LINKSYS®

A Division of Cisco Systems, Inc.

2.4GHz 802.11b

Wireless-B Ethernet Bridge

WIRELESS

User Guide

CISCO SYSTEMS

Model No. **WET11**

Copyright and Trademarks

How to Use this Guide

Your guide to the Wireless-B Ethernet Bridge has been designed to make understanding networking with the Wireless-B Ethernet Bridge easier than ever. Look for the following items when reading this guide:

This checkmark means there is a Note of interest and is something you should pay special attention to while using the Wireless-B Ethernet Bridge.

This exclamation point means there is a Caution or warning and is something that could damage your property or the Wireless-B Ethernet Bridge.

This question mark provides you with a reminder about something you might need to do while using the Wireless-B Ethernet Bridge.

In addition to these symbols, there are definitions for technical terms that are presented like this:

word: *definition.*

Also, each figure (diagram, screenshot, or other image) is provided with a figure number and description, like this:

Figure 0-1: Sample Figure Description

Figure numbers and descriptions can also be found in the “List of Figures” section in the “Table of Contents”.

Table of Contents

List of Figures

Chapter 1: Introduction

Welcome

Thank you for choosing the Wireless-B Ethernet Bridge. The versatile Wireless-B Ethernet Bridge can make any wired Ethernet-equipped device a part of your wireless network. At home, use the Wireless-B Ethernet Bridge to connect game consoles, set-top boxes, or computers into your wireless network to share your high-speed network connection. In the office, convert your Ethernet-wired printer, scanner, camera, notebook or desktop into a wireless networked device.

It's completely driver-free, so it works on any platform and under any operating system! Since there are no drivers to load, setup is a snap—just plug it into your device and configure the network settings through your web browser.

You can also use the Wireless-B Ethernet Bridge as a kind of “cable-less cable” to connect remote areas together. Maybe Shipping is all the way across the warehouse from Receiving. Or maybe you want to set up a home office in your detached garage. With a Wireless-B Ethernet Bridge in the garage, and another one (or a Wireless Access Point) in the house, you're connected—with no cabling hassle.

Let the Wireless-B Ethernet Bridge from Linksys open up exciting new possibilities for your wireless network.

***802.11b**: an IEEE wireless networking standard that specifies a maximum data transfer rate of 11Mbps and an operating frequency of 2.4GHz.*

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

What's in this Guide?

This user guide covers the steps for setting up and using the Wireless-B Ethernet Bridge.

- Chapter 1: Introduction
  This chapter describes the Wireless-B Ethernet Bridge applications and this user guide.
- Chapter 2: Planning your Wireless Network
  This chapter describes the basics of wireless networking.
- Chapter 3: Getting to Know the Wireless-B Ethernet Bridge
  This chapter describes the physical features of the Bridge.
- Chapter 4: Connecting the Wireless-B Ethernet Bridge for Setup
  This chapter instructs you on how to connect the Bridge to your network for setup.
- Chapter 5: Setting Up the Wireless-B Ethernet Bridge
  This chapter explains how to set up the Bridge using the Setup Wizard.
- Chapter 6: Connecting the Wireless-B Ethernet Bridge for Network Use
  This chapter explains how to connect the Bridge to a network device so the device can join your wireless network.
- Chapter 7: Using the Wireless-B Ethernet Bridge Web-based Utility
  This chapter explains how to use the Web-Based Utility to configure the settings on the Bridge.
- Appendix A: Troubleshooting
  This appendix describes some problems and solutions, as well as frequently asked questions, regarding installation and use of the Wireless-B Ethernet Bridge.
- Appendix B: Wireless Security
  This appendix explains the risks of wireless networking and some solutions to reduce the risks.
- Appendix C: Upgrading Firmware
  This appendix instructs you on how to upgrade the firmware on the Bridge should you need to do so.
- Appendix D: Glossary
  This appendix gives a brief glossary of terms frequently used in networking.
- Appendix E: Windows Help
  This appendix describes how you can use Windows Help for instructions about networking, such as installing the TCP/IP protocol.

- Appendix F: Specifications
  This appendix provides the technical specifications for the Bridge.

- Appendix G: Warranty Information
  This appendix supplies the warranty information for the Bridge.

- Appendix H: Regulatory Information
  This appendix supplies the regulatory information regarding the Bridge.

- Appendix I: Contact Information
  This appendix provides contact information for a variety of Linksys resources, including Technical Support.

Chapter 2: Planning Your Wireless Network

Network Topology

A wireless local area network (WLAN) is exactly like a regular local area network (LAN), except that each computer in the WLAN uses a wireless device to connect to the network. Computers in a WLAN share the same frequency channel and SSID, which is an identification name shared by the wireless devices belonging to the same wireless network.

Ad-Hoc versus Infrastructure Mode

Unlike wired networks, wireless networks have two different modes in which they may be set up: infrastructure and ad-hoc. An infrastructure configuration is a WLAN and wired LAN communicating to each other through an access point. An ad-hoc configuration is wireless-equipped computers communicating directly with each other. Choosing between these two modes depends on whether or not the wireless network needs to share data or peripherals with a wired network or not.

If the computers on the wireless network need to be accessible by a wired network or need to share a peripheral, such as a printer, with the wired network computers, the wireless network should be set up in Infrastructure mode. The basis of Infrastructure mode centers around an access point, which serves as the main point of communications in a wireless network (see Figure 2-1). Access points transmit data to PCs equipped with wireless network cards, which can roam within a certain radial range of the access point. Multiple access points can be arranged to work in succession to extend the roaming range, and can be set up to communicate with your Ethernet hardware as well.

If the wireless network is relatively small and needs to share resources only with the other computers on the wireless network, then the Ad-Hoc mode can be used. Ad-Hoc mode allows computers equipped with wireless transmitters and receivers to communicate directly with each other, eliminating the need for an access point. The drawback of this mode is that in Ad-Hoc mode, wireless-equipped computers are not able to communicate with computers on a wired network. And, of course, communication between the wireless-equipped computers is limited by the distance and interference directly between them.

Figure 2-2 shows a typical scenario of four Wireless-B Ethernet Bridges in ad-hoc mode. Figure 2-3 shows a typical wireless bridging scenario using two Wireless-B Ethernet Bridges. Each wireless network is connected to a Wireless-B Ethernet Bridge through a switch. A separate notebook computer is equipped with a wireless network adapter and can communicate with either wireless network when it is configured with the appropriate SSID and channel.

LAN (Local Area Network)*: the computers and networking products that make up your local network.*

SSID*: your wireless network’s name.*

Infrastructure*: a wireless network that is bridged to a wired network via an access point.*

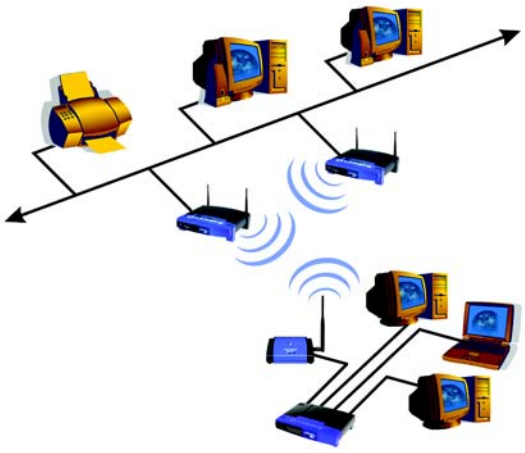


Figure 2-1: Infrastructure Mode

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

With these, and many other, Linksys products, your networking options are limitless. Go to the Linksys website at *www.linksys.com* for more information about products that work with the Wireless-B Ethernet Bridge.

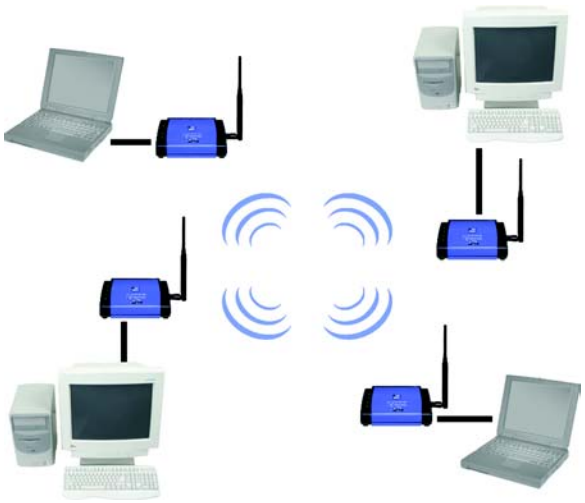


Figure 2-2: Ad-Hoc Mode

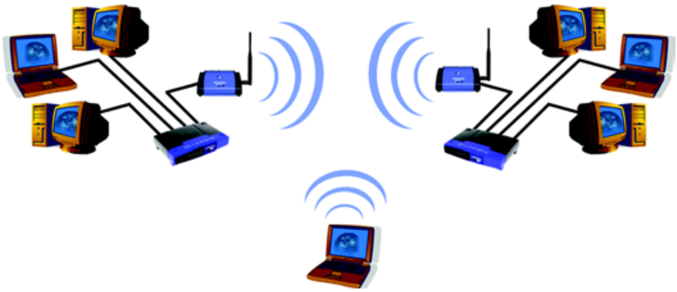


Figure 2-3: Wireless Bridging Using Two Bridges

Chapter 3: Getting to Know the Wireless-B Ethernet Bridge

The Back Panel

All connections to the Bridge are made through the ports in its back panel, shown in Figure 3-1.

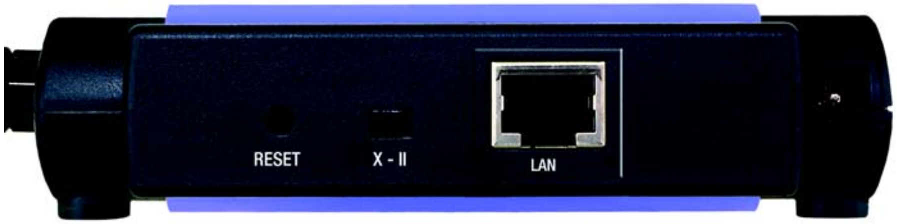


Figure 3-1: Back Panel

Reset The Reset button resets the Bridge to its factory default settings.

X-II The X-II (MDI/MDI-X) slide switch offers a choice between two settings. Use the X setting if you are connecting the Bridge to a network adapter. Use the II setting if you are connecting the Bridge to a hub or switch.

LAN The LAN port is where you will connect the Ethernet network cable.

Power The Power port is where you will connect the power adapter.

Important: Resetting the Wireless-B Ethernet Bridge will erase all of your settings (WEP encryption, wireless settings, etc.) and replace them with the factory defaults. Do not reset the Wireless-B Ethernet Bridge if you want to retain these settings.

The Front Panel

Network activity with the Bridge is shown on the LEDs, shown in Figure 3-2.

PWR Green. The PWR LED will light up when the Bridge is powered on.

DIAG Green. The DIAG LED will light up when there is a connection error. Re-establish the connection to eliminate the error.

LAN Green. The LAN LED will be lit steadily when the Bridge is connected to the wired network. The LED will flash when there is wired network traffic.

WLAN Green. The WLAN LED will be lit steadily when the Bridge is connected to the wireless network. The LED will flash when there is wireless network traffic.

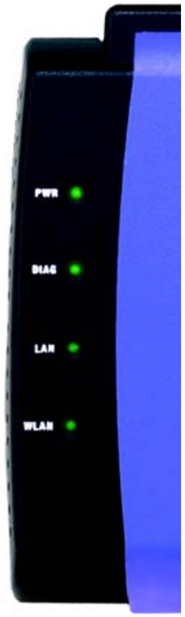


Figure 3-2: Front Panel

Chapter 4: Connecting the Wireless-B Ethernet Bridge for Setup

1. Attach the Bridge’s antenna.
2. Plug the included Ethernet network cable into the LAN port on the back panel of the Bridge, shown in Figure 4-1.
3. The X-II (MDI/MDI-X) slide switch offers a choice between two settings. Slide the X-II switch to the X position if you are connecting the Bridge to a PC’s network adapter. Slide the X-II selection switch to the II position if you are connecting the Bridge to a hub or switch.
4. Plug the other end of the Ethernet network cable into the RJ-45 port of the hub, switch, or PC you wish to use to configure the Bridge.
5. Plug the supplied power adapter into the Power port on the back panel of the Bridge, shown in Figure 4-2. Then plug the other end into an electrical outlet.

Proceed to the next section, “Chapter 5: Setting Up the Wireless-B Ethernet Bridge.”

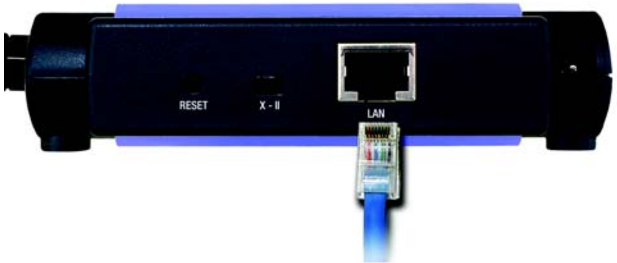


Figure 4-1: Connect the Ethernet Network Cable

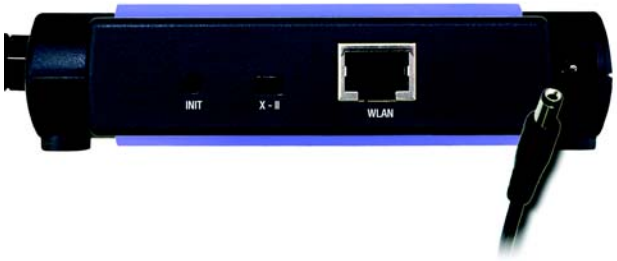


Figure 4-2: Connect the Power Adapter

Chapter 5: Setting Up the Wireless-B Ethernet Bridge

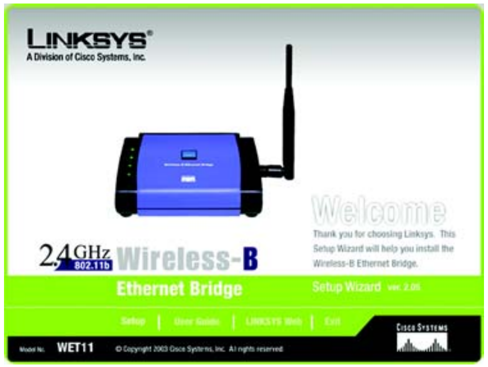
Overview

Now that you've connected the Wireless-B Ethernet Bridge to your wired network, you are ready to set it up. The Setup Wizard will guide you through all the necessary steps.

Setup Wizard

1. Insert the Setup CD-ROM into your PC's CD-ROM drive. The Setup Utility should run automatically, and the screen in Figure 5-1 should appear. If it does not, click the **Start** button and choose **Run**. In the field that appears, enter **D:\setup.exe** (if "D" is the letter of your CD-ROM drive).

- Setup - Click the **Setup** button to proceed with the Setup Wizard.
- User Guide - Click the **User Guide** button to open the PDF file of this User Guide.
- LINKSYS Web - Click the **LINKSYS Web** button to access the Linksys website using an active Internet connection.
- Exit - Click the **Exit** button to exit the Setup Wizard.

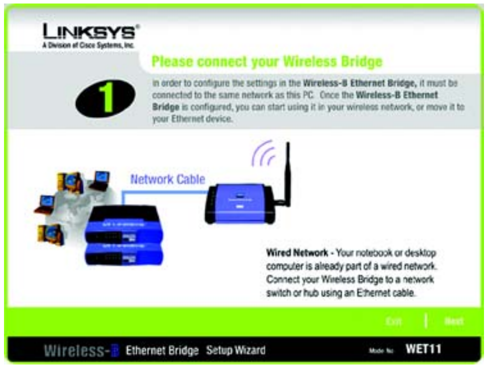


Thank you for choosing Linksys. This Setup Wizard will help you install the Wireless-B Ethernet Bridge.

Figure 5-1: Welcome

2. Click the **Setup** button to begin the setup process.

3. Make sure the Bridge is correctly connected to your wired network (see Figure 5-2). Then click the **Next** button.


LINKSYS®
A Division of Cisco Systems, Inc.
Please connect your Wireless Bridge
1
Network Cable
Exit
Next
Wireless-B Ethernet Bridge Setup Wizard
Model No. WET11

In order to configure the settings in the **Wireless-B Ethernet Bridge,** it must be connected to the same network as this PC. Once the **Wireless-B Ethernet Bridge** is configured, you can start using it in your wireless network, or move it to your Ethernet device.

Wired Network - Your notebook or desktop computer is already part of a wired network. Connect your Wireless Bridge to a network switch or hub using an Ethernet cable.

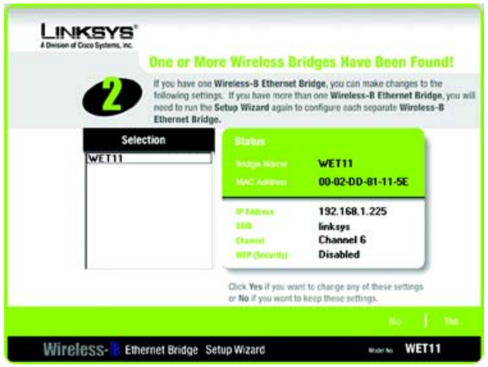
Figure 5-2: Check Connection

4. The screen shown in Figure 5-3 displays a list of Wireless-B Ethernet Bridges on your network, along with the status information for each Bridge. (If you have only one Bridge on your network, it will be the only one displayed.) Select the Bridge you are currently installing by clicking its name in the *Selection* box. Write down the IP address of the Wireless-B Ethernet Bridge, so you can use it to access the Web-based Utility later. Then click the **Yes** button.

5. For security purposes, you will be asked for your password in order to access the Bridge, as shown in Figure 5-4. In lowercase letters, enter **admin** in the *Password* field (later you can change the password through the Web-based Utility). Then click the **Enter** button.

6. The screen shown in Figure 5-5 shows a choice of two wireless modes. Click the **Infrastructure** radio button if you want your wireless computers to network with computers on your wired network using a wireless access point. Click the **Ad-Hoc** radio button if you want multiple wireless computers to network directly with each other. Do not use the Ad-Hoc mode if you want to network your wireless computers with computers on your wired network.

   In the *WB Name* field, enter a unique name for the Bridge. Memorable names are helpful, especially if you are using multiple bridges on the same network. Click the **Next** button to continue or the **Back** button to return to the previous screen.


LINKSYS®
A Division of Cisco Systems, Inc.
2
No
Yes
Wireless-B Ethernet Bridge Setup Wizard
Model No. WET11

One or More Wireless Bridges Have Been Found!

If you have one **Wireless-B Ethernet Bridge**, you can make changes to the following settings. If you have more than one **Wireless-B Ethernet Bridge**, you will need to run the **Setup Wizard** again to configure each separate **Wireless-B Ethernet Bridge.**

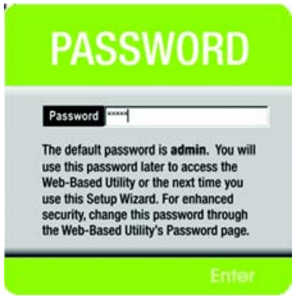
Selection: WET11

Status

Bridge Name: WET11
MAC Address: 00-02-DD-81-11-5E
IP Address: 192.168.1.225
SSID: linksys
Channel: Channel 6
WEP (Security): Disabled

Click **Yes** if you want to change any of these settings or **No** if you want to keep these settings.

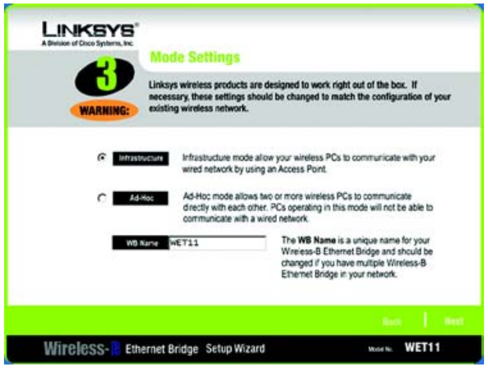
Figure 5-3: List of Bridges



Password: *****

The default password is **admin.** You will use this password later to access the Web-Based Utility or the next time you use this Setup Wizard. For enhanced security, change this password through the Web-Based Utility's Password page.

Figure 5-4: Password


LINKSYS®
A Division of Cisco Systems, Inc.
3
Back
Next
Wireless-B Ethernet Bridge Setup Wizard
Model No. WET11

Mode Settings

WARNING: Linksys wireless products are designed to work right out of the box. If necessary, these settings should be changed to match the configuration of your existing wireless network.

● Infrastructure — Infrastructure mode allow your wireless PCs to communicate with your wired network by using an Access Point.

○ Ad-Hoc — Ad-Hoc mode allows two or more wireless PCs to communicate directly with each other. PCs operating in this mode will not be able to communicate with a wired network.

WB Name: WET11 — The **WB Name** is a unique name for your Wireless-B Ethernet Bridge and should be changed if you have multiple Wireless-B Ethernet Bridge in your network.

Figure 5-5: Mode Settings

7. The *Wireless Settings* screen, shown in Figure 5-6, will now appear. Enter your wireless network's SSID. If you chose Ad-Hoc mode, select the channel at which the network broadcasts its wireless signal. Then click the **Next** button.

- SSID - The SSID is the unique name shared among all devices in a wireless network. The SSID must be identical for all devices in the wireless network. It is case-sensitive and must not exceed 32 alphanumeric characters, which can be any keyboard character.

- Channel - From the drop-down menu, select the appropriate channel to match your network's channel setting (available for Ad-Hoc mode only). All devices in your wireless network must use the same channel in order to function correctly.

8. The *IP Settings* screen will appear next, shown in Figure 5-7. If your network has a router or DHCP server automatically assigning IP addresses, click the radio button next to **Automatically obtain an IP address (DHCP)**. Click the **Next** button to continue or the **Back** button to return to the previous screen. Then proceed to step 9.

   If you need to set a static IP address on the Bridge, click the radio button next to **Set IP configuration manually** to select this option. Enter an IP Address, IP Mask, and Gateway appropriate to your network. You must specify an IP address on this screen. If you are unsure about the IP Mask and Gateway, it is better to leave these two fields blank. Click the **Next** button to continue or the **Back** button to return to the previous screen. Then proceed to step 9.

- IP Address - This IP address must be unique to your network.

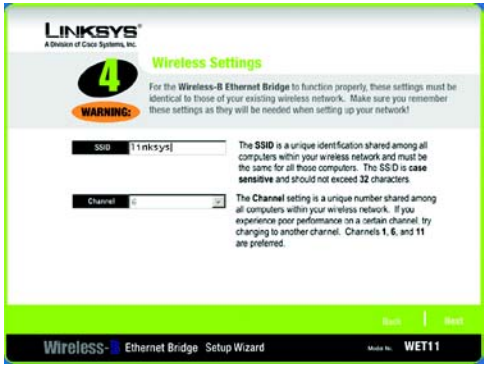
- IP Mask - The Bridge's IP Mask (also known as Subnet Mask) must be the same as your wired network's Subnet Mask.

- Gateway - Enter the IP address of your network's Gateway (usually this is the router's IP address).

9. The *Security Settings* screen, shown in Figure 5-8, appears next. Enable or disable Wired Equivalent Privacy (WEP) encryption for your wireless network. If you enable WEP, select the level of WEP encryption, and then enter a Passphrase. (If you want to enter a WEP key manually, then click the **Next** button.) If you want to disable WEP encryption, keep the default, **Disabled**. Click the **Next** button to continue.

- WEP (Disabled/64-bit WEP/128-bit WEP) - In order to utilize WEP encryption, select **64-bit** or **128-bit WEP** from the drop-down menu. Then enter a Passphrase. (If you want to enter a WEP key manually, then click the **Next** button.) If you do not want to use WEP encryption, keep the default setting, **Disabled**.

- Passphrase - Instead of manually entering a WEP key, you can enter a Passphrase, so a WEP key will be automatically generated after you click the Next button. The Passphrase is case-sensitive and should have 16


LINKSYS
A Division of Cisco Systems, Inc.
4
WARNING:
Back
Next
Wireless-B Ethernet Bridge Setup Wizard
Model No. WET11

Wireless Settings

For the **Wireless-B Ethernet Bridge** to function properly, these settings must be identical to those of your existing wireless network. Make sure you remember these settings as they will be needed when setting up your network!

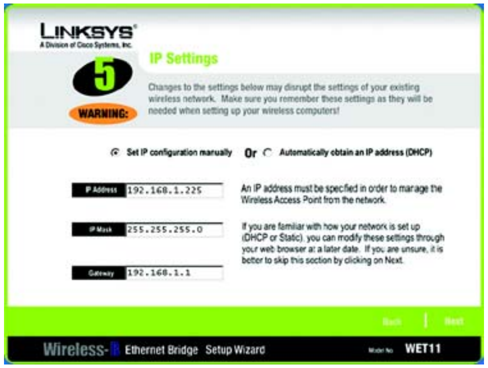
SSID: linksys

The **SSID** is a unique identification shared among all computers within your wireless network and must be the same for all those computers. The SSID is **case sensitive** and should not exceed **32** characters.

Channel: 6

The **Channel** setting is a unique number shared among all computers within your wireless network. If you experience poor performance on a certain channel, try changing to another channel. Channels **1**, **6**, and **11** are preferred.

Figure 5-6: Wireless Settings


LINKSYS
A Division of Cisco Systems, Inc.
5
WARNING:
Back
Next
Wireless-B Ethernet Bridge Setup Wizard
Model No. WET11

IP Settings

Changes to the settings below may disrupt the settings of your existing wireless network. Make sure you remember these settings as they will be needed when setting up your wireless computers!

● Set IP configuration manually Or ○ Automatically obtain an IP address (DHCP)

IP Address: 192.168.1.225

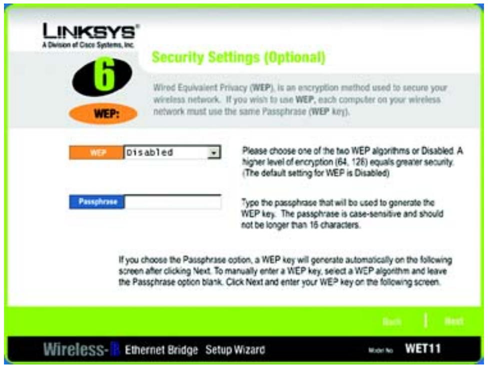
An IP address must be specified in order to manage the Wireless Access Point from the network.

IP Mask: 255.255.255.0

If you are familiar with how your network is set up (DHCP or Static), you can modify these settings through your web browser at a later date. If you are unsure, it is better to skip this section by clicking on Next.

Gateway: 192.168.1.1

Figure 5-7: IP Settings


LINKSYS
A Division of Cisco Systems, Inc.
6
WEP:
Back
Next
Wireless-B Ethernet Bridge Setup Wizard
Model No. WET11

Security Settings (Optional)

Wired Equivalent Privacy (**WEP**), is an encryption method used to secure your wireless network. If you wish to use **WEP**, each computer on your wireless network must use the same Passphrase (**WEP** key).

WEP: Disabled

Please choose one of the two WEP algorithms or Disabled. A higher level of encryption (64, 128) equals greater security. (The default setting for WEP is Disabled)

Passphrase:

Type the passphrase that will be used to generate the WEP key. The passphrase is case-sensitive and should not be longer than 16 characters.

If you choose the Passphrase option, a WEP key will generate automatically on the following screen after clicking Next. To manually enter a WEP key, select a WEP algorithm and leave the Passphrase option blank. Click Next and enter your WEP key on the following screen.

Figure 5-8: Security Settings

or fewer alphanumeric characters. It must match the passphrase of your wireless network and is compatible with Linksys wireless products only. (You will have to enter the WEP key(s) manually on any non-Linksys wireless products.)

10. If you entered a Passphrase, then you will see the automatically generated WEP key in the *Key 1* field, shown in Figure 5-9. Click the **Next** button, and proceed to step 11.

    If you did not enter a Passphrase, then enter a WEP key in the *Key 1* field. If you are using 64-bit WEP encryption, then the key must consist of exactly 10 hexadecimal characters. If you are using 128-bit WEP encryption, then the key must consist of exactly 26 hexadecimal characters. Valid hexadecimal characters are “0”-“9” and “A”-“F”. Then click the **Next** button, and proceed to step 11.

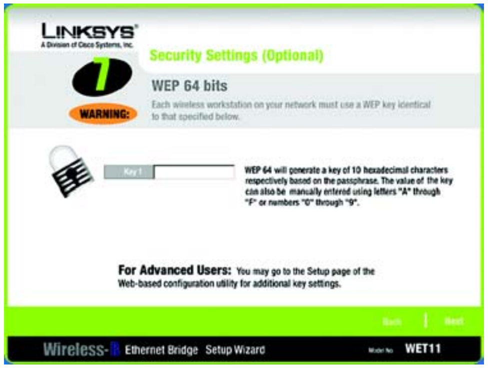
11. Review your settings on the Confirmation screen, shown in Figure 5-10. Write down the Bridge’s IP Address if you want to configure advanced settings through the Bridge’s Web-based Utility. Click the **Yes** button to save these settings. Click the **No** button to exit the Setup Wizard.

12. The next screen, shown in Figure 5-11, shows that the configuration is complete. To configure any other Wireless-B Ethernet Bridges on your network, run this Setup Wizard again. To register the Bridge, click the **Online Registration** button. To exit the Setup Wizard, click the **Exit** button.

The Wireless-B Ethernet Bridge is now successfully configured for your network.

Go to “Chapter 6: Connecting the Wireless-B Ethernet Bridge for Network Use.”

Advanced users: For advanced configuration, proceed to “Chapter 7: Using the Wireless-B Ethernet Bridge Web-based Utility.”


LINKSYS
A Division of Cisco Systems, Inc.
Security Settings (Optional)
7
WARNING:
Key 1
Back
Next
Wireless-B Ethernet Bridge Setup Wizard
Model No. WET11

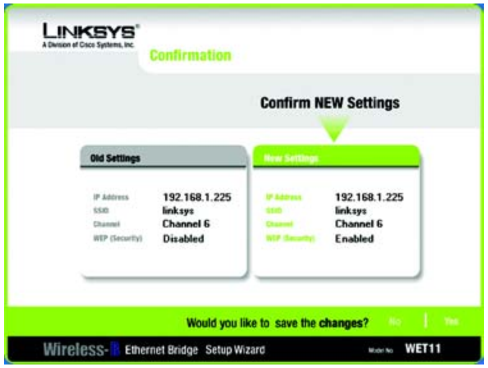
WEP 64 bits

Each wireless workstation on your network must use a WEP key identical to that specified below.

WEP 64 will generate a key of 10 hexadecimal characters respectively based on the passphrase. The value of the key can also be manually entered using letters "A" through "F" or numbers "0" through "9".

For Advanced Users: You may go to the Setup page of the Web-based configuration utility for additional key settings.

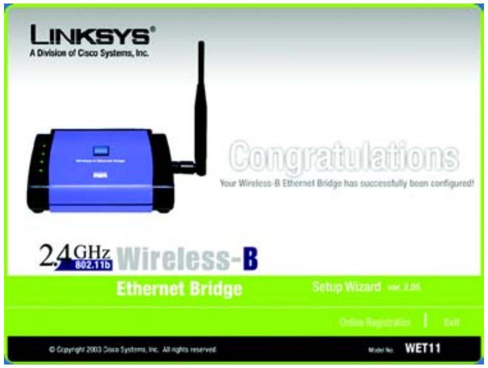
Figure 5-9: WEP Key


LINKSYS
A Division of Cisco Systems, Inc.
Confirmation
Confirm NEW Settings
No
Yes
Wireless-B Ethernet Bridge Setup Wizard
Model No. WET11

Old Settings		New Settings	
IP Address	192.168.1.225	IP Address	192.168.1.225
SSID	linksys	SSID	linksys
Channel	Channel 6	Channel	Channel 6
WEP (Security)	Disabled	WEP (Security)	Enabled

Would you like to save the changes?

Figure 5-10: Confirmation



Your Wireless-B Ethernet Bridge has successfully been configured!

© Copyright 2003 Cisco Systems, Inc. All rights reserved.

Figure 5-11: Congratulations

Chapter 6: Connecting the Wireless-B Ethernet Bridge for Network Use

1. After configuration, unplug the power cable from the electrical outlet, and unplug the Ethernet network cable from the PC, hub, or switch.

2. Plug the Ethernet network cable into the RJ-45 port on the Ethernet-ready network device you wish to add to the wireless network.

3. Plug the power cable into a local electrical outlet.

The installation of the Wireless-B Ethernet Bridge is complete.

If you want to use the Bridge's Web-based Utility, refer to "Chapter 7: The Wireless-B Ethernet Bridge Web-based Utility."

Note: If you do not have an active connection to the Ethernet-ready network device, then change the position of the X-II switch.

Chapter 7: Using the Wireless-B Ethernet Bridge Web-based Utility

Overview

The Bridge is designed to function properly after configuration using the Setup Wizard. However, if you would like to change these settings or make more advanced configuration changes, use your web browser and the Wireless-B Ethernet Bridge Web-based Utility. This chapter explains how to use the Utility.

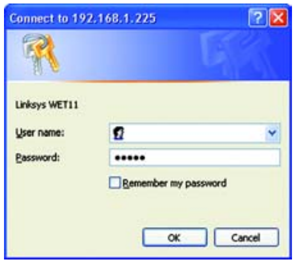
Starting the Web-based Utility

1. Open your web browser, and enter the IP address of the Wireless-B Ethernet Bridge (the default is **192.168.1.225**). Press the **Enter** key, and the screen shown in Figure 7-1 will appear. In lowercase letters, enter the default password, **admin**, in the *Password* field. Click the **OK** button. You can set a new password on the *Password* screen later.

2. The Utility's *Setup* screen, shown in Figure 7-2, will appear.

   The Utility provides a convenient, web-browser-based way to alter the Bridge's settings. It offers five main tabs:

- Setup - Enables you to configure the IP address and wireless settings.
- Password - Allows you to change the password or reset all settings to factory defaults.
- Advanced - Lets you change the advanced wireless settings and clone a MAC address onto the Bridge.
- Status - Displays the Bridge's current settings.
- Help - Provides explanations of various configuration settings and links to online technical support resources.



Linksys WET11

User name:

Password: •••••

□ Remember my password

Figure 7-1: Access the Web-based Utility

Have You: Enabled TCP/IP on your PCs? PCs communicate over the network with this protocol. Refer to "Appendix D: Windows Help" for more information on TCP/IP.

Note: The Wireless-B Ethernet Bridge is designed to function properly after using the Setup Wizard. This chapter is provided solely for those who wish to perform more advanced configuration or monitoring.

Setup

The *Setup* screen, shown in Figure 7-2, lets you configure the wired and wireless network settings for the Bridge.

- Firmware - The version number of the Bridge's firmware is displayed here. Firmware should be upgraded ONLY if you experience problems with the Bridge. Firmware updates are posted at *www.linksys.com*. For more information, refer to "Appendix C: Upgrading Firmware."
- MAC Address - The MAC Address of the Bridge is displayed here.

LAN

- Device Name - You may assign any name to the Bridge. Unique, memorable names are helpful, especially if you are using multiple bridges on the same wireless network.
- Configuration Type - If the Bridge will obtain an IP address automatically from a DHCP server, such as a router, then select **Automatic Configuration-DHCP**. If you are assigning the Bridge a static IP address, then select **Static IP Address**, and enter an IP Address, Subnet Mask, and Gateway address in the *IP Address*, *Subnet Mask*, and *Gateway* fields.

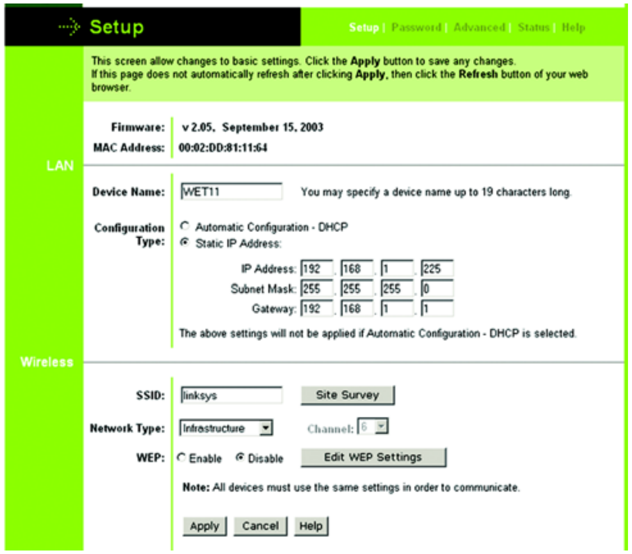
Wireless

- SSID - The SSID is the network name shared among all devices in a wireless network. The SSID must be identical for all devices in the wireless network. It is case-sensitive and must not exceed 32 alphanumeric characters, which may be any keyboard character (do not use any spaces). Make sure this setting is the same for all devices in your wireless network. For added security, Linksys recommends that you change the default SSID (linksys) to a name of your choice.

  To search for available wireless networks, click the **Site Survey** button.

- Network Type - Choose a wireless operating mode for the Bridge. Keep the default setting, **Infrastructure**, if you want your wireless-equipped device to communicate with computers and other devices on your wired network using a wireless access point. Select **Ad-Hoc** button if you want multiple wireless-equipped devices to communicate directly with each other.

  If you chose Ad-Hoc mode, then select the correct operating channel for your network in the *Channel* drop-down menu. The channel you choose should match the channel set on the other devices in your wireless network.



This screen allow changes to basic settings. Click the **Apply** button to save any changes.
If this page does not automatically refresh after clicking **Apply**, then click the **Refresh** button of your web browser.

Firmware: v 2.05, September 15, 2003
MAC Address: 00:02:DD:81:11:64

Device Name: WET11 You may specify a device name up to 19 characters long.

Configuration Type: ○ Automatic Configuration - DHCP ● Static IP Address:

IP Address: 192 . 168 . 1 . 225
Subnet Mask: 255 . 255 . 255 . 0
Gateway: 192 . 168 . 1 . 1

The above settings will not be applied if Automatic Configuration - DHCP is selected.

SSID: linksys
Network Type: Infrastructure Channel: 6
WEP: ○ Enable ● Disable

Note: All devices must use the same settings in order to communicate.

Figure 7-2: Setup Tab

- WEP - To enable WEP encryption, click the **Enable** radio button. To increase wireless network security, using WEP encryption is strongly recommended. Then click the **Edit WEP Settings** button to configure the WEP settings. To disable WEP encryption, keep the default, **Disable**.

  An acronym for Wired Equivalent Privacy, WEP is an encryption method used to protect your wireless data communications. WEP uses 64-bit or 128-bit keys to provide access control to your network and encryption security for every data transmission. To decode a data transmission, each device in a network must use an identical WEP key. Higher encryption levels offer higher levels of security, but due to the complexity of the encryption, they may decrease network performance.

  Click the **Apply** button to save your changes. If your page doesn't automatically refresh itself, then click the **Refresh** button of your web browser. Click the **Cancel** button to cancel your changes. Click the **Help** button for additional on-screen information.

- **Site Survey**

The *Site Survey* screen, shown in Figure 7-3, 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.

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

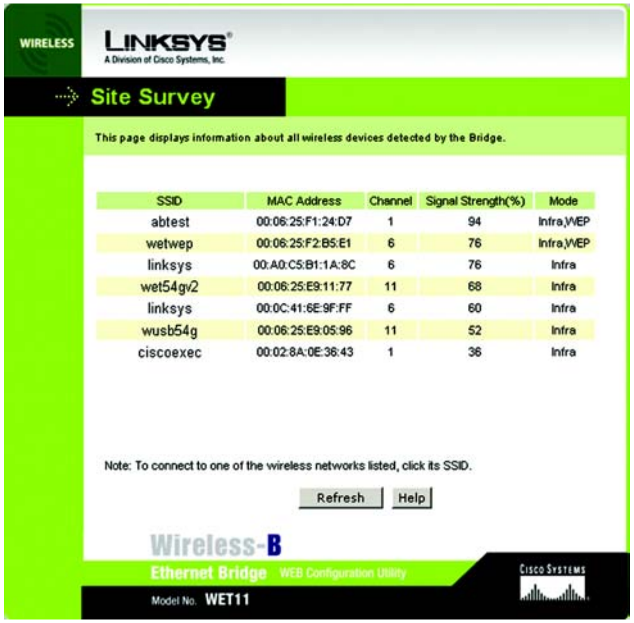
- SSID - The network name. To join a wireless network, click its SSID.
- MAC Address - The MAC address of the network's access point.
- Channel - The channel setting.
- Signal Strength (%) - The percentage of wireless signal strength.
- Mode - The network mode and status of WEP encryption.

Click the **Refresh** button to obtain the most up-to-date data. Click the **Cancel** button to close this screen. Click the **Help** button for additional on-screen information.

- **WEP Encryption**

Use the *WEP* screen, shown in Figure 7-4, to configure the WEP encryption level and WEP keys for the Bridge.

- 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.



This page displays information about all wireless devices detected by the Bridge.

SSID	MAC Address	Channel	Signal Strength(%)	Mode
abtest	00:06:25:F1:24:D7	1	94	Infra,WEP
wetwep	00:06:25:F2:B5:E1	6	76	Infra,WEP
linksys	00:A0:C5:B1:1A:8C	6	76	Infra
wet54gv2	00:06:25:E9:11:77	11	68	Infra
linksys	00:0C:41:6E:9F:FF	6	60	Infra
wusb54g	00:06:25:E9:05:96	11	52	Infra
ciscoexec	00:02:8A:0E:36:43	1	36	Infra

Note: To connect to one of the wireless networks listed, click its SSID.

Figure 7-3: Site Survey

NOTE: Make sure that your WEP key matches the WEP key of the wireless network you want to join. Otherwise, the connection will fail.

- WEP 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 will need to enter your WEP key(s) manually on the non-Linksys wireless products.) After you enter the Passphrase, click the **Generate** button to create WEP key(s).

- Keys 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 in length. Valid hexadecimal characters are “0”-“9” and “A”-“F”.

Click the **Apply** button to save your changes. If your page doesn’t automatically refresh itself, then click the **Refresh** button of your web browser. Click the **Cancel** button to cancel your changes. Click the **Help** button for additional on-screen information.

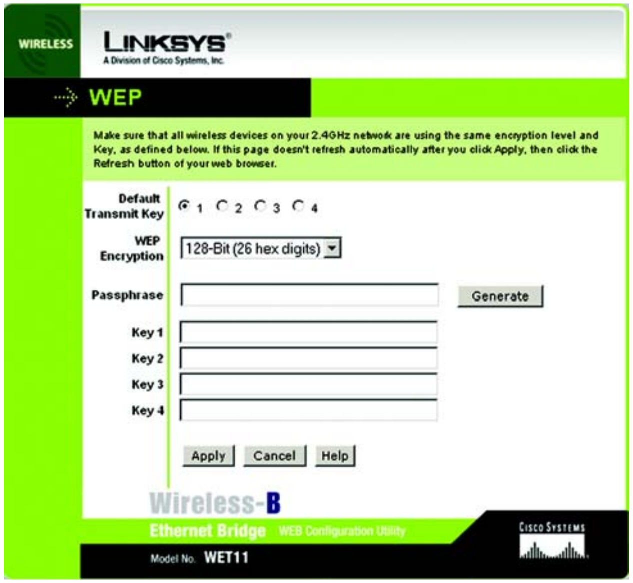
Password

The *Password* screen, shown in Figure 7-5, lets you change the Bridge’s Password and restore the factory default settings.

- Administrative Password - It is strongly recommended that you change the Bridge’s default password (admin). All users who try to access the Bridge’s Web-based Utility will be prompted for the Bridge’s Password. The new Password must not exceed 12 characters in length and must not include any spaces. Enter the new Password a second time to confirm it.

- Restore Factory Defaults - Click the **Yes** radio button to reset all configuration settings to their default values. If you do not want to restore the factory defaults, then keep the default setting, **No**.

To save your changes, click the **Apply** button. Click the **Cancel** button to cancel your changes. Click the **Help** button for additional on-screen information.



Make sure that all wireless devices on your 2.4GHz netwok are using the same encryption level and Key, as defined below. If this page doesn't refresh automatically after you click Apply, then click the Refresh button of your web browser.

Default Transmit Key ● 1 ○ 2 ○ 3 ○ 4

WEP Encryption 128-Bit (26 hex digits)

Passphrase

Key 1

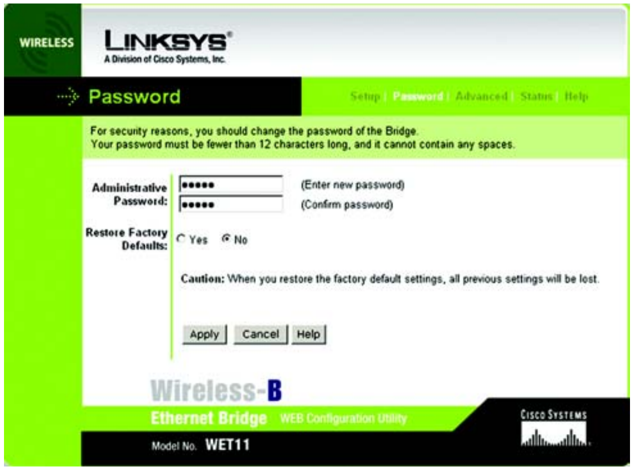
Key 2

Key 3

Key 4

Model No. WET11

Figure 7-4: WEP Encryption


WIRELESS
LINKSYS®
A Division of Cisco Systems, Inc.
Password
Setup | Password | Advanced | Status | Help
Apply
Cancel
Help
Wireless-B
Ethernet Bridge
WEB Configuration Utility
CISCO SYSTEMS

For security reasons, you should change the password of the Bridge.
Your password must be fewer than 12 characters long, and it cannot contain any spaces.

Administrative Password: ●●●●● (Enter new password)
●●●●● (Confirm password)

Restore Factory Defaults: ○ Yes ● No

Caution: When you restore the factory default settings, all previous settings will be lost.

Model No. WET11

Figure 7-5: Password Tab

IMPORTANT: Any settings you have saved will be lost if the default settings are restored.

Advanced

Use the *Advanced Settings* screen, shown in Figure 7-6, to customize advanced wireless settings and clone a MAC address onto the Bridge.

Wireless

- Transmission Rate - The default setting is **Auto**. The range is from 1 to 11Mbps.

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

- Authentication Type - The default setting is **Open System**. The choices are **Open System** and **Shared Key**.

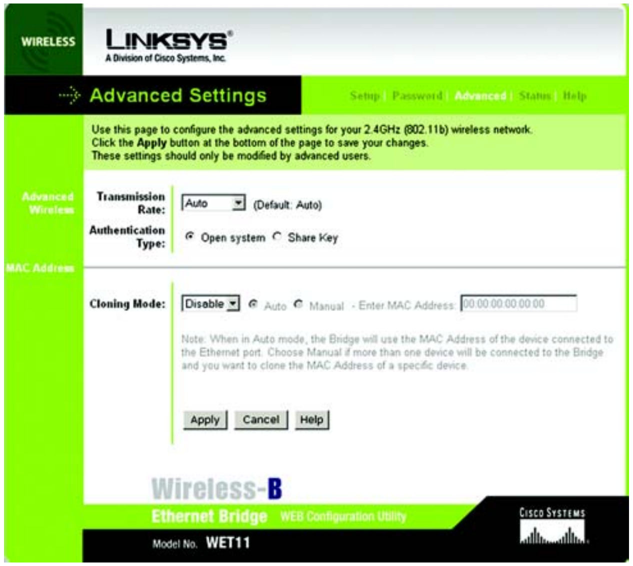
  This setting allows the Bridge to authenticate communication with the wireless devices in your network. With the Shared Key setting, all wireless devices must use the same WEP key so that the Bridge and the client can authenticate each other and start transmitting data. With the Open System setting, any device can join a network without performing any security check. Select the authentication type used by your wireless network.

MAC Address

- 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 the Bridge's LAN port. The Bridge will actively scan for a new MAC address to be cloned whenever you disconnect and re-connect the Bridge through its 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 the **Apply** button to save your changes. If your page doesn't automatically refresh itself, then click the **Refresh** button of your web browser. Click the **Cancel** button to cancel your changes. Click the **Help** button for additional on-screen information.


WIRELESS
LINKSYS®
A Division of Cisco Systems, Inc.
Setup | Password | Advanced | Status | Help
Advanced Wireless
MAC Address
Apply
Cancel
Help
Wireless-B
Ethernet Bridge WEB Configuration Utility
Model No. WET11
Cisco Systems

Advanced Settings

Use this page to configure the advanced settings for your 2.4GHz (802.11b) wireless network.
Click the **Apply** button at the bottom of the page to save your changes.
These settings should only be modified by advanced users.

Transmission Rate: Auto (Default: Auto)

Authentication Type: ● Open system ○ Share Key

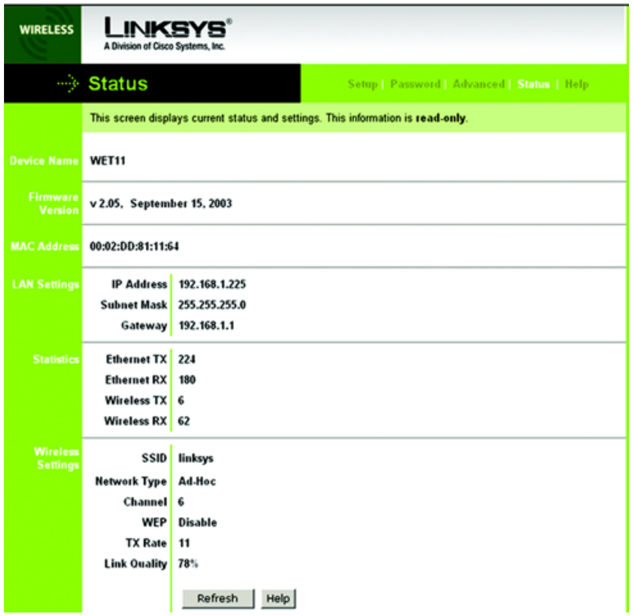
Cloning Mode: Disable ● Auto ○ Manual - Enter MAC Address: 00:00:00:00:00:00

Note: When in Auto mode, the Bridge will use the MAC Address of the device connected to the Ethernet port. Choose Manual if more than one device will be connected to the Bridge and you want to clone the MAC Address of a specific device.

Figure 7-6: Advanced Settings Tab

Status

The *Status* screen displays the Bridge’s current status and settings. All information is read-only.


WIRELESS
LINKSYS®
A Division of Cisco Systems, Inc.
Status
Setup | Password | Advanced | Status | Help
Refresh
Help

This screen displays current status and settings. This information is **read-only**.

Device Name WET11

Firmware Version v 2.05, September 15, 2003

MAC Address 00:02:DD:81:11:64

LAN Settings
IP Address 192.168.1.225
Subnet Mask 255.255.255.0
Gateway 192.168.1.1

Statistics
Ethernet TX 224
Ethernet RX 180
Wireless TX 6
Wireless RX 62

Wireless Settings
SSID linksys
Network Type Ad-Hoc
Channel 6
WEP Disable
TX Rate 11
Link Quality 78%

Figure 7-7: Status Tab

- Device Name - The name you have assigned to the Bridge is displayed here.
- Firmware Version - The version number of the Bridge’s firmware is displayed here. Firmware should be upgraded ONLY if you experience problems with the Bridge. Firmware updates are posted at *www.linksys.com*. For more information, refer to “Appendix C: Upgrading Firmware.”
- MAC Address - The MAC Address of the Bridge is displayed here.

LAN Settings

- IP Address - The Bridge’s IP Address is displayed here.
- Subnet Mask - The Bridge’s Subnet Mask is displayed here.
- Gateway - The Gateway address for the Bridge is displayed here.

LAN Statistics

- Ethernet TX - The number of packets transmitted to the Ethernet network is displayed here.
- Ethernet RX - The number of packets received from the Ethernet network is displayed here.
- Wireless TX - The number of packets transmitted to the wireless network is displayed here.
- Wireless RX - The number of packets received from the wireless network is displayed here.

Wireless Settings

- SSID - The Bridge’s SSID is displayed here.
- Network Type - The Bridge’s mode is displayed here.
- Channel - The Bridge’s channel setting is displayed here.
- WEP - The status of the Bridge’s WEP encryption is displayed here.
- TX Rate - The Bridge’s transmission rate is displayed here.

- Link Quality - The percentage of the Bridge's wireless signal strength is displayed here.

Click the **Refresh** button to obtain the most up-to-date settings and statistics. Click the **Help** button for additional on-screen information.

Help

The *Help* screen offers links to all of the help information for the Web-based Utility's screens and the Bridge's online technical support resources. All information is read-only.

- Linksys Website - Click the **Linksys Website** link to visit Linksys's website, www.linksys.com.
- Online manual in PDF format - Click the **Online manual in PDF format** to view this User Guide online. It is in Adobe Acrobat Portable Document File (.pdf) format, so you will need the free Adobe Acrobat Reader to view the pdf. If you do not have the Reader, click the **Adobe Website** link to download it.
- Adobe Website (software for viewing PDF documents) - If you need to download the Adobe Acrobat Reader to view the User Guide pdf, then click the **Adobe Website** link.

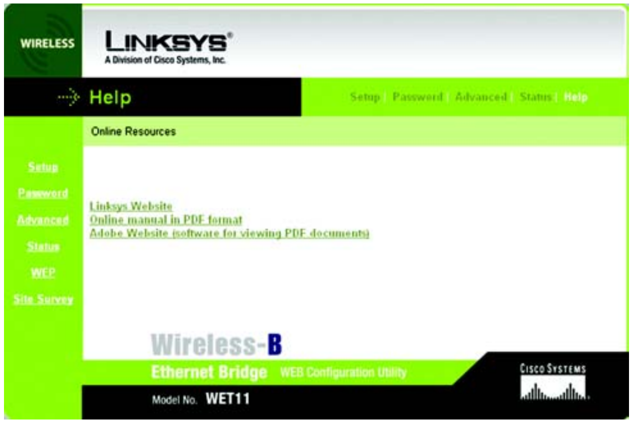

WIRELESS
LINKSYS®
A Division of Cisco Systems, Inc.
Help
Setup | Password | Advanced | Status | Help
Online Resources
Setup
Password
Advanced
Status
WEP
Site Survey
Linksys Website
Online manual in PDF format
Adobe Website (software for viewing PDF documents)
Wireless-B
Ethernet Bridge WEB Configuration Utility
Model No. WET11
Cisco Systems

Figure 7-8: Help Tab

Appendix A: Troubleshooting

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

Common Problems and Solutions

1. ***I can't connect to the access point.***
   Open the Web-based Utility. On the Setup tab, perform the following steps:
   - Verify that the operating mode is set to Infrastructure mode.
   - Make sure that the SSID is the same as the SSID of the access point.
   - On the WEP Encryption screen, make sure that all of the WEP settings are the same as the WEP settings of the access point.

2. ***I want to play head-to-head (ad-hoc) gaming with two Xboxes, but they won't communicate.***
   Perform the following steps:
   - Make sure both Bridges are set to the same SSID, network mode (Ad-Hoc), channel setting, and WEP settings.
   - Verify that the Bridges are set to different IP addresses.
   - You need to enable MAC address cloning on the Bridge for each Xbox. Follow these instructions:
     1. Open the Web-based Utility for one of the Bridges.
     2. Click the **Advanced** tab.
     3. Select **Enable** from the MAC Address Cloning Mode drop-down menu.
     4. Click the **Auto** radio button.
     5. Click the **Apply** button to save your changes. When you connect the Bridge to its Xbox, the Bridge will automatically clone the Xbox's MAC address.
   - Repeat steps 1-5 for the other Bridge.

3. ***I don't know how to change the Bridge's IP address.***
   You have two ways to change the Bridge's IP address.
   - Open the Web-based Utility. On the *Setup* screen, click the **Static IP Address** radio button, and change the IP address there.
   - If you encounter problems, power the Bridge off and on again, or push the Reset button. Then try to change the IP address again.

4. ***The Bridge-enabled PC won't communicate with a wireless-enabled PC or printer.***
   Perform the following steps:
   - Check that the wireless-enabled PC or printer is on the same wireless network as the PC using the Bridge.
   - Make sure that the SSID and network mode are identical for all devices connected to the same wireless network.
   - If the wireless network settings are fine, then make sure that all the devices are on the same IP network.

5. ***The Web-based Utility doesn't detect the Bridge.***
   Make sure that the Ethernet cable is properly connected and that the Ethernet LED is lit. If the LED is not lit, change the position of the X-II slide switch on the Bridge's rear panel. Use the X setting if you are connecting the Bridge to a network adapter. Use the II setting if you are connecting the Bridge to a hub or switch. If you still do not have an active connection, then change the position of the X-II switch again.

6. ***The Web-based Utility won't open.***
   Make sure you correctly entered the Bridge's IP address in the Address field of your web browser. If you are not sure what the Bridge's IP address is, then run the Setup Wizard. Follow the on-screen instructions until you see a screen that lists all the Wireless-B Ethernet Bridges on your network. Select the Bridge you want to access, and its IP address will appear in the Status box. Enter this IP address in your web browser's Address field. For details, see Chapter 5: Setting up the Wireless-B Ethernet Bridge.

7. ***The Web-based Utility does not recognize my password.***
   The password is case-sensitive. Make sure that you are using the correct case(s)—lowercase or uppercase—when entering the password. If you forget your password, you can push the Bridge's Reset button. This will reset the password to the default setting; however, all other Bridge settings will be reset to the factory defaults as well. To use the default setting, enter **admin** in the Password field.

8. ***After I make changes through the Web-based Utility, the new settings aren't displayed on-screen.***
   Click the **Refresh** button of your web browser. If the new settings aren't displayed, then unplug the power adapter from the Bridge. Plug the power adapter back in, and then click the **Refresh** button again.

Frequently Asked Questions

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

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

Can I play multiplayer games with other users of the wireless network?
Yes, as long as the game supports multiple players over a LAN. Refer to the game's user guide for more information.

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

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

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

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

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

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

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

What is Spread Spectrum?

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

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

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

What is WEP?

WEP is Wired Equivalent Privacy, a data privacy mechanism based on a 40/64 bit shared key algorithm, as described in the IEEE 802.11 standard.

Appendix B: Wireless Security

A Brief Overview

Whenever data—in the form of files, e-mails, or messages—is transmitted over your wireless network, it is open to attacks. Wireless networking is inherently risky because it broadcasts information on radio waves. Just like signals from your cellular or cordless phone can be intercepted, signals from your wireless network can also be compromised. What are the risks inherent in wireless networking? Read on.

What Are the Risks?

Computer network hacking is nothing new. With the advent of wireless networking, hackers use methods both old and new to do everything from stealing your bandwidth to stealing your data. There are many ways this is done, some simple, some complex. As a wireless user, you should be aware of the many ways they do this.

Every time a wireless transmission is broadcast, signals are sent out from your wireless PC or access point, but not always directly to its destination. The receiving PC or access point can hear the signal because it is within that radius. Just as with a cordless phone, cellular phone, or any kind of radio device, anyone else within that radius, who has their device set to the same channel or bandwidth can also receive those transmission.

Wireless networks are easy to find. Hackers know that, in order to join a wireless network, your wireless PC will typically first listen for “beacon messages”. These are identifying packets transmitted from the wireless network to announce its presence to wireless nodes looking to connect. These beacon frames are decrypted and contain much of the network’s information, such as the network’s SSID (Service Set Identifier) and the IP address of the network PC or access point. The SSID is analogous to the network's name. With this information broadcast to anyone within range, hackers are often provided with just the information they need to access that network.

One result of this, seen in many large cities and business districts, is called “Warchalking”. This is the term used for hackers looking to access free bandwidth and free Internet access through your wireless network. The marks they chalk into the city streets are well documented in the Internet and communicate exactly where available wireless bandwidth is located for the taking.

Even keeping your network settings, such as the SSID and the channel, secret won’t prevent a hacker from listening for those beacon messages and stealing that information. This is why most experts in wireless networking strongly recommend the use of WEP (Wireless Equivalent Privacy). WEP encryption scrambles your wireless signals so they can only be recognized within your wireless network.

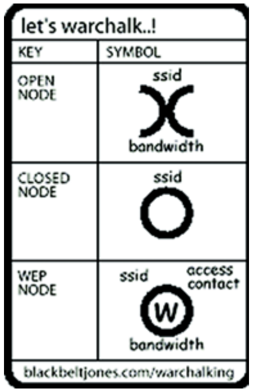


Figure B-1: Warchalking

But even WEP has its problems. WEP’s encryption algorithm is referred to as “simple”, which also means “weak”, because the technology that scrambles the wireless signal isn’t too hard to crack for a persistent hacker.

There are five common ways that hackers can break into your network and steal your bandwidth as well as your data. The five attacks are popularly known as:

1. Passive Attacks
2. Jamming Attacks
3. Active Attacks
4. Dictionary-building or Table Attacks
5. Man-in-the-Middle Attacks

Passive Attacks

There's no way to detect a passive attack because the hacker is not breaking into your network. He is simply listening (eavesdropping, if you will) to the information your network broadcasts. There are applications easily available on the Internet that can allow a person to listen into your wireless network and the information it broadcasts. Information such as MAC addresses, IP addresses, usernames, passwords, instant message conversations, e-mails, account information, and any data transmitted wirelessly, can easily be seen by someone outside of your network because it is often broadcast in clear text. Simply put, any information transmitted on a wireless network leaves both the network and individual users vulnerable to attack. All a hacker needs is a “packet sniffer”, software available on the Internet, along with other freeware or shareware hacking utilities available on the Internet, to acquire your WEP keys and other network information to defeat security.

Jamming Attacks

Jamming Attacks, when a powerful signal is sent directly into your wireless network, can effectively shut down your wireless network. This type of attack is not always intentional and can often come about simply due to the technology. This is especially possible in the 2.4 GHz frequency, where phones, baby monitors, and microwave ovens can create a great deal of interference and jam transmissions on your wireless network. One way to resolve this is by moving your wireless devices into the 5 GHz frequency, which is dedicated solely to information transmissions.

Active Attacks

Hackers use Active Attacks for three purposes: 1) stealing data, 2) using your network, and 3) modifying your network so it's easier to hack in the next time.

In an Active Attack, the hacker has gained access to all of your network settings (SSID, WEP keys, etc.) and is in your network. Once in your wireless network, the hacker has access to all open resources and transmitted data on the network. In addition, if the wireless network’s access point is connected to a switch, the hacker will also have access to data in the wired network.

Further, spammers can use your Internet connection and your ISP’s mail server to send tens of thousands of e-mails from your network without your knowledge.

Lastly, the hacker could make hacking into your network even easier by changing or removing safeguards such as MAC address filters and WEP encryption. He can even steal passwords and user names for the next time he wants to hack in.

Dictionary-Building or Table Attacks

Dictionary-building, or Table attacks, is a method of gaining network settings (SSID, WEP keys, etc.) by analyzing about a day's worth of network traffic, mostly in the case of business networks. Over time, the hacker can build up a table of network data and be able to decrypt all of your wireless transmissions. This type of attack is more effective with networks that transmit more data, such as businesses.

Man-in-the-Middle Attacks

A hacker doesn’t need to log into your network as a user—he can appear as one of the network’s own access points, setting himself up as the man-in-the-middle. To do this, the hacker simply needs to rig an access point with your network’s settings and send out a stronger signal that your access point. In this way, some of your network's PCs may associate with this rogue access point, not knowing the difference, and may begin sending data through it and to this hacker.

The trade-off for the convenience and flexibility wireless networking provides is the possibility of being hacked into through one of the methods described here. With wireless networks, even with WEP encryption, open to the persistent hacker, how can you protect your data? The following section will tell you how to do just that.

Maximizing Wireless Security

Security experts will all tell you the same thing: Nothing is guaranteed. No technology is secure by itself. An unfortunate axiom is that building the better mousetrap can often create a better mouse. This is why, in the examples below, your implementation and administration of network security measures is the key to maximizing wireless security.

No preventative measure will guarantee network security but it will make it more difficult for someone to hack into your network. Often, hackers are looking for an easy target. Making your network less attractive to hackers, by making it harder for them to get in, will make them look elsewhere.

How do you do this? Before discussing WEP, let’s look at a few security measures often overlooked.

1) Network Content

Now that you know the risks assumed when networking wirelessly, you should view wireless networks as you would the Internet. Don’t host any systems or provide access to data on a wireless network that you wouldn't put on the Internet.

2) Network Layout

When you first lay out your network, keep in mind where your wireless PCs are going to be located and try to position your access point(s) towards the center of that network radius. Remember that access points transmit indiscriminately in a radius; placing an access point at the edge of the physical network area reduces network performance and leaves an opening for any hacker smart enough to discover where the access point is transmitting.

This is an invitation for a man-in-the-middle attack, as described in the previous section. To perform this type of attack, the hacker has to be physically close to your network. So, monitoring both your network and your property is important. Furthermore, if you are suspicious of unauthorized network traffic, most wireless products come with a log function, with which you can view activity on your network and verify if any unauthorized users have had access.

3) Network Devices

With every wireless networking device you use, keep in mind that network settings (SSID, WEP keys, etc.) are stored in its firmware. If they get into the hands of a hacker, so do all of your settings. So keep an eye on them.

4) Administrator Passwords

Your network administrator is the only person who can change network settings. If a hacker gets a hold of the administrator's password, he, too, can change those settings. So, make it harder for a hacker to get that information. Change the administrator's password regularly.

5) SSID

There are a few things you can do to make your SSID more secure:

a. Disable broadcast

b. Make it unique

c. Change it often

Most wireless networking devices will give you the option of broadcasting the SSID. This is a option for convenience, allowing anyone to log into your wireless network. In this case, however, anyone includes hackers. So don't broadcast the SSID.

A default SSID is set on your wireless devices by the factory. (The Linksys default SSID is “linksys”.) Hackers know these defaults and can check these against your network. Change your SSID to something unique and not something related to your company or the networking products you use.

Changing your SSID regularly will force any hacker attempting to gain access to your wireless network to start looking for that new SSID.

With these three steps in mind, please remember that while SSIDs are good for segmenting networks, they fall short with regards to security. Hackers can usually find them quite easily.

6) MAC Addresses

Enable MAC address filtering if your wireless products allow it. MAC address filtering will allow you to provide access to only those wireless nodes with certain MAC addresses. This makes it harder for a hacker using a random MAC address or spoofing (faking) a MAC address.

7) Firewalls

Once a hacker has broken into your wireless network, if it is connected to your wired network, they’ll have access to that, too. This means that the hacker has effectively used your wireless network as a backdoor through your firewall, which you've put in place to protect your network from just this kind of attack via the Internet.

You can use the same firewall technology to protect your wired network from hackers coming in through your wireless network as you did for the Internet. Rather than connecting your access point to an unprotected switch, swap those out for a router with a built-in firewall. The router will show the access point coming in through its Internet port and its firewall will protect your network from any transmissions entering via your wireless network.

PCs unprotected by a firewall router should at least run firewall software, and all PCs should run up-to-date antiviral software.

8) WEP

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

WEP encryption implementation was not put in place with the 802.11 standard. This means that there are about as many methods of WEP encryption as there are providers of wireless networking products. In addition, WEP is not completely secure. One piece of information still not encrypted is the MAC address, which hackers can use to break into a network by spoofing (or faking) the MAC address.

Programs exist on the Internet that are designed to defeat WEP. The best known of these is AirSnort. In about a day, AirSnort can analyze enough of the wireless transmissions to crack the WEP key. Just like a dictionary-building attack, the best prevention for these types of programs is by not using static settings, periodically changing WEP keys, SSID, etc.

There are several ways that WEP can be maximized:

a) Use the highest level of encryption possible

b) Use multiple WEP keys

c) Change your WEP key regularly

Current encryption technology offers 64-bit and 128-bit WEP encryption. If you are using 64-bit WEP, swap out your old wireless units for 128-bit encryption right away. Where encryption is concerned, the bigger and more complex, the better. A WEP key is a string of hexadecimal characters that your wireless network uses in two ways. First, nodes in your wireless network are identified with a common WEP key. Second, these WEP keys encrypt and decrypt data sent over your wireless network. So, a higher level of security ensures that hackers will have a harder time breaking into your network.

Setting one, static WEP key on your wireless network leaves your network open the threats even as you think it is protecting you. While it is true that using a WEP key increases wireless security, you can increase it further by using multiple WEP keys.

Keep in mind that WEP keys are stored in the firmware of wireless cards and access points and can be used to hack into the network if a card or access point falls into the wrong hands. Also, should someone hack into your network, there would be nothing preventing someone access to the entire network, using just one static key.

The solution, then, is to segment your network up into multiple groups. If your network had 80 users and you used four WEP keys, a hacker would have access to only ¼ of your wireless network resources. In this way, multiple keys reduce your liability.

Finally, be sure to change your WEP key regularly, once a week or once a day. Using a "dynamic" WEP key, rather than one that is static, makes it even harder for a hacker to break into your network and steal your resources.

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

WEP Encryption

WEP encryption for the Bridge is configured through the Setup Wizard or the Web-based Utility's Setup tab. For more information about the Setup Wizard, refer to "Chapter 5: Setting Up the Wireless-B Ethernet Bridge." To enable WEP encryption through the Web-based Utility, click the **WEP Key Settings** button on the Setup tab. The *Edit WEP Settings* screen will appear, as shown in Figure B-2.

To configure the WEP settings, follow these instructions:

1. For the Default Transmit Key setting, 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.

2. For the WEP Encryption setting, select **64-Bit (10 hex digits)** or **128-Bit (26 hex digits)** from the drop-down menu.

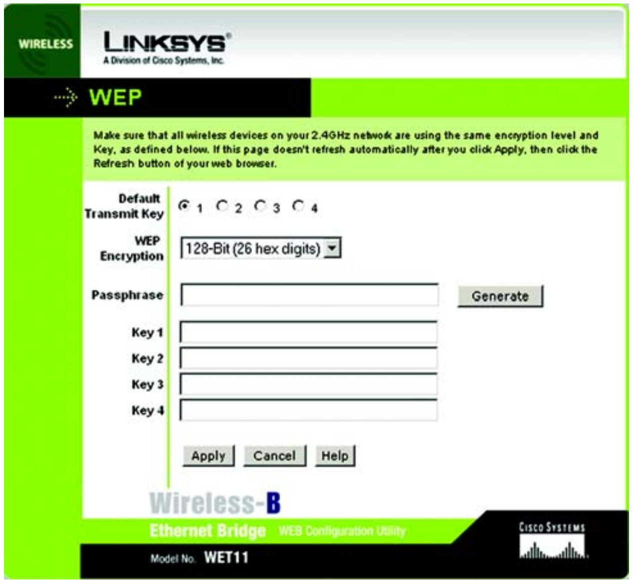
3. The WEP Key can be generated in two ways: you can use a Passphrase or you can enter it manually.

   If you wish to use a Passphrase, enter it and then click the **Generate** key to generate WEP key(s). The Passphrase is case-sensitive and can be a maximum of 16 alphanumeric characters. (The Passphrase function is compatible with Linksys wireless products only. If you want to communicate with non-Linksys wireless products, you will need to enter your WEP key(s) manually on the non-Linksys wireless products.)

   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 in length. Valid hexadecimal characters are "0"-"9" and "A"-"F".

4. Click the **Apply** button to apply your changes and return to the Setup tab or **Cancel** to cancel your changes. Click the **Help** button for additional on-screen information.



Make sure that all wireless devices on your 2.4GHz network are using the same encryption level and Key, as defined below. If this page doesn't refresh automatically after you click Apply, then click the Refresh button of your web browser.

Default Transmit Key: ● 1 ○ 2 ○ 3 ○ 4

WEP Encryption: 128-Bit (26 hex digits)

Passphrase:

Key 1:

Key 2:

Key 3:

Key 4:

Figure B-2: WEP Encryption

Appendix C: Upgrading Firmware

The Bridge’s firmware is upgraded with the firmware utility on the Linksys website at *http://linksys.com/download*. Firmware should be upgraded ONLY if you experience problems with the Bridge.

1. Go to **http://linksys.com/download**.
2. Select **WET11 - Wireless-B Ethernet Bridge - Version 2**, and then select your operating system.
3. Then, click the **Downloads for this Product** button.
4. Select **Firmware**.
5. Read the release notes for the firmware version.
6. Click the word **here** in Click here to download the firmware file.
7. On the *File Download* screen, click **Save** to save the zip file to your computer.
8. Open the zip file and double-click the exe file.
9. The WET11 Firmware Upgrade utility will appear. Follow the on-screen instructions.

Appendix D: Windows Help

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

TCP/IP

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

Shared Resources

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

Network Neighborhood/My Network Places

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

Appendix E: Glossary

802.11a - An IEEE wireless networking standard that specifies a maximum data transfer rate of 54Mbps and an operating frequency of 5GHz.

802.11b - An IEEE wireless networking standard that specifies a maximum data transfer rate of 11Mbps and an operating frequency of 2.4GHz.

802.11g - An IEEE wireless networking standard that specifies a maximum data transfer rate of 54Mbps, an operating frequency of 2.4GHz, and backward compatibility with 802.11b devices.

Access Point - 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.

Adapter - This is a device that adds network functionality to your PC.

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

Backbone - The part of a network that connects most of the systems and networks together, and handles the most data.

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

Beacon Interval - The frequency interval of the beacon, which is a packet broadcast by a router to synchronize a wireless network.

Bit - A binary digit.

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

Bridge - A device that connects two different kinds of local networks, such as a wireless network to a wired Ethernet network.

Broadband - An always-on, fast Internet connection.

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

Buffer - A block of memory that temporarily holds data to be worked on later when a device is currently too busy to accept the data.

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

CSMA/CA (Carrier Sense Multiple Access/Collision Avoidance) - A method of data transfer that is used to prevent data loss in a network.

CTS (Clear To Send) - A signal sent by a device to indicate that it is ready to receive data.

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

Database - A collection of data that is organized so that its contents can easily be accessed, managed, and updated.

DDNS (Dynamic Domain Name System) - The capability of having a website, FTP, or e-mail server-with a dynamic IP address-use a fixed domain name.

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

DHCP (Dynamic Host Configuration Protocol) - A protocol that lets one device on a local network, known as a DHCP server, assign temporary IP addresses to the other network devices, typically computers.

DMZ (Demilitarized Zone) - Removes the Router's firewall protection from one PC, allowing it to be “seen” from the Internet.

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.

DSSS (Direct-Sequence Spread-Spectrum) - A type of radio transmission technology that includes a redundant bit pattern to lessen the probability of data lost during transmission. Used in 802.11b networking.

DTIM (Delivery Traffic Indication Message) - A message included in data packets that can increase wireless efficiency.

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

Encryption - Encoding data to prevent it from being read by unauthorized people.

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

Finger - A program that tells you the name associated with an e-mail address.

Firewall - Security measures that protect the resources of a local network from intruders.

Firmware - 1. In network devices, the programming that runs the device. 2. Programming loaded into read-only memory (ROM) or programmable read-only memory (PROM) that cannot be altered by end-users.

Fragmentation - Breaking a packet into smaller units when transmitting over a network medium that cannot support the original size of the packet.

FTP (File Transfer Protocol) - A standard protocol for sending files between computers over a TCP/IP network and the Internet.

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

Gateway - A system that interconnects networks.

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

Hardware - The physical aspect of computers, telecommunications, and other information technology devices.

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

IEEE (The Institute of Electrical and Electronics Engineers) - An independent institute that develops networking standards.

Infrastructure - Currently installed computing and networking equipment.

Infrastructure Mode - Configuration in which a wireless network is bridged to a wired network via an access point.

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.

ISM band - Radio band used in wireless networking transmissions.

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

LAN (Local Area Network) - The computers and networking products that make up the network in your home or office.

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

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

Multicasting - Sending data to a group of destinations at once.

NAT (Network Address Translation) - NAT technology translates IP addresses of a local area network to a different IP address for the Internet.

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

NNTP (Network News Transfer Protocol) - The protocol used to connect to Usenet groups on the Internet.

Node - A network junction or connection point, typically a computer or work station.

OFDM (Orthogonal Frequency Division Multiplexing) - A type of modulation technology that separates the data stream into a number of lower-speed data streams, which are then transmitted in parallel. Used in 802.11a, 802.11g, and powerline networking.

Packet - A unit of data sent over a network.

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

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

POP3 (Post Office Protocol 3) - A standard protocol used to retrieve e-mail stored on a mail server.

Port - 1. The connection point on a computer or networking device used for plugging in a cable or an adapter. 2. The virtual connection point through which a computer uses a specific application on a server.

PPPoE (Point to Point Protocol over Ethernet) - A type of broadband connection that provides authentication (username and password) in addition to data transport.

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

Preamble - Part of the wireless signal that synchronizes network traffic.

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

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

Router - A networking device that connects multiple networks together, such as a local network and the Internet.

RTS (Request To Send) - A packet sent when a computer has data to transmit. The computer will wait for a CTS (Clear To Send) message before sending data.

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.

Software - Instructions for the computer. A series of instructions that performs a particular task is called a “program”.

Spread Spectrum - Wideband radio frequency technique used for more reliable and secure data transmission.

SSID (Service Set IDentifier) - Your wireless network’s name.

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

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

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

Switch - 1. Device that is the central point of connection for computers and other devices in a network, so data can be shared at full transmission speeds. 2. A device for making, breaking, or changing the connections in an electrical circuit.

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

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 uses UDP and has no directory or password capability.

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

Topology - The physical layout of a network.

TX Rate - Transmission Rate.

UDP (User Datagram Protocol) - A network protocol for transmitting data that does not require acknowledgement from the recipient of the data that is sent.

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.

VPN (Virtual Private Network) - A security measure to protect data as it leaves one network and goes to another over the Internet.

WAN (Wide Area Network) - The Internet.

WEP (Wired Equivalent Privacy) - A method of encrypting data transmitted on a wireless network for greater security.

WINIPCFG - A Windows 98 and Millennium utility that displays the IP address for a particular networking device.

WLAN (Wireless Local Area Network) - A group of computers and associated devices that communicate with each other wirelessly.

Appendix F: Specifications

Model	WET11
Standards	IEEE 802.11b, IEEE 802.3
Ports	One 10BaseT RJ-45 port, Power port
Buttons	MDI/MDI-X slide switch, Reset button
Cabling Type	Category 5 or better
LEDs	Power, LAN, WLAN, Diag
Peak Gain of Antenna	5 dBi
Transmit Power	15 dBm @ Normal Temperature
Receive Sensitivity	-85 dBm
Security	WEP 64/128-bit
Dimensions	4.72" x 1.22" x 3.70" (120 mm x 31 mm x 94 mm)
Unit Weight	7.04 oz. (0.2 kg)
Power	External, DC 5V
Certifications	FCC, CE, IC-03, Wi-Fi
Operating Temp.	32°F to 104°F (0°C to 40°C)
Storage Temp.	-4°F to 158°F (-20°C to 70°C)

Operating Humidity	10% to 85%, Non-Condensing
Storage Humidity	5% to 90%, Non-Condensing
Warranty	1 Year Limited

Appendix G: Warranty Information

LIMITED WARRANTY

Linksys warrants to the original end user purchaser (“You”) that, for a period of one year, (the “Warranty Period”) Your Linksys product will be free of defects in materials and workmanship under normal use. Your exclusive remedy and Linksys's 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.

If the product proves defective during the Warranty Period call Linksys Technical Support in order to obtain a Return Authorization Number. BE SURE TO HAVE YOUR PROOF OF PURCHASE ON HAND WHEN CALLING. When returning a 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.

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, HOWEVER CAUSED REGARDLESS OF THE THEORY OF LIABILITY, ARISING OUT OF OR RELATED TO THE USE OF OR INABILITY TO USE THE PRODUCT, 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 Section 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 USA.

Appendix H: Regulatory Information

FCC STATEMENT

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 change or modification to the product not expressly approved by Linksys could void the user’s authority to operate the device.

FCC RF Radiation Exposure Statement

To comply with the FCC and ANSI C95.1 RF exposure limits, the antenna(s) for this device must comply with the following:

- Access points with 2.4 GHz or 5 GHz integrated antenna must operate with a separation distance of at least 20 cm from all persons using the cable provided and must not be co-located or operating in conjunction with any other antenna or transmitter.

End-users must be provided with specific operations for satisfying RF exposure compliance.

Note: Dual antennas used for diversity operation are not considered co-located.

INDUSTRY CANADA (CANADA)

This Class B digital apparatus complies with Canadian ICES-003.
Cet appareil numérique de la classe B est conforme à la norme NMB-003 du Canada.
The use of this device in a system operating either partially or completely outdoors may require the user to obtain a license for the system according to the Canadian regulations.

EC DECLARATION OF CONFORMITY (EUROPE)

Linksys declares that the Wireless-B Ethernet Bridge conforms to the specifications listed below, following the provisions of the European R&TTE directive 1999/5/EC:

For 11Mbps, 2.4 GHz devices with 100 mW radios, the following standards were applied:

- EN 301 489-1, 301 489-17 General EMC requirements for Radio equipment.
- EN 609 50 Safety
- ETS 300-328-2 Technical requirements for Radio equipment.

Caution: This equipment is intended to be used in all EU and EFTA countries. Outdoor use may be restricted to certain frequencies and/or may require a license for operation. Contact local Authority for procedure to follow.

Note: Combinations of power levels and antennas resulting in a radiated power level of above 100 mW equivalent isotropic radiated power (EIRP) are considered as not compliant with the above mentioned directive and are not allowed for use within the European community and countries that have adopted the European R&TTE directive 1999/5/EC.

For more details on legal combinations of power levels and antennas, contact Linksys Corporate Compliance.

- Linksys vakuuttaa täten että Wireless-B Ethernet Bridge tyyppinen laite on direktiivin 1999/5/EY oleellisten vaatimusten ja sitä koskevien näiden direktiivien muiden ehtojen mukainen.
- Linksys déclare que la Wireless-B Ethernet Bridge est conforme aux conditions essentielles et aux dispositions relatives à la directive 1999/5/EC.
- Dans le cas d'une utilisation privée, à l'extérieur d'un bâtiment, au-dessus d'un espace public, aucun enregistrement n'est nécessaire pour une distance de moins de 300m. Pour une distance supérieure à 300m un enregistrement auprès de l'IBPT est requise. Pour une utilisation publique à l'extérieur de bâtiments, une licence de l'IBPT est requise. Pour les enregistrements et licences, veuillez contacter l'IBPT.

- France F:

  2.4 GHz Bande : les canaux 10, 11, 12, 13 (2457, 2462, 2467, et 2472 MHz respectivement) sont complétement libres d'utilisation en France (en utilisation intérieur). Pour ce qui est des autres canaux, ils peuvent être soumis à autorisation selon le départment. L'utilisation en extérieur est soumis à autorisation préalable et très restreint.

  Vous pouvez contacter l'Autorité de Régulation des Télécommunications (http://www.art-telecom.fr) pour de plus amples renseignements.

  2.4 GHz Band: only channels 10, 11, 12, 13 (2457, 2462, 2467, and 2472 MHz respectively) may be used freely in France for indoor use. License required for outdoor installations.

  Please contact ART (http://www.art-telecom.fr) for procedure to follow.

Appendix I: Contact Information

Need to contact Linksys? Visit us online for information on the latest products and updates to your existing products at:	http://www.linksys.com or ftp.linksys.com
Can't find information about a product you want to buy on the web? Do you want to know more about networking with Linksys products? Give our advice line a call at:	800-546-5797 (LINKSYS)
Or fax your request in to:	949-261-8868
If you experience problems with any Linksys product, you can call us at:	800-326-7114
Don't wish to call? You can e-mail us at:	support@linksys.com
If any Linksys product proves defective during its warranty period, you can call the Linksys Return Merchandise Authorization department for obtaining a Return Authorization Number at:	949-261-1288
(Details on Warranty and RMA issues can be found in the Warranty Information section in this Guide.)	