



ALLSPOT

Worldwide Radio Hotspot Finder

with

USB 2.0 Wi-Fi Adapter

User's Guide

Version 2.0

April 2006

Federal Communications Commission (FCC) Interference Statement

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

- This device may not cause harmful interference.
- This device must accept any interference received, including interference that may cause undesired operations.

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 commercial environment. 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.

If this equipment does cause harmful interference to radio/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 the 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/TV technician for help.

Notice 1

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

Caution

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

Table of Contents

Getting Started with the ALLSPOT	5
Overview of the Wireless Client Utility	6
Working with Profiles	7
Creating a Profile	8
Modifying Profiles	8
Checking for Available Access Points	11
Wireless LAN Networking	12
Transmission Rate (Transfer Rate)	12
Types of Wireless Networks	12
Ad-Hoc (IBSS) Network	12
Infrastructure (BSS) Network	13
Wireless LAN Security	15
Data Encryption with WEP	16
Exploring the Wireless Client Utility Screens	17
The Network Screen	17
Link Information	17
Wireless Setting	18
The Profile Screen	20
Profile List	21
The SiteSurvey Screen	22
Available Networks	22
Configuring Wireless Security	23
Configuring Security	23
Configuring WEP	23
Configuring WPA-PSK & WPA2-PSK	25
Configuring WPA & WPA2	25
Configuring 802.1X	27
Advanced Settings	27
Glossary	29

Appendix	31
Maintenance	31
Checking the Wireless Client Utility Version	31
Uninstalling the Wireless Client Utility	32
Upgrading the Wireless Client Utility	32
Troubleshooting	33
Problems Starting the 802.11 Wireless Client Utility Program	33
Problems with the Link Status	33
Problems with Security Settings	33
Problems Communicating With Other Computers	33
Specifications	35
Wi-Fi Radio :	35
Hardware :	35
Software :	35

Getting Started with the ALLSPOT

Congratulations on purchasing the ALLSPOT! The quick start guide included with your ALLSPOT tells you how to install the Wireless Client Utility and how to operate the Hotspot Finder feature of the ALLSPOT.

This manual provides information for setting up and configuring the ALLSPOT. This manual is intended for both home users and professionals. It is not required to read some of the more technical information in this manual (such as in "Wireless LAN Networking" on page 13 and "Configuring Wireless Security" on page 29) to operate and enjoy the ALLSPOT. It is included for your reference only.

The following conventions are used in this manual:



THE NOTE SYMBOL INDICATES ADDITIONAL INFORMATION ON THE TOPIC AT HAND.



THE TIP SYMBOL INDICATES HELPFULL INFORMATION AND TIPS TO IMPROVE YOUR NETWORK EXPERIENCE.



THE CAUTION SYMBOL ALERTS YOU TO SITUATIONS THAT MAY DEGRADE YOUR NETWORKING EXPERIENCE OR COMPROMISE YOUR SECURITY.



LIKE NOTES AND TIPS, THE IMPORTANT SYMBOL INDICATES INFORMATION THAT CAN IMPROVE NETWORKING. THIS INFORMATION SHOULD NOT BE OVERLOOKED.

This section covers the following topics:

- "Overview of the Wireless Client Utility" on page 2
- "Working with Profiles" on page 3
- "Checking for Available Access Points" on page 10
- "Disabling the Wireless Client Utility" on page 11

Overview of the Wireless Client Utility

The Wireless Client Utility is included on the CD that shipped with the ALLSPOT. Install the utility as described in the Quick Start Guide before attaching the ALLSPOT to your computer.



IMPORTANT

BE SURE TO INSTALL THE WIRELESS CLIENT UTILITY BEFORE YOU ATTACH THE ALLSPOT TO YOUR COMPUTER. ATTACHING THE ALLSPOT BEFORE THE UTILITY IS INSTALLED COULD CAUSE THE INSTALLATION TO FAIL.

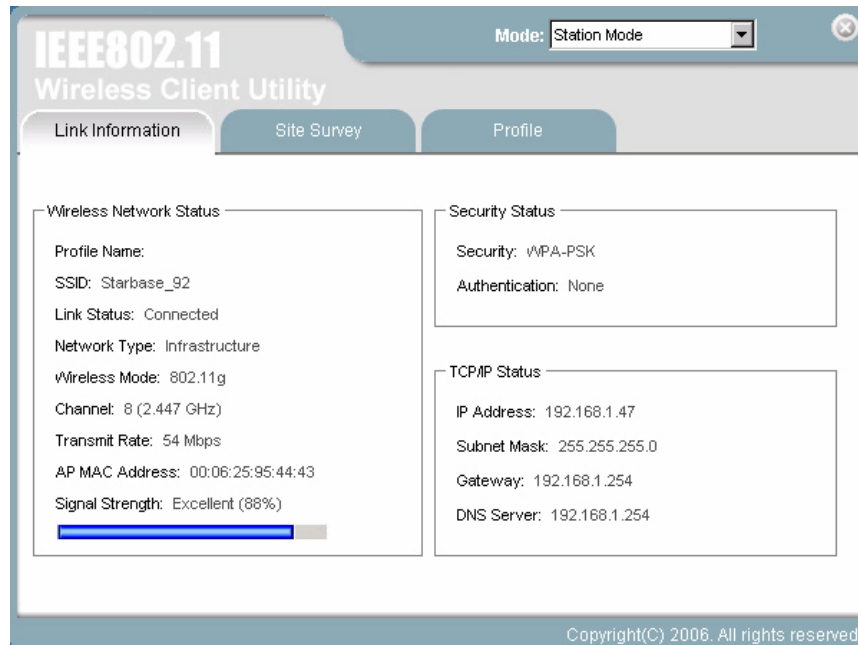
When the ALLSPOT is installed, it is configured to automatically load when you start your computer. The utility icon displays in the system tray at the bottom-right corner of your screen.



NOTE

WHEN THE ALLSPOT IS NOT CONNECTED TO YOUR COMPUTER, MOST SETTINGS IN THE WIRELESS CLIENT UTILITY ARE UNAVAILABLE. SETTINGS OR BUTTONS THAT ARE NOT AVAILABLE ARE GRAYED OUT.

Double-click the ALLSPOT icon in the system tray, the following **Link Information** screen opens:



There are three screens in the utility. Click on the links below for detailed information on each screen:

- “The Link Information Screen”
- “The Site Survey Screen”
- “The Profile Screen”

The **Link Information** (see “Link Information” on page xx) pane provides information on your current connection. This same pane is shown at the bottom of all screens so you are always aware of your connection status.

A profile is a record of the configuration you use to connect to a particular access point. Without profiles, you would have to reconfigure the ALLSPOT each time you change access points. Using the **Profile** screen you can configure the ALLSPOT to access your home network and your office network. Each configuration is saved as a profile. Then when you go from the office to your home you just select the appropriate profile.

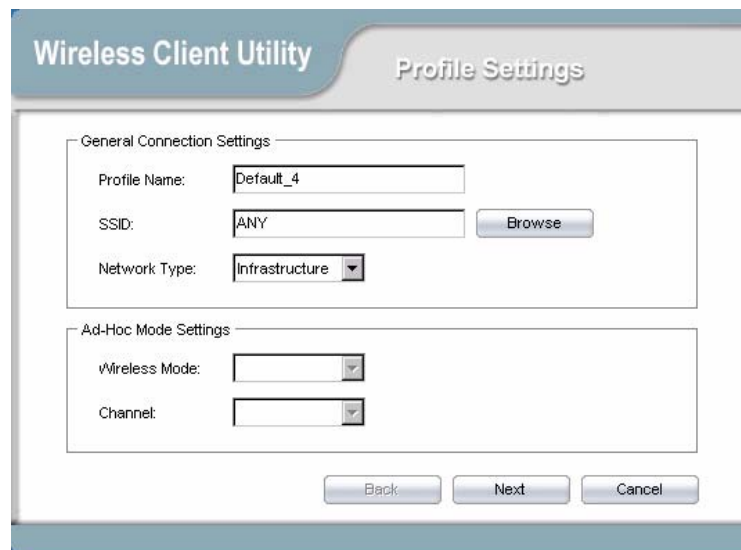
CREATING A PROFILE

Refer to the following to create a profile.

1. Click **Profile**.



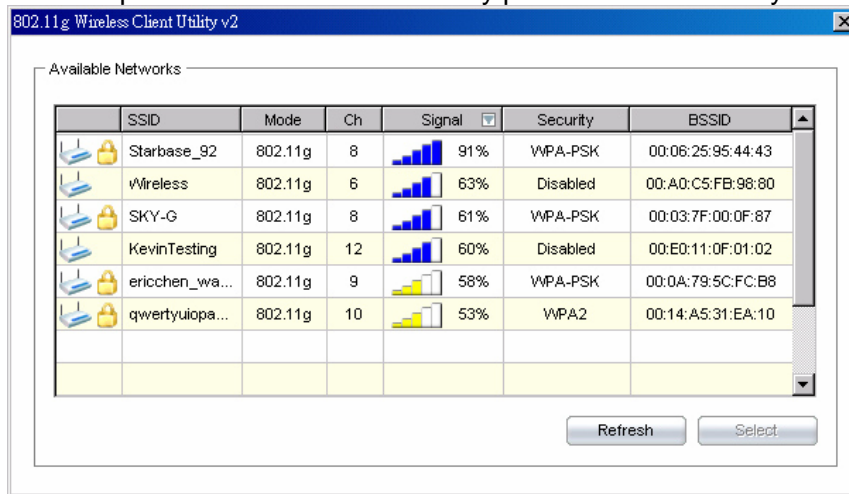
2. Click **Add**. To modify a configuration profile, select the configuration from the Profile list and click the **Edit** button.



2. Type a descriptive name for the profile such as **Default_4** or **Home**.
3. Click the drop-down arrow at Network Mode and select **Infrastructure** or **Ad-Hoc**. Choose **Infrastructure** when connecting to an access point or wireless router. You will need to know the SSID of the access point.

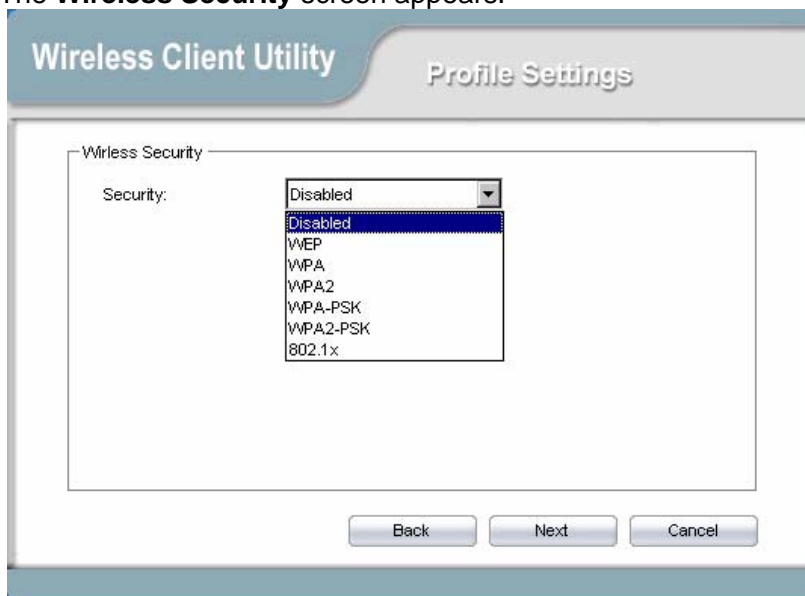
Choose **Ad-Hoc** when connecting directly to another computer without using an access point. You can type anything for the SSID as long as the same SSID is used on the computer you are connecting to.

4. In the **SSID** pane click **Browse**. The utility performs a site survey and displays the results.



The SSID (Service Set IDentifier) is the name assigned to a wireless Wi-Fi network. All devices must use this case-sensitive name, which is a text string up to 32 bytes long, in order to communicate.

5. Select the SSID you want to connect to and click **Select**.
6. The **Wireless Security** screen appears.



This screen reflects the security settings detected in the access point you want to connect to. Security settings vary in complexity and you may have to consult your network administrator for this information. See "Configuring Wireless Security" on page xx for more information.

7. Select the Security Mode from the drop-down list and then select the appropriate settings for the security mode.

WPA/WPA2	<p>Enables the use of Wi-Fi Protected Access (WPA).</p> <p>Choosing WPA/WPA2 opens the WPA/WPA2 Security Settings screen. The options include:</p> <ul style="list-style-type: none"> ■ TLS (Transport Layer Security) is a Point-to-Point Protocol (PPP) extension supporting additional authentication methods within PPP. Transport Layer Security (TLS) provides for mutual authentication, integrity-protected cipher suite negotiation, and key exchange between two endpoints. ■ PEAP (EAP-GTC) (Protected Extensible Authentication Protocol) authenticates wireless LAN clients using only server-side digital certificates by creating an encrypted SSL/TLS tunnel between the client and the authentication server. The tunnel then protects the subsequent user authentication exchange. ■ PEAP (EAP-MSCHAP V2) (Protected Extensible Authentication Protocol) To use PEAP (EAP-MSCHAP V2) security, the server must have WPA-PEAP certificates, and the server properties must already be set. Check with the IT manager ■ TTLS (Tunneled Transport Layer Security) An EAP variant that provides mutual authentication using a certificate for server authentication, and via a secure TLS tunnel for the client ■ LEAP (Lightweight and Efficient Application Protocol) is the general framework for a set of high-performance, efficient protocols which are ideal for mobile and wireless applications. LEAP is designed to address all the technical requirements of the wireless data communications industry, and is oriented towards providing the greatest benefit to the industry and the consumer
WPA-PSK/WPA2-PSK	<p>Enables WPA/WPA2 Passphrase security.</p> <p>Fill in the WPA/WPA2 Passphrase on Security Settings screen.</p>
802.1x	<p>Enables 802.1x security. This option requires IT administration.</p> <p>Choosing 802.1x opens the 802.1x Security Settings screen. The options include:</p> <ul style="list-style-type: none"> ■ TLS ■ PEAP ■ TTLS ■ LEAP

Checking for Available Access Points

The number of access points or hot spots for public use is constantly increasing in major cities. Many Web sites report on the locations of hot spots. Check the following Web sites for updated information for your location.

- <http://intel.jiwire.com>
- www.hotspot-locations.com
- www.hotspotlist.com
- www.wififreespot.com
- www.wifinder.com
- www.wi-fizone.org

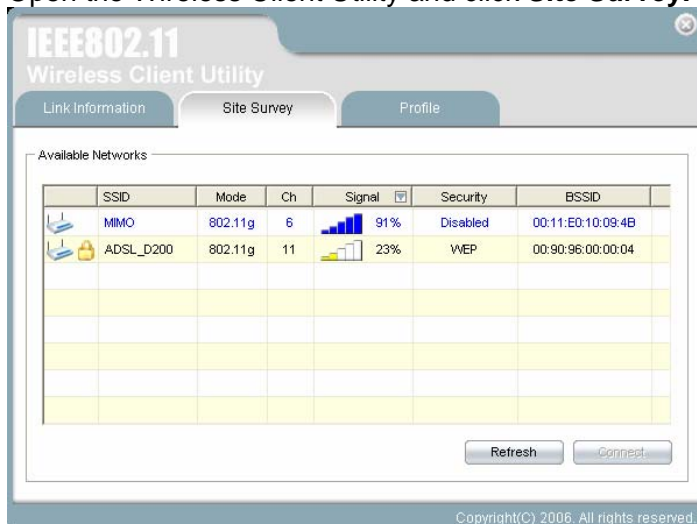
If you think you are in the vicinity of an access point, you can use the SiteSurvey screen to list the ones available.



Remember, you do not have to turn on your computer to find access points. You can use the hot spot finder functionality of the ALLSPOT to locate access points while you are walking around. See the Quick Start Guide for details.

To scan for access points using the ALLSPOT, refer to the following.

1. Open the Wireless Client Utility and click **Site Survey**.



2. Available wireless networks are listed. Click **Refresh** anytime to update the list.
3. Select the network you want and click **Connect**. If no configuration profile exists for that network, the Profile Settings window opens to ask to create a profile for the network. Follow the procedures to create profile for that network.

Wireless LAN Networking

This section provides background information on wireless LAN networking technology. Consult the "Glossary" on page 37 for definitions of the terminology used in this section.



THE INFORMATION IN THIS SECTION IS FOR YOUR REFERENCE. CHANGING NETWORK SETTINGS AND PARTICULARLY SECURITY SETTINGS SHOULD ONLY BE DONE BY AN AUTHORIZED ADMINISTRATOR.

Transmission Rate (Transfer Rate)

The ALLSPOT provides various transmission (data) rate options for you to select. Options include Fully Auto, 1 Mbps, 2 Mbps, 5.5 Mbps, 11 Mbps, 6 Mbps, 9 Mbps, 12 Mbps, 18 Mbps, 22 Mbps, 24 Mbps, 36 Mbps, 48 Mbps and 54 Mbps. In most networking scenarios, the factory default Fully Auto setting proves the most efficient. This setting allows your ALLSPOT to operate at the maximum transmission (data) rate. When the communication quality drops below a certain level, the ALLSPOT automatically switches to a lower transmission (data) rate. Transmission at lower data speeds is usually more reliable. However, when the communication quality improves again, the ALLSPOT gradually increases the transmission (data) rate again until it reaches the highest available transmission rate.

Types of Wireless Networks

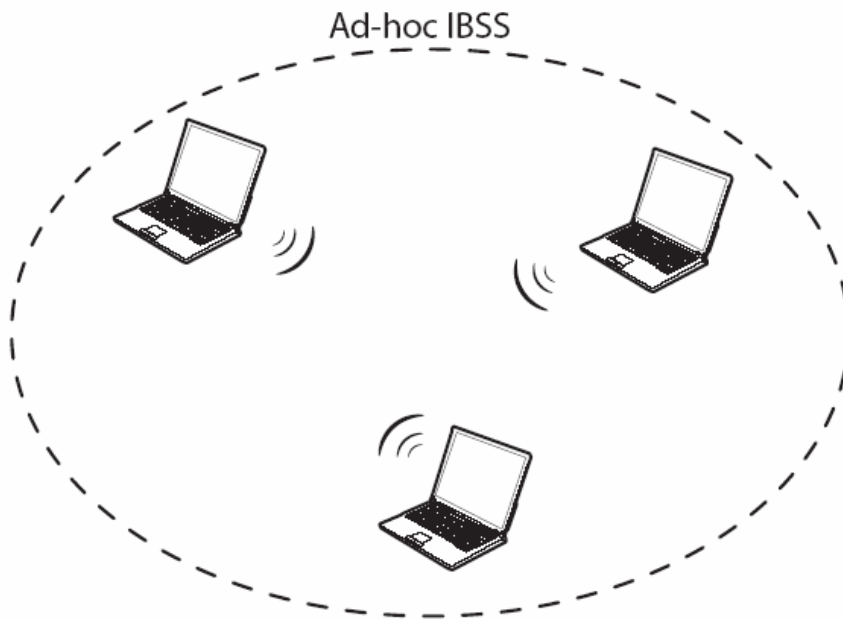
Wireless LAN networking works in either of the two modes: ad-hoc and infrastructure. In infrastructure mode, wireless devices communicate to a wired LAN via access points. Each access point and its wireless devices are known as a Basic Service Set (BSS). An Extended Service Set (ESS) is two or more BSSs in the same subnet. In ad hoc mode (also known as peer-to-peer mode), wireless devices communicate with each other directly and do not use an access point. This is an Independent BSS (IBSS).

To connect to a wired network within a coverage area using access points, set the ALLSPOT operation mode to Infrastructure (BSS). To set up an independent wireless workgroup without an access point, use Ad-hoc (IBSS) mode.

Ad-Hoc (IBSS) NETWORK

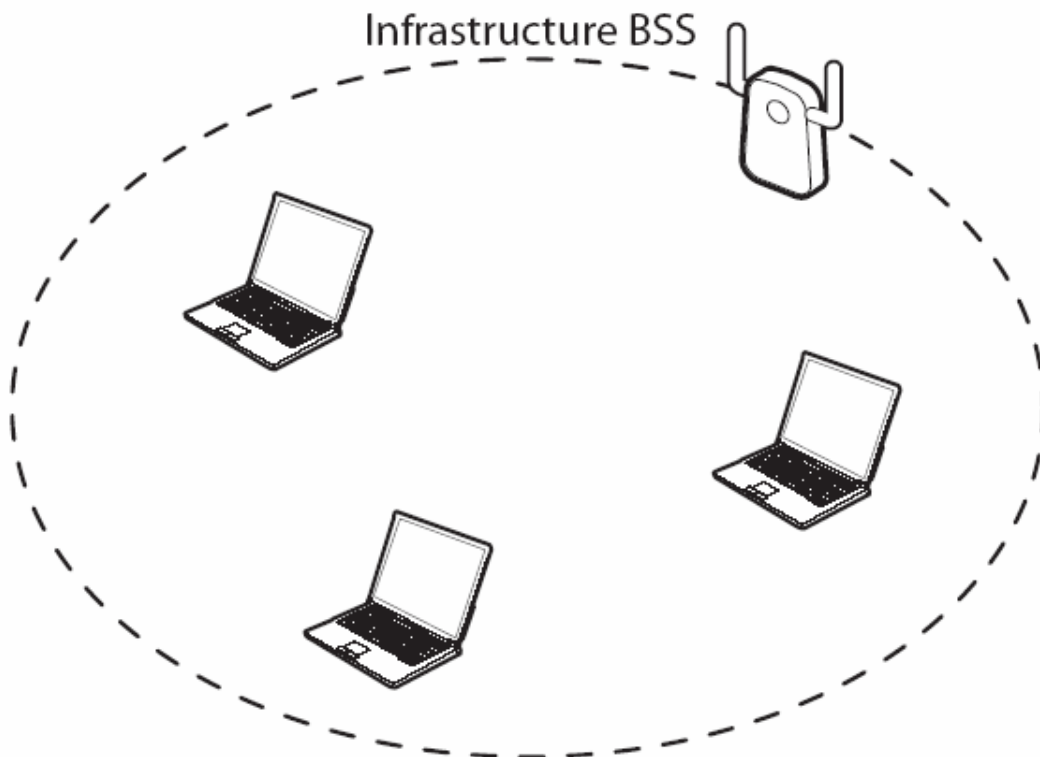
Ad-hoc mode does not require an access point or a wired network. Two or more wireless stations communicate directly to each other. An ad-hoc network may sometimes be referred to as an Independent Basic Service Set (IBSS).

To set up an ad-hoc network, configure all the stations in ad-hoc mode. Use the same SSID and channel for each station.



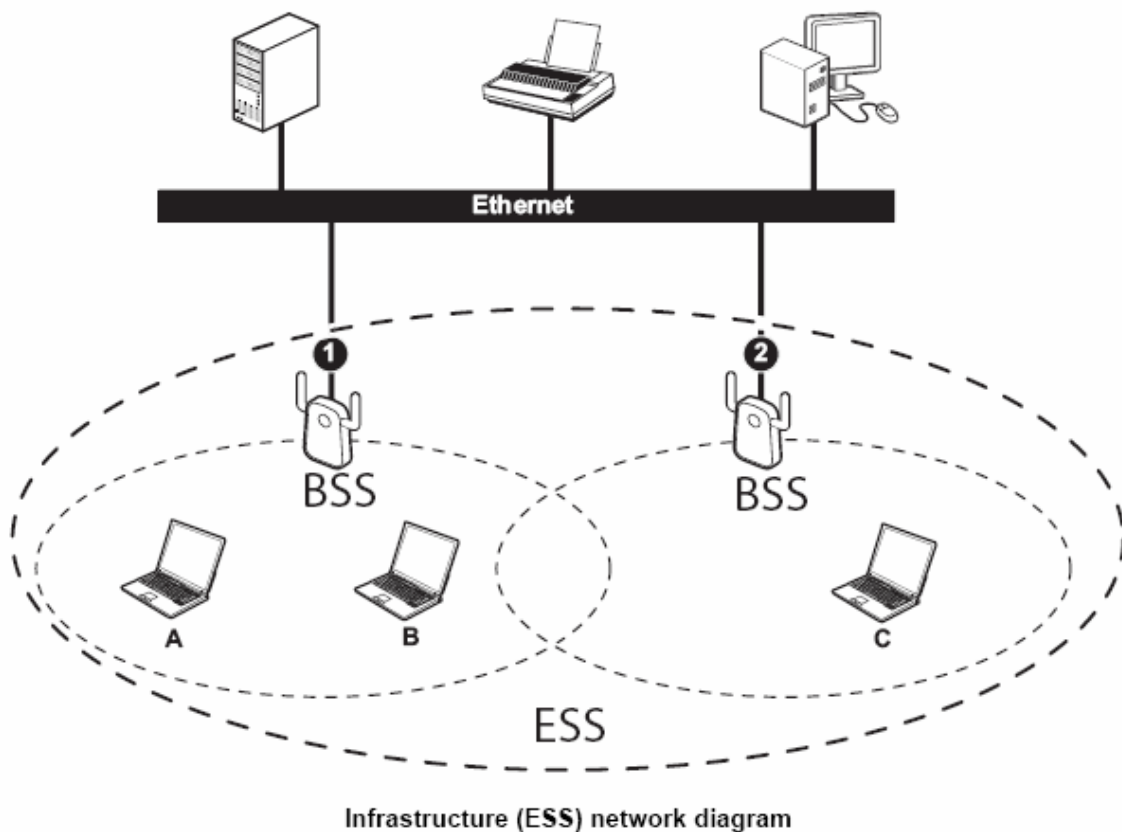
Ad-hoc (also known as peer-to-peer) network diagram

When a number of wireless stations are connected using a single access point, you have a Basic Service Set (BSS).

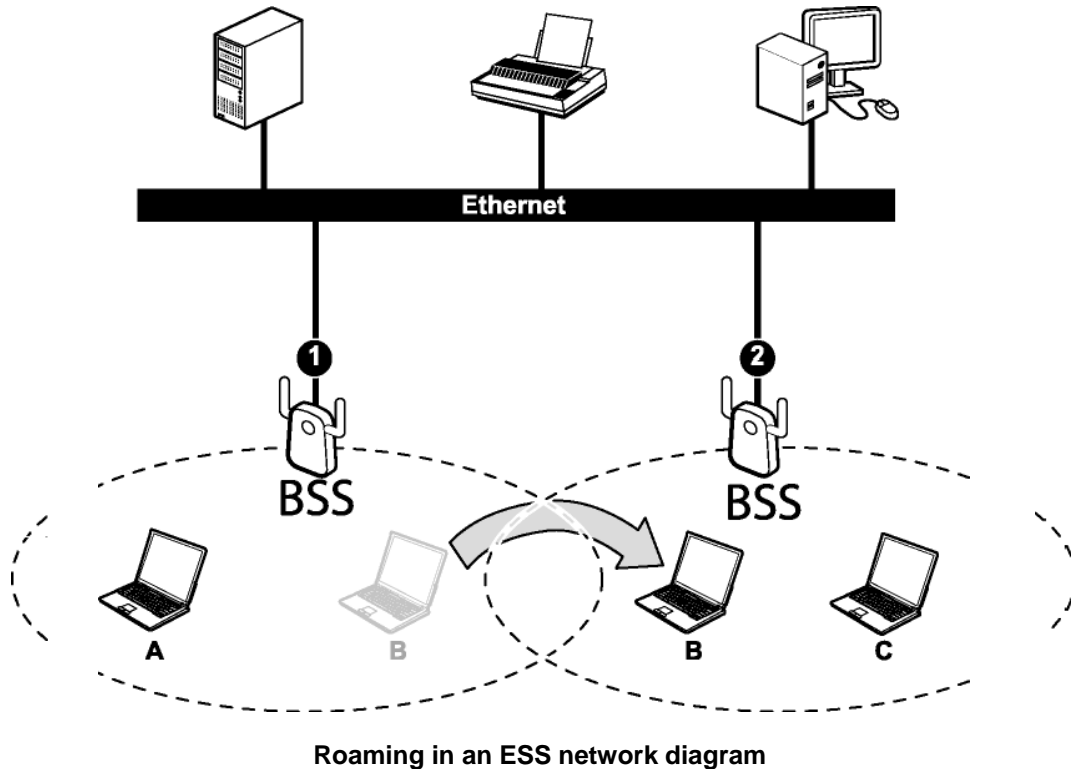


Infrastructure (IBSS) network diagram

In the ESS diagram below, communication is done through the access points, which relay data packets to other wireless stations or devices connected to the wired network. Wireless stations can then access resources, such as a printer, on the wired network.



In an ESS environment, users are able to move from one access point to another without losing the connection. In the diagram below, when the user moves from BSS (1) to BSS (2) the ALLSPOT automatically switches to the channel used in BSS (2).



WIRELESS LAN SECURITY

Because wireless networks are not as secure as wired networks, it's vital that security settings are clearly understood and applied.



DO NOT ATTEMPT TO CONFIGURE OR CHANGE SECURITY SETTINGS FOR A NETWORK WITHOUT AUTHORIZATION AND WITHOUT CLEARLY UNDERSTANDING THE SETTINGS YOU ARE APPLYING. WITH POOR SECURITY SETTINGS, SENSITIVE DATA YOU SEND CAN BE SEEN BY OTHERS.

The list below shows the possible wireless security levels on your ALLSPOT starting with the most secure. EAP (Extensible Authentication Protocol) is used for authentication and utilizes dynamic WEP key exchange. EAP requires interaction with a RADIUS (Remote Authentication Dial-In User Service) server either on the WAN or the LAN to provide authentication service for wireless stations.

1. Wi-Fi Protected Access (WPA)
2. IEEE802.1X EAP with RADIUS Server authentication
3. WEP Encryption
4. Unique ESSID

To check wireless LAN security settings for a connection, open the Wireless Client Utility and select the **Profile** screen. Select the connection you want and click Properties. See "Modifying Profiles" on page 8.

DATA ENCRYPTION WITH WEP

The WEP (Wired Equivalent Privacy) security protocol is an encryption method designed to try to make wireless networks as secure as wired networks. WEP encryption scrambles all data packets transmitted between the ALLSPOT and the access point or other wireless stations to keep network communications private. Both the wireless stations and the access points must use the same WEP key for data encryption and decryption.

There are two ways to create WEP keys in your ALLSPOT.

- Automatic WEP key generation based on a password phrase called a passphrase. The passphrase is case sensitive. You must use the same passphrase for all WLAN adapters with this feature in the same WLAN.
- For WLAN adapters without the passphrase feature, you can still take advantage of this feature by writing down the four automatically generated WEP keys from the **Security Settings** screen of the wireless utility and entering them manually as the WEP keys in the other WLAN adapter(s).

The ALLSPOT allows you to configure up to four WEP keys and only one key is used as the default transmit key at any one time.



THE ALLSPOT SUPPORTS UP TO FOUR 64-BIT, 128-BIT, AND 256-BIT WEP KEYS. THE 256-BIT WEP MUST COMPLY WITH THE WEP SETTING OF YOUR ACCESS POINT OR ROUTER.

Exploring the Wireless Client Utility Screens

This section covers the following topics:

- “The Link Information Screen” on page 17
- “The Profile Screen” on page 20
- “The Site Survey Screen” on page 22

The Link Information Screen

The Wireless Client Utility is included on the CD that shipped with the ALLSPOT. Install the utility as described in the Quick Start Guide before attaching the ALLSPOT to your computer.



BE SURE TO INSTALL THE WIRELESS CLIENT UTILITY BEFORE YOU ATTACH THE ALLSPOT TO YOUR COMPUTER. ATTACHING THE ALLSPOT BEFORE THE UTILITY IS INSTALLED COULD CAUSE THE INSTALLATION TO FAIL.

When the ALLSPOT is installed, it is configured to automatically load when you start your computer. The utility icon displays in the system tray at the bottom-right corner of your screen.






Double-click the ALLSPOT icon in the system tray, the following **Link Information** screen opens:



WIRELESS SETTING

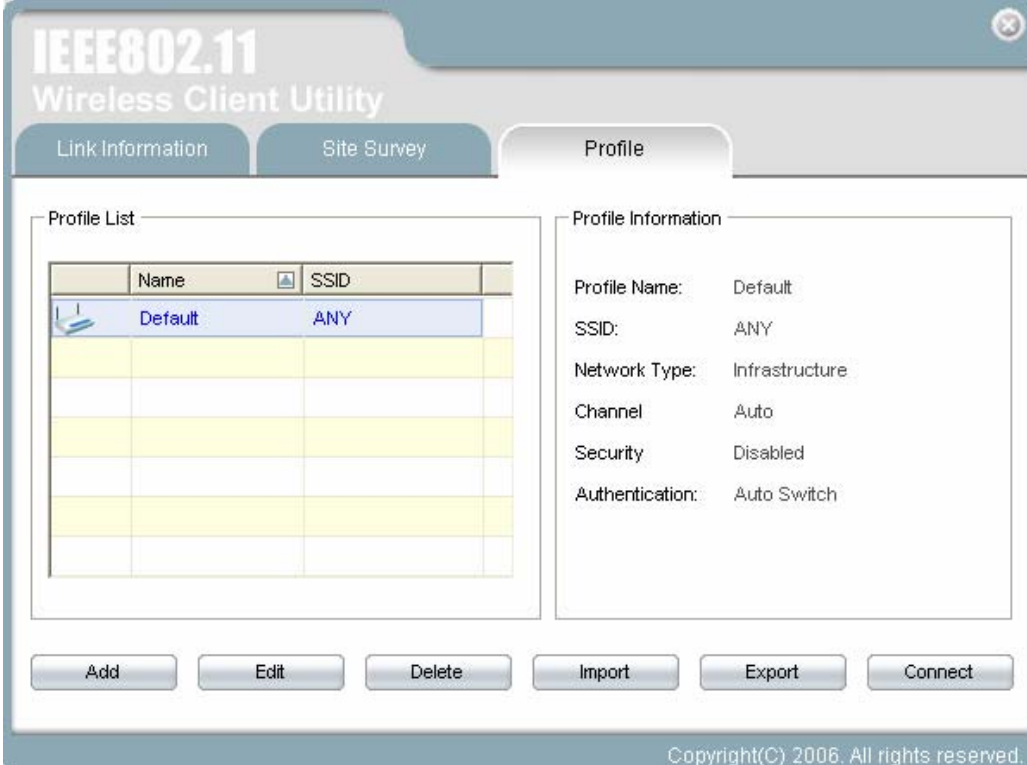
The Wireless Setting pane settings are described below

Wireless Network Status	
Profile Name	The name of the current selected configuration profile. Set up the configuration name on the Profile tab .
SSID	Displays the wireless network name.
Link Status	Shows whether the station is associated to the wireless network.
Network Type	The type of network the station is connected to. The options include: <ul style="list-style-type: none"> <input type="checkbox"/> Infrastructure (access point) <input type="checkbox"/> Ad Hoc
Wireless Mode	Displays the wireless mode. 802.11g or 11b
Channel	Shows the currently connected channel.
Transmit Rate	Displays the current transmit rate in Mbps.
AP MAC Address	Displays the MAC address of the access point the wireless adapter is associated to.
Signal Strength	Shows the strength of the signal.
Security Status	
Security	Shows the security type – Disable, WEP, WPA/WPA2, WAP-PSK/WAP2-PSK or 802.1X
Authentication	Displays the authentication mode.
TCP/IP Status	
IP Address	Displays the computer's IP address.
Subnet Mask	Displays subnet mask
Gateway	Displays gateway address
DNS Server	Display DNS server address

 NOTE	<p>WIRELESS SYSTEMS WORK IN INFRASTRUCTURE MODE OR PEER-TO-PEER MODE. IN INFRASTRUCTURE MODE, WIRELESS DEVICES COMMUNICATE TO A WIRED LAN VIA ACCESS POINTS. IN AD-HOC MODE (ALSO KNOWN AS PEERTO-PEER MODE), WIRELESS DEVICES COMMUNICATE WITH EACH OTHER DIRECTLY AND DO NOT USE AN ACCESS POINT.</p>
 TIP	<p>THE LINK INFORMATION PANEL IS SHOWN IN ALL SCREENS SO YOU CAN ALWAYS SEE THE STATUS OF YOUR CURRENT CONNECTION. MONITOR THIS SETTING AS YOU MOVE AROUND TO ATTAIN A SUITABLE SIGNAL.</p>
 NOTE	<p>WIRELESS SYSTEMS WORK IN INFRASTRUCTURE MODE OR AD-HOC (PEER-TO-PEER) MODE. IN INFRASTRUCTURE MODE, WIRELESS DEVICES COMMUNICATE TO A WIRED LAN VIA ACCESS POINTS. EACH ACCESS POINT AND ITS WIRELESS DEVICES ARE KNOWN AS A BASIC SERVICE SET (BSS). IN AD-HOC MODE (ALSO KNOWN AS PEER-TO-PEER MODE), WIRELESS DEVICES COMMUNICATE WITH EACH OTHER DIRECTLY AND DO NOT USE AN ACCESS POINT. THIS IS AN INDEPENDENT BSS (IBSS).</p>

The Profile Screen

A profile is a record of the configuration you use to connect to a particular access point. Without profiles, you would have to reconfigure the ALLSPOT each time you change access points. Using the **Profile** screen you can configure the ALLSPOT to access your home network and your office network. Each configuration is saved as a profile.



Name	SSID
Default	ANY

Profile Information

Profile Name: Default

SSID: ANY

Network Type: Infrastructure

Channel: Auto

Security: Disabled

Authentication: Auto Switch

Add Edit Delete Import Export Connect

Copyright(C) 2006. All rights reserved.

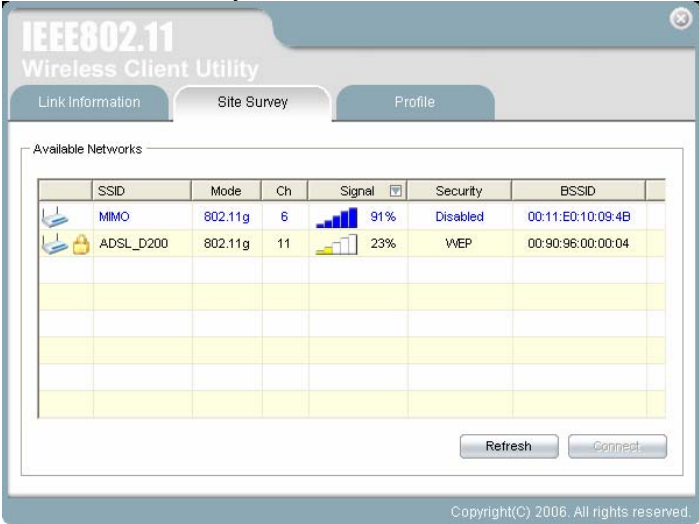
PROFILE LIST

The Profile List pane settings are described below.

Profile Name	Shows the name of the profile that you assigned. If only default displays, no profiles have been added.
SSID	Shows the name (usually the equipment vendor's name) assigned to a wireless Wi-Fi network. (The keyword "ANY" means any available network.)
Network Type	The type of network the station is connected to. The options include: <ul style="list-style-type: none">● Infrastructure (access point)● Ad Hoc
Channel	Shows the currently connected channel.
Security	Shows the security type – Disable, WEP, WPA/WPA2, WAP-PSK/WAP2-PSK or 802.1X
Authentication	Displays the authentication mode.

The SiteSurvey Screen

Use the SiteSurvey screen to scan for available networks in your vicinity.



AVAILABLE NETWORKS

The Available Networks pane settings are described below.

SSID	Shows the name (usually the equipment vendor's name) assigned to a wireless Wi-Fi network.
Mode	Shows the signal type (802.11a/b/g).
Signal	Shows the signal strength.
Ch	Shows the network channel.
Security	Shows the security status.
Refresh (button)	Click to refresh the list of currently available networks.
Connect (button)	Click to connect to the selected network. (The network is not added to the profile list.)

Configuring Wireless Security

This chapter covers the configuration of security options in the 802.11 Wireless Client Utility.

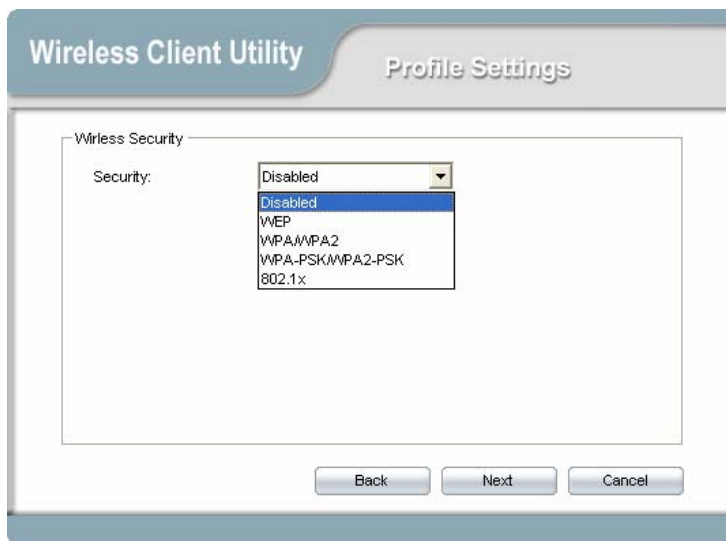
Configuring Security

When you create a profile you need to configure the security settings with the information provided by the administrator. You modify security settings by selecting the profile and clicking **Edit**, then **Next**.

CONFIGURING WEP

Refer to the following to modify WEP settings.

1. In the **Wireless Security** window, click **Security**.



2. Click the drop-down arrow and choose **WEP**. The WEP Configuration screen appears.

The image shows a screenshot of the 'Wireless Client Utility' window, specifically the 'Profile Settings' tab. The 'Security Settings' section is active, showing a configuration for WEP. The 'WEP' dropdown is set to '64 Bits', 'Authentication' is set to 'Auto Switch', and 'Default Key' is set to '1'. There are input fields for 'Passphrase', 'Key 1', 'Key 2', 'Key 3', and 'Key 4'. At the bottom, there are 'Back', 'Next', and 'Cancel' buttons.

WEP	Select the encryption to match your access point: 64, 128, or 256-bit. The encryption level must match the encryption level used by your access point.
Authentication	Options are Auto, Open System, and Shared. For most installations choose Auto.
Pass-Phrase	A WEP Key is automatically generated as you type in any Passphrase of your choice. Use this feature when you have used a Passphrase to generate your WEP key on your access point.
Manual Input (ASCII)	<p>Generate your own WEP Key (4 keys maximum) using ASCII or hexadecimal characters.</p> <p>ASCII: 5 characters for 64-bit, 13 characters for 128-bit, 26 characters for 256-bit</p> <p>HEX: 10 characters for 64-bit, 26 characters for 128-bit, 52 characters for 256-bit</p>
Default Key	Four keys are used for decryption; you have to choose a default key from them for encryption. Make sure access point uses same WEP key.

CONFIGURING WPA-PSK & WPA2-PSK

Refer to the following to configure WPA-PSK & WPA2-PSK.

The screenshot shows the 'Wireless Client Utility' window with the 'Profile Settings' tab selected. The 'Security Settings' section contains a 'Passphrase' text field and an 'Encryption' dropdown menu currently set to 'TKIP'. At the bottom are 'Back', 'Next', and 'Cancel' buttons.

1. Click the drop-down arrow at **Security** and choose **WPA-PSK** or **WPA2-PSK**.
2. Click the drop-down arrow at **Encryption Method** and choose **TKIP** or **AES**. (Most access points use TKIP for WPA-PSK & AES for WPA2-PSK.)
3. At **PSK Passphrase** enter the same pass phrase used to configure the WPA-PSK or WPA2-PSK on your access point.

CONFIGURING WPA & WPA2

Refer to the following to configure WPA & WPA2. This setting requires IT administrator support.

1. Click the drop-down arrow at **Security** and choose **WPA** or **WPA2**.

The screenshot shows the 'Wireless Client Utility' window with the 'Profile Settings' tab selected. The 'Wireless Security' section contains a 'Security' dropdown menu. The dropdown is open, showing options: 'Disabled', 'WEP', 'WPA/WPA2', 'WPA-PSK/WPA2-PSK', and '802.1x'. At the bottom are 'Back', 'Next', and 'Cancel' buttons.

2. Click the drop-down arrow at **Authentication** and choose **TLS**, **PEAP (EAP-GTC)**, **PEAP (EAP-MSCHAP V2)** or **TTLS**

The screenshot shows the 'Wireless Client Utility' window with the 'Profile Settings' tab selected. The 'Security Settings' section is expanded, showing the following fields:

- Authentication:** A drop-down menu with 'TLS' selected.
- User Name:** A text box containing 'test RD'.
- Certificate:** A drop-down menu with 'test RD [Wireless Authen CA]' selected.
- Server CA:** A drop-down menu with '<Trust any installed CA>' selected.
- Validate server certificate:** A checked checkbox.
- Encryption:** A drop-down menu with 'TKIP' selected.

At the bottom of the dialog are three buttons: 'Back', 'Next', and 'Cancel'.

TLS (Transport Layer Security) is a Point-to-Point Protocol (PPP) extension supporting additional authentication methods within PPP. Transport Layer Security (TLS) provides for mutual authentication, integrity-protected cipher suite negotiation, and key exchange between two endpoints.

PEAP (EAP-GTC) (Protected Extensible Authentication Protocol) authenticates wireless LAN clients using only server-side digital certificates by creating an encrypted SSL/TLS tunnel between the client and the authentication server. The tunnel then protects the subsequent user authentication exchange.

PEAP (EAP-MSCHAP V2) (Protected Extensible Authentication Protocol) To use PEAP (EAP-MSCHAP V2) security, the server must have WPA-PEAP certificates, and the server properties must already be set.

TTLS (Tunneled Transport Layer Security) An EAP variant that provides mutual authentication using a certificate for server authentication, and via a secure TLS tunnel for the client

LEAP (Lightweight and Efficient Application Protocol) is the general framework for a set of high-performance, efficient protocols which are ideal for mobile and wireless applications. LEAP is designed to address all the technical requirements of the wireless data communications industry, and is oriented towards providing the greatest benefit to the industry and the consumer

CONFIGURING 802.1X

You need to know if your access point supports 802.1X and then apply the configuration here. This setting requires IT administrator support.

Advanced Settings

After Security Settings finished, the **Advanced Settings** screen will be shown as following.

The screenshot shows the 'Wireless Client Utility' window with the 'Profile Settings' tab selected. The 'Advanced Settings' section contains the following fields:

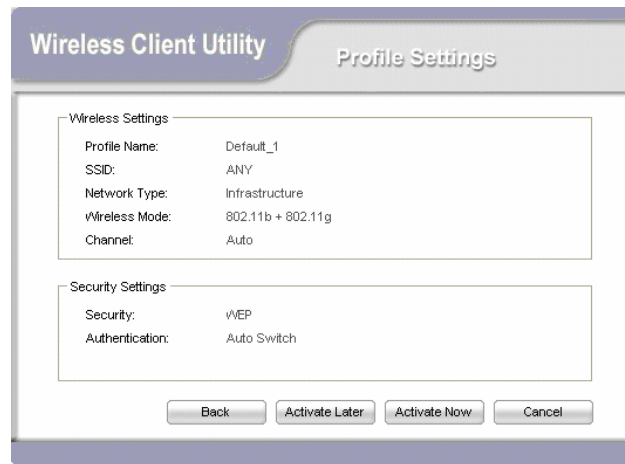
- Power Save Mode:** A dropdown menu set to 'Continuous Access Mode'.
- 802.11b Preamble:** A dropdown menu set to 'Auto'.
- RTS Threshold:** A text box containing '2347' with a range '(0 - 2347)' to its right.
- FRAG Threshold:** A text box containing '2346' with a range '(256 - 2346)' to its right.

The 'Wireless Mode' section contains two checked checkboxes: ☒ 802.11b and ☒ 802.11g. At the bottom are three buttons: 'Back', 'Next', and 'Cancel'.

The following table describes the items found on the Advanced Settings screen.

Power Save Mode	Shows the power save mode. Power management is disabled in ad hoc mode. The options include: <ul style="list-style-type: none"> ● Continuous Access Mode ● Maximum Power Saving ● Fast Power Saving
802.11b Preamble	Displays the 802.11b preamble format. The options include: <ul style="list-style-type: none"> ● Long ● Short ● Auto
RTS Threshold	Value from 0 ~ 2347
FRAG Threshold	Value from 256 ~ 2346
Wireless Mode	Include: <ul style="list-style-type: none"> ● 802.11b ● 802.11g

After advance settings are finished, the following screen showed as below.
You can activate the profile now or later.



The image shows a software window titled "Wireless Client Utility" with a sub-tab "Profile Settings". The window contains two main sections: "Wireless Settings" and "Security Settings".

Wireless Settings:

Profile Name:	Default_1
SSID:	ANY
Network Type:	Infrastructure
Wireless Mode:	802.11b + 802.11g
Channel:	Auto

Security Settings:

Security:	WEP
Authentication:	Auto Switch

At the bottom of the window, there are four buttons: "Back", "Activate Later", "Activate Now", and "Cancel".

Glossary

For unfamiliar terms used below, look for entries elsewhere in the glossary.

AD-HOC (IBSS)

Ad-hoc mode does not require an AP or a wired network. A network that transmits wireless from computer to computer without the use of a base station (access point).

Two or more wireless stations communicate directly to each other. An ad-hoc network may sometimes be referred to as an Independent Basic Service Set (IBSS).

CHANNEL

A radio frequency used by a wireless device is called a channel.

EAP AUTHENTICATION

EAP (Extensible Authentication Protocol) is an authentication protocol that runs on top of the IEEE802.1X transport mechanism in order to support multiple types of user authentication. By using EAP to interact with an EAP-compatible RADIUS server, an access point helps a wireless station and a RADIUS server perform authentication.

ENCRYPTION

The reversible transformation of data from the original to a difficult-to-interpret format. Encryption is a mechanism for protecting confidentiality, integrity, and authenticity of data. It uses an encryption algorithm and one or more encryption keys.

FRAGMENTATION THRESHOLD

This is the maximum data fragment size that can be sent before the packet is fragmented into smaller packets.

IEEE 802.1X

The IEEE 802.1X standard outlines enhanced security methods for both the authentication of wireless stations and encryption key management. Authentication can be done using an external RADIUS server.

INFRASTRUCTURE (BSS)

When a number of wireless stations are connected using a single AP, you have a Basic Service Set (BSS).

ROAMING

In an infrastructure network, wireless stations are able to switch from one BSS to another as they move between the coverage areas. During this period, the wireless stations maintain uninterrupted connection to the network. This is roaming. As the wireless station moves from place to place, it is responsible for choosing the most appropriate AP depending on the signal strength, network utilization among other factors.

SSID

The SSID (Service Set Identity) is a unique name shared among all wireless devices in a wireless network. Wireless devices must have the same SSID to communicate with each other.

TEMPORAL KEY INTEGRITY PROTOCOL (TKIP)

Temporal Key Integrity Protocol (TKIP) uses 128-bit keys that are dynamically generated and distributed by the authentication server.

USER AUTHENTICATION

WPA applies IEEE 802.1X and Extensible Authentication Protocol (EAP) to authenticate wireless clients using an external RADIUS database. If you do not have an external RADIUS server, use WPA-PSK/WPA2-PSK (WPA -Pre-Shared Key) that only requires a single (identical) password entered into each access point, wireless gateway and wireless client. As long as the passwords match, clients will be granted access to a WLAN.

WEP

WEP (Wired Equivalent Privacy) encryption scrambles all data packets transmitted between the ALL0298 and the AP or other wireless stations to keep network communications private. Both the wireless stations and the access points must use the same WEP key for data encryption and decryption.

WPA/WPA2

Wi-Fi Protected Access (WPA) and WPA2 (future upgrade) is a subset of the IEEE 802.11 i security specification draft. Key differences between WPA and WEP are user authentication and improved data encryption. WPA2 is a wireless security standard that defines stronger encryption, authentication and key management than WPA.

Appendix

This section provides maintenance and troubleshooting procedures. Specifications of the ALLSPOT are also provided. The following topics are discussed:

- See “Maintenance” on page 39.
- See “Troubleshooting” on page 41.
- See “Specifications” on page 42.

Maintenance

Installing a newer version of the Wireless Client Utility may improve the performance of the ALLSPOT. Before installing the new version, you must uninstall the old one.

CHECKING THE WIRELESS CLIENT UTILITY VERSION

To check the current Wireless Client Utility version, click right button of your mouse and choose **About**. In the Wireless Client Utility pane, note the **Utility Version** number.



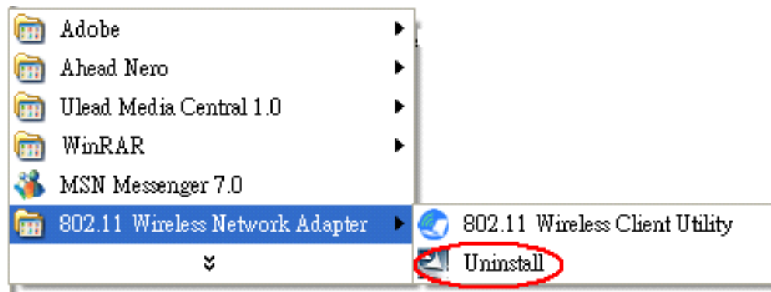
IMPORTANT

If you need to contact technical support, you will need to provide the S/W Information. Be sure to check the screen in the utility that is installed on your computer and not the screen shown in this manual.

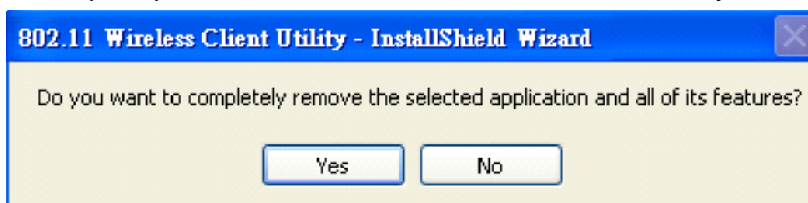
UNINSTALLING THE WIRELESS CLIENT UTILITY

Refer to the following to uninstall (remove) the Wireless Client Utility from your computer.

1. Click **Start -> All Programs (Windows 2000 Programs) -> 802.11 Wireless Network Adapter -> Uninstall.**



2. When prompted, click **Yes** to remove the driver and utility software.



3. Click **Finish** to complete the uninstallation.
4. Reboot your computer if prompted.

UPGRADING THE WIRELESS CLIENT UTILITY

Contact your dealer or technical support for details on downloading the current Wireless Client Utility. Refer to the following to upgrade the Wireless Client Utility.

1. Double-click the Setup.exe file that you downloaded. The installation wizard screen opens.
2. Click **Next** to continue.
3. Click **Next** in the **Choose Destination Location** screen.
4. Click **Install** to begin the installation.
5. Click **Finish** to exit the wizard and complete the installation.

Troubleshooting

PROBLEMS STARTING THE 802.11 WIRELESS CLIENT UTILITY PROGRAM

PROBLEM	CORRECTIVE ACTION
Windows does not auto-detect the ALLSPOT.	Make sure the ALLSPOT power switch is turned off and properly inserted into the USB port and then restart your computer.
	Perform a hardware scan by clicking Start, Settings, Control Panel and then double-click Add/Remove Hardware . (Steps may vary depending on Windows version). Follow the on-screen instructions to search for the ALLSPOT (Wireless 802.11 USB Network Adapter) and install the driver.
	Check for possible hardware conflicts. In Windows, click Start, Settings, Control Panel, System, Hardware and then click Device Manager . Verify the status of the ALLSPOT (Wireless 802.11 USB Network Adapter) under Network Adapter . (Steps may vary depending on the Windows version).
	Install the ALLSPOT in another computer. If the error persists, there may be a hardware problem. In this case, please contact your local dealer for support.

PROBLEMS WITH THE LINK STATUS

PROBLEM	CORRECTIVE ACTION
The link quality and/or signal strength is poor all the time from the status bar.	Search and connect to another AP with a better link quality using the Site Survey screen. Change the channel used by your AP. Move your computer closer to the AP or the peer computer(s) within the transmission range. There may be too much radio interference (for example microwave or another AP using the same channel) around your wireless network. Relocate or reduce the radio interference.

PROBLEMS WITH SECURITY SETTINGS

"Disconnected" (meaning authentication failure) Shown in the Status Bar	Make sure your AP/Router has the same setting as your client adapter and follow AP/Router's security settings.
LED PWR and LINK are on but cannot receive or sending data and connect to network	Make sure your AP/Router has the same setting as your client adapter and follow AP/Router's security settings.

Problems Communicating With Other Computers

PROBLEM	CORRECTIVE ACTION
The ALLSPOT computer cannot communicate with the other computer.	Make sure you are connected to the network.

Infrastructure	<p>Make sure that the AP and the associated computers are turned on and working properly.</p> <p>Make sure the ALLSPOT computer and the associated AP use the same SSID.</p> <p>Change the AP and the associated wireless clients to use another radio channel if interference is high.</p> <p>Make sure that the computer and the AP share the same security option and key. Verify the settings in the Profile Security Settings screen.</p>
Ad-Hoc (IBSS)	<p>Verify that the peer computer(s) is turned on.</p> <p>Make sure the ALLSPOT computer and the peer computer(s) are using the same SSID and channel.</p> <p>Make sure that the computer and the peer computer(s) share the same security option and key.</p> <p>Change the wireless clients to use another radio channel if interference is high.</p>

Specifications

KEY FEATURES

1. Compact, light weight size with friendly user interface.
2. Function Hotspot Finder and high performance USB 2.0 Wi-Fi Adapter in an enclosure.
3. Support LCD screen with complete site survey information: Signal Strength, Security & Encryption, Operation Channel, Radio Band, and SSID.
4. Support up to 300 times continuous scanning.
5. Support 2.4GHz & 5GHz dual-band, 802.11b/g and 802.11a worldwide radio standard.
6. Support enhanced wireless security WEP, WPA, WPA-PSK, and WPA2.
7. Built-in rechargeable battery with auto-charging through USB host port.

WI-FI RADIO:

	802.11 b	802.11 g	802.11 a (ALLSPOT)
Frequency	2.412~2.484 GHz	2.412~2.484 GHz	4.920~5.825 GHz
Modulation	DBPSK, DQPSK, CCK (DSSS)	OFDM with BPSK, SPSK, 16/64 QAM sub-carrier	OFDM with BPSK, SPSK, 16/64 QAM sub-carrier
Data Rate	11, 5.5, 2, 1 Mbps	54, 48, 36, 24, 18, 12, 9, 6 Mbps	54, 48, 36, 24, 18, 12, 9, 6 Mbps
Output Power (Typical)	18 dBm @ 11 Mbps	15 dBm @ 54 Mbps	13 dBm @ 54 Mbps
Receiving Sensitivity (Typical)	-87 dBm @ 11 Mbps	-72 dBm @ 54 Mbps	-71 dBm @ 54 Mbps

HAREWARE

- Host interface: USB 2.0 high speed device port
- One LCD screen
- Two LED indications
- One power switch
- Two push buttons: SCAN, NEXT
- One rechargeable battery: 180 mAh
- Power Consumption: 470 mA (max.)

SOFTWARE:

- Support Windows XP, 2K, ME & 98SE driver
- Support Windows-based Wireless LAN monitor utility
- Compatible with Windows Zero Configuration
- Supports 64-bit, 128-bit, 256-bit WEP (Manual type-in & Passphrase)
- Supports WPA-PSK, WPA, WPA2-PSK, and WPA2
- Supports EAP-TLS, and EAP-PEAP authentication