Wireless USB Adapter 11g CPWUA054, CPWUA054/00, CPWUA054/37

User Manual

Version: 1.0
(December. 2003)

Copyright

Federal Communication Commission Interference Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation.

This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications.

However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

1. Reorient or relocate the receiving antenna.

2. Increase the separation between the equipment and receiver.

3. Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.

4. Consult the dealer or an experienced radio technician for help.

FCC Caution

This equipment complies with FCC radiation exposure limits. However, in order to avoid the possibility of exceeding the FCC exposure limits, this device and its antenna should not be co-located or operating in conjunction with any other antenna or transmitter."

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

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

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

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

R&TTE Compliance Statement

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

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

Safety

This equipment is designed with the utmost care for the safety of those who install and use it. However, special attention must be paid to the dangers of electric shock and static

electricity when working with electrical equipment. All guidelines of this and of the computer manufacture must therefore be allowed at all times to ensure the safe use of the equipment.

EU Countries Intended for Use

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

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

EU Countries Not intended for use

None.

Potential restrictive use

France: Only channels 10,11,12, and 13

Manual Contents

Introduction

The equipment enables high-speed access without wires to network assets. This adapter uses the IEEE 802.11 protocol to enable wireless communications between the host computer and other computers, in the same way that the computer would use an Ethernet adapter.

This manual provides information on installing both the latest Windows driver for your adapter and the Configuration Utility, a Windows application which allows you to configure the adapter and to display the adapter's current configuration and status.

Initial Installation

Note: Do not insert the WLAN Adapter until you are asked to do so, failure of which may result in unsuccessful install of your WLAN device.

Please follow the following steps one by one in order to install the WLAN Adapter successfully.

1. Power on your computer and allow Windows 2000/XP to load fully.

2. Be sure that there is no Wireless LAN Adapter inserted yet.

3. Insert the given Installation CD in the CD-ROM and then click on the **Setup**. At the "Welcome" window, click **Next**.

4. Complete the installation. Click the **Finish.**

5. Click **Yes** to continue the **Digital Signature.**

6. Connect your Wireless LAN USB Adapter to your computer.

7. After the OS reconizes the USB adapter, restart the computer.

Upgrade the Driver

1. Uninstall the Adapter Driver

Note: Please jump to Step 3 if you have not installed any old WLAN driver before

On the Windows desktop, right-click on the **My Computer** icon, move the mouse pointer to **Properties**, and click the left mouse button to display the **System Properties** window. Next click on the **Device Manager** tab (and the **View devices by type** radio button if it is not already selected).

Expand the list of network adapters by clicking on the plus sign to the left of this entry; your display will appear similar to the following:

Click on the entry for the Intersil PHILIPS Wireless LAN 802.11 adapter (the above illustration shows an entry for a PCMCIA card) and click on the **Remove** button beneath the list. The operating system displays a confirmation window warning that you are about to remove this device from your system; click the **OK** button to continue.

Once the operating system removes the device, a dialog box appears asking if you want to restart your computer. Click on the **No** button, close the **System Properties** window, and proceed to the next section to remove the driver for your adapter. Do not physically remove the PHILIPS adapter from your computer.

2. <u>Uninstall the Configuration Utility</u>

Next you must remove the old driver for your Wireless LAN adapter. Start by displaying the Windows control panel and opening the **Add/Remove Programs** window. Then, in the **Install/Uninstall** tab, click on the entry for **802.11g USB Wireless LAN Adapter**.

When you click on the **Add/Remove ...** button, Windows asks you to confirm that you want to completely remove the driver and all its components. Click on the **Yes** button to continue, and after the operation completes, close the confirmation window, the **Add/Remove Programs** window, and the **Control Panel** window. Proceed to the next section to install the new driver.
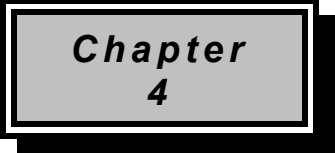
3. <u>Install the New Driver</u>

After uninstalling the PHILIPS adapter and the old driver, run the new SETUP**.exe** file. When the program initial screen appears, click on the **Continue** button. An InstallShield window appears warning you to close any open programs on your computer. Click on the **Next** button to continue. A screen then appears with the software license agreement displayed. Click on the **Yes** button to accept the agreement and continue with the installation. Once the installation is complete, click on the **Finish** button to return to your Windows desktop.

4. <u>Restart the Operating System</u>

After installing the new driver, you must restart the operating system. Click the **Start** button in the taskbar, choose the **Shut Down...** command in the command menu, click the **Restart** radio button in the dialog box, and then click the **OK** button.

Once Windows starts, it displays the **New Hardware Found** wizard, followed immediately by the Configuration menu of the PHILIPS Configuration utility. Examine this information and make any necessary changes (for example, you may need to specify an SSID or encryption keys to reconnect to your network). After you enter the correct information, click the **Apply** button.

Chapter 4

System Tray Icon

The Configuration Utility is installed simultaneously with the driver. The following sections describe operation of the utility.

After the installation of the adapter Configuration Utility, its icon appears in the System Tray in the bottom right corner of your desktop.

The color behind the logo indicates the link status:

Red indicates no or very poor link quality.

Yellow indicates an usable but weak link.

Green indicates a good or excellent link.

A green icon with an "X" over it indicates that you are connected to the LAN but that the driver cannot decrypt received frames.

Entering incorrect WEP keys for encryption causes this; to correct this problem, you must enter the correct keys at the Encryption menu

You can also view the connection status of the link by placing the cursor over the Configuration Utility icon, as shown in the following illustration. This illustration indicates that the 802.11g USB Wireless LAN Adapter is able to communicate, but that the quality of the signal to the radio is only fair.

Chapter 5
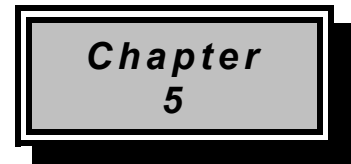
Icon Menu

Clicking on the System Tool Tray Icon displays a menu similar to the following illustration:

The first three items in this menu are present for adapters. The first two items let you turn the wireless radio on or off. When the wireless radio is turned off, the following icon appears in the system tray.

<div style="text-align: right">

Chapter
6

</div>

Configuration Utility

You can launch the Configuration Utility by clicking on the Configuration Utility icon and selecting one of the last four commands in the pop-up menu. If the Configuration Utility icon is not displayed in the System Tray, you can restart the Configuration Utility from the Start Menu by selecting **Programs** and **PHILIPSSTA**

The Configuration Utility consists of a window with a number of tabs. The following sections describe the options displayed by these tabs in detail.

Note: Under Windows XP with the Wireless Zero Configuration service enabled, configuration and encryption are controlled by the operating system. When you start the Configuration Utility with this service enabled, these two tabs do not appear.

<div align="right">

**Chapter
7**

</div>

Settings

7.1 Status Menu

The Status menu displays information on the current status of your connection to the wireless LAN. You can display this menu by choosing the **Wireless Network Status...** command from the pop-up menu, or by clicking on the **Status** tab when the Configuration Utility is displayed on your desktop.

The fields in this menu provide the following information:

- **State:** shows the association state of your computer with the wireless LAN. Possible values for this field are:
- **AdHoc:** The adapter is operating in Peer-to-Peer mode. This field also shows the virtual MAC address used by computers participating in the AdHoc network.
- **Associated:** The adapter is operating in Infrastructure mode. This field also shows the MAC address of the Access Point with which you are communicating.
- **Listening:** Indicates that the adapter is listening on all allowed channels, but has not yet found a peer-to-peer or infrastructure network with which to associate.
- **Stopped:** the Disable Radio Button has stopped the radio.
- **Scanning:** The adapter is scanning for transmissions by other wireless adapters on all channels.
- **Associating:** The adapter is in the process of associating with a network
- **Not Associated:** The adapter has not found any network with which to associate.
- **Hardware Radio Switch OFF:** moving the hardware radio switch to the off position has disabled the radio. Note that not all adapters have a hardware switch.
- **Current Tx Rate:** shows the current transmit rate of the current association.
- **Current Channel:** shows the channel on which the connection is made. In Infrastructure mode, this number changes as the radio scans the available channels.
- **Throughput:** shows the short term transmit and receive throughput in bytes/second, and is continuously updated.
- **Link Quality:** is based on the quality of the received signal of the Access Point beacon.
- **Signal Strength:** is based on the received signal strength measurement of the baseband processor of the Beacon signal.

You can click the **Disable Radio** button to turn off the wireless radio. When you click this button, the **State** field indicates that the radio has been stopped and the remaining fields in this window display either a zero or **Not Applicable**. Click this button again to turn the radio back on. However, if the hardware switch on the adapter has disabled the radio, clicking this button displays a popup message telling you that the radio cannot be enabled.

You can click the **Rescan** button to force the radio to rescan all available channels. If your link quality or signal strength is poor, rescanning can be used to push the radio off a weak Access Point and search for a better link with another Access Point.

7.2 Configuration Menu

The Configuration menu lets you specify the operating parameters for your adapter. You can display this menu by choosing the Advanced Configuration ... command from the pop-up menu, or by clicking on the **Configuration** tab when the Configuration Utility is displayed on your desktop.

Profile Name

A profile is a named set of operating parameters for your PHILIPS WLAN Interface adapter. The **Profile Name:** field lets you set values for all parameters by selecting a previously defined profile. Click the down arrow at the right of this field to display the available profiles for your 802.11g USB Wireless LAN Adapter.

You will always have at least one profile, named **Default**. Initially, this profile contains the parameters configured at installation. You can modify this profile at any time after the installation. After changing parameters, you can save them in the profile named in this field by clicking the **Apply** button in the Configuration Utility panel.

You can also create additional profiles by clicking **Save As** button and typing a name in the **Profile Name:** field. When you change the name in this field and then click the **Apply** button, the Configuration Utility uses the current parameters for your adapter to create a separate profile. You can then switch between profiles by clicking the down arrow at the right of the **Profile Name:** field, selecting a profile from the drop-down list, and clicking the **Apply** button.

The following example describes a situation in which you would want to create multiple profiles. Suppose that you use the wireless LAN at your work, but you also have a network in your home (with a wireless Access Point) for sharing an Internet connection and a printer between several computers. Suppose also that you have another office within your business which also has WLAN capability, but which is configured differently than your main office.

In this situation, you can create a different profile for each of these three environments. Each profile specifies the parameters used on a single network. Moving from one location to another, you need only apply the appropriate profile to be able to participate in the local network.

Network Name

Officially, in wireless networks the network name is known as the SSID (Service Set Identifier), and is used by Access Points and stations to identify a wireless LAN. Your PHILIPS WLAN Interface adapter scans the available channels looking for an Access Point or another station, which has specified this same SSID. It then attempts to associate with these Access Points or stations to form a wireless LAN.

To change the SSID, simply highlight it, type the new SSID, and click the **Apply** button.

In typical infrastructure applications a company will use a single SSID for all Access Points. If the radio is scanning and cannot find a channel when an Access Point is known to be in range, verify that the Network Name is set correctly.

Network Type

The adapter can operate in one of two types of networks, which are specified in the **Network Type:** field of the Configuration menu. Clicking the down arrow at the right of this field displays the available types.

- **Peer-to-Peer**

IEEE 802.11, the standard on which the WLAN protocol is based, defines two modes to handle two separate needs. The first, called AdHoc (or IBSS) mode, is used when two or more wirelessly-enabled PCs exchange data directly, without an Access Point. In this case the PCs can establish a peer-to-peer network in which they are the only members and over which they can exchange data. To exchange data, each computer participating in the AdHoc network must specify the same Network Name in this menu.

Peer-to-Peer networks operate on a single communications channel. You specify the channel on which your adapter communicates in an IBSS network through the IBSS Menu.

- **Access Point**

The second mode defined by the IEEE 802.11 standard is called infrastructure mode, and is the primary application for WLAN operation. In this mode all data on the wireless network is directed to an Access Point, which then routes the data to the appropriate wireless station. The Access Point may also be configured to allow data to be bridged from the wireless network to wired networks.

To participate in a wireless LAN in infrastructure mode, every station and Access Point must specify the same Network Name. In infrastructure mode, all available channels are scanned for traffic, so there is no need to specify a channel.

7.3 Encryption Menu

The Security menu lets you enable encryption and set the encryption keys. Click the down arrow at the right of the Authentication Type field.Choose the WEP. To see the available encryption methods, click the down arrow at the right of the Encryption (WEP security) field.

There are two encryption methods available. The IEEE 802.11 specification defines Wired Equivalent Privacy (WEP) using a 64-bit key. This capability was extended by the industry to allow a 128-bit key.

If you specify an encryption method, you will only be able to communicate with Access Points and stations that use the same encryption method and keys.

• **Disabling Encryption**

To disable encryption, click the down arrow at the right of the Encryption field, select Disabled, and click the Apply button.

• **Enabling Encryption**

To enable encryption, click the down arrow at the right of the Encryption field, select either 64 bit or 128 bit, and click the Apply button. After enabling an encryption method, you must then specify encryption keys, as described in the following sections.

Creating Encryption Keys Manually

When you specify either 64-bit or 128-bit encryption, the Configuration Utility selects **Create Keys Manually**, and allows you to enter keys as either alphanumeric or hexadecimal characters. When you click one of these buttons, the cursor appears in the field for Key 1. For 64-bit encryption, you must type exactly 5 alphanumeric or 10 hexadecimal characters in each of the four key fields; for 128-bit encryption, you must type exactly 13 alphanumeric or 26 hexadecimal characters. You then click the Apply button to create your encryption keys. After you click the Apply button, the Configuration Utility uses asterisks to mask your keys.

The Use WEP Key field lets you specify which of the four encryption keys you use to transmit data on your wireless LAN. You can change the default key by clicking on the down arrow at the right of this field, selecting the number of the key you want to use, and then clicking the Apply button. As long as the Access Point or station with which you are communicating has the same key in the same position, you can use any of the keys as the default.

Creating Encryption Keys Using a Passphrase

To create encryption keys using a Passphrase, click the radio button next to **Create Key with Passphrase** and type a character string in the Passphrase field. As you type, the Configuration Utility displays asterisks to mask your Passphrase and uses an algorithm to generate four keys used for encryption.

Using a Passphrase to generate the four keys makes it easy to set the same keys for all members of your wireless LAN.

7.4 IBSS Menu

IBSS Channel Selection

When communicating in a peer-to-peer network, you may specify a channel on which you prefer communications to take place. To see the available channels, click the up or down arrow or move the box in the scroll bar at the right of the Channel Selection field. When the channel you want to set appears, click on the channel to select it, and then click the **Apply** button.

Note that this is not necessarily the channel on which peer-to-peer communications will be established. If the IBSS network names (SSID) are the same for nodes in the peer-to-peer network but they have different preferred channels, a network can still be established. In this case, if it cannot find a network with the specified network name on the preferred channel, a station will scan other channels until it finds a peer-to-peer network with the specified network name on which to communicate.

If you specified **Access Point** as the network type (in the **Configuration** menu), choosing a channel in this field has no effect until you change the network type to **Peer-to-Peer**.

IBSS Menu

Some PHILIPS adapters are capable of operating in only a single transmission band. For these adapters, the Configuration utility displays the **IBSS** menu:

When communicating in a peer-to-peer network, you may specify a channel on which you prefer communications to take place. To specify a channel, click on the channel to select it, and then click the **Apply** button.

Note that this is not necessarily the channel on which peer-to-peer communications will be established. If the IBSS network names (SSID) are the same for nodes in the peer-to-peer network but they have different preferred channels, a network can still be established. In this case, if it cannot find a

network with the specified network name on the preferred channel, a station will scan other channels until it finds a peer-to-peer network with the specified network name on which to communicate.
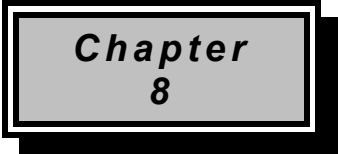
If you specified **Access Point** as the network type (in the **Configuration** menu), choosing a channel in this field has no effect until you change the network type to **Peer-to-Peer**.

7.5 Domain Menu

A domain refers to a territory in which radio frequency transmissions must conform to the standards set by a single regulatory agency. For example, in the United States, the FCC sets the allowed frequencies and channels for wireless data communications. Every country is free to set its own standards, although in practice many countries may use the same standards.

7.6 About Menu

The About menu provides information on the version of the Network Driver, the Configuration Utility, and the firmware in the PHILIPS WLAN Interface adapter. You can display this menu by choosing the **Version Information...** command from the pop-up menu, or by clicking on the **about** tab when the Configuration Utility is displayed on your desktop.

Advanced Properties Tab

The **Advanced Properties** tab provides access to operating parameters for the PHILIPS adapter, which are not controlled by the configuration utility. These properties are accessed through the Windows hardware device manager. The following steps describe how to access these properties under Windows 2000. For other versions of Windows (Windows Poor Windows 98, for example) the details may differ slightly; consult your operating system documentation or your system administrator. Also, the properties that appear in the list displayed by the device manager may differ depending on the adapter installed in your computer.

To display these properties, complete the following steps:

1. With the right mouse button, click on the **My Computer** icon on your desktop and choose the **Properties** item from the menu that appears.

2. Start the Hardware Device Manager to display a list of the devices connected to your computer.

3. With the left mouse button, click on the plus (+) sign to the left of **Network Adapters** to display a list of the network adapters detected by your computer.

4. With the left mouse button, double-click on the Intersil Wireless LAN entry to display your adapter's properties.

When you click on the **Advanced** tab, a display similar to the following appears:

You can see the value for any of these properties by clicking on a property in the list in this display. If a value has been set for the property, it appears in the **Value** field to the right of the list. To disable a value, click in the **Not Present** radio button below the **Value** field.

Moving the mouse pointer to the **Value** field and clicking once with the left mouse button allows you to change the value for the highlighted property. If there are specific values that can be set, a list of values appears below this field when you click in it. To choose one of these values, move the mouse pointer down until the value you want is highlighted, and then click once with the left mouse button. For those values for which you must specify a numeric value, simply type the value in this field.

The following sections provide descriptions for the items in the **Property** list displayed by this tab.

Configuration Profile

Certain PHILIPS adapters have the ability to use pre-defined profiles with standard parameters. Such adapters provide the following profiles:

- B only – for operation in 802.11b environments only
- B WIFI – for operation in 802.11b environments conforming to WiFi standards
- G only – for operation in 802.11g environments only
- Mixed – for operation in either 802.11b or 802.11g environments
- Mixed Long – for long-range operation in either 802.11b or 802.11g environments
- Test – for operation under the widest variety of 802.11 conditions

Fragmentation Threshold

The size at which packets will be fragments. The default setting is 2346 bytes.

Normally you should leave this property disabled unless directed otherwise by your Network Administrator.

Nitro Mode

Nitro mode is an Intersil-proprietary method to increase data throughput over the WLAN, and is particularly effective in mixed 802.11b/g environments. This property determines whether Nitro mode is enabled in the adapter. A value of 0 (zero) disables this mode; a value of 1 (one) enables it.

Power Save Mode

This property turns the Station Power Save feature on or off, or sets it to Auto. When in Auto mode, the station enters Power Save based on the battery condition (XP only) on the host. Power Save mode decreases the amount of power consumed by the adapter by powering off the radio for short periods. Enabling Power Save Mode trades off performance for battery life.

Certain PHILIPS adapters are capable of advanced Power Save settings. For these adapters, the following Power Save settings are available:

- Auto Dynamic – specifies Disable mode when on AC power and Dynamic mode when on battery
- Auto Maximum – specifies Disable mode when on AC power and Maximum mode when on battery
  Note: Auto Dynamic and Auto Maximum require NDIS 5.1 or later, typically available only on Windows XP.

- Disabled – specifies continuous access mode and is the default
- Dynamic – specifies a fast power saving mode that provides the best combination of performance and power usage
- Maximum – specifies the greatest power saving mode

RTS Threshold

The RTS threshold is the packet size (in bytes) at which packet transmission is governed by the RTS/CTS transaction.

You can enter a value from 0 to 2432 in increments of 64 for this property. Normally you should leave this property disabled unless directed otherwise by your Network Administrator.

Chapter
9

Glossary

A

Ad-Hoc Mode - A client setting that provides independent peer-to-peer connectivity in a wireless LAN. An alterative setup is where PCs communicate with each other through an access point. An Ad-hoc integrated wireless LAN is a group of computers, each has a Wireless LAN adapter, Connected as an independent wireless LAN. Ad hoc wireless LAN is applicable at a departmental scale for a branch or SOHO operation.

B

Bandwidth - The transmission capacity of a given facility, in terms of how much data the facility can transmit in a fixed amount of time; expressed in bits per second (bps).

Bit - A binary digit. The value (0 or 1) used in the binary numbering system. Also, the smallest form of data.

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

D

Default Gateway - The routing device used to forward all traffic that is not addressed to a station within the local subnet.

DHCP server and client - DHCP stands for Dynamic Host Configuration Protocol. This protocol is designed to automatically load parameters for the TCP/IP network, including the IP address, host name, domain name, net-mask, default gateway, and name server address. The machine that provides this service is called the DHCP server, and its client computers are called DHCP clients. If client computers support DHCP, a TCP/IP configuration is not needed on each client computer.

Domain - A sub-network comPhilipsed of a group of clients and servers under the control of one security database. Dividing LANs into domains improves performance and security.

Driver - A workstation or server software module that provides an interface between a network interface card and the upper-layer protocol software running in the computer; it is designed for a specific NIC, and is installed during the initial installation of a network-compatible client or server operating system.

DSSS (Direct-Sequencing Spread-Spectrum) - DSSS operate over the radio airwaves in the unlicensed ISM band (industrial, scientific, medical). DSSS uses a radio transmitter to spread data packets over a fixed range of frequency band.

E

Encryption - A security method that applies a specific algorithm to data in order to alter the data's appearance and prevent other devices from reading the information.

Ethernet - The most widely used LAN access method, which is defined by the IEEE 802.3 standard. Ethernet is normally a shared media LAN meaning all devices on the network segment share total bandwidth. Ethernet networks operate at 10Mbp using CSMA/CD to run over 10Base T cables.

F

Firmware - Program that is inserted into programmable read-only memory (programmable read-only memory), thus becoming a permanent part of a computing device.

Fragmentation Threshold Value - Indicates how much of the network resources is devoted to recovering packet errors. The value should remain at its default setting of 2,432. If you experience high packet error rates, you can decrease this value but it will likely decrease overall network performance. Only minor modifications of this value are recommended.

Fragmentation - Breaking a packet into smaller units when transmitting over a network medium that cannot support the original size of the packet.

I

IEEE - The Institute of Electrical and Electronics Engineers

IEEE 802.11b standard - The IEEE 802.11b Wireless LAN standards subcommittee formulating standards for the industry. The objective is to enable wireless LAN hardware from different manufacturers to communicate.

Infrastructure Mode - A client setting providing connectivity to an Access Point. As compared to Ad-Hoc Mode where PCs communicate directly with each other clients set in infrastructure Mode all pass data through a central Access Point. The Access Point not only mediates Wireless network traffic in the immediate neighborhood but also pro-vides communication with the wired network. An integrated wireless and wireless and wired LAN is

called an Infrastructure configuration. Infrastructure is applicable to enter Philips scale for wireless access to central database, or wireless application for mobile workers.

IP Address - An IP address is a 32-bit number that identifies each sender & receiver of information that is sent across the Internet. An IP address has two parts: the identifier of a particular network on the Internet and one identifier of a particular device (which can be a server or a workstation within that network).

ISM band - The FCC and their counterparts outside of the U.S. have set aside bandwidth for unlicensed use in the 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.

L

LAN - A local area network (LAN) is a group of computers and associated devices that share a common communications line and typically share the resources of a single processor or server within a small geographic area (for example, within an office building).

M

MAC Address - 12-digit hexadecimal number that identifies a networking product on the network.

Mbps (Meg**a**bits per second) - One million bits per second; unit of measurement for data transmission.

N

Network - A system that transmits any combination of voice, video and/or data between users.

Node - A network junction or connection point, typically a computer or work station.

O

Open System - Is when the sender and the recipient do not share a secret key. Each party generates its own key-pair and asks the receiver to accept the (usually randomly) generated key. Once accepted, this key is used for a short time only; then a new key is generated and agreed upon.

P

Packet - A unit of data routed between an origin and a destination in a network.

PCMCIA - Personal Computer Memory Card International Association

Plug and Play - The ability of a computer system to configure expansion boards and other devices automatically without requiring the user to turn off the system during installation.

R

Roaming - The ability to use a wireless device and be able to move from one access point's range to another without losing the connection.

RTS/CTS Threshold Value - Should remain at its default setting of 2,347. A preamble is a signal used to synchronize the transmission timing between two or more systems. A series of transmission pulses is sent before the data to indicate that "someone is about transmit data." This ensures that systems receiving the information correctly when the data transmission starts.

S

Shared Key - Is when both the sender and recipient share a secret key. Both units use this key for an extended length of time, sometimes indefinitely. Any eavesdropper that discovers the key may decipher all packets until the key is changed.

Signal Strength - The signal level indicates the strength of the signal as received at the wireless network interface.

SNMP (Simple Network Management Protocol) - A standard network protocol that can be used to manage networks locally, or worldwide via the Internet.

Spread Spectrum - Spread Spectrum technology is a wideband radio frequency technique developed by the military for use in reliable, secure, mission-critical communication systems. It is designed to trade off bandwidth efficiency for reliability, integrity, and security. In other words, more bandwidth is consumed than in the case of narrowband transmission, but the trade off produces a signal that is, in effect, louder and thus easier to detect, provided that the receiver knows the parameters of the spread-spectrum signal being broadcast. If a receiver is not tuned to the right frequency, a spread –spectrum signal looks like background noise. There are two main alternatives, Direct Sequence Spread Spectrum (DSSS) and Frequency Hopping Spread Spectrum (FHSS).

SSID (Service Set Identifier) - Is the unique name shared among all points in a wireless network. The SSID must be identical for all points in the network. It is case sensitive and must not exceed 32 characters.

Static IP Address - A permanent IP address that is assigned to a node in an IP or a TCP/IP network.

Subnet - A subnet is a logical sub-division of a Local Area Network that has been divided by means of routers or gateways. A subnet may include multiple LAN segments. Each subnet is identified by the Subnet Mask.

T

TCP/IP (Transmission Control Protocol/Internet Protocol) - The basic communication language or protocol of the Internet. It can also be used as a communications protocol in a private network (either an intranet or an extranet). When you are set up with direct access to the Internet, your computer is provided with a copy of the TCP/IP program just as every other computer that you may send messages to or get information from also has a copy of TCP/IP.

W

WEP (Wired Equivalent Privacy) - A data privacy mechanism based on a 40 bit shared key algorithm, as described in the IEEE 802 .11 standard. The optional cryptographic confidentiality algorithm specified by IEEE 802.11 used to provide data confidentiality that is subjectively equivalent to the confidentiality of a wired LAN medium that does not employ cryptographic techniques to enhance privacy.

Windows workgroup - A Windows workgroup can consist of either wireless or wired network connections or a combination of the two. Usually a Windows workgroup consists of members who are related because of a shared function, e.g. members of the same department. For a Windows workgroup it is not relevant where the workgroup participants are located, since the members of a Windows workgroup are identified by their workgroup name only.