Security Monitor Account

The *Security Monitor Account* screen provides you with the function to create and modify your Security Monitor account. The Security Monitor account gives access to the administrative functions of the Wireless Network Monitor.

Enter the administrator's **username** and **password** and retype the password in the confirm field. Click **Next** to proceed with more administrative options.

The username and password for the Security Monitor administrator account do not need to be the same as the Access Point's administrator account.

You can select an account from the drop-down menu to create or modify the username and password. There are a total of five accounts available. Click **Save** to save your existing changes.

Figure 5-49: Administration - Security Monitor Account

Chapter 6: The Administrative Functions in the Wireless Network Monitor

When used with the WAP200 Access Point, you can use the administration functions in the Wireless Network Monitor to classify your wireless networks into different groups and monitor the activities and resources within your networks. The following functions under **Classification** and **Security Monitor** screens are only enabled after an administrator or privileged user enters a valid username and password.

Figure 6-1: Wireless Network Monitor Icon

Accessing the Wireless Network Monitor

After installing the Adapter, the Wireless Network Monitor icon will appear in the system tray of your computer. If the Wireless Network Monitor is enabled, then the icon will be green. If the Wireless Network Monitor is disabled or the Adapter is not connected, then the icon will be gray.

Using the Administrative Functions in the Wireless Network Monitor

The Administration tab will give you access to the administrative tasks of the account information and other functions, such as classification and monitoring of your wireless networks. The Classification and Security Monitor functions will be provided after logging in to the Security Monitor account on the Administration screen. To configure trusted and untrusted wireless networks, click the **Classification** tab**.** To view the summarized report of the monitored wireless activities and alert messages, click the **Security Monitor**.

Figure 6-2: Administration - Login Security Monitor
Administration - Login Security Monitor Account

Figure 6-3: Classification

NOTE: You must associate with a WAP200 Access Point to be able to log in to the Security Monitor.
NOTE: You will need to log in with a valid Security Monitor account to view the screens in this chapter.

Classification

The *Classification* tab displays a summary of classified devices. The Classification Summary table shows the number of access points and clients classified as trusted and untrusted by MAC addresses in your networks. It also shows the number of allowed vendors, SSIDs, and channels.

You may uncheck the **Receive classification rules** to disable a client from receiving the network's current classification rules. The default condition is checked, so each client always receives classification rules in synchronization with other clients in the network. You may also click the **Synchronize** button to send out the classification rules to other users within your monitored wireless networks.

Click **Next** to configure your trusted networks.

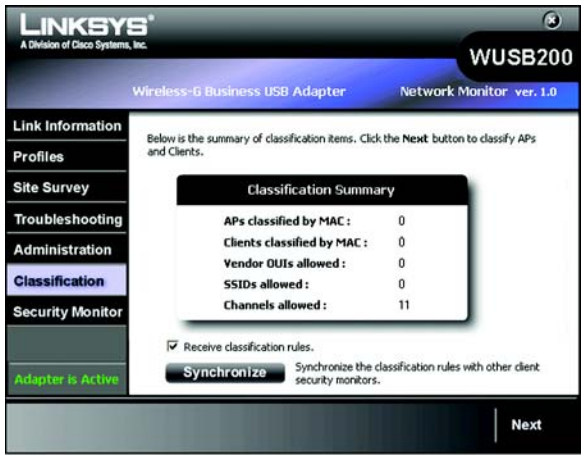


Figure 6-4: AP Classification

NOTE: Classification rules: access points and clients can be classified as trusted or untrusted, and access points can be additionally classified by MAC address, SSID, vendor, or channel.

AP Classification

The *AP Classification* Screen lets you classify the existing access points as trusted or untrusted. A Trusted device is one that has been identified by the system administrator to be known and legitimate. An untrusted device is one that is known and not legitimate. This device could be a malicious device or simply a neighborhood device not part of the network. Remaining devices that have not been classified are considered unclassified or unknown.

The Unclassified Access Points table lists the available unclassified wireless access points with their SSIDs, channels and MAC Addresses. The top right table lists the *Trusted Access Points*. The lower right table lists the *Untrusted Access Points*.

You may select any items from the *Unclassified Access Points* table and click the arrow to classify your selections into *Trusted Access Points* or *Untrusted Access Points*. You may also select any items from the *Trusted Access Points* or *Untrusted Access Points* and click the arrow to de-classify your selections into the*Unclassified Access Points* table.

Click **Refresh** to refresh the list, **Clear** to clear selected items on the list, or click **Back** to go to the previous screen.

Click **AP Classification**, **Client Classification**, or **Advanced Settings** to go to that screen.

Figure 6-5: Client Classification

Client Classification

The *Client Classification* Screen lets you classify the existing wireless clients into trusted networks and untrusted networks. New client information is received from Linksys Business Series access points. New clients start off as Unclassified until the System Administrator classifies them. A Trusted Client is one that has been identified by the System Administrator to be known and legitimate. An Untrusted Client is one that is known and not legitimate; this client could be a malicious client or simply a neighborhood client not part of the network. Remaining clients that have not been classified can be considered as unclassified or unknown.

The left table lists the available unclassified clients with their associated Access Point's SSID. The top right table lists the clients that have been classified as **Trusted**. The lower right table lists the clients that have been classified as **Untrusted.**

You may select any items from the *Unclassified Clients* table and click the arrow to classify your selections into **Trusted Clients** or **Untrusted Clients**. You may also select any items from the **Trusted Clients** or **Untrusted Clients** and click the arrow to de-classify your selections into the*Unclassified Clients* table.

You may click **Refresh** to refresh the list, **Clear** to clear selected items on the list, or **Back** to go to the previous screen.

You may click **AP Classification**, **Client Classification**, or **Advanced Settings** to go to that screen.

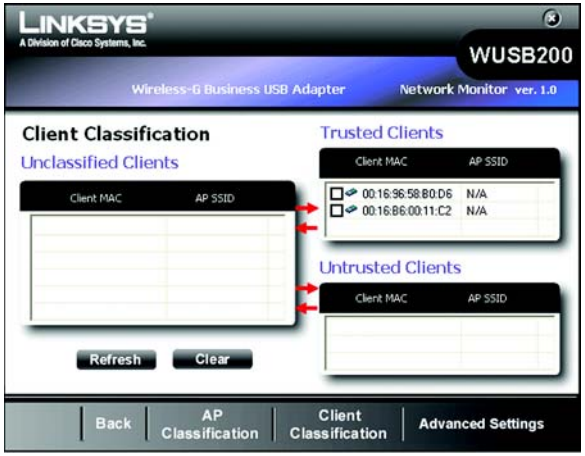


Figure 6-6: Trusted Mac Address

Advanced Settings

Click **Advanced Settings** for classifying your wireless networks by **Mac (**Address), **Vendor**, **SSID** and **Channel**. Click the **MAC** tab to configure the trusted MAC addresses, **Vendor** to configure the trusted AP vendor list, **SSID** to configure the trusted SSID list, **Channel** to configure the trusted channel, or **Back** to go to the previous screen.

Trusted MAC Addresses

Clicking the **MAC** button displays the *Trusted MAC Addresses* screen, which provides information and function for configuring the existing wireless networks as trusted networks with MAC Access control of the access points and the clients. The Trusted AP's MAC Addresess that you enter on this screen will also appear on the *AP Classification* screen as a trusted access point.

The tables list the entry of MAC addresses of your trusted and allowed wireless access points and clients.

Enter the 12-digit hexadecimal numbers in the field and click **Add** to add the entry. To delete an entry, select it, then click **Delete**.

Figure 6-7: Allowed SSID Configuration

Allowed Vendor List Configuration

The Allowed Vendor List Configuration table lists the OUI (Organization Unique Identification) and vendor name of your trusted and allowed AP Vendor OUIs. A OUI is the three-octet (first 6 digits) used to generate LAN MAC Addresses for hardware manufacturers. To delete an item, select it, and click **delete**. The latest vendor OUI lists are available at **http://standards.ieee.org/regauth/oui/index.shtml**.

Vendor Name - This is the name of your desired vendor. Select a vendor's name from the drop-down list and click **Add** to add the vendor.

Vendor OUI - If the vendor OUI is not listed, you may enter the company's OUI and click **Add** to enter your vendor's OUI in the list.

APs from vendors not on the allowed vendor list will be automatically classified as untrusted. A blank list indicates that all vendor OUIs are allowed for AP classification.

Figure 6-8: Allowed Vendor List Configuration

Allowed SSID Configuration

The Allowed SSID Configuration table shows the SSIDs of the allowed APs on your network. APs from SSIDs not on this list will be automatically classified as untrusted. A blank list indicates that all SSIDs are allowed for classification.

SSID - This is the unique name of the wireless network. It is a 32-character unique identifier attached to the header of packets sent over a WLAN.

You may enter the **SSID** of a trusted and allowed wireless network in the field and click **Add** to add it into your list. You may select an item and click **Delete** to delete it from the list.

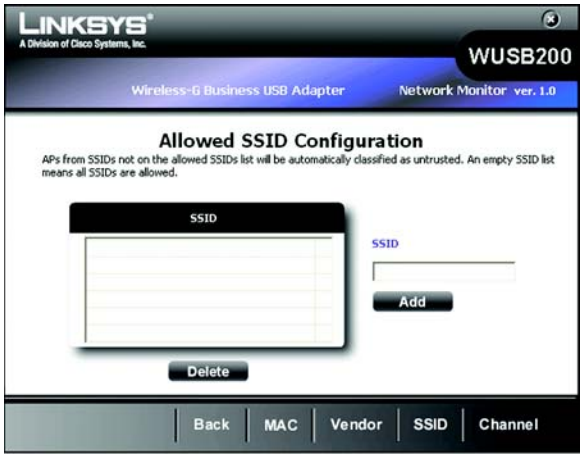


Figure 6-9: Allowed SSID Configuration

Allowed Channel Configuration

The *Allowed Channel Configuration screen* shows the channels that are allowed to be used in your wireless networks. You may select individual channels or click **Check All** to check all of the channels. Unclassified access points on unchecked channels will be automatically classified as untrusted.

Figure 6-10: Allowed Channel Configuration

Security Monitor

IMPORTANT: You must use a WAP200 Access Point with your USB Network Adapter to use the Security Monitor.

The Security Monitor helps to make your network more secure. It monitors the airspace through the WAP200 Access Point and USB Network Adapter for security related issues like vulnerabilities in the network configuration, which allows you to act quickly to solve issues and secure your network. The Monitor runs on the client PC, which allows the administrator to perform initial setup on security profiles and classification on the wireless network devices and later view assorted security alerts.

The *Security Monitor* tab displays the statistics of your wireless network and alerts you of network activity by Channel Usage, AP Inventory, Client Inventory, or Alerts.

Click **Channel Usage, AP Inventory** to view the statistics of the distribution on your AP's classifications, **Client Inventory** to view the distribution of the client's classifications on your wireless networks, or **Alert** to monitor that function.

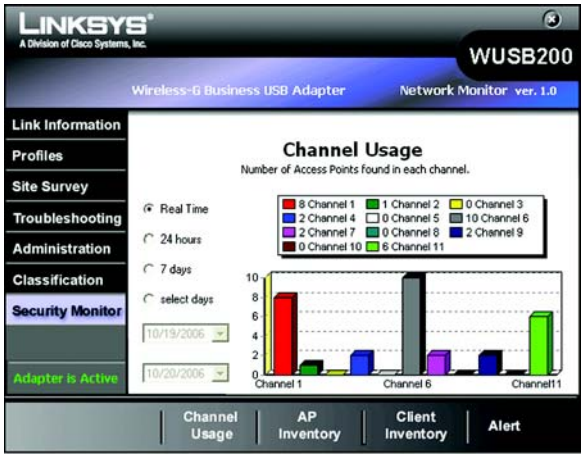


Figure 6-11: Security Monitor - Channel Usage

Channel Usage

The *Channel Usage* screen provides statistics of the distribution on your channel's usages. The histogram shows the number of access points in each channel, so unclassified access points can be detected. Select the specified period of time you want for the data calculations. You may select **Real Time** for current data, **24 hours** for data within the last 24 hours, **7 days** for data within the last 7 days or **select days** for a range of days.

AP Inventory

The *AP Inventory* screen provides statistics of the distribution grouped by your AP's classification of your wireless networks. The pie chart shows the percentage of each classification type, so you can easily view the number of trusted, untrusted, and unknown APs in the airspace. Select the specified period of time you want for the data calculations. You may select **Real Time** for current data, **24 hours** for data within the last 24 hours, **7 days** for data within the last 7 days or **select days** for a range of days.

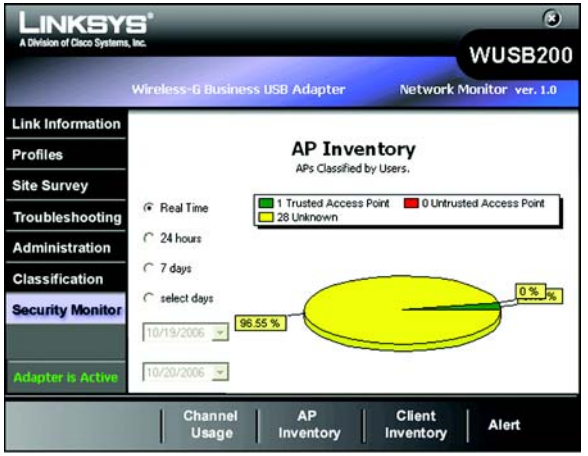


Figure 6-12: Security Monitor - AP Inventory

Client Inventory

The *Client Inventory* screen provides statistics of trusted, untrusted, and unknown clients. The pie chart shows the percentage of each wireless client's classification, so you can easily view the number of trusted, untrusted, and unknown clients in the airspace. Select the specified period of time you want for the data calculations. You may select **Real Time** for current data, **24 hours** for data within the last 24 hours, **7 days** for data within the last 7 days or **select days** for a range of days.

Figure 6-13: Security Monitor - Client Inventory

Alert

Overview

Both the WAP200 Access Point and client USB Network Adapter monitor the state of your wireless network and report on security related issues, ranging from on-going attacks down to vulnerabilities in the network configuration.

The Access Point does most of the security monitoring work while the client USB Network Adapter can detect new and rogue access points. The management software runs on the client PC, which allows the system administrator to perform initial setup on security profiles and classification on the wireless network devices.

When a client USB Network Adapter detects an unknown access point, it will notify its associated Access Point. The Access Points synchronize security alerts with each other and send the alert to the administrator.

Once the administrator is alerted with the security alarm, he or one of his five authorized users can log in to the Security Monitor to retrieve the Alert Log from the Access Point.

There are four categories of policy violation rules listed under *Alert Type*: Intrusion Alarms: unauthorized connection or hacking attack taking place on the network, Denial of Service Alarms: denial of service attack detected on the network, Vulnerability Alarms: potential threat to the security of the network, and Others. Each represents a different kind of threat to the wireless network, ranging from poor performance to unauthorized users connected to the network. A violation will be listed under *Amount*. You can click Retrieve Alert log to view the *Alert List*. When *Detail* is clicked, the *Details* screen appears with more detailed information of the event, then you can click *Advice* to view the suggested advice for the event.

Alerts Summary

The *Alerts Summary* screen lists the alert types, amount of alerts, and available details.

Detail - Click the **Detail** button to view more detailed information for each event.

Receive Alert logs - Select this to receive alert logs from access points.

Retrieve Alert log - Click this button to view an alert log.

Enable Pop-up - Select this to allow this client to receive a pop-up warning message when a new access point or client is detected.

Click **Back** to go to the previous screen.

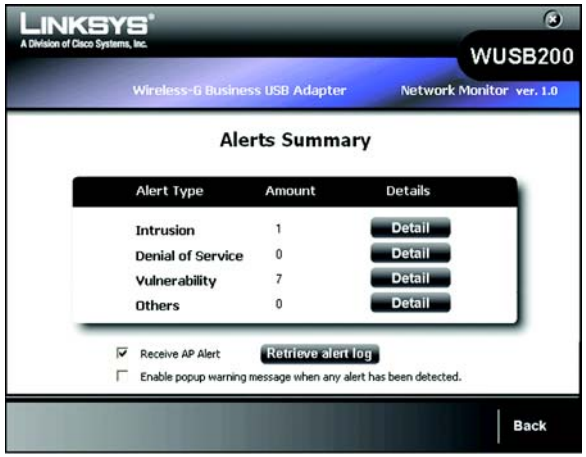


Figure 6-14: Security Monitor - Alerts Summary

Figure 6-15: Security Monitor - POP-UP Alert

NOTE: You will be alerted when an Access Point is detected, if you enable popup.

Alert List

The *Alert List* screen shows the list of the alert activities within your monitored wireless networks.

SSID - This shows the SSID (network name) of your wireless network.

MAC - This shows the MAC Address of the wireless client or access point that was detected.

Alert Description - This shows brief descriptions of the alert activities. The alert system will alert you when new access points or wireless clients are detected, or if other policy violations or attacks are detected.

Date/Time - This indicates the date/time that an alert activity happened.

Delete - Select an item, then click this button to delete the item.

Click **Back** to go to the previous screen or **Exit** to go to the main menu.

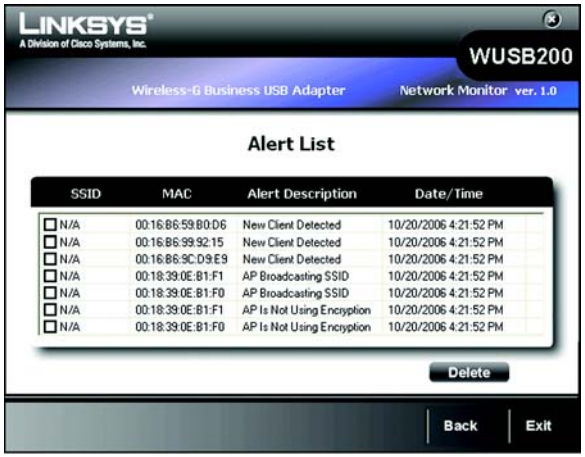


Figure 6-16: Security Monitor - Alert List

Alert Details

The *Details* screen shows the detailed message of each alert event.

Message - This indicates the description of the event.

MAC Address - This shows the MAC Address of the wireless client or Access Point that performed the action.

Severity - This shows the level of the security severity of the action.

Type - This show the type of the networking activity that was performed.

Date/Time - This shows the Date/Time of the alert.

Description - This shows the detailed description of the event.

You may click the **Advice** button to view the advice message, **Back** to go back to the previous screen, or **Exit** to go back to the main menu.

Figure 6-17: Alert Details

Advice

The *Advice* screen gives advice, when applicable, on what can be done for each alert event. You may need to adjust your wireless network settings according to the advice to better protect your networks.

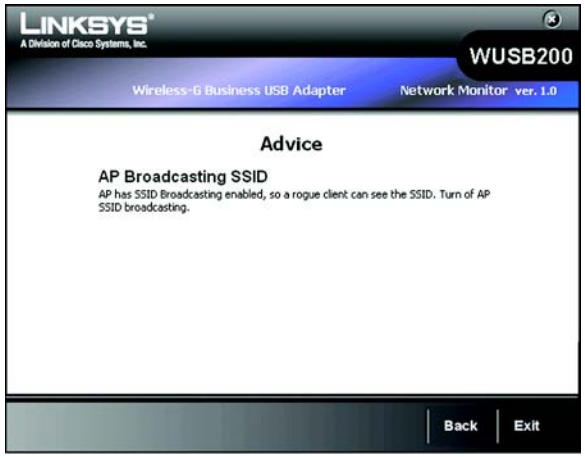


Figure 6-18: Security Monitor - Alert Advice

The following table is a summary of the various alert descriptions and advice.

Table 1: Alerts

Item	Alert	Description	Advice
1	Rogue Client Detected	A Rogue Client is detected. For details, press the Advice button.	Description: Rogue Client is detected doing one or more illegal actions, e.g., causing Message Integrity Check (MIC) errors, sending disassociation frames, sending deauthentication frames, and sending association frames with incorrect encryption. Rogue Client computer information: MAC:__-__-__-__-__-__ MIC error generation: The MIC function prevents attacks on encrypted packets. During an attack, an intruder intercepts an encrypted (WPA - Personal) message, alters it slightly, and retransmits it, and the receiver accepts the retransmitted message as legitimate. This action will cause a MIC error. If an attacker causes two MIC errors within 60 seconds, it will be considered a Rogue Client. Disassociation attacking: Occurs when a wireless station transmits a disassociation request to an AP which it is not associated with. De-authentication attacking: Occurs when a wireless station transmits a de-authentication request to an AP which it is not associated with. Authentication failure: Occurs when the AP receives an association request with different encryption from a wireless client. Action: 1. Contact the network administrator and send the administrator the Rogue Client computer information. 2. Change MAC access control list on the AP and further block the Rogue Client's activities.

Table 1: Alerts

Item	Alert	Description	Advice
2	AP SSID Changed	SSID on the AP has changed. For details, press the Advice button.	Description: AP's SSID was changed by an unknown source. This may be caused by a possible intruder if the AP's SSID was not changed by the administrator. Original SSID: Modified SSID: Action: 1. Contact the network administrator. 2. If an intruder is suspected, change administrator's password on the AP.
3	AP Channel Changed	AP's Channel has Changed. For details, press the Advice button.	Description: AP's Channel was changed by an unknown source. It could possibly be done by an intruder if it was not changed by the administrator or via auto channel selection. Original Channel: Modified Channel: Action: 1. Contact the network administrator and send the administrator the Login Information/history. 2. If an intruder is suspected, change the administrator's password on the AP.
4	Spoofed MAC Address	The AP's MAC Address has been spoofed by a wireless client. For details, press the Advice button.	Description: AP's MAC address has been spoofed by a wireless client. Client sends a frame with a MAC address which is the same as the AP's MAC address. By processing these packets, the AP may be subjected to heavy loading. Action: 1. No actions required. The AP will automatically drop these frames.

Table 1: Alerts

Item	Alert	Description	Advice
5	Client is Sending Spurious Traffic	Client not associated with AP is sending traffic. For details, press the Advice button.	Description: Client not associated with AP is sending traffic. Probable rogue client. The Client might be trying to make the network busy and causing heavy loading to the AP. MAC:__-__-__-__-__-__ Action: 1. Contact network administrator. 2. Add the Client MAC address to MAC Access Control List on AP Web Page.
6	Adhoc SSID is the same as the AP's	A wireless client using Adhoc structure has the same SSID as the AP's SSID. For details, press the Advice button.	Description: A wireless client using Adhoc structure has the same SSID as the AP's SSID. Illegitimate AP could use the same SSID to fool other wireless clients that it is a legitimate AP. Action: 1. Contact network administrator. 2. Try to physically locate the wireless client computers.
7	Duration Attack	Abnormally large duration for packets sent by client. For details, press the Advice button.	Description: Packets with abnormally large duration sent by a client may prevent other clients from sending packets to the AP. Client computer information: MAC:__-__-__-__-__-__ Action: 1. Try to physically locate the wireless client computer. 2. Add the Client's MAC address to MAC Access Control List on the AP.

Table 1: Alerts

Item	Alert	Description	Advice
8	Association Table Full	Possibly a Denial of Service Attack. For details, press the Advice button.	Description: A New client association request is refused due to a lack of memory. It could be an overloaded AP from being associated with too many legitimate clients or it could be a possible Denial of Service attack that will prevent legitimate clients from associating with the AP. Action: 1. AP will stop allowing more client association with the AP. 2. Check the AP's client's list to see if any wireless client is illegitimate.
9	AP Is Not Using Encryption	AP does not have any encryption method enabled. For details, press the Advice button.	Description: AP does not have any authentication method enabled, so it is vulnerable to network attacks or sniffing. Action: 1. Contact the network administrator. 2. In order to make the wireless network more secure, set up the AP with a stronger authentication method, e.g., WPA or WPA2.
10	AP Broadcasting SSID	AP has SSID Broadcasting enabled. For details, press the Advice button.	Description: AP has SSID Broadcasting enabled, so any wireless station can obtain its SSID. Action: 1. In order to avoid being attacked by rogue clients, turn off SSID broadcasting on the AP.
11	Default SSID in Use	AP is using the default SSID.For details, press the Advice button.	Description: AP is using the default SSID. Default SSIDs are easy to identify, so a hacker can effortlessly connect to the AP. Action: 1. In order to keep the connection secure, change the AP SSID to a non-default SSID.

Table 1: Alerts

Item	Alert	Description	Advice
12	Duplicate SSID in Use	Unclassified AP has the same SSID as a trusted AP. For details, press the Advice button.	Description: An unclassified AP has same SSID as the trusted AP. Action: 1. Contact the network administrator and inform the administrator about the untrusted AP's SSID and MAC address. 2. Check if the untrusted AP is legitimate. 3. Unclassified AP needs to be classified and the classification table needs to be updated.
13	New Access Point Detected	New AP is detected. For details, press the Advice button.	Description: New AP is detected. The new Access Point needs to be classified and the classification table needs to be updated. Action: 1. Contact the network administrator and inform the administrator about the new Access Point's SSID and MAC address. 2. Unclassified AP needs to be classified and the classification table needs to be updated.
14	Adhoc Network Operating	Clients are operating in Adhoc mode. For details, press the Advice button.	Description: Clients are operating in Adhoc mode, so network security could be compromised. Action: 1. Contact the network administrator and inform the administrator of the client's SSID and MAC address. 2. Try to physically locate the wireless client's computers.

Table 1: Alerts

Item	Alert	Description	Advice
15	New Client Detected	New client is detected. For details, press the Advice button.	Description: New wireless client computer is detected. Action: 1. Contact the network administrator and inform the administrator about the new client computer's SSID and MAC address. 2. The new Client needs to be classified and the classification table needs to be updated.
16	Low Speed Connection	Connection is at low speed. For details, press the Advice button.	Description: Data packets are being transferred at a very slow rate. Possible cause may be a poor signal reception due to some interference or the client is too far away from the AP. Action: 1. Check the environment and find possible causes for wireless signal interference, e.g., a microwave oven or a cordless telephone. 2. Check the MAC association table on the AP for any illegitimate wireless clients.
17	Rogue AP Detected	Rogue AP is detected. For details, press the Advice button.	Description: A Rogue AP is detected doing an illegal action. The AP is using the same SSID and encryption as the Trusted AP and is trying to crack the client computer's encryption key. During the decryption process, the AP has a 4-way handshake and if compromised, the client computer will detect a MIC error, indicating a Rogue AP. Action: 1. Contact network administrator. 2. Try to physically locate the Access Point.

Table 1: Alerts

Item	Alert	Description	Advice
18	Illegal Channel Usage	An Illegal Channel Usage is detected. For details, please press the Advice button.	Description: The client is using an illegal channel outside the range of channels permitted for use in the country. Action: 1. Contact the network administrator. 2. Change channel selection to a legal channel that is permitted for use in the country.

Windows Firewall

Windows XP users may see a Windows Firewall screen when using the security monitor.

IMPORTANT: DO NOT select **Don't allow exceptions** or the security monitor will not work correctly.

Select **On (recommended)** to use the firewall. Do not select the *Don't allow exceptions* or the Adapter's security monitor will not work properly. Then, click **OK**.

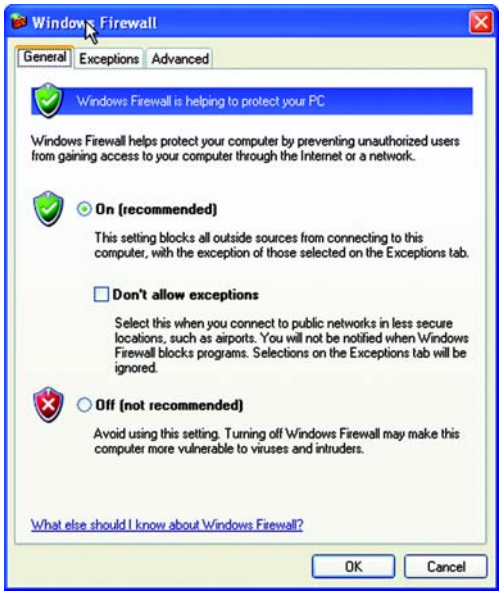


Figure 6-19: Security Monitor - Windows Firewall Screen

Appendix A: Troubleshooting

This appendix consists of two parts: "Common Problems and Solutions" and "Frequently Asked Questions." This appendix provides solutions to problems that may occur during the installation and operation of the Wireless-G Business USB Network Adapter. Read the description below to solve your problems. If you can't find an answer here, check the Linksys website at *www.linksys.com*.

Common Problems and Solutions

1. ***The Wireless-G Business USB Network Adapter does not work properly.***
   - Reinsert the USB cable connections.
   - Right click on My Computer and select Properties. Select the device manager and click on the Network Adapter. You will find the Wireless-G USB Network Adapter with RangeBooster if it is installed successfully. If you see the yellow exclamation mark, the resources are conflicting. You will see the status of the Wireless-G USB Network Adapter with RangeBooster. If there is a yellow question mark, please check the following:
   - Make sure that your PC has a free IRQ (Interrupt ReQuest, a hardware interrupt on a PC.)
   - Make sure that you have inserted the right adapter and installed the proper driver.

   If the Wireless-G Business USB Network Adapter does not function after attempting the above steps, remove the adapter and do the following:
   - Uninstall the driver software from your PC.
   - Restart your PC and repeat the hardware and software installation as specified in this User Guide.

2. ***I cannot communicate with the other computers linked via Ethernet in the Infrastructure configuration.***
   - Make sure that the PC to which the Wireless-G Business USB Network Adapter is associated and is powered on.
   - Make sure that your Wireless-G Business USB Network Adapter is configured on the same channel and with the same security options as with the other computers in the Infrastructure configuration.

Frequently Asked Questions

Can I run an application from a remote computer over the wireless network?
This will depend on whether or not the application is designed to be used over a network. Consult the application's user guide to determine if it supports operation over a network.

How will the Wireless networking technology help with my business?
Keeping your business connected in the internet and managing networking in your office without wires give you the freedom to create a dynamic office environment that changes and grows as your business needs. The Linksys Wirelees–N Business USB Network Adapter will not only let you communicate sensitive data in a wireless setting but also give you the security and management options within your monitored networks. We designed our wireless products to be simple to set up with the advances of the latest data encryption methods and Security Monitor functions. It is aimed to benefit your business from its full wireless networking while stayed protected.

What is the 802.11b standard?
It is one of the standards for wireless networks. The 802.11b standard allows wireless networking hardware from different manufacturers to communicate, provided that the hardware complies with the 802.11b standard. The 802.11b standard states a maximum data transfer rate of 11Mbps and an operating frequency of 2.4GHz.

What is the IEEE 802.11g standard?
It is one of the IEEE standards for wireless networks. The 802.11g standard allows wireless networking hardware from different manufacturers to communicate, provided that the hardware complies with the 802.11g standard. The 802.11g standard states a maximum data transfer rate of 54Mbps and an operating frequency of 2.4GHz.

What 802.11b features are supported?
The product supports the following 802.11b functions:

- CSMA/CA plus Acknowledge protocol
- Multi-Channel Roaming
- Automatic Rate Selection
- RTS/CTS feature
- Fragmentation
- Power Management

What IEEE 802.11g features are supported?
The product supports the following IEEE 802.11g functions:

- CSMA/CA plus Acknowledge protocol

- OFDM protocol
- Multi-Channel Roaming
- Automatic Rate Selection
- RTS/CTS feature
- Fragmentation
- Power Management

What is ad-hoc mode?
When a wireless network is set to ad-hoc mode, the wireless-equipped computers are configured to communicate directly with each other. This type of network will not communicate with any wired network.

What is infrastructure mode?
When a wireless network is set to infrastructure mode, the wireless network is configured to communicate with a wired network through a wireless access point.

What is roaming?
Roaming is the ability of a portable computer user to communicate continuously while moving freely throughout an area greater than that covered by a single access point. Before using the roaming function, the workstation must make sure that it is the same channel number with the access point of dedicated coverage area.

To achieve true seamless connectivity, the wireless LAN must incorporate a number of different functions. Each node and access point, for example, must always acknowledge receipt of each message. Each node must maintain contact with the wireless network even when not actually transmitting data. Achieving these functions simultaneously requires a dynamic RF networking technology that links access points and nodes. In such a system, the user's end node undertakes a search for the best possible access to the system. First, it evaluates such factors as signal strength and quality, as well as the message load currently being carried by each access point and the distance of each access point to the wired backbone. Based on that information, the node next selects the right access point and registers its address. Communications between end node and host computer can then be transmitted up and down the backbone.

As the user moves on, the end node's RF transmitter regularly checks the system to determine whether it is in touch with the original access point or whether it should seek a new one. When a node no longer receives acknowledgment from its original access point, it undertakes a new search. Upon finding a new access point, it then re-registers, and the communication process continues.

What is ISM band?
The FCC and their counterparts outside of the U.S. have set aside bandwidth for unlicensed use in the ISM (Industrial, Scientific and Medical) band. Spectrum in the vicinity of 2.4 GHz, in particular, is being made available

worldwide. This presents a truly revolutionary opportunity to place convenient high-speed wireless capabilities in the hands of users around the globe.

What is Spread Spectrum?

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

What is DSSS? What is FHSS? And what are their differences?

Frequency-Hopping Spread-Spectrum (FHSS) uses a narrowband carrier that changes frequency in a pattern that is known to both transmitter and receiver. Properly synchronized, the net effect is to maintain a single logical channel. To an unintended receiver, FHSS appears to be short-duration impulse noise. Direct-Sequence Spread-Spectrum (DSSS) generates a redundant bit pattern for each bit to be transmitted. This bit pattern is called a chip (or chipping code). The longer the chip, the greater the probability that the original data can be recovered. Even if one or more bits in the chip are damaged during transmission, statistical techniques embedded in the radio can recover the original data without the need for retransmission. To an unintended receiver, DSSS appears as low power wideband noise and is rejected (ignored) by most narrowband receivers.

What is WEP?

WEP is Wired Equivalent Privacy, a data privacy mechanism based on a shared key algorithm, as described in the 802.11 standard.

What is WPA?

WPA is Wi-Fi Protected Access, a wireless security protocol that can be used in conjunction with a RADIUS server.

What is RADIUS?

RADIUS is Remote Authentication Dial-In User Service, which uses an authentication server to control network access.

Appendix B: Windows XP Wireless Zero Configuration

Windows XP Wireless Zero Configuration

If your computer is running Windows XP, then this choice will be available. If you want to use Windows XP Wireless Zero Configuration to control the Adapter, instead of using the Wireless Network Monitor, then right-click on the Wireless Network Monitor and select **Use Windows XP Wireless Configuration**.

If you want to switch back to the Wireless Network Monitor, right-click the **Wireless Network Monitor** icon, and select **Use Linksys Wireless Network Monitor**.

Figure B-1: Wireless Network Monitor Icon

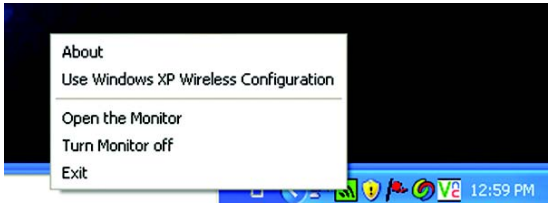


Figure B-2: Windows XP - Use Windows XP Wireless Configuration

1. After installing the Adapter, the Windows XP Wireless Zero Configuration icon will appear in your computer's system tray. Double-click the icon.

NOTE: For more information about Wireless Zero Configuration, refer to Windows Help.

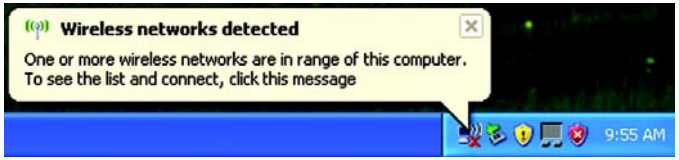


Figure B-3: Windows XP Wireless Zero Configuration Icon

2. The screen that appears will show any available wireless network. Select the network you want. Click the **Connect** button.

   If your network does not have wireless security enabled, go to step 3.

   If your network does have wireless security enabled, go to step 4.

NOTE: Steps 2 and 3 are the instructions and screenshots for Windows XP with Service Pack 2 installed.

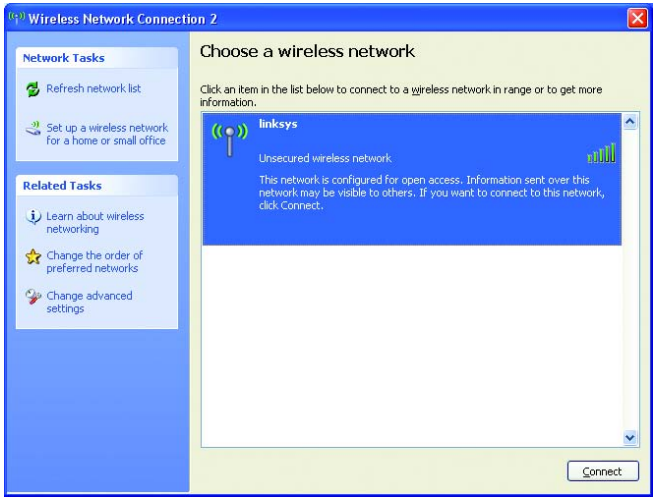


Figure B-4: Available Wireless Network

3. If your network does not have wireless security enabled, click the **Connect Anyway** button to connect the Adapter to your network.

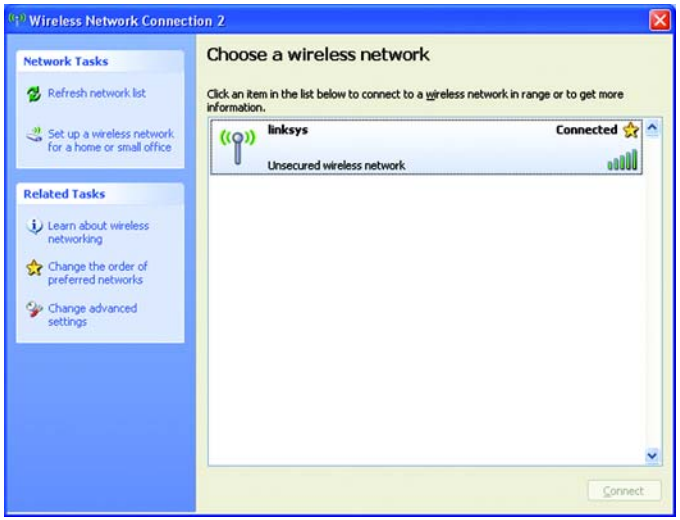
Figure B-5: No Wireless Security

4. If your network uses wireless security WEP, enter the WEP Key used into the *Network Key* and *Confirm network key* fields. If your network uses wireless security WPA Personal, enter the Passphrase used into the *Network Key* and *Confirm network key* fields. Click the **Connect** button.

Figure B-6: Network Connection - Wireless Security

NOTE: Windows XP Wireless Zero Configuration does not support the use of a passphrase. Enter the exact WEP key used by your access point.

5. Your wireless network will appear as Connected when your connection is active.



For more information about wireless networking on a Windows XP computer, click the **Start** button, select **Help**, and choose **Support**. Enter the keyword wireless in the field provided, and press the **Enter** key.

The installation of the Windows XP Wireless Configuration is complete.

Appendix C: Wireless Security

Linksys wants to make wireless networking as safe and easy for you as possible. The current generation of Linksys products provide several network security features, but they require specific action on your part for implementation. So, keep the following in mind whenever you are setting up or using your wireless network.

Security Precautions

The following is a complete list of security precautions to take (at least steps 1 through 5 should be followed):

1. Change the default SSID.
2. Disable SSID Broadcast.
3. Change the default password for the Administrator account.
4. Enable MAC Address Filtering.
5. Change the SSID periodically.
6. Use the highest encryption algorithm possible. Use WPA/WPA2 if it is available. Please note that this may reduce your network performance.
7. Change the WEP encryption keys periodically.

Note: Some of these security features are available only through the network router or access point. Refer to the router or access point's documentation for more information.

Security Threats Facing Wireless Networks

Wireless networks are easy to find. Hackers know that in order to join a wireless network, wireless networking products first listen for "beacon messages". These messages can be easily decrypted and contain much of the network's information, such as the network's SSID (Service Set Identifier). Here are the steps you can take:

Change the administrator's password regularly. With every wireless networking device you use, keep in mind that network settings (SSID, WEP keys, etc.) are stored in its firmware. Your network administrator is the only person who can change network settings. If a hacker gets a hold of the administrator's password, he, too, can change those settings. So, make it harder for a hacker to get that information. Change the administrator's password regularly.

SSID. There are several things to keep in mind about the SSID:

1. Disable Broadcast

2. Make it unique

3. Change it often

Most wireless networking devices will give you the option of broadcasting the SSID. While this option may be more convenient, it allows anyone to log into your wireless network. This includes hackers. So, don't broadcast the SSID.

Wireless networking products come with a default SSID set by the factory. (The Linksys default SSID is "linksys".) Hackers know these defaults and can check these against your network. Change your SSID to something unique and not something related to your company or the networking products you use.

Change your SSID regularly so that any hackers who have gained access to your wireless network will have to start from the beginning in trying to break in.

MAC Addresses. Enable MAC Address filtering. MAC Address filtering will allow you to provide access to only those wireless nodes with certain MAC Addresses. This makes it harder for a hacker to access your network with a random MAC Address.

WEP Encryption. Wired Equivalent Privacy (WEP) is often looked upon as a cure-all for wireless security concerns. This is overstating WEP's ability. Again, this can only provide enough security to make a hacker's job more difficult.

There are several ways that WEP can be maximized:

1. Use the highest level of encryption possible

2. Use "Shared Key" authentication

3. Change your WEP key regularly

WPA. Wi-Fi Protected Access (WPA) is the newest and best available standard in Wi-Fi security. Three modes are available: WPA-Personal, WPA Enterprise, and Radius. WPA-Personal gives you a choice of two encryption methods: TKIP (Temporal Key Integrity Protocol), which utilizes a stronger encryption method and incorporates Message Integrity Code (MIC) to provide protection against hackers, and AES (Advanced Encryption System), which utilizes a symmetric 128-Bit block data encryption. WPA Enterprise offers two encryption methods, TKIP and AES, with dynamic encryption keys. RADIUS (Remote Authentication Dial-In User Service) utilizes a RADIUS server for authentication.

Important: Always remember that each device in your wireless network MUST use the same encryption method and encryption key or your wireless network will not function properly.

WPA-Personal. If you do not have a RADIUS server, Select the type of algorithm, TKIP or AES, and enter a password in the Passphrase field of 8-63 characters.

WPA Enterprise. WPA used in coordination with a RADIUS server. (This should only be used when a RADIUS server is connected to the Router or other device.) WPA Enterprise offers two encryption methods, TKIP and AES, with dynamic encryption keys.

WPA2. WPA2 is a wireless security standard that defines stronger encryption, authentication and key management than WPA.

RADIUS. WEP used in coordination with a RADIUS server. (This should only be used when a RADIUS server is connected to the Router or other device.)

Implementing encryption may have a negative impact on your network's performance, but if you are transmitting sensitive data over your network, encryption should be used.

These security recommendations should help keep your mind at ease while you are enjoying the most flexible and convenient technology Linksys has to offer.

Appendix D: Windows Help

All wireless products require Microsoft Windows. Windows is the most used operating system in the world and comes with many features that help make networking easier. These features can be accessed through Windows Help and are described in this appendix.

TCP/IP

Before a computer can communicate with an access point or wireless router, TCP/IP must be enabled. TCP/IP is a set of instructions, or protocol, all PCs follow to communicate over a network. This is true for wireless networks as well. Your PCs will not be able to utilize wireless networking without having TCP/IP enabled. Windows Help provides complete instructions on enabling TCP/IP.

Shared Resources

If you wish to share printers, folder, or files over your network, Windows Help provides complete instructions on utilizing shared resources.

Network Neighborhood/My Network Places

Other PCs on your network will appear under Network Neighborhood or My Network Places (depending upon the version of Windows you're running). Windows Help provides complete instructions on adding PCs to your network.

Appendix E: Glossary

This glossary contains some basic networking terms you may come across when using this product. For more advanced terms, see the complete Linksys glossary at http://www.linksys.com/glossary.

Access Point - A device that allows wireless-equipped computers and other devices to communicate with a wired network. Also used to expand the range of a wireless network.

Ad-hoc - A group of wireless devices communicating directly with each other (peer-to-peer) without the use of an access point.

AES (**A**dvanced **E**ncryption **S**tandard) - A security method that uses symmetric 128-bit block data encryption.

Bandwidth - The transmission capacity of a given device or network.

Bit - A binary digit.

Boot - To start a device and cause it to start executing instructions.

Broadband - An always-on, fast Internet connection.

Browser - An application program that provides a way to look at and interact with all the information on the World Wide Web.

Byte - A unit of data that is usually eight bits long

Cable Modem - A device that connects a computer to the cable television network, which in turn connects to the Internet.

Daisy Chain - A method used to connect devices in a series, one after the other.

DDNS (**D**ynamic **D**omain **N**ame **S**ystem) - Allows the hosting of a website, FTP server, or e-mail server with a fixed domain name (e.g., www.xyz.com) and a dynamic IP address.

Default Gateway - A device that forwards Internet traffic from your local area network.

DHCP (**D**ynamic **H**ost **C**onfiguration **P**rotocol) - A networking protocol that allows administrators to assign temporary IP addresses to network computers by "leasing" an IP address to a user for a limited amount of time, instead of assigning permanent IP addresses.

DMZ (**Dem**ilitarized **Z**one) - Removes the Router's firewall protection from one PC, allowing it to be "seen" from the Internet.

DNS (**D**omain **N**ame **S**erver) - The IP address of your ISP's server, which translates the names of websites into IP addresses.

Domain - A specific name for a network of computers.

DOS (**D**enial **o**f **S**ervice) - A network security term which defines a type of attack designed to prevent legitimate users from using wireless service by flooding with useless/malicious traffic.

Download - To receive a file transmitted over a network.

DSL (**D**igital **S**ubscriber **L**ine) - An always-on broadband connection over traditional phone lines.

Dynamic IP Address - A temporary IP address assigned by a DHCP server.

EAP (**E**xtensible **A**uthentication **P**rotocol) - A general authentication protocol used to control network access. Many specific authentication methods work within this framework.

Encryption - Encoding data transmitted in a network.

Ethernet - IEEE standard network protocol that specifies how data is placed on and retrieved from a common transmission medium.

Firewall - A set of related programs located at a network gateway server that protects the resources of a network from users from other networks.

Firmware - The programming code that runs a networking device.

FTP (**F**ile **T**ransfer **P**rotocol) - A protocol used to transfer files over a TCP/IP network.

Full Duplex - The ability of a networking device to receive and transmit data simultaneously.

Gateway - A device that interconnects networks with different, incompatible communications protocols.

Half Duplex - Data transmission that can occur in two directions over a single line, but only one direction at a time.

HTTP (**H**yper**T**ext **T**ransport **P**rotocol) - The communications protocol used to connect to servers on the World Wide Web.

Infrastructure - A wireless network that is bridged to a wired network via an access point.

Intrusion attack - A type of internet attacks in which an attacker tries to gain or access the information transimitted through the networks.

IP (**I**nternet **P**rotocol) - A protocol used to send data over a network.

IP Address - The address used to identify a computer or device on a network.

IPCONFIG - A Windows 2000 and XP utility that displays the IP address for a particular networking device.

IPSec (**I**nternet **P**rotocol **Sec**urity) - A VPN protocol used to implement secure exchange of packets at the IP layer.

ISP (**I**nternet **S**ervice **P**rovider) - A company that provides access to the Internet.

LAN - The computers and networking products that make up your local network.

MAC (**M**edia **A**ccess **C**ontrol) **Address** - The unique address that a manufacturer assigns to each networking device.

Mbps (**M**ega**B**its **P**er **S**econd) - One million bits per second; a unit of measurement for data transmission.

NAT (**N**etwork **A**ddress **T**ranslation) - NAT technology translates IP addresses of a local area network to a different IP address for the Internet.

Network - A series of computers or devices connected for the purpose of data sharing, storage, and/or transmission between users.

Packet - A unit of data sent over a network.

Passphrase - Used much like a password, a passphrase simplifies the WEP encryption process by automatically generating the WEP encryption keys for Linksys products.

Ping (**P**acket **IN**ternet **G**roper) - An Internet utility used to determine whether a particular IP address is online.

POP3 (**P**ost **O**ffice **P**rotocol **3**) - A standard mail server commonly used on the Internet.

Port - The connection point on a computer or networking device used for plugging in cables or adapters.

Power **o**ver **E**thernet (**PoE**) - A technology enabling an Ethernet network cable to deliver both data and power.

PPPoE (**P**oint to **P**oint **P**rotocol **o**ver **E**thernet) - A type of broadband connection that provides authentication (username and password) in addition to data transport.

PPTP (**P**oint-to-**P**oint **T**unneling **P**rotocol) - A VPN protocol that allows the Point to Point Protocol (PPP) to be tunneled through an IP network. This protocol is also used as a type of broadband connection in Europe.

QoS (**Q**uality of **S**ervice) - A mechanism which gives priorities to certain types of traffic to ensure the throughput; for example, the streaming multimedia.

RADIUS (**R**emote **A**uthentication **D**ial-**I**n **U**ser **S**ervice) - A protocol that uses an authentication server to control network access.

RJ-45 (**R**egistered **J**ack-**45**) - An Ethernet connector that holds up to eight wires.

Roaming - The ability to take a wireless device from one access point's range to another without losing the connection.

Router - A networking device that connects multiple networks together.

Server - Any computer whose function in a network is to provide user access to files, printing, communications, and other services.

SMTP (**S**imple **M**ail **T**ransfer **P**rotocol) - The standard e-mail protocol on the Internet.

SNMP (**S**imple **N**etwork **M**anagement **P**rotocol) - A widely used network monitoring and control protocol.

SPI (**S**tateful **P**acket **I**nspection) **Firewall** - A technology that inspects incoming packets of information before allowing them to enter the network.

SSID (**S**ervice **S**et **ID**entifier) -It consists of 32 alphanumeric characters to identify a group of wireless network devices uniquely.

Static IP Address - A fixed address assigned to a computer or device that is connected to a network.

Static Routing - Forwarding data in a network via a fixed path.

Subnet Mask - An address code that determines the size of the network.

Switch - 1. A data switch that connects computing devices to host computers, allowing a large number of devices to share a limited number of ports. 2. A device for making, breaking, or changing the connections in an electrical circuit.

TCP (**T**ransmission **C**ontrol **P**rotocol) - A network protocol for transmitting data that requires acknowledgement from the recipient of data sent.

TCP/IP (**T**ransmission **C**ontrol **P**rotocol/**I**nternet **P**rotocol) - A set of instructions PCs use to communicate over a network.

Telnet - A user command and TCP/IP protocol used for accessing remote PCs.

TFTP (**T**rivial **F**ile **T**ransfer **P**rotocol) - A version of the TCP/IP FTP protocol that has no directory or password capability.

Throughput - The amount of data moved successfully from one node to another in a given time period.

TKIP (**T**emporal **K**ey **I**ntegrity **P**rotocol) - a wireless encryption protocol that provides dynamic encryption keys for each packet transmitted.

Topology - The physical layout of a network.

TX Rate - Transmission Rate.

Upgrade - To replace existing software or firmware with a newer version.

Upload - To transmit a file over a network.

URL (**U**niform **R**esource **L**ocator) - The address of a file located on the Internet.

VPN (**V**irtual **P**rivate **N**etwork) - A security measure to protect data as it leaves one network and goes to another over the Internet.

WAN (**W**ide **A**rea **N**etwork)- The Internet.

WEP (**W**ired **E**quivalent **P**rivacy) - A method of encrypting network data transmitted on a wireless network for greater security.

WLAN (**W**ireless **L**ocal **A**rea **N**etwork) - A group of computers and associated devices that communicate with each other wirelessly.

WPA (**W**i-Fi **P**rotected **A**ccess) - a wireless security protocol using TKIP (Temporal Key Integrity Protocol) encryption, which can be used in conjunction with a RADIUS server.

Appendix F: Specifications

Standards	IEEE802.11g, IEEE802.11b, 802.1x (Security Authentication), (802.1i)
Channels	802.11b/802.11g 11 Channels (US, Canada) 13 Channels (Europe) 14 Channels (Japan)
LEDs	Link/Act
Protocols	802.11b: CCK (11 Mbps), DQPSK (2 Mbps), DBPSK (1 Mbps); 802.11g: OFDM
Peak Gain of the Antenna	1.89dBi
Transmitted Power	802.11b: 18 ~19 dBm 802.11g: 18 ~19 dBm
Receive Sensitivity	11Mbps @ -84dBm (Typical) 54Mbps @ -70dBm (Typical)
Security Features	WEP, WPA-Personal, WPA-Enterprise, WPA2-Personal, WPA2-Enterprise with RADIUS
WEP key bit lengths	64 Bit and 128 Bit
Security Monitor	Intrusion Alarms (e.g., Rogue Client Detected, Spoofed MAC address) Vulnerability Alarms (e.g., AP is not using encryption, AP is broadcasting SSID)
Dimensions	3.54" x 2.68" x 0.67" (90 mm x 68 mm x 17 mm)

Unit Weight	2.15 oz (0.061 kg)
Certifications	FCC, IC, CE, Wi-Fi (802.11b/g)
Operating Temp.	32ºF to 113ºF (0ºC to 45ºC)
Storage Temp.	-4ºF to 140ºF (-20ºC to 60ºC)
Operating Humidity	10 to 85%, Non-Condensing
Storage Humidity	5 to 90%, Non-Condensing

Appendix G: Warranty Information

LIMITED WARRANTY

Linksys warrants to You that, for a period of three years (the "Warranty Period"), your Linksys Product will be substantially free of defects in materials and workmanship under normal use. Your exclusive remedy and Linksys' entire liability under this warranty will be for Linksys at its option to repair or replace the Product or refund Your purchase price less any rebates. This limited warranty extends only to the original purchaser.

If the Product proves defective during the Warranty Period call Linksys Technical Support in order to obtain a Return Authorization Number, if applicable. BE SURE TO HAVE YOUR PROOF OF PURCHASE ON HAND WHEN CALLING. If You are requested to return the Product, mark the Return Authorization Number clearly on the outside of the package and include a copy of your original proof of purchase. RETURN REQUESTS CANNOT BE PROCESSED WITHOUT PROOF OF PURCHASE. You are responsible for shipping defective Products to Linksys. Linksys pays for UPS Ground shipping from Linksys back to You only. Customers located outside of the United States of America and Canada are responsible for all shipping and handling charges.

ALL IMPLIED WARRANTIES AND CONDITIONS OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE ARE LIMITED TO THE DURATION OF THE WARRANTY PERIOD. ALL OTHER EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF NON-INFRINGEMENT, ARE DISCLAIMED. Some jurisdictions do not allow limitations on how long an implied warranty lasts, so the above limitation may not apply to You. This warranty gives You specific legal rights, and You may also have other rights which vary by jurisdiction.

This warranty does not apply if the Product (a) has been altered, except by Linksys, (b) has not been installed, operated, repaired, or maintained in accordance with instructions supplied by Linksys, or (c) has been subjected to abnormal physical or electrical stress, misuse, negligence, or accident. In addition, due to the continual development of new techniques for intruding upon and attacking networks, Linksys does not warrant that the Product will be free of vulnerability to intrusion or attack.

TO THE EXTENT NOT PROHIBITED BY LAW, IN NO EVENT WILL LINKSYS BE LIABLE FOR ANY LOST DATA, REVENUE OR PROFIT, OR FOR SPECIAL, INDIRECT, CONSEQUENTIAL, INCIDENTAL OR PUNITIVE DAMAGES, REGARDLESS OF THE THEORY OF LIABILITY (INCLUDING NEGLIGENCE), ARISING OUT OF OR RELATED TO THE USE OF OR INABILITY TO USE THE PRODUCT (INCLUDING ANY SOFTWARE), EVEN IF LINKSYS HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. IN NO EVENT WILL LINKSYS' LIABILITY EXCEED THE AMOUNT PAID BY YOU FOR THE PRODUCT. The foregoing limitations will apply even if any warranty or remedy provided under this Agreement fails of its essential purpose. Some jurisdictions do not allow the exclusion or limitation of incidental or consequential damages, so the above limitation or exclusion may not apply to You.

Please direct all inquiries to: Linksys, P.O. Box 18558, Irvine, CA 92623.

Appendix H: Regulatory Information

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:

FCC Radiation Exposure Statement:

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

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

The availability of some specific channels and/or operational frequency bands are country dependent and are firmware programmed at the factory to match the intended destination. The firmware setting is not accessible by the end user.

Industry Canada statement:

This Class B digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe B est conforme à la norme NMB-003 du Canada.

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.

Règlement d'Industry Canada

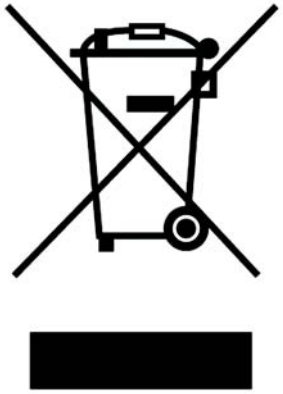
Les conditions de fonctionnement sont sujettes à deux conditions:

1) Ce périphérique ne doit pas causer d'interférence et.
2) Ce périphérique doit accepter toute interférence, y compris les interférences pouvant perturber le bon fonctionnement de ce périphérique.

IMPORTANT NOTE:

Radiation Exposure Statement:

This equipment complies with IC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.



User Information for Consumer Products Covered by EU Directive 2002/96/EC on Waste Electric and Electronic Equipment (WEEE)

This document contains important information for users with regards to the proper disposal and recycling of Linksys products. Consumers are required to comply with this notice for all electronic products bearing the following symbol:

English

Environmental Information for Customers in the European Union

European Directive 2002/96/EC requires that the equipment bearing this symbol on the product and/or its packaging must not be disposed of with unsorted municipal waste. The symbol indicates that this product should be disposed of separately from regular household waste streams. It is your responsibility to dispose of this and other electric and electronic equipment via designated collection facilities appointed by the government or local authorities. Correct disposal and recycling will help prevent potential negative consequences to the environment and human health. For more detailed information about the disposal of your old equipment, please contact your local authorities, waste disposal service, or the shop where you purchased the product.

Ceština/Czech

Informace o ochraně životního prostředí pro zákazníky v zemích Evropské unie

Evropská směrnice 2002/96/ES zakazuje, aby zařízení označené tímto symbolem na produktu anebo na obalu bylo likvidováno s netříděným komunálním odpadem. Tento symbol udává, že daný produkt musí být likvidován odděleně od běžného komunálního odpadu. Odpovídáte za likvidaci tohoto produktu a dalších elektrických a elektronických zařízení prostřednictvím určených sběrných míst stanovených vládou nebo místními úřady. Správná likvidace a recyklace pomáhá předcházet potenciálním negativním dopadům na životní prostředí a lidské zdraví. Podrobnější informace o likvidaci starého vybavení si laskavě vyžádejte od místních úřadů, podniku zabývajícího se likvidací komunálních odpadů nebo obchodu, kde jste produkt zakoupili.

Dansk/Danish

Miljøinformation for kunder i EU

EU-direktiv 2002/96/EF kræver, at udstyr der bærer dette symbol på produktet og/eller emballagen ikke må bortskaffes som usorteret kommunalt affald. Symbolet betyder, at dette produkt skal bortskaffes adskilt fra det almindelige husholdningsaffald. Det er dit ansvar at bortskaffe dette og andet elektrisk og elektronisk udstyr via bestemte indsamlingssteder udpeget af staten eller de lokale myndigheder. Korrekt bortskaffelse og genvinding vil hjælpe med til at undgå mulige skader for miljøet og menneskers sundhed. Kontakt venligst de lokale myndigheder, renovationstjenesten eller den butik, hvor du har købt produktet, angående mere detaljeret information om bortskaffelse af dit gamle udstyr.

Deutsch/German

Umweltinformation für Kunden innerhalb der Europäischen Union

Die Europäische Richtlinie 2002/96/EC verlangt, dass technische Ausrüstung, die direkt am Gerät und/oder an der Verpackung mit diesem Symbol versehen ist nicht zusammen mit unsortiertem Gemeindeabfall entsorgt werden darf. Das Symbol weist darauf hin, dass das Produkt von regulärem Haushaltmüll getrennt entsorgt werden sollte. Es liegt in Ihrer Verantwortung, dieses Gerät und andere elektrische und elektronische Geräte über die dafür zuständigen und von der Regierung oder örtlichen Behörden dazu bestimmten Sammelstellen zu entsorgen. Ordnungsgemäßes Entsorgen und Recyceln trägt dazu bei, potentielle negative Folgen für Umwelt und die menschliche Gesundheit zu vermeiden. Wenn Sie weitere Informationen zur Entsorgung Ihrer Altgeräte benötigen, wenden Sie sich bitte an die örtlichen Behörden oder städtischen Entsorgungsdienste oder an den Händler, bei dem Sie das Produkt erworben haben.

Eesti/Estonian

Keskkonnaalane informatsioon Euroopa Liidus asuvatele klientidele

Euroopa Liidu direktiivi 2002/96/EÜ nõuete kohaselt on seadmeid, millel on tootel või pakendil käesolev sümbol, keelatud kõrvaldada koos sorteerimata olmejäätmetega. See sümbol näitab, et toode tuleks kõrvaldada eraldi tavalistest olmejäätmevoogudest. Olete kohustatud kõrvaldama käesoleva ja ka muud elektri- ja elektroonikaseadmed riigi või kohalike ametiasutuste poolt ette nähtud kogumispunktide kaudu. Seadmete korrektne kõrvaldamine ja ringlussevõtt aitab vältida võimalikke negatiivseid tagajärgi keskkonnale ning inimeste tervisele. Vanade seadmete kõrvaldamise kohta täpsema informatsiooni saamiseks võtke palun ühendust kohalike ametiasutustega, jäätmekäitlusfirmaga või kauplusega, kust te toote ostsite.

Español/Spanish

Información medioambiental para clientes de la Unión Europea

La Directiva 2002/96/CE de la UE exige que los equipos que lleven este símbolo en el propio aparato y/o en su embalaje no deben eliminarse junto con otros residuos urbanos no seleccionados. El símbolo indica que el producto en cuestión debe separarse de los residuos domésticos convencionales con vistas a su eliminación. Es responsabilidad suya desechar este y cualesquiera otros aparatos eléctricos y electrónicos a través de los puntos de recogida que ponen a su disposición el gobierno y las autoridades locales. Al desechar y reciclar correctamente estos aparatos estará contribuyendo a evitar posibles consecuencias negativas para el medio ambiente y la salud de las personas. Si desea obtener información más detallada sobre la eliminación segura de su aparato usado, consulte a las autoridades locales, al servicio de recogida y eliminación de residuos de su zona o pregunte en la tienda donde adquirió el producto.

Ξλληνικά/Greek

Στοιχεία περιβαλλοντικής προστασίας για πελάτες εντός της Ευρωπαϊκής Ένωσης

Η Κοινοτική Οδηγία 2002/96/EC απαιτεί ότι ο εξοπλισμός ο οποίος φέρει αυτό το σύμβολο στο προϊόν και/ή στη συσκευασία του δεν πρέπει να απορρίπτεται μαζί με τα μικτά κοινοτικά απορρίμματα. Το σύμβολο υποδεικνύει ότι αυτό το προϊόν θα πρέπει να απορρίπτεται ξεχωριστά από τα συνήθη οικιακά απορρίμματα. Είστε υπεύθυνος για την απόρριψη του παρόντος και άλλου ηλεκτρικού και ηλεκτρονικού εξοπλισμού μέσω των καθορισμένων εγκαταστάσεων συγκέντρωσης απορριμμάτων οι οποίες παρέχονται από το κράτος ή τις αρμόδιες τοπικές αρχές. Η σωστή απόρριψη και ανακύκλωση συμβάλλει στην πρόληψη πιθανών αρνητικών συνεπειών για το περιβάλλον και την υγεία. Για περισσότερες πληροφορίες σχετικά με την απόρριψη του παλιού σας εξοπλισμού, παρακαλώ επικοινωνήστε με τις τοπικές αρχές, τις υπηρεσίες απόρριψης ή το κατάστημα από το οποίο αγοράσατε το προϊόν.

Français/French

Informations environnementales pour les clients de l'Union européenne

La directive européenne 2002/96/CE exige que l'équipement sur lequel est apposé ce symbole sur le produit et/ou son emballage ne soit pas jeté avec les autres ordures ménagères. Ce symbole indique que le produit doit être éliminé dans un circuit distinct de celui pour les déchets des ménages. Il est de votre responsabilité de jeter ce matériel ainsi que tout autre matériel électrique ou électronique par les moyens de collecte indiqués par le gouvernement et les pouvoirs publics des collectivités territoriales. L'élimination et le recyclage en bonne et due forme ont pour but de lutter contre l'impact néfaste potentiel de ce type de produits sur l'environnement et la santé publique. Pour plus d'informations sur le mode d'élimination de votre ancien équipement, veuillez prendre contact avec les pouvoirs publics locaux, le service de traitement des déchets, ou l'endroit où vous avez acheté le produit.

Italiano/Italian

Informazioni relative all'ambiente per i clienti residenti nell'Unione Europea

La direttiva europea 2002/96/EC richiede che le apparecchiature contrassegnate con questo simbolo sul prodotto e/o sull'imballaggio non siano smaltite insieme ai rifiuti urbani non differenziati. Il simbolo indica che questo prodotto non deve essere smaltito insieme ai normali rifiuti domestici. È responsabilità del proprietario smaltire sia questi prodotti sia le altre apparecchiature elettriche ed elettroniche mediante le specifiche strutture di raccolta indicate dal governo o dagli enti pubblici locali. Il corretto smaltimento ed il riciclaggio aiuteranno a prevenire conseguenze potenzialmente negative per l'ambiente e per la salute dell'essere umano. Per ricevere informazioni più dettagliate circa lo smaltimento delle vecchie apparecchiature in Vostro possesso, Vi invitiamo a contattare gli enti pubblici di competenza, il servizio di smaltimento rifiuti o il negozio nel quale avete acquistato il prodotto.

Latviešu valoda/Latvian

Ekoloģiska informācija klientiem Eiropas Savienības jurisdikcijā

Direktīvā 2002/96/EK ir prasība, ka aprīkojumu, kam pievienota zīme uz paša izstrādājuma vai uz tā iesaiņojuma, nedrīkst izmest nešķirotā veidā kopā ar komunālajiem atkritumiem (tiem, ko rada vietēji iedzīvotāji un uzņēmumi). Šī zīme nozīmē to, ka šī ierīce ir jāizmet atkritumos tā, lai tā nenonāktu kopā ar parastiem mājsaimniecības atkritumiem. Jūsu pienākums ir šo un citas elektriskas un elektroniskas ierīces izmest atkritumos, izmantojot īpašus atkritumu savākšanas veidus un līdzekļus, ko nodrošina valsts un pašvaldību iestādes. Ja izmešana atkritumos un pārstrāde tiek veikta pareizi, tad mazinās iespējamais kaitējums dabai un cilvēku veselībai. Sīkākas ziņas par novecojuša aprīkojuma izmešanu atkritumos jūs varat saņemt vietējā pašvaldībā, atkritumu savākšanas dienestā, kā arī veikalā, kur iegādājāties šo izstrādājumu.

Lietuvškai/Lithuanian

Aplinkosaugos informacija, skirta Europos Sąjungos vartotojams

Europos direktyva 2002/96/EC numato, kad įrangos, kuri ir (arba) kurios pakuotė yra pažymėta šiuo simboliu, negalima šalinti kartu su nerūšiuotomis komunalinėmis atliekomis. Šis simbolis rodo, kad gaminį reikia šalinti atskirai nuo bendro buitinių atliekų srauto. Jūs privalote užtikrinti, kad ši ir kita elektros ar elektroninė įranga būtų šalinama per tam tikras nacionalinės ar vietinės valdžios nustatytas atliekų rinkimo sistemas. Tinkamai šalinant ir perdirbant atliekas, bus išvengta galimos žalos aplinkai ir žmonių sveikatai. Daugiau informacijos apie jūsų senos įrangos šalinimą gali pateikti vietinės valdžios institucijos, atliekų šalinimo tarnybos arba parduotuvės, kuriose įsigijote tą gaminį.

Malti/Maltese

Informazzjoni Ambjentali għal Klijenti fl-Unjoni Ewropea

Id-Direttiva Ewropea 2002/96/KE titlob li t-tagħmir li jkun fih is-simbolu fuq il-prodott u/jew fuq l-ippakkjar ma jistax jintrema ma' skart muniċipali li ma ġiex isseparat. Is-simbolu jindika li dan il-prodott għandu jintrema separatament minn ma' l-iskart domestiku regolari. Hija responsabbiltà tiegħek li tarmi dan it-tagħmir u kull tagħmir ieħor ta' l-elettriku u elettroniku permezz ta' faċilitajiet ta' ġbir appuntati apposta mill-gvern jew mill-awtoritajiet lokali. Ir-rimi b'mod korrett u r-riċiklaġġ jgħin jipprevjeni konsegwenzi negattivi potenzjali għall-ambjent u għas-saħħa tal-bniedem. Għal aktar informazzjoni dettaljata dwar ir-rimi tat-tagħmir antik tiegħek, jekk jogħġbok ikkuntattja lill-awtoritajiet lokali tiegħek, is-servizzi għar-rimi ta' l-iskart, jew il-ħanut minn fejn xtrajt il-prodott.

Magyar/Hungarian

Környezetvédelmi információ az európai uniós vásárlók számára

A 2002/96/EC számú európai uniós irányelv megkívánja, hogy azokat a termékeket, amelyeken, és/vagy amelyek csomagolásán az alábbi címke megjelenik, tilos a többi szelektálatlan lakossági hulladékkal együtt kidobni. A címke azt jelöli, hogy az adott termék kidobásakor a szokványos háztartási hulladékelszállítási rendszerektől elkülönített eljárást kell alkalmazni. Az Ön felelőssége, hogy ezt, és más elektromos és elektronikus berendezéseit a kormányzati vagy a helyi hatóságok által kijelölt gyűjtőredszereken keresztül számolja fel. A megfelelő hulladékfeldolgozás segít a környezetre és az emberi egészségre potenciálisan ártalmas negatív hatások megelőzésében. Ha elavult berendezéseinek felszámolásához további részletes információra van szüksége, kérjük, lépjen kapcsolatba a helyi hatóságokkal, a hulladékfeldolgozási szolgálattal, vagy azzal üzlettel, ahol a terméket vásárolta.

Nederlands/Dutch

Milieu-informatie voor klanten in de Europese Unie

De Europese Richtlijn 2002/96/EC schrijft voor dat apparatuur die is voorzien van dit symbool op het product of de verpakking, niet mag worden ingezameld met niet-gescheiden huishoudelijk afval. Dit symbool geeft aan dat het product apart moet worden ingezameld. U bent zelf verantwoordelijk voor de vernietiging van deze en andere elektrische en elektronische apparatuur via de daarvoor door de landelijke of plaatselijke overheid aangewezen inzamelingskanalen. De juiste vernietiging en recycling van deze apparatuur voorkomt mogelijke negatieve gevolgen voor het milieu en de gezondheid. Voor meer informatie over het vernietigen van uw oude apparatuur neemt u contact op met de plaatselijke autoriteiten of afvalverwerkingsdienst, of met de winkel waar u het product hebt aangeschaft.

Norsk/Norwegian

Miljøinformasjon for kunder i EU

EU-direktiv 2002/96/EF krever at utstyr med følgende symbol avbildet på produktet og/eller pakningen, ikke må kastes sammen med usortert avfall. Symbolet indikerer at dette produktet skal håndteres atskilt fra ordinær avfallsinnsamling for husholdningsavfall. Det er ditt ansvar å kvitte deg med dette produktet og annet elektrisk og elektronisk avfall via egne innsamlingsordninger slik myndighetene eller kommunene bestemmer. Korrekt avfallshåndtering og gjenvinning vil være med på å forhindre mulige negative konsekvenser for miljø og helse. For nærmere informasjon om håndtering av det kasserte utstyret ditt, kan du ta kontakt med kommunen, en innsamlingsstasjon for avfall eller butikken der du kjøpte produktet.

Polski/Polish

Informacja dla klientów w Unii Europejskiej o przepisach dotyczących ochrony środowiska

Dyrektywa Europejska 2002/96/EC wymaga, aby sprzęt oznaczony symbolem znajdującym się na produkcie i/lub jego opakowaniu nie był wyrzucany razem z innymi niesortowanymi odpadami komunalnymi. Symbol ten wskazuje, że produkt nie powinien być usuwany razem ze zwykłymi odpadami z gospodarstw domowych. Na Państwu spoczywa obowiązek wyrzucania tego i innych urządzeń elektrycznych oraz elektronicznych w punktach odbioru wyznaczonych przez władze krajowe lub lokalne. Pozbywanie się sprzętu we właściwy sposób i jego recykling pomogą zapobiec potencjalnie negatywnym konsekwencjom dla środowiska i zdrowia ludzkiego. W celu uzyskania szczegółowych informacji o usuwaniu starego sprzętu, prosimy zwrócić się do lokalnych władz, służb oczyszczania miasta lub sklepu, w którym produkt został nabyty.

Português/Portuguese

Informação ambiental para clientes da União Europeia

A Directiva Europeia 2002/96/CE exige que o equipamento que exibe este símbolo no produto e/ou na sua embalagem não seja eliminado junto com os resíduos municipais não separados. O símbolo indica que este produto deve ser eliminado separadamente dos resíduos domésticos regulares. É da sua responsabilidade eliminar este e qualquer outro equipamento eléctrico e electrónico através dos instalações de recolha designadas pelas autoridades governamentais ou locais. A eliminação e reciclagem correctas ajudarão a prevenir as consequências negativas para o ambiente e para a saúde humana. Para obter informações mais detalhadas sobre a forma de eliminar o seu equipamento antigo, contacte as autoridades locais, os serviços de eliminação de resíduos ou o estabelecimento comercial onde adquiriu o produto.

Slovenčina/Slovak

Informácie o ochrane životného prostredia pre zákazníkov v Európskej únii

Podľa európskej smernice 2002/96/ES zariadenie s týmto symbolom na produkte a/alebo jeho balení nesmie byť likvidované spolu s netriedeným komunálnym odpadom. Symbol znamená, že produkt by sa mal likvidovať oddelene od bežného odpadu z domácností. Je vašou povinnosťou likvidovať toto i ostatné elektrické a elektronické zariadenia prostredníctvom špecializovaných zberných zariadení určených vládou alebo miestnymi orgánmi. Správna likvidácia a recyklácia pomôže zabrániť prípadným negatívnym dopadom na životné prostredie a zdravie ľudí. Ak máte záujem o podrobnejšie informácie o likvidácii starého zariadenia, obráťte sa, prosím, na miestne orgány, organizácie zaoberajúce sa likvidáciou odpadov alebo obchod, v ktorom ste si produkt zakúpili.

Slovenčina/Slovene

Okoljske informacije za stranke v Evropski uniji

Evropska direktiva 2002/96/EC prepoveduje odlaganje opreme, označene s tem simbolom – na izdelku in/ali na embalaži – med običajne, nerazvrščene odpadke. Ta simbol opozarja, da je treba izdelek odvreči ločeno od preostalih gospodinjskih odpadkov. Vaša odgovornost je, da to in preostalo električno in elektronsko opremo odnesete na posebna zbirališča, ki jih določijo državne ustanove ali lokalna uprava. S pravilnim odlaganjem in recikliranjem boste preprečili morebitne škodljive vplive na okolje in zdravje ljudi. Če želite izvedeti več o odlaganju stare opreme, se obrnite na lokalno upravo, odpad ali trgovino, kjer ste izdelek kupili.

Suomi/Finnish

Ympäristöä koskevia tietoja EU-alueen asiakkaille

EU-direktiivi 2002/96/EY edellyttää, että jos laitteistossa on tämä symboli itse tuotteessa ja/tai sen pakkauksessa, laitteistoa ei saa hävittää lajittelemattoman yhdyskuntajätteen mukana. Symboli merkitsee sitä, että tämä tuote on hävitettävä erillään tavallisesta kotitalousjätteestä. Sinun vastuullasi on hävittää tämä elektroniikkatuote ja muut vastaavat elektroniikkatuotteet viemällä tuote tai tuotteet viranomaisten määräämään keräyspisteeseen. Laitteiston oikea hävittäminen estää mahdolliset kielteiset vaikutukset ympäristöön ja ihmisten terveyteen. Lisätietoja vanhan laitteiston oikeasta hävitystavasta saa paikallisilta viranomaisilta, jätteenhävityspalvelusta tai siitä myymälästä, josta ostit tuotteen.

Svenska/Swedish

Miljöinformation för kunder i Europeiska unionen

Det europeiska direktivet 2002/96/EC kräver att utrustning med denna symbol på produkten och/eller förpackningen inte får kastas med osorterat kommunalt avfall Symbolen visar att denna produkt bör kastas efter att den avskiljts från vanligt hushållsavfall. Det faller på ditt ansvar att kasta denna och annan elektrisk och elektronisk utrustning på fastställda insamlingsplatser utsedda av regeringen eller lokala myndigheter. Korrekt kassering och återvinning skyddar mot eventuella negativa konsekvenser för miljön och personhälsa. För mer detaljerad information om kassering av din gamla utrustning kontaktar du dina lokala myndigheter, avfallshanteringen eller butiken där du köpte produkten.

For more information, visit www.linksys.com.

Appendix I: Contact Information

Need to contact Linksys? Visit us online for information on the latest products and updates to your existing products at:	http://www.linksys.com or ftp.linksys.com
Can't find information about a product you want to buy on the web? Do you want to know more about networking with Linksys products? Give our advice line a call at:	800-546-5797 (LINKSYS)
Or fax your request in to:	949-823-3002
If you experience problems with any Linksys product, you can call us at:	800-326-7114
Don't wish to call? You can e-mail us at:	support@linksys.com
If any Linksys product proves defective during its warranty period, you can call the Linksys Return Merchandise Authorization department for obtaining a Return Authorization Number at: (Details on Warranty and RMA issues can be found in the Warranty Information section in this Guide.)	949-823-3000