



# **3Com 802.11g 54Mbps Wireless LAN Building to Building Bridge User's Guide**

**Version 2.0**

**Outdoor: 3CRWEASYG73**

**Indoor: 3CRWE920G73**



Copyright © 2005, 3Com Technologies. All rights reserved. No part of this documentation may be reproduced in any form or by any means or used to make any derivative work (such as translation, transformation, or adaptation) without written permission from 3Com Technologies.

3Com Technologies reserves the right to revise this documentation and to make changes in content from time to time without obligation on the part of 3Com Technologies to provide notification of such revision or change.

3Com Technologies provides this documentation without warranty, term, or condition of any kind, either implied or expressed, including, but not limited to, the implied warranties, terms or conditions of merchantability, satisfactory quality, and fitness for a particular purpose. 3Com may make improvements or changes in the product(s) and/or the program(s) described in this documentation at any time.

If there is any software on removable media described in this documentation, it is furnished under a license agreement included with the product as a separate document, in the hard copy documentation, or on the removable media in a directory file named LICENSE.TXT or !LICENSE.TXT. If you are unable to locate a copy, please contact 3Com and a copy will be provided to you.

#### **UNITED STATES GOVERNMENT LEGEND**

*If you are a United States government agency, then this documentation and the software described herein are provided to you subject to the following:*

All technical data and computer software are commercial in nature and developed solely at private expense. Software is delivered as "Commercial Computer Software" as defined in DFARS 252.227-7014 (June 1995) or as a "commercial item" as defined in FAR 2.101(a) and as such is provided with only such rights as are provided in 3Com's standard commercial license for the Software. Technical data is provided with limited rights only as provided in DFAR 252.227-7015 (Nov 1995) or FAR 52.227-14 (June 1987), whichever is applicable.

You agree not to remove or deface any portion of any legend provided on any licensed program or documentation contained in, or delivered to you in conjunction with, this User Guide.

Unless otherwise indicated, 3Com registered trademarks are registered in the United States and may or may not be registered in other countries.

3Com and the 3Com logo are registered trademarks of 3Com Corporation. XRN is a trademark of 3Com Corporation IEEE and 802 are registered trademarks of the Institute of Electrical and Electronics Engineers, Inc. Intel and Pentium are registered trademarks of Intel Corporation. Microsoft, MS-DOS, Windows, and Windows NT are registered trademarks of Microsoft Corporation. Novell and NetWare are registered trademarks of Novell, Inc. UNIX is a registered trademark in the United States and other countries, licensed exclusively through X/Open Company, Ltd. Netscape Navigator is a registered trademark of Netscape Communications. HP OpenView is a registered trademark of Hewlett Packard. JavaScript is a trademark of Sun Microsystems. All other company and product names may be trademarks of the respective companies with which they are associated.

#### **ENVIRONMENTAL STATEMENT**

It is the policy of 3Com Corporation to be environmentally-friendly in all operations. To uphold our policy, we are committed to:

Establishing environmental performance standards that comply with national legislation and regulations.

Conserving energy, materials and natural resources in all operations.

Reducing the waste generated by all operations. Ensuring that all waste conforms to recognized environmental standards. Maximizing the recyclable and reusable content of all products.

Ensuring that all products can be recycled, reused and disposed of safely.

Ensuring that all products are labelled according to recognized environmental standards.

Improving our environmental record on a continual basis.

#### **End of Life Statement**

3Com processes allow for the recovery, reclamation and safe disposal of all end-of-life electronic components.

#### **Regulated Materials Statement**

3Com products do not contain any hazardous or ozone-depleting material.

#### **Environmental Statement about the Documentation**

The documentation for this product is printed on paper that comes from sustainable, managed forests; it is fully biodegradable and recyclable, and is completely chlorine-free. The varnish is environmentally-friendly, and the inks are vegetable-based with a low heavy-metal content.

# CONTENTS

<b>ABOUT THIS GUIDE</b>	<b>5</b>
Purpose	5
Prerequisite Skills and Knowledge	5
Conventions Used in this Document	6
3Com Corporation Technical Support	6
<b>1 INTRODUCTION</b>	<b>7</b>
Product Overview	7
Operating Modes	8
<b>2 INSTALLING THE WIRELESS BRIDGE</b>	<b>9</b>
Overview	9
Scope of Delivery	9
Hardware Installation	10
Installing the 3CRWE920G73 Indoor Wireless Bridge	10
Installing the 3CRWEASYG73 Outdoor Wireless Bridge	14
Installing the 3CRWEASYG73/3CRWE920G73 Antenna	16
Antenna Specification	17
Connect to the Power Source and the Local Network	18
LED Indicators	19
Software Installation	20
Find your New Wireless Bridge	21
Using the Diagnostic Utility	23
Contents of CD	28
<b>3 WIRELESS BRIDGE CONFIGURATION</b>	<b>29</b>
Initialization	29
The first login	29
Accessing the Web Manager Interface	30
Setup Wizard	31
Wireless Setup	31
Security Setup	32
WDS Links Setup	34
Setup Finished	35
Device Summary	36
General	36
Internet	37
Wireless	38
Security	39
Save Configuration	40
Internet Settings	41
IP Setup	41
DHCP Server	42
Wireless Settings	43

Wireless	43
Security	45
WDS links	48
Device Management	52
Device Information	52
System Access	53
STP	55
Time	56
SNMP	57
System tools	59
Backup/Restore	59
Upgrade	62
Reboot	65
Reset	65
Event Logs	66
Event Log Status	66
Event Log Setup	67
Event Log Filter	68
System Status	69
Statics	69
STP	71
STP Statics	71
STP Port	72
<b>4 TROUBLESHOOTING</b>	<b>73</b>
Reset to Factory Default procedure	73
Setting IP Address Using 3Com Wireless Infrastructure Device Manager	73
Hardware and software requirements	73
Discover the wireless bridge	73
Initializing the IP Address using 3Com Wireless Infrastructure Device Manager	74
<b>5 SPECIFICATIONS</b>	<b>75</b>
Regulatory domains	75
Hardware Specification	76
Software Specification	77
<b>6 GLOSSARY</b>	<b>78</b>
REGULATORY INFORMATION	83

# ABOUT THIS GUIDE

---

## Purpose

This document provides information and procedures on hardware installation, setup, configuration, and management of the 3Com Corporation 802.11g Wireless Bridge.

---

## Prerequisite Skills and Knowledge




To use this document effectively, you should have a working knowledge of Local Area Networking (LAN) concepts and wireless Internet access infrastructures. In addition, you should be familiar with the following:

- ◆ Hardware installers should have a working knowledge of basic electronics and mechanical assembly, and should understand related local building codes.
- ◆ Network administrators should have a solid understanding of software installation procedures for network operating systems under Microsoft Windows 95, 98, Millennium Edition, 2000, NT, and Windows XP and general networking operations and troubleshooting knowledge.

## Conventions Used in this Document

Table 1 and Table 2 list conventions that are used throughout this guide.

**Table 1** Notice Icons

Icon	Notice Type	Description
	Information note	Information that describes important features or instructions.
	Caution	Information that alerts you to potential loss of data or potential damage to an application, system, or device.
	Warning	Information that alerts you to potential personal injury.

**Table 2** Text Conventions

Convention	Description
Screen displays	This typeface represents information as it appears on the screen.
Syntax	The word “syntax” means that you must evaluate the syntax provided and then supply the appropriate values for the placeholders that appear in angle brackets. Example: To change your password, use the following syntax: <code>system password &lt;password&gt;</code> In this example, you must supply a password for <password>.
Commands	The word “command” means that you must enter the command exactly as shown and then press Return or Enter. Commands appear in bold. Example: To display IP information, enter the following command: <code>get ipaddr</code>
The words “enter” and “type”	When you see the word “enter” in this guide, you must type something, and then press Return or Enter. Do not press Return or Enter when an instruction simply says “type.”
Keyboard key names	If you must press two or more keys simultaneously, the key names are linked with a plus sign (+). Example: Press Ctrl+Alt+Del
Words in <i>italics</i>	Italics are used to: <ul style="list-style-type: none"> <li>■ Emphasize a point.</li> <li>■ Denote a new term at the place where it is defined in the text.</li> <li>■ Identify menu names, menu commands, and software button names. Examples: From the <i>Help</i> menu, select <i>Contents</i>. Click <i>OK</i>.</li> </ul>

## 3Com Corporation Technical Support

If you encounter problems when installing or using this product, please consult the 3Com Corporation website at

<http://www.3Com.com>

for

- ◆ The latest software, user documentation and product updates.
- ◆ Frequently Asked Questions (FAQ).
- ◆ Direct contact to the 3Com Corporation support centers.

# 1

## INTRODUCTION

Thank you for choosing the 3Com Corporation 802.11g Wireless LAN Building to Building Bridge.

This manual will give you a short introduction to the device and its hardware and show you how to install and set up the Wireless Bridge.

---

### Product Overview

#### **Maximum Wireless Throughput**

The 3Com Corporation 802.11g Wireless Bridge offers the fastest wireless throughput in the 2.4GHz frequency band and delivers a data transmission rate up to 54Mbps, which is faster than any 802.11b Bridge.

#### **Wireless Access Security**

The 3Com Corporation 802.11g Wireless Bridge provides high-level security with full 128-bit RC4 data encryption or 64-bit WEP encryption. The Wireless Bridge supports WPA-PSK and VPN pass through, which provide a more advanced data protection during wireless transmission.

#### **Install and Maintain**

With an external antenna under point-to-point or point-to-multi-point mode, it enables long range high speed link between buildings.

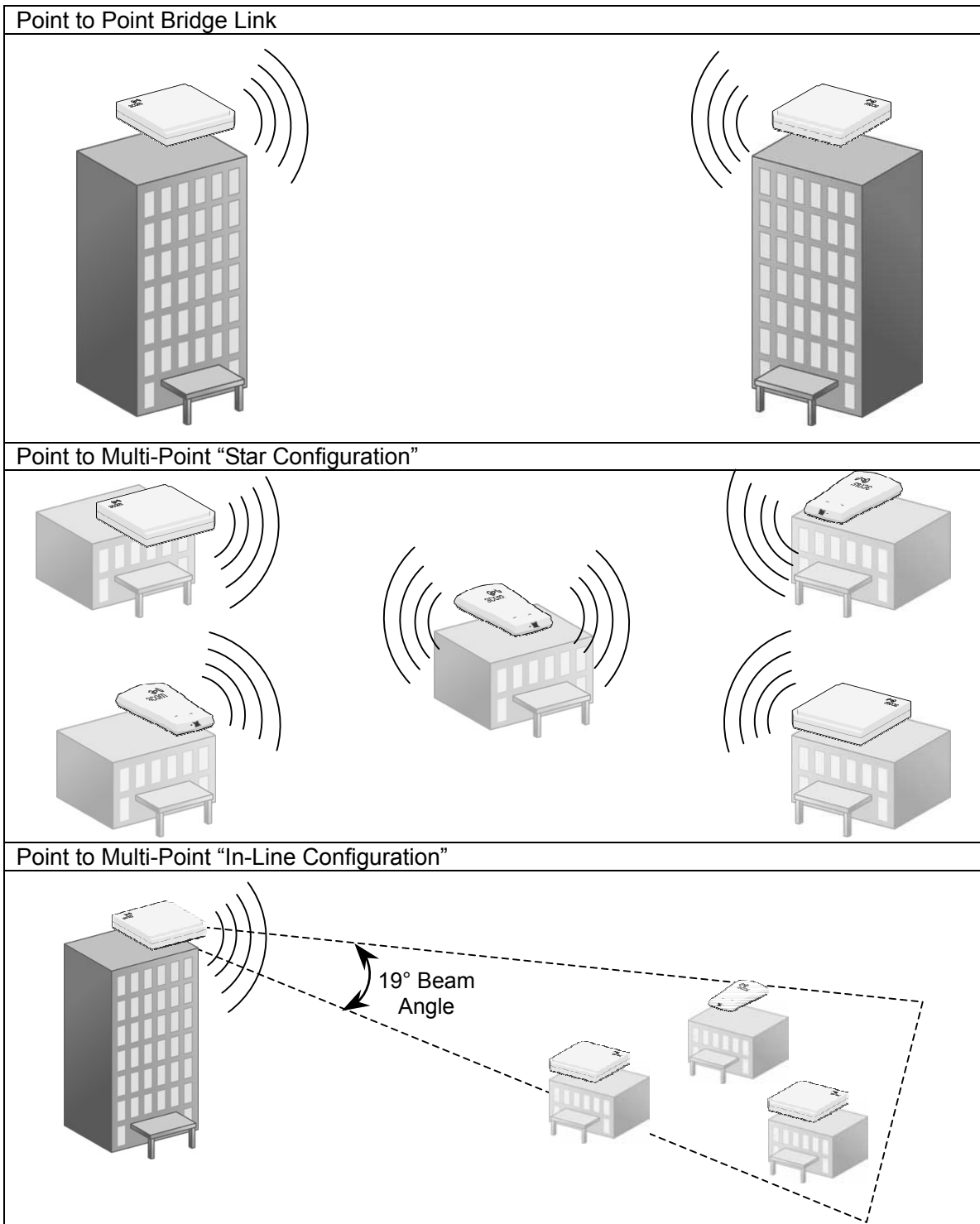
Power over Ethernet reduces installation expenses and increases location options via a single Ethernet cable to provide both data and power to the unit.



## Operating Modes

The 3Com Corporation 802.11g Wireless Bridge can work in point-to-point and point-to-multipoint bridge modes:

In these modes the Wireless Bridge connects two or more wired networks, for example networks in different buildings with no wired connections. You will need a 3Com 802.11g 54Mbps Building to Building Bridge on both sides of the connection. In this case, the Wireless Bridge acts as a network bridge between wireless and wired networks. In bridge mode the Wireless Bridge can connect up to seven remote networks.



# 2

## INSTALLING THE WIRELESS BRIDGE

---

### Overview

This chapter provides installation instructions for the hardware and software components of the 3Com Corporation 802.11g Wireless Bridge. It also includes the following information:

- ◆ Package content
- ◆ Hardware installation
- ◆ Software installation

---

### Scope of Delivery

Please ensure that the package is complete before beginning with the installation. The package should include the following:

- ◆ 3Com 802.11g Wireless Bridge
- ◆ Mounting kit for wall or mast mount (indoor / outdoor respectively)
- ◆ CD-ROM containing software and documentation
- ◆ Power over Ethernet Power Injector
- ◆ Lightning arrestor (outdoor bridge only)

## Hardware Installation

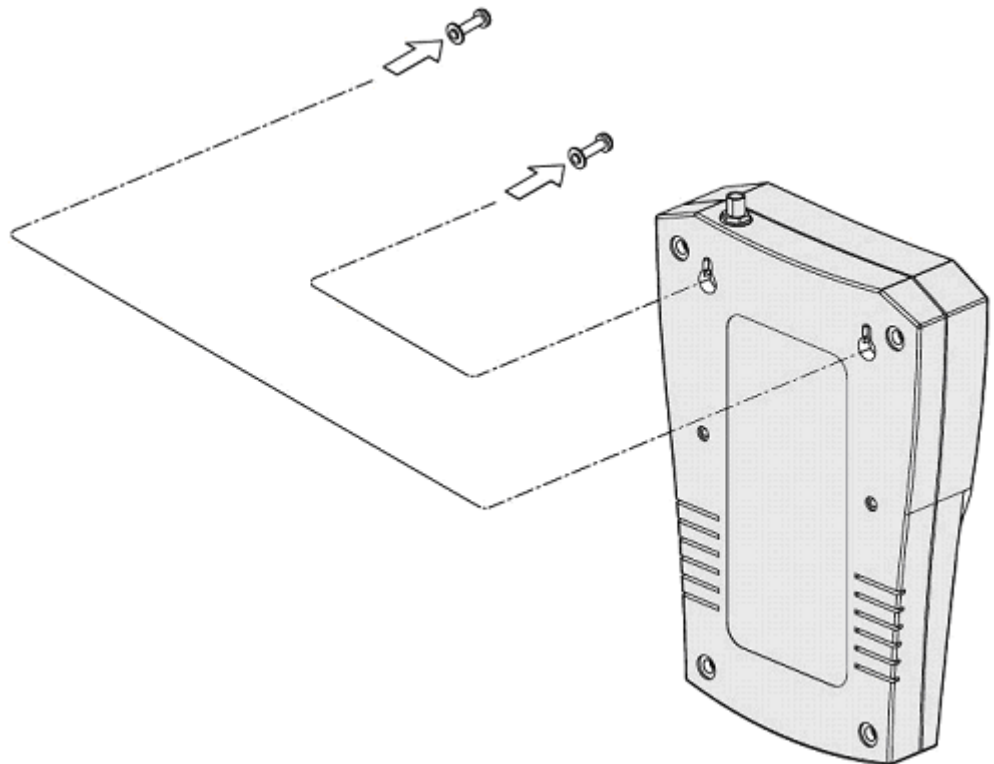
### Installing the 3CRWE920G73 Indoor Wireless Bridge

#### On a flat surface

1. Find a surface that is clear of debris.
2. Set the bridge down on its four rubber feet.

#### On a wall

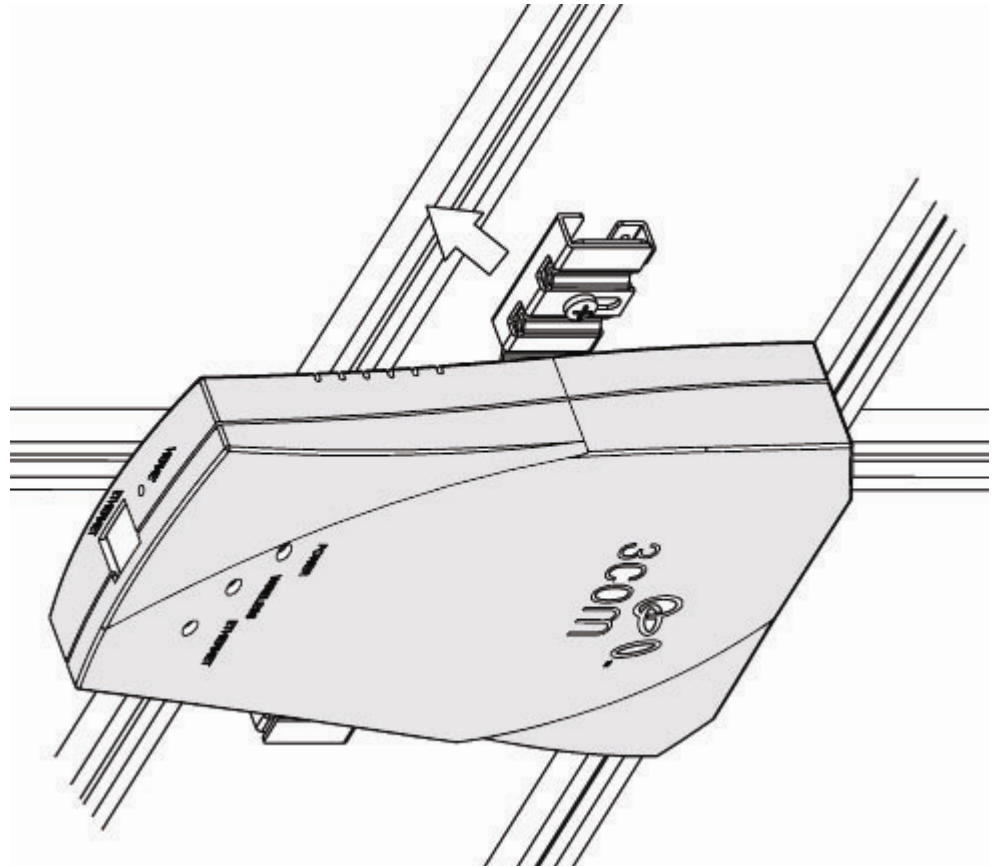
1. Use the mounting template as a guide to make two marks 7.40cm (2.91 inches) apart on the wall.  
Use the vertical line on the template to ensure that the placement of the marks is plumb to the wall.
2. Drill holes at the marks.  
Use a 5-mm (3/16-inch) drill bit if using the provided screw anchors; use a 3-mm (1/8-inch) drill bit if using the screws only.
3. Install the two flathead screws at the marks on the wall.  
Leave the screw heads protruding 6-mm (1/4 inch) from the surface of the wall.
4. Hang the bridge on the screws, using the mounting holes on the back of the bridge.



### On an acoustical ceiling

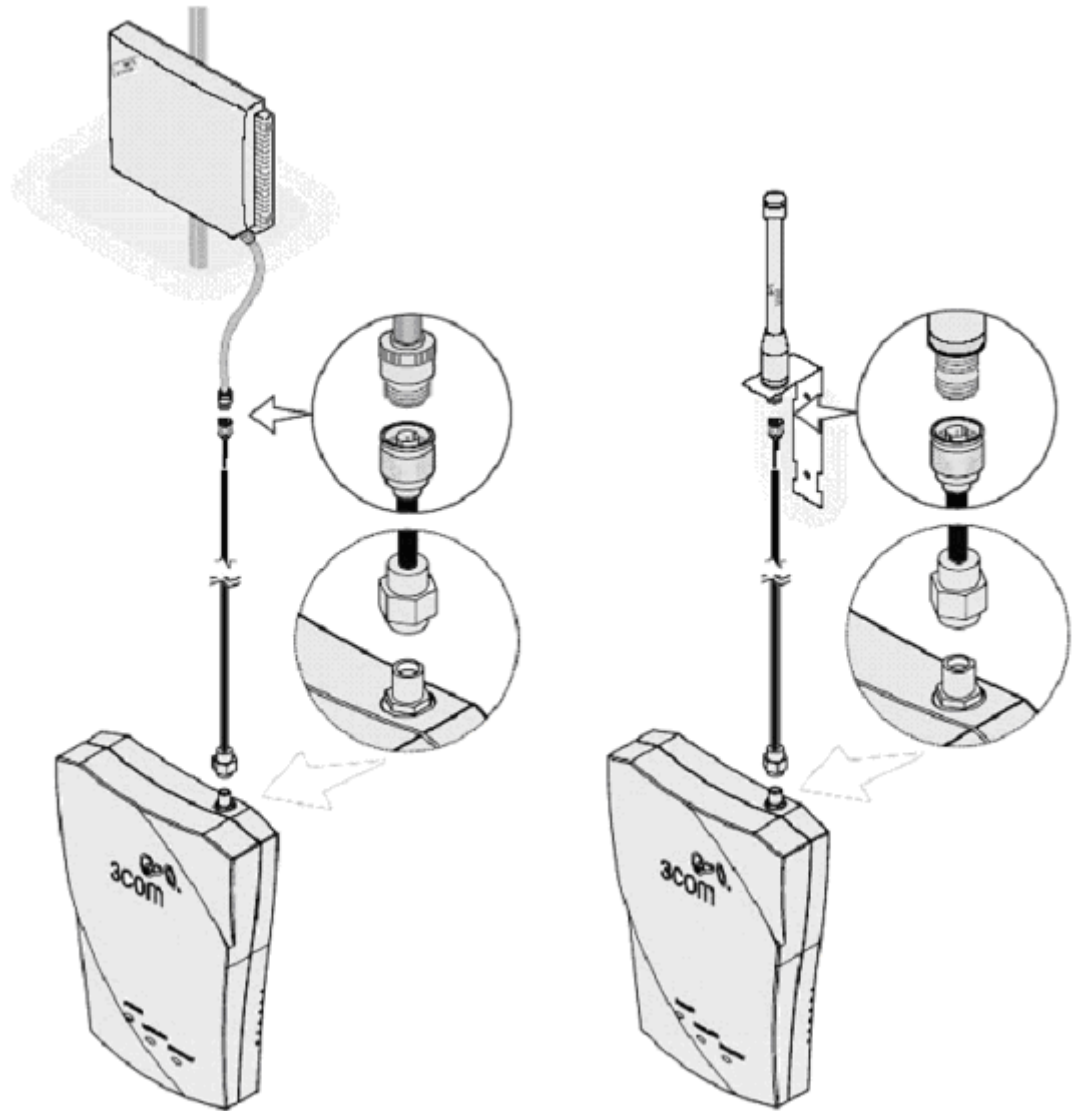
1. Attach the mounting bracket to the back of the bridge with two number 6 panhead screws.
2. Align the T-rail grips with the ceiling T-rail, and adjust them so that they grip the T-rails securely.
3. Tighten the screws on each T-rail grip.

After installation, there may be some play in the fit of the T-rail grips if the T-rails are very narrow. If necessary, add a shim to achieve a secure grip.



### Connect the antenna

1. Connect one end of the antenna cable to the antenna.
2. Connect the free end of the antenna cable to the connection on the bridge.



Follow the instructions that come with the antenna and follow these general guidelines:

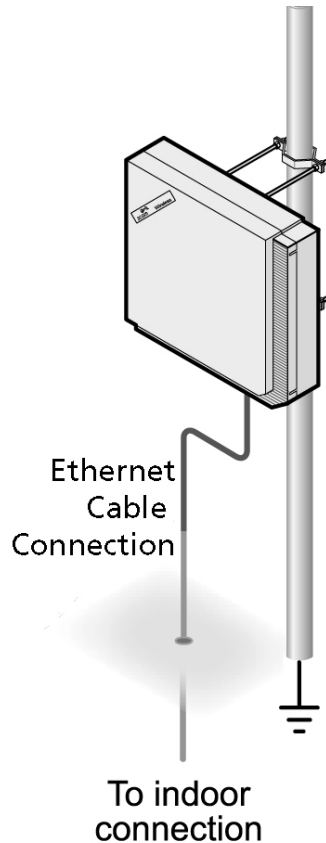
- ◆ For best performance, place the antenna using the mounting hardware provided with the antenna. Outdoor placement is especially important if the building is of metal construction or has metal siding. If necessary, you can mount an antenna inside a building; however, indoor placement reduces the antenna's effective range. For indoor antenna use, try to mount antenna near a window with line of sight to opposite bridge.
- ◆ To ensure the physical safety of anyone near the antenna and to prevent damage to the bridge, follow the building codes for antenna installations in your area.

- ◆ Position the antenna so that there are minimal obstacles between it and any other antenna with which it will communicate. While maintaining a direct line of sight between antennas is not strictly necessary, such an arrangement helps to ensure a strong signal. Ensure that access is available for routing the antenna cable from the antenna to the bridge.
- ◆ Make certain that the antenna and antenna mast are appropriately grounded. Proper grounding prevents injury or damage from lightning strikes. To minimize risk of damage to your network equipment, install and properly ground the included lightning arrestor on the outdoor bridge.

## Installing the 3CRWEASYG73 Outdoor Wireless Bridge

### Mount the Unit to a Mast

Follow the instructions that come with the bridge mounting hardware and follow the general guidelines listed below.



### NOTE:

**Mast should extend above bridge 1 meter (3 ft)**

**Recommended Pole Diameter = 2" – 2.5"**

**Maximum Pole Diameter = 3"**

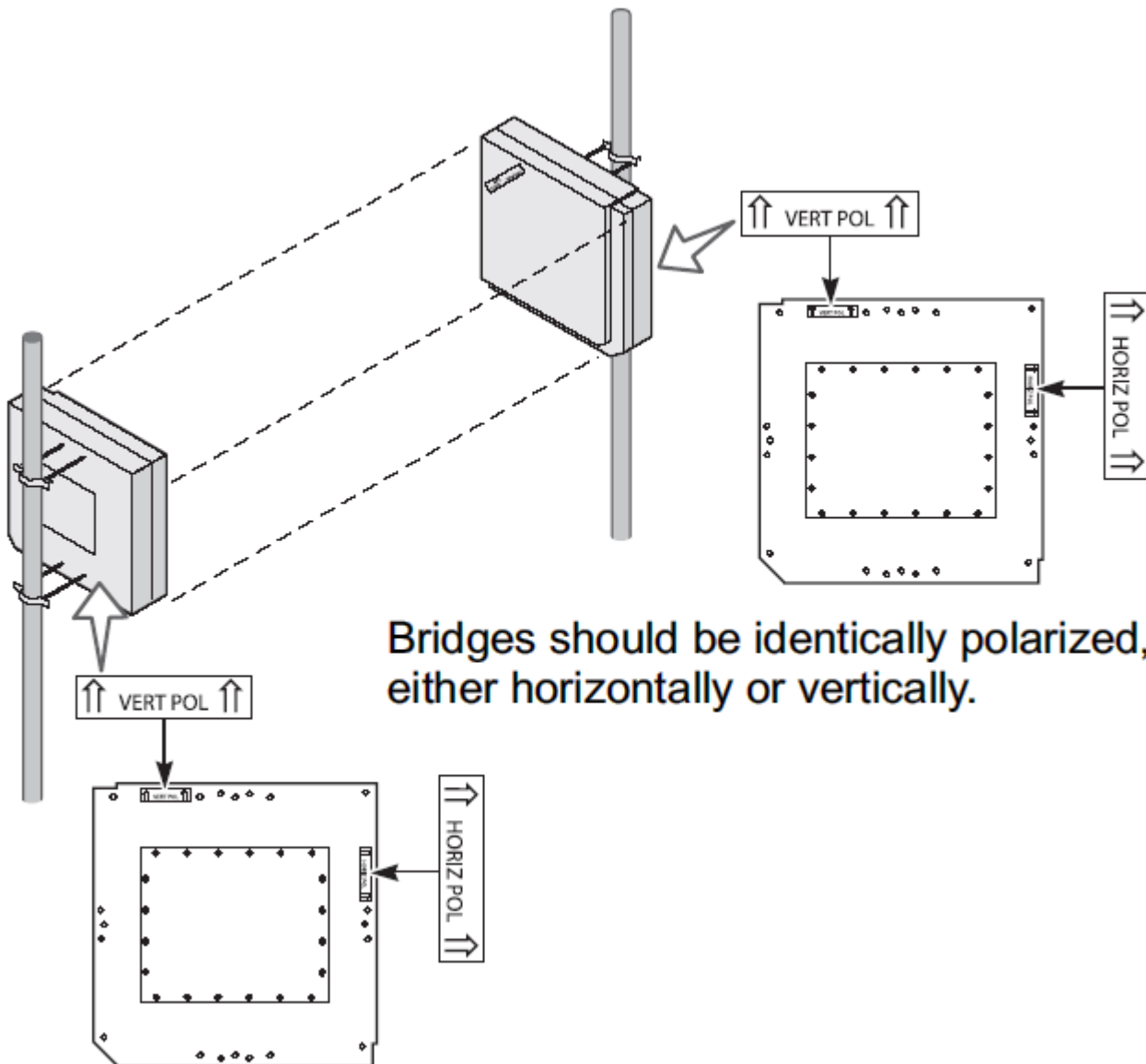
**Bridge may be installed to freestanding or roof mounted mast**

- ◆ For best performance, place the antenna outdoors using the mounting hardware provided with the antenna. Placement is especially important if the building is of metal construction or has metal siding. If necessary, you can mount an antenna inside a building; however, indoor placement reduces the antenna's effective range.
- ◆ To ensure the physical safety of anyone near the antenna and to prevent damage to the bridge, follow the building codes for antenna installations in your area. This is another good reason to make sure that only a professional performs the installation.
- ◆ Keep in mind that in order to comply with FCC radio-frequency radiation exposure guidelines, a minimum body to antenna distance of 2 meters (6 feet) must be maintained while operating this device.
- ◆ Ensure that access is available for routing the Ethernet cable from the bridge to the Ethernet connection inside.
- ◆ Make certain that the antenna mast is appropriately grounded. Proper grounding can prevent injury or damage from lightning strikes.
- ◆ After installing the bridge, the highest allowable power level is automatically set when country selection is configured. Adhering to this configuration ensures compliance with national laws.

### Align and Polarize the Units

For optimal performance, position the antenna so that there are minimal obstacles between it and any other antenna with which it will communicate. While maintaining a direct line of sight between antennas is not strictly necessary, such a configuration helps to ensure a strong signal. As mentioned earlier, this is not always possible in long distance configurations.

Any two bridge units that are to communicate with each other must be set for the same polarization, either horizontally or vertically. If cross-polarization occurs, the link will either work poorly or not at all. Please refer to the “Polarization” section of the User Guide for further details. The following illustration shows proper alignment, orientation and polarization for optimal performance.





## Installing the 3CRWEASYG73/3CRWE920G73 Antenna

The installation of indoor wireless links requires technical expertise. At the very least, you should be able to:

- Install and configure the network components, such as the 3Com wireless bridge hardware.
- Understand, or have a working knowledge of, installation procedures for network operating systems using Microsoft Windows.
- Mount the indoor antenna. Antenna installation must be provided by professional installers.



### **WARNING!**

The indoor antennas to be used with these products are intended for mounting on an antenna tower, on a roof, or on the side of a building. Installation is not to be attempted by someone not trained or experienced in this type of work. The antenna must be installed by a suitably trained professional installation technician or by a qualified antenna installation service. The site prerequisites must be checked by a person familiar with the National Electrical Code and with other regulations governing this type of installation.

Local radio regulations or legislation may impose restrictions on the use of specific combinations of:

- Low-loss antenna cables and indoor antennas
- Radio channels selected at the radios that are connected to specific indoor antennas



**Note:** A basic rule for selecting a combination of cables and antennas is that no combination is allowed unless explicitly approved in the 3Com wireless bridge User Guide for your product. Therefore, always use 3Com recommended antennas in page 16 of User Guide to select the correct type of antenna equipment and to inform your antenna installer and LAN administrator about the impact of regulatory constraints on their job or activities.



**CAUTION:** At all times, it is the customer's responsibility to ensure that an indoor antenna installation complies with local radio regulations.<sup>1</sup>

The customer must verify that:

The antenna installer is aware of these regulations.

The correct cable type and surge arrestor have been used, according to the instructions described in the user guide. 3Com Corporation and its resellers or distributors are not liable for any damage or violation of government regulations that may arise from failing to comply with these guidelines.

*<sup>1</sup>In case you are not certain about the regulations that apply in your country, consult your local 3Com representatives.*

## Antenna Specification

The following antennas and cables are available from 3Com Corporation:

### ◆ Antennas

3CWE492 2.5dBi ceiling mount	3CWE490 4 dBi Omni-directional	3CWE491 8 dBi Omni-directional
		
3CWE498 8 dBi sector panel	3CWE495 13 dBi Sector-Panel Directional	3CWE496 18 dBi Sector-Panel Directional
		
3CWE497 4dBi bi-directional		<b>Antenna Cables:</b>
		



**NOTE:** Because of power level restrictions, use of the 3CWE495 13dBi and 3CWE496 18dBi antennas is not allowed in some countries.

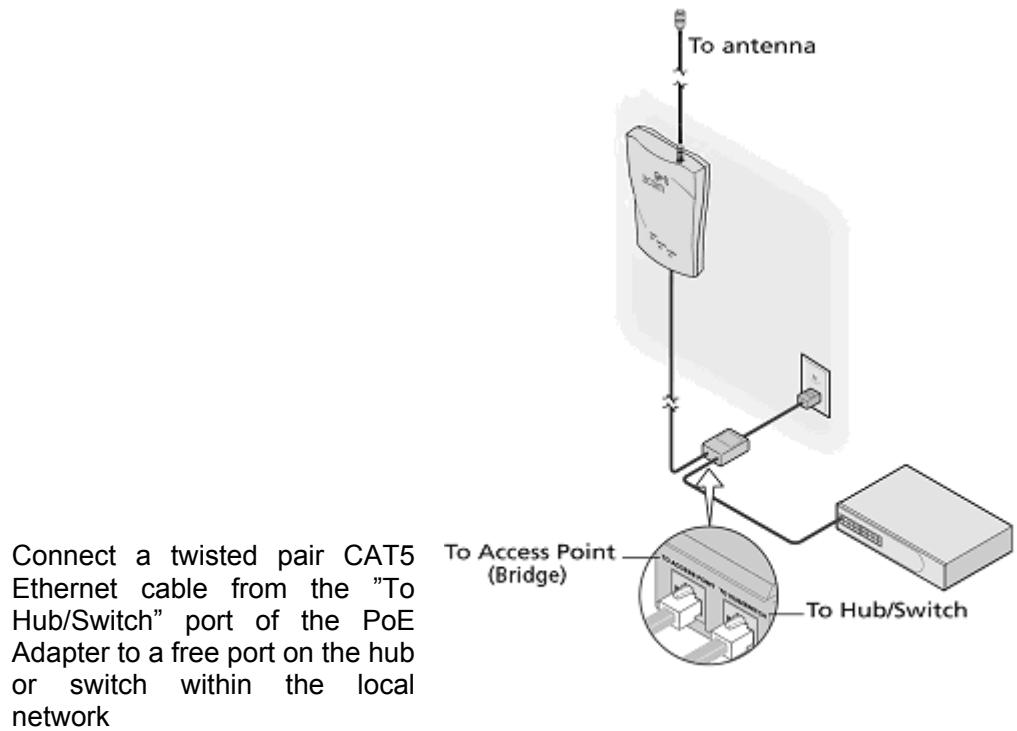
The highest allowable power level is set automatically when you configure antenna selection after installing the bridge.

To comply with power restrictions, identical antennas using 6-foot cable must be separated by at least the minimum distances shown below:

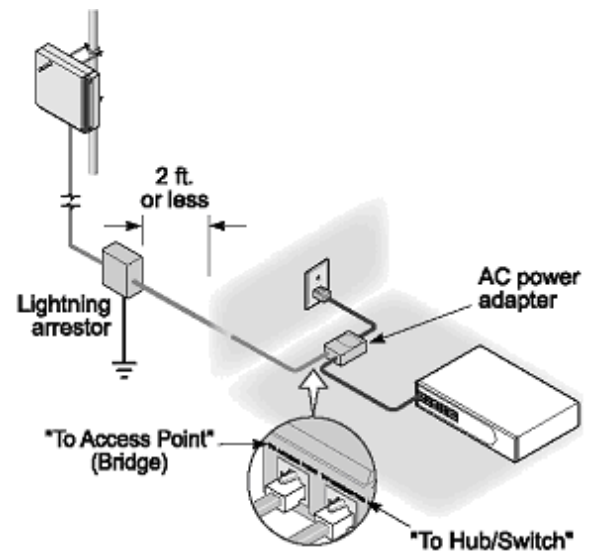
Antenna (dBi)	Minimum Distance for Full Throughput (approximate)	
	Meters	Yards
18	200	218
13	50	55
8	10	11
4	2	2

## Connect to the Power Source and the Local Network

### 3CRWE920G73 Indoor Wireless Bridge

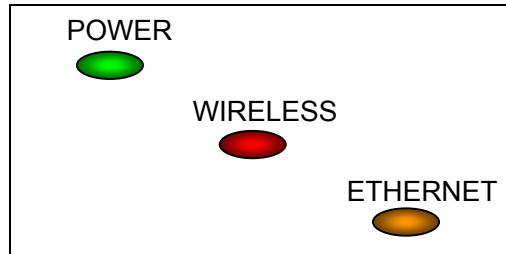


### 3CRWEASYG73 Outdoor Wireless Bridge



## LED Indicators

After the correct connection, the power LED and the LAN link LED of the 3CRWE920G73 indoor bridge should light up. On the front of the Wireless Bridge you will find three LEDs.



1. POWER LED  
Off: Power supply connection not available or broken  
On: Power supply connection OK
2. WIRELESS activity LED  
Off: No activity  
Blinking: Sending and receiving data
3. ETHERNET LAN link LED  
Off: No LAN connection available  
On: LAN connection OK

## Software Installation

Insert the installation CD-ROM delivered with the 3Com WLAN Building to Building Bridge into your CD-ROM drive

The installation wizard starts automatically and will guide you through the rest of the installation process. If the installation wizard does not start automatically, run "setup.exe" from the root directory of the installation CD. Then choose to install the 3Com Wireless Infrastructure Device Manager (WIDMAN) utility for helping you find the Bridge and configuring its IP address.

The 3Com Installation CD contains the following tools and utilities:

**3Com Wireless Infrastructure Device Manager (WIDMAN)** – an administration tool that helps you select 3Com wireless LAN devices and launch their configurations in your Web browser.

**3Com 3CDaemon Server Tool** – a firmware upgrade tool that can act in four different capacities:

- ◆ As a TFTP Server, necessary for firmware upgrades, and backup and restore functions. Use this option if you do not have a TFTP server set up.
- ◆ As a SysLog Server, which is necessary to view SysLog messages.
- ◆ As an optional TFTP Client.
- ◆ As an optional FTP Server.



**NOTE:** It is recommended that you install the 3CDaemon Server tool if you do not already have a firmware tool for upgrades on your computer.

**To install one of the tools on your computer:**

1. **Turn on the computer;**
2. **Insert the 3Com Installation CD in the CD-ROM drive;**  
The setup menu appears. If it does not appear, you can start the setup menu from the Windows Start menu. For example: **Start > Run > d:setup.exe** .
3. **In the menu, click Tools and Utilities.**
4. **In the next screen, click the tool you want to install.**
5. **Follow the instructions on the screens to complete the installation.**

Reboot the computer if prompted to do so.

6. **Launch the tool from the Windows Start menu.**

## Find your New Wireless Bridge

To find your new Wireless Bridge, open the 3Com Wireless Infrastructure Device Manager (WIDMAN) utility. On start up, the dialog box will look like the Figure below:



Click the 'Refresh' button and the 3Com Wireless Infrastructure Device Manager (WIDMAN) utility will begin to discover devices. After finding the new Wireless Bridge, it will appear in the list box.

Choose the Wireless Bridge in the list box, and then click the 'Configure...' button. If 3Com Wireless Infrastructure Device Manager (WIDMAN) finds that your PC cannot connect to the Wireless Bridge by IP, it would pop-up a dialog requesting that you change the IP address of the device. Then the utility will prompt you to enter the password of the bridge. **[Note: default password is "blank"]**



**NOTE:** It can take up to 60 seconds for the 3Com Building to Building Bridge to boot up after power has been connected. The Bridge will not appear in the WIDMAN utility until boot up is complete. Click the REFRESH button occasionally until the Bridge appears.

**Wireless Infrastructure Device Pre-IP Configuration**

To configure this wireless infrastructure device from this computer, you will need to adjust some of the settings so that they are compatible. The IP addresses and subnet masks must be from the same subnetwork.

Please specify an IP address and subnet mask that will be compatible with the settings used by your computer.

Wireless Infrastructure Device Settings

Obtain the settings automatically from a DHCP server

Specify the settings:

IP Address:

Subnet Mask:

Computer Settings

IP Address: 192.168.1.23

Subnet Mask: 255.255.255.0

After setting up a correct IP address for the device, you will be able to configure it through the WEB UI.

**Welcome!** It is the first time you configure the device! Please set the name and password needed for Administrator of your Wireless Bridge.

Username:

Password:

Confirm Password:

Country:

Antenna:

Cable:

The first time you configure the Wireless Bridge, you will see an initial Settings page. In this page, you will setup the username/password for administrator access. And you will select Country, antenna and cable Settings on this page as well.



- NOTE:**
1. Default USERNAME and PASSWORD are both 'admin'.
  2. Antenna and Cable settings only apply to indoor bridge.

After changing these settings, you will be redirected to the Login page. Please input the username and password that you setup on the initial page, and then you will login in the device successfully.

## Using the Diagnostic Utility

The Diagnostic Utility will help you review the status of 3Com wireless bridge, do a site survey for discovering wireless device around the wireless bridge.

The Diagnostic Utility must be installed on a computer that:

- ◆ Has a working Ethernet adapter.
- ◆ Is running one of the Windows operating systems of Win2000 and Win XP.
- ◆ Is on the same subnet as the wireless bridge.

The device to be diagnosed using the Diagnostic Utility must be:

- ◆ Connected to power.
- ◆ Wired to the network, associating with the wireless network, or, in some cases with the bridge, connected directly to the computer.

Before you connect to the device using the Diagnostic Utility, make sure the device IP address is in the same subnet with your computer.

To use the Diagnostic Utility, launch it by selecting **Start > Programs > Diagnostic Utility > Diagnostic Utility**.

The Diagnostic Utility will pop up a dialog to let you input the wireless bridge IP address and SNMP community for access the wireless bridge.

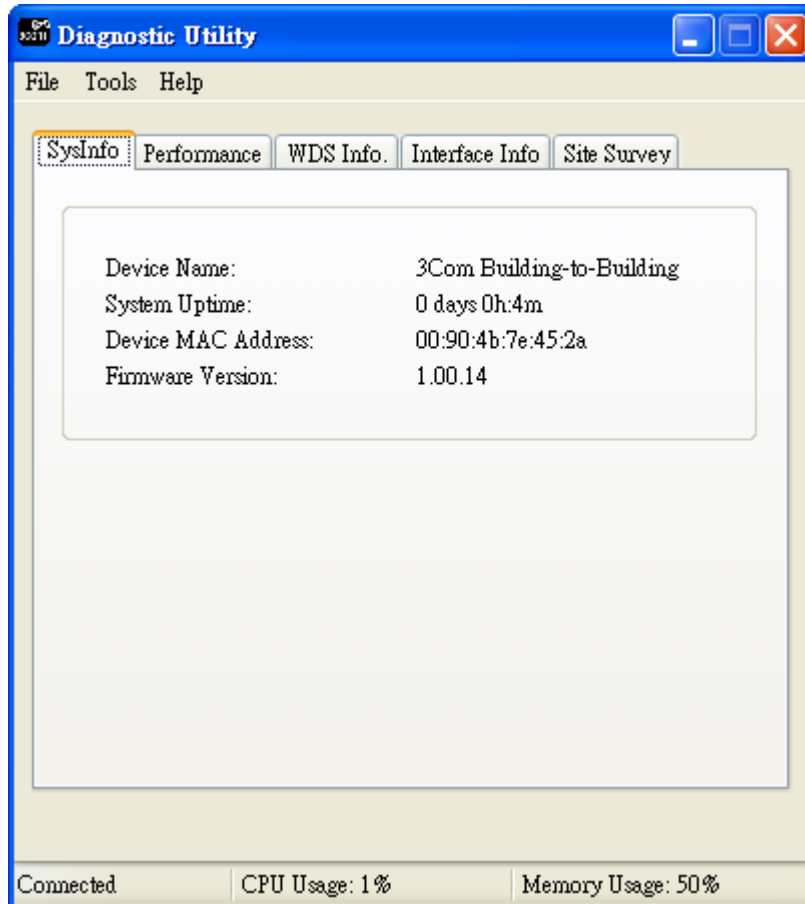
**Figure 1** – Input IP address and SNMP community



If the Diagnostic Utility connects to the wireless bridge successfully, it will open a property page dialog window.



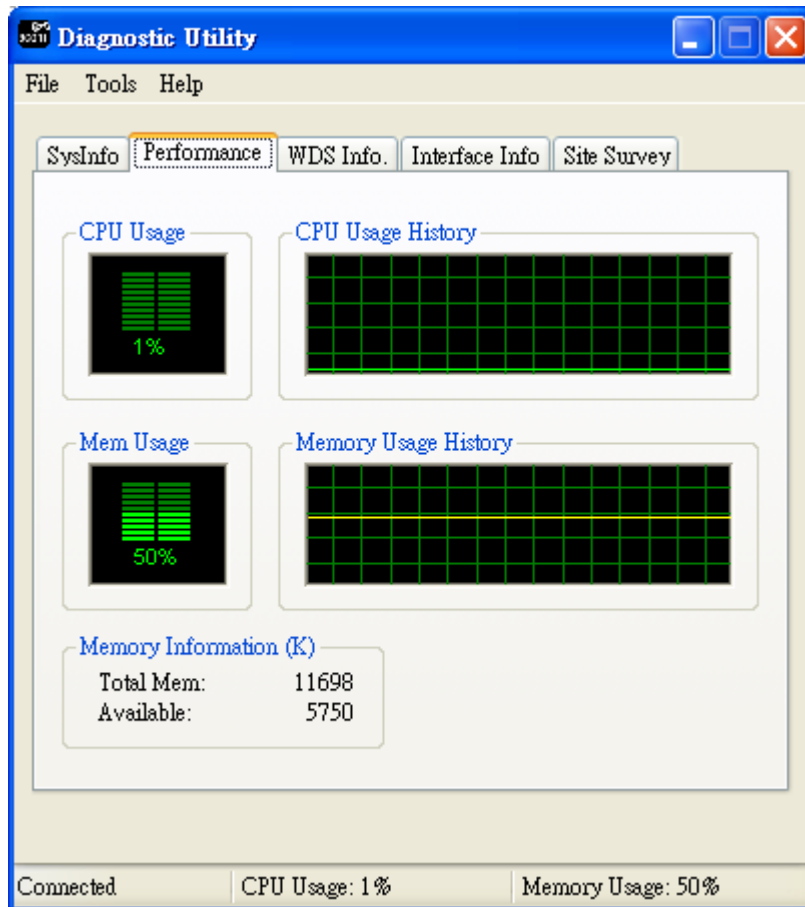
**Figure 2 – Diagnostic Utility Main Page**



On the SysInfo page, you will see the system uptime, bridge MAC address and the Firmware version number.

To check the system performance information, click the Performance tab.

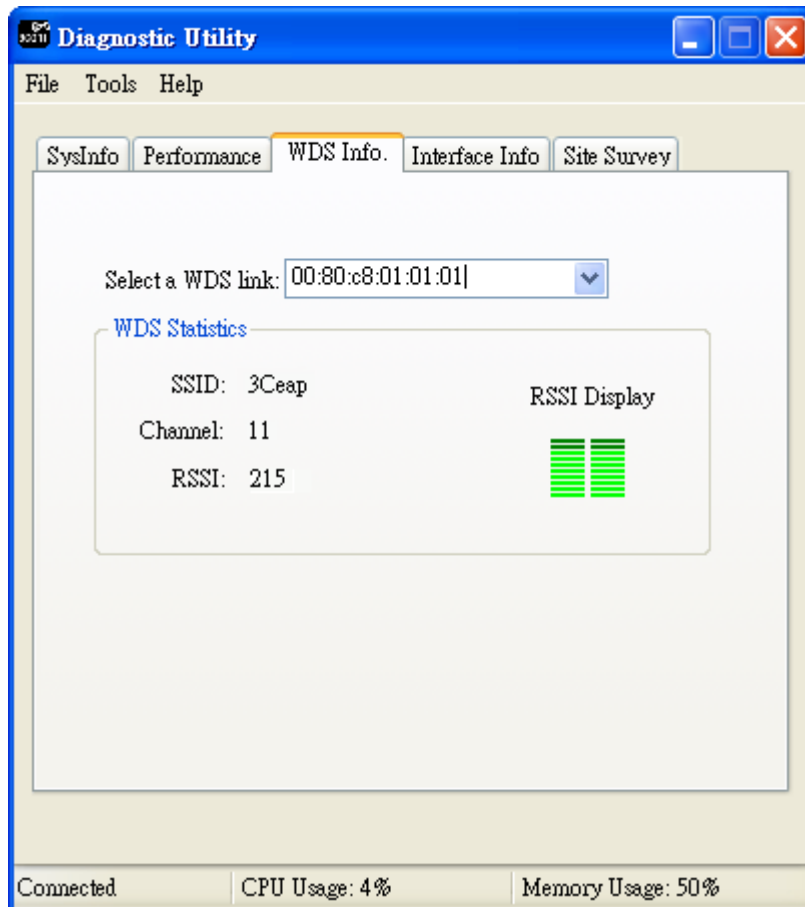
**Figure 3** – System Performances



The Performance tab displays the CPU and memory usage information.

To check the WDS link information, click the WDS Info tab.

**Figure 4 – WDS Information**

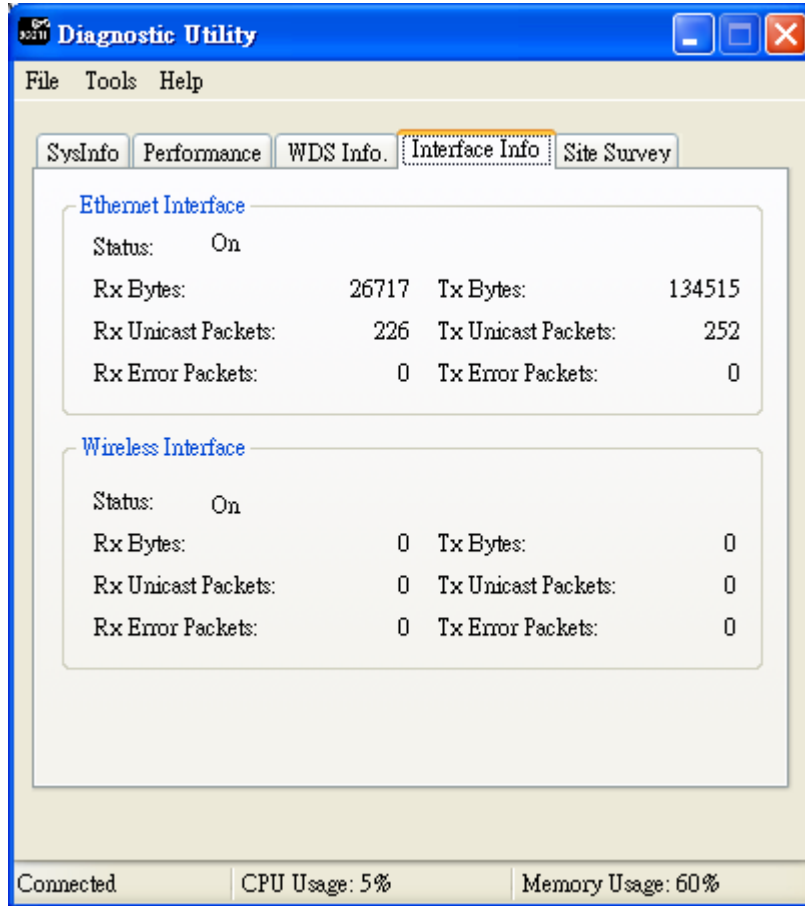


On the WDS Info tab select a WDS link from the drop down menu to see statistics for that link.

If there is no WDS link for the wireless bridge, the list box will be empty.

To check the interface statistics, click the Interface Info tab.

**Figure 5 – Interfaces Information**

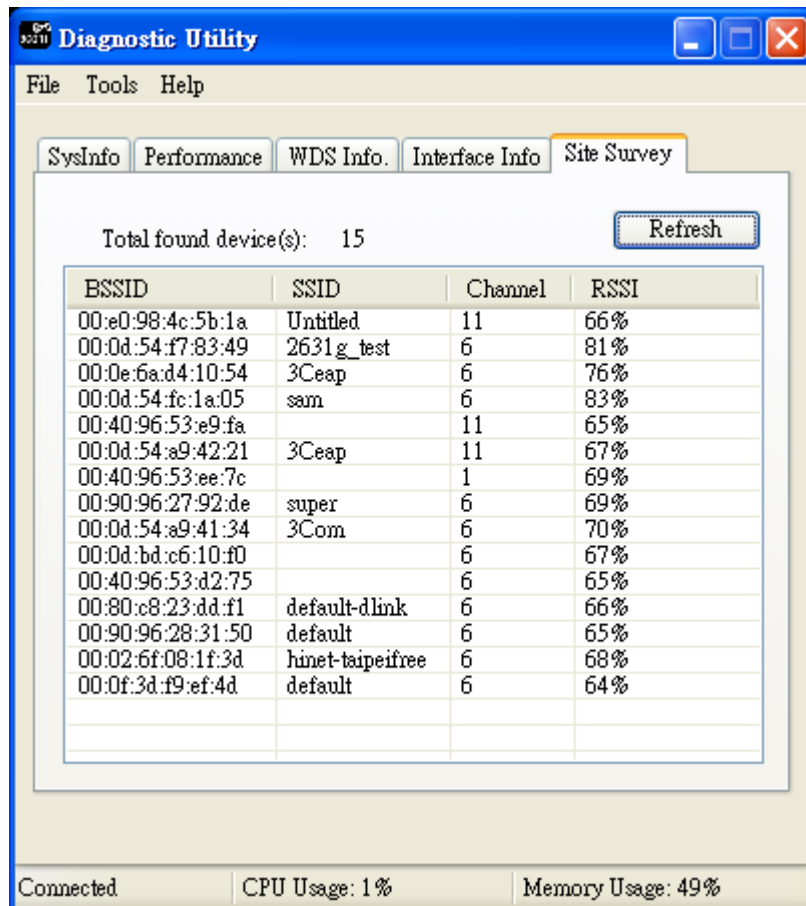


The Interface Info page, displays the Ethernet and Wireless interface information of the wireless bridge.

To scan other wireless sites around the wireless bridge, click the Site Survey tab. On this page, click the Refresh button to scan the wireless site.

NOTE: Doing a site survey will break all WDS links on the wireless bridge. An SNMP write privilege community string is required to do scanning. This can be input in the pop up dialog.

**Figure 6 – Site Survey**



The Site Survey page displays all other wireless sites.

## Contents of CD

The CD-ROM which is enclosed in the package should include the following contents:

- ◆ 3Com 802.11g 54Mbps Wireless LAN Building to Building Bridge User Guide
- ◆ MIB Directory  
Includes 3Com MIBs for Network Management usage
- ◆ Diagnostic Utility
- ◆ 3Com 3CDaemon Server Tool
- ◆ 3Com Wireless Infrastructure Device Manager (WIDMAN)
- ◆ Readme file

# 3

## WIRELESS BRIDGE CONFIGURATION

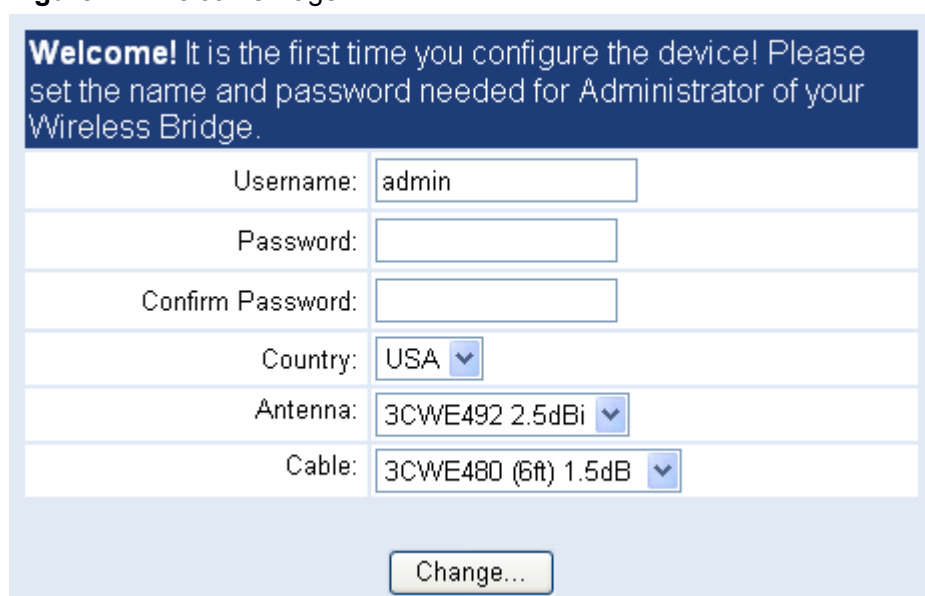
### Initialization

#### The first login

During initial power up and first login, you will need to configure the basic parameters of the bridge, such as the username, password and domain:

1. Connect a computer directly to the Bridge using standard Category 5 (CAT5) UTP Ethernet cable.
2. Open a Web browser on the computer.
3. In the **Address** or **Location** field: enter the IP address of a Bridge on the network. For example if the IP address is 192.168.1.1, type: <http://192.168.1.1> to access the Web Manager.
4. Press the **Enter** key, the **First Welcome** Screen appears:

Figure 7 – Welcome Page



The screenshot shows a web-based configuration page with a dark blue header containing the text: "Welcome! It is the first time you configure the device! Please set the name and password needed for Administrator of your Wireless Bridge." Below the header is a form with the following fields:

Username:	<input type="text" value="admin"/>
Password:	<input type="password"/>
Confirm Password:	<input type="password"/>
Country:	<input type="text" value="USA"/>
Antenna:	<input type="text" value="3CWE492 2.5dBi"/>
Cable:	<input type="text" value="3CWE480 (6ft) 1.5dB"/>

At the bottom of the form is a button labeled "Change..."

5. Set the **administrator name**, **password**, **Country**, and for the indoor bridge, **Antenna** and **Cable** selection. Next, press the **Change** button.

This will set the new administrator name and password.

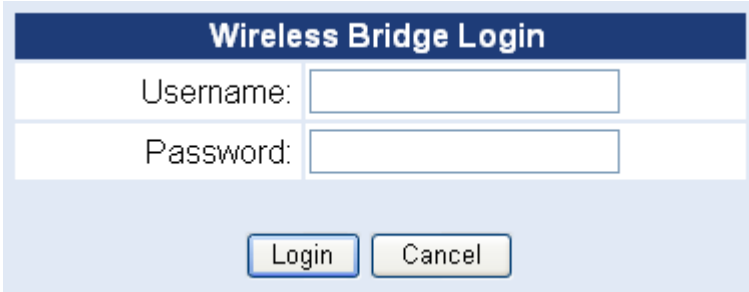


**NOTE:** The Web pages are best viewed at 1024x768.

## Accessing the Web Manager Interface

To log in to the Wireless Bridge configuration interface, launch your browser and enter the IP address of your Wireless Bridge in the address field. The network identification dialogue appears:

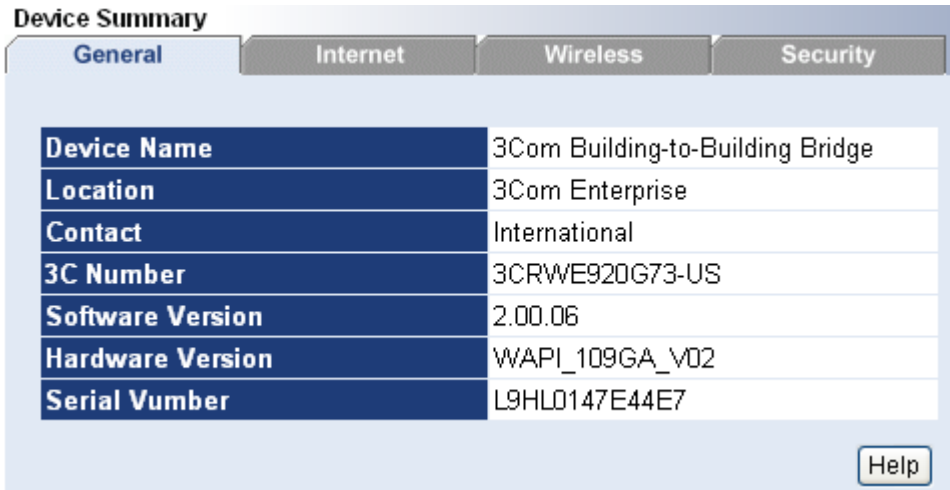
**Figure 8** – Login Page



The login page features a dark blue header with the text "Wireless Bridge Login". Below the header are two input fields: "Username:" and "Password:". At the bottom of the form are two buttons: "Login" and "Cancel".

Enter the administrator name and password, and then press the **Login** button. The Web Manager User interface **Device Summary** will be displayed as follows:

**Figure 9** – Device Summary



The Device Summary page has a tabbed interface with four tabs: "General", "Internet", "Wireless", and "Security". The "General" tab is active. Below the tabs is a table with the following data:

<b>Device Name</b>	3Com Building-to-Building Bridge
<b>Location</b>	3Com Enterprise
<b>Contact</b>	International
<b>3C Number</b>	3CRWE920G73-US
<b>Software Version</b>	2.00.06
<b>Hardware Version</b>	WAPI_109GA_V02
<b>Serial Number</b>	L9HLD147E44E7

A "Help" button is located in the bottom right corner of the page.

## Setup Wizard

To easily configure your bridge step-by-step, click the **Setup Wizard** in the top menu bar. In this wizard you are able to configure these settings:

- ◆ Specify the SSID;
- ◆ Select the radio channel;
- ◆ Choose the security (None, WEP Security, TKIP PSK or AES PSK);

## Wireless Setup

You can now enter the SSID and choose the radio channel:

**Figure 10 – Wireless Settings**

**Setup Wizard Step 1 of 3 - Wireless Setup**

In this Wireless Settings page of Setup Wizard, you can configure the network name and radio channel of your device.

Wireless Network Name (SSID)

Radio Channel

**Wireless Network name (SSID)** – specify the unique name for your wireless bridge.

**Radio Channel** – select the channel that the bridge will use to transmit and receive information.

**Back** – click return to the previous wizard page.

**Next** – click to continue the bridge setup process.

**Cancel** – click to cancel the bridge setup process.

To continue the setup wizard click **Next** button.



## Security Setup

Choose the security method to protect your bridge connection. You can select WEP, WPA-PSK (TKIP), WPA-PSK (AES) or No security for your device.

If no security is needed, simply choose the **None** radio button:

**Figure 11** – Security Settings

**Setup Wizard Step 2 of 3 - Security Setup**

Select the following security technology of your wireless network. Please be aware that when using TKIP or AES as security on WDS links, the SSIDs of both bridges should be identical.

None

Use WEP security

Key length: 64-bits

Key format: Hex

Pre-shared Key

key 1

key 2

key 3

key 4

WPA-PSK(TKIP)

Phrase

WPA-PSK(AES)

Phrase

Help < Back Next > Cancel

**Back** – return to the previous wizard page.

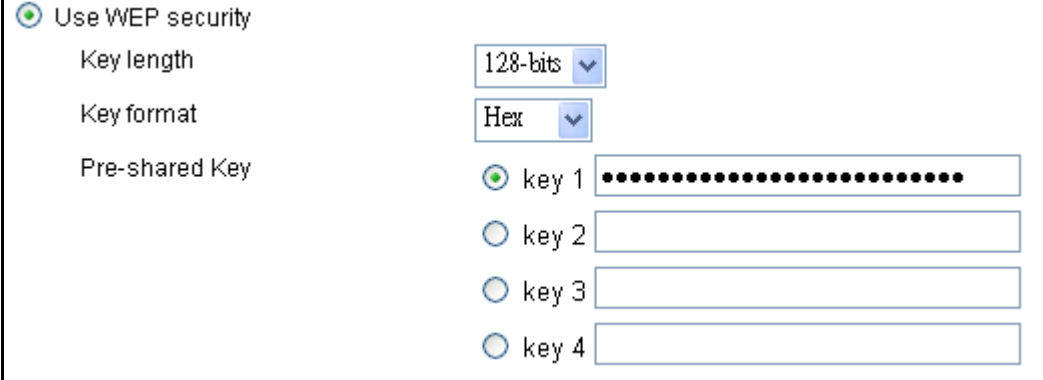
**Next** – continue the bridge setup process.

**Cancel** – cancel the bridge setup process.

## WEP -

To choose WEP encryption, select the **Wired Equivalent Privacy (WEP)** radio button. You can now choose key length and other Security.

**Figure 12 – WEP Encryption Settings**



The screenshot shows the WEP Encryption Settings configuration page. At the top, the 'Use WEP security' radio button is selected. Below it, there are three main settings: 'Key length' is set to '128-bits', 'Key format' is set to 'Hex', and 'Pre-shared Key' is set to 'key 1'. The 'key 1' field contains a series of 26 black dots representing a masked key. Below 'key 1' are three other radio buttons labeled 'key 2', 'key 3', and 'key 4', each with an empty text input field.

**Key Length** – choose the shared Key length from the drop-down menu [64-bits (10 characters)/128-bits (26 characters)].

**Key Format** –choose the Key Format from the drop-down menu [Hex/ ASCII].

**Pre-Shared Key** – specify the shared secret. 5 colon-separated HEX (0-9, A-F, and a-f) pairs (e.g. 00:AC:01:35:FF) for the 64-bits WEP encryption; 13 colon-separated HEX (0-9 A-F, and a-f) pairs (e.g. 00:11:22:33:44:55:66:77:88:99:AA:BB:CC) for the 128-bits WEP encryption.

To continue the setup wizard click the **Next** button and the Confirm Settings page will appear.

## WPA-PSK (TKIP) -

If you want to choose TKIP-PSK encryption, select the **WPA-PSK (TKIP)** radio button in the **Security Setup** page and click the **Next** button to configure the TKIP PSK Phrase.

**Figure 13 – WPA-PSK (TKIP) Settings**




The screenshot shows the WPA-PSK (TKIP) Settings configuration page. The 'WPA-PSK(TKIP)' radio button is selected. Below it, there is a 'Phrase' label and a text input field containing a series of black dots representing a masked password.

**Phrase** – specify WPA-PSK (TKIP) password [8-63 characters] (e.g. aabbccdd).

## WPA-PSK (AES) -

If you want to choose AES-PSK encryption, select the **WPA-PSK (AES)** radio button in the **Security Setup** page and click the **Next** button to configure the AES PSK Phrase.

**Figure 14 – WPA-PSK (AES) Settings**



The screenshot shows the WPA-PSK (AES) Settings configuration page. The 'WPA-PSK(AES)' radio button is selected. Below it, there is a 'Phrase' label and a text input field containing a series of black dots representing a masked password.

**Phrase** – specify WPA-PSK (AES) password [8-63 characters] (e.g. aabbccdd).

## WDS Links Setup

Figure 15 – WDS Links Settings

**Setup Wizard Step 3 of 3 - WDS Links Setup**

Select the following ones that will be used for the peer bridge of your wireless network. It is strongly recommended to select the ones with the same channel as this Wireless Bridge to set up WDS bridge link; Otherwise the WDS bridge link can not work.

Enable	Peer address	Name	SSID	Data Rates	RSSI
<input checked="" type="checkbox"/>	00:0A:5E:45:E1:B9	-	ones	802.11g	-98
<input checked="" type="checkbox"/>	00:0A:5E:45:E1:BA	-	danny	802.11g	-98

2 peer bridges found in all.

Help < Back Next > Cancel

Select the bridges whose channel is the same as your bridge, and then click **Next** button.

**Back** – return to the previous wizard page.

**Next** – continue the bridge setup process.

**Cancel** – cancel the bridge setup process.

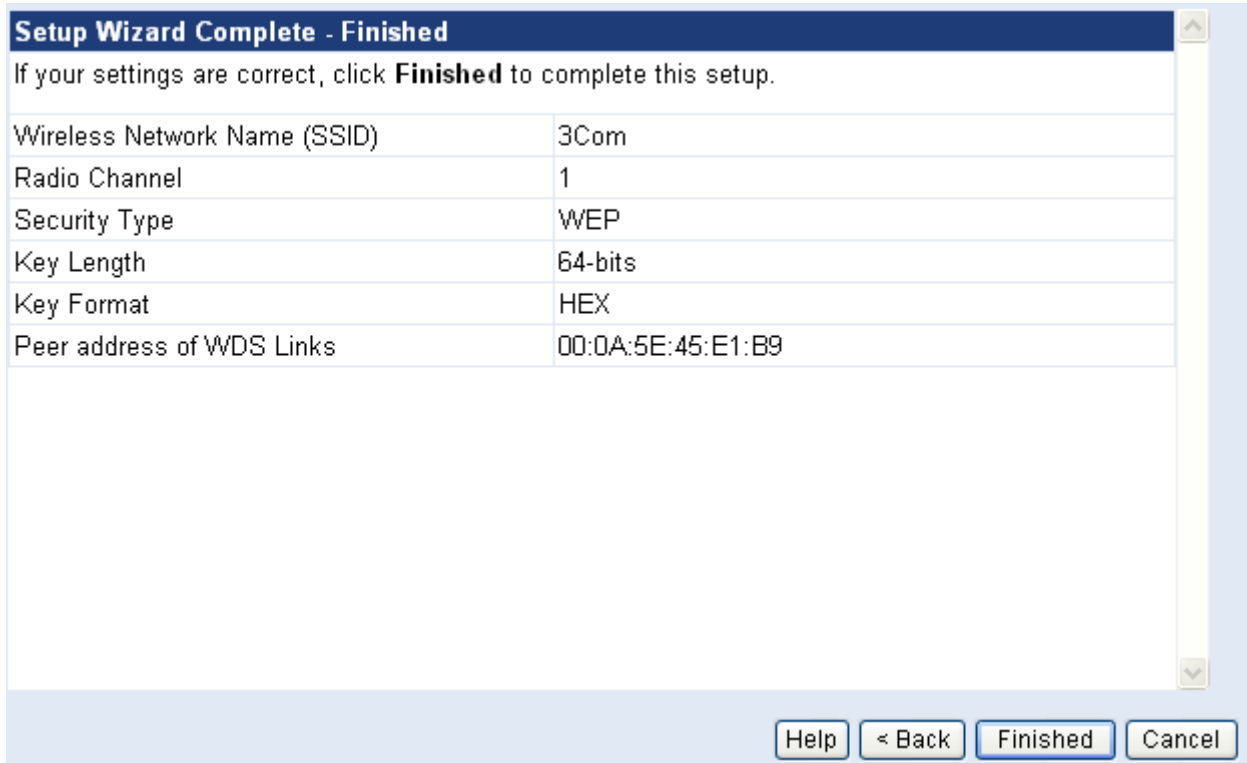


**NOTE:** All WDS links use the same security settings.

## Setup Finished

After all configurations are completed, click the **Finish** button to complete the Setup Wizard.

**Figure 16** – Confirm Settings



**Setup Wizard Complete - Finished**

If your settings are correct, click **Finished** to complete this setup.

Wireless Network Name (SSID)	3Com
Radio Channel	1
Security Type	WEP
Key Length	64-bits
Key Format	HEX
Peer address of WDS Links	00:0A:5E:45:E1:B9

Help < Back Finished Cancel

This Page shows the settings summary of Setup Wizard configuration.

**Back** – return to the previous wizard page.

**Finished** – to complete the setup wizard.

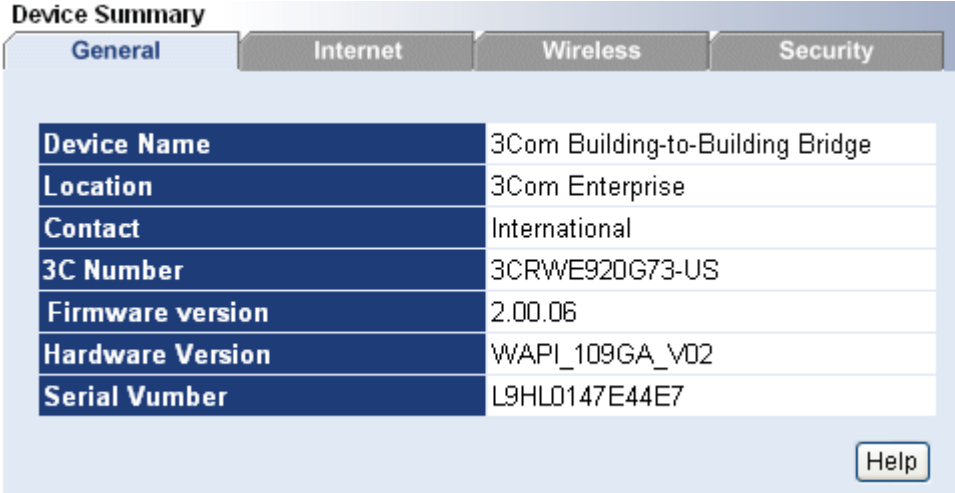
**Cancel** – cancel the bridge setup process.

## Device Summary

### General

The General data for the bridge is displayed here. This page has the device information of the bridge, which is shown in the picture below.

**Figure 17 – General Information**



The screenshot shows a web interface titled "Device Summary" with four tabs: "General", "Internet", "Wireless", and "Security". The "General" tab is active and displays a table of device information. A "Help" button is located in the bottom right corner of the tab area.

Field	Value
Device Name	3Com Building-to-Building Bridge
Location	3Com Enterprise
Contact	International
3C Number	3CRWE920G73-US
Firmware version	2.00.06
Hardware Version	WAPI_109GA_V02
Serial Number	L9HLD147E44E7

**Device Name** – specify new name value used for user authentication in the system [1-60 characters].

**Location Password** – specify new password value used for user authentication in the system [1-60 characters].

**Contact** – specify the name of the person/company responsible for the wireless bridge [1- 60 characters].

**3C number** – 3C number of this bridge. It cannot be changed.

**Firmware version** – The version of current firmware.

**Hardware Version** – displays the version number of the software/firmware that controls the bridge (this will be necessary for troubleshooting).

**Serial Number** – The serial number of this bridge.

## Internet

This page shows all the current Internet setting information of this bridge. From the shown information, you can see which static IP or DHCP Server this bridge is using and other detailed information.

**Figure 18** – Internet Information

Device Summary

General	Internet	Wireless	Security
<b>LAN IP address</b>	192.168.123.13		
<b>LAN Subnet Mask</b>	255.255.255.0		
<b>LAN Default Gateway</b>	192.168.1.254		
<b>DHCP Server</b>	Disable		
<b>DHCP Range</b>	192.168.1.1 - 192.168.1.253		
<b>Lease Time</b>	18000		
<b>Verify Address</b>	Enable		
<b>LAN MAC Address</b>	00:90:4B:7E:48:24		

Help

**LAN IP Address** – Display IP address of this bridge.

**LAN Subnet Mask** – Show subnet mask of the IP address.

**LAN Default Gateway** – Show the gateway IP address of this bridge.

**DHCP Server** – Show if the DHCP server is enabled.

**DHCP Range** – Show the IP address range in the DHCP Server IP pool

**Lease Time** – Show the period over which a network address is allocated to a DHCP client.

**Verify Address** – Probes the network for conflicting IP addresses before giving a suggested IP address to the requesting DHCP client.

**LAN MAC Address** – Shows the MAC Address of this bridge.

## Wireless

The Wireless tab shows the wireless configuration information.

**Figure 19 – Wireless Information**  
**Device Summary**

General	Internet	Wireless	Security
<b>Country</b>	US		
<b>Wireless network name (SSID)</b>	3Com		
<b>Radio Channel</b>	1		
<b>Broadcast SSID</b>	Disable		
<b>Wireless Output Power</b>	12 dBm		
<b>Basic Rate Set</b>	1Mbps, 2Mbps, 5.5Mbps, 11Mbps, 6Mbps, 9Mbps, 12Mbps, 18Mbps, 24Mbps, 36Mbps, 48Mbps, 54Mbps		
<b>Beacon Interval</b>	100		
<b>RTS Threshold</b>	2347		
<b>Fragmentation Threshold</b>	2346		
<b>Preamble Settings</b>	Mixed		
<b>Acknowledgement Delay</b>	0 - 1 Mile (0 - 1.7 Kilometers)		

[Help](#)

**Country** – Shows that this bridge is set for the standards of the chosen country. *This item is read only.*

**Wireless network name (SSID)** – is a unique name for your wireless network [1-32 symbols]. The default SSID is “3Com” but you should change this to a personal wireless network name. The SSID is important to identify bridge to bridge connections when choosing TKIP PSK or AES PSK as the security type. All client bridges must have their client SSID settings configured and must use the same SSID in the same channel.

**Radio Channel** – select the channel that the bridge uses to transmit and receive information. Multiple frequency channels are used to avoid interference between nearby bridges/devices. If you wish to operate more than one bridge in overlapping coverage areas, we recommend a distance of at least four channels between the chosen channels. For example, for three bridges in close proximity choose channels 1, 6 and 11.

**Broadcast SSID** – when selected, your bridge’s SSID is visible in the networks list while scanning the available networks for wireless client. When unselected, the bridge’s SSID is not visible in the available network list.

**Wireless Output Power** – Shows the Maximum output power of this bridge in this domain, read only.

**Basic Rate Set (Mbps)** – select the checkbox to set the Basic data rates at which the station may transmit and receive data.

**Beacon Period (milliseconds)** – this setting specifies the amount of time between beacons in milliseconds. A beacon is a packet broadcast by the bridge to synchronize the wireless network.

**RTS Threshold (bytes)** – specifies the maximum packet size beyond which the Wireless LAN Card invokes its RTS/CTS mechanism. Packets that exceed the

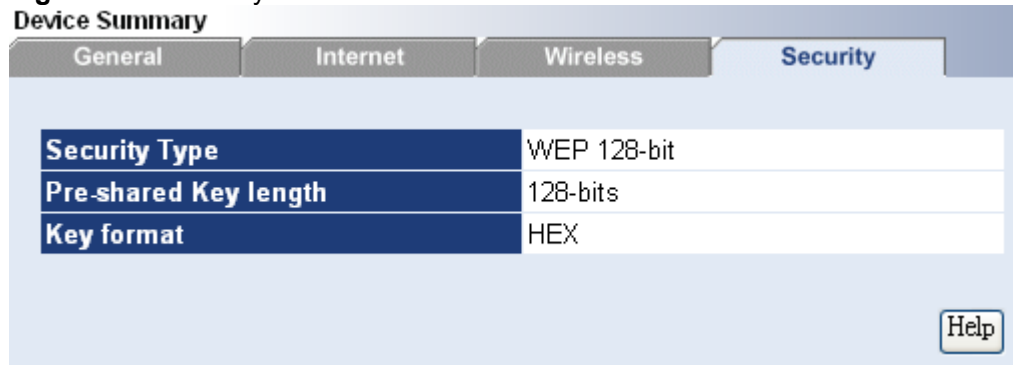
specified RTS threshold trigger the RTS/CTS mechanism. The NIC transmits packets smaller than this threshold without using RTS/CTS [[0-2347] default: 2347 (2347 means that RTS is disabled)].

**Fragmentation Threshold (bytes)** – the fragmentation threshold, specified in bytes, determines whether packets will be fragmented and at what size. On an 802.11 wireless LAN, packets exceeding the fragmentation threshold are fragmented, i.e., split into, smaller units suitable for the circuit size. Packets smaller than the specified fragmentation threshold value are not fragmented [[256-2346] default: 2346 (2346 means that fragmentation is disabled)].

## Security

Security summary displays the general information about wireless security.

**Figure 20** – Security Information



**Security Type** – Displays which security type this bridge is currently using.

**Pre-shared Key length**– Choose the shared Key length from the drop-down menu [64-bits (10 characters)/128-bits (26 characters)].

**Key Format** –choose the Key Format from the drop-down menu [Hex/ ASCII].

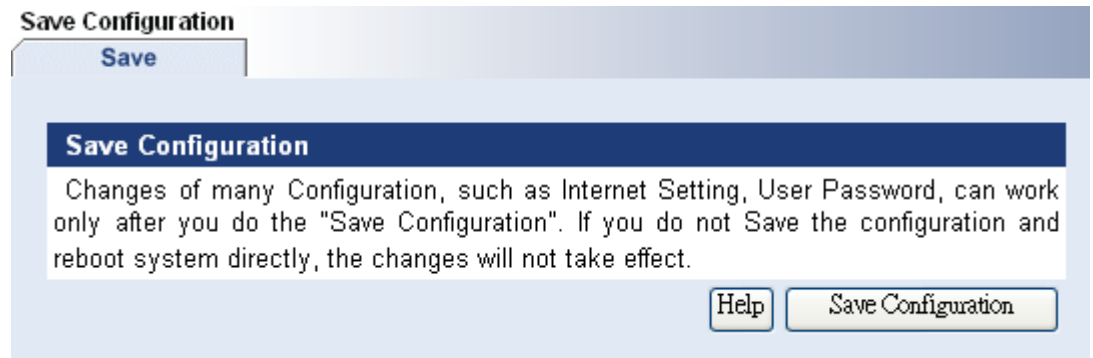


---

## Save Configuration

Save Configuration takes the changes you have made and loads them to the bridge so they are active. If you do not use the **Save Configuration** operation, and direct reboot device. All the changes you have done will be lost and no changes will be applied to the bridge.

**Figure 21** – Save Configuration



## Internet Settings

### IP Setup

The IP Setup Configuration described below is required for device management. IP addresses can either be retrieved from a DHCP server or configured manually.

**Figure 22 – IP Settings**

Internet Settings > IP Setup

IP Setup

**Primary Address Settings**

Dynamic

Static IP

IP Address

Subnet Mask

Default Gateway

Help Apply Cancel

If the **Static IP** radio button is selected, the static IP settings are displayed as follow:

**Figure 23 – Static IP Settings**

Internet Settings > IP Setup

IP Setup

**Primary Address Settings**

Dynamic

Static IP

IP Address

Subnet Mask

Default Gateway

Help Apply Cancel

**IP Address** – specify the bridge's IP address [digit and dots].

**Subnet Mask** – specify the bridge's subnet mask [digit and dots].

**Default Gateway** – specify the IP address of the bridge's gateway [digit and dots].



If you change the IP address manually, make sure that the chosen IP address is free and belongs to the same IP subnet as the wired network; otherwise you will lose the connection to the Wireless Bridge from your current PC. If you enable the DHCP client via a Web browser, the browser will lose the connection after rebooting, because the IP address assigned by the DHCP server is not predictable.

The Wireless Bridge can be set as a DHCP server. Use DHCP configuration to provide dynamic client IP Address from a range of IP Address.

## DHCP Server

If you want to use the internal DHCP server, first go to the **Internet Settings**→**IP Setup** page to set the IP address to **Static**. It is strongly recommended that IP address setting is in the range of the DHCP server.

**Figure 24** – DHCP Server Setup Page

**Internet Settings > DHCP Server**

**Server Setup**   **Reservation**   **DNS Setup**

**DHCP Server Parameters**

DHCP server	<input checked="" type="radio"/> On <input type="radio"/> Off
IP Pool Start Address	<input type="text" value="192.168.1.1"/>
IP Pool End Address	<input type="text" value="192.168.1.253"/>
Lease Time	<input type="text" value="Half hour"/> ▼
Verify Address	<input checked="" type="radio"/> On <input type="radio"/> Off

Click the button **On** to enable the DHCP server.

**IP Pool Start Address** – the first IP address in the range of addresses that you want to assign.

**IP Pool End Address** – the last IP address in the range of addresses that you want to assign.

**Lease Time** – the timeframe in which DHCP client can use the IP address. When lease time is expired, the client must request a DHCP IP address again.

**Verify Address** – probes the network for conflicting IP addresses before giving a suggested IP address to the requesting DHCP client.

## Wireless Settings

### Wireless

The **Wireless Setup** consists of two pages: **Radio** and **Advanced**. Radio part shows the basic settings of radio channel, and Advanced page shows the advanced information. (e.g. Beacon Interval is 100)

**Figure 25** – Wireless Setup → Radio

**Wireless Settings > Wireless Setup**

Radio    Advanced

**Radio Setup**

Country	United States
Regulatory Domain	North America
Wireless network name (SSID)	3Com WLAN
Band	2.4GHz Mixed (Allow both 11b and 11g)
Radio Channel	1
Broadcast SSID	<input type="radio"/> On <input checked="" type="radio"/> Off
Domain Max Output Power	30 dBm
Antenna Gain	3CWE492 2.5dBi
Antenna Cable:	3CWE480 (6ft) 1.5dB
Wireless Output Power	17 dBm
Total Output Power (EIRP)	21 dBm

Help    Apply    Cancel

**Country** – Shows this bridge is set to the regulatory requirements of that country. This item is read only. [North American version of the Bridge only has settings for FCC conformity]

**Regulatory domain** – This is the organization that certifies the Wireless Bridge for use in your country. It determines which radio channels can be used to transmit and receive signals. This is a factory setting and cannot be changed.

**Wireless network name (SSID)** – is a unique name for your wireless network [1-32 characters]. The default SSID is “3Com” you should change this to a personal wireless network name. The SSID is important to identify bridge to bridge connections when choosing TKIP PSK or AES PSK as the security type. All client bridges must have their client SSID settings configured and must use the same SSID in the same channel.

**Radio Channel** – select the channel that the bridge uses to transmit and receive information. Multiple frequency channels are used to avoid interference between nearby bridges/devices. If you wish to operate more than one bridge in overlapping coverage areas, we recommend a distance of at least four channels between the chosen channels. For example, for three bridges in close proximity choose channels 1, 6 and 11.



Before changing radio settings manually, verify that these settings comply with government regulations. At all times, it is the responsibility of the end-user to ensure that the installation complies with local radio regulations. Refer to the appendix, Regulatory Domain section.

**Broadcast SSID** – when selected, your bridge’s SSID is visible in the networks list while scanning the available networks for wireless client. When unselected, the bridge’s SSID is not visible in the available network list.

**Domain Max Output Power** – Shows the maximum output power of this bridge in this domain, read only.

**Cancel** – restore all previous values.

**Apply** – save changed configuration.

**Figure 26** – Wireless Setup → Advanced

Wireless Settings > Wireless Setup

Radio Advanced

**Advanced Setup**

Basic Rate Set	<input checked="" type="checkbox"/> 1Mbps	<input checked="" type="checkbox"/> 2Mbps	<input checked="" type="checkbox"/> 5.5Mbps
	<input checked="" type="checkbox"/> 11Mbps	<input checked="" type="checkbox"/> 6Mbps	<input checked="" type="checkbox"/> 9Mbps
	<input checked="" type="checkbox"/> 12Mbps	<input checked="" type="checkbox"/> 18Mbps	<input checked="" type="checkbox"/> 24Mbps
	<input checked="" type="checkbox"/> 36Mbps	<input checked="" type="checkbox"/> 48Mbps	<input checked="" type="checkbox"/> 54Mbps
	<input checked="" type="checkbox"/> ALL		
Beacon Interval (TUs)	<input type="text" value="100"/>		
RTS Threshold (bytes)	<input type="text" value="2347"/>		
Fragmentation Threshold (bytes)	<input type="text" value="2346"/>		
Preamble Settings	<input type="text" value="Mixed"/>		
Acknowledgement Delay	<input type="text" value="0 - 1 Mile (0 - 1.7 Kilometers)"/>		

Help Apply Cancel

**Basic Rate Set (Mbps)** – select the checkbox to set the Basic data rates at which the station may transmit and receive data.

**Beacon Period (milliseconds)** – this setting specifies the amount of time between beacons in milliseconds. A beacon is a packet broadcast by the bridge to synchronize the wireless network.

**DTIM Period (count)** – this attribute specifies the number of beacon intervals that elapse between transmissions of Beacon frames containing a TIM element whose DTIM Count field is 0. This value is transmitted in the DTIM Period field of Beacon frames.

**RTS Threshold (bytes)** – defines the maximum packet size beyond which the Wireless Bridge invokes its RTS/CTS mechanism. Packets that exceed the specified RTS threshold trigger the RTS/CTS mechanism. The NIC transmits packets smaller than this threshold without using RTS/CTS [[0-2347] default: 2347 (2347 means that RTS is disabled)].

**Fragmentation Threshold (bytes)** – the fragmentation threshold, identifies in bytes, whether packets will be fragmented and at what size. On an 802.11 wireless LAN, packets exceeding the fragmentation threshold are fragmented, i.e., split into, smaller units suitable for the circuit size. Packets smaller than the specified fragmentation threshold value are not fragmented [[256-2346] default: 2346 (2346 means that fragmentation is disabled)].

**Cancel** – restore all previous values.

**Apply** – save changed configuration.

## Security

The **Wireless Security Settings** Page shows the summary of wireless security settings, which includes **Wired Equivalent Privacy (WEP)**, **WPA-PSK (TKIP)** and **WPA-PSK (AES)**. Click each for details.

**Figure 27** – Wireless Security Settings

**Wireless Settings > Security**

**Security**

**Security Setup**

Please be aware that when using TKIP or AES as security on WDS links, the SSIDs of both bridges should be identical

None

Use WEP Security

Key length: 64-bits

Key format: Hex

Pre-shared Key:

key 1

key 2

key 3

key 4

WPA-PSK(TKIP)

Phrase

WPA-PSK(AES)

Phrase

Help Apply Cancel

**Cancel** – restore all previous values.

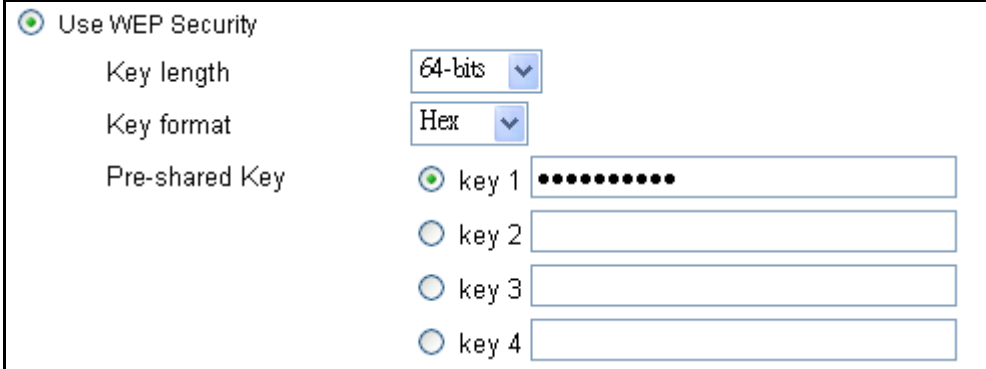
**Apply** – save changed configuration.

## WEP -

WEP is a data privacy mechanism based on a 64-bit or 128-bit shared key algorithm as described in the IEEE 802.11 standard. Static WEP uses a symmetric scheme where the same key and algorithm are used for both encryption and decryption of data.

The radio button **Use WEP Encryption** defines if encryption will be used or not. To enable WEP encryption, select this radio button.

**Figure 28** – Wired Equivalent Privacy (WEP) Settings



The screenshot shows a configuration window for WEP settings. At the top, there is a radio button labeled "Use WEP Security" which is selected. Below this, there are three main settings:

- Key length:** A dropdown menu set to "64-bits".
- Key format:** A dropdown menu set to "Hex".
- Pre-shared Key:** Four radio buttons labeled "key 1", "key 2", "key 3", and "key 4". The "key 1" radio button is selected. To the right of each radio button is a text input field. The "key 1" field contains ten black dots, representing a masked key.

Enter the encryption key to be used to encrypt and decrypt wireless traffic:

**64-bits** – specify pre-shared key as 10 Hex characters or 5 ASCII bytes.

**128-bits** – specify pre-shared key as 26 Hex characters or 13 ASCII bytes.

**Key Format** – choose the Key Format from the drop-down menu [Hex/ ASCII].

**Pre-shared Key** – Setting the WEP key for encrypting data. 64bits and 128bits encryption are supported. This value must be the same as on the host/local and remote bridge(s).

## WPA-PSK (TKIP) -

The Temporal Key Integrity Protocol (TKIP), pronounced “tee-kip”, is part of the IEEE 802.11i encryption standard for wireless LANs. TKIP is the next generation of WEP, the Wired Equivalency Protocol, which is used to secure 802.11 wireless LANs. TKIP provides per-packet key mixing, a message integrity check and a re-keying mechanism, thus fixing the flaws of WEP.

**Figure 29** – WPA-PSK (TKIP) Settings



The screenshot shows a configuration window for WPA-PSK (TKIP) settings. At the top, there is a radio button labeled "WPA-PSK(TKIP)" which is selected. Below this, there is a single setting:

- Phrase:** A text input field containing ten black dots, representing a masked pre-shared key.

**Phrase** – Setting the WPA-PSK (TKIP) key for encrypting data. 8 to 63 characters support. This value must be the same as the one on remote bridge.

## WPA-PSK (AES) -

*Advanced Encryption Standard*, a symmetric 128-bit block data encryption technique. AES works at multiple network layers simultaneously.

**Figure 30 – WPA-PSK (AES) Settings**



The image shows a user interface for configuring WPA-PSK (AES) settings. It features a radio button with a green dot, indicating it is selected, next to the text "WPA-PSK(AES)". Below this, the word "Phrase" is displayed to the left of a text input field. The input field contains a series of black dots, representing a masked password.

**Phrase** – Setting the WPA-PSK (AES) key for encrypting data. 8 to 63 characters support. This value must be the same as the one on remote bridge.

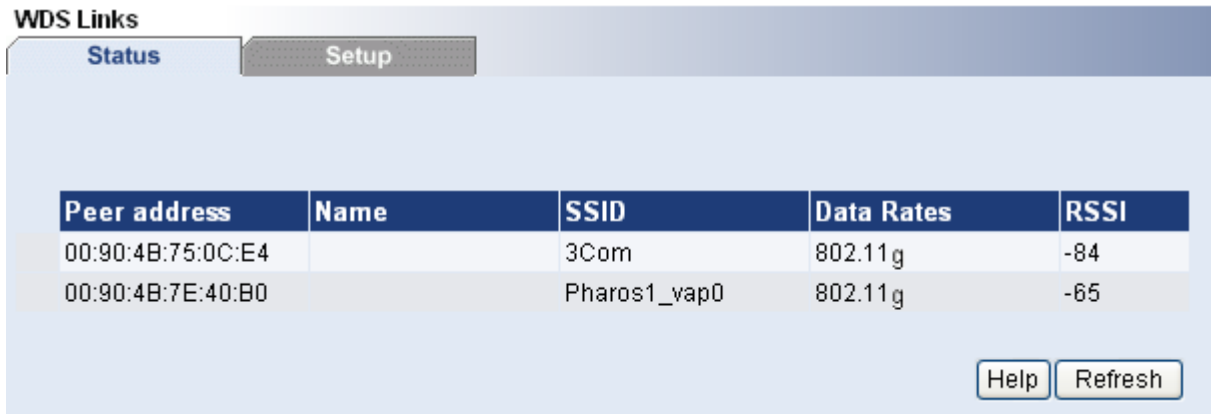


## WDS links

The Wireless Bridge supports WDS (Wireless Distribution System) to act as bridges or repeaters. Choose the **WDS Links** menu if you want to setup bridge links between different bridges.

The figure below shows all the bridges status:

**Figure 31** – WDS Links Status Table



Peer address	Name	SSID	Data Rates	RSSI
00:90:4B:75:0C:E4		3Com	802.11g	-84
00:90:4B:7E:40:B0		Pharos1_vap0	802.11g	-65

**Peer address** – displays the MAC address of the bridge.

**Name** – specify the name of chosen WDS Link.

**SSID** – is a unique name for your wireless network [1-32 characters]. The default SSID is “3Com” you should change this to a personal wireless network name. The SSID is important to identify bridge to bridge connections when choosing TKIP PSK or AES PSK as the security type. All client bridges must have their client SSID settings configured and must use the same SSID in the same channel.

**Data Rates** – displays the data rates that the bridge transmits data.

**RSSI** – displays indicator for the signal strength of the link between the remote and local bridges.

**Cancel** –restore all previous values.

**Apply** – save changed configuration.

The WDS mode is configured by selecting the WDS link peer bridges MAC address in each other’s bridge configuration e.g. Web interface. The **radio channel** and the **operational rates** in all WDS link peer bridges **must be the same**.



Bridges participating in a WDS network DO NOT have to be configured with the same SSID.

On the Wireless Bridge you can add desired bridges in to WDS (wireless distribution system) in two ways: by selecting bridges from the table or you can add them manually.

### Add bridge in WDS from the WDS Links table:

- ◆ Access the WDS Links Table by clicking on the **WDS Links** menu. This table shows information for wireless networks in a local geographic area. On this table an administrator can see WDS Links, their operating channels, data rates, RSSI and the Age.
- ◆ Select the checkbox on the **Enabled** column on chosen WDS link’s row to add this device in the Wireless Distribution System. The checkboxes will be active only of those WDS links that use the same channel as your device:

**Figure 32 – WDS Links Status Table**

**WDS Links**

Status Setup

Select the following ones that will be used for the peer bridge of your wireless network. It is strongly recommended to select the ones with the same channel as this Wireless Bridge to set up WDS bridge link; Otherwise the WDS bridge link can not work.

Enable	Peer address	Name	SSID	Data Rates	RSSI
<input checked="" type="checkbox"/>	00:90:4B:7E:42:00		default_ssid_yap0	802.11g	-60
<input checked="" type="checkbox"/>	00:90:4B:7E:42:01		default_ssid_yap1	802.11g	-63
<input checked="" type="checkbox"/>	00:90:4D:7E:42:40		3Com wlan2-1-v1	802.11g	-58
<input type="checkbox"/>	00:90:4D:7E:42:41		wlan2-2-wep641-2-v1	802.11g	-58
<input type="checkbox"/>	00:90:4D:7E:42:42		wlan2-3-wep642-1	802.11g	-58
<input type="checkbox"/>	00:90:4D:7E:42:43		wlan2-4-wep128-3	802.11g	-58
<input type="checkbox"/>	00:90:4D:7E:42:44		wlan2-5-wep1284-1	802.11g	-58
<input type="checkbox"/>	00:90:4D:7E:42:45		wlan2-6-psk-1	802.11g	-57
<input type="checkbox"/>	00:90:4D:7E:42:47		wlan2-8-aes-3	802.11g	-57
<input type="checkbox"/>	00:90:4D:7E:42:48		wlan2-9	802.11g	-56
<input type="checkbox"/>	00:90:4B:75:0C:E4		3Com	802.11g	-83
<input type="checkbox"/>	00:90:4D:7E:42:46		wlan2-7-aes-1	802.11g	-57

Help Refresh Apply Cancel

**Enable** – select to add the Wireless Bridges to Wireless Distribution System.

**Peer address** – displays the MAC address of the bridge.

**Name** – specify the name of chosen WDS Link.

**SSID** – displays the SSID of the bridge.

**Data Rates** – displays the data rates that the bridge transmits data.

**RSSI** – displays indicator for the signal strength of the link between the remote and local bridges.



**Note:** usually 0 ~ -40 are perfect, the worst is around -90. The value of RSSI changes depends on different antenna and environments.

**Cancel** – restore all previous values.

**Apply** – save changed configuration.



**Note:** All WDS links use the same security settings.

### Add Bridge in WDS manually:

When a WDS bridge is not shown in the WDS table automatically you can add it manually by entering the MAC address of the remote Bridge. And then click on the **Add WDS Links** button.

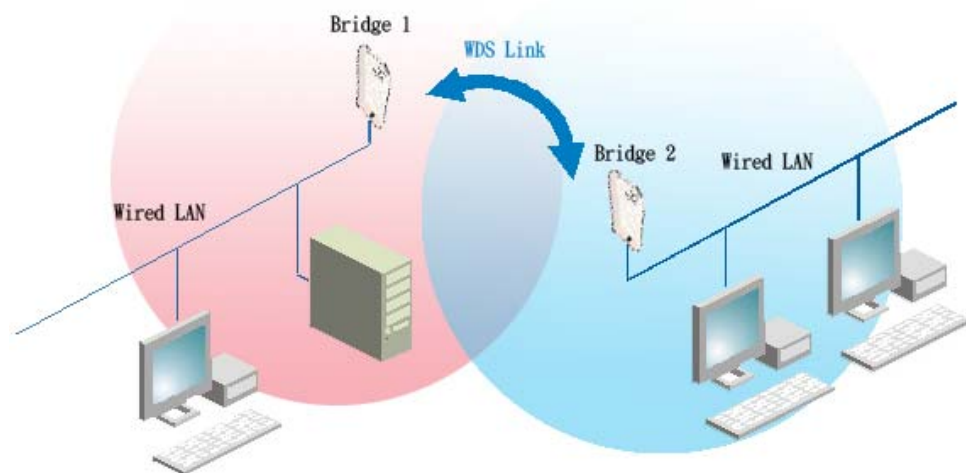
Follow the example to see how to configure a WDS.

### Case 1 – Bridge with WDS (Wireless Bridge)

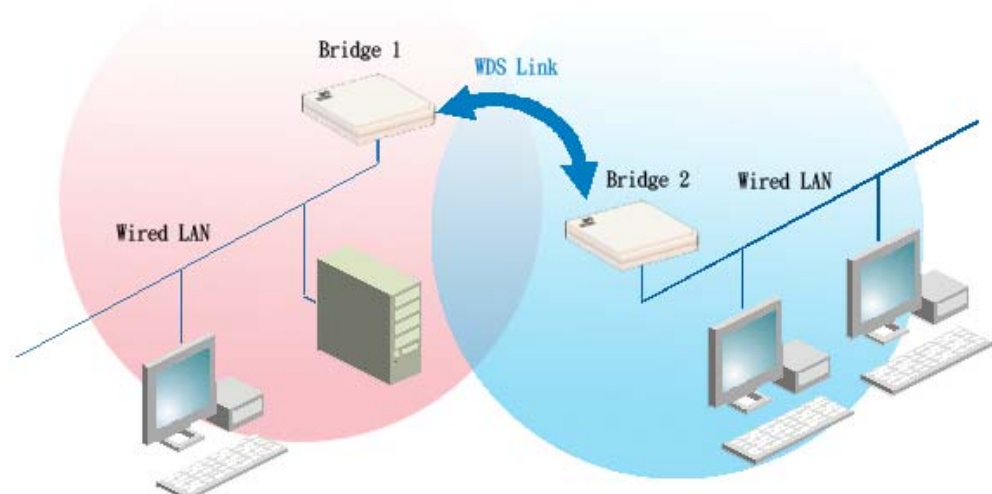
Create the Wireless Bridge between two wired networks: BRIDGE1 can be configured to forward all data to BRIDGE2.

BRIDGE1 and BRIDGE2 need to be changed to Bridge1 and Bridge2. Illustration figures need to be changed to reflect this as well.

#### Indoor:



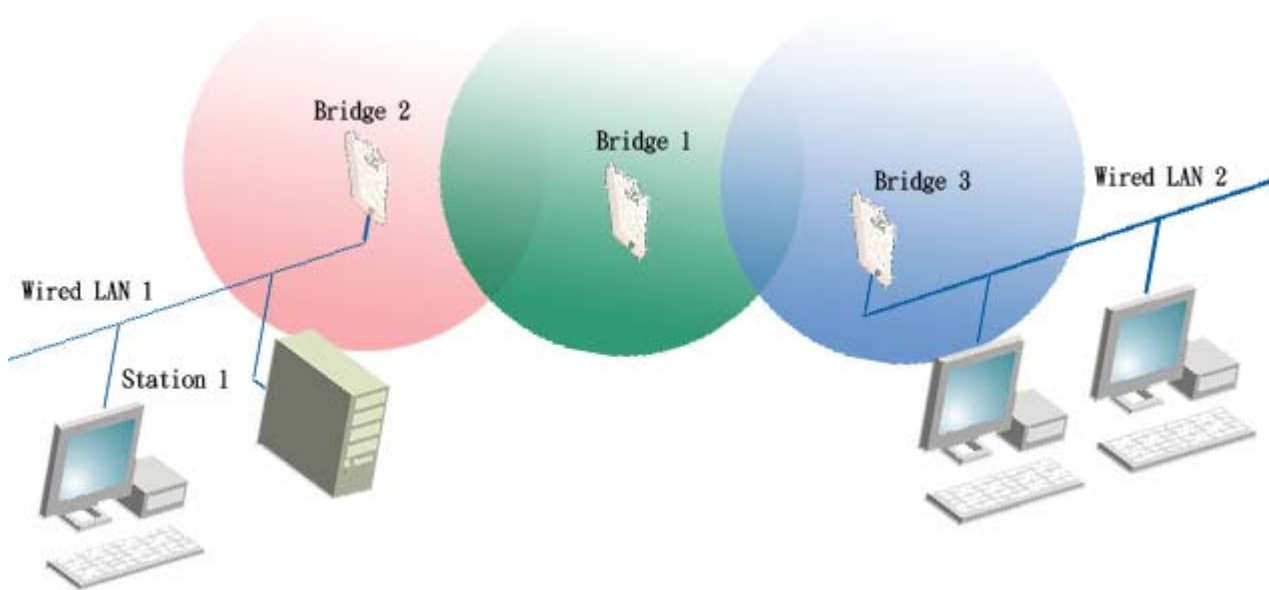
#### Outdoor:



- Choose the wireless MAC address of **Bridge2** in the web configuration interface of **Bridge1**, menu **WDS Links**.
- Choose the wireless MAC address of **Bridge1** in the web configuration interface of **Bridge2**, menu **WDS Links**.
- Select the same radio channel and the data rates for both Bridges using the **Radio** page under the **Wireless Settings > Wireless Setup**.

## Case 2 – Bridge with WDS (Wireless Repeater)

This example shows a configuration where one bridge relays all traffic wirelessly from one bridge to another bridge. In the picture below Station1 is connected to the wired LAN2 via Bridge2. Bridge1 act as a repeater between Bridge2 and Bridge3.



- Choose the **Wireless MAC** address **Bridge2** and **Bridge3** in the **Bridge1** Web interface **WDS Links** menu under the **Configuration**.
- Choose the **Wireless MAC** address **Bridge1** in the **Bridge2** web interface **WDS Links** menu under the **Configuration**.
- Choose the **Wireless MAC** address **Bridge1** in the **Bridge3** Web interface **WDS Links** menu under the **Configuration**.
- Select the **same radio channel** for the three Bridges using the **Radio** page under the **Wireless Settings > Wireless Setup**.

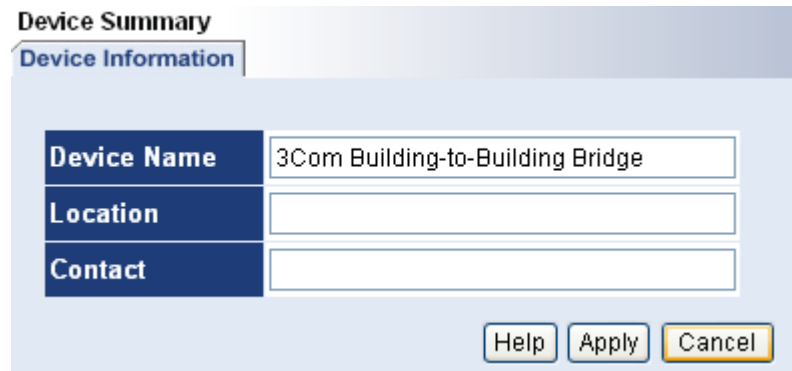
---

## Device Management

### Device Information

You can use the **Device Information** to identify the bridge for yourself and other information of these devices which is shown in the picture below.

Figure 33 – The device information of this bridge.



The screenshot shows a web interface for configuring a bridge. At the top, there is a 'Device Summary' section with a sub-tab for 'Device Information'. Below this, there are three input fields: 'Device Name' (containing '3Com Building-to-Building Bridge'), 'Location', and 'Contact'. At the bottom right of the form are three buttons: 'Help', 'Apply', and 'Cancel'.

Field	Value
Device Name	3Com Building-to-Building Bridge
Location	
Contact	

**Device Name** – specify new name value used for user authentication in the system [1-60 characters].

**Location Password** – specify new password value used for user authentication in the system [1-60 characters].

**Contact** – specify the name of the person/company responsible for the wireless bridge [1- 60 characters].

**Confirm Password** – re-enter the new password to verify its accuracy.

**Apply**– Apply administrator’s password.

## System Access

Use the **Systems Access** menu to change the name and password of the Administrator and User for any further configuration changes.

**Figure 34** – Change Administrator’s Name and Password

Device management > System Access

Administrator User

**Change Administrator's Name and Password**

You can change the password to prevent unauthorized access to the Administration System. New password is 3-16 characters.

Username	admin
New Password	3combridge
Confirm New Password	3combridge

Help Apply Cancel

**Name** – specify new name value used for user authentication in the system [3-16 characters].

**New Password** – specify new password value used for user authentication in the system [3-16 characters].

**Confirm Password** – re-enter the new password to verify its accuracy.

**Apply**– Apply administrator’s password.

**Figure 35 – Change User's Name and Password**

Device management > System Access

Administrator User

### Change User's Name and Password

You can change the password to prevent unauthorized access to the User System.  
New password is 3-16 characters.

Username	<input type="text" value="user"/>
New Password	<input type="text" value="3comwireless"/>
Confirm New Password	<input type="text" value="3comwireless"/>

Help Apply Cancel

**Name** – specify new name value used for user authentication in the system [3-16 characters].

**New Password** – specify new password value used for user authentication in the system [3-16 characters].

**Confirm Password** – re-enter the new password to verify its accuracy.

**Apply**– Apply administrator's password.



Keep in mind that the Reset button will set the username and password back to default.

## STP

Set STP (Spanning Tree Protocol) parameters. Click the radio box button **On** to enable or button **OFF** to disable the STP function.

If **ON** Status is enabled, you will then need setup the **Forward Delay**, **Hello Time**, **Max Age** and **Priority** for this device.

**Figure 36** – STP settings Page

Device Management > STP

STP

STP Setup	
STP Status	<input checked="" type="radio"/> On <input type="radio"/> Off
Forward Delay (seconds)	<input type="text" value="15"/>
Hello Time (seconds)	<input type="text" value="2"/>
MAX Age (seconds)	<input type="text" value="20"/>
Priority	<input type="text" value="0"/>

Help Apply Cancel

**Forward Delay** – is the time intervals (in seconds) in which all devices transmit a configuration message when this device becomes the root.

**Hello Time** –is the time interval (in seconds) in which this device transmits a configuration message.

**Max Age** –is the maximum time (in seconds) this device can wait without receiving a configuration message before attempting to reconfigure.

**Priority** –is the priority of this device. It is a part of the bridge ID, which equal to Priority (2 bytes) plus bridge MAC address (6 bytes).



## Time

Displays the time setting of the Wireless Bridge. If this feature is not necessary, check the **None** radio box button. The Figure below shows Setting Time Manually Information:

**Figure 37 – Set Time Manually**

Device Management > Time

Time

**Time Setup**

None

Setting Time manually

System Time

NTP

System Time Zone

Server Address

**None** – deny setting Wireless Bridge time manually.

**Setting Time manually** – enable setting Wireless Bridge time manually. The format of the setting time is year/month/day hour:minute:second, such as 2000/01/01 20:01:30.

**Get Local Time** – Click button Get Local Time, the time of the PC which the web client is running in can be pulled into input box automatically.

**Figure 38 – Set Time Automatically**

Device Management > Time

Time

**Time Setup**

None

Setting Time manually

System Time

NTP

System Time Zone

Server Address

**None** – deny setting Wireless Bridge time manually.

**System Time Zone** – Specify the Time Zone the place you are in.

**NTP Server IP** – Specify the IP Address of the remote NTP (Network Time Protocol) Server.

# SNMP

SNMP is another way to manage the Wireless Bridge. In particular it provides the ability to send trap messages with notifications or alarms to a management system. You can configure the SNMP agent in Wireless Bridge to send SNMP traps to one or more SNMP managers. We provide two versions SNMP Management way, SNMP V1 and SNMP V3. SNMP V3 is more security than V1.

**Figure 39 – SNMP Settings**

Device Management > SNMP

SNMP Trap

**Enable/Disable SNMP**

SNMP  Enable  Disable

Help Apply Cancel

Please enter the SNMP V1 parameters in the following table.

Access Property	Community String
Read Only Community String	public
Read Write Community String	private

Help Apply Cancel

Please enter the SNMP V3 parameters in the following table.

Access Property	User Name	Password
Read-Only User	user	.....
Read-Write User	admin	.....

Help Apply Cancel

**SNMP V1 PARAMETERS:**

**Read-only Community** is a community string used to access the device by SNMP with only 'get' operation.

**Read/Write Community** is a community string used to access the bridge by SNMP with 'get' and 'set' operations.

**SNMP V3 PARAMETERS:**

In this version, you can assign User Name, password and his right, read-only or read-write.

If you add one host address in this list, the device will send out SNMP Trap information to this host. To add a host into this list, specify the SNMP manager IP address. And then click the **Add** button. To delete a host from the SNMP Trap Host list, select the host IP address that should be deleted, and then click the **Delete** button.

**Figure 40 – SNMP Trap Settings**

Device Management > SNMP

SNMP    Trap

**Add a SNMP Trap Host IP address**


SNMP Trap Host IP address

Help   Apply   Cancel

**Deletea SNMP Trap Host IP Address**

<input type="checkbox"/>	192.168.10.254
--------------------------	----------------

Help   Delete   Cancel



---

## System tools

### Backup/Restore

#### Backup/Restore Configuration via HTTP

**Figure 41**– Backup/Restore configuration via HTTP

The screenshot shows a web interface with three tabs: HTTP, TFTP, and FTP. The HTTP tab is selected. The interface is divided into two main sections: Backup and Restore. The Backup section contains a text box explaining that users can save their current configuration and restore it later, with a recommendation to backup before a firmware update. It includes a 'Help' button and a 'Backup' button. The Restore section contains a text box explaining that users can restore a previously saved configuration by selecting a file and pressing the 'Restore' button. It includes a file selection input field with a 'Browse...' button, a 'Help' button, and a 'Restore' button.

Click the **Browser** button to select a configuration file and then click the **Restore** button to upload it to the device by HTTP protocol. Or click the **backup** button to download the configuration file from device.

## Backup/Restore Configuration via TFTP

Before you backup or restore system configuration via TFTP, you should be sure that the TFTP Server which you assigned is in service first. If it is not, the backup or restore will not be successful and could damage the bridge.

**Figure 42** – Backup/Restore configuration via TFTP

System Tools > Backup/Restore

HTTP TFTP FTP

### TFTP Server Setup

TFTP Server IP Address	<input type="text" value="192.168.1.254"/>
Filename	<input type="text" value="system.conf"/>

Help Apply Cancel

### Backup

You can save your current configuration by using this feature. Saving your configuration will allow you to restore it later if your settings are lost or changed. It is recommended that you backup your current configuration before performing a firmware update.

Help BackUp

### Restore

This option will allow you to restore a previously saved configuration. Please select the configuration file and press the "Restore" button below.

Help Restore

**TFTP Server IP Address** - The TFTP Server's IP Address.

**File Name** - The configure file's name you backup or restore.

**Apply** - Apply the TFTP Server Settings.

**Backup** - Backup system configuration.

**Restore** - Restore system configuration.

## Backup/Restore Configuration via FTP

Before you backup or restore system configuration via FTP, you should be sure that the FTP Server which you assigned is in service first. If it is not, the backup or restore will not be successful and may damage the bridge.

**Figure 43** – Backup/Restore configuration via FTP

The screenshot shows a web-based configuration interface for Backup/Restore via FTP. At the top, there are three tabs: HTTP, TFTP, and FTP, with the FTP tab selected. Below the tabs is a section titled "FTP Server Setup" with four input fields: "FTP Server IP Address" (192.168.1.254), "File Name" (system.conf), "User Name" (3combridge), and "Password" (masked with asterisks). Below these fields are three buttons: "Help", "Apply", and "Cancel".

The next section is titled "Backup" and contains a text block: "You can save your current configuration by using this feature. Saving your configuration will allow you to restore it later if your settings are lost or changed. It is recommended that you backup your current configuration before performing a firmware update." Below this text are two buttons: "Help" and "Backup".

The final section is titled "Restore" and contains a text block: "This option will allow you to restore a previously saved configuration. Please select the configuration file and press the 'Restore' button below." Below this text are two buttons: "Help" and "Restore".

**FTP Server IP Address** - The FTP Server's IP Address.

**File Name** - The configure file's name you backup or restore.

**User Name** - This user point to the ftp server account.

**Password** - User's password.

**Apply** - Apply the FTP Server Settings.

**Backup** - Backup system configuration.

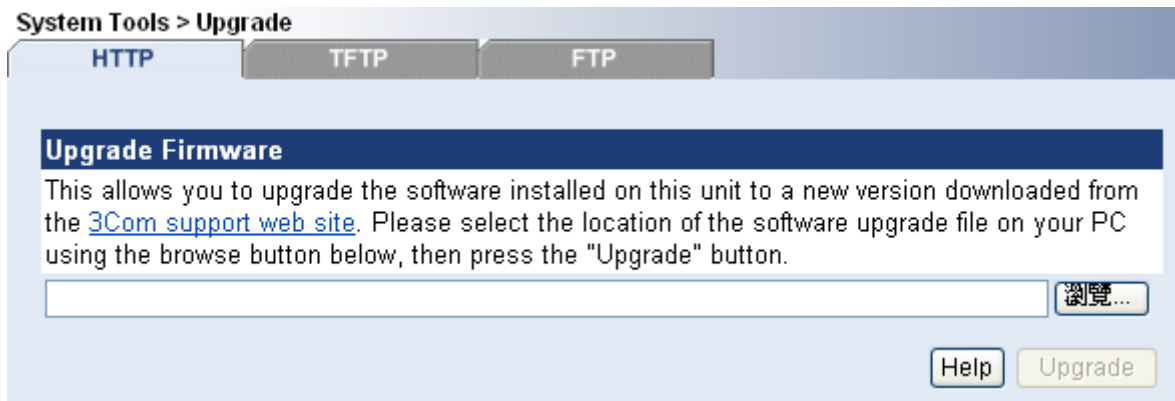
**Restore** - Restore system configuration.

## Upgrade

Attention: To upgrade your bridge firmware, please use the original image 3Com Corporation provided.

### Upgrade Firmware via HTTP

**Figure 44** – Firmware Upgrade via HTTP



Click **Browse** Button and select the firmware file. Then the **Upgrade** button will be active automatically and click it. After you confirm upgrade, Firmware Upgrade will begin and this page will jump to the page shown below which will show the upgrade process.

**Figure 45** – Firmware Upgrade Process



## Upgrade Firmware via TFTP

Before you upgrade firmware image via TFTP, you should be sure that the TFTP Server which you assigned is in service first. If it is not, the upgrade will not be successful and may damage the bridge.

**Figure 46** – Firmware Upgrade via TFTP

The screenshot shows a web-based configuration interface for a device. At the top, there is a breadcrumb trail 'System Tools > Upgrade'. Below this, there are three tabs: 'HTTP', 'TFTP', and 'FTP'. The 'TFTP' tab is currently selected. The main content area is divided into two sections. The first section, titled 'TFTP Server Setup', contains two input fields: 'TFTP Server IP Address' with the value '192.168.1.254' and 'File Name' which is empty. To the right of these fields are three buttons: 'Help', 'Apply', and 'Cancel'. The second section, titled 'Firmware Upgrade', contains a paragraph of text: 'This allows you to upgrade the software installed on this unit to a new version downloaded from the [3Com support web site](#). Please select the location of the software upgrade file on your PC using the browse button below, then press the "Upgrade" button.' Below this text are two buttons: 'Help' and 'Upgrade'.

**TFTP Server IP Address** - The TFTP Server's IP Address.

**File Name** - The configure file's name you backup or restore.

**Apply** - Apply the TFTP Server Settings.

**Upgrade** - Upgrade System software.



## Upgrade Firmware via FTP

Before you upgrade via FTP, you should be sure that the FTP Server which you assigned is in service first. If it is not, the upgrade will not be successful and may damage the bridge.

**Figure 47** – Upgrade Firmware via FTP

System Tools > Upgrade

HTTP TFTP **FTP**

FTP Server Setup	
FTP Server IP Address	192.168.1.254
File Name	system.img
User Name	3comuser
Password	*****

Help Apply Cancel

---

Firmware Upgrade	
This allows you to upgrade the software installed on this unit to a new version downloaded from the <a href="#">3Com support web site</a> . Please select the location of the software upgrade file on your PC using the browse button below, then press the "Upgrade" button.	

Help Upgrade

**FTP Server IP Address** - The FTP Server's IP Address.

**File Name** - The configure file's name you backup or restore.

**User Name** - This user point to the ftp server account.

**Password** - User's password.

**Apply** - Apply the FTP Server Settings.

**Upgrade** - Upgrade Firmware image.

When the upgrade is completed successfully, a confirmation message will appear and the bridge restarts.

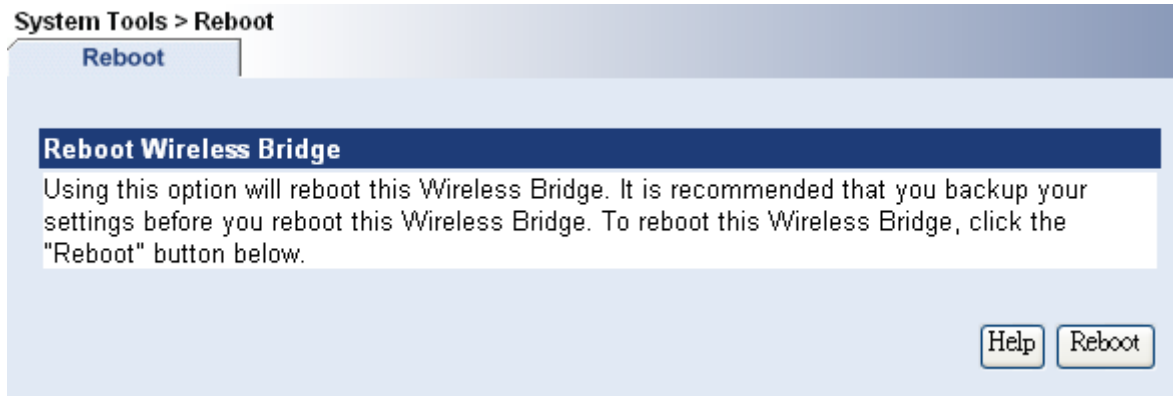


Do not switch off and do not disconnect the Wireless Bridge from the power supply during the firmware upgrade process as this will damage the device.

---

## Reboot

**Figure 48 – Reboot Wireless Bridge**



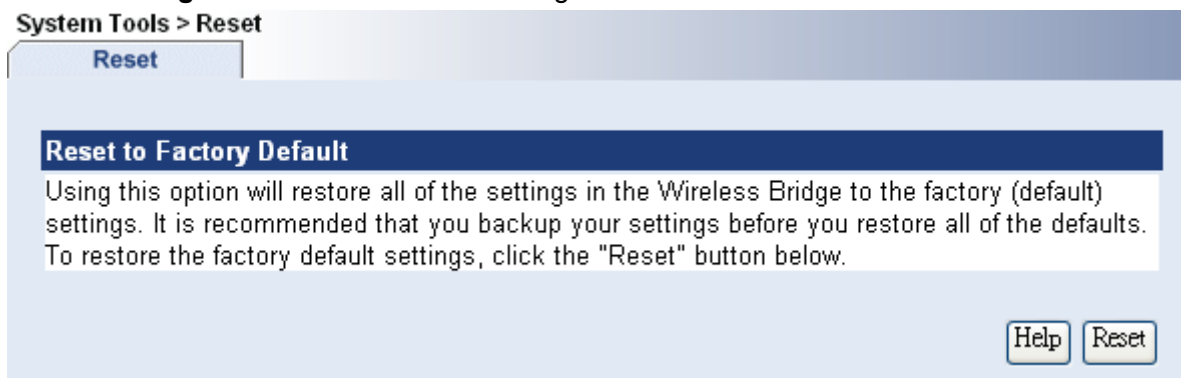
Click **Reboot** button, the device will reboot after you confirm.

Reboot will power down and power up the Bridge. It will not reset any configuration settings.

---

## Reset

**Figure 49 – Reset Wireless Bridge**



Click **Reset** button, the device will reset after you confirm –

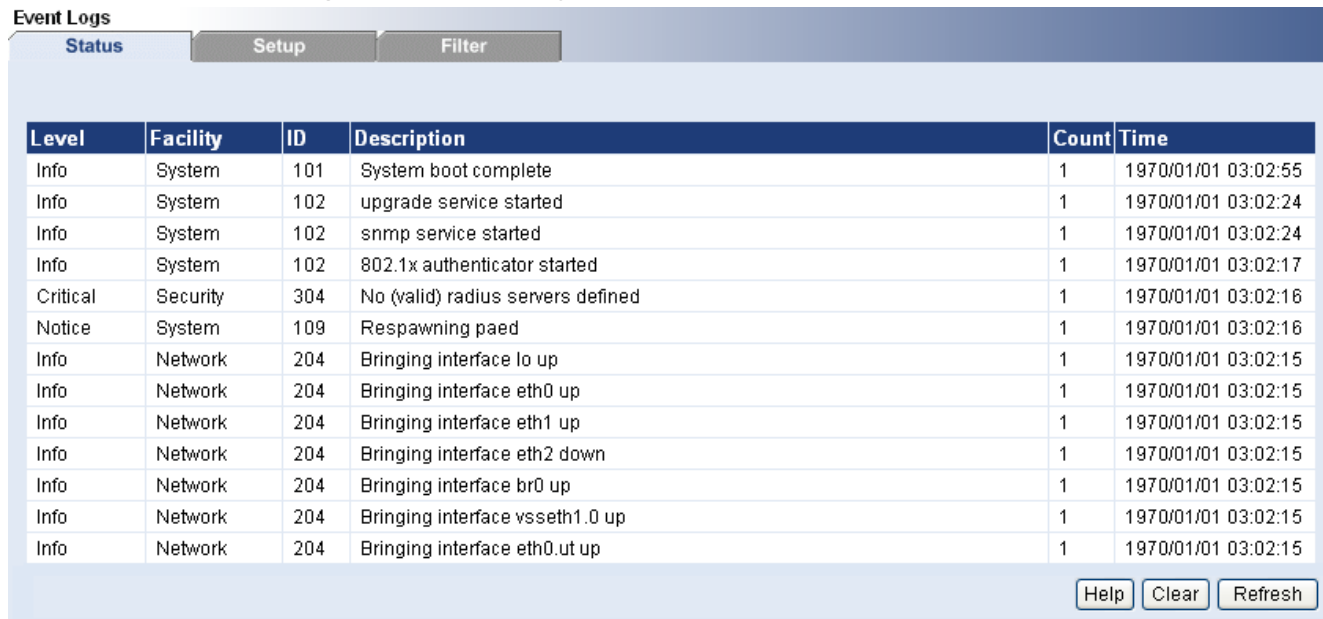
**CAUTION:** All configuration settings will be reset to factory.

## Event Logs

### Event Log Status

The event log system informs about internal services and provides debug messages in case of malfunctions or network problems. The trace system can help operators to locate miss configurations and system errors. Use the Event Log menu to view current Syslog messages in case of troubleshooting of one of the services:

**Figure 50– Event Log Status**



The screenshot shows a web interface for 'Event Logs'. At the top, there are three tabs: 'Status' (selected), 'Setup', and 'Filter'. Below the tabs is a table with the following columns: Level, Facility, ID, Description, Count, and Time. The table contains 14 rows of log entries. At the bottom right of the table area, there are three buttons: 'Help', 'Clear', and 'Refresh'.

Level	Facility	ID	Description	Count	Time
Info	System	101	System boot complete	1	1970/01/01 03:02:55
Info	System	102	upgrade service started	1	1970/01/01 03:02:24
Info	System	102	snmp service started	1	1970/01/01 03:02:24
Info	System	102	802.1x authenticator started	1	1970/01/01 03:02:17
Critical	Security	304	No (valid) radius servers defined	1	1970/01/01 03:02:16
Notice	System	109	Respawning paed	1	1970/01/01 03:02:16
Info	Network	204	Bringing interface lo up	1	1970/01/01 03:02:15
Info	Network	204	Bringing interface eth0 up	1	1970/01/01 03:02:15
Info	Network	204	Bringing interface eth1 up	1	1970/01/01 03:02:15
Info	Network	204	Bringing interface eth2 down	1	1970/01/01 03:02:15
Info	Network	204	Bringing interface br0 up	1	1970/01/01 03:02:15
Info	Network	204	Bringing interface vsseth1.0 up	1	1970/01/01 03:02:15
Info	Network	204	Bringing interface eth0.ut up	1	1970/01/01 03:02:15

**Clear** – delete all displayed logged messages.

**Level** – shows how important the event (or how critical the error) is [Emergency/Alert/Critical/Error/Warning/Notice/Info/Debug].

**Facility** – indicates the unique identifier of the facility that generated the event. A facility can be a hardware device, a protocol, or a module of the system software. [Kernel/User/Security/Clock/LogAudit/LogAlert/System/Network/Wlan/management]

**ID** – indicates an internal number for the event.

**Description** – indicates description of the event.

**Count** – indicates the number of times this event has occurred.

**Time** – indicates time when this event has occurred, in months, days and hours: minutes: seconds since the bridge was started.

## Event Log Setup

This page provides two functions, first one is that you can backup up system logs via TFTP by setting the TFTP Server IP and file name manually. Second one is system logs can be automatically backup to an log server by setting the Remote Log Server.

**Figure 51**– Event Log Setup

The screenshot shows the 'Event Logs' configuration page with the 'Setup' tab selected. It is divided into three main sections:

- TFTP Server Setup:** Includes input fields for 'TFTP Server IP Address' (192.168.1.254) and 'File Name' (log.txt). Buttons for 'Help', 'Apply', and 'Cancel' are located to the right.
- Backup System logs via TFTP:** Contains a text box with the message 'You can save your current configuration by using this feature.' and buttons for 'Help' and 'BackUp'.
- Remote Syslog Server:** Features a 'Syslogs Server' section with radio buttons for 'On' and 'Off' (the 'Off' option is selected). Below it is a 'Syslogs Server IP Address' field containing '192.168.1.254'. Buttons for 'Help', 'Apply', and 'Cancel' are at the bottom right.

**TFTP Server IP Address** - The TFTP Server's IP Address.

**File Name** - The configure file's name you backup or restore.

**Apply** - Apply the TFTP Server Settings.

**Backup** - Backup system logs via TFTP.

**Syslogs Server** - You can active the automatically backup function by enable On button, or inactive it by clicking Off button.

**Syslogs Server IP Address** - Remote Sys-log Server's IP Address.

## Event Log Filter

This page provides two filters, first one can filter logs by **Logs Category**. Second one can filter logs by **Logs level**. You could make the kernel to generate the event logs that you are interested, by selecting the combinations of check boxes in category and level.

**Figure 52**– Event Log Filter

The screenshot shows the 'Event Logs' configuration window with the 'Filter' tab selected. It features two filter sections:

- Logs Category:** A grid of checkboxes with 'kernel' checked. Other categories include user, security, clock, logAudit, logAlert, system, network, wlan, and management.
- Logs Level:** A grid of checkboxes with 'emergency' checked. Other levels include alert, critical, error, warning, notice, information, and debug.

Each section includes 'Help', 'Apply', and 'Cancel' buttons.

**Apply** - Apply the Logs Filter Settings.

## System Status

### Statics

#### Interface Statistics

Use the **Interface Statistics** menu for a summary of interface statistics.

**Figure 53** – Interface Statistics

System Status > Statistics

Interface Wireless

Interface	Status	InOctets	InUcast	InMcast	OutOctets	OutUcast	OutMcast
Local Loopback	up	68971	891	0	68971	891	0
LAN Ethernet	up	111929	943	54	815911	1201	0
Wireless	up	0	0	0	0	0	0

Help Refresh

**Interface** – indicates a unique name for each interface.

**Status** – shows the current operational state of the interface [up/down].

**InOctets** – indicates the amount of received bytes on the interface, including framing characters.

**InUcast** – totals unicast frames received at the port excluding discards.

**InMcast** – totals multicast frames received at the port excluding discards.

**OutOctets** – shows the total transmitted frames of the interface in bytes, including framing characters.

**OutUcast** – totals unicast frames transmitted from the port including discards.

**OutMcast** – totals multicast frames transmitted from the port including discards.

**Refresh** – Refresh local page and all the statistics.

## Wireless Statistics

Use the **Wireless Statistics** menu to view information regarding data traffic for the Wireless interface.

**Figure 54** – Wireless Statistics

System Status > Statistics

Interface	Wireless
Transmitted Fragments	2194
Transmitted Multicasts	0
Transmitted Frame Count	55
Failed Packets	8183
Retry Count	0
Multiple Retry Count	0
Duplicate Frames	0
RTS Success Count	0
RTS Failure Count	0
ACK Failure Count	8183
Received Fragment Count	121158
Received Multicasts	0
FCS Errors	112052
WEP Undecryptable	0

Help Refresh

**Transmitted Fragments** – displays the total of transmitted fragmented frames.

**Transmitted Multicasts** – displays the total of transmitted multicast frames.

**Transmitted Frame Count** – displays count of successfully transmitted MSDU (MAC Service Data Units).

**Failed Packets** – displays the total of not transmitted MSDU.

**Retry Count** – displays the number of successfully transmitted MSDU after one or more retransmissions.

**Multi-Retry Count** – displays the number of successfully transmitted MSDU after more than one retransmission.

**Duplicate Frames** – displays the total of duplicate frames.

**RTS Success Count** – displays the total of successfully received RTS packets.

**RTS Failure Count** – displays total of not received RTS packets.

**ACK Failure Count** – displays total of expected but not received ACK (acknowledgement) frames.

**Rx Fragment Count** – displays total of each successfully received MPDU (MAC Protocol Data Unit) of type Data or Management.

**Rx Multi Casts** – displays the total of MSDU, received with the multicast bit set in the destination MAC address.

**FCS Errors** – displays count of FCS (Frame Check Sequence) errors in received MPDU.

**WEP Undecryptable** – displays the number of not decrypted frames.

**Refresh** – Refresh local page and all the statistics.

## STP

### STP Statics

This page shows the status of STP (Spanning Tree Protocol) function.

**Figure 55** – Spanning Tree Protocol Status

System Status > STP

STP Status	STP Port
STP Status	Off
STP Version	IEEE8021d
Time Since Topology Change	00:00:00
Topology Changes	0
Designated Root	000000904B7E44E7
Max Age(seconds)	0
Hello Time(seconds)	0
Forward Delay(seconds)	0
Priority	0
Bridge Max Age(seconds)	20
Bridge Hello Time(seconds)	2
Bridge FW Delay(seconds)	15
Root Cost	100
Root Port	1

Help Refresh

**STP Status** – is the spanning tree function of this system was enabled or disabled.

**STP Version** – is the STP version number.

**Time Since Topology Change** - is the time since the spanning tree was last reconfigured.

**Topology Changes** - is the number of times the spanning tree has been reconfigured.

**Designated Root** - is the bridge identifier of the root of the spanning tree.

**Max Age** - is the maximum time (in seconds) this device can wait without receiving a configuration message before attempting to reconfigure.

**Hello Time** - is the time interval (in seconds) at which this device transmits a configuration message.

**Forward Delay** is the time (in seconds) this device will wait before changing states.

**Priority** is the priority of this device. It is a part of the bridge ID, which equal to Priority (2 bytes) plus bridge MAC address (6 bytes).

**Bridge Max Age** - is the maximum time (in seconds) that all devices can wait without receiving a configuration message before attempting to reconfigure when this device becomes root.

**Bridge Hello Time** - is the time interval (in seconds) at which all devices transmit a configuration message when this device becomes the root.



**Bridge FW Delay** - is the time (in seconds) that all devices will wait before changing states when this device becomes the root.

**Root Cost** - is the cost for a packet to travel to the root in the current Spanning Tree configuration. The slower the media, the higher the cost. This is 0 if your bridge is the root device.

**Root Port** - is the index of the port on this switch that is closest to the root. This switch communicates with the root device through this port. This is 0 if your bridge is the root device.

**Refresh** – Refresh local page and all the statistics.

## STP Port

This page shows the status of STP (Spanning Tree Protocol) function.

**Figure 56** – Spanning Tree Protocol Status

System Status > STP

STP Status      STP Port

Peer Address	Name	SSID	Channel	Status
00:90:4B:75:0C:E4	-	3Com	1	-
00:90:4B:7E:40:B0	-	Pharos1_vap0	1	-

Help

**Peers Address** –displays the MAC address of the remote WDS bridge(s).

**Name** – The Alias of the remote WDS bridge.

**SSID** – Displays the SSID of the bridge.

**Channel** – Displays the channel of remote bridge

**Status** – Displays the Status of the bridge.

# 4

## TROUBLESHOOTING

---

This section will help you locate problems related to setup. The most common installation problems relate to IP Addressing.

IP Address management is fundamental. It is suggested that you create a chart to document and validate the IP addresses for your WLAN bridges.

If the password is lost or forgotten, you will need to reset the Wireless Bridge to default values. The **Reset Default** procedure resets configuration settings, but does not change the current wireless bridge Image. The **Upgrade** procedure erases the current wireless bridge image if you need to upgrade to a new image.

---

### Reset to Factory Default procedure

Use this procedure to reset the network configuration values, including the wireless bridge IP Address, Subnet Mask, and so on. The current wireless bridge Image is not deleted. This procedure may be required if the device password is forgotten.

1. Press and hold the **RESET** button for at least 5 seconds. Result: The wireless bridge reboots, and the factory default network values are restored.



**NOTE:** on the outdoor bridge, the **RESET** button is located on the PCB, behind the removable panel. Once the panel is removed, the reset button is located next to the CAT5 connection on the PCB

2. After it starts up, use 3Com Wireless Infrastructure Device Manager (WIDMAN) to discover the wireless bridge.
- 

### Setting IP Address Using 3Com Wireless Infrastructure Device Manager

Use the following procedure to set an IP Address for your wireless bridge. The network administrator typically provides the IP Address.

---

### Hardware and software requirements

Microsoft Windows OS, with 20M free disk space and at least 64M Memory.  
An Ethernet LAN interface card.

---

### Discover the wireless bridge

1. Power on the wireless bridge and your computer. By default, the wireless bridge will work as DHCP client to get it's IP address.



**NOTE:** The B2B Bridge may take up to 60 seconds to boot after power is applied. The bridge will not appear in WIDMAN until it is done booting.

2. Install the 3Com Wireless Infrastructure Device Manager (WIDMAN) from the CD attached with the wireless bridge on your computer.
3. Start up the 3Com Wireless Infrastructure Device Manager (WIDMAN).
4. It will discover your wireless bridge and list it on the list box.

---

## Initializing the IP Address using 3Com Wireless Infrastructure Device Manager

After discovering the wireless bridge, you may use the 3Com Wireless Infrastructure Device Manager (WIDMAN) to configure the IP address for the wireless bridge. Once the IP Address has been assigned, use the HTTP Interface to complete the configuration.

Use the following procedure to initialize the wireless bridge IP Address.

1. Open the 3Com Wireless Infrastructure Device Manager (WIDMAN), discover the wireless bridge.
2. Double click the wireless bridge logo listed in the list box.
3. If the 3Com Wireless Infrastructure Device Manager (WIDMAN) found the wireless bridge but could not be access it by it's IP, the 3Com Wireless Infrastructure Device Manager (WIDMAN) will pop up a dialog for configuring the wireless bridge IP address.
4. Enter an IP address and subnet mask then click OK.
5. After the wireless bridge reboots, verify the new IP Address. You can use the ping network command from networked computers to test the new IP Address.
6. When the proper IP Address is set, use the HTTP Interface over the LAN to complete configuration and manage operations.

# 5

## SPECIFICATIONS

### Regulatory domains

Channel	Frequency in MHz	USA, Canada (FCC)	ETSI	WORLD	France	China	Japan	Manual
1	2412	•	•	•	—	•	•	•
2	2417	•	•	•	—	•	•	•
3	2422	•	•	•	—	•	•	•
4	2427	•	•	•	—	•	•	•
5	2432	•	•	•	—	•	•	•
6	2437	•	•	•	—	•	•	•
7	2442	•	•	•	—	•	•	•
8	2447	•	•	•	—	•	•	•
9	2452	•	•	•	—	•	•	•
10	2457	•	•	•	•	•	•	•
11	2462	•	•	•	•	•	•	•
12	2467	—	•	—	•	•	•	•
13	2472	—	•	—	•	•	•	•
14	2484	—	—	—	—	—	•	•
<b>Maximum power levels</b>		30 dBm	20 dBm	20 dBm	20 dBm	10 dBm	20 dBm	20 dBm



Mexico is included in the Americas regulatory domain; however, channels 1 through 8 are for indoor use only while channels 9 through 11 can be used indoors and outdoors. Users are responsible for ensuring that the channel set configuration compiles with the regulatory standards of Mexico.



France is included in the EMEA regulatory domain; however, only channels 10 through 13 can be used in France. Users are responsible for ensuring that the channel set configuration compiles with the regulatory standards of France.

## Hardware Specification

<b>Interface</b>	
Ethernet Interface	10/100 base-T RJ-45 Ethernet port for connection to LAN
<b>Wireless</b>	
Standard	IEEE 802.11b & 802.11g simultaneously (2.4GHz ISM band)
Data Rate	1, 2, 5.5 and 11Mbps (Auto scaling), 6, 9, 12, 18,24, 36, 48 and 54 Mbps
Indoor: 3CRWE920G73 Antenna connector	Standard SMA
Outdoor: 3CRWEASYG73 Integrated Antenna	integrated 18dBi directional panel antenna, 19° beam width vertical and horizontal, vertical polarization
<b>Physical Specification</b>	
Outdoor: 3CRWEASYG73	
Dimension	380 x 352 x 75mm / 14.9 x 13.8 x 3 in (L x W x D)
Weight	3.1Kg (includes mounting kit)
Indoor: 3CRWE920G73	
Dimension	123 x 85 x 38mm / 4.8 x 3.3 x 1.5 in (L x W x D)
Weight	350g (includes mounting kit)
<b>Environment Specification</b>	
Outdoor: 3CRWEASYG73	
Temperature	-33°C to 50°C
Humidity	Up to 95%
Indoor: 3CRWE920G73	
Temperature	-20°C to 65°C
Humidity	Up to 95%
<b>Power Supply</b>	
Power Adaptor	Power-over-Ethernet IEEE 802.3af compliant power injector
Spec.	INPUT: AC 100-240V ~ 50-60Hz 500mA OUTPUT: DC 48V 400mA
<b>Mechanical Specification</b>	
Outdoor: Ruggedized IPX4 and flame-resistant plastic housing, wall or mast mount	
Indoor: Ruggedized and flame-resistant plastic housing and plate that allows for placement on a wall, theft protection	
<b>LEDs</b>	
3 LEDs	RF activity, LAN activity, Power (Indoor only)
<b>Management</b>	
Interfaces	HTTP, SNMP (Ethernet MIB, Bridge MIB, private MIB)
Software Update	Remote Software Update via HTTP/TFTP
Test	Integrated site survey. Loop-back test
Reset	Remote reset / Manufacturing reset
<b>Warranty</b>	
1 year	

---

## Software Specification

- ◆ Support 802.11g, Wi-Fi compliant
- ◆ Wireless Bridge with Point-to-Point and Point-to Multi-Point connections
- ◆ Support WDS
- ◆ Supports WPA-PSK, with TKIP or AES (Advanced Encryption Standard) encryption
- ◆ 64/128 bit WEP
- ◆ DHCP Server/Client
- ◆ Hide SSID Broadcast
- ◆ Web Management Interface
- ◆ NTP Client
- ◆ SNMP Management (MIBII, 802.11MIB, Private MIB)
- ◆ Remote software upgrade

# 6 GLOSSARY

---

## Symbols:

**802.11:** 802.11 is a family of specifications for wireless local area networks (WLANs) developed by a working group of the Institute of Electrical and Electronics Engineers (IEEE). The original specification provides for an Ethernet Media Access Controller (MAC) and several physical layer (PHY) options, the most popular of which uses GFSK modulation at 2.4GHz, enabling data rates of 1 or 2Mbps. Since its inception, two major PHY enhancements have been adopted and become "industry standards".

802.11b adds CCK modulation enabling data rates of up to 11Mbps, and 802.11a specifies OFDM modulation in frequency bands in the 5 to 6GHz range, and enables data rates up to 54Mbps.

---

## A

**AAA:** Authentication, Authorization and Accounting. A method for transmitting roaming access requests in the form of user credentials (typically user@domain and password), service authorization, and session accounting details between devices and networks in a real-time manner.

**AES:** *Advanced Encryption Standard*, a symmetric 128-bit block data encryption technique. AES works at multiple network layers simultaneously.

**authentication:** The process of establishing the identity of another unit (client, user, device) prior to exchanging sensitive information.

---

## B

**backbone:** The primary connectivity mechanism of a hierarchical distributed system. All systems, which have connectivity to an intermediate system on the backbone, are assured of connectivity to each other. This does not prevent systems from setting up private arrangements with each other to bypass the backbone for reasons of cost, performance, or security.

**Bandwidth:** Technically, the difference, in Hertz (Hz), between the highest and lowest frequencies of a transmission channel. However, as typically used, the amount of data that can be sent through a given communication circuit. For example, typical Ethernet has a bandwidth of 100Mbps.

**bps:** bits per second. A measure of the data transmission rate.

---

## D

**DHCP:** Dynamic Host Configuration Protocol (DHCP) is a communications protocol that lets network administrators manage centrally and automate the assignment of Internet Protocol (IP) addresses in an organization's network. Using the Internet Protocol, each machine that can connect to the Internet needs a unique IP address. When an organization sets up its computer users with a connection to the Internet, an IP address must be assigned to each machine. Without DHCP, the IP address must be entered manually at each computer and, if computers move to another location in another part of the network, a new IP address must be entered. DHCP lets a network administrator supervise and distribute IP addresses from a central point and automatically sends a new IP address when a computer is plugged into a different place in the network.

**DNS:** Domain Name Service. An Internet service that translates a domain name such as 3Com Corporation to an IP address, in the form xx.xx.xx.xx, where xx is an 8 bit hex number.

---

## E

**EAP:** Extensible Authentication Protocol. Defined in [RFC2284] and used by IEEE 802.1x Port Based Authentication Protocol [8021x] that provides additional authentication methods. EAP-TLS (Transport Level Security) provides for mutual authentication, integrity-protected ciphersuite negotiation and key exchange between two endpoints [RFC2716]. EAP-TTLS (Tunneled TLS Authentication Protocol) provides an authentication negotiation enhancement to TLS (see Internet-Draft <draft-ietf-pppext-eap-ttls-00.txt>).

---

## G

**gateway:** A gateway is a network point that acts as an entrance to another network. On the Internet, a node or stopping point can be either a gateway node or a host (end-point) node. Both the computers of Internet users and the computers that serve pages to users are host nodes. The computers that control traffic within your company's network or at your local Internet service provider (ISP) are gateway nodes.

---

## H

**hot-spot:** A hot-spot is wireless public access system that allows subscribers to be connected to a wireless network in order to access the Internet or other devices, such as printers. Hot-spots are created by WLAN access points, installed in public venues. Common locations for public access are hotels, airport lounges, railway stations or coffee shops.

**hot-spot operator:** An entity that operates a facility consisting of a Wi-Fi public access network and participates in the authentication.

**HTTP:** The Hypertext Transfer Protocol (HTTP) is the set of rules for exchanging files (text, graphic images, sound, video, and other multimedia files) on the World Wide Web. Relative to the TCP/IP suite of protocols (which are the basis for information exchange on the Internet), HTTP is an application protocol.

**HTTPS:** HTTPS (Hypertext Transfer Protocol over Secure Socket Layer, or HTTP over SSL) is a Web protocol developed by Netscape and built into its browser that encrypts and decrypts user page requests as well as the pages that are returned by the Web server. HTTPS is really just the use of Netscape's Secure Socket Layer (SSL) as a sublayer under its regular HTTP application layering.

---

## I

**ICMP:** ICMP (Internet Control Message Protocol) is a message control and error-reporting protocol between a host server and a gateway to the Internet. ICMP uses Internet Protocol (IP) datagrams, but the messages are processed by the IP software and are not directly apparent to the application user.

**IEEE:** Institute of Electrical and Electronics Engineers. The IEEE describes itself as the world's largest professional society. The IEEE fosters the development of standards that often become national and international standards, such as 802.11.

**IP:** The Internet Protocol (IP) is the method or protocol by which data is sent from one computer to another on the Internet. Each computer (known as a host) on the Internet has at least one IP address that uniquely identifies it from all other computers on the Internet. When you send or receive data (for example, an e-mail note or a Web page), the message gets divided into little chunks called packets. Each of these packets contains both the sender's Internet address and the receiver's address. Any packet is sent first to a gateway computer that understands a small part of the Internet. The gateway computer reads the destination address and forwards the packet to an adjacent gateway that in turn reads the destination address and so forth across the Internet until one gateway recognizes the packet as belonging to a computer within its immediate neighborhood or domain. That gateway then forwards the packet directly to the computer whose address is specified.

**IPsec:** IPsec (Internet Protocol Security) is a developing standard for security at the network or packet processing layer of network communication. Earlier security approaches have inserted security at the application layer of the communications model. IPsec will be especially useful for implementing virtual private networks and for remote user access through dial-up connection to private networks. A big advantage of IPsec is that security arrangements can be handled without requiring changes to individual user computers. Cisco has been a leader in proposing IPsec as a standard (or combination of standards and technologies) and has included support for it in its network routers.

IPsec provides two choices of security service: Authentication Header (AH), which essentially allows authentication of the sender of data, and Encapsulating Security Payload (ESP), which supports both authentication of the sender and encryption of data as well. The specific information associated with each of these services is inserted into the packet in a header that follows the IP packet header. Separate key protocols can be selected, such as the ISAKMP/Oakley protocol.

**ISP:** An ISP (Internet Service Provider) is a company that provides individuals and other companies access to the Internet and other related services such as Web site building and virtual hosting. An ISP has the equipment and the telecommunication line access required to have a point-of-presence on the Internet for the geographic



area served.

---

## L

**LAN:** A local area network (LAN) is a group of computers and associated devices that share a common communications line and typically share the resources of a single processor or server within a small geographic area (for example, within an office building). Usually, the server has applications and data storage that are shared in common by multiple computer users. A local area network may serve as few as two or three users (for example, in a home network) or many as thousands of users (for example, in an FDDI network).

---

## M

**MAC:** Medium Access Control. In a WLAN network card, the MAC is the radio controller protocol. It corresponds to the ISO Network Model's level 2 Data Link layer. The IEEE 802.11 standard specifies the MAC protocol for medium sharing, packet formatting and addressing, and error detection.

---

## N

**NAT:** NAT (Network Address Translation) is the translation of an Internet Protocol address (IP address) used within one network to a different IP address known within another network. One network is designated the inside network and the other is the outside. Typically, a company maps its local inside network addresses to one or more global outside IP addresses and unmaps the global IP addresses on incoming packets back into local IP addresses.

NAT is included as part of a router and is often part of a corporate firewall.

---

## P

**POP3:** POP3 (Post Office Protocol 3) is the most recent version of a standard protocol for receiving e-mail. POP3 is a client/server protocol in which e-mail is received and held for you by your Internet server. Periodically, you (or your client e-mail receiver) check your mail-box on the server and download any mail. POP3 is built into the Netmanage suite of Internet products and one of

the most popular e-mail products, Eudora. It's also built into the Netscape and Microsoft Internet Explorer browsers.

**PPP:** PPP (Point-to-Point Protocol) is a protocol for communication between two computers using a serial interface, typically a personal computer connected by phone line to a server. PPP uses the Internet protocol (IP) (and is designed to handle others). It is sometimes considered a member of the TCP/IP suite of protocols. Relative to the Open Systems Interconnection (OSI) reference model, PPP provides layer 2 (data-link layer) service. Essentially, it packages your computer's TCP/IP packets and forwards them to the server where they can actually be put on the Internet.

PPP is a full-duplex protocol that can be used on various physical media, including twisted pair or fiber optic lines or satellite transmission. It uses a variation of High Speed Data Link Control (HDLC) for packet encapsulation.

PPP is usually preferred over the earlier de facto standard Serial Line Internet Protocol (SLIP) because it can handle synchronous as well as asynchronous communication. PPP can share a line with other users and it has error detection that SLIP lacks. Where a choice is possible, PPP is preferred.

**PPPoE:** PPPoE (Point-to-Point Protocol over Ethernet) is a specification for connecting multiple computer users on an Ethernet local area network to a remote site through common customer premises equipment, which is the telephone company's term for a modem and similar devices. PPPoE can be used to have an office or building-full of users share a common Digital Subscriber Line (DSL), cable modem, or wireless connection to the Internet. PPPoE combines the Point-to-Point Protocol (PPP), commonly used in dialup connections, with the Ethernet protocol, which supports multiple users in a local area network. The PPP protocol information is encapsulated within an Ethernet frame.

PPPoE has the advantage that neither the telephone company nor the Internet service provider (ISP) needs to provide any special support. Unlike dialup connections, DSL and cable modem connections are "always on." Since a number of different users are sharing the same physical connection to the remote service provider, a way is needed to keep track of which user traffic should go to and which user should be billed. PPPoE provides for each user-remote site session to learn each other's network addresses (during an initial exchange called "discovery"). Once a session is established between an individual user and the remote site (for example, an Internet service provider), the session can be monitored for billing

purposes.

**PPTP:** Point-to-Point Tunneling Protocol (PPTP) is a protocol (set of communication rules) that allows corporations to extend their own corporate network through private "tunnels" over the public Internet. Effectively, a corporation uses a wide-area network as a single large local area network. This kind of interconnection is known as a virtual private network (VPN).

---

## R

**RADIUS:** RADIUS (Remote Authentication Dial-In User Service) is a client/server protocol and software that enables remote access servers to communicate with a central server to authenticate dial-in users and authorize their access to the requested system or service. RADIUS allows a company to maintain user profiles in a central database that all remote servers can share. It provides better security, allowing a company to set up a policy that can be applied at a single administered network point. Having a central service also means that it's easier to track usage for billing and for keeping network statistics.

---

## S

**SNMP:** Simple Network Management Protocol (SNMP) is the protocol governing network management and the monitoring of network devices and their functions. It is not necessarily limited to TCP/IP networks.

SNMP is described formally in the Internet Engineering Task Force (IETF) Request for Comment (RFC) 1157 and in a number of other related RFCs.

**SSL:** The Secure Sockets Layer (SSL) is a commonly-used protocol for managing the security of a message transmission on the Internet. SSL has recently been succeeded by Transport Layer Security (TLS), which is based on SSL. SSL uses a program layer located between the Internet's Hypertext Transfer Protocol (HTTP) and Transport Control Protocol (TCP) layers. The "sockets" part of the term refers to the sockets method of passing data back and forth between a client and a server program in a network or between program layers in the same computer. SSL uses the public-and-private key encryption system from RSA, which also includes the use of a digital certificate.

---

## T

**TCP:** TCP (Transmission Control Protocol) is a set of rules (protocol) used along with the Internet Protocol (IP) to send data in the form of message units between computers over the Internet. While IP takes care of handling the actual delivery of the data, TCP takes care of keeping track of the individual units of data (called packets) that a message is divided into for efficient routing through the Internet.

TCP is a connection-oriented protocol, which means that a connection is established and maintained until such time as the message or messages to be exchanged by the application programs at each end have been exchanged. TCP is responsible for ensuring that a message is divided into the packets that IP manages and for reassembling the packets back into the complete message at the other end. In the Open Systems Interconnection (OSI) communication model, TCP is in layer 4, the Transport Layer.

**TCP/IP:** TCP/IP (Transmission Control Protocol/Internet Protocol) is the basic communication language or protocol of the Internet. It can also be used as a communications protocol in a private network (either an intranet or an extranet). When you are set up with direct access to the Internet, your computer is provided with a copy of the TCP/IP program just as every other computer that you may send messages to or get information from also has a copy of TCP/IP.

TCP/IP is a two-layer program. The higher layer, Transmission Control Protocol, manages the assembling of a message or file into smaller packets that are transmitted over the Internet and received by a TCP layer that reassembles the packets into the original message. The lower layer, Internet Protocol, handles the address part of each packet so that it gets to the right destination.

**TKIP:** The Temporal Key Integrity Protocol (TKIP), pronounced "tee-kip", is part of the IEEE 802.11i encryption standard for wireless LANs. TKIP is the next generation of WEP, the Wired Equivalency Protocol, which is used to secure 802.11 wireless LANs. TKIP provides per-packet key mixing, a message integrity check and a re-keying mechanism, thus fixing the flaws of WEP.

**Telnet:** Telnet is the way to access someone else's computer, assuming they have given permission. (Such a computer is frequently called a host computer.) More technically, Telnet is a user command and an underlying TCP/IP protocol for accessing remote computers. On the Web, HTTP

and FTP protocols allow to request specific files from remote computers, but not to actually be logged on as a user of that computer.

---

## U

**UAM:** Universal Access Method is the current recommended methodology for providing secure web-based service presentment, authentication, authorization and accounting of users is a WISP network. This methodology enables any standard Wi-Fi enabled TCP/IP device with a browser to gain access to the WISP network.

---

## W

**WAN:** A wide area network (WAN) is a geographically dispersed telecommunications network. The term distinguishes a broader telecommunication structure from a local area network (LAN). A wide area network may be privately owned or rented, but the term usually connotes the inclusion of public (shared user) networks. An intermediate form of network in terms of geography is a metropolitan area network (MAN).

**WDS:** The Wireless Bridge supports WDS (Wireless Distribution System) to act as bridges or repeaters.

**WPA:** Wi-Fi Protected Access (WPA) is a subset of 802.11i draft that satisfies some of the requirements of the full 802.11i standard.

---

## X

**XSL:** (Extensible Style sheet Language), formerly called Extensible Style Language, is a language for creating a style sheet that describes how data sent over the Web using the Extensible Markup Language (XML) is to be presented to the user.

## REGULATORY INFORMATION

The 3Com 802.11g Wireless LAN Building-to-Building Bridge must be installed and used in strict accordance with the manufacturer's instructions as described in the user documentation that comes with the product. This device complies with the following radio frequency and safety standards.

### Canada (IC)

Operation is subject to the following two conditions: 1) this device may not cause interference and 2) this device must accept any interference, including interference that may cause undesired operation of the device.

This device has been designed to operate with an antenna having a maximum gain of 18 dBi. Antenna having a higher gain is strictly prohibited per regulations of Industry Canada. The required antenna impedance is 50 ohms.

### Federal Communication Commission Interference Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

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

FCC Caution: Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

#### **IMPORTANT NOTE:**

##### **FCC Radiation Exposure Statement:**

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 2 m between the radiator & your body.

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

## **Professional installation instruction**

### 1. Installation personal

This product is designed for specific application and needs to be installed by a qualified personal who has RF and related rule knowledge. The general user shall not attempt to install or change the setting.

### 2. Installation location

The product shall be installed at a location where the radiating antenna can be kept 20 cm from nearby person in normal operation condition to meet regulatory RF exposure requirement.

### 3. Effective power output

According to US Rule, CFR 47 part 15 Section 15.247 “Operation within the bands 902 - 928 MHz, 2400 - 2483.5 MHz, and 5725 - 5850 MHz”, the authorized maximum peak conducted output power at antenna terminal is 1 watt, per the measurement procedure as described in the rule part. Please refer to the related rules for detail.

### 4. Installation procedure

Please refer to user’s manual for the detail.

### 5. Warning

Please carefully select the installation position and make sure that the final output power does not exceed the limit set forth in US Rule CFR 47 part 15 section 15.247. The violation of the rule could lead to serious federal penalty.