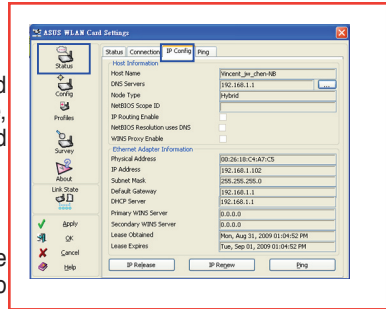


Status - IP Config

IP Config tab shows all the current host and Network adapter information including host name, DNS servers, IP address, Subnet Mask and Default Gateway.

Button

- **IP Release:** If you want to remove the current IP address, click this button to release the IP address from DHCP server.
- **IP Renew:** If you want to obtain a new IP address from DHCP server, click this button to renew the IP address.
- **Ping:** Click this button to open “Ping” tab which is used to ping the devices in your network.



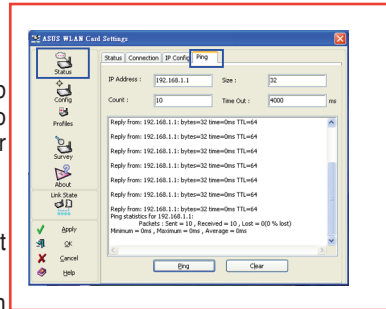
Note: The IP Release and IP Renew buttons can only be used on the Network adapter which gets IP address from DHCP server.

Status - Ping

Click the **Ping** button in Status-IP Config tab to open this page. The Ping tab allows you to verify the accessibility of other computers or network devices.

To ping a connection:

1. Type the IP address of the device you want to verify in the IP Address field.
2. To configure the ping session, assign the ping packet size and number of packet to send, and the timeout value (in milliseconds).
3. Click **Ping**.



During the ping session, the Ping button Changes into a Stop button. To cancel the ping session, click the **Stop** button.

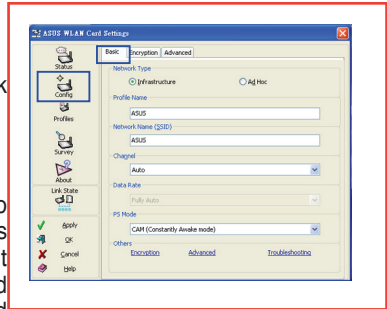
The session field displays information on the verified connection including the roundtrip time (minimum, maximum, and average) and packets sent, received, and lost after a ping session. Click the **Clear** button to clear the session field.

Config - Basic

This page enables you to change the Network adapter configurations.

Network Type

- **Infrastructure:** Infrastructure means to establish a connection with an access point. Once connected, the access point allows you to access wireless LAN and wired LAN (Ethernet). The Channel field turns to **Auto** if the connection is based on Infrastructure.
- **Ad Hoc:** Ad Hoc means to communicate directly with other wireless clients without using an access point. An “Ad Hoc” network can be setup quickly and easily without pre-planning, for example, sharing meeting notes between attendants in a meeting room.



Network Name (SSID)

SSID stands for Service Set Identifier, which is a string used to identify a wireless LAN. Use the SSID to connect with a known access point. You can enter a new SSID or select one from the drop-down list box. If you get connected by designating the SSID, you are only to connect the AP with the SSID you assigned. If the AP is removed from the network, your Network adapter does not roam automatically to other APs. SSIDs must all be printable characters and having a maximum of 32 case sensitive characters, such as “Wireless”.

Channel

The Channel field is for setting radio channel. Your Network adapter can automatically select the correct channel to communicate with a wireless device, and the parameter is fixed to "Auto" in both Infrastructure and Ad Hoc mode.

The available radio channels depend on the regulations in your country. For the United States (FCC) and Canada (IC), channel 1 to 11 are supported. For Europe (ETSI), channel 1 to 13 are supported. For Japan (MCK), channel 1 to 14 are supported.



Note: Click Apply to save and activate the new configurations.

PS Mode

Constantly Awake Mode (CAM), also known as Disable Power Saving Mode, is a full powered state that yields the best performance. We recommend this mode for devices running on AC power.

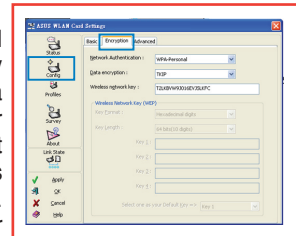
Power Saving Polling Mode (PSP Mode), which is also known as Enable Power Saving mode, periodically wakes up the system to check if there is any data being sent. We recommend this mode for devices running on battery power.

Others

- **Encryption:** Click this link to show the "Encryption" tab.
- **Advanced:** Click this link to show the "Advanced" tab. In most cases, the default values do not have to be changed.

Config - Encryption

This page enables you to configure the Wireless LAN Adapter encryption settings. For data confidentiality in a wireless environment, IEEE 802.11 specifies a Wired Equivalent Privacy (WEP) algorithm to offer transmission privacy. The WEP uses keys to encrypt and decrypt data packets. The encryption process can scramble frame bits to avoid disclosure to others. The WPA/WPA2 is improved security system for 802.11 which are developed to overcome the weakness of the WEP protocol.



Network Authentication

Since there is no precise bound in wireless LANs, the WLAN users need to implement certain mechanism to provide security solution. The Authentication policies in this tab provide protection of different levels such as Open, Shared, WPA-PSK, WPA, WPA2 and WPA2-PSK.

- **Open:** Select this option to make the network operate on Open System mode, which use no authentication algorithm. Open stations and APs can authenticate with each other without checking any WEP Key, even if there is.

- **Shared:** Select this option to make the network operate on Shared key mode. In a Share Key Authentication system, four-step exchange of frames is required to validate that the station is using the same WEP Key as the access point.
- **WPA-PSK/ WPA2-PSK:** Select this option to enable WPA Pre-Shared Key under Infrastructure mode. It enables communication between your client and APs using WPA-PSK/WPA2-PSK encryption mode.
- **WPA/ WPA2:** The network is operating in IEEE 802.1x authentication mode. This mode is for environments with RADIUS (Remote Access Dial-in User Service). In a RADIUS environment, five Extensible Authentication Protocol (EAP) are supported, including PEAP, TLS/Smart Card, TTLS, LEAP and Md5-Challenge.

Data encryption

For Open and Shared authentication mode, the configuration options of encryption type are Disabled and WEP. For WPA, WPA-PSK, WPA2 and WPA2-PSK authentication mode, Temporal Key Integrity Protocol (TKIP) encryption and Advanced Encryption Standard (AES) encryption are supported.

- **Disabled:** Disable the encryption function.
- **WEP:** WEP Key is used to encrypt your data before it is transmitted over air. You can only connect and communicate with wireless devices that use the same WEP keys.
- **TKIP:** TKIP uses an encryption algorithm method that is more stringent than the WEP algorithm. It also uses existing WLAN calculation facilities to perform encryption. TKIP verifies the security configuration after the encryption keys are determined.
- **AES:** AES is a symmetric 128-bit block encryption technique that works simultaneously on multiple network layers.

Wireless Network Key

This option is enabled only if you select WPA-PSK or WPA2-PSK authentication mode. Select “TKIP” or “AES” in the encryption field as encryption mode to begin the encryption proceed. Note: 8 to 64 characters are required in this field.

Wireless Network Key (WEP)

This option is configurable only if you enable WEP in Network Authentication field. The WEP Key is a 64 bits (5 byte) or 128 bits (13 byte) Hexadecimal digits which is used to encrypt and decrypt data packets.

Key Format

You can select to enter Hexadecimal digits (0~9, a~f, and A~F) or ASCII characters to setup keys by defining the Key Format.

Key Length

For 64 bits encryption, each key contains 10 hex digits or 5 ASCII characters. For 128 bits encryption, each key contains 26 hex digits or 13 ASCII characters.

- **Manual assign WEP keys** - When you select this option, the cursor appears in the field for Key 1. For 64-bit encryption, you are required to enter four WEP Keys. Each Key contains exactly 10 hex digits (0~9, a~f, and A~F). For 128-bit encryption, you are required to enter four WEP Keys. Each Key contains exactly 26 hex digits (0~9, a~f, and A~F).

Select one as your Default Key

The Default Key field allows you specify which of the four encryption keys is to use for transmitting data over wireless LAN. You can change the default key by clicking on the downward arrow, selecting the number of the key you want to use, and clicking the “Apply” button. If the access point or station with which you are communicating uses the identical key by the same sequence, you can use any of the keys as the default on your WLAN Adapter.

Click the “Apply” button after you have created the encryption keys, the Wireless Settings Utility uses asterisks to mask your keys.

64/128bits versus 40/104bits

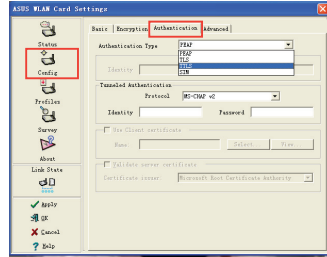
There are two levels of WEP Encryption: 64 bits and 128 bits.

Firstly, 64 bit WEP and 40 bit WEP are the same encryption method and can interoperate in the wireless network. This lower level of WEP encryption uses a 40 bit (10 Hex character) as a “secret key” (set by user), and a 24 bit “Initialization Vector” (not under user control). This together makes 64 bits (40 + 24). Some vendors refer to this level of WEP as 40 bits and others refer to this as 64 bits. Our Wireless LAN products use the term 64 bits when referring to this lower level of encryption.

Secondly, 104 bit WEP and 128 bit WEP are the same encryption method and can interoperate in the wireless network. This higher level of WEP encryption uses a 104 bit (26 Hex character) as a “secret key” (set by user), and a 24 bit “Initialization Vector” (not under user control). This together makes 128 bits (104 + 24). Some vendors refer to this level of WEP as 104 bits and others refer to this as 128 bits. Our Wireless LAN products use the term 128 bits when referring to this higher level of encryption.

Config - Authentication

This tab allows you to set the security settings to match those of your AP. It is configurable only if you have set Network Authentication to WPA or WPA2 in Config-Encryption tab.



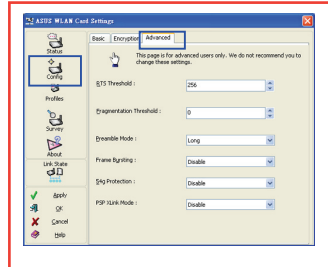
Authentication Type

The authentication type methods include:

- **PEAP:** PEAP (Protected Extensible Authentication Protocol) authentication is a version of Extensible Authentication Protocol (EAP). EAP ensures mutual authentication between a wireless client and a server that resides at the network operations center.
- **TLS:** TLS (Transport Layer Security) authentication is used to create an encrypted tunnel and achieve server-side authentication in a manner similar to Web server authentication using Secure Sockets Layer (SSL) protocol. This method uses digital certificates to verify the identity of a client and server.
- **TTLS:** TTLS authentication uses certificates to authenticate the server, while maintaining similar security properties to TLS such as mutual authentication and a shared confidentiality for session WEP key.

Config - Advanced

Click **Advanced** link on Config-Basic page to show this tab. This tab allows you to set up additional parameters for the wireless Adapter. We recommend using the default values for all items in this window.



RTS Threshold (0-2347)

The RTS/CTS (Request to Send/Clear to Send) function is used to minimize collisions among wireless stations. When RTS/CTS is enabled, the router refrains from sending a data frame until another RTS/CTS handshake is completed. Enable RTS/CTS by setting a specific packet size threshold. The default value (2347) is recommended.

Fragmentation Threshold (256-2346)

Fragmentation is used to divide 802.11 frames into smaller pieces (fragments) that are sent separately to the destination. Enable fragmentation by setting a specific packet size threshold. If there is an excessive number of collisions on the WLAN, experiment with different fragmentation values to increase the reliability of frame transmissions. The default value (2346) is recommended for normal use.

Frame Bursting

Frame Bursting technology improves wireless network efficiency and boosts throughput.

Preamble Mode

54g Protection

PSP Xlink mode

Allows you to PSP system-linked game over the Internet.



Note: For more details, refer to the section **Setting up the XLink Mode** in this user manual. You may also visit the XLink Kai website at www.teamxlink.co.uk.

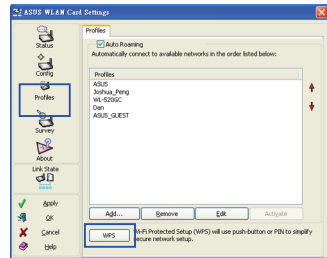
Profiles

This tab allows you to set up the Wi-Fi Protected Setup (WPS) and configure the auto roaming and profile list.

Wi-Fi Protected Setup (WPS)

To set up WPS:

- Click **WPS** from the Profiles page to launch the WPS Wizard.

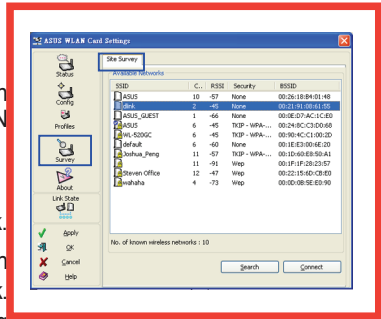


Note: For more details on using WPS, refer to the section **Using the WPS Wizard** in this user manual.

Survey - Site Survey

Use the Site Survey tab to view statistics on the wireless networks available to the WLAN adapter and their parameters.

- **SSID:** The SSID of the available networks.
- **Channel:** The channel used by each network.
- **RSSI:** The Received Signal Strength Indication (RSSI) transmitted by each network. This information is helpful in determining which network to connect to. The value is then normalized to a dBm value.
- **Security:** Wireless network encryption information. All devices in the network should use the same encryption method to ensure the communication.
- **BSSID:** The media access control (MAC) address of the access point or the Basic Service Set ID of the Ad Hoc mode.

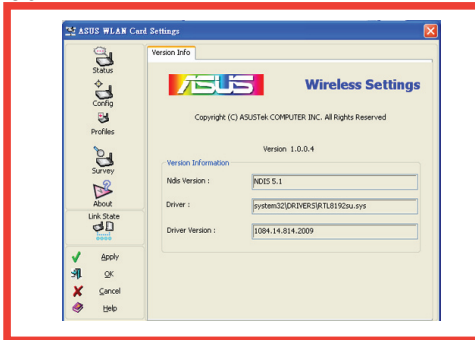


Note: Some access points may disable SSID broadcast and hide themselves from “Site Survey” or “Site Monitor”, however, you can connect such AP if you know their SSID.

- **Search:** To scan all available wireless networks and show the scan result in the “Available Network” list.
- **Connect:** To associate with a network, select the network from the “Available Network” list and click this button.

About - Version Info






Use the Version Info tab to view program and WLAN Adapter version information. The program version information field includes the Copyright and utility version. The version information includes the NDIS version, driver name, driver version and hardware version.

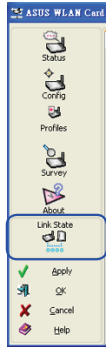


Note: The screen shown above is for reference only.

Link State

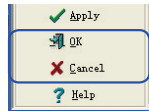
WLAN Adapter “Link State” icon appears on the left side of the WLAN Adapter Settings. Use the icon to view the current signal status.

-  Excellent Link Quality (Infrastructure)
-  Good Link Quality (Infrastructure)
-  Fair Link Quality (Infrastructure)
-  Poor Link Quality (Infrastructure)
-  Not linked (Infrastructure)



Exit Wireless Settings

To exit Wireless Settings, you can click **OK** or **Cancel**.



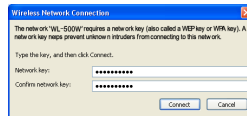
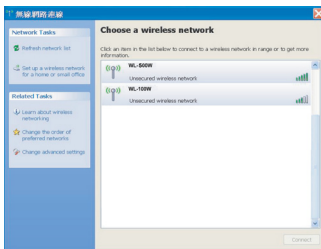
Windows® XP Wireless options

The wireless options window shown below is only available for Windows® XP. It appears when you run the Control Center utility at the first time. Select the utility you want to use for configuring your WLAN Adapter.

- **Only use Windows wireless function**
Only use Windows® XP Wireless Zero Configuration service to configure the WLAN Adapter.
- **Only use our WLAN utilities and disable Windows wireless function**
Only use ASUS WLAN utilities to configure the WLAN Adapter.

Configuring with Windows® Wireless Zero Configuration service

If you want to configure your WLAN Adapter via Windows® Wireless Zero Configuration (WZC) service, follow the instruction below to make the settings.



1. Double-click the wireless network icon on the task bar at the right bottom corner of the desktop 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.