BreadCrumb® JR

USER GUIDE

PRELIMINARY

Version: 1.00-pre1
Date: May 6, 2010

Corporate Headquarters
Rajant Corporation
400 East King Street
Malvern, PA 19355
Tel: (484) 595-0233
Fax: (484) 595-0244

http://www.rajant.com

Document Part Number: 20-100035-001

MESH
WRN
LAN
RDY
ERR
PWR
RAJANT

FCC and IC Statements

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the device is operated in a commercial environment. This device generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with this instruction manual, may cause harmful interference to radio communications. Operation of this device in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at their own expense.

This Class A digital apparatus complies with Canadian ICES-003 and RSS-210 rules.

Cet appareil numérique de la classe A est conforme à la norme NMB-003 et CNR-210 du Canada.

WARNING: To satisfy FCC RF exposure requirements a minimum safe distance of 20 cm must be maintained between this device and all persons while the device is operating.

CAUTION: To reduce potential radio interference to other users, the antenna type and its gain should be chosen so that the equivalent isotropically radiated power (EIRP) is not more than that permitted for successful communication.

CAUTION: Changes or modifications not expressly approved by Rajant Corp. could void the user's authority to operate the equipment.

Copyright Statement

You may use the software provided with the products only on personal computers owned by the purchasing individual or entity, and may not use, load, or run any such software on any network or in any type of service bureau, time-sharing operation, or non-purchasing individual or entity's equipment.

BCAdmin and BCAPI are trademarks; Rajant, the Rajant logo, BreadCrumb, Instamesh, BC|Commander, and Bring Your Network with You! are registered trademarks of Rajant Corp. in the United States and certain other countries.

BreadCrumb® JR User Guide

Table of Contents

List of Figures

List of Tables

Preface

Purpose and Scope

This manual provides information and guidance to all personnel who are involved with and use Rajant Corporation's BreadCrumb JR product.

This manual begins with an introduction to the BreadCrumb Wireless Network (BCWN). It then characterizes the features of the BreadCrumb JR. Finally, it describes common deployment scenarios and provides concise step-by-step instructions for each scenario.

User Information

The user of this manual is encouraged to submit comments and recommended changes to improve this manual. Please send any comments or changes to support@rajant.com. Be sure to include the version number of the manual you are using and please provide the page numbers related to your comments wherever possible.

Related Documentation

For additional BreadCrumb JR information, refer to these documents:

- *BC|Commander® User Guide:* This document contains information on the BC|Commander management application, which is used to configure BreadCrumbs before or during a deployment.
- *BreadCrumb® Video Guide*
- *BreadCrumb® VLAN Guide*
- *Troubleshooting Range User Guide*
- *RF Component Installation and Verification in BreadCrumb® Networks*

1 Introduction

Rajant Corporation's (http://www.rajant.com) BreadCrumb JR utilizes the 802.11g wireless networking standard to form a wireless mesh network. The network is mobile, self-integrating, self-meshing, self-healing, full-duplex and secure. The focus is on flexibility, adaptability, and simplicity.

The BreadCrumb Wireless Network (BCWN) is intended for rapid deployment of a broadband wireless network into a situation or "hot zone." The network can be deployed as a stand-alone wireless network, or bridged to another network (such as the Internet) utilizing available reach-back communication links (such as a DSL, cable, or satellite modem).

BreadCrumb JR provides high bandwidth applications to stream video, audio as well as data over large distances. The network traffic can be secured by using different security features offered by the BCWN. This makes the network optimal for tactical deployments as well as emergency response situations since it offers robustness, stability and ease of setup in mission critical activities.

Note Throughout this document, unless otherwise stated, the terms *Breadcrumb* and *JR* are used to refer to *Rajant BreadCrumb JR.*

1.1 What is a BreadCrumb?

A BreadCrumb is an IEEE 802.11 (Wi-Fi) and Ethernet compatible networking device which has the capacity to connect to other BreadCrumbs or networking devices to form a BreadCrumb network. A BreadCrumb is specifically designed for the following scenarios:

Temporary Wireless Networks

Networks that must be established quickly and with minimal effort for short-term use (e.g., a network established to provide First Responder support at the site of a disaster).

Mobile Wireless Networks

Networks in which the network infrastructure itself is mobile, in addition to client devices (e.g., a convoy viewing a video stream from a UAV).

Wireless Network Extension

Networks in which a wireless network must be quickly extended around or through obstacles that block wireless communications (e.g., urban canyon networks, tunnels/caves, etc.)

Wired Network Extension

Networks in which two or more wired LANs at different locations must be connected wirelessly (e.g., to securely connect combat service support computers with logistics bases)

Any Combination of the Above

Most BreadCrumb deployments include elements from more than one of the above scenarios.

In many cases, BreadCrumbs will perform all of these tasks as shipped with no configuration necessary at all, providing an instant TAN (Tactical Area Network). Moreover, because BreadCrumbs use industry-standard 802.11 communications, client devices such as laptops or handheld computers require no special hardware, software, or configuration to access a BCWN.

Mobility through Meshing

The key component to a BCWN is a technique known as *meshing*. While this is generally handled automatically by BreadCrumbs, complex deployment scenarios require a basic understanding of how BreadCrumbs establish and maintain a mesh.

1.1.1 Mesh – A Definition

A mesh is a collection of network devices (in our case, BreadCrumbs), each of which is linked to one or more other BreadCrumbs. Data can move between BreadCrumbs via these links, possibly passing through several intermediate BreadCrumbs before arriving at its final destination.

The intelligence of a BCWN is in how it adapts rapidly to the creation or destruction of the links in the mesh as devices are moved, switched OFF or ON, blocked by obstructions, interfered with by other devices, or otherwise affected. This adaptation takes place automatically and immediately as needed.

Note	Although all BreadCrumbs can be access points, most access points do not provide mesh capability. Traditional access points simply allow wireless devices within range to connect to a wired network; they do not extend range through other access points.

1.1.2 BreadCrumbs Mesh by Channel and ESSID

Two BreadCrumbs establish a mesh link to each other when they share both a radio channel and an ESSID. An ESSID is essentially a name for a wireless network. By default, BreadCrumbs use the ESSID “breadcrumb54-v10”. The following examples illustrate the use of channels and ESSIDs:

Example 1:

Suppose you have three BreadCrumbs, called A, B, and C. Each has two radios. BreadCrumb A’s radios are on channels 1 and 8, B’s are on 8 and 11, and C’s are on 1 and 11. All three BreadCrumbs are using the default ESSID of "breadcrumb54-v10." Assuming that all three BreadCrumbs are within radio range of one another, the network will be connected, as shown below:

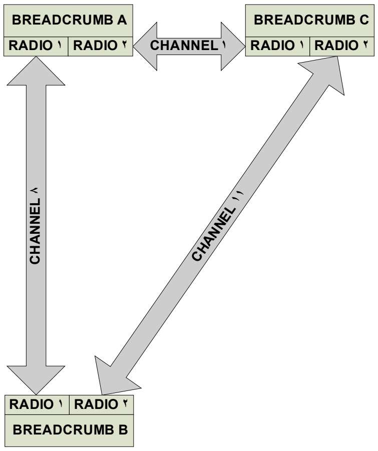

Figure 1: All BreadCrumbs Use the Same ESSID.

Example 2:

Now suppose that you change the ESSID of BreadCrumb C to "lonely". The network will adjust to this change, resulting in the following configuration:

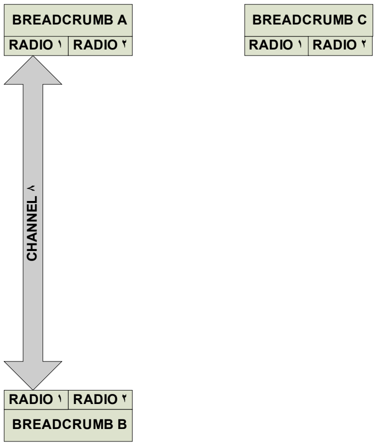

Figure 2: ESSID of BreadCrumb C Changes to "lonely."

Note that BreadCrumb C can no longer communicate with A or B, and vice versa.

1.2 Description of BreadCrumb JR

The BreadCrumb JR is a portable, wireless device deployable in almost any environment. It is light in weight, and offers one external antenna, and is designed to be completely mobile as worn by an individual. The BreadCrumb Jr must be powered by an external source.

1.2.1 Radio

BreadCrumb JR comprises one 802.11b/g radio, which operates in the 2.4 GHz frequency band.

The radio supports the following channels and frequencies in the United States and Canada (see Table 1):

Note Not all channels are allowed for use everywhere around the world. Check with the corresponding wireless spectrum regulatory body to determine the subset of channels authorized for use in your country.

Table 1: 2.4 GHz Radio Channels and Frequencies.

Channel Number	Center Frequency (MHz)
1	2412
2	2417
3	2422
4	2427
5	2432
6	2437
7	2442
8	2447
9	2452
10	2457
11	2462

The default channel for the BreadCrumb JR radio is 11 (2462 MHz).

1.2.2 Enclosure

The JR enclosure has been designed to operate in extreme conditions with protection against ingress of dust as well as protection against immersion in water. The enclosure dimensions are 186 mm x 38 mm x 34 mm (7.32” x 1.48” x 1.348”).

The external features of the enclosure are shown in Figure 3 below.

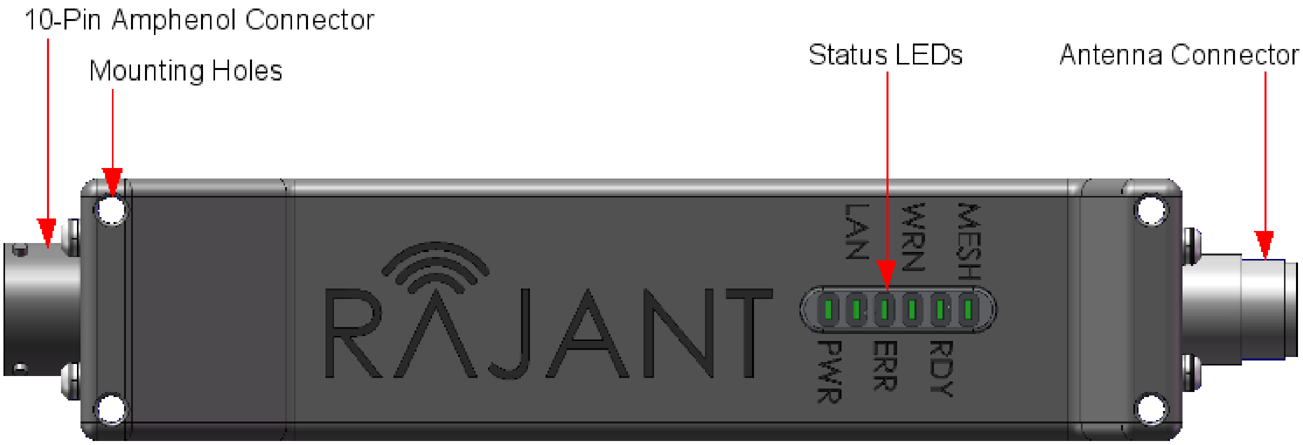

Figure 3: BreadCrumb JR Enclosure Features

1.2.3 Antenna Connector

BreadCrumb JR provides one Type N antenna connector located on the top of the enclosure (see Figure 3).

Warning ⚠

To avoid possible damage to the BreadCrumb radio, always connect or disconnect the external antenna with the power to the BreadCrumb JR off.

1.2.4 10-Pin Amphenol Connector

All of the signals and features of BreadCrumb JR can be accessed through the 10-pin Amphenol connector on the enclosure (see Figure 3 and Figure 4). The five interfaces provided by this connector are input power, Ethernet, GPS data, 3.3 V output power, and GPIO, which are described in more detail in the following sections.

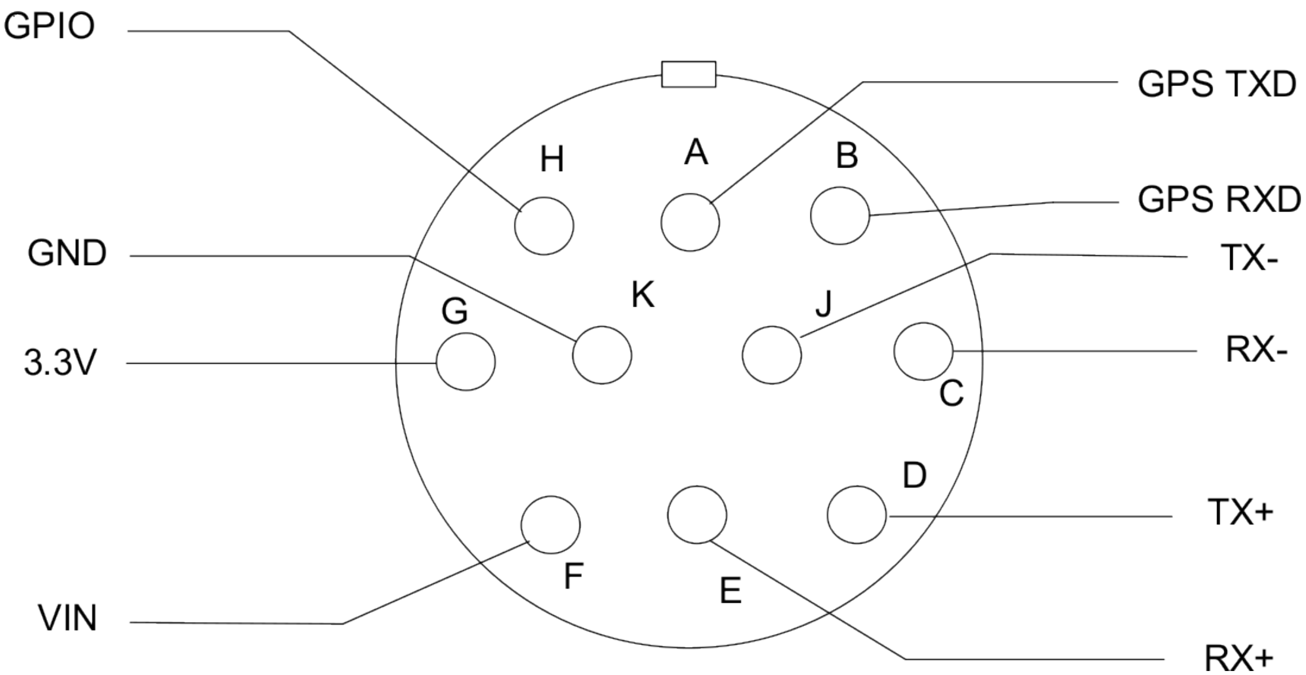

Figure 4: 10-Pin Amphenol Connector

The 10-pin Amphenol connector interfaces with the optional JR cable assemblies which provide access to input power, Ethernet, GPS data, and 3.3 V output power (see section 1.3).

1.2.4.1 Input Power

The input power interface to BreadCrumb JR resides on the F (VIN) and K (GND) pins of the 10-pin Amphenol connector (see Figure 4). The device accepts input power in the range of 10.5 VDC to 25 VDC.

The nominal power consumption of BreadCrumb JR is 3 W at 24 VDC. The actual power consumption may vary between 2.5 W at 24 VDC when the device is idle, to 4.5 W at 24 VDC when the device is operating at full duty cycle.

Note	Nominal power consumption is defined by the scenario in which the device transmits 20% of the time and is idle the remaining 80% of the time. The idle condition is defined as no transmit activity, and continuous idle operation. The full duty cycle condition is defined as continuous transmit activity, and no idle operation.

1.2.4.2 Ethernet

BreadCrumb JR contains one 10/100 Base-TX Ethernet port, which can be accessed through the C (RX-), D (TX+), E (RX+) and J (TX-) pins of the 10-pin Amphenol connector (see Figure 4). The port supports Auto MDI/MDIX allowing the use of either straight-through or crossover data cables for connections.

1.2.4.3 GPS Data Interface

The BreadCrumb JR contains a serial GPS data interface which can be accessed through the A (GPS TXD) and B (GPS RXD) pins of the 10-pin Amphenol connector (see Figure 4).

1.2.4.4 3.3 V Output Power

Pin G (3.3V) on the 10-pin Amphenol connector provides 3.3 V output power at 0.5 A (see Figure 4).

1.2.4.5 GPIO

Pin H (GPIO) on the 10-pin Amphenol connector provides a GPIO interface (see Figure 4) to the BreadCrumb JR. The BreadCrumb JR firmware implements a hardware initiated *Zeroize Keys and Restore Factory Defaults* feature through this interface.

1.2.5 Status LEDs

The Status LEDs (see Figure 3) indicate the current status of a BreadCrumb.

Table 2: Status LED Codes.

LED Name	Status
PWR	Power
LAN	Ethernet connection
ERR[1]	Error
WRN	Warning
WRN & MESH	During Startup, indicates generation and validation of cryptographic keys
RDY	Ready
MESH (blinking)	All peers are connected at less than 24 Mbps
MESH (solid)	At least one peer is connected at 24 Mbps or faster
Scrolling ERR-RDY-MESH	Success/Completion

[1] For a list of error and warning codes refer to Appendix A at the end of this document.

Warning ⚠

Unlike other BreadCrumb models, the Status LEDs on the BreadCrumb JR are always ON. There is not an “Alerts Only” or “OFF” Mode available. The LEDs must be physically masked (such as adding tape to the LED panel) to guarantee that no light is emitted at any time.

1.2.6 Zeroizing Keys and Restoring Factory Defaults

To zeroize a BreadCrumb JR (to restore default settings and remove all cryptographic keys), the user must use BC|Commander. Refer to the BC|Commander User Guide document for more information.

1.3 Optional Cable Assemblies

There are two different optional cable assemblies (part numbers 06-100043-001 and 06-100043-002) available from Rajant for use with the JR. The difference between these two cable assemblies is how the BreadCrumb gets its power. The -001 cable assembly provides power over Ethernet via the RJ45 connector (see Figure 5 below).

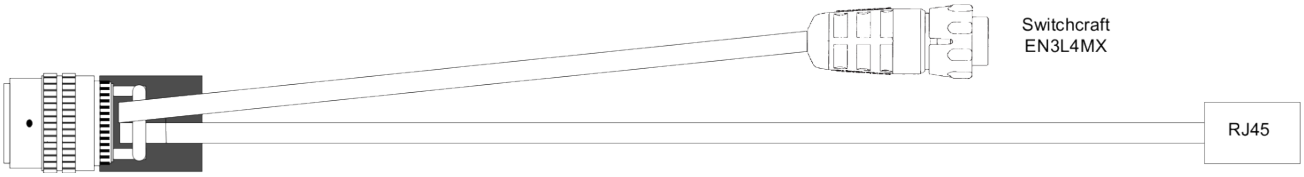

Figure 5: Cable Assembly 06-100043-001

The -002 cable assembly has a separate, unterminated cable which can be used to supply power to the BreadCrumb (see Figure 6 below). This is designed to allow the use of an external battery pack as a power source. The Ethernet connector on this assembly does not carry power.

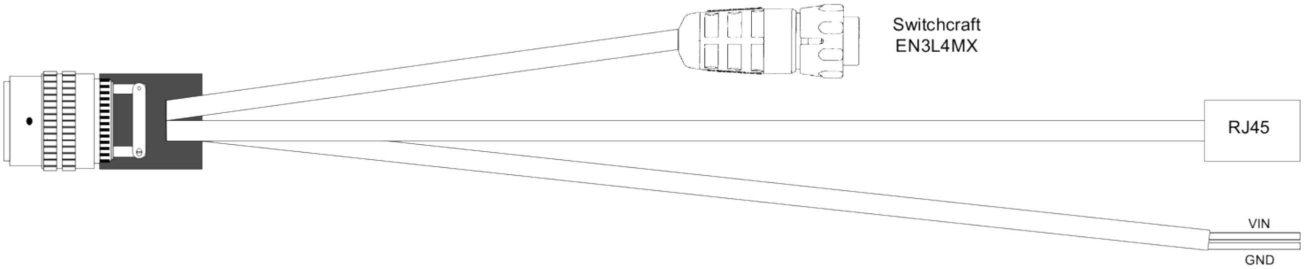

Figure 6: Cable Assembly 06-100043-002

Both of the cable assemblies plug into the 10-pin Amphenol connector and provide a standard RJ-45 Ethernet connector and a customized 4-pin GPS port. The 4-pin GPS port can be used with the optional GPS accessory from Rajant.

Note	The two currently existing optional cable assemblies do not provide access to the GPIO interface of the BreadCrumb JR.

1.3.1 4-Pin GPS Connector

The GPS connector, a Switchcraft EN3L4MX connector (see Figure 7) is designed to interface with an optional GPS device available from Rajant.

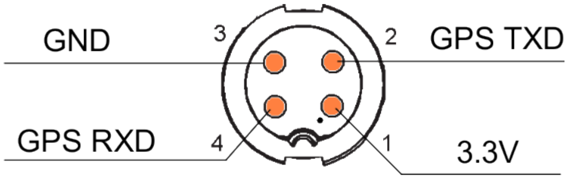

Figure 7: 4-Pin GPS Connector

2 Using BC|Commander

BC|Commander is Rajant's software package used for monitoring the status of BreadCrumbs with **version 10 firmware** on a BreadCrumb Wireless Network (BCWN). BC|Commander is also used for configuring version 10 BreadCrumbs and to graphically portray the network topology.

Note

BC|Commander includes an option called *v10 Transitional Mode*. This allows a user to run a mixture of BreadCrumbs with firmware version 9 and firmware version 10 within the same mesh network. This is very useful when BreadCrumbs in a very large network are being upgraded from version 9 to version 10 firmware.

BC|Commander is typically run on a laptop PC, but can be run on any PC that has access to the entire BCWN. Versions of either software package are available for Microsoft Windows® or Linux.

Note

Some portions of the BC|Commander User Guide document assume a working knowledge of TCP/IP networking, including DHCP, NAT and DNS. While the network lay person may be able to perform some BCWN management tasks, it is recommended that network configuration be performed by experienced network administrators.

Note

The BC|Commander version used must be equal to or greater than the firmware version running on any administered BreadCrumbs in order to administer all BreadCrumb firmware features covered in Rajant's BC|Commander User Guide.

Rajant periodically releases updated BC|Commander software. The updated software must be obtained from Rajant. Refer to Rajant's most recent BC|Commander User Guide document for instructions on how to install the latest version of BC|Commander on your computer and how to use BC|Commander with Rajant's BreadCrumbs.

3 Deploying the BreadCrumb Wireless Network

There are many factors which need to be taken into account when deploying the BreadCrumb Wireless Network (BCWN). Section 3.1 describes the addressing scheme of the BCWN. Section 3.2 discusses channel assignments. Section 3.3 details some of the most commonly occurring environmental factors that will have a major impact on the performance of the BCWN. Finally, section 3.4 details guidelines and methodology needed to follow when deploying the BCWN.

3.1 Addressing

When in gateway mode or when using its own embedded DHCP servers, the BreadCrumb Wireless Network requires that wireless devices use IPv4 addresses in the Class A network 10.0.0.0/8 (that is, any address that begins with '10.'). If you are not connected to another network, or if you are bridging to one rather than routing to it, your wireless client devices may have any address whatsoever.

Note	Any computers running the BC|Commander management application must have an address in the same range as the BreadCrumbs they manage. Refer to the BC|Commander User Guide document for the details of BreadCrumb IP adrress configuration.

3.1.1 BreadCrumb Device Addresses

Each BreadCrumb radio has one IPv4 address in the Class A network 10.0.0.0/8. These addresses are assigned during manufacturing and cannot be changed in the field. Rajant ensures during manufacturing that these addresses are not duplicated between any two BreadCrumb devices. Addresses assigned to BreadCrumb devices can be viewed using BC|Commander.

3.1.2 DHCP

Each BreadCrumb device includes an embedded DHCP server. You may safely enable the DHCP servers of multiple BreadCrumb devices simultaneously, and it is in fact the most common case that all BreadCrumb devices in a BCWN run DHCP servers. Address conflicts among DHCP clients are prevented by using the unique BreadCrumb device addresses assigned at the factory as a base.

A BreadCrumb device determines its DHCP range as follows:

- Start with the first three bytes of the first radio's IPv4 address.
- Add a low-byte range of 10 to 210.

3.2 Channel Assignments

By default, BreadCrumb JR devices use channel 11 upon startup. In some cases, however, it may be necessary to manually set the radios to specific channels. Refer to the BC|Commander User Guide document for the details of BreadCrumb channel configuration.

3.3 Physical Placement and other Considerations

Commonly occurring environmental factors have a significant impact on performance and behavior of the BreadCrumb Wireless Network. LOS (Line of Sight) obstructions, distance, weather, and device placement should all be considered when deploying a wireless network.

IEEE 802.11 wireless operation degrades gradually as distance increases between nodes or as interference becomes prominent. This manifests as a data rate reduction between nodes.

The goal in planning and deploying a BreadCrumb Wireless Network is to maximize both coverage and the data transfer rate between devices. These can be maximized by taking into consideration all of the contributing factors described in this section.

3.3.1 Line-of-Sight

Unobstructed LOS (Line-of-Sight) is critical for optimal performance of the BCWN. Partial LOS obstruction results in noticeable network performance degradation. Total LOS obstruction can result in complete loss of network connectivity.

Elevating the device and external antenna will assist in providing better LOS. This can allow the radio waves to propagate over some possible obstructions.

Unobstructed LOS is not necessary from every BreadCrumb device and wireless client to every other BreadCrumb device and wireless client. However, each device must have unobstructed LOS to the previous and subsequent device.

Client connectivity will degrade and drop if LOS to a BreadCrumb device can not be maintained.

3.3.2 Distance

Many factors determine acceptable distances between BreadCrumb devices when deploying a BCWN:

- If many devices are placed too closely together, it is possible that interference will degrade the performance of the system.
- Devices placed too far away or in RF "shadows" may experience total loss of connection.
- RF transmit power and receive sensitivity are important in determining the distances over which the device will be effective.
- When placing a BreadCrumb device, check the connection status to the nearest available device using either the BreadCrumb device's status LED (described in section 1.2.5 Status LEDs), or the BC|Commander management application. If the connection is poor or non-existent, attempt to relocate the BreadCrumb device closer to another device until an acceptable connection is obtained. If a poor connection or no connection is made at even relatively close distances, you should refer to Chapter 5 Troubleshooting.
- When the connection quality is found to be acceptable from BC|Commander, the distance of the BreadCrumb device from the network can be increased until an optimal balance between distance, connectivity and tactical placement is achieved.

3.3.3 Weather

Precipitation and fog also act as obstructions blocking the propagation of the wireless network's radio waves.

Light fog or precipitation may result in noticeable degradation of wireless network performance. Heavy precipitation or fog may result in severe performance degradation and possible loss of network connectivity.

If the performance of a well functioning network is degraded by worsening weather conditions, it may be advisable to add BreadCrumb devices into the network to act as short haul repeaters to counteract the effects of the weather. An alternative is to move the devices closer together.

3.3.4 Interference

RF interference can degrade network performance and can come from many different sources, including:

- Other BreadCrumb devices that are placed too closely together.
- Other RF devices such as microwave devices, cordless phone base stations, radio transmitters, other wireless networks, jamming devices, etc...
- Metal surfaces such as fences and buildings can cause radio waves to be reflected, causing multipath interference.

Caution ⚠

Plan the BreadCrumb Wireless Network to minimize the effects of RF interference.

3.3.5 Placement of BCWN Components

The placement of BreadCrumb devices has a major impact on maximum effective range, and therefore network performance. The components must be elevated above the surrounding terrain to allow for adequate wave propagation. A device placed directly on the ground has a significantly reduced effective range. Elevating a device above the ground dramatically increased the maximum effective range. Rajant recommends elevating the components a minimum of 6 ft. above the surrounding surface.

3.4 Deployment Guidelines and Methodology

This section addresses the actual on-site deployment of the BCWN. While by no means an exhaustive treatise, it is intended as a good source of guidelines and methodology for the successful deployment of the BCWN in the field.

3.4.1 Deployment Guidelines

Follow these guidelines when deploying the BCWN:

1. Placement of BCWN components

(a) Elevate the BCWN components whenever possible.

i. Directly on the ground, the maximum distance between any two BCWN components is approximately 300 ft. Also, the maximum distance between a wireless client and the nearest BCWN component is approximately 300 ft.

ii. Rajant recommends elevating each BCWN component a minimum of 6 ft. above the surrounding terrain for maximum range. Elevating the BCWN components, as little as 14 inches, has proven to increase the range out to approximately 600 ft.

2. Distance

(a) If you cannot elevate the BCWN components, they can only be approximately 300 ft. apart. Also, any wireless clients can be no farther than approximately 300 ft. from a BCWN component.

3. Line of sight

(a) Obstructions to line of sight block/absorb/deflect the wireless network's radio waves, resulting in poor network performance or total loss of network connectivity.

(b) When placing the BCWN components, scan the area for LOS obstructions. Envision the BCWN's radio waves as a light beam. Look for obstructions that would result in shadows in the light beam, they will most likely weaken or block the BCWN's radio waves.

4. Weather

(a) Light precipitation will reduce the range and performance of the BCWN components and wireless clients.

(b) Heavy precipitation or fog will most likely result in extremely reduced range and frequent or total loss of network connectivity.

3.4.2 Deployment Methodology

The steps detailed in this section should assist you in successfully deploying the BCWN.

1. Scan the terrain on which the BCWN will be deployed.

(a) Determine the initial distances between BreadCrumb devices.

Refer to *Troubleshooting Range User Guide* for more information.

(b) Note any LOS obstructions, and plan BreadCrumb placement to work around them.

2. Identify the PC on which BC|Commander will be run.

(a) This PC should have a wireless NIC, as you will need to carry it with you as you deploy the BCWN.

i. Alternatively, the BC|Commander PC can be stationary with one person monitoring BC|Commander while another deploys the BreadCrumbs. This method requires some form of communication (radio, cell phone, etc.) between the two persons.

3. Determine the location for the first BreadCrumb.

4. Power ON the device.
5. Wait approximately 90 seconds for the device to boot.
6. Power ON the BC|Commander PC.
7. Start BC|Commander.
8. The BC|Commander console should display the first BreadCrumb.
9. Determine the approximate location for the next BreadCrumb.
10. Proceed to the location for this BreadCrumb, observing the network in BC|Commander as you progress.
    (a) If the BreadCrumb loses network connectivity before you reach its destination, backtrack until network connectivity is restored. The point at which network connectivity for this BreadCrumb is restored is most likely the farthest point in this direction at which you will be able to place this BreadCrumb.

    (b) If you reach the destination without losing connectivity you can place it there.
        i. At this point, you may choose to proceed farther in an attempt to make optimal use of the available BreadCrumbs.

        ii. If so, proceed until network connectivity is lost and then backtrack until network connectivity is restored for this BreadCrumb. The point at which network connectivity is restored for this BreadCrumb is most likely the farthest point in this direction at which you will be able to place this BreadCrumb.
11. Repeat steps 9 and 10 for any remaining BreadCrumbs.

4 BreadCrumb JR OTA Firmware Upgrade

Each BreadCrumb relies on low-level software known as *firmware* for proper execution. Rajant periodically releases updated BreadCrumb firmware. The updated firmware must be obtained from Rajant.

For a BreadCrumb to communicate with other BreadCrumb devices or a BC|Commander client, the firmware version of the device must be compatible with the firmware versions of all other devices within the network, and with the version of BC|Commander running on the client computer.

Note For procedures to install and upgrade the BC|Commander management application, refer to the BC|Commander User Guide document.

The following steps are required to perform the Over the Air (OTA) firmware update:

1. Obtain the appropriate firmware file from Rajant for your BreadCrumb model. Save the file on a computer on which the BC|Commander management application has been installed.
2. Using BC|Commander, select a BreadCrumb from either the Table View or the Topology View. Select multiple BreadCrumbs to apply a firmware update to more than one BreadCrumb.
3. Select Upgrade Firmware from the BreadCrumb Menu. A window will appear.
4. Select Choose, and browse to the location of the firmware file.
5. Select Upload to initiate the OTA update process.

After the firmware is uploaded, it is automatically installed on the BreadCrumb JR and the unit is rebooted.

Note The OTA update can take as long as 15 to 20 minutes. While the firmware is being installed, the BreadCrumb JR will not report to BC|Commander, but will continue to forward mesh traffic.

5 Troubleshooting

5.1 Sporadic Network Connectivity

Table 3: Sporadic Network Connectivity Issues.

Problem	Resolution
As a BreadCrumb device's battery approaches exhaustion, network connectivity will become sporadic for the BreadCrumb device and its associated wireless clients.	Monitory battery usage and charge/replace batteries as necessary.
Light precipitation or fog beginning after initial deployment of the BCWN can result in sudden sporadic network connectivity for BreadCrumb devices and their associated wireless clients.	Increase the density of the network by adding more BreadCrumb devices or by moving existing BreadCrumbs closer together.
As a wireless client moves around through the coverage area, LOS to the BreadCrumb device can become obstructed resulting in sporadic network connectivity for this wireless client.	Train users to maintain LOS to known BreadCrumb device locations. Place BreadCrumb devices strategically to ensure coverage of areas through which users are expected to move.
A wireless client that moves beyond the range of the BCWN will experience sporadic, and eventually complete, loss of network connectivity.	Drop more BreadCrumb devices as necessary to increase range.
A wireless client cannot join the network.	• Ensure that BreadCrumb devices are powered on. • Ensure that the wireless card in the client device (laptop) is enabled. This is usually indicated with a blinking light on the card. • Ensure that the wireless card is in "Infrastructure" or "Access Point" mode, and not in "Ad Hoc" mode. Scan for the default ESSID "breadcrumb54-v10" (or the ESSID that you set for the network)

Problem	Resolution
	using the software accompanying your wireless card. • Ensure that the wireless client's IP address settings are configured properly. • Ensure that the security settings on the client device and BreadCrumb devices match. • Ensure that the client device is not prevented from connecting by an ACL. • Ensure that the VLAN settings for the BreadCrumb allow clients of the ESSID being used to communicate to the Local Port of the BreadCrumb. See the VLAN section of the BC|Commander manual for more information.

5.2 BreadCrumb Device Cannot Connect to BCWN

Table 4: BreadCrumb to BCWN Connectivity Issues.

Problem	Resolution
Discharged batteries can cause the BreadCrumb device to appear to power up, but not be able to establish connectivity to the BCWN.	When deploying the BCWN, ensure that the batteries are charged.
When using external antennas, faulty cable connections or crimped cables can result in difficulty establishing and maintaining network connectivity.	Check antenna cables and their connections to the BreadCrumb device.

Appendix A: Error and Warning Codes

All possible BreadCrumb error and warning codes are listed below:

JR/LX/LX3/ME3 Firmware Upgrade Codes (1*).

11 – Flash image file does not exist.

12 – Current flash image version is greater than versions of files found on USB drive.

13 – No flash image files found.

14 – Unable to mount USB drive.

15 – Unlocking of /dev/mtd0 failed.

16 – fconfig for SetFailsafeBoot failed.

17 – Unlocking of /dev/mtd0 failed.

18 – fconfig for SetMainBoot failed.

19 – Copying of zImage failed.

111 – Copying of ramdisk failed.

112 – FIS directory update of ramdisk failed.

113 – Copying of etc failed.

114 – FIS directory update of /etc failed.

115 – Copying failed.

116 – flashunbundle failed.

117 – Version information in flash file name and breadcrumb-buildinfo.conf do not match.

1171 – Platform information in flash file name and breadcrumb-buildinfo.conf do not match.

118 – Untar failed.

119 – FIS directory update of kernel failed.

120 – Failed to mount /etc.

121 – Failed to unmount /etc.

122 – In Failsafe mode, but no USB drive detected.

123 – BreadCrumb will be in failsafe mode and unable to communicate with other BreadCrumbs after next reboot.

124 – Failed to suspend bcconfigd.

125 – Failed to set boot path to next image.

126 – Failed to erase end of next file system image.

127 – Failed to copy file system image.

128 – Failed to checksum file system image.

129 – Failed to create directory for next file system image.

131 – Failed to mount next file system image.

132 – Failed to create directory for settings.

133 – Failed to copy current settings to next file system image.

134 – Failed to unmount next file system image.

141 – Error retrieving flash file.

ME2 Firmware Upgrade Codes (2*)

21 – Flash image file does not exist.

22 – Current flash image version is greater than or equal to versions of files found on the USB drive.

23 – No flash image files found.

24 – Unable to mount USB drive.

25 – Kernel corrupted.

26 – FS corrupted.

27 – Unmounting of old root file system failed.

28 – Mounting of USB drive failed.

29 – flashunbundle failed.

211 – Version information in flash file name and breadcrumb-build info.conf do not match.

212 – In Failsafe mode, but no USB drive detected.

Self-Test Codes (3*)

31 – Hardware configuration not set. Factory initialization required.

311 – Rajant factory servicing required.

32 – BreadCrumb has been zeroized.

321 – BreadCrumb is being zeroized.

33 – Radio not detected. Turn the unit off, and then back on. If the problem persist, contact technical support.

34 – Cannot read /dev/nand6 information, or cannot resize or format /dev/nand6.

36 – Hardware monitor missing.

37 – Failed to add ethernet port to bridge.

38 – Resetting radio due to error.

FIPS Codes (4*)

41 – FIPS self-tests failed.

411 – OpenSSL FIPS vector test programs not found.

412 – OpenSSL FIPS vector test hash mismatch.

413 – 802.11i AES-CCMP test vectors failed.

414 – Unable to use FIPS CCMP encryption.

415 – Kernel integrity check failed.

416 – Filesystem integrity check failed.

42 – Mixed SecNet/Non-SecNet configuration.

43 – Rekeying error.

44 – Rekeying error.

45 – Rekeying error.

46 – Rekeying error.

47 – Rekeying error.

48 – Rekeying error.

49 – Rekeying error.

431 – Rekeying error.

432 – Rekeying error.

433 – Rekeying error.

434 – Rekeying error.

435 – Rekeying error.

436 – Rekeying error.

441 – Status override CPLD feature not available (wrong CPLD version).

Fatal Codes (5*)

51 – instamesh fatal error.

52 – hostapd fatal error.

53 – cvm fatal error.

54 – madwifi fatal error.

55 – Low memory - automatic reboot scheduled.

Battery Gas Gauge Codes (6*)

61 – Battery gas gauge i2c device could not be found.

62 – Incorrect gas gauge revision 1 EEPROM settings.

63 – Incorrect gas gauge revision 2 EEPROM settings.

64 – Incorrect gas gauge revision 3 EEPROM settings.

65 – Unknown gas gauge revision.

66 – Incorrect ME3 gas gauge revision 0 EEPROM settings.

Other Codes (7*)

71 – Host flapping detected.

72 – Critical I2C failure.