BreadCrumb® Wireless Network User Guide

For the BreadCrumb® Wireless Network Release 8.4

Rajant Corporation

BreadCrumb® Wireless Network User Guide: For the BreadCrumb® Wireless Network Release 8.4
by Rajant Corporation
Copyright © 2005-2006 Rajant Corporation

Revision History

Revision 1.1 February 20, 2006

Revision 1.0 October 6, 2005

Table of Contents

List of Tables

List of Figures

Preface

Purpose and Scope

This manual provides information and guidance to all personnel who are involved with and use Rajant Corporation’s BreadCrumb® Wireless Network devices ("BreadCrumb® devices") in tactical situations.

This manual begins with an introduction to the BreadCrumb Wireless Network and a brief overview of the various BreadCrumb device models available. This is followed by a guide to BCAdmin™, the management application used to configure BreadCrumb devices before or during a deployment. Finally, common deployment scenarios are described and concise step-by-step instructions for each scenario are provided.

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.

Chapter 1. Introduction

Rajant Corporation’s (http://www.rajant.com) BreadCrumb Wireless Networks are portable, mobile, battery-powered, automatically-meshing, self-healing, full-duplex, secure, 802.11b access points. Their focus is on flexibility, adaptability, and simplicity.

The BCWN (BreadCrumb Wireless Network) is intended for rapid deployment of a broadband wireless network into a situation or "hot zone."

The BreadCrumb Wireless Network components utilize the 802.11b wireless networking standard to form a wireless mesh network. The network can be deployed as a standalone wireless network or may be connected to other networks (such as the Internet or a LAN in a Tactical Operations Center) utilizing available reachback communication links (satellite modem, DSL, cable modem, etc.).

BreadCrumb devices are available with different configurations designed for specific tasks, described in the next section.

What is a BreadCrumb?

A BreadCrumb device is an 802.11b (Wi-Fi) Access Point 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, BreadCrumb devices will perform all of the above tasks as shipped with no configuration necessary at all, providing an instant TAN - a *Tactical Area Network*. Moreover, because BreadCrumb devices use industry-standard 802.11b communications, client devices such as laptops or handheld computers require no special hardware, software, or configuration to access a BreadCrumb Wireless Network.

Mobility through Meshing

The key component to a BreadCrumb Wireless Network is a technique known as *Meshing*. While this is generally handled automatically by BreadCrumb devices, complex deployment scenarios require a basic understanding of how BreadCrumb devices establish and maintain a mesh.

Mesh - A Definition

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

The intelligence of a BreadCrumb Wireless Network 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 BreadCrumb devices can be Access Points, most Access Points do not provide any meshing capabilities. Traditional Access Points simply allow wireless devices within range to connect to a wired network; they do not extend range through other Access Points.

BreadCrumb Devices Mesh by Channel and ESSID

Two BreadCrumb devices establish a mesh link to one another when they share both a radio channel and an ESSID. The 802.11b radios used by BreadCrumb devices support 11 different channels for communication, numbered 1-11. By default, each BreadCrumb device radio is on channel 1, 8, or 11. Most BreadCrumb devices have two radios, using two of those channels.

An ESSID is essentially a name for a wireless network. By default, BreadCrumb devices use the ESSID "breadcrumb".

Example 1

Suppose you have three BreadCrumb devices, called A, B, and C. Each has two radios. BreadCrumb device 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 BreadCrumb devices are using the default ESSID of "breadcrumb". Assuming that all three BreadCrumb devices are within radio range of one another, the network will be connected like this:

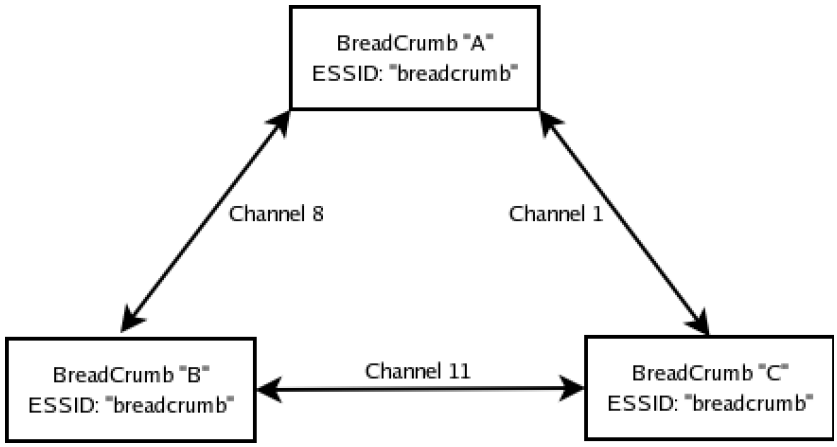

Figure 1-1. Meshing Example 1 - Full Connectivity

Example 2

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

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

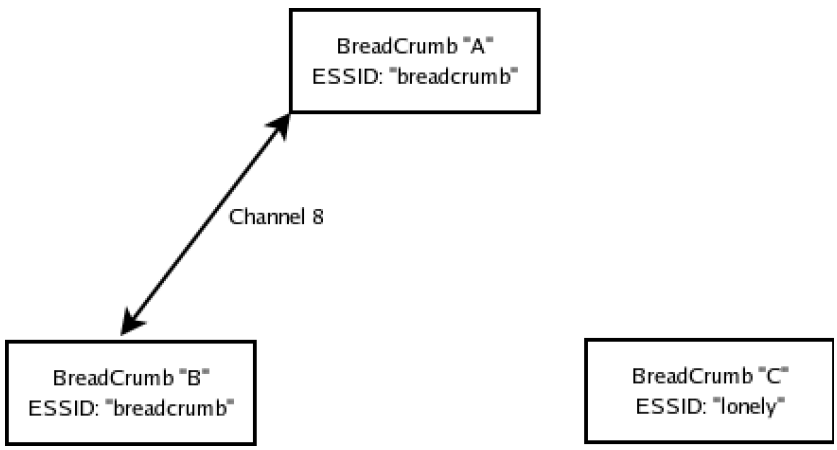

Figure 1-2. Meshing Example 2 - Different ESSIDs Prevent Meshing

Chapter 2. Upgrading to Version 8.4

This section is only necessary for BreadCrumb device/BCAdmin users of versions earlier than 8.4. If your entire BCWN is operating at version 8.4 or higher, you may safely skip this chapter.

New Features

- Fortress Technologies' AES-256 encryption is enabled, allowing Fortress encryption to be used on existing BreadCrumb devices under Rajant's new licensing terms with Fortress Technologies (http://www.fortresstech.com).

Performance / Process Improvements

- Management frames are now capable of using 11Mbps data rates, increasing overall channel bandwidth.
- Enhanced radio frame fragmentation process.

Issues Resolved

- A compatibility issue with the latest version of Java® has been resolved. (The problem manifested as the inability to open a BreadCrumb Properties window).
- Fixed Fortress-Only Mode to work correctly over meshed connections.
- Mesh-transmit timeout condition resets the radio cards, enhancing mesh healing capabilities.
- Radio cards default to "primary antenna only."
- Several minor bugs corrected in the radio driver.

Known Issues

- Signal strength number in BCAdmin is not translated into dBm.
- It is recommended that the mesh feature NOT be disabled. A radio interface with mesh disabled incorrectly displays a connection in BCAdmin even though no link exists.

- Selection of a unique ESSID (network name) for the BreadCrumb network is recommended. A BreadCrumb device equipped with tri-color LED incorrectly indicates a meshed connection (GREEN) when in the presence of an 802.11b access point with the same ESSID.

Installing / Upgrading BCAdmin

1. Install the latest JRE from http://www.java.com
2. Download version 8.4 of BCAdmin for Windows or Linux using the link provided by your Rajant Account Manager.
3. Run the installer (for Windows) or install the rpm (for Linux) and follow any instructions provided on your screen.

Upgrading BreadCrumb Firmware

Follow the following procedure for each BreadCrumb device in your network. Be sure to determine each BreadCrumb board version (step 1) individually.

1. Determine the BreadCrumb board version (version 2 or version 3) as follows:

   - In version 2 units, the power input (where the power wires plug in) are in a straight line, as below:

Figure 2-1. Version 2 Power Input

   - Version 3 units have the power configuration as below:

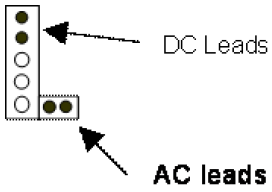

Figure 2-2. Version 3 Power Input

2. Download the correct firmware zip archive for the board determined in the previous step, using the link provided by your Rajant Account Manager.
3. Create a new, empty folder and unzip the archive into it.
4. Copy the unzipped files (and *only* those files) onto an empty (no pre-existing files) ATA Flash Memory Card (of at least 16MB). The flash card may be directly purchased from http://www.magicram.com/flshcrd.htm
5. Proceed with the flash instructions below.

Flash Update Procedure for Version 2 and Version 3 Systems

Note: BreadCrumb Wireless Network-specific parameters, like *name* and *location*, are reset to their default values after the upgrade. The user should record these and other parameters to reload into the BreadCrumb devices after the software installation procedure is completed.

1. Turn OFF power to the BreadCrumb.
2. Remove the top PCMCIA card, *leaving one radio card still installed in the bottom slot*.
   - In dual-radio BreadCrumb products, remove the top radio card.
   - In single-radio BreadCrumb products, move the radio to the bottom slot.
   - Plug the flash card, white label side up, into the top slot.
   - Turn unit ON and observe the amber light ON on the radio card. (The green light sometimes goes ON, sometimes not.)
   - Wait for the amber light to go out.
   - TURN THE POWER OFF to the BreadCrumb.
   - Remove the flash card, and replace the radio(s) to their original positions.
   - Power the unit back ON.

- Allow the BreadCrumb to operate *FOR NO LESS THAN 5 MINUTES* before rebooting or turning OFF.

Important: After a flash update, you should ensure that at least one client device has the new BCAdmin installed, is "permitted" in the device's ACL list, and is designated as an administrator. Important settings that were lost in the flash may be re-keyed, but do not reboot the BreadCrumb device until it has run for at least five minutes after its initial power-up after flash.

Rebooting before the end of the five-minute "bake period" can result in a faulty flash update, requiring the flash operation to be performed again.

Chapter 3. Models

The following table summarizes the differences between the BreadCrumb models available. Each model is described in greater detail later in this chapter.

	ME	WE	SE	XL	XLV	XLE
Usage	Weight/ size-sensitive deployments (UAVs, etc.)	Worn by mobile individual	Placed as necessary, short/ medium range use	Placed as necessary, long range use	Vehicle-mounted, long-range use	Placed as necessary, incl. vehicle mount, contains embedded MPEG video encoder, long-range use
Dimensions	6" x 3.75" x 7.5"	7.25" x 4.75" x 2.5"	8.25" x 6.5" x 3.5"	9" x 6.5" x 4"	9" x 6.5" x 4"	12" x 12" x 2.5"
Weight	1.5lbs	3.9lbs (incl. battery)	2.5lbs	9.7lbs	12.0lbs	14.0lbs
Number of Radios	1 (2 optional)	1	2	2	2	2
Ethernet	Yes (via RJ-45 dongle)	Yes	Yes	Yes	Yes	Yes
Input Power	6-15VDC	6-15VDC	6-15VDC	9-15VDC	6-40VDC (4-amp start)	6-40VDC (4-amp start)
RF Output Power (no antenna gain)	23dBm/ channel +-2dBm	25dBm/ channel +-2dBm	23dBm/ channel +-2dBm	27dBm/ channel +-2dBm	27dBm/ channel +-2dBm	27dBm/ channel +-2dBm

	ME	WE	SE	XL	XLV	XLE
Security	256-bit AES FIPS 140-2 using embedded AirFortress Client; Access Control Lists; WEP; Third-party VPNs	256-bit AES FIPS 140-2 using embedded AirFortress Client; Access Control Lists; WEP; Third-party VPNs	256-bit AES FIPS 140-2 using embedded AirFortress Client; Access Control Lists; WEP; Third-party VPNs; Type 1 encryption with Harris SecNet11	256-bit AES FIPS 140-2 using embedded AirFortress Client; Access Control Lists; WEP; Third-party VPNs; Type 1 encryption with Harris SecNet11	256-bit AES FIPS 140-2 using embedded AirFortress Client; Access Control Lists; WEP; Third-party VPNs; Type 1 encryption with Harris SecNet11	256-bit AES FIPS 140-2 using embedded AirFortress Client; Access Control Lists; WEP; Third-party VPNs; Type 1 encryption with Harris SecNet11
Harris SecNet11 Support	No	No	Yes (waiver required)	Yes (waiver required)	Yes (waiver required)	No
Integrated Antennas	None	5dBi omnidi-rectional	4x2dBi dipole	None	None	None
External Antenna Connectors	SMA (F)	None	1xfemale N-type (optional, connected to one radio only)	1xfemale N-type (radios combined internally)	1xfemale N-type (radios combined internally)	1xfemale N-type (radios combined internally)
Managed Networking Features	Bridging, Gateway, DHCP, NAT, Port Forwarding	Bridging, Gateway, DHCP, NAT, Port Forwarding	Bridging, Gateway, DHCP, NAT, Port Forwarding	Bridging, Gateway, DHCP, NAT, Port Forwarding	Bridging, Gateway, DHCP, NAT, Port Forwarding	Bridging, Gateway, DHCP, NAT, Port Forwarding

Table 3-1. Available BreadCrumb Models

Note: A BreadCrumb Wireless Network can include any combination of these models.

BreadCrumb ME

The BreadCrumb ME is the smallest and lightest BreadCrumb device offered, making it ideal for deployments with strict size and/or weight constraints. The BreadCrumb ME only contains one radio by default (a second radio is available as an option). Our customers have installed BreadCrumb MEs:

- On UAVs
- In portable sensor packages

> **Important:** In a BCWN containing single-radio BreadCrumb devices, all BreadCrumb devices to which the single-radio BreadCrumb device communicates must have one radio on the same channel as the single-radio BreadCrumb device.

External Connectors

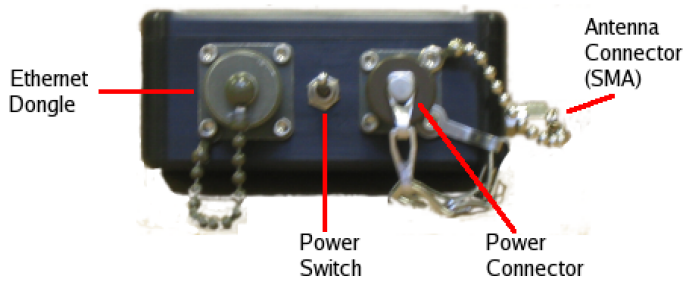

Figure 3-1. BreadCrumb ME - External Connectors

BreadCrumb WE

The BreadCrumb WE is functionally identical to a 1-radio BreadCrumb ME, with a higher-gain antenna, integrated battery, and a case more suited to attach to worn gear. Individuals wearing a BreadCrumb WE automatically extend a BCWN wherever they go, provided that they remain within range of at least one other BreadCrumb device.

> **Important:** In a BCWN containing single-radio BreadCrumb devices, all BreadCrumb devices to which the single-radio BreadCrumb device communicates must have one radio on the same channel as the single-radio BreadCrumb device.

External Connectors

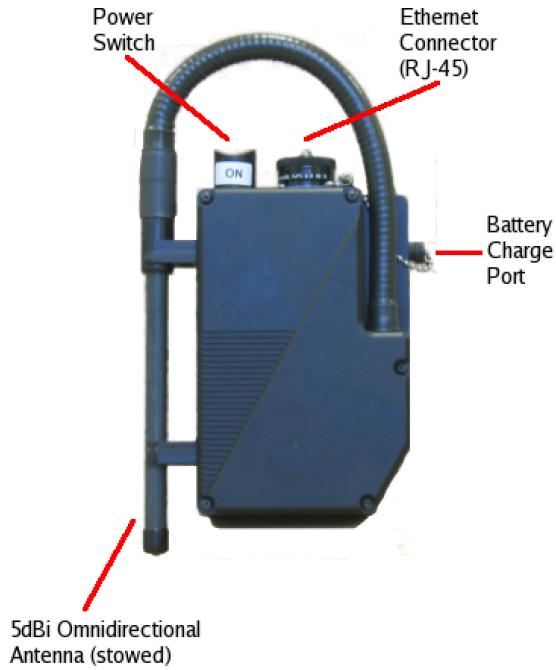

Figure 3-2. BreadCrumb WE - External Connectors

BreadCrumb SE

The BreadCrumb SE is the basic building block of most BCWN networks. Its two radios and ethernet interface enable the full suite of BreadCrumb features (with the exception of long range and integrated video encoder), while its size allows it to be easily transported to and placed wherever necessary. BreadCrumb SEs have been rapidly deployed:

- On rooftops
- In trees or bushes
- Hung from balloons
- In stairwells
- On fences and observation towers
- In shipyards

External Connectors

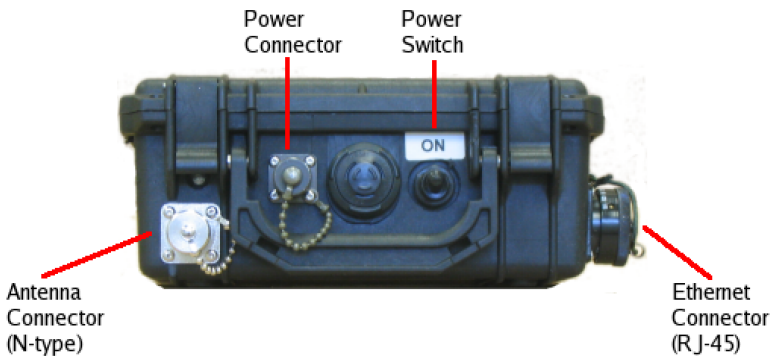

Figure 3-3. BreadCrumb SE - External Connectors

BreadCrumb XL

The BreadCrumb XL is a long-range model, capable of 11Mb communications at distances of 7 miles (11.2km) or more, and lower-speed communications at even greater range. BreadCrumb XLs have been rapidly deployed:

- In Air Traffic Control towers
- On mountaintops
- On ships

> **Important:** The range-extending circuitry within a BreadCrumb XL is permanently tuned to 802.11b channels 1 and 11. Changing these settings may prevent your network from operating properly.

External Connectors

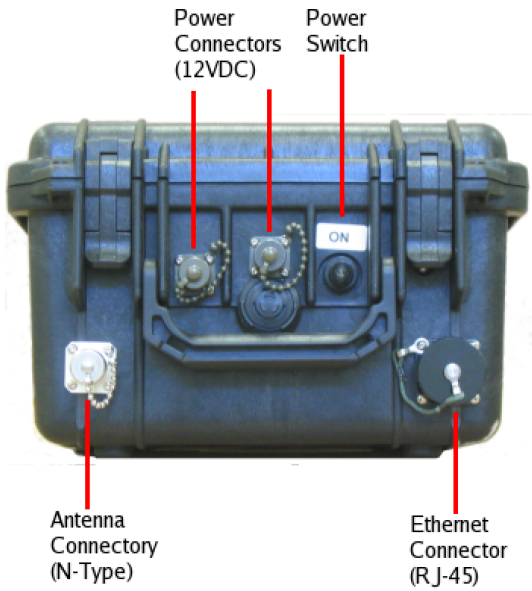

Figure 3-4. BreadCrumb XL - External Connector

BreadCrumb XLV

The BreadCrumb XLV is identical to the BreadCrumb XL, with the exception that it also accepts unfiltered vehicle power (6-40VDC) as a power source. This allows long-range communication within and among vehicle convoys and bases, and enables the bridging of widely spread networks by vehicles. BreadCrumb XLVs have been rapidly deployed:

- In HMMWVs
- In Bradley Fighting Vehicles
- In trucks

External Connectors

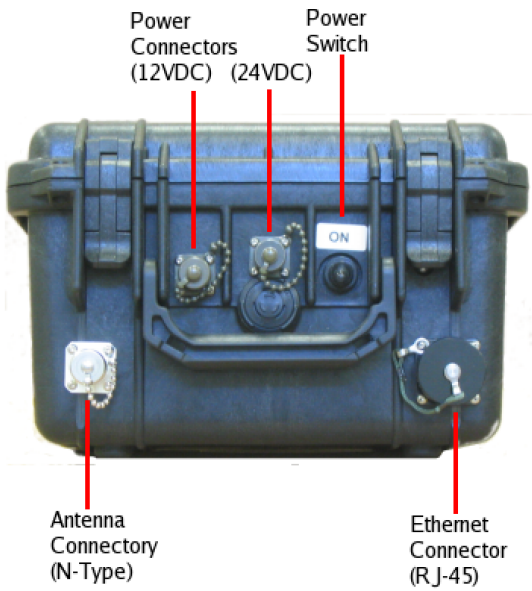

Figure 3-5. BreadCrumb XLV - External Connectors

BreadCrumb XLE

The BreadCrumb XLE further builds upon the BreadCrumb XLV by including an MPEG video encoder and an external BNC video connector. A composite video source can be connected to the BreadCrumb XLE and its video stream will be available to other devices on the BCWN. BreadCrumb XLEs have been rapidly deployed to provide video from:

- Security cameras
- LRASSS (Long-Range Advanced Scout Surveillance System)

External Connectors

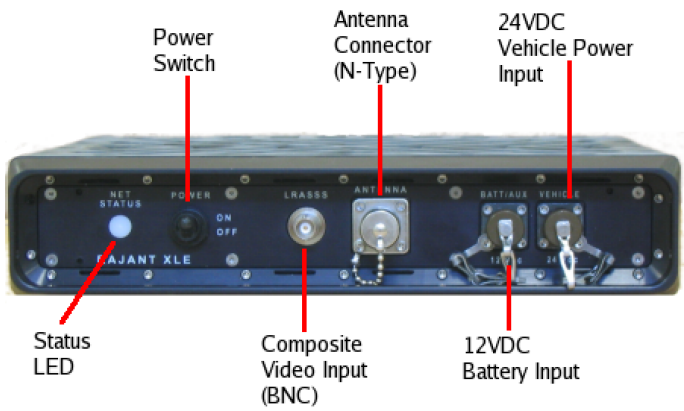

Figure 3-6. BreadCrumb XLE - External Connectors (front)

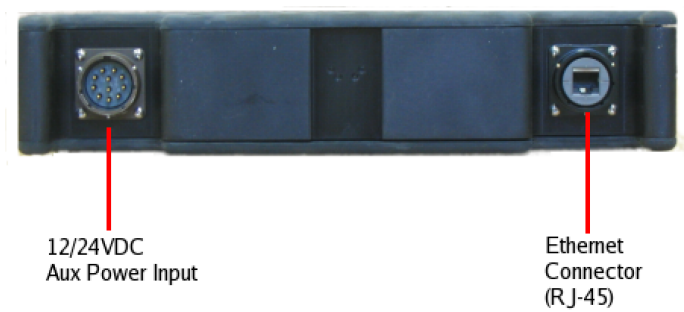

Figure 3-7. BreadCrumb XLE - External Connectors (back)

Chapter 4. Deployment Considerations

Addressing

When routing to another network 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.

> **Important:** Any devices running the BCAdmin management application *must* have an address in the 10.0.0.0/8 range. This may be in addition to other addresses the devices may have configured.

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 BCAdmin. Note that BreadCrumb devices with two radios will have two such addresses.

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:

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

Channel Assignments

By default, BreadCrumb devices choose their radio channels automatically upon startup. Combinations of channels 1, 8, and 11 are automatically chosen using a process designed to provide a robust mesh.

In some cases, however, it is necessary to manually set the radios to specific channels as described below.

Channel Assignment for Single-Radio BreadCrumb Devices (ME and WE)

Single-radio BreadCrumb devices (models ME and WE) present a challenge for deployments in which those BreadCrumb devices are needed to provide critical links within a mesh. For these deployments, it is imperative that any BreadCrumb devices with which the ME or WE is to mesh have a channel in common with the ME or WE.

The upshot of this is that the ME/WE and its intended peers should have their radio channels set manually in order to ensure common channels.

Channel Assignment for Long-Range BreadCrumb Devices (XL, XLV, XLE)

Long-range BreadCrumb devices include additional circuitry that is permanently tuned to 802.11b channels 1 and 11. For these BreadCrumb devices, *radio 1 must always be set to channel 1 and radio 2 must always be set to channel 11*.

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.

802.11b wireless operation degrades gracefully 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.

Line Of Sight

Unobstructed LOS is critical for optimal performance of the BCWN. Partial LOS obstructions 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 travel over possible obstructions. In an open area, at least two meters (six feet) of antenna elevation are recommended.

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.

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 that are placed too far away or in RF "shadows" may experience total loss of connection.

Device power is important in determining distances over which the device will be effective.

The following table can be used as a guide to determine best-case distances between devices with regard to their power:

Device (power)	To Device (power)	Distance * [1]
BreadCrumb device (200mW) with external antenna	BreadCrumb device (200mW) with external antenna	Up to 5km (3.1 miles)
BreadCrumb device (200mW) with external antenna	BreadCrumb device (1W)	Up to 10km (6.2 miles)
BreadCrumb device (1W)	BreadCrumb device (1W)	Up to 15km (9.3 miles)

Notes:

a. These distances are representative of optimal deployment settings:

- Optimal antenna selection
- Clear, unobstructed LOS between devices
- Absence of other RF interference
- Full battery power
- Clear weather

Table 4-1. Best-Case Distances by Radio Power

> **Tip:** It is recommended when deploying a BCWN that you choose initial distances between devices that are half the distance as quoted in Table 4-1.

When placing a BreadCrumb device, check the connection status to the nearest available device using either the BreadCrumb device’s status LED (described in Appendix A), or BCAdmin (described in Chapter 5). 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 7.

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 a 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, reducing the coverage area.

Interference

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

- Other BreadCrumb devices placed too closely together
- Other RF devices such as microwave devices, cordless phone base stations, radio transmitters, other wireless networks, jamming devices, etc.
- Reflections from metal surfaces such as fences and buildings, causing multipath interference

> **Important:** Plan the BCWN to minimize the effects of RF interference!

Altitude

The placement of a BreadCrumb devices has a major impact on its 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 increases the effective range. Rajant recommends elevating the components of a BCWN a minimum of two meters (six feet) above the surrounding surface.

Chapter 5. Using BCAdmin™

> **Note:** Some portions of this section 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.

BCAdmin is an application allowing an administrator to perform several tasks on a BreadCrumb Wireless Network, including:

- Monitor its status
- Configure network-wide settings
- Configure individual BreadCrumb devices
- Graphically view the BCWN topology in real time

BCAdmin typically runs on a laptop PC, but it can be run on any PC that has access to the entire BCWN. Versions are available for Microsoft Windows® or Linux.

Screen Layout

When BCAdmin is launched the screen will initially look like this:

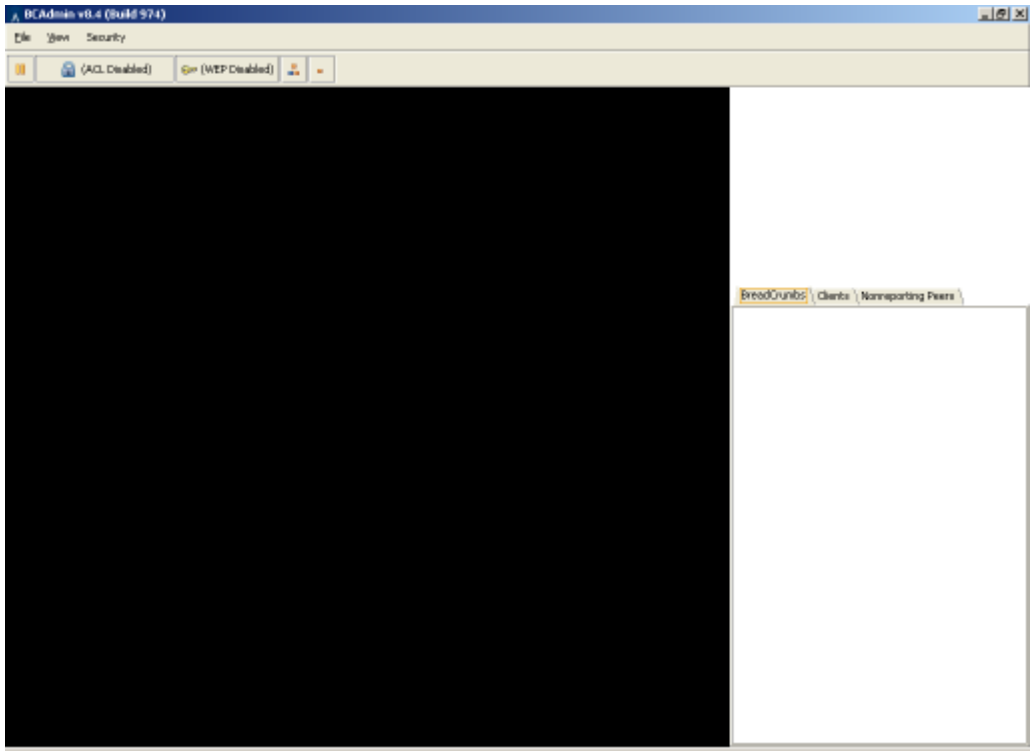

Figure 5-1. BCAdmin Screen at Startup (No Network)

The large area on the left is the Topology Area, showing the current shape of the network at any given time. The Info Area to the right shows detailed information for BreadCrumb devices, client devices, and wireless links.

> **Note:** If your BCAdmin workstation does not have a network address in the 10.0.0.0/8 range, the large black area will instead be red until you obtain such an address. A red Topology Area indicates that no communication with BreadCrumb devices is possible (perhaps because no BreadCrumb devices are turned on, or the workstation has not associated with any).

When BCAdmin is able to communicate to a BCWN, the network topology is shown in the Topology Area, as below (your network will look different).

Topology Area

The Topology Area shows the topology (logical shape) of your network as it changes. BreadCrumb devices and client devices (laptops, etc.) are shown graphically, as well as the links between them.

> **Important:** The Topology Area shows the *logical* layout of your network, not the physical layout. While there may be some correlation between the picture you see and the physical locations of your BreadCrumb devices and client devices, *physical locations are not represented in this diagram*.

Tip: BCAdmin makes an effort to layout the Topology Area in an easily readable way, with a minimum of line intersections and superimposed boxes. Sometimes, however, the screen can get cluttered. BCAdmin provides two features to help cope with this, which may be used in combination:

- A `Play/Pause` button in the toolbar below the `File` menu allows you to enable/disable continuous layout, effectively allowing you to "lock" BreadCrumb devices in place.
- BreadCrumb device and client device icons can be dragged to desired positions in the Topology Area using the mouse.

The larger blocks in the Topology Area represent BreadCrumb devices. The smaller blocks with blue outlines represent client devices.

Detailed information for a BreadCrumb device can be viewed in the Info Area by selecting the BreadCrumb device in the Topology Area. To select a BreadCrumb device, single-click it with your mouse. The selected BreadCrumb device will be highlighted with a dashed border. A description of the detailed information is provided later in this chapter.

Anatomy of the BreadCrumb Box

The following figure shows a close-up image of a BreadCrumb device as represented on the BCAdmin Topology Area.

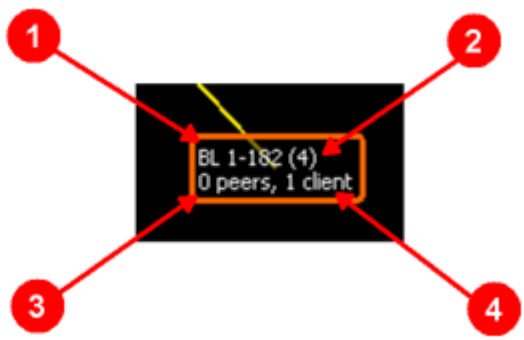

Figure 5-2. The BreadCrumb Box

1. *BreadCrumb Device Name*

   The BreadCrumb device's name is displayed in the upper-left area of the BreadCrumb Box. The name is assigned by an administrator using the process described in the Section called *Configuring*

Individual BreadCrumbs. This allows the administrator to distinguish between multiple BreadCrumb devices in a BCWN.

If the BreadCrumb device has no name assigned, its ID is used. The ID is a unique, alphanumeric, non-editable string used internally by the BreadCrumb device.

2. *Time Since Last Update*

   Each BreadCrumb device sends periodic information updates to BCAdmin, in intervals ranging from about 5 seconds to about 20 seconds. This number shows how long it has been, in seconds, since BCAdmin last heard from this BreadCrumb device.

   By default, BCAdmin will color the BreadCrumb Box red and make a sound if a BreadCrumb device has not sent an update for 60 seconds. This may simply be because a BreadCrumb device has been switched off, or its battery as died, or it may indicate a problem with the network, its deployment, the local radio environment, or other factors.

3. *Number of Peers*

   A *peer* is simply another BreadCrumb device to which a BreadCrumb device has meshed. Data packets are automatically routed through peers as necessary by the BreadCrumb devices.

4. *Number of Clients*

   A client is any 802.11b device that has associated with a BreadCrumb device's access point. Laptops, handheld computers, cameras, VOIP+Wi-Fi phones, etc. are examples of client devices.

Tip: The amount of information displayed for each BreadCrumb device can be changed by right-clicking on a BreadCrumb device and choosing `Show More Detail` or `Show Less Detail`. The detail level for the entire network can be changed via the `View Menu` at the top of the window. The above figure shows BCAdmin's the default level of detail.

Anatomy of the Client Box

Client devices are represented in the Topology Area by a blue box containing the client device's MAC address, as pictured below.

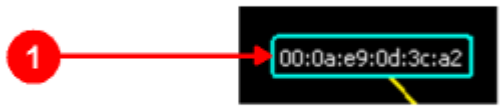

Figure 5-3. The Client Box

1. Client MAC Address/Nickname

   The MAC address or administrator-set nickname of the client device.

> **Tip:** An administrator can set nicknames for each client device. These nicknames are then displayed in the Topology Area instead of the MAC address. To set a nickname, right-click on the client device and choose `Set Client Nickname`.

Anatomy of a Connection Line

If your BCWN has more than one BreadCrumb device, your Topology Area probably includes several lines connecting BreadCrumb boxes to clients and to one another. The color, style, and direction of motion (if any) of a line indicates its channel, speed, and direction as follows:

802.11b Channel	Line Color
1	Yellow
2	Red
3	Red
4	Red
5	Red
6	Red
7	Red
8	Green
9	Red
10	Red

802.11b Channel	Line Color
11	Purple

Table 5-1. BCAdmin Line Colors Legend

Link Speed (Mbps)	Line Style
11	Solid
5.5	Dashed
2	Dot-Dash
1	Dotted

Table 5-2. BCAdmin Line Styles Legend

Asymmetric Connections

For a variety of environmental reasons (antenna placement, radio reflections, interference, etc.), asymmetric connections are sometimes formed between BreadCrumb devices. An asymmetric connection is a connection between two BreadCrumb devices in which each BreadCrumb device is transmitting at a different speed.

When an asymmetric connection is made, the BCAdmin operator will see two lines of the same color connecting two BreadCrumb devices. The speeds will be represented in the line styles as specified in the BCAdmin Line Styles Legend in the previous section. Transmission direction of each link is represented by motion of the dots or dashes comprising the lines. (11Mbps links are solid lines, so their direction in an asymmetric link is determined by elimination; its direction is simply the direction opposite the other link of the same color). The following figure illustrates an asymmetric link:

Figure 5-4. Asymmetric Connection Example

Redundant Connections

When two BreadCrumb devices have two radio channels in common, they often form redundant links between one another - that is, one connection on each channel. In these cases, lines of different colors will connect the two BreadCrumb boxes as in the following figure:

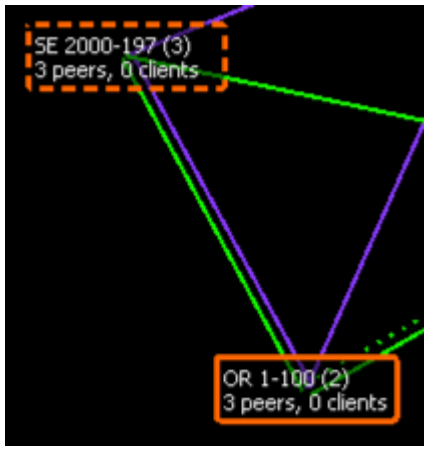

Figure 5-5. Redundant Connection Example

Info Area

The Info Area shows detailed information specific to the currently selected BreadCrumb device, if any. To select a BreadCrumb device in the Topology Area, single-click it with your mouse. The selected BreadCrumb device will be highlighted with a dashed border.

The top portion of the Info Area shows a summary of the selected BreadCrumb device's configuration as pictured below:

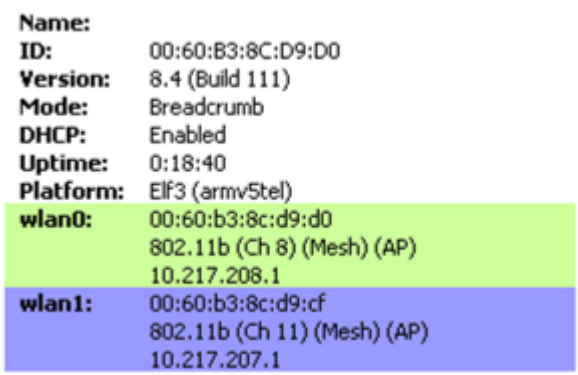

Figure 5-6. BreadCrumb Summary Panel

In this example, you can see that the selected BreadCrumb device is running version 8.4 of the BreadCrumb firmware, and has been running for a little over 18 minutes. It has two radios, on channels 8 and 11, both of which are participating in the mesh and serving as access points. You can also see the two IPv4 addresses assigned to the radio cards, 10.217.208.1 and 10.217.207.1.

The bottom portion of the Info Area contains three tabs, each of which contains a list of connections (if any). The BreadCrumbs tab shows connections to other BreadCrumb devices, the Clients tab shows connections with client devices, and the Pending Peers tab shows connections with other BreadCrumb devices that have not yet reported to BCAdmin (e.g., have just been turned on and are not yet fully booted, or are only reachable via an extremely poor link).

The same information is available in each list. The following figure shows an example listing of BreadCrumb connections.

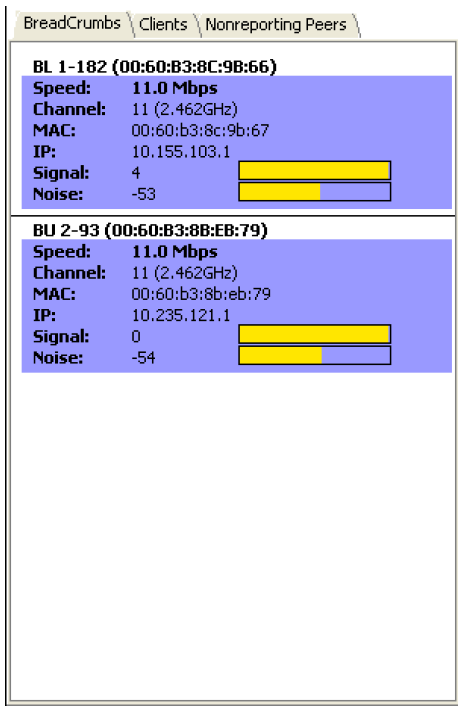

Figure 5-7. Link Detail Tabs

> **Tip:** Hover your mouse over the connection detail in the Info Area to highlight the corresponding line in the Topology Area.

Configuring Individual BreadCrumbs

To configure a specific BreadCrumb device, right-click on the BreadCrumb device in the Topology Area and choose `Properties...`. A window will appear via which the BreadCrumb device can be

configured, with configuration options grouped by tabs into multiple categories. Each tab and its settings are described in this section.

General Settings

The "General" tab contains controls for configuring several simple system-wide settings:

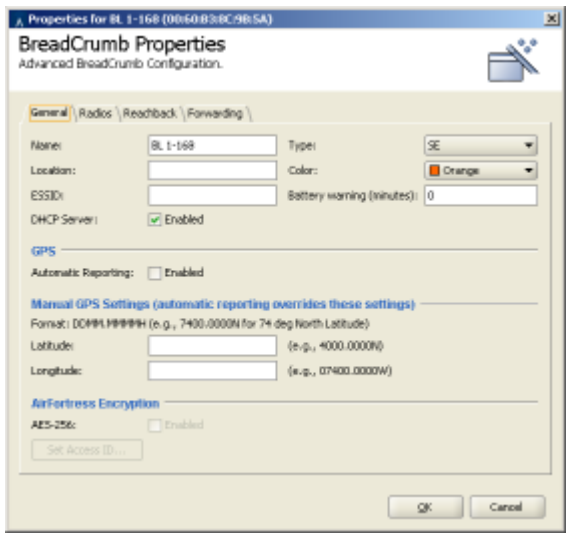

Figure 5-8. BreadCrumb Properties - General Tab

The available settings are:

1. *Name*

   This is a descriptive name used only for identification of the BreadCrumb device within BCAdmin. Any changes to this name are immediately reflected on the screens of other BCAdmin users.

2. *Type*

   This allows the administrator to note the type (model) of BreadCrumb. This is for administrator convenience only and is ignored by BCAdmin.

3. *Location*

   The Location field, if set, is displayed in the BreadCrumb box. It is not automatically updated by GPS or other means; it is rather a place for administrators to put a short description of the BreadCrumb device's location for administrative convenience. For example, "rooftop," "commander's vehicle," etc.

4. *Color*

   This field controls the color of the BreadCrumb box as drawn by BCAdmin. This can be used to reflect the actual color of the BreadCrumb or to represent any other information administrators see fit.

5. *ESSID*

   The ESSID is the name of the network provided by the BreadCrumb device's internal Access Point(s) and used for meshing purposes. When left blank, the default "breadcrumb" is used.

6. *Battery Warning (minutes)*

   Each BreadCrumb device includes a battery timer that monitors run time. When batteries are changed, the battery timer should be reset (by right-clicking on the BreadCrumb box and choosing `Diagnostics and Maintenance`, then `Reset Battery Timer`). When the value set in this field is reached, a visible warning is shown in the Topology Area alerting administrators that a battery must be changed.

7. *DHCP Server*

   Each BreadCrumb device provides an internal DHCP server (see the Section called *DHCP* in Chapter 4 for a description of its addressing scheme). When this checkbox is checked, the DHCP server will run.

8. *GPS: Automatic Reporting*

   For BreadCrumb devices equipped with GPS receivers, this enables their reporting of their coordinates to BCAdmin (and subsequently to a mapping server; see the Section called *Mapping with Fugawi Tracker*).

9. *Manual GPS Settings: Latitude and Longitude*

   For non-GPS-equipped BreadCrumb devices, an administrator may manually enter latitude and longitude coordinates which will be relayed to a mapping application (see the Section called *Mapping with Fugawi Tracker*).

10. *AirFortress Encryption: AES-256 and Set Access ID*

    When this checkbox is checked, the BreadCrumb will enable AirFortress encryption (see the Section called *AES-256 Encryption with AirFortress* for details).

Radio Settings

The "Radios" tab contains controls for configuring each of the BreadCrumb device's 802.11b radio radios:

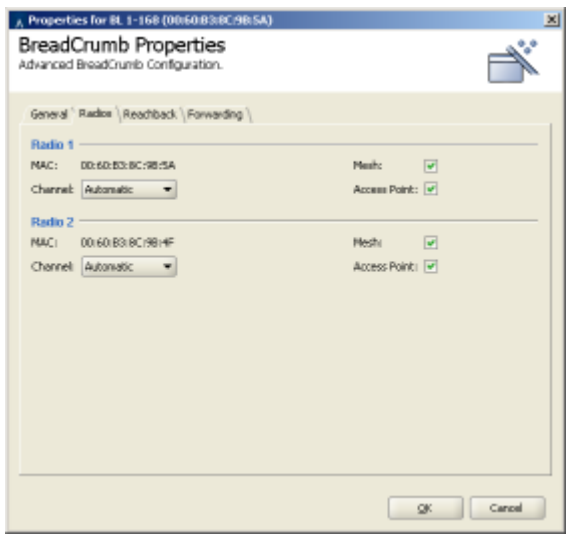

Figure 5-9. BreadCrumb Properties - Radios Tab

The available settings for each radio are:

1. *Channel*

   Channel selection may be automatic as described in the Section called *Channel Assignments* in Chapter 4, or radios may be fixed to specific channels. If one radio is set to use automatic channel selection, so must all of a BreadCrumb device's other radios.

   > **Important:** If you are configuring an XL, XLV, or XLE, the radios *must* be set to channels 1 and 11, respectively!

2. *Mesh*

   If this checkbox is checked, the radio will participate in the BreadCrumb mesh.

3. *Access Point*

   If this checkbox is checked, the radio will provide 802.11b Access Point functionality.

Note: BCAdmin will not allow you disable all of the checkboxes on this tab.

Reachback Settings

The "Reachback" tab contains controls for configuring the BreadCrumb device's interconnection with other networks, both wired and wireless:

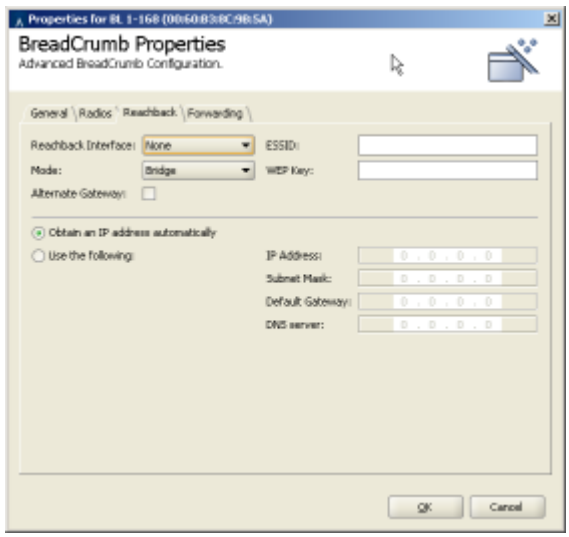

Figure 5-10. BreadCrumb Properties - Reachback Tab

The available settings are:

1. *Reachback Interface*

   This dropdown selects the network interface on the BreadCrumb device that will connect to the other network. Available options are (depending upon the BreadCrumb model and options):

   a. *None*

      Disables reachback.

   b. *Ethernet*

      Reachback will be configured to use the BreadCrumb device's ethernet port (if any).

Note: The type of ethernet cable required depends upon the device to which you are connecting. If the BreadCrumb device's ethernet port is to be connected to a hub or a switch, a conventional ethernet patch cable ("straight-through") should be used. If the BreadCrumb device's ethernet port is to be connected directly to a device such as laptop or camera, a crossover cable should be used. Using the wrong cable will result in no connectivity.

c. *Radio 2*

Reachback will be configured to use the BreadCrumb device's second radio (if any).

d. *Radio 2 (ad hoc)*

Reachback will be configured to use the BreadCrumb device's second radio (if any) in 802.11b ad hoc mode.

2. *Mode*

This dropdown selects the type of reachback to configure. Available options are:

a. *Automatic*

In Automatic Mode, the interface attempts to obtain an IPv4 address using DHCP. If it obtains an address, reachback is configured to use Gateway Mode; if it does not, reachback is configured to use Bridge Mode.

b. *Bridge*

In Bridge Mode, the reachback interface is configured to exist on the same network as the BreadCrumb device's other interfaces. Packets are forwarded into or out of the BCWN through this interface as necessary.

c. *Gateway*

In Gateway Mode, the reachback interface is configured to exist on a different network than the BreadCrumb device's other interfaces. Outbound NAT is configured so that any BCWN traffic destined for the reachback network appears to originate from the reachback interface. Any inbound traffic from the reachback network must be sent through a forwarded port (see the Section called *Forwarding Settings*)

Unless the Alternate Gateway checkbox is checked (see below) the BreadCrumb will assign itself the additional IPv4 address of 10.0.0.1.

d. *Gateway (Ingress)*

In Gateway (Ingress) Mode, as in Gateway mode, the reachback interface is configured to exist on a different network than the BreadCrumb device's other interfaces. NAT, however, is configured in the direction opposite to that of Gateway Mode. Inbound traffic from the reachback network appears to originate from the BreadCrumb, and outbound traffic from the BCWN must be sent through a forwarded port (see the Section called *Forwarding Settings* for details)

e. *Disabled*

Disables reachback regardless of the selected interface.

3. *Alternate Gateway*

If the BreadCrumb is in Gateway Mode and this checkbox is *not* checked, the BreadCrumb device is considered a "Primary Gateway" and assigns itself the additional address of 10.0.0.1 (the gateway address provided by the BreadCrumb DHCP servers). There may be at most one Primary Gateway in a BCWN.

Alternate Gateways do not assign themselves the 10.0.0.1 address, and provide their own addresses as a gateway to their own DHCP clients.

Tip: If you are running a BCWN with multiple gateways, disable DHCP on all non-gateway BreadCrumb devices for a simple form of load-balancing.

4. *ESSID*

For reachback using the "Radio 2" or "Radio 2 (ad hoc)" interfaces, this is the ESSID to which the BreadCrumb device will attempt to connect.

5. *WEP Key*

For reachback using the "Radio 2" or "Radio 2 (ad hoc)" interfaces, this is the WEP key that will be used for the reachback connection. If a WEP key is not required for wireless reachback, leave this field blank.

6. *IP Address Configuration*

If "Obtain an IP Address Automatically" is selected for a Gateway Mode, the BreadCrumb device will obtain its IPv4 address on its reachback interface using DHCP.

If "Use the Following:" is selected for a Gateway Mode, the following must be set manually:

a. IP Address

b. Subnet Mask

c. Default Gateway

d. DNS Server

You may need to contact your network administrator in order to determine the correct settings.

Forwarding Settings

The "Forwarding" tab contains controls for configuring inbound NAT translation for BreadCrumb devices configured as gateways.

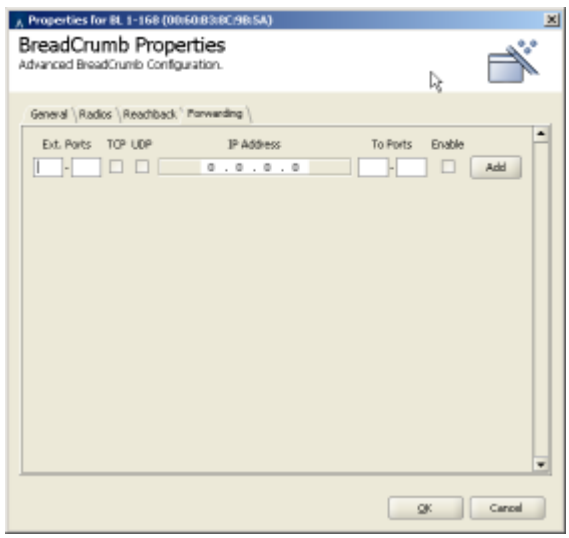

Figure 5-11. BreadCrumb Properties - Forwarding Tab

To forward traffic through a BreadCrumb device in Gateway Mode or Gateway (Ingress) mode, you must know:

- The IPv4 port(s) used by the forwarded traffic (e.g., 25 for SMTP, 80 for HTTP, etc.).
- The TCP protocol(s) used by the forwarded traffic (TCP and/or UDP).
- The IPv4 address to which the forwarded traffic is to be forwarded.
- The IPv4 port(s) at the destination address to which the forwarded traffic is to be forwarded (usually the same as the ports described above).

The checkbox marked "Enable" specifies whether a particular forward configuration is active. This allows an administrator to pre-configure port forwards and selectively enable or disable them in the future.

When a port forward has been configured, click the "Add" button to the right in order to add it to the current configuration.

You may add as many port forwards as necessary to a BreadCrumb.

Example: Port Forwarding Configuration for a Web Server

Suppose a web server exists somewhere within a BCWN, and one of the BCWN BreadCrumb devices is serving as a Gateway connected to the Internet. In order to allow users on the Internet to access the web server, the following port forward configuration is required:

1. Ext. Ports

   We will allow Internet users to access the internal web server using port 80, the default for web traffic. The external port range is therefore 80-80.

2. Protocol

   Web traffic uses TCP, not UDP, so only the TCP checkbox should be checked.

3. IP Address

   This is the IP address of the web server on the BCWN. Note that this should be a fixed IP address, as addresses obtained via DHCP can change over time and thereby cause the port forwarding to fail.

4. To Ports

   The web server on the BCWN is listening for connections on port 80, so the port range should be 80-80.

Once this port forward is enabled and saved to the BreadCrumb, Internet users may direct their web browsers to the *Gateway BreadCrumb device's external IP address* in order to reach the web server on the BCWN.

Security

Several levels of security are available for the BreadCrumb Wireless Network, which may be used individually or in combination with one another. We are constantly adding security features, so please contact your Rajant Account Representative if you have specific needs not included in this section.

WEP

WEP (Wired Equivalency Protocol) was the first scheme to provide security for 802.11 communications. Although since its release it has been determined to contain serious weaknesses, WEP remains an effective means to prevent casual eavesdropping.

WEP settings are made network-wide; all BreadCrumb devices and wireless clients must agree on a WEP key in order to establish and maintain communications.

To enable WEP on a BCWN, make sure that all of the BreadCrumbs to configure are visible in BCAdmin. Then choose `Security`, then `WEP Settings` to display the following window:

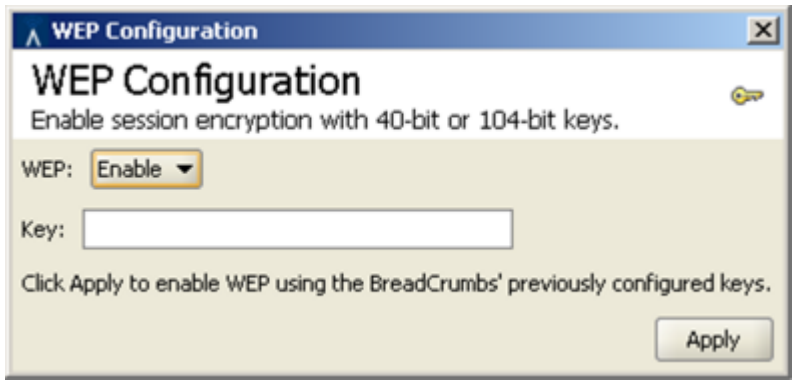

Figure 5-12. WEP Configuration Window

1. *WEP*

   This dropdown allows the administrator to enable or disable WEP on all BreadCrumb devices currently visible in BCAdmin.

2. *Key*

   A 40-bit or 104-bit hexadecimal key is specified in this field. If this field is left blank, WEP can be enabled using a previously configured key.

Access Control Lists (ACLs)

A BCWN may be configured with a network-wide Access Control List (ACL) to specify a list of devices to allow or disallow on the network. Each device communicating on the network (e.g., each BreadCrumb radio or laptop radio card) has a unique identifier known as a MAC address. ACLs consist of lists of these addresses to specify permitted or forbidden devices.

When enabled, the ACL may be in two modes: Deny by Default and Allow by Default. In Deny by Default mode, client devices and BreadCrumb devices are not permitted on the network unless they are

listed in the "Permitted Devices" ACL. In Allow by Default mode, client devices and BreadCrumb devices are permitted on the network unless they are listed in the "Forbidden Devices" ACL.

To edit the ACLs, click the ACL button in the toolbar. A window resembling the following will appear:

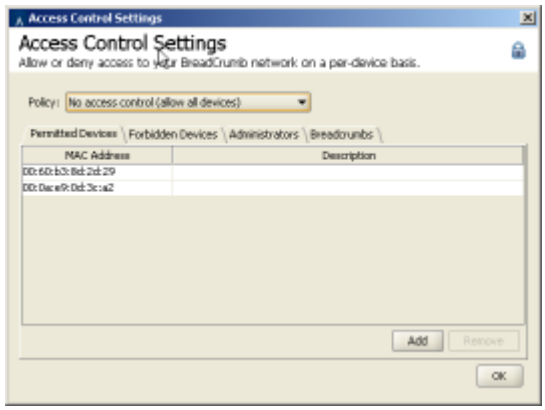

Figure 5-13. Access Control List Window

1. Policy

   This dropdown allows the administrator to select from three different policies:

   - *No access control (allow all devices)*

     This disables ACLs on the BCWN.

   - *Deny by default (allow only permitted devices)*

     This policy only allows devices in the *Permitted Devices*, *Administrators*, or *BreadCrumbs* lists to connect to the BCWN.

   - *Allow by default (deny only forbidden devices)*

     This policy denies BCWN access to all devices in the *Forbidden Devices* list.

2. *ACL List Tabs*

   The *Permitted Devices*, *Forbidden Devices*, *Administrators*, and *BreadCrumbs* tabs allow access to individual device lists.

3. *Add / Remove Buttons*

These buttons allow individual devices to be added to or removed from the currently selected device list.

Note: The BreadCrumbs and Administrators tabs in the ACL are automatically merged into the Permitted Devices and Forbidden Devices lists. Separate tabs are only provided in order to ensure that the administrator has fully considered the ramifications of setting an ACL.

Warning

Be sure to include the BCAdmin workstation in the ACL so that you can continue administering the network!

AES-256 Encryption with AirFortress

Fortress Technologies provides FIPS 140-2-certified encryption via its AirFortress secure client software. This can be installed on any number of client devices without any modifications whatsoever to the BCWN configuration. However, in order for client devices to receive IPv4 addresses from the BreadCrumb devices' embedded DHCP servers, or for an AirFortress-encrypted workstation to communicate to a BreadCrumb device using BCAdmin, Rajant provides support for AirFortress encryption within the BreadCrumb devices themselves.

Contact your Rajant Account Representative to obtain the AirFortress secure client software for your laptops and handheld computers.

Important: When a BreadCrumb device is running with AirFortress enabled internally, only clients using the AirFortress client may communicate over the BCWN.

Tip: For more information about the AirFortress secure client, visit http://www.fortresstech.com.

Registering AirFortress

In order to enable AirFortress support on a BreadCrumb device, its internal driver must be activated via a one-time registration process. To do this, right-click on a BreadCrumb device in BCAdmin and choose `Diagnostics and Maintenance`, then `Register AirFortress Encryption`. If this menu option is not presented, Fortress is already registered on that BreadCrumb device.

Setting the Access ID

The Access ID is a shared credential used by the AirFortress client to negotiate encryption keys. All devices that are to communicate with one another must share a common Access ID.

To set the Access ID on a BreadCrumb device, the BCAdmin workstation *must* be connected to the BreadCrumb device via the BreadCrumb device's ethernet port. This is in order to prevent the transmission of the Access ID over an unsecured wireless connection that the Access ID will help to protect.

> **Important:** In order to communicate to a BreadCrumb device via the BreadCrumb device's ethernet port, the BreadCrumb device's ethernet interface *must* be placed into Bridge Mode in the BreadCrumb device's Reachback settings. If a BreadCrumb device does not have an ethernet port, you cannot set its Access ID.
>
> If your BCAdmin workstation is connected to a BreadCrumb device via ethernet, be sure that the BCAdmin workstation's radio is disabled in order to guarantee that the ethernet connection is in fact being used.

To set the Access ID on a BreadCrumb device, open the General tab of its Properties window and click the button "Change Access ID". You will be presented with a window resembling the following:

Figure 5-14. Set Access ID Window

If the button is disabled, check to ensure that you have registered the AirFortress client and that you are communicating with the BreadCrumb via its ethernet interface.

You must know the current Access ID in order to set a new one. The default Access ID on a BreadCrumb device is "0000000000000000" (16 zeros).

You must supply the new Access ID twice in order to prevent the inadvertent setting of an unknown Access ID.

> **Important:** The Access ID change in a BreadCrumb device has an immediate effect. If you change the Access ID on a BreadCrumb device that has AirFortress encryption already running, you will have to change your BCAdmin workstation's Access ID to match it in order to communicate with the BreadCrumb device again.

Enabling/Disabling AirFortress Encryption

AirFortress encryption is enabled and disabled on a BreadCrumb device using a checkbox on the General tab of the BreadCrumb Properties window. Unlike the Access ID, this setting may be changed when communicating wirelessly with the BreadCrumb device.

> **Important:** Enabling and disabling AirFortress encryption in a BreadCrumb device has an immediate effect. If you change this setting, you will have to change your BCAdmin workstation's setting to match it in order to communicate with the BreadCrumb device again.

Encrypting Wired Traffic

The BreadCrumb devices' AirFortress support includes the ability to encrypt traffic from a wired network provided that the BreadCrumb device's ethernet interface is in either Gateway Mode or Gateway (Ingress) Mode. With AirFortress enabled on a BreadCrumb device in one of these modes, encryption of wired traffic entering the wireless network and decryption of wireless traffic entering a wired network is completely automatic.

> **Tip:** In addition to providing secure wireless extension of a wired network, this feature can be used to encrypt communications from ethernet-enabled devices (such as cameras) for which an AirFortress client is not available. For an example of this, see the Section called *Encrypting a Video Feed* in Chapter 6.

Zeroizing the Access ID

The BreadCrumb Access ID and other settings can be erased remotely or with physical access to the BreadCrumb device by following the steps in the Section called *Restoring Default Settings (Factory Reset)* in Chapter 7.

Harris SecNET11

For security exceeding AES-256 encryption, Rajant provides support for Harris Corporation's SecNet11 product family. You must specify when ordering your BreadCrumb devices that you require this feature; each BreadCrumb radio will be replaced with a SecNet11 Plus PC card.

The SecNet11 Plus PC card has been certified as part of the National Security Agency (NSA) Commercial COMSEC Evaluation Program (CCEP).

> **Tip:** To learn more about the SecNet11, visit http://www.govcomm.harris.com/secure-comm/.

SecNet11 Key Filling

The SecNet11 Plus PC cards included in SecNet11-enabled BreadCrumb devices are user-accessible and do not impose any changes upon existing SecNet11 key fill procedures.

BCAdmin Preferences

Settings specific to BCAdmin are available through the `View` menu, under `Preferences`. The Preferences window is shown below:

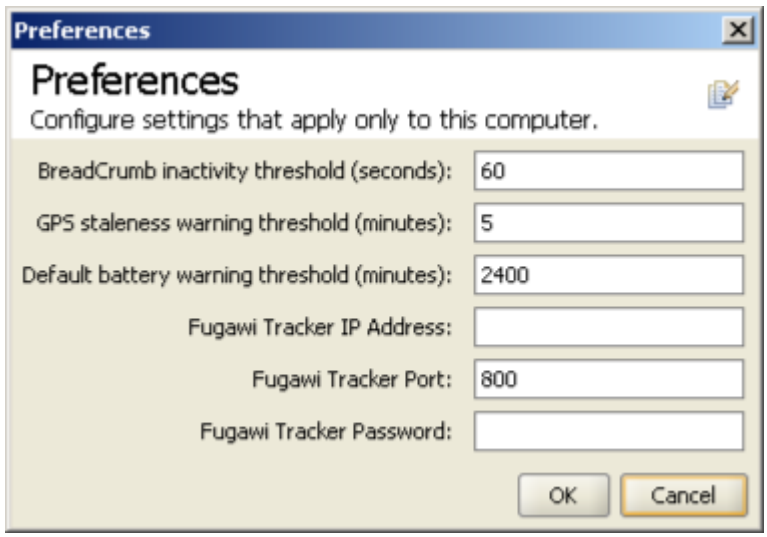

Figure 5-15. BCAdmin Preferences Window

The first three fields are described in this section. The remaining fields are described below in the Section called *Mapping with Fugawi Tracker*.

1. *BreadCrumb inactivity threshold (seconds)*

   If BCAdmin receives no update from a BreadCrumb device for this amount of time, the BreadCrumb box will turn red in the Topology View to call the administrator's attention to a possible problem. A red BreadCrumb box will return to normal upon receipt of an update from the BreadCrumb device, and its inactivity timer will be reset.

2. *GPS staleness warning threshold (minutes)*

   For GPS-enabled BreadCrumb devices, position information shown in BCAdmin is marked as "stale" if it has not been updated for this period of time (for example, if the BreadCrumb device's GPS receiver is no longer able to determine its location).

3. *Default battery warning threshold (minutes)*

   For BreadCrumb devices with no battery warning threshold set, this setting will be used.

Mapping with Fugawi Tracker

BCAdmin has the ability to relay position information from BreadCrumb devices (either manually set by an administrator or obtained via GPS) to the Fugawi Tracker mapping application. Each BreadCrumb device's asset ID within Fugawi Tracker is its BreadCrumb ID as reported by BCAdmin.

To enable the relaying of position information, open the Preferences dialog shown above and provide the following information:

1. *Fugawi Tracker IP Address*

   This is the IPv4 address of the workstation running the Fugawi Tracker application.

2. *Fugawi Tracker Port*

   This is the IPv4 port on which Fugawi Tracker is listening for TCP connections (default is 800).

3. *Fugawi Tracker Password*

   This is the password configured within Fugawi Tracker that BCAdmin must use upon connecting.

Chapter 6. Configuration Examples

Connecting Remote Wired LANs

Unencrypted Point-to-Multipoint

To connect two or more wired LANs that are physically remote from one another, the simplest configuration is as follows:

1. Attach a BreadCrumb device to each LAN using the BreadCrumb devices' ethernet interfaces.
2. Configure the LAN-connected BreadCrumb devices to use Bridge Mode reachback over ethernet.
3. Add intermediate BreadCrumb devices as necessary to cover the distance between/among LANs.
4. If you do not want support for wireless clients using the BCWN, disable the Access Points on each BreadCrumb radio.

   Note: This will prevent wireless clients from using the BCWN to transmit data, but will not prevent wireless monitoring of traffic. For encrypted point-point links, see the Section called *Encrypted Point-to-Point*.

5. For further security, enable ACLs and/or WEP to prevent other devices from accessing the BCWN.

   Note: This will only protect your traffic from inadvertent or casual monitoring. For encrypted point-to-point links, see the Section called *Encrypted Point-to-Point*.

Encrypted Point-to-Point

Two wired LANs that are physically remote from one another can be connected with all wireless traffic encrypted using AirFortress, provided that the following conditions are met:

1. The two wired networks use different address ranges.
2. Neither of the two wired networks uses the 10.0.0.0/8 address range.

For example, Network A could use 192.168.1.0/24, while Network B uses 192.168.2.0/24.

The simplest configuration for this scenario is possible when one of the networks (Network B) is a consumer of services provided by the other network (Network A). That is, Network B initiates connections to Network A, but Network A does not initiate connections to Network B.

The configuration steps for such a network are:

1. Attach a BreadCrumb device to each of the two LANs using the BreadCrumbs' ethernet interfaces.
2. Configure the Network A BreadCrumb device as follows:
    a. Reachback Interface: Ethernet
    b. Reachback Mode: Gateway
    c. Alternate Gateway: Disabled
    d. IP Address Settings: as appropriate for a member of wired Network A.
    e. AirFortress Encryption: Enabled
3. Configure the Network B BreadCrumb device as follows:
    a. Reachback Interface: Ethernet
    b. Reachback Mode: Gateway (Ingress)
    c. Alternate Gateway: Disabled
    d. IP Address Settings: as appropriate for a member of wired Network B. Make a note of this address as it will be Network B's default gateway address later.
    e. AirFortress Encryption: Enabled
4. Configure your Network B devices to use the Network B BreadCrumb device's ethernet address as their default gateway.
5. Add intermediate BreadCrumb devices as necessary to cover the distance between/among LANs.

Note: This configuration can be extended to allow connections from Network A to Network B by configuring the Network A BreadCrumb device to use Port Forwarding, as described in the Section called *Forwarding Settings* in Chapter 5.

Convoy with UAV-Based Camera for Forward Observation

A convoy with an associated UAV can provide a UAV-based video feed to one or all of the vehicles in the convoy. One possible configuration for such a network including a network camera is:

1. Affix a BreadCrumb ME and camera to the UAV. Connect the BreadCrumb ME's ethernet interface to the camera's ethernet port using a crossover cable.

2. Optionally encrypt the video signal as described below in the Section called *Encrypting a Video Feed*.
3. Install a BreadCrumb XLV in each convoy vehicle that is to receive the video signal.
4. For long convoys, or for convoys that will be passing through environments such as urban canyons that inhibit line-of-sight radio signals, install additional BreadCrumb XLVs in intermediate convoy vehicles to bridge gaps between the vehicles viewing the video feed.
5. Install a computer in each vehicle to view the video feed. This may be a wireless client of the XLV or, preferably, a wired client connected to the XLV's ethernet port in Bridge Mode.
6. If the video is encrypted, be sure to install the appropriate Fortress Secure Client and Access ID on the viewing PCs.

Encrypting a Video Feed

A BreadCrumb device can be used to encrypt the video feed from a network camera with ethernet support. It is useful for administrators to configure all of their cameras in exactly the same way so as to minimize any BreadCrumb device-specific configuration. The following approach takes this into consideration.

1. Connect the camera or video encoder to the BreadCrumb device using a crossover cable.
2. Configure the camera for the mini-network between the BreadCrumb device and the camera. The following settings may be used on all cameras:
   a. IP Address: 192.168.3.2
   b. Subnet Mask: 255.255.255.0
   c. Default Gateway: 192.168.3.1

   (In this example, 192.168.3.0/24 is used).
3. Configure the BreadCrumb device for the mini-network between the BreadCrumb device and the camera. The following settings may be used on all cameras:
   a. Reachback Interface: Ethernet
   b. Reachback Mode: Gateway (Ingress)
   c. IP Address: 192.168.3.1
   d. Subnet Mask: 255.255.255.0
   e. Default Gateway: 10.0.0.1
4. Configure the BreadCrumb device for port forwarding to the camera. Assuming that the camera provides a web-based front end, use the following settings:
   a. Ext Ports: 80-80

b. TCP: Checked

c. UDP: Unchecked

d. IP Address: 192.168.3.2 (i.e., the camera's address)

e. To Ports: 80-80

f. Enable: Checked

5. Enable AirFortress on the BreadCrumb device.
6. Access the camera by directing a web browser to one of the BreadCrumb device's IPv4 addresses (as reported by BCAdmin).

Setting the AirFortress Access ID for a Gateway or Gateway (Ingress) BreadCrumb Device

As noted earlier in this manual, the AirFortress Access ID for a BreadCrumb device can only be set using the BreadCrumb device's ethernet interface. When a BreadCrumb device is configured in either Gateway Mode or Gateway (Ingress) Mode, this becomes more difficult as the gateway modes prevent wired communication between BCAdmin and the BreadCrumb device.

Follow these steps to work around this and set the Access ID:

1. Using a BCAdmin workstation connected wirelessly to the BCWN, configure the BreadCrumb device to use Bridge Mode on its ethernet interface.
2. Reboot the BreadCrumb device.
3. Disable the BCAdmin workstation's wireless interface and connect the BCAdmin workstation directly to the BreadCrumb device's ethernet port. (Note: BCAdmin must have a 10.0.0.0/8 address on its ethernet port. If DHCP is enabled on the BreadCrumb device and on the workstation, this will happen automatically).
4. Set the Access ID on the BreadCrumb device.
5. If AirFortress is already running, change the BCAdmin workstation's Access ID to match the BreadCrumb device's new Access ID.
6. Configure the BreadCrumb device to use Gateway (Ingress) mode or Gateway Mode as it was previously configured.
7. Reboot the BreadCrumb.
8. Disconnect the BCAdmin workstation from the BreadCrumb device's ethernet interface, and re-enable the BCAdmin workstation's wireless interface.

Chapter 7. Troubleshooting

Individual BreadCrumbs

Problem	Resolution
When the BreadCrumb is powered on, its LED remains solid red, and devices cannot communicate with the BreadCrumb.	Ensure that radio cards are properly seated in their PCMCIA slots. If problem persists, re-flash BreadCrumb or contact customer service.
When the BreadCrumb is powered on, its LED blinks red, and devices cannot communicate with the BreadCrumb.	The BreadCrumb has detected that it contains both SecNet and Non-SecNet radios. Ensure that all radios are SecNet or Non-SecNet and reboot BreadCrumb.

Table 7-1. Individual BreadCrumb Issues

The BreadCrumb Wireless Network

Sporadic Network Connectivity

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.

Problem	Resolution
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 ESSID "breadcrumb" (or the ESSID that you set for the network) using the software accompanying your wireless card. • Ensure that the wireless client's IP address settings are configured properly. • Ensure that the WEP settings on the client device and BreadCrumb devices match. • Ensure that the client device is not prevented from connecting by an ACL. • If the BreadCrumb devices comprising the network have AirFortress encryption enabled, ensure that the client does as well.

Table 7-2. Sporadic Network Connectivity Issues

BreadCrumb Device Cannot Connect to BCWN

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 should be fully charged.
On rare occasions, the PCMCIA cards within a BreadCrumb device can work loose, resulting in the BreadCrumb device's not being able to establish connectivity to the BCWN.	Open the BreadCrumb device's case and verify that the PCMCIA cards are securely seated in the PCMCIA slots.
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.

Table 7-3. BreadCrumb-BCWN Connectivity Issues

BCAdmin

Problem	Resolution
The screen is red and empty.	The BCAdmin workstation does do not have a 10.x.x.x address, which is required to administer the BCWN.
The screen is black and empty.	BCAdmin is unable to communicate with any BreadCrumb devices. Verify that a personal firewall application such as BlackICE or Zone Alarm is not preventing BCAdmin from communicating with the BreadCrumb devices. The Windows XP® Service Pack 2 built-in firewall also blocks communications with BreadCrumb devices by default.
BreadCrumb boxes are turning red on the screen.	This means that BCAdmin has been unable to communicate with that BreadCrumb device for 60 seconds. This could be due to several factors:• LOS obstructions • Dead or failing BreadCrumb battery • BreadCrumb device is rebooting • Fortress encryption settings are mismatched between BCAdmin and the affected BreadCrumb devices
I clicked `BreadCrumb Properties` from the BreadCrumb box's popup menu, but nothing happened.	You are running an old version of BCAdmin with a new version of the JRE) Java® Runtime Environment. Install the latest version of BCAdmin.

Table 7-4. BCAdmin Issues

Restoring Default Settings (Factory Reset)

In an emergency, a BreadCrumb device can be restored to its default settings to both erase its configuration and allow access to an administrator who has inadvertently locked himself out of the BCWN (via WEP, ACLs, or Fortress, for example). Use the following procedure to restore a BreadCrumb to its default settings:

1. Open the BreadCrumb device.
2. Locate the radio lights and the small, black reset button on the side of the main circuit board as depicted in the following figure:

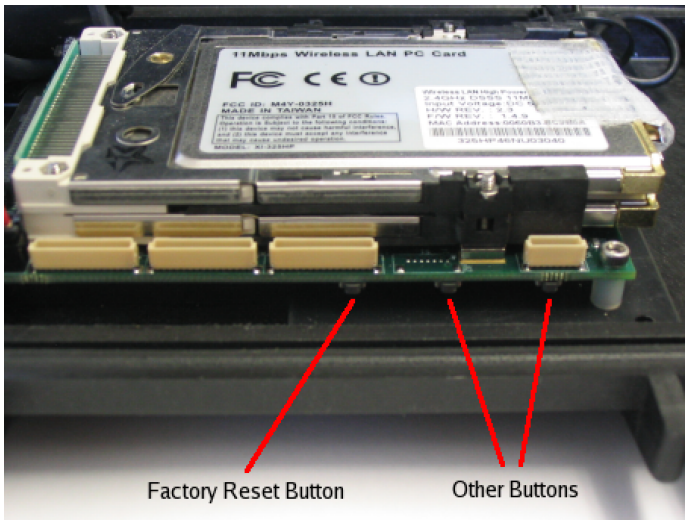

Figure 7-1. Factory Reset Button

3. PRESS AND IMMEDIATELY RELEASE the reset button.
4. Wait 5 seconds.
5. PRESS AND IMMEDIATELY RELEASE the reset button again.

Within a few seconds after completing this procedure, you should see the radio lights go out, pause, and come back on as the BreadCrumb device restarts.

> **Important:** A BreadCrumb device coming up in its default state will obtain an ACL from any BreadCrumb device to which it connects. If you are trying to correct an ACL problem by restoring a BreadCrumb device's default settings, TURN OFF THE BREADCRUMB IMMEDIATELY when the radio lights go out following step 5. Do this for all BreadCrumb devices in your BCWN, turning them back on only after all the BreadCrumb devices have been reset. This will ensure that the problematic ACL is not reapplied to your BreadCrumb devices.

> **Important:** If you are resetting an extended-range BreadCrumb device (XL, XLV, XLE), be sure to set its radios to channels 1 and 11 after it restarts (see the Section called *Channel Assignments* in Chapter 4 for details).

Chapter 8. Case Study: Military Exercise in Thailand

Rajant BreadCrumb devices were used by the Thai Military as an integral part of a Joint Air Land Sea Amphibious Assault Exercise last week in Pattaya, Thailand. The beach assault took place at a Thai Naval Base and Thai media from a major news channel was present to document the exercise.

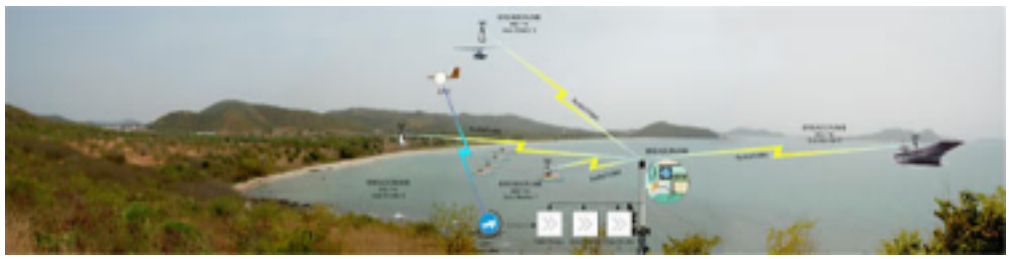

Figure 8-1. Joint Exercise Network

There was a BreadCrumb XL on each of two ships, an XL on a Black Hawk helicopter, an XL on the observation bluff, and multiple SEs deployed as needed. The observation center was set up 2km away from the beach, on a bluff overlooking the bay. There were two ships at sea, one 2km away from the bluff with a camera streaming live feed of the ship's control center (Mission Control Center) and another 10km away from the bluff with a camera streaming live feed of the landing deck for the helicopters. There was a camera on one helicopter as well, streaming live video as it performed its duties. Finally, there was a UAV flown that was equipped with video to its base station. Using a new addition to the Rajant product line, a Video Encoder XL, the analog video stream was encoded to MPEG-4 and sent over the BreadCrumb network to be viewed by anyone on the network.

A total of eight Rajant BreadCrumb devices were used to create the portable, wireless, secure, meshed network. Through this network, the Thai Prime Minister and Commander of the Joint Supreme Command were able to monitor each stage of the assault by viewing streaming video from the helicopter, flight deck, UAV and ship based command center on two big screen televisions placed at the observation center. Most impressive was the consistent 10Km link to the far away ship and the automatic meshing of the XL and transmission of video from an on-the-go helicopter. The assault exercise was deemed a huge success by the Thai military, Prime Minister, Commander of the Joint Supreme Command and all others involved.

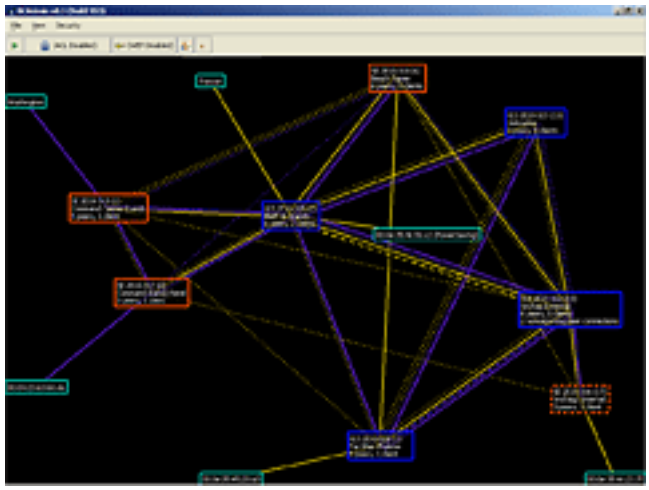

Figure 8-2. BCAdmin screen during exercise showing BreadCrumb network

Figure 8-3. View of beach from command center

Rajant also teamed up with the Naval Postgraduate School, Mercury Data Systems, Redline Communications and the Thai Military to set up a demonstration border security network in Lop Buri, Thailand. The Thai military was impressed by the capabilities of the BreadCrumb network, most importantly by the ease and speed of deployment when compared to other wireless technologies they have tried.

The network consisted of cameras placed on a mountain top and an airborne balloon with live video feed streaming back to the base command. An 802.16 link provided by Redline Communications streamed Internet capabilities from Bangkok and the camera feed from the mountain top. There were three BreadCrumb devices placed around the command base creating a meshed network. A fourth BreadCrumb device was placed on the balloon, ensuring that the camera stayed within the network and

the fifth and final BreadCrumb was placed in a moving vehicle at the foot of the mountain providing NetMeeting capabilities with military personnel back at the base.

Figure 8-4. Balloon with Camera and BreadCrumb

Figure 8-5. Soldier communicating over BCWN using Microsoft NetMeeting

Rajant employees also returned to Phuket, where Rajant BreadCrumb devices had been left this past January to aid in the tsunami relief effort. The BreadCrumbs were all operational and working, with the exception of one that had been directly struck by lightning. Each remaining BreadCrumb device had operated continually without user intervention, with the entire network supporting up to 70 users at a time.

Glossary

ACL

Access Control List; a list of MAC addresses that are used to control access to the BreadCrumb Wireless Network.

AES/AES-256

Advanced Encryption Standard. An encryption standard adopted by the U.S. Government.

AP

Access Point; a networking device allowing clients with IEEE 802.11 network cards in infrastructure mode to communicate wirelessly with a network. All radios in a BreadCrumb usually provide AP functionality.

802.11b

A wireless networking standard providing raw data rates of up to 11Mbps

BCAdmin

The BreadCrumb Wireless Network management application

BCWN

BreadCrumb Wireless Network

BreadCrumb / BreadCrumb Device

Any of the family of BreadCrumb products offered by Rajant corporation.

crossover cable

A networking cable that internally swaps its transmit and receive wires, allowing direct connection between devices without a switch or hub.

DHCP

Dynamic Host Configuration Protocol; the means by which some networking devices obtain an address automatically from a network

DSL

Digital Subscriber Line

ESSID

Extended Service Set Identifier; a set of Access Points or BreadCrumbs that appear as a single network. Also referred to as a "network name."

LAN

Local Area Network

MAC

Media Access Control

MAC Address

A unique identifier (usually of the form 11:22:33:44:55:66) associated with an individual network interface.

NAT

Network Address Translation

peer

A BreadCrumb device that is meshed with another BreadCrumb device.

pending peer

A BreadCrumb device that is meshed with another BreadCrumb device, but has not yet communicated with BCAdmin itself.

reachback

A connection to another network, such as the Internet, an office network, or a TOC

TAN

Tactical Area Network

TOC

Tactical Operations Center

UAV

Unmanned Aerial Vehicle

Appendix A. Status Indicator LED

Beginning in June, 2005, each BreadCrumb includes a multi-color LED to indicate the BreadCrumb state. Use the following table to interpret the LED output:

Color	Blinking/Solid	Status
Red	Solid	Starting up
Red	Blinking	Error
Blue	Solid	No Peers
Green	Blinking	At Least 1 Peer
Green	Solid	At Least 1 Peer at 11Mbps

Table A-1. LED Status Indications

Appendix B. Radio Frequencies

The BCWN uses the 11 802.11b channels allocated for use in the U.S. These channels and their frequencies are listed in the following table:

802.11b Channel	Frequency (GHz)
1	2.412
2	2.417
3	2.422
4	2.427
5	2.432
6	2.437
7	2.442
8	2.447
9	2.452
10	2.457
11	2.462

Table B-1. 802.11b Channel Frequency Table

Appendix C. Customer Service

Please contact Rajant Support at +1 610-873-6788 to assist you through any issues you encounter regarding this release.

Please forward all feedback regarding the BreadCrumb system functionality to <support@rajant.com>. Other than speaking with a Rajant representative, this is the best way to communicate with us any operational issues you may find.

Thank you for your ongoing business and support.