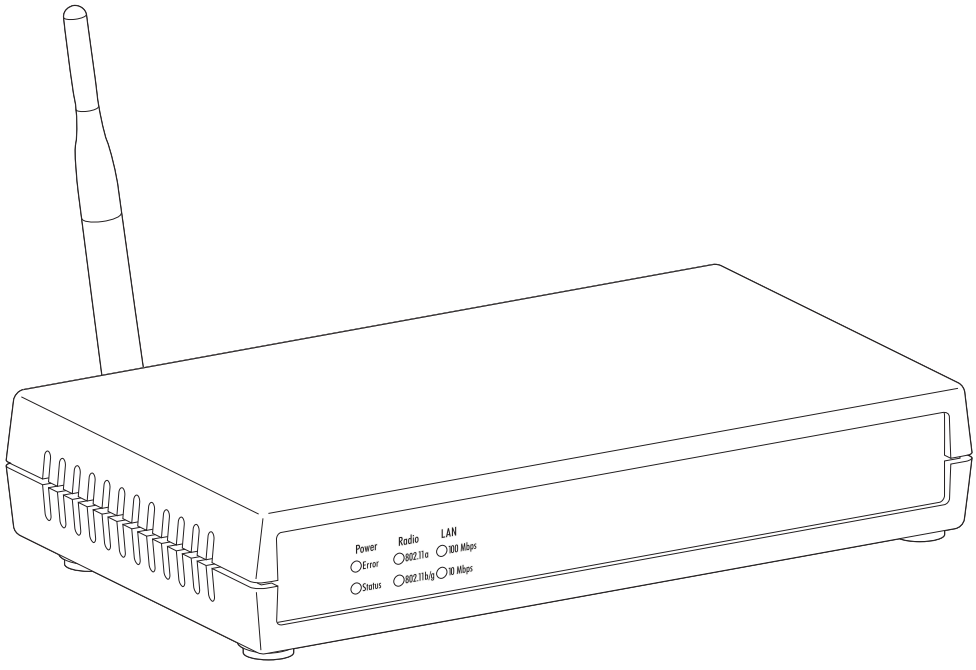
CB3000 Client Bridge

Installation Guide



Contents

Chapter 1: Document Conventions

To the Installer 1-1
Document Conventions 1-1

Chapter 2: CB3000 Overview

Before Installing the CB3000 2-1
- Prerequisite Requirements 2-2
- Verifying the Package Contents 2-2
- Verifying the Installation Site 2-2

Installing the CB3000 2-3
Displaying the CB3000 User Interface 2-5
- Connecting to the User Interface Using a Web Browser 2-5
- Connecting to the User Interface Using the Discovery Tool 2-6

Configuring CB3000 WLAN Settings 2-8
Configuring CB3000 Ethernet Settings 2-11
Configuring CB3000 Security 2-13
- Configuring CB3000 Basic Encryption 2-13

Testing Device Connectivity 2-15
Where to Go From Here? 2-16
CB3000 Troubleshooting 2-16
Technical Specifications 2-17
Support 2-18
Regulatory Compliance 2-19
- Country Approvals 2-19
- FCC / EU RF Exposure Guidelines 2-19
- Wireless Devices 2-20
- Radio Frequency Interference Requirements—FCC 2-20
- CE Marking and European Economic Area (EEA) 2-21
- Statement of Compliance 2-21
- Waste Electrical and Electronic Equipment (WEEE) 2-22

1

Document Conventions

To the Installer

This guide is intended for the technician responsible for installing the CB3000 Client Bridge. It is assumed the technician is familiar with Ethernet LAN-based networking concepts.

The purpose of this document is to provide specifications, features and guidelines for use during default device installation and configuration.

For advanced installation and configuration instructions, refer to the *CB3000 Client Bridge User Guide* available on the CB3000 Product CDROM shipped with the CB3000 and from the Support site at: *www.zebra.com/support.*

Document Conventions

Before working on any equipment, be aware of the hazards associated with its installation and use. Also, become familiar with standard practices for preventing accidents.

NOTE: Indicates tips or special requirements.

CAUTION: Indicates conditions that can cause equipment damage or data loss.

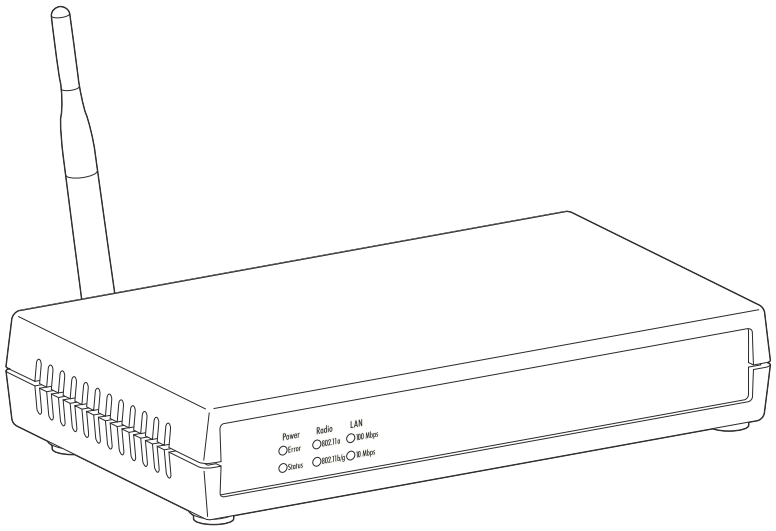
WARNING! Indicates a condition or procedure that could result in personal injury or equipment damage.

2

CB3000 Overview

The CB3000 Client Bridge (Part No. CB-3000-0010-WWR) is an IEEE 802.11a/b/g compliant wireless LAN Ethernet adapter. The CB3000 operates in both 2.4GHz (GigaHertz) and 5.2GHz frequencies. The CB3000 extends wireless networking capabilities to printers, scales, medical equipment, manufacturing machinery, bar code readers, time clocks, point-of-sale and other data collection devices. It provides a reliable, cost-effective interface between devices utilizing Ethernet ports, wireless LAN switches and access points.

Multiple devices can share one CB3000 using a 10/100Base-T Ethernet hub. This feature saves equipment costs when several devices require wireless Ethernet connectivity. The CB3000 has an on-board TCP/IP stack to provide a reliable data transport mechanism. It can initiate up to 16 client connections (including one POS device connection) to your server or accept datagrams from multiple sources. Use the CB3000 to network devices that do not have PC Card or PCI card slots (printers, scanners, etc.).



Before Installing the CB3000

Before installing the CB3000, review the guidelines in the following sections:

- Prerequisite Requirements
- Verifying the Package Contents
- Verifying the Installation Site

Prerequisite Requirements

The following hardware and software resources are required to install and operate a CB3000:

- **PC to be used during device configuration**. The PC must have an RJ-45 Ethernet port and a CDROM drive. The PC must be running the following:
  - Windows 2000 or XP operating system
  - Internet Explore 5.0 (or higher) or Netscape 6.0 (or higher)
- An *Access Point* (AP) (for infrastructure mode operation) or a networked client (for Ad Hoc mode peer-to-peer operation).

Verifying the Package Contents

Before installing the CB3000, verify the package contains the following:

- CB3000 Installation Guide (this guide)
- CB3000 Software and Documentation CDROM
- CB3000 Client Bridge (Part No. CB-3000-0010-WWR)
- Ethernet cable
- Power adapter with 5 localized plugs
- Single detachable omni-directional antenna.
- Mounting hardware.

CAUTION: Only qualified and approved antennas can be used with the CB3000.

NOTE: Contact **Support** to report any missing or improperly functioning components.

Verifying the Installation Site

Mounting options for the CB3000 include table top, wall or under a counter mounting using the keyholes and mounting hardware provided with the unit.

Before installing CB3000, verify the installation site meets the following requirements:

- The Environmental Specifications as defined in the "*Technical Specifications*" section of this guide.
- The site should have access to a properly rated power source.
- The site should be dry and within 100 meters of the device(s) (hub, telephone, computers, point-of-sale) to be connected to the CB3000.
- The site should not be near other equipment (transformers, fluorescent lights etc.) that could interfere with the CB3000's radio transmissions.
- The site should be within 250 ft. of the access point the CB3000 is targeting for association.

Installing the CB3000

Cable and test the CB3000 before moving it to its table top, wall or under a counter operational location. To cable the CB3000:

Note

NOTE: A cross-over cable is not required to directly connect the CB3000 to a PC.

Caution

CAUTION: Do not connect a CB3000 set to Infrastructure mode directly to a LAN (for example, through a wall port). Such a connection could cause a transmission loop between the CB3000 and its associated access point, disrupting network connectivity.

1. Screw the antenna clockwise onto the antenna connector on the rear of the CB3000

Note

NOTE: The back of the CB3000 also contains a Kensington lock mechanism for attaching the CB3000 to an immovable objects in order to prevent theft.

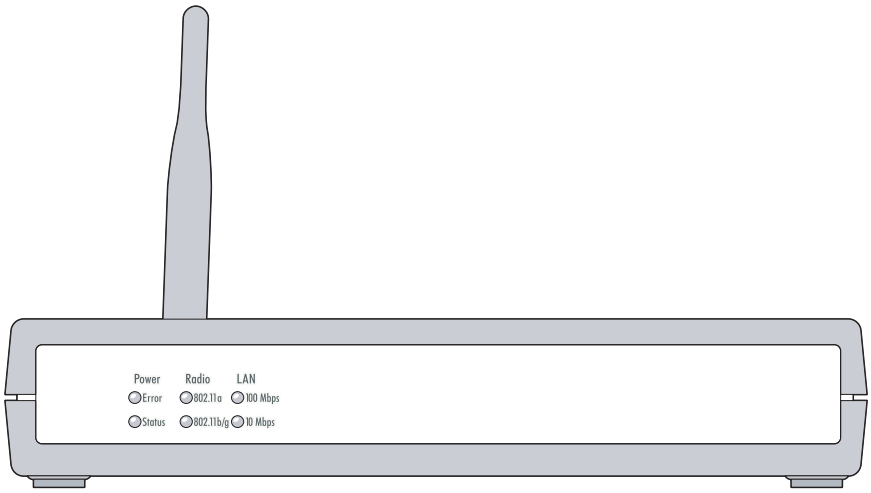
2. Attach one end of an Ethernet cable to a RJ-45 jack on a computer or hub.
3. Connect the other end of the Ethernet cable to the **LAN** connector on the rear of the CB3000.
4. Plug the power adapter into the **DC-IN** connector on the rear of the CB3000.

Caution

CAUTION: Only use the power adapter supplied with the CB3000. Using an incorrect power adapter could damage the CB3000 and void the product warranty.

5. Connect the plug end of the power adapter into a power outlet.

   The built-in power converter automatically selects and adjusts the power for the appropriate voltage.
6. Verify the installation by checking the status of the LEDs on the front of the CB3000.



The CB3000 Power, Radio and LAN LEDs provide the following functionality:

Power LEDs	Activity	Description
Error	OFF	No errors detected
Error	Orange ON	Hardware error
Status	OFF	Power OFF
Status	Green ON	Power ON/Device ready
Status	Green Blinking	Booting, system self-test or firmware upgrade

Radio LEDs	Activity	Description
802.11a 802.11b/g	OFF	Connectivity disabled
802.11a	Orange ON	802.11a radio associated
802.11a	Orange Blinking	802.11 a radio scanning
802.11b/g	Green ON	802.11b/g radio associated
802.11b/g	Green Blinking	802.11b/g radio scanning

LAN LEDs	Activity	Description
100 Mbps 10 Mbps	OFF	No Ethernet activity
100 Mbps	Orange ON	100 Mbps connection over LAN
100 Mbps	Orange Blinking	100 Mbps transmit/receive

LAN LEDs	Activity	Description
10 Mbps	Green ON	10 Mbps connection over LAN
10 Mbps	Green Blinking	10 Mbps transmit/receive

When the CB3000's LED functionality has been verified, launch the CB3000's user interface to begin the basic device configuration outlined within this guide.

Displaying the CB3000 User Interface

Connect to the CB3000 by entering the its IP address within a Web browser or use the CB3000 *Discovery Tool* to locate the CB3000 within the network and launch the user interface.

Connecting to the User Interface Using a Web Browser

The CB3000 contains a built-in browser interface for system configuration and remote management using a standard Web browser such as Microsoft Internet Explorer or Netscape Navigator. The browser interface also allows for CB3000 system monitoring.

NOTE: Web management of the CB3000 requires either Microsoft Internet Explorer 5.0 or later or Netscape Navigator 6.0 or later.

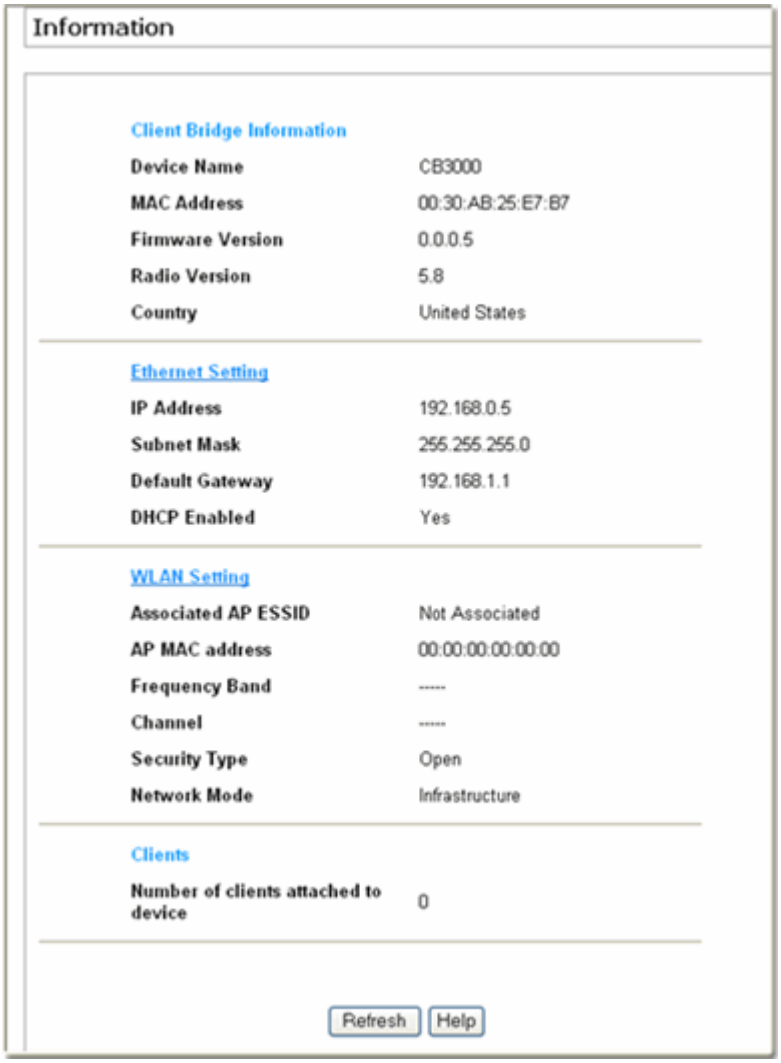
To launch the CB3000 Web interface:

1. If you know the DHCP assigned IP address for the CB3000, enter it in the browser. If no DHCP services are available, enter the default IP address of *https://10.10.1.1.* within your browser.

   A user name and password screen displays to access the address entered within the browser.

   The applet recommends changing the password when you first log into the CB3000.

2. Enter a default user name of **admin** and a default password of **symbol**. Click **OK.** The *Information* screen displays.



The *Information* screen displays high level device name and network address information. The page is read-only with no configurable data fields. The CB3000 is now ready to have its WLAN settings configured, then its Ethernet Settings. For more information, see sections *Configuring CB3000 WLAN Settings* and *Configuring CB3000 Ethernet Settings*.

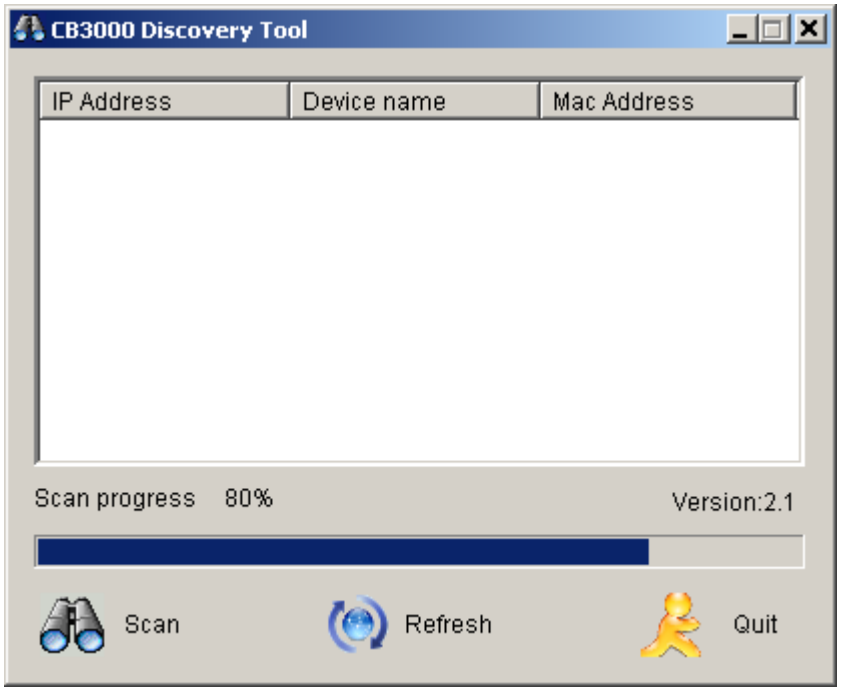
Connecting to the User Interface Using the Discovery Tool

Use the *Discovery Tool* to locate and identify CB3000s. In addition, you can double-click a located device within the *Discovery Tool* window to launch the Web interface. After power-up, the CB3000 sends several DHCP packets requesting an IP address. If the CB3000 does not receive any replies within 20 seconds, it uses a default IP address of 10.10.1.1.

The *Discovery Tool* is available on the CB3000 product CDROM and from the Support Website.

To launch and use the CB3000 Discovery Tool:

1. Insert the *CB3000 Software and Documentation CDROM* or download and launch the *CB3000 Software and Documentation* image from the Support site. Go to *www.zebra.com/support* to download the image.
2. Accept the terms of the End User License Agreement once the CB3000 flash menu displays.
3. Select the **CB3000 Discovery Tool** menu item.



The *CB3000 Discovery Tool* screen displays and begins a device search for CB3000's. The **Scan** button can also be clicked to initiate a device search, but a valid IP address is required on your system's Ethernet port for the Scan to function properly. If running a VPN client on the scanning computer, ensure it is disabled or the Scan function will not work.

4. Double-click on one of the CB3000s listed within the *Discovery Tool* window.

   If the IP address of the CB3000 is not in the same subnet as your PC's IP address, change the CB3000's IP address to be within the PC's subnet.

A *Security Alert* screen displays stating issues could exist with the CB3000's current security certificate.

5. Click **Yes** to continue. A logon screen displays.

6. Enter a default user name of *'admin'* and a default password of *'symbol'*. Click **OK.**

The *Information* screen displays high level device name and network address information. The page is read-only with no configurable data fields. The CB3000 is now ready to have its WLAN settings configured, then its Ethernet Settings. For more information, see sections *Configuring CB3000 WLAN Settings* and *Configuring CB3000 Ethernet Settings*.

Configuring CB3000 WLAN Settings

Use the *WLAN Settings* screen to define a CB3000 network (operating) mode of either *Infrastructure* or *Ad Hoc*, select the ESSID (Wireless LAN Service Area) for CB3000 connection and assess the available networks available for CB3000 connection.

Note

NOTE: The WLAN settings for the CB3000 must be configured before Ethernet settings or any other configuration.

Use *Infrastructure* mode to interoperate with an *access point* (AP). Using the *Infrastructure* mode, the CB3000 can roam freely between AP cells within the network. *Infrastructure* mode is the CB3000 default mode.

Caution

CAUTION: Do not connect a CB3000 in *Infrastructure* mode directly to a LAN (for example, through a wall port). Such a connection could cause a transmission loop between the CB3000 and its associated access point, disrupting network connectivity.

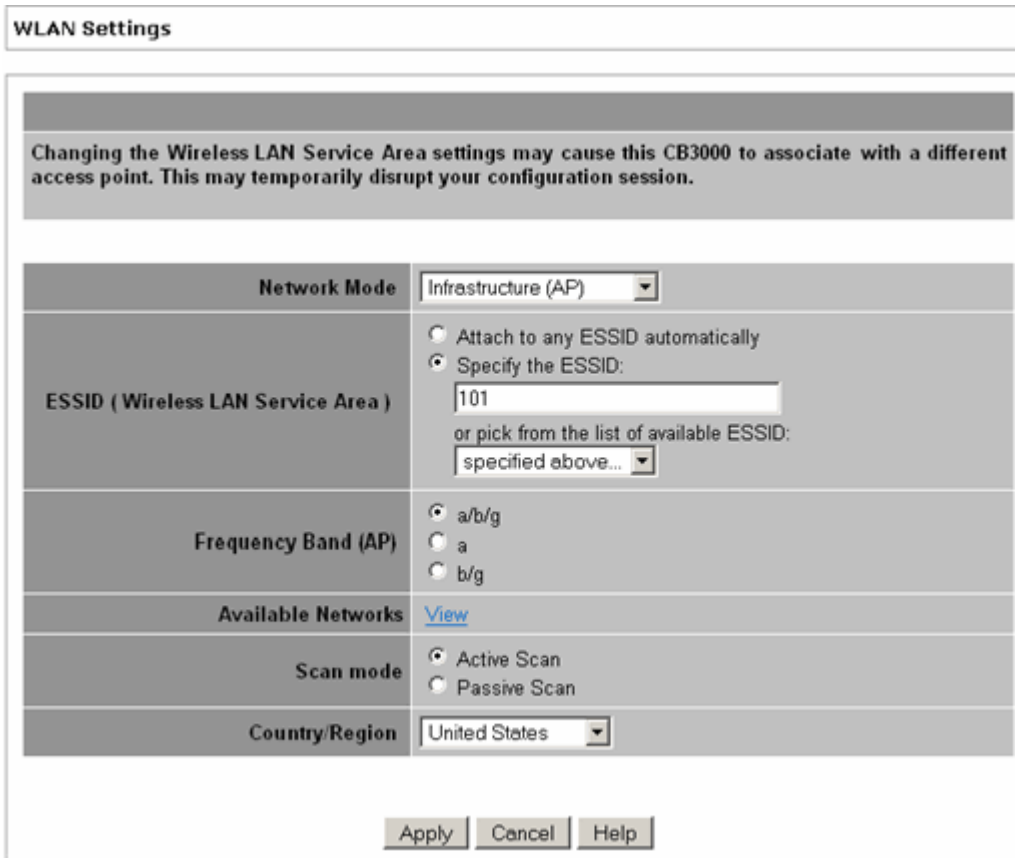
Select *Ad Hoc* to form peer-to-peer CB3000 networks without using access points. Use *Ad Hoc* mode to create networks within established network coverage areas or networks free of the physical constraints of access point provided radio coverage areas.

Note

NOTE: For the scope of the basic CB3000 configuration discussed in this guide, only a CB3000 *Infrastructure mode* configuration is described. For information on configuring the CB3000 for *Ad Hoc (Peer-to-Peer)* operation, refer to the *CB3000 Client Bridge User Guide* available on your product CDROM or at the Support site (*www.zebra.com/support*).

To configure CB3000 communication settings:

1. Select **Settings -> Wireless Settings -> WLAN Settings** from the CB3000 menu tree.



2. Select a network (operating) mode for the CB3000.

Network Mode — Select either *Infrastructure (AP)* or *Ad-hoc (Peer-to-Peer)*.

Select *Infrastructure (AP)*, to enable the CB3000 to transmit and receive with an access point within the CB3000's subnet.

3. Select an ESSID (network) for CB3000 connection.

ESSID (Wireless LAN Service Area) — The following options are available for CB3000 network connection:

Select **Attach to any ESSID automatically** to enable the CB3000 to randomly select a target ESSID for connection.

Select the **Specify the ESSID** option to manually enter the name of the target ESSID or use the drop-down menu to select the ESSID. The list of ESSIDs available to the CB3000 from the drop-down menu does not automatically refresh as devices come and go from range of the CB3000.

4. Select the **Frequency Band (AP)**. By restricting the frequency band, you can reduce the time the CB3000 takes to search for available APs.

a/b/g	Click this option to enable the CB3000 to work in the 'a' and the 'b/g' frequencies.
a	Click this option to enable the CB3000 to work only in the 'a' frequencies
b/g	Click this option to enable the CB3000 to work only in the 'b/g' frequencies

5. Click **View** to display the *Available Networks* screen.Use this screen to view a list of available ESSIDs (networks) available to the CB3000 for connection. Select the checkbox to the left of the target ESSID and click the **Connect** button to associate with that ESSID (Infrastructure mode) or networked peer (Ad Hoc mode). Unlike the networks displayed within the drop-down menu, the networks within the Available Networks screen can be updated by clicking the **Refresh** button. Refer to the *Information* screen to verify the connection to the target ESSID.
6. Select the **Scan Mode** the device uses to discover networks.

Active Scan	When using *Active Scan*, the device transmits probe requests. It then waits for response from APs and uses the responses to associate.
Passive Scan	When using *Passive Scan*, the device waits for a beacon from any Access Point. It then uses the beacon data to associate. A Passive scan is slower than an Active Scan.

7. In the **Country/Region** drop-down list, select the appropriate operating region/country.

NOTE: Each country has its own regulatory restrictions concerning electromagnetic emissions and the maximum RF signal strength that can be transmitted. Consequently, selecting a country different from the country you are actually operating the CB3000 in results in the illegal operation of the CB3000.

8. Click **Apply** to implement the updated settings.

   If the CB3000's security settings match the security settings of the ESSID, device association takes place without having to click **Apply**. However, if the CB3000's security settings do not match the ESSID, the *Security Settings* page displays and the device is required to be configured to match the security settings of the target ESSID to ensure association compatibility.
9. Click **Cancel** to revert the *WLAN Settings* screen back to the last saved configuration.

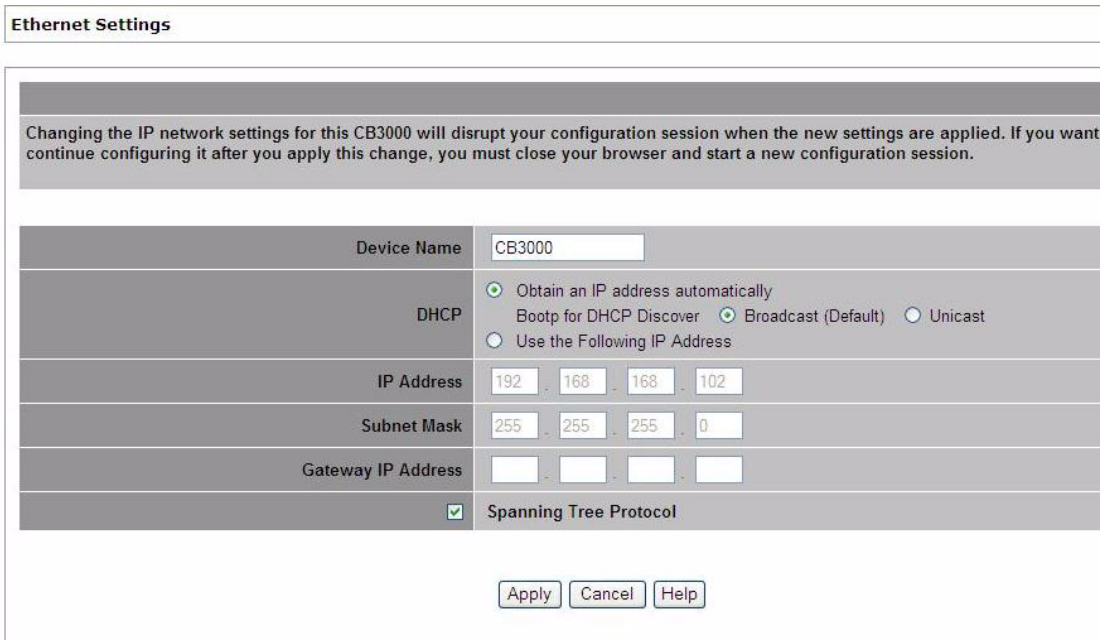
The CB3000 is now ready to have its Ethernet settings configured.

Configuring CB3000 Ethernet Settings

Use the *Ethernet Settings* screen to specify the name of the CB3000 and assign network address information required as part of the CB3000 basic configuration:

To configure required Ethernet settings for the CB3000:

1. Select **Settings -> Ethernet Settings** from the CB3000 menu tree.



2. Configure the **Ethernet Settings** screen to assign a device name and set network address information the CB3000 uses.

Device Name	Specify a device name for the CB3000. Consider selecting a name serving as a reminder of the user base the CB3000 supports (engineering, retail etc.).
DHCP	Select the **Obtain an IP address automatically** option if the CB3000 will use a DHCP server to obtain an IP address. By default, **Bootp for DHCP Discover** is set to *Broadcast*. Use the *Unicast* option for **Bootp for DHCP Discover** if you have issues using the *Broadcast* options with some DHCP servers. Select the **Use the following IP Address** option if an IP address is entered manually (static) for the CB3000.
IP Address	The **IP Address** refers to the address other devices use to address the CB3000.
Subnet Mask	A subnet mask accompanies an IP address and the two values work together. Applying the subnet mask to an IP address splits the address into two parts, an "extended network address" and a host address.
Gateway IP Address	The **Gateway IP Address** is the address of the device providing the connection to the network.
Spanning Tree Protocol	Select the **Spanning Tree Protocol** checkbox to detect loops in a network and logically block redundant paths, thus ensuring only one route exists between any two LANs. Default is disabled.

3. Click **Apply** to save the settings within the *Ethernet Settings* screen.
4. Click **Cancel** to revert the screen back to the last saved configuration.

The CB3000 is now ready to transmit and receive with a connected device in the open without security. However, configuring a basic security scheme is recommended (for the purposes of this initial basic configuration, WEP 128) to ensure initial communication between the CB3000 and its connected device are secure.

Configuring CB3000 Security

NOTE: For testing basic connectivity as described in this guide, there is no reason to enable Secure 802.1x authentication (an advanced authentication scheme). For details on configuring Secure 802.1x authentication, refer to the *CB3000 User Guide* available on the CB3000 product CDROM or go to the Support site *(www.zebra.com/support)* and download the guide.

Configuring CB3000 Basic Encryption

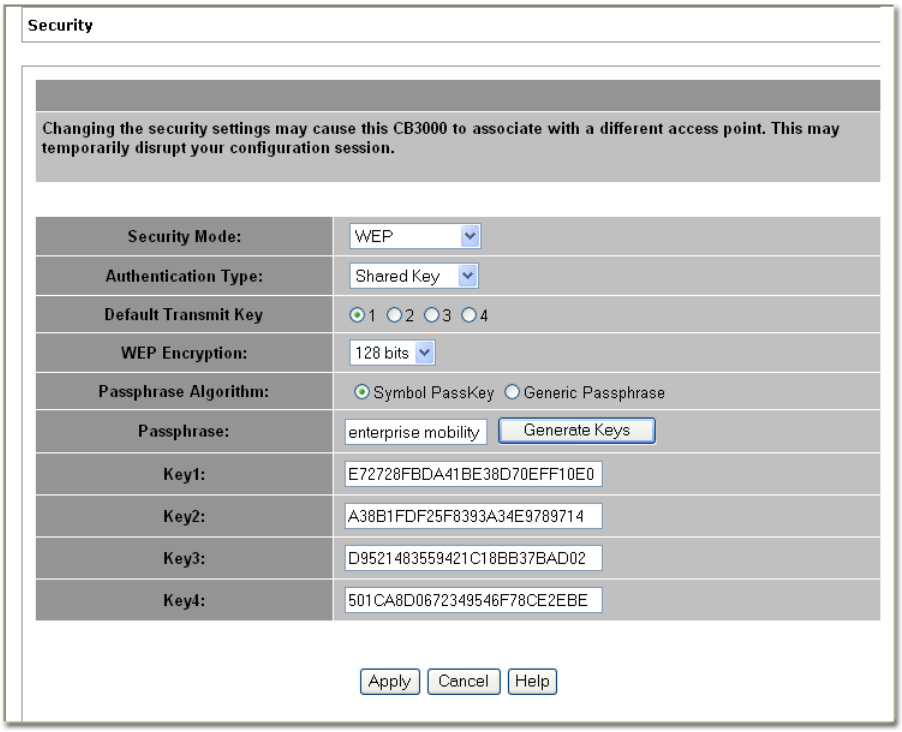
Encryption applies a specific algorithm to data to alter its appearance and prevent unauthorized decoding. Decryption applies the algorithm in reverse to restore the data to its original form. Sender and receiver employ the same encryption/decryption method.

Wired Equivalent Privacy (WEP) is a security protocol specified in the IEEE *Wireless Fidelity* (Wi-Fi) standard, 802.11b. WEP is designed to provide a WLAN with a level of security and privacy comparable to that of a wired LAN. WEP could be all that a small-business user needs for the simple encryption of wireless data.

For the basic configuration and device connection described in this guide, WEP 128 will be configured for the CB3000. WEP 128 ensures initial communications with the CB3000 are secure.

To configure WEP 128 for the CB3000:

1. Select **Settings -> Wireless Settings - > Security** from the menu tree.
2. Select **WEP** From the **Security Mode** drop-down menu.



3. Use the **Authentication Type** drop-down menu to specify whether a shared key is implemented between the CB3000 and its associated device or no key is used (*Open System*).

   If a shared key is used, both the CB3000 and its connected device are required to use the same key (as selected from 1 to 4) to interoperate. A shared key increases the level of security within the network as opposed sending information without one (*Open System*).

4. Use the **Default Transmit Key** checkboxes to specify which key is used to transmit WEP algorithm information between the CB3000 and its associated device.

NOTE: The CB3000 and its associated device are required to use the same key and key length to inter-operate.

5. Select *128-bits* from the **WEP Encryption** drop down menu.

   For WEP 128 (104-bit key), the keys are 26 hexadecimal characters in length.

6. Use the **Passphrase algorithm** option to specify whether the optional passphrase is a *Symbol Passkey* or a *Generic Passphrase*. Pass keys and pass phrases provides an easy to remember way of entering WEP key data without having to manually enter the keys each time WEP keys are created.

   Select **Symbol PassKey** to use a proprietary algorithm the CB3000 uses exclusively with other clients. The CB3000 decodes the PassKey into a set of 4 WEP keys using MD5 algorithms. The WEP keys display as alphanumeric text in the key fields until saved or the user navigates away from the **WEP** screen.

   Select **Generic Passphrase** if the CB3000 is sharing WEP keys with another vendor's clients. The CB3000 decodes the passphrase into a set of 4 WEP keys, with the length depending on the 64 or 128 bit key length. The WEP keys display as alphanumeric text in the key fields until saved or the user navigates away from the WEP screen.

7. Specify a 4 to 32 character **Passphrase** and click the **Generate Keys** button.

   The passphase is helpful for entering WEP keys without having the remember all of the characters comprising the key. The passphase can be any alphanumeric string. The CB3000, other proprietary routers and devices use the algorithm to convert an ASCII string to the same hexadecimal number. This conversion is not required for a wireless connection. Wireless devices without adapters need to use WEP keys manually configured as hexadecimal numbers.

8. Click **Apply** to save the settings defined for WEP 128.
9. Click **Cancel** to revert the screen back to the last saved configuration.

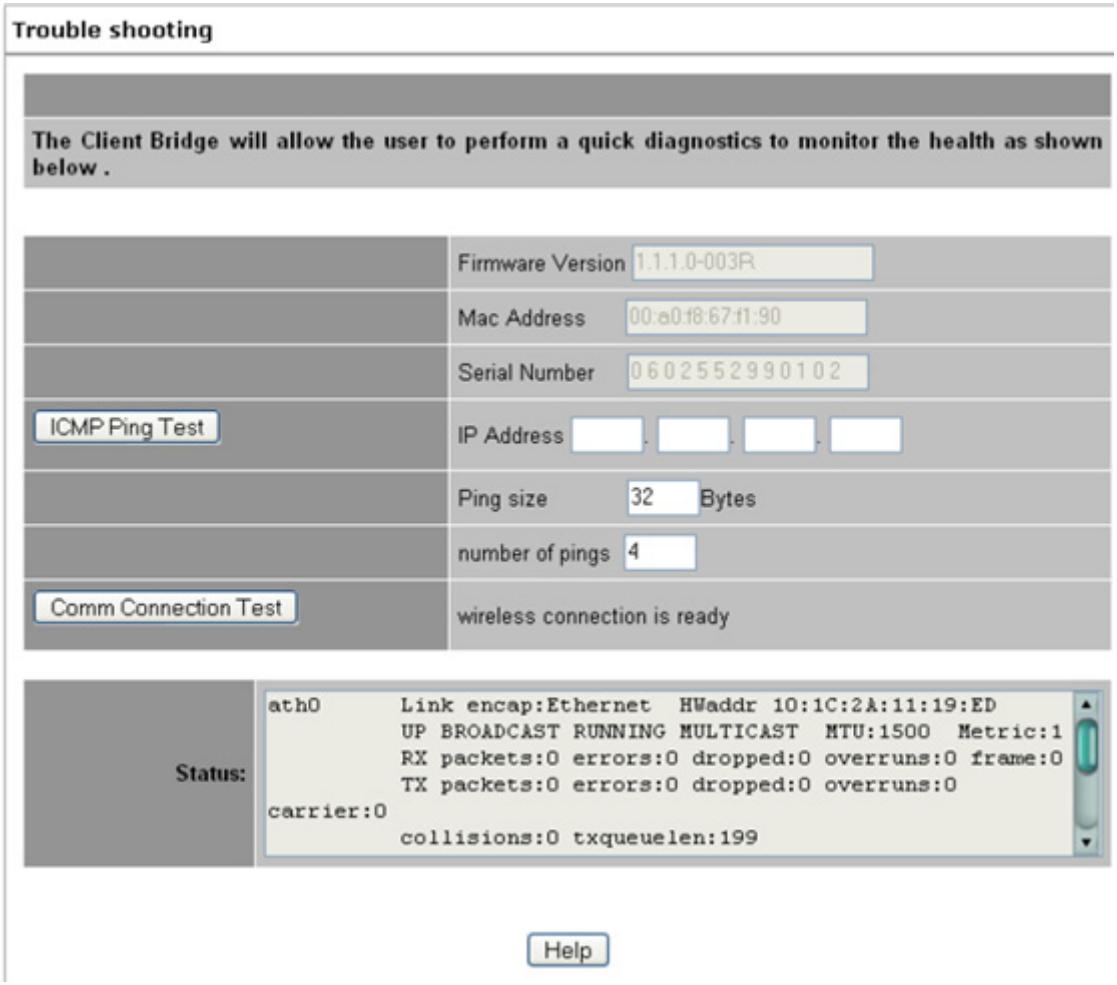
With a basic CB3000 device configuration set and WEP 128 defined for the CB3000 and its associated network device, the CB3000 is now ready to test for device connectivity.

Testing Device Connectivity

The CB3000 Web interface has a *Trouble shooting* screen with an ICMP Ping Test function. For the purposes of completing the CB3000 basic configuration and connection verification, this screen will be used to ping the CB3000's associated device.

To test CB3000 device connectivity:

1. Select **Tools -> Trouble shooting** from the CB3000 menu tree. The *Trouble shooting* screen displays.



2. The CB3000 can verify its link with an associated access point by sending ping packets to the device. To conduct a ping test:
   a. Enter the IP address of the target device.
   b. Specify the length of each data packet transmitted. This value is defined in bytes (The default is 32 bytes).
   c. Specify the number of ping packets to transmit (4 packets is recommended).
   d. Click the **ICMP Ping Test** button. Results of the ping test display in the **Status** text box. If the Status test box displays **Success**, the CB3000 can interoperate with its associated access point. If not connected, go to *CB3000 Troubleshooting*.

Where to Go From Here?

Once basic connectivity has been verified, the CB3000 can be configured to meet the needs of the network and the users it supports. The sections referenced below are located within the *CB3000 Client Bridge User Guide* available on your product CDROM or from the Support site *www.zebra.com/support*.

- Refer to Chapter 3 in the User Guide for information on configuring CB3000 network address information, and operational mode information.
- Refer to Chapter 3 in the User Guide for information on configuring encryption (WEP, WPA1 and WPA2) and authentication (Secure 802.1x) security schemes.
- Refer to Chapter 4 in the User Guide for information on accessing statistics helpful in monitoring the connection between the CB3000 and its connected devices.

CB3000 Troubleshooting

The following troubleshooting tips are recommended before contacting Support:

Problem	Corrective Action
Power LED is Off or Orange	Ensure only the supplied power adapter is used and is plugged into a power supply appropriately rated for the country of operation. Unplug the power adapter and re-insert it back into the power outlet. If the problem persists, a hardware problem likely exists. Contact Support.
LAN LED is Off	Verify the cable connection is secure between the CB3000 and the PC's LAN port. Ensure the computer network card is functioning properly.
Configuration updates lost or device hangs after reboot.	Wait at least 10 seconds after changing and saving the configuration before rebooting. If the CB3000 is hung, reset the device and implement your changes again.
CB3000 user interface hangs and cannot be navigated	Press the *Reset* button on back of CB3000 unit for less than 10 seconds to reset the device. Press the *Reset* button for 10 seconds (or more) to restore the CB3000 to its factory default configuration.
Discovery Tool Scan function does not display the CB3000 after changing the IP address (using the Discovery Tool).	Ensure the Ethernet port is set to 100Mb/full duplex on the PC/laptop. A valid IP address is also needed on the Ethernet port in order for the Discovery Tool Scan function to work properly. Ensure the computer's VPN client is disabled before performing a scan or the scan will not function properly.

Technical Specifications

Weight (with antenna)	0.65 lbs (0.30 kg)
Dimensions	7 in. wide x 4 in. deep x 1.2 in. high (17.78 cm. wide x 10.16 cm. deep x 3.05 cm high) excluding external antenna and foot stand
Protocol Support	TCP/IP, DHCP
Standards Conformance	IEEE 802.11 IEEE 802.3 IEEE 802.1d IEEE 802.11a IEEE 802.11g IEEE 802.1x IEEE 802.3u HTTP
Network Architectures	Infrastructure Ad-Hoc (Peer-to-Peer)
Operating Frequencies	802.11a: 4.9 – 5.9 GHz 802.11b/g: 2.4 – 2.5 GHz
Operating Channels	Country specific and bound by regulatory restrictions.
LAN (Ethernet) Connection	One 10/100 Base-T
Ethernet Frame	Ethernet_II and IEEE 802.3
Data Rate	IEEE 802.11a: 54, 48, 36, 24, 18, 12, 9, 6 Mbps IEEE 802.11b: 11, 5.5, 2, 1 Mbps IEEE 802.11g: 54, 48, 36, 24, 18, 12, 9, 6 Mbps
Modulation	IEEE 802.11a: Orthogonal Frequency Division Multiplexing (64QAM, 16QAM, QPSK and BPSK) IEEE 802.11b: Direct Sequence Spread Spectrum (CCK, DQPSK, DBPSK) IEEE 802.11g: Orthogonal Frequency Division Multiplexing (64QAM, 16QAM, QPSK and BPSK)
Security	64/128-Bit WEP IEEE 802.1x WPA/WPA-PSK
Peak Antenna Gain	3 dBi at 2.4 GHz 4 dBi at 5 GHz
Operating Temperature	0 – 50° Celsius
Storage Temperature	- 20 – 70° Celsius
Operating Humidity	10 – 90% relative humidity, non-condensing
Storage Humidity	5 – 85% relative humidity, non-condensing
Power Supply	Switching DC 12V, 1A

Other Features	Supports SNMP MIBs (Simple network management protocol) Features: Embedded HTTP Web management server that works with a Web browser supporting HTML

Support

If you have a problem with your equipment, contact support for your region.

Contact information is available at: *www.zebra.com/support.*

When contacting support, please provide the following information:

- Serial number of the unit
- Model number or product name
- Software type and version number

Support responds to calls by e-mail, telephone, or fax within the time limits set forth in support agreements. If you purchased your product from a business partner, contact that business partner for support.

Customer Support Web Sites

Support located at: *www.zebra.com/support* provides information and online assistance including developer tools, software downloads, product manuals and online repair requests.

Manuals

Documentation is available at:*www.zebra.com/support*.

Regulatory Compliance

All Zebra devices are designed to be compliant with rules and regulations in locations they are sold and will be labeled as required.

Local language translations are available at the following Website: *www.zebra.com/support*.

Any changes or modifications to Zebra equipment, not expressly approved by Zebra, could void the user's authority to operate the equipment.

Zebra devices must be professionally installed. The Radio Frequency Output Power will not exceed the maximum allowable limit for the country of operation.

Use only the supplied or an approved replacement antenna. Unauthorized antennas, modifications, or attachments could cause damage and may violate regulations.

Country Approvals

Regulatory markings are applied to the device signifying approval for use in the following countries: United States, Canada, Australia, Japan and Europe 1, 2.

Please refer to the *Declaration of Conformity* (DoC) for details of other country markings. This is available at *www.zebra.com/doc*.

NOTE: For 2.4GHz Products: Europe includes, Austria, Belgium, Czech Republic, Croatia, Cyprus, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Slovak Republic, Slovenia, Spain, Sweden, Switzerland and the United Kingdom.

NOTE: The use of 5GHz RLAN's has varying restrictions of use; please refer to the *Declaration of Conformity* (DoC) for details.

Operation of the device without regulatory approval is illegal.

Safety in Hospitals

Wireless devices transmit radio frequency energy and may affect medical electrical equipment. When installed adjacent to other equipment, it is advised to verify that the adjacent equipment is not adversely affected.

FCC / EU RF Exposure Guidelines

Safety Information

The device complies with Internationally recognized standards covering *Specific Absorption Rate (*SAR) related to human exposure to electromagnetic fields from radio devices.

Reducing RF Exposure—Use Properly

It is advisable to use the device only in the normal operating position.

To comply with FCC RF exposure requirements, antennas that are mounted externally at remote locations or operating near users at stand-alone desktop of similar configurations must operate with a minimum separation distance of 20 cm from all persons

Power Supply

Use only the approved power supply (pt # 0993036903) output rated 12 Vdc and minimum 1 A. The power supply is certified to EN60950 with SELV outputs. Use of alternative power supply will invalidate any approval given to this device and may be dangerous.

Wireless Devices

Ad-Hoc Operation

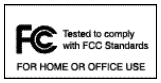
Ad-Hoc operation is limited to Channels 36-48 (5150-5250 MHz). Use of this band is restricted to Indoor Use Only; any other use will make the operation of this device illegal.

Restrictions - FCC & IC

Use of the 5150-5250 MHz band is restricted to Indoor Use Only; any other use will make the operation of this device illegal.

Symbol declares that FCC ID: H9PCB3000 is limited to Channel 1 - Channel 11 by firmware.

Radio Frequency Interference Requirements—FCC



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 or more 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.

Radio Transmitters (Part 15)

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.

Radio Frequency Interference Requirements – Canada

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

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

Radio Transmitters

This device complies with RSS 210 of Industry & Science Canada. 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.

Label Marking: The Term “IC:” before the radio certification signifies that Industry Canada technical specifications were met.

Antennas

Use only the supplied or an approved replacement antenna. Unauthorized antennas, modifications, or attachments could cause damage and may violate regulations.

Part Number	Type and Gain
ML-2499-HPA3-01	2.4 GHz Dipole, 3.3 dBi
ML-2499-SD3-01	2.4 GHz Patch, 3.5 dBi
ML-2499-BYGA2-01	2.4 GHz Yagi, 13.9 dBi
ML-5299-HPA1-01	5 GHz Dipole, 5 dBi
ML-5299-WPNA1-01	5 GHz Panel, 13 dBi
ML-2452-APA2-01	2.4/5 GHz Dipole, 3/4 dBi

CE Marking and European Economic Area (EEA)

The use of 2.4GHz RLAN's, for use through the EEA, have the following restrictions:

- Maximum radiated transmit power of 100 mW EIRP in the frequency range 2.400 -2.4835 GHz.
- France outside usage, the equipment is restricted to 2.400-2.45 GHz frequency range.
- Belgium outside usage, the equipment is restricted to 2.460-2.4835 GHz frequency range.
- Italy requires a user license for outside usage.

Caution

CAUTION: The use of 5GHz RLAN's has varying restrictions for use within the EEA; please refer to the *Declaration of Conformity* (DoC) for details at *www.zebra.com/doc*.

Statement of Compliance

Zebra hereby, declares that this device is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC. A Declaration of Conformity may be obtained from *www.zebra.com/doc*.

Taiwan

經型式認證合格之低功率射頻電機，非經許可，公司、商號或使用者均不得擅自變更頻率、加大功率或變更原設計之特性及功能。 低功率射頻電機之使用不得影響飛航安全及干擾合法通信；經發現有干擾現象時，應立即停用，並改善至無干擾時方得繼續使用。前項合法通信，指依電信法規定作業之無線電通信。低功率射頻電機須忍受合法通信或工業、科學及醫療用電波輻射性電機設備之干擾。

Other Countries

Mexico - Restrict Frequency Range to: 2.450 – 2.4835 GHz.
Sri Lanka - Restrict Frequency Range to: 2.400 – 2.430 GHz.
Taiwan - Frequency Range 2400 – 2483.5 MHz, 5250 – 5350 MHz, 5725 – 5850 MHz

Channel List -	2.4 GHz - 11 Channels, 5 GHz - 8 Channels	
Power Output -	2.4 GHz	21.50 dBm
	5.25 - 5.35 GHz	14.5 dBm
	5.725 - 5.850 GHz	19.53 dBm

Waste Electrical and Electronic Equipment (WEEE)

English: For EU Customers: All products at the end of their life must be returned to Zebra for recycling. For information on how to return a product, please go to: www.zebra.com/weee.

Français: Clients de l'Union Européenne: Tous les produits en fin de cycle de vie doivent être retournés à Zebra pour recyclage. Pour de plus amples informations sur le retour de produits, consultez: www.zebra.com/weee

Español: Para clientes en la Unión Europea: todos los productos deberán entregarse a Zebra al final de su ciclo de vida para que sean reciclados. Si desea más información sobre cómo devolver un producto, visite: www.zebra.com/weee.

Български: За клиенти от ЕС: След края на полезния им живот всички продукти трябва да се връщат на Zebra за рециклиране. За информация относно връщането на продукти, моля отидете на адрес: www.zebra.com/weee.

Deutsch: Für Kunden innerhalb der EU: Alle Produkte müssen am Ende ihrer Lebensdauer zum Recycling an Zebra zurückgesandt werden. Informationen zur Rücksendung von Produkten finden Sie unter www.zebra.com/weee.

Italiano: per i clienti dell'UE: tutti i prodotti che sono giunti al termine del rispettivo ciclo di vita devono essere restituiti a Zebra al fine di consentirne il riciclaggio. Per informazioni sulle modalità di restituzione, visitare il seguente sito Web: www.zebra.com/weee.

Português: Para clientes da UE: todos os produtos no fim de vida devem ser devolvidos à Zebra para reciclagem. Para obter informações sobre como devolver o produto, visite: www.zebra.com/weee.

Nederlands: Voor klanten in de EU: alle producten dienen aan het einde van hun levensduur naar Zebra te worden teruggezonden voor recycling. Raadpleeg www.zebra.com/weee voor meer informatie over het terugzenden van producten.

Polski: Klienci z obszaru Unii Europejskiej: Produkty wycofane z eksploatacji nale¿y zwróciæ do firmy Zebra w celu ich utylizacji. Informacje na temat zwrotu produktów znajduj¹ siê na stronie internetowej www.zebra.com/weee.

Čeština: Pro zákazníky z EU: Všechny produkty je nutné po skonèení jejich životnosti vrátit spoleènosti Zebra k recyklaci. Informace o zpùsobu vrácení produktu najdete na webové stránce: www.zebra.com/weee.

Eesti: EL klientidele: kõik tooted tuleb nende eluea lõppedes tagastada taaskasutamise eesmärgil Zebra. Lisainformatsiooni saamiseks toote tagastamise kohta külastage palun aadressi: www.zebra.com/weee.

Magyar: Az EU-ban vásárlóknak: Minden tönkrement terméket a Zebra vállalathoz kell eljuttatni újrahasznosítás céljából. A termék visszajuttatásának módjával kapcsolatos tudnivalókért látogasson el a www.zebra.com/weee weboldalra.

Svenska: För kunder inom EU: Alla produkter som uppnått sin livslängd måste returneras till Zebra för återvinning. Information om hur du returnerar produkten finns på www.zebra.com/weee.

Suomi: Asiakkaat Euroopan unionin alueella: Kaikki tuotteet on palautettava kierrätettäväksi Zebra-yhtiöön, kun tuotetta ei enää käytetä. Lisätietoja tuotteen palauttamisesta on osoitteessa www.zebra.com/weee.

Dansk: Til kunder i EU: Alle produkter skal returneres til Zebra til recirkulering, når de er udtjent. Læs oplysningerne om returnering af produkter på: www.zebra.com/weee.

Ελληνικά: Για πελάτες στην Ε.Ε.: Όλα τα προϊόντα, στο τέλος της διάρκειας ζωής τους, πρέπει να επιστρέφονται στην Zebra για ανακύκλωση. Για περισσότερες πληροφορίες σχετικά με την επιστροφή ενός προϊόντος, επισκεφθείτε τη διεύθυνση www.zebra.com/weee στο Διαδίκτυο.

Malti: Għal klijenti fl-UE: il-prodotti kollha li jkunu waslu fl-aħħar tal-ħajja ta' l-użu tagħhom, iridu jiġu rritornati għand Zebra għar-riċiklaġġ. Għal aktar tagħrif dwar kif għandek tirritorna l-prodott, jekk jogħġbok żur: www.zebra.com/weee.

Românesc: Pentru clienţii din UE: Toate produsele, la sfârşitul duratei lor de funcţionare, trebuie returnate la Zebra pentru reciclare. Pentru informaţii despre returnarea produsului, accesaţi:www.zebra.com/weee.

Slovenski: Za kupce v EU: vsi izdelki se morajo po poteku življenjske dobe vrniti podjetju Zebra za reciklažo. Za informacije o vračilu izdelka obiščite: www.zebra.com/weee.

Slovenčina: Pre zákazníkov z krajín EU: Všetky výrobky musia byť po uplynutí doby ich životnosti vrátené spoločnosti Zebra recykláciu. Bližšie informácie o vrátení výrobkov nájdete na: www.zebra.com/weee.

Lietuvių: ES vartotojams: visi gaminiai, pasibaigus jų eksploatacijos laikui, turi būti grąžinti utilizuoti į kompaniją „Zebra“. Daugiau informacijos, kaip grąžinti gaminį, rasite: www.zebra.com/weee.

Latviešu: ES klientiem: visi produkti pēc to kalpošanas mūža beigām ir jānogādā atpakaļ Zebra otrreizējai pārstrādei. Lai iegūtu informāciju par produktu nogādāšanu, lūdzu, skatiet: www.zebra.com/weee.

Türkçe: AB Müşterileri için: Kullanım süresi dolan tüm ürünler geri dönüştürme için Zebra 'ya iade edilmelidir. Ürünlerin nasıl iade edileceği hakkında bilgi için lütfen şu adresi ziyaret edin: www.zebra.com/weee.

Zebra Technologies Corporation.

Lincolnshire, IL 60069 USA

MN001687A01 Revision A April 2015