AG1-5250M Cardinal Module Version 11 User Guide

Model: AG1-5250M
User Guide Version: 11.27 Rev A
Firmware Version: 11.27.x
Document Part Number: 03-100178-001

Corporate Headquarters:

Rajant Corporation
200 Chesterfield Pkwy
Malvern, PA 19355
Tel: (484) 595-0233
Fax: (484) 595-0244
🌐 http://www.rajant.com

Table of Contents

Document Revision History

Revision	Date	Changes
11.27 Rev A	02/07/2024	Initial release

Copyright Statement

Rajant, the Rajant logo, BreadCrumb, InstaMesh, Kinetic Mesh, BC|Commander, and Bring Your Network with You! are registered trademarks of Rajant Corp. in the United States and certain other countries.

Rajant's patented InstaMesh® networking software enables the network to quickly adapt to rapidly-deployed and moving network elements. U.S. Patents 9,001,645, US 9,001,645 B2, US 9,319,922 B2 and US 9,979,635 B2.

AG1 Cardinal Module Version 11 User Guide

FCC, CE and Other Certification Statements

FCC ID: VJA-AG15250M

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

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

Déclaration de la FCC

1. Cet appareil est conforme à la partie 15 des règles de la FCC. Les opérations sont soumises aux deux conditions suivantes:
   (1) Cet appareil ne peut pas causer d'interférences nocives.
   (2) L'appareil doit accepter toute interférence reçue, y compris celles qui peuvent entraîner un fonctionnement indésirable.

Les changements ou modifications qui ne sont pas expressément approuvés par la partie responsable de la réglementation de l'OCDE peuvent faire perdre à l'utilisateur le droit d'utiliser l'appareil.

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.

Industry Canada

This Class A digital apparatus complies with Canadian ICES-003 and RSS-247 rules.

Cet appareil numérique de la classe A est conforme à la norme NMB-003 et CNR-247 du Canada.

CE:

Rajant Corporation declares that the AG1 is in compliance with the essential requirements and other relevant provisions of Directive 2014/53/EC.

CE Declaration of Conformity may be requested from Rajant.

> **◑ NOTE**
> Please refer to the product spec sheet at **◉** http://www.rajant.com for a list of certified model numbers.

Antennas

> **⚠ Antenna Installation WARNING**
> The installer should configure the conducted output power level according to country regulations and the applicable EIRP limit. Professional installation of equipment is required to ensure compliance with health and safety issues.

Required Antenna Separation

The antennas from any transceiver of the AG1 Cardinal Module may not be co-located with the antennas of any other transceiver. The co-location restriction is satisfied by maintaining 20 cm separation between the antennas of different transceivers. There is no restriction for the separation between the antennas from the same transceiver, but testing at installation is recommended to verify the system performance that is achieved with a specific antenna deployment.

> **⚠ IMPORTANT: Exposure to Radio Frequency Radiation**
> To satisfy FCC RF exposure requirements, the following minimum safe distances must be maintained between this device's antennas and all persons while the device is operating:
> - AG1: 20cm/br>

Notice As per FCC Part 15 178919 D01 Permissive Change Policy v06 "Equivalent antennas must be of the same type (e.g., yagi, dish, etc.), must be of equal or less gain than an antenna previously authorized under the same grant of certification (FCC ID), and must have similar in-band and out-of-band characteristics (consult specification sheet for cutoff frequencies). Any new antenna type, or higher gain antenna, approved under Part 15 requires a Class II permissive change, and the requirements of § 15.203 must be met".

Rajant has certified the Cardinal module under FCC part 15 with the following Rajant antennas, to permit maximum power high performance use, and minimal footprint dual-band dual-port MIMO use:

• KMA-2400 - Vertically Polarized Dipole, Omni Directional, 2.4-2.5GHz, 5dBi peak gain

• KMA-5800 - Vertically Polarized Dipole, Omni Directional, 5.7-5.9GHz, 6dBi peak gain

• KMA-5250 - Vertically Polarized Dipole, Omni Directional, 5.15-5.35GHz, 7dBi peak gain

•RLP-2450-5-4 - Vertically Polarized Dipole, Omni Directional, MIMO, 2.4-2.5/5.0-7.2GHz, 7.5dBi peak gain

• KMA-5550 - Vertically Polarized Dipole, Omni Directional, 5.35-5.75GHz, 6dBi peak gain
• The maximum gain certified is 7db

If the Cardinal module is deployed with one of the antennas certified by Rajant or with an alternate Rajant approved antenna which is of the same type and equal or lesser gain, Rajant's modular certification may be leveraged. With this approach, the final product should only require FCC Digital emissions testing: Part 15B. Otherwise, you will have to complete radio certifications for every country in which you deploy the Cardinal module.

Unlike most Rajant BreadCrumb products, the Cardinal module utilizes standard SMA female type antenna connectors rather than N type connectors. The Cardinal module does not use RP-SMA type connectors. This needs to be taken into consideration during the installation of coax as these connectors are more susceptible to damage. Coax should be secured with strain relief near the Cardinal module to prevent damage from vibration or other movement.

Notice Be sure to terminate any unused or disabled RF Ports using a 50 Ohm load.

> **⊙ DFS Additional Antenna Separation**
> For 5 GHz transceivers using channels that require DFS radar detection, a recommendation is to mount each antenna for a DFS channel at least 2 feet from the antenna for any other 5 GHz transceiver.

Safety

> **⚠ Warning**
> The AG1 Cardinal Module is not user serviceable. Repairs must be performed at a Rajant designated service center by trained personnel.

> **⚠ Warning**
> The enclosure of the AG1 Cardinal Module is conductive. To protect the user against the risk of electric shock during high voltage transient events which may occur when this equipment is installed outdoors, protective earth grounding of the AG1 Cardinal Module enclosure is required. Protective earth grounding operations must be performed by trained personnel, and according to local electrical codes and industry best practices, as well as Rajant's own recommendations.

> **⚠ Warning**
> To protect the user against the risk of electric shock during high voltage transient events which may occur when this equipment is installed outdoors, protective earth grounding of the POE power supply is required. Case ground connections are provided on all Rajant supplied POE power supplies. The case ground connections must be used and must be connected to a protective earth ground. Protective earth grounding operations must be performed by trained personnel, and according to local electrical codes and industry best practices, as well as Rajant's own recommendations.

Modifications

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

Rajant Products are compliant and warranted against manufacturing defects only so long as Rajant-authorized accessories are used in deployment of Rajant Breadcrumbs. It is the responsibility of the operator and the installer to ensure the system as installed operates within regional requirements.

Professional Installation Attestation

Rajant Corporation addresses the following items to ensure that the above referenced equipment is professionally installed:

The device will only be sold by Rajant Corporation or one of its authorized dealers. Rajant Corporation and its authorized dealers will be under strict marketing control and will only market and sell the device to professionals.

Professional installation is required for this device and will be performed only by someone knowledgeable of its use. Rajant Corporation will ensure that the device is only marketed and sold to professionals.

The device is not sold to the general public and is sold only for industrial or commercial use by professional installers.

> ⚠ **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.

Maximum Certified Power

ISM band radio modules may be operated at full certified power when configured with the granted antenna type. Operation of a radio at power levels that exceed the equivalent EIRP of the granted configuration is prohibited. See the tables below.

Table: Maximum Certified Power: FCC (United States), **IC** (Canada)

> ⚠ **IMPORTANT**
> In Canada, a license is required to use channels in the frequency range 5150-5250 MHz on models that offer these channels. The license may restrict transmit power. Licensing information may be found at
> 🌐 http://www.ic.gc.ca/eic/site/smt-gst.nsf/eng/sf11294.html

AG1-5250M FCC Compliance Table

Frequency Range (MHz)	Mode	Antenna Type	Antenna Detail	Antenna Gain (dBi)	Conducted Power (dBm)	EIRP (dBm)
2412-2462	Point-to-Multipoint	Omni	KMA-2400-5 or equivalent	5	24	29
2412-2462	Point-to-Multipoint	Omni MIMO	RLP-2450-5-4 or equivalent	5	24	28.9
5150-5350	Point-to-Multipoint	Omni	KMA-5250-7 or equivalent	7	22	29
5170-5250	Point-to-Multipoint	Omni MIMO	RLP-2450-5-4 or equivalent	7.5	22	26.3
5735-5835	Point-to-Multipoint	Omni	KMA-5800-6 or equivalent	6	24	30
5735-5835	Point-to-Multipoint	Omni MIMO	RLP-2450-5-4 or equivalent	7.5	24	28.3
5350-5750	Point-to-Multipoint	Omni	KMA-5550-6 or equivalent	6	21	27

Table: Maximum Certified Power: CE

Frequency Range (MHz)	Mode	Antenna Type	Antenna Detail	Antenna Gain (dBi)	Conducted Power (dBm)	EIRP (dBm)
2412-2462	Point-to-Multipoint	Omni	KMA-2400-5 or equivalent	5	14	19
2412-2462	Point-to-Multipoint	Omni MIMO	RLP-2450-5-4 or equivalent	5	14	18.9
5150-5350	Point-to-Multipoint	Omni	KMA-5250-7 or equivalent	7	15	22

Frequency Range (MHz)	Mode	Antenna Type	Antenna Detail	Antenna Gain (dBi)	Conducted Power (dBm)	EIRP (dBm)
5170-5250	Point-to-Multipoint	Omni MIMO	RLP-2450-5-4 or equivalent	7.5	15	19.3
5260-5320	Point-to-Multipoint	Omni	KMA-5250-7 or equivalent	7	13	20
5260-5320	Point-to-Multipoint	Omni MIMO	RLP-2450-5-4 or equivalent	7.5	13	17.3
5350-5750	Point-to-Multipoint	Omni	KMA-5550-6 or equivalent	6	21	27
5500-5720	Point-to-Multipoint	Omni MIMO	RLP-2450-5-4 or equivalent	7.5	21	25.3
5735-5835	Point-to-Multipoint	Omni	KMA-5800-6 or equivalent	6	23	29
5735-5835	Point-to-Multipoint	Omni MIMOi	RLP-2450-5-4 or equivalent	7.5	23	27.3

C E

This radio transmitter [IC: 7382A-AG15250M] has been approved by Innovation, Science and Economic Development Canada to operate with the antenna types listed in above compliance table, with the maximum permissible gain indicated. Antenna types not included in this list that have a gain greater than the maximum gain indicated for any type listed are strictly prohibited for use with this device.

GNU General Public License Statement

Certain components of the Rajant BreadCrumb firmware are subject to the GNU General Public License Version 2, or other so-called open source licenses ("Open Source Software"). In compliance with the terms of certain Open Source Software licenses like the GNU General Public License Version 2 ("GPLv2"), Rajant makes certain modifications to Open Source Software that Rajant uses, modifies and distributes pursuant to such licenses available to customers in source code form upon request. You are free to use, modify and distribute Open Source Software so long as you comply with the terms of the relevant Open Source Software license. In particular, the GPLv2 is available in the appendix of this manual or at ⊕ http://www.gnu.org/copyleft/gpl.html.

Preface

Purpose and Scope

This user guide provides information and guidance to all personnel who are involved with and use Rajant Corporation's AG1 Cardinal Module.

This user guide begins with an introduction to the BreadCrumbs and the Rajant Kinetic Mesh Network. This user guide then describes the features of the AG1 Cardinal Module. Finally, this user guide describes common deployment scenarios and provides concise step-by-step instructions for each scenario.

> ⊘ **Note**
> Throughout this document, unless otherwise stated, the terms AG1 Cardinal Module and BreadCrumb are used to refer to Rajant AG1 Cardinal Module.

How to Use This Guide

This User Guide is an HTML document to be viewed using a web browser. The browser's right scroll bar, mouse scroll wheel, up/down cursor keys or Page Up/Page Down keys may be used to navigate sequentially forward or backward through the guide. In most browsers, CTRL-F can be used to search the guide and navigate to matching text. The Table of Contents at the left (or top in a small window) contains a link to the start of each chapter or appendix. After a web link or cross-reference is clicked in the guide, the browser's back arrow should return to the previous page location.

Feedback Welcome

Rajant welcomes any reader of this guide to submit comments and recommended changes to improve any Rajant user guide or Rajant product. Please send your feedback to feedback@rajant.com. For a BreadCrumb, please include the BreadCrumb model, firmware version and relevant configuration settings. For a Rajant software product, please include the product name and version number. For a Rajant user guide, please include the title, software version or firmware version and document revision.

Related Documentation

The Rajant BC|Commander® software application is required to configure and monitor BreadCrumbs in a mesh network. Refer to the *BC|Commander Version 11 User Guide* for information about BC|Commander.

The following documents provide technical information about BreadCrumbs:

- BreadCrumb® Video Guide
- Range Troubleshooting Guide
- BreadCrumb RF Guide
- BreadCrumb® Security Technical Brief

These documents are available from the Rajant website at ⊕ http://www.rajant.com in the **Tech Support** section.

Note About Shared Guide Content

Rajant BreadCrumb models have some differences in hardware and software features. Rajant hardware and software product guides include some general content that is shared between guides and may include features or settings not found in every model. The following table summarizes the main differences between several standard BreadCrumb models.

Feature	LX5	ME4/KM3	ME5	ES1/ ES1-2450IS	JR3	SlipStream	Peregrine/ Hawk	AG1
Wireless Transceivers	3-4	2	2	2	1	no	4 (Peregrine) /2 (Hawk)	2
Ethernet	2x 1000	1x 1000, 1x 100	10/100/1000	1x 1000	1x 100	2x 1000	2x 1000	1x1000
LTE	no	no	no	no	no	no	yes (Peregrine) /no (Hawk)	no
Input Voltage	18-48 VDC	8-48 VDC (ME4)/ 24-48 VDC (KM3)	9 — 30 VDC Passive PoE	9-30 VDC	9-30 VDC	12 VDC	20-60 VDC	10-53 VDC
Min. Recommended PoE	24-48 VDC, 26-33	24-48 VDC, 23 W @ 24 V	24 VDC, 19 W	24 VDC, 19 W	24 VDC, 19 W	(AC adapter)	IEEE 802.3bt Type 3/PoE++ or 38-60 VDC	24 VDC, 19 W

Feature	LX5	ME4/KM3	ME5	ES1/ ES1-2450IS	JR3	SlipStream	Peregrine/ Hawk	AG1
	W @ 24 V (3-4 un-heated radios)						Passive PoE, 34 W (Peregrine)/ IEEE 802.3at Type 2/PoE+ or 38-60 VDC Passive PoE, 24 W (Hawk)	
USB Ports	2	1	1	1 (ES1)/no (ES1-2450IS)	no	6	1	1
Serial Port	no (see Notes)	no (see Notes)	no	no	no	no	no	no
Realtime Clock	yes	yes	no	no	no	yes	yes	no
Case	metal	metal	metal	plastic (ES1)/metal (ES1-2450IS)	plastic	metal	metal	magne-sium
Environment	IP67	IP67(ME4)/ Indoor(KM3)	IP67	IP67	Weather Resistant	Indoor	IP67	Unseale
Encryption	HW/SW	HW/SW	SW	SW	SW	HW/SW	HW/SW	SW
TRoIP	yes	yes	yes	yes (ES1)/ no (ES1-2450IS)	no	yes	yes	yes
Modbus	yes	yes	yes	yes	no	yes	yes	yes
SNMP	yes	yes	yes	yes	no	yes	yes	yes
Packet Capture	yes	yes	yes	yes	no	no	yes	yes
Gateway Mode	yes	yes	yes	yes	no	yes	yes	yes
Performance Tests	yes	yes	yes	yes	no	yes	yes	yes
Max Peers per Transceiver	250+	250+	250+	250+	50	0	250+	250+
RTLS	yes	yes	yes	yes	no	no	yes	yes

Notes:

- Top Ethernet link speed (Mbps). Ethernet ports also adapt to standard slower speeds.
- Supports Long-Term Evolution (LTE) standard.
- Unless stated otherwise, all PoE wattages are @ 24 V.
- Add 2 W per heated radio and 2.5 W per powered USB peripheral.
- JR2 included TRoIP settings but no USB port for using TRoIP.
- Performance Tests are available with firmware version 11.19 or later.
- KM3 is an indoor version of ME4.
- To provide a serial port, ME4 has serial pins on an Amphenol connector that supports modbus protocol.
- To provide a serial port, ME4 can use an optional cable assembly with serial pins.
- To provide a serial port, KM3 requires a special USB cable.
- To provide a serial port, LX5 has serial pins on an Amphenol connector that supports modbus protocol.
- Supports Simple Network Management Protocol (SNMP).
- Supports Real Time Location System (RTLS).

1. Introduction to BreadCrumbs

1.1 BreadCrumbs

A Rajant BreadCrumb® is a networking device product of Rajant Corporation (http://www.rajant.com).

Each product family is designed to support particular environmental or operational requirements. BreadCrumb models within a product family differ in component parts. The hardware and firmware features in each BreadCrumb model support specific operational and administrative capabilities.

Most BreadCrumbs include wireless radios that use the IEEE 802.11 (Wi-Fi) wireless networking standard protocols. Some BreadCrumbs support the Long-Term Evolution (LTE) standard. Some BreadCrumbs provide only wired connectivity through a Local Area Network (LAN) to the Ethernet. Many BreadCrumbs provide both wireless and wired Ethernet connections.

Refer to the BreadCrumb user guide for each BreadCrumb model for detailed information. BreadCrumb user guides are available from the Tech Support section of Rajant Corporation website.

1.2 Rajant Mesh Networks

A collection of Rajant BreadCrumbs and other networking devices can be linked to form a Rajant mesh network. A customer application can use these links to transmit data from a source through any number of BreadCrumbs to a destination. BreadCrumb radios provide high bandwidth for applications to stream video, audio and data over large distances. Each BreadCrumb performs any required encryption or decryption of data sent through the network.

Any BreadCrumb can serve as an access point to enable wireless client devices (such as laptops or cell phones) within range to connect through a LAN to the Ethernet. Because BreadCrumbs use standard IEEE 802.11 communication protocols, client devices require no special hardware or software and little or no configuration to access a BreadCrumb network.

In a Rajant Kinetic Mesh™ network, the InstaMesh® protocol seamlessly connects fixed, wireless and mobile nodes. The key feature of a Rajant mesh network is the capability to create or bypass links to direct traffic along the best available path across the network. The network adapts automatically and immediately as the devices move, switch on or off, encounter obstructions or experience radio interference.

1.3 Rajant Mesh Network Scenarios

BreadCrumbs are designed to meet the requirements of any combination of the following network scenarios:

- Temporary wireless network that can be set up quickly and easily for short-term use
- Mobile wireless network that does not require a central stationary controller node to manage traffic
- Extension to a wireless network that quickly enables communication around or through an obstacle
- Wireless connections between multiple wired LANs at different locations
- Broadband wireless network deployed as a standalone wireless network or bridged to another network (such as the Internet) using a digital subscriber line (DSL), cable or satellite modem connection

2. Description of an AG1 Cardinal Module

The AG1 Cardinal Module is a powerful, lightweight module specifically tailored to the needs of the warehouse automation market and Industry 4.0. Designed with automation robots in mind, including collaborative robots, automated storage/retrieval systems, autonomous mobile robots (AMRs), unmanned guided vehicles (UGVs), and more, the Cardinal module can enhance your on-the-move connectivity in the most challenging environments. The Cardinal module extends the range of traditional Wi-Fi past the limitations of fixed infrastructure using two transceivers having a combined PHY data rate of 1.73 Gbps.

2.1 Radios

The AG1 Cardinal Module contains 2x2 MIMO 802.11 AC Wave2 radios. See Appendix Radio Channels and Frequencies for a list of the channels and frequencies that may be supported by the radio(s), depending on locale and regulatory certification.

2.2 Enclosure

2.2.1 Enclosure Dimensions

The dimensions of the AG1 Cardinal Module are 17.8 x 98.0 x 60.68 mm (0.70" x 3.86" x 2.39") including all built-in features of the enclosure. This measurement does not include any antennas, cables or soft cable boot for USB. The weight of the AG1 Cardinal Module is 90 g ± 3 g (3.2 oz ± 0.1) (weight depends on transceiver configuration).

2.2.2 Enclosure Features

The external features of the AG1 Cardinal Module enclosure are shown in the following images.

Figure: AG1 Cardinal Module Enclosure Features (Front)
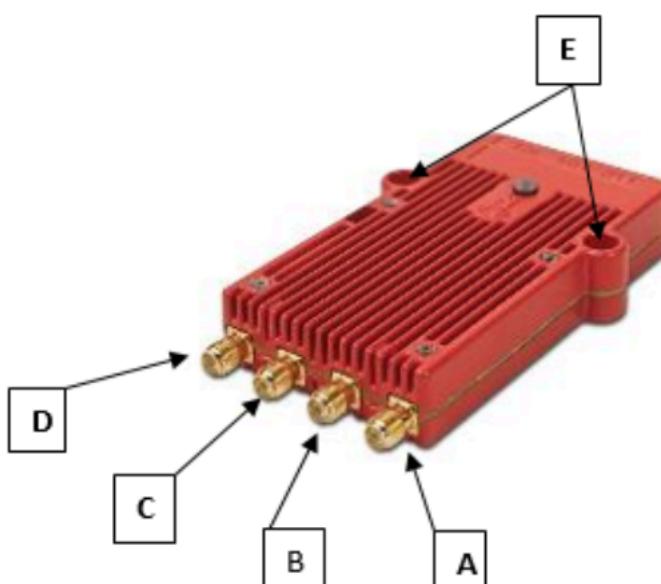
A. SMA Antenna Port "A" Dual-band 2.4/5 GHz, 2x2 MIMO transceiver wlan0

B. SMA Antenna Port "B" Dual-band 2.4/5 GHz, 2x2 MIMO transceiver wlan0

C. SMA Antenna Port "C" 5 GHz 2x2 MIMO transceiver wlan1

D. SMA Antenna Port "D" 5 GHz 2x2 MIMO transceiver wlan1

E. Bolt/Screw Mounting Holes – M6 or 0.25in x 16mm long hole

Figure: AG1 Cardinal Module Enclosure Features (Back)
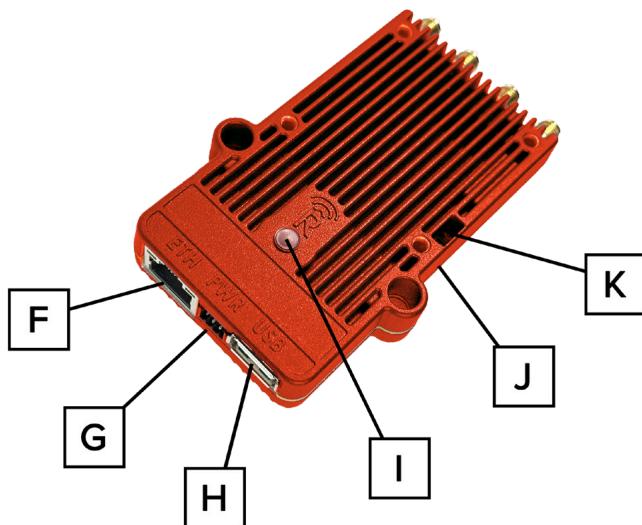
F. RJ45 female connector for Ethernet and PoE (Power over Ethernet)

G. 3 Pin Direct DC power connector. Hirose part DF3A-3P-2DS (*Mating connector, Hirose part DF3-3S-2C with crimp pins DF3-2428SC)

H. USB Type-A female

I. Status LED (RGB) – status, warning, error codes, and link state (refer to the User Guide)

J. Zeroize – Pinhole metal cutout for inset pushbutton switch, on bottom side

K. Fan connector – 4-pin connector for Fan power and control (optional)

2.3 Antenna Connectors

The AG1 Cardinal Module provides four SMA female antenna connectors. The antenna connectors are located on the front of the enclosure (see the *Enclosure Features* images above). Most BreadCrumb radios offer antenna diversity or Multiple-Input and Multiple-Output (MIMO) features, in which case two antenna ports per radio are utilized. Some radios may only utilize one antenna port. Each antenna connector will be labeled with a unique letter (A or B).

> ⚠ **Important: Antenna Frequency Band and Gain**
> Choose antennas that are correct for the frequency band you plan to use. Adjust down the BreadCrumb's transmit power if your antennas have a higher gain than those that were certified for use on this BreadCrumb model in your frequency band and region(see the *FCC and Other Certification Statements* chapter of this guide.

Required Antenna Separation

The antennas from any transceiver of the AG1 Cardinal Module may not be co-located with the antennas of any other transceiver. The co-location restriction is satisfied by maintaining 20 cm separation between the antennas of different tranceivers. There is no restriction for the separation between the antennas from the same transceiver, but testing at installation is recommended to verify the system performance that is achieved with a specific antenna deployment.

> ⚠ **Warning**
> For installations that will experience vibration or shock, all antennas should be externally mounted and attached to the AG1 Cardinal Module using cables. Low loss RF cable such as LMR-400 is recommended for cable attached antennas. If an antenna port is not required for a given application, the port should be disabled in software using BC|Commander, and a 50 Ohm terminator should be installed.

> ⮞ **DFS Additional Antenna Separation**
> For 5 GHz transceivers using channels that require DFS radar detection, a recommendation is to mount each antenna for a DFS channel at least 2 feet from the antenna for any other 5 GHz transceiver.

Most of Rajant's standard antennas are characterized by high-gain and therefore small vertical beamwidth. Antennas in fixed locations should be installed plumb and at the same elevation so that BreadCrumbs using these antennas will see each other without a significant loss of signal strength.

> ⚠ **Warning**

To avoid possible damage to the BreadCrumb radio(s), always connect or disconnect external antennas with the power to the BreadCrumb turned off.

The following table lists the radio band and antenna port(s) for each wlan of current and recent AG1 Cardinal Module models. This information is also available in the Details panel of BC|Commander.

Table: AG1 Cardinal Module Radios and Antenna Ports

Model Number	AG1-5250M
wlan 0	2.4/5 GHz: A+B
wlan 1	5 GHz: C+D

2.4 Power and Ethernet

The AG1 Cardinal Module has one RJ45 Ethernet port. The Ethernet port (ETH0) on the AG1 Cardinal Module supports 10 Base-T, 100 Base-TX or 1000 Base-T configuration. The port supports Auto MDI/MDIX allowing the use of either straight-through or crossover data cables for connections. The data interface includes electrostatic discharge, and electrical fast transient/burst immunity compliant to the IEC 61000-4-2, and IEC 61000-4-4-EFT standards, respectively.

2.4.1 Power Requirements

The Cardinal module will operate from two power sources; either Passive PoE or direct DC Power. The Direct DC Power connector is field installable. Input Voltage PWR Port: 10–53VDC Direct DC input to the 3-pin PWR connector shall meet the following criteria:

• 10 to 53v VDC Absolute, 12/24/48 VDC Nominal

• Input Load Regulation < 5% (of nominal supply)

• Input Ripple and Noise < 1% (of nominal supply)

• Startup Delay based on minimal input voltage threshold of 10VDC

• Minimum Startup Load of 4W

• Input Isolation of 1500VDC typical

• DC Power Input is revers bias protected but not reverse operational

Input Voltage ETH Port: 24–48VDC Passive PoE

The AG1 Cardinal Module ETH0 port supports Passive Power over Ethernet (Passive PoE), and therefore acts as a dual function Ethernet and DC power input port for the AG1 Cardinal Module. An external inline passive PoE injector is used to merge DC power for the AG1 Cardinal Module with data from a LAN port or a wired client.

To ensure proper operation of the AG1 Cardinal Module, the inline injector must output a DC voltage between 10 VDC to 53 VDC @ 19 W minimum. Using a higher output voltage facilitates longer cable runs between the inline injector and the ETH0 port on the AG1 Cardinal Module. For details on Rajant's VHDC-Series power accessories, please refer to the VHDC-Series spec sheet.

The average idle power consumption of a AG1 Cardinal Module is 4.2 Watts W at 24 V. The maximum peak power consumption of AG1 Cardinal Module is 14.4 W at 24 V. Up to 2.5 W of additional power will be needed if a peripheral is being powered by USB (500 mA at 5 V is available at the USB port).

Table: AG1 Cardinal Module Power Requirements (Passive PoE)

Input Voltage	Avg Idle Usage @ 24 V	Max Peak Usage @ 24 V
24 - 48 VDC	4.4 W + USB usage	14.4 W + USB usage

Table: AG1 Cardinal Module Power Supply Options

Model	Rajant Part Number	Type	Output Voltage (V)	Max. Output Current (A)	Ethernet Link Speed (Mbps)	Environmental
AC 24V	25-100168-001	AC to DC	24	0.8	10/100/1000	Non-sealed

Model	Rajant Part Number	Type	Output Voltage (V)	Max. Output Current (A)	Ethernet Link Speed (Mbps)	Environmental
AC 24V	25-100168-002	AC to DC	24	1.5	10/100/1000	Non-sealed
AC 48V	25-100172-001	AC to DC	48	1.04	10/100/1000	Non-sealed
DC-24V	25-100173-001	DC to DC	24	1.0	10/100/1000	Non-sealed

> ➲ **NOTE: Regarding 10/100 PoE power supplies**
> If a 10/100 PoE power supply is used to connect a gigabit-capable (1000 Mbps) BreadCrumb Ethernet port and a gigabit-capable (1000 Mbps) network switch, autonegotiation of Ethernet speed may may be very slow or may result in failed negotiation and no link. In this case, set the BreadCrumb configuration Ports: ethX: Port Speed explicitly to 100 Mbps.

Additional information about Rajant power supply accessories can be found in the Power Accessories product spec sheet at ➲ www.rajant.com.

2.4.2 PoE Power Supply Usage

The laptop in these diagrams could instead be a non-PoE switch port connecting the BreadCrumb to a LAN.

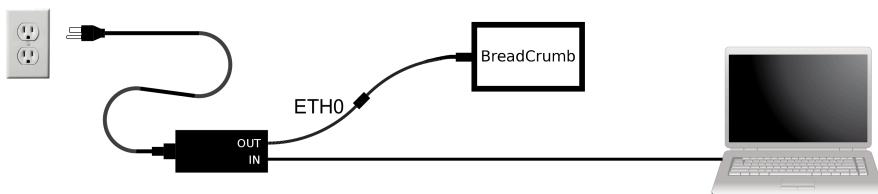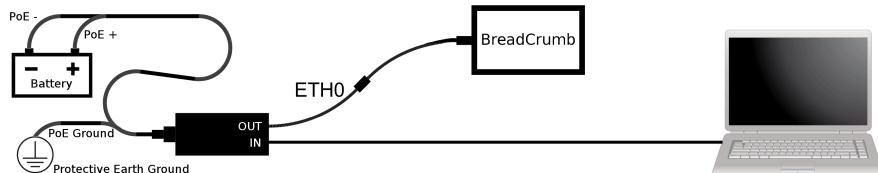*Figure: AG1 Cardinal Module Ethernet and Passive PoE AC Connections*

Figure: AG1 Cardinal Module Ethernet and Passive PoE DC Connections

The following steps describe the recommended best practice for connecting PoE power to the AG1 Cardinal Module.

1. Disconnect power from the PoE power supply.
2. Connect PoE *Out* to BreadCrumb using a shielded Ethernet cable.
3. (Optional) Connect PoE *In* (aka *Data*) to a computer or a non-powered LAN Ethernet port.
4. Reconnect power to the PoE power supply.

> ⚠ **Warnings: Regarding PoE Power Supply Connections**
> Unlike active PoE methods such as IEEE 802.3af/at, passive PoE does not include any kind of handshaking or voltage checking.
> - Only connect the passive PoE power supply Output to the BreadCrumb. The output power over Ethernet can damage other devices and may damage the PoE power supply.
> - Never connect the passive PoE power supply Output to an Ethernet port that supplies PoE power. This can damage equipment and may cause a fire. The Output should only be connected to the BreadCrumb.
> - Never connect the passive PoE power supply Input to an Ethernet port that supplies PoE power. Applying power to the PoE Input can damage the PoE power supply. For more information see the *Technical Bulletins* Appendix document: Never Apply Power to the Data Input Port of a Rajant Mid-Span Power over Ethernet (POE) Power Supply.
> - If you choose to connect a Rajant passive PoE-supporting BreadCrumb to an active PoE switch, you must first turn off the PoE capability of that switch port. For more information see the *Technical Bulletins* Appendix document: BreadCrumb Models Support Only Passive PoE.
> - Unsealed PoE power supplies are for indoor use only.

Please note that Rajant warranty protection does not cover any damage caused by misuse of power supplies or by use of third-party power supplies.

> **⚠ Warning**
>
> To avoid sparking and possible damage to the unit, connect the powered Ethernet Output cable to the BreadCrumb before applying power to the power supply.

> **⚠ Warning**
>
> To protect the user and the equipment against the risk of electric shock during high voltage transient events, which may occur when this equipment or its antennas are installed outdoors, protective earth grounding of the POE power supply is required. Case ground connections are provided on all POE power supplies supplied by Rajant. The case ground connections must be used and must be connected to a protective earth ground. Protective earth grounding operations must be performed by trained personnel and according to local electrical codes and industry best practices, as well as Rajant's own recommendations.

For more information on physical installation, grounding, waterproofing connections, see Installation Guidelines and the Appendix Technical Bulletins.

2.5 USB

The AG1 Cardinal Module includes a female USB 2.0 typeA connector which is found on the front of the AG1 Cardinal Module.

The port is compliant to the Enhanced Host Controller Interface (EHCI) and USB Transceiver 2.0 Macrocell Interface (UTMI+) Level 2 specifications. The port supports all three standard data transfer rates of low speed (1.5Mbps), full speed (12Mbps), and high speed (480Mbps). The power switch for the port includes over current protection, thermal protection, in-rush current limiting, and hot-plug noise filtering.

The USB port can be used to perform BreadCrumb firmware upgrades and USB-based zeroize (or alternately, these actions can be accomplished via software using BC|Commander). The USB port can also interface to an optional GPS receiver accessory available from Rajant.

2.6 Status LED

2.6.1 Status LED Operation

The Status LED is located on the top of the AG1 Cardinal Module enclosure.

The Status LED is used to indicate warning codes and error codes or the link state.

Table: Status LED Descriptions

Status LED Color and Behavior	Status
Green solid; Green slow blinking; Green fast blinking	Boot process
Green slow blinking	Ready, but no connected Mesh peers (unit may have Ethernet peers)
Green solid	At least one connected Mesh peer
Red blinking (with short and long pauses between blinks)	Numeric error code (see Appendix Error and Warning Codes
Green blinks, then red '32' error code for several seconds, then off	Zeroize (full) in progress
Rapid red-green, then off	Config Reset (brief Zeroize that retains logs)
Red, green, then longer off, all repeated	BreadCrumb configuration is locked; ready for reboot
Red and Green rapidly alternating	Identify mode is ON

2.6.2 LED Mode Setting

In BC|Commander, in the BreadCrumb configuration, in the General category, in the Status LED area, the LED Mode setting is used to set the mode of operation for the Status LED to **On** (default), **Alerts Only**, **Off** or **OFF (switchable)**.

When LED Mode is **On**, the Status LED will alternate between indicating the link state and indicating any warnings or errors.

When LED Mode is **Off** or **Off (Switchable)**, the Staus LED will not indicate any warnings, errors or the link state.

When LED Mode is **Alerts Only**, when the BreadCrumb has errors or warnings to report, the Status LED will alternate between indicating warning codes or error codes and indicating the link state. When there are no warnings or errors to report, the Status LED will indicate nothing.

The AG1 Cardinal Module Status LED can be red or green. The color and behavior of the Status LED indicates the BreadCrumb status, as described in the following table.

2.6.3 LED Status Mode Setting

In BreadCrumb firmware and BC|Commander version 11.21 or higher, in the BreadCrumb configuration, if the LED Mode setting is set to **ON** (default), the LED Status Mode setting must be set to define how to interpret the Status LED.

If LED Status Mode setting is set to **Cost to Gateway**, the BreadCrumb status is based on the InstaMesh cost to the IPv4 gateway. A solid green Status LED indicates that the BreadCrumb has a configured path to the gateway.

If LED Status Mode setting is set to **Mesh Peers**, the BreadCrumb status is based on the existance and speed of the mesh peer links. A solid green Status LED indicates that the BreadCrumb has at least one peer is running at an 802.11 data rate of 24 mbps or higher.

Prior to firmware and BC|Commander version 11.21, in the BreadCrumb configuration, in the InstaMesh category, then Advanced, in the Tracing area, selecting the **Enable Live Trace to Gateway** check box enabled the **Cost to Gateway** behavior for LED Status Mode setting.

3. Using BC|Commander

The Rajant BC|Commander software is the primary application for configuring and monitoring BreadCrumbs in an active mesh network. BC|Commander provides a graphical user interface to enable users to visualize an entire mesh network in real time and configure individual BreadCrumbs.

The *BC|Commander Version 11 User Guide* is available from the Tech Support section of Rajant's website at 🌐 http://www.rajant.com.

> ⚠ **Important**
> Rajant recommends that the active version of BC|Commander be equal to or greater than the BreadCrumb firmware version running on any BreadCrumbs in the mesh network.

The latest version of the BC|Commander software must be obtained from Rajant and then installed on at least one personal computer or laptop with a connection to the mesh network. For installation requirements and instructions, refer to the corresponding version of the *BC|Commander Version 11 User Guide*.

In BC|Commander, each user must log in to BreadCrumbs to obtain access privileges to perform tasks for a particular User role, as follows:

- **view (Read-Only Viewer):** Read-only access to BreadCrumb configuration and status information.
- **admin (Administrator):** Read access to BreadCrumb configuration settings and status information. Read/Write access to non-security-related BreadCrumb configuration settings. Permission to execute non-security-related BreadCrumb functions, such as reboot, upgrade firmware and zeroize.
- **co (Crypto Officer):** Read access to BreadCrumb status information. Read/Write access to all BreadCrumb configuration settings. Permission to execute all BreadCrumb commands, set encryption keys and set passwords.

All users must become familiar with the layout of the BC|Commander window.

All users must learn to use BC|Commander to do the following common procedures:

- Start BC|Commander and close BC|Commander
- Use the BreadCrumb Table and Topology View to monitor BreadCrumbs in the mesh network

Users who log in to BreadCrumbs with the appropriate user role can do the following procedures for BreadCrumbs:

- Change the default passwords for a BreadCrumb
- Compute the default IP address for a BreadCrumb
- Discover new BreadCrumbs
- Configure BreadCrumbs for operation
- Update BreadCrumb firmware
- Zeroize a BreadCrumb to remove security settings, restore default configuration settings and optionally clear internal logs and support data stored on the BreadCrumb

BC|Commander provides utilities to analyze network performance and perform troubleshooting tasks for BreadCrumbs during operation in a mesh network.

The user guide for each BreadCrumb model may contain BC|Commander procedures specific to that BreadCrumb model. BreadCrumb user guides are available from the Tech Support section of Rajant's website at 🌐 http://www.rajant.com.

4. Deploying a BreadCrumb Mesh Network

Many factors must be considered when deploying a BreadCrumb mesh network. This chapter describes the addressing scheme of the mesh, channel assignments and some of the most common environmental factors that will have a major impact on the performance of the mesh. The Deployment Methodology subchapter provides guidelines and a methodology for deploying the mesh.

For information on physical installation, grounding waterproofing connections, see Installation Guidelines and the Appendix Technical Bulletins.

4.1 Addressing

When in gateway mode or when using its own embedded DHCP servers, the BreadCrumb mesh 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 your network is not connected to another network or your network is bridging to another network, rather than routing to the network, the wireless client devices may not have any addresses whatsoever.

> **❂ Note**
> Each BC|Commander host must have an address in the same range as the managed BreadCrumbs. Refer to the *BC|Commander Version 11 User Guide* for details about IP address configuration for a BreadCrumb.

4.1.1 BreadCrumb Device Addresses

Each BreadCrumb radio has one IPv4 address in the Class A network 10.0.0.0/8. During the manufacturing process, Rajant ensures that default addresses are not duplicated between any two BreadCrumb devices. Addresses assigned to BreadCrumb devices can be viewed in BC|Commander. Addresses can be configured manually or set to **DHCP**.

4.1.2 DHCP

Each BreadCrumb device includes an embedded DHCP server. You may safely enable the DHCP servers of multiple BreadCrumb devices simultaneously. 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 IPv4 address for the BreadCrumb.
- Add a low-byte range of 10 to 210.

4.2 Channel Assignments

Each BreadCrumb radio has default channels assigned based on the frequency and type of the radio.

The following table lists each radio frequency and the corresponding default channel assignments. When more than one radio of the same frequency is present, there may be default channels for the additional radios. This table includes radios that may be found in various BreadCrumb models, not one specific model.

Table: Default Channel Assignments

Radio Card Frequency and Type	Default Channel	Second Default	Third Default
900 MHz 802.11g/900 MHz 802.11n	5		
2.4 GHz 802.11n	11	1	
2.4 GHz 802.11g	11	1	
4.8 GHz 802.11a	164	184	174
4.9 GHz 802.11a	20		
5 GHz 802.11a	153	161	
5 GHz 802.11ac	FCC:157, CE:136	FCC:48, CE:100	
5 GHz 802.11n (ME4, LX5)	FCC:157, CE:136	FCC:149, CE:100	
5 GHz 802.11n (ES1)	FCC:157, CE:136	FCC:48, CE:100	
Dual band 2.4/5 GHz 802.11n	11 (2.4 GHz)		

In some cases, it may be necessary to manually set the radios to specific channels to provide critical links within a mesh. This can be especially important when using single-radio BreadCrumb devices. Refer to the *BC|Commander Version 11 User Guide* for the details about BreadCrumb channel configuration.

4.3 Physical Placement and other Considerations

Commonly occurring environmental factors have a significant impact on performance and behavior of the BreadCrumb Wireless Network. Line-of-sight (LOS) 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 mesh network is to maximize both coverage and the data transfer rate between devices by taking into consideration all of the contributing factors described in this section.

4.3.1 Line-of-Sight

Unobstructed line-of-sight (LOS) between BreadCrumb and wireless client devices is critical for optimal performance of the mesh. 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 to enable radio waves to propagate over some possible obstructions.

Each BreadCrumb must have unobstructed LOS to the previous and subsequent BreadCrumb.

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

Unobstructed LOS is not necessary from every BreadCrumb and wireless client device to every other BreadCrumb and wireless client device.

Fresnel Radius

In BC|Commander version 11.9 or later, on the **Peers** tab, the radius value in the **Fresnel Radius** column can help determine where antennas must be placed for the wireless signal to sufficiently clear any obstacles between two BreadCrumbs. Obstacles include buildings, trees, vehicles and the ground.

In the following figure, "r" represents the radius of the first Fresnel Zone at a point halfway between two peer BreadCrumbs.
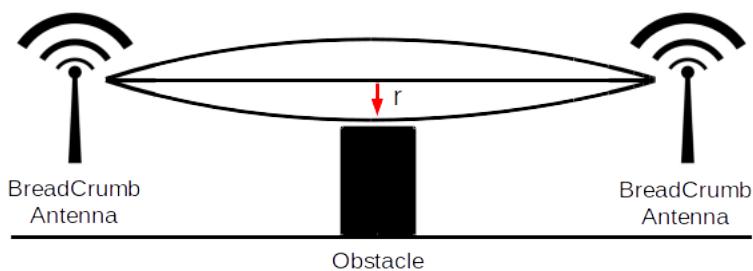
In the BreadCrumb configurations for two peer BreadCrumbs, when the **Latitude** settings and **Longitude** settings are correct, the **Fresnel Radius** column will contain the value "r" for both BreadCrumbs. The greater the distance between the peer BreadCrumbs, the greater the value "r" will be.

Rajant recommends that antennas be placed to achieve at least 60% (ideally 80%) first Fresnel Zone clearance in all directions.

For obstacles that are closer to one of the peer BreadCrumbs, BreadCrumb antennas with unmatched elevations or BreadCrumb placements affected by the curvature of the Earth use a Fresnel Zone calculator that includes obstacle distance and other factors.

Antenna Tuning

BC|Commander version 11.9 or later can monitor the quality of a single wireless connection between two BreadCrumbs for the purpose of antenna tuning (aka antenna peaking).

To use the Antenna Tuning feature, the BC|Commander host must be on the same network/subnet as the BreadCrumbs being monitored and must be able to directly connect to the BreadCrumbs.

To monitor the quality of a wireless connection between a selected BreadCrumb and a peer BreadCrumb, do the following:

1. If BC|Commander is currently viewing the mesh through a BC|Connector, to switch to a Live Mesh view, on the **Mesh** menu, click **Live Mesh**.
2. In the BreadCrumb table, select a BreadCrumb. The **Peers** tab lists each peer BreadCrumb for the selected BreadCrumb and the network device for each peer connection.
3. On the **Peers** tab, right-click the row for a wireless peer connection, and then click **Antenna Tune**. The **Antenna Tune** dialog box opens and begins to graph the signal-to-noise (SNR) ratio, Signal and Cost as reported by the selected BreadCrumb and peer over the wlan link indicated for the peer BreadCrumb.

The BreadCrumbs being monitored will send wireless connection information to BC|Commander at one-second intervals (regardless of the BreadCrumb configuration setting *BCAPI: General Update Interval*). These accelerated updates will continue until the **Antenna Tuning** dialog box is closed.

Each graph is a sliding window view of the collected information and will begin to discard/age-out older data after 4 minutes of usage. Historical data is not maintained.

If either BreadCrumb were to lose the peer connection, the graphs will flatline or pause until the connection is restored. If BC|Commander were to lose connection to one of the BreadCrumbs, graphing will pause until the connection is reestablished.
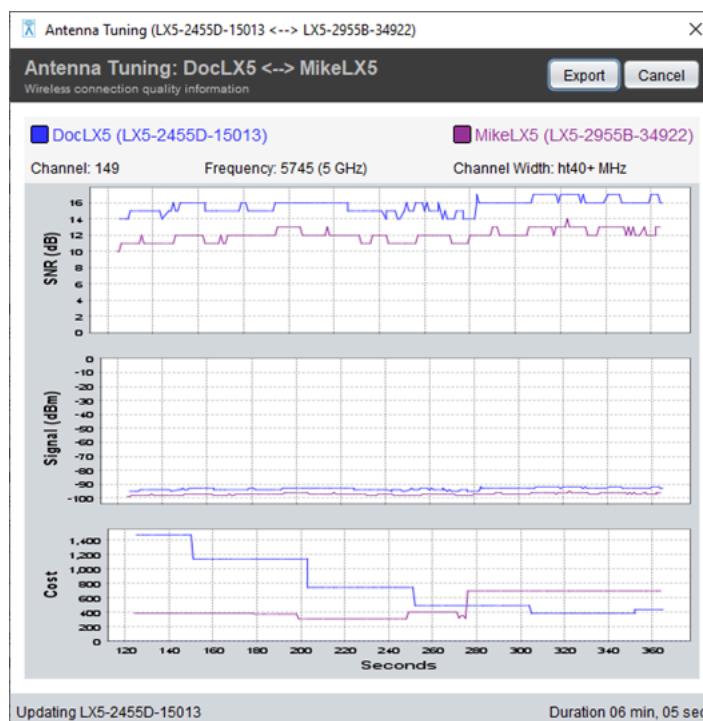
> **→ Note**
> The Antenna Tuning feature is unlikely to work well with BreadCrumbs running firmware prior to version 11.8, where on-demand fast updates of cost, signal and SNR were added for antenna tuning.

> **⚠ CAUTION:**
> If multiple **Antenna Tuning** dialog boxes are open simultaneously, each will add additional traffic on the mesh and use additional resources on the BC|Commander host. Reconfiguring a BreadCrumb during Antenna Tuning may lead to unexpected anomalies in BC|Commander and is strongly discouraged.

4.3.2 Distance

Many factors determine the acceptable distance between BreadCrumbs when deploying a mesh, for example:

- If many BreadCrumbs are placed too closely together, interference may degrade system performance.
- A BreadCrumb that is placed too far away from another BreadCrumb or in an RF "shadow" may experience total loss of connection.
- RF transmit power and receive sensitivity are important in determining the distances over which the BreadCrumb device will be effective.

- When placing a BreadCrumb, use the BreadCrumb Status LED or BC|Commander to check the connection status to the nearest available BreadCrumb. If the connection is poor or non-existent, attempt to place the BreadCrumb closer to another BreadCrumb until an acceptable connection is made. If a poor connection or no connection is made at even relatively close distances, refer to the Troubleshooting chapter.
- When the connection quality indicated in BC|Commander is found to be acceptable, the distance of the BreadCrumb from the network can be increased until an optimal balance between distance, connectivity and tactical placement is achieved.

4.3.3 Weather

Precipitation and fog act as obstructions that block the propagation of radio waves in the wireless network.

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 BreadCrumbs to the network to act as short haul repeaters to counteract the effects of the weather. An alternative is to move the BreadCrumbs closer together.

4.3.4 Interference

RF interference can degrade network performance. RF interference can come from various sources, including:

- Other BreadCrumbs 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 multi-path interference.

> ⚠ **Caution**
> Plan the BreadCrumb wireless network to minimize the effects of RF interference.

4.3.5 Placement of Mesh Components

The placement of BreadCrumbs has a major impact on maximum effective range and, therefore, network performance. Each component must be elevated above the surrounding terrain to allow for adequate wave propagation. A device that is placed directly on the ground has a significantly reduced effective range. Elevating a device above the ground will dramatically increase the maximum effective range. Rajant recommends elevating each component a minimum of 6 feet above the surrounding terrain.

4.4 Deployment Guidelines and Methodology

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

4.4.1 Deployment Guidelines

Follow these guidelines when deploying the mesh:

1. Placement of BreadCrumbs
   a. Directly on the ground, the maximum distance between two successive BreadCrumbs is approximately 300 feet.
   b. Directly on the ground, the maximum distance between a wireless client and the nearest BreadCrumb is approximately 300 feet.
   c. Elevate a BreadCrumb above the surrounding terrain whenever possible.
   d. Rajant recommends elevating a BreadCrumb a minimum of 6 feet for maximum range.
   e. Elevating a BreadCrumb as little as 14 inches has proven to increase the range approximately 600 feet.
2. Distance
   a. BreadCrumbs that cannot be elevated can be no more than approximately 300 feet apart.
   b. Any wireless client device can be no more than approximately 300 feet from a BreadCrumb.
3. Line-of-sight (LOS)
   a. Obstructions to LOS block/absorb/deflect radio waves in a wireless network, resulting in poor network performance or total loss of network connectivity.
   b. When placing a BreadCrumb, scan the area for LOS obstructions. Envision the BreadCrumb's radio waves as a light beam. Look for obstructions that would result in shadows in the light beam.

These obstructions will most likely weaken or block the BreadCrumb's radio waves.

4. Weather
    a. Light precipitation will reduce the range and performance of a BreadCrumb and wireless client devices.
    b. Heavy precipitation or fog will most likely result in extremely reduced range and frequent or total loss of network connectivity.

4.4.2 Deployment Methodology

The deployment process for the mesh consists of deploying each BreadCrumb. The deployment process for a BreadCrumb consists of installing the BreadCrumb hardware, powering up the BreadCrumb and waiting for the BreadCrumb to boot. BC|Commander can then discover the BreadCrumb in the network.

To achieve optimal performance for BreadCrumbs in a mesh network, refer to the Rajant *Troubleshooting Range User Guide* available from the Tech Support section of Rajant's website at ⊕ http://www.rajant.com.

To successfully deploy BreadCrumbs in the mesh, adhere to the following steps:

1. Determine the location where each BreadCrumb is to be deployed within the mesh network.
    a. Scan the terrain where BreadCrumbs are to be deployed.
    b. Determine a proposed location for each BreadCrumb.
    c. Note any LOS obstructions from that location.
    d. Designate a target location for each BreadCrumb to work around any LOS obstructions.
2. Designate BC|Commander host(s) to be used to deploy BreadCrumbs.
    a. Designate a user who is to monitor the deployment of BreadCrumbs in the network from a stationary BC|Commander host, such as a personal computer.
    b. Designate each user who is to transport and then deploy each BreadCrumb at each location. Each user must also carry a portable BC|Commander host, such as a laptop with a wireless Network Interface Card (NIC), to each BreadCrumb location.
    c. Each user for a portable BC|Commander host requires a mobile device (radio, cell phone, etc.) to communicate with other users in the field.
3. Deploy the first BreadCrumb, as follows:
    a. Determine the location for the BreadCrumb.
    b. Transport the BreadCrumb to the designated location.
    c. Power ON the BreadCrumb.
    d. Wait approximately 90 seconds for the BreadCrumb to boot.
    e. Start BC|Commander on the BC|Commander host(s).
    f. Wait for BC|Commander to discover the BreadCrumb.
    g. In BC|Commander, verify that the BreadCrumb is listed in the BreadCrumb Table or shown in the Topology View.
4. Deploy each subsequent BreadCrumb, as follows:
    a. While at the location of a deployed BreadCrumb, determine the target location for the next BreadCrumb.
    b. Proceed to the target location for the next BreadCrumb while monitoring network connectivity in BC|Commander.
    c. If network connectivity is lost before reaching the target location, backtrack until network connectivity is restored. The location where network connectivity is restored is most likely the farthest point in this direction where this BreadCrumb can be deployed.
    d. When a location is reached without losing network connectivity, to deploy the BreadCrumb at that location, complete Steps 3.c through 3.g.

5. Firmware Upgrade and Zeroize Processes

5.1 BreadCrumb Firmware Releases

5.1.1 Description

Each BreadCrumb model includes firmware to support specific functional, operational and administrative capabilities.

Rajant sells each BreadCrumb model with the latest version of firmware already installed on the BreadCrumb. Rajant will then routinely release updates to the BreadCrumb firmware to add new product features, support new applications and fix reported problems.

BreadCrumb firmware releases usually coincide with major releases of Rajant software products, particularly the BC|Commander software. An interim release of BreadCrumb firmware may occur, as needed, between major software releases.

A BreadCrumb firmware release file may apply to one or more BreadCrumb models.

5.1.2 BreadCrumb Firmware Release Names

The name for a BreadCrumb firmware release is listed on the Rajant Support page in the following format:

```
Firmware *model-list* *version*
```

where,

```
Firmware indicates a BreadCrumb firmware release.

*model-list* is a space-separated list of model name identifiers for each affected
BreadCrumb model.

*version* identifies the version number for the firmware release in the format
v11.*xx*.*y*.
```

Example:

```
Firmware DX2 ES1 FE1 JR3 KM3 LX5 ME4 SLIPSTREAM v11.25.0
```

5.1.3 Downloaded BreadCrumb Firmware Release File Names

A downloaded BreadCrumb firmware release file is a .flash file named in the following format:

breadcrumb*model-list**version*_b*n*-release.flash

where,

breadcrumb indicates a BreadCrumb firmware release file.

model-list is an underscore-separated list of model name identifiers for each affected BreadCrumb model.

version identifies the version number for a major BreadCrumb firmware release in the format v11.*xx.y*.

b*n* indicates the build number, *n*, for an update to a major BreadCrumb firmware release.

Example:

breadcrumb_ DX2_ES1_FE1_JR3_KM3_LX5_ME4_SLIPSTREAM_v11.25.0_b13-release.flash

5.1.4 Firmware release version numbers

Each firmware release is identified by a version number in the following format:

```
v11.*xx*.*y*_b*n*
```

where,

```
v11 is the base firmware version.

*xx* is a major firmware release number.

*y* is an update to a major firmware release.

*n* is a build number for an update to a major firmware release.
```

5.1.5 Requirements

To enable BreadCrumbs in a mesh network to communicate with each other and with BC|Commander, all BreadCrumbs in the network must be operating with compatible firmware versions that are also compatible with the version of the BC|Commander software in use throughout the network.

The Rajant customer is responsible for maintaining the BreadCrumb firmware throughout the network.

To maintain the BreadCrumb firmware on each BreadCrumb, the Rajant customer must do the following:

1. Check for available updates to BreadCrumb firmware for each BreadCrumb model in use in the network.
2. Download the firmware update file from the Rajant Support web site to the BC|Commander host.
3. Upload the latest firmware file from the BC|Commander host to each affected BreadCrumb remotely using BC|Commander or locally using a USB flash drive at the BreadCrumb location.

5.2 Check for Available Updates to BreadCrumb Firmware

The customer is responsible for checking for available updates to BreadCrumb firmware files.

A customer can view a list of the latest available updates to BreadCrumb firmware release files for all BreadCrumb models managed by BC|Commander at that site.

To view the latest available updates to BreadCrumb firmware release files, do the following:

1. In BC|Commander, on the **Help** menu, point to **Check for Updates…**, and then click **Firmware Upgrades…**. The **Firmware Upgrades** dialog box opens. A list of the latest available updates to BreadCrumb firmware release files for all BreadCrumb models managed by BC|Commander at that site is displayed.
2. Determine which available update files should be downloaded to the BC|Commander host at this time.
3. Click **Close**. The **Firmware Upgrades** dialog box closes.

5.3 Download an Update File for a BreadCrumb Firmware Release

A customer can use BC|Commander to download an update file for a BreadCrumb firmware release from the Rajant Support web site to a BC|Commander host.

To download an update file for a BreadCrumb firmware release, do the following:

1. In BC|Commander, on the **Help** menu, point to **Check for Updates…**, and then click **Firmware Upgrades…**. The **Firmware Upgrades** dialog box opens. A list of the latest available updates to BreadCrumb firmware release files for all BreadCrumb models managed by BC|Commander at that site is displayed.
2. Determine which available update files should be downloaded to the BC|Commander host at this time.
3. To the right of the name of the file that is to be downloaded, click **Download**. The **Login** page for the Rajant Support web site opens.
4. Supply your email address and Password for the Rajant Support web site.
5. Click **Login now**. The Rajant Downloads page opens for the selected BreadCrumb firmware release file.
6. Wait for the file to be downloaded to the **Downloads** folder on BC|Commander host.

5.4 Upload BreadCrumb Firmware Remotely

After a firmware file has been downloaded to the BC|Commander host, the customer can use BC|Commander to remotely upload and install a firmware file for a AG1 Cardinal Module, from the BC|Commander host to the BreadCrumb. For instructions, refer to the *BC|Commander Version 11 User Guide*.

> ⚠ **CAUTION**
> Do NOT turn off or reboot a BreadCrumb while new firmware is being installed. An interruption to power during the firmware installation process can result in the BreadCrumb being unable to boot properly.

5.5 Upload Firmware on Location at the BreadCrumb

On a BreadCrumb that has a Universal Serial Bus (USB) port, a USB storage device can be used to upgrade the BreadCrumb firmware at the BreadCrumb location.

To use a USB storage device to upgrade firmware on a BreadCrumb, do the following:

1. Use BC|Commander to prepare a USB storage device that contains the updated firmware file. For instructions, refer to the *BC|Commander Version 11 User Guide*.

2. Do one of the following:
   - If the BreadCrumb is powered ON, connect the USB storage device to the USB port on the BreadCrumb.
   - If the BreadCrumb is powered OFF, connect the USB storage device to the USB port, and then power ON the BreadCrumb.

   The firmware upgrade process begins automatically.

> ⚠ **CAUTION**
> Do NOT turn off or reboot a BreadCrumb while new firmware is being installed. An interruption to power during the firmware installation process can result in the BreadCrumb being unable to boot properly.

3. Observe the Status LED on the BreadCrumb for several minutes to monitor the progress of the firmware upgrade.
   a. When the USB firmware upgrade begins, the Status LED will start blinking yellow once per second to indicate progress. When the upgrade process nears completion, the blink rate will increase to several times per second.
   b. If the firmware upgrade completes successfully, the color of the Status LED will rapidly rotate between red, green, blue, cyan, magenta, yellow and white.
   c. If an error condition occurs, the Status LED will repeat a particular sequence of long and short blinks in red to indicate an error code. Do the following:
      1) Take note of the error code.
      2) For error code descriptions, see Appendix Error and Warning Codes.
      3) Leave the USB storage device connected.
      4) Turn OFF power to the BreadCrumb.
      5) Turn ON power to the BreadCrumb. A second firmware upgrade is attempted.
      6) Observe the Status LED to monitor the progress of the second firmware upgrade. If another error occurs, take note of the new error code and then apply for technical support.
4. When the USB upgrade process is complete, power OFF the BreadCrumb.
5. With the BreadCrumb powered OFF, disconnect the USB storage device.
6. Power ON the BreadCrumb. The BreadCrumb reboots with the updated firmware.

5.6 Zeroize

5.6.1 Remote Zeroize Process

BC|Commander provides a remote Zeroize process for a wired or wireless BreadCrumb.

The remote Zeroize process for a BreadCrumb, completes the following actions:

1. Deletes all security keys from the BreadCrumb configuration.
2. Restores all BreadCrumb configuration settings to the factory default values.
3. (Optional) Clears all internal logs and other support data stored on the BreadCrumb.
4. Reboots the BreadCrumb.

> ➲ **NOTE:**
> The option to clear or retain all internal logs and other support data is available with firmware version 11.17.7 or later.

To perform the remote Zeroize process for a BreadCrumb, refer to the *BC|Commander Version 11 User Guide* for instructions.

> ⚠ **CAUTION**
> Do NOT turn off or reboot a BreadCrumb during the Zeroize process. An interruption to power during the zeroize process can result in the BreadCrumb being unable to boot properly.

> ⚠ **Important:**
> A remotely Zeroized BreadCrumb will not be able to mesh with properly-configured BreadCrumbs. Reapplication of mesh settings to the zeroized BreadCrumb may require an Ethernet connection or a mesh connection with another Zeroized BreadCrumb.

5.6.2 USB-based Zeroize Process

On a BreadCrumb that has a Universal Serial Bus (USB) port, a USB storage device can be used to perform the Zeroize operation. The USB-based zeroize operation does not affect the firmware version running on the BreadCrumb.

The USB-based Zeroize process for a BreadCrumb completes the following actions:

1. Deletes all security keys from the BreadCrumb configuration.
2. Restores all BreadCrumb configuration settings to the factory default values.
3. Clears all internal logs and other support data stored on the BreadCrumb.

4. Reboots the BreadCrumb.

To perform a USB-based Zeroize operation for a BreadCrumb, do the following:

1. In BC|Commander, use the USB Flash Manager utility to prepare a USB storage device for use in a Zeroize operation. For instructions, refer to the *BC|Commander Version 11 User Guide*.
2. Connect the USB storage device to the USB port on the BreadCrumb (and, if the BreadCrumb is powered OFF, power ON the BreadCrumb at this time).

> **⊘ Note**
> The USB flash drive can be connected to a live BreadCrumb. The zeroize process will begin automatically.

3. The USB-based zeroize process will finish in less than one minute. Observe the Status LED on the BreadCrumb to monitor progress. Warning 321 "BreadCrumb has been zeroized" should be displayed. Then wait for the LED to flash error code 32 "BreadCrumb has been zeroized".
4. Power OFF the BreadCrumb, disconnect the USB storage device, and then power ON the BreadCrumb.

6. Troubleshooting

> **➲ Note**
> Battery tips apply to any BreadCrumb that is powered by batteries, solar power or any power source that may become irregular or weak.

> **➲ DFS and Troubleshooting**
> When troubleshooting problems with a BreadCrumb radio on a 5 GHz DFS channel, remember that a radio must listen for radar and not transmit (or mesh) for typically 1 minute after the BreadCrumb is fully-booted. Channels in frequencies 5600-5650 MHz, if available, may require a 10-minute wait. In addition, if a radar-like noise pattern is detected on the channel, the radio will shut down for 30 minutes. For more information, including some potential causes of false radar detections, see Appendix Radio Channels and Frequencies, DFS and TPC.

6.1 Sporadic Network Connectivity

Issue: If a BreadCrumb is powered by a battery, as the battery approaches exhaustion, network connectivity will become sporadic for the BreadCrumb and its associated wireless client devices.

Corrective action: Monitor battery usage and charge or replace batteries as necessary.

Issue: Light precipitation or fog beginning after initial deployment of the mesh can result in sudden sporadic network connectivity for BreadCrumbs and their associated wireless client devices. **Corrective action:** Increase the density of the network by adding more BreadCrumbs or moving existing BreadCrumbs closer together.

Issue: As a mobile wireless client device moves through the coverage area, line of sight (LOS) to a BreadCrumb can become obstructed resulting in sporadic network connectivity for a wireless client device.

Corrective actions: * Train users of mobile wireless client devices to maintain LOS to known BreadCrumb locations. * Place BreadCrumbs strategically to ensure coverage of areas through which users are expected to move.

Issue: A mobile wireless client device that moves beyond the range of the mesh will experience sporadic and, eventually, complete loss of network connectivity.

Corrective action: Drop more BreadCrumb devices as necessary to increase range.

Issue: A wireless client device cannot join the network.

Corrective actions: * Ensure that BreadCrumbs are powered on. * In the BreadCrumb configuration, for the wlanx interface, select the Enable Access Point check box. By default, the Enable Access Point check box is cleared. * In the wireless client device, ensure that the wireless card is enabled. This is usually indicated by a blinking LED on the card. * Use the software for the wireless card for the client devise to scan for the ESSID configured for the network (default "rajant"). Ensure that the wireless card is in Infrastructure mode or Access Point mode, not Ad Hoc mode. * Ensure that the IP address settings for the wireless client device are correctly configured.
* Ensure that the security settings on the wireless client device and the BreadCrumbs match. * Ensure that the wireless client device is not prevented from connecting by an Access Control List (ACL) in the BreadCrumb configurations. * Ensure that the VLAN settings for the BreadCrumbs allow clients of the ESSID being used to communicate to the Local Port of the BreadCrumb. For more information, in the *BC|Commander Version 11 User Guide*, refer to the "Using VLANs with BreadCrumbs" chapter.

6.2 BreadCrumb Device Cannot Connect to Mesh

Issue: A new BreadCrumb or a BreadCrumb that has been reset to factory defaults is running with BreadCrumb configuration settings that do match the network to be joined.

Corrective action: In the BreadCrumb configuration, configure the Network settings to match the network to be joined.

Issue: Discharged batteries can cause the BreadCrumb to appear to power up, but be unable to establish connectivity to the mesh.

Corrective action: When deploying any battery-powered BreadCrumbs to the mesh, ensure that the batteries are fully charged.

Issue: When using external antennas, faulty cable connections or crimped cables can result in difficulty establishing and maintaining network connectivity.

Corrective action: Check antenna cables and their connections to the BreadCrumb.

6.3 BreadCrumb Power and Start-up Issues

Issue: Discharged external batteries can cause a BreadCrumb power LED to turn on, although the BreadCrumb fails to start.

Corrective action: Monitor battery usage and charge/replace batteries as necessary.

Issue: Electrostatic Discharge can cause a BreadCrumb power LED to turn on, although the BreadCrumb fails to start.

Corrective action: Manually reboot the BreadCrumb by turning off the BreadCrumb or disconnecting power to the BreadCrumb and then power-up the BreadCrumb.

> ⚠ **Caution**
> To avoid sparking and possible damage to the BreadCrumb, be sure to connect the power cable to the BreadCrumb before applying power to the power supply.

7. Appendices

Appendix A: Radio Channels and Frequencies

A Rajant BreadCrumb contains from one to four radios, depending on the model. 802.11g radios are used in the 900 MHz and 2.4 GHz bands. 802.11a radios are used in the 4.8 GHz, 4.9 GHz and 5 GHz bands. 802.11n radios are used in the 2.4 GHz and 5 GHz bands. Each BreadCrumb model supports a specified radio or combination of radios.

The radios support the channels and frequencies listed in the following tables. The channels that are available for use in each country are specified by a local regulatory agency.

> **⊙ 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 each country.

> **⚠ CAUTION**
> Because radios operate at different frequencies, each radio must use the correct type of antenna for that radio. For example, a 2.4 GHz antenna will not work with a 5 GHz radio and vice versa.

A.1 Radio: 2.4 GHz 802.11n

Table: 2.4 GHz 802.11n Radio Channels and Frequencies

Channel Number	Center Frequency (MHz)	HT40 Capability
1	**2412**	HT40 +
2	2417	HT40 +
3	2422	HT40 +
4	2427	HT40 +
5	2432	HT40 +, HT40 -
6	2437	HT40 +, HT40 -
7	2442	HT40 +, HT40 -
8	2447	HT40 +, HT40 -
9	2452	HT40 +, HT40 -
10	2457	HT40 -
11	**2462**	HT40 -
12	2467	HT40 -
13	2472	HT40 -
14	2484	HT20 only

The default channel and channel mode for a BreadCrumb 2.4 GHz 802.11n radio is 11 (2462 MHz) and HT20. If a second 2.4 GHz 802.11n radio is present, its default channel and channel mode is 1 (2412 MHz) and HT20.

2.4 GHz channels support HT40 mode. In HT40 mode, the radio binds two standard 20 MHz channels to obtain a wider bandwidth 40 MHz channel. The + or - designates the second channel as above or below the base channel. Plus (+) indicates that the additional 20 MHz occurs above (at a higher frequency than) the first 20 MHz. Minus (-) indicates that the additional 20 MHz occurs below (at a lower frequency than) the first 20 MHz.

> **⊙ Note**
> The frequency indicated is the center frequency of the base 20 MHz channel. HT40 operation (+ or -) is compatible with 802.11b and 802.11g 20 MHz, and 802.11n HT20 modes.

A.2 Radio: 5 GHz 802.11ac

Table: 5 GHz 802.11ac Radio Channels and Frequencies

Channel Number	Center Frequency (MHz)	HT40 Capability	VHT80 Capability
36	5180	HT40 +	VHT80
40	5200	HT40 -	VHT80
44	5220	HT40 +	VHT80
48	**5240**	**HT40 -**	**VHT80**
52	5260	HT40 +	
56	5280	HT40 -	
60	5300	HT40 +	
64	5320	HT40 -	
100	5500	HT40 +	
104	5520	HT40 -	
108	5540	HT40 +	
112	5560	HT40 -	
116	5580	HT40 +	
120	5600	HT40 -	
124	5620	HT40 +	
128	5640	HT40 -	
132	5660	HT40 +	
136	5680	HT40 -	
140	5700	HT20 only	
144			VHT80 only
149	5745	HT40 +	VHT80
153	5765	HT40 -	VHT80
157	**5785**	**HT40 +**	VHT80
161	5805	HT40 -	VHT80
165	5825	HT20 only	

In the United States, for a BreadCrumb 5 GHz 802.11ac radio, the default channel number is 157 (5785 MHz) with channel mode HT40+. If a second 5 GHz 802.11ac radio is present, the default channel number for that radio is 48 (5240 MHz) with channel mode HT40-.

In Canada, for a BreadCrumb 5 GHz 802.11ac radio, the default channel number is 157 (5785 MHz) with channel mode HT20+. If a second 5 GHz 802.11ac radio is present, the default channel number for that radio is 48 (5240 MHz) with channel mode HT40-.

In most European countries, the default channel number is 136 (5680 MHz) with channel mode HT40-. If a second radio is present, the default channel number is 100 (5500 MHz) with channel mode HT40+. In other European countries, the default channels may differ based on local regulations.

> **⊙ Note**
> If the default channels are not available, the default channel will instead be the first valid channel (in order by channel number) with the largest bandwidth (up to 20 MHz) that does not conflict with other radios. If that fails, meshing will be disabled on that radio.

Some 5 GHz channels support HT40 mode. In HT40 mode, the radio binds two standard 20 MHz channels to obtain a wider bandwidth 40 MHz channel. The + or - designates whether the second channel is above or below the base channel. Plus (+) indicates that the additional 20 MHz occurs above (at a higher frequency than) the first 20 MHz. Minus (-) indicates that the additional 20 MHz occurs below (at a lower frequency than) the first 20 MHz.

5 GHz channels support VHT 80 mode. In VHT 80 mode, the radio bonds four contiguous 20 MHz channels to obtain a wider bandwidth 80-MHz channel. One of these 20 Mhz channels is the "control channel" for the 80 Mhz channel.

In BC|Commander, in the BreadCrumb configuration, for wlan0 and wlan1, the Channel Number list is used to select the channel number and center frequency for the 20 MHz control channel for the 80 MHz

channel.

The following six 80 Mhz channels are available:

- The first 80 Mhz channel bonds channels 36+40+44+48.
- The second 80 Mhz channel bonds channels 52+56+60+64.
- The third 80 Mhz channel bonds channels 100+104+108+112.
- The fourth 80 Mhz channel bonds channels 116+120+124+128.
- The fifth 80 Mhz channel bonds channels 132+136+140+144.
- The sixth 80 Mhz channel bonds channels 149+153+157+161.

To determine which channels support VHT 80 mode, refer to the latest channel plan at the following Web page:

🌐 https://secure.rajant.com/staticFiles/latest/channelPlans/FE1-2255B.html

> **↻ Note**
> The 802.11ac frequency is the center frequency of the base 20 MHz channel. This is different from 802.11a turbo mode, where the frequency was the center of a single 40 MHz wide channel. HT40 operation (+ or -) is compatible with 802.11a 20 MHz mode and 802.11ac HT20 mode. HT40 operation is NOT compatible with 802.11a turbo mode.

> **⚠ Caution**
> Most 5 GHz antennas support only a subset of the 802.11ac 5 GHz frequency channels at which the Rajant radio is capable of operating. Before changing the channel of a 5 GHz radio, verify that the channel is supported by the connected antenna.

> **⚠ IMPORTANT: Regarding indoor-only frequencies**
> In regions where radio frequencies are regulated by ETSI (CE), the frequency range 5170-5350 MHz is restricted to indoor use only. Check local regulations before using these channels.

> **⚠ IMPORTANT**
> In many regions where radio frequencies are regulated by ETSI (CE), a license is required to use channels in the frequency range 5735-5835 MHz (on models that offer these channels). Check local regulations before using these channels.

> **⚠ IMPORTANT**
> In Canada, a license is required to use channels in the frequency range 5150-5250 MHz (on models that offer these channels). The license may restrict transmit power. Licensing information may be found at 🌐 http://www.ic.gc.ca/eic/site/smt-gst.nsf/eng/sf11294.html.

A.3 DFS and TPC

DFS and TPC for 5 GHz Channels

Many channels in the 5 GHz band are subject to Dynamic Frequency Selection (DFS) regulations that require active avoidance of interference with weather radar and other radars. In many countries, regulations also require Transmit Power Control (TPC), lower transmit power for nearby wireless connections on the same channels. In some countries, DFS channels may be available for use on BreadCrumbs with 5 GHz radios that provide hardware support for radar detection.

The list of 5 GHz channels that are subject to DFS and TPC regulations depends on the regulatory domain of the region of operation. In many regions, any available channels from 5260-5700 MHz require DFS or DFS and TPC. In some regions, additional channels require DFS and TPC.

DFS channels will not be available immediately upon BreadCrumb startup and will become non-operational for a fixed period of time after radar or any radar-like pulse of noise is detected.

DFS Behavior for a BreadCrumb

DFS behavior for a BreadCrumb is the following:

- **After power-on or restart, all transmits on a DFS channel will be disabled for 1 minute** (typically) while the radio performs the Channel Availability Check (CAC) to pre-check for radar on that channel. After 1 minute without detecting radar, the radio can start normal operation on the channel while still continuously checking for radar. Note: Channels from 5600 MHz to 5650 MHz, if available, may have a 10-minute CAC period.
- **If radar detection is triggered on a DFS channel, that radio will stop transmitting for 30 minutes**, the Non-Occupancy Period (NOP). If the affected unit was able to report its warning status over another radio or over Ethernet, in BC|Commander, a Warning code 382 "Radar detection paused radio: wlan*x* (wlan*x* …)" will be displayed.
- **After the NOP, before reusing the DFS channel, the radio must not transmit for 1 additional minute** (perhaps 10 minutes for 5600-5650 MHz) during the CAC. If no radar is detected during the CAC, normal radio operation is resumed with continuous checking for radar.

- **When resuming normal operation after a radar detection,** the radar detection warning 382 will be removed from the radio and a warning 383 "Radio resumed from radar pause: wlanx (wlanx, …)" will be added. The "unpaused" warning 383 will remain for 12 hours so that network personnel will know which radios were affected by DFS stoppages. Warning 383 will be removed when all listed radios have been aged out.

About Radar Detection

Radar is detected as pulses (spikes) of radio frequency (RF) noise. If pulses of noise make it past several range checks, and the pattern of pulses is sufficiently similar to a radar pattern, a radar detection event will occur. False detections may be caused by anything that creates RF interference, including electrical equipment, improperly positioned antennas, nearby wireless radio devices and RF reflections caused by antennas that are too close to the ground, walls or other RF-reflecting surfaces.

If possible, use of DFS channels should be avoided for critical network paths, especially if the BreadCrumb has no other Ethernet or wireless network connections to the mesh.

> **⦿ DFS Additional Antenna Separation**
> For 5 GHz transceivers using channels that require DFS radar detection, a recommendation is to mount each antenna for a DFS channel at least 2 feet from the antenna for any other 5 GHz transceiver.

In BC|Commander, on the **BCAPI Explorer** tab, the following DFS-related fields are available:

- state.wireless[n].stats.pulseEvents – Raw count of interference pulses detected by the radio
- state.wireless[n].stats.radarDetections – Count of pulses that triggered radar detector

For wireless DFS channels, these fields will indicate the count of RF interference pulses encountered as well as a count of how many were deemed sufficiently similar to radar by the radar pattern detector.

Terminal Doppler Weather Radar (TDWR)

Terminal Doppler Weather Radar (TDWR) operates in the frequencies 5600-5650 MHz.

TDWR helps protect airplanes from hazardous weather, such as wind shear and gusts. Wireless network installations within 35 km of or in Line-of-Sight (LOS) of a TDWR must not use TDWR frequencies and should avoid using channels within 30 MHz of the TDWR frequencies. A list of U.S. Time-Frequency Domain Reflectometry (TFDR) radar coordinates is available at ⊕ WISPA.org (see TDWR Resources).

> **⚠ Warning**
> Operating this equipment in violation of local, regional or national standards, including interfering with radar, is likely to result in substantial sanctions to the user, including fines, imprisonment, confiscation of equipment, and other penalties as determined by local regulatory authorities.

Appendix B: Error and Warning Codes

In BC|Commander, the **Alerts** tab will list all errors or warnings for a BreadCrumb. However, the Status LED on the BreadCrumb will flash to indicate only one error or warning code. A few codes, such as 811 and 335, are non-flashing alerts. For other active alerts, the Status LED on the BreadCrumb will indicate only the lowest numbered error code. For a BreadCrumb with no errors, the Status LED will indicate only the lowest numbered warning code.

The Status LED on the BreadCrumb will indicate each numeric code as a series of red (error) or yellow (warning) flashes. For example, a meshed BreadCrumb normally displays a green LED. To indicate warning code 37, the LED will flash as follows: green (link state), 3 yellow flashes, short pause, 7 yellow flashes, long pause of green (link state), 3 yellow flashes, short pause, 7 yellow flashes, etc.

Model-specific differences:

- JR models have multiple green LEDs. A JR model flashes error codes on the ERR LED and warnings on the WARN LED.
- DX2 models have a bicolor green/red LED. Both errors and warnings flash in red.
- SlipStream does not have a software-controllable LED and cannot display error or warning codes. Use BC|Commander to view error status.

The following table lists each possible BreadCrumb error and warning code in numerical sequence with a description.

Code	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.
16	Continuous Transmit Mode.
115	Copying failed.
116	Flash unbundle 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.
121	License does not permit installation of this firmware image.
125	Failed to set boot path to next image.
127	Failed to copy file system image.
135	Failed to copy init image.
136	Failed to copy bootloader image.
137	This flash image may not be installed onto this BreadCrumb.
142	The version you are installing does not support the configured Packet Cipher.
143	The version you are installing does not support the configured MAC Address Cipher.
144	The version you are installing does not support the configured Per-hop Authentication algorithm.
145	The version you are installing does not support the configured security policy.
146	Failed to verify consistent country settings.
147	The configured countries are not consistent.
151	Pre-manufacturing install process failed.
152	Firmware install failed.
153	Post-manufacturing install process failed.
154	The autorun is missing required symbols.

Code	Firmware Upgrade Codes (1*)
155	GSC firmware update failed.
Code	**Diagnostic Codes (2*)**
21	Recovery log detected. To clear this message, please take a diagnostic snapshot and contact your Rajant Kinetic Mesh Associate, Kinetic Mesh Partner, or Kinetic Mesh Premier Partner.
22	Internal error detected. Please take a diagnostic snapshot and contact your Rajant Kinetic Mesh Associate, Kinetic Mesh Partner, or Kinetic Mesh Premier Partner. This message will be cleared on the next reboot.
23	Internal developer settings detected - may cause undefined behavior. Use zeroize to clear.
233	This device is not configured for commercial use and will cause undefined behavior. Contact your Rajant Kinetic Mesh Associate, Kinetic Mesh Partner, or Kinetic Mesh Premier Partner to rectify.
234	This device is running BETA software. Contact your Rajant Kinetic Mesh Associate, Kinetic Mesh Partner, or Kinetic Mesh Premier Partner for the latest supported version.
24	Stress mode is running - may cause undefined behavior. Reboot to clear.
242	Internal hardware error detected via stress testing. Take a diagnostic snapshot and upload to https//secure.rajant.com for analysis.
25	Internal developer overrides detected.
Code	**Self-Test Codes (3*)**
31	Hardware configuration not set. Factory initialization required.
311	Hardware error detected.
32	BreadCrumb has been zeroized.
321	BreadCrumb is being zeroized.
322	Breadcrumb is in Deployment Mode.
33	Radio(s) not detected.
331	Radio in MANUAL compliance mode is violating country regulation.
332	Spectrum Access not granted.
333	Low Battery.
334	Gas gauge not initialized. To initialize, please power off unit and fully charge.
335	Non-compliant radio configuration in use.
336	Radios are not correct revision. Contact your Rajant Kinetic Mesh Associate, Kinetic Mesh Partner, or Kinetic Mesh Premier Partner to rectify this issue.
37	Failed to configure Ethernet port.
38	Resetting radio due to error.
381	Noise floor threshold exceeded.
382	Radar detection paused radio.
383	Radio resumed from radar pause.
385	Radio(s) failed to initialize.
386	Radio(s) warming up.
387	High internal temperature detected.
388	Low input voltage detected.
389	High input voltage detected.
Code	**FIPS Codes (4*)**
41	FIPS Power-on self-tests failed.
411	FIPS DRBG power-on self-test failed.
412	FIPS DRBG continuous test failed.

Code	Firmware Upgrade Codes (1*)
413	FIPS DRBG health check failed.
414	Kernel integrity check failed.
415	Filesystem integrity check failed.
417	FIPS Invalid configuration.
421	Default password in use.
Code	**Fatal and Serious Codes (5*)**
51	Internal error, system will restart.
52	hostapd fatal error.
521	HT40 bandwidth reduced to HT20 due to nearby access point on HT40 secondary channel.
522	IEEE 802.11 TKIP countermeasures initiated.
53	Taking over as APT master.
531	High cost APT link.
532	BreadCrumb with the indicated serial number has a connected BreadCrumb with the indicated Encap ID and a different APT timeout value, as indicated. Configure the same APT Timeout value for all BreadCrumbs with Ethernet ports connected to the same LAN.
541	Software error
56	APT peer bridge settings do not match
57	logwatcher start timeout
Code	**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.
67	Internal battery charger disabled.
Code	**Other Codes (7, 8, 9*)**
71	Host flapping detected.
73	Invalid channel configured.
74	Channel overlap detected"
741	Signing key installation failure.
76	Potential loop detected, turned off port.
77	Model is not supported in this version of firmware. Contact your Rajant Kinetic Mesh Associate, Kinetic Mesh Partner, or Kinetic Mesh Premier Partner.
81	reserved
811	Default Network Key is in use.
82	reserved
83	reserved
84	reserved
85	reserved
86	reserved
87	reserved
88	reserved

Code	Firmware Upgrade Codes (1*)
89	reserved
91	Invalid SSL Handshake Priority String:
92	Failed to configure client mode.
93	Maximum BCAPI session count reached.
94	Multiple radios on the same channel is unsupported.
95	Modem PIN code failed verification.
951	Modem PIN code required.
952	Modem PIN code entry blocked.
953	Modem PIN code entry permanently blocked.
96	Modem SIM card is not present.
961	Error accessing the Modem SIM card.
Code	**BC|Commander Additional Codes**
8091	Conflicting BreadCrumb serial numbers detected. Possibly multiple BreadCrumbs with the same IP Address.
8092	Unable to negotiate key for BCCommander session. Provided key is invalid.
8093	Duplicate MAC address detected.
8120	Required Firmware license not found for (NameOrSerial).
8121	Firmware license for (NameOrSerial) is invalid: (ErrorMessage).
8122	Firmware license for (NameOrSerial) will expire in (X) days.
8123	Firmware license for (NameOrSerial) expired on (EXPIRE_DATE).
8200	RiSM (SerialNumber)s current/next network key exipres on (DATE) with no replacement.
8201	Key gap detected for RiSM (SerialNumber): Current key end date (DATE) UTC does not match key start date (DATE).
8202	reserved
8203	RiSM (SerialNumber) is not using (Enclave)'s configured current/next network key.

Appendix C: Ports and Protocols

Table: Ports and Protocols

Service	From	To	Protocol
BreadCrumb discovery at BC|Commander startup	Ephemeral port on BC|Commander host	224.0.0.224, port 35057 (UDP IPv4 multicast); FF02::1, port 35057 (UDP IPv6 multicast); BreadCrumb IPv4 or IPv6 addresses, port 35057 (UDP IPv4 or IPv6 unicast)	IPv4 UDP, IPv6 UDP
BreadCrumb discovery at BreadCrumb startup	BreadCrumb IPv4 or IPv6 address, port 35057	Ephemeral port on BC|Commander host (UDP IPv4 or IPv6 unicast); FF02::1, port 35057 (UDP IPv6 multicast)	IPv4 UDP, IPv6 UDP
BreadCrumb Application Programming Interface (BCAPI)	Ephemeral port on BC|Commander host	BreadCrumb IPv4 or IPv6 addresses, port 2300 (default)	IPv4 TCP, IPv6 TCP
BC|Connector discovery by BC|Commander	Ephemeral port on BC|Commander host	BC|Connector server port 35057	IPv4 UDP, IPv6 UDP
BC|Connector discovery by BC|Enterprise	Ephemeral port on BC|Enterprise server	BC|Connector server port 35057	IPv4 UDP, IPv6 UDP
BC|Connector communication with BreadCrumbs	Ephemeral port on BC|Connector server	BreadCrumb IPv4 or IPv6 addresses, port 2300	IPv4 TCP, IPv6 TCP
BC|Connector with user authentication through LDAP directory	Ephemeral port on BC|Connector server	LDAP server port 3268 or 389 (whichever is used)	IPv4 UDP, TCP; IPv6 UDP, TCP
BC|Enterprise setup only	Ephemeral port on BC|Enterprise server	BC|Connector TCP port 23000	IPv4 TCP, IPv6 TCP
BC|Enterprise graphing service	Ephemeral port on BC|Enterprise server	BC|Enterprise server port 3000	IPv4 TCP, IPv6 TCP
BC|Enterprise metrics service	Ephemeral port on BC|Enterprise server	BC|Enterprise server port 8889	IPv4 TCP, IPv6 TCP
BC|Enterprise time-series database service	Ephemeral port on BC|Enterprise server	BC|Enterprise server port 9090	IPv4 TCP, IPv6 TCP
BC|Enterprise user interface	Internet browser on BC|Enterprise client workstation	BC|Enterprise server port 8888	IPv4 HTTP, IPv6 HTTP
BC|Enterprise metrics request and publishing	Ephemeral port on BC|Enterprise server	BC|Connector server port 23002	IPv4 TCP, IPv6 TCP
Automatic Protocol Tunneling (APT)	BreadCrumb Ethernet interface IPv6 link-local address, ephemeral port	BreadCrumb Ethernet interface IPv6 link-local address port 2210 for the service listener, ephemeral port for data flow	IPv6 UDP
Remote Protocol Tunneling (RPT) SCTP option (default)	BreadCrumb IPv4 or IPv6 address, ephemeral port	BreadCrumb IPv4 or IPv6 address, SCTP port 2210 for the service listener,	IPv4 or IPv6 SCTP

Service	From	To	Protocol
		ephemeral port for data flow	
RPT UDP option	BreadCrumb IPv4 or IPv6 address, ephemeral port	BreadCrumb IPv4 or IPv6 address, UDP port 2211 for the service listener, ephemeral port for data flow	IPv4 or IPv6 UDP
Tactical Radio over Internet Protocol (TRoIP) Audio RTP Traffic	BreadCrumb IPv4 address, ephemeral port	IPv4 multicast address 225.0.0.1-225.0.2.255 port 24680	IPv4 UDP
Remote Packet Capture	Remote Packet Capture client (BC|Commander)	BreadCrumb configured TCP port 5825 (default)	IPv4 TCP
Performance Test (iperf3)	BreadCrumb IPv4 or IPv6 address, ephemeral port	BreadCrumb IPv4 or IPv6 address, port 5201	IPv4 UDP, TCP; IPv6 UDP, TCP
Real Time Location System (RTLS)	BreadCrumb ephemeral port	RTLS server UDP port 12092	IPv4 UDP
RTLS	RTLS server ephemeral port	BreadCrumb UDP port 1144 (default)	IPv4 UDP

Appendix D: Installation Guidelines

This appendix provides guidelines for installing a typical Rajant BreadCrumb.

The sequence of installation for multiple BreadCrumbs will depend on the location where each BreadCrumb is to be installed and configured.

All warnings and guidance throughout this guide apply during BreadCrumb installation.

D.1 Professional Installation Is Required

Model: AG1 Cardinal Module

This BreadCrumb must be installed professional who has been trained by Rajant and is knowledgeable of how the BreadCrumb is to be used.

Rajant Corporation will ensure that the BreadCrumb is marketed and sold only to professionals and only for industrial or commercial use. The BreadCrumb will not be sold to the general public.

> ⚠ **Antenna Installation WARNING**
> The BreadCrumb installer should configure the conducted output power level according to regulations that apply to the BreadCrumb location and the applicable EIRP limit. Professional installation of equipment is required to ensure compliance with health and safety issues.

> ⚠ **IMPORTANT: Exposure to Radio Frequency Radiation**
> To satisfy Radio Frequency (RF) exposure requirements, a minimum safe distance must be maintained between the BreadCrumb antennas and all persons while the device is operating. The minimum safe distance for this BreadCrumb model is stated in the FCC Certification Statements chapter at the beginning of this user guide.

D.2 Safety

> ⚠ **Warning**
> The AG1 Cardinal Module is not user-serviceable. Repairs must be performed at a Rajant-designated service center by trained personnel.

> ⚠ **Warning**
> The AG1 Cardinal Module single-board computer assembly contains a Lithium button cell battery. The customer should never attempt to replace this battery. This battery must be replaced by authorized repair personnel trained by Rajant Corporation. CAUTION: Risk of explosion if battery is replaced by an incorrect type. Dispose of used batteries according to the battery manufacturer's instructions.

Adhere to the guidelines in Connecting Power in this Appendix.

D.3 Modifications

> ⚠ **CAUTION**
> Changes or modifications not expressly approved by Rajant Corporation could void the user's authority to operate the equipment.

Rajant products are compliant and warranted against manufacturing defects only so long as Rajant-authorized accessories are used in deployment of Rajant Breadcrumbs. It is the responsibility of the operator and the installer to ensure the system as installed operates within regional requirements.

D.4 Attaching Antenna Cables and Antennas

Most of Rajant's standard antennas are characterized by high-gain and, therefore, small vertical beamwidth. Antennas in fixed locations should be installed plumb and at the same elevation so that BreadCrumbs using these antennas will see each other without a significant loss of signal strength.

> ⚠ **Warning**
> To avoid possible damage to the BreadCrumb radios, always turn off power to the BreadCrumb before connecting or disconnecting external antennas.

Required Antenna Separation

The antennas from any transceiver on the AG1 Cardinal Module may not be co-located with the antennas any other transceiver. The co-location restriction is satisfied by maintaining a separation of 20 cm between the antennas. There is no restriction for the separation between the antennas from the same transceiver; but testing at installation is recommended to verify the system performance that is achieved with a specific antenna deployment configuration.

> **⚠ Warning**
> For installations that will experience vibration or shock, all antennas should be externally mounted and attached to the AG1 Cardinal Module using cables. Low Loss RF cable such as LMR-400 is recommended for cable attached antennas. If a radio port is not required for a given application, the port should be disabled in software using BC|Commander, and a 50-Ohm terminator should be installed.

> **⊙ DFS Additional Antenna Separation**
> For 5 GHz transceivers using channels that require DFS radar detection, a recommendation is to mount each antenna for a DFS channel at least 2 feet from the antenna for any other 5 GHz transceiver.

Summary

The following is a summary of antenna separation requirements:

- Each antenna must be installed at least 20 cm from the antennas of any other transceivers.
- For locations with vibration or shock, no antennas are to be directly attached to the BreadCrumb.
- For antennas connected to the BreadCrumb via cables, low loss cabling, such as LMR-400, is recommended.
- Any unused antenna ports should be disabled in BC|Commander and have a 50 Ohm terminator installed.
- Antennas in fixed locations should be installed plumb and at the same elevation.
- The BreadCrumb and its antennas must be located a distance from any persons when operating. The minimum distance for this model is stated in the FCC Certification Statements chapter at the beginning of this guide.

Additional Notes

The following additional notes apply to antenna separation:

- Power to the BreadCrumb should be powered OFF when attaching or removing antennas or terminators.
- To reduce shock and vibration, BreadCrumbs on mobile equipment should be mounted in or on the cab.
- See Physical Placement and other Considerations regarding Line of Sight and Fresnel Radius.
- Mounting hardware for cabled antennas may be purchased from Rajant.
- 5 GHz channels requiring DFS radar detection may get false triggers if antennas are placed near reflecting surfaces/objects or other electrical or radio equipment.

D.5 Grounding and Surge Protection

> **⚠ Warning**
> The enclosure of the AG1 Cardinal Module is conductive. To protect the user against the risk of electric shock during high voltage transient events which may occur when this equipment is installed outdoors, protective earth grounding of the AG1 Cardinal Module enclosure is required. Protective earth grounding operations must be performed by trained personnel, and according to local electrical codes and industry best practices, as well as Rajant's own recommendations.

> **⚠ Warning**
> To protect the user against the risk of electric shock during high voltage transient events which may occur when this equipment is installed outdoors, protective earth grounding of the PoE power supply is required. Case ground connections are provided on all Rajant supplied PoE power supplies. The case ground connections must be used and must be connected to a protective earth ground. Protective earth grounding operations must be performed by trained personnel, and according to local electrical codes and industry best practices, as well as Rajant's own recommendations.

To ensure continuity of ground from the BreadCrumb to the PoE to the ground, and to help protect the BreadCrumb and any attached equipment from electrical damage, in Appendix: Technical Bulletins, see Rajant Best Practices: Grounding and Surge Protection.

D.6 Waterproofing

For outdoor installations, Rajant recommends waterproofing all connections. For more information, in Appendix: Technical Bulletins, see the following: - Waterproofing Rajant BreadCrumb RF Connections

D.7 Connecting Power

The following guidelines apply when connecting power to the BreadCrumb:

- For power requirements and PoE usage diagrams, see Power and Ethernet.
- The BreadCrumb's on/off switch (if any) should be off when connecting or disconnecting power.

- BreadCrumbs only support Passive PoE. Do not use a Cisco switch PoE to power a BreadCrumb (set switch port's power to **never**).

D.8 BreadCrumb Configuration

Configure the BreadCrumb to be compatible with any existing or planned BreadCrumb mesh network. This will include configuring the desired channel and bandwidth and configuring security settings. Complete and test the BreadCrumb configuration before mounting the BreadCrumb anywhere unreachable.

For more information, see the following:

- In this BreadCrumb model user guide, see the chapter, "Deploying a BreadCrumb Mesh Network".
- In the *BC|Commander Version 11 User Guide* refer to chapters "Configure BreadCrumbs" and "BreadCrumb Configuration."

D.9 BreadCrumb Placement

The placement of BreadCrumbs on location can greatly impact the performance of the mesh.

For guidelines for placing BreadCrumbs on location, in this BreadCrumb model user guide, see the chapter "Deploying a BreadCrumb Mesh Network," starting at Physical Placement and other Considerations.

Appendix E: Mounting Instructions

The AG1 Cardinal Module provides features that enable the BreadCrumb to be mounted to a surface.

Notice The Cardinal module is not a sealed "stand-alone" BreadCrumb and is not meant to be installed in any way exposed to the outside elements. The Cardinal module requires installation inside a protected enclosure, drone, UGV, robot, or cabinet as the module is not sealed from ingress of dust, dirt, or water.

- The Cardinal module should be mounted securely using the 2 mounting holes provided
- Outdoors, the Cardinal should be mounted in an enclosure with sufficient metal contact to provide a thermal conductive path for heat dissipation and/or provide ample airflow as the device will generate heat during times of high-level data processing.
- A fan is recommended if the ambient air around the module is at or near the limits of the device during operation.
- All cables (RF and Power) should be secured with strain relief.
- Antennas should never be mounted directly to the Cardinal, use cables.
- Cardinal should not be mounted nearby other heat generating sources.
- The Cardinal module should not be mounted in close proximity to other RF-generating devices. If other RF-generating devices are adjacent, care should be taken to isolate to a minimum of 10 times the wavelength of the transmitted frequencies to reduce interference potentials.
- The Cardinal module may be used indoors in open air with as much surface exposed as possible to maximize airflow.

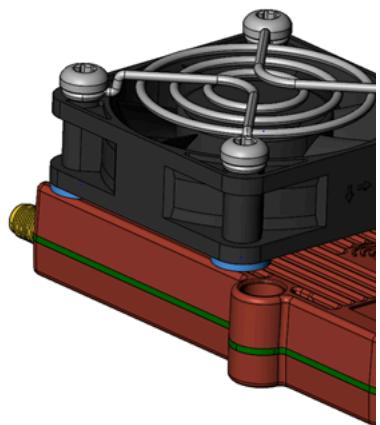*Figure: AG1 Cardinal Module Mounting Holes*

Dimensions

Always refer to the partner portal for the most up to date product support and mechanical models.
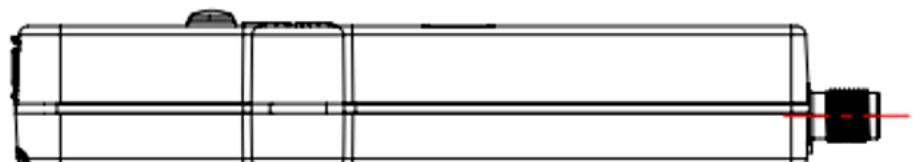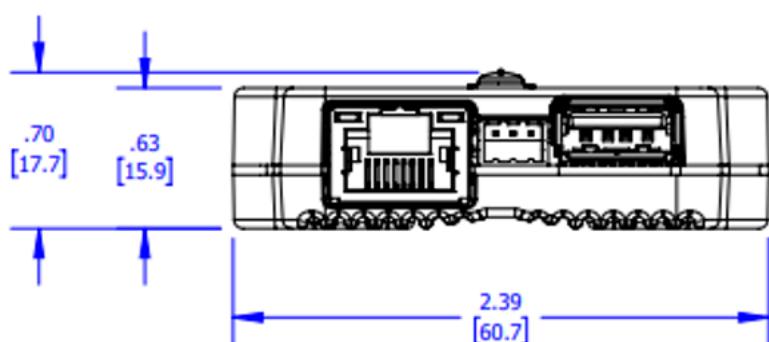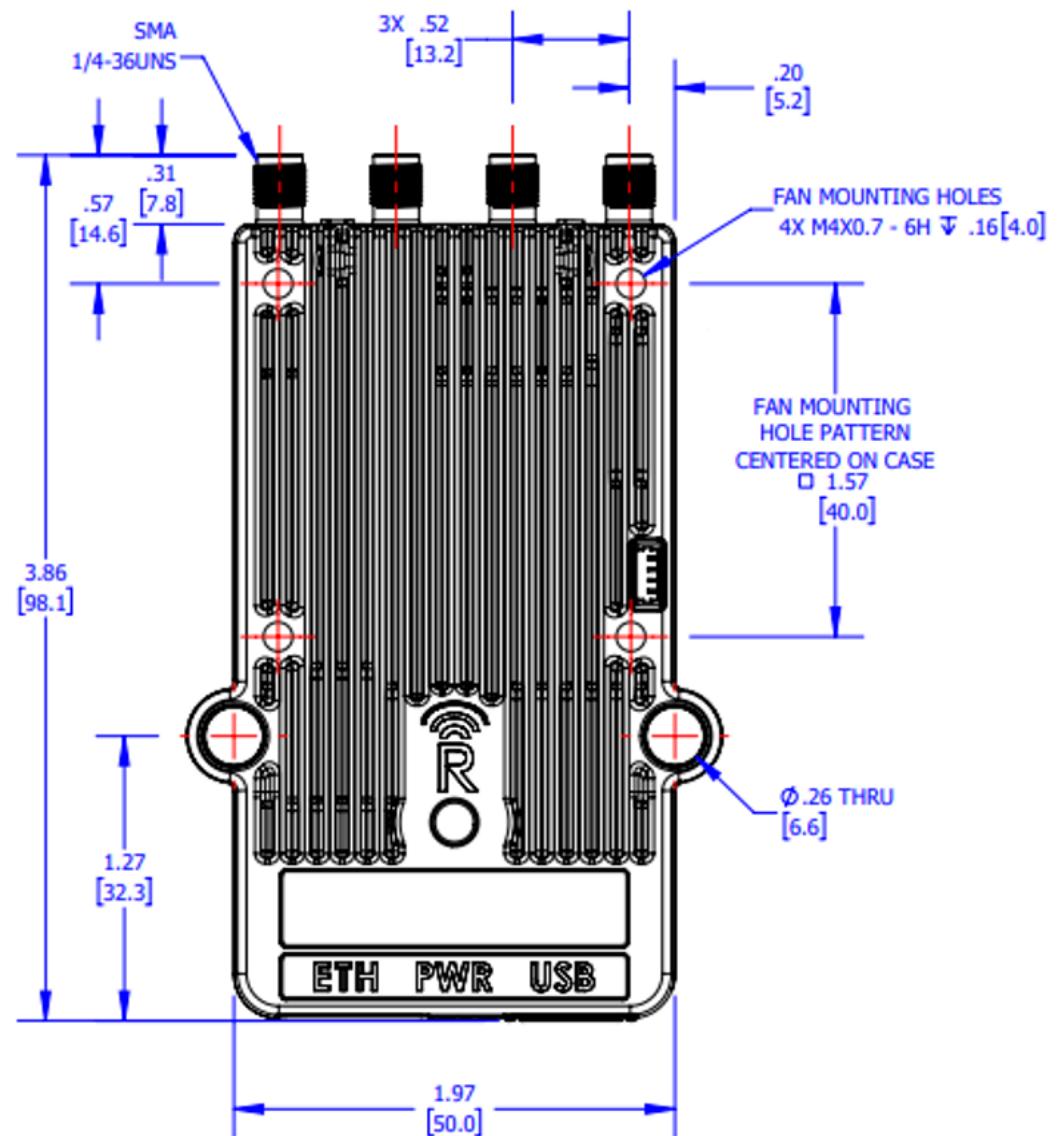
Fan Mounting (Optional)

If a fan is desired it should be mounted as shown below, with spacers below the fan to protect wiring.

4-Position Fan Connector to AG1

AGI 4-Wire Fan Connections		
Pin #	**Color**	**Signal**
1	Black	-Vin
2	Red	+Vin
3	Blue	PWM (NC cable)
4	Yellow	FG (NC cable)

Pin-1

Pin-1

Molex 51021-0400
4-Position Connector

Molex 50058-8000
28-32 AWG Crimp

BOM: Rajant PN: 22-100043-001: Sub-ASSY, Two-Wire Fan-Assembly for AGI

|Item QTY|Rajant PN|Name|MFG|MFG PN| |1|170-100004-001|Fan, "2-Wire" Fan, 5V, for AGI|CUI Devices|CFM-5010V-052-300| |2|171-100124-001|Conn, 4-Position 1.25mm, Molex 51021 Series|Molex|51021-0400| |3|273-100129-001|Terminal Pin, crimp, 1.25 28-32 AWG|Molex|Molex|500588000|

02-100159-001:

|1|122-100043-001|Sub-ASSY, 2-Wire Fan-Assembly for AGI|Rajant|22-100043-001| |2|172-100027-001|Cover, Fan-Cover, 50mm-Sq|Qualtek|8248| |3|495-100030-001|Spacer, Washer, Black, for # 8 & M4 Size|McMaster|91755a398| |4|492-100098-001|Screw, M4 x 0.70 mm Thread Size, 16 mm Long|McMaster|90991A124|

Appendix F: Technical Bulletins

F.1 Rajant Best Practices: Grounding and Surge Protection

F.1.1 Introduction

Rajant BreadCrumb® products are commonly installed in environments that are susceptible electro-static discharge (ESD), lightning and other high-energy electrical surge events. BreadCrumbs are designed to withstand the toughest conditions imposed by military and industrial scenarios. However, the basic built-in protective measures will not prevent the damaging effects of high-energy ESD or lightning. To ensure reliable operation and long service life, these additional best practices are required to protect BreadCrumbs from lightning and high-energy electrical surges.

> ⚠ **Important**
> Rajant BreadCrumb equipment will most likely *not* survive a *direct* lightning strike. However, the electro-magnetic forces caused by lightning are so powerful that even a strike that lands near the equipment may cause damage. These best practices can protect equipment from a nearby lightning strike, not a direct hit.

F.1.2 Environment

A dry windy environment is more likely to create a large buildup of static energy that leads to electro-static discharges.

F.1.3 Recommendations

Rajant recommends the following best practices for installing BreadCrumb equipment (except the C1D2 model):

- Use only shielded Ethernet cables with metal-shielded connectors. Metal-encased connectors provide the continuity of the ground from the BreadCrumb case to the Power over Ethernet (PoE) and AC ground or protective earth ground.
- Use an Ethernet surge protector for each utilized Ethernet port on a BreadCrumb.
- Use antenna surge protectors on all pole-mounted antennas.
- To avoid sparking and damage to the BreadCrumb, always connect the surge protector and the powered Ethernet cable to the BreadCrumb before applying power to the PoE power supply.
- Always power off a BreadCrumb prior to connecting or disconnecting external antennas.
- Ground all equipment, as follows:
    - Ground the BreadCrumb enclosure.
    - Ground the BreadCrumb power supply.
    - Ground the Ethernet surge protector(s).
    - If an antenna is not connected directly on a BreadCrumb antenna port and offers an exposed metal base, ground the base of the antenna.
    - Any antenna connected directly on a BreadCrumb antenna port will be grounded through the BreadCrumb enclosure.

F.1.4 Ethernet Surge Protection

Ethernet Cable Requirements

An Ethernet cable provides a path for a power surge to enter a BreadCrumb. The longer the cable, the more susceptible the cable is to picking up surges. In the event of a lightning strike, the cable will act as an antenna and absorb the electro-magnetic wave caused by the strike, even from a long distance. Surges through an Ethernet port can be suppressed by an Ethernet surge protector.

Selecting Ethernet Surge Protectors

When selecting an Ethernet surge protector, consider the following:

- It is important to know how large a surge the protector can handle and how many strikes the protector can withstand before needing to be replaced.
- Be sure that the surge protector supports passive PoE. Installing the wrong surge protector on the PoE line can prevent the BreadCrumb from getting enough power to turn on.
- The surge protector will cause a voltage drop in the PoE power carried over the Ethernet cable. The voltage drop should be small enough to allow enough power to reach the BreadCrumb.
- The surge protector will cause some degradation to the Ethernet data signal. Be sure that the degradation to the signal does not severely impact Ethernet throughput, especially on longer Ethernet cable runs.

L-Com ALS-CAT6HPW Ethernet Surge Protector

For Ethernet surge protection, Rajant recommends the L-Com ALS-CAT6HPW Ethernet surge protector (🌐 L-com Part Number 🌐 ALS-CAT6HPW).

The features of this device are the following:

- Designed to meet the GR-1089 Intra-Building surge protection requirements
- Weatherproof ABS enclosure with gasketed cover and PG16 cable glands for outdoor operation
- External ground clamp to provide a tie point for earth ground
- Compatible with 10/100/1000 Base-T equipment
- Compatible with CAT5, CAT5e and CAT6 cables
- Robust, two-stage transient-voltage-suppression (TVS) diode and differential gas tube suppression
- Tested and fully-compatible with Rajant BreadCrumb ME3, ME4 and LX4 devices

L-Com LPXT-WP-GB-POE++60V Data Line and PoE Surge Protection (FE1 BreadCrumbs)

For the FE1 family of BreadCrumbs, for data input and PoE surge protection, Rajant recommends the L-Com LPXT-WP-GB-POE++60V Data Line and POE surge protector (🌐 L-com Part Number 🌐 LPXT-WP-GB-POE++60V).

The features of this device are the following:

- Connectors: Enclosed protected shielded RJ45
- Compatible Cables: Cat5/5e UTP/STP, Cat6/6A STP
- Data Protocols: GbE, PoE+, PoE++
- Impedance: 100ohms max
- Vdc: 48V type, 60V max
- PoE Power: 100W max, 1.5A max per pin

Installing the Ethernet Surge Protector

The Ethernet surge protector should be installed as close to the BreadCrumb as practical, ideally within 50 cm (20 in) of the BreadCrumb.

The surge protector should be grounded as described in the operation manual for the surge protector and according to local electrical codes and industry best practices.

When a BreadCrumb is powered through an Ethernet port (i.e., PoE) on the BreadCrumb, the surge protector should *always* be installed between the BreadCrumb and the power source.

> ⚠ **Warning**
> To avoid sparking and possible damage to the BreadCrumb, be sure to connect the surge protector and the powered Ethernet cable to the BreadCrumb before applying power to the PoE power supply.

F.1.5 Antenna Surge Protection

Antenna surge protectors should be used for all pole-mounted BreadCrumb antennas.

Consider the following aspects when choosing an antenna surge protector:

- It is important to know how large a surge the protector can handle and how many strikes the surge protector can withstand before needing to be replaced.
- The equipment side of the surge protector should have an N male connector to allow for direct connection to the BreadCrumb antenna port.
- The Voltage Standing Wave Ratio (VSWR) of the surge protector should be less than 1.2:1 for 0–3 GHz and less than 1.5:1 for 3–6 GHz.
- The insertion loss of the surge protector should be less than 0.2 dB for 0–3 GHz and less than 0.35 dB for 3–6 GHz.
- The surge protector will cause some degradation to the RF signal. Be sure that the degradation to the signal does not severely impact radio throughput, especially on longer wireless links.

Rajant recommends the PolyPhaser GT-NFM-AL antenna surge protector (🌐 Streakwave Part Number 🌐 GT-NFM-AL).

> **⚠ Warning**
> To avoid sparking and possible damage to the BreadCrumb, be sure to connect the antenna surge protector to the BreadCrumb before applying power to the BreadCrumb power supply.

F.1.6 DC Input Power Surge Suppression (FE1 BreadCrumbs)

For the FE1 family of BreadCrumbs, for DC input power surge suppression for 24VDC power lines, Rajant recommends the L-com ALS-D25P24DW lightning surge protector for power lines (🌐 L-com Part Number 🌐 ALS-D25P24DW).

The features of this device are the following:

- Electrical Specs: DC Power
- Connectors: (2) Phillips-head screw type metal terminal blocks (+/-)
- Stage 1 Clamping Voltage = +/- 90V
- Stage 2 Current Rating = 4A
- Stage 3 TVS Diode = 30V

F.1.7 The Goal: The Ground

The goal is to have a continuity of ground from the BreadCrumb to the destination AC ground or protective earth ground.

For a BreadCrumb that uses an AC PoE power supply, the ground pin of the AC plug should be plugged into a properly-grounded AC socket.

For a BreadCrumb that uses a DC PoE power supply, the grounding connections of the DC PoE should be properly connected to an earth ground. Use 10 AWG or lower (larger) gauge wire for grounding cables and be careful to avoid any sharp bends.

The following are examples of an earth ground:

- A conductive metal rod buried in the ground (ground rod).
- A metal electrical service panel (should be connected to a ground rod).
- A grounded metal conduit or raceway.
- A grounded metal water pipe that directly contacts the earth.
- The metal frame of a building, if grounded.

F.2 BreadCrumb Models Support Only Passive PoE

> **⚠ IMPORTANT**
> This Technical Information Bulletin (TIB) applies to any Rajant BreadCrumb model that supports passive Power over Ethernet (PoE), not only those indicated as Products Affected. Refer to the BreadCrumb user guide for each model for information about passive PoE support.

RĀJANT Product TIB Notice No.: 2015002

Revision Date: 09/28/2022

Technical Information Bulletin

Product(s) Affected: Rajant BreadCrumb® ME4, LX5 and AG1/JR3 models; passive PoE devices

Description: The first ME4 Ethernet port (eth0), both LX5 Ethernet ports (eth0, eth1), and the only Ethernet port on the AG1/JR3 support passive Power over Ethernet (passive PoE). Unlike other PoE methods, such as IEEE 802.3af/at, passive PoE does not include any kind of handshaking or voltage checking.

Some Cisco switches support both IEEE 802.3af/at PoE or a proprietary version of PoE. Their default mode is named "auto" mode. In auto mode, the switch will try to automatically detect the type of PoE the plugged-in device supports. The Cisco switch auto method does not work with passive PoE equipment, including plugging into the data input ports of Rajant PoE devices that are used with the ME4, LX5 and JR3. The link will not come up or will "flicker" up and down.

To connect a Cisco PoE switch to a Rajant PoE-capable device, you must turn off the PoE capability for this port. You must set the ""power inline"" setting for the port to ""never." For information about configuring this port, refer to the following:

includes information for configuring the port.

Remarks:

Do not attempt to combine Cisco automatic PoE detection with the input port of Rajant passive PoE devices used with the ME4, LX5, and JR3 models. Set the "power inline" setting of the port to "never". Contact a technical support representative for further information.

F.3 Never Apply Power to the Data Input Port of a Rajant Mid-Span Power over Ethernet (PoE) Power Supply

> ⚠ **IMPORTANT**
> This Tech Service Bulletin (TSB) applies to Rajant BreadCrumb models that use a passive PoE power supply.

RAJANT Product TSB Notice No.: 03-100162-001

Revision Date: 09/28/2022

TECH SERVICE BULLETIN

Summary:

Except for the Rajant VHDC-24V-50W-GbE power supply, never connect the data input port of a Rajant-supplied mid-span PoE power supply to a PoE-powered data port. A Rajant 10/100 PoE power supply will not work properly, and a Rajant 10/100/1000 PoE power supply will be permanently damaged causing the Ethernet data link to fail.

Background:

Many Rajant BreadCrumb product families, such as KM3, ME4, ME3, LX5, LX4 and JR3, do not support 802.3 af/at automatic power negotiation. These BreadCrumbs must be powered from a Rajant-approved mid-span passive PoE power supply. These power supplies do not support 802.3 af/at automatic power negotiation. Except for the Rajant VHDC-24V-50W-GbE power supply, the data input port of a Rajant PoE power supply must never be connected to a PoE-powered data port.

The Ethernet data lines of a Rajant 10/100/1000 AC/DC mid-span PoE power supply are protected by low-voltage Transient Voltage Suppressor (TVS) diodes. These diodes are intended to prevent damage to equipment from short-duration voltage transients, such as electrostatic discharge. The TVS diodes will fail to a permanent short circuit condition if continuous DC voltage is applied. When the TVS diodes are damaged, the PoE data path will no longer work. The Ethernet data link will fail, or will never form.

Field Test:

Use the following procedure to test a Rajant mid-span PoE power supply for data path damage:

1. Remove the AC power cord from the Rajant PoE power supply.
2. Using two data cables, connect both the data INPUT and data plus PoE OUTPUT port of the Rajant PoE power supply to an unmanaged switch.
3. Inspect the link lights on the Ethernet switch ports to confirm that a data link is formed.
4. If the PoE power supply does not form a data link on both ports of the Ethernet data switch, replace the PoE power supply with a new one.

Mitigation:

The recommended best practice is to only connect the PoE IN port on a Rajant PoE power supply to a non-PoE Ethernet switch. Always connect the OUT port on a Rajant PoE power supply to a BreadCrumb.

If only a PoE switch is available, a data isolation transformer, such as L-COM BT-CAT6-P1, may be used with a Rajant PoE power supply. Connect the data port of the L-COM BT-CAT6-P1 to the PoE switch port, and connect the DATA+POWER port of the L-COM BT-CAT6-P1 to the data input port on the Rajant PoE power supply.

F.4 Installation Constraints for Rajant AC Powered Accessory POE Power Supplies

Revision Date: 11/09/2023

TECH SERVICE BULLETIN

The approved use of any Rajant-supplied AC-powered mid-span Power-over-Ethernet (PoE) power supply (see illustration) is limited to indoor, environmentally-sheltered, non-damp locations that are isolated from shock and vibration. These power supplies are not sealed for dust or water ingress and are not intended to operate in an environment with condensing humidity. The construction of these power supplies is not ruggedized for exposure to mechanical shock or vibration.

Failure to observe the recommended installation restrictions for any of these power supplies may result in network outages and poor network performance. Device failure is likely and will void the Rajant warranty for the power supply. Damage to a Rajant BreadCrumb resulting from misuse of an AC-powered PoE power supply may not be covered by the BreadCrumb warranty.

Rajant Corporation offers the VHDC series of DC-powered mid-span PoE power supplies that are suitable for use in non-environmentally sheltered locations, such as vehicles and outdoor trailers. When selecting a mid-span PoE power supply for a specific application, refer to the product datasheet of a specific Rajant VDHC model power supply to verify the ingress performance.

Appendix G: Rajant End User License Agreement

IMPORTANT: PLEASE READ THIS END USER LICENSE AGREEMENT CAREFULLY. IT IS ENCLOSED IN THE SOFTWARE PACKAGE AND /OR PRESENTED ELECTRONICALLY WHEN ACCESSING THE SOFTWARE. BY CLICKING "I AGREE", YOU ARE AGREEING TO BE BOUND BY THE TERMS OF THIS LICENSE. IT IS VERY IMPORTANT THAT YOU CHECK THAT YOU ARE PURCHASING RAJANT SOFTWARE OR EQUIPMENT FROM AN APPROVED SOURCE AND THAT YOU, OR THE ENTITY YOU REPRESENT (COLLECTIVELY, THE "CUSTOMER") HAVE BEEN REGISTERED AS THE END USER FOR THE PURPOSES OF THIS RAJANT END USER LICENSE AGREEMENT. IF YOU ARE NOT REGISTERED AS THE END USER YOU HAVE NO LICENSE TO USE THE SOFTWARE AND THE LIMITED WARRANTY IN THIS END USER LICENSE AGREEMENT DOES NOT APPLY. ASSUMING YOU HAVE PURCHASED FROM AN APPROVED SOURCE, DOWNLOADING, INSTALLING OR USING RAJANT OR RAJANT-SUPPLIED SOFTWARE CONSTITUTES ACCEPTANCE OF THIS AGREEMENT.

RAJANT CORPORATION OR ITS AFFILIATE LICENSING THE SOFTWARE ("RAJANT") IS WILLING TO LICENSE THIS SOFTWARE TO YOU ONLY UPON THE CONDITION THAT YOU PURCHASED THE SOFTWARE FROM AN APPROVED SOURCE AND THAT YOU ACCEPT ALL OF THE TERMS CONTAINED IN THIS END USER LICENSE AGREEMENT PLUS ANY ADDITIONAL LIMITATIONS ON THE LICENSE SET FORTH IN A SUPPLEMENTAL LICENSE AGREEMENT ACCOMPANYING THE PRODUCT OR AVAILABLE AT THE TIME OF YOUR ORDER (COLLECTIVELY THE "AGREEMENT"). TO THE EXTENT OF ANY CONFLICT BETWEEN THE TERMS OF THIS END USER LICENSE AGREEMENT AND ANY SUPPLEMENTAL LICENSE AGREEMENT, THE SUPPLEMENTAL LICENSE AGREEMENT SHALL APPLY. BY DOWNLOADING, INSTALLING, OR USING THE SOFTWARE, YOU ARE REPRESENTING THAT YOU PURCHASED THE SOFTWARE FROM AN APPROVED SOURCE AND BINDING YOURSELF TO THE AGREEMENT. IF YOU DO NOT AGREE TO ALL OF THE TERMS OF THE AGREEMENT, THEN RAJANT IS UNWILLING TO LICENSE THE SOFTWARE TO YOU AND (A) YOU MAY NOT DOWNLOAD, INSTALL OR USE THE SOFTWARE, AND (B) YOU MAY RETURN THE SOFTWARE (INCLUDING ANY UNOPENED PACKAGE AND ANY WRITTEN MATERIALS) FOR A FULL REFUND, OR, IF THE SOFTWARE AND WRITTEN MATERIALS ARE SUPPLIED AS PART OF ANOTHER PRODUCT, YOU MAY RETURN THE ENTIRE PRODUCT FOR A FULL REFUND. YOUR RIGHT TO RETURN AND REFUND EXPIRES 30 DAYS AFTER PURCHASE FROM AN APPROVED SOURCE, AND APPLIES ONLY IF YOU ARE THE ORIGINAL AND REGISTERED END USER PURCHASER. FOR THE PURPOSES OF THIS END USER LICENSE AGREEMENT, AN "APPROVED SOURCE" MEANS (A) RAJANT; OR (B) A DISTRIBUTOR OR SYSTEMS INTEGRATOR AUTHORIZED BY RAJANT TO DISTRIBUTE / SELL RAJANT EQUIPMENT, SOFTWARE AND SERVICES WITHIN YOUR TERRITORY TO END USERS; OR (C) A RESELLER AUTHORIZED BY ANY SUCH DISTRIBUTOR OR SYSTEMS INTEGRATOR IN ACCORDANCE WITH THE TERMS OF THE DISTRIBUTOR'S AGREEMENT WITH RAJANT TO DISTRIBUTE / SELL THE RAJANT EQUIPMENT, SOFTWARE AND SERVICES WITHIN YOUR TERRITORY TO END USERS.

THE FOLLOWING TERMS OF THE AGREEMENT GOVERN CUSTOMER'S USE OF THE SOFTWARE (DEFINED BELOW), EXCEPT TO THE EXTENT: (A) THERE IS A SEPARATE SIGNED CONTRACT BETWEEN CUSTOMER AND RAJANT GOVERNING CUSTOMER'S USE OF THE SOFTWARE, OR (B) THE SOFTWARE INCLUDES A SEPARATE "CLICK-ACCEPT" LICENSE AGREEMENT OR THIRD-PARTY LICENSE AGREEMENT AS PART OF THE INSTALLATION OR DOWNLOAD PROCESS GOVERNING CUSTOMER'S USE OF THE SOFTWARE. TO THE EXTENT OF A CONFLICT BETWEEN THE PROVISIONS OF THE FOREGOING DOCUMENTS, THE ORDER OF PRECEDENCE SHALL BE (1) THE SIGNED CONTRACT, (2) THE CLICK-ACCEPT AGREEMENT OR THIRD-PARTY LICENSE AGREEMENT, AND (3) THE AGREEMENT. FOR PURPOSES OF THE AGREEMENT, "SOFTWARE" SHALL MEAN COMPUTER PROGRAMS, INCLUDING FIRMWARE AND COMPUTER PROGRAMS EMBEDDED IN RAJANT EQUIPMENT, AS PROVIDED TO CUSTOMER BY AN APPROVED SOURCE, AND ANY UPGRADES, UPDATES, BUG FIXES OR MODIFIED VERSIONS THERETO (COLLECTIVELY, "UPGRADES"), ANY OF THE SAME WHICH HAS BEEN RELICENSED UNDER THE RAJANT SOFTWARE TRANSFER AND RE-LICENSING POLICY (AS MAY BE AMENDED BY RAJANT FROM TIME TO TIME) OR BACKUP COPIES OF ANY OF THE FOREGOING.

License. Conditioned upon compliance with the terms and conditions of the Agreement, RAJANT grants to Customer a nonexclusive and nontransferable license to use for Customer's internal business purposes the Software and the Documentation for which Customer has paid the required license fees to an Approved Source. "Documentation" means written information (whether contained in user or technical manuals, training materials, specifications or otherwise) pertaining to the Software and made available by an Approved Source with the Software in any manner (including on CD-Rom, or on-line). In order to use the Software, Customer may be required to input a registration number or product authorization key and register Customer's copy of the Software online at RAJANT'S website to obtain the necessary license key or license file.

Customer's license to use the Software shall be limited to, and Customer shall not use the Software in excess of, a single hardware chassis or card or such other limitations as are set forth in the applicable Supplemental License Agreement or in the applicable purchase order which has been accepted by an Approved Source and for which Customer has paid to an Approved Source the required license fee (the "Purchase Order").

Unless otherwise expressly provided in the Documentation or any applicable Supplemental License Agreement, Customer shall use the Software solely as embedded in, for execution on, or (where the applicable Documentation permits installation on non- RAJANT equipment) for communication with RAJANT

equipment owned or leased by Customer and used for Customer's internal business purposes. No other licenses are granted by implication, estoppel or otherwise.

For evaluation or beta copies for which Rajant does not charge a license fee, the above requirement to pay license fees does not apply.

General Limitations. This is a license, not a transfer of title, to the Software and Documentation, and Rajant retains ownership of all copies of the Software and Documentation. Customer acknowledges that the Software and Documentation contain trade secrets of Rajant or its suppliers or licensors, including but not limited to the specific internal design and structure of individual programs and associated interface information. Except as otherwise expressly provided under the Agreement, Customer shall only use the Software in connection with the use of Rajant equipment purchased by the Customer from an Approved Source and Customer shall have no right, and Customer specifically agrees not to:

(i) transfer, assign or sublicense its license rights to any other person or entity (other than in compliance with any Rajant relicensing/transfer policy then in force), or use the Software on Rajant equipment not purchased by the Customer from an Approved Source or on secondhand Rajant equipment, and Customer acknowledges that any attempted transfer, assignment, sublicense or use shall be void;

(ii) employ others, nor assist others to make error corrections to or otherwise modify or adapt the Software or create derivative works based upon the Software, or permit third parties to do the same;

(iii) employ others, nor assist others to reverse engineer or decompile, decrypt, disassemble or otherwise reduce the Software to human-readable form, except to the extent otherwise expressly permitted under applicable law notwithstanding this restriction or except to the extent that Rajant is legally required to permit such specific activity pursuant to any applicable open source license;

(iv) publish any results of benchmark tests run on the Software;

(v) use or permit the Software to be used to perform services for third parties, whether on a service bureau or time-sharing basis or otherwise, without the express written authorization of Rajant; or

(vi) disclose, provide, or otherwise make available trade secrets contained within the Software and Documentation in any form to any third party without the prior written consent of Rajant. Customer shall implement reasonable security measures to protect such trade secrets.

To the extent required by applicable law, and at Customer's written request, Rajant shall provide Customer with the interface information needed to achieve interoperability between the Software and another independently created program, on payment of Rajant's applicable fee, if any. Customer shall observe strict obligations of confidentiality with respect to such information and shall use such information in compliance with any applicable terms and conditions upon which Rajant makes such information available.

Software, Upgrades and Additional Copies. NOTWITHSTANDING ANY OTHER PROVISION OF THE AGREEMENT: (1) CUSTOMER HAS NO LICENSE OR RIGHT TO MAKE OR USE ANY ADDITIONAL COPIES OR UPGRADES UNLESS CUSTOMER, AT THE TIME OF MAKING OR ACQUIRING SUCH COPY OR UPGRADE, ALREADY HOLDS A VALID LICENSE TO THE ORIGINAL SOFTWARE AND HAS PAID THE APPLICABLE FEE TO AN APPROVED SOURCE FOR THE UPGRADE OR ADDITIONAL COPIES; (2) USE OF UPGRADES IS LIMITED TO RAJANT EQUIPMENT SUPPLIED BY AN APPROVED SOURCE FOR WHICH CUSTOMER IS THE ORIGINAL END USER PURCHASER OR LESSEE OR OTHERWISE HOLDS A VALID LICENSE TO USE THE SOFTWARE WHICH IS BEING UPGRADED; AND (3) THE MAKING AND USE OF ADDITIONAL COPIES IS LIMITED TO NECESSARY BACKUP PURPOSES ONLY.

Proprietary Notices. Customer agrees to maintain and reproduce all copyright, proprietary, and other notices on all copies, in any form, of the Software and Documentation in the same form and manner that such copyright and other proprietary notices are included on the Software. Except as expressly authorized in the Agreement, Customer shall not make any copies or duplicates of any Software without the prior written permission of Rajant.

Term and Termination. The Agreement and the license granted herein shall remain effective until terminated. Customer may terminate the Agreement and the license at any time by destroying all copies of Software and any Documentation. Customer's rights under the Agreement will terminate immediately without notice from RAJANT if Customer fails to comply with any provision of the Agreement. Upon termination, Customer shall destroy or return to RAJANT all copies of Software and Documentation in its possession or control. All confidentiality obligations of Customer, all restrictions and limitations imposed on the Customer under the section titled "General Limitations" and all limitations of liability and disclaimers and restrictions of warranty shall survive termination of this Agreement. In addition, the provisions of the sections titled "U.S. Government End User Purchasers" and "General Terms Applicable to the Limited Warranty Statement and End User License Agreement" shall survive termination of the Agreement.

Customer Records. Customer grants to RAJANT and its independent accountants the right to examine Customer's books, records, accounts, and network configuration(s) during Customer's normal business hours to verify compliance with this Agreement. In the event such audit discloses non-compliance with

this Agreement, Customer shall promptly pay to RAJANT the appropriate license fees, plus the reasonable cost of conducting the audit.

Export, Re-Export, Transfer and Use Controls. The Software, Documentation and technology or direct products thereof (hereafter referred to as Software and Technology), supplied by RAJANT under the Agreement are subject to export controls under the laws and regulations of the United States ("U.S.") and any other applicable countries' laws and regulations. Customer shall comply with such laws and regulations governing export, re-export, import, transfer and use of RAJANT Software and Technology and will obtain all required U.S. and local authorizations, permits, or licenses. RAJANT and Customer each agree to provide the other information, support documents, and assistance as may reasonably be required by the other in connection with securing authorizations or licenses. Information regarding compliance with export, re-export, transfer and use.

U.S. Government End User Purchasers. The Software and Documentation qualify as "commercial items," as that term is defined at Federal Acquisition Regulation ("FAR") (48 C.F.R.) 2.101, consisting of "commercial computer software" and "commercial computer software documentation" as such terms are used in FAR 12.212. Consistent with FAR 12.212 and DoD FAR Supp. 227.7202-1 through 227.7202-4, and notwithstanding any other FAR or other contractual clause to the contrary in any agreement into which the Agreement may be incorporated, Customer may provide to Government end user or, if the Agreement is direct, Government end user will acquire, the Software and Documentation with only those rights set forth in the Agreement. Use of either the Software or Documentation or both constitutes agreement by the Government that the Software and Documentation are "commercial computer software" and "commercial computer software documentation," and constitutes acceptance of the rights and restrictions herein.

Identified Components; Additional Terms. The Software may contain or be delivered with one or more components, which may include third-party components, identified by RAJANT in the Documentation, readme.txt file, third-party click-accept or elsewhere (e.g. on www.rajant.com) (the "Identified Component(s)") as being subject to different license agreement terms, disclaimers of warranties, limited warranties or other terms and conditions (collectively, "Additional Terms") than those set forth herein. You agree to the applicable Additional Terms for any such Identified Component(s).

Limited Warranty

Subject to the limitations and conditions set forth herein, RAJANT warrants that commencing from the date of shipment to Customer (but in case of resale by an Approved Source other than RAJANT, commencing not more than ninety (90) days after original shipment by RAJANT), and continuing for a period of the longer of (a) ninety (90) days or (b) the warranty period (if any) expressly set forth as applicable specifically to software in the warranty card accompanying the product of which the Software is a part (the "Product") (if any): (a) the media on which the Software is furnished will be free of defects in materials and workmanship under normal use; and (b) the Software substantially conforms to the Documentation. The date of shipment of a Product by RAJANT is set forth on the packaging material in which the Product is shipped. Except for the foregoing, the Software is provided "AS IS". This limited warranty extends only to the Software purchased from an Approved Source by a Customer who is the first registered end user. Customer's sole and exclusive remedy and the entire liability of RAJANT and its suppliers under this limited warranty will be (i) replacement of defective media and/or (ii) at RAJANT's option, repair, replacement, or refund of the purchase price of the Software, in both cases subject to the condition that any error or defect constituting a breach of this limited warranty is reported to the Approved Source supplying the Software to Customer, within the warranty period. RAJANT or the Approved Source supplying the Software to Customer may, at its option, require return of the Software and/or Documentation as a condition to the remedy. In no event does RAJANT warrant that the Software is error free or that Customer will be able to operate the Software without problems or interruptions. In addition, due to the continual development of new techniques for intruding upon and attacking networks, RAJANT does not warrant that the Software or any equipment, system or network on which the Software is used will be free of vulnerability to intrusion or attack.

No representation or other affirmation of fact, including but not limited to statements regarding capacity, suitability for use or performance of Software, whether made by Rajant employees or otherwise, shall be deemed to be a warranty for any purpose or give rise to any liability of Rajant whatsoever unless contained in this Agreement.

Restrictions. This warranty does not apply if the Software, Product or any other equipment upon which the Software is authorized to be used (a) has been altered, except by RAJANT or its authorized representative, (b) has not been installed, operated, repaired, or maintained in accordance with instructions supplied by RAJANT, (c) is assembled or deployed with non-authorized Rajant accessories; (d) has been subjected to abnormal physical or electrical stress, abnormal environmental conditions, misuse, negligence, or accident; or (e) is licensed for beta, evaluation, testing or demonstration purposes. The Software warranty also does not apply to (f) any temporary Software modules; (g) any Software not posted on RAJANT's Software Center; (h) any Software that RAJANT expressly provides on an "AS IS" basis on RAJANT's Software Center; (i) any Software for which an Approved Source does not receive a license fee; and (i) Software supplied by any third party which is not an Approved Source.

Hardware Limited Warranty

THE BREADCRUMB WIRELESS LAN UNITS ("BREADCRUMB"), EXCLUSIVE OF THE JR FAMILY OF BREADCRUMBS, PROVIDED UNDER THIS AGREEMENT ARE PROVIDED WITH A 1-YEAR WARRANTY AGAINST DEFECTS IN WORKMANSHIP OR MATERIAL UNDER ORDINARY USE. SUCH WARRANTY APPLIES ONLY TO THE BREADCRUMB DEVICE AND DOES NOT EXTEND TO ANY OTHER PRODUCTS, PRODUCTS OR SERVICES, INCLUDING BUT NOT LIMITED TO POWER SUPPLIES, CABLES, ANTENNAS, AND MOUNTING BRACKETS, EVEN IF PACKAGED OR SOLD WITH THE BREADCRUMB.

THE JR FAMILY OF BREADCRUMBS ARE WARRANTED ONLY AGAINST DEFECTIVE WORKMANSHIP FOR 90 DAYS WHEN DELIVERED NEW. RAJANT MAKES NO WARRANTY, AND DISCLAIMS ANY WARRANTY, EXPRESS OR IMPLIED AT LAW, ON THE JR FAMILY OF BREADCRUMBS' FITNESS FOR A PARTICULAR PURPOSE OR MERCHANTABILITY. MANUFACTURER'S RMA POLICIES AND PROCEDURES APPLY.

RAJANT PRODUCTS CLASSIFIED AS ACCESSORY ON MANUFACTURER'S PRICE LIST ARE WARRANTED AGAINST DEFECTS FOR A PERIOD OF 90 DAYS FROM DATE OF DELIVERY.

THE RAJANT HARDWARE LIMITED WARRANTY ONLY APPLIES WHEN GENUINE RAJANT HARDWARE AND AUTHORIZED ACCESSORIES ARE USED BY THE INSTALLER AND END USER. USE OF ANY NON-AUTHORIZED ACCESSORIES OR PERIPHERAL EQUIPMENT VOIDS THE RAJANT LIMITED HARDWARE LIMITED WARRANTY.

Unless otherwise listed on this Warranty Schedule, Rajant warrants to the purchaser that the Products will perform in all material respects in accordance with their written specifications for a period of ninety (90) days from the date of purchase. Reseller and purchaser's sole and exclusive right and remedy, and Rajant's sole and exclusive obligation and liability, with respect to any breach of the foregoing warranty shall be that, upon receipt by Rajant from Reseller or purchasers of written notice of the breach in reasonable detail so as to permit Rajant to duplicate the failure to so perform, which notice is received by Rajant within thirty (30) days after Reseller or purchaser discovers the failure, Rajant shall – after duplicating the failure – exercise its commercially reasonable efforts to deliver to Reseller or purchaser a replacement or repaired Product at Rajant's discretion. Rajant replacement parts used in such replacement may be new or equivalent to new. Rajant's obligations hereunder are conditioned upon the return of the affected Product in accordance with Rajant's then-current Return Material Authorization (RMA) procedures.

This warranty shall not apply to any Product that has been subjected to unusual physical, environmental or electrical stress. The warranty shall not apply to any problems or non-performance directly resulting from Reseller or purchaser's hardware, software, network(s) and/or host system(s) or the combination, operation or use of the Product with such hardware, software, network(s) and/or host system(s), or which results from any alteration or modification to the Product or its components by anyone other than Rajant. The warranty also does not cover any (a) Product for which the serial number has been removed or made illegible; (b) freight costs to the repair center; (c) scratches or other cosmetic damage to Product surfaces that do not affect the operation of the Product; and (d) normal and customary wear and tear.

The date of shipment of a Product by Rajant is set forth on the packaging material in which the Product is shipped. This limited warranty extends only to the original user of the Product.

Replacement, Repair or Refund Procedure for Products Covered by Warranty

Rajant will use commercially reasonable efforts to ship a repaired or replacement part within fifteen (15) working days after receipt of the RMA request. Actual delivery times may vary depending on Reseller's or purchaser's location.

To Receive a Return Materials Authorization (RMA) Number

Please contact the party from whom you purchased the Product. If you purchased the Product directly from Rajant, contact your Rajant Sales and Service Representative or email support@rajant.com.

DISCLAIMER OF WARRANTY

EXCEPT AS SPECIFIED IN THIS WARRANTY SECTION, ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS, AND WARRANTIES INCLUDING, WITHOUT LIMITATION, ANY IMPLIED WARRANTY OR CONDITION OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, NON-INFRINGEMENT, SATISFACTORY QUALITY, NON-INTERFERENCE, ACCURACY OF INFORMATIONAL CONTENT, OR ARISING FROM A COURSE OF DEALING, LAW, USAGE, OR TRADE PRACTICE, ARE HEREBY EXCLUDED TO THE EXTENT ALLOWED BY APPLICABLE LAW AND ARE EXPRESSLY DISCLAIMED BY RAJANT, ITS SUPPLIERS AND LICENSORS. TO THE EXTENT THAT ANY OF THE SAME CANNOT BE EXCLUDED, SUCH IMPLIED CONDITION, REPRESENTATION AND/OR WARRANTY IS LIMITED IN DURATION TO THE EXPRESS WARRANTY PERIOD REFERRED TO IN THE "LIMITED WARRANTY" SECTION ABOVE. BECAUSE SOME STATES OR JURISDICTIONS DO NOT ALLOW LIMITATIONS ON HOW LONG AN IMPLIED WARRANTY LASTS, THE ABOVE LIMITATION MAY NOT APPLY IN SUCH STATES. THIS WARRANTY GIVES CUSTOMER SPECIFIC LEGAL RIGHTS, AND CUSTOMER MAY ALSO HAVE OTHER RIGHTS WHICH VARY FROM JURISDICTION TO JURISDICTION. This disclaimer and exclusion shall apply even if the express warranty set forth above fails of its essential purpose.

Disclaimer of Liabilities—Limitation of Liability. IF YOU ACQUIRED THE SOFTWARE IN THE UNITED STATES, LATIN AMERICA, CANADA, JAPAN OR THE CARIBBEAN, NOTWITHSTANDING ANYTHING ELSE IN THE AGREEMENT TO THE CONTRARY, ALL LIABILITY OF RAJANT, ITS AFFILIATES, OFFICERS, DIRECTORS,

EMPLOYEES, AGENTS, SUPPLIERS AND LICENSORS COLLECTIVELY, TO CUSTOMER, WHETHER IN CONTRACT, TORT (INCLUDING NEGLIGENCE), BREACH OF WARRANTY OR OTHERWISE, SHALL NOT EXCEED THE PRICE PAID BY CUSTOMER TO ANY APPROVED SOURCE FOR THE SOFTWARE THAT GAVE RISE TO THE CLAIM OR IF THE SOFTWARE IS PART OF ANOTHER PRODUCT, THE PRICE PAID FOR SUCH OTHER PRODUCT. THIS LIMITATION OF LIABILITY FOR SOFTWARE IS CUMULATIVE AND NOT PER INCIDENT (I.E. THE EXISTENCE OF TWO OR MORE CLAIMS WILL NOT ENLARGE THIS LIMIT).

IF YOU ACQUIRED THE SOFTWARE IN EUROPE, THE MIDDLE EAST, AFRICA, ASIA OR OCEANIA, NOTWITHSTANDING ANYTHING ELSE IN THE AGREEMENT TO THE CONTRARY, ALL LIABILITY OF RAJANT, ITS AFFILIATES, OFFICERS, DIRECTORS, EMPLOYEES, AGENTS, SUPPLIERS AND LICENSORS COLLECTIVELY, TO CUSTOMER, WHETHER IN CONTRACT, TORT (INCLUDING NEGLIGENCE), BREACH OF WARRANTY OR OTHERWISE, SHALL NOT EXCEED THE PRICE PAID BY CUSTOMER TO RAJANT FOR THE SOFTWARE THAT GAVE RISE TO THE CLAIM OR IF THE SOFTWARE IS PART OF ANOTHER PRODUCT, THE PRICE PAID FOR SUCH OTHER PRODUCT. THIS LIMITATION OF LIABILITY FOR SOFTWARE IS CUMULATIVE AND NOT PER INCIDENT (I.E. THE EXISTENCE OF TWO OR MORE CLAIMS WILL NOT ENLARGE THIS LIMIT). NOTHING IN THE AGREEMENT SHALL LIMIT (I) THE LIABILITY OF RAJANT, ITS AFFILIATES, OFFICERS, DIRECTORS, EMPLOYEES, AGENTS, SUPPLIERS AND LICENSORS TO CUSTOMER FOR PERSONAL INJURY OR DEATH CAUSED BY THEIR NEGLIGENCE, (II) RAJANT's LIABILITY FOR FRAUDULENT MISREPRESENTATION, OR (III) ANY LIABILITY OF RAJANT WHICH CANNOT BE EXCLUDED UNDER APPLICABLE LAW.

Disclaimer of Liabilities—Waiver of Consequential Damages and Other Losses. IF YOU ACQUIRED THE SOFTWARE IN THE UNITED STATES, LATIN AMERICA, THE CARIBBEAN OR CANADA, REGARDLESS OF WHETHER ANY REMEDY SET FORTH HEREIN FAILS OF ITS ESSENTIAL PURPOSE OR OTHERWISE, IN NO EVENT WILL RAJANT OR ITS SUPPLIERS BE LIABLE FOR ANY LOST REVENUE, PROFIT, OR LOST OR DAMAGED DATA, BUSINESS INTERRUPTION, LOSS OF CAPITAL, OR FOR SPECIAL, INDIRECT, CONSEQUENTIAL, INCIDENTAL, OR PUNITIVE DAMAGES HOWEVER CAUSED AND REGARDLESS OF THE THEORY OF LIABILITY OR WHETHER ARISING OUT OF THE USE OF OR INABILITY TO USE SOFTWARE OR OTHERWISE AND EVEN IF RAJANT OR ITS SUPPLIERS OR LICENSORS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. BECAUSE SOME STATES OR JURISDICTIONS DO NOT ALLOW LIMITATION OR EXCLUSION OF CONSEQUENTIAL OR INCIDENTAL DAMAGES, THE ABOVE LIMITATION MAY NOT APPLY TO YOU.

IF YOU ACQUIRED THE SOFTWARE IN JAPAN, EXCEPT FOR LIABILITY ARISING OUT OF OR IN CONNECTION WITH DEATH OR PERSONAL INJURY, FRAUDULENT MISREPRESENTATION, AND REGARDLESS OF WHETHER ANY REMEDY SET FORTH HEREIN FAILS OF ITS ESSENTIAL PURPOSE OR OTHERWISE, IN NO EVENT WILL RAJANT, ITS AFFILIATES, OFFICERS, DIRECTORS, EMPLOYEES, AGENTS, SUPPLIERS AND LICENSORS BE LIABLE FOR ANY LOST REVENUE, PROFIT, OR LOST OR DAMAGED DATA, BUSINESS INTERRUPTION, LOSS OF CAPITAL, OR FOR SPECIAL, INDIRECT, CONSEQUENTIAL, INCIDENTAL, OR PUNITIVE DAMAGES HOWEVER CAUSED AND REGARDLESS OF THE THEORY OF LIABILITY OR WHETHER ARISING OUT OF THE USE OF OR INABILITY TO USE SOFTWARE OR OTHERWISE AND EVEN IF RAJANT OR ANY APPROVED SOURCE OR THEIR SUPPLIERS OR LICENSORS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

IF YOU ACQUIRED THE SOFTWARE IN EUROPE, THE MIDDLE EAST, AFRICA, ASIA OR OCEANIA, IN NO EVENT WILL RAJANT, ITS AFFILIATES, OFFICERS, DIRECTORS, EMPLOYEES, AGENTS, SUPPLIERS AND LICENSORS, BE LIABLE FOR ANY LOST REVENUE, LOST PROFIT, OR LOST OR DAMAGED DATA, BUSINESS INTERRUPTION, LOSS OF CAPITAL, OR FOR SPECIAL, INDIRECT, CONSEQUENTIAL, INCIDENTAL, OR PUNITIVE DAMAGES, HOWSOEVER ARISING, INCLUDING, WITHOUT LIMITATION, IN CONTRACT, TORT (INCLUDING NEGLIGENCE) OR WHETHER ARISING OUT OF THE USE OF OR INABILITY TO USE THE SOFTWARE, EVEN IF, IN EACH CASE, RAJANT, ITS AFFILIATES, OFFICERS, DIRECTORS, EMPLOYEES, AGENTS, SUPPLIERS AND LICENSORS, HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. BECAUSE SOME STATES OR JURISDICTIONS DO NOT ALLOW LIMITATION OR EXCLUSION OF CONSEQUENTIAL OR INCIDENTAL DAMAGES, THE ABOVE LIMITATION MAY NOT FULLY APPLY TO YOU. THE FOREGOING EXCLUSION SHALL NOT APPLY TO ANY LIABILITY ARISING OUT OF OR IN CONNECTION WITH: (I) DEATH OR PERSONAL INJURY, (II) FRAUDULENT MISREPRESENTATION, OR (III) RAJANT's LIABILITY IN CONNECTION WITH ANY TERMS THAT CANNOT BE EXCLUDED UNDER APPLICABLE LAW.

Customer acknowledges and agrees that RAJANT has set its prices and entered into the Agreement in reliance upon the disclaimers of warranty and the limitations of liability set forth herein, that the same reflect an allocation of risk between the parties (including the risk that a contract remedy may fail of its essential purpose and cause consequential loss), and that the same form an essential basis of the bargain between the parties.

Controlling Law, Jurisdiction. Customer agrees that all sales occurred, and contracts entered into at Malvern, Pennsylvania, notwithstanding the location of any affiliate or Customer's location or principal place of business. All contracts for the license of software and/or purchase of hardware are deemed to have occurred at Malvern, Pennsylvania and the Agreement and warranties ("Warranties") are controlled by and construed under the laws of the Commonwealth of Pennsylvania, United States of America, notwithstanding any conflicts of law provisions; and the state and federal courts of Pennsylvania shall have exclusive jurisdiction over any claim arising under the Agreement or Warranties.

The parties specifically disclaim the application of the UN Convention on Contracts for the International Sale of Goods. Notwithstanding the foregoing, either party may seek interim injunctive relief in any court of appropriate jurisdiction with respect to any alleged breach of such party's intellectual property or proprietary rights. If any portion hereof is found to be void or unenforceable, the remaining provisions of the Agreement and Warranties shall remain in full force and effect. Except as expressly provided herein, the Agreement constitutes the entire agreement between the parties with respect to the license of the Software, Hardware and Documentation and supersedes any conflicting or additional terms contained in any Purchase Order or elsewhere, all of which terms are excluded. The Agreement has been written in the English language, and the parties agree that the English version will govern.

Product warranty terms and other information applicable to RAJANT products are available at the following URL: www.rajant.com

RAJANT and the RAJANT Logo are trademarks of RAJANT Corporation and/or its affiliates in the U.S. and other countries. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between RAJANT and any other company.

Appendix H: GNU General Public License

Version 2, June 1991

PREAMBLE

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software–to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

1. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

1. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1

above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

1. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

1. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.
2. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.
3. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to

these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

4. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

1. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.
2. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

1. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

1. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.
2. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

HOW TO APPLY THESE TERMS TO YOUR NEW PROGRAMS

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

one line to give the program's name and an idea of what it does. Copyright © yyyy name of author

This program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 2 of the License, or (at your option) any later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with this program; if not, write to the Free Software Foundation, Inc., 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301, USA.

Also add information on how to contact you by electronic and paper mail.

If the program is interactive, make it output a short notice like this when it starts in an interactive mode:

Gnomovision version 69, Copyright © year name of author Gnomovision comes with ABSOLUTELY NO WARRANTY; for details type 'show w'. This is free software, and you are welcome to redistribute it under certain conditions; type 'show c' for details.

The hypothetical commands 'show w' and 'show c' should show the appropriate parts of the General Public License. Of course, the commands you use may be called something other than 'show w' and 'show c'; they could even be mouse-clicks or menu items–whatever suits your program.

You should also get your employer (if you work as a programmer) or your school, if any, to sign a "copyright disclaimer" for the program, if necessary. Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the program 'Gnomovision' (which makes passes at compilers) written by James Hacker.

signature of Ty Coon, 1 April 1989 Ty Coon, President of Vice

This General Public License does not permit incorporating your program into proprietary programs. If your program is a subroutine library, you may consider it more useful to permit linking proprietary applications with the library. If this is what you want to do, use the GNU Lesser General Public License instead of this License.