Use this feature to determine which wireless client is allowed to get the wireless access. The options are:</p> <p>All Wireless Stations - All wireless client stations are allowed to use the access point, once the correct SSID and security password is entered.</p> <p>Trusted Wireless stations only - Only the wireless client station you select as "Trusted" is allowed to grant the access, others will be denied.</p> <p>Note: this feature uses the MAC address to identify Wireless client station. The MAC address is a low-level network identifier which is unique to each PC or network device.</p> <p>To define the trusted wireless stations, click on the "Set Stations" button.</p>
Set Stations Button	Click this button to manage the trusted wireless client station database.
Wi-Fi Protect Setup	
Enable WPS	Enable this if you need to use the WPS function. The default value is Enabled.
AP PIN Code	Use the default displayed value or click the Regenerate button to regenerate new pin code.
Input Client PIN Code	Enter the client's PIN code in the field and click <i>OK</i> to add the client device.

Options	
802.11 Mode	<p>Select the desired mode:</p> <ul style="list-style-type: none"> • Off - Wireless function is off. • 11b only – this device will only allow 802.11b wireless network clients to connect to it. (Maximum transfer rate is 11Mbps) • 11g only –this device will only allow 802.11g wireless network clients to connect to it. (Maximum transfer rate is 54Mbps) • 11b + 11g – this device will only allow 802.11b and 802.11g wireless network clients to connect to it. • 11b/g/n – this device will allow 802.11b, 802.11g or 802.11n wireless network clients to connect to it.
Channel No.	<p>Select the Channel you wish to use for your wireless LAN.</p> <ul style="list-style-type: none"> • If you experience interference (shown by lost connections and/or slow data transfers) please try to assign a different channel to avoid signal collision. • If using multiple Access Points, adjacent Access Points should use different Channels to reduce interference.
Extension Channel	<p>This option will be selectable under the following conditions:</p> <p>802.11 Mode: 11b+g+n Bandwidth: 20MHz + 40MHz auto Channel No.: Channel 5 ~ 9</p> <p>40MHz spectrum transmission will use up to 5 wireless channels, therefore, between channel 5 ~ 9, you can choose “Up channel” or “Down channel”. For example, channel 5 and up channel is selected, which means the wireless spectrum transmission will use channel 1 ~ 5.</p>
Isolation between SSID	<p>If Enabled, SSID1 and SSID2 will be isolated and operating independently. SSID1 users and SSID2 users will not be able to see each other.</p>
WMM Support	<p>Wi-Fi Multi Media (WMM) enhances the data transfer performance of multimedia contents when they’re being transferred over a wireless network.</p> <p>Note: This function can only be available when client’s wireless card also supports WMM feature.</p>
Bandwidth	<p>Select the desired bandwidth from the list.</p> <p>Note: Do not modify the default value if you aren’t familiar with this function.</p>

WDS	
Enable WDS	This feature allows you to connect multiple access points and build up a huge wireless network. In order to make the WDS work properly, the access points must use the same channel, SSID, as well as the wireless encryption method.
MAC Address List	Enter the MAC address of the AP that you wish to build up the WDS connection.

3.4 Wireless Security

This screen is accessed by clicking the "**Configure SSID**" button on the **Wireless** screen. There are 3 options for Wireless security:

- **Disabled** - no data encryption is used.
- **WEP** - data is encrypted using the WEP standard.
- **WPA-PSK** - data is encrypted using the WPA-PSK standard. This is a later standard than WEP, and provides much better security than WEP. If all your Wireless stations support WPA-PSK, you should use WPA-PSK rather than WEP.
- **WPA2-PSK** - This is a further development of WPA-PSK, and offers even greater security, using the AES (Advanced Encryption Standard) method of encryption.
- **Mixed WPA-PSK/WAP2-PSK** - This method, sometimes called "Mixed Mode", allows clients to use EITHER WPA-PSK OR WPA2-PSK.
- **WPA-802.1x** - This version of WPA requires a Radius Server on your LAN to provide the client authentication according to the 802.1x standard. Data transmissions are encrypted using the WPA standard.

If this option is selected:

- This Access Point must have a "client login" on the Radius Server.
- Each user must have a "user login" on the Radius Server.
- Each user's wireless client must support 802.1x and provide the login data when required.
- All data transmission is encrypted using the WPA standard. Keys are automatically generated, so no key input is required.

WEP Wireless Security

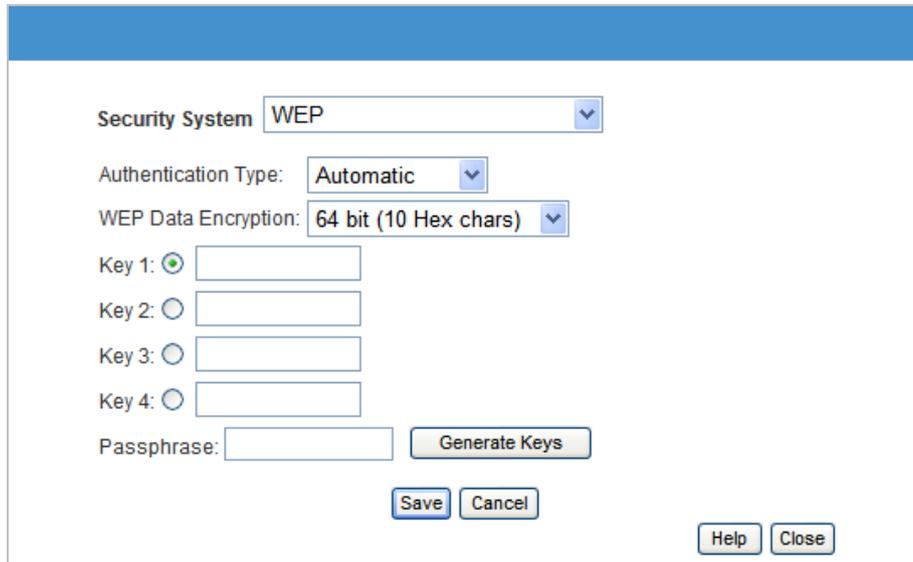
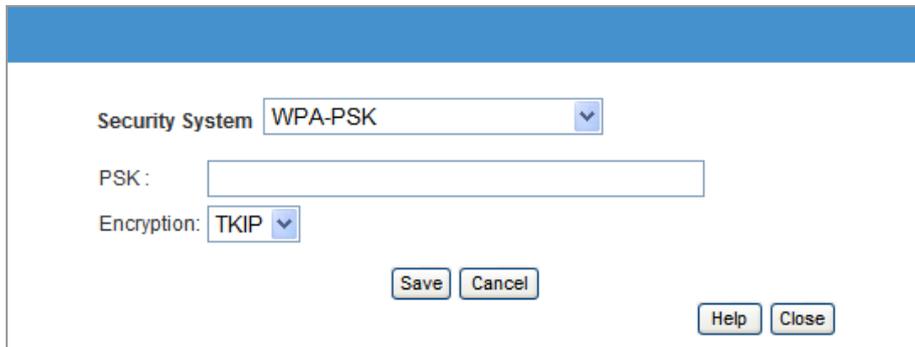


Figure: WEP

WEP Screen

WEP Data Encryption	
Authentication Type	Normally, this should be left at the default value of "Automatic". If changed to "Open System" or "Shared Key", ensure that your wireless client station uses the same setting.
WEP Data Encryption	Select the desired option, and ensure the Wireless Stations use the same setting. <ul style="list-style-type: none"> • 64 Bit - data is encrypted, using the default key, before being transmitted. You must enter at least the default key. For 64 Bit Encryption, the key size is 10 chars in HEX (0~9 and A~F). • 128 Bit - data is encrypted, using the default key, before being transmitted. You must enter at least the default key. For 128 Bit Encryption, the key size is 26 chars in HEX (0~9 and A~F).
Default Key	Select the key you wish to be the default. Transmitted data is ALWAYS encrypted using the Default Key; the other Keys are for decryption only. You must enter a Key Value for the Default Key .
Key Value	Enter the key value or values you wish to use. The Default Key is required, the other keys are optional. Other stations must have the same key.
Passphrase	If desired, you can generate a key from a phrase, instead of entering the key value directly. Enter the desired phrase, and click the "Generate Keys" button.

WPA-PSK Wireless Security



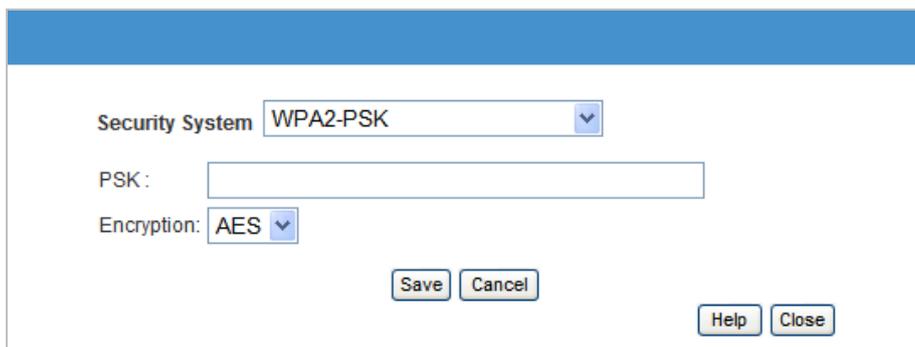
The screenshot shows a configuration dialog box for WPA-PSK. It features a blue header bar. Below the header, there are three main fields: 'Security System' with a dropdown menu set to 'WPA-PSK', 'PSK' with an empty text input field, and 'Encryption' with a dropdown menu set to 'TKIP'. At the bottom of the dialog, there are four buttons: 'Save', 'Cancel', 'Help', and 'Close'.

Figure: WPA-PSK

WPA-PSK Screen

WPA-PSK Data Encryption	
PSK	Enter the PSK (network key). Data is encrypted using a key derived from the network key. Other Wireless Stations must use the same network key. The PSK must be from 8 to 63 characters in length.
Encryption	The WPA-PSK standard allows different encryption methods to be used. Select the desired option. Wireless Stations must use the same encryption method.

WPA2-PSK Wireless Security



The screenshot shows a configuration dialog box for WPA2-PSK. It features a blue header bar. Below the header, there are three main fields: 'Security System' with a dropdown menu set to 'WPA2-PSK', 'PSK' with an empty text input field, and 'Encryption' with a dropdown menu set to 'AES'. At the bottom of the dialog, there are four buttons: 'Save', 'Cancel', 'Help', and 'Close'.

Figure: WPA2-PSK

WPA2-PSK Screen

WPA2-PSK Data Encryption	
Authentication	This is a further development of WPA-PSK, and offers even greater security.
PSK	Enter the PSK (network key). Data is encrypted using a key derived from the network key. Other Wireless Stations must use the same network key. The PSK must be from 8 to 63 characters in length.
Encryption	The WPA2-PSK standard allows different encryption methods to be used. Select the desired option. Wireless Stations must use the same encryption.

Mixed WPA-PSK/WAP2-PSK Wireless Security

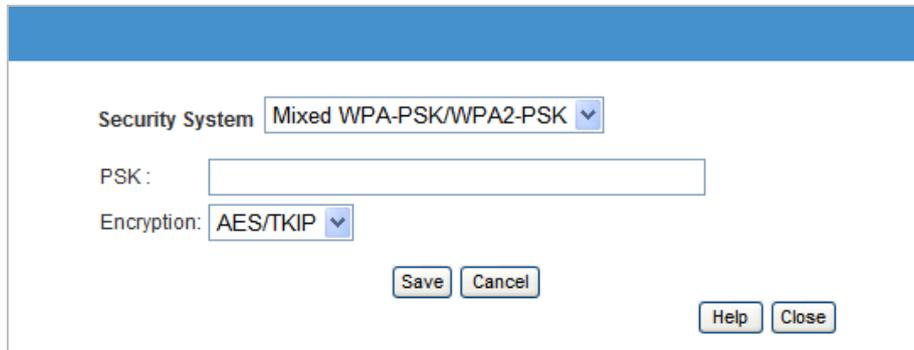
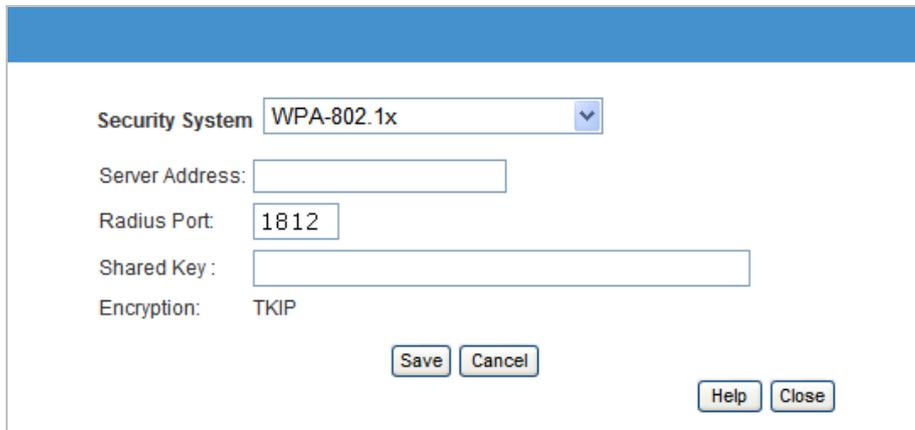


Figure: Mixed WPA-PSK/WAP2-PSK

Mixed WPA-PSK/WAP2-PSK Screen

Mixed WPA-PSK/WAP2-PSK Data Encryption	
Authentication	This method, sometimes called "Mixed Mode", allows client to use WPA-PSK OR WPA2-PSK.
PSK	Enter the PSK (network key). Data is encrypted using a key derived from the network key. Other wireless client stations must use the same network key. The PSK must be from 8 to 63 characters in length.
Encryption	The Mixed WPA-PSK/WAP2-PSK standard allows different encryption methods to be used. Select the desired option. Wireless client station must use the same encryption method.

WPA-802.1x Wireless Security



Security System: WPA-802.1x

Server Address:

Radius Port: 1812

Shared Key:

Encryption: TKIP

Buttons: Save, Cancel, Help, Close

Figure: WPA-802.1x

WPA-802.1x Screen

WPA-802.1x Data Encryption	
Server Address	Enter the server address here.
Radius Port	Enter the port number used for connections to the Radius Server.
Shared Key	Enter the shared key. Data is encrypted using a key derived from the network key. Other Wireless Stations must use the same key. The key must be from 8 to 63 characters in length.
Encryption	The encryption method is TKIP. Wireless Stations must also use TKIP.

Trusted Wireless Stations

This feature can be used to prevent unknown wireless client stations from using the Access Point. This list has no effect unless the setting **Allow access by trusted stations only** is enabled.

To change the list of trusted wireless stations, use the **Modify List** button on the **Access Control** screen. You will see a screen like the sample below.

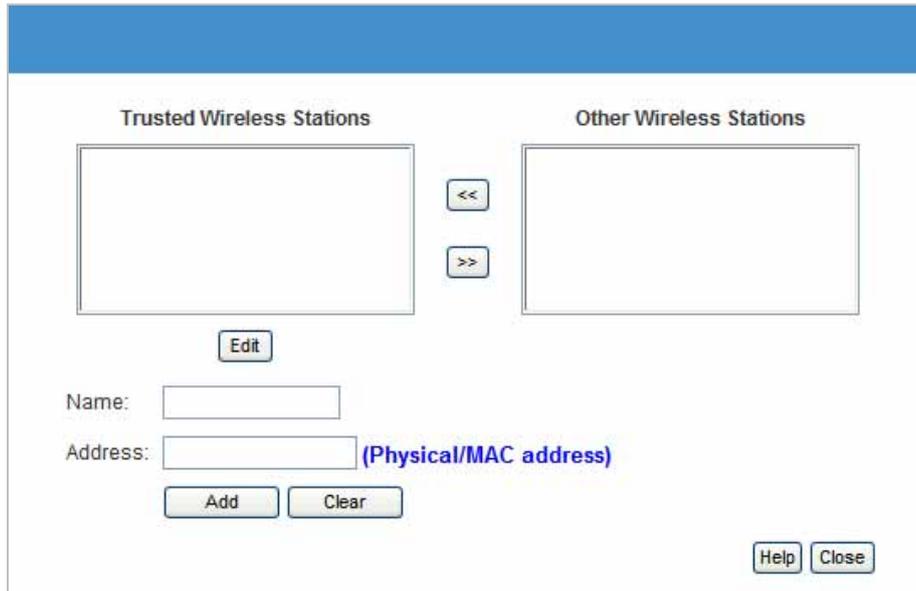


Figure: Trusted Wireless Stations

Trusted Wireless Stations

Trusted Wireless Stations	
Trusted Wireless Stations	This lists is listed all the wireless client station which you have designated as "Trusted".
Other Wireless Stations	This list any Wireless Stations detected by the Access Point, which you have not designated as "Trusted".
Name	The name assigned to the Trusted Wireless Station. Use this when adding or editing a Trusted station.
Address	The MAC (physical) address of the Trusted wireless client station. Use this when adding or editing a Trusted client station.

Buttons	
<<	<p>Add a Trusted wireless client station to the list (move from the "Other Stations" list).</p> <ul style="list-style-type: none"> • Select an entry (or entries) in the "Other Stations" list, and click the "<<" button. • Enter the Address (MAC or physical address) of the wireless station, and click the "Add" button.
>>	<p>Delete a Trusted wireless client station from the list (move to the "Other Stations" list).</p> <ul style="list-style-type: none"> • Select an entry (or entries) in the "Trusted Stations" list. • Click the ">>" button.
Edit	<p>Use this to change an existing entry in the "Trusted Stations" list:</p> <ol style="list-style-type: none"> 1. Select the Station in the Trusted Station list. 2. Click the Edit button. The address will be copied to the "Address" field, and the Add button will change to Update. 3. Edit the address (MAC or physical address) as required. 4. Click Update to save your changes.
Add (Update)	<p>To add a Trusted Station which is not in the "Other Wireless Stations" list, enter the required data and click this button.</p> <p>When editing an existing Wireless Station, this button will change from Add to Update.</p>
Clear	<p>Clear the <i>Name</i> and Address fields.</p>

3.5 Password Screen

The password screen allows you to assign a password to the WN-151ARM.

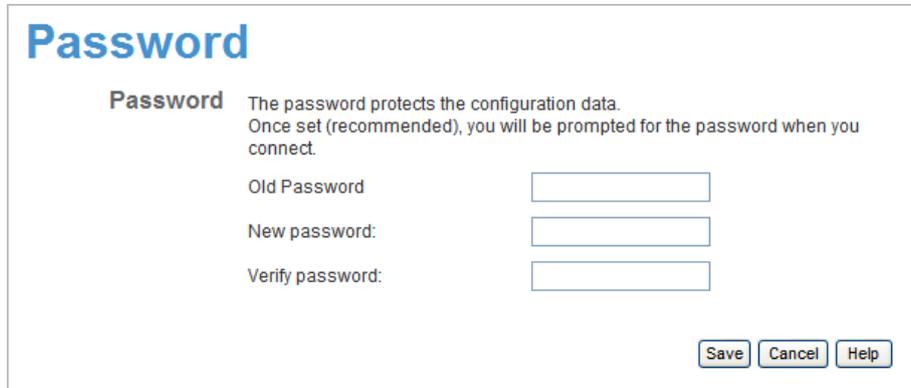


Figure: Password Screen

Old Password	Enter the existing password in this field.
New password	Enter the new password here.
Verify password	Re-enter the new password here.

You will be prompted for the password when you connect, as shown below.

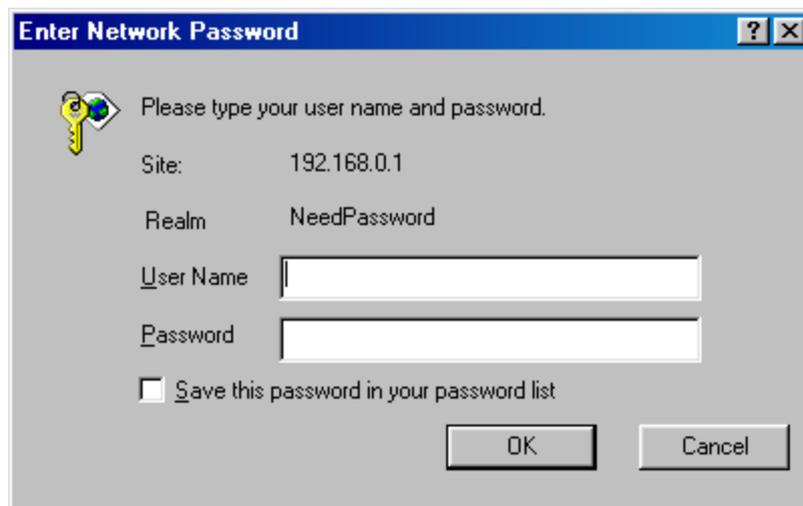


Figure: Password Dialog

- The "User Name" is always admin
- Enter the password for the WN-151ARM, as set on the **Password** screen above.

3.6 Mode Screen

Use this screen to change the mode between Router mode and Modem (Bridge) mode.



Figure: Mode Screen

Select the desired option, and click "Save".

Router (Modem + Router)	Both the ADSL Modem and the Router features are operational. In this mode, this device can provide shared Internet Access to all your LAN users. Also, by default, it acts a DHCP Server, providing an IP address and related information to all Wireless and LAN users.
Modem	Only the ADSL Modem component is operating. <ul style="list-style-type: none"> • All Router features are disabled. This device is "transparent" - it does not perform any operations or make any changes to the network traffic passing through it. • You need to have a DHCP Server on your LAN to provide IP addresses to the Wireless clients using this Access Point. • All traffic received on either the Wireless or LAN interface will be sent over the ADSL connection.

Notes:

- Generally, you should NOT use modem mode. Only select this mode if you are sure this is what you want.
- After changing the mode, this device will restart, which will take few seconds. The menu will also change, depending on the mode you are in.
- The Wireless Access Point can function in either Router or Modem mode. But generally it is not a good idea to combine a Modem with an Access Point because all data received from the wireless stations will be sent over the modem connection. (Since the modem is transparent, it does not examine the traffic to determine whether the traffic is for the LAN or the WAN.)
- For details on using Modem Mode, see Chapter 8.

4

Operation and Status

Operation - Router Mode

Once both the WN-151ARM and the computers are configured, operation is automatic.

However, there are some situations where additional Internet configuration may be required. Refer to

Chapter 6 - Advanced Features for further details.

Operation - Router Mode

Use the **Status** link on the main menu to view this screen.



The screenshot displays the 'Status' page of the Air Live WN-151ARM router. The page is organized into several sections, each with its own set of status information:

- ADSL:** Modem Status (Negotiating), DownStream Connection Speed (0 kbps), UpStream Connection Speed (0 kbps).
- Internet:** Connection Method (DHCP), Connection Status (Idle), Internet IP Address (---), Wan MAC Address (00:c0:02:ff:cb:2b). A 'Connection Details' button is located below this section.
- LAN:** IP Address (192.168.1.254), Network Mask (255.255.255.0), DHCP Server (On), MAC Address (00:C0:02:FF:CB:2A).
- Wireless:** SSID1 (airlive), MAC Address (00:C0:02:FF:CB:2A), SSID2 (Guest), MAC Address (00:c0:02:ff:cb:2b), Region (--), Channel (6), Wireless AP (enable), Broadcast Name (enable).
- System:** Device Name (Airlive), Firmware Version (1.00.00).

Additional interface elements include a 'Log Out' button in the left sidebar, and 'Attached Devices', 'Refresh Screen', and 'Help' buttons at the bottom right of the main content area.

Figure: Status Screen

Status Screen

ADSL	
Modem Status	This indicates the status of the ADSL modem component.
DownStream Connection Speed	Displays the speed for the DownStream Connection.
UpStream Connection Speed	Displays the speed for the Up Stream (upload) ADSL Connection.
Internet (VC1)	
Connection Method	Displays the current connection method, as set in the Setup Wizard .
Connection Status	<p>This indicates the current status of the Internet Connection</p> <ul style="list-style-type: none"> • Active - Connection exists • Idle - No current connection, but no error has been detected. This condition normally arises when an idle connection is automatically terminated. • Failed - The connection was terminated abnormally. This could be caused by Modem failure or the loss of the connection to the ISP's server. <p>If there is an error, you can click the "Connection Details" button to find out more information.</p>
Internet IP Address	This IP Address is allocated by the ISP (Internet Service Provider). If using a dynamic IP address and no connection currently exists, this information is unavailable.
WAN MAC Address	It displays the MAC address for the WAN.
Connection Details	Click this button to open a sub-window and view a detailed description of the current connection. Depending on the type of connection, a "log" may also be available.
LAN	
IP Address	The IP Address of the WN-151ARM.
Network Mask	The Network Mask (Subnet Mask) for the IP Address above.
DHCP Server	This shows the status of the DHCP Server function. The value will be "On" or "Off".
MAC Address	This shows the MAC Address for the WN-151ARM, as seen on the LAN interface.

Wireless	
SSID 1	It displays the name of the SSID 1.
SSID 2	It displays the name of the SSID 2.
Region	The current region, as set on the Wireless screen.
Channel	This shows the Channel currently used, as set on the Wireless screen.
Wireless AP	This indicates whether or not the Wireless Access Point feature is enabled.
Broadcast Name	This indicates whether or not the SSID is Broadcast. This setting is on the Wireless screen.
System	
Device Name	The current name of the device. This name is also the "hostname" for users with "@Home" type connection.
Firmware Version	The version of the current firmware installed.
Buttons	
Connection Details	Click this button to open a sub-window and view a detailed description of the current connection.
Attached Devices	This will open a sub-window, showing all LAN and Wireless devices currently on the network.
Refresh Screen	Update the data displayed on screen.
Help	The description of Status item.

Connection Status - PPPoE & PPPoA

If using PPPoE (PPP over Ethernet) or PPPoA (PPP over ATM), a screen like the following example will be displayed when the "Connection Details" button is clicked.

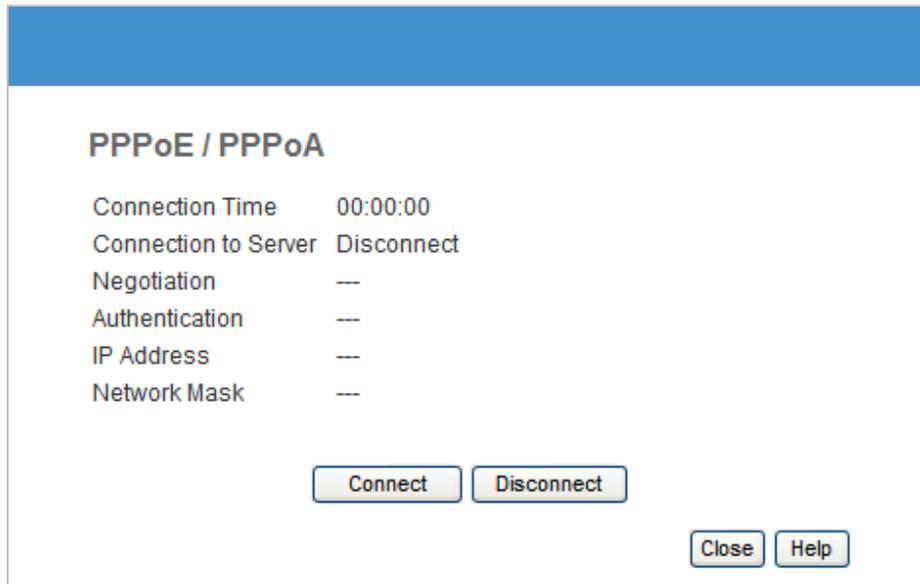


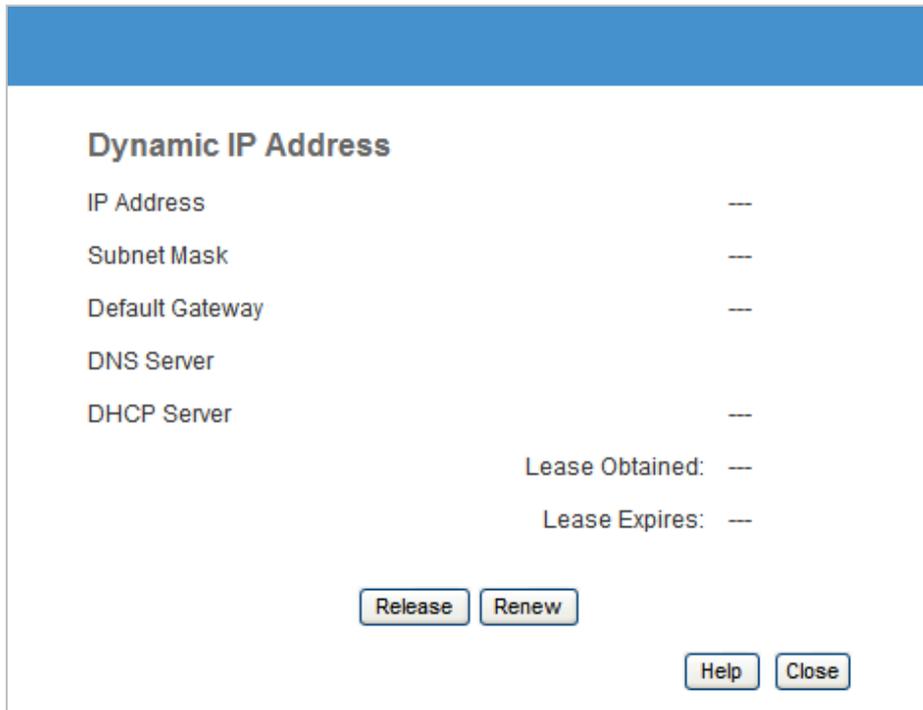
Figure: PPPoE Status Screen

PPPoE/PPPoA Screen

Connection Time	This indicates how long the current connection has been established.
Connection to Server	This indicates whether or not the connection is currently established. <ul style="list-style-type: none"> • If the connection does not exist, the "Connect" button can be used to establish a connection. • If the connection currently exists, the "Disconnect" button can be used to break the connection.
Negotiation	This indicates the status of the PPPoE Server login.
IP Address	The IP Address of this device, as seen by Internet users. This address is allocated by your ISP (Internet Service Provider).
Network Mask	The Network Mask associated with the IP Address above.
Buttons	
Connect	If not connected, establish a connection to your ISP.
Disconnect	If connected to your ISP, hang up the connection.
Close	Close this window.

Connection Details - Dynamic IP Address

If your access method is "Direct" (no login), with a Dynamic IP address, a screen like the following example will be displayed when the "Connection Details" button is clicked.



Dynamic IP Address	
IP Address	--
Subnet Mask	--
Default Gateway	--
DNS Server	--
DHCP Server	--
Lease Obtained:	--
Lease Expires:	--
<input type="button" value="Release"/> <input type="button" value="Renew"/>	
<input type="button" value="Help"/> <input type="button" value="Close"/>	

Figure: Connection Details - Fixed/Dynamic IP Address

Dynamic IP address

Internet	
IP Address	The current IP Address of this device, as seen by Internet users. This address is allocated by your ISP (Internet Service Provider).
Network Mask	The Network Mask associated with the IP Address above.
Default Gateway	The IP address of the remote Gateway or Router associated with the IP Address above.
DNS Server	The IP address of the Domain Name Server which is currently used.
DHCP Server	The IP address of your ISP's DHCP Server.
Lease Obtained Lease Expires	This indicates when the current IP address was obtained, and how long before this IP address allocation (the DHCP lease) expires.
Buttons	
Release	If an IP Address has been allocated to the WN-151ARM (by the ISP's DHCP Server), clicking the "Release" button will break the connection and release the IP Address.
Renew	If the ISP's DHCP Server has NOT allocated an IP Address for the WN-151ARM, clicking the "Renew" button will attempt to re-establish the connection and obtain an IP Address from the ISP's DHCP Server.

Connection Details - Fixed IP Address

If your access method is "Direct" (no login), with a fixed IP address, a screen like the following example will be displayed when the "Connection Details" button is clicked.

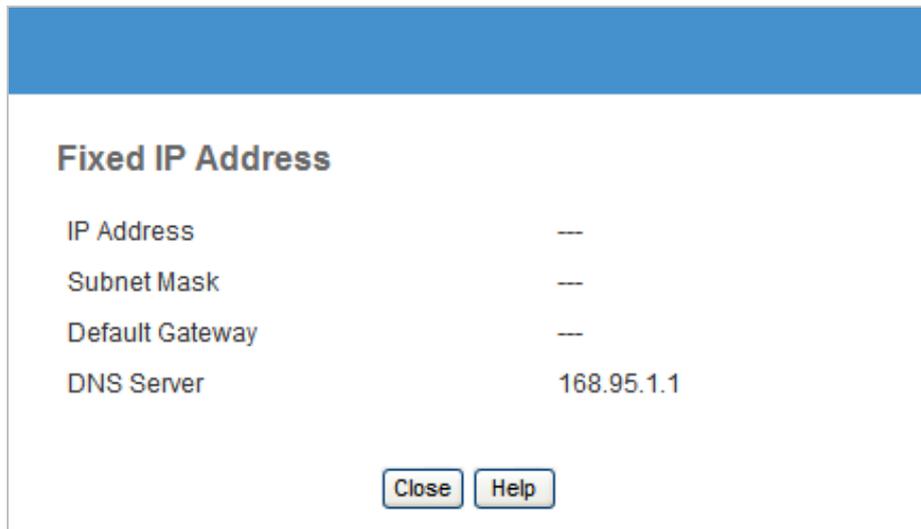


Figure: Connection Details - Fixed/Dynamic IP Address

Fixed IP address Screen

Internet	
IP Address	The IP Address of this device, as seen by Internet users. This address is allocated by your ISP (Internet Service Provider).
Subnet Mask	The Subnet Mask associated with the IP Address above.
Default Gateway	The IP Address of the remote Gateway or Router associated with the IP Address above.
DNS Server	The IP Address of the Domain Name Server which is currently used.

5

Advanced Features

Overview

The following advanced features are provided:

- Internet:
 - DMZ
 - URL filter
- Access Control
- Dynamic DNS
- Options
- Schedule
- Port Trigger
- Port Forward
- Port Range Forward
- QoS

5.1 Internet

This screen provides the access to the DMZ, Special Applications and URL Filter features.



Figure: Internet Screen

DMZ

The DMZ host is a local computer exposed to the Internet. For example, if you have a local computer that cannot run an Internet application properly behind the NAT firewall, then you can open the client up to unrestricted two-way access by defining a DMZ host.

Note: The DMZ host is effectively outside the Firewall, making it more vulnerable to be attacked. For this reason, you should only enable the DMZ feature when is necessary.

URL Filter

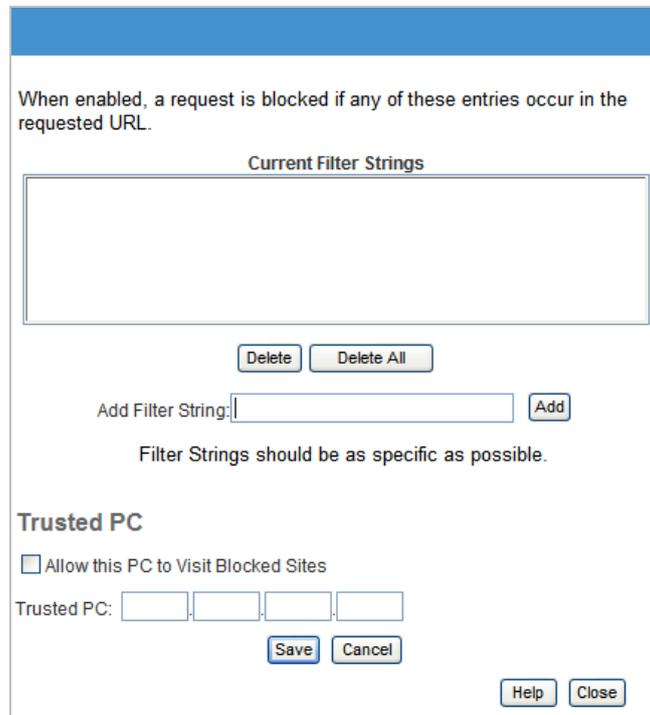
The URL filter will limit the access to certain websites on the Internet. The URL filter will check each Website access. If the address or part of the address is included in the block site list, access will be denied.

Click *Advanced, Internet*, select the desired setting:

- **Disable** - disable this feature.
- **Block Always** – Enabled the URL filter and block the URL filter list the all time.
- **Block By Schedule** - block according to the settings on the **Schedule** page.

Click the **Configure URL Filter** button to open the URL Filter screen and allows you to create or modify the filter strings which determine which sites to be blocked.

The **URL Filter** screen is displayed when the **Configure URL Filter** button on the **Advanced Internet** screen is clicked.



When enabled, a request is blocked if any of these entries occur in the requested URL.

Current Filter Strings

Delete Delete All

Add Filter String: Add

Filter Strings should be as specific as possible.

Trusted PC

Allow this PC to Visit Blocked Sites

Trusted PC: ...

Save Cancel

Help Close

Figure: URL Filter Screen



URL Filter Screen

Current Filter Strings	
Current Filter Strings	<p>The list contains the website to be blocked.</p> <ul style="list-style-type: none">• To add to the list, use the "Add" option below.• To delete an entry, select it and click Delete button.• To delete all entries, click the Delete All button.
Add Filter String	<p>To add to the list, type-in the website address or domain name you want to block into the field provided, and then click the Add button. Filter strings should be as specific as possible. Otherwise, you may block access to the wrong sites.</p>
Trusted PC	
Allow this PC to Visit Blocked Sties	<p>Enable this to allow one computer to have unrestricted access to the Internet. For this PC, the URL filter will be ignored. If enabled, you must select the PC to be the trusted PC.</p>
Trusted PC	<p>Enter the IP address and make it the Trusted PC.</p>

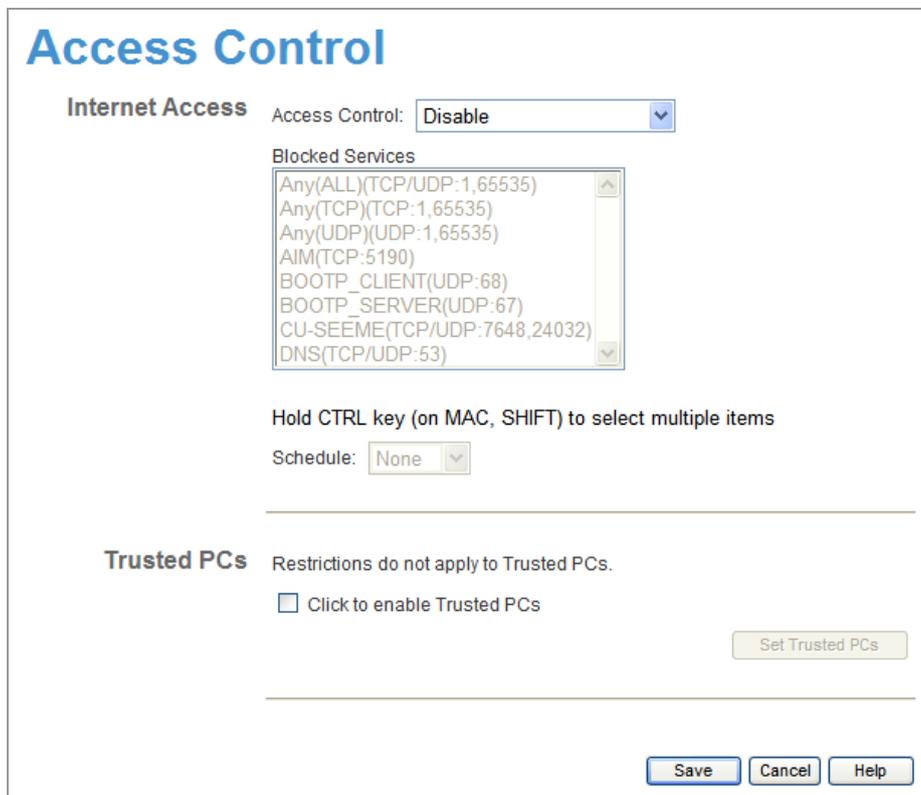
5.2 Access Control

Overview

The Access Control feature allows administrators to restrict the level of Internet Access available to PCs on your LAN. With the default settings, everyone has unrestricted Internet access.

Access Control Screen

To view this screen, select the **Access Control** link on the **Advanced** menu.



The screenshot shows the 'Access Control' configuration page. At the top, the title 'Access Control' is displayed in blue. Below it, the 'Internet Access' section has an 'Access Control' dropdown menu set to 'Disable'. Underneath is a 'Blocked Services' list box containing several entries: Any(ALL)(TCP/UDP:1,65535), Any(TCP)(TCP:1,65535), Any(UDP)(UDP:1,65535), AIM(TCP:5190), BOOTP_CLIENT(UDP:68), BOOTP_SERVER(UDP:67), CU-SEEME(TCP/UDP:7648,24032), and DNS(TCP/UDP:53). Below the list is a note: 'Hold CTRL key (on MAC, SHIFT) to select multiple items'. A 'Schedule' dropdown menu is set to 'None'. The 'Trusted PCs' section states 'Restrictions do not apply to Trusted PCs.' and includes a checkbox for 'Click to enable Trusted PCs' which is currently unchecked. A 'Set Trusted PCs' button is located to the right of this checkbox. At the bottom right of the page are three buttons: 'Save', 'Cancel', and 'Help'.

Figure: Access Control Screen



Access Control Screen

Internet Access	
Access Control	Select the desired options for the current group: <ul style="list-style-type: none">• Disable - Nothing is blocked. Use this to create the least restrictive group.• Block all Internet access - All traffic via the WAN port is blocked. Use this to create the most restrictive group.• Block selected Services - You can select which Services are to block. Use this to gain fine control over the Internet access for a group.
Blocked Services	This lists all defined Services. Select the Services you wish to block. To select multiple services, hold the CTRL key while selecting. (On the Macintosh, hold the SHIFT key rather than CTRL.)
Schedule	If Internet access is being blocked, you can choose to apply the blocking only during scheduled times. (If access is not blocked, no Scheduling is possible, and this setting has no effect.)
Trusted PCs	
Click to Enable Trusted PC	If enabled, restrictions set on this screen do not apply to Trusted PCs.
"Set Trusted PCs" Button	Click this button to add or remove PCs of the Trusted PCs. See the following section for details of the <i>Trusted PCs</i> screen.

Trusted PC Screen

This screen is displayed when the **Set Trusted PCs** button on the **Access Control** screen is clicked.

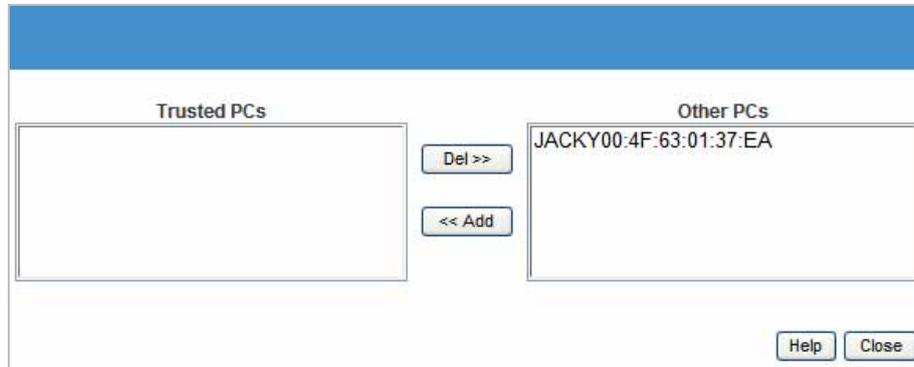


Figure: Trusted PC Screen

Use this screen to add or remove PCs from the current group.

- The "Del >>" button will remove the selected PC (in the **Trusted PCs** list) from the current group.
- The "<< Add" button will add the selected PC (in the **Other PCs** list) to the Trusted PCs group.

5.3 Dynamic DNS

DDNS allows mapping of the static domain name to a dynamic IP address. Obtain an account, password and static domain name from the DDNS service providers.

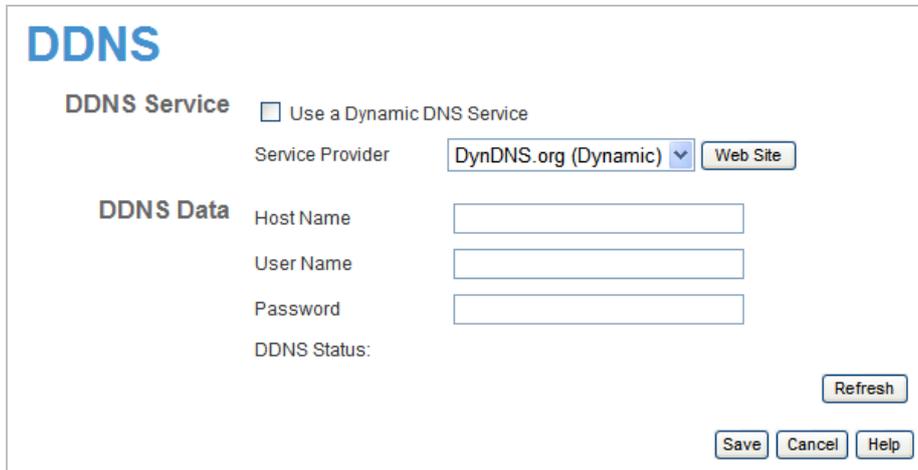
This free service is very useful when combining with the **Virtual Server** feature. It allows Internet users to connect to your Virtual Servers using a URL, rather than an IP Address.

DDNS Services work as follows:

1. You must register for the service at one of the listed DDNS Service providers.
2. After registration, use the Service provider's normal procedure to obtain your desired Domain name.
3. Enter your DDNS data on the WN-151ARM's DDNS screen, and enable the DDNS feature.
4. The WN-151ARM will then automatically ensure that your current IP Address is recorded at the DDNS service provider's Domain Name Server.
5. From the Internet, users will be able to connect to your Virtual Servers (or DMZ PC) using your Domain name, as shown on this screen.

Dynamic DNS Screen

Select **Advanced** on the main menu, then **Dynamic DNS**, to see a screen like the following:



The screenshot shows a web interface titled "DDNS". It has two main sections: "DDNS Service" and "DDNS Data".

- DDNS Service:** Includes a checkbox labeled "Use a Dynamic DNS Service" which is currently unchecked. Below it is a "Service Provider" dropdown menu set to "DynDNS.org (Dynamic)" and a "Web Site" button.
- DDNS Data:** Includes three input fields for "Host Name", "User Name", and "Password". Below these is a "DDNS Status:" label.

At the bottom right of the form are three buttons: "Refresh", "Save", "Cancel", and "Help".

Figure: DDNS Screen

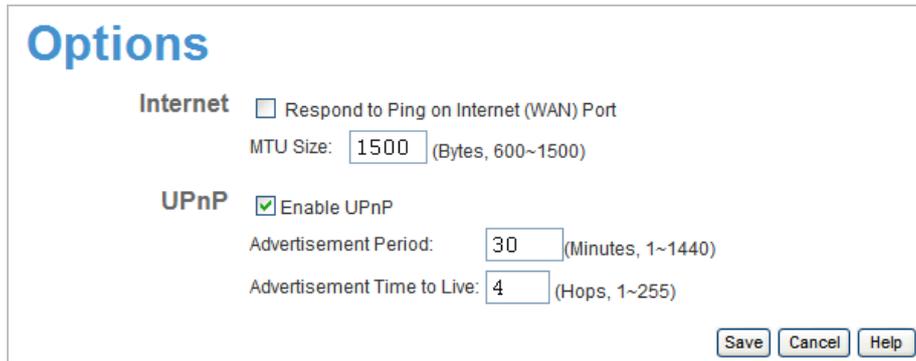
Dynamic DNS Screen

DDNS Service	
Use a Dynamic DNS Service	Use this to enable or disable the DDNS feature as required.
Service Provider	Select the desired DDNS Service provider.
Website	Click this button to open a new window and connect to the Website of the selected DDNS service provider.
DDNS Data	
Host Name	Enter the domain name allocated to you by the DDNS Service. If you have more than one name, enter the name you wish to use.
User Name	Enter your Username for the DDNS Service. (TZO.com uses your E-mail address.)
Password	Enter your current password for the DDNS Service. (TZO.com calls this a key.)
DDNS Status	<ul style="list-style-type: none"> • This message is returned by the DDNS Server. • Normally, this message should be "Update successful" • If the message indicates some problem, you need to connect to the DDNS Service provider and correct this problem.

5.4 Option

This screen allows advanced users to enter or change a number of settings. For normal operation, there is no need to use this screen or change any settings.

An example **Options** screen is shown below.



The screenshot shows the 'Options' configuration screen. It is divided into two main sections: 'Internet' and 'UPnP'. In the 'Internet' section, there is a checkbox for 'Respond to Ping on Internet (WAN) Port' which is currently unchecked. Below it is a text input field for 'MTU Size' with the value '1500' and a note '(Bytes, 600~1500)'. In the 'UPnP' section, there is a checked checkbox for 'Enable UPnP'. Below it are two text input fields: 'Advertisement Period' with the value '30' and note '(Minutes, 1~1440)', and 'Advertisement Time to Live' with the value '4' and note '(Hops, 1~255)'. At the bottom right of the form are three buttons: 'Save', 'Cancel', and 'Help'.

Figure: Options Screen

Options Screen

Internet	
Respond to Ping	<ul style="list-style-type: none"> • If checked, the WN-151ARM will respond to Ping (ICMP) packets received from the Internet. • If not checked, Ping (ICMP) packets from the Internet will be ignored. Disabling this option provides a slight increase in security.
MTU Size	Enter a value between 600 and 1500. Note: MTU (Maximum Transmission Unit) size should only be changed if advised to do so by Technical Support.
UPnP	
Enable UPnP	<ul style="list-style-type: none"> • UPnP (Universal Plug and Play) allows automatic discovery and configuration of equipment attached to your LAN. UPnP is supported by Windows ME, XP, or later. • If Enabled, this device will be visible via UPnP. • If Disabled, this device will not be visible via UPnP.
Advertisement Period	Enter the desired value, in minutes. The valid range is from 1 to 1440.
Advertisement Time to Live	Enter the desired value, in hops. The valid range is from 1 to 255.

5.5 Schedule

This Schedule can be used for the Firewall Rules and the URL filter.

Schedule

Schedule Use 24 hour clock. On all day: 00:00 to 24:00
Off all day: All fields left 00

Day	Session 1		Session 2	
	Start	Finish	Start	Finish
Monday	00:00	12:00	12:00	24:00
Tuesday	00:00	12:00	12:00	24:00
Wednesday	00:00	12:00	12:00	24:00
Thursday	00:00	12:00	12:00	24:00
Friday	00:00	12:00	12:00	24:00
Saturday	00:00	12:00	12:00	24:00
Sunday	00:00	12:00	12:00	24:00

Local Time Time Zone: (GMT-08:00) Pacific Time(US, Canada); Tijuana ▼

Adjust for Daylight Savings Time

Use this NTP Server

Current Time: 1999-12-31 16:57:31 Weekday :Friday

Save
Cancel
Help

Figure: Schedule Screen

Schedule Screen

Schedule	
Day	Each day of the week can be scheduled independently.
Session 1 Session 2	Two (2) separate sessions or periods can be defined. Session 2 can be left blank if not required.
Start Time	Enter the start using a 24 hr clock.
Finish Time	Enter the finish time using a 24 hr clock.
Local Time	
Time Zone	In order to display your local time correctly, you must select your "Time Zone" from the list.
Adjust for Daylight Savings Time	If your region uses Daylight Savings Time, you must manually check "Adjust for Daylight Savings Time" at the beginning of the adjustment period, and uncheck it at the end of the Daylight Savings period.
Use this NTP Server	If you prefer to use a particular NTP server as the primary NTP server, check the checkbox "Use this NTP Server" and enter the Server's IP address in the fields provided. If this setting is not enabled, the default NTP Servers is used.
Current Time	This displays the current time on the WN-151ARM, at the time the page is loaded.

5.6 Port Trigger

If you use Internet applications which use non-standard connections or port numbers, you may find that they do not function correctly because they are blocked by the WN-151ARM's firewall. In this case, you can define the application as a "Port Trigger".

The **Port Trigger** screen can be reached by clicking the **Port Trigger** on the screen.

You can then define your Port Trigger. You will need detailed information about the application; this is normally available from the supplier of the application.

Also, note that the terms "Incoming" and "Outgoing" on this screen refer to traffic from the client (PC) viewpoint

Port Trigger

Enable	Name	Outgoing Ports			Incoming Ports		
		Type	Start	Finish	Type	Start	Finish
1. <input type="checkbox"/>	<input type="text"/>	TCP ▾	<input type="text"/>	<input type="text"/>	TCP ▾	<input type="text"/>	<input type="text"/>
2. <input type="checkbox"/>	<input type="text"/>	TCP ▾	<input type="text"/>	<input type="text"/>	TCP ▾	<input type="text"/>	<input type="text"/>
3. <input type="checkbox"/>	<input type="text"/>	TCP ▾	<input type="text"/>	<input type="text"/>	TCP ▾	<input type="text"/>	<input type="text"/>
4. <input type="checkbox"/>	<input type="text"/>	TCP ▾	<input type="text"/>	<input type="text"/>	TCP ▾	<input type="text"/>	<input type="text"/>
5. <input type="checkbox"/>	<input type="text"/>	TCP ▾	<input type="text"/>	<input type="text"/>	TCP ▾	<input type="text"/>	<input type="text"/>
6. <input type="checkbox"/>	<input type="text"/>	TCP ▾	<input type="text"/>	<input type="text"/>	TCP ▾	<input type="text"/>	<input type="text"/>
7. <input type="checkbox"/>	<input type="text"/>	TCP ▾	<input type="text"/>	<input type="text"/>	TCP ▾	<input type="text"/>	<input type="text"/>
8. <input type="checkbox"/>	<input type="text"/>	TCP ▾	<input type="text"/>	<input type="text"/>	TCP ▾	<input type="text"/>	<input type="text"/>
9. <input type="checkbox"/>	<input type="text"/>	TCP ▾	<input type="text"/>	<input type="text"/>	TCP ▾	<input type="text"/>	<input type="text"/>
10. <input type="checkbox"/>	<input type="text"/>	TCP ▾	<input type="text"/>	<input type="text"/>	TCP ▾	<input type="text"/>	<input type="text"/>
11. <input type="checkbox"/>	<input type="text"/>	TCP ▾	<input type="text"/>	<input type="text"/>	TCP ▾	<input type="text"/>	<input type="text"/>
12. <input type="checkbox"/>	<input type="text"/>	TCP ▾	<input type="text"/>	<input type="text"/>	TCP ▾	<input type="text"/>	<input type="text"/>

Figure: Port Trigger Screen

Port Trigger Screen

Port Trigger	
Enable	Use this to Enable or Disable this Special Application as required.
Name	Enter a descriptive name to identify this Special Application.
Outgoing Ports	<ul style="list-style-type: none"> • Type - Select the protocol (TCP or UDP) used when you send data to the remote system or service. • Start - Enter the beginning of the range of port numbers used by the application server, for data you send to it. If the application uses a single port number, enter it in both the "Start" and "Finish" fields. • Finish - Enter the end of the range of port numbers used by the application server, for data you send to it. If the application uses a single port number, enter it in both the "Start" and "Finish" fields.
Incoming Ports	<ul style="list-style-type: none"> • Type - Select the protocol (TCP or UDP) used when you receive data from the special application or service. (Note: Some applications use different protocols for outgoing and incoming data). • Start - Enter the beginning of the range of port numbers used by the application server, for data you receive. If the application uses a single port number, enter it in both the "Start" and "Finish" fields. • Finish - Enter the end of the range of port numbers used by the application server, for data you receive.



Port Forwarding Screen

Port Forwarding	
Application	Enter the desired application type.
External Port	Traffic from the Internet using this port number will be sent to the Server. This is normally the same as the Internal Port Number. If it is different, this device will perform a "mapping" or "translation" function, allowing the server to use a different port to the clients.
Internal Port	Enter the port numbers which the Server software is configured to use.
Protocol	Select the protocol (TCP or UDP) used by the Server.
IP Address	Enter the desired IP address.
Enabled	Use this to Enable or Disable support for this Server, as required.

5.8 Port Range Forward

This feature allows you to make Servers on your LAN accessible to Internet users. Normally, Internet users would not be able to access a server on your LAN because:

Port Range Forwarding

Application	Start	End	Protocol	IP Address	Enable
<input type="text"/>	<input type="text"/>	<input type="text"/>	TCP ▼	192.168.0. <input type="text"/>	<input type="checkbox"/>
<input type="text"/>	<input type="text"/>	<input type="text"/>	TCP ▼	192.168.0. <input type="text"/>	<input type="checkbox"/>
<input type="text"/>	<input type="text"/>	<input type="text"/>	TCP ▼	192.168.0. <input type="text"/>	<input type="checkbox"/>
<input type="text"/>	<input type="text"/>	<input type="text"/>	TCP ▼	192.168.0. <input type="text"/>	<input type="checkbox"/>
<input type="text"/>	<input type="text"/>	<input type="text"/>	TCP ▼	192.168.0. <input type="text"/>	<input type="checkbox"/>
<input type="text"/>	<input type="text"/>	<input type="text"/>	TCP ▼	192.168.0. <input type="text"/>	<input type="checkbox"/>
<input type="text"/>	<input type="text"/>	<input type="text"/>	TCP ▼	192.168.0. <input type="text"/>	<input type="checkbox"/>
<input type="text"/>	<input type="text"/>	<input type="text"/>	TCP ▼	192.168.0. <input type="text"/>	<input type="checkbox"/>
<input type="text"/>	<input type="text"/>	<input type="text"/>	TCP ▼	192.168.0. <input type="text"/>	<input type="checkbox"/>
<input type="text"/>	<input type="text"/>	<input type="text"/>	TCP ▼	192.168.0. <input type="text"/>	<input type="checkbox"/>
<input type="text"/>	<input type="text"/>	<input type="text"/>	TCP ▼	192.168.0. <input type="text"/>	<input type="checkbox"/>

Figure: Port Range Forwarding Screen

Port Range Forwarding Screen

Port Range Forwarding	
Application	Enter the desired application type.
Start	Enter the beginning of the range of port numbers used by the application server.
End	Enter the end of the range of port numbers used by the application server.
Protocol	Select the protocol (TCP, UDP or Both) used by the Server.
IP Address	Enter the desired IP address.
Enable	Use this to Enable or Disable support for this Server, as required.

5.9 QoS

The QoS (Quality of Service) feature allows you specify priorities for different traffic. Lower priority traffic will be slowed down to allow greater throughput or less delay for high priority traffic.

An example **QoS** screen is shown below.

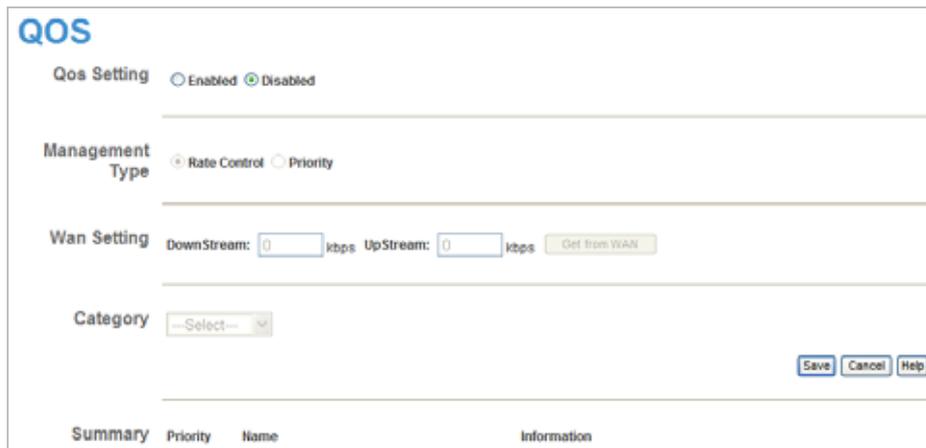


Figure: QoS Screen

QoS Screen

QoS Setting	
QoS Setting	To disable QoS (Quality of Service), keep the default setting, Disable. To enable QoS (Quality of Service), click Enable and follow these instructions.
Management Type	There are 2 options: <ul style="list-style-type: none"> • Rate Control - The QoS will be managed by the size of the bandwidth. • Priority - The QoS will be managed by the priority.
WAN Setting	
DownStream	Enter the desired value for the DownStream Connection.
UpStream	Enter the desired value for the UpStream Connection.
Get from WAN	Click this button to get the values for DownStream and UpStream from WAN.

Category	<p>Normal-Applications:</p> <ul style="list-style-type: none"> • Add a New Application (Once selected, please complete the following setups.) • Ip/Net: Enter the IP addresses. • Rate: Enter the desired rate value. • Priority: Select the desired option (High, Normal, Low) • Direct: Select Upstream or Downstream as required. <p>Self-Define</p> <ul style="list-style-type: none"> • Name. Enter a name for your device. • Port Range: Enter the values for the desired port range. • Protocol: Select the desired option. • Ip/Net: Enter the IP addresses of your device. • Rate: Enter the desired rate value. • Priority: Select the option (High, Normal, Low) from the list. • Direct: Select Upstream or Downstream as required. <p>Special-Applications:</p> <ul style="list-style-type: none"> • Add a New Application (Once selected, please complete the following setups.) • Ip/Net: Enter the IP addresses. • Outbound Rate: Enter the desired rate value. • Inbound Rate: Enter the desired rate value. • Priority: Select the desired option (High, Normal, Low)
Summary	
Priority	The priority of the application.
Name	The Name of this Application or IP Address.
Information	The general Information of this Application or IP Address.

6

Administration

Overview

Normally, it is not necessary to use these screens, or change any settings. These screens and settings are provided to deal with non-standard situations, or to provide additional options for advanced users.

The available settings and features are:

PC Database	This is the list of PCs shown when you select the "DMZ PC" or a "Virtual Server". This database is maintained automatically, but you can add and delete entries for PCs which use a Fixed (Static) IP Address.
Config File	Backup or restore the configuration file for the WN-151ARM. This file contains all the configuration data.
Logs & E-mail	View or clear all logs, set E-Mailing of log files and alerts.
Diagnostics	Perform a Ping or DNS Lookup.
Remote Admin	Allow settings to be changed from the Internet.
Routing	Only required if your LAN has other Routers or Gateways.
Upgrade Firmware	Upgrade the Firmware (software) installed in your WN-151ARM.

6.1 PC Database

The PC Database is used whenever you need to select a PC (e.g. for the "DMZ" PC).

- It eliminates the need to enter IP addresses.
- Also, you do not need to use fixed IP addresses on your LAN.

However, if you do use a fixed IP address on some devices on your LAN, you should enter details of each such device into the PC database, using the PC Database screen.

PC Database Screen

An example *PC Database* screen is shown below.

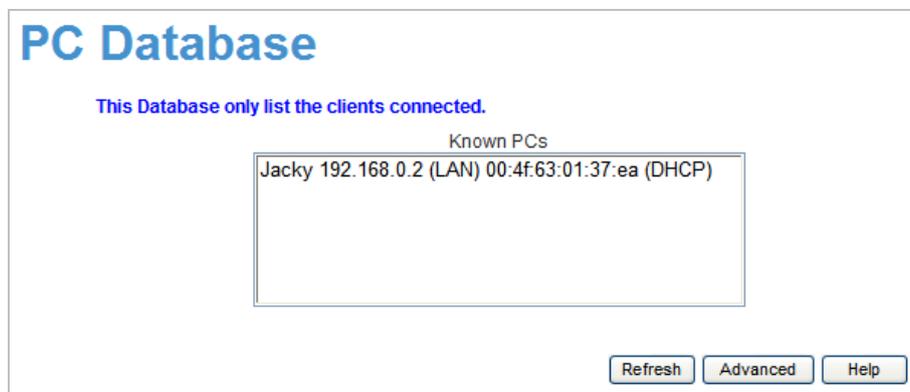


Figure: PC Database

- PCs which are "DHCP Clients" are automatically added to the database, and updated as required.
- The WN-151ARM uses the "Hardware Address" to identify each PC, not the name or IP address. The "Hardware Address" can only change if you change the PC's network card or adapter.



PC Database Screen

Known PCs	This lists all current entries. Data displayed is <i>name (IP Address) type</i> . The "type" indicates whether the PC is connected to the LAN.
Name	If adding a new PC to the list, enter its name here. It is best if this matches the PC's "hostname".
IP Address	Enter the IP Address of the PC. The PC will be sent a "ping" to determine its hardware address. If the PC is not available (not connected, or not powered On) you will not be able to add it.
Buttons	
Refresh	Update the data on screen.
Advanced	View the Advanced version of the PC database screen. See below for details.

Advanced PC Database Screen

This screen is displayed if the "Advanced" button on the **PC Database** is clicked. It provides more control than the standard **PC Database** screen.

PC Database - Advanced

Any PC may be added, edited or deleted. If adding a PC which is not connected and On, you must provide the MAC (hardware) address

Known PCs

Jacky 192.168.0.2 (LAN) 00:4f:63:01:37:ea (DHCP)
--

PC Properties

Name:

IP Address: Automatic (DHCP Client)
 DHCP Client - reserved IP address:
 Fixed IP address (set on PC):

MAC Address: Automatic discovery (PC must be available on LAN)
 MAC address is

Figure: PC Database - Advanced



Advanced PC Database Screen

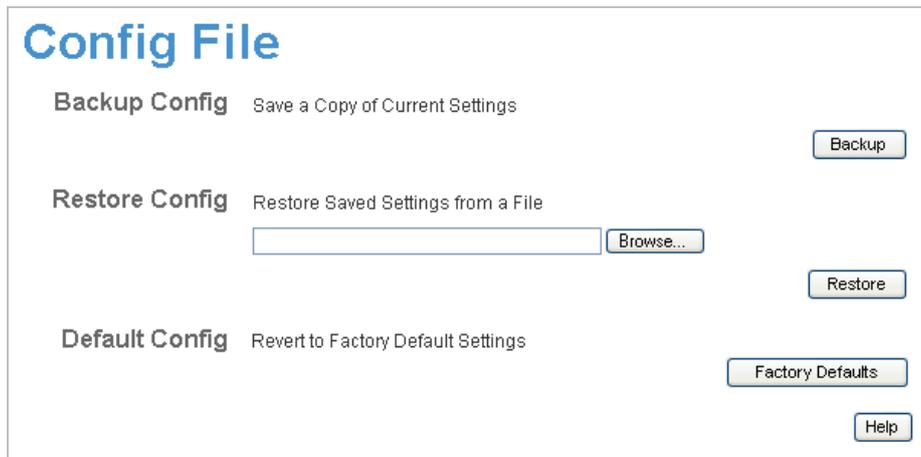
Known PCs	This lists all current entries. Data displayed is name (IP Address) type . The "type" indicates whether the PC is connected to the LAN.
PC Properties	
Name	If adding a new PC to the list, enter its name here. It is best if this matches the PC's "hostname".
IP Address	<p>Select the appropriate option:</p> <ul style="list-style-type: none"> • Automatic - The PC is set to be a DHCP client (Windows: "Obtain an IP address automatically"). The WN-151ARM will allocate an IP address to this PC when requested to do so. The IP address could change, but normally won't. • DCHP Client - Reserved IP Address - Select this if the PC is set to be a DCHP client, and you wish to guarantee that the WN-151ARM will always allocate the same IP Address to this PC. Enter the required IP address. Only the last field is required; the other fields must match the WN-151ARM's IP address. • Fixed IP Address - Select this if the PC is using a Fixed (Static) IP address. Enter the IP address allocated to the PC. (The PC must be configured to use this IP address.)
MAC Address	<p>Select the appropriate option</p> <ul style="list-style-type: none"> • Automatic discovery - WN-151ARM will contact the PC and find its MAC address. This is only possible if the PC is connected to the LAN and powered on. • MAC address is - Enter the MAC address on the PC. The MAC address is also called the "Hardware Address", "Physical Address", or "Network Adapter Address". The WN-151ARM uses this to provide a unique identifier for each PC. Because of this, the MAC address can NOT be left blank.

Buttons	
Add as New Entry	Add a new PC to the list, using the data in the "PC Properties" box. If "Automatic discovery" (for MAC address) is selected, the PC will be sent a "ping" to determine its hardware address. This will fail unless the PC is connected to the LAN, and powered on.
Update Selected PC	Update (modify) the selected PC, using the data in the "Properties" box.
Clear Form	Clear the "Properties" box, ready for entering data for a new PC.
Refresh	Update the data on screen.
Standard Screen	Click this to view the standard "PC Database" screen.

6.2 Config File

This feature allows you to download the current settings from the WN-151ARM, and save them to a file on your PC. You can restore a previously-downloaded configuration file to the WN-151ARM, by uploading it to the WN-151ARM.

This screen also allows you to set the WN-151ARM back to its factory default configuration. Any existing settings will be deleted. An example **Config File** screen is shown below.



The screenshot shows a web interface titled "Config File". It contains three main sections:

- Backup Config:** "Save a Copy of Current Settings" with a "Backup" button.
- Restore Config:** "Restore Saved Settings from a File" with a text input field, a "Browse..." button, and a "Restore" button.
- Default Config:** "Revert to Factory Default Settings" with a "Factory Defaults" button and a "Help" button.

Figure: Config File Screen

Config File Screen

Backup Config	Use this to download a copy of the current configuration, and store the file on your PC. Click Backup to start the download.
Restore Config	<p>This allows you to restore a previously-saved configuration file back to the WN-151ARM.</p> <p>Click Browse to select the configuration file, then click Restore to upload the configuration file.</p> <p>WARNING!</p> <p>Uploading a configuration file will destroy (overwrite) ALL of the existing settings.</p>
Default Config	<p>Clicking the Factory Defaults button will reset the WN-151ARM to its factory default settings.</p> <p>WARNING!</p> <p>This will delete ALL of the existing settings.</p>

6.3 Logs

The Logs record various types of activity on the WN-151ARM. This data is useful for troubleshooting, but enabling all logs will generate a large amount of data and adversely affect performance.

Since only a limited amount of log data can be stored in the WN-151ARM, log data can also be E-mailed to your PC. Use the **E-mail** screen to configure this feature.

Logs

Logs Current time: 1999-12-31 18:47:45

```
[admin login]:client 192.168.0.2 login Fri,
[Router]:Start up Fri, 1999-12-31 16:10:21
[admin logout]:The previous client log Out F
[admin login]:client 192.168.0.2 login Fri,
[admin logout]:The previous client log Out F
[admin login]:client 192.168.0.2 login Fri,
[admin logout]:The previous client log Out F
[admin login]:client 192.168.0.2 login Fri,
[admin logout]:The previous client log Out F
[admin login]:client 192.168.0.3 login Fri,
[admin logout]:The previous client log Out F
[admin logout]:The previous client log Out F
[admin login]:client 192.168.0.2 login Fri,
```

Include in Log

- Attempted access to blocked sites
- Connections to the Web-based interface of this Router
- Router operation (start up, get time etc)
- Known DoS attacks and Port Scans
- Outgoing (Internet) connections
- Access control

Syslog

- Disable
- Broadcast on LAN
- Send to this Syslog Server: . . .

Figure: Logs Screen

Logs Screen

Logs	
Current Time	The current time on the WN-151ARM is displayed.
Log Data	Current log data is displayed in this panel.
Buttons	<p>There are three (3) buttons</p> <ul style="list-style-type: none"> • Refresh - Update the log data. • Clear Log - Clear the log, and restart it. This makes new messages easier to read. • Send Log - E-mail the log immediately. This is only functional if the <i>E-mail</i> screen has been configured.
Include in Log	
Include (Checkboxes)	<p>Use these checkboxes to determine which events are included in the log. Checking all options will increase the size of the log, so it is good practice to disable any events which are not really required.</p> <ul style="list-style-type: none"> • Attempted access to blocked sites - If checked, attempted Internet accesses which were blocked are logged. • Connections to the Web-based interface of this Router - If checked, this will log connections TO this Router, rather than through this Router to the Internet. • Router operation - If checked, other Router operations (not covered by the selections above) will be logged. • Known DoS attacks and Port Scans - If checked, Denial of Service attacks, as well as port scans, will be logged.
Syslog	
Disable	Data is not sent to a Syslog Server.
Broadcast on LAN	<p>The Syslog data is broadcast, rather than sent to a specific Syslog server. Use this if your Syslog Server does not have a fixed IP address.</p>
Send to this Syslog Server	If your Syslog server has a fixed IP address, select this option, and enter the IP address of your Syslog server.

6.4 Email

This screen allows you to E-mail Logs and Alerts. A sample screen is shown below.

E-Mail

E-mail Notification Turn E-mail Notification On

Send to this E-mail Address:

Outgoing (SMTP) Mail Server:

Mail Sender Address:

My SMTP Mail Server requires authentication

User Name:

Password:

E-mail Alerts Send E-Mail alerts immediately

- If a DoS attack is detected.
- If a Port Scan is detected.
- If someone attempts to access a blocked site.

E-mail Logs Send Logs According to this Schedule

Hourly

Day

Time a.m. p.m.

Figure: E-mail Screen

E-mail Screen

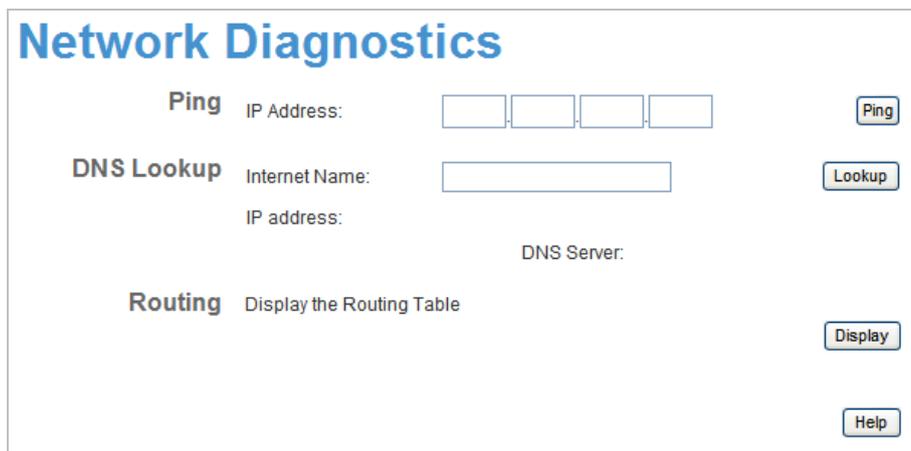
E-Mail Notification	
Turn E-mail Notification on	Check this box to enable this feature. If enabled, the E-mail address information (below) must be provided.
Send to this E-mail address	Enter the E-mail address the Log is to be sent to.
Outgoing (SMTP) Mail Server	Enter the address or IP address of the SMTP (Simple Mail Transport Protocol) Server you use for outgoing E-mail.
Mail Sender Address	Enter the mail address of the sender. The E-mail will also show this address as the Sender's address.

My SMTP Mail Server requires authentication	To stop spammers, many SMTP mail servers require you to log in to send mail. In this case, enable this checkbox, and enter the login information (User name and Password) in the fields below.
User Name	If you have enabled "My SMTP Mail Server requires authentication" above, enter the User Name required to login to your SMTP Server.
Password	If you have enabled "My SMTP Mail Server requires authentication" above, enter the password required to login to your SMTP Server.
E-mail Alerts	
Send E-mail alerts immediately	<p>You can choose to have alerts E-mailed to you, by checking the desired checkboxes. The WN-151ARM can send an immediate alert when it detects a significant security incident such as</p> <ul style="list-style-type: none"> • A known hacker attack is directed at your IP address • A computer on the Internet scans your IP address for open ports • Someone on your LAN (Local Area Network) tries to visit a blocked site.
E-mail Logs	
Send Logs	<p>Select the desired option for sending the log by E-mail.</p> <ul style="list-style-type: none"> • Never (default) - This feature is disabled; Logs are not sent. • When log is full - The time is not fixed. The log will be sent when the log is full, which will depend on the volume of traffic. • Hourly, Daily, Weekly... - The log is sent on the interval specified. <ul style="list-style-type: none"> • If Daily is selected, the log is sent at the time specified. Select the time of day you wish the E-mail to be sent. • If Weekly is selected, the log is sent once per week, on the specified day, at the specified time. Select the day and the time of day you wish the E-mail to be sent. <p>Note: If the log is full before the time specified to send it, it will be sent regardless of the day and time specified.</p>

6.5 Diagnostics

This screen allows you to perform a "Ping" or a "DNS lookup". These activities can be useful in solving network problems.

An example **Network Diagnostics** screen is shown below.



The screenshot shows a web interface titled "Network Diagnostics" in blue text. It features three main sections: "Ping", "DNS Lookup", and "Routing".

- Ping:** Labeled "Ping" in bold. It includes the text "IP Address:" followed by four empty input boxes separated by dots. A "Ping" button is located to the right.
- DNS Lookup:** Labeled "DNS Lookup" in bold. It includes the text "Internet Name:" followed by a single wide input box, and "IP address:" followed by a smaller input box. Below these is the text "DNS Server:" followed by another input box. A "Lookup" button is located to the right.
- Routing:** Labeled "Routing" in bold. It includes the text "Display the Routing Table". A "Display" button is located to the right.

At the bottom right of the interface is a "Help" button.

Figure: Network Diagnostics Screen

Network Diagnostics Screen

Ping	
IP Address	<p>Enter the IP address you wish to ping. The IP address can be on your LAN, or on the Internet.</p> <p>Note that if the address is on the Internet, and no connection currently exists, you could get a "Timeout" error. In that case, wait a few seconds and try again.</p>
Ping Button	<p>After entering the IP address, click this button to start the "Ping" procedure. The results will be displayed in the <i>Ping Results</i> pane.</p>
DNS Lookup	
Internet Name	<p>Enter the Domain name or URL for which you want a DNS (Domain Name Server) lookup.</p> <p>Note that if the address is on the Internet, and no connection currently exists, you could get a "Timeout" error. In that case, wait a few seconds and try again.</p>
Lookup Button	<p>After entering the Domain name/URL, click this button to start the "DNS Lookup" procedure.</p>
Routing	
Display	<p>Click this button to display the internal routing table. This information can be used by Technical Support and other staff who understand Routing Tables.</p>

6.6 Remote Administration

If enabled, this feature allows you to manage the WN-151ARM via the Internet.

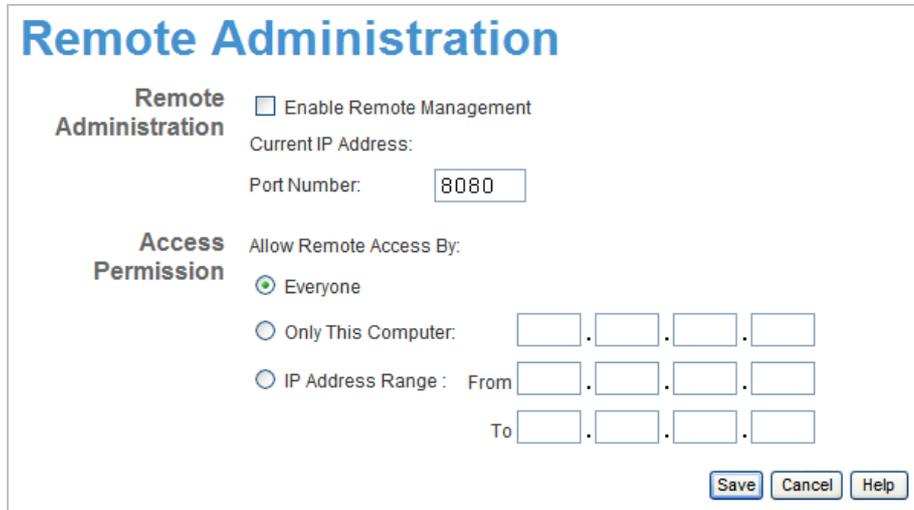


Figure: Remote Administration Screen

Remote Administration Screen

Remote Administration	
Enable Remote Management	Check to allow administration/management via the Internet. (To connect, see below). If Disabled, this device will ignore Administration connection attempts from the Internet.
Current IP Address	This is the current address you will use when accessing this device from the Internet. To connect, see details and an example below.
Port Number	Enter a port number between 1 and 65535. The default for HTTP (Web) connections is port 80, but using port 80 will prevent the use of a Web "Virtual Server" on your LAN. So using a different port number is recommended. The default value is 8080. The port number must be specified in your Browser when you connect. See the following section for details.

Access Permission	
Allow Remote Access	<p>Select the desired option.</p> <ul style="list-style-type: none">• Everyone - allow access by everyone on the Internet.• Only This Computer - allow access by only one IP address. Enter the desired IP address.• IP Address Range - allow access from a range of IP addresses on the Internet. Enter a beginning and ending IP address to define the allowed range. <p>For security, you should restrict access to as few external IP addresses as practical.</p>

To connect from a remote PC via the Internet

1. Ensure your Internet connection is established, and start your Web Browser.
2. In the "Address" bar, enter "http://" followed by the Internet IP Address of the WN-151ARM. If the port number is not 80, the port number is also required. (After the IP Address, enter ":" followed by the port number.)

e.g.

http://123.123.123.123.8080

This example assumes the WAN IP Address is 123.123.123.123, and the port number is 8080.

3. You will then be prompted for the login name and password for this device.

6.7 Routing

Overview

You can ignore the "Routing" page if your network topology is constructed as following:

- If you don't have other Routers or Gateways on your LAN.
- If the WN-151ARM is only acting as a Gateway for the local LAN segment, ignore the "Routing" page even if your LAN has other Routers.

You can ignore the RIP Routing page if your network topology is constructed as following:

- If your LAN has other Gateways and Routers, and you wish to control which LAN segments use each Gateway, do NOT enable RIP (Routing Information Protocol). Configure the Static Routing table instead. (You also need to configure the other Routers.)

You can ignore the Static Routing page if your network topology is constructed as following:

- If your LAN has a standard Router (e.g. Cisco) on your LAN, and the WN-151ARM is to act as a Gateway for all LAN segments, you can enable RIP (Routing Information Protocol).
- If using Windows 2000 Data center Server as a software Router, enable RIP on the WN-151ARM, and ensure the following Windows 2000 settings are correct:
 - Open **Routing and Remote Access**
 - In the console tree, select **Routing and Remote Access, [server name], IP Routing, RIP**
 - In the "Details" pane, right-click the interface you want to configure for RIP version 2, and then click "Properties".
 - On the "General" tab, set **Outgoing packet protocol** to "RIP version 2 broadcast", and **Incoming packet protocol** to "RIP version 1 and 2".

Routing Screen

The routing table is accessed by the **Routing** link on the **Administration** menu.

Using this Screen

Generally, you will use either RIP (Routing Information Protocol) or the Static Routing Table, as explained above, although it is possible to use both methods simultaneously.

Static Routing Table

- If RIP is not used, an entry in the routing table is required for each LAN segment on your Network, other than the segment to which this device is attached.
- The other Routers must also be configured. See **Configuring Other Routers on your LAN** later in this chapter for further details and an example.



Figure: Routing Screen

Routing Screen

RIP	
RIP Direction	Select the desired RIP Direction.
RIP Version	Choose the RIP Version for the Server.
Static Routing	
Static Routing Table Entries	<p>This list shows all entries in the Routing Table.</p> <ul style="list-style-type: none"> This area shows details of the selected item in the list. Change any the properties as required, then click the "Edit" button to save the changes to the selected entry.
Buttons	
Add	Add a new entry to the Static Routing table, using the data shown in the "Properties" area on screen. The entry selected in the list is ignored, and has no effect.
Edit	Update the current Static Routing Table entry, using the data shown in the table area on screen.
Delete	Delete the current Static Routing Table entry.
Save	Save the RIP setting. This has no effect on the Static Routing Table.

Configuring Other Routers on your LAN

It is essential that all IP packets for devices are not on the local LAN be passed to the WN-151ARM, so that they can be forwarded to the external LAN, WAN, or Internet. To achieve this, the local LAN must be configured to use the WN-151ARM as the **Default Route** or **Default Gateway**.

Local Router

The local router is the Router installed on the same LAN segment as the WN-151ARM. This router requires that the **Default Route** is the WN-151ARM itself. Typically, routers have a special entry for the **Default Route**. It should be configured as follows.

Destination IP Address	Normally 0.0.0.0, but check your router documentation.
Network Mask	Normally 0.0.0.0, but check your router documentation.
Gateway IP Address	The IP Address of the WN-151ARM.
Metric	1

Other Routers on the Local LAN

Other routers on the local LAN must use the WN-151ARM's **Local Router** as the **Default Route**. The entries will be the same as the WN-151ARM's local router, with the exception of the **Gateway IP Address**.

- For a router with a direct connection to the WN-151ARM's local Router, the **Gateway IP Address** is the address of the WN-151ARM's local router.
- For routers which must forward packets to another router before reaching the WN-151ARM's local router, the **Gateway IP Address** is the address of the intermediate router.

Static Routing - Example

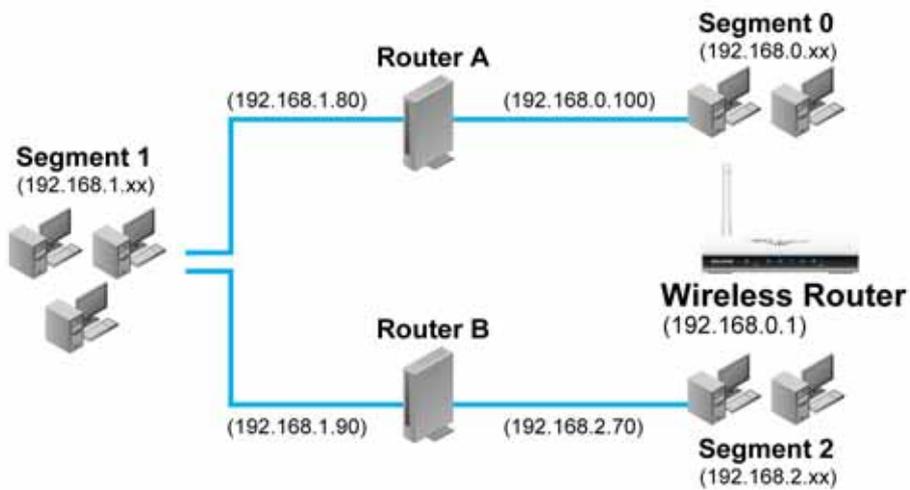


Figure: Routing Example

For the WN-151ARM's Routing Table

For the LAN shown above, with 2 routers and 3 LAN segments, the WN-151ARM requires 2 entries as follows.

Entry 1 (Segment 1)	
Destination IP Address	192.168.1.0
Network Mask	255.255.255.0 (Standard Class C)
Gateway IP Address	192.168.0.100 (WN-151ARM's local Router)
Metric	2
Entry 2 (Segment 2)	
Destination IP Address	192.168.2.0
Network Mask	255.255.255.0 (Standard Class C)
Gateway IP Address	192.168.0.100
Metric	3

For Router A's Default Route

Destination IP Address	0.0.0.0
Network Mask	0.0.0.0
Gateway IP Address	192.168.0.1 (WN-151ARM's IP Address)

For Router B's Default Route

Destination IP Address	0.0.0.0
Network Mask	0.0.0.0
Gateway IP Address	192.168.1.80 (WN-151ARM's local router)

6.8 Upgrade Firmware

The firmware (software) in the WN-151ARM can be upgraded using your Web Browser.

You must first download the upgrade file, then to select **Upgrade Firmware** on the **Administration** menu.

You will see a screen like the following.



The screenshot shows a web interface titled "Upgrade Firmware". Below the title, it says "Locate and Select the Upgrade File from your Hard Disk:". There is a text input field followed by a "Browse..." button. At the bottom right, there are three buttons: "Upload", "Cancel", and "Help".

Figure: Router Upgrade Screen

To perform the Firmware Upgrade:

1. Click the **Browse** button and navigate to the location of the upgrade file.
2. Select the upgrade file. Its name will appear in the **Upgrade File** field.
3. Click the **Upload** button to commence the firmware upgrade.

7

Modem Mode

Overview

There are two modes available on the **Mode** screen.

- **Router** - Both the ADSL Modem and the Router features are operational. In this mode, this device can provide shared Internet Access to all your LAN users. Also, by default, it acts a DHCP Server, providing an IP address and related information to all Wireless and LAN users.
- **Modem** - Only the ADSL Modem component is operational. All Router features are disabled. This device is "transparent" - it does not perform any operations or make any changes to the network traffic passing through it. You need to have a DHCP Server on your LAN to provide IP addresses to the Wireless clients using this Access Point.

This Chapter describes operation while in **Modem Mode**, also called **Bridge Mode**.

Management Connections

When this device restarts in Modem mode, the IP address does not change, but the DHCP server is disabled. However, your PC will usually retain the IP address provided by the DHCP Server, so the connection will be automatically re-established. You then need to ensure that the IP address of this modem is suitable for your LAN.

- You need to have a DHCP Server on your LAN to provide IP addresses to the Wireless clients using this Access Point.
- This Modem/AP must be a valid device on your LAN, to allow management connections. You must assign a (fixed) IP address which is within the address range used on your LAN, but not within the address range used by your DHCP server.



When you connect in future, just connect normally, using the IP address you assigned.

1. Start your WEB browser.
2. In the **Address** box, enter "http://" and the current IP Address of the WN-151ARM as in this example, which uses the WN-151ARM 's default IP Address:

http://192.168.1.254

3. When prompted for the User name and Password, enter admin for the user name, and the current password, as set on the password screen. (The password is the same regardless of the mode.)

Home Screen

If in Modem mode, the home screen will look like the example below.

Airlive		
Wireless:	SSID1:	airlive
	Security:	Disabled
	SSID2:	Guest
	Security:	Disabled
<hr/>		
LAN:	IP Address:	192.168.1.254

Figure: Home Screen - Modem Mode

Note: When it sets to Modem mode, the menu has also changed, many of the options in Router mode are not available. The screens available are:

- **Mode** - change back to Router mode, if desired.
- **LAN** - set IP address, mask and gateway. This is the same as in Router mode, except that the DHCP server is not available while in Modem mode.
- **Wireless** - this screen, and related sub-screens, is the same as in Router mode.
- **Password** - this screen is the same as in Router mode.
- **Upgrade FW** - this screen is the same as in Router mode.
- **Status** - displays current settings and status. See the following section for details.
- **Binding** - this screen is the same as in Router mode.

Mode Screen

This screen is change back to Router mode, if desired.



Mode

Device Mode Device Name: Airlive
Device Mode: Modem (Modem only) ▼

Save Help

Figure: Mode Screen



Mode Screen

Device Name	This field displays the current name of this device.
Device Mode	<p>Select the desired device mode for the router:</p> <ul style="list-style-type: none">• Router - Both the ADSL Modem and the Router features are operational. In this mode, this device can provide shared Internet Access to all your LAN users. Also, by default, it acts a DHCP Server, providing an IP address and related information to all Wireless and LAN users.• Modem - Only the ADSL Modem component is operational. All Router features are disabled. This device is "transparent" - it does not perform any operations or make any changes to the network traffic passing through it. You need to have a DHCP Server on your LAN to provide IP addresses to the Wireless clients using this Access Point. This mode is also called <i>Bridge Mode</i>. <p>After changing the mode, this device will restart, which will take a few seconds. The menu will also change, depending on the mode you are in.</p>

Operation

Operation is automatic and transparent.

- Wireless clients can connect to the Access Point if they have the correct SSID and security, but they must obtain an IP address from the DHCP Server on your LAN.

The modem will act like any other ADSL modem. No routing will be performed, and no client login will be done.

If a client login is required, it must be performed by your Router/Gateway or by software on your PC.

Status Screen

In Modem mode, the Status screen looks like the example below.

Status - Bridge Mode

ADSL	Modem Status	Negotiating
	DownStream Connection Speed	0 kbps
	UpStream Connection Speed	0 kbps
ADSL Details		
LAN	IP Address:	192.168.0.1
	Network Mask:	255.255.255.0
	MAC Address	00:C0:02:FF:C7:46
Wireless	SSID1	Airlive
	MAC Address	00:C0:02:FF:C7:46
	SSID2	Guest
	MAC Address	62:c0:02:ff:c7:47
	Region	—
	Channel	6
	Wireless AP	enable
	Broadcast Name	enable
System	Device Name:	Airlive
	Firmware Version:	1.00.00

[Attached Devices](#)

[Refresh Screen](#) [Help](#)

Figure: Status Screen - Bridge Mode



Status Screen (Bridge Mode)

ADSL	
Modem Status	This indicates the status of the ADSL modem component.
DownStream Connection Speed	Displays the speed for the DownStream Connection.
UpStream Connection Speed	If connected, displays the speed for the Up Stream (upload) ADSL Connection.
LAN	
IP Address	The IP Address of the WN-151ARM.
Network Mask	The Network Mask (Subnet Mask) for the IP Address above.
MAC Address	This shows the MAC Address for the WN-151ARM, as seen on the LAN interface.

Wireless	
SSID 1/2	If using an ESS (Extended Service Set, with multiple access points) this ID is called an ESSID (Extended Service Set Identifier).
Region	The current region, as set on the Wireless screen.
Channel	This shows the Channel currently used, as set on the Wireless screen.
Wireless AP	This indicates whether or not the Wireless Access Point feature is enabled.
Broadcast Name	This indicates whether or not the SSID is Broadcast. This setting is on the Wireless screen.

System	
Device Name	The current name of the Router. This name is also the "hostname" for users with an "@Home" type connection.
Firmware Version	The version of the current firmware installed.

Buttons	
Attached Devices	This will open a sub-window, showing all LAN and Wireless devices currently on the network.
Refresh Screen	Update the data displayed on screen.

Appendix A - Troubleshooting

Overview

This chapter covers some common problems that may be encountered while using the WN-151ARM and some possible solutions to them. If you follow the suggested steps and the WN-151ARM still does not function properly, contact your dealer for further advice.

General Problems

Problem 1: Can't connect to the WN-151ARM to configure it.

Solution 1: Check the following:

- The WN-151ARM is properly installed, LAN connections are OK, and it is powered ON.
- Ensure that your PC and the WN-151ARM are on the same network segment. (If you don't have a router, this must be the case.)
- If your PC is set to "Obtain an IP Address automatically" (DHCP client), 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 192.168.1.253 and thus compatible with the WN-151ARM's default IP Address of 192.168.1.254. Also, the Network Mask should be set to 255.255.255.0 to match the WN-151ARM.

In Windows, you can check these settings by using **Control Panel-Network** to check the **Properties** for the TCP/IP protocol.

Internet Access

Problem 1: When I enter a URL or IP address I get a time out error.

Solution 1: A number of things could be causing this. Try the following troubleshooting steps.

- Check if other PCs work. If they do, ensure that your PCs IP settings are correct. If using a Fixed (Static) IP Address, check the Network Mask, Default gateway and DNS as well as the IP Address.
- If the PCs are configured correctly, but still not working, check the WN-151ARM. 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.)
- Check the WN-151ARM's status screen to see if it is working correctly.

Problem 2: Some applications do not run properly when using the WN-151ARM.

Solution 2: The WN-151ARM processes the data passing through it, so it is not transparent.

For incoming connections, you must use the Virtual Server or Firewall Rules to specify the PC which will receive the incoming traffic.

You can also use the **DMZ** function. This should work with almost every application, but:

- 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 Access Point.

Solution 1: Check the following.

- Your PC is set to **Infrastructure Mode**. (Access Points are always in **Infrastructure Mode**)
- The SSID on your PC and the Wireless Access Point are the same. Remember that the SSID is case-sensitive. So, for example "Workgroup" does NOT match "workgroup".
- Both your PC and the WN-151ARM must have the same setting for WEP. The default setting for the WN-151ARM is disabled, so your wireless station should also have WEP disabled.
- If WEP is enabled on the WN-151ARM, your PC must have WEP enabled, and the key must match.
- If the WN-151ARM's *Wireless* screen is set to **Allow Trusted PCs only**, then each of your Wireless stations must have been designated as "Trusted", or the Wireless station will be blocked.
- To see if radio interference is causing a problem, see if connection is possible when close to the WN-151ARM. 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: 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:

- WN-151ARM location.
Try adjusting the location and orientation of the WN-151ARM.
- Wireless Channel
If interference is the problem, changing to another channel may show a marked improvement.
- Radio Interference
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.
- RF Shielding
Your environment may tend to block transmission between the wireless stations. This will mean high access speed is only possible when close to the WN-151ARM.



Appendix B - Wireless LAN

Overview

Wireless LANs can work in either of two (2) modes:

- Ad-hoc
- Infrastructure

Ad-hoc Mode

Ad-hoc mode does not require an Access Point or a wired (Ethernet) LAN. Wireless Stations (e.g. notebook PCs with wireless cards) communicate directly with each other.

Infrastructure Mode

In Infrastructure Mode, one or more Access Points are used to connect Wireless Stations (e.g. Notebook PCs with wireless cards) to a wired (Ethernet) LAN. The Wireless Stations can then access all LAN resources.

Note: Access Points can only function in "Infrastructure" mode, and can communicate only with Wireless Stations which are set to "Infrastructure" mode.

BSS/ESS

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.

ESS

A group of Wireless Stations, and multiple Access Points, all using the same ID (ESSID), form an Extended Service Set (ESS).

Different Access Points within an ESS can use different Channels. In fact, to reduce interference, it is recommended that adjacent Access Points SHOULD use different channels.

As Wireless Stations are physically moved through the area covered by an ESS, they will automatically change to the Access Point which has the least interference or best performance. This capability is called

Roaming. (Access Points do not have or require Roaming capabilities.)

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.)
- If using "Ad-hoc" mode (no Access Point), all Wireless stations should be set to use the same Channel. However, most Wireless stations will still scan all Channels to see if there is an existing "Ad-hoc" group they can join.

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 settings for each of the following:

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



WPA-PSK

WPA-PSK is another standard for encrypting data before it is transmitted. This is a later standard than WEP (Wired Equivalent Privacy), and provides greater security for your data. Data is encrypted using a 256Bit key which is automatically generated and changed often.

If all your Wireless stations support WPA-PSK, you should use this instead of WEP.

If WPA-PSK is used, the Wireless Stations and the Access Point must have the same settings for each of the following:

WPA PSK (Pre-shared Key)	Enter the same value on every station and the AP. The PSK must be from 8 to 63 characters in length. The 256Bit key used for the actual encryption is derived from this key.
Encryption	The same encryption method must be used. The most common encryption method is TKIP. Another widely-supported method is AES.

WPA2-PSK

This is a later version of WPA (WPA-PSK). The major change is the use of AES (Advanced Encryption System) for protecting data. AES is very secure, considered to be unbreakable. The PSK (Pre-shared Key) must be entered on each Wireless station.

If WPA2-PSK is used, the Wireless Stations and the Access Point must have the same settings for each of the following:

WPA2 PSK (Pre-shared Key)	Enter the same value on every station and the AP. The PSK must be from 8 to 63 characters in length. The 256Bit key used for the actual encryption is derived from this key.
Encryption	The same encryption method must be used. The most common encryption method is TKIP. Another widely-supported method is AES.

WPA-802.1x

This version of WPA requires a Radius Server on your LAN to provide the client authentication according to the 802.1x standard. Data transmissions are encrypted using the WPA standard.

If this option is used:

- The Access Point must have a "client login" on the Radius Server.
- Each user must have a "user login" on the Radius Server.
- Each user's wireless client must support 802.1x and provide the login data when required.

All data transmission is encrypted using the WPA standard. Keys are automatically generated, so no key input is required.

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	On client Wireless Stations, the mode must be set to "Infrastructure". (The Access Point is always in "Infrastructure" mode.)
SSID (ESSID)	Wireless Stations should use the same SSID (ESSID) as the Access Point they wish to connect to. Alternatively, the SSID can be set to "any" or null (blank) to allow connection to any Access Point.
Wireless Security	The Wireless Stations and the Access Point must use the same settings for Wireless security. (None, WEP, WPA-PSK, WPA2-PSK, WPA-802.1x).



Appendix C - Specifications

Standards

- IEEE 802.3 (10BaseT Ethernet)
- IEEE 802.3u (100BaseTX Fast Ethernet)
- IEEE 802.11b (11Mbps Wireless LAN)
- IEEE 802.11g (54Mbps Wireless LAN)
- ITU G.992.1 Annex A (ADSL/POTS)
- ITU G.992.2 G.lite
- ITU G.992.3 Annex A, ADSL2
- ITU G.992.3 Annex A, DELT
- ITU G.992.3 Annex L, READSL
- ITU G.992.5 Annex A, ADSL2+
- ITU G.992.5 Annex M
- Multi-Mode code support
- ANSI T1413 support

General

- WAN port: 1 x RJ11 ADSL line
- LAN port: 1 x RJ45 10/100Mbps Auto MDI/MDI-X
- Flash: 4MB
- Memory: 16MB SDRAM
- Certifications: CE Mark, FCC Class B, RoHS

Router

- Supported connection types:
 - PPP over Ethernet (RFC 2516)
 - PPP over AAL5 (RFC 2364)
 - Multiple protocols over AAL5 (RFC 1483/2684)
- NAT
 - Virtual Server
 - DMZ (demilitarized zone)
 - Port forward
- Firewall
 - MAC address filter
 - URL filter
- UPnP (Universal Plug and Play)
- DHCP (server/client)
- VPN passthrough (PPTP, L2TP, IPSec)
- DDNS (Dynamic Domain Name Service)
- WDS (Wireless Distribution System)
- QoS (Quality of Service)

Wireless

- Chipset: Ralink
- Wireless Frequency Range: 2.4 ~ 2.4835 GHz
- Modulation Technologies:
 - 802.11b: Direct Sequence Spread Spectrum (DSSS): DBPSK, DQPSK, CCK
 - 802.11g: Orthogonal Frequency Division Multiplexing (OFDM): BPSK, QPSK, 16QAM, 64QAM
 - 802.11n: Orthogonal Frequency Division Multiplexing (OFDM): BPSK, QPSK, 16QAM, 64QAM
- Channels:
 - USA & Canada: 11 channels
 - Europe: 13 channels



- Data Rates:
 - IEEE 802.11b (11Mbps, 5.5Mbps, 2Mbps, 1Mbps)
 - IEEE 802.11g (54Mbps, 48Mbps, 36Mbps, 24Mbps, 18Mbps, 12Mbps, 11Mbps, 9Mbps, 6Mbps)
 - IEEE 802.11n 40MHz (135Mbps, 121.5Mbps, 108Mbps, 81Mbps, 54Mbps, 40Mbps, 27Mbps, 13.5Mbps)
 - IEEE 802.11n 20MHZ (65Mbps, 58.5Mbps, 52Mbps, 39Mbps, 26Mbps, 19.5Mbps, 13Mbps, 6Mbps)
- Wireless Security
 - WEP (64/128bit)
 - WPA-PSK
 - WPA2-PSK
 - 802.1x
- Antenna
 - 1 x detachable dipole antenna with 2dBi gain

LEDs

- Security (White)
- Power (Orange)
- LAN (Blue)
- Wireless (Blue)
- Internet (Blue)
- ADSL (Green)

Environmental

- Dimensions: 145(W) x 120(D) x 34(H) mm
- Product weight:
- Operating temperature: 0~40°C
- Operating humidity: 0~85% (Non-Condensing)
- Storage temperature: -20~60°C

Power

- External power adapter: 12V DC, 1A

Appendix D - Wireless Network Glossary

The wireless network glossary contains explanation or information about common terms used in wireless networking products. Some of information in this glossary might be outdated, please use with caution.

802.11a

An IEEE specification for wireless networking that operates in the 5 GHz frequency range (5.15 GHz to 5.850 GHz) with a maximum of 54Mbps data transfer rate. The 5GHz frequency band is not as crowded as the 2.4GHz band. In addition, the 802.11a have 12 non-overlapping channels, comparing to 802.11b/g's 3 non-overlapping channels. This means the possibility to build larger non-interfering networks. However, the 802.11a deliver shorter distance at the same output power when comparing to 802.11g.

802.11b

International standard for wireless networking that operates in the 2.4GHz frequency band (2.4 GHz to 2.4835 GHz) and provides a throughput up to 11 Mbps.

802.11d

Also known as "Global Roaming". 802.11d is a standard for use in countries where systems using other standards in the 802.11 family are not allowed to operate.

802.11e

The IEEE QoS standard for prioritizing traffic of the VoIP and multimedia applications. The WMM is based on a subset of the 802.11e.

802.11g

A standard provides a throughput up to 54Mbps using OFDM technology. It also operates in the 2.4GHz frequency band as 802.11b. 802.11g devices are backward compatible with 802.11b devices.

802.11h

This IEEE standard define the TPC (transmission power control) and DFS (dynamic frequency selection) required to operate WiFi devices in 5GHz for EU.

802.11i

The IEEE standard for wireless security, 802.11i standard includes TKIP, CCMP, and AES encryption to improve wireless security. It is also know as WPA2.

802.11n

802.11n is a recent amendment which improves upon the previous 802.11 standards by adding multiple-input multiple-output (MIMO) and many other newer features. The IEEE has approved the amendment and it was published in October 2009. Enterprises, however, have already begun migrating to 802.11n networks based on the Wi-Fi Alliance's certification of products conforming to a 2007 draft of the 802.11n proposal.

802.11n provides a throughput up to 300Mbps using OFDM technology.

802.3ad

802.3ad is an IEEE standard for bonding or aggregating multiple Ethernet ports into one virtual port (also known as trunking) to increase the bandwidth.

802.3af

This is the PoE (Power over Ethernet) standard by IEEE committee. 803.af uses 48V POE standard that can deliver up to 100 meter distance over Ethernet cable.

802.1d STP

Spanning Tree Protocol. It is an algorithm to prevent network from forming. The STP protocol allows net work to provide a redundant link in the event of a link failure. It is advise to turn on this option for multi-link bridge network.

802.1Q Tag VLAN

In 802.1Q VLAN, the VLAN information is written into the Ethernet packet itself. Each packet carries a VLAN ID (called Tag) as it traveled across the network. Therefore, the VLAN configuration can be configured across multiple switches. In 802.1Q spec, possible 4096 VLAN ID can be created. Although for some devices, they can only view in frames of 256 ID at a time.

802.1x

802.1x is a security standard for wired and wireless LANs. In the 802.1x parlance, there are usually supplicants (client), authenticator (switch or AP), and authentication server (radius server) in the network. When a supplicants request a service, the authenticator will pass the request and wait for the authentication server to grant access and register accounting. The 802.1x is the most widely used method of authentication by WISP.

Ad-hoc

A Peer-to-Peer wireless network. An Ad-hoc wireless network do not use wireless AP or router as the central hub of the network. Instead, wireless client are connected directly to each other. The disadvantage of Adhoc network is the lack of wired interface to Internet connections. It is not recommended for network more than 2 nodes.

Access Point (AP)

The central hub of a wireless LAN network. Access Points have one or more Ethernet ports that can connect devices (such as Internet connection) for sharing. Multi-function Access Point can also function as an Ethernet client, wireless bridge, or repeat signals from other AP. Access Points typically have more wireless functions comparing to wireless routers.

ACK Timeout

Acknowledgement Timeout Windows. When a packet is sent out from one wireless station to the other, it will wait for an Acknowledgement frame from the remote station. The station will only wait for a certain amount of time; this time is called the ACK timeout. If the ACK is NOT received within that timeout period then the packet will be re-transmitted resulting in reduced throughput. If the ACK setting is too high then throughput will be lost due to waiting for the ACK Window to timeout on lost packets. If the ACK setting is too low then the ACK window will have expired and the returning packet will be dropped, greatly lowering throughput. By having the ability to adjust the ACK setting we can effectively optimize the throughput over long distance links. This is especially true for 802.11a and 802.11g networks. Setting the correct ACK timeout value needs to consider 3 factors: distance, AP response time, and interference.

Bandwidth Management

Bandwidth Management controls the transmission speed of a port, user, IP address, and application. Router can use bandwidth control to limit the Internet connection speed of individual IP or Application. It can also guarantee the speed of certain special application or privileged IP address - a crucial feature of QoS (Quality of Service) function.

Bootloader

Bootloader is the under layering program that will start at the power-up before the device loads firmware. It is similar to BIOS on a personal computer. When a firmware crashed, you might be able to recover your device from bootloader.

Bridge

A product that connects 2 different networks that uses the same protocol. Wireless bridges are commonly used to link network across remote buildings. For wireless application, there are 2 types of Bridges. WDS Bridge can be used in Point-to-Point or Point-to-Multipoint topology. Bridge Infrastructure works with AP mode to form a star topology.

Cable and Connector Loss

During wireless design and deployment, it is important to factor in the cable and connector loss. Cable and connector loss will reduce the output power and receiver sensitivity of the radio at connector end. The longer the cable length is, the more the cable loss. Cable loss should be subtracted from the total output power during distance calculation. For example, if the cable and connector loss is 3dBm and the output power is 20dBm; the output power at the cable end is only 17dBm.

Client

Client means a network device or utility that receives service from host or server. A client device means end user device such as wireless cards or wireless CPE.

CPE Devices

CPE stands for Customer Premises Equipment. A CPE is a device installed on the end user's side to receive network services. For example, on an ADSL network, the ADSL modem/router on the subscriber's home is the CPE device. Wireless CPE means a complete Wireless (usually an AP with built-in Antenna) that receives wireless broadband access from the WISP. The opposite of CPE is CO.

CTS

Clear To Send. A signal sent by a device to indicate that it is ready to receive data.

DDNS

Dynamic Domain Name System. An algorithm that allows the use of dynamic IP address for hosting Internet Server. A DDNS service provides each user account with a domain name. A router with DDNS capability has a built-in DDNS client that updates the IP address information to DDNS service provider whenever there is a change. Therefore, users can build website or other Internet servers even if they don't have fixed IP connection.

DHCP

Dynamic Hosting Configuration Protocol. A protocol that enables a server to dynamically assign IP addresses. When DHCP is used, whenever a computer logs onto the network, it automatically gets an IP address assigned to it by DHCP server. A DHCP server can either be a designated PC on the network or another network device, such as a router.

DMZ

Demilitarized Zone. When a router opens a DMZ port to an internal network device, it opens all the TCP/UDP service ports to this particular device. The feature is used commonly for setting up H.323 VoIP or Multi-Media servers.

DNS

A program that translates URLs to IP addresses by accessing a database maintained on a collection of Internet servers.

Domain Name

The unique name that identifies an Internet site. Domain Names always have 2 or more parts, separated by dots. In www.airlive.com, the "airlive.com" is the domain name.

DoS Attack

Denial of Service. A type of network attack that floods the network with useless traffic. Many DoS attacks, such as the Ping of Death and Teardrop attacks, exploit limitations in the TCP/IP protocols.

Encryption

Encoding data to prevent it from being read by unauthorized people. The common wireless encryption schemes are WEP, WPA, and WPA2.

ESSID (SSID)

The identification name of an 802.11 wireless network. Since wireless network has no physical boundary like wired Ethernet network, wireless LAN needs an identifier to distinguish one network from the other. Wireless clients must know the SSID in order to associate with a WLAN network. Hide SSID feature disables SSID broadcast, so users must know the correct SSID in order to join a wireless network.

Firewall

A system that secures a network and prevents access by unauthorized users. Firewalls can be software, router, or gateway. Firewalls can prevent unrestricted access into a network, as well as restricting data from flowing out of a network.

Firmware

The program that runs inside embedded device such as router or AP. Many network devices are firmware upgradeable through web interface or utility program.



FTP

File Transfer Protocol. A standard protocol for sending files between computers over a TCP/IP network and the Internet.

Fragment Threshold

Frame Size larger than this will be divided into smaller fragment. If there are interferences in your area, lower this value can improve the performance. If there are not, keep this parameter at higher value. The default size is 2346. You can try 1500, 1000, or 500 when there are interference around your network.

Full Duplex

The ability of a networking device to receive and transmit data simultaneously. In wireless environment, this is usually done with 2 or more radios doing load balancing.

Gateway

In the global Internet network, the gateways are core routers that connect networks in different IP subnet together. In a LAN environment with an IP sharing router, the gateway is the router. In an office environment, gateway typically is a multi-function device that integrates NAT, firewall, bandwidth management, and other security functions.

Hotspot

A place where you can access Wi-Fi service. The term hotspot has two meanings in wireless deployment. One is the wireless infrastructure deployment, the other is the Internet access billing system. In a hotspot system, a service provider typically need an authentication and account system for billing purposes, and a wireless AP network to provide access for customers.

IGMP Snooping

Internet Group Management Protocol (IGMP) is a Layer 3 protocol to report IP multicast memberships to neighboring multicast switches and routers. IGMP snooping is a feature that allows an Ethernet switch to "listen in" on the IGMP conversation between hosts and routers. A switch support IGMP snooping has the possibility to avoid multicast traffic being treated as broadcast traffic; therefore, reducing the overall traffic on the network.

Infrastructure Mode

A wireless network that is built around one or more access points to provide wireless clients access to wired LAN / Internet service. The opposite of Infrastructure mode is Ad-hoc mode.

IP address

IP (Internet Protocol) is a layer-3 network protocol that is the basis of all Internet communication. An IP address is 32-bit number that identifies each sender or receiver of information that is sent across the Internet. An IP address has two parts: an identifier of a particular network on the Internet and an identifier of the particular device (which can be a server or a workstation) within that network. The new IPv6 specification supports 128-bit IP address format.

IPsec

IP Security. A set of protocols developed by the IETF to support secure exchange of packets at the IP layer. IPsec has been deployed widely to implement Virtual Private Networks (VPNs). IPsec supports two encryption modes: Transport and Tunnel. Transport mode encrypts only the data of each packet, but leaves the header untouched. The more secure Tunnel mode encrypts both the header and the payload. On the receiving side, an IPsec-compliant device decrypts each packet.

LACP (802.3ad) Trunking

The 802.3ad Link Aggregation standard defines how to combine the several Ethernet ports into one high-bandwidth port to increase the transmission speed. It is also known as port trunking. Both device must set the trunking feature to work.

MAC (Media Access Control)

MAC address provides layer-2 identification for Networking Devices. Each Ethernet device has its own unique address. The first 6 digits are unique for each manufacturer. When a network device have MAC access control feature, only the devices with the approved MAC address can connect with the network.

Mbps (Megabits per Second)

One million bits per second; a unit of measurement for data transmission

MESH

Mesh is an outdoor wireless technology that uses Spanning Tree Protocol (STP) and Wireless Distribution system to achieve self-forming, self-healing, and self-configuring outdoor network. MESH network are able to take the shortest path to a destination that does not have to be in the line of site.

MIMO (Multi-Input-Multi-Output)

A Smart Antenna technology designed to increase the coverage and performance of a WLAN network. In a MIMO device, 2 or more antennas are used to increase the receiver sensitivity and to focus available power at intended Rx.



NAT (Network Address Translation)

A network algorithm used by Routers to enables several PCs to share single IP address provided by the ISP. The IP that a router gets from the ISP side is called Real IP, the IP assigned to PC under the NAT environment is called Private IP.

Node

A network connection end point, typically a computer.

Packet

A unit of data sent over a network.

Passphrase

Used much like a password, a passphrase simplifies the WEP encryption process by automatically generating the WEP encryption keys for the company products.

PoE (Power over Ethernet)

A standard to deliver both power and data through one single Ethernet cable (UTP/STP). It allows network device to be installed far away from power source. A PoE system typically compose of 2 main component: DC Injector (Base Unit) and Splitter(Terminal Unit). The DC injector combines the power and data, and the splitter separates the data and power back. A PoE Access Point or CPE has the splitter built-in to the device. The IEEE 802.3af is a POE spec that uses 48 volt to deliver power up to 100 meter distance.

Port

This word has 2 different meaning for networking.

The hardware connection point on a computer or networking device used for plugging in a cable or an adapter.

The virtual connection point through which a computer uses a specific application on a server.

PPPoE

Point-to- Point Protocol over Ethernet. PPPoE relies on two widely accepted standards: PPP and Ethernet.

PPPoE is a specification for connecting the users on an Ethernet to the Internet through a common broadband medium, such as a single DSL line, wireless device or cable modem.

PPTP

Point-to-Point Tunneling Protocol: A VPN protocol developed by PPTP Forum. With PPTP, users can dial in to their corporate network via the Internet. If users require data encryption when using the Windows PPTP client, the remote VPN server must support MPPE (Microsoft Point-To-Point Encryption Protocol) encryption. PPTP is also used by some ISP for user authentication, particularly when pairing with legacy Alcatel / Thomson ADSL modem.

Preamble Type

Preamble are sent with each wireless packet transmit for transmission status. Use the long preamble type for better compatibility. Use the short preamble type for better performance

Rate Control

Ethernet switches' function to control the upstream and downstream speed of an individual port. Rate Control management uses "Flow Control" to limit the speed of a port. Therefore, the Ethernet adapter must also have the flow control enabled. One way to force the adapter's flow control on is to set a port to half-duplex mode.

RADIUS (Remote Authentication Dial-In User Service)

An authentication and accounting system used by many Internet Service Providers (ISPs). When you dial in to the ISP, you must enter your username and password. This information is passed to a RADIUS server, which checks that the information is correct, and then authorizes access to the ISP system. Radius typically uses port 1812 and port 1813 for authentication and accounting port. Though not an official standard, the RADIUS specification is maintained by a working group of the IETF.

Receiver Sensitivity

Receiver sensitivity means how sensitive is the radio for receiving signal. In general; the slower the transmission speed, the more sensitive the radio is. The unit for Receiver Sensitivity is in dB; the lower the absolute value is, the higher the signal strength. For example, -50dB is higher than -80dB.

RJ-45

Standard connectors for Twisted Pair copper cable used in Ethernet networks. Although they look similar to standard RJ-11 telephone connectors, RJ-45 connectors can have up to eight wires, whereas telephone connectors have only four.

Router

An IP sharing router is a device that allows multiple PCs to share one single broadband connection using NAT technology. A wireless router is a device that combines the functions of wireless Access Point and the IP sharing router.



RSSI

Receiver Sensitivity Index. RSSI is a value to show the Receiver Sensitivity of the remote wireless device. In general, remote APs with stronger signal will display higher RSSI values. For RSSI value, the smaller the absolute value is, the stronger the signal. For example, “-50db” has stronger signal than “-80dB”. For outdoor connection, signal stronger than -60dB is considered as a good connection.

RTS

Request To Send. A packet sent when a computer has data to transmit. The computer will wait for a CTS (Clear To Send) message before sending data.

RTS Threshold

RTS (Request to Send). The RTS/CTS(clear to send) packet will be send before a frame if the packet frame is larger than this value. Lower this value can improve the performance if there are many clients in your network. You can try 1500, 1000 or 500 when there are many clients in your AP's network.

SNMP (Simple Network Management Protocol)

A set of protocols for managing complex networks. The SNMP network contains 3 key elements: managed devices, agents, and network-management systems (NMSs). Managed devices are network devices that content SNMP agents. SNMP agents are programs that reside SNMP capable device's firmware to provide SNMP configuration service. The NMS typically is a PC based software such as HP Openview that can view and manage SNMP network device remotely.

SSH

Developed by SSH Communications Security Ltd., Secure Shell is a program to log into another computer over a network, to execute commands in a remote machine, and to move files from one machine to another. It provides strong authentication and secure communications over insecure channels. It is a replacement for rlogin, rsh, rcp, and rdist.

SSL

Secure Sockets Layer. It is a popular encryption scheme used by many online retail and banking sites to protect the financial integrity of transactions. When an SSL session begins, the server sends its public key to the browser. The browser then sends a randomly generated secret key back to the server in order to have a secret key exchange for that session. SSL VPN is also known as Web VPN. The HTTPS and SSH management interface use SSL for data encryption.

Subnet Mask

An address code mask that determines the size of the network. An IP subnet are determined by performing a BIT-wise AND operation between the IP address and the subnet mask. By changing the subnet mask, you can change the scope and size of a network.

Subnetwork or Subnet

Found in larger networks, these smaller networks are used to simplify addressing between numerous computers. Subnets connect to the central network through a router, hub or gateway. Each individual wireless LAN will probably use the same subnet for all the local computers it talks to.

Super A

Super A is an Atheros proprietary turbo mode to increase speed over standard 802.11a mode. It adds Bursting and Compression to increase the speed. If you live in countries that prohibit the channel binding technology (i.e. Europe), you should choose "Super-A without Turbo) if you need more speed than 11a mode

TCP

A layer-4 protocol used along with the IP to send data between computers over the Internet. While IP takes care of handling the actual delivery of the data, TCP takes care of keeping track of the packets that a message is divided into for efficient routing through the Internet.

Turbo A

Turbo A is an Atheros proprietary turbo mode to increase speed over standard 802.11a mode. It uses channel binding technology to increase speed. There are 2 types of Turbo A modes: Dynamic Turbo and Static Turbo. In Dynamic Turbo, the channel binding will be used only if necessary. In Static Turbo, the channel binding is always on. This protocol may be combined with Super-A model to increase the performance even more. The used of channel binding might be prohibited in EU countries.

TX Output Power

Transmit Output Power. The TX output power means the transmission output power of the radio. Normally, the TX output power level limit for 2.4GHz 11g/b is 20dBm at the antenna end. The output power limit for 5GHz 802.11a is 30dBm at the antenna end.

UDP (User Datagram Protocol)

A layer-4 network protocol for transmitting data which does not require acknowledgement from the recipient of the data.



Upgrade

To replace existing software or firmware with a newer version.

Upload

To send a file to the Internet or network device.

URL (Uniform Resource Locator)

The address of a file located on the Internet.

VPN (Virtual Private Network)

A type of technology designed to increase the security of information transferred over the Internet. VPN creates a private encrypted tunnel from the end user's computer, through the local wireless network, through the Internet, all the way to the corporate network.

Walled Garden

On the Internet, a walled garden refers to a browsing environment that controls the information and Web sites the user is able to access. This is a popular method used by ISPs in order to keep the user navigating only specific areas of the Web

WAN (Wide Area Network)

A communication system of connecting PCs and other computing devices across a large local, regional, national or international geographic area. A WAN port on the network device means the port (or wireless connection) that is connected to the Internet side of the network topology.

WEP (Wired Equivalent Privacy)

A wireless encryption protocol. WEP is available in 40-bit (64-bit), 108-bit (128-bit) or 152-bit (Atheros proprietary) encryption modes.

WPA (Wi-Fi Protected Access)

It is an encryption standard proposed by WiFi for advance protection by utilizing a password key (TKIP) or certificate. It is more secure than WEP encryption. The WPA-PSK utilizes pre-share key for encryption/authentication.

WPA2 (Wi-Fi Protected Access 2)

WPA2 is also known as 802.11i. It improves on the WPA security with CCMP and AES encryption. The WPA2 is backward compatible with WPA. WPA2-PSK utilizes pre-share key for encryption/authentication.

Wi-Fi (Wireless Fidelity)

An interoperability certification for wireless local area network (LAN) products based on the IEEE 802.11 standards. The governing body for Wi-Fi is called Wi-Fi Alliance (also known as WECA).

WiMAX (Worldwide Interoperability for Microwave Access)

A Wireless Metropolitan Network technology that complies with IEEE 802.16 and ETSI Hiperman standards. The original 802.16 standard call for operating frequency of 10 to 66Ghz spectrum. The 802.16a amendment extends the original standard into spectrum between 2 and 11 Ghz. 802.16d increase data rates to between 40 and 70 Mbps/s and add support for MIMO antennas, QoS, and multiple polling technologies. 802.16e adds mobility features, narrower bandwidth (a max of 5 mhz), slower speed and smaller antennas. Mobility is allowed up to 40 mph.

WDS (Wireless Distribution System)

WDS defines how multiple wireless Access Point or Wireless Router can connect together to form one single wireless network without using wired uplinks. WDS associate each other by MAC address, each device

WLAN (Wireless Local Area Network)

A type of local-area network that uses high-frequency radio waves rather than wires to communicate between nodes. The most popular standard for WLAN is the 802.11 standards.

WMM (Wi-Fi Multimedia)

WMM is a standard to prioritize traffic for multimedia applications. The WMM prioritize traffic on Voice-over-IP (VoIP), audio, video, and streaming media as well as traditional IP data over the AP.

WMS (Wireless Management System)

One of the utility programs that uses to manage multiple wireless AP/Bridges.