



Wireless Broadband Router 100G+

WL-122

---

---

*Full Manual*

---

---

# Table of Contents

<b>REQUIREMENTS</b> .....	<b>3</b>
<b>INTRODUCTION</b> .....	<b>3</b>
<b>WL-122 Features</b> .....	<b>3</b>
Internet Access Features .....	3
Advanced Internet Functions .....	3
Wireless Features .....	4
LAN Features .....	4
Configuration & Management .....	4
Security Features.....	4
<b>SETTING UP THE ROUTER</b> .....	<b>5</b>
<b>Physical installation</b> .....	<b>5</b>
Top LEDs .....	7
Rear Panel .....	8
<b>PC SETUP</b> .....	<b>9</b>
<b>Set up TCP/IP</b> .....	<b>9</b>
Using DHCP .....	9
Windows 98/ME.....	9
Windows 2000/XP.....	9
Windows NT.....	11
Macintosh Clients.....	12
Linux Clients .....	12
Wireless Adapter .....	12
<b>Internet access</b> .....	<b>13</b>
Windows 98/ME/2000 .....	13
Windows XP .....	13
Accessing AOL.....	13
<b>ROUTER CONFIGURATION</b> .....	<b>14</b>
<b>Your country/ISP is not listed</b> .....	<b>17</b>
<b>Home Screen</b> .....	<b>23</b>
<b>Setup Screen</b> .....	<b>24</b>
LAN IP.....	24
Wan Type .....	25
DHCP Server .....	26
WLAN screen.....	29
WLAN Security .....	31
<b>Advanced Screen</b> .....	<b>37</b>
Virtual Server.....	37
Firewall .....	38
<b>Toolbox Screen</b> .....	<b>41</b>
Password.....	41
Firmware update .....	41
<b>APPENDIX A TROUBLESHOOTING</b> .....	<b>42</b>
<b>Overview</b> .....	<b>42</b>
<b>General Problems</b> .....	<b>42</b>
<b>Internet Access</b> .....	<b>42</b>
<b>Wireless Access</b> .....	<b>43</b>
<b>FCC Statement</b> .....	<b>45</b>
FCC Radiation Exposure Statement .....	45
CE Marking Warning.....	45

# Requirements

- Cable modem or DSL/ADSL modem.
- Standard 10/100BaseT (UTP) network cables with RJ45 connectors.
- PCs that make use of the TCP/IP network protocol.

# Introduction

Congratulations on the purchase of your new WL-122 Broadband Router. The WL-122 is a multi-function device providing the following services:

- **Shared Broadband Internet Access** for all LAN users.
- **4-Port Switching Hub** for 10BaseT or 100BaseT connections.

## WL-122 Features

The WL-122 incorporates many advanced features, carefully designed to provide sophisticated functions while being easy to use.

### Internet Access Features

- **Shared Internet Access.** All users on the LAN or WLAN can access the Internet through the WL-122, 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).
- **DSL & Cable Modem Support.** The WL-122 has a 10/100BaseT Ethernet port for connecting a DSL or Cable Modem. All popular DSL and Cable Modems are supported.
- **Supports multiple Connection Methods.** The Internet (WAN port) connection supports PPPoE (PPP over Ethernet), PPTP (Peer-to-Peer Tunneling Protocol), as well as "Direct Connection" type services.
- **Fixed or Dynamic IP Address.** On the Internet (WAN port) connection, the WL-122 supports both Dynamic IP Address (IP Address is allocated on connection) and Fixed IP Address.

### Advanced Internet Functions

- **Virtual Servers.** This feature allows Internet users to access Internet servers on your LAN. The required setup is quick and easy.
- **DMZ.** One (1) PC on your local LAN can be configured to allow unrestricted 2-way communication with Servers or individual users on the Internet. This provides the ability to run programs which are incompatible with Firewalls.
- **Internet Access Log.** See which Internet connections have been made.
- **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

- **Standards Compliant.** The WL-122 complies with the IEEE802.11g (DSSS) specifications for Wireless LANs.
- **Supports both 802.11b and 802.11g Wireless Stations.** The 802.11g standard provides for backward compatibility with the 802.11b standard, so both 802.11b and 802.11g Wireless stations can be used simultaneously.
- **Speeds to 100Mbps.** All speeds up to the 802.11g maximum of 54Mbps are supported. When using a G+ client adapter up to 100Mbps.
- **WEP support.** Support for WEP (Wired Equivalent Privacy) is included. Key sizes of 64 Bit and 128 Bit are supported.
- **WPA support** Support for WPA (Wi-Fi Protected Access) is included. Including key rotating function.
- **802.1x**
- **Wireless MAC Access Control.** The Wireless Access Control feature can check the the MAC address (hardware address) of Wireless stations to ensure that only trusted Wireless Stations can access your LAN.
- **Simple Configuration.** If the default settings are unsuitable, they can be changed quickly and easily.

## LAN Features

- **4-Port Switching Hub.** The WL-122 incorporates a 4-port 10/100BaseT switching hub, making it easy to create or extend your LAN.
- **DHCP Server Support.** Dynamic Host Configuration Protocol provides a dynamic IP address to PCs and other devices upon request. The WL-122 can act as a **DHCP Server** for devices on your local LAN and WLAN.

## Configuration & Management

- **Easy Setup.** Use your WEB browser from anywhere on the LAN for configuration.
- **Configuration File Upload/Download.** Save (download) the configuration data from the WL-122 to your PC, and restore (upload) a previously-saved configuration file to the WL-122.
- **Remote Management.** The WL-122 can be managed from any PC on your LAN. And, if the Internet connection exists, it can also (optionally) be configured via the Internet.
- **UPnP Support.** UPnP (Universal Plug and Play) allows automatic discovery and configuration of the WL-122. UPnP is by supported by Windows ME, XP, or later.

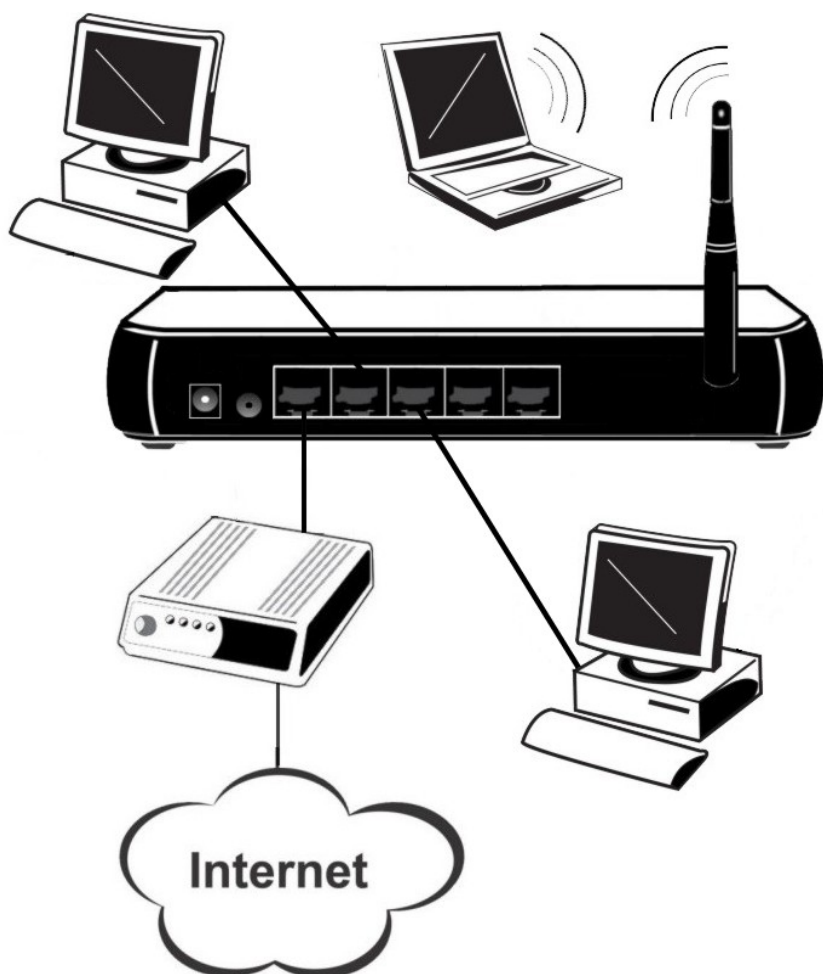
## Security Features

- **Password - protected Configuration.** Optional password protection is provided to prevent unauthorized users from modifying the configuration data and settings.
- **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 WL-122.

## *Setting up the Router*

### **Physical installation**

1. For the installation of the wireless router it is assumed that you have at least one PC with a working broadband Internet connection. It is also assumed that the modem is configured in accordance with the requirements of your ISP and of the modem manufacturer. If not, consult your ISP support literature.
2. Before you begin, ensure that the power lead is not connected to either the wireless router or the cable modem/DSL modem. Leave your cable modem/DSL modem plugged in (telephone line or cable input).



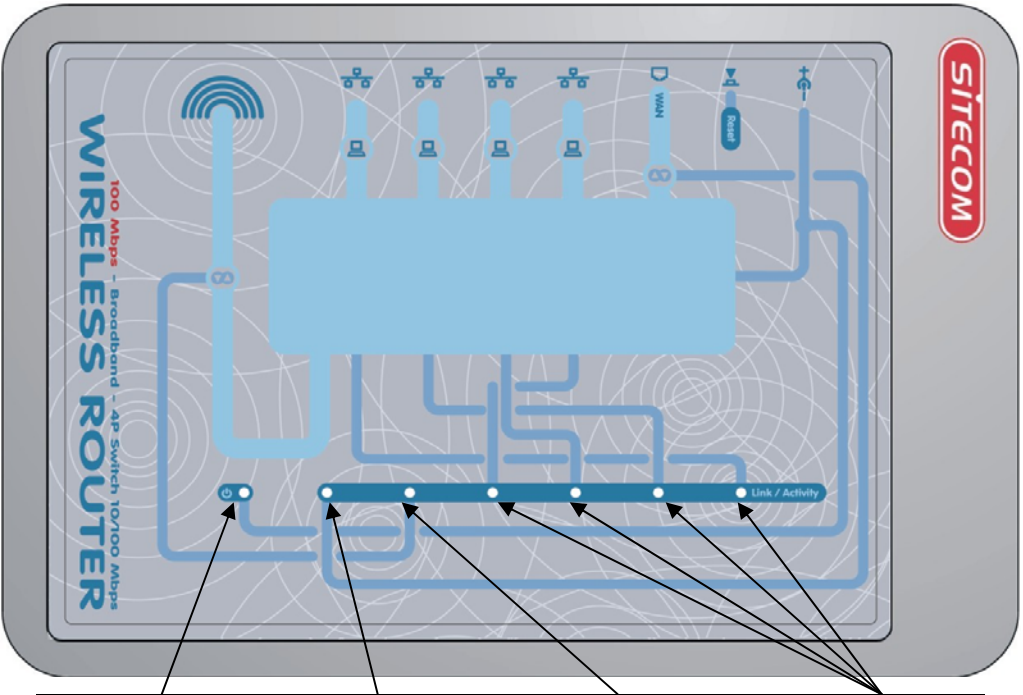
Installation WL-122

3. Connect the LAN cables: For the WL-122, use standard LAN cables to connect the PCs to the LAN ports (switch) on the wireless router. If necessary connect the "Uplink" port to a standard port on another hub. You must use a standard LAN cable for this.

**Note:** If you use the "Uplink" port, then port 4 CANNOT be used.

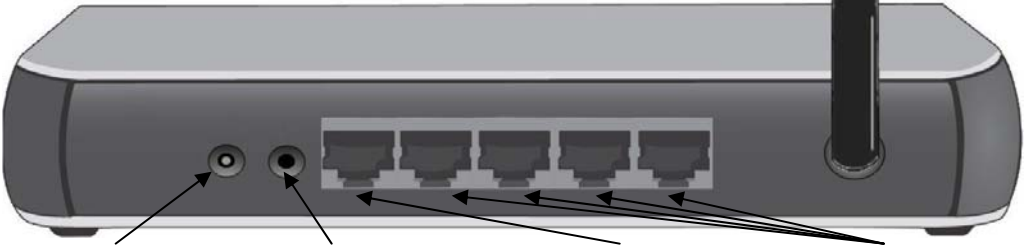
4. Connect your cable modem/DSL modem to the WAN-port on the wireless router. Use the cable supplied with your cable modem/DSL modem. If no cable was supplied with your modem, use a standard network cable.
5. Your wireless PC's need some configuration which is explained later on in this manual.
6. Switch on the cable modem/DSL modem.
7. Connect the power supply adapter to the wireless router. Use only the adapter supplied with the router.
8. Check the LEDs
  - The *Power* LED should be ON.
  - The *Status* LED should flash, then turn Off. If it stays on, there is a hardware error.
  - For each LAN (PC) connection, the LAN *Link/Act* LED should be ON (provided the PC is also ON.)
  - The *WAN* LED should be ON.
  - The *WLAN* LED should be ON
  - The *USB* LED should be ON.

Top LEDs



Power	WAN Status (Red)	WLAN LED (Link/Activity)	LAN
<b>On</b> - Power on. <b>Off</b> - No Power.	<b>On</b> - Connection to the modem attached to the WAN (Internet) port is established. <b>Flashing</b> - Data is being transmitted or received via the WAN port. For each port, there are 2 LEDs	<b>On</b> - Wireless connection is available, but Idle (no traffic). <b>Off</b> - Error - No Wireless connection available. <b>Flashing</b> - Data is being transmitted or received via the Wireless access point. This includes "network traffic" as well as user data.	<u><b>Link/Act</b></u> <b>On</b> - Corresponding LAN (hub) port is active. <b>Off</b> - No active connection on the corresponding LAN (hub) port. <b>Flashing</b> - Data is being transmitted or received via the corresponding LAN (hub) port.

Rear Panel



Power port	Reset Button	WAN port (10/100BaseT)	10/100BaseT LAN connections
Connect the supplied power adapter here.	<p>To Clear All Data and restore the factory default values:</p> <p>Hold the Reset Button down for more as 10 seconds.</p> <p>Release the button</p> <p>After every LED has flashed more than one time the Access Point is active again.</p> <p>It may take up to a minute to reconnect to the clients</p>	Connect the DSL or Cable Modem here. If your modem came with a cable, use the supplied cable. Otherwise, use a standard LAN cable.	<p>Use standard LAN cables (RJ45 connectors) to connect your PCs to these ports.</p> <p><b>Note:</b></p> <p>Any LAN port on the WL-122 will automatically function as an "Uplink" port when required. Just connect any port to a normal port on the other hub, using a standard LAN cable.</p>



# PC Setup

## Set up TCP/IP

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

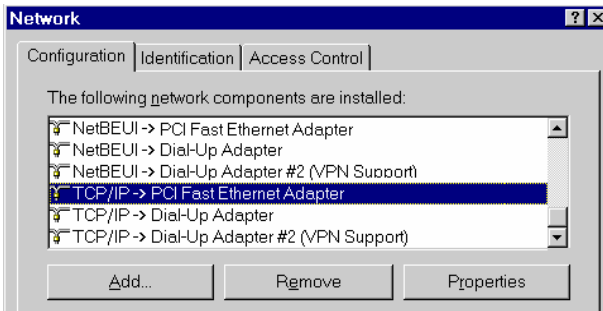
- The *Gateway* must be set to the IP address of the WL-122
- The *DNS* should be set to the address provided by your ISP.

## Using DHCP

To use DHCP, select the radio button *Obtain an IP Address automatically*. This is the default Windows setting. **Using this is recommended.** By default, the WL-122 will act as a DHCP Server.

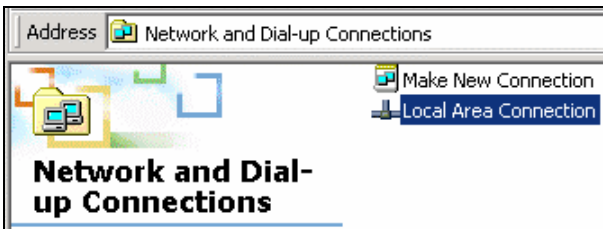
## Windows 98/ME

Right click the *Network Neighbourhood* icon on the desktop and click *Properties*. The following window will be displayed:

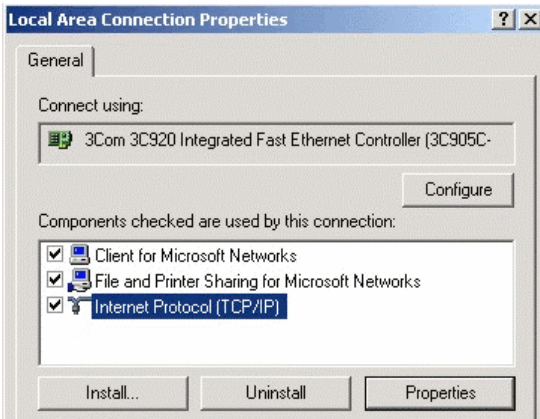


## Windows 2000/XP

Right click the *My Network Places* icon on the desktop and click *Properties*. The following window will be displayed:



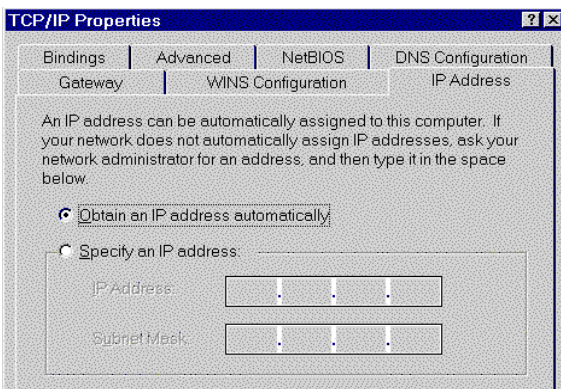
Right click the *Local Area Connection* of the correct network card, and then choose *Properties*.



If the list that appears on screen does not include a line, such as the one that has been selected above ("TCP/IP -> network card"), then follow the steps indicated below for adding this line:

- Click on the button "Add"
- Double-click on "Protocol"
- Select "Microsoft" and thereafter "TCP/IP"
- Click on "OK"
- Wait a few seconds, so that TCP/IP can be added. Thereafter, click on "OK" to leave the network properties screen. Restart your PC.

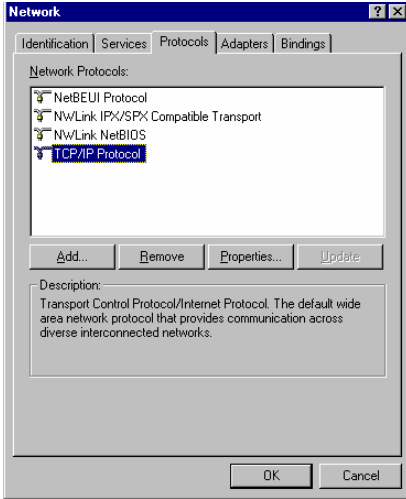
Select the line "TCP/IP -> Network card" as shown above. Click on the button *Properties* to obtain a window similar to the following:



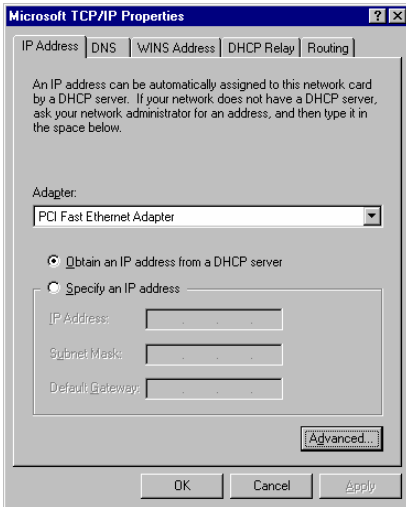
Check whether the setting "**Obtain an IP address automatically**" has been selected, as is illustrated above. The DHCP server in the broadband router will now assign an IP address to the PC.

## Windows NT

Select *Control Panel - Network*, and, on the *Protocols* tab, select the TCP/IP protocol, as shown below.



Click the *Properties* button to see a screen like the one below.



Select the network card for your LAN.

Select the appropriate radio button - *Obtain an IP address from a DHCP Server*

**Restart your PC**, even if you have not made any changes.

## Macintosh Clients

From your Macintosh, you can access the Internet via the WL-122. The procedure is as follows.

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

### Note:

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

- Set the *Router Address* field to the WL-122's IP Address.
- Ensure your DNS settings are correct.

## Linux Clients

To access the Internet via the WL-122, it is only necessary to set the WL-122 as the "Gateway".

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

### Fixed IP Address

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

- Set your "Default Gateway" to the IP Address of the WL-122.
- Ensure your DNS (Name server) settings are correct.

### To act as a DHCP Client (recommended)

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

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

## Wireless Adapter

If your network adapter is a wireless adapter, besides above TCP/IP settings you also have to set the ESSID to 'Sitecom' and the mode to 'Infrastructure' in order to make a connection with the Wireless Broadband Router

## Internet access

### Windows 98/ME/2000

- In the Taskbar, click on the Start button and select Settings - Control Panel - Internet options.
- Select the tab page *Connections* and click on the button *Settings*.
- Select "I want to configure my Internet connection manually" or "I want to make a connection via a LAN network" and click on "Next >".
- Select "I want to connect via a LAN network" and click on "Next >".
- Check carefully that all of the checkboxes in the screen *Internet configuration for a LAN* have **not been checked**.
- Continue with the steps in the wizard, until the task is completed.
- The configuration is now completed.

### Windows XP

- In the Taskbar, click on the Start button and select - Settings – Control Panel - Internet options.
- Select the tab *Connections* and click the *Setup...* button.
- When the New Connection Wizard starts, click on *Next*.
- Select *Connect to internet* and click on *Next*.
- Select *Set up my connection manually* and click on *Next*.
- Select *Connect using a broadband connection that is always on* and click on *Next*.
- Click on *Finish* to close the Wizard.
- In the Taskbar, click on the Start button and select - Settings – Control Panel - Internet options.
- Select the *Connections* tab and click on the *LAN Settings* button.
- Check carefully that **none** of the boxes in the *Local Area Network (LAN) Settings* window are checked.
- The configuration is now completed.

### Accessing AOL

To access AOL (America On Line) through the WL-122, the *AOL for Windows* software must be configured to use TCP/IP network access, rather than a dial-up connection. The configuration process is as follows:

- Start the *AOL for Windows* communication software. Ensure that it is Version 2.5, 3.0 or later. This procedure will not work with earlier versions.
- Click the *Setup* button.
- Select *Create Location*, and change the location name from "New Locality" to "WL-122".
- Click *Edit Location*. Select *TCP/IP* for the *Network* field. (Leave the *Phone Number* blank.)
- Click *Save*, then *OK*. Configuration is now complete.
- Before clicking "Sign On", always ensure that you are using the "WL-122" location.

# Router configuration

1. Make **TCP/IP** settings on your PC, as described in the foregoing section.

**Do not forget to restart your PC after you have finished.**

2. Start your web browser. In the *Address* field, enter the following:  
**192.168.1.254.**

## If you can't connect

If the WL-122 does not respond, check the following:

- The WL-122 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 no response is received, either the connection is not working, or your PC's IP address is not compatible with the WL-122's IP Address. (See next item.)
- If your PC is using a fixed IP Address, its IP Address must be within the range 192.168.1.1 to 192.168.1.253 to be compatible with the WL-122's default IP Address of 192.168.1.254. Also, the *Network Mask* must be set to 255.255.255.0. See *Chapter 4 - PC Configuration* for details on checking your PC's TCP/IP settings.
- Ensure that your PC and the WL-122 are on the same network segment. (If you don't have a router, this must be the case.)

3. Type in the password and click on 'OK'. The default password is '**sitecom**'. After logging in the first time change the password to ensure a secure connection to the Sitecom Wireless Router 100G+. Check the manual on the CD-ROM for more information about changing the password.



4. The start up screen of the WL-122 Wireless Router will now be displayed. Click on 'Wizard' in the menu on the left.

Address <http://192.168.1.254/main.shtml>

**SITECOM**  
Wireless router 100G+ WL-122

**Status**

**System Info**

Firmware Version:	N/A
Web Fileset Version:	N/A

**AccessPoint properties**

SSID of AP:	Sitecom
-------------	---------

**Wide Area Network (WAN):**

Connection type:	Dynamic IP
IP Address:	

**Local Area Network (LAN):**

IP Address:	192.168.1.254
DHCP Server:	Enabled
Firewall:	Enabled

5. The 'Set up wizard' will now be displayed; check that the modem is connected and click on 'Next'.



6. Select your country from the **Country** list. If your Country isn't listed, please see the next Chapter "**Your Country/ISP is not listed**"

**Setup Wizard - Internet Access**

Select your country and ISP.

What type of Internet access do you have ?

Country: Other

Service: Other

< Back Next > Cancel

**Setup Wizard - Internet Access**

Select your country and ISP.

What type of Internet access do you have ?

Country: UK

Service: Netherlands, Germany, France, Italy, UK, Other

< Back Next > Cancel

7. From **Service**, select your internet provider. Click **Next**.



**Setup Wizard - Internet Access**

Select your country and ISP.

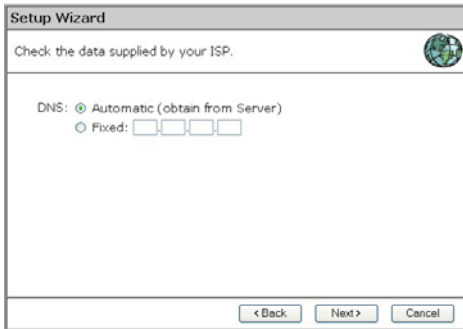
What type of Internet access do you have ?

Country:

Service:

< Back   Next >   Cancel

8. Depending on the chosen provider, you may need to enter your user name and password and MAC address or hostname in the following window. Then click on **Next**.



**Setup Wizard**

Check the data supplied by your ISP.

DNS: ☒ Automatic (obtain from Server)  
☐ Fixed:

< Back   Next >   Cancel

9. Click **finish** to complete the configuration.



**Setup Wizard**

Data input completed.

Click "Finish" to save all data to the Internet Gateway.

< Back   Finish   Cancel

The configuration is now completed.



## Your country/ISP is not listed

Select the type of your Internet connection, and then click on **Next**.



Fill in the **Hostname** and the **Domain name**, if you received this from your Internet service provider.

For some providers it will be necessary to fill in the **MAC address** of the network card the Modem was attached to originally.

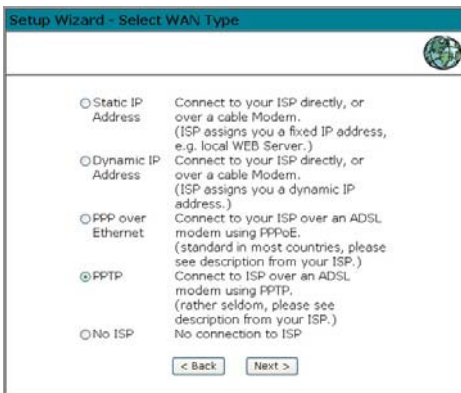
If you received an *username and password* from your ISP, then choose **PPPoE**

If you received an *Server address* from your provider besides an *username and password*, then choose **PPTP**

*(Currently L2TP is only used by a Dutch provider and not supported)*

If you didn't receive a username and password, then choose **Dynamic IP Address**

If you didn't receive a username and password but received a fixed IP address, then choose **Static IP Address**



## - PPPoE

Fill in your **Username** and your **password**.

If needed, clone the MAC address of the original Ethernet adapter the modem was connected with in the original situation.

Fill in an optional Service name

If your provider has assigned you a fixed IP address, you input this in the field **IP Address**

**Setup Wizard - Internet Access**

WAN Type: **PPP Over Ethernet**

MAC Address: 00:00:00:00:00:00

Username:

Password:

Service name:

IP Address: 0.0.0.0

PPPoE Connection Type: Auto-connection ▼

PPPoE Timeout: 300

PPPoE Status:

Please wait 5 seconds until proceeding any action.

< Back   Cancel   Next>

If you select **Auto-connection** the router will keep the connection with your ISP open at all time.

When **Dial-up on Demand** is selected, you can manually connect or disconnect via the status screen

Auto-connection ▼

Auto-connection

Dial-up on Demand

**Status**

Status

Item	Status
<b>System Info</b>	
Firmware Version:	WL-111v2_FW_1_0_11
Web Fileset Version:	SIT_WEB_1.0.9
<b>AccessPoint properties</b>	
SSID of AP:	Sitecom
<b>Wide Area Network (WAN):</b>	
Connection type:	PPPoE
PPPOE Status:	
Change PPPOE Status:	<input type="button" value="Connect PPPOE Session"/>
IP Address:	


### Status

Status

Item	Status
<b>System Info</b>	
Firmware Version:	WL-111v2_FW_1_0_11
Web Fileset Version:	SIT_WEB_1.0.9
<b>AccessPoint properties</b>	
SSID of AP:	Sitecom
<b>Wide Area Network (WAN):</b>	
Connection type:	PPPoE
PPPOE Status:	
Change PPPOE Status:	<div>Disconnect PPPOE Session</div>
IP Address:	

Click **Return** to complete the configuration.

### Setup Wizard - Internet Access



Configuration is Completed. Click Return.

Return

The configuration is now completed.

**- PPTP**

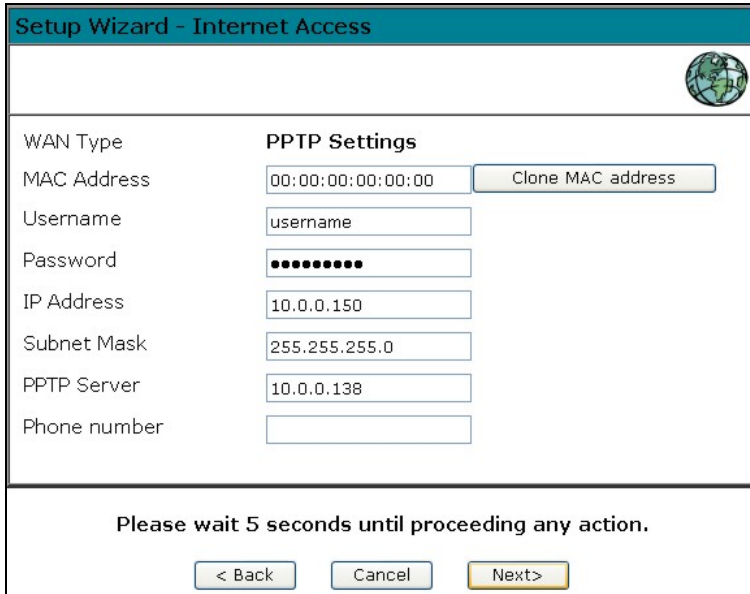
If needed, clone the MAC address of the original Ethernet adapter the modem was connected with in the original situation.

Fill in your **Username** and your **password**.

Fill in the **IP address**, **Subnetmask** and **PPTP server** as provided by your ISP.

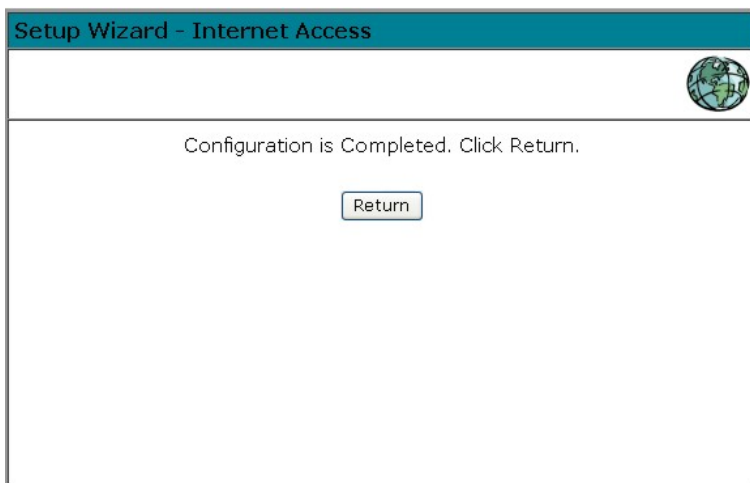
Fill in the optional **phone number** from your ISP.

Click **Next**



The screenshot shows the 'Setup Wizard - Internet Access' window. It has a title bar with a globe icon. The main area is divided into two sections: 'WAN Type' and 'PPTP Settings'. Under 'PPTP Settings', there are several input fields: 'MAC Address' (with a 'Clone MAC address' button), 'Username' (containing 'username'), 'Password' (masked with dots), 'IP Address' (containing '10.0.0.150'), 'Subnet Mask' (containing '255.255.255.0'), 'PPTP Server' (containing '10.0.0.138'), and 'Phone number' (empty). At the bottom, there is a message 'Please wait 5 seconds until proceeding any action.' and three buttons: '< Back', 'Cancel', and 'Next>'.

Click **Return** to complete the configuration.



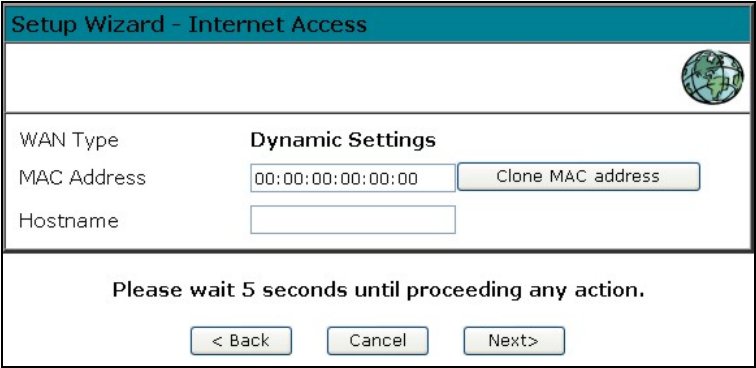
The screenshot shows the 'Setup Wizard - Internet Access' window. It has a title bar with a globe icon. The main area contains the text 'Configuration is Completed. Click Return.' and a single button labeled 'Return'.

The configuration is now completed.

**- Dynamic**

If needed, clone the MAC address of the original Ethernet adapter the modem was connected with in the original situation.

Fill in an optional Hostname, click **Next**



Setup Wizard - Internet Access

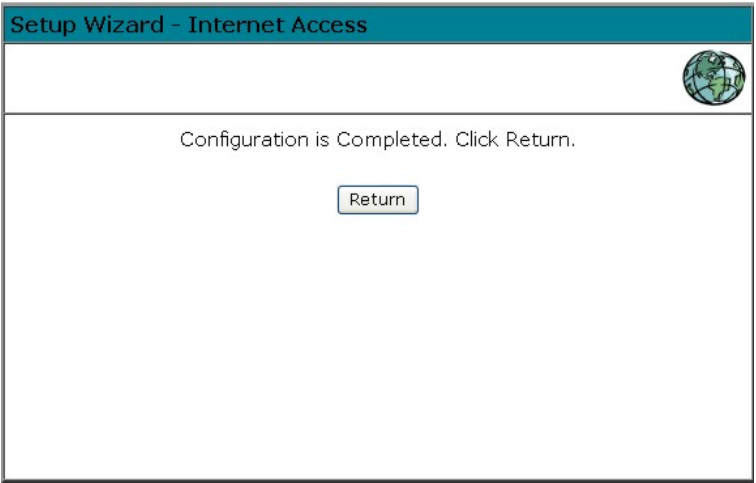
WAN Type: Dynamic Settings

MAC Address: 00:00:00:00:00:00

Hostname:

Please wait 5 seconds until proceeding any action.

Click **Return** to complete the configuration.



Setup Wizard - Internet Access

Configuration is Completed. Click Return.

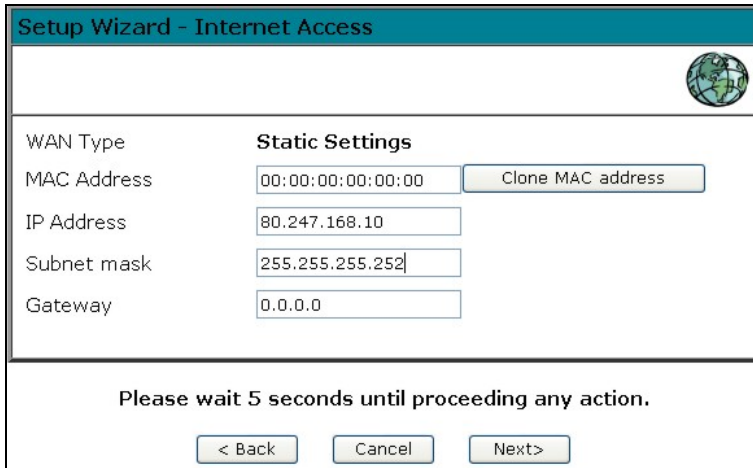
The configuration is now completed.

## - Static

If needed, clone the **MAC address** of the original Ethernet adapter the modem was connected with in the original situation.

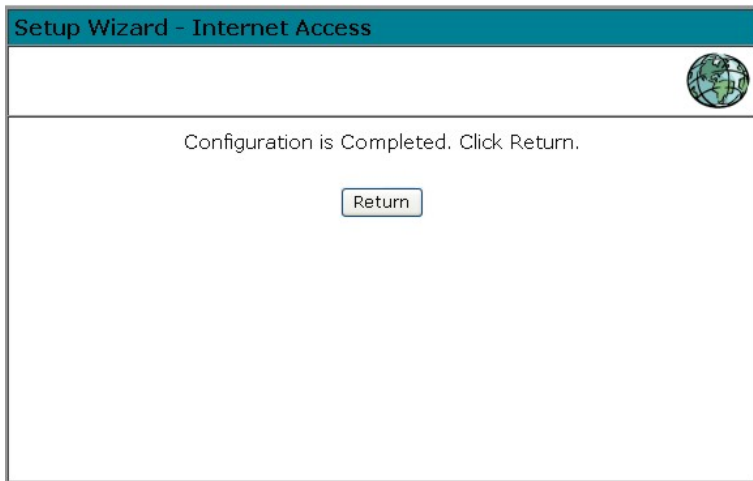
Fill in the **IP address**, **Subnetmask** and **Gateway** as provided by the ISP

Click **Next**



The screenshot shows a web-based configuration window titled "Setup Wizard - Internet Access". It features a globe icon in the top right corner. The main content area is divided into two sections: "WAN Type" and "Static Settings". Under "Static Settings", there are input fields for "MAC Address" (00:00:00:00:00:00), "IP Address" (80.247.168.10), "Subnet mask" (255.255.255.252), and "Gateway" (0.0.0.0). A "Clone MAC address" button is located next to the MAC Address field. At the bottom of the window, there is a message: "Please wait 5 seconds until proceeding any action." and three buttons: "< Back", "Cancel", and "Next>".

Click **Return** to complete the configuration.






The screenshot shows the same "Setup Wizard - Internet Access" window, but now it displays a completion message: "Configuration is Completed. Click Return." with a "Return" button centered below the message. The globe icon remains in the top right corner.

The configuration is now completed.

## Home Screen

After finishing the Setup Wizard, you will see the *Home* screen. When you connect in future, you will see this screen when you connect. An example screen is shown below.

Address  http://192.168.1.254/main.shtml

  
**Wireless router 100G+  
WL-122**  
  
**Setup**  
> Primary  
> Advanced  
> Tool  
**Status**  
**Wizard**  
**Logout**

### Status

Status

Item	Status
<b>System Info</b>	
Firmware Version:	N/A
Web Fileset Version:	N/A
<b>AccessPoint properties</b>	
SSID of AP:	Sitecom
<b>Wide Area Network (WAN):</b>	
Connection type:	Dynamic IP
IP Address:	
<b>Local Area Network (LAN):</b>	
IP Address:	192.168.1.254
DHCP Server:	Enabled
Firewall:	Enabled

## 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.



**On each screen, clicking the "Help" button will display help for that screen.**

**From any help screen, you can access the list of all help files (help index).**

## Setup Screen

### LAN IP

Click the *LAN IP* tab In the Primary Setup menu to reach the **LAN** screen  
An example screen is shown below.

Primary Setup

LAN IP

WAN Type

DHCP Server

WLAN

WLAN Security

WDS

Item	Setting
LAN IP Address Type	<input type="radio"/> Dynamic <input checked="" type="radio"/> Static
LAN IP Address	<input type="text" value="192.168.1.254"/>
Subnet Mask	<input type="text" value="255.255.255.0"/>
Gateway	<input type="text" value="0.0.0.0"/>

Save

Undo

ATTENTION: Do not change the IP address of the AccessPoint unless you have adapted the settings in the DHCP Server. Otherwise all Clients retrieving its IP address from the AP will loose connection and will not get reconnected. Changing the IP address will cause a disconnection from the AP after pressing Save.

### Data - LAN IP

TCP/IP	
LAN IP Address Type	If you plan to use any external DHCP server, select <b>Dynamic</b> . Otherwise set the LAN address to <b>Static</b> . Under the <b>Static IP</b> , you have the option to turn on the internal DHCP server. First enter the setting on the DHCP server page and enable the default DHCP server. Once DHCP is enabled, you have to make sure the IP address at the <b>Static IP</b> settings is in the range of the DHCP server in which the default DHCP server is usually enabled.
LAN IP address	IP address for the WL-122, 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. If Enabled, the WL-122 will allocate IP Addresses to PCs (DHCP clients) on your LAN when they start up. The default (and recommended) value is Enabled.
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 WL-122 is attached (the same value as the PCs on that LAN segment).
Buttons	
Save	Save the data on screen.
Cancel	The "Cancel" button will discard any data you have entered and reload the file from the WL-122.



Wan Type

Primary Setup

LAN IP

WAN Type

DHCP Server

WLAN

WLAN Security

WDS

Item	Setting
WAN Type	Dynamic Settings <div>Change...</div>
MAC Address	<div>00:60:B3:00:E5:19</div> <div>Clone MAC address</div>
Hostname	<div></div>

Save

Undo

In the **WAN Type** screen you can make the same settings as in the [Setup Wizard](#)

Primary Setup

LAN IP

WAN Type

DHCP Server

WLAN

WLAN Security

WDS

Choose WAN Type

Type	Usage
<input type="radio"/> Static IP Address	Connect to your ISP directly, or over a cable Modem. (ISP assigns you a fixed IP address, e.g. local WEB Server.)
<input checked="" type="radio"/> Dynamic IP Address	Connect to your ISP directly, or over a cable Modem. (ISP assigns you a dynamic IP address.)
<input type="radio"/> PPP over Ethernet	Connect to your ISP over a ADSL modem using PPPoE. (standard in most countries, please see description from your ISP.)
<input type="radio"/> PPTP	Connect to ISP over a ADSL modem using PPTP. (rather seldom, please see description from your ISP.)
<input type="radio"/> No ISP	No connection to ISP

Save

Cancel

## DHCP Server

**Primary Setup**

LAN IPWAN Type**DHCP Server**WLANWLAN SecurityWDS

Item	Setting
DHCP Server	Enabled
IP Pool Starting Address	192.168.1.100
IP Pool Ending Address	192.168.1.200
Netmask	255.255.255.0
Gateway	192.168.1.254 (Optional)
Lease Time (minutes)	300

SaveUndoClients List...Fixed Mapping...DNS Setting...

### What DHCP Does

A 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 WL-122 can act as a **DHCP server**.
- Windows 95/98/ME and 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.)

### Data - LAN IP

TCP/IP	
<b>DHCP Server</b>	Enable or Disable the WL-122's <i>DHCP Server</i> function.
<b>IP Pool starting ending Address</b>	Set the range of IP Addresses allocated to PCs by the DHCP Server function.
<b>Subnet Mask</b>	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 WL-122 is attached (the same value as the PCs on that LAN segment).
<b>Lease Time</b>	Lease time is the time value for clients to retain the assigned IP address. DHCP automatically renews IP addresses without client notification. The default value is 300 minutes.
Buttons	
<b>Save</b>	Save the data on screen.
<b>Undo</b>	The "Undo" button will discard any data you have entered and reload the file from the WL-122.
<b>Clients List</b>	Shows a screen with information about connected DHCP clients

<b>Fixed mapping</b>	When the DHCP server is turned of, you can reserve IP address for specific clients, based on MAC address
<b>DNS setting</b>	For some purposes, you may specify a static IP address for the DNS server so as to provide to its DHCP clients.

Client List

**Primary Setup**

LAN IPWAN Type**DHCP Server**WLANWLAN SecurityWDS

DHCP Clients List

IP Address	Host Name	MAC Address	Select
192.168.1.100	0	undefined	1 minutes

BackRefresh

Shows a list of connected DHCP clients

Fixed mapping

**Primary Setup**

LAN IPWAN Type**DHCP Server**WLANWLAN SecurityWDS

DHCP reservation

IP Address	MAC Address
- No Reservations configured	

Add...Delete...

Click **ADD** to assign IP addresses to specific clients based on MAC address

Add reservation to DHCP server - Microsoft Internet E...

**Add reservation to DHCP server**

MAC Address08:00:46:64:1D:9B

IP Address to reserve192.168.1.2

OKCancel

DNS Settings

**Primary Setup**

LAN IP | WAN Type | **DHCP Server** | WLAN | WLAN Security | WDS

**DNS Setting**

Priority	IP Address
- No static DNS entries configured	

Add... Delete...

Click **ADD** to configure a DNS server

Add static DNS address to the DHCP server - Microsoft Internet Explorer

**Add static DNS address to the DHCP server**

IP Address of DNS server: 195.121.1.34

OK Cancel

Click **OK** to add the DNS server address

**Primary Setup**

LAN IP | WAN Type | **DHCP Server** | WLAN | WLAN Security | WDS

**DNS Setting**

Priority	IP Address
Primary DNS	195.121.1.34

Add... Delete...



**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 WL-122's, the following procedure is required.

1. Disable the DHCP Server feature in the WL-122. This setting is on the LAN screen.
2. Configure the DHCP Server to provide the WL-122's IP Address as the *Default Gateway*.

WLAN screen

**Primary Setup**

LAN IP | WAN Type | DHCP Server | **WLAN** | WLAN Security | WDS

Item	Setting
Country / Region	Netherlands
Wireless network name (SSID)	Sitecom
Band	2.4 GHz (Mixed) B/G Mixed Mode
Radio Channel	6
Turbo Mode	<input checked="" type="checkbox"/>

Save | Undo

Select the correct country.

Country / Region

Wireless network name (SSID)

Band

Radio Channel

Turbo Mode

Netherlands  
Italy  
Liechtenstein  
Luxembourg  
Netherlands  
Norway  
Portugal  
Spain  
Sweden  
Switzerland  
United Kingdom

A warning message will appear. Click 'OK' to agree.



**Data - Wireless Screen**

<b>Identification</b>	
<b>Country / Region</b>	It is illegal to use this device in any location outside of the regulatory domain.
<b>SSID (ESSID)</b>	The SSID is an unique ID used by Access Point and stations to identify a wireless LAN. Make sure all wireless stations and Access Points have the same SSID. The SSID can be set up to 32 characters and is case sensitive.
<b>Options</b>	
<b>Band</b>	<p>Select the desired option.</p> <ul style="list-style-type: none"> <li>• g &amp; b - This is the default, and should normally be used.</li> <li>• g only - If selected, this ensures that "g" mode stations will connect at high speed, but "b" mode stations will be unable to connect at all.</li> <li>• b only - If selected, "g" mode is unavailable. "g" mode stations will only be able to connect if they are fully backward-compatible with "b" mode.</li> </ul>
<b>Radio Channel</b>	<ul style="list-style-type: none"> <li>• Select the Channel you wish to use on your Wireless LAN.</li> <li>• If you experience interference (shown by lost connections and/or slow data transfers) you may need to experiment with different channels to see which is the best.</li> <li>• if using multiple Access Points, adjacent Access Points should use different Channels to reduce interference.</li> </ul>
<b>Turbo Mode</b>	<ul style="list-style-type: none"> <li>• Check 'Turbo Mode' to activate the 100Mbps mode.</li> </ul>
<b>Buttons</b>	
<b>Save</b>	Save the data on screen.
<b>Undo</b>	The "Undo" button will discard any data you have entered since the last "Save" operation.

## WLAN Security

### Primary Setup

LAN IPWAN TypeDHCP ServerWLANWLAN SecurityWDS

Item	Status
<a href="#">Wired Equivalent Privacy (WEP)</a> Base security level to protect your WLAN.	disabled
<a href="#">Wi-Fi Protected Access (WPA)</a> Advanced security level with key rotating function.	disabled
802.1X Security Configure 802.1X protocol. <a href="#">Requires a radius server</a>	disabled
<a href="#">Radius Servers</a> Set-up connection to a Radius Server for authentication.	disabled
<a href="#">Access Control List (ACL)</a> Grant or deny access to individual clients.	disabled

## WEP

### Primary Setup

LAN IPWAN TypeDHCP ServerWLANWLAN SecurityWDS

#### WEP Settings

Item
Use WEP security <input checked="" type="radio"/> Enable <input type="radio"/> Disable
Encryption Strength <span>128 bits</span>
Security Encryption (WEP) Key Passphrase: <input type="text"/> <span>Generate Keys</span>
Key 1: <input checked="" type="radio"/> SitecomEurope
Key 2: <input type="radio"/> *****
Key 3: <input type="radio"/> *****
Key 4: <input type="radio"/> *****
<span>Save</span> <span>Undo</span> <span>Back</span>

WEP Data Encryption	
Use WEP security	<p>Select the option to match other Wireless Stations:</p> <ul style="list-style-type: none"><li><b>Disabled</b> - data is NOT encrypted before being transmitted.</li><li><b>Enable</b> – data is encrypted before being transmitted</li></ul>
Encryption Strenght	<ul style="list-style-type: none"><li><b>64 Bit</b> - 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 5 chars (ASCII) or 10 chars in HEX (0~9 and A~F).</li><li><b>128 Bit</b> - 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 13 chars (ASCII) or 26 chars in HEX (0~9 and A~F).</li></ul>
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.
Keys 1 ~ 4	<ul style="list-style-type: none"><li><b>Key Value</b> - Enter the key value you wish to use. Other stations must have the same key.</li></ul>

## WPA

Primary Setup	
<a href="#">LAN IP</a> <a href="#">WAN Type</a> <a href="#">DHCP Server</a> <a href="#">WLAN</a> <a href="#">WLAN Security</a> <a href="#">WDS</a>	
Wi-Fi Protected Access(WPA)	
Item	Setting
WPA Security Mode:	<div>disabled ▾</div> <div> <b>Pre-Shared Key Mode:</b>            Password Phrase (8-63 characters) <input type="text"/> </div> <div> <b>Enterprise Mode:</b>  <a href="#">» Requires a radius server</a>  <input type="checkbox"/> Update if station leaves BSS            Group Key Rekey settings:  <input checked="" type="radio"/> No rekeying  <input type="radio"/> Rekey every <input type="text" value="60"/> minutes  <input type="radio"/> Rekey every <input type="text" value="10"/> x 1000 packets         </div>
<div>Save Undo Back</div>	

Currently one of the highest levels of security a wireless network can achieve. Wi-Fi Protected Access is a subset of the security specification and has been introduced as an interim solution for most known security weaknesses in relation to plain WEP. TKIP, the successor to WEP, includes enhancements that eliminate the known vulnerabilities of WEP. Enterprises that already have RADIUS authentication in place can use WPA with 802.1x (WPA-EAP / Enterprise Mode). Small business and home wireless LAN can use WPA without 802.1x (WPA-PSK / Pre-Shared Key).

disabled ▾

disabled

Pre-Shared Key Mode

Enterprise Mode

### Use WPA with Pre-Shared Key:

Instead of using RADIUS for authentication, systems with WPA-PSK will be configured with a secret password phrase. Enter your password phrase and press "Generate". You can now create a pre-shared key in the Access Point and copy the characters you input to the station's WPA-PSK entry. A shared secret is only secure as long as no third party knows about it.

### Use WPA with Radius Server:

In cooperation with [RADIUS](#), systems with WPA-EAP will be used with a new encryption method called Temporal Key Integrity Protocol (TKIP) implementation with 802.1x dynamic key exchange.

**Note:** A WLAN client with WPA capabilities is needed for working with the AP



## IEEE 802.1x

is a standard for network access control (port based), which was introduced especially for distributing encryption keys in a wireless network. The Access Point supports 802.1x for keeping out unauthorized users and for verifying the credentials of users with RADIUS so that authorized users can access the network and services. Before you set 802.1x, you need to enable at least one [RADIUS](#) server on the RADIUS setting page.

**Primary Setup**

LAN IPWAN TypeDHCP ServerWLAN**WLAN Security**WDS

**802.1X Settings**

Authentication with the 802.1X protocol requires a Radius Server. One mode can be used to authenticate WLAN Clients:

Mixed Mode: 802.1X + Radius Server + WEP Encryption

Using the mixed mode will improve the security by rekeying, based on time or throughput.

Item	Setting
802.1X Authentication Mode	disabled
Key Size	<input type="radio"/> 40-bits <input checked="" type="radio"/> 104-bits
Group Key Rekey Settings	<input checked="" type="radio"/> No rekeying <input type="radio"/> Rekey every <input type="text" value="60"/> minutes <input type="radio"/> Rekey every <input type="text" value="10"/> x 1000 packets

SaveUndoBack

To use 802.1x, you will need at least one common Extensible Authentication Protocol (EAP) method on your authentication server, APs (authenticator) and stations (supplicant). 802.1x is also used to perform generation and distribution of encryption keys from AP to the station as part of or after the authentication process. A further factor here is dynamic WEP, which is based on legacy RC4 WEP encryption and is available in this Access Point under the setting for enabling 802.1x security in association with disabled Wired Equivalent Privacy (WEP) settings. There are two options for the key length, i.e. 40 and 104bits. The longer the key length, the greater security it will offer.

Radius Server

Primary Setup

LAN IP

WAN Type

DHCP Server

WLAN

WLAN Security

WDS

Radius Server Settings

Item	Setting
Reauthentication Time:	<div>3600</div> seconds

Save

Undo

Back

Item	Setting
IP Address:	<div></div>
UDP Port:	<div>1812</div>
Secret:	<div></div>
	<div>Add</div> <div>Cancel</div>

ID	IP Address	Port Number
- No RADIUS Servers configured		
<div>Delete...</div>		

RADIUS performs the authentication function required to check the credentials of users and intermediate Access Points and indicates whether the users are authorized to access the Access Points. Enabling RADIUS is therefore the first step toward building up an 802.1x-capable environment. Even more, it is also a must-do to accommodate the recently introduced Wi-Fi protected access (WPA-EAP) to wireless networks.

Setting up RADIUS information in your Access Point is quite simple; just click Add and input the IP address of the RADIUS server and its port number, which is usually set to 1812, as well as the secret key, which is identified with the given key in RADIUS. Press **Add** to apply the settings.

When you finish adding RADIUS information, return to the Wireless Security Settings page, where you will be allowed to continue configuring 802.1x as the picture shows. You can choose here to have either 802.1x with static WEP or with dynamic WEP and WPA-EAP to ensure even higher security in your wireless network.

## Access Control List

Primary Setup

LAN IP

WAN Type

DHCP Server

WLAN

WLAN Security

WDS

MAC Address Control

Item

Setting

MAC Address Control

☐ enable

☒ ALLOW

All devices in the table will have access to your network.  
Selection of WLAN will allow specific device to connect to wireless network.  
Selection of LAN/WAN will allow specific device to connect to your wired network (Printer / ISP / ...)

☐ DENY

All devices in the table will be filtered out. If no entry is made, the network is fully accessible.

Save

Undo

Item

Property

MAC Address:

00:00:00:00:00:00

Access Policy:

☐ Accept

☒ Reject

Add

ID

MAC Address

Access

Delete...

MAC Address Control	
Mac Address Control	To activate the Access Control function, check "Enable"
Allow	All devices in the MAC address control table will have access to the network.
Deny	All devices in the MAC address control table will be denied access to the network
MAC address	Fill in the MAC address of the client adapter which wants to connect to the network
Access Policy	<ul style="list-style-type: none"><li><b>Accept</b> The client adapter with the specified MAC address is accepted to connect the network</li><li><b>Reject</b> The client adapter with the specified MAC address is rejected to connect the network. This only makes sense if you know that intruders are trying to enter your network in combination with a few known wireless clients</li></ul>

WDS Screen

Primary Setup

LAN IP

WAN Type

DHCP Server

WLAN

WLAN Security

WDS

ID	Enable	Peer address	Name	SSID	Data Rates	Channel	Age	RSSI
- There are no WDS Links using the internal radio								

Save

Undo

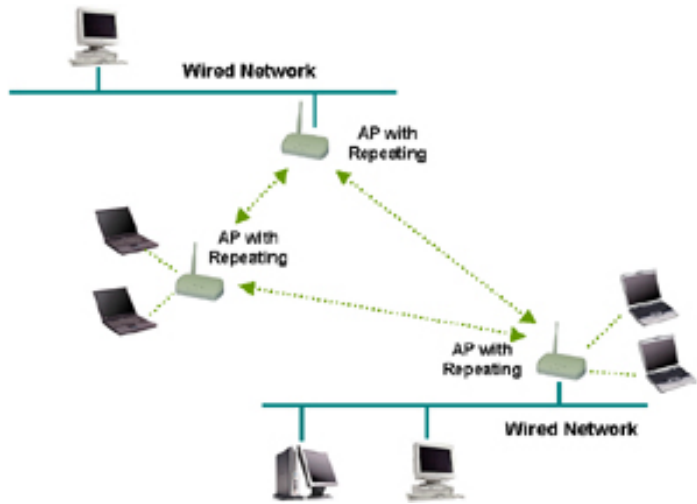
Rescan

Add WDS link manually:

Item	Property
MAC Address:	<div><div>00:00:00:00:00:00</div><div>Add</div></div>

Extend the range of your network without having to use cables to link the Access Points by using the Wireless Distribution System (WDS): Put simply, you can link the Access Points wirelessly. Under WDS, your Access Points are still functioning as a regular Access Point, which can provide the link services to wireless clients.

Enter the MAC address of another AP you wirelessly want to connect to into the MAC Address field or select the Access Point that your Access Point finds. The implementation can be done as below.



## Advanced Screen

### Virtual Server

**Advanced Setting**

**Virtual Server** Firewall

Source port	Protocol	Destination IP	Destination port
- No port forwarding rules available			

Add...

Delete...

This feature, sometimes called "Port Forwarding", 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:

- Your Server does not have a valid external IP Address.
- Attempts to connect to devices on your LAN are blocked by the firewall in this device.

The "Virtual Server" feature solves these problems and allows Internet users to connect to your servers.

Click **ADD** to forward a port

Add Port Forwarding Rule - Microsoft Internet Explorer

**Add Port Forwarding Rule**

Incoming port

80

Protocol

☒ TCP  
☐ UDP

Destination IP

192.168.1.1

Destination port

80

OK

Cancel

Specify the **Incoming port** (for example port 80 for HTTP access, if you run a webserver on your LAN which need to be accessible from the internet)

Specify the **Protocol** which is used (TCP or UDP)

Specify the **Destination IP** (The PC on your network which is running the server)

Specify the **Destination port**

Click **OK**

## Firewall

The firewall is a set of programs located at the gateway, which limits the exposure of a computer or a group of computers to users from other networks. Based on the default policies and the specified rules, network administrators can easily manage the traffic from any network access. The default policies allow you to accept or block all traffic. You can also define rules: these determine what to do with specific types of traffic where rules override the default policies.

### Advanced Setting

Virtual ServerFirewall

Item	Setting
Firewall status:	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
Default policies:	Input <input checked="" type="radio"/> Accept <input type="radio"/> Discard
	Output <input checked="" type="radio"/> Accept <input type="radio"/> Discard
	Forward <input checked="" type="radio"/> Accept <input type="radio"/> Discard

Id	Chain	Target	Source/Destination IP & Subnet	SRC/DST.Port	Count	Enabled
- No firewall rules configured						

Add...Delete...

UndoSave

Default policies concern where the traffic goes to or comes from:

**Input:** All traffic with the Access Point as destination.

**Output:** All traffic with the Access Point as origin.

**Forward:** All traffic between LAN and WAN that passes through the Access Point.

You can either select “**Accept**” to send the packet through or “**Discard**” to stop the traffic concerning how Access Points react.

Once you have set the default policies, you can create rules.

### Add Firewall Rule

Click **Add** to create a rule.

Add Firewall Rule - Microsoft Internet...

### Add Firewall Rule

Select chain type:

☐ input

☒ output

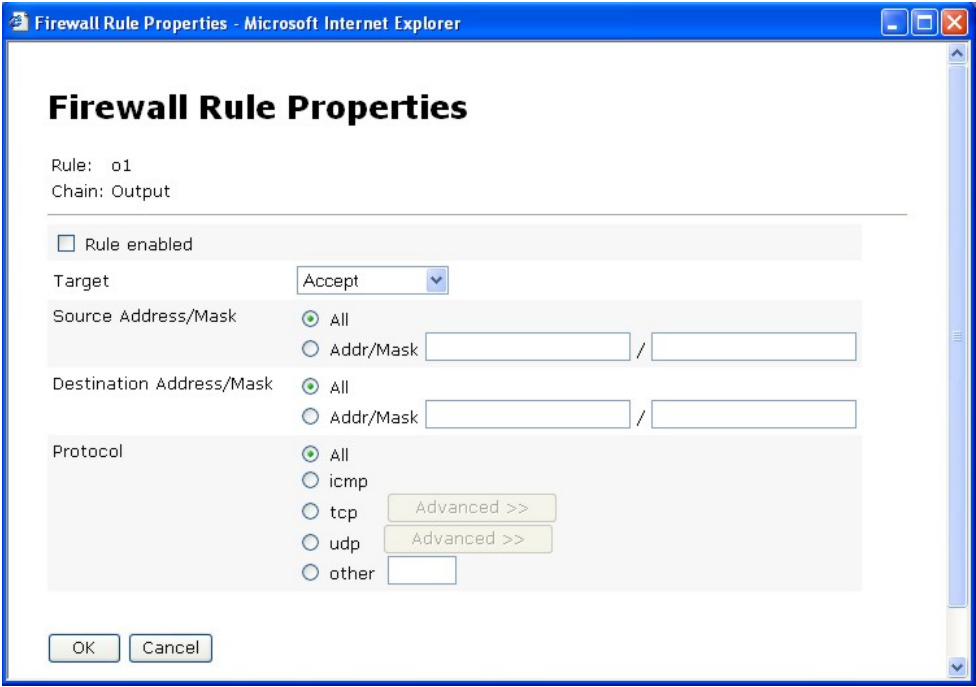
☐ forward

Enter rule number:

name

OKCancel

Select the chain type to determine the direction of traffic that you want to restrict. Also enter a number for the rule. This will be used to identify the rule and the order in which rules are applied.



**Firewall Rule Properties**

Rule: 01  
Chain: Output

☐ Rule enabled

Target: Accept

Source Address/Mask: ☒ All  
☐ Addr/Mask  /

Destination Address/Mask: ☒ All  
☐ Addr/Mask  /

Protocol: ☒ All  
☐ icmp  
☐ tcp Advanced >>  
☐ udp Advanced >>  
☐ other

OK Cancel

**Rule enabled:** While the rule is enabled, there are four ways to present the rule.

**Target:**

**Accept:** The traffic will be allowed.

**Drop:** The traffic will be stopped, with no response to the sender.

**Reject:** The traffic will be stopped and a response will be returned to the sender.

**Continue:** The traffic packet will be counted instead; meanwhile the next rule will be continued.



Accept  
Accept  
Drop  
Reject  
Continue

Now you can enter the conditions for the rule.

**Source Address/Mask:**

Enter the IP addresses for the source. You can enter an address range by giving the network address and the net mask. Select **"All"** to choose all IP addresses as source.

**Destination Address/Mask:**

Enter the IP addresses for the destination. You can enter an address range by giving the network address and the net mask. Select **"All"** to choose **"all IP addresses"** as destination.

**Protocol:**

Select the type of traffic you want to be affected by the rule. If you select **"TCP"** or **"UDP"**, you can click **"Advanced"** to select a specific port number or port number range. To set a port range, enter the first and last port number in the range in the edit boxes. For TCP traffic, you can also select specific flags. Use this to block only incoming TCP traffic (such as Telnet), but allow outgoing (from LAN to WAN) traffic. To do this, tick the matched TCP flags checkbox, and set these flags: SYN to Yes, ACK to NO, RST to NO.

Protocol	<input type="radio"/> All <input type="radio"/> icmp <input checked="" type="radio"/> tcp <span>Advanced &lt;&lt;</span> <input type="radio"/> udp <span>Advanced &gt;&gt;</span> <input type="radio"/> other <input type="text"/>																				
Source port	<input checked="" type="radio"/> All <input type="radio"/> Single port <input type="text"/> <input type="radio"/> Port range <input type="text"/> / <input type="text"/>																				
Destination port	<input checked="" type="radio"/> All <input type="radio"/> Single port <input type="text"/> <input type="radio"/> Port range <input type="text"/> / <input type="text"/>																				
TCP flags	<table> <tr> <td>SYN</td> <td><input checked="" type="radio"/> Ignore</td> <td><input type="radio"/> Yes</td> <td><input type="radio"/> No</td> </tr> <tr> <td>ACK</td> <td><input checked="" type="radio"/> Ignore</td> <td><input type="radio"/> Yes</td> <td><input type="radio"/> No</td> </tr> <tr> <td>FIN</td> <td><input checked="" type="radio"/> Ignore</td> <td><input type="radio"/> Yes</td> <td><input type="radio"/> No</td> </tr> <tr> <td>RST</td> <td><input checked="" type="radio"/> Ignore</td> <td><input type="radio"/> Yes</td> <td><input type="radio"/> No</td> </tr> <tr> <td>PSH</td> <td><input checked="" type="radio"/> Ignore</td> <td><input type="radio"/> Yes</td> <td><input type="radio"/> No</td> </tr> </table>	SYN	<input checked="" type="radio"/> Ignore	<input type="radio"/> Yes	<input type="radio"/> No	ACK	<input checked="" type="radio"/> Ignore	<input type="radio"/> Yes	<input type="radio"/> No	FIN	<input checked="" type="radio"/> Ignore	<input type="radio"/> Yes	<input type="radio"/> No	RST	<input checked="" type="radio"/> Ignore	<input type="radio"/> Yes	<input type="radio"/> No	PSH	<input checked="" type="radio"/> Ignore	<input type="radio"/> Yes	<input type="radio"/> No
SYN	<input checked="" type="radio"/> Ignore	<input type="radio"/> Yes	<input type="radio"/> No																		
ACK	<input checked="" type="radio"/> Ignore	<input type="radio"/> Yes	<input type="radio"/> No																		
FIN	<input checked="" type="radio"/> Ignore	<input type="radio"/> Yes	<input type="radio"/> No																		
RST	<input checked="" type="radio"/> Ignore	<input type="radio"/> Yes	<input type="radio"/> No																		
PSH	<input checked="" type="radio"/> Ignore	<input type="radio"/> Yes	<input type="radio"/> No																		
<input type="button" value="OK"/> <input type="button" value="Cancel"/>																					



## Toolbox Screen

### Password

**ToolBox**

**Password** Firmware Update

**Change System Password**

New Password  (3-16 characters)

Reconfirm

Change password... Clear

**Miscellaneous Information & Commands**

Lock Access Point

### Change Password:

This option enables you to change the system password. If you forget the password, reset your device to recover the default settings. For security reasons, we strongly recommend you change the system password.

### Lock Access Point:

Enabling this option will deny configuration changes to the accesspoint. You need to have physical access to the Access Point to unlock it.

## Firmware update

**ToolBox**

Password **Firmware Update**

**Firmware Filename**

Browse...

Current firmware version is WL-111v2\_FW\_1\_0\_10BETA The upgrade procedure takes about 20 seconds. Note! Do not power off the unit when it is being upgraded. When the upgrade is done successfully, the unit will be restarted automatically

Upgrade

This option is used for uploading the newest firmware. You may either enter the file name in the entry field or browse the file. Check [www.sitecom.com](http://www.sitecom.com) for information about new firmwares

# Appendix A

## Troubleshooting

### Overview

This chapter covers some common problems that may be encountered while using the WL-122 and some possible solutions to them. If you follow the suggested steps and the WL-122 still does not function properly, contact your dealer for further advice.

### General Problems

**Problem 1:** Can't connect to the WL-122 to configure it.

**Solution 1:** Check the following:

- The WL-122 is properly installed, LAN connections are OK, and it is powered ON.
- Ensure that your PC and the WL-122 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 WL-122's default IP Address of 192.168.1.254. Also, the Network Mask should be set to 255.255.255.0 to match the WL-122. 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 WL-122. Ensure that it is connected and ON. Connect to it and check its settings. (If you can't connect to it, check the LAN and power connections.)
- If the WL-122 is configured correctly, check your Internet connection (DSL/Cable modem etc) to see that it is working correctly.

**Problem 2:** **Some applications do not run properly when using the WL-122.**

**Solution 2:** The WL-122 processes the data passing through it, so it is not transparent.

Use the *firewall rules* feature to allow the use of Internet applications which do not function correctly.

## 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 Wireless Access Point must have the same setting for WEP. The default setting for the WL-122 is disabled, so your wireless station should also have WEP disabled.
- If WEP is enabled on the WL-122, your PC must have WEP enabled, and the key must match.
- If the WL-122's is set to *ACL*, then each of your Wireless stations must have been selected, or access will be blocked.
- To see if radio interference is causing a problem, see if connection is possible when close to the Wireless Access Point.  
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:

- Access Point location.  
Try adjusting the location and orientation of the Access Point.
- 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 ex-

periment 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 Access Point.

## FCC Statement

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.

### Federal Communications Commission (FCC) Statement

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

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

## FCC Radiation Exposure Statement



This Transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

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

## CE Marking Warning

This is a Class B product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.