LINKSYS®
A Division of Cisco Systems, Inc.

USER GUIDE

BUSINESS SERIES

Wireless-G Business Ethernet Bridge

Model: WET200

cisco

About This Guide

Icon Descriptions

While reading through the User Guide you may encounter various icons designed to call attention to a specific item. 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

Table of Contents

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

Table of Contents

Switch > MAC Table 18
Administration 18
Administration > Password 18
Administration > SNMP 18
Administration > Configuration Management 19
Administration > Factory Defaults 19
Administration > Firmware Upgrade 19
System Status 20
System Status > System Status 20
System Status > Wireless Status 20
System Status > Port Statistics 20

Appendix A: Wireless Security Checklist 21

General Network Security Guidelines 21
Additional Security Tips 21

Appendix B: Glossary 22

Appendix C: Specifications 26

Appendix D: Warranty Information 27

Appendix E: Regulatory Information 28

FCC Statement 28
FCC Radiation Exposure Statement 28
Safety Notices 28
Industry Canada Statement 28
Industry Canada Radiation Exposure Statement: 28
Avis d'Industrie Canada 29
Avis d'Industrie Canada concernant l'exposition aux radiofréquences : 29
Wireless Disclaimer 29
Avis de non-responsabilité concernant les appareils sans fil 29
User Information for Consumer Products Covered by EU Directive 2002/96/EC on Waste Electric and Electronic Equipment (WEEE) 30

Appendix F: Contact Information 34

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 qualilty 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.

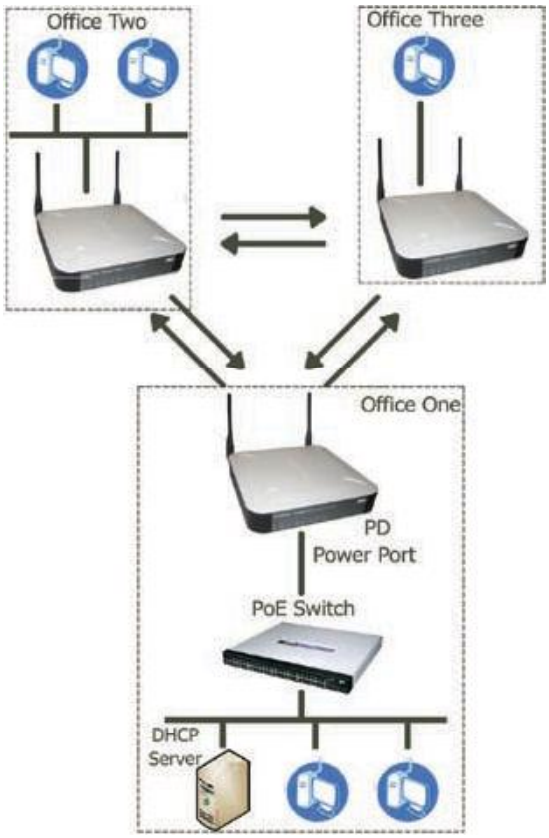
Go to the Linksys website at **www.linksys.com** for more information about wireless products.

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."

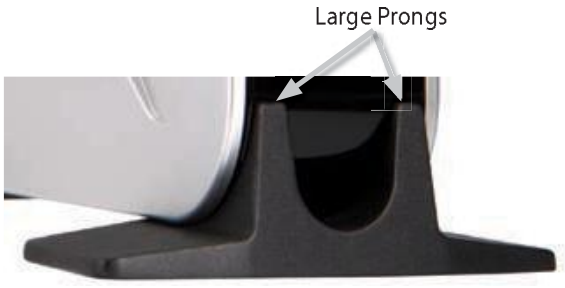
Placement Options

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.

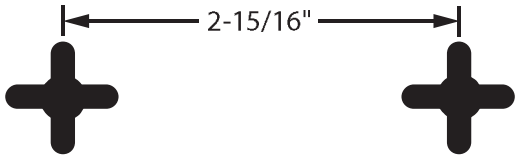


Stand Installation

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 utiity'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.

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.

RTS Threshold 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 64 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.

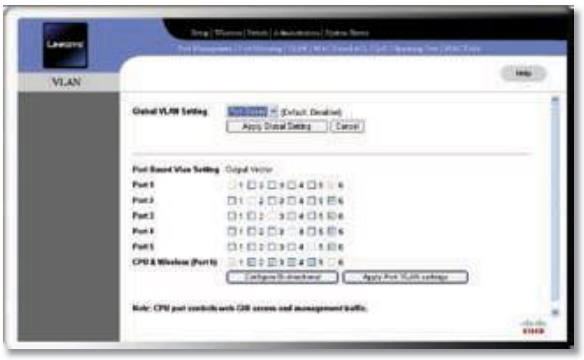
VLAN Membership Configuration This is located on the bottom half of the page. You use these fields to create the VLAN membership table.

- **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.