RADIOFRAME™
NETWORKS

RadioFrame Networks

RadioFrame System Method of Procedure GSM/802.11b

April 25, 2005

998-4002-00 Rev C

Service Information

This equipment complies with part 15 of the FCC Rules. Operation is subject to the two following conditions: This device may not cause harmful interference, and this device must accept any interference received, including interference that may cause undesired operation. This equipment has been tested and found to comply with the limits pursuant to part 90.691 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment.

Notices

These installation standards have been prepared to provide RadioFrame Networks Customers with general standards necessary to ensure that installed RadioFrame Networks equipment operates in accordance with the design parameters in the owned or leased buildings of RadioFrame Networks Customers and their customers, and to make certain equipment is installed safely and efficiently.

RadioFrame Networks reserves the right to revise this document for any reason, including, but not limited to, conformity with standards promulgated by various governmental or regulatory agencies, utilization of advances in the state of the technical arts, or to reflect changes in the design of equipment, techniques, or procedures described or referred to herein.

Liability to anyone arising out of use or reliance upon any information set forth herein is expressly disclaimed, and no representation or warranties, expressed or implied, are made with respect to the accuracy or utility of any information set forth herein.

Revision History

Software Release	Date
Pre-release	July 2004

To Obtain Copies

Contact RadioFrame Networks at:

- RadioFrame Networks, Inc.
  1120 112th Avenue NE, Suite 600
  Bellevue, WA 98004
- Telephone (425) 278-2780
- FAX (425) 278-2781
- E-mail USinfo@radioframenetworks.com

Final copies of this document are also posted as .pdf files on the RadioFrame Networks web site at: http//www.radioframenetworks.com.

Your Comments are Valued

The information in this document is subject to change. Please do not hesitate to point out discrepancies, express your concerns and make suggestions.

Copyrights and Trademarks

Throughout this publication, the terms RadioFrame Networks, RadioFrame and RFN signify RadioFrame Networks, Inc.

RadioFrame System GSM/802.11b/g Method of Procedure

Contents

List of Figures

1 Introduction

1.1 Scope of the Manual

This manual describes standards for installing, modifying and maintaining RadioFrame Networks' equipment at RadioFrame Networks customer sites. All specifications and requirements pertain to the RadioFrame Networks equipment required in Global System for Mobile communications (GSM)/802.11b/g installations. RadioFrame Networks recommends reading the entire manual before attempting to install or operate RadioFrame Networks equipment.

1.1.1 Prerequisites and Responsibilities

All installers are required to be trained and certified to install RadioFrame Networks equipment as follows:

- Installers shall be trained for specific equipment or the warranty on that equipment may be invalidated.
- All installers shall be able to use required tools and test equipment properly.
- Installers shall clean up and properly store tools at the end of each day's work.

The installation Project Manager shall be responsible for, but not limited to:

- Ensuring that all detailed engineering specifications, job drawings, technical information, and documentation required to successfully complete an installation are on site.
- Identifying any physical damage, defects, or problems that may prevent the proper installation, maintenance, or operation of equipment and reporting this information to the proper parties involved.
- Making an inventory and conducting a visual inspection of all equipment shipped to the job site prior to the installation.
- Ensuring that all installation job activities are completed in a safe and professional manner whether or not the specific activity is mentioned in this manual.
- Ensuring that all locations where painted surfaces have been marred are touched up. The touch-up paint shall be the same quality and shade as the paint used on the item being touched up.
- Using this *RadioFrame System GSM/802.11b/g Method of Procedure* manual to ensure that each specific job has been performed.
- Ensuring that the site is cleaned up after installation.

Preparation of a site and installation of equipment requires close coordination between RadioFrame and its customers, and designated third-party RadioFrame Certified Integration Partner(s). Domains of responsibilities are shown in the following table.

Task	Responsible Party
Prepares system design and quotes	Customer
Provides Project Management, including site survey	Customer
Constructs site, including racks, ironwork (ceiling support, ladder racks, etc.), AC power, DC power, and battery backup systems.	Customer
Lays conduit and cable, installs new fiber raceways, and fire stopping after cables have been laid.	RFN Certified Integration Partner
Installs, tests, and commissions RadioFrame Networks equipment, including site acceptance.	RFN Certified Integration Partner
Maintains RadioFrame Networks equipment, including logbook.	Customer

1.1.2 Site Documentation

The following documents are required for installing, commissioning, testing, and maintaining RadioFrame Networks equipment. Some or all of this documentation will be left on site. In addition, a logbook will be stored on site that will be used for tracking all changes, updates, and maintenance work done on RadioFrame System equipment.

Document
Site Survey
Pre-Installation Checklist
Equipment Inventory
Site Acceptance Test
Equipment Functionality Acceptance Test
Site As-built
Alarms
Alarm Procedures

1.1.3 Reference Documents

The following documents are intended to supplement the information contained in this manual.

- *RadioFrame System Field Guide*, RadioFrame Networks, 998-1000-00
- *RF Planning Guidelines*, RadioFrame Networks, 990-1001-00
- *Customer Release Notes*, RadioFrame Networks, 991-1000-00
- *National Electrical Code (NEC)*, current edition

1.2 Repair and Technical Support

RadioFrame Networks provides technical support services to its customers for the installation and maintenance of RadioFrame Networks equipment.

1.2.1 Before calling...

To minimize downtime, have the following information available prior to contacting the RadioFrame Networks Technical Assistance Center (TAC):

- Location of the RadioFrame System
- Date the RadioFrame System was put into service
- System Manager software version
- Symptoms of the problem
- If an alarm was generated, the alarm information including the information from the **Alarm Data** and **DebugFlag** fields on the Alarms page in System Manager
- Date the problem was first noticed
- If the problem can be reproduced
- What causes the problem to occur
- Any unusual circumstances contributing to the problem (i.e., dropped calls)

1.2.2 Technical Assistance Center

For support of RadioFrame Networks equipment, contact the RadioFrame Networks Technical Assistance Center at:

(US) (800) 328-0847

1.2.3 Repair Procedure

RadioFrame Networks boards are not field repairable. Do not attempt to repair RFN boards in the field. If RFN equipment should require service or repair, note the following information, then contact the RFN Technical Assistance Center at (800) 328-0847:

NOTE: Always use a static grounding wrist strap before handling any board or RadioBlade.

- Include the warranty and serial numbers of the affected equipment.
- Give a clear return address, including:
  - contact person,
  - phone number
  - alternate contact person and phone number (if possible)
- Securely package the board in the original shipping carton, if available. Otherwise, package in a static protection bag in a well padded carton.

1.3 Safety Precautions

Read all the notices in this section prior to installing or using the RadioFrame System or any of its components.

1.3.1 Static Sensitive Precautions

Electrostatic discharge (ESD) can damage equipment and impair electrical circuitry. It occurs when electronic printed circuit cards are improperly handled and can result in complete or intermittent failures.

Extreme care must be taken while handling, shipping, and servicing boards and RadioBlades. To avoid static damage, observe the following precautions:

- Prior to handling, shipping, and servicing equipment, always put on a conductive wrist strap connected to a grounding device. This discharges any accumulated static charges. All RFN RadioBlades and Field Replaceable Units (FRUs), including BPCs and APCs, are shipped with a disposable anti-static wrist strap (RFN P/N 110-0610-00).

Warning!

Use extreme caution when wearing a conductive wrist strap near sources of high voltage. The low impedance provided by the wrist strap also increases the danger of lethal shock should accidental contact with high voltage sources occur.

- Handle boards by the edges and avoid touching any conductive parts of the board with your hands.
- Never remove a board with power applied to the unit (hot-pull) unless you have verified it is safe to do so. Make sure the unit will not be damaged by removing the board.
- Avoid carpeted areas, dry environments, and certain types of clothing (silk, nylon, etc.) during service or repair due to the possibility of static buildup.
- Apply power to the circuit under test before connecting low impedance test equipment (such as pulse generators, etc.). When testing is complete, disconnect the test equipment before power is removed from the circuit under test.
- Be sure to ground all electrically powered test equipment. Connect a ground lead (-) from the test equipment to the board or module before connecting the test probe (+). When testing is complete, remove the test probe first, and then remove the ground lead.
- Place all boards and RadioBlades on a conductive surface (such as a sheet of aluminum foil) when removed from the system. The conductive surface must be connected to ground through 100kΩ.
- Never use non-conductive material for packaging boards or RadioBlades for shipment or storage. All units should be wrapped with anti-static (conductive) material. Replacement units shipped from the factory are packaged in a conductive material.
- If possible, retain all original packing material for future use.

1.3.2 Safety Warnings

Warning!	Only trained and qualified personnel should be allowed to install, replace, or service this equipment.
Warning!	This product relies on the building's installation for short-circuit (over current) protection. Ensure that a fuse or circuit breaker no larger than 120VAC, 15A U.S. (240VAC, 10A international) is used on the phase conductors (all current-carrying conductors).
Warning!	To comply with FCC RF exposure requirements, RadioBlade antennas must be installed to provide at least 8 inches (20 cm) separation from all persons, with antenna gain not exceeding zero (0) dBi.
Warning!	Never defeat the ground conductor or operate the equipment in the absence of a suitably installed ground conductor. Contact the appropriate electrical inspection authority or an electrician if you are uncertain that suitable grounding is available.
Warning!	The plug-socket combination must be accessible at all times because it serves as the main disconnecting device.
Warning!	Please read the RFU mounting instructions carefully before beginning the installation. Failure to use the correct hardware or to follow the correct procedures could result in a hazardous situation to people and damage to the system.
Warning!	Ultimate disposal of this product should be handled according to all national laws and regulations.
Warning!	To ensure FCC compliance of this equipment, it is the user's responsibility to obtain and use only shielded and grounded interface cables.
Warning!	**FCC RF Exposure Compliance:** FCC RF exposure compliance must be addressed at the time of licensing, as required by the responsible FCC Bureau(s), including antenna co-location requirements of 1.1307(b)(3). The applicable exposure limits, to demonstrate compliance, are specified in FCC Part 1.1310. Additionally, to comply with FCC RF exposure compliance requirements, the antenna(s) used for this transmitter must be fixed-mounted with at least 20 cm separation distance from any person. The installer of the antenna to be used with this transmitter may be required to perform an MPE evaluation and an Environmental Assessment (EA) of the location at the time of licensing per CFR 47 Part 1.1307. Fixed mounted antenna(s) that are co-located with other antenna(s) must satisfy the co-location requirements of Part 1.1307 for satisfying RF exposure compliance

1.3.3 Safety with Electricity

Warning!	To avoid electric shock, do not connect safety extra-low voltage (SELV) circuits to telephone-network voltage (TNV) circuits. LAN ports contain SELV circuits, and WAN ports contain TNV circuits. Some LAN and WAN ports both use RJ45 connectors; incorrect interconnection can cause equipment damage. Use caution when connecting cables.
Warning!	Before working on equipment that is connected to power lines, remove jewelry (including rings, necklaces, and watches). Metal objects will heat up when connected to power and ground and can cause serious burns or weld the metal object to the terminals.
Warning!	Hazardous network voltages are present in WAN ports regardless of whether power to the attached equipment is OFF or ON. To avoid electric shock, use caution when working near WAN ports. When detaching cables, detach the end away from the router first.
Warning!	Do not touch the power supply when the power cord is connected. For systems with a power switch, line voltages are present within the power supply even when the power switch is off and the power cord is connected. For systems without a power switch, line voltages are present within the power supply when the power cord is connected.

1.3.4 Recommendations

1.3.4.1 Safety Recommendations

- Keep tools away from walk areas where you and others could fall over them.
- Wear safety glasses if you are working under any conditions that might be hazardous to your eyes.
- Do not perform any action that creates a potential hazard to people or makes the equipment unsafe.

1.3.4.2 Guidelines for Working on Equipment Powered by Electricity

- Locate the emergency power off switch for the room in which you are working. Then, if an electrical accident occurs, you can act quickly to turn off the power.
- Before installing, removing, or repairing a BCU or ACU, unplug the power cord.
- Disconnect all power before working near power supplies.
- Do not work alone if potentially hazardous conditions exist.
- Never assume that power is disconnected from a circuit. Always check.
- Look carefully for possible hazards in your work area, such as moist floors, ungrounded extension cables, frayed power cords, and missing safety grounds.

1.3.4.3 In the Event of an Electrical Accident

- Use caution; do not become a victim yourself.
- Turn off power to the system.
- If possible, send another person to get medical aid. Otherwise, assess the condition of the victim and then call for help.
- Determine if the victim needs rescue breathing or external cardiac compressions, then take appropriate action.

2 System Description

The RadioFrame Networks GSM/802.11b/g solution generates RF within the building using low-power transceivers that are placed as needed to meet coverage and capacity requirements. The low-power nature of the transceivers minimizes interference with the surrounding macrocell system so that the macrocell system views the RFN GSM/802.11b/g solution as a peer. The RFN GSM/802.11b/g solution is remotely monitored down to the component level, including alarms and system performance, using a web-based interface, and over the Abis interface. The RadioFrame System is comprised of several components, which are connected in a 'tree'-style architecture:

- The Base Chassis Unit (BCU) acts as the sole connection point (i.e. the 'root') to all ACUs (and RFUs) which 'branch' off this 'root' chassis. The BCU also connects to the customer LAN.
- Up to eight Airlink Chassis Units (ACUs) connect from the BCU and send traffic, power and timing to the RFUs over standard CAT-5 wiring.
- Up to 64 RadioFrame Units (RFUs), 8 per ACU, which house the RadioBlades are mounted on walls and ceilings.
- Up to six GSM RadioBlades (RBs) can be installed per RFU, or a combination of four GSM RBs and one 802.11b/g integrated RadioFrame Access Point (RAP) per RFU.

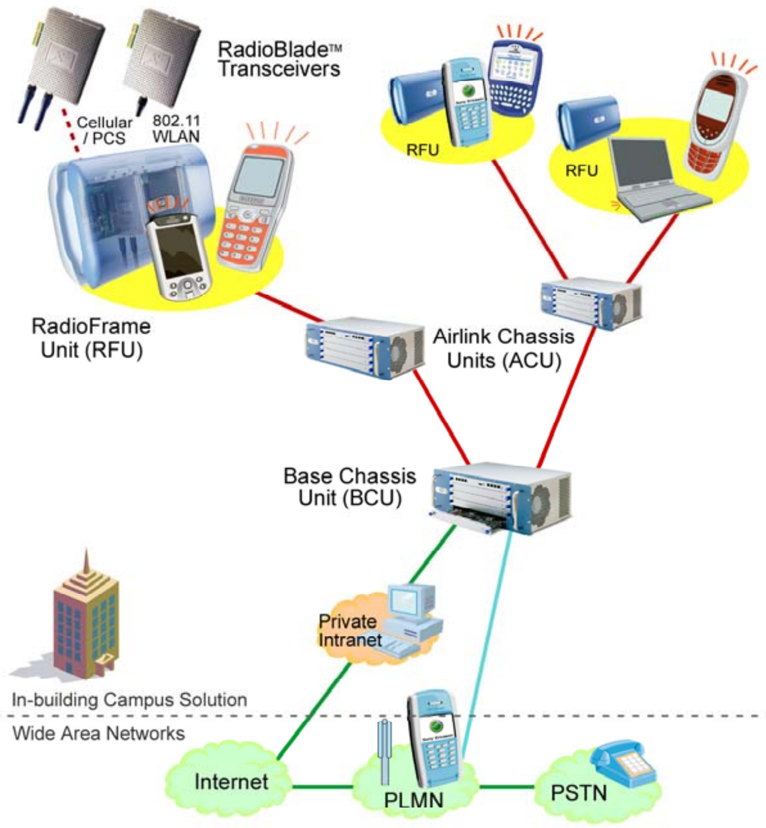


Figure 1 The RadioFrame System uses a 'tree'-style architecture.

2.1 Base Chassis Unit (BCU)

The Base Chassis Unit (BCU) is the main controller of the RFS and provides:

- The central processing function of the GSM RFS,
- The Abis interface towards the BCU (with TRAU remotely located within the BCU),
- Most of the data link layer and layer 3 functions of the BTS, and
- Network management

The main purpose of the BCU is to accommodate the need for simulcasting and to provide a single Abis interface to the BSC for each BTS function, therefore the partition of different BTS functions between BCU and ACU shall be designed with the consideration of processing load, traffic throughput and delay, user capacity, as well as supporting both simulcasting and non-simulcasting configurations.

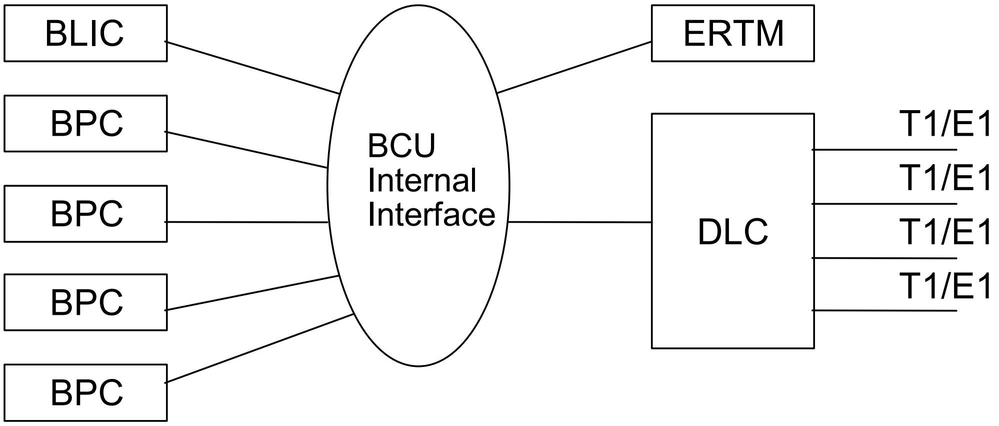


Figure 2 BCU functional diagram.

2.2 Airlink Chassis Unit (ACU)

The Airlink Chassis Unit provides the baseband airlink processing for up to 8 RadioFrame Units. The ACU is the interface between the RFUs and the Base Chassis Unit, and provides power, signals, and timing to the RFUs.

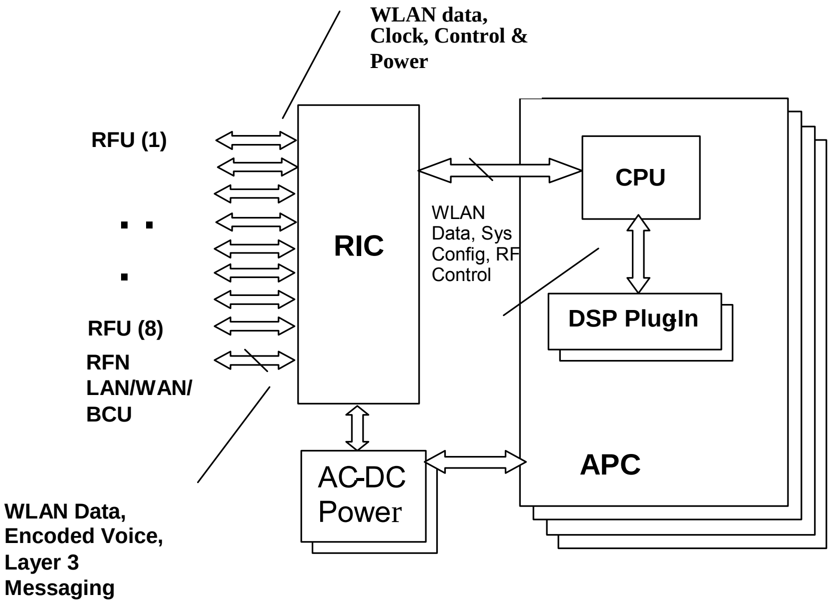

WLAN data, Clock, Control & Power
RFU (1)
RFU (8)
RFN LAN/WAN/ BCU
WLAN Data, Encoded Voice, Layer 3 Messaging
RIC
WLAN Data, Sys Config, RF Control
CPU
DSP PlugIn
AC-DC Power
APC

Figure 3 ACU functional diagram.

2.3 RadioFrame Unit (RFU)

The RadioFrame Unit serves as the access interface between signals received from mobile terminals and the airlink processing performed in the ACU. The RFU connects to the ACU via a single CAT-5 connection, and receives its power, signals, and timing from the ACU. Each RFU holds up to 6 RadioBlades in combination of: a maximum of 6 GSM RadioBlades, or 4 GSM RadioBlades and one 802.11 integrated RadioFrame Access Point (RAP).

2.4 GSM RadioBlade (RadioBlade or RB)

Each GSM RadioBlade provides a single RF channel transceiver supporting the GSM voice standard. Each RadioBlade contains an onboard omnidirectional antenna and inserts into a slot in the RFU.

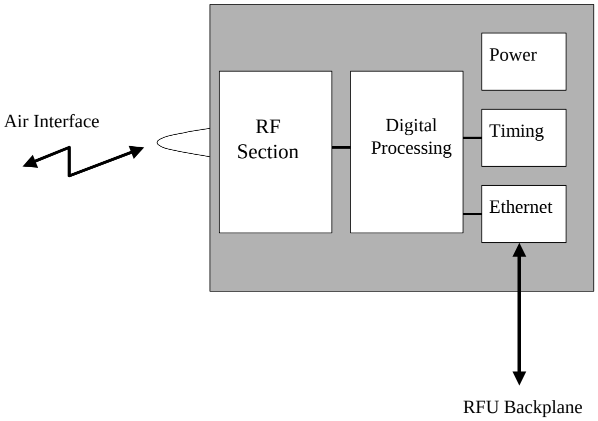


Figure 4 GSM RadioBlade functional diagram.

2.5 802.11b/g integrated RadioFrame Access Point (RAP)

The 802.11b/g integrated RadioFrame Access Point (RAP) is a dual-band transceiver supporting the 802.11b/g (WLAN) standards for wireless data. Each iRAP contains two Ethernet ports and inserts into a slot in the RFU.

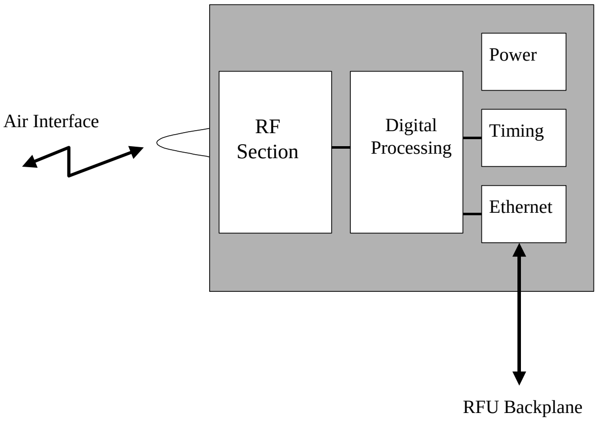


Figure 5 integrated RadioFrame Access Point (RAP) functional diagram.

2.6 Local Area Network (LAN)

The RadioFrame System plugs into the customer's local area network (LAN) using a standard Ethernet connection over CAT-5 wiring. The customer's LAN may include a variety of equipment, including switches, routers, and gateways. The RFS connects to the LAN via Ports 2-7 on the front of the BCU. The iRAPs installed in the RFUs support the LAN.

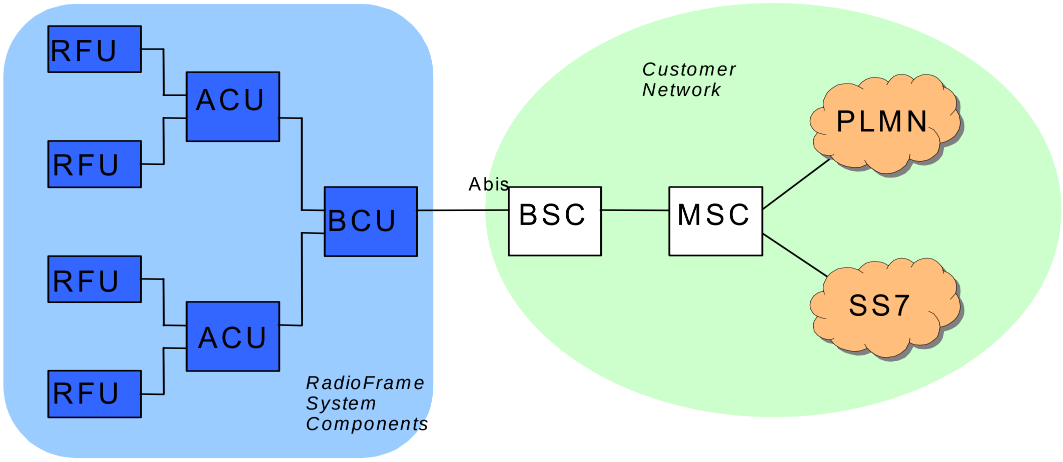


Figure 6 RFS and customer LAN functional diagram.

An optional "gateway" device may be used between the customer LAN and the RFS to provide a point of control, thus isolating the RFS from the customer's LAN. The gateway may be used to perform inter-network routing and access control, permitting only authorized users access to the customer LAN via the RFS. It may also perform service accounting and user mobility functions.

NOTE: Though not required, the use of a gateway device is strongly recommended, particularly for use as an access control mechanism to prevent unauthorized access to the customer LAN. In addition, while a router between the RFS and the customer LAN is not required, it is highly recommended that a combination router and security gateway be used.

The RFN implementation of 802.11b/g provides a transparent MAC layer bridging function between the RFS and the customer's LAN. No layer 3 (IP) protocol routing is required for operation.

2.7 Physical Relationships

The RadioFrame System is laid out as follows:

- Main rack: Located in a Telco closet, the main rack typically houses the BCU and one ACU.
- Remote ACUs: Up to seven additional ACUs can be connected to the BCU. The remote ACUs are installed in closets or Telco rooms throughout the building to support additional RFUs.
- RFUs: Up to 8 RFUs per ACU are installed on walls or on or above ceilings throughout the building to provide coverage for the GSM/802.11b/g RFS; RFUs house the GSM RadioBlades and iRAPs.
- LAN: Customer equipment located in a customer-defined area.

The two following illustrations show an example of a high-capacity and a low- capacity configuration of the RadioFrame Networks GSM/802.11 system. Both examples show a four story-building configuration depicting the difference in capacity provided by sectorization and the corresponding hardware changes. To gain three times the capacity (three times the number of BRs), no additional RadioBlades are required.

Remote ACUs are located on Floors 1, 2 and 3, with each ACU supporting up to eight RFUs. The ACU located on Floor 1 also supports RFUs in the parking level.

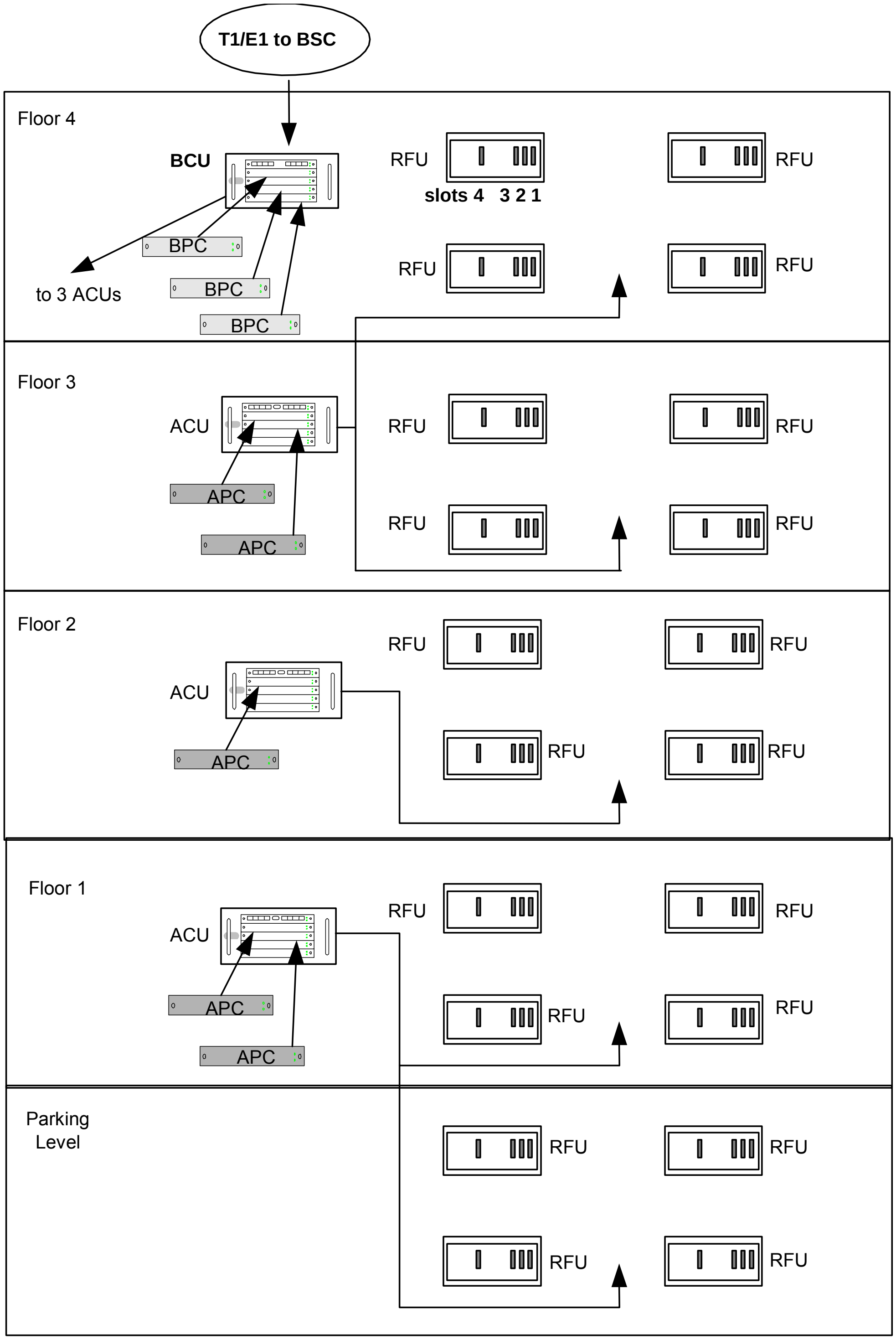


Figure 7 A typical high capacity (12 BR) RFS installed in a four-story office building.

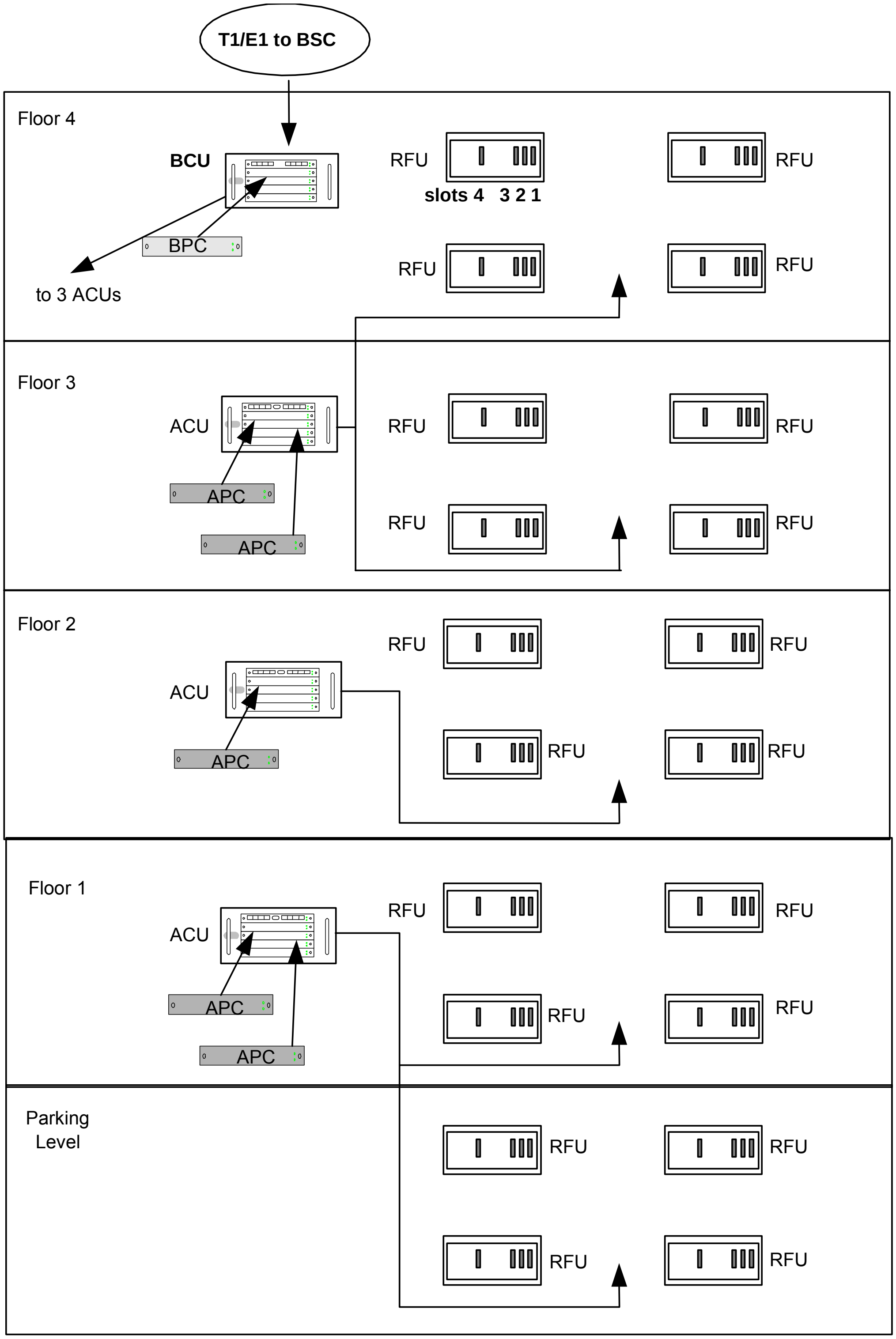


Figure 8 A typical low capacity (4 BR) RadioFrame System installed in a four-story office building.

2.7.1 Main Rack

The main rack is a 19” EIA standard rack and that is typically used to house the BCU and one ACU.

2.7.2 Remote ACUs

Remote ACUs are located in Telco rooms or other closets throughout the building mounted in 19” EIA-standard compliant racks or equivalent. The racks for remote ACUs may be either floor or wall-mounted racks. Any other method used to mount the remote ACU is not approved, and could void the warranty on the product and other components in the RFS.

2.7.3 RFUs

RFUs are located throughout the building to provide coverage for specific areas. RFUs are typically mounted on or above the ceiling, or on a wall. The following illustration depicts typical RFU locations using a simple floor plan. Three RFUs, denoted by triangles, are located along the central hallway providing coverage to each portion of the floor.

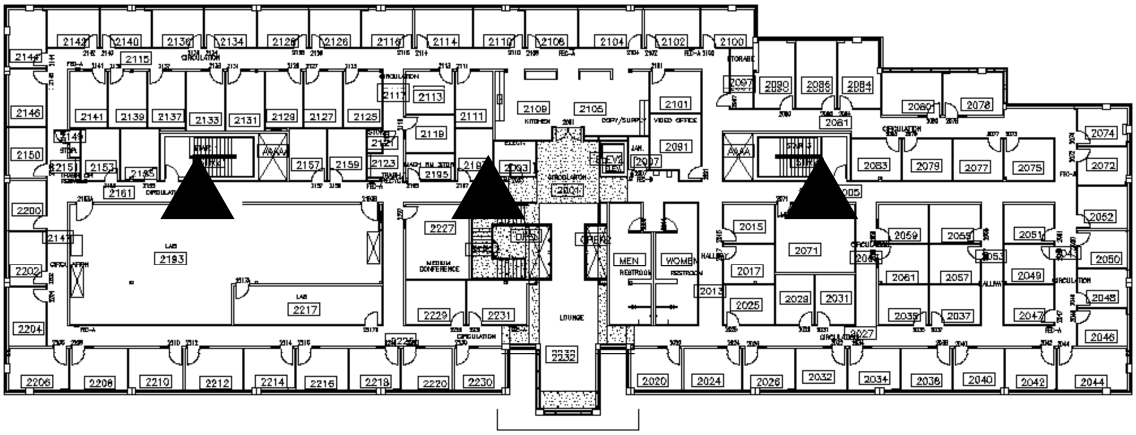
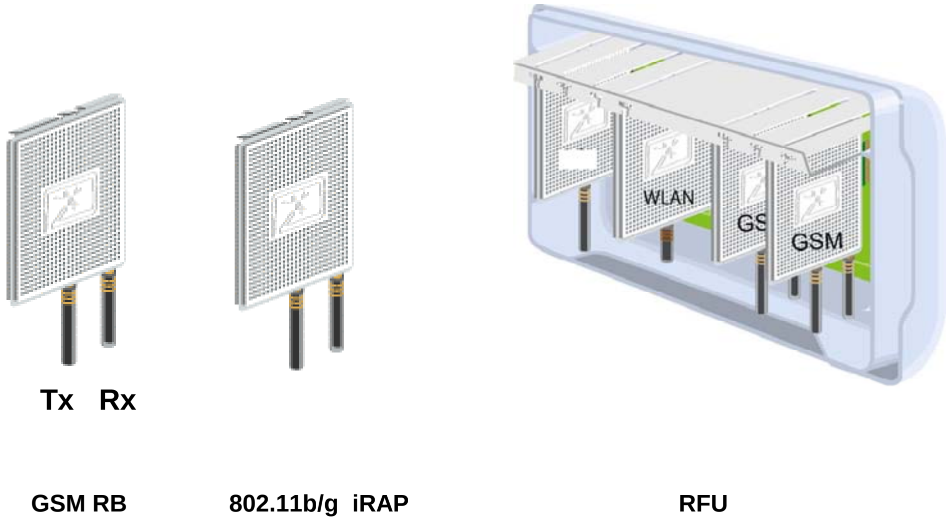


Figure 9 RFUs are located throughout the building to provide coverage.

2.7.3.1 RadioBlades and iRAPS

The number and combination of RadioBlades and iRAPs to be installed in each RFU is driven by the coverage and capacity requirements of that particular portion of the building. A maximum of six GSM RadioBlades can be installed in each RFU. A maximum of two iRAPs can be installed in each RFU. Each RadioBlade is supplied with an antenna that must be installed vertically and pointed down towards the ground.



GSM RB **802.11b/g iRAP** **RFU**

Figure 10 RadioBlades and iRAPs are inserted into the RFU so that the antennas point straight down to the ground.

2.7.4 LAN

The customer LAN equipment can be located anywhere within the building. An Ethernet cable connection must available from the LAN to the main rack for connection to the BCU.

3 Pre-Installation

This section provides pre-installation information for a RadioFrame System at a customer site. A pre-installation site review and evaluation helps prevent potential equipment installation problems. Consider every subject discussed in this section before installing the GSM/802.11b/g RFS.

3.1 Receipt of Equipment

RadioFrame Networks equipment is shipped as follows: the BCU, and each ACU and RFU are each shipped in its own box. The GSM RadioBlades and iRAPs are shipped several to a box and individually wrapped in antistatic packaging. Unpack each unit only at the time of installation—leave items in their shipping containers until ready for use.

3.1.1 Equipment Inspection

Inspect the RadioFrame Networks equipment immediately upon receipt. If obvious damage has occurred to shipping containers before unpacking, contact the shipping agent. Ask that a representative of the shipping company be present while the equipment is unpacked. Observe guidelines for safe handling of electrostatic sensitive devices or equipment to prevent damage due to electrostatic discharge. A conductive wrist strap is provided with each RFU and should always be worn when handling any electrical component, including GSM RadioBlades.

Check for the following:

- loose or damaged equipment in the pre-installed main rack
- dents, scratches, or other damage on all sides of each component
- physical damage to GSM RadioBlade or iRAP antennas or connectors

If any equipment is damaged, contact the shipping company immediately, then your customer representative.

3.1.2 Equipment Inventory

Check all the RadioFrame System equipment against the itemized packing list to ensure receipt of all equipment. If available, check the sales order with the packing list to account for all equipment ordered. Contact your customer representative to report missing items and for additional information.

3.1.3 RadioFrame Networks Documents Shipped with the RFS

The following RadioFrame Networks documents are shipped with the RadioFrame System.

Document Title	RFN Part Number
Product Specification: Chassis Unit	981-0500-00
Product Specification: 802.11b/g integrated RadioFrame Access Point	981-0532-00
Product Specification: NA GSM Dual Band RadioBlade	981-0631-00
Product Specification: RFU	981-1025-00
RadioFrame System Method of Procedure	998-4000-00

3.2 Site Planning

Licensing and the availability of space help to determine a site selection. Planning helps prevent potential on-site and off-site interference from other RF systems. Site layouts should always be planned to minimize inter-cabling lengths between RF equipment.

3.2.1 Site Considerations

3.2.1.1 Main Rack

The site for the main rack should not contain windows and must be able to resist extreme weather conditions. It should be designed to meet the requirements of the American National Standards, *Building Code Requirements for Minimum Design Loads in Buildings and Other Structure*s. RFN recommends the following considerations when selecting a site:

- A minimum floor space of at least 42 square feet is recommended to allow enough space for front and rear access to the main rack.
- The minimum ceiling height of at least 8’6” above a finished floor is required to allow enough space for the height of the main rack and cable access at the top of the cabinet.
- The ceiling structure should be able to support a cable tray assembly for routing the inter-cabinet cabling and other site cabling. The cable tray assembly is mounted to the site ceiling and walls per site plan and should be at least 7’6” from the site floor to allow for the height of the main rack.
- The minimum door dimensions should be at least 3’ wide and 6’8” high.
- All exterior doors should have tamper proof locks installed for security purposes.
- The interior site environment should be maintained at a constant 78° F (25.6° C). The site should be capable of maintaining this temperature in an outside ambient temperature range of -10 to +105° F (-23.4 to +40.6° C). RadioFrame Networks GSM solution equipment is not approved or recommended for outdoor use.
- Proper surge protection is required for all power inputs to prevent potential damage to site equipment.
- The site floor should be level to within 1/8” and able to support the weight of site equipment.

3.2.1.2 Remote ACUs

Remote ACUs are located in Telco rooms or other closets throughout the building. Any such location must be free of dust, wind, salt and liquids. All other operating environment specifications that apply to an ACU in the main rack also apply to a remote ACU.

Remote ACUs must be mounted in a 19” EIA-standard compliant rack or equivalent. The racks for remote ACUs must be either floor or wall mounted. Any other mounting method is not approved, and could void the warranty on the product and other components in the RFS.

The number of RFUs required to provide coverage for the GSM/802.11b/g RFS determines the number and location of remote ACUs.

3.2.1.3 RFUs

The RadioFrame System is designed to simplify site planning. The capacity requirements of the site determine the number of GSM RadioBlades and 802.11b/g iRAPs that will be required. RFUs are mounted so that the antennas of the installed GSM RadioBlades and 802.11b/g iRAPs point to the ground. This orientation of the antennas must not be changed.

The number and exact location of RFUs is determined by capacity and coverage requirements, as well as site considerations, such as mounting considerations, interior structures, and interference from macro systems.

3.2.1.4 LAN

Connecting the RFS to the customer LAN requires only a single Ethernet cable from the BCU in the main rack to the customer’s LAN equipment (gateway, switch, router etc.). No other site considerations are required.

3.3 Main Rack and Supporting Hardware

Most communications equipment is mounted into standard 19” EIA racks or enclosed cabinets. Follow the rack and/or equipment manufacturer's instructions when installing equipment into racks or cabinets.

For example:

- All supplied bracing hardware shall be properly utilized.
- Proper hardware shall be used to secure equipment.
- Convected heat transfer from one piece of equipment rack to another shall be considered. Heat baffles may be required.

3.3.1 Mounting

The front panels of the BCU and ACUs are 19” wide to allow for installation into 19” wide cabinets. For rack installation instructions for the BCU and ACU, see Appendix C BCU and ACU Main Rack Installation.

3.3.1.1 Plumb and Squareness

Equipment shall be level and plumb. Equipment level shall be tested on a known flat surface in at least two directions to verify accuracy.

Equipment shall be parallel or perpendicular to the surrounding walls and adjacent installed equipment.

3.3.1.2 Anchoring

Anchoring is the mechanical fastening of the communications equipment to suitable locations using hardware acceptable for the application.

Although every installation is unique, certain methods for anchoring shall be adhered to for all installations. Typically, at least four anchor points shall be used on each item of equipment mounted to the floor. The only exception is when the equipment manufacturer supplies other than four mounting points.

3.3.1.3 Mounting on Concrete Floors

Equipment racks or cabinets should be positioned and anchored to the floor using preferred mounting methods. In general, observe the following:

- An anchor specifically designed for concrete shall be used. The preferred method for anchoring racks, or other ancillary equipment to concrete floors is to use flush-mount expansion anchors properly sized for the application. Flush mount expansion anchors do not extend above the surface of the floor and provide an easy bolt down. They also provide the required pullout and shear strength. If at a later time equipment needs to be moved, flush mount expansion anchors do not get in the way.

  NOTE: Unless an isolating mounting scheme is used (refer to section 3.3.1.4 Isolated Mounting, next in this section), ensure that no anchors come in contact with reinforcing rods or wire mesh buried in the concrete; the rack shall be electrically isolated from any other equipment or materials at the site.

- In applications where flush-mount expansion anchors are not preferred or acceptable, then wedge-type stud anchors may be used.
- All concrete anchors shall be zinc-plated carbon steel for standard applications, galvanized steel for mildly humid or corrosive environments, and yellow zinc or stainless steel for humid, highly corrosive, or acidic environments. Minimum bolt diameter shall be 10 mm (0.375 in.) with 12 mm (0.5 in.) preferred. Anchor embedment depth should be at least 76 mm (3 in.) to provide good tensile and shear strength. Follow manufacturer's instructions for depth reduction when rebar is encountered. A heavy-duty washer should be part of the anchor assembly to ensure the equipment is secure.

3.3.1.4 Isolated Mounting

Isolated mounting is recommended to prevent a second electrical path to ground through the concrete floor, and is required for the installation of certain equipment. In these cases expansion anchors are inserted into the concrete floor. However, isolation of the equipment rack is ensured using an insulating plate and hardware. If the installation is in an earthquake zone, additional anchors are used.

3.3.1.5 Mounting on Wood or Fiberglass Floors

Appropriately sized lag bolts shall be used for mounting on wood or fiberglass floors. If the underside is accessible and the floor stability is questionable, then thru-bolting may be desirable.

RFN recommends mounting non-racked ancillary equipment on a "C-channel" type of mounting track where possible. This provides for easy cleaning and some isolation in the case of standing water. Another benefit of installing non-rack mounted equipment off the floor is that the weight is distributed across the floor. In these cases, C-channel type mounting provides multiple floor anchor points where the equipment provides only four to six anchor points.

When mounting racks to raised computer floors, 0.5 in. (13 mm) minimum diameter allthread rod and flush-mount expansion anchors shall be used to anchor to the concrete subfloor. When mounting consoles to a raised floor,
0.375 in. (10 mm) minimum allthread rod and hardware shall be used for anchoring. Mounting arrangement shall be in accordance with mounting kit manufacturer's instructions.

3.3.1.6 Anchoring Equipment to Raised Floors

The anchoring of overhead and wall-mounted devices present a number of considerations. Placement is very important; if equipment is bolted to a wall that is on an aisle, the aisle may be unacceptably narrowed with the danger of injury to personnel. Also, the serviceability of the equipment being mounted to adjacent equipment may be inhibited.

Overhead applications generally include coax cabling, cable runways, and mounts for earthquake bracing. All overhead applications should keep in mind loading of overhead surfaces. Care must be exercised when deciding how much can be held by the ceiling without some sort of building foundation support. In the case of earthquake bracing equipment, cable runways can be secured overhead then affixed to the equipment racks providing acceptable foundation support.

When anchoring cable runways to ceilings or walls, the manufacturer-supplied support hardware shall be used.

Anchors used in overhead applications vary depending on the ceiling structure as follows:

- For concrete and wood ceilings, the same principles discussed in floor anchoring apply.
- For an exposed steel I-Beam ceiling, many cable runway manufacturers make beam clamps for C-channel or threaded drop rods.
- For corrugated steel ceilings, C-channel tracks can be affixed to the ceiling using properly sized lag bolts. The C-channel will span the corrugated steel and provide multiple anchor points.

For drywall or plasterboard ceilings, special considerations are required:

- If the drywall is on steel or wooden roof joists, locate and tap into the roof joist with lag bolts.
- C-channel mounting can be used.
- An alternative to C-channel mounting is using large toggle or molly wings with hex head tap bolts.

  NOTE: Make certain joists are properly located before drilling into drywall.

3.3.1.7 Seismic Anchoring

Seismic anchors are designed, tested, and specified for seismic zones 3 and 4. Seismic anchors enhance the stability of equipment due to the special characteristics specifically suited to the dynamic and cyclic loading effects experienced during earthquake events. As such, anchors shall be used that are manufactured to particular specifications that make them the most resistant to the effects of dynamic and cyclic loading effects.

Selected anchors shall meet standards set forth in NESS (Network Equipment Building Systems) TR-64 and ASTM (American Society For Testing and Materials) 488-90 for earthquake compliance. This testing evaluates anchors for bolt failure from shearing and from pullout or slippage. Compliance with these standards requires that the anchor not allow a standard top heavy 7 ft. (2.2 m) rack to have a deflection greater than 3 in. (7.6 cm) at the top of the frame. This compliance will also adhere to Bellcore Technical Specifications AU-434 for earthquake concrete expansion anchors.

Anchor selection criteria shall comply with all general requirements for standard concrete anchors plus meet the above seismic requirements. All seismic anchoring shall be enhanced with top cabinet or rack bracing.

<u>Seismic Considerations</u>

All RadioFrame Networks equipment is seismically rated to withstand vibrations of a Level 3 earthquake. The property owner is responsible for any damage to RFN equipment due to building or rack structures that are not rated to withstand vibrations of a Level 3 earthquake, or not secured to withstand vibrations of a Zone 4 earthquake.

Site protection from earthquakes may be required in certain areas. Typically, this would be an area having historical data indicating a Moment Magnitude rating of 3 or 4. Note that areas other than historically prone areas may need consideration. Obviously, addressing such concerns results in increased costs of equipment installation.

A certified architect specializing in earthquake-resistant installation shall be consulted for seismic designs and recommendations in areas where the potential loss of the site may outweigh associated costs of earthquake-resistant design. In the United States, it is recommended to consult the US Geological Survey for more information regarding earthquake probability and historical data for various areas. In other areas, similar consultation should be done.

- The US Geological Survey information can be accessed at:
  http://geohazards.cr.usgs.gov
- Seismic maps are available at:
  http: //www.neic.cr.usgs.gov

Earthquake-resistant design should be contracted to a firm specializing in such work. However, the following general considerations need to be observed and factored into a seismic design program:

- Equipment shall not be secured to both the shelter walls and floors, since dissimilar movement between these surfaces is likely in an earthquake.
- Mounting should provide for some "sway" in the overall equipment mounting, thereby absorbing the energy of an earthquake. This is typically accomplished by rigid mounting of racked equipment or cabinets at the base, while semi-rigidly attaching the rack top using 1/8 in (3.2 cm) diameter steel braided wire rope. Wire rope anchors are then secured to ceilings joists. The benefit of this type of installation is that racks are allowed to sway within limits but can't fall over.
- Cabinet designs with wide footprints can be used to help prevent cabinets from tipping over.
- Columns of cabinets stacked and bolted back-to-back present a very stable and wide footprint. The bottom cabinets shall still, however, be bolted to the floor for complete security.
- Some cabinets can be outfitted with outrigger-type support legs to prevent tip-over. These outriggers alone do not provide adequate earthquake protection, but are typically adequate if the cabinet is bolted to the floor.

  NOTE: If a rack is seismic rated, any add-on aftermarket equipment or equipment that is not seismic rated will render the overall package as not being seismic tested and certified as a unit. Therefore, the unit would no longer be considered as seismic rated.
- When bolting down to computer floor, be sure to anchor all the way to the subfloor.
- Columns of cabinets must be supported, though not rigidly. Rigid mounting will result in extreme vibration and resultant mechanical failure during an earthquake. Semi-rigid mounting is preferred. Semi-rigid bracing is defined as bracing which allows a measurable amount of movement.
- Some computer floors lose mechanical integrity if several panels are simultaneously removed. This could lead to equipment floor collapse during at earthquake. The flooring manufacturer shall be consulted for floor removal procedures.
- Equipment shall be stabilized by a top support. This is critical in preventing a column of equipment from toppling, causing injury to personnel. The footings cabinet columns and racks shall be bolted to the floor as appropriate, using concrete anchors. Sometimes the cabinet columns are placed on C-channel tract or wooden pedestals.
- Cables and transmission lines should not be installed rigidly, and without strain relief. Make broad service loops.
- Lighting fixtures should be prevented from swaying by the addition of one or more guy wires. A fluorescent lighting fixture in particular, can be very dangerous if allowed to swing against a wall or equipment racks, shattering and spraying broken glass below. Fluorescent lighting fixtures shall have protective lenses or protective plastic sleeves that cover the fluorescent tube, preventing broken glass from falling on occupants.

- Storage cabinets shall be secured to the wall to prevent upset. Storage cabinets shall also have closable, secured doors to prevent contents from spilling during an earthquake.
- Ladders and other large objects shall be secured to a wall or removed from the equipment room when not in use. These items have been known to fall into “live” equipment during earthquakes.

3.3.2 Clearances

Proper spacing of equipment is essential for efficient use of the room area, ease of maintenance, and safety of personnel. The following specifications have been established to meet the National Fire Protection Associations (NFPA) Code, and the American Society of Heating, Refrigerating, and Air Conditioning Engineers (ASHRAE) standards. Any local regulations, as applicable, shall also be adhered to.

- To provide adequate working space, a 576 sq. in. (0.37 m^2) footprint (as measured from facing equipment surfaces) shall be used for combining equipment.

  NOTE: Local codes may require additional clearance. In such cases, the local code shall prevail.
- 36 in. (91 cm) front and side aisles shall be maintained around electrical panel boards (NPPA 70, Article 110-26).
- 36 to 48 in. (91 to 123 cm) front, side, and (where applicable) rear aisles are required for servicing equipment.
- 36 in. (91 cm) aisle shall be maintained in front of all equipment.
- 36 in. (91 cm) aisle shall be maintained between at least one end of an equipment row and building wall or other obstruction; longer aisles may require additional access breaks. Larger aisles and additional access breaks in a row may be require as the row becomes longer, such that a fire in the aisle does not prevent egress. Comply with any codes regarding fire egress specifications.
- Ingress and egress to equipment rooms shall conform to NFPA 70, Article 111 and local building and fire codes.
- In US installations where a facility is to be normally occupied, American with Disabilities Act (ADA) shall be complied with. Some general requirements of ADA are 91.5 cm (36 in.) wide doors, ramps and safety rails, 36 in. (91.5 cm) can turn around clearance for wheelchairs, and specific placement of telephones, fire extinguishers, light switches, etc.

  NOTE: ADA compliance in architectural plans may be required in obtaining a construction permit in some localities.

Main Rack Clearances	
BACK	36”
FRONT	36”
SIDES	36”
ABOVE	36”

System	Unit	Equipment Dimensions		
		Width	Depth	Height
RadioFrame System	BCU	19”	13”	7”
	ACU	19”	13”	7”

3.3.2.1 Back

System	Unit	Back Clearance
RadioFrame System	BCU	7”
	ACU	7”

3.3.2.2 Front

System	Unit	Front Clearance
RadioFrame System	BCU	12”
	ACU	12”

3.3.2.3 Sides

System	Unit	Side Clearance
RadioFrame System	BCU	right side facing 2”; left side 0”
	ACU	right side facing 2”; left side 0”

3.3.2.4 Above

System	Unit	Above Clearance
RadioFrame System	BCU	0”
	ACU	0”

3.3.3 Weight

System	Unit	Weight
RadioFrame System	BCU	27 lbs max.
	ACU	27 lbs max.

3.3.4 Power

System	Unit	Power
RadioFrame System	BCU	▪ 100-240 Volts AC, 47-63 Hz, 8A max. or ▪ Negative 52.5 ±.5 Volts DC, 10A max.
	ACU	▪ 100-240 Volts AC, 47-63 Hz, 8A max. or ▪ Negative 52.5 ±.5 Volts DC, 10A max.

3.3.5 Grounding

System	Unit	Grounding
Main Rack		▪ #2 AWG green-insulated copper wire between the main rack and the master ground bar ▪ do not daisy-chain multiple equipment cabinet grounds using a single ground wire
RadioFrame System	BCU	▪ internal grounding (UL and CE safety certified) ▪ bonding point provided for protective earth grounding; #8 screw with internal sems washer
	ACU	▪ internal grounding (UL and CE safety certified) ▪ bonding point provided for protective earth grounding; #8 screw with internal sems washer

3.3.6 Environment

System	Unit	Storage Temp	Operating Ambient Temperature	
			MIN	MAX
RadioFrame System	BCU*	-40ºF to +158ºF (-40ºC to +70ºC)	+32ºF (0ºC)	+104ºF (+40ºC)
	ACU*	-40ºF to +158ºF (-40ºC to +70ºC)	+32ºF (0ºC)	+104ºF (+40ºC)

* Altitude: -200 to +8,000 feet above mean sea level; above 8000’ reduce maximum operating ambient temperature by 2ºC per 1000’ to a maximum of 13,000’.

System	Unit	Relative Humidity
RadioFrame System	BCU	10-90% non condensing
	ACU	10-90% non condensing

3.3.7 Heat Load

System	Unit	BTUs per Hour
RadioFrame System	BCU	700
	ACU	700

3.3.8 Surge Arrestors

The local telephone company installs the T1/E1 line, which terminates in an 8-pin modular plug. This demarcation (demarc) point connects to the T1/E1 through a surge arrestor. The following illustration shows the T1/E1 interface with the GSM/802.11b/g RFS.

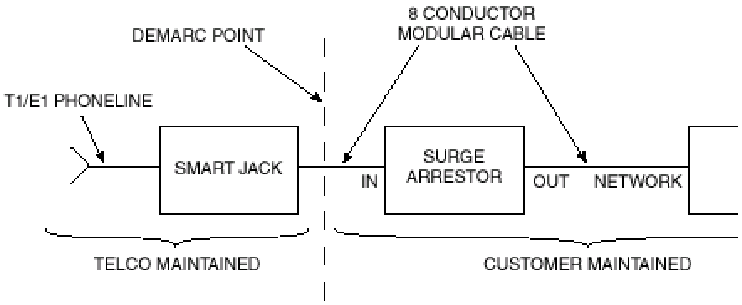


Figure 11 Telco (T1/E1) interface with the GSM/802.11b/g RFS.

The surge arrestor must be adequately grounded. The surge arrestor usually mounts near the demarcation (demarc) point. The cable connecting the surge arrestor to the Telco SmartJack should be locally procured, or should be provided with the surge arrestor. The following table lists RFN-approved surge suppression equipment.

AC Data Part #	Application	Clamp Voltage
TJ1010B	T1/E1 Surge Suppression, SAD + Gas Tube Hardwire and/or RJ connection	10 V
TJ3010B	T1/E1 Surge Suppression, SAD + Gas Tube Hardwire	7 V

3.3.9 Cable Support

This section describes requirements for cabling within equipment cabinets and racks. Cabling within racks and cabinets shall conform to the requirements of NFPA 70, Article 300, Article 800, Article 810, and Article 820. (Refer to ANSI/TIA/EIA-568(a) and 569(a) for additional information.)

All cables shall be installed and routed so that personal safety and equipment functionality is not compromised and that all equipment is accessible for servicing. The following requirements apply to cabling installed in racks or cabinets.

3.3.9.1 Securing cabling within racks or cabinets

To help prevent damage or accidental disconnection, cables and conductors shall be secured at intervals of no more than 3 ft (91 cm). Attachment shall be accomplished in a manner that does not restrict access to the equipment in the rack or cabinet.

Insulated standoffs are recommended for use in racks or cabinets. The standoffs should be of sufficient length to maintain the proper cable separation.

Nonmetallic cable ties shall be used to secure cables and conductors. Attachment shall be tight enough to secure cables without crushing them.

Cables that span a gap greater than 2 ft (61 cm) shall be supported.

3.3.9.2 Routing cables within racks and cabinets

Grounding conductors within racks or cabinets shall be routed toward the RGB, MGB, SSGB, or ground bus conductor. Connections to the RGB or ground bus conductor shall always be made with the equipment grounding or tap conductors being routed toward the MGB, SSGB, or RGB.

At points where grounding conductors must pass through a hole in a metallic surface and the hole is slightly larger than the conductor, the conductor shall be bonded to the metallic surface through which it passes. If the hole or opening is much larger than the conductor, and it is intended to accommodate several conductors, the conductor is not required to be bonded.

Cables in racks or cabinets shall be sized to length, and shall be installed and routed neatly and in a professional manner.

Excess cable shall not be coiled on top of cabinets or racks.

AC power cords longer than necessary may be looped down and back up a rack or cabinet. Excess lengths of AC power cord shall not be coiled on top of racks or cabinets.

3.3.9.3 Protecting cables within racks and cabinets

Grounding conductor tap joints shall be installed in order to prevent the conductor or connection device from coming in contact with metallic surfaces.

Where cables or conductors are routed through holes in metallic surfaces or near sharp edges, the sharp surfaces shall be suitably protected with a grommet or similar material to help protect the cable or conductor from damage caused by sharp edges.

3.3.9.4 Cable bending radius within racks and cabinets

Grounding conductors of all sizes shall maintain a minimum bending radius of 8 in. (20 cm). The angle of any bend shall be not less than 90°.

The bending radius of CAT-5 cables shall be not less than 10 times the outside diameter of the cable. Follow the cable manufacturer's recommendation and refer to ANSI/TIA/EIA-568 and CSA-T529 for additional information.

All other cables shall not have sharp bends that will damage or degrade the performance of the cable. The cable manufacturer's specifications shall be followed.

3.3.9.5 Cable separation and grouping within racks or cabinets

Cabling in racks or cabinets shall be grouped according to function.

Cable groups within racks and cabinets shall be separated by a minimum of
2 in. (5.1 cm) from other cable groups. Refer to ANSI/TIA/EIA-568a and -569; and NFPA 70, Articles 800-52, 810-18, and 820-52 for more information.

3.4 Remote ACUs

Up to seven remote ACUs may be installed for a total of 8 ACUs per BCU.

3.4.1 Mounting

Remote ACUs are located in Telco rooms or other closets throughout the building, mounted in 19” EIA-standard compliant racks or equivalent. Any other method used to mount the remote ACU is not approved, and could void the warranty on the product and other components in the RFS.

NOTE: The ACU may be placed on a flat surface only if the front and back of the unit are accessible and if the side vents are not blocked. In this case, the ACU is not secured and, therefore, is not rated to withstand any level of earthquake, and the warranty may be voided.

Currently, the remote ACU does not include a Universal Power Supply (future enhancement). Grounding of the remote ACU is not required by RadioFrame Networks and is the responsibility of the customer. A bonding ground point for protective earth grounding is provided; #6 screw with internal sems washer.

3.4.2 Clearances

- Dimensions: 19" wide x 7" high x 13" deep (approx.)

3.4.2.1 Back

- 7”

3.4.2.2 Front

- 12”

3.4.2.3 Sides

- Left side (facing unit): 0”; right side: 2”

3.4.2.4 Above

- Above: 0”

3.4.3 Weight

- 27 lbs (fully loaded)

3.4.4 Power

- 100-240 Volts AC, 47-63 Hz, 8-3.5A , or
- Negative 48-56 Volts DC, 11A

3.4.5 Grounding

The ACU is internally grounded by connecting the appliance inlet earthing ground to the power supply ground terminal.

The chassis unit is also internally bonded by connecting the appliance inlet earthing ground directly to the chassis (#6 AWG screw with internal sems washer).

3.4.6 Environment

- Operating Ambient Temperature: 0^{o}C to +40^{o}C (+32^{o}F to +104^{o}F)
- Altitude: -200 to +8000 feet above mean sea level; above 8000', reduce maximum operating ambient temperature by 2^{o}C per 1000' to a maximum of 13000'
- Storage Temperature: -40^{o}C to +70^{o}C (-40^{o}F to +158^{o}F)
- Relative Humidity: 10-90% non condensing
- Shock: 40 g’s
- Vibration: Level 3 earthquake
- Keep product free from dust, wind, salt, liquids

3.4.7 Heat Load

- 700 BTUs

3.4.8 Cable Support

- Power cord
- CAT-5 wiring to BCU
- CAT-5 wiring to as many as 8 RFUs

3.5 RFUs

3.5.1 Location

RFU placement is determined by first choosing an approximate location for each RFU using basic coverage requirements, then identifying the mounting configuration for each RFU (ceiling or wall). Typically, a floor plan of each story in the building is used as an aid to identify RFU placement.

In addition, RFU placement requires taking into consideration such factors as interior structures, multiple-floor installations, elevators and stairwells, and neighboring macro cell systems.

3.5.2 Mounting

Once the approximate RFU locations have been identified, determine the mounting configuration required for each RFU—on or above the ceiling, or on a wall. Wall mounts are ideal, provided the wall is of low density. Mounting the RFU to a structural brick or concrete wall can alter the unit’s omni directional pattern. Also, each RadioBlade installed in an RFU is supplied with an antenna designed to be installed vertically and pointed down. Do not change this orientation.

Suspended ceilings are very common in commercial buildings and mounting the RFU above the ceiling can work well, provided lower half of the RFU is kept clear of metal objects such as water pipes, wire bundles and light fixtures. The added benefit of an above-ceiling installation is that the RFU is hidden yet still easily accessed. Generally, suspended ceiling panels are of low-density lightweight materials that do not attenuate RF. The metal grid supports typically are spaced at greater than 2-foot intervals and will not dramatically affect the RFUs’ performance if they are kept at least 1-foot away from the antennas.

3.5.3 Clearances

- Dimensions: 13.5" wide x 8" high x 5" deep (approx.)

3.5.3.1 Back

- 0”

3.5.3.2 Front

- 0”

3.5.3.3 Sides

- 0”

3.5.3.4 Above

- Leave at least 1.25” between the top of the RFU and the ceiling or any overhead structure.
- Leave at least 3” below the RFU.

3.5.4 Weight

- 12 lbs (fully loaded with 6 RadioBlades/RAPs)

3.5.5 Power

- Negative 36-56 Volts DC, 0.8A

3.5.6 Grounding

- No additional grounding required

3.5.7 Environment

- Operating Ambient Temperature: 0^{o}C to +40^{o}C (+32^{o}F to +104^{o}F)
- Altitude: -200 to +8000 feet above mean sea level; above 8000', reduce maximum operating ambient temperature by 2^{o}C per 1000' to a maximum of 13000'
- Storage Temperature: -40^{o}C to +70^{o}C (-40^{o}F to +158^{o}F)
- Relative Humidity: 10-90% non condensing
- Shock: 40 g’s
- Vibration: Level 3 earthquake
- Keep product free from dust, wind, salt, liquids

3.5.8 Heat Load

- 85 BTUs

3.5.9 RF Exposure

To comply with FCC RF exposure requirements, GSM antennas must be installed to provide at least 8 inches (20 cm) separation from all persons, with antenna gain not exceeding zero (0) dBi.

3.5.10 Cable Support

- CAT-5 wiring to ACU

3.6 GSM RadioBlades

3.6.1 Mounting

- The GSM RadioBlades are inserted into the RFU.
- RFUs must be mounted in such a way that the GSM RadioBlade antenna points downward to the ground.

3.6.2 Clearances

- Dimensions: 3” wide x 4” high (plus antenna) x 0.5” thick (approx.)
- The GSM RadioBlade is housed in the RFU. If the RadioBlade is properly inserted into the RFU, no additional clearances are required.

3.6.2.1 Back

- 0”

3.6.2.2 Front

- 0”

3.6.2.3 Sides

- 0”

3.6.2.4 Above

- 0”

3.6.3 Weight

- 1 lb (approx.)

3.6.4 Power

- 3.3 VDC, 720mA max
- 2.5 VDC, 50mA max

3.6.5 Grounding

- No additional grounding is required

3.6.6 Environment

- Operating Ambient Temperature: 0^{o}C to +40^{o}C (+32^{o}F to +104^{o}F)
- Altitude: -200 to +8000 feet above mean sea level; above 8000', reduce maximum operating ambient temperature by 2^{o}C per 1000' to a maximum of 13000'
- Storage Temperature: -40^{o}C to +70^{o}C (-40^{o}F to +158^{o}F)
- Relative Humidity: 10-90% non condensing
- Shock: 40 g's
- Vibration: Level 3 earthquake
- Keep product free from dust, wind, salt, liquids

3.6.7 Heat Load

- Not applicable

3.6.8 Cable and Connector Wiring

- Connector type is RJ-45.
- If directly cabling to the GSM RB without an antenna, use female SMA connectors.
- Appropriate color-coding and jack pair assignments should be followed when wiring modular jacks, connectors, and cables.

Pin#	Name	Input / Output
1	Rx Ring	Input
2	Rx Tip	Input
4	Tx Ring	Output
5	Tx Tip	Output

Warning!

Crimp all connector wiring *completely*. Ensure that all crimps have fully penetrated the protective coating on the wiring. Ensure that enough of the protective coating is left in place to fit inside the connector. Failure to follow these instructions may cause system failures to occur.

3.6.9 Output Power Level

- Nominal (maximum): 10 dB
- Can be adjusted downward in 2 dB increments.

- Ability to turn on power control: YES

3.7 RAPs

3.7.1 Mounting

- The 802.11b/g integrated RadioFrame Access Points (RAPs) are inserted into the RFU.
- RFUs must be mounted in such a way that the iRAP antennas point downward to the ground.

3.7.2 Clearances

- Dimensions: 3” wide x 4” high (plus antenna) x 0.5” thick (approx.)
- The iRAP is housed in the RFU. If the iRAP is properly inserted into the RFU, no additional clearances are required.

3.7.2.1 Back

- 0”

3.7.2.2 Front

- 0”

3.7.2.3 Sides

- 0”

3.7.2.4 Above

- 0”

3.7.3 Weight

- 1 lb (approx.)

3.7.4 Power

- 3.3 VDC, 1.5A

3.7.5 Grounding

- No additional grounding is required

3.7.6 Environment

- Operating Ambient Temperature: 0^{o}C to +40^{o}C (+32^{o}F to +104^{o}F)
- Altitude: -200 to +8000 feet above mean sea level; above 8000', reduce maximum operating ambient temperature by 2^{o}C per 1000' to a maximum of 13000'
- Storage Temperature: -40^{o}C to +70^{o}C (-40^{o}F to +158^{o}F)
- Relative Humidity: 10-90% non condensing
- Shock: 40 g’s
- Vibration: Level 3 earthquake
- Keep product free from dust, wind, salt, liquids

3.7.7 Heat Load

- Not applicable

3.8 Interconnecting Cabling

Site planning requires true single point grounding. The Telco entrance and Telco termination board should be located as close to the transmission line entry and AC service entrance as possible. This enables the individual ground leads to bond to a single point, with the least amount of distance between the ground leads.

3.8.1 T1/E1

T1/E1 lines are used to connect the RadioFrame System with the Base Station Controller (BSC). Each GSM/802.11b/g RFS site is typically fed with a single T1/E1 line, and subsequently protected with a surge suppressor. The suppressor is located between the "smart jack" (maintained by the local telephone company) and the Channel Service Unit (CSU). The suppressor should be grounded downward directly to the master ground bus (MGB) using a #6 AWG green wire.

The Telco board and the MGB should be mounted adjacent to each other on the same wall (the coax ground and power ground should also be at this same location to achieve single point grounding). The Smart Jack and T1/E1 suppressor are located on the Telco board near the T1/E1 line entrance to the site.

3.8.2 Power Cabling

All electrical wiring for the site must meet the requirements of NEC and all applicable local codes.

3.8.2.1 AC Power Cabling

This section describes only the AC power. All grounding shall limit the exterior connections to a single point. The transmission wire entrance for the Telco service and board must be installed on a common wall to have true single point grounding.

Caution

Facility AC wiring within junction boxes, receptacles, and switches shall be performed by a licensed and bonded electrical contractor. Personnel safety and liability hazards can result from AC wiring performed by installation personnel other than an electrical contractor.

When an open equipment rack is used, hardwiring of power is not always possible. Mounting a dedicated simplex receptacle or receptacle assembly on the rack may be the most convenient method of supplying power, especially if multiple pieces of equipment are mounted on the rack. This is also a convenient way to install personal protection type 3 SPD devices to the equipment.

These receptacle assemblies can be pre-manufactured and mounted to the top face of an equipment rack. Mounting can also use a fabricated power pole mounted between racks.

Equipment that contains its own AC power supply is typically fitted with a standard grounded line cord. Where this equipment is used, the rack shall be equipped with a dedicated simplex receptacle or receptacle assembly.

Use only the power cables provided by RadioFrame Networks. Use of any other cable is strictly prohibited and may void the warranty and/or cause electrical fire and damage.

Caution

Under no circumstances shall consumer-grade power outlet strips be used In any Installation. Extension cords of any type shall not be used for connecting line power to communications equipment.

AC input power

Main Rack: The AC input power for the GSM/802.11b/g RFS shall be of 120 and shall be coming off one designated 20 amp breaker.

Remote ACUs: for 120VAC power, use the power cord provided (use of a different cord may void the warranty and/or cause electrical fire and damage).

3.8.2.2 DC Power Cabling

RFN provides a nine-foot –48VDC power cord (part number 111-0561-xx) with each -48VDC chassis unit (BCU and ACU). The power cord is 16AWG wire terminated on one end with a MOLEX connector wired according to the following table. This end plugs into the power connector on the RFN chassis unit. Terminate the other end to the provided power equipment as described below.

Wire Connection
-48 Volts DC Return (black)
-48 Volts DC (red)

Caution

The power supply cord is used as the main disconnect device for the chassis unit.

Length of run

For runs longer than nine feet, use only a UL-approved cable (the suggested standard is UL1007), with approved connectors as shown in the following table. Wire shall be sized to carry a minimum of 11 Amps per these recommendations:

Length of Run	Minimum recommended wire gauge
Up to 6’	16 AWG
6’ - 10’	14 AWG
10’ - 15’	12 AWG
15’ - 24’	10 AWG

3.8.3 Category 5 Cabling

All components of the RFS are connected using standard CAT-5 cabling installed in existing raceways or conduits when available. Use only RJ45 (T568B) connectors for system components. The same is true for connecting the RFS to the Customer LAN.

If using a patch panel between RFS components, ensure the following:

- **Use only a CAT-5e- or CAT-6-rated patch panel.**
- **Follow all TIA 568B standards.**
- **Total impedance, end to end, *cannot* exceed 8 ohms.**
- **Use only CAT-5e or CAT-6 wiring.**

Maximum length between RFS components shall not exceed 328’ (100 meters).

The maximum DC resistance allowed cannot exceed 26.2 Ohms per 1000 feet.

Use plenum rated cable if the cable traverses through a plenum (open air) space.

The proper installation of computer network cabling is critical to the safe and reliable operation of the computer network. It is recommended that standards developed by the

Telecommunications Industry Association/Electronic Industries Association (TIA/EIA) and the Canadian equivalent (or equivalent standards in other countries) be followed. Applicable NFPA codes, local electrical codes, local building codes and other standards in this manual shall also be conformed to when installing computer network cabling.

NOTE: It is recommended that a specialist in the installation of computer networks perform computer network cable installations. The specialist should have the expertise, knowledge of applicable local codes, and the test equipment required for a quality installation.

NOTE: This section cites standards from the American National Standards Institute (ANSI), the Electronic Industry Association (EIA), the Telecommunications Industry Association/Electronic Industries Association (TIA/EIA), and the Canadian Standards Association (CSA). Even in non-domestic installations, these standards should be adhered to.

3.8.3.1 Case Type

CAT-5 Unshielded Twisted Pair (UTP), 100-ohm cable is the recommended cable type for computer network cabling, and will be the assumed cable type throughout this section. CAT-5 cable is preferred over CAT-3 and CAT-4 cables because of its ability to support 100Mbps (Megabits per second) systems and because of its better immunity to Electromagnetic Interference (EMI) and Radio Frequency Interference (RFI). Refer to ANSI/TIA/EIA-568-A, and CSA-T529 for more information.

3.8.3.2 Connecting Hardware

UTP cables shall be terminated with connecting hardware of the same category rating or higher. This includes all connectors, punch blocks, cross-connect jumpers and patch cords. It is recommended that hardware used to terminate cables be of the insulation displacement (IDC) type. Modular connectors shall also be of the proper typed for the cable used; solid conductor cable uses a different connector than stranded cable. Refer to ANSI/TIA/EIA-568-A, and CSA-T529 for more information.

3.8.3.3 Cable and Connector Wiring

Appropriate color-coding and jack pair assignments should be followed when wiring modular jacks, connectors, and cables. The same wiring standard shall be used throughout the cabling system. ANSI/TIA/EIA T568B is the recommended standard. The following illustration shows end views of an 8-pin Modular female jack for T568B with the pairs and colors identified. Refer to ANSI/TIA/EIA-568-A, and CSA-T529 for more information.

⚠ Warning!	Crimp all connector wiring *completely*. Ensure that all crimps have fully penetrated the protective coating on the wiring. Ensure that enough of the protective coating is left in place to fit inside the connector. Failure to follow these instructions may cause system failures to occur.

Pin#	Color Code (wires)
1	white/orange
2	orange/white
3	white/green
4	blue/white
5	white/blue
6	green/white
7	white/brown
8	brown/white

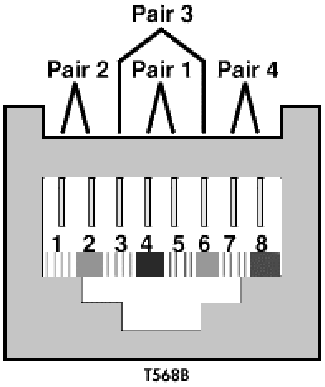


Figure 12 T568B standard.

3.8.4 Installation

Avoid any unnecessary junction points and cross-connects. Every added junction point and cross-connect can decrease the performance of the network.

Multiple appearances of the same cable at different locations, referred to as bridge taps shall be avoided. Each cable segment shall have only one source and one destination.

Never untwist the twisted pairs of a CAT-5 cable beyond 1.3 cm (0.5 in.) from the point of termination. Untwisting the wires can decrease the cable's category performance rating and degrade system performance. Refer to ANSI/TIA/EIA-568-A and CSA-T529 for more information.

Do not make sharp bends in CAT-5 cable. The bend radius for CAT-5 cable shall not be less than ten times the outside diameter of the cable. Bending the cable with a shorter bend radius can affect the electrical characteristics of the cable and degrade system performance. Refer to ANSI/TIA/EIA-568-A and CSA-T529 for more information.

Do not pull a CAT-5 cable with excessive force. CAT-5 cable should not be pulled with a force greater than 110 Newtons (25 lbs force), or as suggested by the cable manufacturer. Pulling a cable with too much force can change the cable's electric characteristics and degrade its performance. Refer to ANSI/TIA/EIA-568-A and CSA-T529 for more information.

Do not over tighten CAT-5 cable with cable ties or other supports. Over tightening cable ties or other supports can change the electrical characteristics of the cable and degrade the system performance. Refer to ANSI/TIA/EIA-568-A and CSA-T529 for more information.

CAT-5 segment lengths shall not exceed 100 m (328 ft.). This includes 90 m (295 ft.) of building cabling and up to 10 m (32.8 ft.) of equipment cords, cross-connects and patch cords. Of the 10 m (32.8 ft.) allowed for equipment cords, cross-connects and patch cords, a maximum of 3 m (9.8 ft.) should be used from the computer workstation to the information outlet. Refer to ANSI/TIA/EIA-568-A and CSA-T529 for more information.

For simplifying installation and reducing cable runs, a single CAT-5 cable may be run from the equipment room hub to an additional hub in the computer workstation area for distribution to the individual computers. This can reduce the number of cables required between the equipment room and the individual computers. Refer to ANSI/TIA/EIA-569-A for more information.

3.8.4.1 NEC Compliance

All RadioFrame Networks products and equipment are NEC compliant.

3.8.4.2 Local Jurisdictions

Local jurisdiction codes shall apply and override any other requirements specified in this document.

3.8.4.3 Routes

Consideration should be given to using some method of cable management and containment for runs of CAT-5 cable. Such methods can be dedicated cable runs, lay-in wireways, cable runways and conduits. Refer to ANSI/TIA/EIA-569-A and CSA-T530 for more information.

CAT-5 cable shall not be installed in the same conduit, cable runway, outlet box, or similar device with AC power cables, unless separated by a barrier as allowed in NFPA 70, Article 800-52. Doing so can be unsafe and is likely to cause EMI onto the CAT-5 cable, causing network errors. Refer to NFPA 70, Article 800-52, ANSI/TIA/EIA-568-A, and CSA-T529 for more information.

Precautions should be taken to avoid routing CAT-5 cable near sources of EM/RFI. Such noise sources may be electrical power wiring, dimmer switches, radio frequency transmitters, motors, generators, and fluorescent lights. Precautions may include, increasing the physical distance between the CAT-5 cable and the source of the EMI/RFI, installing the CAT-5 cable inside of a grounded metallic conduit, or use of a CAT-5 100-ohm screened twisted pair cable as permitted by ANSI/TIA/EIA-568-A. Routing cables near sources of EMI/RFI can cause data errors and degraded system performance. Refer to ANSI/TIA/EIA-568-A and CSA-T529 T530 for more information.

Cables shall be separated by at least 5.1 cm (2 in.) from AC power conductors. Refer to NFPA 70, Article 800-52 for more information.

CAT-5 cables installed in ducts, plenums, and other air-handling spaces shall be installed in accordance with other sections of this document and NFPA 70, Article 300-22. Also refer to NFPA 70, Article 645.

CAT-5 cables installed in hazardous areas as defined in NFPA 70, Article 500 shall be installed in accordance with NFPA 70, Article 500 and any other applicable electrical and building codes.

CAT-5 cable shall not be attached by any means to the exterior of a conduit or other raceway as a means of support. Refer to NFPA 70, Article 725-54 and NFPA 70, Article 800-52 for more information.

Suspended ceiling support rods and wires may be used as a means of support for computer network cabling if used in conjunction with appropriate cable fasteners. Refer to ANSI/TIA/EIA-569-A and CSA-T530 for more information.

CAT-5 cables shall not be laid directly on the tiles of a false ceiling. Refer to ANSI/TIA/EIA-569-A and CSA-T530 for more information.

CAT-5 cables shall not be run from one building to another building. If the computer network needs to be extended to another building, a specific cabling system shall be engineered. Options for extending from one building to another may include the use of fiber optic cable or a T1/E1. Computer network cabling entering and/or leaving a building shall be properly grounded and protected from surges as required elsewhere in this document.

3.8.4.4 Testing

Every effort should be made to ensure a quality installation of the computer network cabling system. Even the best installation effort cannot guarantee a properly working system. It is therefore required that a computer network cabling system be tested for proper performance.

The procedures and specifications in the TIA/EIA Telecommunications System Bulletin (TSB) 67 shall be used for this testing. TSB 67 has four primary parameters to test. Below is an overview of the four test parameters needed to assure a properly working system.

Wire map

The wire map test is used to verify wire pair to pin termination at each end of the cable and to check for installation connectivity errors. It is recommended that 100% of cables be tested using a testing tool such as Microtest® Microscanner™ Pro. (Be sure the tester can check for a “split pair” configuration).

Each of the 8 conductors in the cable are tested for:

- Conductor continuity to the remote end of the cable
- Shorts between any two or more conductors in the cable
- Crossed pairs in the cable
- Reversed pairs in the cable
- Split pairs in the cable
- Any other wiring errors in the cable

Length

The length test is used to determine the maximum physical length of the cable segments. The Microscanner™ Pro and many other models can be used to check cable length, which are accurate within a few feet. The RFN guideline for cable length is 100 meters (approximately 328’ for less).

Attenuation

Attenuation is the measure of signal loss in the cable segment.

Near-End Crosstalk (NEXT) loss

NEXT loss is a measure of signal coupling from one wire pair to another within a single UTP cable segment.

3.8.4.5 Labeling

Cabling shall be identified with a standardized, double-ended system to facilitate cable and equipment connection identification. (Refer to ANSI/TIA/EIA-606 for more information.) The label should show the following:

- Equipment identification for each end of cable.
- Connector reference designator for each end of cable.
- Direction along the cable where terminating equipment is located.
- Floor and room of the equipment.

In general, the following considerations need to be observed in implementing a labeling system:

- Labeling shall indicate the destination ends of the cable, in terms of equipment name and connector reference designator or name. This applies to connectorized, lugged, or punched-down cable terminations, regardless of the application (RF, audio, or control).
- Labeling shall be imprinted on white opaque material (preferably plastic or plasticized paper) using indelible black ink.
- Labeling should wrap entirely around the cable. It should be secure enough to assure label retention if the cable is to be pulled through conduit.
- Label placement shall be between 10 and 16 cm (4 and 6 in.) from each end of the cable (or the most logical point that would allow the label to be easily read).
- Information printed on each label should be brief but clearly understandable. Because of limited space, abbreviations and acronyms should be used. If abbreviations are used, they should be industry standard.
- All cables shall be properly labeled by the manufacturer as to the type, capacity, and approval ratings of the cable.

3.9 Main Rack Configuration

The main rack typically contains the BCU and one ACU of the RadioFrame System. The rack must be an standard 19” EIA-compliant rack, or equivalent.

3.10 RF Planning

RF planning places a minimum number of RadioFrame Units in locations that will provide optimal coverage and voice quality. RF planning for the RadioFrame System takes into consideration anything that might affect RF propagation, including:

- RFU locations, including coverage and mounting requirements, multi-story installations, and elevator shafts and stairwells
- Simulcasting, including single-sector and multi-sector systems
- Interference, including out-of-building emissions and in-building interference from macro systems

3.11 Site Survey

An informal site survey can be conducted to determine RFS equipment locations. Based upon the RFS square footage model, preliminary site designs are relatively easy to calculate prior to a formal site survey (refer to Appendix B “Site Survey” for an example of site survey questions and information).

3.12 Tools Required

The RadioFrame System comes with all the parts necessary to mount each component of the system. This section describes all of the equipment necessary to install the RadioFrame System.

3.12.1 Hand Tools

- #2 Phillips screw driver.
- Optional: For RFU ceiling mounts, a drill with a 3/16” bit for use with provided wood screws, or a 9/32” bit and four ¼” bolts (not provided).

3.12.2 Laptop Computer

A laptop computer is required to bring up the RFS. The laptop must be loaded with the following fully functional equipment (or equivalent):

- Serial cable (DB9/RS232)
- Ethernet cables to connect to the BLIC:
  - crossover EIA/TIA 568A
  - straight through EIA/TIA 568B
- CD-ROM capability
- FTP server (WFTPD) 32- shareware
- Telnet and serial communications software (TeraTerm) - shareware
- Administration rights to change IP settings on laptop

3.12.3 RadioFrame System Software

- Up-to-date version loaded on the laptop
- Loaded on a CD ROM
- New versions can also be downloaded from RFN web site

3.12.4 Additional Materials

- Wire ties
- Straight blade screwdriver
- Spare RJ45 connectors
- Wire cutters
- RJ45 connector crimper
- CAT-5 tester

4 Installation

Following all construction work, both exterior and interior, the site and facility shall be in a suitable condition for the installation of communications equipment. In general, the following considerations need to be observed:

- Interior of facility shall be free of excessive dust.
- All refuse related to the installation tasks shall be removed.

Consideration should be exercised when laying out a site to allow primarily for all code requirements for spacing, and then the most efficient use of space. Special attention shall be given to future expansion with regard to cable runway heights, electrical outlet placement, and equipment placement.

Prior to performing the installation procedures, prepare the site with all associated antennas, phone lines, and other related site equipment. This information is covered in the Pre-Installation chapter. The main rack may already be installed, depending on the site configuration.

4.1 Main Rack and Supporting Hardware

This section provides installation instructions for a cabinet already containing the RadioFrame Networks BCU and ACU. The procedure listed here is for permanently mounting the equipment cabinet within a site.

The following procedures describe how to mount non-wheeled cabinets in a system site building. Be sure to read all of the procedures carefully to ensure a quality installation.

4.1.1 Main Rack

The main rack must be secured to the floor for optimum stability. Since the main rack is very heavy, this procedure is written so that the rack is moved only once.

Warning!

Always use two or more persons whenever moving a cabinet. A fully configured equipment cabinet weighs approximately 800 lbs (360 kg).

Perform the following steps to properly install the main rack within the site building:

1 Measure the mounting location for the main rack within the row.

2 Carefully mark the mounting holes with a pencil, as indicated on the appropriate main rack footprint.

3 Drill the marked mounting holes to the appropriate depth of the mounting hardware with a hammer drill and bit.

4 Insert an anchor into the drilled hole.

If necessary, tap the anchor into place using a hammer.

5 Remove the four screws securing the bottom kick panel to the front and back of the main rack.

Remove the kick panel and set aside during installation.

6 Carefully move the main rack into the position indicated by the holes in the floor.

Adjust and level the main rack as necessary to align the rack mounting holes with the pre-drilled holes in the floor.

7 Secure the main rack to the site floor with the locally procured mounting hardware.

8 If required, connect adjacent cabinets to each other using ganging hardware.

4.1.2 Auxiliary Equipment

Auxiliary equipment for the main rack includes:

- Surge arrestors
- Grounding
- Cable supports

4.1.2.1 Surge Arrestors

T1/E1

The T1/E1 surge arrestor must be adequately grounded. The surge arrestor usually mounts near the demarcation (demarc) point. The cable connecting the surge arrestor to the Telco SmartJack should be locally procured, or should be provided with the surge arrestor.

AC power (optional)

An RFN-approved surge arrestor must be installed adjacent to the AC power panel. Very short wire lengths between the arrestor and the power panel are required for proper operation of equipment.

4.1.2.2 Grounding

Within the site, ground the main rack with a single dedicated connection between the main rack and the master ground bar. The connecting wire must be a #2 AWG green-insulated copper wire.

Use appropriate lugs (and split ring lock washers when possible) with an anti-oxidant grease applied for interior grounding connections and exterior secondary grounding connections. If lock washers are used, they should be placed between the nut and the lug to ensure the mechanical integrity of the connection. The washer must not be secured between the lug and the surface to which it is connected. Painted connections must be scraped clean before applying the anti-oxidant grease and lug.

The main rack (ground bus) must be connected to the site ground using a single dedicated ground wire.

Warning!

Never use a bare or damaged wire for the connection of chassis ground or for the electrical wiring to prevent damage to equipment or potential injury to personnel.

4.1.2.3 Cable Supports

All installations requiring cable trays shall be the responsibility of the customer. Cable tray requirements vary from site to site and are not specific to the RadioFrame System. All cable tray installations shall receive permits from and be inspected by the local municipality governing tenant improvements, including mechanical and electrical inspections. Site plans, procurement, installation, grounding/bonding, and inspecting of the cable tray shall be the responsibility of the customer.

4.2 Remote ACUs

To install a remote ACU, first mount the unit then connect the ACU to the BCU and each associated RFU. Repeat the following two procedures for each remote ACU.

4.2.1 Mount the remote ACU

Mount each remote Airlink Chassis Unit (ACU) as follows:

1 Find these items in the ACU shipping container: one ACU, four mounting screws, and one 120VAC power cord.

2 Mount the ACU only in an EIA-standard compliant (19”) rack using all 4 screws provided. Refer to the site documentation for the exact location of the ACU. For safe operation, follow these guidelines:

- Do not mount the ACU in any orientation other than that specified in the following illustration.
- Mount the ACU so that both the front and the back are accessible.
- If the mounting holes do not line up, adjust the ACU up or down until the mounting holes line up.

Caution

Do not block the air vents on the sides or rear of the ACU.

3 Plug the ACU into an approved power source with the provided power cord.

Caution

The power supply cord is used as the main disconnect device; ensure that the socket-outlet is located/installed near the equipment and is easily accessible.

4 Verify that the ACU is receiving power and that all cards installed in the ACU, front and back, are operational.

Each card installed in the front and back of the ACU has two LEDs: Power and Status. All LEDs should light green, except for the Status LED, which remains red until the T1/E1 line is connected.

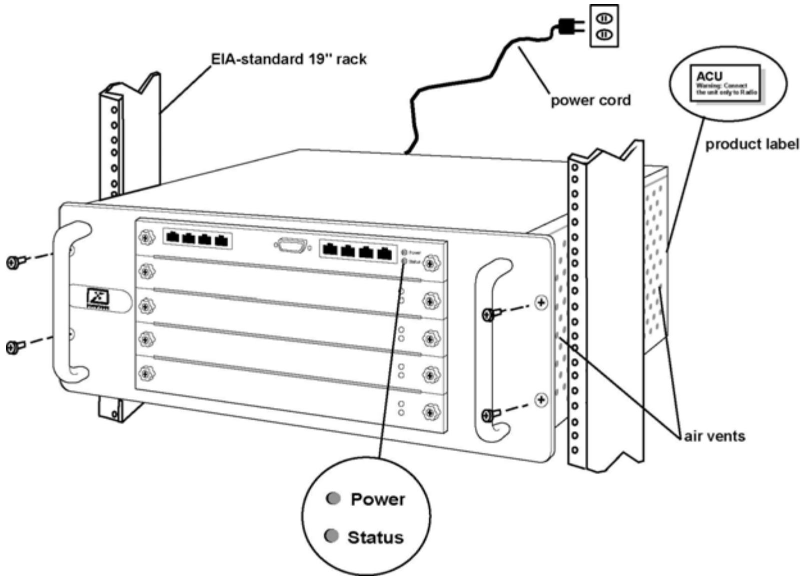


Figure 13 Mount the ACU only in an EIA-standard compliant 19” rack.

4.2.2 Connect the ACU to the BCU and the RFUs

1 Connect Port 2 on the front of the ACU to the specified port (1 through 8) on the back of the BCU using an RJ45-to-RJ45 CAT-5 cable (see the following illustration).

2 Verify that the ACU is connected to the BCU.

The Link and Activity LEDs on Port 2 should both light green, and the Activity LED should blink rapidly indicating that the connection to the BCU is operating.

3 Connect the RJ45-to-RJ45 CAT-5 cable for each RFU to the specified port (1 through 8) on the back of the ACU.

The Link and Activity LEDs on the ports will remain unlit until each RFU has been installed.

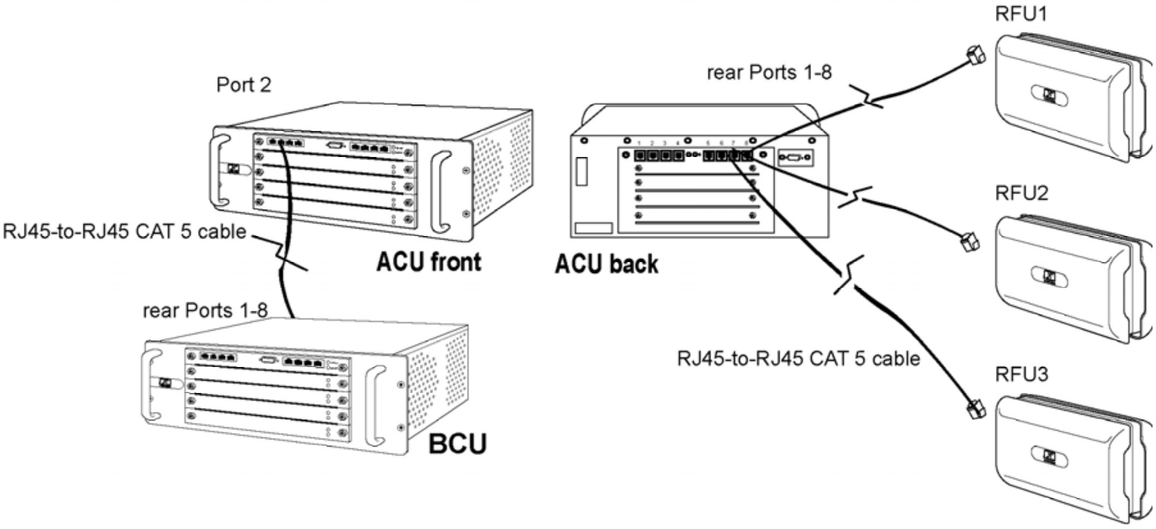


Figure 14 Connect Port 2 on the front of the ACU to the specified port (1-8) on the back of the BCU, and connect RFUs to ports 1-8 on the back of the ACU.

4.3 RFU

This section describes the methods used to mount an RFU, including wall and ceiling mounts. The RFU is shipped with mounting screws and anchors, two mounting templates (wall and ceiling), and one ceiling bracket (optional).

First, mount an RFU, then connect it to the ACU and verify that the RFU is receiving power from the ACU. Next, insert the RadioBlades into the RFU in the configuration specified in the site documentation, and replace the front cover on the RFU.

4.3.1 Mounting and Anchoring

The RFU is to be installed on a wall or on or above the ceiling. The RFU is to be fix-mounted on indoor permanent structures providing a separation distance of at least 8 inches (20 cm) from all persons during normal operation and 10 feet (3 meters) from other RFU mounted assemblies.

The RadioFrame Unit (RFU) is not intended for mounting to drop ceilings. Mounting this unit to a drop ceiling voids any warranty, expressed, implied, or otherwise. Mounting this unit to a drop ceiling voids any regulatory agency approvals, including, but not limited to, Underwriters Laboratories (UL), Canadian Standards Association (CSA), and the European Community (CE).

NOTE: Mounting the RFU directly to a drop ceiling is expressly forbidden by the National Electric Code (NEC), National Fire Protection Association (NFPA), and the Uniform Building Code (UBC). RadioFrame Networks is not liable for any direct, indirect, special, incidental, or consequential damages arising out of mounting this unit in any fashion not recommended and approved by RadioFrame Networks. This includes, but is not limited to, damage to, or loss of, equipment, loss of data, or loss of profit, even if RadioFrame Networks was advised of the possibility of such damages

4.3.1.1 Wall Mount

1. Place the 11” x 17” drawing template (P/N 981-1020-00) on the wall where the RadioFrame Unit is to be mounted.
2. Mark the two locations indicated on the template.
3. Screw the two supplied anchors into the locations as shown in the following diagram.
4. Screw the two supplied screws into the anchors, leaving approximately 1/4” of each screw exposed.
5. Hang the RFU on the anchors and fully tighten both screws.

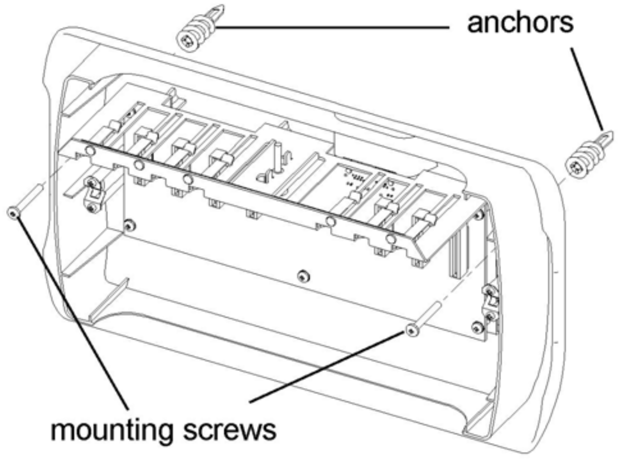


Figure 15 A wall mount requires two screws to anchor the RFU.

4.3.1.2 Ceiling Mount

1. Place the 8.5” x 11” drawing template (P/N 981-1010-00) on the ceiling where the RFU is to be mounted.
2. Mark the four locations indicated on the template.
3. Drill four holes with the appropriately sized bit: 3/16” for the provided wood screws, or 9/32” for 1/4” bolts (bolts not provided).

   If using the provided wood screws, ensure that all four screws penetrate wood. Otherwise, use alternative mounting screws or bolts to secure the ceiling bracket.
4. Using four screws or bolts, attach the ceiling bracket to the ceiling as shown in the following diagram.
5. Attach the RFU to the ceiling mount bracket and fully tighten the thumbscrew.

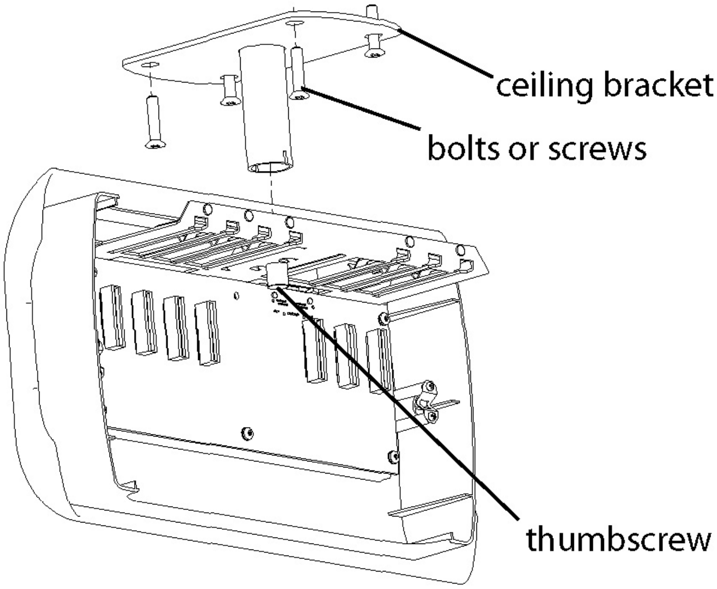


Figure 16 Use the provided bracket when mounting an RFU on the ceiling, ensuring that all bolts or screws penetrate wood.

4.3.2 Connect the RFUs to the ACU

1 Connect the RJ45 port labeled MAIN on the top of the RFU to the ACU using an RJ45-to-RJ45 CAT-5 cable (see the following illustration).

⚠ Caution

Do not remove the protective cover from or use the RFU port labeled AUX. Damage may occur to the RFU, ACU, or both.

2 Verify that the RFU is receiving power and connectivity from the ACU.

The Link and Activity LEDs on the MAIN port should light as green, and the Activity LED should blink rapidly indicating connectivity. If the LEDs do not light, verify that the ACU is powered on.

3 Complete the next procedure “Insert the RadioBlades” before placing the front cover on the RFU.

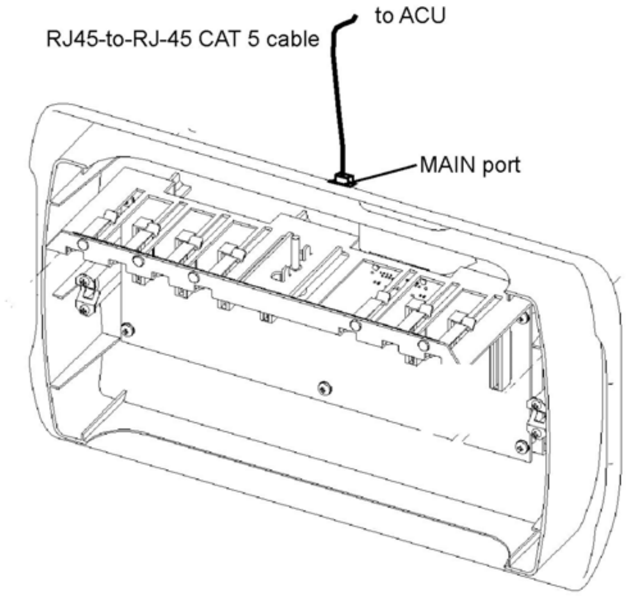


Figure 17 Connect the RFU to the ACU, then ensure that the RFU is receiving power and connectivity from the ACU.

4.3.3 Insert the GSM RadioBlades and iRAPs into the RFU

The GSM RadioBlades and 802.11 iRAPs are shipped several to a box in individually wrapped antistatic packaging. Each box of RadioBlades/RAPs includes a disposable antistatic wrist strap to be used when inserting the RadioBlades/RAPs into the RFU. Refer to the site documentation for the exact slot location of each RadioBlade/iRAP within the RFU.

1. Unwrap 30 cm (12”) of the disposable wrist strap and wrap the adhesive side around your wrist.
2. Unroll the rest of the band and remove the liner from the copper tape.
3. Attach the copper tape to the metal card cage inside the RFU.
4. Un-package the GSM RadioBlades to be inserted in the RFU.
5. Insert the GSM RadioBlades, one at a time, into the specified slots (1 through 7, numbered right to left) in the RFU until the connector on each RadioBlade seats firmly into the back of the RFU (see the following illustration).

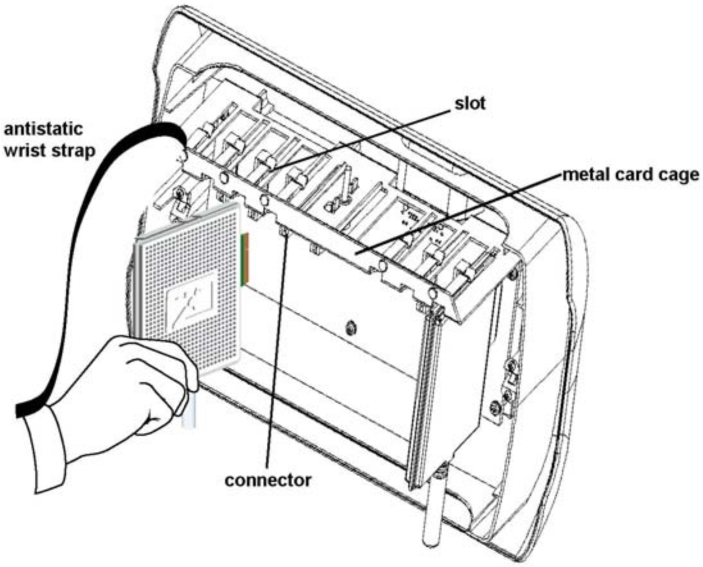


Figure 18 Slide each GSM RadioBlade into the specified slot in the RFU.

6 Insert the 802.11b/g iRAPs, one at a time, into the specified slots in the RFU until the connector on each iRAP seats firmly into the back of the RFU (see the following illustration).

7 Remove the antistatic wrist strap and place the front cover on the RFU.

4.4 Interconnecting Cabling

4.4.1 T1/E1

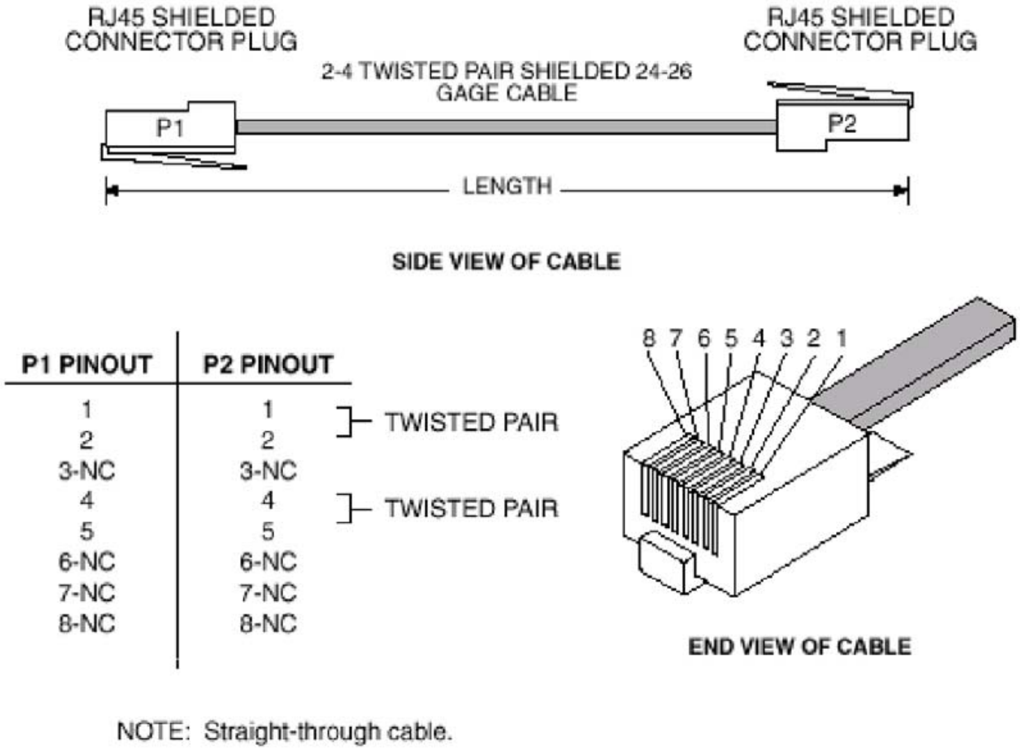
The Telco interface should have been installed according to the Pre-installation chapter.

NOTE: The equipment can be installed and tested without the Telco T1/E1 present. The T1/E1 must be connected for proper operation of the site.

NOTE: Some modular cables have a ridge along one side of the cable for purposes of alignment with the connector.

NOTE: The SmartJack is capable of passing -48V Telco power through to the site controller. For operation, GSM does not require this power. If -48V is present on the network connection to the site controller, the SmartJack is incorrectly configured. Contact the service provider immediately to correct this situation. The SmartJack switch should be set so that -48V power does not pass through to the site controller.

If this cable is locally manufactured, crimp the 8-pin connectors as shown in the following illustration. The wires should be routed straight through. Make sure that the conductor color is the same at both ends for each conductor of the cable.


RJ45 SHIELDED CONNECTOR PLUG
RJ45 SHIELDED CONNECTOR PLUG
2-4 TWISTED PAIR SHIELDED 24-26 GAGE CABLE
P1
P2
LENGTH
SIDE VIEW OF CABLE
TWISTED PAIR
TWISTED PAIR
8 7 6 5 4 3 2 1
END VIEW OF CABLE

P1 PINOUT	P2 PINOUT
1	1
2	2
3-NC	3-NC
4	4
5	5
6-NC	6-NC
7-NC	7-NC
8-NC	8-NC

NOTE: Straight-through cable.

Figure 19 T1/E1 interface cable configuration

4.4.2 RFS to Customer LAN

The RFS is connected to the customer LAN only after all other connections have been made and all other system functionality has been tested and is performing accurately. The RFS is connected to the Customer LAN using an RJ45-to-RJ45 CAT-5 cable. For more information, refer to Chapter 6 “Connecting the RFS to the Customer LAN”.

5 Final Checkout

The procedures in this chapter describe how to conduct commissioning and system test procedures for the GSM/802.11 RadioFrame System. Following the successful completion of procedures described in this chapter, the RFS can be connected to the customer LAN as described in Chapter 6 “Connecting the RFS to the Customer LAN”.

The procedures in this chapter are to be used in conjunction with troubleshooting and repair information provided in Chapter 7 Operations and Maintenance and the RFN document, *Field Guide to the RadioFrame System*. Together, these troubleshooting solutions and commissioning procedures provide the necessary information to isolate failures to a Field Replaceable Unit (FRU). This minimizes system downtime by quickly returning the site to normal operation.

This chapter’s procedures check system functions and help isolate failures down to the FRU level. If a failure cannot be isolated after performing these tests, refer to Chapter 1 “Repair and Technical Support” for technical assistance information.

5.1 Start System Manager

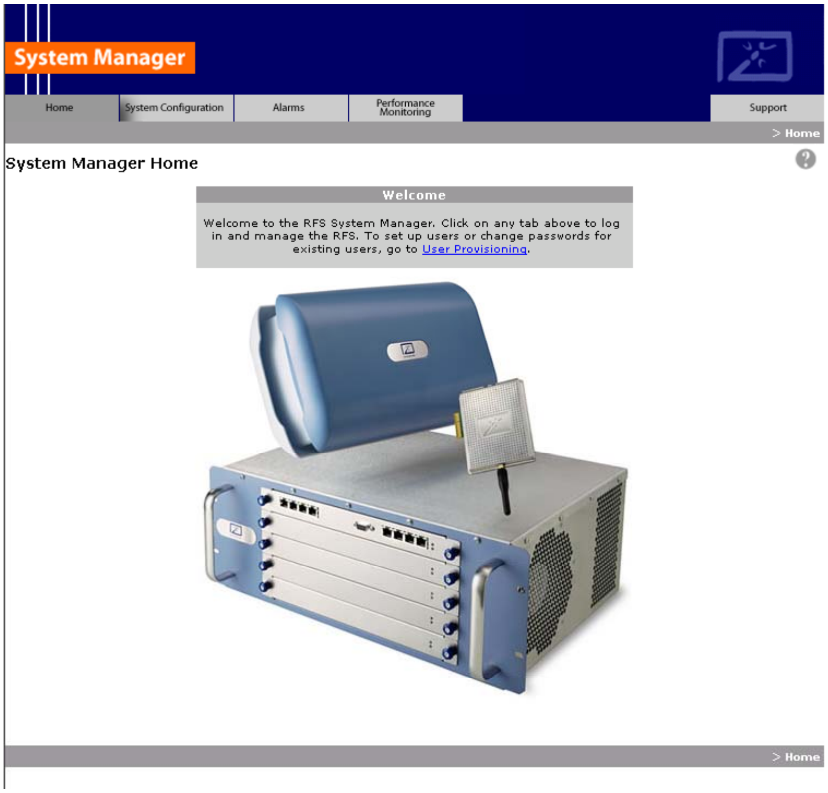
After installation of all RadioFrame Networks equipment, including verification that each unit is receiving power, start System Manager to complete the installation of the RadioFrame System. System Manager automatically downloads information about each component in the RFS, including assigned IP addresses, sector information, port connections, and component status, as well as specifying default information that can be changed, or ‘configured’.

1 Using a 9-pin serial cable, connect a laptop computer to the RS232 port on the front of the BCU.

2 Start the browser on the laptop, and enter the provided URL to start System Manager.

The System Manager Home page appears (see the following illustration). System Manager contains five tabs you select from to set up and monitor the RadioFrame System:

- *Home*—displays a welcome banner and a link for setting up users and changing the RFS password.
- *System Configuration*—displays the configuration of each RFS component, and depicts the location and status of each component, including the BCU, ACUs, and RFUs.
- *Alarms*—displays alarm information for each component of the RFS.
- *Performance Monitoring*—displays real-time performance information about the RFS.
- *Support*—displays support information, including online help.



System Manager Home

Welcome

Welcome to the RFS System Manager. Click on any tab above to log in and manage the RFS. To set up users or change passwords for existing users, go to User Provisioning.

3 To log in, select any tab except the Home tab.

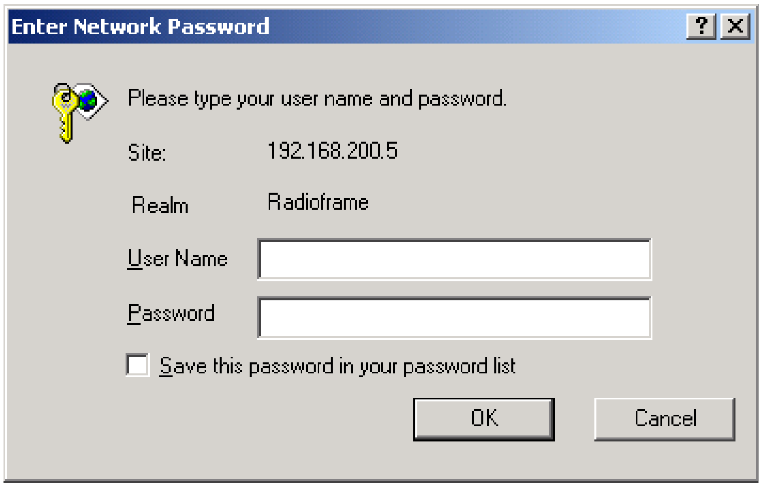
The login page appears (see the following illustration).

4 For **User Name**, type your RFS user name.

5 For **Password**, type your RFS password.

6 To save the password so you don't have to retype it the next time you log in, check '**Save this password in your password list**' checkbox.

7 Select **OK**.



Please type your user name and password.

Site: 192.168.200.5

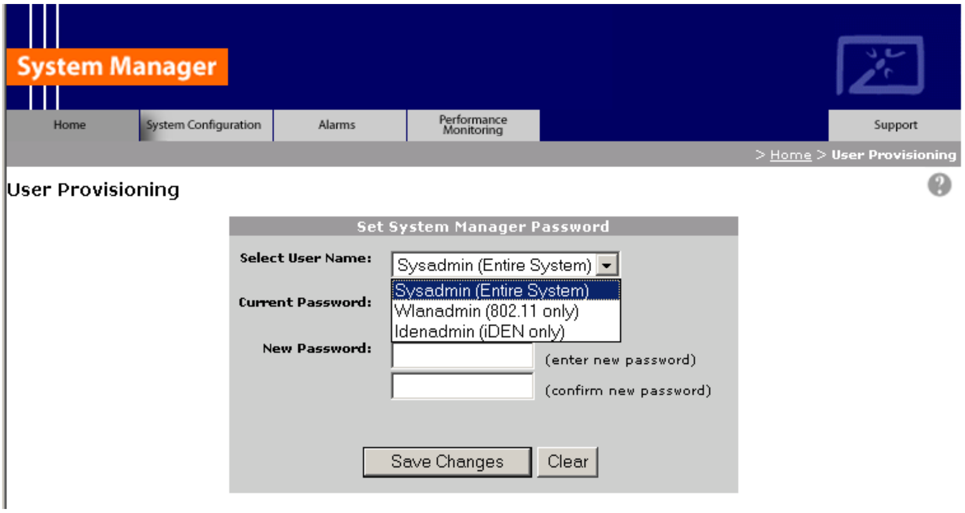
Realm Radioframe

User Name

Password

□ Save this password in your password list

NOTE: To change the password, select the User Provisioning link on the Home page, and then select the User Name from the drop down menu. Type the current password for the selected user name, and then type the new password and confirm it. Select Save Changes.



Select User Name: Sysadmin (Entire System)

Current Password:

New Password:

5.1.1 Navigating the System Configuration

The System Configuration displays icons representing each component included in the RFS starting with the BCU (see the following illustration). In the following example, ACU 192.168.200.10 is connected to the BCU rear port 1. Generally, the ACU connected to BCU rear port 1 is the ACU located in the main rack, and the remaining are remote ACUs. Configuration information for the BCU is displayed on the left side of the page, including the device name and IP address.

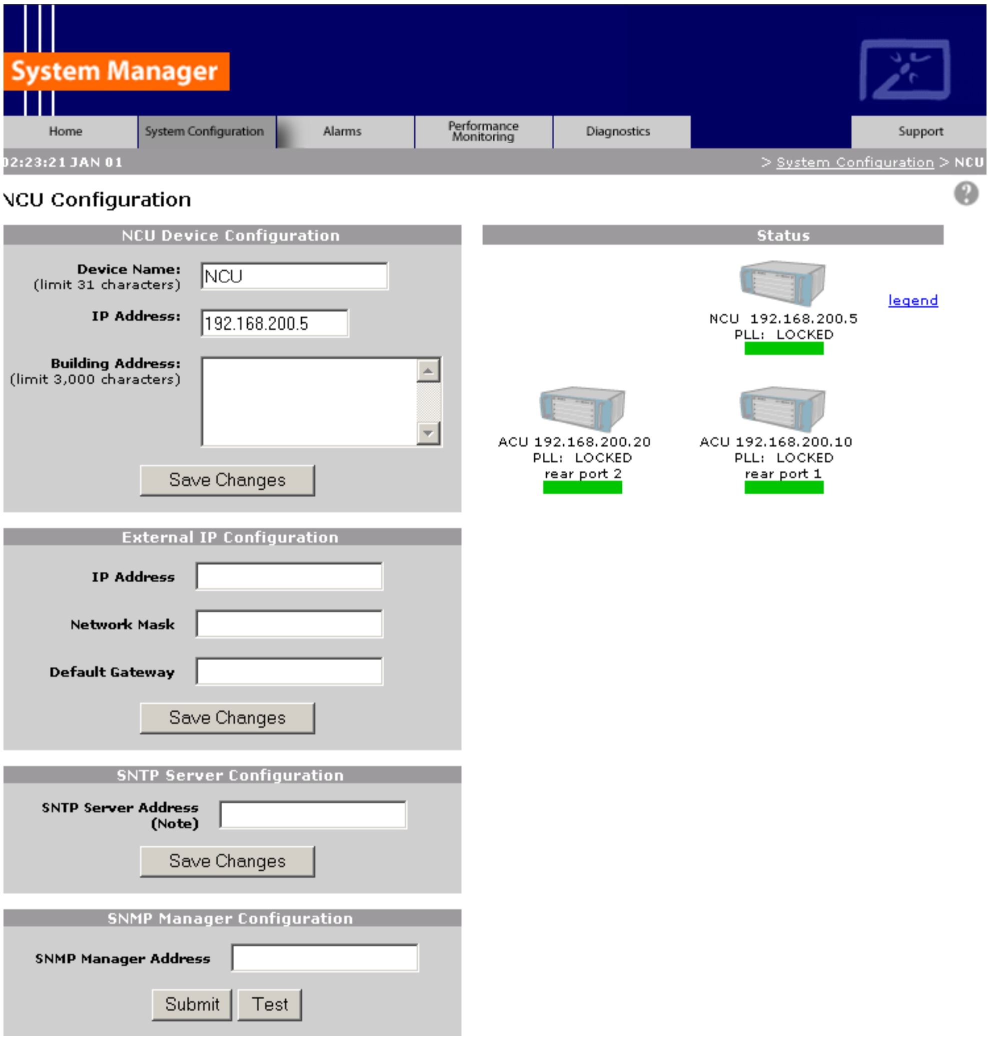
1 To view configuration information for an ACU, select its icon.

A page similar to the BCU page appears displaying configuration information for the selected ACU and icons for each RFU connected to the ACU. In the same way you can view the status of each GSM RadioBlade installed in every RFU in the RFS by selecting an RFU icon.

2 To return to a previous page, select the component pathname shown at the top of the tab (System Configuration>BCU>ACU…).

3 To return to the BCU, select the System Configuration tab at any time.

Final Checkout



02:23:21 JAN 01

NCU Configuration

NCU Device Configuration

Device Name: (limit 31 characters) NCU

IP Address: 192.168.200.5

Building Address: (limit 3,000 characters)

Status

NCU 192.168.200.5
PLL: LOCKED

ACU 192.168.200.20
PLL: LOCKED
rear port 2

ACU 192.168.200.10
PLL: LOCKED
rear port 1

External IP Configuration

IP Address

Network Mask

Default Gateway

SNTP Server Configuration

SNTP Server Address (Note)

SNMP Manager Configuration

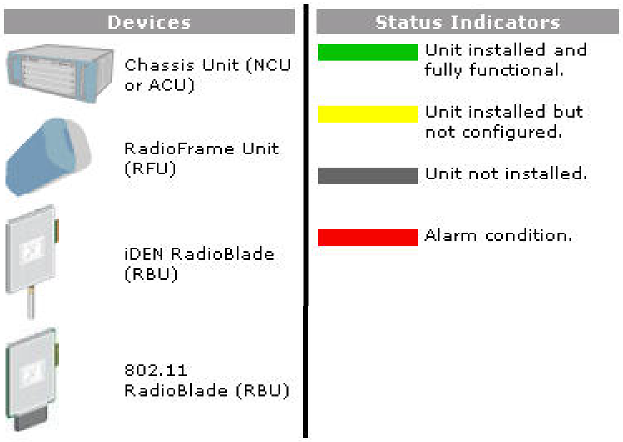
SNMP Manager Address

5.1.2 Component Status

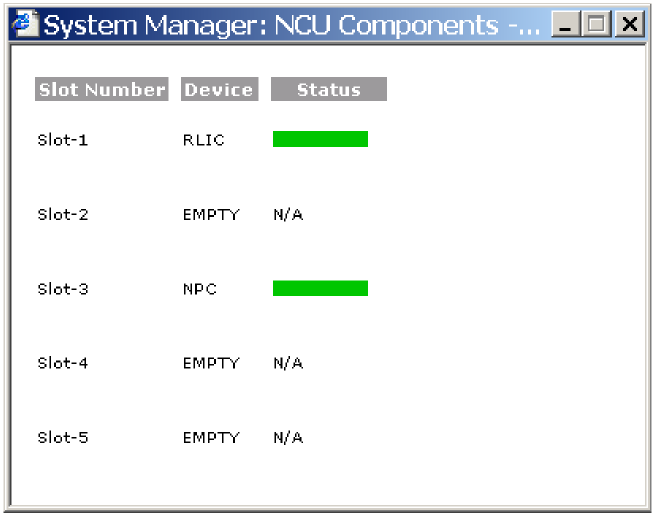
The colored bar displayed under each component icon on the configuration pages shows the status of the component:

- Green—Unit installed and fully functional.
- Yellow—Unit installed but not configured.
- Gray—Unit not installed.
- Red—Alarm condition.

To display the legend of status conditions, select the **legend** link at the top right corner of the configuration page.



To view the status of chassis unit components (NPCs, APCs, CRICs), select the icon (for the ACU, you must first navigate to the ACU Configuration page, then select the ACU icon). The BCU/ACU Components page appears,

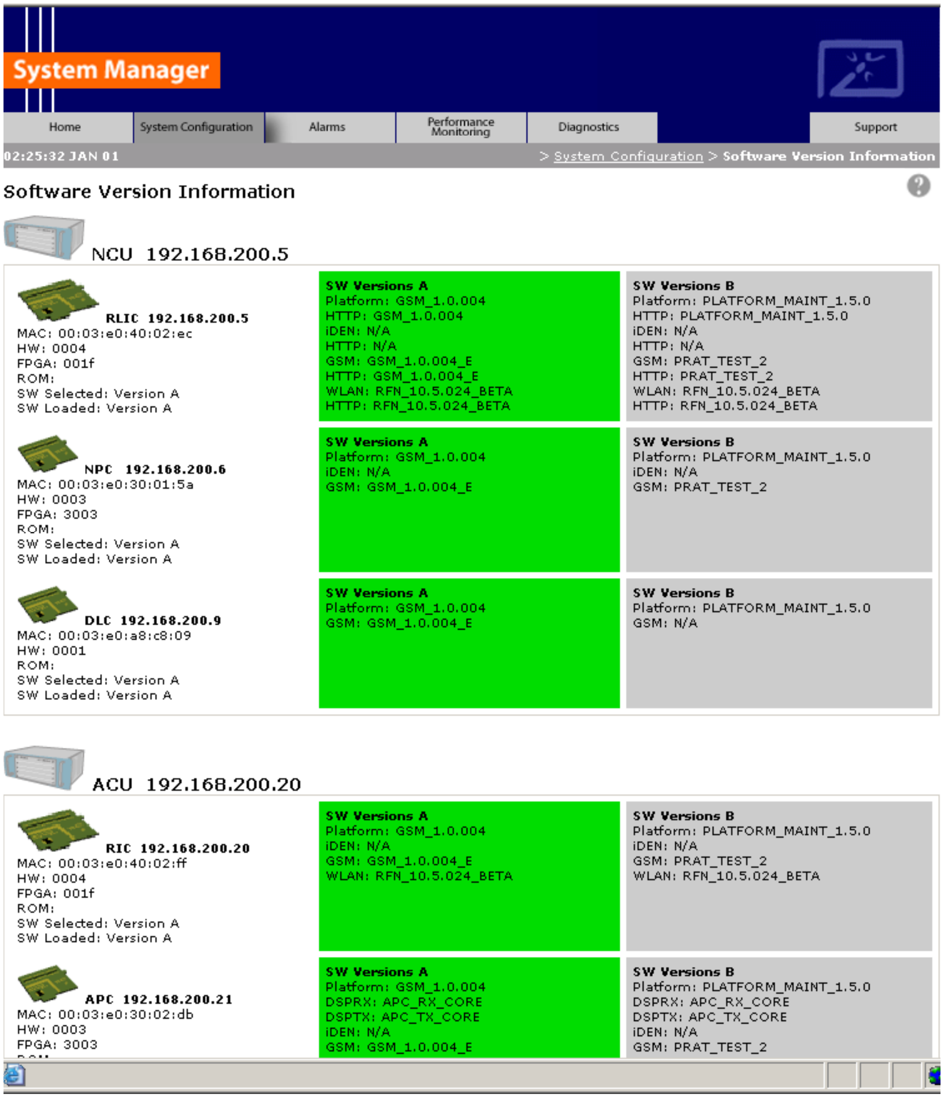


Slot Number	Device	Status
Slot-1	RLIC	🟩
Slot-2	EMPTY	N/A
Slot-3	NPC	🟩
Slot-4	EMPTY	N/A
Slot-5	EMPTY	N/A

5.1.3 Software Version Information

Select the Software Version Information link on the BCU Configuration page to display the software versions for all boards in the in the RadioFrame System. For each board, this page displays the following:

- Hardware version
- FPGA version
- ROM version
- Selected software version (SW Version A or Software Version B)
- Loaded software version (SW Version A or Software Version B)



02:25:32 JAN 01 > System Configuration > Software Version Information

Software Version Information

NCU 192.168.200.5

RLIC 192.168.200.5 MAC: 00:03:e0:40:02:ec HW: 0004 FPGA: 001f ROM: SW Selected: Version A SW Loaded: Version A	**SW Versions A** Platform: GSM_1.0.004 HTTP: GSM_1.0.004 iDEN: N/A HTTP: N/A GSM: GSM_1.0.004_E HTTP: GSM_1.0.004_E WLAN: RFN_10.5.024_BETA HTTP: RFN_10.5.024_BETA	**SW Versions B** Platform: PLATFORM_MAINT_1.5.0 HTTP: PLATFORM_MAINT_1.5.0 iDEN: N/A HTTP: N/A GSM: PRAT_TEST_2 HTTP: PRAT_TEST_2 WLAN: RFN_10.5.024_BETA HTTP: RFN_10.5.024_BETA
NPC 192.168.200.6 MAC: 00:03:e0:30:01:5a HW: 0003 FPGA: 3003 ROM: SW Selected: Version A SW Loaded: Version A	**SW Versions A** Platform: GSM_1.0.004 iDEN: N/A GSM: GSM_1.0.004_E	**SW Versions B** Platform: PLATFORM_MAINT_1.5.0 iDEN: N/A GSM: PRAT_TEST_2
DLC 192.168.200.9 MAC: 00:03:e0:a8:c8:09 HW: 0001 ROM: SW Selected: Version A SW Loaded: Version A	**SW Versions A** Platform: GSM_1.0.004 GSM: GSM_1.0.004_E	**SW Versions B** Platform: PLATFORM_MAINT_1.5.0 GSM: N/A

ACU 192.168.200.20

RIC 192.168.200.20 MAC: 00:03:e0:40:02:ff HW: 0004 FPGA: 001f ROM: SW Selected: Version A SW Loaded: Version A	**SW Versions A** Platform: GSM_1.0.004 iDEN: N/A GSM: GSM_1.0.004_E WLAN: RFN_10.5.024_BETA	**SW Versions B** Platform: PLATFORM_MAINT_1.5.0 iDEN: N/A GSM: PRAT_TEST_2 WLAN: RFN_10.5.024_BETA
APC 192.168.200.21 MAC: 00:03:e0:30:02:db HW: 0003 FPGA: 3003	**SW Versions A** Platform: GSM_1.0.004 DSPRX: APC_RX_CORE DSPTX: APC_TX_CORE iDEN: N/A GSM: GSM_1.0.004_E	**SW Versions B** Platform: PLATFORM_MAINT_1.5.0 DSPRX: APC_RX_CORE DSPTX: APC_TX_CORE iDEN: N/A GSM: PRAT_TEST_2

5.1.4 System Manager Support

Select the Support tab to display resources to help you use System Manager:

- **System Manager Online Help**
  The Help button in the top right corner of each page opens a Help window that briefly describes the features of the current System Manager page.
- **Support on the web**
  Get current product documentation, release notes, FAQ, and other product documentation online at http://radioframenetworks.com/support/. (You'll need your customer **username** and **password** to log in.)
- **Contact RadioFrame Networks Technical Assistance Center**

Telephone	(800) 328-0847
E-mail	support@radioframenetworks.com

5.2 Configure the System Components

To configure each system component, specify a device name, adding building/site location information for each component. Anytime an RFU port connection is moved or changed, or when a BPC or APC is moved to another slot within the same chassis unit (BCU and ACU, respectively), System Manger incorporates the new information. For other RFS component changes, RFN recommends validating that the port change is reflected in System Manager. When new releases of RadioFrame System software are provided, download the new release as described in section 7.1 Upgrading System Software.

NOTE: During configuration, verify that the following information displayed in System Manager matches the Equipment Inventory. If any changes are made in System Manager, those changes must also be shown on the Equipment Inventory or site as-built documentation.

- Physical location
- IP addresses
- Port connections
- Sector locations

5.2.1 Configuring the BCU

The BCU System Configuration page displays the **BCU Device Configuration**, including the Device Name, IP Address, and Building Address for the BCU—you can change this information at any time. This page also displays the **External IP Configuration**, the information that systems outside the RFS use to recognize the RFS, the **SNTP Server Configuration**, and **Other Configuration Options**.

1 For **Device Name**, enter up to 31 alphanumeric characters to uniquely identify the BCU.

2 The **IP Address** is assigned during the installation of the RFS. You don't need to change the value of this internal address.

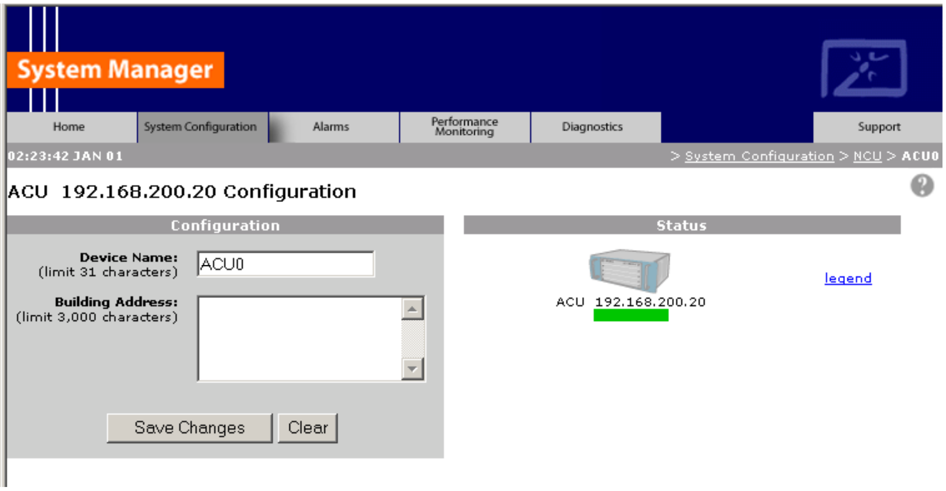
3 For **Building Address**, enter up to 3,000 alphanumeric characters specifying the location of the BCU.
You can describe the street address, mailing address, building, and other site information, as well as the building floor, Telco closet, and rack to indicate the location of the unit.

4 Select **Save Changes**.

5.2.2 Configuring the ACUs

Configure each ACU as you would the BCU. For each ACU, the System Configuration page shows the RFUs connected to the ACU (by port) and which ACU ports are dedicated to which sectors in the GSM installation.

1 Navigate to the page of the ACU you want to configure.



ACU 192.168.200.20 Configuration

Device Name: (limit 31 characters) ACU0

Building Address: (limit 3,000 characters)

2 For **Device Name**, enter up to 60 alphanumeric characters to uniquely identify the ACU.

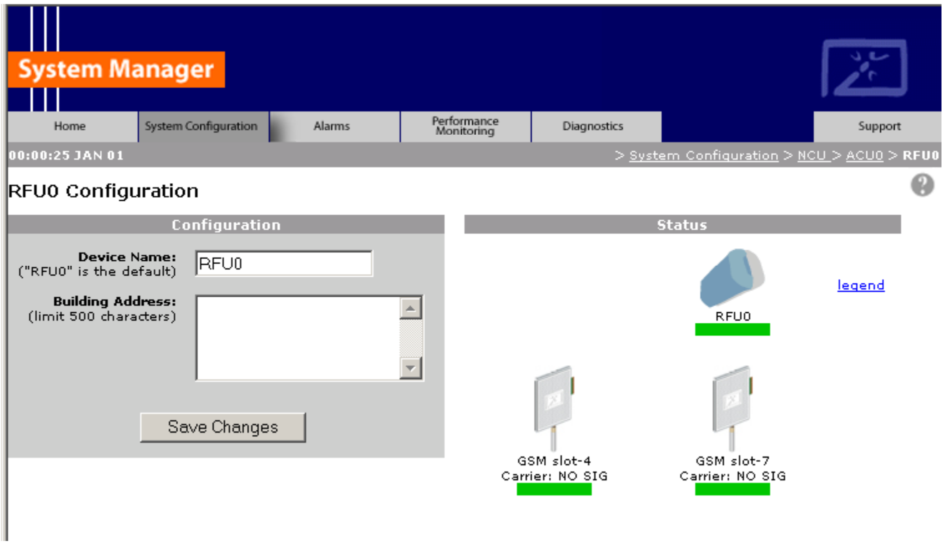
3 For **Building Address**, enter up to 3,000 alphanumeric characters specifying the location of the ACU.
You can describe the street address, mailing address, building, and other site information, as well as the building floor, Telco closet, and rack to indicate the location of the ACU.

4 Select **Save Changes** or **Clear** to start over.

5.2.3 Configuring the RFUs

Configure an RFU as you would the BCU or ACU, by entering a device name and site address information. For each RFU, the configuration page shows the GSM RadioBlades and iRAPs inserted into the RFU by slot.

1 Select the icon of the RFU you want to configure.



Device Name: ("RFU0" is the default) RFU0

Building Address: (limit 500 characters)

2 For **Device Name**, enter up to 60 alphanumeric characters to uniquely identify the RFU.
Use names that are meaningful to the installation.

3 For **Building Address**, enter up to 3,000 alphanumeric characters specifying the location of the BCU.
You can describe the street address, mailing address, building, and other site information, as well as the building floor to indicate the location of the unit.

4 Select **Save Changes**.

5.3 Configure the RFS GSM Services

To set up the RFS for GSM services to match the in-building site planning requirements, complete the following procedure.

1 Select GSM Provisioning link under Other Configuration Options on the BCU Configuration page.

2 For **BTS ID**, enter a value that uniquely identifies the BTS.

3 For **DLC port number** represents the port number on the DLC that the customer's BSC is connected to.

4 For **Number of TRX**, enter the total number of TRXs that will be used in the RFS.

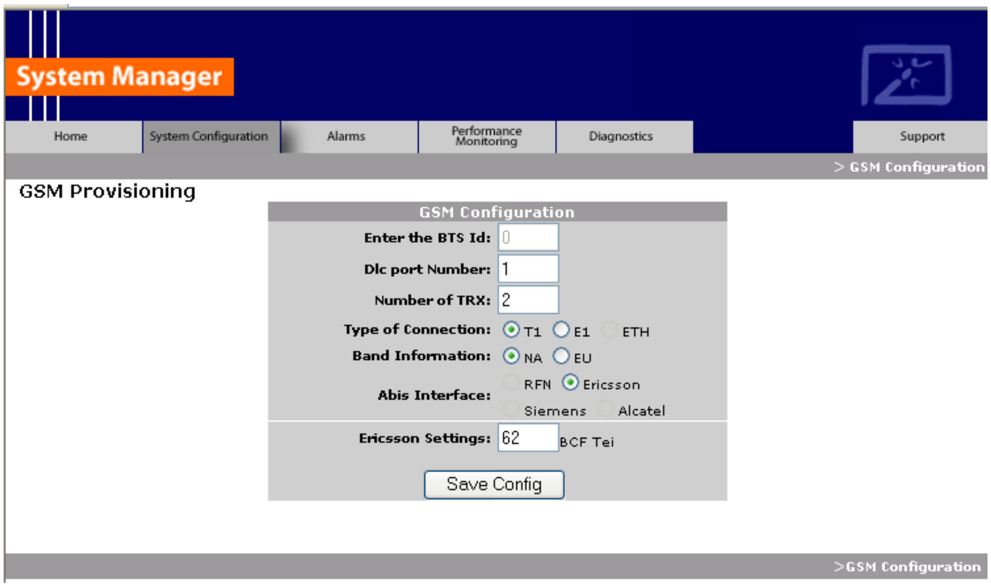
5 For **Type of Connection**, select T1 or E1.

6 For **Band Information**, select the appropriate band—NA for North America or EU for Europe.

7 For **ABIS Interface**, select the ABIS that matches the customer's BSC ABIS type.

8 For **Ericsson Settings**, enter the Ericsson BCF Tei.

9 Select the **Save Config** button to save your changes.



GSM Provisioning

GSM Configuration

Enter the BTS Id: 0

Dlc port Number: 1

Number of TRX: 2

Type of Connection: ● T1 ○ E1 ○ ETH

Band Information: ● NA ○ EU

Abis Interface: ○ RFN ● Ericsson ○ Siemens ○ Alcatel

Ericsson Settings: 62 BCF Tei

5.4 Coverage Validation

After configuring all RFS components, use measurement software, a laptop and a GSM handset to check for regions of low signal strength or low signal quality (RXQUAL).

5.4.1 Detailed Building Plans—RF Modeling

Testing by RFN has shown that simple Linear Attenuation Models (LAM) as discussed in COST 231, Chapter 4 section 4.7 "Indoor Propagation Models" work well when used on a floor-by-floor basis. An attenuation coefficient of 0.62dB/m is recommended for dense, single-floor propagation, but this can double if concrete walls are present.

5.4.2 Measurement-based Estimate

A battery-powered test transmitter can be moved between each proposed RFU location and a handheld signal strength meter used to monitor RSSI. This method is useful when RF penetration is desired through suspect walls or where wall construction data is lacking. Generally, this method provides good agreement when used to identify regions of poor coverage rather than to establish sufficient coverage zones. This is because it is usually inconvenient to duplicate an RFUs' position during initial coverage surveys.

5.4.3 Floor Plan Estimate

Oftentimes, only simple floor plans are available for the building in which the RFUs are to be installed. Without specifics about the building construction, such as interior wall, floor and ceiling construction, propagation models are of limited value. A measurement-based approach (discussed earlier) works well, but for simple buildings, installing RFUs at the candidate locations and then testing the results will likely be adequate. If regions of poor coverage are found, additional RFUs may be added.

5.5 Site Acceptance Guidelines

5.5.1 Site As-Built Documentation

As-built documentation consists of the original site development documentation with post-installation information. On the job, installers use site development documentation for reference, to make notes, and to document completion of each step of the installation.

Conduct an onsite walk through to verify that the following Site Development Punch List items have been properly installed. This inspection ensures that the site installation meets quality standards.

- Grounding
  - buss bar OK (optional)
  - BCU/ACU rack(s)
- T1/E1 Information, Primary and Secondary
  - T1/E1 circuit ID#
  - T1/E1 surge arrestor installed/grounded

- T1/E1 repeater shelf / cfl cabinet location
- T1/E1 level at extended demarc (RJ48 x jack)

- Summary
  - log book at site with recent entry
  - outstanding issues/punch list items for site
  - defective equipment found/replaced

5.5.2 Site As-Built Acceptance Test Procedures

Complete the test procedures described in this section to record the site as built.

5.5.2.1 Grounding

Record the following grounding information. For any unacceptable item, take corrective action and record what occurred, or record the item for the next site visit.

	Yes	No
Buss Bar O.K. (optional)		
BCU/ACU rack(s)		

5.5.2.2 T1/E1 Line

Record the following information for the T1/E1line.

T1/E1 circuit ID #	Primary		Secondary	
T1/E1 surge arrestor installed/grounded	Yes		No	
T1/E1 repeater shelf/cfl cabinet location	Inside		Outside	
T1/E1 level at extended demarc (RJ48x jack)	+/- dbsx		Voltage	

5.5.3 RadioFrame System As-Built Documentation

As-built documentation for the RadioFrame Networks equipment includes the following:

- Equipment inventory
- Cabling pathways
- Floor Plan with site configuration and component locations

5.5.3.1 Equipment Inventory

The final Equipment Inventory should show the following information for the RFS components installed:

- Part number
- Serial number

- Rack position (BCUs and ACUs only)
- Card position (APCs and BPCs only)
- RFU location (including floor and sector)
- GSM RadioBlade and iRAP slot positions in RFU
- MAC Address
- IP Address
- Channel (RAPs only)
- Port connections between RFS components

5.5.3.2 Cabling Pathways

A schematic showing the route of each cable run at the site. For each cable run, list the following:

- Cable length
- Cable type
- Connector types (both ends)
- Cable labeling completed per specs
- Port Connections
- Continuity test results
- Distance test results

5.5.3.3 Floor Plan/Site Drawing

Use a floor plan or site drawing to denote the location of the following on each floor of the building:

- Main rack
- Remote ACUs, including power source
- RFUs

5.5.4 RadioFrame System Acceptance Test

During installation, each component of the RFS is verified for power and connectivity. Assuming that each component (BCU, ACU, and RFU) has been properly installed and is receiving power, double check that all Power, Status, Link and Activity LEDs throughout the system are lit and are green. For any other condition on any system component or connection, refer to section 7.3 Corrective Maintenance for troubleshooting procedures.

5.6 RadioFrame System Functionality Test

RFS System Functionality Testing is to be co-developed with the customer.

6 Connecting the RFS to the Customer LAN

Once the RadioFrame System has been installed, commissioned, and all GSM Acceptance Test and System Functionality procedures have been successfully completed, the RFS can be connected to the Customer LAN. Once the LAN has been physically connected, the RFS must be globally configured to support the LAN. Individual iRAPs can also be configured, overriding certain global configuration options.

6.1 Connect the BCU to the Customer LAN

In an 802.11b/g installation, iRAPs are installed in each RFU supporting the WLAN. Once the RFS has been physically connected to the LAN, use the System Manager to configure the RFS to support the WLAN.

1 Connect the specified port on the front of the BCU (2 through 7) to the customer's local area network using an RJ45-to-RJ45 CAT-5 cable.

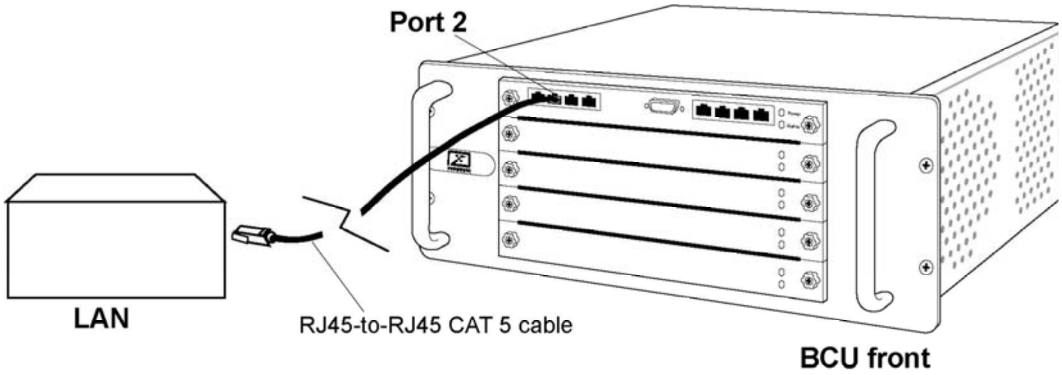


Figure 20 Connect the specified port on the front of the BCU (port 2 through 7) to the customer's LAN.

6.2 802.11 Global Configuration

This section describes how to configure the RFS global (system-wide) 802.11 configuration settings using either MAC address access control or, if your system includes a RADIUS server, using RADIUS security and accounting.

6.2.1 MAC Address Access Control

This section describes how to configure the RFS global, or system-wide, 802.11 configuration settings, including:

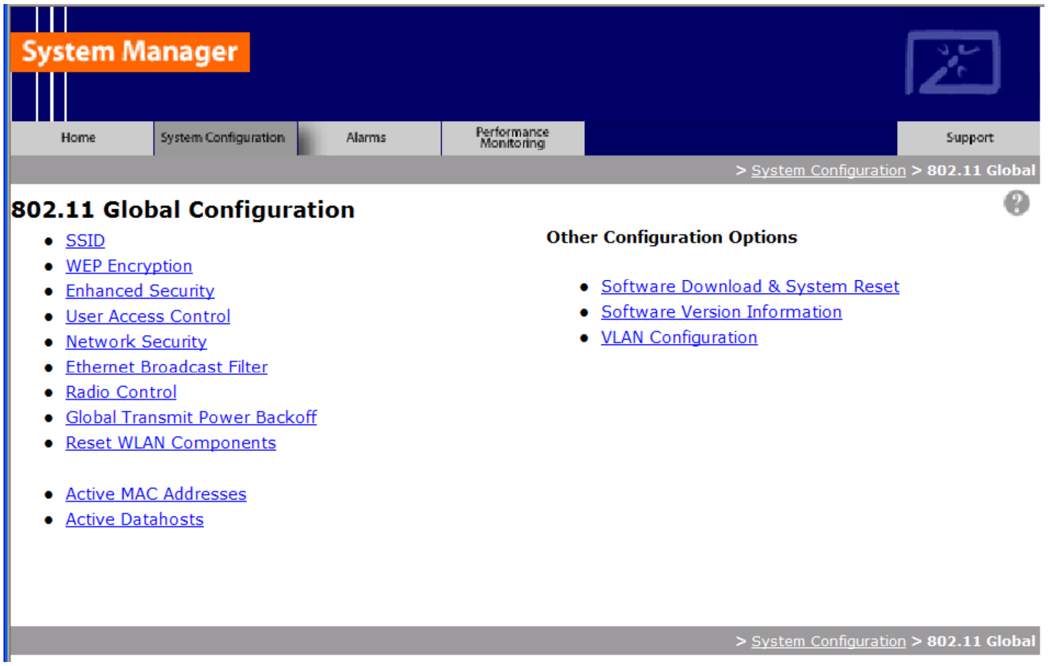
- Service Set identity (mandatory)
- WEP Encryption (optional)
- Enhanced Security (optional)
- User Access Control (optional)
- Add/Remove MAC Addresses (optional)

1 Start System Manager and log in to the RFS.

2 Select the System Configuration tab.

3 Select the 802.11 Global Configuration link under **Other Configure Options**.

The 802.11 Global Configuration page appears.


System Manager
Home
System Configuration
Alarms
Performance Monitoring
Support
> System Configuration > 802.11 Global

802.11 Global Configuration

- SSID
- WEP Encryption
- Enhanced Security
- User Access Control
- Network Security
- Ethernet Broadcast Filter
- Radio Control
- Global Transmit Power Backoff
- Reset WLAN Components

- Active MAC Addresses
- Active Datahosts

Other Configuration Options

- Software Download & System Reset
- Software Version Information
- VLAN Configuration

> System Configuration > 802.11 Global

4 Select the **SSID** link, and enter up to 32 alphanumeric characters to identify the Service Set identity for the RFS, and then select Save Changes to save your changes.

You must enter an SSID in order for the RFS to have 802.11 capabilities. Typically, the SSID reflects the owner of the RFS. For more information, refer to section 6.2.2 Service Set identity (SSID).

5 Select the **WEP Encryption** link, and enter the following information, and then select Save Changes to save your changes.

NOTE: RFN recommends that either WEP or WPA **Encryption** is enabled. If WEP Encryption is used, you must also define the four WEP keys.

To enter a **WEP Key**, first select the radio button next to the text box of the WEP key you want to enter or change. Enter each WEP key in hexadecimal format consisting of five pairs of hex digits. Five pairs of hex digits form a
40-bit binary string, which is the standard length of a WEP key. Only one WEP Key can be selected at a time (the radio button is selected). Then, choose one of the four keys to be used for iRAP Identification (select the radio button of the key you want to use).

For **Shared Key Authentication**, RFN recommends that you leave this option disabled, that is, do not select the option.

Refer to section 6.2.3 WEP Encryption for more information on using WEP Encryption settings.

6 Select the **Enhanced Security** link, select on or off, and then select Save Changes.

NOTE: RFN recommends that you select “On” to prevent iRAPs from broadcasting their SSIDs.

For more information, refer to section 6.2.4 Enhanced Security for more information on using this setting.

7 Select the **User Access Control** link, choose **Expand All**, and set the following information.

For **User Access Control**, RFN recommends that you select “On” to control which devices will have access to the customer LAN via the RFS. For more information, refer to section 6.2.5 User Access Control for more information on using this setting.

For **Add MAC Address**, enter the MAC address of each device that will be authorized to the use the customer LAN. You can enter MAC addresses one at a time, or copy them from a database or other file (**Add MAC Addresses from file**). You can also remove the entire list of MAC addresses (**Remove All MAC Addresses**), or save the list of MAC addresses to a file (**Save MAC Addresses to File**). For more information, refer to section 6.2.6 Add/Remove MAC Addresses for more information on using these options.

6.2.2 Service Set identity (SSID)

The only mandatory RFS 802.11b/g configuration setting is the Service Set identity (SSID). The SSID must be configured in all installations where 802.11b/g integrated RadioFrame Access Points are installed. If the SSID is not configured, the 802.11b/g capability will not be available.

The SSID is necessary because, unlike wired LANs, a device that is part of an 802.11 LAN may be within radio range of multiple “groups” of 802.11 stations. In order to isolate stations in one group from stations in another group, the SSID was created. It is an 802.11-only construct, which does not exist for any other type of LAN. The SSID identifies a collection of 802.11 stations for the purpose of communication as a group.

The SSID is 1 to 32 characters in length. Typically, the SSID reflects the owner of the RFS. This way, users can distinguish their LAN from any other 802.11 LAN that might physically overlap their area.

For example, the SSID “Customer_Marketing” could provide the Marketing department with its own distinct wireless LAN. Other departments, such as “Customer_Operations”, might be in close proximity to the Marketing department. The staff in the two departments would both have 802.11 access to the company LAN, but their access would be provided via different iRAPs, based on which SSID they use.

6.2.3 WEP Encryption

The Wired Equivalent Privacy (WEP) encryption technology is defined in the IEEE 802.11 standard, and is intended to provide the same quality of privacy and access control for an 802.11 LAN as is provided for a wired LAN. That is, a WEP-protected 802.11 should be no easier to infiltrate or eavesdrop than would be on a wired LAN.

Any LAN (wired or wireless) can be made more secure and private by applying additional security measures (such as encryption, centralized strong authentication, firewalling, etc.). The difference between a wired LAN and a wireless LAN, however, is that without including encryption of user traffic and encryption-based access control, a wireless LAN is inherently less secure than a wired LAN, all other things being equal.

6.2.3.1 Encryption (On/Off)

WEP encryption is enabled or disabled by selecting “On” or “Off,” respectively. When “Off” is selected, all other items related to WEP encryption are disabled (WEP Keys and Shared Key Authentication), and need not be configured. When “On” is selected, then the WEP keys must be entered.

6.2.3.2 Shared Key Authentication

When Shared Key Authentication is enabled, or “checked,” the iRAPs will require client devices (such as laptop computers) to prove their authenticity by answering a challenge from the iRAP. This challenge (authentication protocol) can be answered correctly only if the client device “knows” the WEP keys configured into this RFS.

NOTE: RFN does not recommend the use of Shared key authentication, because the messages used to accomplish this authentication may provide information to eavesdroppers as an aid in cracking the WEP encryption on future messages. The ability to enable or disable Shared Key Authentication is provided mainly for compatibility purposes. Some client adapters may require Shared Key Authentication whenever WEP encryption is enabled. If this is not the case with the client adapters used in your location, then it is best to leave this setting disabled. This does not compromise security, however, because with WEP encryption enabled, the iRAP will not accept traffic from 802.11 client devices unless the traffic is encrypted.

6.2.3.3 WEP Keys

When WEP Encryption is enabled, you must enter values for the four WEP keys in order for the RFS 802.11 implementation to function. WEP Keys are used to encrypt 802.11 traffic that is transmitted by a iRAP.

Each WEP Key has a radio button. When you select the radio button, you can enter, change, or delete information for that key only. Each WEP key consists of five pairs of hex digits forming a 40-bit binary string, which is the standard length of a WEP key.

Only one WEP Key can be selected at a time. The selected key is used to encrypt 802.11 traffic that is transmitted by a iRAP. However, any of the four keys may be used by client devices for their transmissions. The determination of which key is used by a client device is performed at the client device, usually in a manner similar to the way the iRAP is configured.

6.2.4 Enhanced Security

Enhanced Security provides another layer of protection for the RFS 802.11 implementation. When enabled, or “On”, this setting prevents iRAPs from broadcasting their SSID information. This helps to prevent unwanted users from accessing the customer’s WLAN. When disabled, or “Off”, any system can ‘see’ the SSID of iRAPs in the customer WLAN.

6.2.5 User Access Control

The RFS provides the ability to restrict access to the customer LAN to certain pre-authorized devices. If a RADIUS Server is not available for user authentication, RFN recommends setting the User Access Control option to “On” to provide a means to identify those devices that are authorized to communicate over the customer’s LAN via the RFS. When this option is disabled, set to “Off”, any client device may associate with the RFS.

Devices are Identified by a number that is programmed into the 802.11b/g network interface installed in the device. For instance, laptop PCs typically use a PCMCIA card plugged into the laptop’s PCMCIA bay to access an 802.11 network. Every 802.11b/g PCMCIA card comes from the manufacturer with a unique numeric identifier. No two devices are ever manufactured with the same identifier.

In IEEE 802 networking terminology, this identifier serial number is the MAC address (Media Access Control address), an addressing mechanism that is present in all types of IEEE 802 LANs. The MAC address is typically represented as six sets of hexadecimal (base 16) numbers, with two hexadecimal digits in each set. The following is an example of how a MAC address may be written:

00:04:16:A3:29:B7

Authorized MAC addresses/devices are listed below the User Control option. To learn how to add and remove MAC addresses, read the following section 6.2.5 Add/Remove MAC Addresses. When you are done adding and removing MAC addresses, you’ll select the Save Changes button under User Access Control.

6.2.6 Add/Remove MAC Addresses

Start by collecting a list of MAC addresses for all user devices that will be authorized to access the customer's LAN via the RFS 802.11. It is best to keep a permanent list (on paper, in a spreadsheet, or other computer storage) that includes each MAC address and a description of the device, including the name of the person who owns the device, etc. Also refer to section 6.4 Viewing WLAN User/iRAP Associations, later in this chapter.

6.2.6.1 Adding MAC Addresses

MAC addresses are added to the list of authorized client devices in one of two ways: one, you can enter the addresses one at a time, or two, you can enter the MAC addresses into a text file and "upload" this list into the MAC address database.

To add an individual MAC address, enter it in the box labeled **Address**. Enter each MAC address in the format described above, that is, six pairs of hexadecimal digits (for example 00:04:16:A3:29:B7). The alphabetic values of hexadecimal digits—A,B,C,D,E,F—may be in either upper case or lower case. For **Name**, enter a meaningful device name or identifier, or the name of the person who owns the device. For **VLAN**, enter the VLAN desired for that user (typically the default VLAN configured for the BCU network connection), and then select **Add Address.**

To add MAC addresses from a file, either enter the file name under **Import/Export File** (including drive letter and full pathname), or select the **Browse…** button to locate the file. Then, select **Add**. This appends the MAC addresses from the file to any other MAC addresses already entered into System Manager. The file is transferred to the BCU using anonymous FTP. An FTP server running on the host management terminal is required.

TIP The MAC address file is stored in comma-delimited format. The format is name, MAC address, VLAN. Here is an example:

test_user, 00:11:22:33:44:55,2

6.2.6.2 Removing MAC Addresses

To remove a MAC address, select the delete option listed next to the MAC address you wish to remove.

To remove all MAC addresses, select the **Remove All MAC Addresses** button under **Remove All**.

6.2.7 Network Security & Accounting

In a typical enterprise network, WEP encryption and MAC address authentication do not provide the level of security that most users require. To help protect these networks, the RadioFrame System offers both Wi-Fi Protected Access Support and 802.1x authentication with dynamic WEP keys.

Wi-Fi Protected Access (WPA) provides security through data encryption and user authentication. In order to overcome the limitations of WEP, WPA uses a Temporal Key Integrity Protocol (TKIP) for data encryption. This provides per-packet key mixing, a message integrity check (MIC), an extended initialization vector (IV) with sequencing rules, and a re-keying mechanism.

WPA offers strong user authentication through 802.1X and the Extensible Authentication Protocol (EAP). EAP uses a RADIUS server to authenticate each user on the network before they join it, and also employs "mutual authentication" so that the wireless user does not accidentally join a rogue network that might steal its network credentials. If the network is not using a RADIUS server or EAP, WPA may use a Pre-Shared Key (PSK). With PSK, the client and access point use the same key to establish an association. Once this key is verified, WPA then encrypts frames using TKIP to provide improved security.

The RadioFrame System can also be configured to use 802.1x for authentication and key management if TKIP is not supported by the WLAN clients. In this scenario, 802.1x is still used for authentication however WEP is used for data encryption.

When an unauthenticated supplicant (wireless client) attempts to connect to an authenticator (the iRAP), the iRAP responds by enabling a port for passing only EAP packets from the client to the RADIUS server connected to the RFS. These EAP packets are encrypted using a unique session key. The iRAP blocks all other traffic until the RADIUS server indicates it has verified the client's identity. The iRAP then opens the client's port for other types of traffic. The iRAP may then use the session key to derive a unique WEP key for encrypting data between the client and the iRAP. These keys are passed to the client in an EAP key message.

If your network includes a RADIUS (Remote Authentication Dial-In User Service) server for authentication, you can also enable accounting on the RFS to send network accounting information about wireless client devices to the RADIUS server.

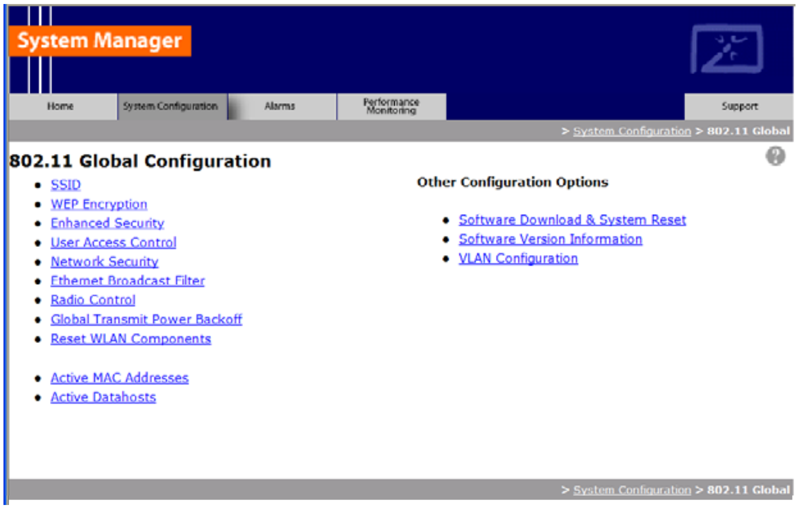
Accounting information includes statistics about the data transmitted and received by the iRAP, including account session ID, user name, client IP address, bytes received, number of packets, and a timestamp. Enable accounting on the iRAPs to send network accounting information about wireless client devices to a RADIUS server on your network. (See the RADIUS server documentation for instructions on retrieving accounting data.)

1 Start System Manager and log in to the RFS.

2 Select the System Configuration tab.

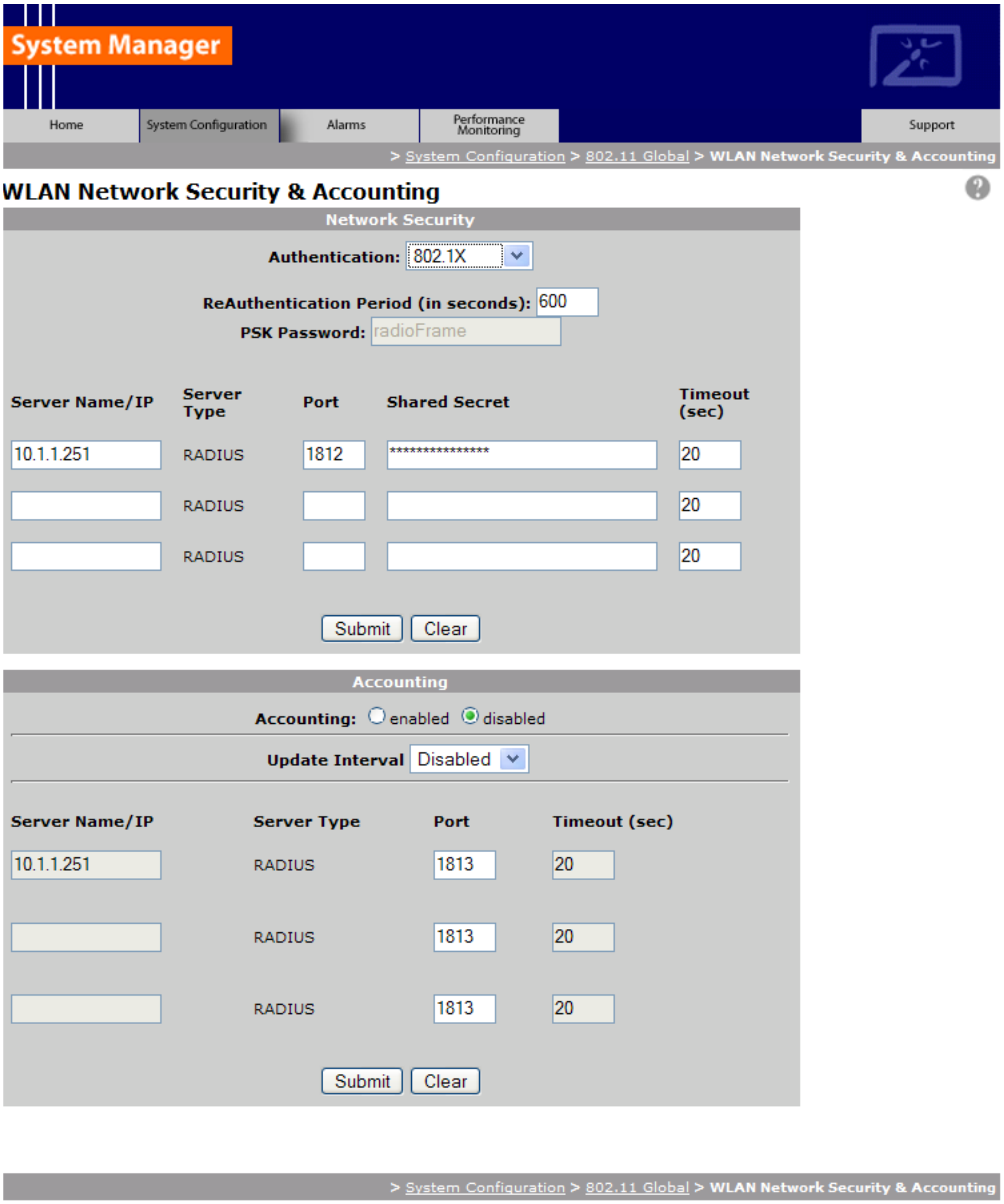
3 Select the 802.11 Global Configuration link under **Other Configure Options**.

The 802.11 Global Configuration page appears.


System Manager
Home
System Configuration
Alarms
Performance Monitoring
Support
> System Configuration > 802.11 Global
802.11 Global Configuration
SSID
WEP Encryption
Enhanced Security
User Access Control
Network Security
Ethernet Broadcast Filter
Radio Control
Global Transmit Power Backoff
Reset WLAN Components
Active MAC Addresses
Active Datahosts
Other Configuration Options
Software Download & System Reset
Software Version Information
VLAN Configuration
> System Configuration > 802.11 Global

4 Select Network Security.

The WLAN Network Security & Accounting page appears. Settings are divided into two parts: security and accounting.



> System Configuration > 802.11 Global > WLAN Network Security & Accounting

WLAN Network Security & Accounting

Network Security

Authentication: 802.1X

ReAuthentication Period (in seconds): 600

PSK Password: radioFrame

Server Name/IP	Server Type	Port	Shared Secret	Timeout (sec)
10.1.1.251	RADIUS	1812	***************	20
	RADIUS			20
	RADIUS			20

Accounting

Accounting: ○ enabled ● disabled

Update Interval Disabled

Server Name/IP	Server Type	Port	Timeout (sec)
10.1.1.251	RADIUS	1813	20
	RADIUS	1813	20
	RADIUS	1813	20

> System Configuration > 802.11 Global > WLAN Network Security & Accounting

5 For **Authentication** in the Network Security section, choose from Disabled, 802.1x, WPA, or WPA-PSK.

If WPA-PSK is enabled, enter the pre-shared key in the PSK Password box. This password must also be given to the WLAN client as described in the WLAN client's documentation. Setup is now complete.

If WPA or 802.1x is enabled, configure the RADIUS server as described below.

6 For **Reauthentication Period**, enter the amount of time before reauthentication is forced. Note, that if the value for the System Manager differs from the value set for the RADIUS server, the System Manager is given priority.

7 For **Server Name/IP**, enter the name or IP address of the RADIUS server on the network.

Configure up to three servers for authentication services, so the network can have backup authenticators. If you set up more than one server for the same service, the first server in the list will be the primary server for that service, and the others are used in the order listed when the previous server times out.

NOTE: You cannot change the **Server Type** (RADIUS).

8 For **Port**, enter the port number the RADIUS server uses for authentication.

The default setting, 1812, is the port setting for Microsoft's RADIUS server.

9 For **Shared Secret**, enter the shared secret used by your RADIUS server.

The shared secret on the iRAPs must match the shared secret on the RADIUS server.

10 For **Timeout**, enter the number of seconds the iRAPs should wait before authentication fails. If the server does not respond within this time, the iRAP tries to contact the next authentication server in the list, if one is specified. Other backup servers are used in the order listed when the previous server times out.

11 Repeat Steps 7 through 10 for each RADIUS server in the network.

12 Select the **Submit** button to save your changes.

13 For **Accounting:** select **enabled** to turn on accounting for your wireless network.

14 For **Update Interval**, enter the number of minutes between accounting update messages that the iRAP sends for each associated client device.

15 For **Server Name/IP**, enter the name or IP address of the server to which the iRAPs send accounting data.

16 For **Port**, enter the communication port used by the iRAP and the server.

The default setting, 1813, is the correct setting for the RadioFrame System and the iRAPs.

17 For **Timeout**, enter the number of seconds the iRAPs should wait for the server to respond. If the server does not respond within this time, the iRAP tries to contact the next accounting server in the list if one is specified. The iRAP uses backup servers in list order when the previous server times out.

18 Repeat Steps 15 through 17 for each RADIUS server in the network that will receive accounting information.

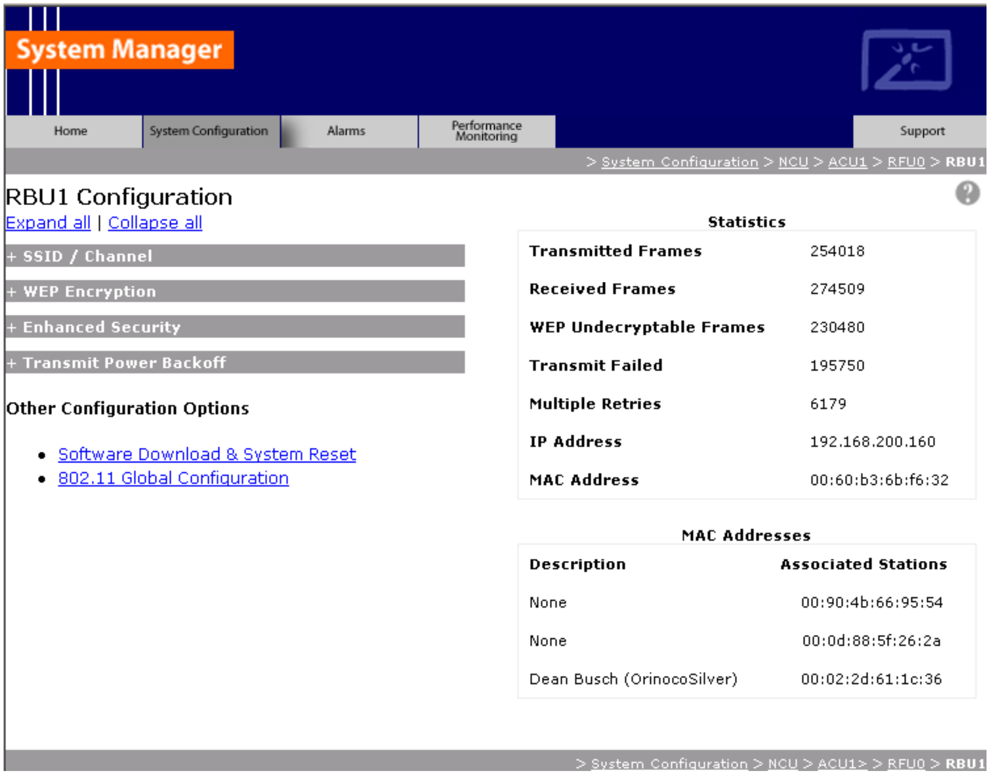
19 Select the **Submit** button to save your changes.

6.3 Configuring an Individual iRAP

The integrated RadioFrame Access Point (iRAP) provides the 802.11b/g wireless interface between the RFS and the corporate local area network (LAN). Typically, all iRAPs in the RFS are configured at one time using the 802.11 Global Configuration options. These global settings can be overridden by changing configuration information for individual iRAPs. Individual iRAPs can also be isolated from further global changes as well.

NOTE: WEP Encryption and Enhanced Security settings override global 802.11 settings. Typically, changing these settings is done to isolate the iRAP for testing.

1 Using the System Configuration tab, drill down to the RFU that contains the iRAP(s) you want to configure, and then select the iRAP icon to display its configuration page.



RBU1 Configuration

Expand all | Collapse all

+ SSID / Channel

+ WEP Encryption

+ Enhanced Security

+ Transmit Power Backoff

Other Configuration Options

- Software Download & System Reset
- 802.11 Global Configuration

Statistics

Transmitted Frames	254018
Received Frames	274509
WEP Undecryptable Frames	230480
Transmit Failed	195750
Multiple Retries	6179
IP Address	192.168.200.160
MAC Address	00:60:b3:6b:f6:32

MAC Addresses

Description	Associated Stations
None	00:90:4b:66:95:54
None	00:0d:88:5f:26:2a
Dean Busch (OrinocoSilver)	00:02:2d:61:1c:36

2 For **SSID**, either leave the globally configured SSID name as it is, or enter up to 31 alphanumeric characters to change it.

The SSID you enter must be a valid SSID that is recognized by System Manager.

3 For **Channel**, type 1, 6, or 11 to specify the channel to be used by the iRAP.

At the time of shipment, all iRAPs are set to Channel 6 by default. Channel numbers can only be changed at the iRAP level—channels cannot be changed using global settings. If a 3-channel frequency plan is implemented, RFN recommends using channels 1, 6, and 11 (in countries where these channels are permitted).

4 Select ‘Save Changes’ to save the SSID and Channel settings.

5 When **WEP Encryption** is disabled or “Off”, all other items related to WEP encryption are disabled (WEP Keys and Shared Key Authentication). When “On”, a **WEP Key** other than the globally configured WEP key can be selected. Also, **Shared Key Authentication** can be enabled or disabled, “checked” or “unchecked” respectively. For more information about Shared Key Authentication, refer to section 6.2.3.2 Shared Key Authentication.

RFN recommends that iRAP WEP Encryption settings be set globally rather than individually.

iRAP WEP Encryption changes remain until changes are made to the global 802.11 settings.

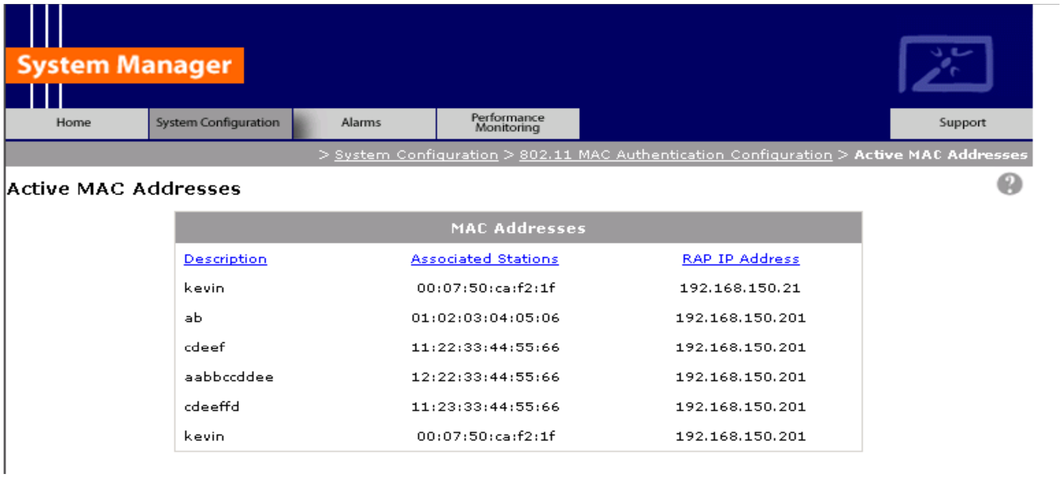
6 **Statistics** lists information about the functioning of the iRAP, including:

Statistic	Description
Transmitted Frames	Number of frames transmitted by the iRAP
Received Frames	Number of frames received by the iRAP
FCS Errors	Number of FCS errors
WEP Undecryptable Frames	Number of frames that could not be unencrypted
Transmit Failed	Number of failed transmissions
Multiple Retries	Number of retries attempted
IP Address	IP address of the iRAP
MAC Address	MAC address of the iRAP

7 For **Enhanced Security**, select either “On” or “Off”, and then select Save Changes.

6.4 Viewing WLAN User/iRAP Associations

To view clients and their associated iRAP(s), select the Active MAC addresses link on the 802.11 Global Configuration page. For each iRAP, the Active MAC Addresses page lists each user associated with the iRAP, including the user name (Description) and the IP address of the workstation or piece of equipment. Information is sorted by the iRAP IP address.

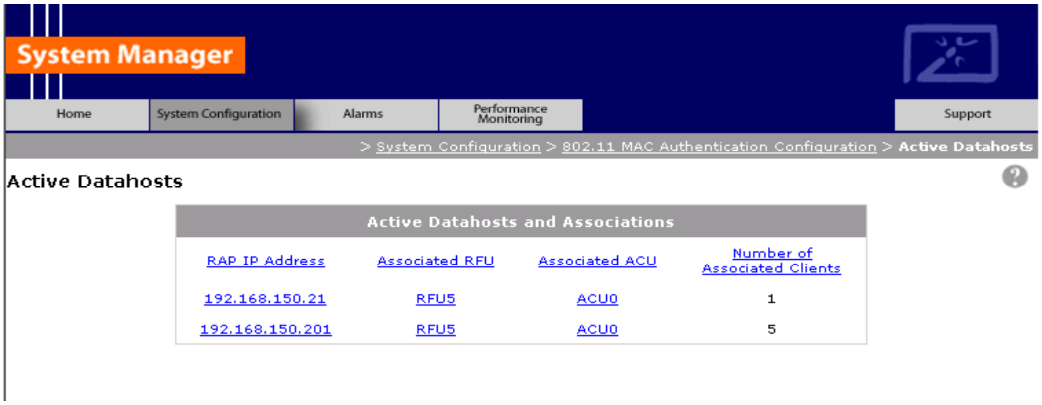

System Manager
Home
System Configuration
Alarms
Performance Monitoring
Support
> System Configuration > 802.11 MAC Authentication Configuration > Active MAC Addresses

Active MAC Addresses

MAC Addresses

Description	Associated Stations	RAP IP Address
kevin	00:07:50:ca:f2:1f	192.168.150.21
ab	01:02:03:04:05:06	192.168.150.201
cdeef	11:22:33:44:55:66	192.168.150.201
aabbccddee	12:22:33:44:55:66	192.168.150.201
cdeeffd	11:23:33:44:55:66	192.168.150.201
kevin	00:07:50:ca:f2:1f	192.168.150.201

To view the number of users supported by each iRAP, select the Active DataHosts and Associations link at the top of the 802.11 Global Configuration page. The Active DataHosts page identifies the location of each iRAP by RFU and ACU, and displays the number of users associated to the iRAP. You can view the configuration for each iRAP, RFU or ACU by selecting the link for that component. This information can be used to analyze the load distribution in the WLAN RadioFrame system.


System Manager
Home
System Configuration
Alarms
Performance Monitoring
Support
> System Configuration > 802.11 MAC Authentication Configuration > Active Datahosts

Active Datahosts

Active Datahosts and Associations

RAP IP Address	Associated RFU	Associated ACU	Number of Associated Clients
192.168.150.21	RFU5	ACU0	1
192.168.150.201	RFU5	ACU0	5

6.5 Verifying the Wireless LAN (802.11b) Installation

Verifying the LAN installation requires a laptop that has 802.11b/g internally or a client card that plugs into the PCMCIA port.

1 Associate with a iRAP in the RFS by matching the SSID on the client (laptop) and the SSID that is configured in the System Manager.

2 Setup a static address on the client to communicate with the RFS (refer to Appendix D for a list of default IP addresses for the RFS).

3 Once associated, open a command window and ping the BLIC IP addresses to confirm that the client is properly associated with the iRAP (this also confirms connectivity up to the BLIC).

4 Once associated, navigate to a few Internet addresses. This requires that the Administrator correctly configure their network for this navigation.

7 Operations and Maintenance

A report of the RFS GSM/802.11 site should be maintained and left on site. This report will provide metrics for possible concerns with individual components of the entire system.

It is important that the technician performing the checks understand the equipment theory and operation. Review the documentation (references) prior to verification and performing service.

This chapter contains procedures for the following:

- Upgrading System Software
- Preventive maintenance
- Corrective maintenance
- Field replaceable units (FRUs)
- Alarm resolution procedures,
- Repair and technical support

7.1 Upgrading System Software

The RadioFrame System is shipped with the latest software and hardware installed. With each new software release, RFN provides its customers with the new software (this software can also be downloaded from the RFN FTP site) and upgrade instructions for that release in the *Customer Release Notes.* The instructions describe how to upgrade to the latest software from any prior version. To upgrade hardware, refer to section 7.4 Field Replaceable Units—RadioFrame System.

Periodically RadioFrame System software will be updated. You can opt to upgrade your RFS software at that time, or wait until another time. You can also revert to the previous version of System Manager software at any time. This section includes the following procedures:

- Downloading System Manager software updates
- Downloading other RFS applications (GSM and WLAN)
- Verifying the software downloads
- Resetting the system to install the software updates
- Reverting to the previous version of System Manager software

7.1.1 Download the System Manager software update

1 Connect to the RFS and run the FTP server software (for instructions, refer to Appendix E “Connecting to the RFS”.

2 Open System Manager, and display the BCU System Configuration page.

1 Select the **Software Download & System Reset** link located under 'Other Configuration Options' to display the Software Configuration page.

2 Select the textbox for **Download to Version A** or **Download to Version B**.

RFN highly recommends that you select the 'Download to Version X' that is *not* selected in the System Reset section. In this example, Version B is selected under System Reset. Therefore, you would choose the 'Download to Version A' textbox.

3 Select the **Browse** button and locate the file **platform_download.txt**.

4 Select the **Download to Version** (A or B) button to start the platform software download.

Wait for the download to complete successfully, which may take several minutes.

7.1.2 Download other RFS applications (GSM and WLAN)

1 To download a GSM software update, browse in the **Download to Version** (A or B) text box (the same one used to download the platform software) to locate the file: **\gsm\loads\gsm_download.txt**.

2 Select the **Download to Version** (A or B) button to download the GSM upgrade file.

Wait for the download to complete successfully.

3 To download a WLAN software update, browse in **Download to Version** (A or B) text box to locate the file: **\wlan\loads\wlan_download.txt** (complete this step only if there are 802.11b/g datahosts (RAPs) present in the system).

4 Select the **Download to Version** (A or B) button to download the WLAN file.

Wait for the download to complete successfully.

7.1.3 Verify the Software Downloads

1 Select the **Software Version Information** link on the Software Configuration page to display the Software Version information page.

2 Review the SW Versions A and SW Versions B for the RFS to make sure the latest software is loaded.

3 Verify that the SW Selected and SW Loaded for each component in the RFS is correct.

7.1.4 Reset the system

1 Display the **Software Configuration** page.

2 Under **System Reset**, select the **Version A** or **Version B** radio button (use the same version that was used to download the software; in this example, Version A).

3 Select the **Reset System** button to cause a system reset.

CAUTION!!! Do not interrupt the reset in any way…do not power cycle any equipment. The reset may take more than an hour to complete. Do not interrupt the reset!

Wait for the system to come back, and then refresh the page or reopen the web browser to force the page to update.

7.1.5 Reverting to the previous version of System Manager software

Revert to a previous version of system software only if the upgrade fails.

1 Display the BCU Configuration page and select the **Software Download & System Reset** link under ‘Other Configuration Options’.

2 Under **System Reset**, select the radio button that is not currently selected to revert to the previously loaded version of RFS software.

3 Select the **Reset System** button.

This reboot will take several minutes to complete. Wait for the system to come back, and then refresh the page or reopen the web browser to force the page to update.

7.2 Preventive Maintenance

Conduct the following **semi-annual maintenance**:

- Visually inspect all RFS components for loose or foreign items and for visible damage.
- Confirm that each component is receiving power (refer to the troubleshooting tables listed in 7.3 Corrective Maintenance, next in this chapter).
- Verify that all RFS components are operational (refer to section 5.1).
- Verify coverage validation by conducting spot tests described in section 5.4 Coverage Validation.
- Verify GSM functionality by conducting spot tests using the procedures described in section 5.6 RFS Functionality Test.

7.3 Corrective Maintenance

The fault indications Identified in this section provide a guide for isolating failures to a Field Replaceable Unit (FRU). The service technician should perform troubleshooting whenever a failure occurs during normal operation.

Some indications list several possible failures along with corresponding corrective actions. If a failure is isolated to the FRU level, the suspected component should be replaced with a new one. This restores the system to normal operation as quickly as possible. For more information, refer to section 1.3 Repair and Technical Support.

RadioFrame Networks equipment and components are not field repairable. Do not attempt to repair RFN equipment and components in the field. RFN components are individually tested prior to shipment. Should a failure occur replacement boards must be inserted and the RFS re-booted.

This section describes troubleshooting information for each component of the RadioFrame System: BCU, ACU, and RFU. If the provided solutions do not resolve the problem, refer to the *Field Guide to the RadioFrame System* for further troubleshooting information. If none of the provided solutions resolve the problem, contact the Customer Assistance Center (TAC) at (800) 328-0847.

7.3.1.1 Base Chassis Unit

BLIC front ports	**Description**
Port 1 (RJ45)	Not currently used
Port 2-7 (RJ45)	Ethernet LAN
Ports 8 (RJ45)	for maintenance—Customer Service use only
EIA-232 9-pin serial port	for maintenance—Customer Service use only
BLIC back ports	
Ports 1-8 (RJ45)	ACUs—up to 8 ACUs may be connected to the BCU
5MHz/1PPs IN	Not currently used
5MHz/1PPs OUT	Not currently used
GPS ANT	Not currently used
DLC back ports	
Port 1 (RJ45)	T1/E1

Each card installed in the front and back of the BCU has two LEDs: Power (top) indicates power, and Status (lower) indicates the status of the card. Each RJ45 port has two LEDs: Link (right) indicates Ethernet connectivity, and Activity (left) blinks to indicate Ethernet activity. All LEDs should light as green. For all other conditions, refer to the following table.

Indication	Possible failure	Corrective action
Power and Status LEDs for cards installed in front or back of BCU are not lit	no power to BCU	▪ Verify that the power cord is installed and properly seated. ▪ Verify that the power source is operational (120VAC or –48VDC). ▪ Contact Customer Support.
Status LED is red—top front card *only*	timing source not available	▪ Connect the timing source. ▪ Check all connections.
	failed initialization	▪ Reboot the system: unplug the BCU, and plug it in again. Boot up may take several minutes.
	fan is not working	▪ Verify that the fan is operational. ▪ If the fan is not working, unplug the BCU and contact Customer Support.
Status LED is red—any card	card is not operational	▪ Remove and reseat card. ▪ Contact Customer Support.
RJ45 port Link and Activity LEDs are not lit, or the Activity LED is not blinking	connection is not being made between RFS components	▪ For the affected port, verify that all cabling between components is properly connected.

7.3.1.2 Airlink Chassis Unit

ACU front ports	Description
RJ45 Port 1	BCU—connects the ACU to the BCU
RJ45 Ports 2-8	not currently used
EIA-232 9-pin serial port	for maintenance—Customer Service use only
ACU back ports	
Ports 1-8 (RJ45)	RFUs—up to 8 RFUs may be connected to the ACU
5MHz/1PPs IN	not currently used
5MHz/1PPs OUT	not currently used
GPS ANT	not currently used

Each card installed in the front and back of the ACU has two LEDs: Power (top) indicates power, and Status (lower) indicates the status of the card. Each RJ45 port has two LEDs: Link (right) indicates Ethernet connectivity, and Activity (left) blinks to indicate Ethernet activity. All LEDs should light as green. For all other conditions, refer to the following table.

Indication	Possible failure	Corrective action
Power or Status LEDs for cards installed in front or back of ACU are not lit	no power to ACU	▪ Verify that the power cord is installed and properly seated. ▪ Verify that the power source is operational (120VAC or –48VDC). ▪ Contact Customer Support.
Status LED is red—top front card *only*	timing source not available	▪ Connect the timing source. In some cases. ▪ Check all connections.
Status LED is red—any card	card is not operational	▪ Remove and reseat card. ▪ Contact Customer Support.
	failed initialization	▪ Reboot the system: unplug the

Indication	Possible failure	Corrective action
	fan is not working	ACU, and plug it in again. Boot up may take several minutes. ▪ Verify that the fan is operational. ▪ If the fan is not working, unplug the ACU and contact Customer Support.
RJ45 port Link and Activity LEDs are not lit, or the Activity LED is not blinking	connection is not being made between RFS components	▪ For the affected port, verify that all cabling between components is properly connected.

7.3.1.3 RadioFrame Unit

During installation, ensure that the RFU is receiving power and connectivity from the ACU before inserting RadioBlades into the RFU or placing the front cover on the RFU.

Warning!

Do not remove the protective cover from or insert a connector into the AUX port. This will cause damage to the RFU, the ACU, or both.

The MAIN RJ45 port has two LEDs: Link (right) indicates Ethernet connectivity, and Activity (left) blinks to indicate Ethernet activity between the RFU and the ACU. For all other conditions, refer to the following table.

Indication	Possible failure	Corrective action
MAIN Port LEDs do not light	connection is not being made between the RFU and the ACU	▪ Verify that all cabling between the ACU and the RFU is properly connected. ▪ Verify that the ACU is powered on. ▪ Contact Customer Support.

7.4 Field Replaceable Units

In the case of chassis units, replacement boards must be inserted and the RFS re-booted.

1 Always use a static grounding wrist strap before handling any board—*do not* attach the wrist strap to any painted surface on the chassis unit.

Note It is not necessary to unplug the BCU or the ACU prior to removing or inserting a board.

2 Facing the chassis unit, remove the card that is to be replaced, or the blank faceplate, following these guidelines:

- Loosen the blue knurled knobs on both sides of the board.
- Pull firmly to unseat the board from the connectors inside the chassis unit.
- Gently slide the board straight out and away from the chassis unit so as not to damage any components contained on the board.

3 Remove the new board from its antistatic packaging and insert it into the chassis unit as shown in the following illustration, and follow these guidelines:

- Do not jam the board in any way while inserting it.
- Do not mount the board in any orientation other than that specified in the diagram.
- Insert the board straight into the chassis unit so as not to damage any components contained on the board.
- Press firmly to seat the board into the connectors within the chassis unit.
- Tighten the blue knurled knobs on each end of the board finger tight only—do not use a screwdriver to tighten the screws and do not over tighten.

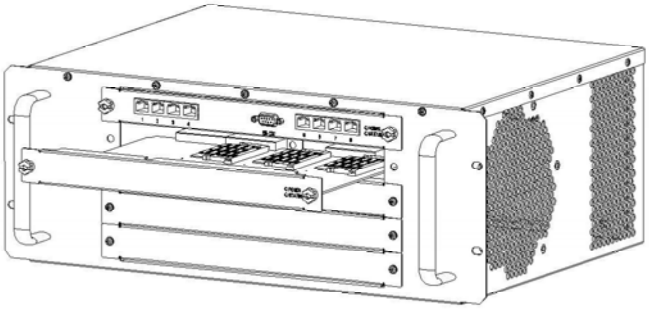


Figure 21 Replacing a board in a BCU or an ACU.

4 Place the old board in the antistatic packaging for shipment.

5 Restart the RadioFrame System.

Select the Software Download & System Reset link located at the bottom of the BCU configuration page, and select the “Reset System” button to cause a system reset. The reboot may take several minutes to complete.

7.5 Alarm Resolution Procedures

The RFS provides fault alarming and isolation within System Manager for individual components, which consists of detecting catastrophic faults that prevent an RFS component from responding to a periodic “ping”.

This section describes:

- How to view alarms in System Manger, and
- System Manager alarms and resolution procedures.

7.5.1 Viewing System Manager Alarms

System Manager displays system-related errors.

1 To view alarms and other system-related errors in System Manager, select the Alarms tab.

The **Alarms Log** displays RFS alarms, listed by **Time** of occurrence (including the date), in a sequence of 400 alarms at a time—**No.** (see the following illustration). Approximately 25 alarms are visible at any one time. At the bottom of the page, you can see which alarms are currently displayed, in this case, 99 through 118 of 118 alarms.

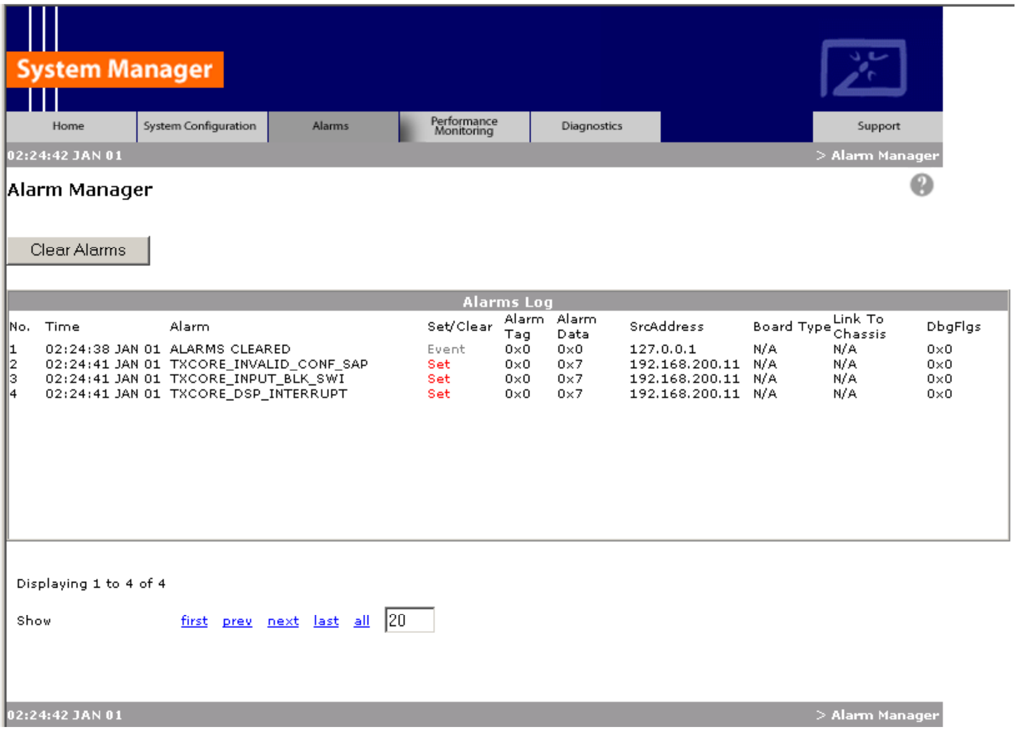
NOTE: If the Alarms page is empty, System Manager is still loading the page.

2 To display alarms that have scrolled out of view, select **first**, **prev**, **next**, **last** or **all** at the bottom of the alarm page, then enter a value in the **Show** text box and press enter.

For example, to view the first 20 alarms, click first and type 20 in the text box, then press Enter. To return to the bottom of the list of alarms, select last and type a value in the text box.

For each **Alarm**, System Manager displays the alarm description and whether the alarm is new (**Set**) or has been cleared (**Clear**). The same alarm will continue to be listed as a set alarm until it has been cleared. If an alarm is not cleared, it will be sent to the OMC (see “System Manager Alarm Descriptions” later in this section). Other alarms might occur before an alarm clears, so the ‘set’ and ‘clear’ for the same alarm do not necessarily appear in sequence.

The **Alarm Tag** uniquely identifies each alarm using either the actual IP address or hex digits to represent the IP address of the affected component. In the latter case, the last four digits of the alarm tag represent the last two sets of digits of the IP address of the



02:24:42 JAN 01

Alarm Manager

Alarms Log

No.	Time	Alarm	Set/Clear	Alarm Tag	Alarm Data	SrcAddress	Board Type	Link To Chassis	DbgFlgs
1	02:24:38 JAN 01	ALARMS CLEARED	Event	0x0	0x0	127.0.0.1	N/A	N/A	0x0
2	02:24:41 JAN 01	TXCORE_INVALID_CONF_SAP	Set	0x0	0x7	192.168.200.11	N/A	N/A	0x0
3	02:24:41 JAN 01	TXCORE_INPUT_BLK_SWI	Set	0x0	0x7	192.168.200.11	N/A	N/A	0x0
4	02:24:41 JAN 01	TXCORE_DSP_INTERRUPT	Set	0x0	0x7	192.168.200.11	N/A	N/A	0x0

Displaying 1 to 4 of 4

Show

02:24:42 JAN 01

Figure 22 Alarms are listed up to 400 at time and continue to scroll as events occur.

component. For example, 0xc0a80679 represents xxx.xxx.06.121. The IP address of the board generating the alarm is shown under **SrcAddress**, or 'source address'.

Board Type identifies which board within a chassis unit is affected (APC, CRIC, etc.). For these alarms, select **Click for chassis** link to display the page for that component.

NOTE: When troubleshooting alarms that require assistance from RadioFrame Networks, you'll need to provide the data displayed in the **Alarm Data** and **DbgFlgs** fields.

7.5.2 System Manager Alarms

The table below describes all System Manager alarms, and what action is required, if any, to resolve the problem.

System Manager Alarm	Description	Action
ALARMS CLEARED	Alarm Manager was cleared using the Clear Alarms button.	No action required.
APC NO SPAM	There are more BRs than the current SPAM resources can support.	Add more SPAMs as required.

System Manager Alarm	Description	Action
COMMANDED RESET	System Reset was initiated via System Manager. Causes a system reset.	
COVERAGE HOLE	One BR in a sector has fewer RBs than other BRs in that sector. The BR that is short of RadioBlades has locked.	
DHRB RESET	A problem in the iRAP has caused it to reset.	No action required.
DHRB TASK EXCEP	Task Exceptions has occurred for some task on the iRAP. iRAP resets.	No action required.
DSP 1180 FLOOD	The RB 1180 DSP address is flooding all ports. Sends a Stop Tx command to the RB and causes a system reset.	
DSP HPI ERROR	Problem in accessing HPI interface for a DSP. If errors go beyond a threshold, SPAM is reset.	
DSP LOAD ERROR	DSP software not found. DSP was not initialized.	Check the ffs files etc.
DSP LOST PDU	DSP is not sending any PDUs to the APC. The CPU received fewer than threshold PDUs within a fixed period from the DSP. SPAM is reset.	
DSP TX IQ FAIL	DSP Tx counter is not incrementing as per expectations, implying that DSP has stopped transmitting. SPAM is reset.	
DSP TX NULL PDU	DSP is transmitting too many NULL packets because it didn’t receive PDUs from CPU. SPAM is reset.	
EXC DSP RESET	DSP SPAM has been reset more than four times within the last 20 minutes. Causes a system reset.	
EXT BR RESET	BR received a reset command from the iSC. Event logged to indicate that BRs went down on iSC request.	
FAN1 ALARM	Chassis FAN1 is malfunctioning.	Check chassis fans for proper

;ystem Manager Alarm	Description	Action
		operation.
FAN2 ALARM	Chassis FAN2 is malfunctioning.	Check chassis fans for proper operation.
FFS PARTITION	Board booted from wrong partition. May indicate problem with the files on boot partition.	Verify software versions for each partition in System Manager.
GSMRB LOSS	Communication with the GSM RadioBlade has been lost. The corresponding BR is locked and all associated RBs have stopped.	
LAPD LINK FAIL	The LAPD connection between the BR and the iSC has been lost. The BR will try to re-establish the LAPD and sends a state change trap to iSC.	Check the iSC connection.
LOST RFU	All the GSM RBs and Datahosts in an RFU have been lost.	Check the RFU connections, etc.
NET POOL ERROR	The free Mblock cluster has gone below 40 on a BPC or APC, the threshold for APC_NETPOOL_LOWMARK or NPC_NETPOOL_LOWMARK. Causes a system reset.	
OVERTEMP	A chassis has overheated.	Check the chassis for proper operation.
PEER LOSS	Communication with a board has been lost. RIC has detected a PEER LOSS from the BLIC. Causes a system reset, unless the cause is a iRAP, which self resets.	Check board connections. If frequent, capture alarms and serial logs and submit to RFN.
PLL LOCK	A RIC or BLIC PLL went out of lock. The BLIC locks and de-key all BRs, and then sends a state change trap to the iSC.	
ROM MISMATCH	Board boot version is not the same as the BLIC.	
SPAM FAILED	Lost DSP PDUs have exceeded threshold. SPAM is reset.	
SW VER MISMATCH	Board software version is not the same as the BLIC.	
SYSTEM RESET	Alarms that result in a system reset cause this alarm, except for the BLIC. All BRs and boards are locked and reset except the BLIC.	

System Manager Alarm	Description	Action
TASK STARVATION	A task is using all the CPU time and starving other tasks. Prints a list of ready task and causes a system reset (unless it's a DHRB, which resets itself).	Check board for Flash corruption or other malfunctions at startup. Capture alarms and serial logs and submit to RFN.
TASK SUSPEND	A task got suspended on a board. Board is reset (unless source is BLIC).	Check board connections. Capture RAM and serial logs, and submit to RFN.

Appendix A Glossary

Acronym	Term	Description
10BaseT		10BaseT is the most common form of Ethernet cabling. The cable is thinner and more flexible than the coaxial cable used for the 10Base2 standard. 10BaseT is also known as unshielded twisted-pair (UTP). 10BaseT cables support speeds up to 10 Mbps. The maximum distance per segment is 500 meters.
ACU	Airlink Chassis Unit	The central baseband processing unit for the RFS. Rx/Tx airlink traffic to/from RFUs.
APC	Airlink Processing Card	Interface to the RIC for the control of RFU components and the transfer of voice I/Q samples to/from RFUs.
BCU	Base Chassis Unit	The central network processing unit for the RFS. Also central management entity for managing configuration and User Information.
BLIC	RadioFrame LAN Interface Card	Provide the Ethernet switch fabric to route packets to/from ACUs. Also hosts a micro-P serving as primary controller of BPCs.
BPC	Baseband Processing Cards	Interface to the BLIC for the bi-directional transfer of voice I and Q samples to/from RFUs.
CRIC	Common RadioFrame Interface Card	When a CRIC is installed in a chassis unit, it looks to see if there is a PERTM. If there is a PERTM, the CRIC acts as a RIC (see RIC). If there is not a PERTM, the CRIC acts as an BLIC (see BLIC).
CSU	Channel Service Unit	The CSU provides the T-1 connection between the RFS and the telephone company that provides the T-1 line.
DLC	Digital Line Card	
EIA	Electronic Industries Alliance	The EIA organization establishes electronic interface standards.
EAS	Environmental Alarm System	The EAS provides a central location for site alarm signal processing. The EAS monitors environmental conditions of the site, including power, smoke alarms, and intrusion alarms.
ERTM	Ethernet Rear Transition Module	Located in the BCU, provides clock and data to the ACU.
ESD	Electrostatic Discharge	The dissipation of electricity, commonly known as a shock. ESD can destroy semiconductor products, even when the discharge is too small to be felt.
FRU	Field Replaceable Unit	Any unit (module, board, or card) that can be “hot-swapped”, that is, replaced with another unit while the power is connected to the item housing the unit.
GSM	Global System for Mobile Communications	
PERTM	Powered Ethernet Rear Transition Module	Located in the ACU, provides power, clock, and data to the RFUs.
RB	RadioBlade	Provides the airlink interface for the GSM standard.
RFN	RadioFrame Networks	Equipment designer and manufacturer of RFS equipment.

Appendix A: Glossary

Acronym	Term	Description
RFS	RadioFrame System	Digital Communication System for indoor wireless device users. The RFS consists of several components: BCU, ACU, RFUs and GSM RadioBlades.
RFU	RadioFrame Unit	RF front end for each of the implemented air interface to the User equipment and connects to ACU on the other end.
RFU BP	RadioFrame Unit - Back Plane	Facilitates High speed intermodule communication between RFU components and between RFU and ACU.
RIC	RadioFrame Interface Card	Provide the Ethernet switch fabric to route packets to/from ACUs, RFUs and external IP networks. Also will host a micro-P (MPC-8240) as primary controller to APCs.
RSSI	Received Signal Strength Indication	Strength of the received call signal, in dBm.
SELV	Safety Extra-Low Voltage	A secondary electrical circuit designed so that under normal and signal fault conditions, its voltages do not exceed a safe-value.
SPAM	Signal Processing Array Module	A connectorized card which plugs into an APC or BPC and provides the digital signal processing resources.
SQE	Signal Quality Estimate	An estimate of signal quality, based on the received signal strength and quality.
T1/E1	Digital Transmission Rate 1	A North American leased-line connection capable of carrying 1.544 megabits of data per second (Mbps). T-1 lines are commonly used to connect networks, ISPs and others to the Internet. An E-1 line is the European equivalent to the North American T-1. However, an E-1 line carries information at the rate of 2.048 Mbps instead of the 1.544 Mbps of a T-1.
T568B		Wiring standard for RadioFrame System CAT-5 cables. Denotes a specific order of the CAT-5 wires leading into the RJ-45 connector.

Appendix B Site Survey

Site Survey REV A

RADIOFRAME™ NETWORKS

Carrier _______ Date___

Customer _______ Project #______

Site Location _______ RFN Project Engineer__

Present for Site Survey		Name	Email	Phone
	Carrier representative			
	Customer representative			
	Building/Site Manager			
	Installation vendor			
	RFN Engineer			
	RFN Project Manager			
	Other			
Customer Expectations				
	Who will provide RF measurements?			
	Who will install the RFS?			
	Who will commission the installation?			
	Will the RFS be shipped directly to the site or staged?			
	Will the RFS be assembled and tested at the customer site?			
	Digital photos permitted during the site survey?			

Customer Expectations (continued)	
	Troubleshooting expectations?
	Other
RF Planning	
	Which and how many channels will be provided for indoor use?
	Coverage requirements (see RF Measurements below)
	Vertical coverage required?
Site WLAN	
	How/where does the RFS connect to the wireless LAN?
	WLAN configuration?
	Authentication requirements?
	Encryption requirements?
	Static/administration of IP?
	24 X 7 point of contact
RFS Equipment Requirements	
	Wall mount or ceiling mount of RFUs preferred?
	BCU
	BCU location
	Power requirements
	4U 19” rack space available per BCU?
	BSC to T1/E1 connectivity?

RFS Equipment Requirements (continued)	
	ACU
	ACU location
	Power requirements
	4U 19” rack space available per ACU?
	Cable run distance from BCU
	RFU
	Wall mount?
	Above ceiling panels available? If so, which floors?
	Power Requirements
	120VAC or –48VDC available?
	UPS required?
Installation Requirements	
	Cable and Path Requirements
	Plenum rated cable required?
	Innerduct required?
	Conduit required?
	Existing vertical access between floors?
	Space available for additional new cable in existing stubs and/or conduit?
	Core drill required?
	Dedicated CAT-5 (or higher) available?
	Ceiling Type

Installation Requirements (continued)	
	Open
	Suspended
	Acoustical tile
	Hard plaster
	Metal
	Other
	Ceiling Height
	Standard
	Other
	Wall Type
	Standard drywall construction
	Cement/brick
	Metal
	Other
	Firewall
	Load bearing
	Other RF Barriers
	identify RF blocking areas, items and locations
	Local Issues
	Union(s) required (identify)?
	Local code requirements?
	Building management standards?

Installation Requirements (continued)	
	Permits required?
	Other
	Access
	When can work be conducted (regular hours, after hours, weekends)?
	Special scheduling requirements
	Point of contact
	Access (continued)
	Escort required
	Between Buildings Only
	Space available to mount hubs in 19” racks (fiber solution only)?
	New rack space location Identified?
	identify all Telecom closets for remote fiber units
Other Requirements/Comments	

Appendix C BCU and ACU Main Rack Installation

This section includes procedures for:

- Mounting the BCU in the a rack
- Mounting the ACU in the rack
- Connecting the BCU to the ACUs

Mount the BCU in a Rack

The BCU is the main controller of the RadioFrame System. The BCU is mounted in a rack supplied with –48VDC power.

1 Find these items in the BCU shipping container: one BCU, four mounting screws, and one set of product documentation.

2 Mount the BCU only in an EIA-standard compliant (19”) rack using all 4 screws provided. Refer to the site documentation for the exact location of the BCU. For safe operation, follow these guidelines:

- Do not mount the BCU in any orientation other than that specified in the following illustration.
- Mount the BCU so that both the front and the back are accessible.
- If the mounting holes do not line up, adjust the BCU up or down until the mounting holes line up.
-

Caution Do not block the air vents on the sides or rear of the BCU.

3 Plug the BCU into main rack power source (rectifier or PDU).

4 Verify that the BCU is receiving power and that each BCU card is operational.

Each card installed in the front and back of the BCU has two LEDs: Power and Status. All LEDs should light green.

Note The Status LED on the top card in the front of the BCU will remain red until the BCU is connected to a timing source.

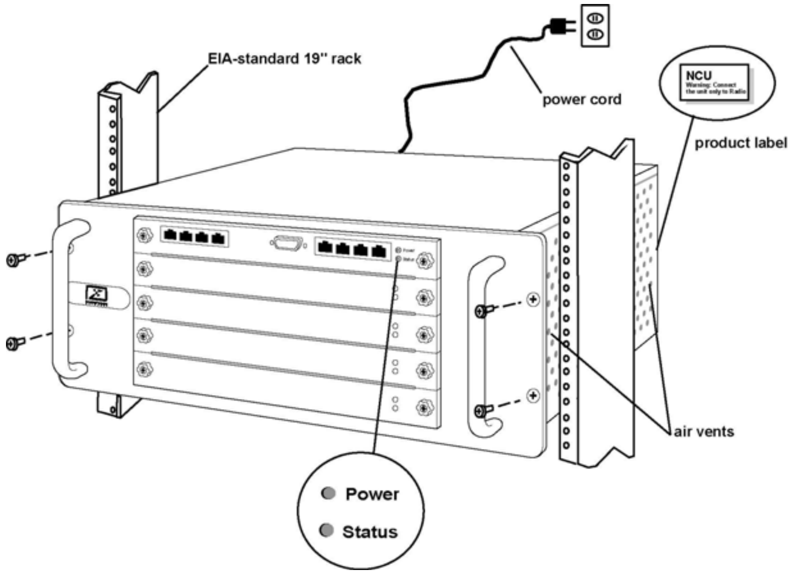


Figure 23 Mount the BCU only in an EIA-standard compliant 19” rack.

Mount the ACU in the Main Rack

The ACU is mounted in the main rack supplied with –48VDC power.

1 Find these items in the ACU shipping container: one ACU and four mounting screws.

2 Mount the ACU only in an EIA-standard compliant (19”) rack using all 4 screws provided. For safe operation, follow these guidelines:

- Do not mount the ACU in any orientation other than that specified in the following illustration.
- Mount the ACU so that both the front and the back are accessible.
- If the mounting holes do not line up, adjust the ACU up or down until the mounting holes line up.

⚠ Caution

Do not block the air vents on the sides or rear of the ACU.

3 Plug the ACU into main rack power source (rectifier or PDU).

4 Verify that the ACU is receiving power and that each BCU card is operational.

Each card installed in the front and back of the ACU has two LEDs: Power and Status. All LEDs should light green.

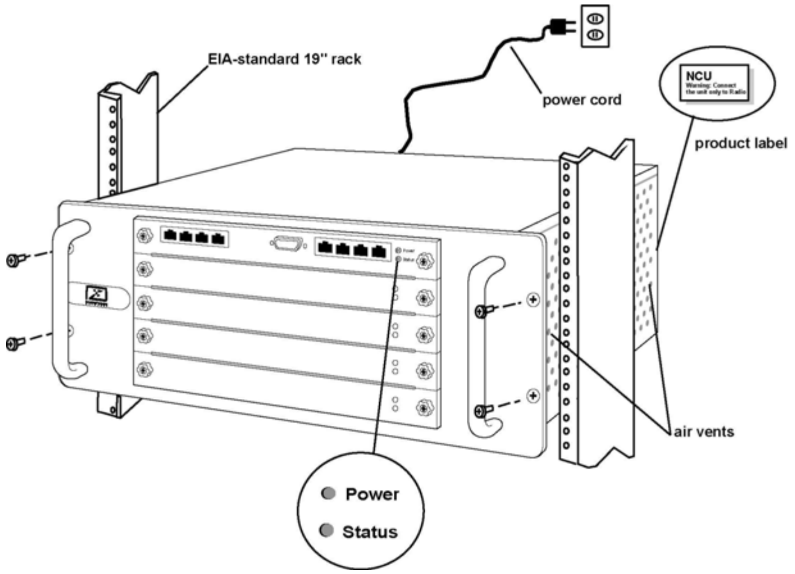


Figure 24 Mount the ACU only in an EIA-standard compliant 19” rack.

Connect the ACUs to the BCU

After the main rack has been installed and all wiring for the RFS has been completed, connect the main rack ACU and all remote ACUs to the BCU.

1 Connect the RJ45-to-RJ45 CAT-5 cable from Port 2 on the front of the ACUs to the specified RJ45 port (1-8) on the back of the BCU.

Refer to the site documentation to determine which ACU connects to each port on the BCU. The Activity and Link LEDs above the ports will remain unlit until each ACU has been installed and plugged in.

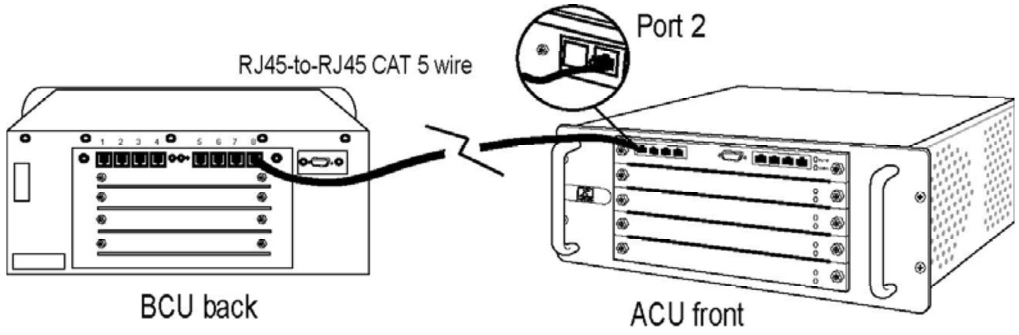


Figure 25 Connect the RJ45-to-RJ45 CAT-5 cable from Port 2 on the front of the ACU to the specified RJ45 port on the back of the BCU.

Appendix D RFS Default IP Addresses

All chassis boards, RFU backplanes, and iRAPs are issued a default IP address during initial setup (GSM RadioBlades do not require IP addresses). The following table lists default IP addresses for all chassis boards, RFU backplanes, and the default IP address required for logging in to the RadioFrame System. iRAP default IP addresses are 192.168.200.154 through 192.168.200.254.

Device	Card Type	Chassis Slot/Port	IP Address	
Laptop	N/A	N/A	192.168.200.	4
BCU	BLIC	Slot 0	192.168.200.	5
	BPC	Slot 1	192.168.200.	6
	BPC	Slot 2	192.168.200.	7
	BPC	Slot 3	192.168.200.	8
	DLC	Slot 3 (rear)		
ACU-1	RIC	Slot 0	192.168.200.	10
	APC	Slot 1	192.168.200.	11
	APC	Slot 2	192.168.200.	12
	APC	Slot 3	192.168.200.	13
	RFU-1	PERTM Port 1	192.168.200.	90
	RFU-2	PERTM Port 2	192.168.200.	91
	RFU-3	PERTM Port 3	192.168.200.	92
	RFU-4	PERTM Port 4	192.168.200.	93
	RFU-5	PERTM Port 5	192.168.200.	94
	RFU-6	PERTM Port 6	192.168.200.	95
	RFU-7	PERTM Port 7	192.168.200.	96
	RFU-8	PERTM Port 8	192.168.200.	97
ACU-2	RIC	Slot 0	192.168.200.	20
	APC	Slot 1	192.168.200.	21
	APC	Slot 2	192.168.200.	22
	APC	Slot 3	192.168.200.	23
	RFU-1	PERTM Port 1	192.168.200.	98
	RFU-2	PERTM Port 2	192.168.200.	99
	RFU-3	PERTM Port 3	192.168.200.	100

Device	Card Type	Chassis Slot/Port	IP Address	
	RFU-4	PERTM Port 4	192.168.200.	101
	RFU-5	PERTM Port 5	192.168.200.	102
	RFU-6	PERTM Port 6	192.168.200.	103
	RFU-7	PERTM Port 7	192.168.200.	104
	RFU-8	PERTM Port 8	192.168.200.	105
ACU-3	RIC	Slot 0	192.168.200.	30
	APC	Slot 1	192.168.200.	31
	APC	Slot 2	192.168.200.	32
	APC	Slot 3	192.168.200.	33
	RFU-1	PERTM Port 1	192.168.200.	106
	RFU-2	PERTM Port 2	192.168.200.	107
	RFU-3	PERTM Port 3	192.168.200.	108
	RFU-4	PERTM Port 4	192.168.200.	109
	RFU-5	PERTM Port 5	192.168.200.	110
	RFU-6	PERTM Port 6	192.168.200.	111
	RFU-7	PERTM Port 7	192.168.200.	112
	RFU-8	PERTM Port 8	192.168.200.	113
ACU-4	RIC	Slot 0	192.168.200.	40
	APC	Slot 1	192.168.200.	41
	APC	Slot 2	192.168.200.	42
	APC	Slot 3	192.168.200.	43
	RFU-1	PERTM Port 1	192.168.200.	114
	RFU-2	PERTM Port 2	192.168.200.	115
	RFU-3	PERTM Port 3	192.168.200.	116
	RFU-4	PERTM Port 4	192.168.200.	117
	RFU-5	PERTM Port 5	192.168.200.	118
	RFU-6	PERTM Port 6	192.168.200.	119
	RFU-7	PERTM Port 7	192.168.200.	120
	RFU-8	PERTM Port 8	192.168.200.	121
ACU-5	RIC	Slot 0	192.168.200.	50
	APC	Slot 1	192.168.200.	51
	APC	Slot 2	192.168.200.	52

Device	Card Type	Chassis Slot/Port	IP Address	
	APC	Slot 3	192.168.200.	53
	RFU-1	PERTM Port 1	192.168.200.	122
	RFU-2	PERTM Port 2	192.168.200.	123
	RFU-3	PERTM Port 3	192.168.200.	124
	RFU-4	PERTM Port 4	192.168.200.	125
	RFU-5	PERTM Port 5	192.168.200.	126
	RFU-6	PERTM Port 6	192.168.200.	127
	RFU-7	PERTM Port 7	192.168.200.	128
	RFU-8	PERTM Port 8	192.168.200.	129
ACU-6	RIC	Slot 0	192.168.200.	60
	APC	Slot 1	192.168.200.	61
	APC	Slot 2	192.168.200.	62
	APC	Slot 3	192.168.200.	63
	RFU-1	PERTM Port 1	192.168.200.	130
	RFU-2	PERTM Port 2	192.168.200.	131
	RFU-3	PERTM Port 3	192.168.200.	132
	RFU-4	PERTM Port 4	192.168.200.	133
	RFU-5	PERTM Port 5	192.168.200.	134
	RFU-6	PERTM Port 6	192.168.200.	135
	RFU-7	PERTM Port 7	192.168.200.	136
	RFU-8	PERTM Port 8	192.168.200.	137
ACU-7	RIC	Slot 0	192.168.200.	70
	APC	Slot 1	192.168.200.	71
	APC	Slot 2	192.168.200.	72
	APC	Slot 3	192.168.200.	73
	RFU-1	PERTM Port 1	192.168.200.	138
	RFU-2	PERTM Port 2	192.168.200.	139
	RFU-3	PERTM Port 3	192.168.200.	140
	RFU-4	PERTM Port 4	192.168.200.	141
	RFU-5	PERTM Port 5	192.168.200.	142
	RFU-6	PERTM Port 6	192.168.200.	143
	RFU-7	PERTM Port 7	192.168.200.	144
	RFU-8	PERTM Port 8	192.168.200.	145

Device	Card Type	Chassis Slot/Port	IP Address	
ACU-8	RIC	Slot 0	192.168.200.	80
	APC	Slot 1	192.168.200.	81
	APC	Slot 2	192.168.200.	82
	APC	Slot 3	192.168.200.	83
	RFU-1	PERTM Port 1	192.168.200.	146
	RFU-2	PERTM Port 2	192.168.200.	147
	RFU-3	PERTM Port 3	192.168.200.	148
	RFU-4	PERTM Port 4	192.168.200.	149
	RFU-5	PERTM Port 5	192.168.200.	150
	RFU-6	PERTM Port 6	192.168.200.	151
	RFU-7	PERTM Port 7	192.168.200.	152
	RFU-8	PERTM Port 8	192.168.200.	153
RAP-1	N/A	N/A	192.168.200	154
RAP-2	N/A	N/A	192.168.200	155
RAP-3	N/A	N/A	192.168.200	156
				.
				.
RAP-100				254

Appendix E Connecting to the RFS

To connect to the RFS, you need a workstation (a PC or laptop computer). This section describes how to configure the workstation and connect it to the RFS.

Connect the Workstation to the NCU

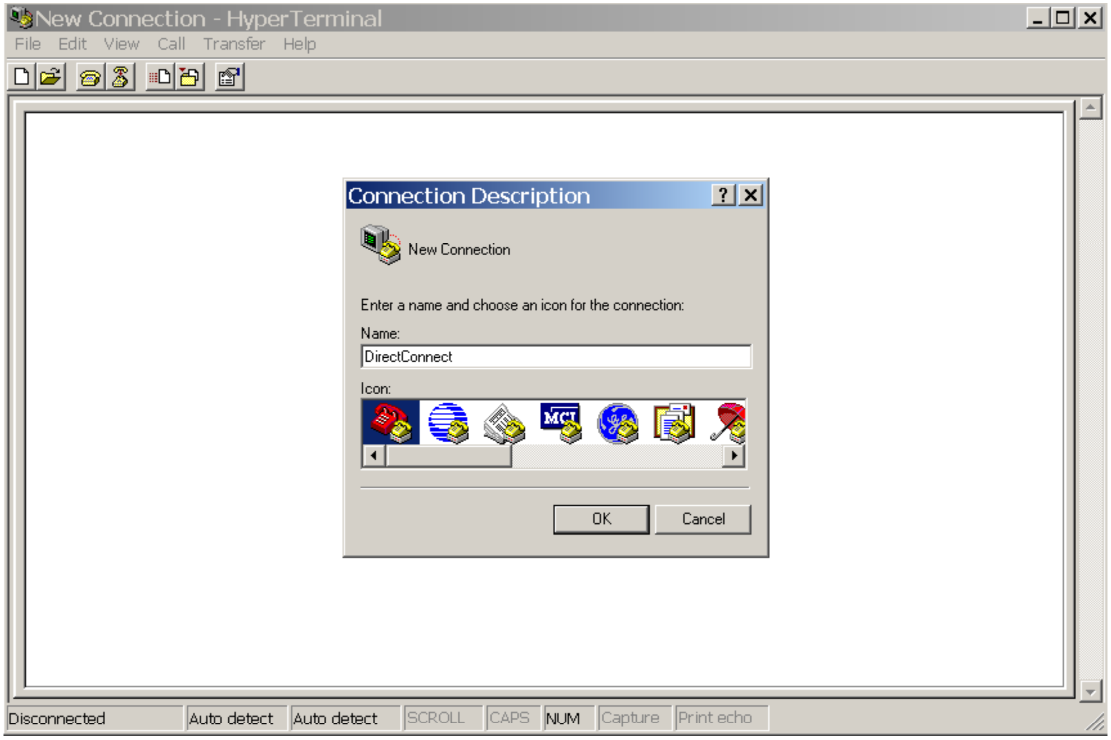
1 Configure the IP address of the workstation's (PC or laptop computer) Ethernet port as 192.168.200.4, and the subnet mask to 255.255.255.0.

2 Connect an Ethernet cable from the workstation Ethernet port to the NCU RLIC using Ethernet port 2-7 (do not use Port 1, which is configured for iSC communications, or Port 8, which is reserved for maintenance purposes).

3 Connect a serial cable between the PC serial port and the DB9 connector on the NCU CRIC.

4 Start a HyperTerm session on the PC (or an equivalent terminal emulation program, such as TeraTerm or Procomm).

5 For **Name**, enter a name for the connection, and then select **OK** (see the following illustration).



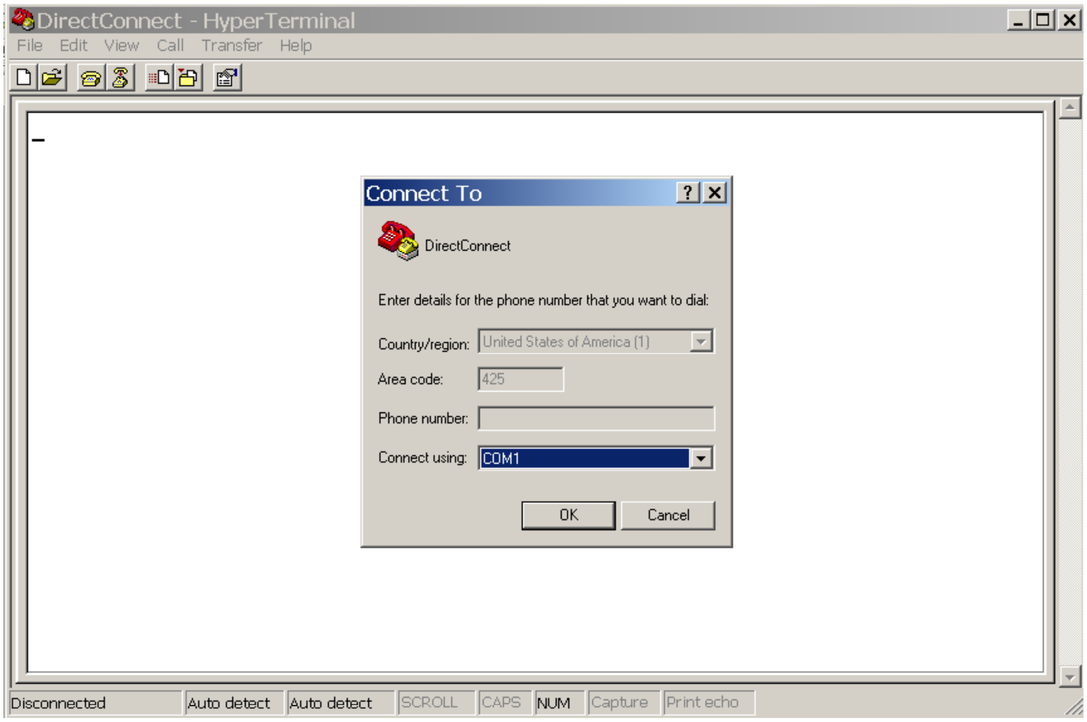
Connection Description

New Connection

Enter a name and choose an icon for the connection:

Name: DirectConnect

6 For **Connect using**, select the COM port to which the serial cable is connected on the PC (the default is COM1), and then select **OK**.



DirectConnect

Enter details for the phone number that you want to dial:

Country/region: United States of America (1)

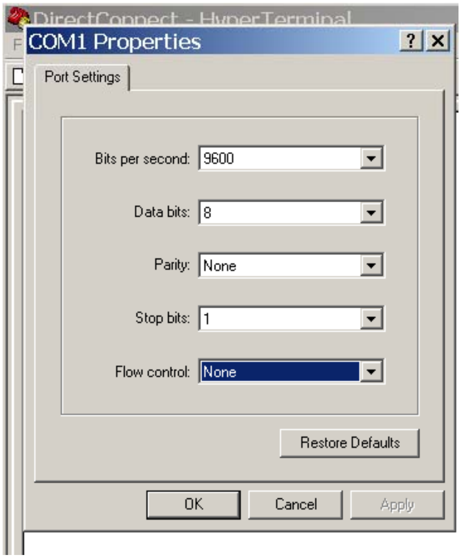
Area code: 425

Phone number:

Connect using: COM1

7 On the **COMx Properties** page, make the settings shown in the following illustration, and then select **OK**.

The prompt “→” appears, indicating that the serial connection setup is complete.



Bits per second: 9600

Data bits: 8

Parity: None

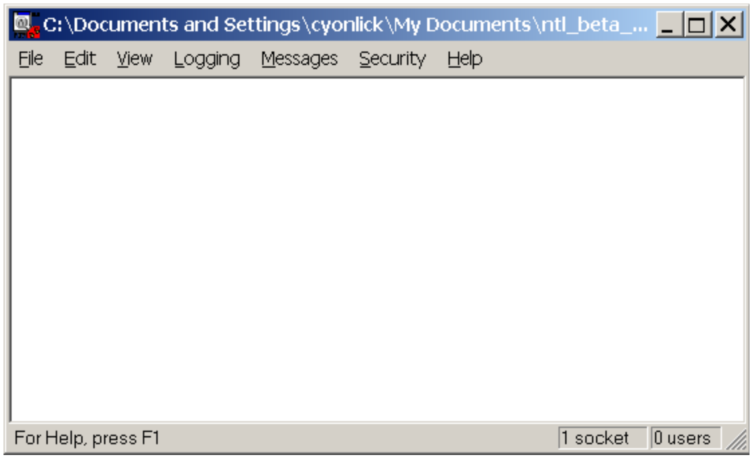
Stop bits: 1

Flow control: None

Configure the FTP Software

FTP (file transfer protocol) server software is required on the workstation. System Manager uses the FTP protocol as the mechanism to transfer files from the workstation to the RFN system. The FTP Server software can be obtained via the World Wide Web at http://www.wftpd.com.

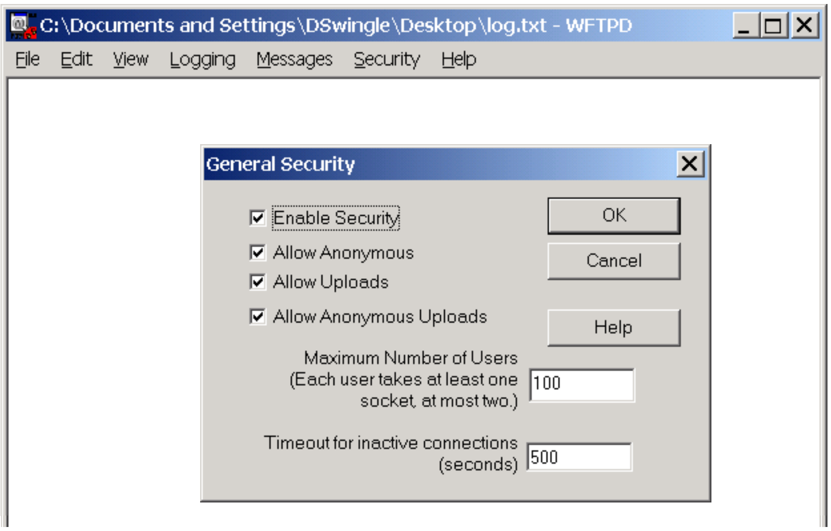
1 Open FTP Server (wftpd32.exe). The following configuration is for WFTPD.



2 In the **HyperTerm** session, type **LL** and press **Return** to verify that the FTP server is up and running.

You should see a list of files in the C:\ directory for the user 'board'. If the FTP server is not running, you'll get an error message, or 'value =', or both.

3 From the **Security menu**, select **General**, configure the General Security page as shown, and then select **OK**.



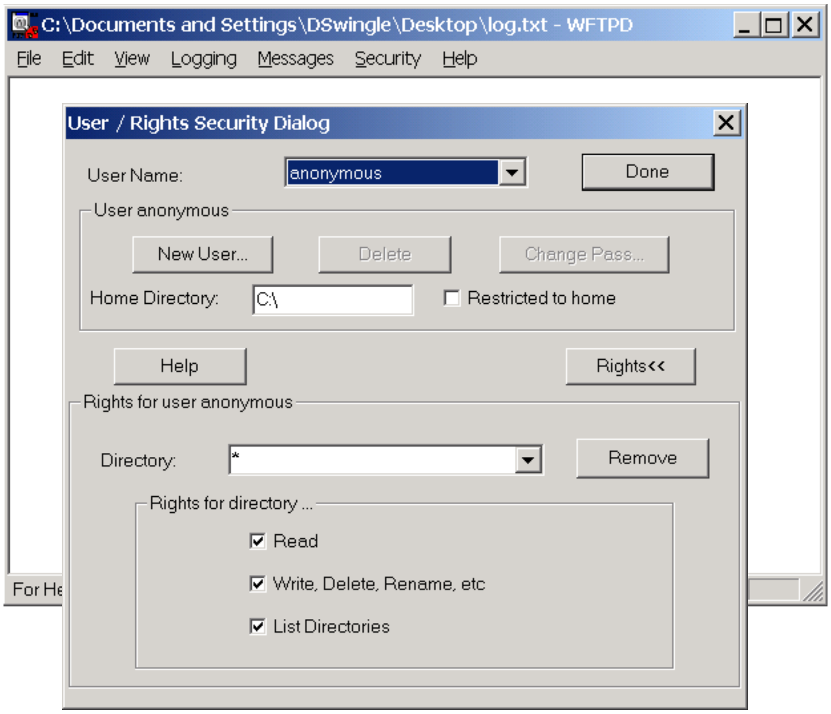
☑ Enable Security
☑ Allow Anonymous
☑ Allow Uploads
☑ Allow Anonymous Uploads

Maximum Number of Users (Each user takes at least one socket, at most two.) 100

Timeout for inactive connections (seconds) 500

4 From the **Security menu**, select **User/rights**, and for **User Name**, select **anonymous** from the drop down menu.

5 Select the **Rights** button and verify that the settings are the same as shown below.


C:\Documents and Settings\DSwingle\Desktop\log.txt - WFTPD
File Edit View Logging Messages Security Help
User / Rights Security Dialog
Done
New User...
Delete
Change Pass...
Help
Rights<<
Remove
For He

User Name: anonymous

User anonymous

Home Directory: C:\

☐ Restricted to home

Rights for user anonymous

Directory: *

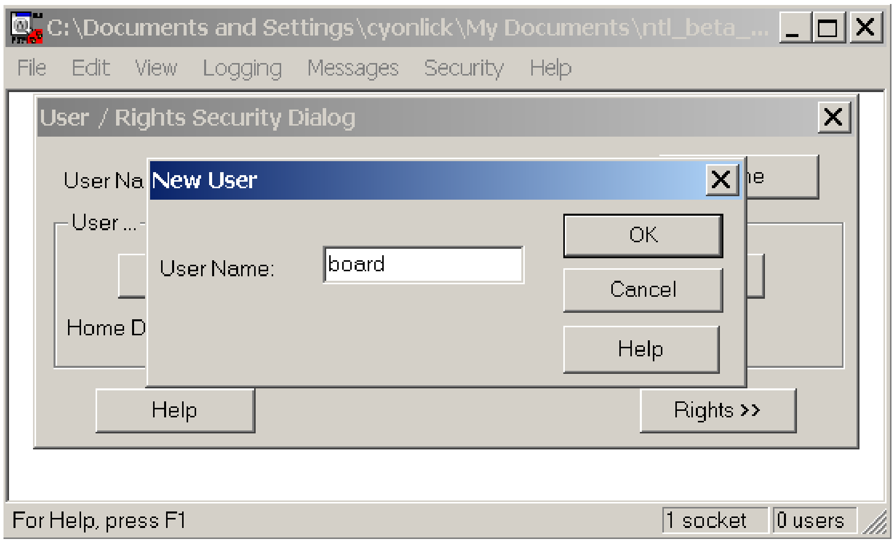
Rights for directory ...

☑ Read

☑ Write, Delete, Rename, etc

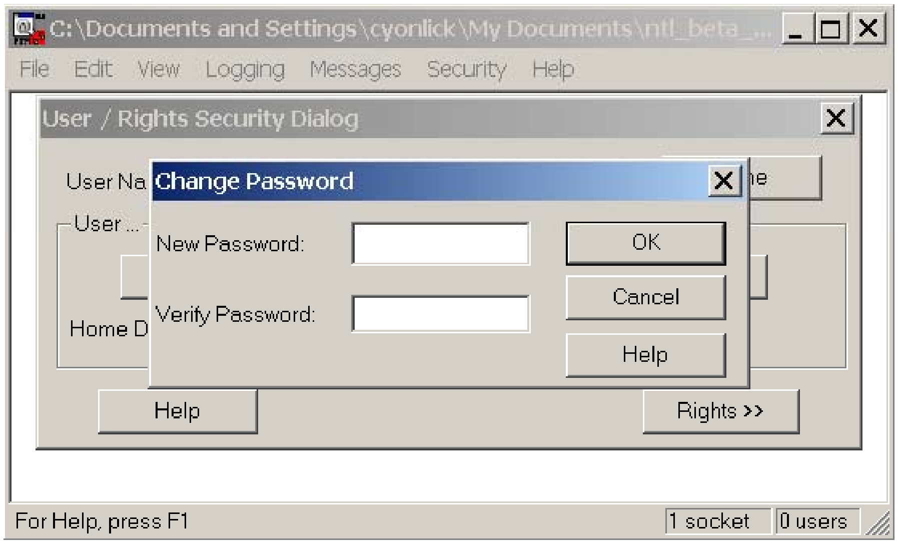
☑ List Directories

6 Select the **New User…** button, and then for **User Name**, type **board** in the text box, and then select **OK**.

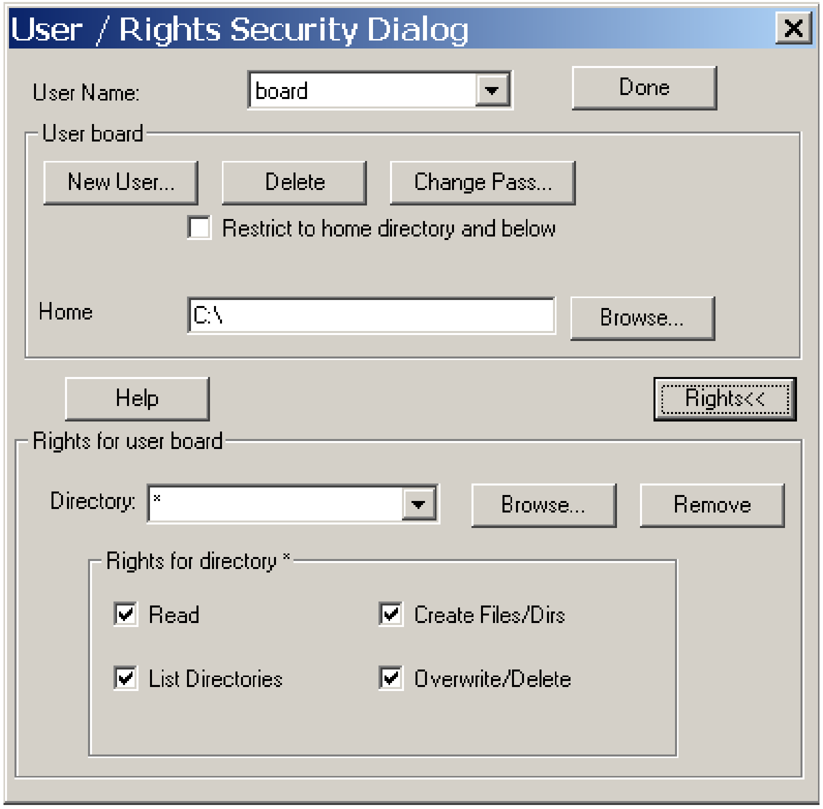

C:\Documents and Settings\cyonlick\My Documents\ntl_beta_...
File Edit View Logging Messages Security Help
User / Rights Security Dialog
User Na
User ...
Home D
ne
Help
Rights >>
New User
OK
Cancel
Help
For Help, press F1
1 socket
0 users

User Name: board

7 For **New Password** type **wind**, then retype wind in the **Verify Password** text box, and sthen select **OK**.



8 The User/Rights Security dialog box reappears, and the **User Name** is now set to **board**. Select the **Rights** button and verify that the settings are the same as shown below, and then select **Done**.



User Name: board

User board

☐ Restrict to home directory and below

Home C:\

Rights for user board

Directory: *

Rights for directory *

☑ Read

☑ Create Files/Dirs

☑ List Directories

☑ Overwrite/Delete