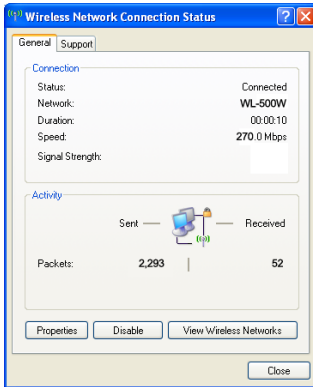
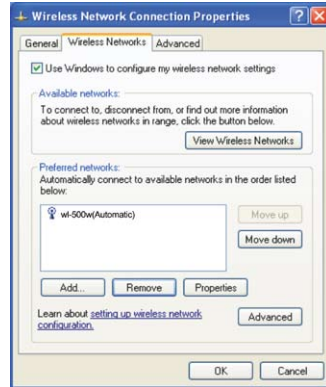


Chapter 3 - Software Reference

To set up the wireless connection properties, right-click the wireless icon on the taskbar and select **Open Network Connection**. Then right-click the network connection icon and select **Property** to open the Wireless Network Connection Status page.



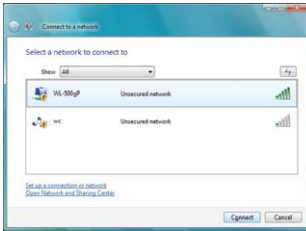
1. The **General** page shows status, duration, speed, and signal strength. The green bars represent signal strength, with 5 bars indicating excellent signal and 1 bar meaning poor signal.



2. Select "Wireless Networks" tab to show **Preferred networks**. Use the **Add** button to add the "SSID" of available networks and set the connection preference order with the **Move up** and **Move down** buttons. The radio tower with a signal icon identifies the currently connected access point. Click **Properties** to set the authentication of the wireless connection.

Windows® Vista Wireless Options

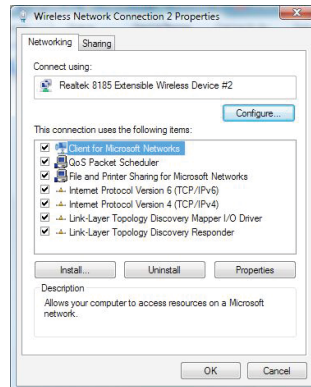
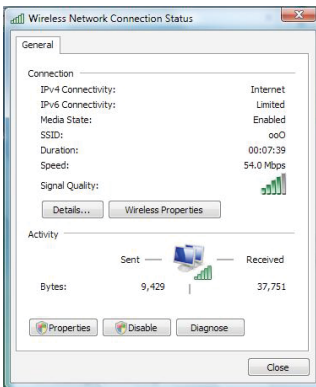
If you want to configure your WLAN Adapter via Windows® Wireless Client service, follow the instruction below to make the settings.



1. Right-click the network icon on the task bar at the right bottom corner of the desktop. Then select **Connect to a network** to view available networks. Select the AP and click **Connect**.
2. A window prompts out asking you for the key if you have set up encryption on your wireless router, input the keys and click **Connect**. The connection is complete.

To set up the wireless connection properties,

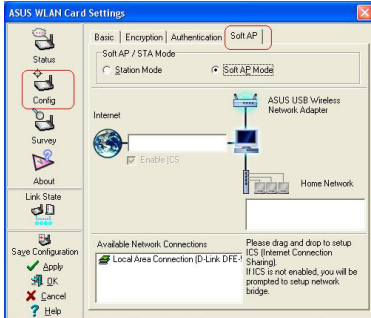
1. Right-click the network icon on the taskbar and select **Network and sharing Center**.
2. Select **Manage network connections** from the prompt window.
- 3 Double click the wireless network connection icon to open the Wireless Network Connection Status page.
- 4 Click **Properties** to open the Property page from the Wireless Network Connection Status page.



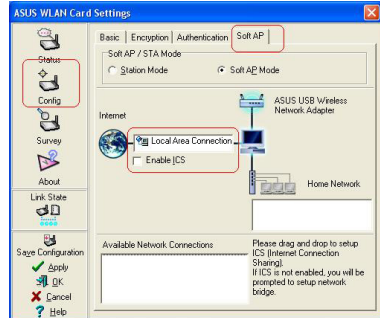
1. The General page shows status,SSID, duration, speed, and signal strength. The green bars represent signal strength, with 5 bars indicating excellent signal and 1 bar meaning poor signal.
2. Click **Properties** from the Property page to set the authentication of the wireless connection, . .

Soft AP (Windows XP Only)

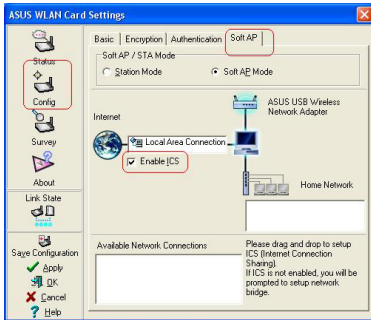
Soft AP mode allows the Wireless LAN card to act as a virtual access point. The computer needs to be connected to a wired network using an Ethernet connection in order to provide network access to Wireless LAN clients.



1. Select Soft AP Mode



2. Drag and drop a wired network connection next to the globe icon.



3. Enable ICS* and Firewall as desired. Refer to Windows help for information on "Internet Connection Sharing".



4. You can easily switch between Soft AP and Station mode by right clicking the taskbar icon and selecting "A-S Change Mode".

*ICS is used to share this computer's Internet connection with the rest of the computers on your network. When this computer is connected to the Internet, communication to and from the Internet to all the computers on your network are sent through this computer, called the host computer. Other computers can send and receive email and access the Web as if it were connected directly to the Internet.

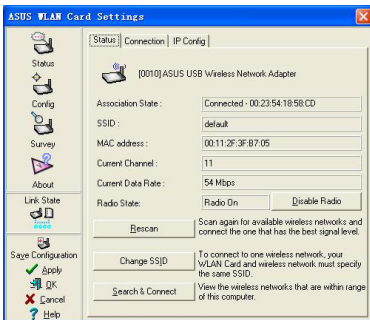
Soft AP (Windows XP Only) Cont.

Soft AP mode allows you to configure Access Control settings.

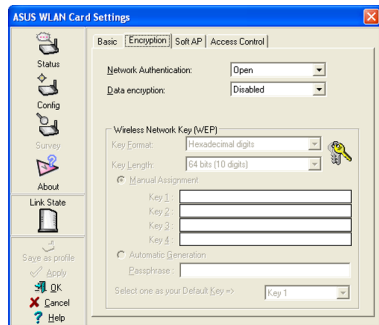
Access Control

The AP provides facilities to limit the wireless clients that associate with it and the data packets that can forward through it. Filters provide network security or improve performance by eliminating broadcast/multicast packets from the radio network.

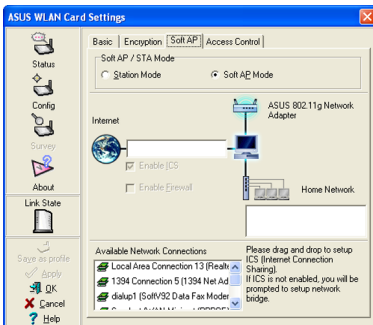
The Access Control List (ACL) contains MAC addresses for wireless clients allowed to associate with the AP. This provides security by preventing unauthorized access. The AP also uses a disallowed address list of destinations. This feature prevents the AP from communicating with specified destinations. This can include network devices that do not require communication with the AP or its wireless clients.



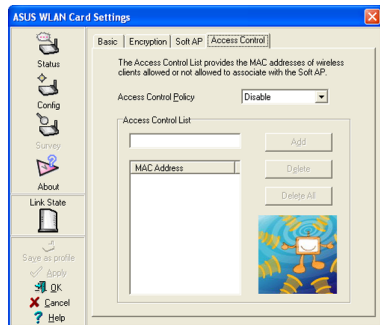
Status Page



Encryption Page

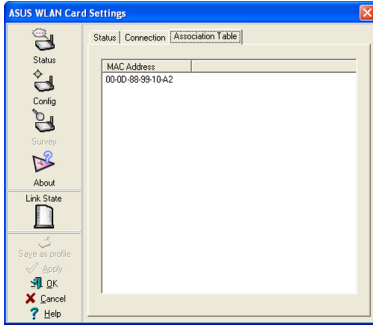


Clicking Apply after configuring Soft AP will show the "Access Control" tab.

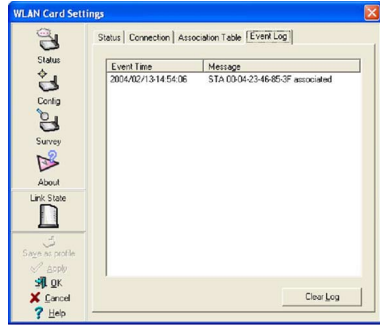


Enter a MAC Address on the Access Control page and select "Accept" or "Reject" or "Disable" from the pull-down menu.

Soft AP (Windows XP Only) Cont.



Soft AP Mode will also provide two extra tabs on the Status pages - Association Table and Event Log. The Association Table shows clients that are currently connected to the Soft AP.



The Event Log tracks messages associated with the Soft AP.

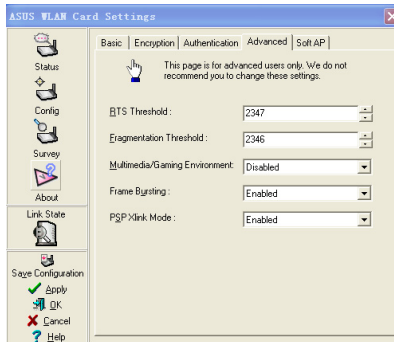


IMPORTANT: If the end points of a chain are connected to each other a loop is created. Normally it is advised to avoid loops involving bridges as it can lead to performance breakdowns, and broadcast and multicast storms.

XLink Mode configuration

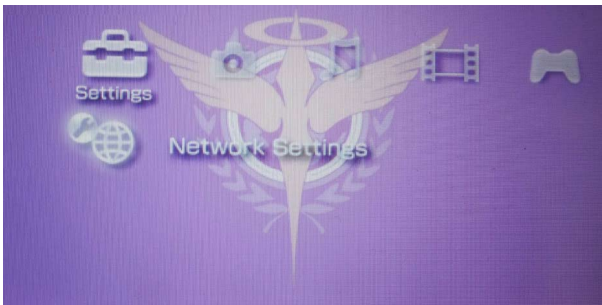
Set up under Windows XP:

Click **ASUS WLAN Control Center > Config > Advanced** to enable the PSP Xlink Mode.

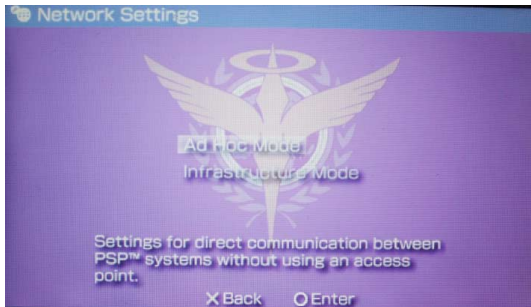


Turn on PSP to set up the configuration.

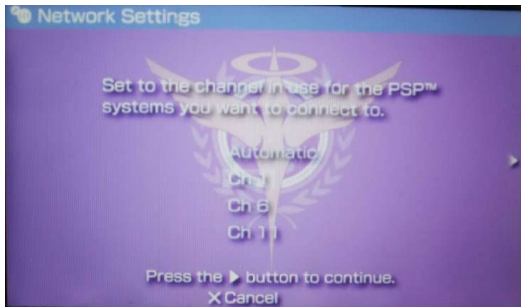
Select **Network Settings**.



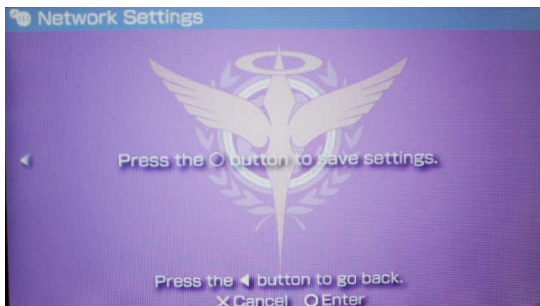
Select **AD Hoc Mode**.



Select the PSP channel connection.



When done, select **O** to save settings.

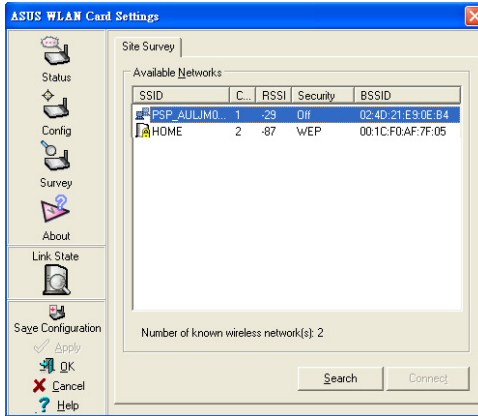


Chapter 4 - Software

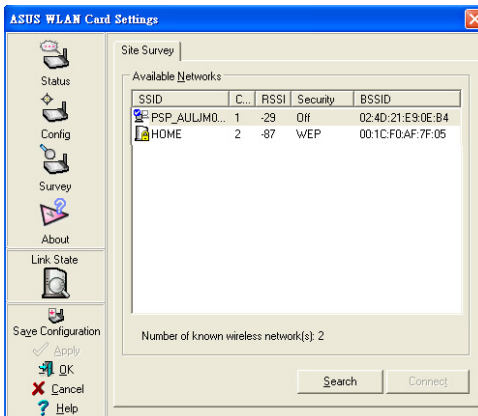
Select the game you want to play then select the connection type. The PSP can provide you the SSID named **PSP_****** to connect.

Click ASUS WLAN control center > survey to search the available connection.

Select PSP_**** to connect.



When done, click **Connect**.



Set up under MAC OS:

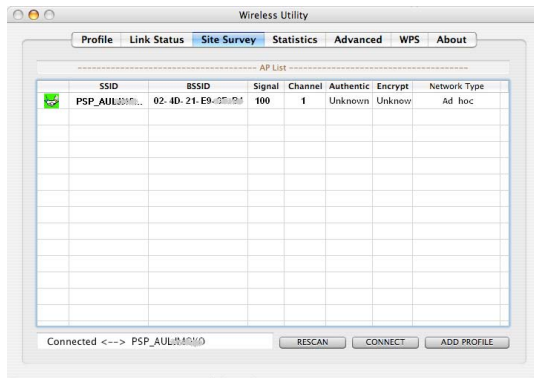
Select **USBWirelessUtility > Advanced** to enable PSP Xlink.



Click **USBWirelessUtility > Site survey** to search the available connection.

Select **PSP_****** to connect.

When done, click **connect**



5. Troubleshooting

The following troubleshooting guides provide answers to some of the more common problems, which you may encounter while installing or using WLAN Adapter products. If you encounter difficulties that are not mentioned in this section, please contact the Wireless LAN Technical Support.

Verify if the WLAN Adapter is installed correctly.

When the WLAN Adapter setup is complete, you can verify if the driver has been setup properly. Right click **My Computer**, select **Properties**, and click the **Device Manager** tab. Then double-click the **Network adapters** icon; you should see “**802.11g Network Adapter**” with an icon of an expansion adapter. There should not be a “!” or “?” (problem) or “x” (disabled) symbol over this icon.

There is a yellow exclamation mark or a yellow question mark in Device Manager in front of my WLAN Adapter.

To resolve the problem, you should update/reinstall the WLAN Adapter driver. In “Device Manager”, right click **802.11g Network Adapter**, select **Properties**, and select **Driver** tab. Click on **Update Driver** button, then follow the “Update Device Driver Wizard” to complete the driver installation.

Cannot connect to any access points

Follow the procedure below to configure your WLAN Adapter.

- a. Verify that the “Network Type” is in “Infrastructure” mode.
- b. Verify that the “SSID” of your WLAN Adapter is set to the same “SSID” of an access point.
- c. Verify that the “Encryption” type is the same as that of an access point. If you enabled “WEP” encryption, you must also set the same WEP Keys on both sides.

Cannot connect to a Station (WLAN Adapter)

Follow the procedure below to configure your WLAN Adapter.

- a. Verify that the “Network Type” is in “Ad Hoc” mode.
- b. Verify that the “SSID” of your WLAN Adapter is set to the same “SSID” of the other station (or another WLAN Adapter).
- c. Verify that the “channel” of the WLAN Adapter is “Auto” or set to the same “channel” of the other station (or another WLAN Adapter).
- d. Verify that the “Encryption” type is the same as the other station (or another WLAN Adapter). If “WEP” encryption is enabled, you must set the same “WEP” Keys on both stations.

Bad link quality or bad signal strength

There are two possible reasons. First is radio interference, keep the environment around the WLAN Adapter away from microwave ovens and large metal objects. Then try to reorient the WLAN Adapter antenna. Second is the distance, decrease the distance between your WLAN Adapter and the access point or station (or another WLAN Adapter).

The TCP/IP protocol did not bind to the WLAN PC Adapter.

This will occur when the computer already has six TCP/IP bindings in Windows 98 or ten bindings in Windows Me. These limits are imposed by the Microsoft operating system.

Solution: If your computer already has the maximum number of TCP/IP bindings, remove one of the network adapters from the Network configuration before installing the WLAN Adapter driver.

6. Glossary

Access Point (AP)

A networking device that seamlessly connects wired and wireless networks. Access points combined with a distributed system support the creation of multiple radio cells that enable roaming throughout a facility.

Ad Hoc

A wireless network composed solely of stations within mutual communication range of each other (no access point).

Basic Rate Set

This option allows you to specify the data transmission rate.

Basic Service Area (BSS)

A set of stations controlled by a single coordination function.

Broadband

A type of data transmission in which a single medium (such as cable) carries several channels of data at once.

Channel

An instance of medium use for the purpose of passing protocol data units that may be used simultaneously, in the same volume of space, with other instances of medium use (on other channels) by other instances of the same physical layer, with an acceptably low frame error ratio due to mutual interference.

Client

A client is the desktop or mobile PC that is connected to your network.

COFDM (for 802.11a or 802.11g)

Signal power alone is not enough to maintain 802.11b-like distances in an 802.11a/g environment. To compensate, a new physical-layer encoding technology was designed that departs from the traditional direct-sequence technology being deployed today. This technology is called COFDM (coded OFDM). COFDM was developed specifically for indoor wireless use and offers performance much superior to that of spread-spectrum solutions. COFDM works by breaking one high-speed data carrier into several lower-speed subcarriers, which are then transmitted in parallel. Each high-speed carrier is 20 MHz wide and is broken up into 52 subchannels, each approximately 300 KHz wide. COFDM uses 48 of these subchannels for data, while the remaining four are used for error correction. COFDM delivers higher data rates and a high degree of multipath reflection recovery, thanks to its encoding scheme and error correction.

Each subchannel in the COFDM implementation is about 300 KHz wide. At the low end of the speed gradient, BPSK (binary phase shift keying) is used to encode 125 Kbps of data per channel, resulting in a 6,000-Kbps, or 6 Mbps, data rate. Using quadrature phase shift keying, you can double the amount of data encoded to 250 Kbps per channel, yielding a 12-Mbps data rate. And by using 16-level quadrature amplitude modulation encoding 4 bits per hertz, you can achieve a data rate of 24 Mbps. The 802.11a/g standard specifies that all 802.11a/g-compliant products must support these basic data rates. The standard also lets the vendor extend the modulation scheme beyond 24 Mbps. Remember, the more bits per cycle (hertz) that are encoded, the more susceptible the signal will be to interference and fading, and ultimately, the shorter the range, unless power output is increased.

Default Key

This option allows you to select the default WEP key. This option allows you to use WEP keys without having to remember or write them down. The WEP keys generated using the Passphrase is compatible with other WLAN products. The Passphrase option is not as secure as manual assignment.

Device Name

Also known as DHCP client ID or network name. Sometimes provided by an ISP when using DHCP to assign addresses.

DHCP (Dynamic Host Configuration Protocol)

This protocol allows a computer (or many computers on your network) to be automatically assigned a single IP address from a DHCP server.

DNS Server Address (Domain Name System)

DNS allows Internet host computers to have a domain name and one or more IP addresses. A DNS server keeps a database of host computers and their respective domain names and IP addresses, so that when a user enters a domain name into the Internet browser, the user is sent to the proper IP address. The DNS server address used by the computers on your home network is the location of the DNS server your ISP has assigned.

DSL Modem (Digital Subscriber Line)

A DSL modem uses your existing phone lines to transmit data at high speeds.

Direct-Sequence Spread Spectrum (for 802.11b)

Spread spectrum (broadband) uses a narrowband signal to spread the transmission over a segment of the radio frequency band or spectrum. Direct-sequence is a spread spectrum technique where the transmitted signal is spread over a particular frequency range.

Chapter 6 - Glossary

Direct-sequence systems communicate by continuously transmitting a redundant pattern of bits called a chipping sequence. Each bit of transmitted data is mapped into chips and rearranged into a pseudorandom spreading code to form the chipping sequence. The chipping sequence is combined with a transmitted data stream to produce the output signal.

Wireless mobile clients receiving a direct-sequence transmission use the spreading code to map the chips within the chipping sequence back into bits to recreate the original data transmitted by the wireless device. Intercepting and decoding a direct-sequence transmission requires a predefined algorithm to associate the spreading code used by the transmitting wireless device to the receiving wireless mobile client.

This algorithm is established by IEEE 802.11b specifications. The bit redundancy within the chipping sequence enables the receiving wireless mobile client to recreate the original data pattern, even if bits in the chipping sequence are corrupted by interference. The ratio of chips per bit is called the spreading ratio. A high spreading ratio increases the resistance of the signal to interference. A low spreading ratio increases the bandwidth available to the user. The wireless device uses a constant chip rate of 11Mchips/s for all data rates, but uses different modulation schemes to encode more bits per chip at the higher data rates. The wireless device is capable of an 11 Mbps data transmission rate, but the coverage area is less than a 1 or 2 Mbps wireless device since coverage area decreases as bandwidth increases.

Encryption

This provides wireless data transmissions with a level of security. This option allows you to specify a 64-bit or a 128-bit WEP key. A 64-bit encryption contains 10 hexadecimal digits or 5 ASCII characters. A 128-bit encryption contains 26 hexadecimal digits or 13 ASCII characters.

64-bit and 40-bit WEP keys use the same encryption method and can interoperate on wireless networks. This lower level of WEP encryption uses a 40-bit (10 hexadecimal digits assigned by the user) secret key and a 24-bit Initialization Vector assigned by the device. 104-bit and 128-bit WEP keys use the same encryption method.

All wireless clients in a network must have identical WEP keys with the access point to establish connection. Keep a record of the WEP encryption keys.

Extended Service Set (ESS)

A set of one or more interconnected basic service set (BSS) and integrated local area networks (LANs) can be configured as an Extended Service Set.

ESSID (Extended Service Set Identifier)

You must have the same ESSID entered into the gateway and each of its wireless clients. The ESSID is a unique identifier for your wireless network.

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 10Mbps using CSMA/CD to run over 10-BaseT cables.

Firewall

A firewall determines which information passes in and out of a network. NAT can create a natural firewall by hiding a local network's IP addresses from the Internet. A Firewall prevents anyone outside of your network from accessing your computer and possibly damaging or viewing your files.

Gateway

A network point that manages all the data traffic of your network, as well as to the Internet and connects one network to another.

IEEE

The Institute of Electrical and Electronics Engineers. The IEEE sets standards for networking, including Ethernet LANs. IEEE standards ensure interoperability between systems of the same type.

IEEE 802.11

IEEE 802.xx is a set of specifications for LANs from the Institute of Electrical and Electronic Engineers (IEEE). Most wired networks conform to 802.3, the specification for CSMA/CD based Ethernet networks or 802.5, the specification for token ring networks. 802.11 defines the standard for wireless LANs encompassing three incompatible (non-interoperable) technologies: Frequency Hopping Spread Spectrum (FHSS), Direct Sequence Spread Spectrum (DSSS), and Infrared. 802.11 specifies a carrier sense media access control and physical layer specifications for 1 and 2 Mbps wireless LANs.

IEEE 802.11a (54Mbps/sec)

Compared with 802.11b: The 802.11b standard was designed to operate in the 2.4-GHz ISM (Industrial, Scientific and Medical) band using direct-sequence spread-spectrum technology. The 802.11a standard, on the other hand, was designed to operate in the more recently allocated 5-GHz UNII (Unlicensed National Information Infrastructure) band. And unlike 802.11b, the 802.11a standard departs from the traditional spread-spectrum technology, instead using a frequency division multiplexing scheme that's intended to be friendlier to office environments.

The 802.11a standard, which supports data rates of up to 54 Mbps, is the Fast Ethernet analog to 802.11b, which supports data rates of up to 11 Mbps. Like Ethernet and Fast Ethernet, 802.11b and 802.11a use an identical MAC (Media Access Control). However, while Fast Ethernet uses the same physical-layer encoding scheme as Ethernet (only faster), 802.11a uses an entirely different encoding scheme, called OFDM (orthogonal frequency division multiplexing).

Chapter 6 - Glossary

The 802.11b spectrum is plagued by saturation from wireless phones, microwave ovens and other emerging wireless technologies, such as Bluetooth. In contrast, 802.11a spectrum is relatively free of interference.

The 802.11a standard gains some of its performance from the higher frequencies at which it operates. The laws of information theory tie frequency, radiated power and distance together in an inverse relationship. Thus, moving up to the 5-GHz spectrum from 2.4 GHz will lead to shorter distances, given the same radiated power and encoding scheme.

Compared with 802.11g: 802.11a is a standard for access points and radio NICs that is ahead of 802.11g in the market by about six months. 802.11a operates in the 5GHz frequency band with twelve separate non-overlapping channels. As a result, you can have up to twelve access points set to different channels in the same area without them interfering with each other. This makes access point channel assignment much easier and significantly increases the throughput the wireless LAN can deliver within a given area. In addition, RF interference is much less likely because of the less-crowded 5 GHz band.

IEEE 802.11b (11Mbps/sec)

In 1997, the Institute of Electrical and Electronics Engineers (IEEE) adopted the 802.11 standard for wireless devices operating in the 2.4 GHz frequency band. This standard includes provisions for three radio technologies: direct sequence spread spectrum, frequency hopping spread spectrum, and infrared. Devices that comply with the 802.11 standard operate at a data rate of either 1 or 2 Mbps.

In 1999, the IEEE created the 802.11b standard. 802.11b is essentially identical to the 802.11 standard except 802.11b provides for data rates of up to 11 Mbps for direct sequence spread spectrum devices. Under 802.11b, direct sequence devices can operate at 11 Mbps, 5.5 Mbps, 2 Mbps, or 1 Mbps. This provides interoperability with existing 802.11 direct sequence devices that operate only at 2 Mbps.

Direct sequence spread spectrum devices spread a radio signal over a range of frequencies. The IEEE 802.11b specification allocates the 2.4 GHz frequency band into 14 overlapping operating Channels. Each Channel corresponds to a different set of frequencies.

IEEE 802.11g

802.11g is a new extension to 802.11b (used in majority of wireless LANs today) that broadens 802.11b's data rates to 54 Mbps within the 2.4 GHz band using OFDM (orthogonal frequency division multiplexing) technology. 802.11g allows backward compatibility with 802.11b devices but only at 11 Mbps or lower, depending on the range and presence of obstructions.

Infrastructure

A wireless network centered about an access point. In this environment, the access point not only provides communication with the wired network but also mediates wireless network traffic in the immediate neighborhood.

IP (Internet Protocol)

The TCP/IP standard protocol that defines the IP datagram as the unit of information passed across an Internet and provides the basis for connectionless packet delivery service. IP includes the ICMP control and error message protocol as an integral part. It provides the functional equivalent of ISO OSI Network Services.

IP Address

An IP address is a 32-bit number that identifies each sender or 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 an identifier of the particular device (which can be a server or a workstation) within that network.

ISM Bands (Industrial, Scientific, and Medicine Bands)

Radio frequency bands that the Federal Communications Commission (FCC) authorized for wireless LANs. The ISM bands are located at 902 MHz, 2.400 GHz, and 5.7 GHz.

ISP (Internet Service Provider)

An organization that provides access to the Internet. Small ISPs provide service via modem and ISDN while the larger ones also offer private line hookups (T1, fractional T1, etc.).

LAN (Local Area Network)

A communications network that serves users within a defined geographical area. The benefits include the sharing of Internet access, files and equipment like printers and storage devices. Special network cabling (10 Base-T) is often used to connect the PCs together.

MAC Address (Media Access Control)

A MAC address is the hardware address of a device connected to a network.

NAT (Network Address Translation)

NAT masks a local network's group of IP addresses from the external network, allowing a local network of computers to share a single ISP account. This process allows all of the computers on your home network to use one IP address. This will enable access to the Internet from any computer on your home network without having to purchase more IP addresses from your ISP.

NIC (Network Interface Card)

A network adapter inserted into a computer so that the computer can be connected to a network. It is responsible for converting data from stored in the computer to the form transmitted or received.

Chapter 6 - Glossary

Packet

A basic message unit for communication across a network. A packet usually includes routing information, data, and sometimes error detection information.

Passphrase

The Wireless Settings utility uses an algorithm to generate four WEP keys based on the typed combination.

PPP (Point-to-Point Protocol)

PPP is a protocol for communication between computers using a serial interface, typically a personal computer connected by phone line to a server.

PPPoE (Point-to-Point Protocol over Ethernet)

Point-to-Point Protocol is a method of secure data transmission. PPP using Ethernet to connect to an ISP.

Preamble

Allows you to set the preamble mode for a network to Long, Short, or Auto. The default preamble mode is Long.

Radio Frequency (RF) Terms: GHz, MHz, Hz

The international unit for measuring frequency is Hertz (Hz), equivalent to the older unit of cycles per second. One megahertz (MHz) is one million Hertz. One gigahertz (GHz) is one billion Hertz. The standard US electrical power frequency is 60 Hz, the AM broadcast radio frequency band is 0.55-1.6 MHz, the FM broadcast radio frequency band is 88-108 MHz, and wireless 802.11 LANs operate at 2.4 GHz.

SSID (Service Set Identifier)

SSID is a group name shared by every member of a wireless network. Only client PCs with the same SSID are allowed to establish a connection. Enabling the **Response to Broadcast SSID requests** option allows the device to broadcast its SSID in a wireless network. This allows other wireless devices to scan and establish communication with the device. Unchecking this option hides the SSID to prevent other wireless devices from recognizing and connecting to the device.

Station

Any device containing IEEE 802.11 wireless medium access conformity.

Subnet Mask

A subnet mask is a set of four numbers configured like an IP address. It is used to create IP address numbers used only within a particular network.

TCP (Transmission Control Protocol)

The standard transport level protocol that provides the full duplex, stream service on which many application protocols depend. TCP allows a process or one machine to send a stream of data to a process on another. Software implementing TCP usually resides in the operating system and uses the IP to transmit information across the network.

WAN (Wide Area Network)

A system of LANs, connected together. A network that connects computers located in separate areas, (i.e., different buildings, cities, countries). The Internet is a wide area network.

WECA (Wireless Ethernet Compatibility Alliance)

An industry group that certifies cross-vender interoperability and compatibility of IEEE 802.11b wireless networking products and to promote that standard for enterprise, small business, and home environments.

WPA (Wi-Fi Protected Access)

Wi-Fi Protected Access (WPA) is an improved security system for 802.11. It is part of the 802.11i draft security standard. WPA encompasses TKIP (Temporal Key Integrity Protocol) along with MIC (Message Integrity Check) and other fixes to WEP such as Weak IV (Initialization Vector) filtering and Random IV generation. TKIP uses 802.1x to deploy and change temporary keys as opposed to static WEP keys once used in the past. It is a significant improvement over WEP. WPA is part of a complete security solution. WPA also requires authentication servers in enterprise security solutions.

Requirements

(1) A WPA compatible access point or Wireless router, (2) Operating system updates that support WPA. In XP, an updated Windows Zero Config service is needed. Users can download the Windows XP WPA patch here:

<http://microsoft.com/downloads/details.aspx?FamilyId=009D8425-CE2B-47A4-ABEC-274845DC9E91&displaylang=en>

Please note that this patch requires the installation Windows XP Service Pack 1, which is available here: <http://www.microsoft.com/WindowsXP/pro/downloads/servicepacks/sp1/default.asp>

For earlier Windows Operating systems, a WPA capable supplicant is required such as Funk Software's Odyssey Client.

WLAN (Wireless Local Area Network)

This is a group of computers and other devices connected wirelessly in a small area. A wireless network is referred to as LAN or WLAN.

7. Appendix



FCC Warning 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.

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.



CAUTION:

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

Prohibition of Co-location

This device and its antenna(s) must not be co-located or operating in conjunction with any other antenna or transmitter

Declaration of Conformity for R&TTE directive 1999/5/EC

Essential requirements – Article 3

Testing for electric safety according to EN 60950-1 has been conducted. These are considered relevant and sufficient.

Protection requirements for electromagnetic compatibility – Article 3.1b

Testing for electromagnetic compatibility according to EN 301 489-1 and EN 301 489-17 has been conducted. These are considered relevant and sufficient.

Effective use of the radio spectrum – Article 3.2

Testing for radio test suites according to EN 300 328- 2 has been conducted. These are considered relevant and sufficient.

CE Mark 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.

REACH

Complying with the REACH (Registration, Evaluation, Authorisation, and Restriction of Chemicals) regulatory framework, we published the chemical substances in our products at ASUS REACH website at <http://green.asus.com/english/REACH.htm>.

Chapter 7 - Appendix

FCC statement:

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 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 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 Caution: Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this 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.

IMPORTANT NOTE:

Radiation Exposure Statement:

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. End users must follow the specific operating instructions for satisfying RF exposure compliance. To maintain compliance with FCC RF exposure compliance requirements, please follow operation instruction as documented in this manual.

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

Industry Canada statement:

This device complies with RSS-210 of the Industry Canada 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.

IMPORTANT NOTE:

Radiation Exposure Statement:

This equipment complies with IC radiation exposure limits set forth for an uncontrolled environment. End users must follow the specific operating instructions for satisfying RF exposure compliance. To maintain compliance with IC RF exposure compliance requirements, please follow operation instruction as documented in this manual.