

**X - MICRO**

**WLAN 11g Broadband Router**

User Manual

# X - MICRO

## Plug & Fly

This product is in compliance with the essential requirements and other relevant provisions of the R&TTE directive 1999/5/EC.



**Product Name:** X-Micro WLAN 11g Broadband Router

**Model Name :** XWL-11GRIX

COUNTRY		CHANNELS	MAX. OUT POWER	
			INDOOR	OUTDOOR
<b>Spain</b>	2400-2483.5 MHz	1-13	< 100 mW EIRP	< 100 mW EIRP
<b>France</b>	2400-2454 MHz	1-8	< 100 mW EIRP	< 100 mW EIRP
<b>France</b>	2454-2483.5 MHz	9-13	< 100 mW EIRP	< 10 mW EIRP
<b>Italy</b>	2400-2483.5 MHz	1-13	< 100 mW EIRP	< 100 mW EIRP
<b>UK</b>	2400-2483.5 MHz	1-13	< 100 mW EIRP	< 100 mW EIRP
<b>Netherlands</b>	2400-2483.5 MHz	1-13	< 100 mW EIRP	< 100 mW EIRP
<b>Germany</b>	2400-2483.5 MHz	1-13	< 100 mW EIRP	< 100 mW EIRP
<b>Austria</b>	2400-2483.5 MHz	1-13	< 100 mW EIRP	< 100 mW EIRP
<b>Belgium</b>	2400-2483.5 MHz	1-13	< 100 mW EIRP	< 100 mW EIRP
<b>Switzerland</b>	2400-2483.5 MHz	1-13	< 100 mW EIRP	< 100 mW EIRP
<b>Luxemburg</b>	2400-2483.5 MHz	1-13	< 100 mW EIRP	< 100 mW EIRP
<b>Ireland</b>	2400-2483.5 MHz	1-13	< 100 mW EIRP	< 100 mW EIRP
<b>Portugal</b>	2400-2483.5 MHz	1-13	< 100 mW EIRP	< 100 mW EIRP
<b>Norway</b>	2400-2483.5 MHz	1-13	< 100 mW EIRP	< 100 mW EIRP
<b>Denmark</b>	2400-2483.5 MHz	1-13	< 100 mW EIRP	< 100 mW EIRP
<b>Finland</b>	2400-2483.5 MHz	1-13	< 100 mW EIRP	< 100 mW EIRP
<b>Iceland</b>	2400-2483.5 MHz	1-13	< 100 mW EIRP	< 100 mW EIRP
<b>Greece</b>	2400-2483.5 MHz	1-13	< 100 mW EIRP	< 100 mW EIRP
<b>Lichtenstein</b>	2400-2483.5 MHz	1-13	< 100 mW EIRP	< 100 mW EIRP
<b>Sweden</b>	2400-2483.5 MHz	1-13	< 100 mW EIRP	< 100 mW EIRP

## **FCC INFORMATION**

### **FCC Radiation Exposure Statement**

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body. This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

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

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

**Notice:** The Part 15 radio device operates on a non-interference basis with other devices operating at this frequency. Any changes or modification not expressly approved by the party responsible could void the user's authority to operate the device.

### **REGULATORY INFORMATION**

X-Micro WLAN 11g Broadband Router must be installed and used in strict accordance with the instructions. This device complies with the following radio frequency and safety standards.

#### **USA - Federal Communications Commission (FCC)**

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

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

### **Copyright**

Copyright 2004 by X-Micro Technology Corp., All rights reserved. No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language or computer language, in any form or by any means, electronic, mechanical, magnetic, optical, chemical, manual or otherwise, without the prior written permission of X-Micro Technology Corp.

### **Disclaimer**

X-Micro Technology Corp. makes no representations or warranties, either expressed or implied, with respect to the contents hereof and specifically disclaims any warranties, merchantability or fitness for any particular purpose. Any software described in this manual is sold or licensed "as is". Should the programs prove defective following their purchase, the buyer (and not this company, its distributor, or its dealer) assumes the entire cost of all necessary servicing, repair, and any incidental or consequential damages resulting from any defect in the software. Further, X-Micro Technology Corp., reserves the right to revise this publication and to make changes from time to time in the contents hereof without obligation to notify any person of such revision or change.

All brand and product names mentioned in this manual are trademarks and/or registered trademarks of their respective holders.

# Contents

1. OVERVIEW .....	6
1.1 Product Feature .....	6
1.2 System Requirements .....	6
1.3 Applications .....	6
2. Installing Your Router .....	7
2.1 Installation Instructions .....	7
3. Preparing Your Network .....	8
3.1 Configuring Windows for IP Networking .....	8
3.2 To Configure Windows to Receive Dynamic IP Address: .....	8
3.3 Collecting ISP Information .....	10
4. Basic Functions .....	11
4.1 To Open the Web-based Administration Tool: .....	11
4.2 Setup .....	13
4.3 Global Address .....	17
4.4. Wireless .....	20
4.5 Tools .....	29
4.6 Status .....	33
4.7 DHCP .....	36
4.8 Log .....	38
4.9 Statistics .....	41
5. Advanced Function .....	43
5.1. To Toggle between Basic Functions and Advanced Functions: .....	43
5.2 Virtual Servers .....	44
5.3 Filters .....	47
5.4 IP/URL Block .....	51
5.5 Special Apps .....	54
5.6 DMZ Host .....	58
5.7 MAC Clone .....	60
5.8 Dynamic DNS .....	61
5.9 Proxy DNS .....	63
5.10 SNMP .....	65
5.11 Static Routing .....	68

# **1. OVERVIEW**

## **1.1 Product Feature**

Compliance with IEEE 802.11g and 802.11b standards

Highly efficient design mechanism to provide unbeatable performance

Strong network security with WEP and 802.1X encryption

Achieving data rate up to 54Mbps for 802.11g and 11Mbps for 802.11b with wide range coverage; high performance to deliver up to 54Mbps raw data rate for 802.11g

Quick and easy setup with Web-based management utility

## **1.2 System Requirements**

Windows 98, 98SE, Millennium Edition (ME), 2000 and XP operating systems

Microsoft Internet Explorer 5.5 or higher

DSL/ Cable Modem Broadband Internet connection and ISP account

PCs equipped with 10 Mbps or 10/100 Mbps Ethernet connection to support TCP/IP protocol

One CD-ROM driver

## **1.3 Applications**

Home SOHO networking for device sharing and wireless multimedia

Wireless office provides a wider range for home and SOHO Ethernet

Enables wireless building-to-building data communication

Built-in infrastructure mode

Router provides ideal solution for:

Temporary LANs for scenarios such as trade-exhibitions and meetings

Enables LAN adaptability to frequently changing environments

Enables remote access to corporate network information, for example e-mail and company home page

## **2. Installing Your Router**

In this chapter, you'll learn how to connect your router.

### **2.1 Installation Instructions**

#### **To Connect the Router:**

- 2.1.1.** Make sure all equipments are turned off, including the router, Desktop or Laptop PCs, the cable and DSL modem, and so on.
- 2.1.2.** Connect the WAN Port of the router to the cable and DSL modem, Ethernet Server or the hub.
- 2.1.3.** Connect your client PCs to the LAN Ports.
- 2.1.4.** Connect the Power Adaptor (5VDC, 1.2A) to the power jack of the router and plug the power cable into the outlet.
- 2.1.5.** Turn on our PCs.

## 3. Preparing Your Network

In this chapter, you'll learn what to do before configuring your network.

**Before configuring your router, you need set up the computers in your network for TCP/IP networking and collect relevant ISP information if necessary.**

### 3.1 Configuring Windows for IP Networking

Each computer in your network should be configured for TCP/IP networking. There are two ways to configure your computers:

You are commended to use DHCP, then you can simply choose to receive an IP address automatically. For detailed instructions, see **Configure Windows to Receive Dynamic IP Address**.

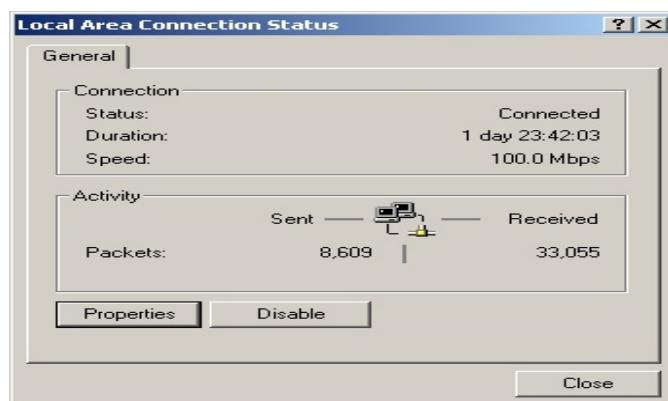
If you don't use DHCP, you need assign an IP address to each computer manually. For detailed instructions, refer to your Windows Documentation.

### 3.2 To Configure Windows to Receive Dynamic IP Address:

3.2.1. Click Start, then choose Settings > Network and Dial-up Connections.

3.2.2. Select the name of your ISP connection.

The Local Area Connection Status dialog box appears, seen in FIGURE 3-1:

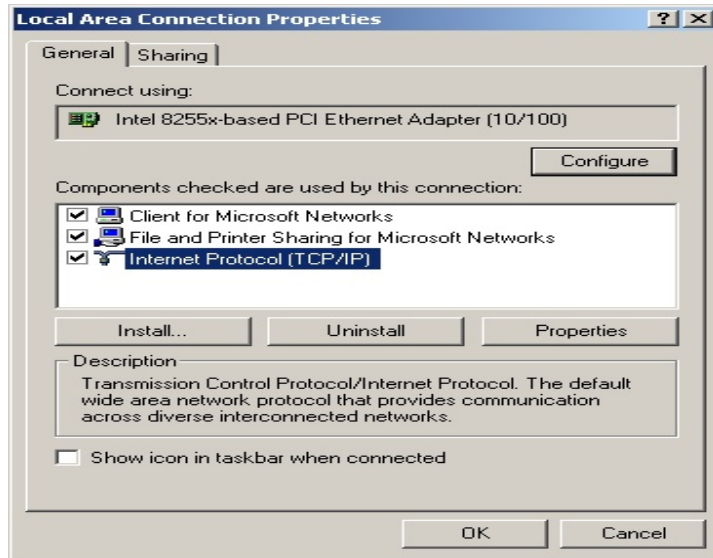




**FIGURE 3-1: Local Area Connection Status dialog box**

**3.2.3. Click Properties.**

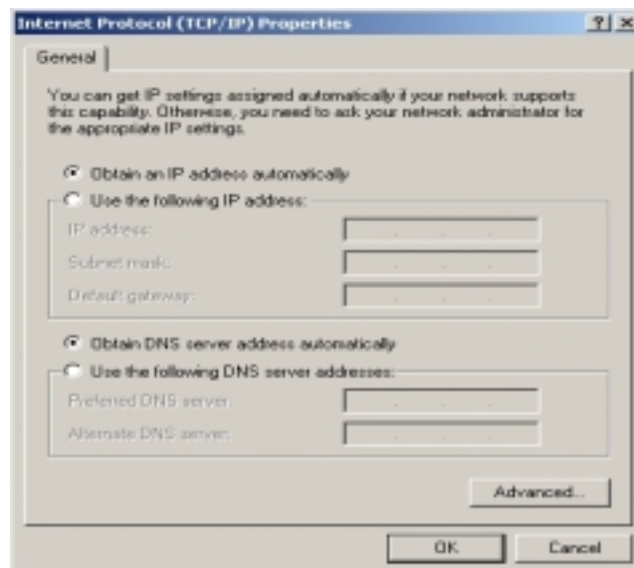
The Local Area Connection Properties dialog box appears, seen in FIGURE 3-2:



**FIGURE 3-2: Local Area Connection Properties dialog box.**

**3.2.4. Click Internet Protocol (TCP/IP), then click Properties.**

The Internet protocol (TCP/IP) Properties dialog box appears, seen in FIGURE 3-3:



### **FIGURE 3-3: Internet Protocol (TCP/IP) Properties dialog box**

**3.2.5. Click Obtain an IP address automatically and Obtain DNS server address automatically.**

**3.2.6. Click OK.**

You need restart your computer now or at a later time.

**Note :**

**The procedural steps above apply to Windows 2000 only. For Windows 95/98/ME/NT/XP, refer to your Windows Documentation.**

## **3.3 Collecting ISP Information**

You need query the relevant information from your ISP before configuring your router, for example:

Has your ISP assigned you a static or dynamic IP address? If you have obtained one static IP address, what is it?

Does your ISP use PPPoE? If so, what is your PPPoE user name and password?

If you are not sure of the above questions, call your ISP to clarify them.

## 4. Basic Functions

In this chapter, you will learn how to use basic functions that the Company AP Router provides, including Setup, Global Address, Wireless Tools, Status, DHCP, Log and Printer.

**The X-Micro WLAN 11g Broadband Router provides you a Web-based Administration Tool with which you can easily set up the router and customize the basic router settings. You can use this Web-based Tool from any computer in your network.**

**Notes :**

**Microsoft Internet Explorer 5.0 or later is highly recommended for using this Web-based Tool.**

**Graphics sampled in this chapter are provided for illustrations only. They may slightly differ from your own router screens.**

### 4.1 To Open the Web-based Administration Tool:

4.1.1. Open the browser on your PC.

4.1.2. Type *http://192.168.62.1* in the Address bar.

The Logon dialog box appears, seen in FIGURE 4-1:



**FIGURE 4-1: Logon dialog box**

4.1.3. Type *admin* in the User Name box.

4.1.4. Type the password in the box.

**Note :**

**The default password is “1234”. You can change the password on the Tools page. For detailed instructions, see To Change the Administrative Password for Your Router.**

4.1.5. Optional. To log on to the Administration Tool once for all, select the check box of Save this password in your password list.

4.1.6. Click OK.

The Company AP Router Administration Tool appears.

**Note :**

**The Administration Tool will time out after a period of idling, the Router may ask you to log on again.**

## 4.2 Setup

The Setup page allows you to edit the basic configuration parameters for your router, such as *Host Name*, *Domain Name*, *LAN IP Address*, *WAN IP Address*, *PPPoE Login*, *UPNP*, and so on.

In most cases, the default settings will be Okay for you. However, different ISPs (Internet Service Provider) may ask for specific requirements, please check it with your ISP if you are not sure.

### 4.2.1. To Configure Setup Parameters:

#### 4.2.1.1. Click Setup on the navigation bar.

The Setup page appears, seen in **FIGURE 4-2**:

The Setup page is displayed with a blue sidebar on the left containing labels for various configuration sections. The main content area contains the following fields and options:

- Host Name:** Text input field with a note "(Required by some ISPs)".
- Domain Name:** Text input field with a note "(Required by some ISPs)".
- Firmware Version:** Displays "20-06-07, Oct 20 2003 17:09:22".
- Time:** Displays "Thu Nov 6 3:52:57 2003".
- Set Time Zone:** Dropdown menu showing "(GMT-08:00)Pacific Time (US&Canada):Tijuana".
- Daylight Savings:** Radio buttons for "Enable" and "Disable" (selected).
- Daylight Period:** Two dropdown menus for month and day, both set to "JAN" and "01".
- LAN IP Address:** Fields for "Device IP Address" (192, 168, 62, 1) and "Subnet Mask" (255, 255, 255, 0).
- WAN IP Address:** Radio buttons for "Obtain an IP Address Automatically" (selected) and "Specify an IP Address".
  - Fields for "WAN IP Address", "Subnet Mask", "ISP Gateway Address", and "DNS" (1, 2, 3) are visible.
- PPPoE Login:** Radio buttons for "Enable" (selected) and "Disable".
  - "User Name" field: ad50189026
  - "Password" field: masked with asterisks.
  - Radio buttons for "Connect on Demand" and "Connect Manually" (selected).
  - Checkbox for "Max Idle Time" (checked) with a value of 10 minutes.
- UPNP:** Radio buttons for "Enable" (selected) and "Disable".

At the bottom of the page are three buttons: "Apply", "Cancel", and "Help".

**FIGURE 4-2: Setup page**

4.2.1.2. Type the Host Name, System Name or Account Name in the Host Name box if your ISP requires.

4.2.1.3. Type the Domain Name of your ISP in the box if your ISP requires, such as *xyz.isp.com*.

4.2.1.4. Optional. Review the firmware version number and date information that you are currently using.

4.2.1.5. Select a specific Time Zone from the Set Time Zone drop-down list, such as *(GMT+08:00) Beijing, Chongqing, Hong Kong, Urumqi*.

4.2.1.6. If you want to use Daylight Savings time, click Enable and select the start date and end date from the Daylight Period drop-down lists.

4.2.1.7. If you don't want to use Daylight Savings time, click Disable. If you select to disable the Daylight Savings, Daylight Period will not take effect any more.

4.2.1.8. Optional. Review the Device IP Address and Subnet Mask next to LAN IP Address and change the information if necessary.

LAN IP Address:	Device IP Address:	<input type="text" value="192"/>	.	<input type="text" value="168"/>	.	<input type="text" value="62"/>	.	<input type="text" value="1"/>
	Subnet Mask:	<input type="text" value="255"/>	.	<input type="text" value="255"/>	.	<input type="text" value="255"/>	.	<input type="text" value="0"/>

**Notes :**

*Device IP Address* and *Subnet Mask* are invisible to users on the LAN (Local Area Network) only.

In most cases, you need not make any change to LAN IP Address. If you change the LAN IP Address with DHCP enabled, you need to restart your client PCs; otherwise, you need reconfigure your client's IP addresses manually.

4.2.1.9. If you have enabled the DMZ feature on the DHCP page, review the DMZ IP Address and Subnet Address next to DMZ IP Address and change the information if necessary.

4.2.1.10. For WAN IP Address (Wide Area Network, also called Public IP), choose either Obtain an IP Address automatically or Specify an IP Address if your ISP has assigned you with static IP).

**Note :**

If you choose to obtain an IP Address automatically, skip Step 11.

**4.2.1.11. Optional.** If you select Specify an IP Address, type the WAN IP Address, Subnet Mask, ISP Gateway Address and DNS in the boxes, seen in FIGURE 4-3. You can collect such information from your ISP.

The screenshot shows a configuration window titled "Specify an IP Address" with a radio button selected. It contains the following fields:

- WAN IP Address: Four input boxes for IP octets.
- Subnet Mask: Four input boxes for subnet mask octets.
- ISP Gateway Address: Four input boxes for gateway IP octets.
- DNS: Three rows, each with a label (1:, 2:, 3:) and four input boxes for DNS server IP octets.

**FIGURE 4-3: WAN IP Address - Specify an IP Address**

**4.2.1.12.** If your ISP uses PPPoE (Point to Point Protocol over Ethernet), click Enable next to PPPoE Login; otherwise, click Disable. For detailed instructions on how to set the PPPoE Login parameters in FIGURE 3-4, see [To Set PPPoE Login Parameters](#) below.

**Notes :**

Using PPPoE, your ISP can authenticate your connection with a specific user name and password for security issues.

If you enable PPPoE, make sure to uninstall all existing applications on any computer in your network.

**4.2.1.13.** If you want to use UPNP (Universal Plug and Play) to plug devices like PCs, routers and others into a network and to automatically know about each other, click Enable next to UPNP; otherwise, click Disable.

**4.2.1.14.** When you have completed all the settings, click Apply, or click Cancel to undo your changes.

## 4.2.2. To Set PPPoE Login Parameters:

### 4.2.2.1. Click Enable next to PPPoE Login.



The screenshot shows a configuration window for PPPoE Login. On the left, there is a blue vertical bar with the text "PPPoE Login:". To the right, there are several settings: "Enable" is selected with a radio button, "Disable" is unselected; "User Name:" is followed by a text box containing "ad50159026"; "Password:" is followed by a text box containing "\*\*\*\*\*"; "Connect on Demand" is selected with a radio button, "Connect Manually" is unselected; and "Max Idle Time" is checked with a checkbox, followed by a text box containing "10" and the word "Minutes".

**FIGURE 4-4: Set PPPoE Login Parameters**

### 4.2.2.2. Type the User Name and Password provided by your ISP.

### 4.2.2.3. For connection types, you can select either Connect on Demand or Connect Manually.

### 4.2.2.4. Optional. If you want to limit the idling minutes, select Max Idle Time and type a maximum number in minutes.



## 4.3 Global Address

On the Global Address page, you can set up NAT (Network Address Translation) to provide internal-to-external IP address mappings. Have you enabled DMZ on the DHCP page? Depending on whether DMZ is enabled, you may follow different procedural steps.

### Notes :

**If you want to use Global Address mapping, you must enable NAT on the Filters page. For detailed instructions, see [To Set up a Port Filtering or Raw IP Filter](#).**

**If you have chosen to retrieve an IP address automatically, you will not need to use this function. Instead, the default public IP address will display on the Global Address page.**

What do you want to do?

### [Set up Global Address with DMZ Disabled](#)

### [Set up Global Address with DMZ Enabled](#)

### [Remove Global Addresses](#)

4.3.1. To Set up Global Address with DMZ Disabled:

4.3.1.1. Click Global Address on the navigation bar.

The Global Address page with DMZ Disabled appears, seen in **FIGURE 4-5:**

Setup	Global Address	Wireless	Tools	Status	DHCP	Log	Statistics
1:	0.0.0.0 (default public IP)						
2	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
3	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
4	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
5	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
6	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
7	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
8	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>

Apply Cancel Help

**FIGURE 4-5: Global Address Page with DMZ Disabled**

4.3.1.2. Review the first line in the above figure. It shows the default WAN IP address which is specified on the Setup page. If your ISP assigns you an IP address automatically, it will display here.

4.3.1.3. In Line 2 – Line 8, you can list up to 7 additional static, external IP addresses provided by your ISP.

4.3.1.4. When you have completed editing all the settings, click Apply, or click Cancel to undo your changes.

4.3.2. To Set up Global Address with DMZ Enabled:

4.3.2.1. Click Global Address on the navigation bar.

The Global Address page with DMZ Enabled appears, seen in FIGURE 4-6:

Setup	Global Address	Wireless	Tools	Status	DHCP	Log	Statistics
<b>External-Internal</b>							
1	200	168	76	2			
2	0	0	0	0			
3	0	0	0	0			
4	0	0	0	0			
5	0	0	0	0			
6	0	0	0	0			
<b>External-DMZ</b>							
1	0	0	0	0			
2	0	0	0	0			
3	0	0	0	0			
4	0	0	0	0			
5	0	0	0	0			
6	0	0	0	0			
				Apply	Cancel	Help	

FIGURE 4-6: Global Address Page with DMZ Enabled

**4.3.2.2. Review the first line in the above figure. It shows the default WAN IP address which is specified on the Setup page. If your ISP assigns you an IP address automatically, it will display here.**

**4.3.2.3. Next to External - Internal, you can list up to 6 static, external IP addresses provided by your ISP.**

**4.3.2.4. Next to External – DMZ, define for your DMZ network up to 6 static, external global IP addresses provided by your ISP.**

**4.3.2.5. When you have completed editing all the settings, click Apply, or click Cancel to undo your changes.**

**4.3.3. To Remove Global Addresses:**

**4.3.3.1. Click Global Address on the navigation bar.**

**4.3.3.2. For any entry you want to delete, enter 0.0.0.0, and click Apply.**

## 4.4. Wireless

Using Wireless, you can configure your router for wireless access. There are three parts on the Wireless page:

**Radio Settings:** Allows you to configure your Gateway for wireless access, including *Wireless Enable/Disable, Mode, ESSID, Beacon Interval, RTS Threshold, Preamble Type, Distribution System*, and so on.

**Security Setting:** Allows you to configure your Gateway for security issues.

**Status:** Allows you to find out your Gateway's AP Radio statistics and wireless devices of which the AP (Access Point) is aware.

You can easily toggle between the above three parts on the Wireless page.

On the Radio Settings page, Wireless Distribution System as defined by the IEEE 802.11 standard has been made available on the Company AP Router now. Hence, it is possible to wirelessly connect Access Points using up to 8 MAC Addresses of PC cards, so that you can extend a wired infrastructure to locations where cabling is not available. Thus those users can roam or stay connected to the available network resources.

What do you want to do?

### **Set the Wireless Radio Parameters**

### **Set the Wireless Security Parameters**

### **Review Wireless Status**

### **Disable Wireless**

#### 4.4.1. To Set the Wireless Radio Parameters:

##### 4.4.1.1. On the Wireless page, select Radio Settings.

The Radio Settings page appears, seen in FIGURE 4-7:

**FIGURE 4-7: Wireless – Radio Settings Page**

**4.4.1.2. Click Enable next to Wireless.**

**4.4.1.3. Optional. Review the firmware version number and date information that you are currently using.**

**4.4.1.4. Enter the following basic radio parameters:**

Parameter	Description
Mode	<p>Selects the <b>Wireless Mode</b> that your <b>Company AP Router</b> supports from the drop-down list.</p> <p>Available options are <b>802.11B</b>, <b>802.11G</b>, and <b>MIXED</b> which supports both 802.11B and 802.11G.</p>
ESSID	<p>Type the unique identifier for the <b>Extended Service Set</b> which is shared by client stations in an infrastructure association, such as <b>WLAN-test</b>.</p>

	It is case-sensitive and cannot exceed 32 characters.
Channel	<p>Selects one IEEE 802.11G channel for wireless LAN transmissions from the drop-down list.</p> <p>Specifies the bandwidth which the wireless radio operates. AP and the client stations that is associated work in one of channels from 1 to 14.</p>

**4.4.1.5. Enter the following advanced radio parameters:**

Parameter	Description
Beacon Interval	Type the time interval in milliseconds between beacons broadcast by AP (Access Point) in the Beacon Interval box, such as 100.
RTS Threshold	<p>Type a number in the RTS Threshold box.</p> <p>Also called Request-to-Send Threshold. This field specifies the minimum size of data frames above which RTS protocol is used, ranging from 256 to 2432. RTS helps prevent data collision from hidden nodes.</p>
Fragmentation Threshold	<p>Type a number in the Fragmentation Threshold box.</p> <p>For efficiency in high-traffic situations, large files are split into fragments. This field specifies the default packet size, an even number ranging from 256 to 2346.</p>
DTIM Interval	<p>Type a number in the DTIM Interval box.</p> <p>Also called Delivery Traffic Indication Map. This field specifies the number of beacon intervals between successive DTIMs, ranging from 1 to 255.</p>
Preamble Type	Select either Short Preamble (72 bits) or Long Preamble (144 bits).
Distribution System	<p>If you want to use Wireless Distribution System on your Router, click Enable next to Distribution System, then type the distributed client PCs' physical addresses, as described in Step 6.</p> <p>Otherwise, click Disable.</p>

**Note :**  
You can see the default values of the above advanced wireless settings on the right of the page. If you don't know how to change the settings, please leave as they are in Figure 4-8:

Default Values for Radio Settings	
Beacon Interval	100
RTS Threshold	2432
Fragmentation Threshold	2346
DTIM Interval	1
Preamble Type	Long Preamble
Distribution System	Disable

FIGURE 4-8: Default Values for Radio Settings

**4.4.1.6. Optional.** If you have enabled Distribution System, type the physical addresses of distributed client PCs in a wireless network in the Peer AP MAC Address 1-8 boxes, seen in FIGURE 4-9:

Distribution System:	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Peer AP MAC Address 1:	<input type="text"/>
Peer AP MAC Address 2:	<input type="text"/>
Peer AP MAC Address 3:	<input type="text"/>
Peer AP MAC Address 4:	<input type="text"/>
Peer AP MAC Address 5:	<input type="text"/>
Peer AP MAC Address 6:	<input type="text"/>
Peer AP MAC Address 7:	<input type="text"/>
Peer AP MAC Address 8:	<input type="text"/>

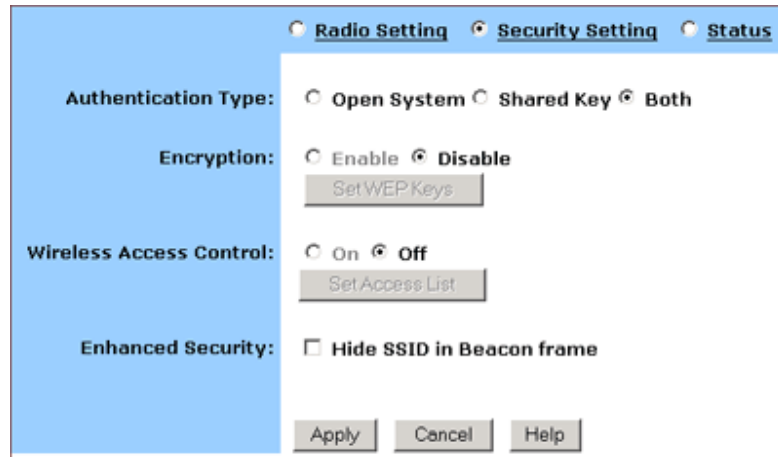
FIGURE 4-9: Peer AP MAC Addresses for Distribution Systems

**4.4.1.7.** When you have completed editing all the settings, click Apply, or click Cancel to undo your changes.

4.4.2. To Set Wireless Security Parameters:

4.4.2.1. Click Security Settings on the Wireless page.

The Security Settings appears, seen in FIGURE 4-10:



**FIGURE 4-10: Wireless – Security Settings Page**

**4.4.2.2. Select one of *Open System*, *Shared Key* and *Both* from the Authentication Type drop-down list.**

**Notes :**

**Authentication Type** indicates an authentication algorithm which can be supported by the Access Point:

**Open System:** The simplest of available authentication algorithms. Essentially it is a null algorithm. Any station that requests authentication with this algorithm may become authenticated if Open System is set at the recipient station.

**Shared Key:** Allows stations with a specific WEP (Wired Equivalent Privacy) Keys to be authenticated.

**Both:** Supports the authentications of either stations who know a shared key or those who do not.

**If you want to prevent other stations without specific WEP (Wired Equivalent Privacy) keys from linking to the AP, select Enable next to Encryption and then click Set WEP Keys to specify relevant keys; otherwise, select Disable. For detailed instructions on how to set the WEP Keys, see below To Set WEP Keys.**

**If you want to allow access to the Internet based on user’s MAC (Media Access Control) address, select On next to Wireless Access Control and then click Set Access List to specify relevant MAC addresses; otherwise, click Off. For detailed instructions on how to specify relevant MAC addresses, see below To Set Wireless Access Control.**



4.4.2.3. Next to Enhanced Security, select either Enable or Disable. If you choose to enable the enhanced security feature, go to Step 6.

4.4.2.4. Optional. If you have enabled Enhanced Security, you can choose to hide your SSID (Service Set Identifier) in Beacon frame.

4.4.2.5. When you have completed editing all the settings, click Apply, or click Cancel to undo your changes.

#### 4.4.3. To Set WEP Keys:

4.4.3.1. On the Security Settings page, enable the Encryption and click Set WEP Keys.

The Set WEP Keys window appears, seen in FIGURE 4-11:

The screenshot shows a window titled "Set WEP Keys". On the left is a blue sidebar with the following labels: "Encryption Level:", "WEP Key Type:", "Passphrase:", and "Default TX Key:". The main content area contains the following elements: "Encryption Level:" with radio buttons for "64 Bit" (selected) and "128 Bit"; "WEP Key Type:" with radio buttons for "Automatic" (selected) and "Manually"; "Passphrase:" with a text input field and a "Generate" button; four "Key" input fields labeled "Key 1:", "Key 2:", "Key 3:", and "Key 4:", each containing the text "00000"; a "Clear Keys" button; and a "Default TX Key:" dropdown menu with "1" selected. At the bottom of the window are "Apply" and "Cancel" buttons.

FIGURE 4-11: Set WEP Keys Window

4.4.3.2. Select either 64 Bit or 128 Bit next to Encryption Level.

**Note :**

**128 Bit encryption can provide you a more secure encryption algorithm, but it will slow down your network data transmission rates.**

**4.4.3.3.** If you want to generate WEP Keys automatically, do the following action:

**4.4.3.3.1.** Select Automatic next to WEP Key Type.

**4.4.3.3.2.** Type a string of any words in the Passphrase box, and click Generate.

**Four newly generated WEP Keys will display in the Key 1 – Key 4.**

**4.4.3.3.3.** Optional. Click Clear Keys to reset all the keys to null.

**Note :**

**Make sure that you write down the passphrase string, so that you can refer to it if necessary.**

**4.4.3.4.** If you want to enter the key elements manually, do the following action:

**4.4.3.4.1.** Select Manually next to WEP Key Type.

**4.4.3.4.2.** If you select Alphanumeric: 5 characters, type a string of 5 alphanumeric characters in the Key 1 – Key 4 boxes respectively.

**4.4.3.4.3.** If you select Hexadecimal: 10 digits (0-9, A-F), type a string of 10 hexadecimal digits in the Key 1 – Key 4 boxes respectively.

**4.4.3.4.4.** Optional. Click Clear Keys to reset all the keys to null.

4.4.3.5. Select the default encryption key from the Default TX Key drop-down list, such as Key 1.

4.4.3.6. When you have completed editing all the settings, click Apply, or click Cancel to undo your changes.

4.4.4. To Set Wireless Access Control:

4.4.4.1. On the Security Settings page, set the Wireless Access Control On and click Set Access List.

The Window Control List window appears, seen in FIGURE 4-12:

The screenshot shows a window titled "Wireless Control List" with a "Refresh" button in the top right corner. Below the title, there are 11 rows, each labeled "mac 1" through "mac 11" on the left. To the right of each label is a text input field containing the hexadecimal string "000000000000".

mac 1	000000000000
mac 2	000000000000
mac 3	000000000000
mac 4	000000000000
mac 5	000000000000
mac 6	000000000000
mac 7	000000000000
mac 8	000000000000
mac 9	000000000000
mac 10	000000000000
mac 11	000000000000

FIGURE 4-12: Wireless Control List window

4.4.4.2. Type the MAC addresses that you want to allow to access the Internet. You can specify up to 80 MAC addresses in the list.

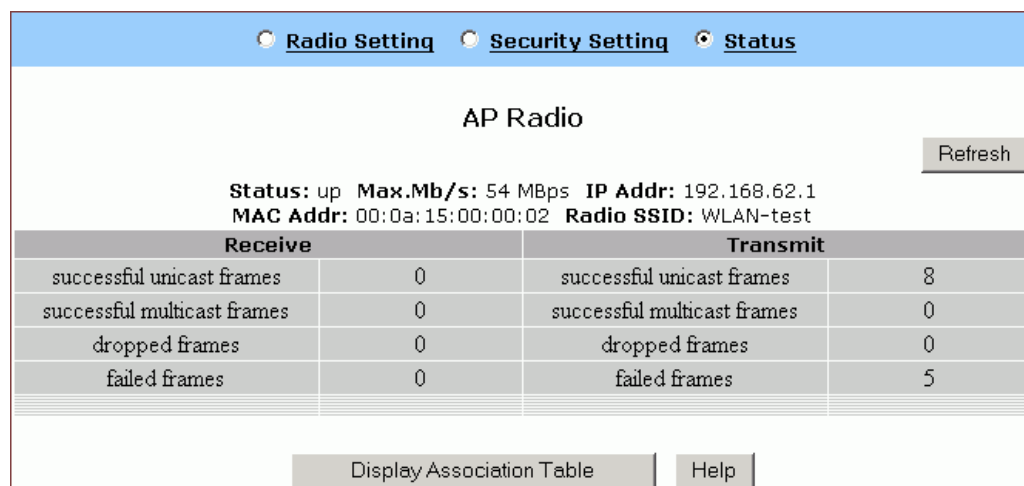
4.4.4.3. When you have complete editing all the MAC addresses, click Submit, or click Cancel to undo your changes.

4.4.4.4. Optional. You can click Refresh to see the most current MAC addresses in effect.

4.4.5. To Review Wireless Status:

4.4.5.1. On the Wireless page, select Status.

The Status page appears with your GateWay's AP Radio statistics including *Status*, *Max.Mb/s*, *IP Addr*, *MAC Addr*, *Radio SSID*, *Receive data* and *Transmit data*. Seen in FIGURE 4-13:



**FIGURE 4-13: Wireless – Status Page**

**4.4.5.2. To see the wireless devices of which the AP (Access Point) is aware, click Display Association Table.**

Index	Time	Mac Address	Add/Delete from Access List
1	None	None	None

**4.4.5.3. Optional. You can click Refresh to see the most current data.**

**4.4.6. To Disable Wireless:**

**4.4.6.1. On the Wireless page, select Radio Settings.**

**The Radio Settings page appears, seen in FIGURE 4-7.**

**If you don't want the router to support Wireless, select Disable.**

**Note :**  
**None of the router's wireless functions will work unless you enable it.**

## 4.5 Tools

On the Tools page, you can:

[Change the Administrative Password for Your Router](#)

[Restore the Factory Default Configuration](#)

[Reset Gateway](#)

[Upgrade the Firmware](#)

**! Important:**

We strongly recommend that you change the administrative password after the first login.

Restoring the default factory settings will reset all of the router configurations in every page, so we recommend that you backup the configuration data from the Gateway to your PC simply using DOS commands. In addition, you can also restore the factory defaults under the DOS window. For detailed instructions, see [To Backup or Restore the Configuration Data Using DOS Commands](#).

If you want to reset the hardware, you need reset the Gateway.

Before upgrading the firmware, you need download the firmware image file from the Gateway Web site and save it to your root local drive first.

4.5.1. To Change the Administrative Password for Your Router:

4.5.1.1. Click Tools on the navigation bar.

The Tools page appears, seen in FIGURE 4-14:

The screenshot shows a web interface with a blue sidebar on the left containing the following menu items: "Change Password:", "Restore Factory Defaults:", "Reset Gateway:", and "Upgrade Firmware:". The main content area contains the following elements:

- Change Password:** Three input fields for "Old Password:", "New Password:", and "Confirm Password:". Below the "New Password:" field is the text "(\* Maximum 31 characters)". Below these fields are three buttons: "Apply", "Cancel", and "Help".
- Restore Factory Defaults:** Two buttons: "Restore to Default" and "Backup/Restore Help".
- Reset Gateway:** One button: "Reset".
- Upgrade Firmware:** One input field, followed by three buttons: "Browse...", "Upgrade now", and "Help".

**FIGURE 4-14: Tools Page**

4.5.1.2. Type the Old Password in the box. The default password is 1234.

4.5.1.3. Type a New Password in the box.

**Note :**  
Password must be less than 64 characters.

4.5.1.4. Type the new password in the Confirm Password box.

4.5.2. To Restore the Factory Default Configuration:

4.5.2.1. On the Tools page, click Restore to Default next to Restore Factory Defaults.

The Warning dialog box appears, see FIGURE 4-15:



FIGURE 4-15: Warning Dialog Box

4.5.2.2. Click OK.

**Important:**  
Restoring the default factory settings will reset all of the router configurations in every page, so we recommend that you backup the configuration data from the Gateway to your PC first using DOS commands. For details, see [To Backup or Restore the Configuration Data Using DOS Commands.](#)  
In addition, you can also restore the factory defaults using DOS commands. For detailed instructions, see [To Backup or Restore the Configuration Data Using DOS Commands.](#)

4.5.3. *To Backup or Restore the Configuration Data Using DOS Commands:*

For the backup of the configuration data from the Gateway to your PC, Gateway acts as a TFTP server.

To backup the configuration data, under the DOS window, use the following command:

**tftp -i gateway\_ip\_address GET filename**

To restore the configuration data, under the DOS window, use the following command:

**tftp -i gateway\_ip\_address PUT filename**

gateway\_ip\_address: The IP address of the Gateway where you want to back the configuration data.

filename: The file name for backup from the Gateway. It must begin with “*nvr*am” which is not case-sensitive, such as “*nvr*am\_\_11032003”.

#### 4.5.4. To Reset Gateway:

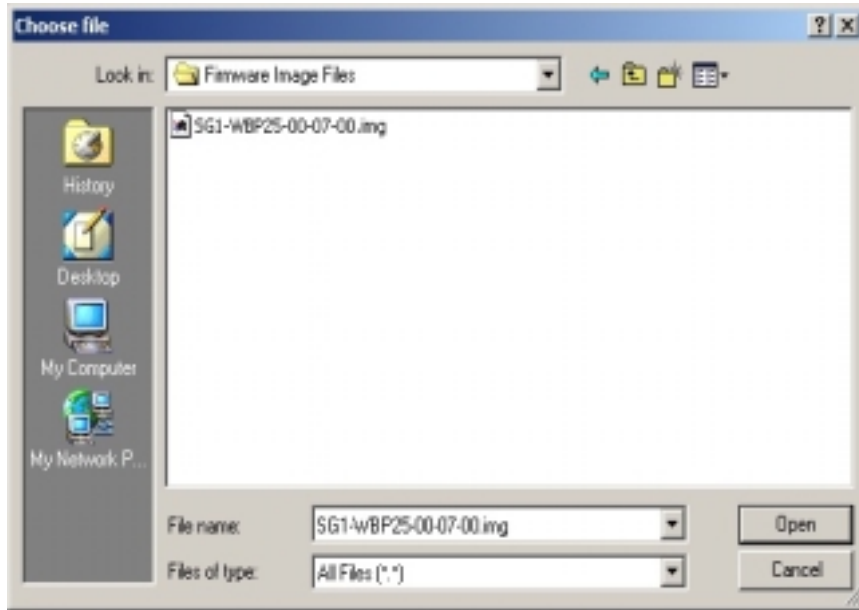
**If you want to reset the hardware, click Reset next to Reset Gateway on the Tools page.**

#### 4.5.5. To Upgrade the Firmware:

**4.5.5.1. Download a firmware image file from the Gateway Web site and save it to your root local drive.**

**4.5.5.2. Type the file path and file name in the Upgrade Firmware box, or click Browse to launch a Choose file dialog box, seen in**

**FIGURE 4-15:**



**FIGURE 4-15: Choose File Dialog Box for Upgrading Firmware**

**4.5.5.3. Locate the firmware you have downloaded and click Open.**

**4.5.5.4. The Choose file dialog box closes.**

**4.5.5.5. Click Upgrade Now. The firmware of the device will be**

**Caution :**

**The firmware upgrade may take about 10 seconds, please DONOT power off the unit when it is being upgraded.**

**upgraded.**



## 4.6 Status

On the Status page, you can view the most current information about your Router which will be continuously refreshed per 10 seconds, such as *Host Name*, *Domain*, *PPPoE Login*, *LAN/WAN* and *DDNS Status*. Different configuration may bring you to different data, compared in FIGURE 3-16 and FIGURE 4-17.

**Note :**

**If you want to change the configuration, go to the Setup page. For detailed instructions, see [Setup](#).**

If you have enabled the PPPoE Login, the Status page will display as illustrated in FIGURE 4-16:

<b>Host Name:</b>	StartGate
<b>Domain:</b>	xyz.isp.com
<b>PPPoE Login:</b>	Enabled Status: Disconnected
	<input type="button" value="Connect"/>
<b>LAN:</b>	
	<b>IP Address:</b> 192.168.62.1
	<b>Subnet Mask:</b> 255.255.255.0
<b>WAN:</b>	Dynamic
	<b>IP Address:</b> 0.0.0.0
	<b>Subnet Mask:</b> 255.0.0.0
	<b>Default Gateway:</b> 255.255.255.255
	<b>DNS:</b> 0.0.0.0
	0.0.0.0
	0.0.0.0
<b>DDNS Status:</b>	
	<b>Server:</b> The service is disabled
	<b>Status:</b> The account is not set yet.
	<input type="button" value="Help"/>

FIGURE 4-16: Status Page with PPPoE Login Enabled

If you have chosen the Dynamic IP and disabled PPPoE Login, the Status page will display as illustrated in FIGURE 4-17:

<b>Host Name:</b>	StartGate	
<b>Domain:</b>	xyz.isp.com	
<b>PPPoE Login:</b>	Disabled	
<b>LAN:</b>	<b>IP Address:</b>	192.168.62.1
	<b>Subnet Mask:</b>	255.255.255.0
<b>WAN:</b>	Dynamic	
	<b>IP Address:</b>	0.0.0.0
	<b>Subnet Mask:</b>	255.0.0.0
	<b>Default Gateway:</b>	255.255.255.255
	<b>DNS:</b>	0.0.0.0
		0.0.0.0
		0.0.0.0
	<input type="button" value="DHCP Release"/>	<input type="button" value="DHCP Renew"/>
<b>DDNS Status:</b>	<b>Server:</b>	The service is disabled
	<b>Status:</b>	The account is not set yet.
	<input type="button" value="Help"/>	

**Notes :**

**If you have chosen the Dynamic IP and disabled PPPoE Login, you can see the DHCP Release and DHCP Renew buttons:**

**To release the most current WAN IP address, click DHCP Release.**

**To renew the WAP IP address, click DHCP Renew.**

FIGURE 4-17: Status Page with PPPoE Login Disabled

**Status Detail:**

Parameter	Description
Host Name	<b>Shows the name of the device.</b>
Domain	<b>Shows the domain name of the device.</b>
PPPoE Login	<b>Shows the current status of PPPoE Login:</b>  Disabled  Enabled: Connected, Connecting or

	Disconnected.
LAN	<b>Shows the current IP Address and Subnet Mask of the device, as seen by users in your internal network.</b>
WAN	<b>Shows the IP Address, Subnet Mask, Default Gateway, and DNS of the router, as seen by external users on the Internet.</b>
DDNS	<b>Shows the Dynamic DNS Server and Status.</b>  <b>If you want to change the setting, go to the Advanced Dynamic DNS page. For details instructions, see <u><a href="#">To Configure a Dynamic DNS Server</a></u>.</b>

## 4.7 DHCP

On the DHCP page, you can set your NAT/Firewall Gateway as a DHCP (Dynamic Host Configuration Protocol) server, and DHCP servers will automatically assign IP addresses to all the client PCs in

### Notes

**If you want to enable DHCP, make sure that there is not already a DHCP server on your router.**

**If you don't enable DHCP on your router, you will need to manually configure an IP address for each PC in your network; if you do enable DHCP, make sure that each PC is configured to receive an IP address automatically.**

your network.

What do you want to do then?

[Set Your Router as a DHCP Server](#)

[View the Active IP Table](#)

[Disable DHCP on Your Router](#)

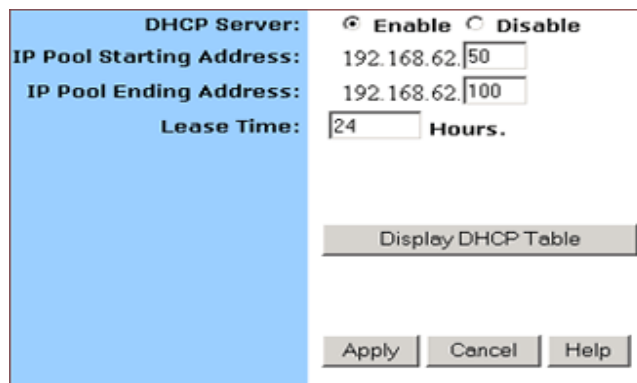
4.7.1. To Set Your Router as a DHCP Server:

**4.7.1.1. Make sure that there is not already a DHCP server on your router.**

**4.7.1.2. Make sure that each PC in your network is configured to receive an IP address automatically.**

**4.7.1.3. Click DHCP on the navigation bar.**

The DHCP page appears, seen in FIGURE 4-18:



The screenshot shows a configuration interface for DHCP. On the left, there is a blue vertical bar. To its right, the following fields are visible:

- DHCP Server:**  Enable  Disable
- IP Pool Starting Address:** 192.168.62.50
- IP Pool Ending Address:** 192.168.62.100
- Lease Time:** 24 Hours.

Below these fields are three buttons: "Display DHCP Table", "Apply", "Cancel", and "Help".

**FIGURE 4-18: DHCP Page**

**4.7.1.4. Click Enable next to DHCP Server.**

**4.7.1.5. Type a IP Pool Starting Address to designate the first IP address that can be assigned to a PC in your network.**

**4.7.1.6. Type a IP Pool Ending Address to designate the last IP address that can be assigned to a PC in your network.**

**4.7.1.7. When you have completed editing all the settings, click Apply, or click Cancel to undo your changes.**

**4.7.2. To Disable DHCP on Your Router:**

**4.7.2.1. On the DHCP page, click Disabled next to DHCP Server.**

**4.7.2.2. Click Apply.**

**4.7.3 To View the Active IP Table:**

**If you want to find out the information about PCs that have been assigned IP addresses by the DHCP server, click Display DHCP Table.**

***DHCP Server IP Address, Client Host Name, IP Address and MAC Address for each active client PC will be listed out in the table, seen in FIGURE 4-19:***

DHCP Active IP Table			
<input type="button" value="Refresh"/>			
DHCP Server IP Address:		192.168.62.1	
Index	Client Host Name	IP Address	MAC Address
1	swlab2	192.168.62.51	00:06:5b:a5:7b:59

**FIGURE 4-19: DHCP Active IP Table**

**Note :**

**If you have enabled the DMZ and LAN features, you can also find the relevant information in the DHCP Active IP Table for DMZ Zone and the DHCP Active IP Table for LAN.**

**Optional. Click Refresh to obtain the most current data.**

## 4.8 Log

On the Log page, you can set up Access Log and view log files that record the access activity of LAN and WAN client PCs, including *Session Event Log*, *Block Event Log*, *Intrusion Event Log* and *Wireless Event Log*.

What do you want to do?

[Set up Access Log on Your Router](#)

[View Session Event Log](#)

[View Block Event Log](#)

[View Intrusion Event Log](#)

[View Wireless Event Log](#)

4.8.1. To Set up Access Log on Your Router:

4.8.1.1. Click Log on the navigation bar.

The Log page appears, seen in FIGURE 4-20:

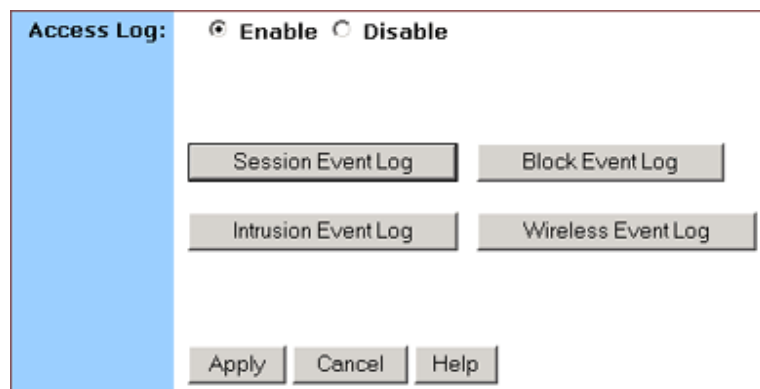


FIGURE 4-20: Log Page

4.8.1.2. Select Enable.

4.8.1.3. Click Apply, or click Cancel to undo your changes.

4.8.2. To View Session Event Log:

4.8.2.1. Click Session Event Log on the Log page.

The Session Event Log Table appears, including each session event entry information like *Record Name*, *Transport type*, *Source IP* and so on, seen in FIGURE 4-21:

Session Event Log Table							
Index	Record Time	Transport Type	Source IP	Source Port (Type:Code)	Destination IP	Destination Port (Type:Code)	Terminate Reason
1	2003.11.06 03:34:22	ICMP	61.173.63.220	0:8	61.171.242.88	0:0	POLICY_MIGRATION
2	2003.11.06 03:34:45	ICMP	218.80.56.153	0:8	61.171.242.88	0:0	POLICY_MIGRATION
3	2003.11.06 03:34:38	UDP	61.171.242.88	123	192.5.41.40	123	POLICY_MIGRATION
4	2003.11.06 03:35:49	ICMP	61.172.27.50	0:8	61.171.242.88	0:0	TIMOUT
5	2003.11.06 03:36:41	ICMP	61.172.104.82	0:8	61.171.242.88	0:0	TIMOUT

FIGURE 4-21: Session Event Log Table

4.8.2.2. Optional. Click Refresh to obtain the most current data.

4.8.2.3. Optional. Click Clear to delete all the log information.

4.8.3. To View Block Event Log:

4.8.3.1. Click Block Event Log on the Log page.

The Block Event Log Table appears, including each block event entry information like *Record Name*, *Transport type*, *Source IP* and so on, seen in FIGURE 4-22:

Block Event Log Table							
Index	Record Time	Transport Type	Source IP	Source Port (Type:Code)	Destination IP	Destination Port (Type:Code)	Terminate Reason
1	2003.11.06 03:34:46	TCP	218.80.56.153	3820	61.171.242.88	135	Default Defense
2	2003.11.06 03:34:52	TCP	218.80.56.153	3820	61.171.242.88	135	Default Defense
3	2003.11.06 03:35:01	TCP	61.171.212.54	3196	61.171.242.88	445	Default Defense
4	2003.11.06 03:35:04	TCP	61.171.212.54	3196	61.171.242.88	445	Default Defense
5	2003.11.06 03:36:00	TCP	195.117.228.35	4066	61.171.242.88	2098	Default Defense

FIGURE 4-22: Block Event Log Table

4.8.3.2. Optional. Click Refresh to obtain the most current data.

4.8.3.3. Optional. Click Clear to delete all the log information.

4.8.4. To View Intrusion Event Log:

**4.8.4.1. Click Intrusion Event Log on the Log page.**

The Intrusion Event Log Table appears, including each intrusion event entry's *Record Name* and *Intrusion Type*, seen in **FIGURE 4-23:**



Intrusion Event Log Table		
Index	Record Time	Intrusion Type
1	None	None

**FIGURE 4-23: Intrusion Event Log Table**

**4.8.4.2. Optional. Click Refresh to obtain the most current data.**

**4.8.4.3. Optional. Click Clear to delete all the log information.**

**4.8.5. To View Wireless Event Log:**

**4.8.5.1. Click Wireless Event Log on the Log page.**

The Session Event Log Table appears, including each wireless event entry's *Time*, *Severity* and *Description*, seen in **FIGURE 4-24:**



Wireless Event Log Table			
Index	Time	Severity	Description
1	2003.11.06 03:33:10	Info	WLAN zone information is not set
2	2003.11.06 03:33:11	Info	WLAN Access Point started
3	2003.11.06 03:49:42	Info	WLAN zone information is not set
4	2003.11.06 03:49:42	Info	WLAN Access Point started
5	2003.11.06 03:50:42	Info	WLAN zone information is not set
6	2003.11.06 03:50:42	Info	WLAN Access Point started
7	2003.11.06 03:51:42	Info	WLAN zone information is not set
8	2003.11.06 03:51:42	Info	WLAN Access Point started
9	2003.11.06 03:52:12	Info	WLAN zone information is not set
10	2003.11.06 03:52:12	Info	WLAN Access Point started

**FIGURE 4-24: Wireless Event Log Table**

**4.8.5.2. Optional. Click Refresh to obtain the most current data.**

**4.8.5.3. Optional. Click Clear to delete all the log information.**

**4.8.6. To Disable Access Log on Your Router:**

**4.8.6.1. On the Log page, click Disabled next to Access Log.**

**4.8.6.2. Click Apply.**



## 4.9 Statistics

On the Statistics page, you can view the statistics information of LAN, WAN and AP (Access Point) Radio ports, including *Status*, *Max.Mb/s*, *IP Addr* and *MAC Addr*, *Receive data* and *Transmit data*.

You can click Statistics on the navigation bar, and then the Statistics page appears, seen in FIGURE 4-25:

<a href="#">LAN</a>   <a href="#">WAN</a>   <a href="#">AP</a>			
<b>LAN Statistics</b>			
<a href="#">Refresh</a>			
Status: up Max.Mb/s: 100.0 IP Addr: 192.168.62.1 MAC Addr: 00:0a:15:00:00:00			
Receive		Transmit	
total bytes	180771	total bytes	2673637
unicast pkts	4542	unicast pkts	2001
multicast pkts	160	multicast pkts	1764
discards	0	discards	0
errors	0	errors	0
unknown protocols	901	packets queued	0
<b>WAN Statistics</b>			
<a href="#">Refresh</a>			
Status: up Max.Mb/s: 100.0 IP Addr: 0.0.0.0 MAC Addr: 00:0a:15:00:00:01			
Receive		Transmit	
total bytes	0	total bytes	1800
unicast pkts	0	unicast pkts	0
multicast pkts	0	multicast pkts	30
discards	0	discards	0
errors	0	errors	0
unknown protocols	0	packets queued	0
<b>AP Radio</b>			
<a href="#">Refresh</a>			
Status: up Max.Mb/s: 54 Mbps IP Addr: 192.168.62.1 MAC Addr: 00:0a:15:00:00:02 Radio SSID: WLAN-test			
Receive		Transmit	
successful unicast frames	0	successful unicast frames	9
successful multicast frames	0	successful multicast frames	0
dropped frames	0	dropped frames	0
failed frames	0	failed frames	3

**FIGURE 4-25: Statistics Page**

4.9.1. The Statistics page includes three parts:

4.9.1.1. LAN Statistics: Lists out the data on the LAN port.

4.9.1.2. WAN Statistics: Lists out the data on the WAN port.

4.9.1.3. AP Radio: Lists out the data on the Access Point's radio.

**Note :**

**You can also click Refresh in any part above to obtain the most current data.**

## 5. Advanced Function

In this chapter, you will learn how to use the advanced administrative functions that the Company AP Router provides, including Virtual Server, Filters, IP/URL Block, Special Apps, DMZ Host, MAC Clone, Dynamic DNS, Proxy DNS and SNMP.

The Web-based Administration Tool provides you some advanced services on the Advanced Function navigation bar, such as Filtering and cloning your MAC addresses.

In most cases, basic functions are Okay. If you want to set the advanced configuration, you will need to toggle to the Advanced Function navigation bar first.

### 5.1. To Toggle between Basic Functions and Advanced Functions:

5.1.1. To toggle to the Advanced window, click Advanced on the right side of the Basic window, seen in FIGURE 5-1:

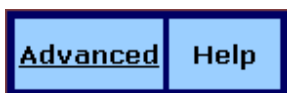


FIGURE 5-1: Advanced Button on the Basic Window

5.1.2. Once you are already in the Advanced window, click Basic on the right side of the Advanced window to return to the Basic Window, seen in FIGURE 5-2:

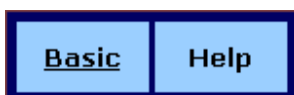


FIGURE 5-2: Advanced Button on the Basic Window

## 5.2 Virtual Servers

In some situations, you might want users on the Internet to be able to access servers on your LAN, such as an FTP Server, Telnet Server or Web Server. Such remote services are accomplished by creating *Virtual Server*.

Each virtual server has its own IP address and shares a single public IP address. It is defined by the Protocol type (*TCP, UDP or Both*) and a TCP/UDP/Both port number. Only the enabled virtual servers

**Note :**

**Configuring virtual servers may cause filters to be automatically created on the Filters page.**

can be accessed by remote users over the Internet.

What do you want to do?

[Set up a Client PC on the LAN as a Virtual Server](#)

[Delete Virtual Servers on the LAN](#)

5.2.1. To Set up a Client PC on the LAN as a Virtual Server:

5.2.1.1. On the Advanced navigation bar, click **Virtual Servers**.

The Virtual Servers page appears with a list of existing virtual servers, seen in **FIGURE 5-3**:

Service	Public IP Address	Public Port	Private Port	Protocol	Private IP Address
	0.0.0.0	0	0	TCP	192.168.62.0
	0.0.0.0	0	0	TCP	192.168.62.0
	0.0.0.0	0	0	TCP	192.168.62.0
	0.0.0.0	0	0	TCP	192.168.62.0
	0.0.0.0	0	0	TCP	192.168.62.0
	0.0.0.0	0	0	TCP	192.168.62.0
	0.0.0.0	0	0	TCP	192.168.62.0
	0.0.0.0	0	0	TCP	192.168.62.0
	0.0.0.0	0	0	TCP	192.168.62.0
	0.0.0.0	0	0	TCP	192.168.62.0
	0.0.0.0	0	0	TCP	192.168.62.0
	0.0.0.0	0	0	TCP	192.168.62.0

Apply Cancel Help

**FIGURE 5-3: Virtual Servers Page**

**5.2.1.2. If you have enabled DMZ and your Gateway is not configured to retrieve an IP address automatically, select either of the following options from the Choose Interface drop-down list:**

**(1) External – Internal: To set up Virtual Server in your LAN network.**

**(2) External – DMZ: To set up Virtual Servers in your DMZ network.**

**5.2.1.3. If you are using the Windows XP operating system, type a remote service name in the Service box.**

**Note :**

**It is only available for client PCs using Windows XP. Because Windows XP takes an advantage of the UPnP (Universal Plug and Play) feature of the Company AP Router, it allows client PCs that support UPnP to identify the router automatically.**

**5.2.1.4. Select a Public IP Address from the drop-down list.**

**Note :**

**The IP Address of a DMZ host will not appear in the list.**

**Type a port number in the Public Port and Private Port boxes, such as 80 for HTTP. For help on which port to choose, refer to Well-known Ports on the right of the page, seen in FIGURE 5-4:**

Well-known Ports	
7	Echo
21	FTP
23	TELNET
25	SMTP
53	DNS
79	finger
80	HTTP
110	POP3
113	auth
119	NNTP
161	SNMP
162	SNMP Trap
1723	PPTP

**FIGURE 5-4: Well-know Ports**

**Notes :**

**Public Port is the TCP/UDP/Both port number used by the server PC on the WAN. It is also called the external port number because this port number is visible to the users on the Internet.**

**Private Port is the TCP/UDP/Both port number used by the server PC on the LAN. The designated Public Port will be translated into this internal port number**

**5.2.1.5. Select one of *TCP*, *UDP* and *Both* from the Protocol drop-down list.**

**5.2.1.6. Type a local IP address of the server PC on the LAN in the Private IP Address box.**

**5.2.1.7. When you have completed editing all the settings, click Apply, or click Cancel to undo your changes.**

**5.2.2. To Delete Virtual Servers on the LAN:**

**5.2.2.1. On the Advanced navigation bar, click Virtual Servers.**

**A list of existing virtual servers appears.**

**5.2.2.2. For any virtual server you want to delete, select *0.0.0.0* from the Public IP Address drop-down list.**

**5.2.2.3. Click Apply.**

## 5.3 Filters

On the Filters page, you can set up filters that can selectively allow traffic to pass in and out of your network. The Company AP Router comes with 9 factory default filters for you.

In addition to 9 default filters, some filters may be created automatically to allow Virtual Servers or Special Applications to function.

We strongly recommend that you choose an empty row when you want to set up new filters, because overwriting or deleting these filters may cause some services to be disabled, for example, your client PCs may NOT be able to access the Internet.

**Note – If you have overwritten or deleted the factory default filters, you can retrieve them at a later time using the Restore Factory Defaults function on the Tools page. For detailed instructions, see [To Restore the Factory Default Configuration](#).**

What do you want to do?

[Set up a Port Filtering or Raw IP Filter](#)

[Delete a Port Filtering or Raw IP Filter](#)

5.3.1. To Set up a Port Filtering or Raw IP Filter:

5.3.1.1. On the Advanced navigation bar, click **Filters**.

The Filters page appears, seen in **FIGURE 5-5**:

Filtering Page: Page1 (1~12) ▾

ID	Filtering Layer	Proto Num	Direction	Private Port Range	Protocol
1	Port Filtering ▾	0	Outbound ▾	21 - 21	TCP ▾
2	Port Filtering ▾	0	Outbound ▾	1720 - 1720	TCP ▾
3	Port Filtering ▾	0	Outbound ▾	80 - 80	TCP ▾
4	Port Filtering ▾	0	Outbound ▾	53 - 53	UDP ▾
5	Port Filtering ▾	0	Outbound ▾	25 - 25	TCP ▾
6	Port Filtering ▾	0	Outbound ▾	110 - 110	TCP ▾
7	Port Filtering ▾	0	Outbound ▾	1503 - 1503	TCP ▾
8	Port Filtering ▾	0	Outbound ▾	443 - 443	TCP ▾
9	Raw IP ▾	1	Both ▾	0 - 0	TCP ▾
10	Port Filtering ▾	0	Inbound ▾	8080 - 8080	TCP ▾
11	Port Filtering ▾	0	Inbound ▾	0 - 0	TCP ▾
12	Port Filtering ▾	0	Inbound ▾	0 - 0	TCP ▾

NAT:  Enable  Disable  
 Firewall:  Enable  Disable  
 Remote Management:  Enable  Disable  
 IPSec Pass Through:  Enable  Disable  
 PPTP Pass Through:  Enable  Disable  
 Intrusion Detection:  Enable  Disable

FIGURE 5-5: Filters Page

5.3.1.2. Select an option from the Filtering Page drop-down list: 1~12, 13~24, 25~36.

5.3.1.3. If you select Port Filtering from the Filtering Layer drop-down list, do the following action:

5.3.1.3.1. Select a traffic direction from the drop-down list: *Inbound*, *Outbound* and *Both*.

5.3.1.3.2. Type the start port number and end port number that you want to allow in the Private Port Range boxes.

5.3.1.3.3. Select a protocol type from the drop-down list: *TCP*, *UDP* and *Both*.

5.3.1.4. If you select Raw IP from the Filtering Layer drop-down list, do the following action:



**5.3.1.4.1. Type an IP Protocol Number in the Proto**

**Note - It ranges from 0 to 255, but can not be 6 (TCP) or 17 (UDP); otherwise, this port filter will not work.**

**5.3.1.4.2. Select a traffic direction from the drop-down list: *Inbound Outbound* and *Both*.**

**5.3.1.4.3. Select an option from the Protocol drop-down list: *TCP, UDP* and *Both*.**

**5.3.1.5. Optional. Select Enable or Disable for the following additional filtering options:**

Parameter	Description
NAT	Allows you to set up NAT (Network Access Translation).
Firewall	Allows you to protect your network with a firewall.
Remote Management	Allows you to access your router's Web-based Administration Tool through your WAN connection.
IPSec Pass Through	Allows you to use IP Security Pass Through.
PPTP Pass Through	Allows you to use PPTP (Point-to-Point Tunneling Protocol), used to enable VPN sessions.
Intrusion Detect	Allows you to detect and record intrusion attempts into your network.

**5.3.1.6. When you have completed editing all the settings, click **Apply**, or click **Cancel** to undo your changes.**

### 5.3.2. To Delete Filters:

You can delete any existing Port Filtering or Raw IP filter, but make sure that you are deleting an unwanted one, otherwise deleting the filters associated with Virtual Servers or Special Applications may cause services to collapse down.

#### *5.3.2.1. To Delete a Port Filtering Filter:*

**5.3.2.1.1.** On the Filters page, for any Raw IP filter you want to delete, type *0* in the Private Port Range boxes.

**5.3.2.1.2.** Click Apply.

#### *5.3.2.2. To Delete a Raw IP Filter:*

**5.3.2.2.1.** On the Filters page, for any Raw IP filter you want to delete, type *0* in the Proto Num box.

**5.3.2.2.2.** Click Apply.

## 5.4 IP/URL Block

On the IP/URL Block page, you can create filters that can selectively block users from specific IP addresses and domain names to pass in and out of your network. The Company AP Router provides two ways of blocking users:

**IP Block:** Allows you to block a single IP address or a range of IP addresses.

**URL Block:** Allows you to block up to 36 domain names.

**Note – This IP/URL Block feature will block in both directions from specified IP addresses or domain names.**

What do you want to do?

[Block a Single IP Address](#)

[Block a Range of IP Address](#)

[Block a Specific Domain Name](#)

[Delete a Specific or All IP Blocks](#)

[Delete a Specific or All URL Blocks](#)

### 5.4.1. To Block a Single IP Address:

**Do either of the following:**

**5.4.1.1.** Click IP/URL Block on the Advanced navigation bar.

**5.4.1.2.** If you are on the URL Block page, select IP Block on the upper of the page.

**The IP Block page appears, seen in FIGURE 5-6:**

	IP Block Starting Address	IP Block Ending Address
1	[0] . [0] . [0] . [0]	[0] . [0] . [0] . [0]
2	[0] . [0] . [0] . [0]	[0] . [0] . [0] . [0]
3	[0] . [0] . [0] . [0]	[0] . [0] . [0] . [0]
4	[0] . [0] . [0] . [0]	[0] . [0] . [0] . [0]
5	[0] . [0] . [0] . [0]	[0] . [0] . [0] . [0]
6	[0] . [0] . [0] . [0]	[0] . [0] . [0] . [0]

Apply Cancel Clear All Help

**FIGURE 5-6: IP Block Page**

**5.4.1.3. In Line 1 – Line 6, type the same IP addresses in both IP Block Starting Address and IP Block Ending Address boxes respectively.**

**5.4.1.4. Optional. You can click Clear All to conveniently delete all the existing IP addresses and then do Step 2.**

**5.4.1.5. When you have completed editing all the IP addresses you want to block, click Apply, or click Cancel to undo your changes.**

#### **5.4.2. To Block a Range of IP Address:**

##### **5.4.2.1. Do either of the following:**

Click IP/URL Block on the Advanced navigation bar.  
If you are on the URL Block page, select IP Block on the upper of the page.

**The IP Block page appears, seen in FIGURE 4-6.**

**5.4.2.2. In Line 1 – Line 6, type the different IP addresses in both IP Block Starting Address and IP Block Ending Address boxes respectively.**

**5.4.2.3. Optional. You can click Clear All to conveniently delete all the existing IP addresses and then do Step 2.**

**5.4.2.4. When you have completed editing all the IP addresses you want to block, click Apply, or click Cancel to undo your changes.**

#### **5.4.3. To Block a Specific Domain Name:**

##### **5.4.3.1. Click IP/URL Block on the advanced navigation bar.**

**The IP Block page appears, seen in FIGURE 5-6.**

##### **5.4.3.2. Select URL Block on the IP Block page.**

**The URL Block page appears, seen in FIGURE 5-7:**

URL Block Domain Name	
1	<input type="text"/>
2	<input type="text"/>
3	<input type="text"/>
4	<input type="text"/>
5	<input type="text"/>
6	<input type="text"/>
7	<input type="text"/>

**FIGURE 5-7: URL Block Page**

**5.4.3.3. In Line 1 – Line 36, type the URLs you want to block.**

**5.4.3.4. Optional. You can click Clear All to conveniently delete all the existing URLs and then do Step 2.**

**5.4.3.5. When you have completed editing all the domain names you want to block, click Apply, or click Cancel to undo your changes.**

**5.4.4. To Delete a Specific or All IP Blocks:**

**5.4.4.1. On the IP Block page, do either of the following:**

**For any IP block you want to delete, type 0.0.0.0 in both IP Block Starting Address and IP Block Ending Address boxes respectively. If you want to delete all IP blocks, click Clear All.**

**5.4.4.2. Click Apply.**

**5.4.5. To Delete a Specific or All URL Blocks:**

**5.4.5.1. On the URL Block page, do either of the following:**

**For any domain name block you want to delete, clear out the URL in the box.**

**If you want to delete all URL blocks, click Clear All.**

**5.4.5.2. Click Apply.**

## 5.5 Special Apps

On the Special Apps page, you can authorize certain ports to communicate with PCs outside your network. It may be necessary for multi-session applications, such as online games and voice conferencing.

There are two ways of set up new special applications on your router:

**Popular Application Copy:** Allows you to select one of frequently used applications from the Popular Applications drop-down list and copy it to your Special Application Table. Available options are *AIM*, *Diablo II (1)*, *Diablo II (2)*, *StarCraft*, *StarCraft III*, *ICU11*, *FTP*, *CUseMe*, *MSN Messenger* and *Real Player*.

**Manual Configuration:** If the application you want to configure is not in the Popular Applications list, you can configure its settings manually.

Before configuring a new special application, would you please check the list of those popular applications first? If it is already in the list, we recommend that you use the Popular Application Copy unless you know exactly which settings to choose.

### Notes

**Configuring special applications may cause filters to be automatically created on the Filters page.**

**The Company AP Router provides two factory default special applications for FTP and NetMeeting, if you overwrite them or any other existing application, they will not work.**

What do you want to do?

[Copy a Popular Application to a Specific Line](#)

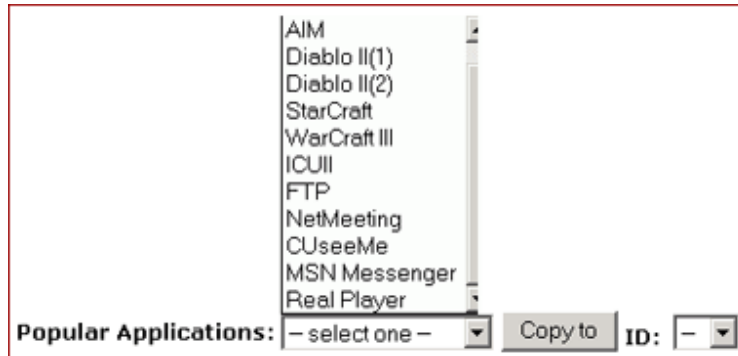
[Configure a Special Application Manually](#)

[Delete Special Applications](#)

5.5.1. To Copy a Popular Application to a Specific Line:

**5.5.1.1. On the Advanced navigation bar, click Special Apps.**

**The Popular Applications list appears on the Special Apps page, seen in FIGURE 5-8:**



**FIGURE 5-8: Popular Applications List**

5.5.1.2. Select an option from the Popular Applications drop-down list, including AIM, Diablo II (1), Diablo II (2), StarCraft, StarCraft III, ICUII, FTP, CUseeMe, MSN Messenger and Real Player.

**Note :**

**Make sure the specified ID presents an empty line unless you want to overwrite an existing application.**

**Select a specific line number from the ID drop-down list.**

**5.5.1.3. Click Copy to.**

**5.5.1.4. The selected application's configuration is added to your Special Applications Table on the upper of the page.**

**5.5.1.5. When you have completed editing all the settings, click Apply, or click Cancel to undo your changes.**

5.5.2. To Configure a Special Application Manually:

**5.5.2.1. On the Advanced navigation bar, click Special Apps.**

**5.5.2.2. The Special Apps page appears, seen in FIGURE 5-9:**

ID	Protocol	Trigger Port Range	Maximum Activity Interval	Session Chaining	Chaining on UDP	Address Replacement	Address Translation Type	Two Way Only
1	TCP	21 - 21	3000	Disable	Disable	Disable	TCP	Enable
2	TCP	1720 - 1720	30000	Enable	Disable	Enable	TCP	Disable
3	TCP	0 - 0	50	Enable	Enable	Enable	TCP	Enable
4	TCP	0 - 0	50	Enable	Enable	Enable	TCP	Enable
5	TCP	0 - 0	50	Enable	Enable	Enable	TCP	Enable
6	TCP	0 - 0	50	Enable	Enable	Enable	TCP	Enable
7	TCP	0 - 0	50	Enable	Enable	Enable	TCP	Enable
8	TCP	0 - 0	50	Enable	Enable	Enable	TCP	Enable
9	TCP	0 - 0	50	Enable	Enable	Enable	TCP	Enable
10	TCP	0 - 0	50	Enable	Enable	Enable	TCP	Enable
11	TCP	0 - 0	50	Enable	Enable	Enable	TCP	Enable
12	TCP	0 - 0	50	Enable	Enable	Enable	TCP	Enable

Apply Cancel Help

**FIGURE 5-9: Special Apps Page**

**5.5.2.3. Select a line corresponding to a specific ID.**

**Note :**

**Make sure you have selected an empty line unless you want to overwrite an existing application.**

**Enter the following configuration information:**

Parameter	Description
Protocol	<b>Specifies the communication protocol used by the application.</b>  <b>Available options are <i>TCP</i>, <i>UDP</i> and <i>Both</i>.</b>
Trigger Port Range	<b>Range of ports used for outgoing traffic. It will trigger the Gateway to accept certain incoming requests.</b>
Maximum Activity Interval	<b>Maximum number of miliseconds after the port trigger function, within which incoming requests will be accepted.</b>
Session Chaining	<b>Allows you to select either Enable or Disable.</b>  <b>Specifies whether dynamic sessions can be chained, allowing multi-session triggering.</b>
Chaining	<b>Allows you to select Enable or Disable only</b>



on UDP	<p>when <b>Session Chaining</b> is enabled.</p> <p><b>Specifies whether the session chaining is allowed on UDP.</b></p>
Address Replacement	<p><b>Allows you to select Enable or Disable only when Chaining on UDP is enabled.</b></p> <p><b>Specifies whether binary address replacement should be performed.</b></p>
Address Translation Type	<p><b>Allows you to select TCP or UDP only when Address Replacement is enabled.</b></p> <p><b>Specifies whether address translation is performed on TCP or UDP packets.</b></p>
Two Way Only	<p><b>Allows you to select either Enable or Disable.</b></p> <p><b>Specifies that a new session is allowed to be initiated from the same remote host.</b></p>

**5.5.2.4. When you have completed editing all the settings, click Apply, or click Cancel to undo your changes.**

**5.5.3. To Delete Special Applications:**

**5.5.3.1. On the Special Apps page, for any application you want to delete, type 0 – 0 in the Trigger Port Range box.**

**5.5.3.2. Click Apply.**

## 5.6 DMZ Host

On the DMZ Host page, you can expose one or more client PCs in your network to the Internet. It is often used for online games that require unrestricted two-way communications.

The total number of DMZ (Demilitarized Zone) hosts you can have depends on how many Global Addresses you have configured on the Global Address page. For example, if you have defined 5 Global Addresses (including the default IP), you are limited to 5 DMZ hosts. Since the maximum number of Global Addresses is 8, the total number of DMZ hosts you can configure is also 8.

**Caution :**

**Once a PC in your network is designated as DMZ host, it will not have any firewall protection.**

### What do you want to do?

[Designate a PC in Your Network as a DMZ Host](#)

[Delete DMZ Hosts](#)

5.6.1. To Designate a PC in Your Network as a DMZ Host:

5.6.1.1. On the Advanced navigation bar, click DMZ Host.

The DMZ Host page appears, seen in FIGURE 5-10:

Public IP Address	Private IP Address
0.0.0.0	192.168.62.0
0.0.0.0	192.168.62.0
0.0.0.0	192.168.62.0
0.0.0.0	192.168.62.0
0.0.0.0	192.168.62.0
0.0.0.0	192.168.62.0
0.0.0.0	192.168.62.0
0.0.0.0	192.168.62.0

Apply Cancel Help

FIGURE 5-10: DMZ Host Page

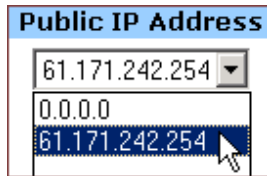
5.6.1.2. Select a Public IP Address from the drop-down list.

5.6.1.3. Type the IP address of a PC in your network that you want to designate as a DMZ Host in the Private IP Address box.

**5.6.1.4. When you have completed editing all the settings, click Apply, or click Cancel to undo your changes.**

**5.6.2. To Delete DMZ Hosts:**

**5.6.2.1. On the DMZ Host page, for any DMZ host you want to delete, select 0.0.0.0 from the Public IP Address drop-down list.**



**5.6.2.2. Click Apply.**

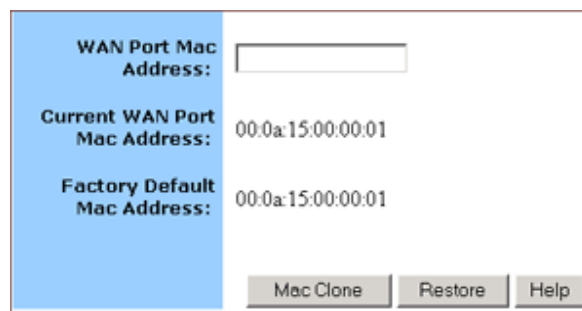
## 5.7 MAC Clone

If your ISP restricts services at a PC level, using MAC Clone, you can copy a PC MAC (Media Access Control) address to the router. Then what story will begin? The router will appear as a single PC, and multiple PCs in your network will access the Internet via this “*Single PC*”.

### 5.7.1. To Clone the MAC Address:

#### 5.7.1.1. On the Advanced navigation bar, click MAC Clone.

The MAC Clone page appears with the current WAN port address and the factory default MAC address for your convenience, seen in FIGURE 5-11:



The screenshot shows a web interface for cloning a MAC address. It features a light blue vertical bar on the left side. The main content area has three rows of labels and values. The first row is 'WAN Port Mac Address:' followed by an empty text input field. The second row is 'Current WAN Port Mac Address:' followed by the value '00:0a:15:00:00:01'. The third row is 'Factory Default Mac Address:' followed by the value '00:0a:15:00:00:01'. At the bottom right, there are three buttons: 'Mac Clone', 'Restore', and 'Help'.

WAN Port Mac Address:	<input type="text"/>
Current WAN Port Mac Address:	00:0a:15:00:00:01
Factory Default Mac Address:	00:0a:15:00:00:01

Mac Clone   Restore   Help

**Note :**

You may need to use the Ethernet MAC address of the NIC (Network Interface Card) that your PC is registered with your ISP.

**FIGURE 5-11: MAC Clone Page**

#### 5.7.1.2. Click Mac Clone, or click Restore to retrieve the default settings.

## 5.8 Dynamic DNS

On the Dynamic DNS page, you can tie up your domain name to a dynamic DNS provider. These providers allow you to associate a static hostname with a dynamic IP address, then you can connect to the Internet with a dynamic IP address and use applications that require a static IP address.

The Company AP Router supports three dynamic DNS providers:

[DynDNS.org](#)

[no-IP.com](#)

[no-IP.com](#)

What do you want to do?

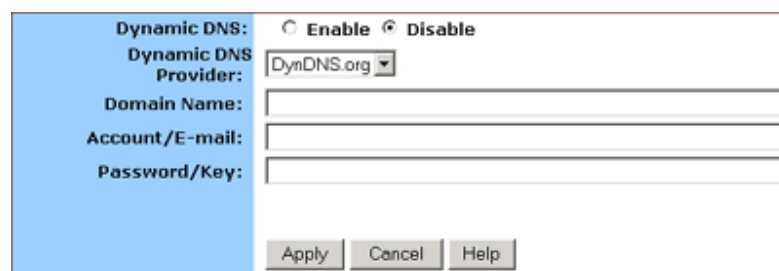
[Configure a Dynamic DNS Server](#)

[Disable a Dynamic DNS Server](#)

### 5.8.1. To Configure a Dynamic DNS Server:

**5.8.1.1. On the Advanced navigation bar, click Dynamic DNS.**

**The Dynamic Server page appears, seen in FIGURE 5-12:**



Dynamic DNS:  Enable  Disable  
Dynamic DNS Provider: DynDNS.org  
Domain Name:   
Account/E-mail:   
Password/Key:   
Apply Cancel Help

**FIGURE 5-12: Dynamic DNS page**

**5.8.1.2. Select Enable next to Dynamic DNS.**

**5.8.1.3. Select one of *DynDNS.org*, *no-IP.com*, *no-IP.com* from the Dynamic DNS Provider drop-down list.**

**5.8.1.4. Type your Domain Name in the box.**

**5.8.1.5. Type your Account or E-mail in the box.**

**5.8.1.6. Type your Password or Key in the box.**

**5.8.1.7. When you have completed editing all the settings, click Apply, or click Cancel to undo your changes.**

**5.8.2. To Disable a Dynamic DNS Server:**

**5.8.2.1. On the Dynamic DNS page, select Disable next to Dynamic DNS.**

**5.8.2.2. Click Apply.**

## 5.9 Proxy DNS

On the Proxy DNS page, you can map a domain name to a server IP address. Acting as a DNS server for internal and DMZ networks, it allows you to connect to local machines in your network without using an external DNS server. It simplifies the configuration and management of your network.

What do you want to do?

[Configure a Proxy DNS Server](#)

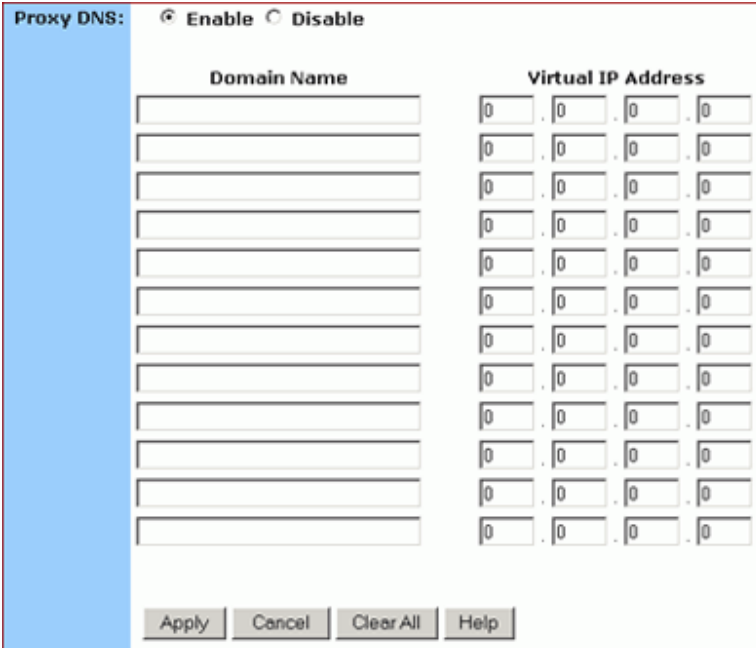
[Delete a Specific or All Proxy DNS Servers](#)

[Disable the Proxy DNS on Your Router](#)

5.9.1. To Configure a Proxy DNS Server:

5.9.1.1. On the Advanced navigation bar, click Proxy DNS.

The Proxy DNS page appears, seen in FIGURE 5-13:



Proxy DNS:  Enable  Disable

Domain Name	Virtual IP Address
<input type="text"/>	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>
<input type="text"/>	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>
<input type="text"/>	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>
<input type="text"/>	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>
<input type="text"/>	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>
<input type="text"/>	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>
<input type="text"/>	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>
<input type="text"/>	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>
<input type="text"/>	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>
<input type="text"/>	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>
<input type="text"/>	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>
<input type="text"/>	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>

FIGURE 5-13: Proxy DNS Page

5.9.1.2. Select Enable next to Proxy DNS.

5.9.1.3. Type a name for one PC in your network that you want to use as a Proxy DNS server in the Domain Name box.

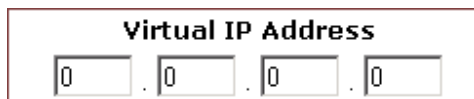
**5.9.1.4. Type the IP address for the PC in the Virtual IP Address box.**

**5.9.1.5. Optional. If you want to delete all the existing Proxy DNS servers first, click Clear All and do Step 3 and Step 4.**

**5.9.1.6. When you have completed editing all the settings, click Apply, or click Cancel to undo your changes.**

**5.9.2. To Delete a Specific or All Proxy DNS Servers:**

**5.9.2.1. On the Proxy DNS page, for any Proxy DNS server you want to delete, type 0.0.0.0 in the Virtual IP Address box.**



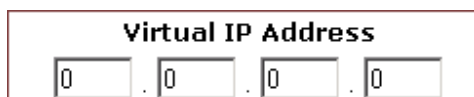
The image shows a rectangular input field with a red border. At the top, it is labeled "Virtual IP Address". Below the label, there are four small input boxes, each containing the digit "0", separated by dots. The entire field is enclosed in a red border.

**5.9.2.2. If you want to delete all the existing Proxy DNS servers, click Clear All.**

**5.9.2.3. Click Apply.**

**5.9.3. To Disable the Proxy DNS on Your Router:**

**5.9.3.1. On the Proxy DNS page, for any Proxy DNS server you want to delete, type 0.0.0.0 in the Virtual IP Address box.**



The image shows a rectangular input field with a red border. At the top, it is labeled "Virtual IP Address". Below the label, there are four small input boxes, each containing the digit "0", separated by dots. The entire field is enclosed in a red border.

**5.9.3.2. If you want to delete all the existing Proxy DNS servers, click Clear All.**

**5.9.3.3. Click Apply.**



## 5.10 SNMP

The Simple Network Management Protocol (SNMP) is an application layer protocol that facilitates the exchange of management information between network devices. It is part of TCP/IP (Transmission Control protocol/Internet Protocol) suite and enables you to control and monitor the network in a simple way.

On the SNMP page, you can edit the basic Agent information and also configure up to 6 SNMP trap receiver's IP Addresses. When a trap condition occurs, your router will send an SNMP trap message to any NMS (Network Management System) specified as trap receivers, for example, when power supply errors occur.

**Notes :**

**NMS (Network Management System) is an SNMP management application together with the computer it runs on.**

**Currently the Company AP Router supports SNMPv1 (SNMP version 1) and SNMPv2 (SNMP version 2) which have a number of features in common except for some enhancements.**

And moreover, you can specify different community names for authenticating access to the management information, which function as embedded passwords:

**Read:** Gives you READ access to all the management information, but does not allow WRITE access.

**Write:** Gives you both READ and WRITE access to all the

**Note :**

**The community name definitions on your NMS must match at least one of the above two community name definitions.**

management information.

What do you want to do?

[Configure Agent Information, SNMP Trap Host IP Addresses and Community Names on Your Router](#)

[Delete an Existing SNMP Trap Receiver](#)

[Delete SNMP Community Names](#)

5.10.1. To Configure Agent Information, SNMP Trap Host IP Addresses and Community Names on Your Router:

5.10.1.1. On the Advanced navigation bar, click SNMP.

The SNMP page appears, seen in FIGURE 5-14:

The screenshot shows the SNMP configuration interface. On the left, a blue sidebar contains the following labels: Name, Contact, Location, SNMP Trap Host IP 1, SNMP Trap Host IP 2, SNMP Trap Host IP 3, SNMP Trap Host IP 4, SNMP Trap Host IP 5, and SNMP Trap Host IP 6. The main content area has input fields for Name (containing 'SOHO Router'), Contact, and Location. Below these are six rows of IP address input fields, each consisting of four boxes separated by dots. At the bottom of the main area are 'Apply', 'Cancel', and 'Help' buttons. Below the main area is a 'Community List' table with the following structure:

	SNMP Community	SNMP Access	
	<input type="text"/>	Read	<< Add
1	None	None	Delete

FIGURE 5-14: SNMP Page

Enter the following Agent information:

Parameter	Description
Name	<p>Specifies an administratively-assigned name for this managed node, like <i>SOHO Router</i>.</p> <p>It is a string of the maximum 31 alphanumeric characters.</p>
Contact	<p>Specifies the contact person of this managed node, plus phone number, Email address, etc.</p> <p>It is a string of the maximum of 255 alphanumeric characters.</p>
Location	<p>Specifies the physical location of this managed node, for example, city, address and specific office location.</p> <p>It is a string of the maximum of 255 alphanumeric characters.</p>

**5.10.1.2. To send SNMP trap messages to any NMS, type up to 6 trap receiver IP addresses in the SNMP Trap Host IP Address 1 – SNMP Trap Host IP Address 6 boxes.**

**5.10.1.3. To secure SNMP with community names, do the following action:**

**5.10.1.3.1.** Type a string in the SNMP Community box, like Public.

**5.10.1.3.2.** Select an option from the SNMP Access drop-down list, for example, Read.

**Note :**

**Usually, we define a string of “Public” for Read access and “Private” for Read-Write access.**

**5.10.1.3.3.** Click Add. If you want to add more community names, do Step 4.1 – Step 4.3 again.

**5.10.1.4. When you have completed editing all the settings, click Apply, or click Cancel to undo your changes.**

**5.10.2. To Delete an Existing SNMP Trap Receiver:**

**5.10.2.1. On the SNMP page, for any SNMP trap receiver that you want to delete, enter 0.0.0.0 in the SNMP Trap Host IP Address box.**

Community List:			
	SNMP Community	SNMP Access	
	<input type="text"/>	Read	<< Add
1	Public	Read	Delete

**5.10.2.2. Click Apply.**

**5.10.3. To Delete SNMP Community Names:**

**5.10.3.1. On the SNMP page, for any SNMP community name that you want to delete, click Delete in the corresponding row.**

**5.10.3.2. Click Apply.**

## 5.11 Static Routing

The Static Routing is used to configure static routes to remote networks manually, where the route is predefined and is not supervised by the Routing Information Protocol (RIP). It can explicitly reduce the network traffic and speed the Internet connects for a small network.

However, it may fall into a certain disadvantage. When a static router involves more than one Hop, if the connection to the next hop goes down, the router cannot be aware of the invalid path and continues to route traffic on this hop.

On the Static Routing page, you can add up to 20 static routes by indicating:

Destination LAN IP address and Subnet Mask

Remote gateway

Hop

Router interface through which to forward the packets to the destination.

**Note :**

**If the network topology changes, you may have to make changes to the static routing tables for relevant static routes.**

What do you want to do?

[Add a New Static Route](#)

[Delete a Static Route](#)

### 5.11.1. To Add a New Static Route:

#### 5.11.1.1. On the Advanced navigation bar, click Routing.

The Static Routing page appears, seen in FIGURE 5-15:

Static Routing:							
Destination LAN IP	Subnet Mask			Gateway	Hop	Interface	
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	WAN	<< Add
192.168.99.10	255	255	255	0	192.168.99.1	3	WAN Delete

FIGURE 5-15: Static Routing Page

#### 5.11.1.2. Enter the following static route information:

Parameter	Description
Destination LAN IP	<b>Specifies the network address of the remote LAN segment. For standard class "C" LANs, the network address is the first 3 fields of this Destination LAN IP, the 4th field can be left at 0.</b>
Subnet Mask	<b>Specifies the Subnet Mask used on the remote LAN segment. For class "C" networks, the standard Network Mask is 255.255.255.0.</b>
Gateway	<b>Specifies the IP Address of the router on the local LAN segment to which this device is attached.</b>  <b>Note that it is NOT the router on the remote LAN segment.</b>
Hop	<b>Specifies the number of routers that must be traversed to reach the remote LAN segment. Valid values are 1 to 16.</b>
Interface	<b>Specifies the interface through which the router goes to the next hop or a particular network. Available options are WAN, LAN and DMZ.</b>

**5.11.1.3. Click <<Add.**

**The new static route appears in the static routing list.**

**5.11.2. To Delete a Static Route:**

**5.11.2.1. On the Static Routing page, for any static route that you want to delete, review the relevant information, seen in FIGURE 5 – 15.**

**5.11.2.2. Click Delete.**

## 6. Glossary

### **IEEE 802.11 Standard**

The IEEE 802.11 Wireless LAN standards subcommittee, which is formulating a standard for the industry.

### **Access point**

An Internet working device that seamlessly connects wired and wireless networks together.

### **Ad hoc**

An ad hoc wireless LAN is a group of computers, each with a WLAN adapter, connected as an independent wireless LAN. Ad hoc wireless LAN is applicable at a departmental scale for a branch or SOHO operation.

### **BSSID**

A specific ad hoc LAN is called a Basic Service Set (BSS). Computers in a BSS must be configured with the same BSSID.

### **DHCP**

Dynamic Host Configuration Protocol - a method in which IP addresses are assigned by a server dynamically to clients on the network. DHCP is used for dynamic IP addressing and requires a dedicated DHCP server on the network.

### **DSSS**

Direct Sequence Spread Spectrum. This is the method the wireless adapters use to transmit data over the frequency spectrum. An alternative method is frequency hopping. Direct sequence spreads the data over one frequency range (channel) while frequency hopping jumps from one narrow frequency band to another many times per second.

### **ESSID**

An infrastructure configuration could also support roaming capability for mobile workers. More than one BSS can be configured as an extended service set (ESS). Users within an ESS can roam freely between BSSs while served as a continuous connection to the network wireless stations and access points within an ESS must be configured with the same ESSID and the same radio channel.

### **Ethernet**

Ethernet is a 10/100Mbps network that runs over dedicated home/office wiring.

Users must be wired to the network at all times to gain access.

### **Gateway**

A gateway is a hardware and software device that connects two dissimilar systems, such as a LAN and a mainframe. In Internet terminology, a gateway is another name for a router.

Generally a gateway is used as a funnel for all traffic to the Internet.

## **IEEE**

Institute of Electrical and Electronics Engineers

## **Infrastructure**

An integrated wireless and wired LAN is called an infrastructure configuration. Infrastructure is applicable on an enterprise scale for wireless access to a central database, or wireless application for mobile workers.

## **ISM Band**

The FCC and their counterparts outside of the U.S. have set aside bandwidth for unlicensed use in the so-called ISM (Industrial, Scientific and Medical) band. Spectrum in the vicinity of 2.4 GHz, in particular, is being made available worldwide. This presents a truly revolutionary opportunity to place convenient high speed wireless capabilities in the hands of users around the globe.

## **LAN**

Local Area Network. A LAN is a group of computers, each equipped with the appropriate network adapter connected by cable/air that share applications, data, and peripherals. All connections are made via cable or wireless media, but a LAN does not use telephone services. It typically spans a single building or campus.

## **Network**

A network is a system of computers that is connected. Data, files, and messages can be transmitted over this network. Networks may be local or wide area networks.

## **Protocol**

A protocol is a standardized set of rules that specify how a communication is to take place, including the format, timing, sequencing and/ or error checking.

## **SSID**

Service Set Identifier. A network ID unique to a network. Only clients and access points that share the same SSID are able to communicate with each other. This string is case-sensitive.

## **SNMP**

Simple Network Management Protocol is the network management protocol of TCP/IP. In SNMP, agents-which can be hardware as well as software-monitor the activity in the various devices on the network and report to the network console workstation. Control information about each device is maintained in a structure known as a management information block.

## **Static IP addressing**

A method of assigning IP addresses to clients on the network. In networks with static IP address, the network administrator manually assigns an IP address to each computer. Once a static IP address is assigned, a computer uses the same IP address every time it reboots and logs on to the network, unless it is manually changed.

## **TCP/IP**

Transmission Control Protocol / Internet Protocol. TCP/IP is the protocol suite developed by



the Advanced Research Projects Agency (ARPA). TCP governs how a packet is sequenced for transmission the network. The term "TCP/IP" is often used generically to refer to the entire suite of related protocols.

**Transmit / Receive**

The wireless throughput in bytes per second (Bps) averaged over two seconds.

**WAN**

Wide Area Network. A WAN consists of multiple LANs that are tied together via telephone services and / or fiber optic cabling. WANs may span a city, a state, a country, or even the world.

**X - MICRO**  
*Plug & fly*

*[www.x-micro.com](http://www.x-micro.com)*