

LINKSYS®

A Division of Cisco Systems, Inc.



USER GUIDE

BUSINESS SERIES

Wireless-G Business Ethernet Bridge

Model: WET200

About This Guide

Icon Descriptions

While reading through the User Guide you may see various icons that call attention to specific items. Below is a description of these icons:



NOTE: This check mark indicates that there is a note of interest and is something that you should pay special attention to while using the product.



WARNING: This exclamation point indicates that there is a caution or warning and it is something that could damage your property or product.



WEB: This globe icon indicates a noteworthy website address or e-mail address.

Online Resources

Website addresses in this document are listed without **http://** in front of the address because most current web browsers do not require it. If you use an older web browser, you may have to add **http://** in front of the web address.

Resource	Website
Linksys	www.linksys.com
Linksys International	www.linksys.com/international
Glossary	www.linksys.com/glossary
Network Security	www.linksys.com/security

Copyright and Trademarks



A Division of Cisco Systems, Inc.



Linksys, Cisco and the Cisco Logo are registered trademarks or trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries. Copyright © 2008 Cisco Systems, Inc. All rights reserved. Other brands and product names are trademarks or registered trademarks of their respective holders.

Chapter 1: Introduction	1
Chapter 2: Planning Your Wireless Network	2
Network Topology	2
Network Layout	2
Example of WET200 in Infrastructure Mode	2
Example of WET200 in Ad-Hoc Mode	3
Chapter 3: Product Overview	4
Front Panel	4
Back Panel	4
Chapter 4: Installation	5
Overview	5
Connection	5
Power over Ethernet	5
Power Adapter	5
Placement Options	5
Stand Option	5
Wall-Mount Option	6
Chapter 5: Quick Configuration Overview	7
Overview	7
Accessing the Web-Based Utility	7
Navigating the Web-Based Utility	7
Setup	7
Wireless	7
Switch	8
Administration	8
System Status	8
Chapter 6: Advanced Configuration	9
Setup	9
Wireless	10
Wireless > Basic Settings	10
Wireless > Wireless Security	11
Wireless > Advanced Settings	13
Switch	13
Switch > Port Management	13
Switch > Port Mirroring	14
Switch > VLAN	14
Switch > MAC Based ACL	16
Switch > QoS	17
Switch > Spanning Tree	17

Switch > MAC Table18
Administration18
Administration > Password18
Administration > Web Access18
Administration > SNMP19
Administration > Configuration Management19
Administration > Factory Defaults19
Administration > Firmware Upgrade20
System Status20
System Status > System Status20
System Status > Wireless Status.20
System Status > Port Statistics21
Appendix A: Wireless Security Checklist	22
General Network Security Guidelines22
Additional Security Tips22
Appendix B: Glossary	23
Appendix C: Specifications	27
Appendix D: Warranty Information	28
Appendix E: Regulatory Information	29
FCC Statement29
FCC Radiation Exposure Statement29
Safety Notices.29
Industry Canada Statement29
Industry Canada Radiation Exposure Statement:.29
Avis d'Industrie Canada.30
Avis d'Industrie Canada concernant l'exposition aux radiofréquences :.30
Wireless Disclaimer30
Avis de non-responsabilité concernant les appareils sans fil30
User Information for Consumer Products Covered by EU Directive 2002/96/EC on Waste Electric and Electronic Equipment (WEEE)31
Appendix F: Contact Information	35

Chapter 1: Introduction

Thank you for choosing the Wireless-G Business Ethernet Bridge.

The Linksys WET200 Wireless Bridge seamlessly bridges separate Ethernet networks together wirelessly and is ideal for small businesses with offices and resources that are in different office suites of a building or a closely adjacent building. The WET200 is a Power over Ethernet (PoE) end device so it can be installed anywhere an Ethernet cable can be run if there is not ready access to a power outlet. PoE enables delivery of both data and power to the WET200. An AC adapter is also included if the device installation site has a power outlet nearby.

Advanced security features include Wi-Fi Protected Access™ (WPA2 Enterprise) with up to 256-bit AES encryption using EAP (Extensible Authentication Protocol) giving small businesses the protection they need to communicate and transfer data securely. The integrated QoS features provide consistent voice and video quality on both the wired and wireless networks, enabling the deployment of business quality VoIP and video applications.

Additional support for VLANs, SNMP, Spanning Tree, and Port Mirroring make this an ideal solution for network administrators to incorporate into larger organizations.

Chapter 2: Planning Your Wireless Network

Network Topology

A wireless network is a group of computers, each equipped with one or more wireless adapters. Computers in a wireless network must be configured to share the same radio channel to talk to each other. Several PCs equipped with wireless cards or adapters can communicate with each other to form an ad-hoc network without the use of an access point.

Linksys wireless adapters also provide access to a wired network when using an access point or wireless router. An integrated wireless and wired network is called an infrastructure network. Each wireless PC in an infrastructure network can talk to any computer in a wired or wireless network via the access point or wireless router.

An infrastructure configuration extends the accessibility of a wireless PC to a wired network, and may double the effective wireless transmission range for two wireless adapter PCs. Since an access point is able to forward data within a network, the effective transmission range in an infrastructure network may be doubled (depending on antenna characteristics).

Network Layout

The Wireless-G Business Ethernet Bridge can be used in either Infrastructure mode or Ad-Hoc mode. In Infrastructure mode, the WET200 can be used to bridge a separate Ethernet segment wirelessly to the company network backbone. In Ad-Hoc mode, the WET200 communicates directly with other wireless devices, much like a wireless client card. The WET200 has been designed for use with 802.11g and 802.11b products, such as the WAP200 Wireless-G Access Point, in addition to various wireless adapters for notebook and desktop PC.

Go to the Linksys website at www.linksys.com for more information about wireless products.

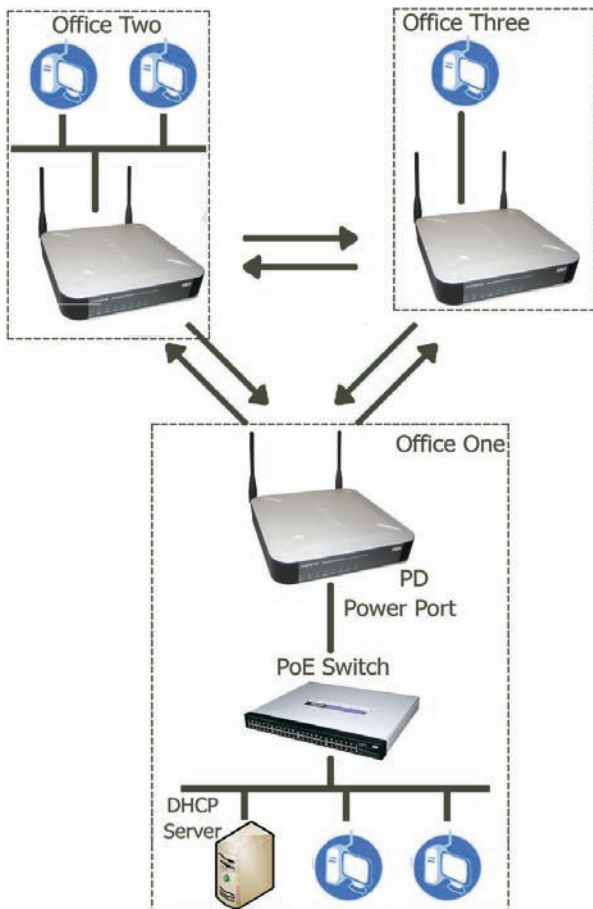
Example of WET200 in Infrastructure Mode



Example of WET200 in Infrastructure Mode

The above diagram shows a typical infrastructure wireless network setup where the WET200 is being used to manage multiple VLANs, with one VLAN connected wirelessly to the company network and Internet. In this example, the WET200 is connected to a wireless Access Point, which is in turn connected to the network backbone.

Example of WET200 in Ad-Hoc Mode



Example of WET200 in Ad-Hoc Mode

The WET200 can also be used to quickly set up a temporary network, as shown above. The diagram shows three wired networks, Office One, Office Two, and Office Three, each with a direct connection to the other wired networks via an Ad-Hoc network connection. The Bridge in Office One is connected to a Linksys switch that provides power to the Bridge. In this example, a DHCP server is set up to assign IP addresses automatically, since the WET200 does not have a built-in DHCP server. Alternatively, static IP addresses can be used.

Chapter 3: Product Overview

Front Panel

The Bridge's LEDs, where information about network activity is displayed, are located on the front panel.



Front Panel

- **POWER** (Green) Lights up when the Bridge is powered on.
- **PoE** (Green) Lights up when power is being supplied through Ethernet cable.
- **WIRELESS** (Green) Lights up when the wireless module is active on the Bridge. Flashes to indicate that the Bridge is actively sending or receiving data from a wireless device.
- **ETHERNET (1-5)** Lights up to indicate a functional 10/100 Mbps network link through the corresponding port (1 through 5) with an attached device. Blinks to indicate that the Bridge is actively sending or receiving data over that port.

Back Panel

The reset button, the Ethernet ports, and the power port are located on the back panel of the Bridge.



Back Panel

- **RESET** Press and hold the Reset button for approximately ten seconds to reset the Bridge to the factory default settings.



- **ETHERNET 1-5** These RJ-45 ports support network speeds of either 10 Mbps or 100 Mbps, and can operate in half and full-duplex modes. Auto-sensing technology enables each port to automatically detect the speed of the device connected to it (10 Mbps or 100 Mbps), and adjust its speed and duplex accordingly.

Port 5 also supports the IEEE 802.3af Power-over-Ethernet (PoE) PD standard that enables DC power to be supplied to the Bridge using wires in the connecting twisted-pair cable. This allows the Bridge to draw power directly from the Ethernet cable without requiring its own separate power source. If a PoE power source is not available, you can use the supplied AC power adaptor.

To connect a device to a port, you need to use Category 5 (or better) network cable.



- **POWER** The Power port is where you connect the AC power. This port is not used if you are using Power over Ethernet (PoE) to supply power through the Ethernet cable.

Chapter 4: Installation

Overview

This chapter explains how to place and connect the Bridge. Depending on your application, you might want to set up the device first before mounting the device. Refer to “Chapter 6: Advanced Configuration”.

Connection

There are two ways to install the Bridge: using Power over Ethernet (PoE), or using the supplied power adapter. Follow the appropriate procedure below.

Power over Ethernet

1. Connect one end of an Ethernet network cable to the LAN port on your PC, then connect the other end to Ethernet port 1, 2, 3, or 4 on the Bridge.



Connect the Bridge to a PC

2. Connect one end of an Ethernet network cable to your PoE-equipped network switch or router, and connect the other end of the cable to port 5 on the Bridge.



Connect the PoE Cable

3. The Power LED on the front panel lights up green as soon as the power is connected properly.”

Proceed to the section, “Placement Options.”

Power Adapter

1. Connect one end of an Ethernet network cable to the LAN port on your PC, then connect the other end to Ethernet port 1, 2, 3, 4, or 5 on the Bridge.



Connect the Bridge to a PC

2. Connect the included power adapter to the Bridge’s Power port. Then plug the power adapter into an electrical outlet.



Connect the Power Adapter

3. The Power LED on the front panel lights up green as soon as the power is connected properly.”

Proceed to the following section, “Placement Options.”

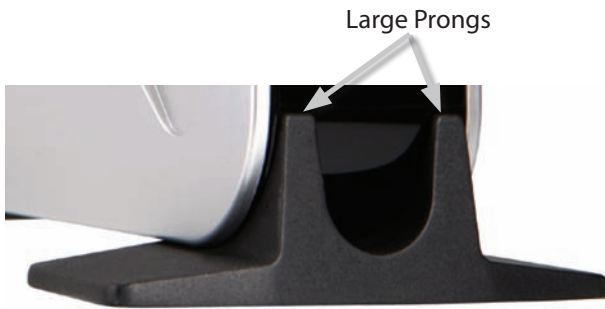
Placement Options

There are three ways to place the Bridge. The first way is to place it on a horizontal surface, so that it sits securely on its four rubber feet. The second way is to stand the Bridge upright on a horizontal surface by attaching the included stands. The third way is to mount it on a wall. The stand and wall-mount options are explained in further detail below.

Stand Option

1. Locate the Bridge’s left side panel.
2. The Bridge includes two stands. Position one of the stands with its two large prongs facing outward, then insert the short prongs into the small slots in the

Bridge, and push the stand upward until it snaps into place. Repeat this step with the other stand.

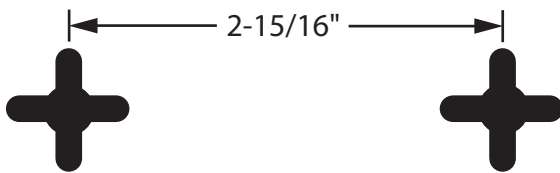


Stand Installation

Proceed to "Chapter 6: Advanced Configuration," for directions on how to set up the Bridge.

Wall-Mount Option

1. On the Bridge's back panel are two crisscross wall-mount slots.



Wall-Mount Slots on Bridge's Back Panel

2. Determine where you want to mount the Bridge, and install two screws that are 2-15/16" apart.
3. Line up the Bridge so that the wall-mount slots line up with the two screws.
4. Place the wall-mount slots over the screws and slide the Bridge down until the screws fit snugly into the wall-mount slots.

Proceed to "Chapter 6: Advanced Configuration," for directions on how to set up the Bridge..

Chapter 5: Quick Configuration Overview

Overview

The Ethernet switch of the WET200 is designed to be functional right out of the box with the default settings. In order to use the wireless bridge function, however, you must first perform a minimal configuration on the Bridge so that it can find and communicate with the access point. The Bridge can be configured through your web browser with the web-based utility. This chapter explains how to use the utility.

The utility can be accessed via web browsers, such as Microsoft Internet Explorer or Mozilla Firefox through the use of a computer that is networked with the Bridge.

For a basic network setup, most users only have to use the following screens of the Utility:

- **Setup** The *Setup* screen is the first screen displayed. Enter your basic network settings (IP address) here to allow your PC to access the web-based utility.



NOTE: If your network backbone has a DHCP server, you must first create a wireless connection between the bridge and the access point before you attempt to configure DHCP. Otherwise, the bridge will not be able to obtain an IP address and the web-based utility will be inaccessible. For information on how to create the wireless connection, see Chapter 6, "Advanced Configuration."

- **Password** Click the **Administration** tab, then select the *Password* sub tab. The Bridge's default password is **admin**. To secure the Bridge, change the Password from its default.
- **Wireless** Click the **Wireless** tab to access the *Wireless* screen to configure a wireless connection. This is most easily done using the **Site Survey** feature. Click **Site Survey**, then select your wireless network's access point from the list. If you are prompted for security settings, enter the requested information (such as passphrase or shared secret), The wireless bridge will now be connected to the access point.

Accessing the Web-Based Utility

To access the web-based utility, perform these steps:

1. Configure your PC with a static IP address in the same subnet as the Bridge's default IP address, **192.168.1.226**. If a DHCP server is to be connected to the switch, configure it to assign the IP address in subnet 192.168.1.0/24. Your PC will get an IP address in the subnet through the DHCP.
2. Launch your web browser, such as Internet Explorer or Mozilla Firefox, and enter the Bridge's default IP address, **192.168.1.226**, in the *Address* field. Press the **Enter** key.
3. Enter **admin** in the *User Name* field. The first time you open the web-based utility, use the default password, **admin**. (You can set a new password from *Administration > Password*) Then click **OK**.

When you are finished setting up the Bridge's IP address, either by manually assigning it a new IP address or by configuring it to use DHCP, move your Bridge to the desired network. You will have to use the new IP address the next time you access the web-based utility.

Navigating the Web-Based Utility

The web-based utility consists of the following five main tabs: **Setup**, **Wireless**, **Switch**, **Administration**, and **System Status**. Additional screens (sub tabs) will be available from most of the main tabs.

The following briefly describes the main and sub tabs of the Utility.

Setup

Setup Enter the Host Name and IP Address settings on this screen.

Wireless

You use the *Wireless* tabs to enter a variety of wireless settings for the Bridge.

Basic Settings Choose the wireless network mode (e.g. wireless-G), wireless channel, network type, and SSID configuration on this screen.

Wireless Security Use this screen to configure the Bridge's security settings including security mode, authentication, and encryption information.

Advanced Settings This screen allows you to configure the Bridge's more advanced wireless settings such as Transmission Rate, RTS Threshold, etc.

Switch

You use the *Switch* tabs to enter settings that are used by the Bridge's switching features.

Port Management Use this screen to configure the Administrative Status, Flow Control, Link, Duplex, and Speed of the Bridge's ports.

Port Mirroring Configure Port Mirroring on this screen.

VLAN This screen lets you configure Port-Based or 802.1Q VLAN settings.

MAC Based ACL Use this screen to create a MAC-based Access List (ACL) to control which MAC addresses can access your network.

QoS On this screen you configure the Quality of Service (QoS) settings on the Bridge's ports.

Spanning Tree This screen is used to configure the Spanning Tree Protocol settings on the Bridge.

MAC Table Use this screen to configure the Bridge's MAC address table settings.

Administration

You use the *Administration* tabs to manage the Bridge.

Password Use this screen to change the password.

SNMP This screen is used to enter the Simple Network Management Protocol (SNMP) settings.

Config Management Use this screen to save the Bridge's configuration to a file, and to restore the configuration from a file.

Factory Default Use this screen to reset the Bridge to its factory default settings.

Firmware Upgrade Upgrade the Bridge's firmware on this screen.

System Status

The *System Status* tab lets you view status information for your local network, wireless networks, and network performance.

System Status This screen displays basic system information, including system up time, firmware version, MAC address, and LAN settings.

Wireless Status This screen displays wireless network settings including SSID, network type, wireless mode and channel, security mode, transmit rate, and link quality.

Port Statistics This screen displays the current traffic statistics of the Bridge's Wireless and LAN ports.

Chapter 6: Advanced Configuration

Open your web browser, enter **http://192.168.1.226** in the *Address* field, and press the **Enter** key.

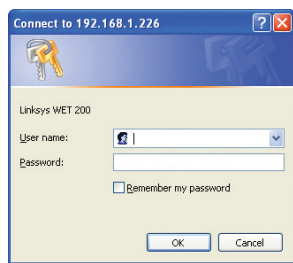


Address Bar



NOTE: The default IP address is **192.168.1.226**. If the IP address is changed using DHCP, enter the assigned IP address instead of the default.

The web-based utility's login screen appears. The first time you open the utility, enter **admin** (the default username) in the *username* field, enter **admin** in the *password* field, then click **OK**. You can change the username and password later from the Administration tab's *Password* screen.



Login Screen

After you log in, the *Setup* screen appears. To access other screens, select one of the five tabs at the top of the screen: **Setup**, **Wireless**, **Switch**, **Administration**, and **System Status**. Each tab contains additional screens. These tabs and their screens are explained in detail below.

Setup

The Setup tab contains one screen, the *Setup* screen. The *Setup* screen contains basic information for the Bridge.

Host Name This is the host name assigned to the Bridge. This host name will be published to your DNS server if the Bridge is configured to acquire its IP address through DHCP. In that case, Linksys recommends following company policy for host name assignment. The default name is **Linksys**.

Device Name You may assign any device name to the Bridge. This name is used only by the Bridge administrator for identification purposes. Unique, memorable names are helpful. The default name is **WET200**.

Contact Enter the name of the administrator responsible for the system.

Location This field is used for entering a description of where the Bridge is located, such as 3rd floor.

IP Address Type Select how the WET200 will obtain its IP address, either **Static IP Address** (default) or **Automatic Configuration-DHCP**.

- **Automatic Configuration-DHCP** The WET200 will obtain its IP address automatically from a DHCP server.



NOTE: If the DHCP server is not connected to the Bridge ports but will be accessed via the wireless interface, you must first create a wireless connection before attempting to enable DHCP on the WET200. Otherwise, the device will not be able to obtain an IP address and the web-based utility will be inaccessible. For detailed information on creating a wireless connection, see the "Wireless > Basic settings" section.

- **Static IP Address** To assign a static IP address to the Bridge, select this option and fill in the *IP Settings* fields. You should make sure that this IP address does not conflict with the IP addresses of any other devices on the network.

IP Settings If you set the *IP Address Type* field to **Static IP Address**, complete the following fields.

- **Local IP Address** Enter the IP address of the Bridge (default **192.168.1.226**) into this field.
- **Subnet Mask** Enter the subnet mask into this field.
- **Default Gateway** IP address of the gateway router (default **0.0.0.0**) on the current IP subnet, used to reach other IP networks.
- **Primary DNS Server** Enter the IP address of the DNS server (default **0.0.0.0**) into the field.
- **Secondary DNS Server** A second DNS address (default **0.0.0.0**) can be specified in this field.



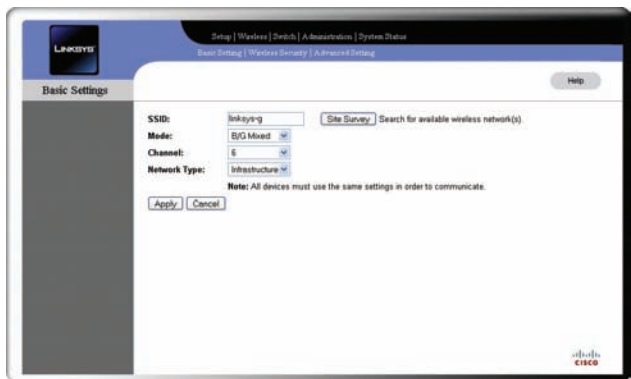
Setup Screen

Wireless

The Wireless tab contains the following three screens that allow you to configure the Bridge's wireless interfaces: *Basic Settings*, *Wireless Security*, and *Advanced Settings*.

Wireless > Basic Settings

The *Basic Settings* screen allows you to set the following information.



Wireless > Basic Settings

SSID The SSID is the network name used by all devices in a wireless network. It is case-sensitive, must not exceed 32 characters in length, and can contain any keyboard character except spaces. For added security, you should change the default SSID (**linksys**) to a unique name.

If you are using the WET200 in Infrastructure mode to communicate with a wireless access point, enter the SSID of the access point, or click **Site Survey** to see a list of available access points. For more information, see the "Wireless Site Survey" section.

If you are using the WET200 in Ad-Hoc mode to communicate with other clients on a wireless network, enter the SSID of that wireless network.

Mode Select the network mode of your wireless access point. If you are unsure of the mode, keep the default setting, **B/G Mixed**. Select **Disabled** to disable wireless access. If you use the Site Survey feature, it will search for available networks based on your mode configuration.

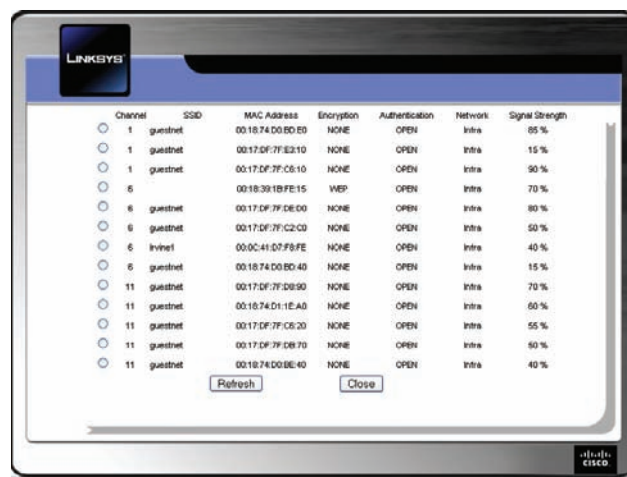
Channel Select the correct operating channel for your network from the drop-down menu. This should match the channel setting of the other devices in your wireless network. If you are using Infrastructure mode, this should match your Access Point's channel number. If you are using Ad-Hoc mode, this should match your peer device's channel number. If you use the Site Survey feature to connect to your wireless network, the channel setting is configured automatically.

Network Type Keep the default setting, **Infrastructure**, if you want your wireless Bridge to connect to another wired network through an Access Point. Select **Ad-Hoc** if you want to connect to another wired network through a second wireless Bridge which is also in Ad-Hoc mode.

Click **Apply** to apply your changes, or click **Cancel** to cancel your changes.

Wireless Site Survey

When you click **Site Survey** on the *Basic Settings* screen, the *Wireless Site Survey* screen appears. This screen shows all the wireless networks detected by the Bridge and their general information. You can use this screen to connect to one of these networks. If wireless security is configured in a network, the wireless security screen will also appear; enter the passphrase information on this screen.



Wireless > Basic Settings > Wireless Site Survey

For each wireless network detected, the following information is displayed:

Channel The channel setting.

SSID The network name. To join a wireless network, click the radio button to its left.

MAC Address The MAC address of the network's access point.

Encryption The encryption type.

Authentication The authentication type.

Network The type of the network.

Signal Strength The wireless signal strength in percent.

Click **Refresh** to obtain the most up-to-date data. Click **Close** to close this screen.

Wireless > Wireless Security

The *Wireless Security* screen allows you to configure security on your wireless network.



Wireless > Wireless Security - Security Disabled

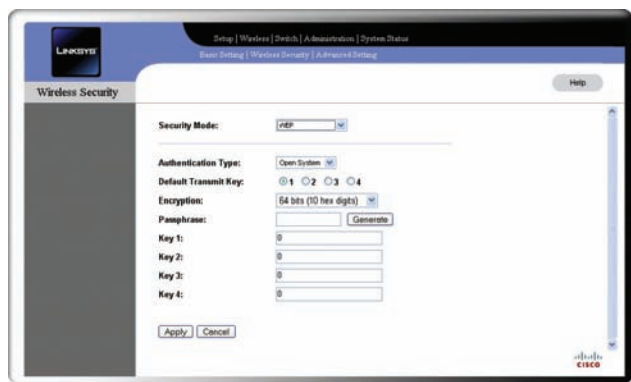
Security Mode Enter the security configuration to match the wireless Access Point that this bridge will connect to. To disable security, keep the default setting, **Disabled**. To enable security, select the desired type of security: **WEP**, **WPA-Personal**, **WPA2-Personal**, **WPA-Enterprise**, **WPA2-Enterprise**. Then fill in all the fields that appear on the screen. The fields you see depend on the type of security you select and are described in detail below.

WEP

Use the *WEP* screen to configure WEP encryption.



NOTE: WEP security is not recommended now due to its weak security protection. Users are urged to migrate to WPA or WPA2.



Wireless > Wireless Security - WEP

Authentication Type Select the 802.11 authentication type, either **Open System** (default) or **Shared Key**.

Default Transmit Key Select which WEP key (1-4) will be used when the Bridge sends data. Make sure the other wireless-equipped devices are using the same key.

Wireless-G Business Ethernet Bridge

Encryption In order to use WEP encryption, select **64-Bit (10 hex digits)** or **128-Bit (26 hex digits)** from the drop-down menu.

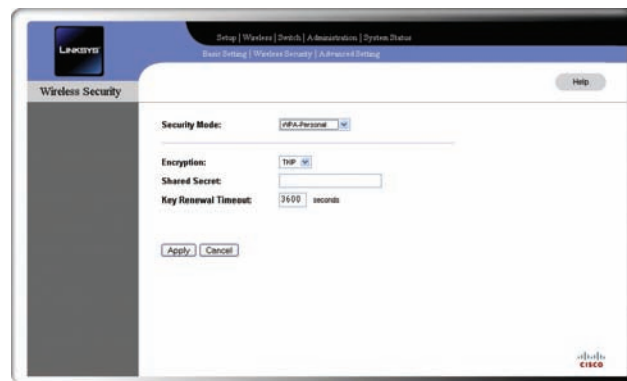
Passphrase Instead of manually entering WEP keys, you can enter a Passphrase. This Passphrase is used to generate one or more WEP keys. It is case-sensitive and should not be longer than 16 alphanumeric characters. (The Passphrase function is compatible with Linksys wireless products only. If you want to communicate with non-Linksys wireless products, you must enter your WEP key manually on those products.) After you enter the Passphrase, click **Generate** to create WEP key(s).

Key 1-4 If you are not using a Passphrase, then you can enter one or more WEP keys manually. In each key field, manually enter a set of values. (Do not leave a key field blank, and do not enter all zeroes. These are not valid key values.) If you are using 64-bit WEP encryption, then each key must consist of exactly 10 hexadecimal characters in length. If you are using 128-bit WEP encryption, then each key must consist of exactly 26 hexadecimal characters. Valid hexadecimal characters are **0-9** and **A-F**.

Click **Apply** to apply your changes, or click **Cancel** to cancel your changes.

WPA-Personal (aka WPA-PSK)

Use the *WPA Personal* screen to configure WPA Personal encryption for the Bridge.



Wireless > Wireless Security - WPA Personal

Encryption WPA offers two methods, **TKIP** and **AES**, for data encryption. Select the encryption method you want to use. The default is **TKIP**.

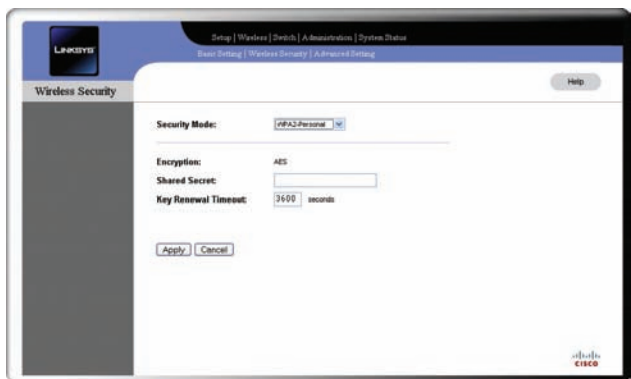
Shared Secret Enter a WPA Shared Secret of 8-63 characters.

Key Renewal Timeout Enter a Key Renewal Timeout period, which instructs the Access Point how often it should change the encryption keys. The default is **3600** seconds.

Click **Apply** to apply your changes, or click **Cancel** to cancel your changes.

WPA2-Personal

Use the *WPA2 Personal* screen to configure WPA2 Personal encryption for the Bridge.



Wireless > Wireless Security - WPA2 Personal

Encryption This is set to AES and cannot be changed as WPA2 always uses AES encryption.

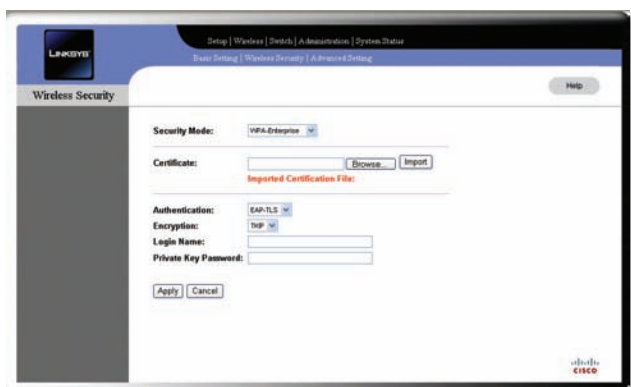
Shared Secret Enter a WPA Shared Secret of 8-63 characters.

Key Renewal Timeout Enter a Key Renewal Timeout period, which instructs the Access Point how often to change the encryption keys. The default is **3600** seconds.

Click **Apply** to apply your changes, or click **Cancel** to cancel your changes.

WPA-Enterprise

Use the *WPA Enterprise* screen to configure WPA Enterprise encryption for the Bridge.



Wireless > Wireless Security - WPA Enterprise

WPA Enterprise provides WPA security in coordination with a RADIUS server connected to the Bridge. WPA Enterprise offers two authentication methods, EAP-TLS and PEAP, as well as two encryption methods, TKIP and AES, with dynamic encryption keys.

Authentication Select the authentication method your network is using, either **EAP-TLS** (default) or **PEAP**.

EAP-TLS

EAP-TLS uses a Certificate file for authentication. The Login Name and Private Key Password are used to decrypt the certificate file.

Encryption Select either **TKIP** (default) or **AES** encryption.

Login Name Enter your login name for the RADIUS server.

Private Key Password Enter your password.

Certificate Enter the name of your certificate file or click **Browse** to locate it. Click **Import** to load and decode the certificate file. Click **Apply** to save the configuration for wireless authentication while being associated with an Access Point.

PEAP

EAP-PEAP uses the Login Name and Password to perform authentication with the RADIUS server.

Encryption Select either **TKIP** (default) or **AES** encryption.

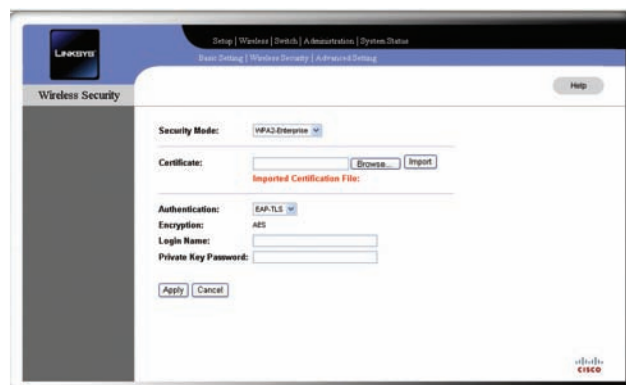
Login Name Enter your login name for the RADIUS server.

Private Key Password Enter your password.

When you are finished configuring the above settings, click **Apply** to apply your changes, or click **Cancel** to cancel your changes.

WPA2-Enterprise

Use the *WPA2 Enterprise* screen to configure WPA2 Enterprise encryption for the Bridge.



Wireless > Wireless Security - WPA2 Enterprise

WPA2 Enterprise provides WPA security in coordination with a RADIUS server connected to the Bridge. WPA2 Enterprise offers two authentication methods, EAP-TLS and PEAP, but only one encryption method, AES.

Authentication Select the authentication method your network is using, either **EAP-TLS** (default) or **PEAP**.

EAP-TLS

EAP-TLS uses a Certificate file for authentication. The Login Name and Private Key Password are used to decrypt the certificate file.

Encryption This is set to AES and cannot be changed.

Login Name Enter your login name for the RADIUS server.

Private Key Password Enter your password.

Certificate Enter the name of your certificate file or click **Browse** to locate it. Click **Import** to load and decode the certificate file. Click **Apply** to save the configuration for wireless authentication while being associated with an Access Point.

PEAP

EAP-PEAP uses the Login Name and Password to perform authentication with the RADIUS server.

Encryption This is set to AES and cannot be changed.

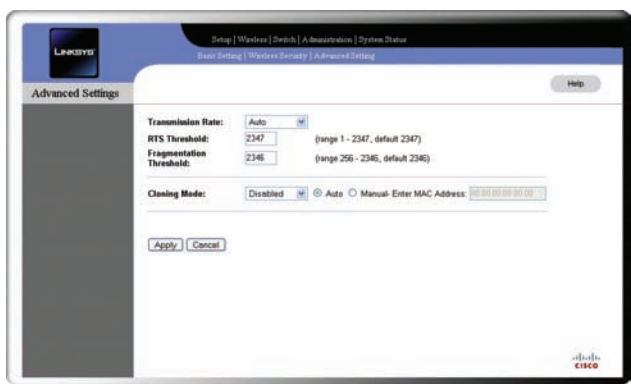
Login Name Enter your login name for the RADIUS server.

Private Key Password Enter your password.

When you are finished configuring the above settings, click **Apply** to apply your changes, or click **Cancel** to cancel your changes.

Wireless > Advanced Settings

This screen lets you configure advanced wireless settings. Linksys recommends letting the Bridge automatically adjust the parameters for maximum data throughput.



Wireless > Wireless Security - Advanced Settings

Transmission Rate The default setting is **Auto**. The range is from 1 to 54 Mbps. The rate should be set depending on the speed of your wireless network. You can select from a range of speeds, or keep the default setting, **Auto**, to have the Bridge automatically use the fastest possible data rate and enable the Auto-Fallback feature. Auto-Fallback negotiates the best possible connection speed between the Bridge and another wireless-equipped device.

RTSThreshold This determines how large a packet can be before the Bridge coordinates transmission and reception to ensure efficient communication. It should remain at its default setting of **2347**. If you encounter inconsistent data flow, only minor modifications are recommended.

Fragmentation Threshold The maximum size of a data packet before it is split to create a new packet. It should remain at its default setting of **2346**. A smaller setting means smaller packets, resulting in more packets per transmission. If you experience high packet error rates, you can decrease this value, but it will likely decrease overall network performance. Only minor modifications of this value are recommended.

Cloning Mode You can clone the MAC address of any network device onto the Bridge. To disable MAC address cloning, keep the default setting, **Disable**. To use the MAC cloning feature, select **Enable**.

If you have enabled MAC cloning, then select **Auto** if you want to clone the MAC address of the device currently connected to one of the LAN ports. The Bridge will actively scan for a new MAC address to be cloned whenever you disconnect and reconnect the Bridge through a LAN port. Select **Manual** if you want to specify a MAC address in the *Enter MAC Address* field. This is useful when the Bridge is connected to multiple devices through a switch or a hub.

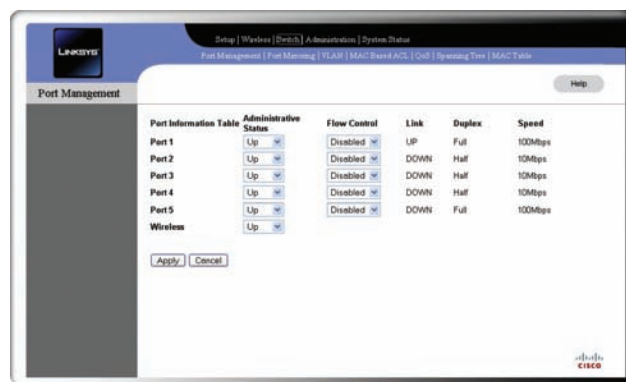
Click **Apply** to apply your changes, or click **Cancel** to cancel your changes.

Switch

The Switch tab contains seven screens that allow you to configure the advanced Ethernet switch features. The managed switch has five 10/100 Ethernet ports which allow advanced VLAN and QoS settings.

Switch > Port Management

The *Port Management* screen allows you to configure and set the status of each of the Bridge's ports—the five Ethernet ports and the wireless "virtual" interface.



Switch > Port Management

You can configure the Administrative Status and Flow Control of the five Ethernet ports. The link speed and duplex settings are done automatically through auto-negotiation. Flow control should be enabled to control network traffic during periods of congestion and prevent the loss of packets when port buffer thresholds are exceeded. The flow control feature is based on IEEE 802.3x which uses control frames to throttle the outgoing packets from a switch port to another IEEE 802.3x-compatible device. This feature is not available on the wireless interface.

Administrative Status To configure the administrative status of the port, select either **Up** (default) or **Down**. A port can be shut down even if it is physically connected.

Flow Control To configure flow control for the port, select either **Enabled** or **Disabled** (default).



NOTE: Flow Control should be disabled when QoS mode (802.1p, TOS, or DSCP) is configured. QoS mode allows priority differentiation during congestion instead of throttling off the traffic.

Link Displays the port's link status (UP or DOWN), which is a combination of the Administrative Status and the physical link connection.

Duplex Displays the port's duplex mode through auto-negotiation if the link is UP.

Speed Displays the port's speed in Mbps through auto-negotiation if the link is UP.

Click **Apply** to apply your changes, or click **Cancel** to cancel your changes.

Switch > Port Mirroring

Use this screen to configure Port Mirroring, which lets you mirror traffic to/from any port (including wireless) to Port 1 for real-time analysis. This can be helpful for troubleshooting purposes.



Switch > Port Mirroring

If this feature is enabled, Port 1 will only be able to communicate with the source port and monitor the source port's traffic. Port 1 will not be able to communicate with any other port while port mirroring is in effect.

Port Mirroring Setting

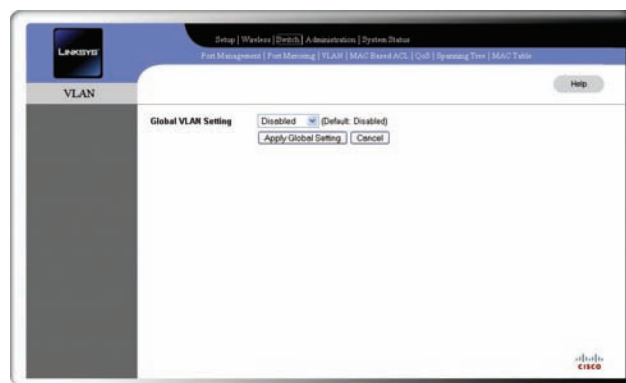
Type To use port mirroring, select the direction in which to monitor traffic: **Monitor Egress**, **Monitor Ingress**, or **Monitor Both**. To disable port mirroring, keep the default setting, **Disabled**.

Source Port If you have enabled port mirroring, select the port whose packets will be duplicated to Port 1: **Port 2** (default), **Port 3**, **Port 4**, **Port 5**, or **Wireless**.

Click **Apply** to apply your changes, or click **Cancel** to cancel your changes.

Switch > VLAN

The VLAN screen allows you to enable VLANs and select the type of VLANs to be used on the switch.



Switch > VLAN

A VLAN is a group of ports that can be located anywhere in a network, but communicate as if they are on the same physical segment. VLANs help to simplify network management by letting you move a device to a new VLAN without changing any physical connections. VLANs can be easily organized to reflect departmental groups (such as Marketing or R&D), usage groups (such as e-mail), or multicast groups (used for multimedia applications such as videoconferencing).

Global VLAN Setting To disable the VLAN feature, keep the default setting, **Disabled**. Otherwise select the type of VLAN to be used on the switch, either **Port Based** or **802.1Q**, then click **Apply Global Setting**.

- **Port Based** The switch uses port-based VLAN mapping to limit traffic between the ports.
- **802.1Q** The switch uses 802.1Q-based VLAN to configure VLAN membership for all ports.

802.1Q

In 802.1Q-based VLAN mode, tags are inserted into the data packets to distinguish between different VLANs.



Switch > VLAN - 802.1Q

A VLAN can include any of the five physical Ethernet ports (ports 1-5) as well as port 6, which controls the wireless interface and CPU access (management traffic and web-based utility access).



NOTE: The default 802.1Q settings define one VLAN whose VLAN ID (VID) is 1 and which includes ports 1-6. This is to allow access to the web-based utility from any of the ports. In addition, port 1 and port 6 (Wireless & CPU port) are permanently defined as part of VLAN 1; these settings cannot be changed. This ensures that you can always access the web-based utility through at least port 1, regardless of your particular 802.1Q VLAN settings.

You can create up to 16 VLANs on the Switch. The valid VLAN ID range is 1-4095. A VLAN with ID 1 has been pre-configured by default and cannot be deleted.

802.1Q VLAN Port Setting Each row of the table corresponds to one port. For each port, configure the 802.1Q VLAN settings, then click **Apply 802.1Q VLAN settings**.

- **Default VID** The default VLAN ID (VID) for this port. Port 1 and port 6 are set to 1 permanently. All other ports are set to 1 by default but may be changed.
- **Acceptable Frame Type** Select the type of frame to accept, either **All Frames** (default) or **Tagged Only**.
- **Ingress Filtering** Select this option to enable ingress filtering. Ingress filtering allows only packets with VLAN IDs that are configured in the port's membership table.. This option is not selected by default.

The following summarizes 802.1Q VLAN operation when a packet is received on a port:

1. If the packet has an 802.1Q tag, then go to step 3. If it does not have an 802.1Q tag, then continue to step 2.
2. If the Acceptable Frame Type field is set to **Tagged Only**, then the packet is dropped. Otherwise, an 802.1Q tag with the default VLAN ID is inserted.
3. If Ingress Filtering is disabled, then the frame is accepted.
4. If Ingress Filtering is enabled, then the membership table is checked to see if it contains the tag ID. If the ID is not found, the packet is dropped; otherwise the packet is accepted.

VLAN Membership Configuration This is located on the bottom half of the page. You use these fields to create the VLAN membership table.

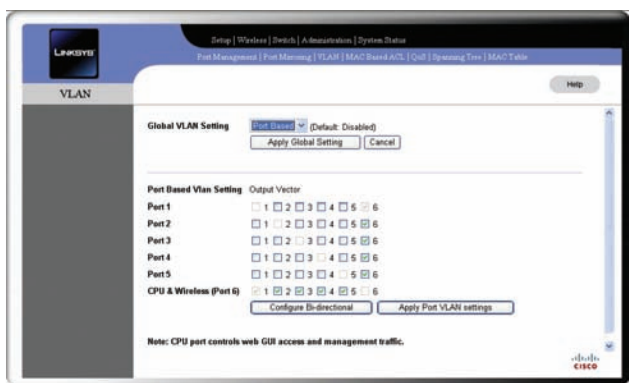
- **ID #** Enter the ID number of the VLAN to be created or modified. The valid range is 2 to 4095. Note that VLAN #1 is created by default and cannot be removed. By default all ports are part of VLAN #1 with membership status set to UnTag.
- **Port 1-6** For each VLAN ID to be created or modified, you can select the membership status for its ports from these drop-down menus. The default is **Drop**.
 - **Drop** This port will not be part of the VLAN.
 - **UnTag** This port will be part of the VLAN and frames will exit this port without an 802.1Q tag.
 - **Tag** This port will be part of the VLAN and frames will exit this port with an 802.1Q tag.
- **Add/Modify Entry** After you have entered the VLAN ID # and selected the membership status for its ports, click **Add/Modify Entry** to add or modify the entry in the VLAN membership table.
- **Delete VLAN Entry** Select the VLAN(s) to be deleted and click **Delete VLAN Entry** to remove those entries.

Port-Based

In port-based VLAN mode, the wireless bridge uses a port-based VLAN map to limit the traffic between the ports. A VLAN can include any of the five physical Ethernet ports (ports 1-5) as well as port 6, which controls the wireless interface and CPU access (management traffic and web-based utility access).



NOTE: The default port-based VLAN settings consist of connections between port 6 and each of the five Ethernet ports. This is to allow access to the web-based utility from any of the Ethernet ports. In addition, the connection between ports 1 and 6 is permanent and cannot be changed. This ensures that you can always access the web-based utility through at least port 1, regardless of your particular port-based VLAN settings.

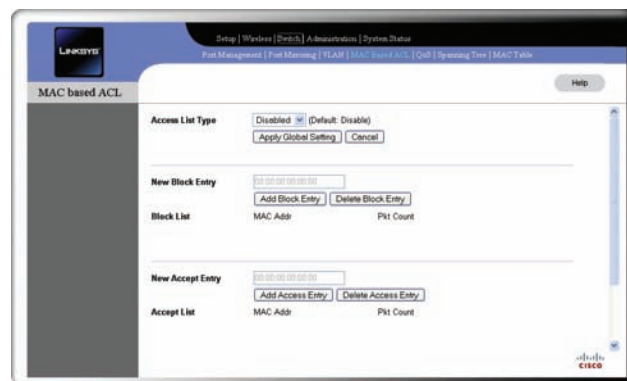


Switch > VLAN - Port-Based

Output Vector Use these fields to configure your VLANs as follows:

1. Each row of the table corresponds to one of the ports. For each port, specify its connections by selecting all of its exit ports. For example, to specify a VLAN connection from port 1 to port 2, select **2** in the row labeled *Port 1*.
2. Each exit port you select specifies a unidirectional connection only. (In the example in step 1, the direction is from port 1 to port 2.) To automatically add the connection in the opposite direction (from port 2 to port 1 in the example), click **Configure Bi-directional**.
3. When you are finished defining the connections for the VLAN(s), click **Apply Port VLAN Settings** to save and activate your VLAN configuration.

Switch > MAC Based ACL



Switch > MAC Based ACL

An Access List (ACL) is a list of source MAC addresses that is used to grant or deny access. If a packet passes from the wireless port to a LAN port or vice versa, the Bridge will check if the packet's source MAC address matches any entry in the access list, then use the match result to pass or drop the packet. However, packets from LAN port to LAN port are not checked. You can select from two types of Access Lists. A Block list blocks specific MAC addresses specified in the table; all other MAC addresses are accepted. An Accept list only accepts the MAC addresses listed in the table; all other MAC addresses are blocked.

Access List Type To disable the Access List feature, keep the default setting, **Disabled**. To enable Access Lists, select **Accept** or **Block**, then click **Apply Global Setting**.

If you choose to use an Accept list, you must remember to include your computer's MAC address in the list before you click **Apply**. Failure to do so may result in your computer being denied access to the device.

New Block Entry To block packets with a specific MAC address, enter the MAC address in this field, and click **Add Block Entry**. To unblock the MAC address, enter the MAC address in the field, click **Delete Block Entry**, then click **Apply Global Setting**.

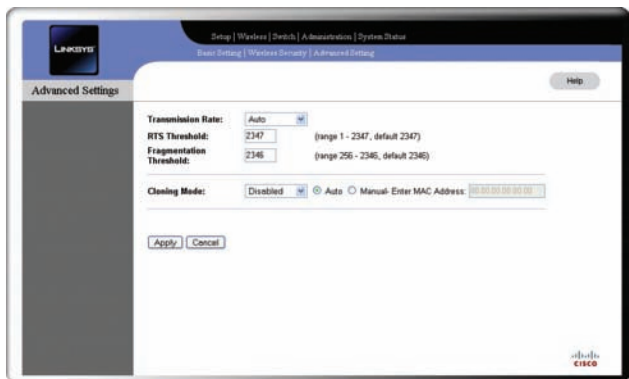
Block List Displays a list of blocked MAC addresses and number of packets dropped for each address.

New Accept Entry To accept packets with a specific MAC address, enter the MAC address in this field, and click **Add Access Entry**. To unaccept the MAC address, enter the MAC address in the field, click **Delete Access Entry**, then click **Apply Global Setting**.

Accept List Displays a list of accepted MAC addresses and number of packets accepted for each address.

Drop Count, Accept Count When Access List is enabled, these display the total number of packets dropped and accepted. Click **Refresh** to display the latest information.

Switch > QoS



Switch > QoS

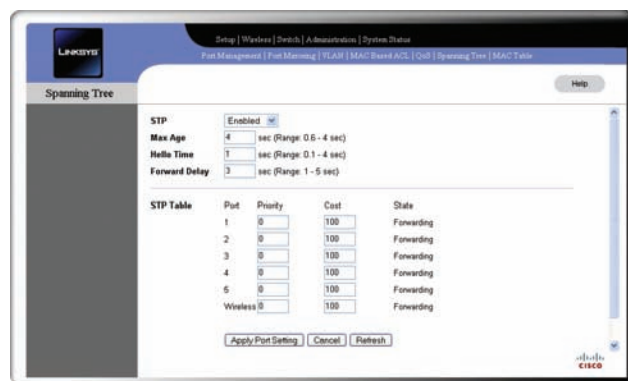
The Quality of Service (QoS) configuration in this switch has two parts: QoS Mode and Rate Limiting. QoS Mode is used to classify and prioritize packets. Rate Limiting is used to limit the amount of bandwidth used by data passing in or out of the switch port.

QoS Port Setting Select the QoS settings for ports 1-5 and the wireless port, then click **Apply Port Setting**.

- **QoS Mode** Select the desired QoS mode: **Force Priority** (default), **Trust 802.1p**, **Trust IP TOS**, or **Trust IP DSCP**.
- **Default Priority (on Ingress)** Select **Critical** (default), **Low**, **Medium**, or **High**. This is only used if the *QoS Mode* field is set to **Force Priority**.
- **Ingress Rate** Select the maximum rate allowed for the port. For ports 1-5, the range is **128 kbps** to **64 Mbps** and for the wireless port the range is **128 kbps** to **16 Mbps**. The default is **No Limit**.
- **Egress Rate** Select the maximum rate allowed for the port. For ports 1-5, the range is **128 kbps** to **64 Mbps** and for the wireless port the range is **128 kbps** to **16 Mbps**. The default is **No Limit**.

Switch > Spanning Tree

This screen allows you to configure the Spanning Tree Protocol (STP) settings for the switch. STP can be used to detect and disable network loops, and to provide backup links between switches, bridges or routers. This allows the switch to interact with other bridging devices (that is, an STP-compliant switch, bridge or router) in your network to ensure that only one route exists between any two stations on the network, and provide backup links which automatically take over when a primary link goes down. STP is enabled by default.



Switch > Spanning Tree

STP To enable STP, keep the default setting, **Enabled**. To disable STP, select **Disabled**.

Max Age The maximum time in seconds that a device can wait without receiving a configuration message before attempting to reconfigure. The range is from **0.6** to **4** seconds. The default value is **4** seconds.

Hello Time The interval in seconds at which the root device transmits a configuration message. The range is from **0.1** to **4** seconds. The default value is **1** second.

Forward Delay The maximum time in seconds that this device will wait before changing states, such as from discarding to learning to forwarding. The range is **1** to **5** seconds. The default is **3** seconds.

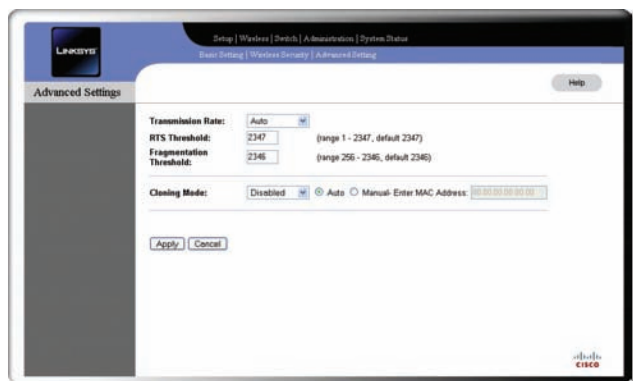
STP Table Select the settings for the Spanning Tree table, then click **Apply Port Setting**.

- **Priority** The priority of this port. The smaller the priority value, the higher the priority. If two ports form a loop, the port with higher priority will change to block state, thus breaking the loop.
- **Cost** The path cost to forward packets from this port. It is usually inversely proportional to the port's speed.
- **State** The Spanning Tree protocol: state: **Blocking**, **Learning**, or **Forwarding**.

To apply the settings, click **Apply Port Setting**. To cancel, click **Cancel**. To see the latest information, click **Refresh**.

Switch > MAC Table

Use this screen to configure the MAC address table for the switch. The MAC table is used to switch frames to the correct ports. Before the MAC table is populated, a frame is broadcast to all ports. Learning mode is enabled, then the MAC table is populated automatically.



Switch > MAC Table

Global ATU Setting This is a global MAC address table setting. Select the desired settings, then click **Apply Global Setting**.

- **Address Learning** This indicates if the switch should automatically learn the MAC address of packets. Select **Enable Learning** (default) or **Disable Learning**.
- **Age timer** Detects and purges obsolete table entries, such as when a connected device moves from one port to another, by checking the idle timeout value of the entries. The range is from **1** to **300** seconds. You can also disable this feature. The default is **300 seconds**.

Static MAC Entry Besides dynamically learned entries, the MAC table can also contain static, user-defined entries that you enter here. The *MAC Address* field shows the destination MAC address. The check boxes specify the output ports (1-5 and Wireless) where a packet is routed if its destination MAC address matches the *MAC Address* field. You can specify more than one output port. To add an entry, enter the destination MAC address, select the output port(s), and click **Add New Entry**. The new entry will then appear in the *Status Address Table* list. Note that static MAC entries are not affected by the Age timer and can only be deleted manually.

Static Address Table This lists the static MAC address entries and their port vector settings. To delete an entry, select its check box and click **Delete Selected Entry**.

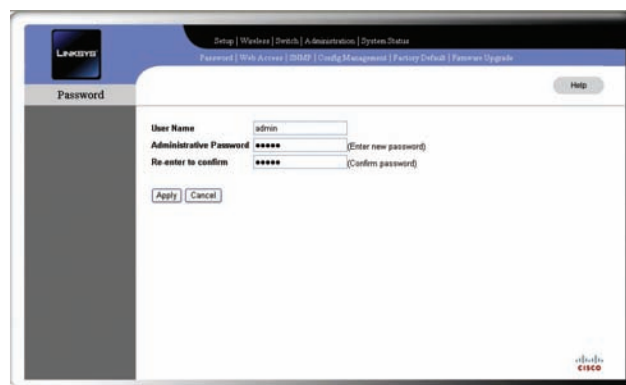
Address Table Dump A complete dump of the MAC address table, including both learned and static entries. If a topology change occurs, click **Refresh** to remove the learned entries and force the entries to be relearned. At most 64 entries are displayed per page. If there are more than 64 entries, click **Get Next Page** to see more entries.

Administration

The Administration tab is used for various administrative tasks, such as to change the login password, configure SNMP, save and restore system configuration, restore the factory default settings, and upgrade the firmware.

Administration > Password

This screen allows you to change the username and/or password for the Bridge. It is recommended that you change the password from its default setting, **admin**.



Administration > Password

User Name The current user name is displayed (default **admin**). To change the user name, enter the new user name.

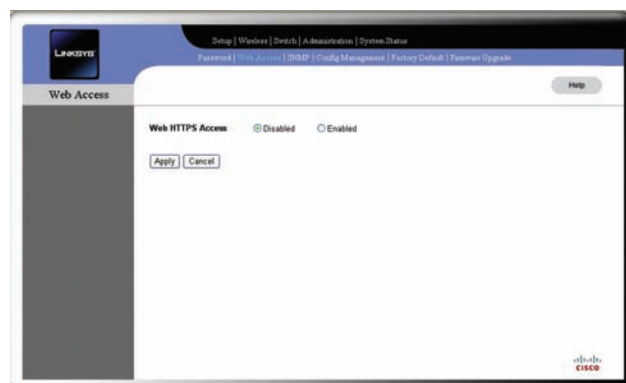
Administrative Password Enter a new password from 4 to 63 characters in length.

Re-enter to confirm Enter password again to confirm.

Click **Apply** to apply your changes, or click **Cancel** to cancel your changes.

Administration > Web Access

This screen allows you to enable or disable https access to the utility.



Administration > Web Access

Web HTTPS Access If you want to enable https access, select **Enabled**. The default setting is **Disabled**.

Click **Apply** to apply your changes, or click **Cancel** to cancel your changes.

Administration > SNMP

This screen is used to configure Simple Network Management Protocol (SNMP), a popular network monitoring and management protocol.



Administration > SNMP

SNMP To disable SNMP, leave **Disabled** selected (default). To enable SNMP, select **Enabled**, then select the type of SNMP to use, either **SNMP V1 & V2** or **SNMP V3**.

Device Name Enter the name of the Wireless Bridge.

Contact Enter the contact information for the Bridge.

Location Enter the location of the Wireless Bridge.

SNMP V.3 Username Enter the username for the SNMP V3 administrator who will access and manage the MIB objects.

Authentication Password Enter the authentication password for the SNMP V3 administrator. The password must be at least 8 characters in length.

Privacy Password Enter the privacy password for the SNMP V3 administrator. The password must be at least 8 characters in length.

Get Community Enter the name of your Get community.

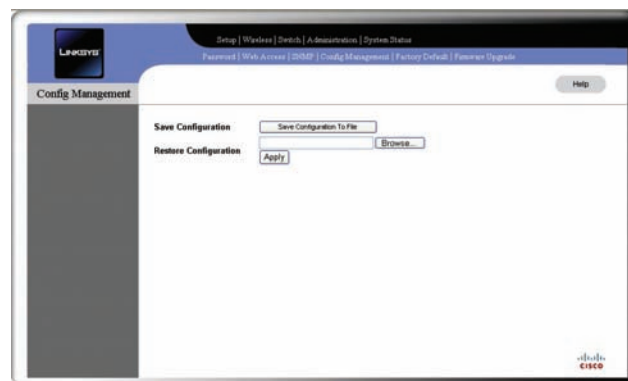
Set Community Enter the name of your Set community.

SNMP Trap-Community Enter the name of your Trap community.

SNMP-Trusted Host Enter the IP address of your Trusted host. To have the Access Point respond to SNMP messages from every host in your LAN, enter **0.0.0.0**.

SNMP Trap-Destination Enter the destination IP address for traps. To prevent traps from being sent to any of your LAN hosts, enter **0.0.0.0**.

Administration > Configuration Management



Administration > Configuration Management

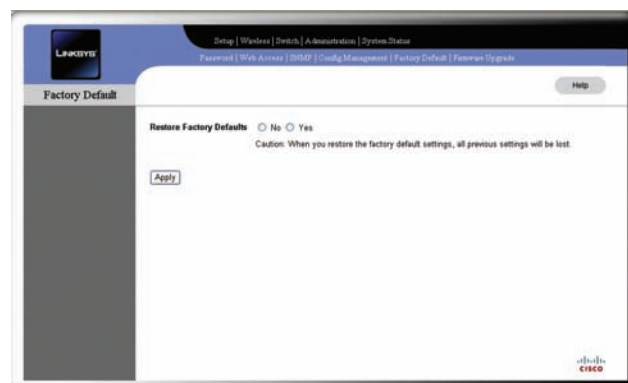
This screen lets you save the system configuration to a file as well as restore the system configuration from a previously saved file.

To save the configuration, click **Save Configuration To File**, then follow the prompts to save the file to your computer.

To restore the configuration from a file, enter the name of the file or click **Browse** to locate it, then click **Apply**.

Administration > Factory Defaults

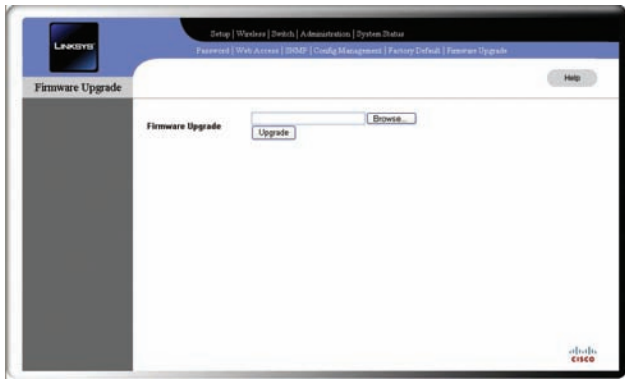
This screen is used to restore the Bridge's factory default settings. When you do this, you will lose all previously configured settings and cannot recover that configuration unless you have saved it using the *Configuration Management* screen.



Administration > Factory Defaults

Select **Yes** next to **Restore Factory Defaults**, then click **Apply** to restore the defaults and restart the Bridge.

Administration > Firmware Upgrade



Administration > Firmware Upgrade

This screen allows you to upgrade the Bridge's firmware after you have downloaded a new firmware file from the Linksys website. Firmware should only be upgraded if you experience problems with the Bridge.

Enter the name of the firmware file or click **Browse** to locate the file on your computer, then click **Upgrade** to begin the upgrade.

System Status

The System Status tab displays the Bridge's current status and configuration information. These screens only display information and cannot be used to change any settings.

System Status > System Status

This is the System Status tab's default screen. It displays basic status information for the Bridge.



System Status > System Status

System Up Time The Bridge's live time.

Firmware Version The version number of the currently installed firmware.

MAC Address The MAC address currently assigned to the Bridge.

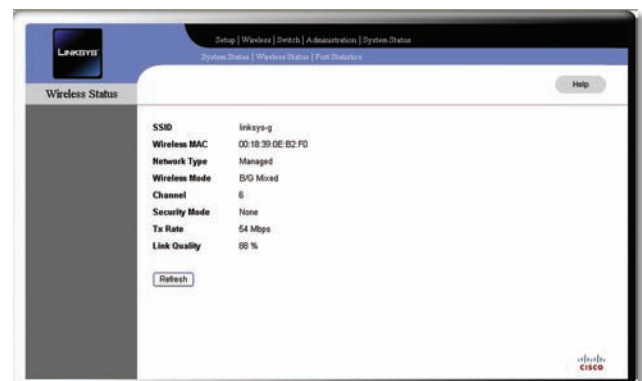
LAN Settings The basic LAN settings.

- **IP Address, Subnet mask** The Bridge's IP address and subnet mask.
- **Gateway** The IP address of the Bridge's gateway.

Click **Refresh** to display the most current information.

System Status > Wireless Status

This screen displays status information for the Bridge's wireless network.



System Status > Wireless Status

SSID Name of the wireless network.

Network Type Wireless network type (**Infrastructure** or **Ad-Hoc**).

Wireless Mode Wireless network mode (**disabled**, **B/G Mixed**, etc.).

Channel Wireless network channel number.

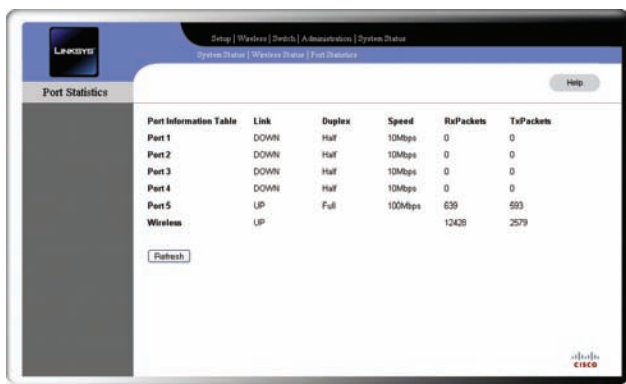
Security Mode Security mode (**disabled**, **WEP**, **WPA-Personal**, etc.)

Tx Rate Wireless network transmission rate.

Link Quality Quality level of the wireless connection.

Click **Refresh** to display the most current information.

System Status > Port Statistics



Port Information Table	Link	Duplex	Speed	RxPackets	TxPackets
Port 1	DOWN	Half	10Mbps	0	0
Port 2	DOWN	Half	10Mbps	0	0
Port 3	DOWN	Half	10Mbps	0	0
Port 4	DOWN	Half	10Mbps	0	0
Port 5	UP	Full	100Mbps	639	593
Wireless	UP			12428	2579

Refresh

System Status > Port Statistics

This screen displays status information for the Bridge's ports.

Port 1-5, Wireless Displays the following settings for each of these ports.

- **Link** Status of link, either **UP** (connected) or **DOWN** (not connected).
- **Duplex** The duplex mode resulting from auto-negotiation, either **Half** or **Full**.
- **Speed** The speed resulting from auto-negotiation, either **10Mbps** or **100Mbps**.
- **RxPackets** Total number of packets received.
- **TxPackets** Total number of packets sent.

Click **Refresh** to display the most current information.

Appendix A: Wireless Security Checklist

Wireless networks are convenient and easy to install, so homes with high-speed Internet access are adopting them at a rapid pace. Because wireless networking operates by sending information over radio waves, it can be more vulnerable to intruders than a traditional wired network. Like signals from your cellular or cordless phones, signals from your wireless network can also be intercepted. Since you cannot physically prevent someone from connecting to your wireless network, you need to take some additional steps to keep your network secure.



1. Change the default wireless network name or SSID

Wireless devices have a default wireless network name or Service Set Identifier (SSID) set by the factory. This is the name of your wireless network, and can be up to 32 characters in length. Linksys wireless products use **linksys** as the default wireless network name. You should change the wireless network name to something unique to distinguish your wireless network from other wireless networks that may exist around you, but do not use personal information (such as your Social Security number) because this information may be available for anyone to see when browsing for wireless networks.



2. Change the default password

For wireless products such as access points and routers, you will be asked for a password when you want to change their settings. These devices have a default password set by the factory. The Linksys default password is **admin**. Hackers know these defaults and may try to use them to access your wireless device and change your network settings. To thwart any unauthorized changes, customize the device's password so it will be hard to guess.



3. Enable MAC address filtering

Linksys routers give you the ability to enable Media Access Control (MAC) address filtering. The MAC address is a unique series of numbers and letters assigned to every networking device. With MAC address filtering enabled, wireless network access is provided solely for wireless devices with specific MAC addresses. For example, you can specify the MAC address of each computer in your home so that only those computers can access your wireless network.



4. Enable encryption

Encryption protects data transmitted over a wireless network. Wi-Fi Protected Access (WPA/WPA2) and Wired Equivalency Privacy (WEP) offer different levels of security for wireless communication. Currently, devices that are Wi-Fi certified are required to support WPA2, but are not required to support WEP.

A network encrypted with WPA/WPA2 is more secure than a network encrypted with WEP, because WPA/WPA2 uses dynamic key encryption. To protect the information as it passes over the airwaves, you should enable the highest level of encryption supported by your network equipment.

WEP is an older encryption standard and may be the only option available on some older devices that do not support WPA.

General Network Security Guidelines

Wireless network security is useless if the underlying network is not secure.

- Password protect all computers on the network and individually password protect sensitive files.
- Change passwords on a regular basis.
- Install anti-virus software and personal firewall software.
- Disable file sharing (peer-to-peer). Some applications may open file sharing without your consent and/or knowledge.

Additional Security Tips

- Keep wireless routers, access points, or gateways away from exterior walls and windows.
- Turn wireless routers, access points, or gateways off when they are not being used (at night, during vacations).
- Use strong passphrases that are at least eight characters in length. Combine letters and numbers to avoid using standard words that can be found in the dictionary.

Appendix B: Glossary

This glossary contains some basic networking terms you may come across when using this product.



WEB: For additional terms, please visit the glossary at www.linksys.com/glossary

Access Mode Specifies the method by which user access is granted to the system.

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.

Access Profiles Allows network managers to define profiles and rules for accessing the device. Access to management functions can be limited to user groups, which are defined by the following criteria:

- Ingress interfaces
- Source IP address and/or Source IP subnets.

ACE Filters in Access Control Lists (ACL) that determine which network traffic is forwarded. An ACE is based on the following criteria:

- Protocol
- Protocol ID
- Source Port
- Destination Port
- Wildcard Mask
- Source IP Address
- Destination IP Address

ACL (Access Control List) Access Control Lists are used to grant, deny, or limit access devices, features, or applications.

Auto-negotiation Allows 10/100 Mbps or 10/100/1000 Mbps Ethernet ports to automatically establish the optimal duplex mode, flow control, and speed.

Back Pressure A mechanism used with Half Duplex mode that enables a port not to receive a message.

Bandwidth The transmission capacity of a given device or network.

Bandwidth Assignments Indicates the amount of bandwidth assigned to a specific application, user, and/or interface.

Baud Indicates the number of signaling elements transmitted each second.

Best Effort Indicates that traffic is assigned to the lowest priority queue, and packet delivery is not guaranteed.

Bit A binary digit.

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

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

Bridge A device that connect two networks. Bridges are hardware specific, however they are protocol independent. Bridges operate at Layer 1 and Layer 2 levels.

Broadcast Domain Devices sets that receive broadcast frames originating from any device within a designated set. Routers bind Broadcast domains, because routers do not forward broadcast frames.

Broadcast Storm An excessive amount of broadcast messages simultaneously transmitted across a network by a single port. Forwarded message responses are heaped onto the network, overloading network resources or causing the network to time out.

Burst A packet transmission at faster than normal rates. Bursts are limited in time and only occur under specific conditions.

Burst Size Indicates the burst size transmitted at a faster than normal rate.

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.

CBS (Committed Burst Size) Indicates the maximum number of data bits transmitted within a specific time interval.

CIR (Committed Information Rate) The data rate is averaged over a minimum time increment.

Class Maps An aspect of Quality of Service system that is comprised of an IP ACL and/or a MAC ACL. Class maps are configured to match packet criteria, and are matched to packets in a first-fit fashion.

Combo Ports A single logical port with two physical connections, including an RJ-45 connection and a SFP connection.

Communities Specifies a group of users which retain the same system access rights.

CoS (Class of Service) The 802.1p priority scheme. CoS provides a method for tagging packets with priority information. A CoS value between 0-7 is added to the Layer II header of packets, where zero is the lowest priority and seven is the highest.

DDNS (Dynamic Domain Name System) 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 (Dynamic Host Configuration Protocol) 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.

DHCP Clients An Internet host using DHCP to obtain configuration parameters, such as a network address.

DHCP Server An Internet host that returns configuration parameters to DHCP clients.

DNS (Domain Name Server) 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.

Download To receive a file transmitted over a network.

DSL (Digital Subscriber Line) An always-on broadband connection over traditional phone lines.

DSCP (DiffServ Code Point) Provides a method of tagging IP packets with QoS priority information.

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

EIGRP (Enhanced Interior Gateway Routing Protocol) Provides fast convergence, support for variable-length subnet mask, and supports multiple network layer protocols.

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.

Firmware The programming code that runs a networking device.

Flow Control Enables lower speed devices to communicate with higher speed devices. This is implemented by the higher speed device refraining from sending packets.

FTP (File Transfer Protocol) 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.

GARP (General Attributes Registration Protocol) Registers client stations into a multicast domain.

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

GBIC (GigaBit Interface Converter) A hardware module used to attach network devices to fiber-based transmission systems. GBIC converts the serial electrical signals to serial optical signals and vice versa.

GVRP (GARP VLAN Registration Protocol) Registers client stations into a VLANs.

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

HTTP (HyperText Transport Protocol) The communications protocol used to connect to servers on the World Wide Web.

HTTPS (HyperText Transport Protocol Secure) An extension to the standard HTTP protocol that provides confidentiality by encrypting the traffic from the website. By default this protocol uses TCP port 443.

ICMP (Internet Control Message Protocol) Allows the gateway or destination host to communicate with the source host. For example, to report a processing error.

IGMP (Internet Group Management Protocol) Allows hosts to notify their local switch or router that they want to receive transmissions assigned to a specific multicast group.

IP (Internet Protocol) 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 (Internet Protocol Security) A VPN protocol used to implement secure exchange of packets at the IP layer.

ISP (Internet Service Provider) A company that provides access to the Internet.

Jumbo Frames Enable transporting identical data in fewer frames. Jumbo Frames reduce overhead, lower processing time, and ensure fewer interrupts.

LAG (Link Aggregated Group) Aggregates ports or VLANs into a single virtual port or VLAN.

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

MAC (Media Access Control) Address The unique address that a manufacturer assigns to each networking device.

Mask A filter that includes or excludes certain values, for example parts of an IP address.

Mbps (MegaBits Per Second) One million bits per second; a unit of measurement for data transmission.

MD5 (Message Digest 5) An algorithm that produces a 128-bit hash. MD5 is a variation of MD4, and increases MD4 security. MD5 verifies the integrity of the communication and authenticates the origin of the communication.

MDI (Media Dependent Interface) A cable used for end stations.

MDIX (Media Dependent Interface with Crossover) A cable used for hubs and switches.

MIB (Management Information Base) MIBs contain information describing specific aspects of network components.

Multicast Transmits copies of a single packet to multiple ports.

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

NMS (Network Management System) An interface that provides a method of managing a system.

OID (Object Identifier) Used by SNMP to identify managed objects. In the SNMP Manager/Agent network management paradigm, each managed object must have an OID to identify it.

Packet A unit of data sent over a network.

Ping (Packet Internet Groper) An Internet utility used to determine whether a particular IP address is online.

Policing Determines if traffic levels are within a specified profile. Policing manages the maximum traffic rate used to send or receive packets on an interface.

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

Port Mirroring Monitors and mirrors network traffic by forwarding copies of incoming and outgoing packets from one port to a monitoring port.

Power over Ethernet (PoE) A technology enabling an Ethernet network cable to deliver both data and power.

QoS (Quality of Service) Provides policies that contain sets of filters (rules). QoS allows network managers to decide how and what network traffic is forwarded according to priorities, application types, and source and destination addresses.

RADIUS (Remote Authentication Dial-In User Service) A protocol that uses an authentication server to control network access.

RJ-45 (Registered Jack-45) An Ethernet connector that holds up to eight wires.

RMON (Remote Monitoring) Provides network information to be collected from a single workstation.

Router A networking device that connects multiple networks together.

RSTP (Rapid Spanning Tree Protocol) Detects and uses network topologies that allow a faster convergence of the spanning tree, without creating forwarding loops.

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

SMTP (Simple Mail Transfer Protocol) The standard e-mail protocol on the Internet.

SNMP (Simple Network Management Protocol) A widely used network monitoring and control protocol.

SSH Secure Shell. A utility that uses strong authentication and secure communications to log in to another computer over a network.

SSL (Secure Socket Layer) Encryption technology for the Internet used to provide secure transactions, such as the transmission of credit card numbers for e-commerce.

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

STP (Spanning Tree Protocol) Prevents loops in network traffic. The Spanning Tree Protocol (STP) provides tree topography for any arrangement of bridges. STP provides one path between end stations on a network, eliminating loops.

Subnet (Sub-network) Subnets are portions of a network that share a common address component. In TCP/IP networks, devices that share a prefix are part of the same subnet. For example, all devices with a prefix of 157.100.100.100 are part of the same subnet.

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

Switch Filters and forwards packets between LAN segments. Switches support any packet protocol type.

TACACS+ (Terminal Access Controller Access Control System Plus) Proprietary Cisco enhancement to Terminal Access Controller Access Control System (TACACS). Provides additional support for authentication, authorization, and accounting.

TCP (Transmission Control Protocol) A network protocol for transmitting data that requires acknowledgement from the recipient of data sent.

TCP/IP (Transmission Control Protocol/Internet Protocol) 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 (Trivial File Transfer Protocol) 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.

Trunking Link Aggregation. Optimizes port usage by linking a group of ports together to form a single trunk (aggregated groups).

TX Rate Transmission Rate.

UDP (User Data Protocol) Communication protocol that transmits packets but does not guarantee their delivery.

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

Upload To transmit a file over a network.

URL (Uniform Resource Locator) The address of a file located on the Internet.

VLAN (Virtual Local Area Networks) Logical subgroups that constitute a Local Area Network (LAN). This is done in software rather than defining a hardware solution.

WAN (Wide Area Network) Networks that cover a large geographical area.

Wildcard Mask Specifies which IP address bits are used, and which bits are ignored. A wild card mask of 255.255.255.255 indicates that no bit is important. A wildcard of 0.0.0.0 indicates that all the bits are important.

For example, if the destination IP address is 149.36.184.198 and the wildcard mask is 255.36.184.00, the first two bits of the IP address are used, while the last two bits are ignored.

Appendix C: Specifications

Specifications

Model	WET200
Standards	IEEE802.11g, IEEE802.11b, IEEE802.3, IEEE802.3u, IEEE802.3af (Power over Ethernet), 802.1p (QoS Priority), 802.1Q (VLAN), 802.1X (Security Authentication), 802.11i-Ready (Security WPA2), 802.11e-Ready (Wireless QoS)
Ports	5 10/100 Base-T Ethernet, 12 VDC Power
Cabling Type	UTP CAT 5
LEDs	Power, PoE, Wireless, Ethernet 1-5
Operating System	Linux

Setup/Configuration

Web User Interface (UI)	Built-in Web UI for Easy Browser-based Configuration (HTTP/HTTPS)
-------------------------	---

Management

SNMP Version	SNMP Version 1, 2c, 3
Web Firmware Upgrade	Firmware Upgradable Through Web Browser
DHCP	DHCP Client

Operating Modes

Wireless Client	Infrastructure or Ad-Hoc
-----------------	--------------------------

Wireless

Spec/Modulation	Radio and Modulation Type: 802.11b/DSSS, 802.11g/OFDM
Channels	Operating Channels: 11 North America, 13 Most of Europe (ETSI and Japan)
Internal Antennas	None
External Antennas	2 (Omnidirectional) SMA Detachable
Transmit Power	Transmit Power (Adjustable) @ Normal Temperature Range: 11b: 12 ± 1 dBm, 11g: 16 ± 1 dBm
Antenna Gain	2 dBi
Receiver Sensitivity	11g: 54 Mbps @ -69 dBm, 11b: 11 Mbps @ -82 dBm

Security

WEP/WPA/WPA2	WEP 64-bit/128-bit, WPA-PSK, WPA2-PSK, WPA-ENT, WPA2-ENT
Access Control	MAC-Based ACL between wired and wireless interfaces
802.1X	IEEE 802.1X Support

Quality of Service

QoS	4 Queues; Queue Mapping on Ingress Based on Default Priority, 802.1p Tag, DSCP & IP ToS; Rate Limiting on Both Ingress and Egress Direction
-----	---

VLAN

802.1Q VLAN	Support for up to 16 VLANs on the switch
-------------	--

Environmental

Dimensions W x H x D	6.69" x 8.07" x 7.68" (170 x 205 x 195 mm)
Unit Weight	0.76 lb (345 g)
Power	12V 0.5A DC Input, IEEE802.3af-Compliant PoE
Certification	FCC, ICES-003, CE
Operating Temp.	32 to 104°F (0 to 40°C)
Storage Temp.	-4 to 158°F (-20 to 70°C)
Operating Humidity	10 to 85% Noncondensing
Storage Humidity	5 to 90% Noncondensing

Appendix D: 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 E: Regulatory Information

FCC Statement

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

This product has been tested and complies with the specifications 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 according to 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 is found by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna
- Increase the separation between the equipment or devices
- Connect the equipment to an outlet other than the receiver's
- Consult a dealer or an experienced radio/TV technician for assistance

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.

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 and your body.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter. IEEE 802.11b or 802.11g operation of this product in the USA is firmware-limited to channels 1 through 11.

Safety Notices

- Caution: To reduce the risk of fire, use only No.26 AWG or larger telecommunication line cord.
- Do not use this product near water, for example, in a wet basement or near a swimming pool.
- Avoid using this product during an electrical storm. There may be a remote risk of electric shock from lightning.



WARNING: This product contains lead, known to the State of California to cause cancer, and birth defects or other reproductive harm. Wash hands after handling.

Industry Canada Statement

This Class B digital apparatus complies with Canadian ICES-003 and RSS210.

Operation is subject to the following two conditions:

1. This device may not cause interference and
2. This device must accept any interference, including interference that may cause undesired operation of the device. This device has been designed to operate with an antenna having a maximum gain of 2dBi. Antenna having a higher gain is strictly prohibited per regulations of Industry Canada. The required antenna impedance is 50 ohms.

To reduce potential radio interference to other users, the antenna type and its gain should be so chosen that the EIRP is not more than required for successful communication.

Industry Canada 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.

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

Avis d'Industrie Canada

Cet appareil numérique de la classe B est conforme aux normes NMB-003 et RSS210 du Canada.

L'utilisation de ce dispositif est autorisée seulement aux conditions suivantes :

1. il ne doit pas produire de brouillage et
2. il doit accepter tout brouillage radioélectrique reçu, même si ce brouillage est susceptible de compromettre le fonctionnement du dispositif. Le dispositif a été conçu pour fonctionner avec une antenne ayant un gain maximum de 2 dBi. Les règlements d'Industrie Canada interdisent strictement l'utilisation d'antennes dont le gain est supérieur à cette limite. L'impédance requise de l'antenne est de 50 ohms.

Afin de réduire le risque d'interférence aux autres utilisateurs, le type d'antenne et son gain doivent être choisis de façon à ce que la puissance isotrope rayonnée équivalente (p.i.r.e.) ne soit pas supérieure au niveau requis pour obtenir une communication satisfaisante.

Avis d'Industrie Canada concernant l'exposition aux radiofréquences :

Ce matériel est conforme aux limites établies par IC en matière d'exposition aux radiofréquences dans un environnement non contrôlé. Ce matériel doit être installé et utilisé à une distance d'au moins 20 cm entre l'antenne et le corps de l'utilisateur.

L'émetteur ne doit pas être placé près d'une autre antenne ou d'un autre émetteur, ou fonctionner avec une autre antenne ou un autre émetteur.

Wireless Disclaimer

The maximum performance for wireless is derived from IEEE Standard 802.11 specifications. Actual performance can vary, including lower wireless network capacity, data throughput rate, range and coverage. Performance depends on many factors, conditions and variables, including distance from the access point, volume of network traffic, building materials and construction, operating system used, mix of wireless products used, interference and other adverse conditions.

Avis de non-responsabilité concernant les appareils sans fil


Les performances maximales pour les réseaux sans fil sont tirées des spécifications de la norme IEEE 802.11. Les performances réelles peuvent varier, notamment en fonction de la capacité du réseau sans fil, du débit de la transmission de données, de la portée et de la couverture. Les performances dépendent de facteurs, conditions et variables multiples, en particulier de la distance par rapport au point d'accès, du volume du trafic réseau, des matériaux utilisés dans le bâtiment et du type de construction, du système d'exploitation et de la combinaison de produits sans fil utilisés, des interférences et de toute autre condition défavorable.

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.


Български (Bulgarian) - Информация относно опазването на околната среда за потребители в Европейския съюз

Европейска директива 2002/96/EC изисква уредите, носещи този символ  върху изделието и/или опаковката му, да не се изхвърлят с несортирани битови отпадъци. Символът обозначава, че изделието трябва да се изхвърля отделно от сметосъбирането на обикновените битови отпадъци. Вашата отговорност е този и другите електрически и електронни уреди да се изхвърлят в предварително определени от държавните или общински органи специализирани пунктове за събиране. Правилното изхвърляне и рециклиране ще спомогнат да се предотвратят евентуални вредни за околната среда и здравето на населението последствия. За по-подробна информация относно изхвърлянето на вашите стари уреди се обърнете към местните власти, службите за сметосъбиране или магазина, от който сте закупили уреда.


Čeština (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 Haushaltsmüll 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.


Ελληνικά (Greek) - Στοιχεία περιβαλλοντικής προστασίας για πελάτες εντός της Ευρωπαϊκής Ένωσης

Η Κοινοτική Οδηγία 2002/96/ΕΚ 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 κοινотικά 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 nešķīrotā 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 mājāsaimniecības 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  kurios pakuotė yra pažymėta šiuo simboliu (įveskite simbolį), 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 Kliġenti fl-Unjoni Ewropea

Id-Direttiva Ewropea 2002/96/KE titlob li t-tagħmir li jkun fi h simbolu  fuq il-prodott u/jew fuq l-ippakkjar ma jistax jintrema ma' skart municipali li ma giex 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 hulladékészállítási rendszerektől elkülönített eljárást kell alkalmazni. Az Ön felelőssége, hogy ezt, és más elektromos és elektronikus berendezéseit a kormányzati vagy a helyi hatóságok által kijelölt gyűjtőrendszerben 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 das 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.


Română (Romanian) - Informații de mediu pentru clienții din Uniunea Europeană

Directiva europeană 2002/96/CE impune ca echipamentele care prezintă acest simbol  pe produs și/sau pe ambalajul acestuia să nu fie casate împreună cu gunoiul menajer municipal. Simbolul indică faptul că acest produs trebuie să fie casat separat de gunoiul menajer obișnuit. Este responsabilitatea dvs. să cașati acest produs și alte echipamente electrice și electronice prin intermediul unităților de colectare special desemnate de guvern sau de autoritățile locale. Casarea și reciclarea corecte vor ajuta la prevenirea potențialelor consecințe negative asupra sănătății mediului și a oamenilor. Pentru mai multe informații detaliate cu privire la casarea acestui echipament vechi, contactați autoritățile locale, serviciul de salubritate sau magazinul de la care ați achiziționat produsul.


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.



WEB: For additional information, please visit www.linksys.com

Appendix F: Contact Information

Linksys Contact Information	
Website	http://www.linksys.com
Support Site	http://www.linksys.com/support
FTP Site	ftp.linksys.com
Advice Line	800-546-5797 (LINKSYS)
Support	800-326-7114
RMA (Return Merchandise Authorization)	http://www.linksys.com/warranty



NOTE: Details on warranty and RMA issues can be found in the Warranty section of this Guide.
