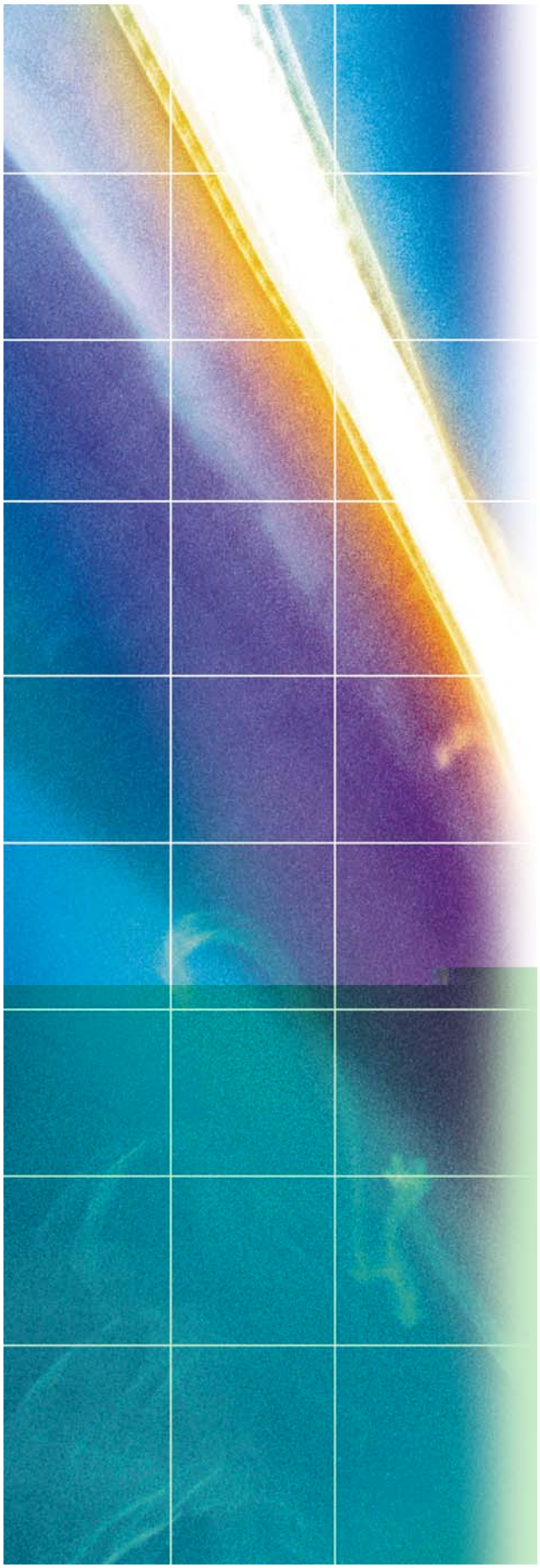


FORTRESS™ TECHNOLOGIES

Fortress Security System

Secure Wireless Access Bridge

User Guide

www.fortresstech.com

Fortress Secure Wireless Access Bridge 2.6.1

DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

FCC EMISSIONS COMPLIANCE STATEMENT

THIS EQUIPMENT HAS BEEN TESTED AND FOUND TO COMPLY WITH THE LIMITS FOR A CLASS A DIGITAL DEVICE, PURSUANT TO PART 15 OF THE FCC RULES. THESE LIMITS ARE DESIGNED TO PROVIDE REASONABLE PROTECTION AGAINST HARMFUL INTERFERENCE WHEN THE EQUIPMENT IS OPERATED IN A COMMERCIAL ENVIRONMENT. THIS EQUIPMENT GENERATES, USES, AND CAN RADIATE RADIO FREQUENCY ENERGY AND, IF NOT INSTALLED AND USED IN ACCORDANCE WITH THE INSTRUCTION MANUAL, MAY CAUSE HARMFUL INTERFERENCE TO RADIO COMMUNICATIONS. OPERATION OF THIS EQUIPMENT IN A RESIDENTIAL AREA IS LIKELY TO CAUSE HARMFUL INTERFERENCE IN WHICH CASE THE USER WILL BE REQUIRED TO CORRECT THE INTERFERENCE AT HIS OWN EXPENSE.

FCC CLASS A WARNING

MODIFYING THE EQUIPMENT WITHOUT FORTRESS AUTHORIZATION MAY RESULT IN THE EQUIPMENT NO LONGER COMPLYING WITH FCC REQUIREMENTS FOR CLASS A DIGITAL DEVICES. IN THAT EVENT, YOUR RIGHT TO USE THE EQUIPMENT MAY BE LIMITED BY FCC REGULATIONS, AND YOU MAY BE REQUIRED TO CORRECT ANY INTERFERENCE TO RADIO OR TELEVISION COMMUNICATIONS AT YOUR OWN EXPENSE.

TO COMPLY WITH FCC RF EXPOSURE COMPLIANCE REQUIREMENTS, THE ANTENNAS USED FOR THESE TRANSMITTERS MUST BE INSTALLED TO PROVIDE A SEPARATION DISTANCE OF AT LEAST 20 CM FROM ALL PERSONS AND MUST NOT BE CO-LOCATED OR OPERATED IN CONJUNCTION WITH ANY OTHER ANTENNA OR TRANSMITTER.

Table of Contents

Chapter 1 Introduction

1.1 Fortress Secure Wireless Access Bridge

The Fortress Secure Wireless Access Bridge is an all-in-one network access device with the most stringent security available today built in. It can serve as a wireless bridge, a WLAN access point, and an eight-port LAN switch, while performing all the functions of a Fortress controller device: encrypting wireless traffic and providing Multi-factor Authentication for devices on the network it protects.

The rugged, compact chassis is uniquely designed, acting as an external heat sink to eliminate the need for fans and filters. The Bridge can be used indoors or outdoors with the Mast-Mounting and Weatherizing kits that ship with every device.

The Bridge can be quickly and transparently integrated into an existing network. It can be powered with standard AC current or as an Ethernet powered device (PD) through its WAN port, which supports power over Ethernet (PoE).

Once it is installed and configured, operation is automatic, requiring no administrator intervention as it protects data transmitted on WLANs and between WLAN devices and the wired LAN.

1.1.1 Management Interfaces

The Bridge can be administered through either of two native management tools: the Bridge GUI or Bridge CLI. The Bridge also supports Simple Network Management Protocol (SNMP).

1.1.1.1 Bridge GUI

The Bridge's graphical user interface is a browser-based management tool that provides administration and monitoring functions in a menu- and dialog-driven format. It is accessed over the network via the Bridge's IP address. The Bridge supports Microsoft® Internet Explorer and Mozilla Firefox™.

1.1.1.2 Bridge CLI

The Bridge's command-line interface provides administration and monitoring functions via a command line. It is accessed over the network via the Bridge's IP address or through a terminal connected directly to the Bridge's serial **Console** port.

1.1.1.3 SNMP

The Bridge supports versions 1 and 2 of the Simple Network Management Protocol (SNMP) Internet standard for network management. The Fortress Management Information Base (MIB) is included on the Bridge CD and available from: **www.fortresstech.com/support/products_updates.asp**.

NOTE: You cannot configure SNMP management on a Fortress Bridge in *FIPS* operating mode (the default).

1.2 Network Security Overview

Network security measures take a variety of forms; key components include:

- *Access controls* prevent unwanted users and devices from connecting to the network. Typically some form of ***authentication*** is required, in which credentials are validated before a connection is allowed. Additionally, ***policy*** can be applied to determine what on the network the authenticated user or device can access, when, and with what permissions.
- *Privacy,* or *confidentiality,* implementations prevent information from being derived from intercepted network traffic through the use of data ***encryption***, and guard against network tampering by checking the ***integrity*** of transmitted data.

1.3 The Fortress Security System

The Fortress Security System applies a combination of established and unique methodologies to both network access and data privacy.

1.3.1 Multi-factor Authentication™

Fortress guards the network against illicit access with Multi-factor Authentication: checking three levels of access credentials before allowing a connection.

1) *Network authentication* mandates that connecting devices use the correct shared identifier for the network. The Fortress Security System requires all members of a secure network to authenticate with the correct *Access ID*.
2) *Device authentication* mandates that a connecting device is individually recognized on the network through its unique device identifier. The Fortress Security System requires each device to authenticate on the secure network with the unique *Device ID* generated for that device.

3) *User authentication* requires the user of a connecting device to enter a recognized user name and valid credentials, a password, for example, or a digital certificate. The Fortress Security System can authenticate users locally or through existing user-authentication provisions.

1.3.2 Strong Encryption at the MAC Layer

Fortress ensures network privacy at the Media Access Control (MAC) sublayer, within the Data Link Layer (Layer 2) of the Open System Interconnection (OSI) networking model. This allows a transmission's entire contents, including the IP address and any broadcast messages, to be encrypted. Additionally, Fortress supports the FIPS-validated encryption algorithm: AES-128/192/256.

1.3.3 System Components

The Fortress Security System comprises three components:

- A Fortress controller device (Gateway/Controller/Bridge) provides internal network security by bridging encrypted wired or wireless communications to the wired LAN or by remotely bridging point-to-point or -multipoint LAN and WLAN connections.
- The Fortress Secure Client provides device security and secure wireless connectivity for mobile devices connected to networks protected by a Fortress controller device.
- Fortress Management and Policy Server (MaPS™) provides centralized management of network devices and resources, as well as rules-based access control and network, device and user authentication, by itself or integrated with back-end corporate authentication servers.

1.3.4 Operating Modes

The Fortress Security System can be operated in either of two, mutually exclusive modes.

1.3.4.1 Normal Operating Mode

In *Normal* operating mode, the Fortress Security System provides the highest available level of network security, without the additional safeguards Federally mandated for some government networks. *Normal* mode of operation is generally more than adequate for even the most stringent security and privacy requirements in unregulated environments.

1.3.4.2 FIPS Operating Mode

In *FIPS* mode, the Fortress Security System complies fully with the Federal Information Processing Standards (FIPS) 140-2 standard for cryptographic products. Because of its added administrative complexities, however, *FIPS* mode is recommended only for networks that explicitly require FIPS compliance.

1.3.5 Deployment Options

The Fortress Security System is flexible and expandable.

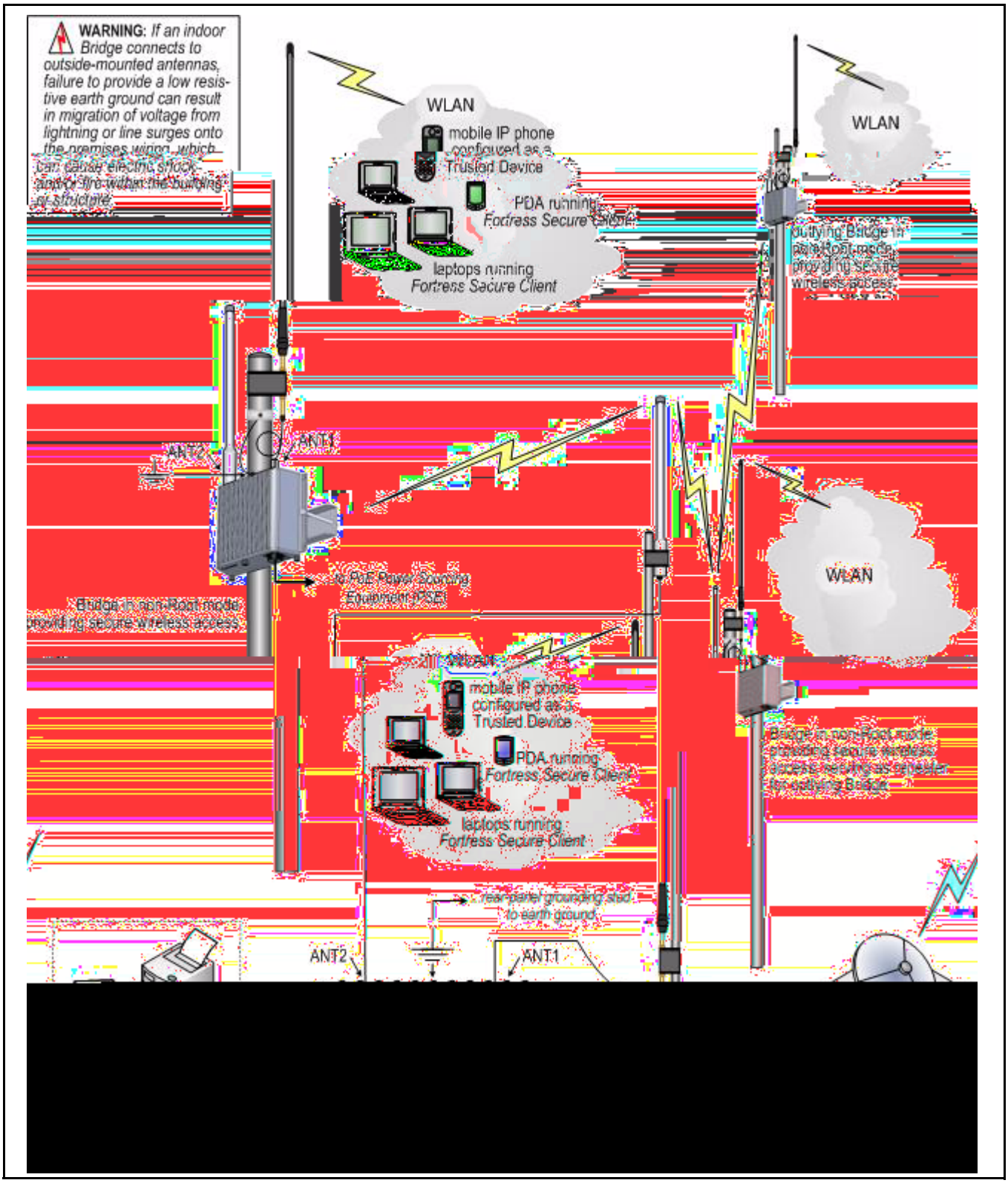


Figure 1.1 Example Point-to-Multipoint Deployment of the Fortress Secure Wireless Access Bridge

The Bridge can provide a secure edge for a WLAN (or infrastructure-mode) deployments, as shown in Figure 1.1

1.4 This Document

This user guide assumes its users have a level of expertise consistent with a professional Network Administrator.

1.4.1 Document Conventions

This is a task-oriented document, and the procedures it contains are, wherever possible, self-contained and complete in themselves. Internal cross references do appear, however, rather than verbatim repetition.

Introductory matter before numbered steps will generally contain information necessary to the successful completion of the task. Descriptive matter below a stepped procedure may add to your understanding, but is not essential to the task.

Side notes throughout this document are intended to alert you to particular kinds of information, as visually indicated by their icons. Examples appear to the right of this section, in descending order of urgency.

WARNING: can cause physical injury or death to you and/or your equipment.

CAUTION: can corrupt your network, your data or an intended configuration result.

NOTE: may assist you in executing the task, e.g. a convenient software feature or notice of something to keep in mind.

1.4.2 Related Documents

A printed Fortress *Secure Wireless Access Bridge Quick Start Guide* was included with your shipment.

For guidance on the Fortress Secure Client, please refer to your Fortress Secure Client user guide.

Chapter 2
Installation

2.1 Introduction

The Fortress Secure Wireless Access Bridge is a full-featured Fortress controller device, providing strong data encryption and Multi-factor Authentication™, including native RADIUS authentication, to users and devices on the network it secures.

The Bridge additionally comprises three, independent network components that can be employed alone or simultaneously in any combination:

1. *Radio 1* is a tri-band 802.11a/b/g radio that can be configured to use either the 802.11b/g band or the 802.11a band. It can function as a wireless access point (AP), providing secure WLAN connectivity to wireless devices within range, or as a wireless bridge in a point-to-point or point-to-multipoint network.
2. *Radio 2* is fixed on the 802.11a band. As the higher powered of the two radios, it would normally be the first choice for the bridging function in a mixed AP/wireless bridge deployment, but it can equally function as an 802.11a AP.
3. The eight RJ-45 10/100 Mbps Auto-MDIX Ethernet ports (labeled **1-8**) are connectors for the Bridge's internal LAN switch.

The Bridge is also an 802.3af power-over-Ethernet (PoE) powered device (PD), drawing power through its WAN port, when that port is connected to 802.3af power sourcing equipment (PSE).

NOTE: Only essential configuration settings, as required for basic installation, are covered in this chapter. The full complement of Bridge configuration options is described in the following chapter, Bridge Administration.

NOTE: The internal LAN does not support NAT (network address translation).

2.1.1 System Requirements

To display properly, the Bridge GUI requires a monitor resolution of at least 1024 × 768 pixels and the following (or later) browser versions:

- Microsoft® Internet Explorer 6.0
- Mozilla Firefox™ 1.5

2.1.2 Compatibility

The Fortress Bridge is fully compatible with Fortress Secure Client versions 2.4 and higher.

2.2 Preparation

2.2.1 Shipped and Optional Parts

Included in each Fortress Bridge shipment are:

- Fortress Secure Wireless Access Bridge, comprising:
  - one eight-port Ethernet LAN switch
  - one PoE Ethernet WAN port
  - two USB ports
  - one 802.11 a/b/g multi-mode radio
  - one 802.11a radio
  - two lightning arrestor modules
- one universal AC-to-48V DC power adapter
- AC power cord
- one EBU-101-01 PoE adapter[1]
- one RJ-45-to-DB9 adapter
  (for use with a standard, straight-through CAT5 assembly)
- ES520 Weatherizing Kit, including:
  - one front-panel cover plate
  - one RJ-45 connector boot assembly (six pieces)
  - one antenna port cap
- ES520 Mast-Mounting Kit, including:
  - one mast mounting bracket
  - two 4" long, fully threaded 1/4-20 hex bolts
  - two 1/4" split lock washers

Optionally, you can purchase from Fortress Technologies:

- 5.*x* GHz 9dBi omnidirectional antenna with an N-type male direct connector
- 2.4–2.485 GHz 9dBi omnidirectional antenna with an integrated 2' antenna cable terminating in an N-type male connector
- 802.11a/b/g 2/2dBi tri-band rubber duck antenna with an RP-TNC connector and RP-TNC-to-N-type male connector adapter

The availability and specifications of antennas offered for purchase from Fortress Technologies are subject to change. Contact your Fortress representative for details and pricing.

1. In outdoor installations, it is mandatory that the Bridge be powered with the EBU-101-01 PoE adapter (or equivalent).

2.2.2 Preparing the Network

Any Ethernet device—including hubs, switches and access points—directly connected to the Bridge must have auto-negotiation capability (and have the feature enabled), or link and/or packet loss could result. Refer to a device's documentation to configure its negotiation options.

Secure Clients (and other Fortress Bridges) in communication with the Fortress Bridge must use the same encryption algorithm and must be assigned the same Access ID (as established in Step 5 of Section 2.4.2).

NOTE:

- ***General:*** This equipment must be installed by qualified service personnel according to the applicable installation codes. Do not locate the Bridge or antennas near power lines or power circuits. When installing an external antenna, take extreme care not to come into contact with such circuits as they can cause serious injury or death. Avoid metal ladders wherever possible. For proper installation and grounding, refer to national and/or local codes (WSNFPA 70 or, Canadian Electrical Code 54).
- ***Indoor/Outdoor Siting:*** The Secure Wireless Access Bridge, with or without externally sited antennas, is intended only for installation in Environment A as defined in IEEE 802.3.af. All interconnected equipment connected to the indoor/outdoor Bridge must be contained within the same building, including the interconnected equipment's associated LAN connections.

  In outdoor environments, the Secure Wireless Access Bridge shall be mounted on a wall, pole, mast or tower using the included mounting bracket. When mounted outside, the Bridge's Front Panel Cover Plate (included) provides the necessary water and dust resistance to environmentally protect the unit. In addition, the three Front Panel Cover Plate thumbscrews must be hand-tightened (taking care not to over-tighten) to prevent the operator-access area (USB, Console, Ethernet ports, and power inlets) from being exposed. The Bridge should not be used outside a home, school, or other public area where the general population has access to it.

  When sited inside, the unit is powered within SELV low voltage safety limits with 48VDC PoE or 48VDC external power. The included front-panel cover plate is not required for indoor installations.
- ***Ambient Temperature:*** The temperature of the environment in which the Bridge operates should not exceed the maximum (122º F/50º C) or drop below the minimum (14º F/-10º C) operating temperatures.
- ***Powering:*** *For external environments,* the Bridge WAN (PoE-PD) port ***must*** be PoE powered with the included EBU101-01 adapter (or equivalent). The PoE adapter ***must*** derive power from the included Fortress AC-to-48V DC (70 Watt) power source to meet the safety isolation requirements defined in UL 60950. The PoE adaptor is designed for indoor use only. Never mount the power injector outside with the Secure Wireless Access Bridge.

  For internal environments, the Bridge can be 1) direct powered by the universal AC-to-48V DC (70 Watt) power adapter, 2) PoE powered over the WAN port with the included EBU101-01 POE adapter (or equivalent), or 3)

WARNING: The Bridge contains a 3V (7 year) lithium battery for time-keeping purposes. It is *not* intended to be operator- or user-replaceable. To avoid risk of personal injury (and voiding of the Bridge's warranty), refer all hardware servicing to Fortress Technical Support. *There is a risk of explosion if the battery is replaced by an incorrect type.* Dispose of used batteries according to the new battery disposal instructions.

WARNING: To avoid the risk of severe electrical shock, never remove the cover, an exterior panel, or any other part of the Bridges's chassis. There are no user-serviceable parts inside. Refer all hardware servicing to Fortress Technical Support.

PoE powered from a remote 802.11af (13 Watt) PoE midspan source.

- ***Circuit Overloading:*** The Bridge includes a 48 V main resettable fuse specified at 1.8 A.
- ***Lightning/Electrostatic Protection:*** The Bridge's antenna ports conform to IEC1000-4-5 10 KV 8/20us waveform. The WAN port conforms to IEC-61000-4-2 8 KV waveform with 58 V additional transient protection.
- ***Grounding:*** The Bridge features a rear panel grounding stud which, on Bridges with externally mounted antennas, must be connected to protective earth ground via a 20 gauge (minimum) cable, before any other physical connection is made.

  The antenna/cable distribution system should be grounded (earthed) in accordance with ANSI/NFPA 70, the National Electrical Code (NEC), in particular, Section 820.93, Grounding of Outer Conductive Shield of a Coaxial Cable.

  The antenna mast and Secure Wireless Access Bridge, when used outside, should be grounding per Article 810 of the NEC; of particular note is the requirement that the grounding conductor not be less than 10 AWG(Cu).
- ***Cabling:*** Cables must be installed in accordance with NEC Article 725 and 800, and all requirements must be met in relationship to clearances with power lines and lighting conductors. All cabling must be category 5e per TIA/EIA-568-B.2.
- ***Waterproofing:*** The Bridge has a UL (NEMA) 3/3S/4 raintight rating. The Front-panel Cover Plate of the ES520 Weatherizing Kit includes a "Raintight" label. The Bridge is water resistant when the Weatherizing Kit (cover plate, WAN-port RJ-45 connector boot assembly, and antenna cap—included) is properly installed.
- ***Radio Frequency:*** The Bridge's internal radios conform to the FCC's safety standard for human exposure to RF electromagnetic energy, provided that you follow these guidelines:
  - Do not touch or move the antennas while the unit is transmitting or receiving.
  - To safeguard Bridge transmitting circuitry, relocate the Bridge and its antennas only when the Bridge is powered off.
  - When the Bridge is transmitting, do not hold it so that the antenna is very close to or touching any exposed parts of the body, especially the face or eyes.

WARNING: If the Bridge connects to outside-mounted antennas, failure to provide a low resistive earth ground can result in migration of voltage from lightning or line surges onto the premises wiring, which can cause electric shock and/or fire within the building or structure.

- Antennas must be installed to provide a separation of at least 20 cm (7.9") from all persons and any co-located antenna or transmitter.
- Regarding use in specific environments: *• Do not operate near unshielded blasting caps or in an explosive environment. • Limit use in a hazardous location to the constraints imposed by the location's safety director. • Abide by the rules of the Federal Aviation Administration for the use of wireless devices on airplanes. • Restrict the use of wireless devices in hospitals to the limits set forth by each hospital.*

NOTE: The ES520 complies with UL60950-1 safety specifications. It has a UL (NEMA) 3/3S/4 (and IEC60529) environmental rating. The Front-panel Cover Plate of the ES520 Weatherizing Kit includes a "Raintight" label.

2.3 Installation Instructions

The following instructions assume that you are installing the Fortress Bridge with the minimum number of possible changes to its default configuration:

- The Fortress Bridge will operate in *Normal* operating mode.
- Radio 1 will be used, in the 802.11g band, as a WLAN access point (AP) for wireless devices within range, and it will transmit and receive on channel 1.
- Radio 2 will be used for bridging in a point-to-point or point-to-multipoint deployment of multiple Fortress Bridges, and it will transmit and receive on channel 149, with a distance setting of 1 mile.
- *STP* (Spanning Tree Protocol) is enabled on the Bridge, and *Multicast* is enabled on the non-root Bridge(s).
- In indoor deployments, the Bridge's internal LAN switch will be used to connect a local area network.

Complete configuration guidelines, covering the full set of Fortress Bridge functions and options, are provided in Chapter 3, Configuration.

Procedures differ between indoor and outdoor installations. Refer to the instructions that apply to your deployment.

2.4 Outdoor Installation

NOTE: Third party antennas are subject to local regulatory requirements. For outdoor installations, they must be waterproof.

When installing the Fortress Bridge outdoors, you *must* use the Mast-Mounting Kit and the Weatherizing Kit—both included in every shipment—to mount and weatherize the Bridge.

When the Weatherizing Kit is installed, the only available connections to the Bridge are the front-panel WAN port and the rear-panel antenna ports.

Before installing the Bridge in a hard-to-reach, outdoor location, Fortress recommends connecting and preconfiguring the Bridge.

2.4.1 Connecting the Bridge for Preconfiguration

1. Position the Bridge so that it operates only within its safe temperature range (14º–122º F/–10º–50º C).
2. Connect a waterproof, standard 802.11a/b/g-capable antenna with an N-type male connector to antenna port 1 (**ANT1**).
3. Connect an antenna cable with an N-type male connector between antenna port 2 (**ANT2**) and a high-gain omnidirectional or directional antenna. The antenna and cable must be waterproof.
4. Connect the Bridge's **WAN** port to an external 802.3af PSE/PoE (Power Sourcing Equipment/Power over Ethernet) source, which—if the WAN port will connect to a satellite link or a DSL or cable modem—provides an in-line connection to the necessary network device.

   (Outdoor Bridge installations require a PoE source; the 48V power inlet cannot be connected when the Weatherizing Kit is installed.)
5. Connect one of the Bridge's Auto-MDIX Ethernet LAN ports (numbered **1**–**8**) to a computer or switch on the wired LAN.
6. Verify that all link/activity and power LEDs illuminate for all connected ports.

WARNING: To comply with FCC rules, *antennas must be professionally installed*. Improperly grounded outdoor antennas pose a particularly serious safety hazard.

CAUTION: The FCC requires co-located radio antennas to be at least 7.9" apart. The Bridge's antenna connectors are only 5" apart. *Avoid directly mounting two antennas to the Bridge's rear-panel connectors.*

2.4.2 Preconfiguring the Bridge for Outdoor Operation

The computer through which you configure the Bridge must have a direct (non-routed) connection to the Bridge's unencrypted interface and an IP address in the same subnet (192.168.254.0) as the Controller's default IP address.

1 Open a browser application on a computer on your LAN and, in the browser address field, enter the Bridge's default IP address: `192.168.254.254`.

2 Log on to the Bridge GUI, entering `admin` as both *User ID* and *Password* and then clicking **Login**.

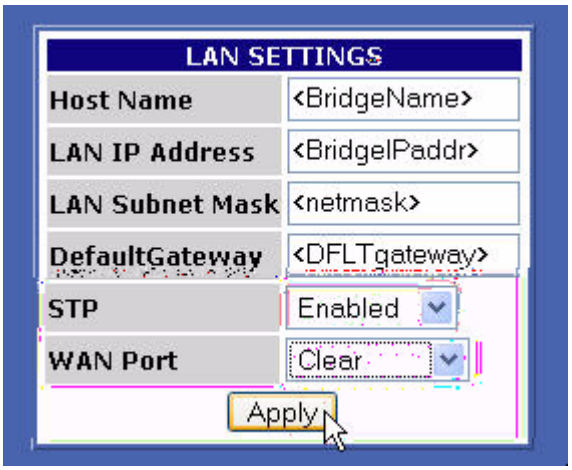
(When prompted, agree to accept the security certificate.)

3 From the main menu on the left choose **LAN SETTINGS**, and on the *LAN SETTINGS* screen*:*

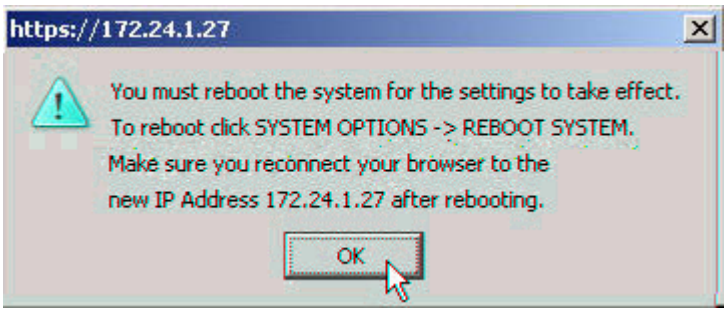
- In *Host name*, enter a descriptive name for the Fortress Bridge.
- In *LAN IP address*, enter a network address for the Fortress Bridge's management interface (the address to be used for all subsequent administrative access to the Bridge).
- In *LAN Subnet mask*, enter the correct subnet mask for the Bridge's IP address.
- In *Default gateway*, enter the IP address of the default gateway (or router) for the network on which you are installing the Bridge.
- If the WAN port is connected to a satellite link or a DSL or cable modem, select **Clear** for *WAN Port*.

NOTE: The IP address must be unique on the network.

NOTE: For information about the Bridge's *STP* and *WAN Port* encryption features refer to Section 3.2.



Click **Apply**.

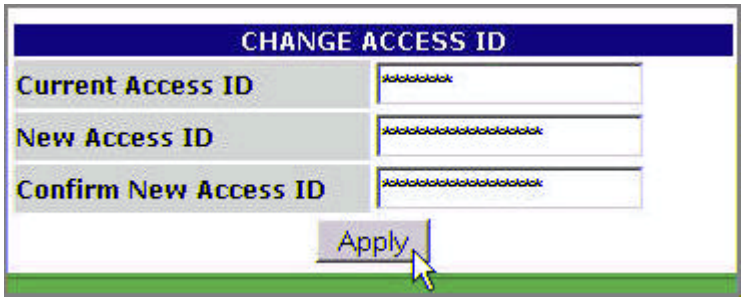


4 Click **OK** to clear the system dialog that instructs you to reboot, but do not reboot until Step 10 of these procedures, when you are again instructed to do so.

5 From the main menu, select **SECURITY SETTINGS**, and on the *SECURITY SETTINGS* screen, in the *CHANGE ACCESS ID* section:

- In *Current Access ID* enter 16 zeros or the word **`default`**.
- In *New Access ID* enter the 16-digit hexadecimal Access ID to be used by the Bridge and its Secure Clients.
- In the *Confirm New Access ID* field, re-enter the new Access ID to ensure against entry errors.

detail:



Click **Apply**.

CAUTION: For security reasons, the Access ID in effect on the Bridge cannot be displayed. *Make a note of the new Access ID:* you will need it to configure the Bridge's Secure Clients, as well as to change the Access ID on the Bridge.

6 From the main menu on the left choose **BRIDGE PASSWORD**, and on the *BRIDGE PASSWORD* screen*:*

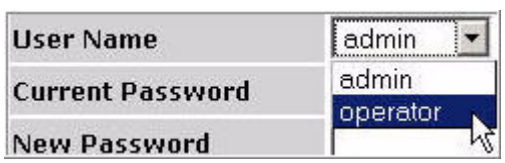
- Leave *User Name* at its default setting, **admin**.
- In *Current Password*, enter the default system administrator password: **`admin`**.
- In *New Password*, enter the password to be used to access administrative functions on the Bridge GUI.
- In *Confirm New Password*, re-enter the new password.

Click **Apply**.

CAUTION: The Bridge is *not* secure until you have changed the default Access ID and wireless SSIDs and reset both GUI passwords and the CLI password to a minimum of eight, mixed alphanumeric, upper- and lowercase characters.

7 On the same *PASSWORD* screen, repeat Step 6, *except* in *User Name*, select **operator** from the dropdown menu.

detail:

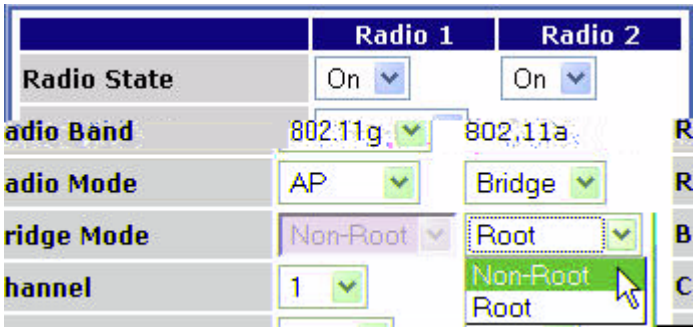


8 If the Fortress Bridge is the root node in the point-to-point/multipoint deployment, skip this step.

or

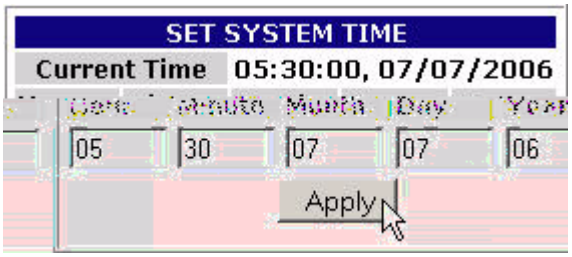
If the Fortress Bridge is the non-root node in the point-to-point/multipoint deployment, choose **RADIO SETTINGS** from the main menu and in *Bridge Mode* setting for *Radio 2*, choose **Non-Root**, and click **Apply.**

detail:



9 From the main menu on the left choose **SYSTEM OPTIONS**, and on the *SYSTEM OPTIONS* screen, in the *SET SYSTEM TIME* section, enter the correct date and time in the fields provided, using two-digit values (**hh**:**mm** **MM**:**DD**:**YY**), and click **Apply**.

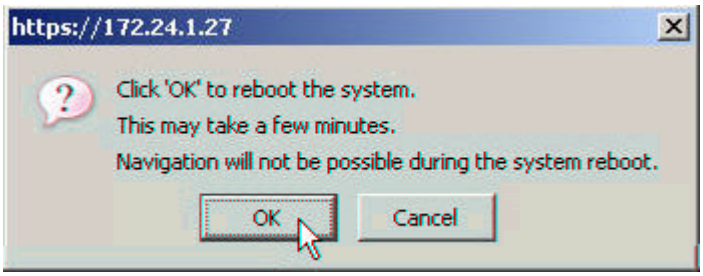
detail:



10 On the same screen, under *REBOOT SYSTEM*, click **OK**.

detail:

11 Click **OK** again to clear the system dialog.



12 Close your browser.

NOTE: If you are deploying multiple Fortress Bridges in a point-to-point/multipoint network they must be correctly configured for their network roles, typically with one serving as the root node and the rest configured as non-root nodes (refer to Section 2.2 for more detail).

NOTE: The *SYSTEM OPTIONS* screen features an informational timestamp under *SET SYSTEM TIME*. The refresh function of your browser updates this timestamp.

13 After the Bridge reboots, change the CLI password (according to the instructions in Section 6.4.4.2) and configure unique SSIDs for the Bridge (according to the instructions in Section 3.3).

If you want to use the received signal strength indicator (RSSI) to aim the antenna of a non-root Bridge, you may want to enable it now (refer to Section 3.3.2.7).

14 Disconnect the LAN, WAN and antenna ports in advance of weatherizing and mast-mounting the Bridge.

NOTE: The Bridge CLI provides access to some configuration settings that cannot be accessed from the Bridge GUI.

2.4.3 Weatherizing the Bridge

All front-panel ports must be disconnected before you can install the Weatherizing Kit.

CAUTION: ***Do not*** assemble the connector boot without first referring to these instructions. Several assembly steps are irreversible. ***Incorrectly assembled connector boots are unusable***, and cannot be disassembled.

To install the Weatherizing Kit:

1 Install the RJ-45 connector boot assembly on the end of the cable that you will be plugging into the Fortress Bridge's WAN port, as shown in Figure 2.2:

- If the RJ-45 connector is equipped with a molded plastic boot, remove it from the connector. (Some Ethernet cable connectors have a molded plastic outer casing that is not designed for removal. This style of connector is incompatible with the connector boot.)

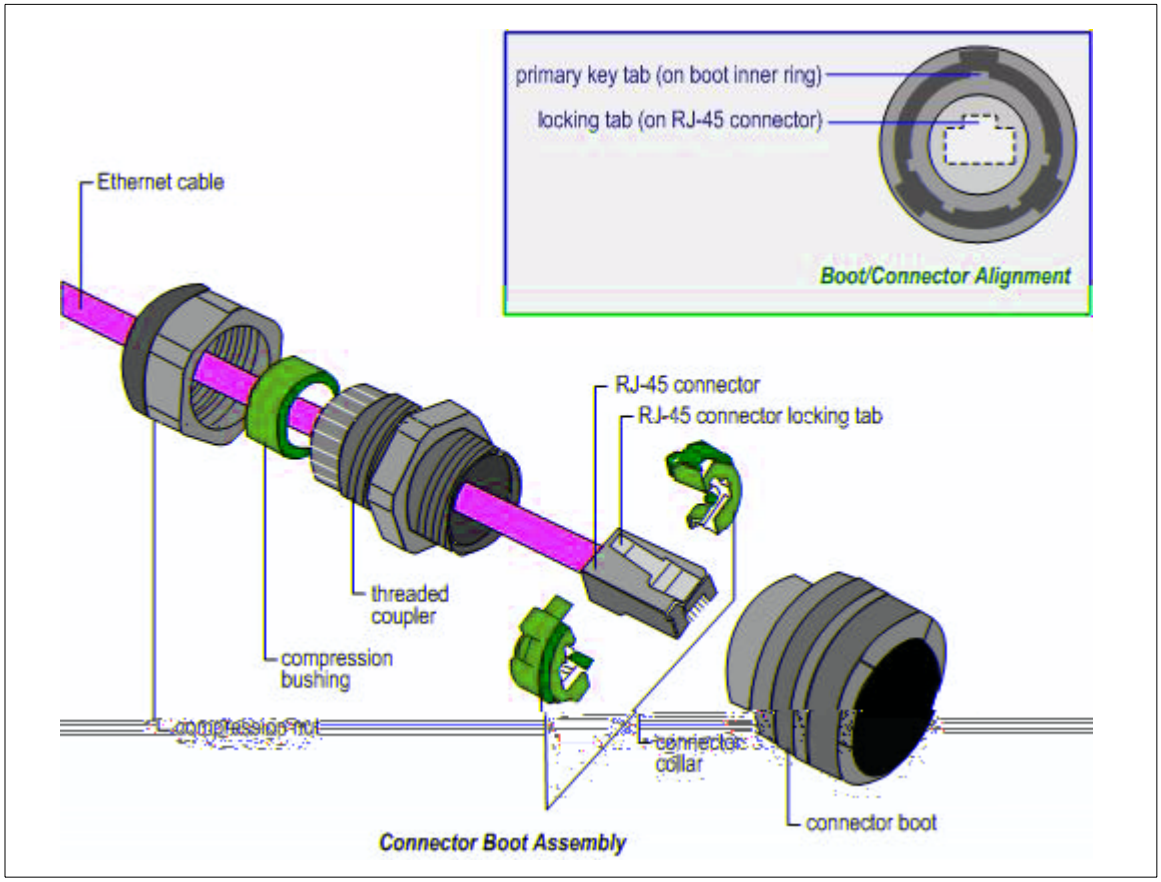


Figure 2.2 Installing the RJ-45 Connector Boot Assembly

- Slide the compression nut, with the threaded opening facing toward the connector, over the connector and onto the cable.
- Slide the compression bushing over the connector and onto the cable.
- Slide the threaded coupler, with the flanged end facing toward the compression nut and bushing, over the connector and onto the cable.
- With the smooth-side prongs on the two halves of the connector collar facing out and aligned with the RJ-45 connector's locking tab, fit the collar around the connector so that the connector's locking tab is compressed (the contact end of the connector extends approximately 1/2" from the collar). Fit the outer tabs on one half of the connector collar into the slots of the other, and squeeze the two halves of the connector collar together until they snap into place.
- Align the primary key tab on the inner ring of the connector boot with the cable connector's locking tab. Maintaining this alignment, fit the RJ-45 connector-collar assembly into the boot through the boot's threaded end and snap the collar tabs into the boot slots. Screw the connector boot securely onto the threaded coupler.
- Fit the compression bushing into the flanged end of the threaded connector, and fit the compression nut over the flanges. Screw the compression nut securely onto the threaded connector until the bushing is compressed around the cable to provide a water seal.

CAUTION: There are four different possible alignments between the RJ-45 connector and the connector boot. If the boot and connector are not in the correct alignment, the RJ-45 connector will not plug into the Bridge's WAN port.

NOTE: Plugging the connector/boot into the **WAN** port is described in Step 4 of Section 2.4.5.

WARNING: To avoid the risk of severe electrical shock, do not remove the cover plate while the Fortress Bridge is out of doors.

2 Attach the cover plate to the Bridge's front panel with the plate's three captive screws, as shown in Figure 2.3.

3 If only one antenna will be attached to the Bridge, screw the antenna port cap onto the unused antenna port.

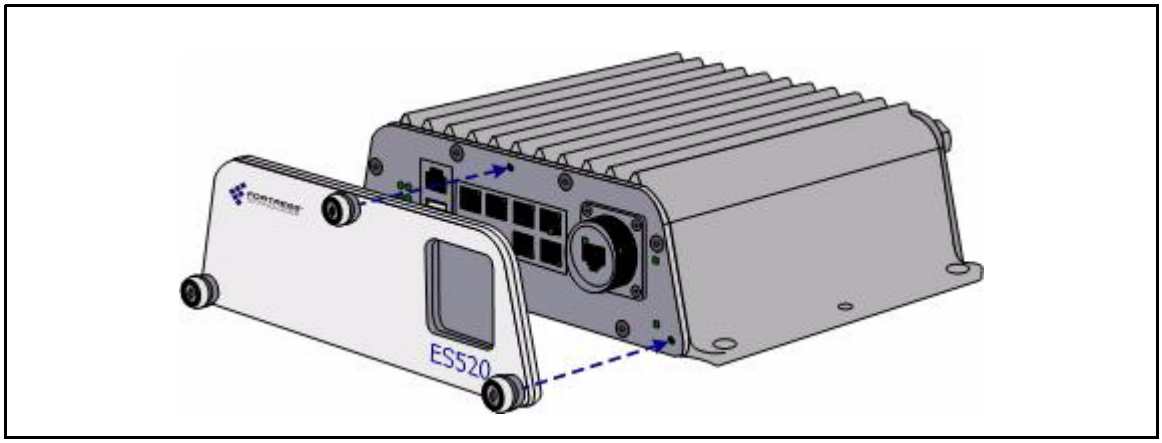


Figure 2.3 Attaching the Front-panel Cover Plate

2.4.4 Mast Mounting the Bridge

The Mast-Mounting Kit accommodates masts from 1.5" to 3" in diameter.

To install the Mast-Mounting Kit:

1. Position the Bridge at the desired position on the mast, with the Bridge's underside facing toward the mast and the front panel facing down, as shown in Figure 2.4
2. Sandwich the mast between the underside of the Bridge and the mounting bracket, fitting the mast into the bracket's toothed cut-outs.
3. Place a split lock washer on each of the two hex bolts, sliding them down to the head of the bolt.
4. Fit the bolts through the bolt holes in the mounting bracket and then into the mounting holes in the underside of the Bridge.
5. Tighten the bolts securely, until the split lock washers are flattened between the bolt heads and the mounting bracket.

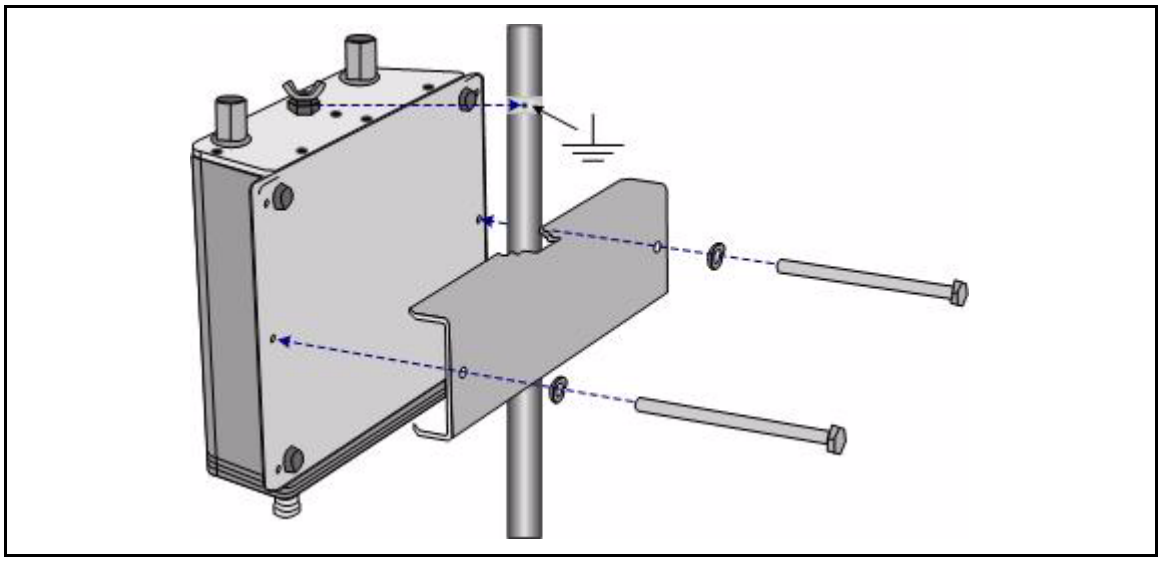


Figure 2.4 Attaching the Mast-Mounting Bracket and Grounding Stud

2.4.5 Reconnecting the Bridge for Outdoor Operation

Review the *Radio Frequency Safety Requirements* (Section 2.2.4) before installing or operating Bridge radios.

WARNING: To comply with FCC rules, *antennas must be professionally installed*. Improperly grounded outdoor antennas pose a particularly serious safety hazard.

1. Connect the rear-panel grounding stud (shown in Figure 2.4) to protective earth ground with a 20 gauge (minimum) cable.
2. Connect a waterproof, standard 802.11a/b/g-capable antenna with an N-type male connector to antenna port 1 (**ANT1**).
3. Connect an antenna cable with a N-type male connector between antenna port 2 (**ANT2**) and a high-gain

omnidirectional or directional antenna. The antenna and cable must be waterproof.

4 Connect the Bridge's **WAN** port to an external 802.3af PSE/PoE (Power Sourcing Equipment/Power over Ethernet) source, which—if the **WAN** port will connect to a satellite link or a DSL or cable modem—provides an in-line connection to the necessary network device.

To plug in the RJ-45 connector with the boot assembly installed: orient the connector correctly with the WAN port, and then twist the outer ring of the connector boot clockwise until the channels in the ring align with the locking studs on the Bridge's WAN port casing. Continue twisting the boot's outer ring clockwise until the locking channels are fully engaged and the boot is flush with the port casing. A distinct click in the final turn of the boot's outer ring indicates that connector and boot are securely plugged into the Bridge. (Installing the connector boot assembly is covered in Section 2.4.3.)

NOTE: Third party antennas are subject to local regulatory requirements. For outdoor installations, they must be waterproof.

2.5 Indoor Installation

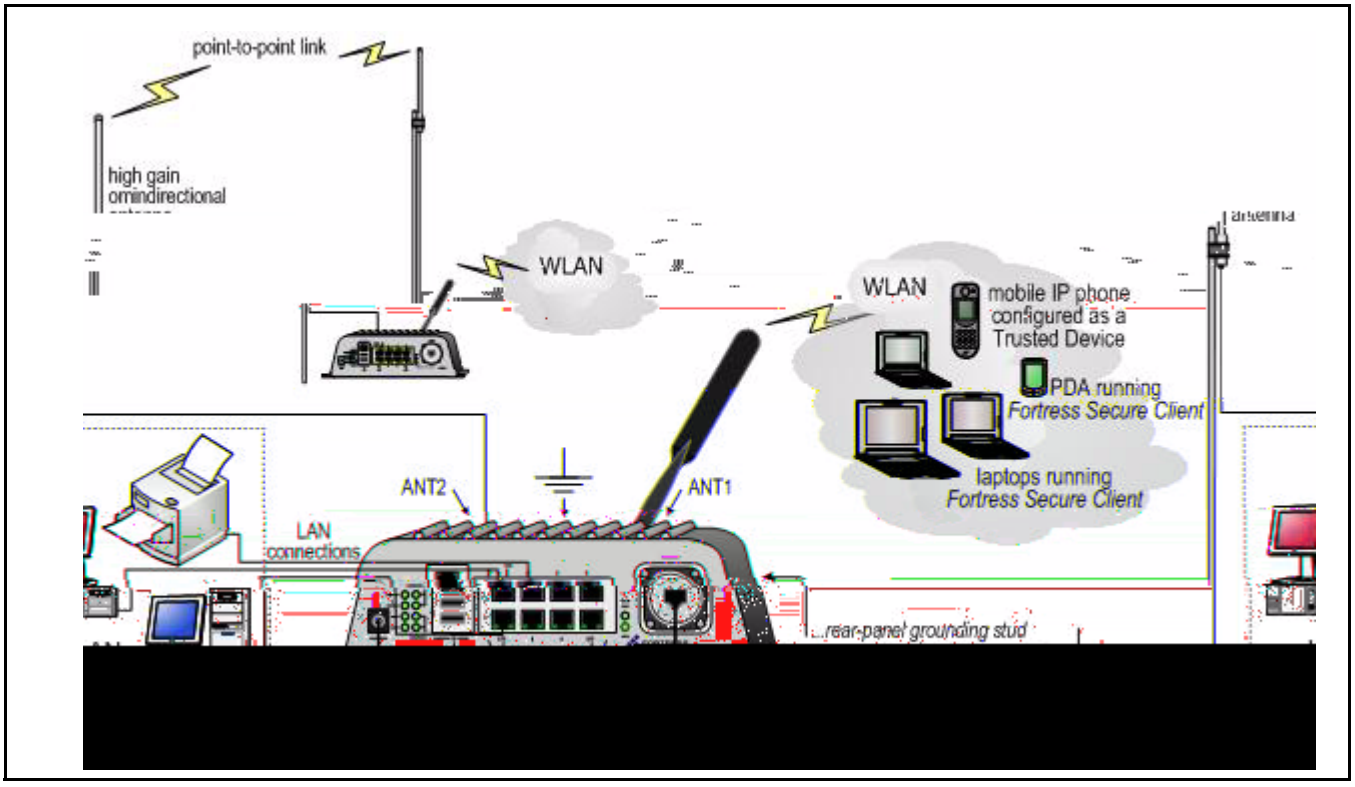


Figure 2.5 Indoor Fortress Bridge Connections

2.5.1 Connecting the Bridge for Indoor Operation

When the Fortress Bridge is installed indoors, it can be located directly on a desktop with no additional hardware, or it can be wall mounted, in any orientation—with four, #8, 3/4" wall-anchored, flathead screws—through the mounting holes in the chassis's four corners.

1 Position the Bridge so that it operates only within its safe temperature range (14º–122º F/-10º–50º C).

2 Connect a standard 802.11a/b/g-capable antenna with an N-type male connector to antenna port 1 (**ANT1**).

3 Connect an antenna cable with an N-type male connector between antenna port 2 (**ANT2**) and a high-gain omnidirectional or directional antenna.

4 Connect the Bridge to at least one power source:

- Connect the external +48V DC power supply that came with the Bridge to the front-panel **+48V DC** power inlet and plug the power supply into a properly rated AC power outlet with the cord provided.

and/or

- Connect the Bridge's **WAN** port to an external 802.3af PSE/PoE (Power Sourcing Equipment/Power over Ethernet) source. (If the **WAN** port will connect the Bridge to a satellite link or a DSL or cable modem, ensure the PSE/PoE source is in line with the necessary network device.)

5 Connect up to eight wired LAN devices to the RJ-45 Ethernet ports (numbered **1-8**).

6 If the **WAN** port will connect the Bridge to a satellite link or a DSL or cable modem (and it was not connected in Step 4), connect the 10/100 **WAN** Ethernet port to the necessary network device.

7 Verify that all link/activity and power LEDs illuminate for all connected ports.

CAUTION: The FCC requires co-located radio antennas to be at least 7.9" apart. The Bridge's antenna connectors are only 5" apart. *Avoid directly mounting two antennas to the Bridge's rear-panel connectors.*

NOTE: When both power supplies are connected, the external +48V power supply is automatically selected as the Bridge's primary power source.

2.5.2 Configuring the Bridge for Indoor Operation

Configuration procedures for an indoor Bridge are no different from outdoor Bridge preconfiguration procedures. Follow steps 1 through 12, Section 2.4.2.

To access the Bridge GUI after initial configuration, use a new instance of your browser and the IP address you set in Step 3 of Section 2.4.2.

Chapter 3
Configuration

3.1 The Bridge GUI

The Fortress Wireless Access Bridge's graphical user interface provides access to Bridge administrative functions.

Access Bridge GUI help screens by clicking **Help**, the last link on the main menu.

3.1.1 User Accounts

There are two user accounts on the Bridge GUI, and the predetermined names associated with them are *not* user-configurable.

- The *admin* (administrator) account has full access to the all functions and reconfiguration options on the Bridge.
- The *operator* account can only view Bridge and network settings and status. When the Bridge GUI is accessed through the *operator* account, the GUI functions used to reconfigure the Bridge and the network it secures are not displayed—or, when displayed, are grayed out.

3.1.2 Accessing the GUI

You can access the Bridge GUI from any computer with access to the Bridge—any computer in the Bridge-secured network's unencrypted zone, as well as any computer in the encrypted zone and running the Fortress Secure Client.

If you are installing the Bridge for the first time, refer to Section 2.4.2.

To access the Bridge GUI:

1. Open a browser and, in the address field, enter the IP address assigned to the Bridge's management interface.
2. On the *Login* screen, enter the appropriate *UserName:* **`admin`** or **`operator`**.
3. Enter the account *Password*.
4. Click **Login**.

NOTE: The default IP address is *192.168.254.254*. Default passwords are the accounts' respective user names: *admin* and *operator*. (These should be changed during installation.)

The Bridge GUI opens on the *Welcome* screen. Configuration settings are accessed through the main menu links on the left of the screen.

3.1.3 Logging Off

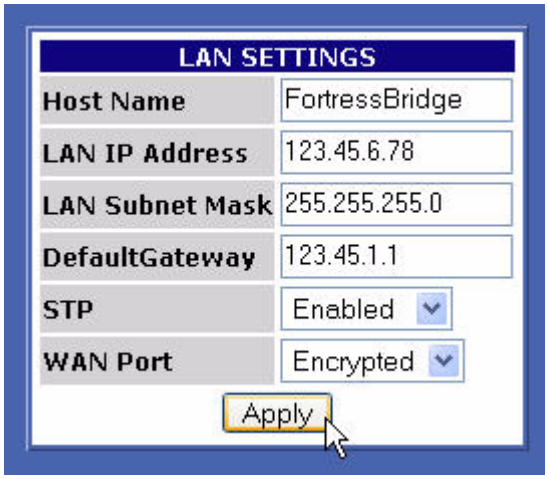
To log off the Bridge GUI, click **Logout** (below the main menu).

If you simply close the browser you have used to access the Bridge GUI, you will automatically be logged off. (If you are using Firefox's tabbed browsing, you will only be logged off when you close the active browser instance *completely*. Closing only the Bridge GUI's active tab in the browser will not log you off.)

3.2 LAN Settings

LAN settings are those that configure network access to the Bridge's management interface: its network host name, IP address, subnet mask, and default gateway.

Additionally, the Bridge's STP (Spanning Tree Protocol) and WAN port encryption options are configured on this screen.



3.2.1 Spanning Tree Protocol

STP is a link management protocol that prevents bridging loops on the network while providing path redundancy. You should enable it only in deployments in which multiple OSI layer 2 paths to the same device(s)—i.e., bridging loops—are possible.

NOTE: Bridging loops can occur on a WLAN only when multiple APs share the same ESS (extended service set).

STP requires multicasting capability. When *STP* is **Enabled**, *Multicast*—which is configured, per radio, on the *RADIO SETTINGS* screen—is automatically **Enabled** for both of the Bridge's internal radios and the fields that configure the setting (on the *RADIO SETTINGS* screen) are grayed out.

The only radio to which multicasting applies is one with a *Radio Mode* setting of **Bridge** and a *Bridge Mode* setting of **Non-Root**. If you disable STP on the *LAN SETTINGS* screen, the *Multicast* field (on the *RADIO SETTINGS* screen) of any radio so configured will be enabled, giving you the option of turning multicasting off for that radio. (Refer to Section 3.3.2.6 for more detail on the multicast function of Bridge radios.)

If you enable STP on the Bridge, you should enable it across all devices on the Bridge-secured network.

3.2.2 WAN Port Encryption

By default, the Bridge's WAN port is in the encrypted zone of the Bridge-secured network, in which all traffic on the port is encrypted.

It can be configured to be in the network's unencrypted zone and so to pass unencrypted traffic (cleartext).

The encrypted and unencrypted zones are mutually exclusive and the WAN port cannot be in both zones at once.

To reconfigure Bridge LAN settings:

1. Log on to the Bridge GUI *admin* account and select **LAN SETTINGS** from the menu on the left.
2. On the *LAN SETTINGS* screen, make your changes to the relevant field(s). These include:
   - *Host name* - a descriptive name for the Bridge
   - *LAN IP address* - the network address of the Bridge
   - *LAN Subnet mask* - the correct subnet mask for the Bridge
   - *Default gateway* - the IP address of the default gateway
   - *STP* - enables/disables Spanning Tree Protocol (enabled by default)
   - *WAN Port* - configures the WAN port to reside in either the encrypted zone of the Bridge-secured network or in the unencrypted zone.

   Click **Apply**.
3. Click **OK** on the system prompt that instructs you to reboot.
4. Follow the instructions in Section 4.7 to reboot the Bridge.

   You must use a new instance of the browser (and the new IP address, if it has changed) when you next access the Bridge's management interface.

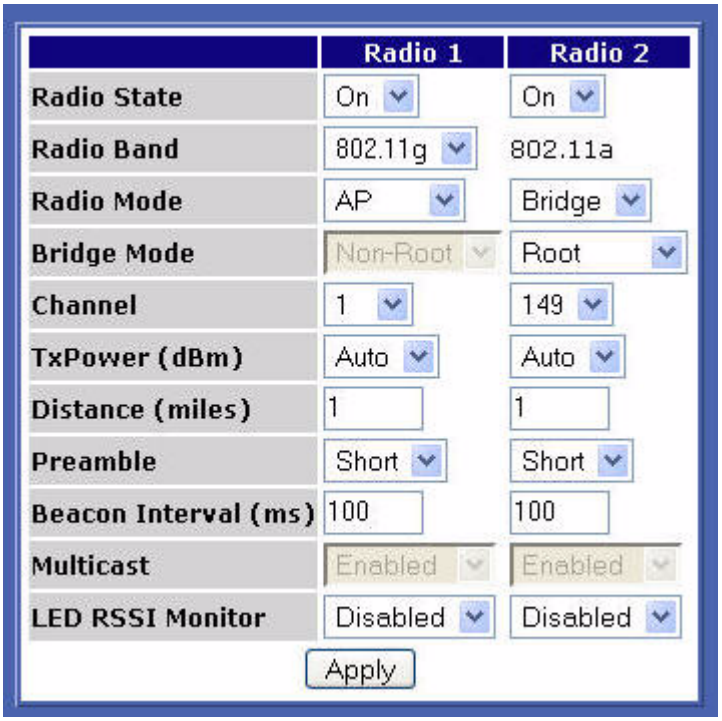
NOTE: The IP address you assign must be unique on the network.

CAUTION: If the WAN port is providing the link to an unencrypted interface, such as a cable or DSL modem or satellite uplink, the WAN port ***must*** reside in the network's unencrypted zone.

NOTE: If you are using Firefox's tabbed browsing, you must close the active browser instance *completely*—not just Bridge GUI's active tab in the browser.

3.3 Radio Settings

The Fortress Bridge is equipped with two, independent internal radios, the basic configuration settings for which appear on the *RADIO SETTINGS* screen. The default settings are shown below.



NOTE: Additional radio interface settings can be configured through *VIRTUAL ACCESS POINT SETTINGS* (accessible from the *INTERFACES* screen, Section 3.3.4) and through the Controller CLI (sections 6.4.3 and 6.7).

Radio 1 is the tri-band 802.11a/b/g radio, which can be configured as an 802.11g or an 802.11a radio. *Radio 2* always functions as an 802.11a radio.

NOTE: 802.11b devices are fully compatible with the 802.11g radio.

RADIO SETTINGS fields are described in sections 3.3.1 and 3.3.2. Section 3.3.3 provides step-by-step instructions to change them.

3.3.1 Radio State, Band and Mode Settings

The first four settings on the *RADIO SETTINGS* screen determine whether and how the radio will be used in the network implementation.

NOTE: *Radio 1* uses antenna port 1 (**ANT1**); *Radio 2* uses antenna port 2 (**ANT2**).

3.3.1.1 Radio State

The *Radio State* setting simply turns the radio **On** and **Off**. Both radios are on by default.

3.3.1.2 Radio Band

Only *Radio 1* can operate on either the **802.11a**, 5 Ghz band or the **802.11g**, 2.4 Ghz band, according to your selection in the *Radio Band* field. By default, *802.11g* is selected for *Radio 1*.

Radio 2 can function only on the 802.11a band.

3.3.1.3 Radio Mode

Either radio can operate in either of two modes:

- **AP** - A radio in **AP** mode functions exclusively as a wireless access point, allowing connections only from wireless devices. It does not permit connections to or from other Fortress Bridges.
- **Bridge** - A radio in **Bridge** mode functions as network bridge in a point-to-point/multipoint network of other Fortress Bridges, and it allows connections from wireless devices. In **Bridge** mode, then, a radio can serve simultaneously as a network bridge and as a wireless AP.

By default, *Radio 1* is in **AP** mode and *Radio 2* is in **Bridge** mode.

3.3.1.4 Bridge Mode

When deploying the Fortress Bridge as a wireless bridge in a point-to-point or point-to-multipoint network—with a *Radio Mode* setting of **Bridge** on one of the internal radios— you must correctly configure the radio used for bridging for its network role, by selecting one of two possible *Bridge Mode* settings:

- **Root** - A radio with a *Bridge Mode* of **Root** does not initiate connections with other Fortress Bridges. Radios in root mode only receive connections initiated by other devices—either from the radios of other Bridges (in **Non-Root** mode) or from wireless devices.

NOTE: You can also change the *Bridge Mode* of Radio 2 through the Bridge's front-panel switches (refer to Section 3.10.1.1).

- **Non-Root** - Radios in **Non-Root** mode do initiate connections with other Fortress Bridges—either directly with a root Bridge or with other non-root Bridges (as well as receiving connections from other non-root Bridges and wireless devices).

Typically, one Bridge serves as the root node (or root Bridge) and any other Bridges in the deployment are configured as non-root nodes.

In the Bridge's default configuration, only *Radio 2* is configured with a *Radio Mode* of **Bridge**, and it is in **Root** mode.

3.3.2 Radio Transmission and Reception Settings

In addition to establishing the basic uses and roles of the Bridge's internal radios (Section Section 3.3.1), you can configure a number of operating parameters through the Bridge GUI.

CAUTION: In point-to-point/multi-point deployments the radios used to connect the networked Bridges must be configured with identical transmission and reception settings.

3.3.2.1 Channel

The *Channel* setting selects the portion of the radio spectrum over which the radio will communicate.

Radios in non-root bridging mode do not bind to a channel, but rather to an SSID. The *Channel* setting will therefore be grayed out for either radio with a *Radio Mode* setting of **Bridge** and a *Bridge Mode* setting of **Non-Root**.

The channels available for a radio in **AP** *Radio Mode* or in **Root** *Bridge Mode* are a function of the frequency band it uses.

- On *Radio 2* and *Radio 1* when it is configured to use the 802.11a band, you can select channels **36**, **40**, **44**, **48**, **52**, **56**, **60**, **64**, **149**, **153**, **157**, or **161**.
- On *Radio 1*, when it is configured to use the 802.11g band, you can select channels **1**–**11**, inclusive.

The default channel setting for *Radio 1* when it is using the 802.11G band is *1*; on the 802.11a band its default setting is *36*. The default channel setting of *Radio 2* is *149*.

Selectable channel options for *Radio 1* therefore depend on the *Radio Band* selection made for it. (*Radio 2* is fixed on the 802.11a band; its channel selection options do not change.)

3.3.2.2 Transmit Power

The *TxPower* setting specifies the power level at which the radio will transmit—from **1** to **18** dBm (decibels referenced to milliwatts), in increments of 1 dBm—or, by selecting **Auto** (the default for both radios), which configures the radio to transmit at maximum power (26 dBm for both radios).

In environments with a dense distribution of APs (and resulting potential for interference), it may be desirable to select a lower *TxPower* setting than the default (*Auto*) for *Radio 1* when it is configured to use the 802.11g band. The *Auto* setting is otherwise appropriate for both radios.

3.3.2.3 Distance

The *Distance* setting configures the maximum distance—from 1 to 35 miles, in increments of 1 mile—for which the radio must adjust for the propagation delay of its transmissions.

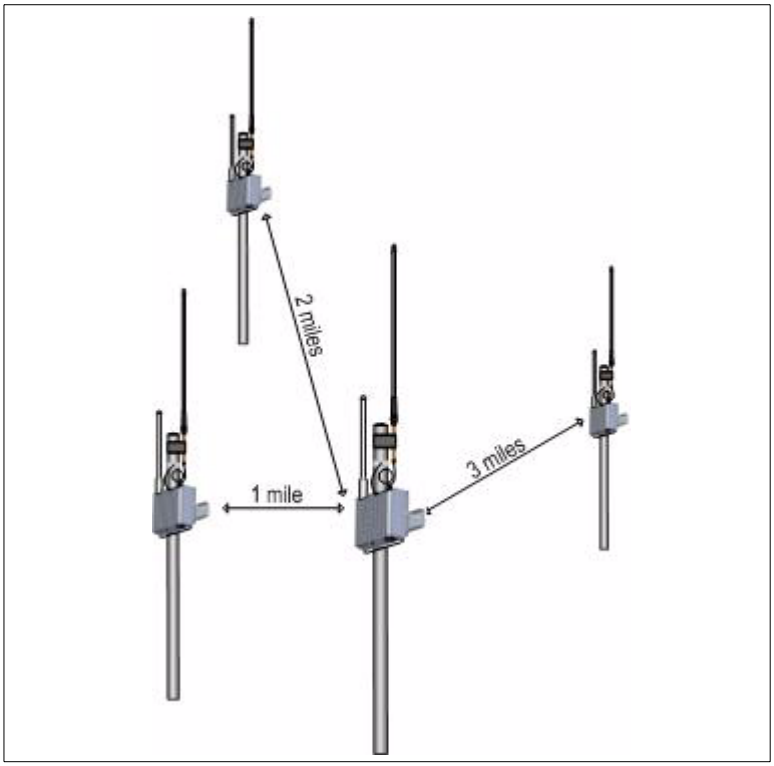


Figure 3.1. Point-to-multipoint Bridge deployment with bridging radio *Distance* settings of *3* miles

In a point-to-multipoint deployment, the *Distance* setting on the networked radios of *all* member Bridges should be the number of miles separating the two Bridges with the greatest, unbridged distance between them. In Figure 3.1, above, the *Distance* setting would be 3 miles: the longest distance in the network between two Bridges without another Bridge between them.

Propagation delay is not a concern at distances of one mile and under, at which you should leave the setting at 1 mile (the default for both radios).

Additional radio configuration can be done through the Bridge CLI (refer to Section 6.7).

3.3.2.4 Preamble

The short preamble is used by virtually all wireless devices currently being produced. The default *Preamble* setting of **Short** is therefore optimal for most network implementations.

Some older 802.11b devices, however, still use the long preamble, and if the network must support such devices, you must configure the radio they will communicate with to use a *Preamble* setting of **Long**.

3.3.2.5 Beacon Interval

The Bridge's radios transmit beacons at regular intervals to announce their presence on the network. You can configure the number of milliseconds between beacons in whole numbers between `25` and `1000`. You cannot disable the beacon.

The default beacon interval is `100` milliseconds.

3.3.2.6 Multicasting

Wireless is an inherently broadcast medium. A multicast packet, like any other, is broadcast (by the root Bridge) to all nodes (non-root Bridges) on the wireless network. Each non-root Bridge then examines the packet and:

- If the Bridge is an intended receiver, it accepts the packet.

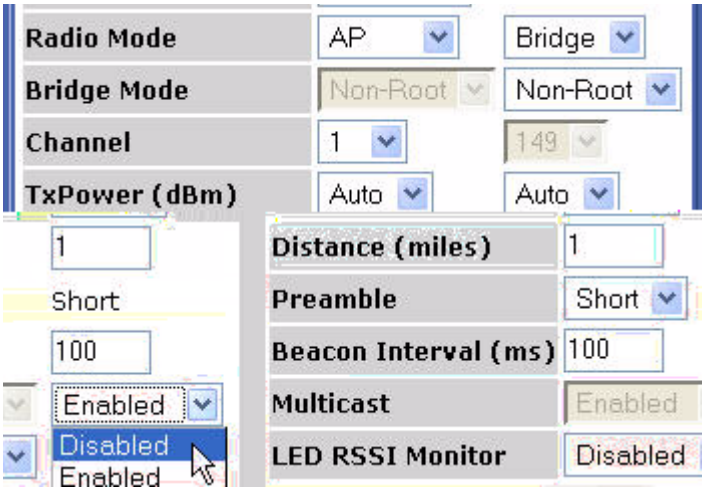
  and/or
- If the Bridge is serving as a repeater for an outlying Bridge that is an intended receiver, it passes the packet along this route.

  or
- If the Bridge is neither an intended receiver nor the repeater for an intended receiver, it drops the packet.

Non-root Bridges on which *Multicast* is disabled will drop all multicast packets.

The *Multicast* function applies exclusively to non-root Bridges, and so can only be **Enabled** on Bridges with a *Radio Mode* setting of *Bridge* and a *Bridge Mode* setting of *Non-Root*.

detail:



The *Multicast* field is grayed out for Bridges with a *Radio Mode* of **AP** or with a *Bridge Mode* of **Root**.

The *Multicast* field is also grayed out for Bridge's with *STP* **Enabled** on the *LAN SETTINGS* screen. Because STP requires multicasting capability, *Multicast* is automatically **Enabled** (and the field that configures the setting is grayed out) when *STP* is

Enabled on the *LAN SETTINGS* screen. If you disable STP on a non-root Bridge, the *Multicast* field for the radio with a *Radio Mode* setting of **Bridge** and a *Bridge Mode* setting of **Non-Root** will be configurable. Refer to Section 3.2.1 for more information on STP.

3.3.2.7 Received Signal Strength Indicator

In outdoor, point-to-point/multipoint installations, the *LED RSSI Monitor* allows you to make the first adjustments to the directional antenna(s) of the non-root Bridge(s) in the network.

When the *LED RSSI Monitor* is **Enabled** on a given radio, all other monitoring functions of both of the front-panel LEDs for that radio (described in Section 5.6.2) are disabled.

Then, as you point a directional antenna of a non-root Bridge toward the root Bridge, the lower LED for that radio dynamically indicates the strength of the signal received from the root Bridge, as shown in Table 3.1.

The *LED RSSI Monitor* is **Disabled** by default.

NOTE: Because radios in **AP** *Radio Mode* or in **Root** *Bridge Mode* accept multiple, simultaneously connections, the *LED RSSI Monitor* is not used to set up radios configured in this way (although it remains available).

Table 3.1. RSSI Behaviors and Meanings in Radio LEDs

Behavior	Meaning
off	no connection
slow green flash (approx. 1 Hz)	poor connection (signal level ≤ -85 dBm)
fast green flash (approx. 4 Hz)	good connection (signal level > -85 dBm but < -60 dBm)
steady green	excellent connection (signal level > -60 dBm)

3.3.3 Configuring Basic Radio Settings

1. Log on to the Bridge GUI *admin* account and select **RADIO SETTINGS** from the menu on the left.
2. On the *RADIO SETTINGS* screen, in the column that corresponds to the radio you want to configure, enter new values into the relevant fields (described in sections 3.3.1 and 3.3.2).
3. Click **Apply** at the bottom of the screen.
4. If a system prompt instructs you to reboot, click **OK**.
5. If you changed *TxPower* to *Auto*, or you were prompted to reboot the Bridge, follow the instructions in Section 4.7.

NOTE: When you change *TxPower* from *Auto* to another value, the change takes effect immediately. When you change the setting from another value to *Auto*, you must reboot Bridge in order to effect the change.

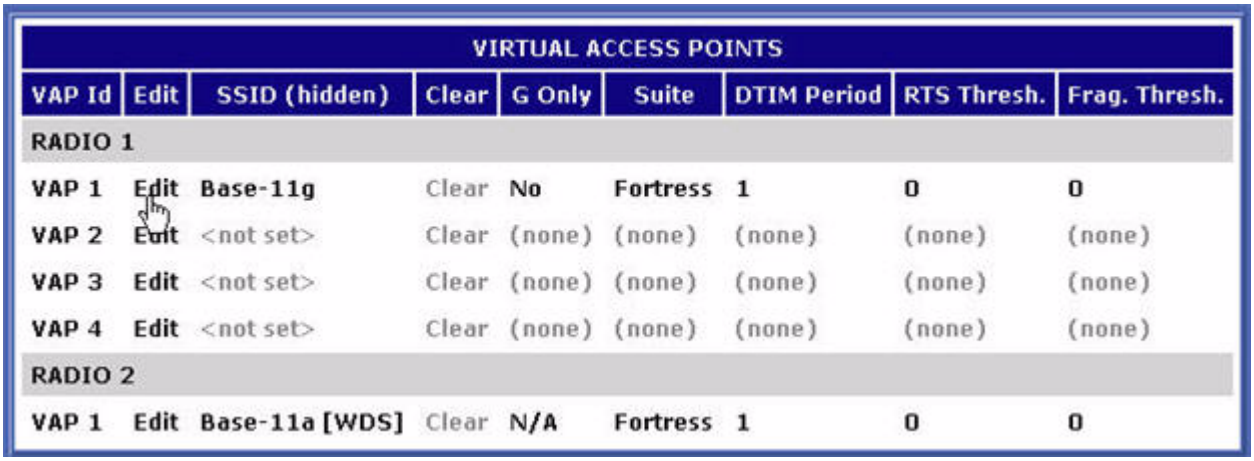
3.3.4 Virtual Radio Interface Settings

A radio with a *radio mode* of **Bridge**, whether it is configured as a root or a non-root bridge, can comprise only a single Virtual Access Point (or *VAP*), with its single associated SSID.

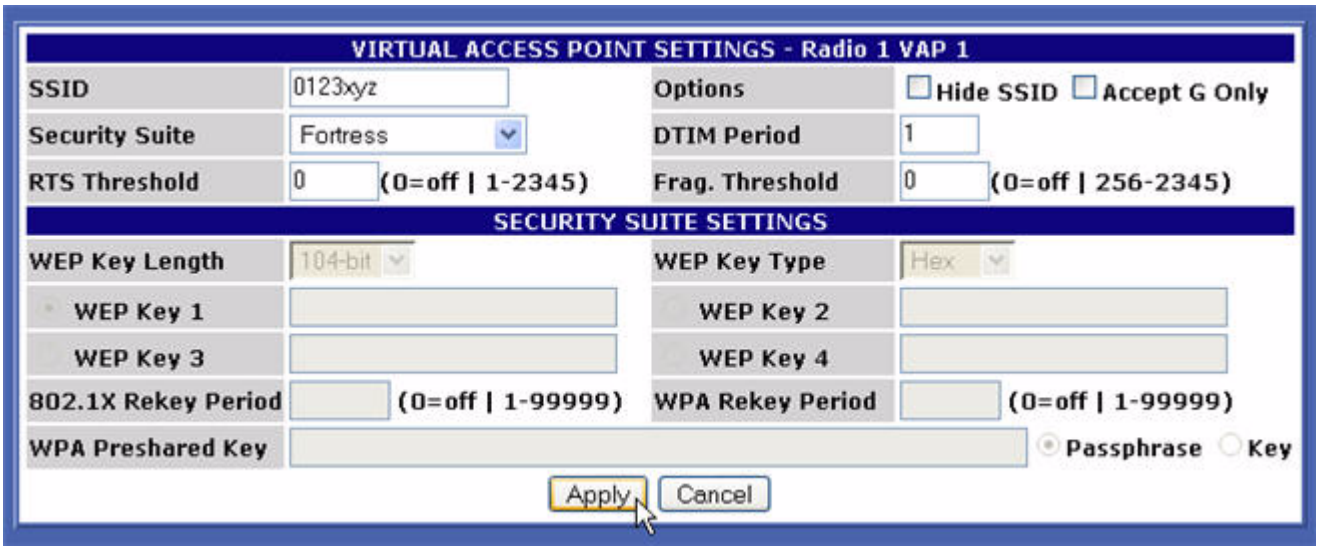
A radio with a *radio mode* of **AP**, can comprise up to four VAPs each with its own SSID and associated settings.

By default, only one VAP is configured per radio, regardless of the radio *Mode* settings. You can however observe the added,

unconfigured VAPs for radios in **AP** *radio mode* on the *VIRTUAL ACCESS POINTS* display frame on the *INTERFACES* screen.



You can view the settings that assign SSIDs (and associated settings) for the radio's VAPs in the *VIRTUAL ACCESS POINTS* frame on the *INTERFACES* screen. The **Edit** button for each VAP provides access to the fields that configure these settings.



Sections 3.3.4.1 through 3.3.4.5 describe the fields available through the **Edit** buttons in the *VIRTUAL ACCESS POINTS* frame. Section 3.3.4.6 provides step-by-step instructions to configure them.

3.3.4.1 SSID

The service set identifier associated with each VAP is a unique string of up to 32 characters included in the packet headers of wireless traffic. SSIDs are used like passwords to identify which devices can connect to the wireless network and to determine the parameters of their access once they are connected.

CAUTION: The network is not fully secure until the radio SSIDs have been changed from their default settings.

Radio 1 is preconfigured with a default SSID of **`Base-11g`**; the default SSID for *Radio 2* is **`Base-11a`**.

3.3.4.2 Hide SSID and Accept G Only Options

To the right of the SSID field are two options that you can enable through their checkboxes:

- **Hide SSID** - Enabling this option deletes the SSID string from the packet headers of beacon and probe responses. It is disabled by default.
- **Accept G Only** - Enabling this option prevents 802.11b wireless devices from connecting to *Radio 1* when it is configured to use the 802.11g band. When this option is disabled (the default), Radio 1 (configured with a *Radio Band* of **802.11g**) accepts connections from both 802.11g and 802.11b devices.

3.3.4.3 DTIM Period

APs buffer broadcast and multicast messages for devices on the network and then send a Delivery Traffic Indication Message to “wake-up” any inactive devices and inform all network clients that the buffered messages will be sent after a specified number of beacons have been transmitted. (The beacon interval, described in Section 3.3.2.5, is configured on the *RADIO SETTINGS* screen.)

The *DTIM Period* determines the number of beacons in the countdown between transmitting the initial DTIM and sending the buffered messages. Whole values from `1` to `255`, inclusive, are accepted; the default is `1`.

3.3.4.4 RTS and Fragmentation Thresholds

The *RTS Threshold* allows you to configure the maximum size of the frames the VAP sends without using the RTS/CTS protocol. Frame sizes over the specified threshold cause the VAP to first send a Request to Send message and then receive a Clear to Send message from the destination device before transmitting the frame.

The *RTS Threshold* is measured in bytes. Zero (0) and whole values between `1` and `2345` are accepted. The default *RTS Threshold* value of `0` turns off RTS/CTS for all frames.

The *Frag. Threshold* allows you configure the maximum size of the frames the VAP sends whole. Frame sizes over the specified threshold are broken into smaller frames before they are transmitted.

The *Frag. Threshold* is measured in bytes. Zero (`0`) and whole values between `256` and `2345` are accepted. The default *Frag. Threshold* value of `0` turns off fragmentation for all frames (i.e., frames will be sent whole regardless of size).

3.3.4.5 Security Suite and Security Suite Settings

The security protocol(s) employed by the Bridge's virtual access point are configured per VAP.

Your selection in the *Security Suite* field of the *VIRTUAL ACCESS POINT SETTINGS* frame determines which fields are configurable (and which are grayed-out) in the *SECURITY SUITE SETTINGS* frame (in the lower half of the same screen), as described below.

NOTE: Certain *Security Suite* options require that an 802.1X authentication server be configured for the Bridge. These include: 802.1X and those WPA and WPA2 settings that do not use PSK. Refer to Section 3.4.1.

Cleartext Security

Selecting **Cleartext** as a VAP's *Security Suite* essentially turns off security measures for that VAP. Wireless devices connected to the VAP send and receive all traffic in the clear (i.e., unencrypted).

A *Security Suite* setting of **Cleartext** requires no further configuration.

Fortress Security

Selecting **Fortress** as a VAP's *Security Suite* requires all traffic on that VAP to use Fortress's Mobile Security Protocol (MSP), as configured on the Bridge itself (on the *SECURITY SETTINGS* screen of the Bridge GUI or in the Bridge CLI).

When the *Radio Mode* is **Bridge**, whether in **Root** or **Non-Root** mode, you must select **Fortress** as the *Security Suite* setting for that radio's single VAP.

A *Security Suite* setting of **Fortress** requires no further configuration in the *SECURITY SUITE SETTINGS* frame.

Open WEP and Shared WEP

Open WEP (Wired Equivalent Privacy) and Shared WEP both use static keys for data encryption. They are distinguished by their authentication methods.

Open WEP operates on the assumption that the keys configured on the VAP and on connecting devices have been entered correctly. It allows devices to connect without challenge and then uses the configured keys to encrypt the data passing between the Bridge and the connected device.

Shared WEP does not allow a device to connect until it has successfully encrypted a challenge sent by the VAP. When the VAP's challenge receives a correct response from the connecting device, it allows the connection and then uses the configured keys to encrypt the data passing between the Bridge and the connected device.

Selecting **Open-WEP** or **Shared-WEP** as a VAP's *Security Suite* requires the same settings to be configured in the *SECURITY SUITE SETTINGS* frame. These include:

WEP Key Length - WEP keys can be 104 or 40 bits long. **104-bit** is the default.

WEP Key Type - WEP keys can be composed of an **ASCII** (plaintext) passphrase or hexadecimal string. **Hex** is the default.

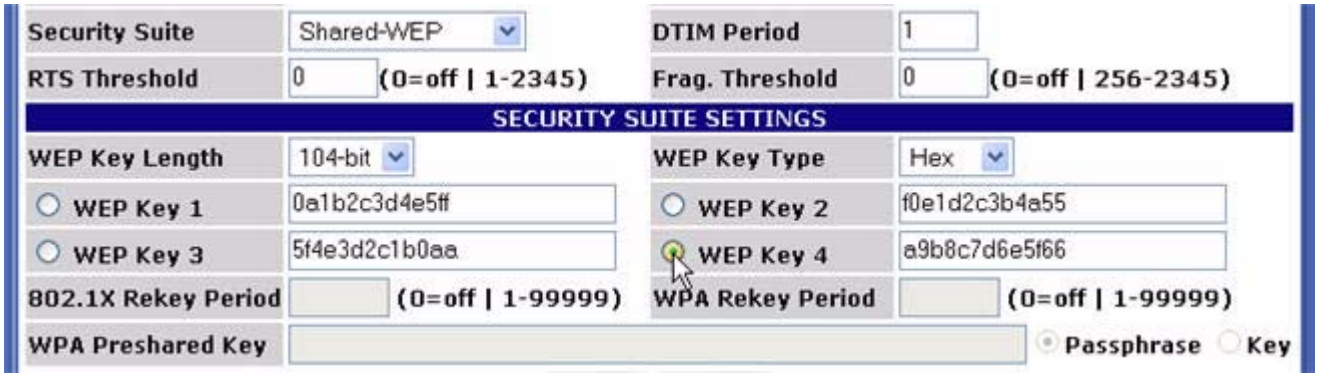
WEP Keys 1–4 - You must manually enter at least one static key to be used in Open WEP and Shared WEP transactions, within the specifications you set in the two fields above, which determine the usable key lengths for these fields.

Table 3.2. Usable WEP Key Lengths

bit-length	in hex	in ASCII
104-bit	13 digits	7 characters
40-bit	10 digits	5 characters

Use the radio button to select the default transmit key: the key to be used when transmitting multicast/broadcast messages on the network.

detail:



802.1X Security

802.1X security uses WEP encryption with dynamically generated keys rather than static keys for encryption.

The dynamic keys used when you select a *Security Suite* of **802.1X** are generated and exchanged automatically at user-specified intervals. This interval is the only additional setting required for 802.1X security. Specify the interval in seconds in the *802.1X Rekey Period* field. Whole numbers between `0` and `99999`, inclusive, are allowed. A value of `0` (zero), disables the rekeying function; the keys used by connecting devices will remain unchanged for the duration of their sessions.

WPA, WPA2 and WPA-Mixed Security

WPA (Wi-Fi Protected Access) and WPA2 are the *enterprise* modes of these two WPA types (as distinguished from the *pre-shared key* modes described below).

You can specify that **WPA** or **WPA2** be used exclusively on a given VAP, or you can configure a single VAP to be able to use either (by selecting **WPA-Mixed**), depending on the WPA type in use by the connecting device.

WPA and WPA2 generate encryption keys dynamically and exchange keys automatically with connected devices at user-specified intervals. This interval is the only additional setting required for WPA security. Specify the interval in seconds in the *WPA Rekey Period* field. Whole numbers between `0` and `99999`, inclusive, are allowed. A value of `0` (zero), disables the rekeying function; the keys used by connecting devices will remain unchanged for the duration of their sessions.

WPA-PSK, WPA2-PSK and WPA-Mixed-PSK Security

WPA-PSK (Wi-Fi Protected Access) and WPA2-PSK are the *pre-shared key* modes of these two WPA types (as distinguished from the *enterprise* modes described above).

Pre-shared key mode differs from enterprise mode in that PSK bases its key generation on a user-specified key or passphrase.

You can specify that **WPA-PSK** or **WPA2-PSK** be used exclusively on a given VAP, or you can configure a single VAP to be able to use either (by selecting **WPA-Mixed-PSK**), depending on the WPA-PSK type in use by the connecting device.

Like enterprise-mode WPA, WPA-PSK and WPA2-PSK generate encryption keys dynamically and exchange keys automatically with connected devices at user-specified intervals. Specify the interval in seconds in the *WPA Rekey Period* field. Whole numbers between `0` and `99999`, inclusive, are allowed. A value of `0` (zero), disables the rekeying function; the keys used by connecting devices will remain unchanged for the duration of their sessions.

Additionally you must enter the *WPA Preshared Key* itself, in the form of either a plaintext passphrase between 8 and 63 characters in length or a 64-digit hexadecimal string, and then use the radio buttons to specify whether the key is a **Passphrase** or a hexadecimal **Key**.

3.3.4.6 Configuring Virtual Radio Settings

1. Log on to the Bridge GUI *admin* account and select **INTERFACES** from the menu on the left.
2. In the *VIRTUAL ACCESS POINTS* frame, click the **Edit** button for the VAP you want to configure.
3. Select and/or enter the values you want to set for the VAP. Your options are described in sections 3.3.4.1 through 3.3.4.5).
4. Click **Apply** at the bottom of the screen.

3.4 802.1X Server and LAN Port Settings

The Fortress Bridge can be used with an external 802.1X authentication server and its internal switch ports can be individually configured to allow or block 802.1X traffic.

The Fortress Bridge supports *non*-802.1X authentication through a separate and unrelated set of configuration settings. The global settings for non-802.1X authentication are described in Section 3.6.6. Individual non-802.1X device and user authentication settings are described in sections 4.1 and 4.2, respectively.

NOTE: The RADIUS server internal to the Bridge cannot be used for 802.1X authentication.

3.4.1 802.1X Authentication Server

When an 802.1X authentication server is configured for it, the Bridge acts as an 802.1X authenticator, conveying 802.1X queries and responses between 802.1X supplicants and the configured authentication server.

In order to support 802.1X authentication—whether for wireless (*802.1X Security* in Section 3.3.4.5) or wired devices (Section 3.4.2)—the Bridge must be configured to use an external, 802.1X authentication server.

NOTE: If you are using both RADIUS and 802.1X authentication services, they can run on the same external server, but you must enter the server's settings both on the *SECURITY SETTINGS* screen (in the *AUTHENTICATION SETTINGS* section) and on the *INTERFACES* screen (in the *802.1X AUTHENTICATION SERVER* frame).

Certain other VAP *Security Suite* settings—specifically those WPA and WPA2 options that do *not* use PSK (pre-shared key mode)—also require the use of an 802.1.X authentication server. (Possible VAP *Security Suite* settings are described in detail in Section 3.3.4.5.)

Finally, even in configurations that do not require the use of an 802.1X authentication server, ***the fields that configure the server cannot be empty.*** In these instances, you can leave the default 802.1X authentication servers settings in place, without reference to an actual 802.1X server.

Before configuring the Bridge to use the 802.1X authentication server, you should first configure the service to use the Bridge as an 802.1X authenticator (refer to your 802.1X server documentation for guidance).

To configure the Bridge for use with an external 802.1X authentication server:

1 Log on to the Bridge GUI *admin* account and select **INTERFACES** from the menu on the left.

2 In the *801.1X AUTHENTICATION SERVER* frame:
   - In *Server Address*, enter the IP address of the network 802.1X authentication server (the default is `127.0.0.1`).
   - In *Server Port*, enter the port used by the server for 802.1X requests (the default is `1812`).
   - In *Auth Server Key*, enter the shared key assigned to the Bridge in the 802.1X service. (The default is `fortress`.)
   - In *Confirm Server Key*, re-enter the shared key (to guard against entry errors).
3 Click the frame's **Apply** button.

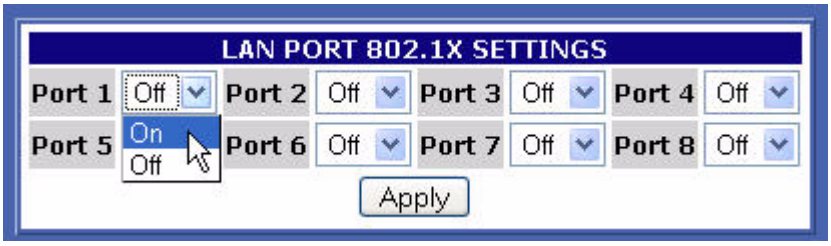
NOTE: The server key you enter here should already be present in the 802.1X authentication service configuration.

3.4.2 LAN Port 802.1X Settings

The Bridge's internal LAN switch can be configured, per port, to require that the connected device is an 802.1X supplicant successfully authenticated by the 802.1X server configured for the Bridge (Section 3.4.1).

NOTE: The internal LAN does not support NAT (network address translation).

Configure this function in the *LAN PORT 802.1X SETTINGS* frame of the *INTERFACES* screen, where the port numbers shown in the GUI correspond to the numbered ports **1**–**8**, as labeled on the Bridge's front panel (shown in Figure 2.1).



1 Log on to the Bridge GUI *admin* account and select **INTERFACES** from the menu on the left.
2 In the *LAN PORT 801.1X SETTINGS* frame, use the dropdown menu for each port to select whether:
   - the device connecting through the port will *not* be required to authenticate through an 802.1X authentication server: **Off** (the default)

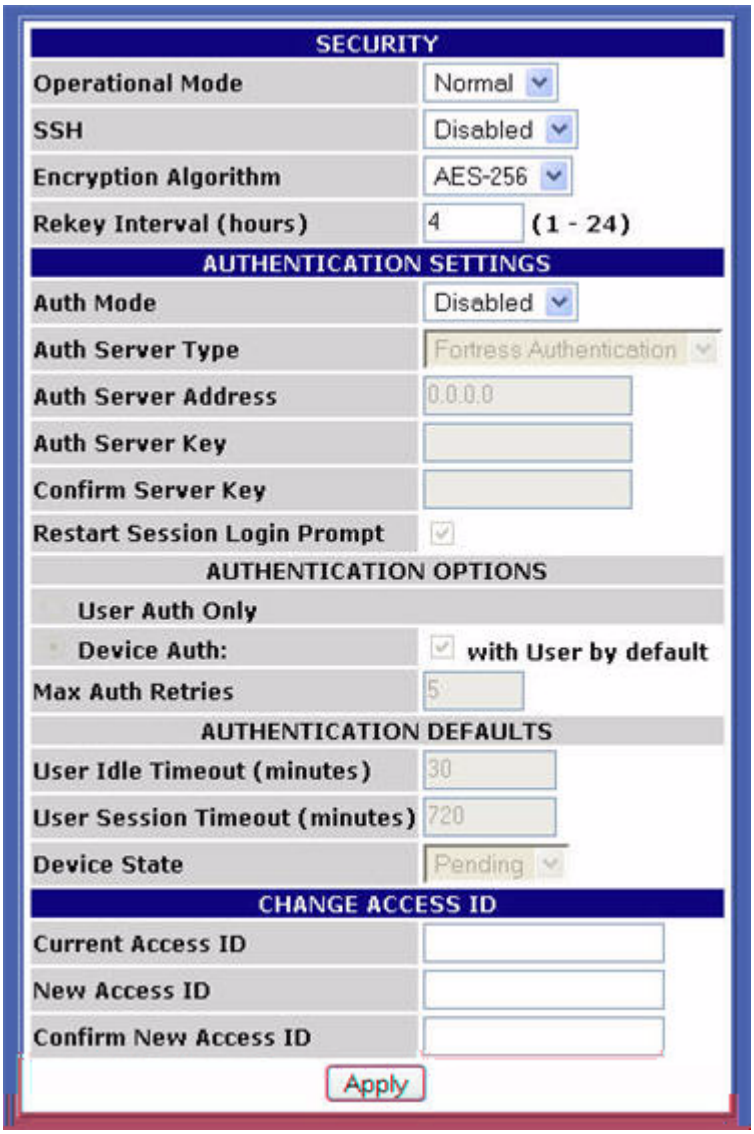
   or
   - the device will be required to authenticate through the 802.1X server configured for the Bridge: **On**.
3 When you have made your selections for each of the Bridge's LAN ports, click the frame's **Apply** button.

3.5 Bridge Passwords

Two passwords apply to the Bridge GUI, one for the *admin* account, which grants full administrative permissions on the Bridge, and one for the *operator* account, which grants view-only access. A third password is set for the Bridge CLI; it can be changed only in the CLI (refer to Section 6.4.4.2).

NOTE: For security

The viewable, default security settings are shown below.



3.6.1 Operating Mode

The Fortress Bridge can be operated in either of two modes: *Normal* (the default) or *FIPS*.

FIPS operating mode is necessary for deployments and applications that are *required* to comply with the Federal Information Processing Standards (FIPS) for cryptographic modules. The high levels of security that can be implemented in the Fortress Security System's *Normal* operating mode meet or exceed the needs of virtually all unregulated networked environments.

FIPS operating mode is compliant with FIPS 140-2. It enforces security measures beyond those of Normal operating mode, the most significant of which include:

NOTE: The Bridge (in either operating mode) flashes the front-panel cleartext LED (**Clr**) whenever unencrypted data is passing in an encrypted zone. In FIPS terminology, the cleartext signal indicates that the Bridge is in *Bypass Mode (BPM)*.

- If the Bridge fails any self-test on startup, it is rendered inoperable and must be returned to the vendor for repair or replacement.
- Only a designated Crypto Officer, as defined by the Federal Information Processing Standards, may perform administrative functions on the Bridge and its Secure Clients.

detail:

To change the Bridge operating mode:

1. Log on to the Bridge GUI *admin* account and select **SECURITY SETTINGS** from the menu on the left.
2. In the *SECURITY* section of the *SECURITY SETTINGS* screen, select the Bridge's operating mode.
3. Click **Apply** at the bottom of the screen.

3.6.2 Secure Shell Access

In order to access the Bridge CLI from a network connection to the Bridge's management interface, Secure Shell (SSH) must be enabled. When SSH is disabled, you can access the Bridge CLI exclusively through a direct connection to its **Console** port.

Secure Shell (SSH) is disabled on the Bridge by default.

detail:

To configure SSH access to the Bridge CLI:

1. Log on to the Bridge GUI *admin* account and select **SECURITY SETTINGS** from the menu on the left.
2. In the *SECURITY* section of the *SECURITY SETTINGS* screen, select whether SSH is **Enabled** or **Disabled**.
3. Click **Apply** at the bottom of the screen.

3.6.3 Encryption Algorithm

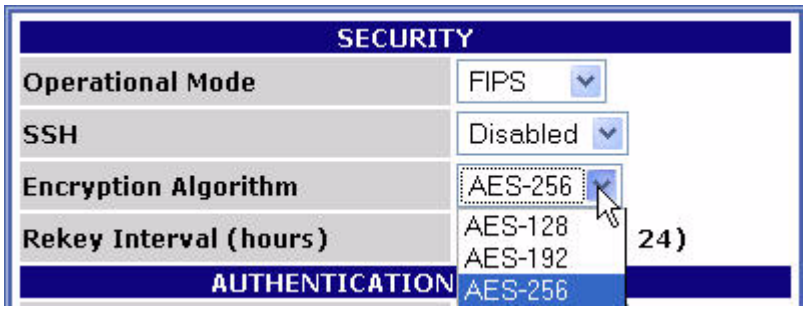
The Bridge supports the strong, AES encryption standard at these user-specified key lengths:

- AES-256 (default)
- AES-192
- AES-128

All Secure Clients logging on to the Bridge must be configured to use the same encryption algorithm and key length as the

Bridge. For information on setting encryption algorithms on Secure Clients, refer to your Fortress Secure Client user guide.

detail:



To change the Bridge encryption algorithm:

1. Log on to the Bridge GUI *admin* account and select **SECURITY SETTINGS** from the menu on the left.
2. On the *CRYPTO ALGORITHM* section of the *SECURITY SETTINGS* screen, select the AES key length to be used to encrypt network data.
3. Click **Apply** at the bottom of the screen.

3.6.4 Re-keying Interval

The Fortress Bridge generates new keys at defined intervals, renegotiating dynamic keys with Secure Clients whenever those Clients are logged on. You can specify the re-keying interval, in hours, at values between 1 and 24. The default is 4.

At the default, for example, to decrypt data intercepted over a twelve-hour period, a hacker would have to recover three sets of keys from the Bridge, in addition to the keys generated by connecting devices' re-keying behaviors, quickly enough to use them before the next re-key—the possibility of which is vanishingly remote.

NOTE: Every new key negotiation adds network traffic, and the increased security of shorter re-keying intervals should be balanced against throughput considerations.

To change the Bridge's re-keying interval:

1. Log on to the Bridge GUI *admin* account and select **SECURITY SETTINGS** from the menu on the left.
2. On the *RE-KEYING INTERVAL* section of the *SECURITY SETTINGS* screen, select the number of hours, in whole numbers from 1 to 24, that will elapse between new key negotiations with the Bridge.
3. Click **Apply** at the bottom of the screen.

3.6.5 Access ID

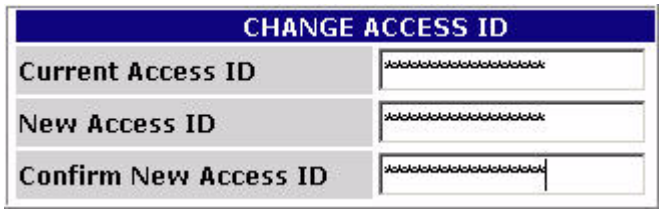
The Access ID provides network authentication for the Fortress Security System. This 16-digit hexadecimal ID is established during Bridge installation, after which the same Access ID must be specified for every Fortress Secure Client of the Bridge.

NOTE: The default Access ID is represented by 16 zeros or the word *default*, which, when configured as a new Access ID, returns the Bridge's Access ID to its default setting.

Likewise, if you change the Bridge's Access ID, you must subsequently make the same change to all of its Secure Clients' Access IDs. For information on setting the Access ID

on Secure Clients, refer to your Fortress Secure Client user guide.

detail:



To change the Bridge's Access ID

1. Log on to the Bridge GUI *admin* account and select **SECURITY SETTINGS** from the menu on the left.
2. In the *CHANGE ACCESS ID* frame of the *SECURITY SETTINGS* screen:
   - Enter the *Current Access ID.*
   - Enter a 16-digit hexadecimal number to serve as the *New Access ID*.
   - Re-enter the new Access ID in *Confirm New Access ID*.
3. Click **Apply** at the bottom of the screen.

CAUTION: For security reasons, the Access ID in effect on the Bridge cannot be displayed. *Make a note of the new Access ID:* you will need it to configure the Bridge's Secure Clients, as well as to change the Access ID on the Bridge.

3.6.6 Non-802.1X Authentication Global and Default Settings

The settings that enable and disable non-802.1X device and user authentication on the Fortress Bridge are located in the *AUTHENTICATION SETTINGS* frame of the *SECURITY SETTINGS* screen.

802.1X Security, in Section 3.3.4.5, describes the settings that select and configure 802.1X authentication for wireless devices. Section 3.4 covers *802.1X Server and LAN Port Settings*.

NOTE: The Bridge supports 802.1X authentication through separate and unrelated configuration settings.

This screen is also where the global setting for the maximum number of allowable authentication attempts is set and where the session timeout login prompt is disabled/enabled.

Default values for new devices and users are configured on the *SECURITY SETTINGS* screen as well.

Subsequent authentication configuration options are determined by whether you choose to enable authentication and, if you do, whether you implement authentication locally or through an external RADIUS (Remote Authentication Dial-In User Service) server. Your choices are also affected by whether you use both user and device authentication. The availability of Bridge GUI *AUTHENTICATION SETTINGS* reflects these differences when you apply new settings.

NOTE: To support smart cards authenticated through PKI (Public Key Infrastructure), the Bridge must be configured to use an **External** RADIUS server that supports EAP-TLS authentication. (Refer to your RADIUS documentation for guidance on configuring the service.)

The Bridge GUI includes separate, dedicated screens to manage authentication for devices and for users. These screens are only available when **Local** authentication has been

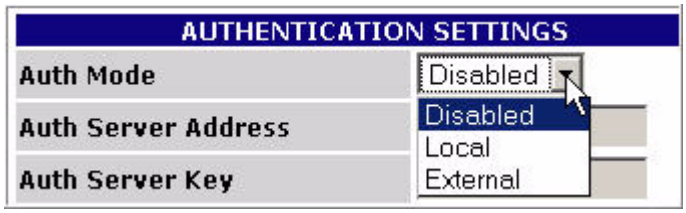
selected and, in the case of device authentication, when it has been globally enabled in the *AUTHENTICATION SETTINGS* frame of the *SECURITY SETTINGS* screen. These screens are described in Section 4.1 (Device Authentication) and Section 4.2 (User Authentication), in the next chapter.

3.6.6.1 Enabling/Disabling Authentication Globally

The Fortress Bridge has an internal RADIUS server built-in. The Bridge additionally supports an external RADIUS server.

Authentication (device and user) is disabled/enabled globally on the Bridge by selecting **Disabled**, **Local** or **External** in the *AUTHENTICATION SETTINGS* frame of the *SECURITY SETTINGS* screen.

detail:



To enable/disable all authentication:

1. Log on to the Bridge GUI *admin* account and select **SECURITY SETTINGS** from the menu on the left.
2. In the *AUTHENTICATION SETTINGS* frame, in the *Mode* field, select one of:
   - **Disabled** - disables authentication (the default)
   - **Local** - enables authentication through the Bridge's internal RADIUS server (and enables local configuration of authentication settings)
   - **External** - enables authentication through an external RADIUS server (and disables local configuration of authentication settings)
3. Click **Apply** at the bottom of the screen.
4. If you selected **Disabled** or **Local**, skip this step.

   or

   If you selected **External**, go on to the instructions in Section 3.6.6.3, to configure an external RADIUS server.

NOTE: If you are using the RADIUS server internal to a Bridge in a point-to-point or point-to-multi-point deployment, configure the root Bridge to use **Local** authentication. Then configure the non-root Bridge(s) to use **External** authentication and their *AUTHENTICATION SETTINGS* to point to the root Bridge.

3.6.6.2 Local Authentication Server

Because the Fortress Bridge's RADIUS server is built in, once you have chosen **Local** authentication, no further server configuration is required, and the field that configures the external authentication server's IP address is grayed out to reflect your choice.

The RADIUS server internal to the Fortress Bridge automatically adopts the shared key configured on the Bridge.

NOTE: Device authentication is supported only for **Local** authentication.

The default *Auth Server Key* is **`fortress`**, which you can optionally change.

Selecting **Local** authentication enables the screens and fields that configure local authentication settings for both users and devices.

3.6.6.3 External Authentication Server

The Bridge can be integrated with an external Remote Authentication Dial-In User Service (RADIUS). It supports the open source freeRADIUS.

Also, in a point-to-point or point-to-multipoint Bridge deployment that uses the RADIUS server internal to the root Bridge for authentication, only the root Bridge is configured for **Local** authentication, while the other Bridge(s) in the network are configured to use the root Bridge's RADIUS server as an **External** authentication server.

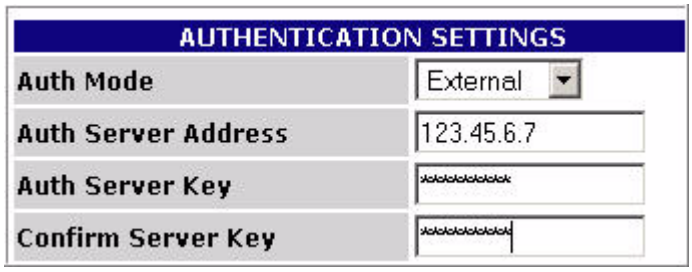
The screens and fields that configure local authentication settings for users and devices are disabled when **External** authentication is selected. (These settings are configured on the external authentication server.)

To use the Bridge with an external RADIUS server, the Bridge must be added as a RADIUS Network Access Server (NAS) client and assigned a shared key for communication with RADIUS. Please refer to your RADIUS documentation for guidance.

NOTE: The Bridge has not been tested with, and may not fully support, other common RADIUS servers. Contact your Fortress representative for more detail about third-party RADIUS support.

NOTE: If you are using both RADIUS and 802.1X authentication services, they can run on the same external server, but you must enter the server's settings both on the *SECURITY SETTINGS* screen (in the *AUTHENTICATION SETTINGS* section) and on the *INTERFACES* screen (in the *802.1X AUTHENTICATION SERVER* frame).

detail:



To configure an external RADIUS server:

1. Log on to the Bridge GUI *admin* account and select **SECURITY SETTINGS** from the menu on the left.
2. In the *AUTHENTICATION SETTINGS* frame:
   - Ensure that *Auth Mode* is **External**.
   - In *Auth Server Address*, enter the IP address of your external RADIUS server.
   - In *Auth Server Key,* enter the shared key assigned to the Bridge in RADIUS.
   - In *Confirm Server Key,* re-enter the shared key (to guard against entry errors).
3. Click **Apply** at the bottom of the screen.

NOTE: The server key you enter here should already be present in the RADIUS service configuration.

3.6.6.4 Enabling/Disabling Device Authentication

On a Fortress Bridge configured for **Local** authentication, the settings in the *AUTHENTICATION OPTIONS* section of the *AUTHENTICATION SETTINGS* frame globally enable/disable device authentication, according to whether device authentication is included in the selection you make.

detail:

To enable/disable device authentication:

1. Log on to the Bridge GUI *admin* account and select **SECURITY SETTINGS** from the menu on the left.
2. In the *AUTHENTICATION SETTINGS* frame, *Auth Mode*, ensure that **Local** authentication is enabled.
3. In the *AUTHENTICATION OPTIONS* fields, click the button to select one of:
   - **User Auth Only** - disables device authentication
   - **Device Auth** - enables device authentication
4. If you disabled device authentication, skip this step.

   or

   If you enabled device authentication, determine the default user authentication setting for new devices:
   - check the box beside **with User Auth by default** to enable user authentication by default for new devices auto-populating the *DEVICE AUTHENTICATION* screen. This is the default setting.

   or
   - clear the checkbox beside **with User Auth by default** to disable user authentication by default for new devices auto-populating the *DEVICE AUTHENTICATION* screen.
5. Click **Apply** at the bottom of the screen.

NOTE: Although devices are not required to use it, user authentication cannot be globally disabled on the Bridge, as such. As long as authentication is enabled, you can enter users into the user database.

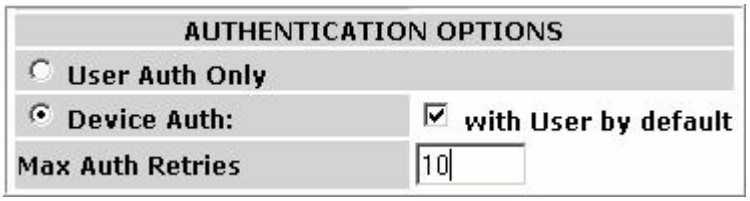
NOTE: You can change the user authentication setting for devices individually—on the *DEVICE AUTHENTICATION* screen, described in Section 4.1.2.

3.6.6.5 Maximum Authentication Retries

The setting that configures the maximum number of unsuccessful authentication attempts that the Bridge will allow before terminating a session applies simultaneously to both device and user authentication. It can be configured on the Bridge only when **Local** authentication is selected.

This parameter can not be configured for individual users or devices nor can it be set separately for the two types of authentication. It can only be set globally.

detail:



To configure maximum authentication attempts:

1. Log on to the Bridge GUI *admin* account and select **SECURITY SETTINGS** from the menu on the left.
2. In the *AUTHENTICATION SETTINGS* frame, in the *Auth Mode* field, ensure that **Local** authentication is enabled.
3. Under *AUTHENTICATION OPTIONS*, in the *Max Auth Retries* field, enter a whole number between 1 and 255.
4. Click **Apply** at the bottom of the screen.

A devices that exceeds the maximum allowable retry attempts to connect to the Bridge-secured network is locked out until the device's *State* is set to **Allowed**. Such a device is locked out on every Bridge in a point-to-multipoint network, and you must change the device's *State* setting on every Bridge that handles traffic from the device.

Users who exceed the maximum allowable retry attempts to log on to the Bridge-secured network are locked out until you reset their sessions.

3.6.6.6 Restart Session Login Prompt

When the *Restart Session Login Prompt* is enabled on the Bridge, the sessions of users whose traffic is passed by that Bridge timeout at the configured interval, forcing these users' devices to renegotiate encryption keys and prompting users to reauthenticate by entering their user names and passwords.

In point-to-point and point-to-multipoint deployments, such a user would be prompted for his credentials by every Bridge that passes traffic from that user's device.

To avoid repeated login prompts for these users, disable *Restart Session Login Prompt* on all of the non-root Bridges on the network. This will allow the user to reauthenticate and the device to re-key with only the root Bridge.

detail:

To enable/disable user session timeout login prompts:

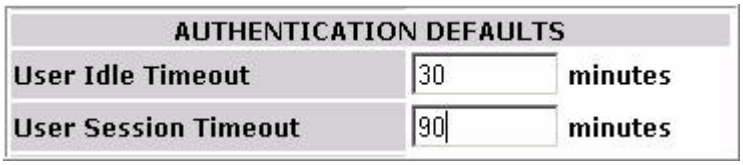
1. Log on to the Bridge GUI *admin* account and select **SECURITY SETTINGS** from the menu on the left.
2. In the *AUTHENTICATION SETTINGS* frame:
   - Check the box for **Restart Session Login Prompt** to enable user session timeout prompts (the default).

   or
   - Clear the checkbox for **Restart Session Login Prompt** to disable user session timeout prompts.
3. Click **Apply** at the bottom of the screen.

3.6.6.7 Default User Authentication Settings

The default *Idle Timeout* and *Session Timeout* settings that will automatically populate the corresponding fields in the *ADD USER* frame of the *USER AUTHENTICATION* screen are configured on the *SECURITY SETTINGS* screen. You can change these settings for users individually (on the *USER AUTHENTICATION* screen, described in Section 4.2.2).

detail:



To configure default idle and session timeouts for authenticated users:

1. Log on to the Bridge GUI *admin* account and select **SECURITY SETTINGS** from the menu on the left.
2. In the *AUTHENTICATION SETTINGS* frame, in *Auth Mode*, ensure that **Local** authentication is enabled.
3. Under *AUTHENTICATION DEFAULTS*:
   - In *User Idle Timeout* - enter the number of whole minutes, between 1 and 9999, that a user's device can be idle on the network before it must renegotiate keys with the Bridge. Enter zero (0) to disable idle timeouts. The default setting is 30 minutes.
   - In *User Session Timeout* - enter the number of whole minutes, between 1 and 9999, that a user's device can be present on the network before the current session is ended and the user must log back in to re-establish the connection. Enter zero (0) to disable session timeouts. The default setting is 720 minutes.
4. Click **Apply** at the bottom of the screen.

3.6.6.8 Default Device Authentication Settings

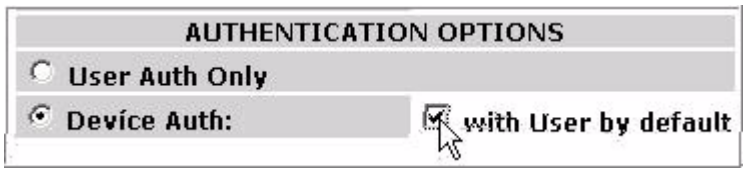
Whether or not user authentication is enabled by default for new devices automatically populating the *DEVICE AUTHENTICATION* screen is configured on the *SECURITY SETTINGS* screen, as is the default *Device State* setting they are initially assigned.

To configure the default user authentication and device state for authenticating devices:

1 Log on to the Bridge GUI *admin* account and select **SECURITY SETTINGS** from the menu on the left.

2 In the *AUTHENTICATION SETTINGS* frame, in *Auth Mode*, ensure that **Local** authentication is enabled and that *Device Auth* is selected under *AUTHENTICATION OPTIONS* (refer to sections 3.6.6.1 and 3.6.6.4, respectively).

detail:



3 Under *AUTHENTICATION OPTIONS*, to the right of *Device Auth*:

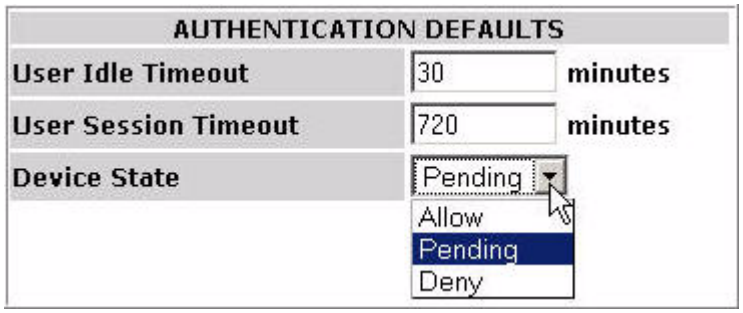
- check the box beside **with User Auth by default** to enable user authentication for new devices by default. (This is the default setting.)

or

- clear the checkbox beside **with User Auth by default** to disable user authentication for new devices by default.

NOTE: You can change the user authentication and device state settings for devices individually—on the *DEVICE AUTHENTICATION* screen, described in Section 4.1.2.

detail:



4 Under *AUTHENTICATION DEFAULTS*, in the *Device State* field, select one of:

- **Allow** - the device will be allowed to connect.
- **Pending** - connection requires administrator action (explicitly changing the device's *Auth State* to **Allow**).
- **Deny** - the device is not allowed on the network.

5 Click **Apply** at the bottom of the screen.

3.7 Blackout Mode

The *BLACKOUT MODE* setting on the Fortress Bridge globally turns the front-panel LEDs on and off.

When *BLACKOUT MODE* is *Enabled*, none of the front-panel indicators will illuminate for any reason—except for a single, initial blink (green) of less than half a second, at the beginning of the boot process.

When *BLACKOUT MODE* is *Disabled* (the default), the front-panel LED indicators function normally.

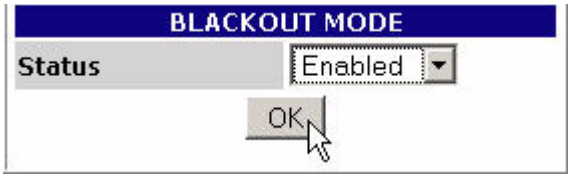
Front-panel LED behaviors and their associated meanings are covered in Section 5.6.

NOTE: When the Bridge is in blackout mode, you can temporarily toggle front-panel LEDs back on—to use them during front-panel configuration—by pressing **SW1** on the front panel.

To enable/disable blackout mode:

1 Log on to the Bridge GUI *admin* account and select **SYSTEM OPTIONS** from the menu on the left.

detail:



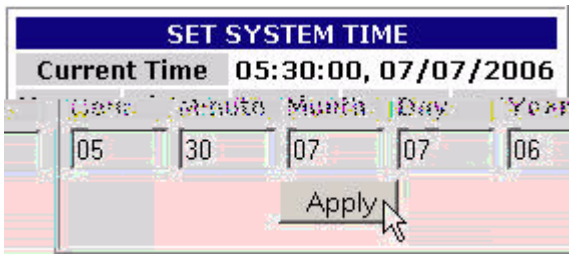
2 Under *BLACKOUT MODE*, in the *Status* field choose to **Enable** *BLACKOUT MODE* (turn the LEDs off) or **Disable** *BLACKOUT MODE* (turn the LEDs on).

3 Click **OK** in the *BLACKOUT MODE* frame.

You can also enable/disable blackout mode through the Bridge's front-panel switches (refer to Section 3.10.1.2)

3.8 System Date and Time

detail:



To change the date and time on the Bridge:

1 Log on to the Bridge GUI *admin* account and select **SYSTEM OPTIONS** from the menu on the left.

2 At the top of the *SYSTEM OPTIONS* screen, under *SET SYSTEM TIME*, enter the time and date, using two-digit values, according to the format: **hh:mm MM:DD:YY**.

3 Click **Apply** at the bottom of the *SET SYSTEM TIME* frame.

NOTE: The *SYSTEM DATE AND TIME* screen features an informational timestamp. The refresh function of your browser updates this timestamp.

3.9 Restoring Default Settings

The Fortress Bridge's factory default configuration settings can be restored in their entirety through the Bridge CLI (refer to Section 6.4.7) or via the front-panel switches (refer to Section 3.10.3).

After default settings are restored, the Bridge will have to be reconfigured for use, just as though it were newly installed, out of the box.

Because the Bridge's configuration settings could themselves be sensitive, Fortress Technologies recommends restoring them to their default values whenever the Bridge is to be shipped (or otherwise transported) out of a secured location.

3.10 Front-Panel Operation

The Fortress Bridge front panel is equipped with three, recessed buttons: two switches (labeled **SW1** and **SW2**) and a **Reset** button.

3.10.1 Mode Selection from the Front Panel

The front-panel switches can be used to select the *Bridge Mode* of the Bridge's internal Radio 2 as well as to turn the Bridge's front-panel LEDs off and on (enable/disable blackout mode).

Each of these Bridge settings has only two possible values. Configuring them through the front-panel switches toggles the setting from its current value to the alternate value.

NOTE: Refer to Section 3.3.1.4 for more information about *Bridge Mode* and to Section 3.7 for an explanation of blackout mode.

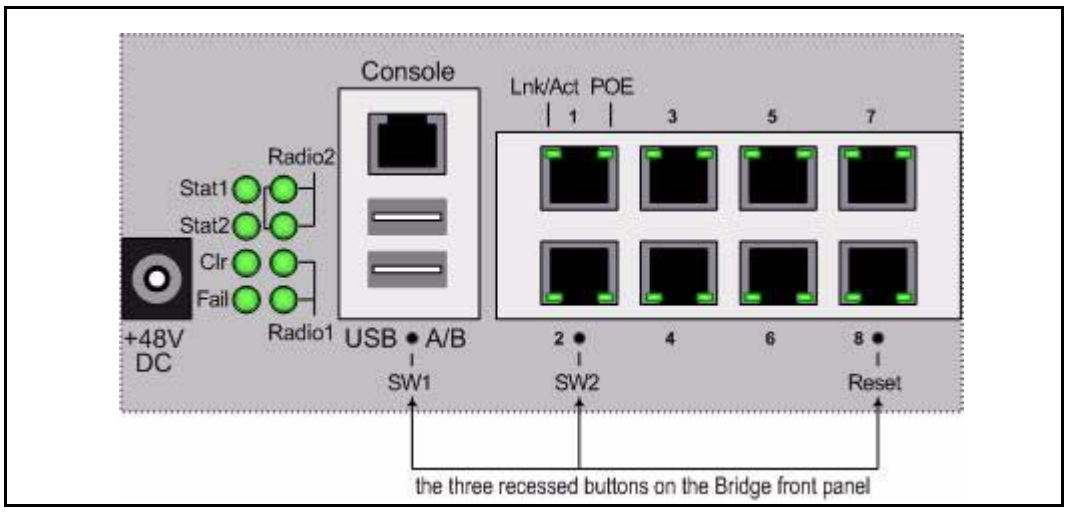


Figure 3.2. Front-panel buttons

3.10.1.1 Toggling the Bridge Mode Setting on Radio 2

Radio 2 is in **Bridge** *Radio Mode* by default, and its default *Bridge Mode* setting is **Root**.

If this setting is still at its default value, the procedure below will change the *Bridge Mode* setting to **Non-Root**. (If the setting is currently **Non-Root**, the procedure will return the setting to **Root**.)

If Radio 2's *Radio Mode* setting has been changed to **AP**, the procedure below will still toggle the radio's *Bridge Mode* setting, but the new setting will not take effect until the *Radio Mode* has been set again to **Bridge**.

NOTE: You can also change the *Bridge Mode* setting in the Bridge GUI (Section 3.3.1.4) or in the Bridge CLI (Section 6.4.3).

1. Press **SW1** and hold it down for five seconds—just until the upper **Radio** LEDs go out, then immediately release it. The **Stat1** LED should be flashing slowly (green).
2. While **Stat1** is flashing, press and quickly release **SW2** once. Reconfiguration of Radio 2's *Bridge Mode* setting is

indicated by the **Stat2** LED, which flashes rapidly (green) when the new mode is selected.

If you accidentally cycle past the *Bridge Mode* setting, continue pushing **SW2** until **Stat2** again begins flashing.

3 When **Stat2** is flashing, press **SW1** and hold it down for two seconds to save the new *Bridge Mode* setting. The **Stat1** and **Stat2** LEDs will stop flashing and light solid green to indicate that you have successfully changed Radio 2's *Bridge Mode*.

If you skip Step 3, the front-panel configuration operation will time out after 60 seconds, and the *Bridge Mode* setting will remain unchanged.

After you have successfully saved the new setting, the Bridge will reboot automatically so that the new setting can take effect.

After booting, Bridge LEDs will resume normal operation.

3.10.1.2 Toggling the Blackout Mode setting

The default blackout mode setting is *Disabled*, in which state the Bridge's front-panel LEDs illuminate to indicate various conditions on the Fortress Bridge. (Front-panel LED behaviors and their associated meanings are covered in Section 5.6.)

Enabling blackout mode turns all front-panel LEDs off.

If blackout mode is *Disabled*, the procedure below will enable it (turn off the front-panel LEDs). If the Bridge is already in blackout mode, the procedure will disable it (turn the front-panel LEDs back on)

1 Press **SW1** and hold it down for five seconds—just until the upper **Radio** LEDs go out, then immediately release it. The **Stat1** LED should be flashing slowly (green).

2 While **Stat1** is flashing, press and quickly release **SW2** twice. Reconfiguration of the blackout mode setting is indicated by the **Clr** LED, which flashes rapidly (green) when the new mode is selected.

If you accidentally cycle past the blackout mode setting, continue pushing **SW2** until **Clr** again begins flashing.

3 When **Clr** is flashing, press **SW1** and hold it down for two seconds to save the new blackout mode setting. The **Stat1** and **Clr** LEDs will stop flashing and light solid green to indicate that you have successfully changed the Bridge's blackout mode.

If you skip Step 3, the front-panel configuration operation will time out after 60 seconds, and the blackout mode setting will remain unchanged.

After you have saved the change, Bridge LEDs will either resume their normal operation (*BLACKOUT MODE: Disabled*), or go completely dark (*BLACKOUT MODE: Enabled*), according to the new setting.

NOTE: You can also change the *BLACKOUT MODE* setting in the Bridge GUI (Section 3.7) or in the Bridge CLI (Section 6.4.5.9).

NOTE: When the Bridge is in blackout mode, you can temporarily toggle front-panel LEDs back on—to use during further front-panel configuration—by pressing **SW1**.

3.10.2 Rebooting the Bridge from the Front Panel

To reboot the Fortress Bridge from the front-panel:

1. Press and hold the **Reset** button for one second, until the **Stat1** LED exhibits a slow green flash to indicate that the Bridge is rebooting.
2. Release the button.

After the Bridge reboots the **Stat1** LED will again light solid green.

NOTE: There are no LED indications in a Bridge in blackout mode (refer to Section 3.7).

3.10.3 Restoring Defaults from the Front Panel

To restore the Bridge's configuration settings to their factory-default values:

1. Press and hold **SW1**.
2. Still holding **SW1**, press and hold **SW2** for 10 seconds.

   All LEDs will flash fast (green) to indicate that factory default settings will be restored.
3. Hold both switches down for another 10 seconds, until all LEDs light solid green.

   If you release the switches before the LEDs light solid green, the operation is cancelled and settings will remain unchanged.
4. Release both switches.

After you have successfully initiated the restore operation, the Bridge will reboot automatically.

After booting, the Bridge LEDs will resume normal operation and all configuration settings, including the IP address of the Bridge's management interface will be at their factory-default values.

NOTE: You can also restore the Bridge's factory default settings from the Bridge CLI (Section 6.4.7).

Chapter 4
Administration

4.1 Device Authentication

Device authentication is supported only for **Local** authentication. (When **External** authentication is selected, the settings that configure device authentication are grayed out to reflect your selection.)

On a Fortress-secured network with device authentication enabled, a unique *Device ID* is generated for each device connecting from an encrypted zone. The Device ID is subsequently used to authenticate that device on the network.

The Fortress Bridge has an internal RADIUS (Remote Authentication Dial-In User Service) server built-in. The Bridge additionally supports external RADIUS servers.

Authentication (device and user) is enabled and disabled globally on the Bridge by selecting **Disabled**, **Local** or **External** on the *AUTHENTICATION SETTINGS* frame of the *SECURITY SETTINGS* screen. Device authentication can be enabled only when **Local** authentication is selected.

When device authentication is enabled, the Bridge detects devices attempting to access the Bridge's encrypted zone and lists them on the *DEVICE AUTHENTICATION* screen.

Device authentication is globally enabled—for Bridge's configured for **Local** authentication—when it is included in the selection made in *AUTHENTICATION OPTIONS* on the *SECURITY SETTINGS* screen.

For any given device, device authentication can be used by itself or combined with the Bridge's provisions for user authentication.

NOTE: The Bridge supports 802.1X authentication through separate and unrelated configuration settings. These are described in *802.1X Security* (for wireless devices) and in Section 3.4, *802.1X Server and LAN Port Settings*.

NOTE: Refer to Section 3.6.6.1 for instructions on globally enabling authentication and to Section 3.6.6.4 for instructions on globally enabling device authentication and configuring devices' default user authentication option.

4.1.1 Maximum Device Authentication Retries

The maximum number of unsuccessful authentication attempts a device will be allowed before ending its session is also configured globally; the same setting configures the maximum number of times users can unsuccessfully attempt to

authenticate on the network. (Refer to Section 3.6.6.5 for detailed instructions.)

If a device exceeds the maximum allowable retry attempts to connect to the Bridge-secured network, that device will be locked out until the device's *State* is set to **Allow**. Such a device is locked out on every Bridge in a point-to-multipoint network, and you must change the device's *State* setting on every Bridge that handles traffic from the device.

4.1.1 Default Device Authentication Settings

As devices auto-populate the *DEVICE AUTHENTICATION* screen, they are permitted or denied immediate access to the network based on the default *Device State* setting, located in the *AUTHENTICATION SETTINGS* frame of the *SECURITY SETTINGS* screen (under *AUTHENTICATION DEFAULTS*).

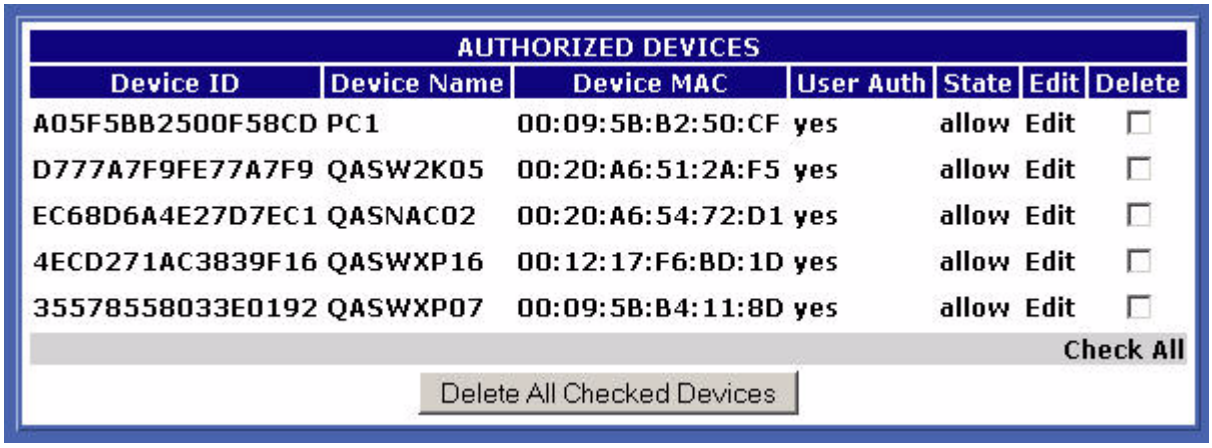
Another default setting in the *AUTHENTICATION SETTINGS* frame determines whether user authentication is included by default for devices auto-populating the *DEVICE AUTHENTICATION* screen.

Whatever default settings you choose for authenticating devices, you can change the initial *Device State* and *AUTHENTICATION OPTIONS* settings individually for any device on the *DEVICE AUTHENTICATION* screen.

NOTE: Refer to Section 3.6.6.8 for detailed instructions on configuring the default device state and user authentication option settings for new devices.

4.1.2 Individual Device Authentication Settings

Devices will auto-populate the *DEVICE AUTHENTICATION* screen only when device authentication is enabled in the *AUTHENTICATION SETTINGS* frame of the *SECURITY SETTINGS* screen (refer to Section 3.6.6, Non-802.1X Authentication Global and Default Settings).



The Fortress Bridge tracks and manages access for devices on the Fortress-secured network through two identifiers, which are *not* user-configurable:

- *Device ID* - a unique, 16-digit hexadecimal identifier generated for the device and used to authenticate it on the network
- *Device MAC* - the device's MAC address

Access user configurable settings for an authenticating device by clicking its **Edit** button under *AUTHORIZED DEVICES* (Section 4.1.2.1). Configurable settings include:

- *Device Name* - accepts up to 64 alphanumeric characters by which you can identify the device.

  If a device has a hostname associated with it (the hostname of a laptop running the Fortress Secure Client, for instance), that hostname is included for the device when it is first added to the *DEVICE AUTHENTICATION* screen. If no hostname is associated with the device, it will be added without one.
- *Auth Option* - configures whether the Bridge will additionally require user authentication before allowing the device to connect to the encrypted zone.

  If you enabled **Local** authentication while leaving the settings under *AUTHENTICATION OPTIONS* (Section 3.6.6.8) at their defaults, devices auto-populate the *AUTHORIZED DEVICES* list with the user authentication option.
- *Auth State* - configures the initial state of the device's connection to the encrypted zone:
  - **Allow** - the device will be allowed to connect.
  - **Pending** - connection requires administrator action: Change the device's *Auth State* to **Allow**.

    If you enabled **Local** authentication while leaving settings under *AUTHENTICATION DEFAULTS* (Section 3.6.6.8) at their defaults, devices auto-populate the *AUTHORIZED DEVICES* list a *State* of **Pending**.
  - **Deny** - the device is not allowed on the network.

4.1.2.1 Editing a Device

You can edit an existing hostname or add one for a device that has no hostname. You can also reconfigure any individual device's *Auth Option* and *Auth State*.

To edit a device:

1 Log on to the Bridge GUI *admin* account and choose **DEVICE AUTHENTICATION** from the menu on the left.

2 On the *DEVICE AUTHENTICATION* screen, click the **Edit** button of the device for which you want to change settings.

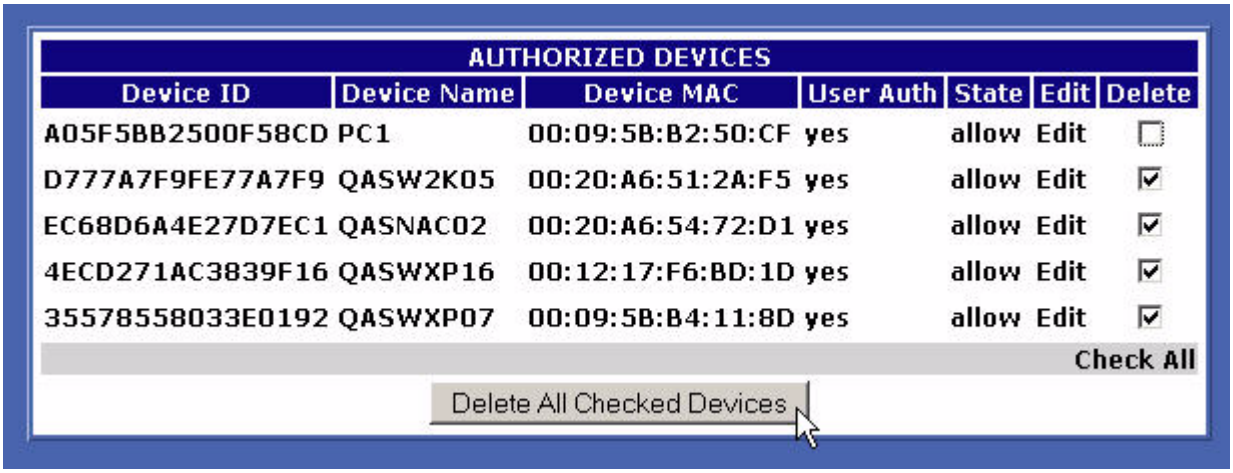
3 In the *EDIT DEVICE* frame (above the device list) where the device's current settings are displayed, enter new values into the relevant fields (described in Section 4.1.2).

4 Click **Update** to save the edited settings (or **Cancel** your changes).

The device's entry in *AUTHORIZED DEVICES* reflects your changes.

4.1.2.2 Deleting Devices

You can delete one device, multiple devices or all devices from device authentication.



To delete one or more devices:

1 Log on to the Bridge GUI *admin* account and choose **DEVICE AUTHENTICATION** from the menu on the left.

2 On the *DEVICE AUTHENTICATION* screen, in the *AUTHORIZED DEVICES* display, place a check in the box(es) in the *Delete* column for the device(s) you want to delete, or click **Check All** below the column to select all devices for deletion.

3 Click **Delete All Checked Devices**.

The device(s) you selected will be removed from the *AUTHORIZED DEVICES* display.

4.2 User Authentication

NOTE: The Bridge supports 802.1X authentication through separate and unrelated configuration settings. These are described in *802.1X Security* (for wireless devices) and in Section 3.4, *802.1X Server and LAN Port Settings*.

You can configure default and individual user authentication parameters through the Bridge only when **Local** authentication is selected. (When **External** authentication is selected, these settings are configured on the external authentication server.)

The Fortress Bridge has an internal RADIUS (Remote Authentication Dial-In User Service) server built-in. The Bridge additionally supports external RADIUS servers.

Authentication (device and user) is enabled and disabled globally on the Bridge by selecting **Disabled**, **Local** or **External**

on the *AUTHENTICATION SETTINGS* frame of the *SECURITY SETTINGS* screen.

On a Fortress Bridge-secured network, user authentication can be used by itself or combined with device authentication. The options that determine whether device authentication is enabled are also configured globally, in the *AUTHENTICATION SETTINGS* frame of the *SECURITY SETTINGS* screen.

4.2.1 Maximum User Authentication Retries

The maximum number of unsuccessful authentication attempts a user will be allowed before being locked out is another global setting; the same setting configures the maximum number of times devices can unsuccessfully attempt to authenticate on the network. (Refer to Section 3.6.6.5 for detailed instructions.)

If a user exceeds the maximum allowable retry attempts to log on to the Bridge-secured network, s/he will be locked out until you reset the session.

NOTE: Refer to Section 3.6.6.1 and for instructions on globally enabling **Local** authentication and to Section 3.6.6.4 for instructions on enabling device authentication.

4.2.1 Default User Authentication Settings

While idle timeout and session timeout settings can be individually configured for each user, the default values for these settings are determined by the *AUTHENTICATION DEFAULTS* set in the *AUTHENTICATION SETTINGS* frame of the *SECURITY SETTINGS* screen.

NOTE: Refer to Section 3.6.6.7 for detailed instructions on configuring default user authentication settings.

4.2.2 Individual User Authentication Settings

User authentication on the Fortress Bridge requires the usual settings to identify, track and manage access for each user on the Fortress-secured network:

- *Username* - identifies the user on the network—from 1 to 16 alphanumeric characters—required.
- *Full Name* - associates the person, by name, with his/her user account—up to 64 alphanumeric characters, including spaces, dashes, dots and underscores—optional.
- *Password/Verify Password* - establishes the credentials the user must key in to access his/her user account—from 4 to 16 alphanumeric characters, including shifted numeral-key symbols—required.
- *Idle Timeout* - sets the amount of time the user's device can be idle on the network before it must renegotiate keys with the Bridge.

  Idle Timeout is set in minutes, between 0 and 9999. A value of zero disables idle timeout for that user (his device can be idle indefinitely without timing out). If you enabled **Local** authentication while leaving the settings under *AUTHENTICATION DEFAULTS* (Section 3.6.6.7) at their defaults, the *Idle Timeout* value in the *ADD USER* frame will be at 30 minutes.

- *Session Timeout* - sets the amount of time the user's device can be present on the network before the current session is ended and he/she must log back in to re-establish the connection.

  Session Timeout is set in minutes, between 0 and 9999. A value of zero disables session timeout for that user (her device can be present on the network indefinitely without timing out). If you enabled **Local** authentication while leaving the settings under *AUTHENTICATION DEFAULTS* (Section 3.6.6.7) at their defaults, the *Session Timeout* value in the *ADD USER* frame will be at 720 minutes.

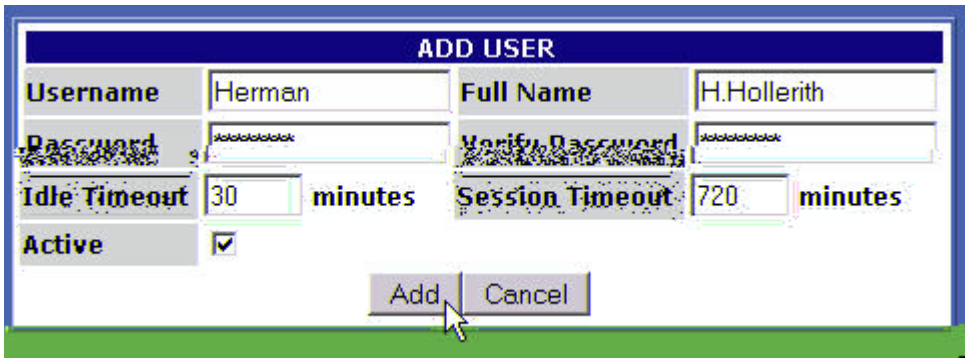
- **Active** - enables/disables user access to the account.

  A check in the box enables the account (the default); clearing the checkbox disables it.

NOTE: In point-to-point/multipoint deployments, Fortress recommends that you disable the *Restart Session Login Prompt* for users on all non-root Bridges on the network, so that, when users' sessions time out, they are prompted for their credentials by only the root Bridge. Refer to Section 3.6.6.6 guidance.

4.2.2.1 Adding a User

New user accounts can only be created on the Bridge when **Local** authentication is globally enabled (refer to Section 4.2, above).



To add a user:

1. Log on to the Bridge GUI *admin* account and choose **USER AUTHENTICATION** from the menu on the left.
2. On the *USER AUTHENTICATION* screen, in the *ADD USER* frame, enter valid values into the relevant fields (described above).
3. Click **Add** to save the new user account (or **Cancel** the addition).

   The *USER ACCOUNTS* frame shows the user you have added, with the settings you specified.

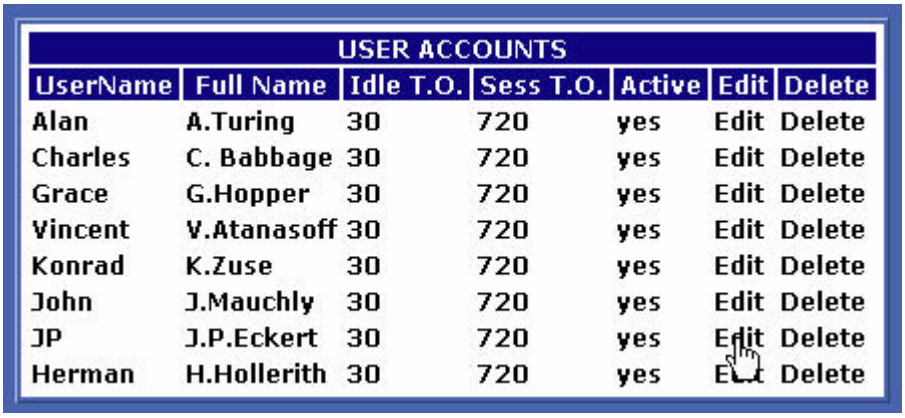
4.2.2.2 Editing a User Account

Once configured, *Username* cannot be changed. You can only delete a user's account and create a new account with a new *Username*. You can edit any other value associated with a user account.

To edit a user account:

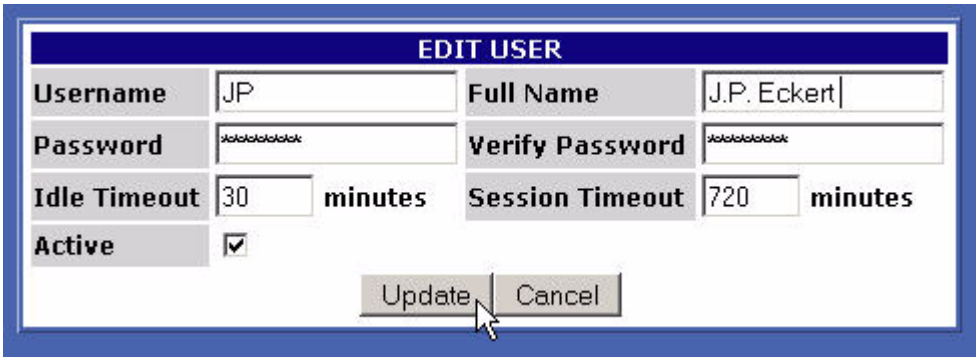
1. Log on to the Bridge GUI *admin* account and choose **USER AUTHENTICATION** from the menu on the left.

2 On the *USER AUTHENTICATION* screen, click the **Edit** button of the user for which you want to change settings.



3 In the *EDIT USER* frame (above *USER ACCOUNTS*) where the account's current settings are displayed, enter new values into the relevant fields (described in Section 4.2.2).

4 Click **Update** to save the edited settings (or **Cancel** your changes).



The user's entry in *USER ACCOUNTS* reflects your changes.

4.2.2.3 Deleting a User Account

You can delete a user account at any time. Alternatively, you can edit a user account to be temporarily inactive—by clearing the **Active** checkbox—reactivating the account at a later date (refer to Section 4.2.2.2, above).

To delete a user account:

1 Log on to the Bridge GUI *admin* account and choose **USER AUTHENTICATION** from the menu on the left.

2 On the *USER AUTHENTICATION* screen, click the **Delete** button of the user you want to delete.

3 Click **OK** in the confirmation dialog (or **Cancel** the deletion).

The user you deleted will be removed from the *USER ACCOUNTS* display.

4.3 Trusted Devices

Some wireless devices—IP phones, digital scales or printers, and APs, for example—are not equipped to run additional software such as the Fortress Secure Client. In order to allow such a device access to the encrypted zone, the Fortress Bridge must be configured to identify it as a *Trusted Device*—to which the narrowest possible access rules should be applied.

All traffic to and from Trusted Devices is sent in the clear (unencrypted).

Once its status as a Trusted Device has been configured, the Bridge uses the settings you establish for it to identify, track and manage access for the device on the network. These are:

- *TD Identifier* - accepts up to twelve, alphanumeric characters to uniquely identify the Trusted Device.
- *IP Address* - establishes the device's IP address—or, by entering the word **any**, configures the Trusted Device to accept any IP address, as provided by the network DHCP (Dynamic Host Configuration Protocol) server.
- *MAC Address* - establishes the device's MAC address.
- *Port Number(s)* - specifies the port numbers through which the Trusted Device can access the encrypted zone—or, by entering the word **any**, configures access for the device through any port.

  For reference, the screen displays commonly used port numbers to the right of the configuration fields.

When one or more Trusted Devices are configured on the Fortress Bridge, the Bridge will continually signal—through the flashing green, front-panel cleartext LED (labeled **Clr**)—that cleartext is being passed on the network. While the cleartext signal occurs in either operating mode, in FIPS terminology, it indicates that the Bridge is in *Bypass Mode* (*BPM*)

NOTE: Trusted Devices must be uniquely named on the Bridge. An error message will result if you attempt to add a Trusted Device with a name already in use.

CAUTION: Specifying that **any** port can access a TD can pose a ***significant*** security risk.

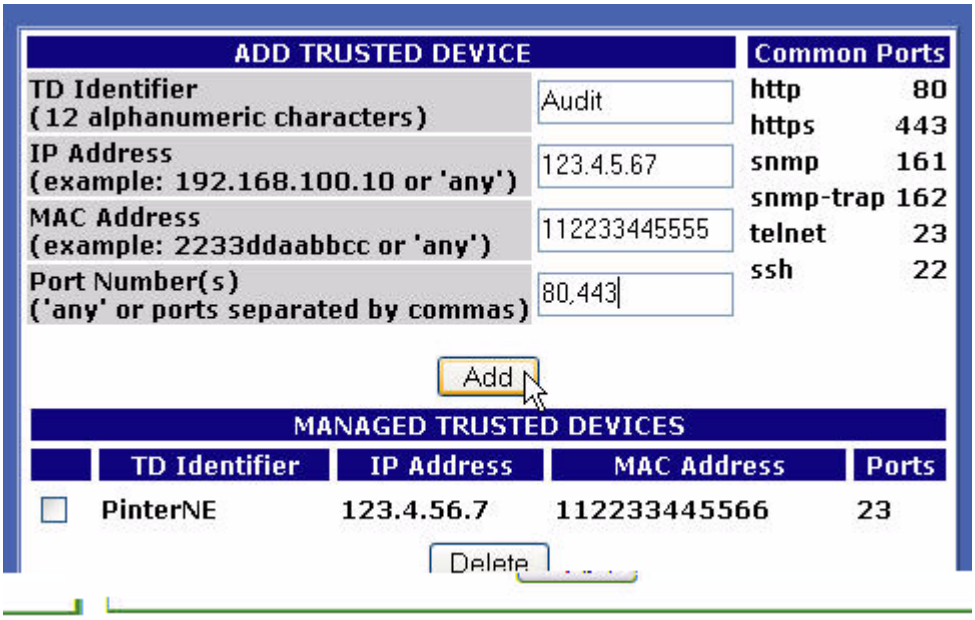
4.3.1 Adding Trusted Devices

Trusted Devices are added one at a time.

To add a Trusted Device:

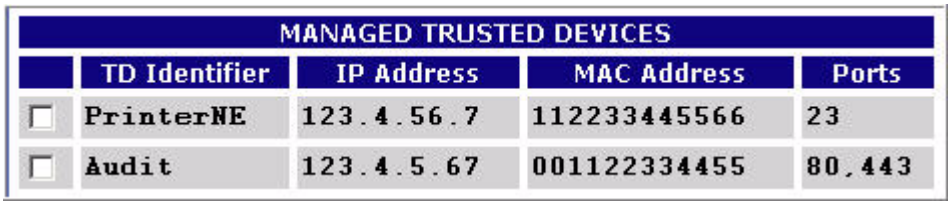
1. Log on to the Bridge GUI *admin* account and choose **TRUSTED DEVICES** from the menu on the left.
2. On the *TRUSTED DEVICES* screen, in the *ADD TRUSTED DEVICE* frame, enter valid values into the relevant fields (described above).
3. Click **Add** to save the new Trusted Device (or **Cancel** the addition).

CAUTION: Network security is maximized when the smallest possible number of Trusted Devices are configured and the smallest effective set of ports is specified for each.



The section of the frame under *MANAGED TRUSTED DEVICES* shows the Trusted Device you added, with the settings you specified.

detail:



4.3.1 Editing Trusted Devices

You can edit the IP and MAC addresses of an existing Trusted Device and change its port settings, but you cannot change its *TD Identifier*. To edit a Trusted Device:

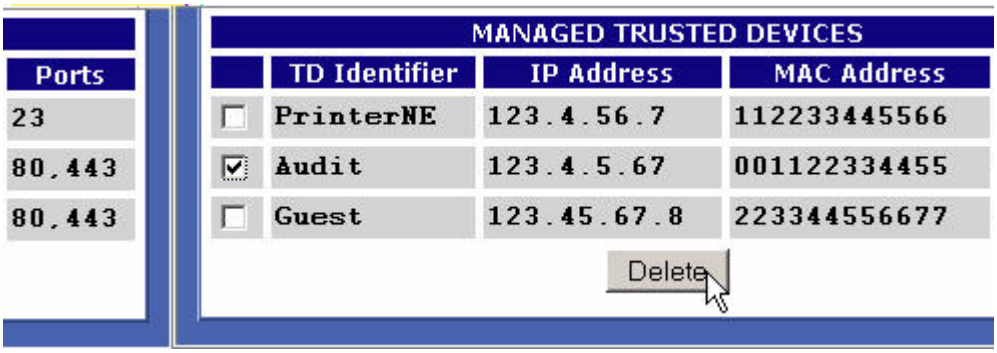
1. Log on to the Bridge GUI *admin* account and choose **TRUSTED DEVICES** from the menu on the left.
2. On the *TRUSTED DEVICES* screen, under *MANAGED TRUSTED DEVICES*, click the *TD Identifier* of the device for which you want to change the settings.
3. In the resulting *EDIT TRUSTED DEVICE* dialog, enter valid values into the relevant fields (described above).
4. Click **OK** to save the new settings (or **Cancel** your changes).

   The Trusted Device's entry under *MANAGED TRUSTED DEVICES* reflects your changes.

4.3.2 Deleting Trusted Devices

You can delete Trusted Devices one at a time, or by selecting multiple devices for deletion.

detail:



1 Log on to the Bridge GUI *admin* account and choose **TRUSTED DEVICES** from the menu on the left.

2 On the *TRUSTED DEVICES* screen, in the *MANAGED TRUSTED DEVICES* frame, check the box(es) beside the Trusted Device(s) you wish to delete and click **Delete** at the bottom of the frame.

The selected Trusted Device(s) will be removed from list of *MANAGED TRUSTED DEVICES*.

4.3.3 Visitor Access through Trusted Devices

Visitors using their own mobile devices at your facilities can be granted temporary access to the WLAN by configuring Trusted Device access for their devices, with appropriately limited port access.

Trusted Devices for visitors are managed no differently from other Trusted Devices.

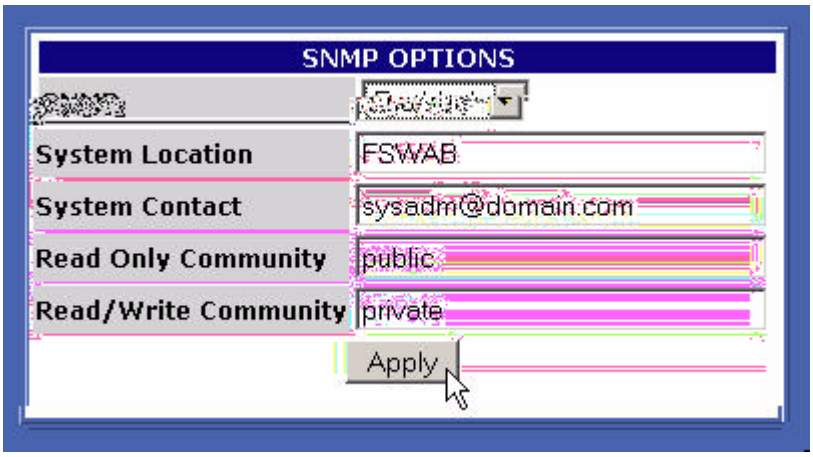
4.4 SNMP Settings

The Fortress Bridge can be configured for monitoring through SNMP (Simple Network Management Protocol) versions 1 and 2. The Fortress MIB (management information base) is included on the Bridge CD and available from: **https://www.fortresstech.com/support/products_updates.asp**.

SNMP monitoring is configured through these settings:

- *SNMP* - determines whether SNMP is **Enabled** or **Disabled** on the Bridge, according to your selection on the dropdown.
- *System Location* - identifies the Fortress Bridge.
- *System Contact* - specifies the E-mail address to which SNMP notifications are sent.
- *Read Only Community* - identifies the SNMP read-only community.
- *Read/Write Community* - identifies the SNMP read/write community.

NOTE: You cannot configure SNMP monitoring on a Fortress Bridge in *FIPS* operating mode (the default). Refer to Section 3.6.1 for more information about Bridge operating modes and to Section 6.4.5.5 for details on changing it.



4.4.1 Configuring SNMP

1. Log on to the Bridge GUI *admin* account and choose **SNMP SETTINGS** from the menu on the left.
2. In the *SNMP OPTIONS* frame, enter valid values into the relevant fields (described above).
3. Click **Apply**.

4.5 Backing Up and Restoring

The backup function of the Bridge creates and downloads a configuration file that can be used to restore those Bridge settings it saves. You can create multiple backup files under pathnames of your choosing.

Table 4.1 shows those configuration settings that are saved to, and so will be restored from, a backup file.

Because recording them could pose a security risk, no passwords are backed up. In order to maintain network security, after restoring from a backup file all passwords must be reset for each of the Bridge's password-protected accounts:

- Bridge GUI *admin* and *operator* accounts
- Bridge CLI account

Fortress Technologies recommends backing up your Bridge configuration:

- when you first set up the Bridge
- immediately before you upgrade Bridge software or make significant configuration changes
- after you have tested significant configuration changes and they have proved fully operational

NOTE: The *Bridge Mode* setting, which determines whether a Fortress Bridge in bridge mode will act a root or a non-root node, is not backed up.

Table 4.1. User Configured Settings Backed Up for the Bridge

function	setting
network	STP enable/disable
	WAN port encrypted/unencrypted
radios	radio state enable/disable
	radio band (Radio 1) 802.11g/802.11a
	radio mode AP/Bridge
	channel
	transmit power
	distance
	preamble
	beacon interval
	multicasting enable/disable
	LED RSSI monitor enable/disable
	VAP SSIDs and related settings
	any created Wireless Extension Tools scripts
802.1X authentication	802.1X authentication server settings
	LAN ports 1–8 802.1X off/on
	VAP *Security Suite* settings
security	Access ID[a]
	encryption algorithm[a]
	re-keying interval
	operating mode FIPS/Normal
	blackout mode enable/disable
	encrypted zone cleartext enable/disable
	data compression enable/disable
	SSH access on/off
non-802.1X authentication	global authentication enable/disable
	local authentication server - *or* - external server IP address
	authentication server key (local or external)
	if local authentication: device and user databases
	restart session login prompt enable/disable
SNMP	system location
	system contact
	read-only community
Trusted Devices	ID
	IP address
	MAC address
	accessible ports

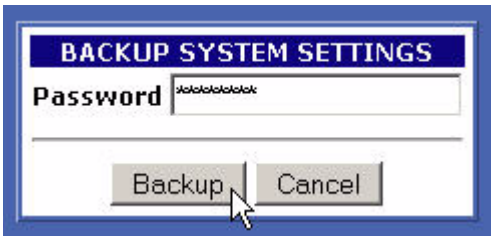
a. The Access ID and encryption algorithm are *not* backed up for a Bridge in FIPS operating mode.

4.5.1 Backing Up the Bridge Configuration

1. Log on to the Bridge GUI *admin* account and choose **SYSTEM OPTIONS** from the menu on the left.
2. On the *SYSTEM OPTIONS* screen under *BACKUP SYSTEM SETTINGS*, click **Next**.

detail:

3. On the resulting screen:
   - Optionally enter a *Password* to protect the backup file.
   - Click **Backup** (or **Cancel** the operation).



4. On the system dialog, choose to save the file to disk. The file is named *settings.fti* by default. (Windows® may append a *.gz* extension to the filename.) You can save it to any location and rename it if you choose.

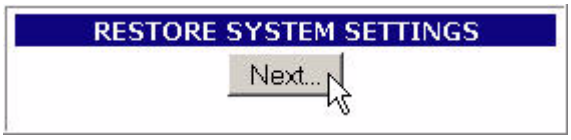
NOTE: If you choose to password-protect the backup file, remember that the password will be required in order to restore from the file.

4.5.2 Restoring from a Backup File

Keep in mind that the restore operation restores only those settings present in the backup file, as described in Section 4.5.

1. Log on to the Bridge GUI *admin* account and choose **SYSTEM OPTIONS** from the menu on the left.
2. On the *SYSTEM OPTIONS* screen under *RESTORE SYSTEM SETTINGS*, click **Next**.

detail:



3. On the resulting screen:
   - Enter or browse to the pathname of the backup file.
   - If the backup file is password-protected enter the *Password*.
   - Click **Restore** (or **Cancel** the operation).

   The GUI informs you *The settings have been successfully restored* and advises that you must reboot the system in order for the settings to take effect.
4. Click **OK** to clear the system dialog.
5. Follow the instructions in Section 4.7.
6. After you have rebooted the Bridge, change all three Bridge account passwords from their defaults, according to the instructions in Section 3.5 and Section 6.4.4.2, respectively.

CAUTION: The restore operation overwrites existing settings with those in the backup file (shown in Table 4.1), including local device and user authentication databases.

CAUTION: Restoring from a backup file causes all passwords to revert to their default values. The WLAN is *not* secure until you change all three Bridge account passwords from their defaults.

4.6 Software Versions and Upgrades

Fortress Technologies regularly releases updated versions of the Bridge software that add new features, improve functionality and/or fix known bugs. Upgrade files may be shipped to you on CD-ROM or, more often, made available for download from your account on the Fortress Technologies website.

www.fortresstech.com/support/products_updates.asp

The Fortress Bridge is compatible with Fortress Secure Client versions 2.4 and higher. Fortress recommends that the Secure Clients of the Bridge be upgraded to the most recent version of the Secure Client software available for their respective platforms and appropriate to your environment.

4.6.1 Viewing Current Software Version

The version of the firmware currently running on the Fortress Bridge is displayed on the *DIAGNOSTICS* screen, as well as on every help screen. To view the current software version:

1. Log on to the Bridge GUI *admin* account and choose **HELP** from the menu on the left.
2. Observe the version information at the top of the screen.

detail:

Alternatively:

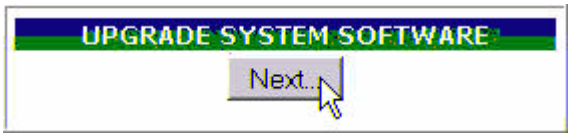
1. Log on to the Bridge GUI *admin* account and choose **DIAGNOSTICS** from the menu on the left.
2. Observe the version information at the top of the frame.

4.6.2 Upgrading Bridge Software

If necessary, download the upgrade file from Fortress Technologies web site (at the address given above).

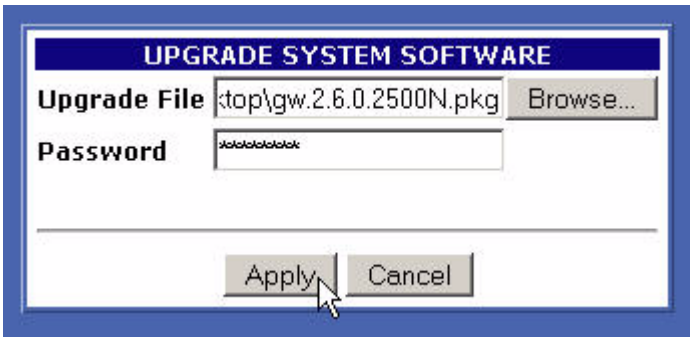
1. Log on to the Bridge GUI *admin* account and choose **SYSTEM OPTIONS** from the menu on the left.
2. On the *SYSTEM OPTIONS* screen under *UPGRADE SYSTEM SOFTWARE*, click **Next**.

detail:



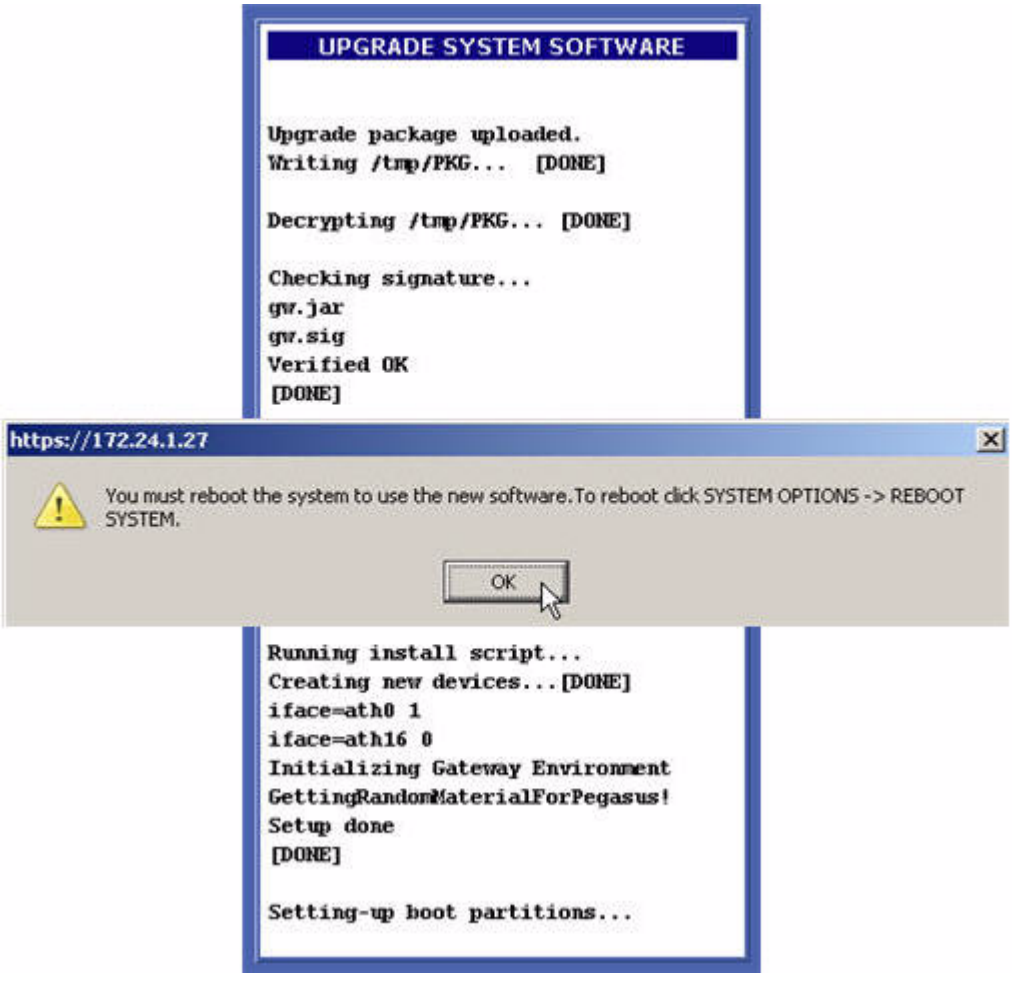
3. On the resulting screen:
   - Enter or browse to the pathname of the upgrade file.
   - In *Password* enter the default upgrade file password **`fortress`**.

- Click **Apply** (or **Cancel** the operation).



4 Click **OK** on the system confirmation dialog.

The frame displays *Uploading file...* (with crawling dots to indicate system activity), then changes to the *Performing upgrade...* status display, which presents a series of progress messages. When the process completes, the frame displays *[DONE]*, and a system dialog prompts you to reboot the Bridge.



5 Click **OK** on the system prompt.

6 Follow the instructions in Section 4.7, below.

4.7 Rebooting the Bridge

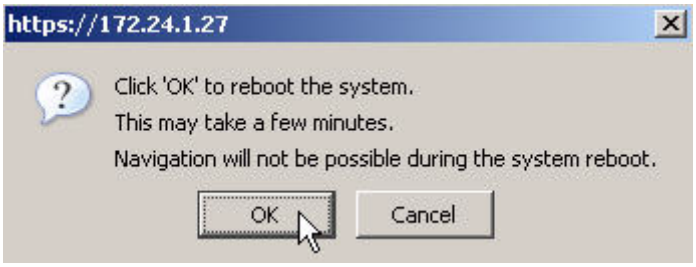
The reboot option power cycles the Bridge, ending all sessions and forcing Secure Client devices (and any other Fortress Bridges) in communication with the Bridge to re-key in order to start a new session.

1 Log on to the Bridge GUI *admin* account and choose **SYSTEM OPTIONS** from the menu on the left.

2 On the *SYSTEM OPTIONS* screen under *REBOOT SYSTEM*, click **OK**.

detail:

3 On the resulting system dialog, click **OK** again (or **Cancel** the reboot).



The Bridge emits a short chirp and its front-panel LEDs light briefly and then go briefly dark, as the Bridge begins the boot process. **Stat1** LED exhibits a slow green flash when the LEDs come back on. Then the Bridge, running the upgraded firmware, returns to normal operation (the **Stat1** LED lights solid green).

NOTE: Beyond the initial blink at the beginning of the boot process, there are no LED indications in a Bridge in blackout mode (refer to Section 3.7).

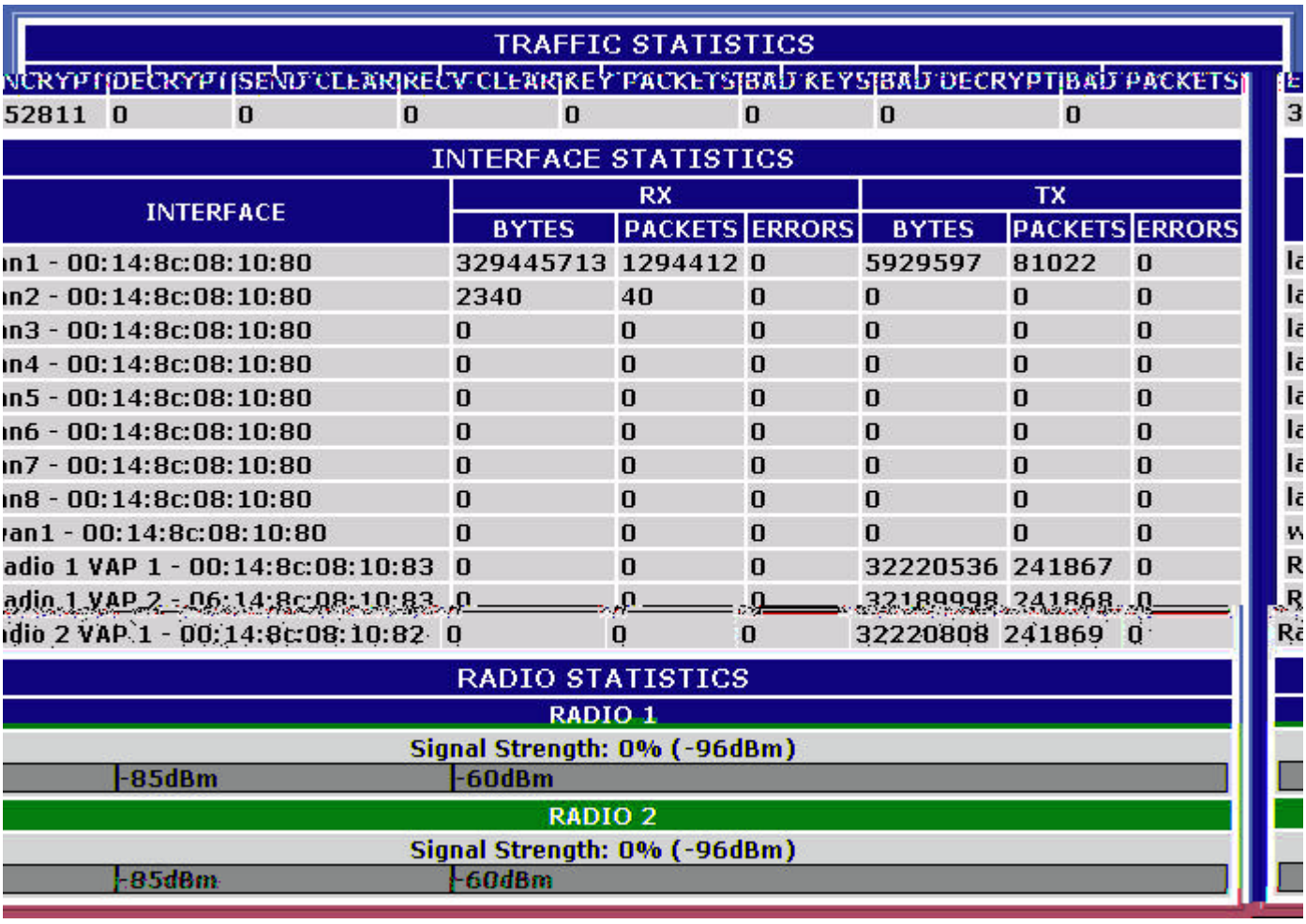
You can reboot the Bridge from the front panel (described in Section 3.10.2), from the Bridge CLI (described in Section 6.5.4), or from the Bridge GUI (described above).

Several configuration changes on the Bridge require a reboot in order to take effect. Software upgrades require you to reboot, as well. You will also need to reboot the Bridge to apply network configuration changes, and you may want to do so as part of a troubleshooting operation.

Chapter 5
Monitoring and Diagnostics

5.1 Statistics

The statistics screen displays statistics for overall encrypted-zone traffic, each of the Bridge's logical interfaces (including physical Ethernet ports and all configured virtual radio interfaces), as well as for each of the Bridge's internal radios.



TRAFFIC STATISTICS

ENCRYPT	DECRYPT	SEND CLEAR	RECV CLEAR	KEY PACKETS	BAD KEYS	BAD DECRYPT	BAD PACKETS
52811	0	0	0	0	0	0	0

INTERFACE STATISTICS

INTERFACE	RX			TX		
	BYTES	PACKETS	ERRORS	BYTES	PACKETS	ERRORS
lan1 - 00:14:8c:08:10:80	329445713	1294412	0	5929597	81022	0
lan2 - 00:14:8c:08:10:80	2340	40	0	0	0	0
lan3 - 00:14:8c:08:10:80	0	0	0	0	0	0
lan4 - 00:14:8c:08:10:80	0	0	0	0	0	0
lan5 - 00:14:8c:08:10:80	0	0	0	0	0	0
lan6 - 00:14:8c:08:10:80	0	0	0	0	0	0
lan7 - 00:14:8c:08:10:80	0	0	0	0	0	0
lan8 - 00:14:8c:08:10:80	0	0	0	0	0	0
wan1 - 00:14:8c:08:10:80	0	0	0	0	0	0
radio 1 VAP 1 - 00:14:8c:08:10:83	0	0	0	32220536	241867	0
radio 1 VAP 2 - 06:14:8c:08:10:83	0	0	0	32189998	241868	0
radio 2 VAP 1 - 00:14:8c:08:10:82	0	0	0	32220808	241869	0

RADIO STATISTICS

RADIO 1

Signal Strength: 0% (-96dBm)

-85dBm -60dBm

RADIO 2

Signal Strength: 0% (-96dBm)

-85dBm -60dBm

5.1.1 Traffic Statistics

The packets that the Fortress Bridge has transmitted to and received from the encrypted zone since cryptographic processing was last started are shown in the *STATISTICS* frame:

- *Encrypt* - encrypted packets—the packets received from the unencrypted zone, encrypted, and then transmitted to the encrypted zone
- *Decrypt* - decrypted packets—the packets received from the encrypted zone, decrypted, and then transmitted to the unencrypted zone
- *SendClear* - cleartext packets received from Trusted Devices and sent to the unencrypted zone
- *RcvClear* - received clear—cleartext packets received from Trusted Devices in the encrypted zone
- *KeyPackets* - valid key exchange packets
- *BadKeys* - bad key packets—malformed key exchange packets
- *BadDecrypt* - key packets the Bridge was unable to decrypt
- *Bad Packets* - malformed packet received (Packets can be malformed for a number of reasons, such as version incompatibility or a failed hash check.)

5.1.2 Interface Statistics

The *DIAGNOSTICS* screen displays a MAC address and statistics for each of the Bridge's physical and virtual interfaces:

- The *lan1–8* interfaces correspond to the ports of the internal LAN switch.
- The *wan1* interface identifies the Bridge's WAN port.
- *Radio 1* is the Bridge's internal tri-band, 802.11a/b/g radio, the primary interface for which is labeled *Radio 1 VAP 1*.
  - Up to three additional SSIDs are optional and can configured only on a radio with a *Radio Mode* setting of **AP** (Section 3.3.1.3). When configured, the virtual interfaces to which the additional SSIDs correspond are numbered *VAP 2*, *VAP 3* and *VAP 4*.
- Radio 2 is the internal 802.11a, radio, the primary interface for which is labeled *Radio 2 VAP 1*.
  - Up to three additional SSIDs are optional and can configured only on a radio with a *Radio Mode* setting of **AP** (Section 3.3.1.3). When configured, the virtual interfaces to which the additional SSIDs correspond are numbered *VAP 2*, *VAP 3* and *VAP 4*.

INTERFACE STATISTICS provides a set of three values for each interface's receive (*RX*) and transmit (*TX*) functions:

- *BYTES* - the total number of bytes received/transmitted on the interface
- *PACKETS* - the total number of packets received/transmitted on the interface
- *ERRORS* - the total number of receive/transmit errors reported on the interface

5.1.3 Radio Statistics

RADIO 1 is the tri-band, 802.11a/b/g radio and *RADIO 2* is the higher-gain 802.11a radio.

Signal Strength is measured in real time, in decibels referenced to milliwatts, and displayed as a dynamic value in the *RADIO STATISTICS* frame of the *INTERFACE STATISTICS SCREEN*.

The *Signal Strength* for a radio with a *Radio Mode* setting of **Bridge** can be static or changing, according to the network deployment. In a point-to-point deployment, the signal level being measured is from the only other Bridge in the deployment, and so it remains constant. In a point-to-multipoint deployment, the Bridge displays the strength of the signal from each of the other Bridges in the deployment in rotation, at one-second intervals.

5.2 Tracking

The Bridge tracks devices in the encrypted zone, including other Fortress Bridges, any configured Trusted Devices, and Secure Clients.

The *TRACKING* screen displays:

- *MAC Address* - the Media Access Control address of the connected device
- *Client ID* - the Device ID of the connected device, if the connected device is another Fortress controller device or is running the Secure Client
- *State* - the state of the device's connection to the Bridge-secured network (see Table 5.1, below)
- *User Name* - the user name associated with the device, if a user is locally configured for the device (This field is absent when authentication is globally **Disabled** on the Bridge or **External** authentication is selected.)
- *IP Address* - the network address of the device, or *0.0.0.0*, if the device has been configured to accept **any** IP address (from the networks DHCP server)
- *Computer Name* - the hostname of the device on which the Secure Client is running, if the connected device is another Fortress controller device or is running the Secure Client (and has a hostname configured)

NOTE: The Bridge's *Tracking* screen does not display the Device ID and IP addresses of devices on a LAN secured by another Fortress controller device. All such devices display the IP address and Device ID of the controller device securing them. The MAC addresses of these devices display accurately.

- *Idle Since* - the number of hours, minutes and seconds since the device was last active on the network.

Reset	MAC Address	Client ID	State	Username	IP Address	Computer Name	Idle Since
☐	00:09:5B:B2:50:CF	A05F5BB2500F58CD	Authenticating (13)	NONE	0.0.0.0		00 hrs 01 mins 00 secs
☐	00:20:A6:51:2A:F5	D777A7F9FE77A7F9	Secure connection (06)	qas	172.17.48.97	QASW2K05	00 hrs 00 mins 00 secs
☐	00:D0:B7:E5:8A:52	4022CA573053DA8F	Secure connection (06)	NONE	172.28.19.92		00 hrs 02 mins 36 secs
☐	00:20:A6:54:72:D1	EC68D6A4E27D7EC1	Secure connection (06)	qas	172.17.200.3	QASNAC02	00 hrs 00 mins 00 secs
☐	00:14:8C:08:01:00	E82AF8E19F6DD618	Secure connection (06)	NONE	172.17.48.11		00 hrs 00 mins 30 secs
☐	00:12:17:F6:BD:1D	4ECD271AC3839F16	Secure connection (06)	1	172.17.200.4	QASWXP16	00 hrs 00 mins 00 secs
☐	00:14:8C:08:0F:40	A51AAE56FC0BDF65	Secure connection (06)	NONE	172.17.48.20		00 hrs 12 mins 00 secs
☐	00:E0:F4:11:DC:E6	8BA324C98E7C240F	Secure connection (06)	NONE	172.17.48.25	8BA324C98E7C240F	00 hrs 00 mins 00 secs
☐	00:09:5B:B4:11:8D	3557855803 3E0192	Authenticating (13)	NONE	172.17.200.5	QASWXP07	00 hrs 00 mins 00 secs
☐	00:14:8C:F8:04:80	F810D18EE6518D3C	Secure connection (06)	NONE	172.17.48.13		00 hrs 12 mins 00 secs
☐	00:C0:1B:00:8B:26	F810D18EE6518D3C	Secure connection (06)	NONE	172.17.48.13		00 hrs 03 mins 06 secs
☐	00:14:8C:08:01:02	E82AF8E19F6DD618	Secure connection (06)	NONE	172.17.48.11		00 hrs 01 mins 42 secs
☐	00:02:2D:28:18:38	Trusted Device	Trusted connection	NONE	172.17.48.88	UNKNOWN	00 hrs 00 mins 00 secs

Check All

Reset Checked Sessions

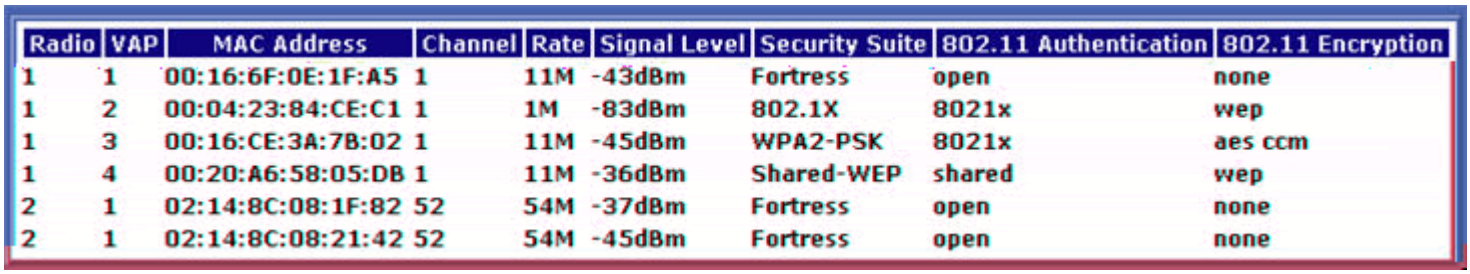
Table 5.1. Commonly Seen Tracking State Codes

State	Meaning
00	new partner not in database
01	static key exchange start
03	static key exchange complete
04	dynamic key exchange start
06	dynamic key exchange complete: secure connection
08	unsecure connection
13	user authentication
15	maximum retries exceeded: locked out

Each device entry on the *TRACKING* screen is preceded by a checkbox that, when checked, resets the network session of that device when **Reset Checked Sessions** (at the bottom of the screen) is clicked.

5.3 AP Associations

The AP Associations screen provides information about devices currently connected through the Bridge's wireless interfaces.



Radio	VAP	MAC Address	Channel	Rate	Signal Level	Security Suite	802.11 Authentication	802.11 Encryption
1	1	00:16:6F:0E:1F:A5	1	11M	-43dBm	Fortress	open	none
1	2	00:04:23:84:CE:C1	1	1M	-83dBm	802.1X	8021x	wep
1	3	00:16:CE:3A:7B:02	1	11M	-45dBm	WPA2-PSK	8021x	aes ccm
1	4	00:20:A6:58:05:DB	1	11M	-36dBm	Shared-WEP	shared	wep
2	1	02:14:8C:08:1F:82	52	54M	-37dBm	Fortress	open	none
2	1	02:14:8C:08:21:42	52	54M	-45dBm	Fortress	open	none

- *Radio* - shows whether the device is connected through Radio *1* or Radio *2.*
- *VAP* - varies according to the if the *Radio Mode* setting:

  If the radio through which the device is connected has a *Radio Mode* setting of **AP**: indicates which of the radio's virtual access point (VAP) interfaces the device is associated with, by number.

  If the radio through which the device is connected has a *Radio Mode* of **Bridge**: VAP displays *WDS* (wireless distribution system) to indicate that the connected device is another Fortress Bridge in a point-to-point/multipoint deployment. (Refer to Section 3.3.1.3 for more information on the Bridge's *Radio Mode* setting.)
- *MAC Address* - displays the media access control address of the associated device.

- *Channel* - identifies the channel, by number, over which the Bridge and the associated device are communicating, as selected for the radio being used (Section 3.3.2.1).
- *Rate* - provides a dynamic measurement of the data rate of the connection to the associated device, in megabits per second.
- *Signal Level* - provides a dynamic measurement of the strength of the signal between the Bridge and the associated device, in decibels referenced to milliwatts.
- *Security Suite* - indicates the type of security that has been selected for the VAP with which the device is associated. (Refer to Section 3.3.4.5 for more information about VAPs' Security Suite settings.)
- *802.11 Authentication* - displays the type of authentication required for the device, as determined by the *Security Suite* setting of the associated VAP and illustrated in Table 5.2.
- *802.11 Encryption* - displays the type of data encryption in effect for the device, as determined by the *Security Suite* setting of the associated VAP and illustrated in Table 5.2.

NOTE: The **Fortress** *Security Suite* setting implements proprietary authentication and encryption without reference to the 802.11 standard. The *open* and *none* values shown on the *AP Associations* screen do not mean that no authentication or encryption is used for a VAP with this setting.

NOTE: WPA and WPA2 use the 802.1X authentication protocol. In PSK mode, however, the pre-shared key obviates the need for an actual 802.1X authentication server.

Table 5.2. AP Association 802.11 Authentication and Encryption

Security Suite Setting	802.11 Authentication	802.11 Encryption
Cleartext	open	none
Fortress	open	none
Open WEP	open	WEP
Shared WEP	open	shared
802.1X	802.1X	none
WPA	802.1X	tkip
WPA2	802.1X	aes ccm
WPA-Mixed	802.1X	tkip *or* aes ccm[a]
WPA-PSK	802.1X	tkip
WPA2-PSK	802.1X	aes ccm
WPA-Mixed-PSK	802.1X	tkip *or* aes ccm[a]

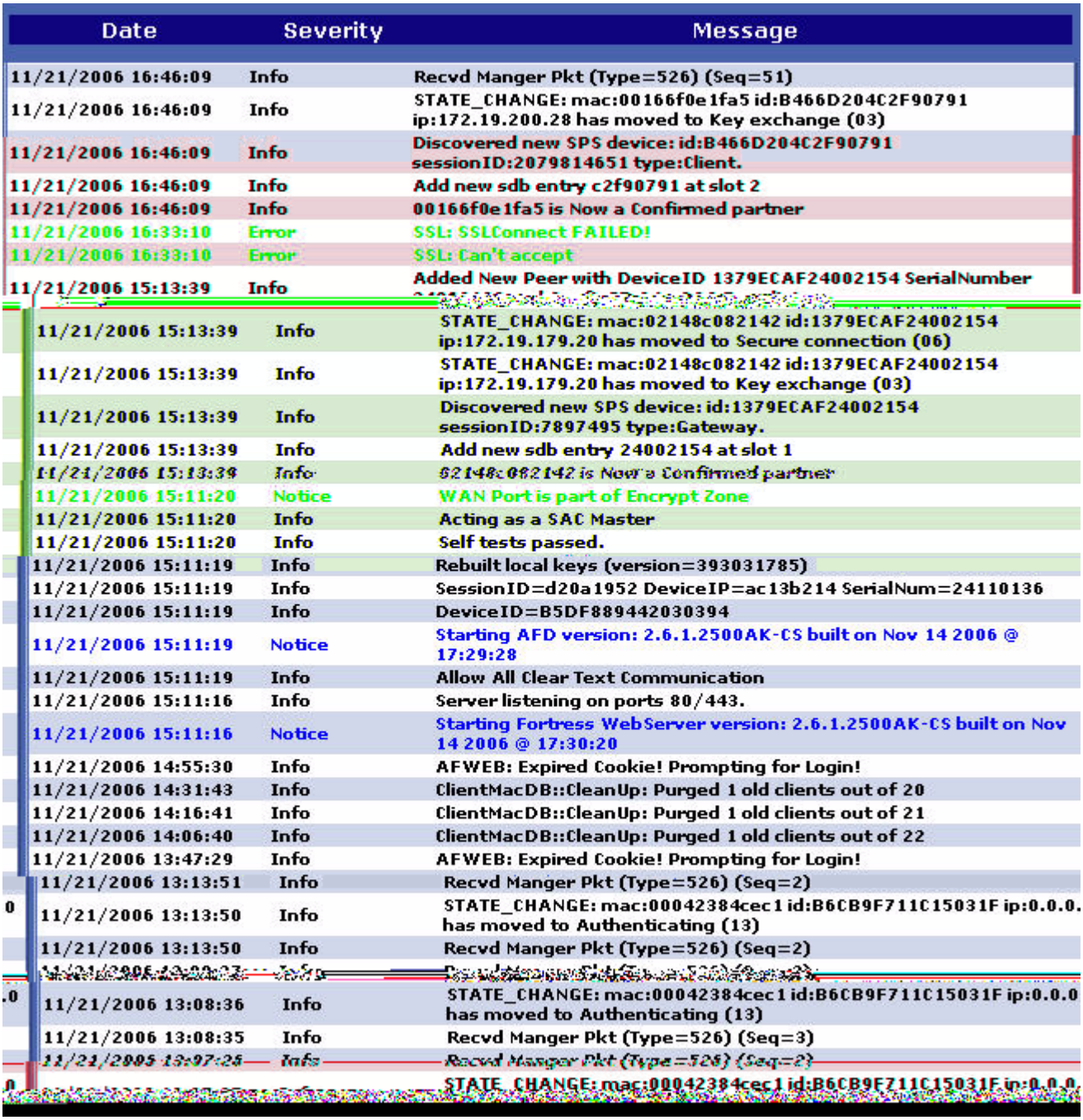
a. Varies according to connected client type.

5.4 View Log

The Fortress Bridge logs significant system activity and status information. Access the log by logging into the *admin* account and choosing **SYSTEM LOG** from the menu on the left.

Each activity item is date-and-time stamped, its severity is indicated and a brief text description is given. Among other information, the log records:

- when Secure Clients contact and negotiate keys with the Fortress Bridge
- system configuration changes
- when cryptographic processing is restarted
- system and communication errors



Date	Severity	Message
11/21/2006 16:46:09	Info	Recvd Manger Pkt (Type=526) (Seq=51)
11/21/2006 16:46:09	Info	STATE_CHANGE: mac:00166f0e1fa5 id:B466D204C2F90791 ip:172.19.200.28 has moved to Key exchange (03)
11/21/2006 16:46:09	Info	Discovered new SPS device: id:B466D204C2F90791 sessionID:2079814651 type:Client.
11/21/2006 16:46:09	Info	Add new sdb entry c2f90791 at slot 2
11/21/2006 16:46:09	Info	00166f0e1fa5 is Now a Confirmed partner
11/21/2006 16:33:10	Error	SSL: SSLConnect FAILED!
11/21/2006 16:33:10	Error	SSL: Can't accept
11/21/2006 15:13:39	Info	Added New Peer with DeviceID 1379ECAF24002154 SerialNumber
11/21/2006 15:13:39	Info	STATE_CHANGE: mac:02148c082142 id:1379ECAF24002154 ip:172.19.179.20 has moved to Secure connection (06)
11/21/2006 15:13:39	Info	STATE_CHANGE: mac:02148c082142 id:1379ECAF24002154 ip:172.19.179.20 has moved to Key exchange (03)
11/21/2006 15:13:39	Info	Discovered new SPS device: id:1379ECAF24002154 sessionID:7897495 type:Gateway.
11/21/2006 15:13:39	Info	Add new sdb entry 24002154 at slot 1
11/21/2006 15:13:39	Info	02148c082142 is Now a Confirmed partner
11/21/2006 15:11:20	Notice	WAN Port is part of Encrypt Zone
11/21/2006 15:11:20	Info	Acting as a SAC Master
11/21/2006 15:11:20	Info	Self tests passed.
11/21/2006 15:11:19	Info	Rebuilt local keys (version=393031785)
11/21/2006 15:11:19	Info	SessionID=d20a1952 DeviceIP=ac13b214 SerialNum=24110136
11/21/2006 15:11:19	Info	DeviceID=B5DF889442030394
11/21/2006 15:11:19	Notice	Starting AFD version: 2.6.1.2500AK-CS built on Nov 14 2006 @ 17:29:28
11/21/2006 15:11:19	Info	Allow All Clear Text Communication
11/21/2006 15:11:16	Info	Server listening on ports 80/443.
11/21/2006 15:11:16	Notice	Starting Fortress WebServer version: 2.6.1.2500AK-CS built on Nov 14 2006 @ 17:30:20
11/21/2006 14:55:30	Info	AFWEB: Expired Cookie! Prompting for Login!
11/21/2006 14:31:43	Info	ClientMacDB::CleanUp: Purged 1 old clients out of 20
11/21/2006 14:16:41	Info	ClientMacDB::CleanUp: Purged 1 old clients out of 21
11/21/2006 14:06:40	Info	ClientMacDB::CleanUp: Purged 1 old clients out of 22
11/21/2006 13:47:29	Info	AFWEB: Expired Cookie! Prompting for Login!
11/21/2006 13:13:51	Info	Recvd Manger Pkt (Type=526) (Seq=2)
11/21/2006 13:13:50	Info	STATE_CHANGE: mac:00042384cec1 id:B6CB9F711C15031F ip:0.0.0. has moved to Authenticating (13)
11/21/2006 13:13:50	Info	Recvd Manger Pkt (Type=526) (Seq=2)
11/21/2006 13:08:36	Info	STATE_CHANGE: mac:00042384cec1 id:B6CB9F711C15031F ip:0.0.0 has moved to Authenticating (13)
11/21/2006 13:08:35	Info	Recvd Manger Pkt (Type=526) (Seq=3)
11/21/2006 13:07:26	Info	Recvd Manger Pkt (Type=526) (Seq=2)
		STATE_CHANGE: mac:00042384cec1 id:B6CB9F711C15031F ip:0.0.0.

The log is allocated 500 Kbytes of memory and can contain a maximum of approximately 16,000 log messages (approximate because record sizes vary somewhat). When the log is full, the oldest records are overwritten as new messages are added to the log.

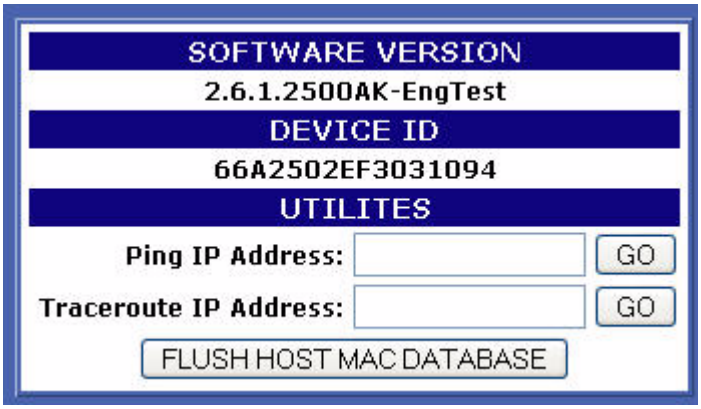
5.5 Diagnostics

Access Fortress Bridge diagnostic utilities by logging into the Bridge GUI *admin* account and selecting **DIAGNOSTICS** from the menu on the left.

NOTE: Radio 1 uses antenna port 1 (**ANT1**); Radio 2 uses antenna port 2 (**ANT2**).

The *DIAGNOSTICS* screen displays:

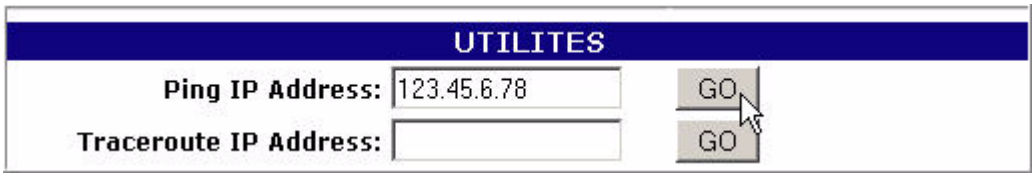
- The version and build number of the firmware currently running on the Fortress Bridge, under *SOFTWARE VERSION*.
- The *DEVICE ID* of the Fortress Bridge, as uniquely generated for each device on a Fortress-secured network and used, when applicable, for device authentication. (Refer to Section 4.1 for more information about Device IDs.)



5.5.1 Pinging a Device

1. Log on to the Bridge GUI *admin* or *operator* account and choose **DIAGNOSTICS** from the menu on the left.
2. On the *DIAGNOSTICS* screen under *UTILITIES*, in *Ping IP Address*, enter the IP address of the device you want to ping.
3. Click **GO**. The Bridge will ping the target IP five times and display the *PING RESULTS*.

detail:



5.5.2 Tracing a Packet Route

1. Log on to the Bridge GUI *admin* or *operator* account and choose **DIAGNOSTICS** from the menu on the left.
2. On the *DIAGNOSTICS* screen under *UTILITIES*, in *Traceroute IP Address*, enter the IP address of the device to which you want to trace the route.
3. Click **GO**. The Bridge will trace the route to the target IP and display the *TRACEROUTE RESULTS*.

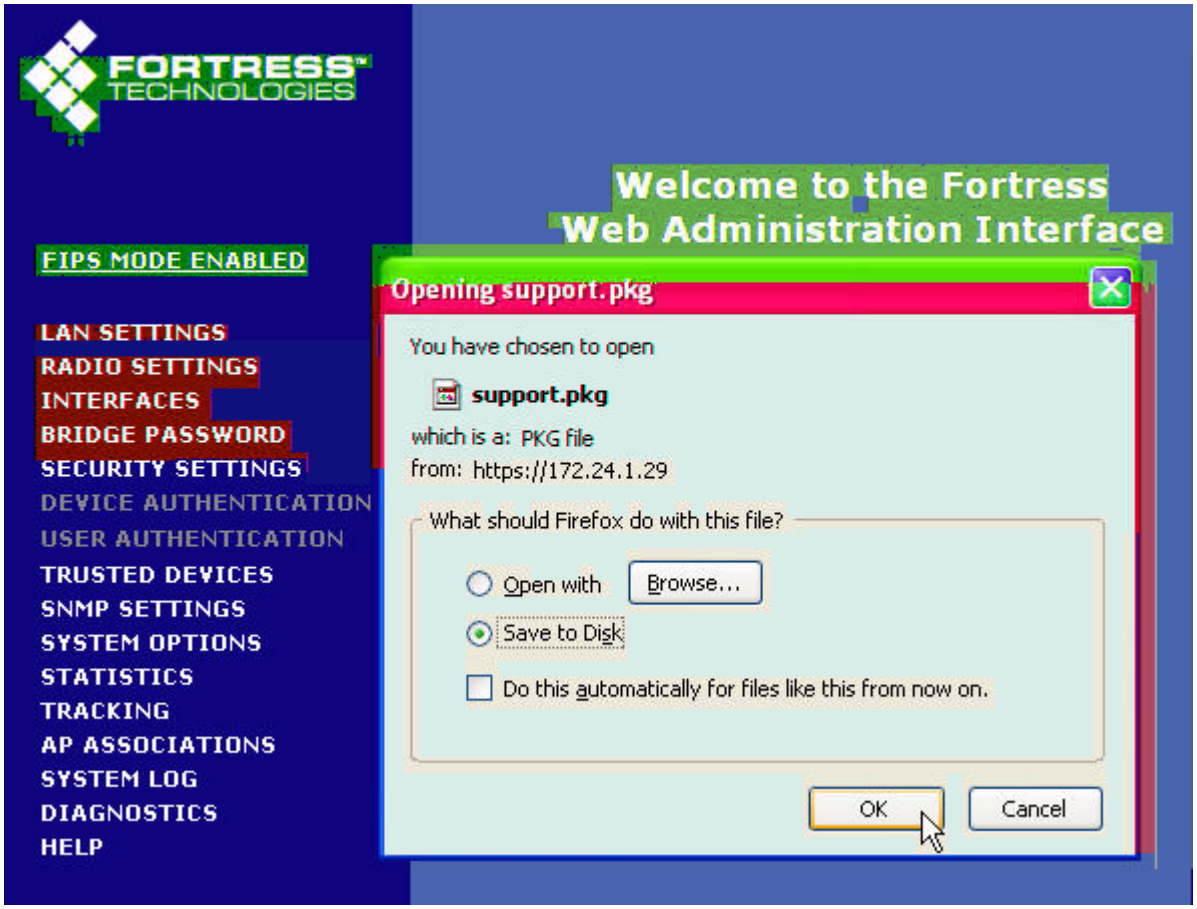
5.5.3 Flushing the Host MAC Database

The Fortress Bridge maintains a database of the MAC addresses of devices in the unencrypted zone. You can flush the *HOST MAC DATABASE*:

1. Log on to the Bridge GUI *admin* account and choose **DIAGNOSTICS** from the menu on the left.
2. At the bottom of the *DIAGNOSTICS* screen, click the **FLUSH HOST MAC DATABASE** button.
3. Click **OK** on the confirmation system dialog. The Bridge resets all connections to the unencrypted zone.

5.5.4 Generating a Diagnostics File

To assist in diagnosing a problem with your Bridge, the Customer Support team at Fortress Technologies may request that you generate a diagnostics file. Diagnostics files encrypt the information collected from the Bridge, so the file can be securely sent to Fortress Support as an e-mail attachment.



1. Log on to the Bridge *admin* account and access this page:
   `http://<IP_address>/support_package.html`
   where *`<IP_address>`* is the Bridge's IP address.
2. On the system dialog, choose to save the file, *support.pkg*.

5.6 Front-Panel Indicators

NOTE: There are no LED indications in a Bridge in blackout mode (refer to

Stat2 ***can exhibit:***

- *solid green* - The Bridge is operating in root mode.
- *off* - The Bridge is operating in non-root mode.

Clr ***can exhibit:***

- *fast green flash* - The Bridge is passing cleartext (unencrypted data) in the encrypted zone.

Fail ***can exhibit:***

- *off* - The **Fail** LED does not apply to version 2.6.*x* of the Fortress Bridge software. It is reserved for future support for failover Bridge deployments.

Pwr ***can exhibit:***

- *solid green* - The Bridge is powered on, either through the +48V DC adapter inlet or the WAN port's PoE connection.
- *off* - Bridge is powered off.

5.6.2 Radio LEDs

The Bridge's internal radios are each associated with a pair of front-panel LEDs, labeled **Radio1** and **Radio2**.

Radio LEDs are arranged one above the other. Each radio then has an associated *upper* and *lower* LED.

When the radio's *LED RSSI Monitor* is **Disabled** (the default) the **Radio1** and **Radio2** LEDs behave as shown below. (The *LED RSSI Monitor* and associated LED behaviors are described in Section 3.3.2.7).

color / behavior	upper LED	lower LED	both LEDs	all four LEDs
solid green	n/a	*in* **AP** *or* **Root Bridge** *modes:* active *in* **Non-Root Bridge** *mode:* connected to root	n/a	n/a
intermittent green	passing traffic	n/a	n/a	n/a
solid amber	n/a	n/a	n/a	firmware error
off	n/a	*in* **Non-Root Bridge** *mode:* not connected to root	radio disabled	both radios disabled

The upper LED can exhibit:

- *intermittent green flash* - The radio is passing traffic.

The lower LED can exhibit:

- *solid green* - The meaning depends upon the radio's mode settings:
  - In **AP** or **Root Bridge** modes - The radio is active and acting as an AP or a root Bridge.
  - In **Non-Root Bridge** mode - The radio is connected to the root Bridge.
- *off* - This state is meaningful only for a radio in **Non-Root Bridge** mode and indicates that the radio is not connected to the root Bridge.

Both upper and lower LEDs can exhibit:

- *off* - The associated radio is disabled (in the Bridge GUI or CLI).

All four Radio LEDs can exhibit:

- *solid amber* - A firmware error has occurred.
- *off* - Both radios are disabled (in the Bridge GUI or CLI).

5.6.3 Port LEDs

The Fortress Bridge's Ethernet ports—including those for the LAN switch, numbered **1** through **8**, and for the **WAN** port—are each equipped with two LEDs.

- The **Lnk/Act** (link/activity) LEDs are located in the upper left corner of each LAN switch port and to the left of the WAN port. They indicate when a link has been established for the port (solid green) and show data activity on the link (irregular flashing green).
- The **POE** LED in the upper right corner of each LAN switch port does not apply to version 2.6.*x* of the Fortress Bridge firmware. It is reserved for future support for Bridge Power over Ethernet (PoE) power sourcing equipment (PSE) functionality.
- The **Pwr** LED to the left of the WAN port illuminates whenever the Bridge is powered up—whether the source of power is PoE PSE or the +48V DC power inlet.

Chapter 6
Command-Line Interface

6.1 Introduction

The Fortress Bridge CLI provides commands for managing the Fortress Bridge and the network it secures. You can access it through a direct connection to the Bridge's serial console port or, using Secure Shell (SSH), from any computer with access to the Bridge—i.e., any computer in the Bridge's unencrypted zone or a computer running the Fortress Secure Client.

NOTE: Fortress Bridge features and functions are described in greater detail in the preceding chapters describing the use of the Bridge GUI.

You do not need to be a root user to access the Bridge CLI.

Up and down (↑↓) arrow keys scroll through the command history for a given CLI session, and the left and right (←→) arrow keys navigate the current command line. The **Home** key moves the cursor to the beginning of the command line; the **End** key moves the cursor to the end of the line. If your terminal keyboard is not equipped with arrow keys, you can use these keyboard equivalents:

arrow / numeric keypad	keyboard equivalent
up arrow (↑)	**Ctrl-u**
down arrow (↓)	**Ctrl-d**
left arrow (←)	**Ctrl-l**
right arrow (→)	**Ctrl-r**
Home	**Ctrl-a**
End	**Ctrl-e**

The **Tab** key auto-completes partial commands that are sufficient to uniquely identify the command.

The `clear` command clears the current terminal screen.

If the command output is longer than the display screen, the CLI stops the list when the display is full and provides a `more` option that displays the next ten lines of output when you strike **Enter**↵. To return to the command prompt without viewing all available output, strike `Ctrl-c`.

Bridge CLI commands return `[OK]` when they execute and `[Error]`, with a brief description of the error, when they do not.

6.1.1 CLI Administrative Modes

There are two administrative modes in the Bridge CLI.

When you first access the CLI you are, by default, in *Gateway* mode, indicated by the command prompt: `[GW]>`. In Gateway mode, you can manage the Bridge's Fortress controller device functions, including basic administration and security settings.

The functions associated with the Bridge's internal radios—its AP/wireless bridge functions—are administered from Access Point mode, indicated by the command prompt: `[AP]>`.

To access one mode from the other, simply enter the two-letter mode designation: **`AP`** if you are in Gateway mode; **`GW`** if you are in Access Point mode.

```
[GW]> ap
[AP]> gw
[GW]>
```

AP mode uses a submenu of commands to view and configure virtual radio interfaces settings, otherwise known as virtual access points (VAPs). Refer to Section 6.4.3.1 for more detail.

NOTE: Bridge CLI `help` output shows only those commands and arguments that are valid in the current administrative mode (refer to Section 6.2 for more detail.)

6.1.2 Accessing the CLI through the Serial Port

1. Using a standard Ethernet cable and the RJ-45-to-DB9 adapter that came with the Bridge, connect the Fortress Bridge's **Console** port to a serial port on a computer.
2. Start your serial application and, if it is not already at these settings, configure it to use:
   - bits per second: **`9600`**
   - data bits: **`8`**
   - parity: **`none`**
   - stop bits: **`1`**
   - hardware flow control: **`none`**

NOTE: An RJ-45-to-DB9 adapter—included with each Bridge—is required to connect the serial **Console** port to a DB9 terminal connection. Pin outs for these adapters are given in Table 7.1 on page 116.

6.1.3 Accessing the CLI Remotely

When SSH is enabled, you can access the CLI through a network connection to the Bridge's **Unencrypted** port by simply pointing your terminal emulation application, configured with the settings shown above, to the Bridge's IP address.

Secure Shell (SSH) is disabled on the Fortress Bridge by default. You must either enable SSH through the Bridge GUI (Section 3.6.2) before you access the CLI remotely, or you must make your initial connection to the Bridge CLI through a direct connection to its **Console** port (see above).

To enable SSH access to the Bridge CLI, follow the instructions in Section 6.4.5.7 (for the CLI) or Section 3.6.2 (for the GUI).

6.1.4 Logging On and Off the CLI

To log on to the CLI, access the Fortress Bridge through a terminal application and at the prompts enter the logon ID, **`sysadm`** and the password set for *CLI access* during installation.

```
WSG login: sysadm
Password: <password>
Fortress Wireless Security Gateway
[GW]>
```

NOTE: The default CLI password is **sysadm**. Passwords should never be left at their defaults.

The login ID, `sysadm`, cannot be changed.

If you are changing the CLI password for the first time as part of an installation procedure (Chapter 2) use the default password, **sysadm**.

To log off the CLI, use the `exit` command or its synonyms:

```
[GW]> exit
[GW]> quit
[GW]> q
```

The CLI will time out and exit after five minutes of inactivity, and you must log back in to regain access. This behavior is not user configurable.

6.2 Getting Help in the CLI

Use the `help` command (or its synonym, `?`) without arguments to obtain the list of valid commands for the current administrative mode.

You can obtain a usage example—and list the command's valid options with their valid arguments for the current administrative mode—by entering a basic command without options:

```
[GW]> show
Description: Displays system information, configuration
Usage: show [args]. Possible args:
  8021X
  auth
  blackout
  cleartext
  clock
  clients
  compression
  crypto
  device
  fips
  gui
  log
  multicast
  network
  partners
  radius
  sac
  snmp
  sp
  ssh
  stp [bridgeName]
  td
  uptime
  wanport
  eapretryint
  ?|help
```

Note that only those options available in the current administrative mode are displayed and that valid command options differ significantly between modes.

```
[AP]> show
Description: Displays Access Point information, configuration
Usage: show [args]. Possible args:
  associations
  radio
  radius
  ?|help
```

Several of the commands that change Bridge configuration settings can be run interactively. When you enter a command with one of its options, the parameters that can be configured display as consecutively presented fields.

Obtain a usage example of command options for interactive commands—and list the option's valid switches and arguments with a brief explanation of each—by entering `help` (or its synonym, `?`) after the command option:

```
[GW]> set network ?
Description: Sets network configuration
Usage: set network [-h hostname][-ip IP][-nm netmask][-gw defaultGW]
  -gw 0: delete default gateway
```

For help with non-interactive command options, you can enter the command-option combination without arguments:

```
[GW]> set accessid
Description: Sets Access ID from a HEX string
Usage: set accessid <default|hexString>
  default: set to all 0's
  string of 16 HEX characters, ex: 0A0B0C0D0E0F2345
```

6.3 Command Syntax

In this document, command-line text supplied by the CLI is set in `plain` (non-bold, non-italic) type. All user input is indicated by **`bold`** typeface. The template for the CLI command syntax is shown below:

```
[GW]> command option <parameter> {-switch req_arg1|req_arg2|req_arg3} [-switch opt_arg1|opt_arg2]
```

in which you can also note the terminology and punctuation used here to describe command strings and parse input elements:

- *Command* refers to the basic operation to be performed (ex., **`set`**, **`show`**, etc.).
- *Option* refers to the configuration element upon which the command will operate (ex., **`clock`**, **`ap`**, **`clients`**, etc.)
- *Parameter* refers to a user-supplied variable, (ex., **`<name>`**, **`<IPaddr>`**, etc.).
- *Arguments* (**`_arg`**, above) are additional command inputs. Some arguments are required by the command (**`req_arg`**). Others are optional (**`opt_arg`**). Multiple arguments must be separated by commas and entered without spaces.

NOTE: Bridge CLI commands, options, arguments and switches are case-sensitive, and all user-supplied inputs must be entered without spaces.

- *Switch* refers to the identifier, preceded by a dash (hyphen), for the argument to follow (ex., **-ip**, **-n**, etc.) Switches allow permissible arguments to be entered in any combination and order.
- Angle brackets: indicate variable, user-supplied inputs (parameters and variable arguments), which are also italicized (ex., ***<sharedkey>***, ***<port1,port2,...>***).
- The absence of angle brackets and italics indicates literal (or fixed) user-supplied input (ex., **[P|B|N]**).
- Braces indicate that the arguments enclosed are required by the command (ex., **{y|n}**).
- Square brackets indicate optional arguments (ex., **[all|*<port1,port2,...>*]**.
- Pipes are placed between mutually exclusive arguments (ex., **[*<accessID>*|default]**.
- An ellipse indicates than the argument can include more entries of the same kind (ex., ***<port1,port2,...>***).

6.4 Configuration in the Bridge CLI

6.4.1 LAN Settings in the CLI

View network properties with the `show network` command:

```
[GW]> show network
Hostname:FTIPegasus
DefaultGateway:192.168.254.1
IP(Private):192.168.254.254
Netmask(Private):255.255.255.0
```

Configurable parameters assign the Bridge's host name and its management interface IP and subnet addresses and identify the default gateway (or router) for the network on which you are installing the Bridge.

The `show network` command is valid only in `GW` (gateway) mode (refer to Section 6.1.1 for more detail).

Configure network properties for the Fortress Bridge with the `set network` command, as follows:

NOTE: The Fortress Bridge's default IP address is: `192.168.254.254`

```
[GW]> set network
Hostname: <BridgeName>
[OK] setting hostname
IPaddress: <BridgeName>
[OK] IP accepted, will test with netmask before setting
Netmask: <BridgeSubnet>
[OK] setting netmask
DefaultGateway: <BridgeIPaddr>
[OK] setting default gateway
[OK] setting IP
Update Certificate done
Reboot is required. [Y|N]?
```

NOTE: The IP address you assign should be unique on the network.

The CLI displays the configurable fields for `set network` one at a time. Enter a new value for the field—or leave the field blank and the setting unchanged—and strike **Enter**↵, to display the next field. The final reboot query displays only when you have entered a value into at least one of the fields presented.

Entering the `0` (zero) argument for the `DefaultGateway` option deletes the default gateway from the Bridge's network configuration.

Alternatively, you can run `set network` non-interactively with valid switches and arguments in any order and combination:

```
[GW] > set network [-h <BridgeName>] [-ip <BridgeIP>] [-nm <BridgeSubnet>] [-gw <DFLTgatewayIP>|0]
```

Regardless of the method you use to reconfigure these settings, you must reboot the Bridge in order for the change to any network setting other than host name to take effect. To do so, simply strike **Enter**↵ at the prompt (**Y** is the default).

The `set network` command is valid only in GW (gateway) mode (refer to Section 6.1.1 for more detail).

6.4.2 Spanning Tree Protocol in the CLI

STP link managementis enabled on the Fortress Bridge by default.

You can view whether STP is currently enabled (`on`) or disabled (`off`) with `show stp`:

```
[GW] > show stp
On
```

```
[AP]> show radio
[RADIO 1]
    Radio State: On
     Radio Band: 802.11g
     Radio Mode: AP
        Channel: 1
       Tx Power: Auto
       Distance: 1
Beacon Interval: 100
       Preamble: Short
      Multicast: On
   RSSI Monitor: Off
[RADIO 2]
          State: On
     Radio Band: 802.11a
     Radio Mode: Bridge
    Bridge Mode: Root
        Channel: 149
       Tx Power: Auto
       Distance: 1
Beacon Interval: 100
      Multicast: On
   RSSI Monitor: Off
```

`RADIO 1` identifies the 802.11a/b/g, multi-mode radio associated with the Bridges' antenna port 1 (**ANT1**), while `RADIO 2` identifies the higher-gain 802.11a radio associated with antenna port 2 (**ANT2**).

To view the current setting for a radio individually, specify the radio by number (`1` or `2`):

NOTE: The Bridge CLI makes available certain Linux® Wireless Extension Tools for the configuration of the Atheros® wireless driver. These can be used for additional WLAN configuration. Refer to Section 6.7 for more detail.

```
[AP]> show radio 1
[RADIO 1]
    Radio State: On
     Radio Band: 802.11g
     Radio Mode: AP
        Channel: 1
       Tx Power: Auto
       Distance: 1
Beacon Interval: 100
       Preamble: Short
      Multicast: On
   RSSI Monitor: Off
```

Configure radio settings interactively by entering the `set` command with just the `radio 1` or `radio 2` argument. The Bridge CLI presents one field at a time, and you can either enter a new value for a given field or strike **Enter**↵ to leave the value unchanged and go on to the next field.

The options presented depend, in part, on the configuration choices you make. A radio with a `Radio Mode` setting of `ap`, for instance, will not provide you an opportunity to set the `Bridge Mode`, unless you change the `Radio Mode` to **`bridge`**, at which point the `Bridge Mode` option will be inserted dynamically, as shown below.

NOTE: If you are deploying multiple Fortress Bridges in a point-to-point/multi-point network they must be correctly configured for their network roles, typically with one serving as the root node and the rest configured as non-root nodes (refer to Section 3.3.1.4 for more detail).

```
[AP]> set radio 1
Radio state [on|off] (on):
Radio band [802.11g|802.11a] (802.11g): 802.11a
[OK]
Reboot is required when changing radio band
Radio Mode [ap|bridge|ids] (ap): bridge
[OK]
Bridge Mode [root|nonroot] (nonroot): nonroot
Radio is in nonroot mode...cannot set channel
Transmit Power [auto|1-18] (auto):
Distance in miles [1-35] (1): 3
[OK]
Beacon interval (ms) [25..1000] (100):
Multicast [on|off] (on):off
RSSI Monitor [on|off] (off): on
[OK]
Committing changes...
Reboot is required. [Y|N]? y
```

As indicated in the output above, the `Channel` setting does not apply to the bridging radios of non-root Bridges, which do not bind to a channel, but rather to an SSID. In contrast, `Multicast` applies exclusively the bridging radios of non-root Bridges, and it is only when configuring such radios that you will see the `Multicast` option.

In root bridge and AP radios, the channels available for selection depend on the 802.11 band used by the radio: channels 36, 40, 44, 48, 52, 56, 60, 64, 149, 153, 157, or 161 are available for 802.11a radios; channels 1–11, inclusive are available for Radio 1 when it is configured to use the 802.11g band.

Configuration settings for Radio 2 omit the `Radio band` option; Radio 2 is fixed on the 802.11a band. Configurable options—with their selection-dependent permutations—are otherwise the same for both radios.

NOTE: Because STP requires multicasting, the multicast option will be absent (and the feature enabled) for non-root bridging radios. If you disable STP (Section 6.4.2) the `multicast` option will be presented for a non-root bridging radio.

```
[AP]> set radio 2
Radio state [on|off] (on):
Radio 2 band fixed at 802.11a
Radio Mode [ap|bridge] (bridge): ap
[OK]
Channel [36|40|44|48|52|56|60|64|149|153|157|161] (149): 44
[OK]
Transmit Power [auto|1-18] (auto): 18
[OK]
Beacon interval (ms) [25..1000] (100):
RSSI Monitor [on|off] (off):
Committing changes...
Reboot is required. [Y|N]?
```

Alternatively, you can use the `set radio` command with valid switches and arguments to change the settings of either radio:

```
[AP]> set radio {1|2} [-state on|off] [-band 802.11g|802.11a] [-rmode ap|bridge]
[-bmode root|nonroot] [-channel <channel#>] [-txpower auto|1-18] [-distance 1-35]
[-beaconint 20-1000] [-preamble short|long] [-multicast on|off] [-rssimon on|off]
```

The sample output for the `show radio` command (at the beginning of this section) shows the default radio settings.

As shown in the example interactive `set radio` output, reconfiguring radio settings requires that you reboot the Bridge in order to effect your changes.

The `show radio` and `set radio` commands are valid only in AP (access point) mode (refer to Section 6.1.1 for more detail).

6.4.3.1 Virtual Radio Interface Settings in the CLI

The Bridge CLI AP mode uses a submenu of commands to view and configure virtual radio interfaces settings, otherwise known as virtual access points (VAPs).

Use the `vapcfg` command to access these commands. You must specify the radio associated with the virtual interface(s) you want to configure with the `vapcfg` command (the CLI will prompt you for a radio number if you do not enter it with the command).

```
[AP]> vapcfg radio 1
[VAP]>
```

The command prompt (`VAP`) reflects the fact that you are in VAP-configuration mode.

The `vapcfg` command is valid only in AP mode. So in order to access the VAP command set for the other radio, you must return to AP mode and re-enter the `vapcfg` command. This is illustrated in the output of the `show` command below. Use the `show` command to view the current virtual radio interface configuration:

```
[AP]> vapcfg radio 1
[VAP]> show vap
[RADIO 1]
    [VAP 1]
          SSID: Base-11g
          DTIM: 1
     Hide SSID: off
 RTS Threshold: off
Frag Threshold: off
      Only 11g: off
Security Suite: fortress

[VAP]> ap
[AP]> vapcfg radio 2
[VAP]> show vap
[RADIO 2]
    [VAP 1]
          SSID: Base-11a
          DTIM: 1
     Hide SSID: off
 RTS Threshold: off
Frag Threshold: off
Security Suite: fortress
```

By default a single virtual access point (`vap 1`) is configured for each radio. The SSIDs associated with these two primary VAPs should never be left at their defaults (shown above). SSID strings can be up to 32 characters long.

Configure VAP settings interactively by entering the `set` command with just the `vap <N>` argument, where *N* is the VAP number. The Bridge CLI presents one field at a time, and you can either enter a new value for a given field or strike **Enter**↵ to leave the value unchanged and go on to the next field.

You can reconfigure existing VAPs with the `set` command:

```
[VAP]> set vap 1
SSID [String <= 32] (Base-11g): 0123xyz
[OK]
DTIM [1-255] (1):
Hide SSID [on|off] (off):
RTS Threshold [off|1-2345] (off):
Frag Threshold [off|256-2345] (off):
Only 11g [on|off] (off):
Security Suite [? for options] (fortress):
Committing changes...
Reboot is required. [Y|N]?
```

You can also use the `set` command interactively to configure the same parameters for new VAPs.

Entering a dot (**.**) at the SSID prompt clears the SSID string.

The `Security Suite` field will accept any of eleven possible entries, and the differing parameters required for each are presented interactively once you have entered your selection. The CLI provides a list of possible `Security Suite` options when a question mark (**?**) is entered for the field. (`Security Suite` options and the parameters required to configure them are described in detail in Section 3.3.4).

```
[AP]> vapcfg radio 1
[VAP]> set vap 2
SSID [String <= 32] (): 0987abc
[OK]
DTIM [1-255] (1):
Hide SSID [on|off] (off): on
[OK]
RTS Threshold [off|1-2345] (off):
Frag Threshold [off|256-2345] (off):
Only 11g [on|off] (off):
Security Suite [? for options] (fortress): ?
Possible Security Suites: [fortress|clear|open-wep|shared-
wep|8021x|wpa|wpa-psk|
wpa2|wpa2-psk|wpa-mixed|wpa-mixed-psk]
Security Suite [? for options] (fortress): wpa
[OK]
Rekey period [seconds] (600): 300
[OK]
Committing changes...
Reboot is required. [Y|N]??
```

Alternatively, you can use the `set vap` command with valid switches and arguments to change the settings of any VAP:

```
[VAP]> set vap {1|2|3|4} [-ssid <ssidstring>|.] [-dtim 1-255] [-hidessid on|off]
[-rts 1-2345|off] [-frag 256-2345|off] [-only11g on|off]
[-suite fortress|clear|open-wep|shared-wep|8021x|wpa|wpa-psk|wpa2|wpa2-psk|wpa-mixed|wpa-mixed-psk]
[-wepkeytype hex|passphrase] [-wepkeysize 40|104] [-wepkey1 <key>] [-wepkey2 <key>]
[-wepkey3 <key>] [-wepkey4 <key>] [-weptxkey 1-4] [-keytype hex|passphrase] [-rekeyperiod <sec>]
[-passphrase <phrase>] [-hex <key>]
```

In the dot (`.`) input for the `-ssid` switch clears the SSID string. The output of `set vap help` provides guidance for many of the Security Suite parameters shown above (described in detail in Section 3.3.4).

Security Suite options `fortress` and `clear` require no further parameters to be set. When you have configured a different Security Suite setting, you can view the parameters configured for it with the `show` command.

```
[VAP]> show vap 2
[RADIO 1]
    [VAP 2]
          SSID: 0987abc
          DTIM: 1
     Hide SSID: on
 RTS Threshold: off
Frag Threshold: off
      Only 11g: off
Security Suite: wpa
  Rekey period: 300
```

You can clear the settings for VAPs 2 through 4, effectively deleting them from the radio configuration.

```
[VAP]> clear vap 2
Committing changes...
Reboot is required. [Y|N]?
```

Radio 1 and Radio 2 each require a VAP 1 to be configured at all times. So, while you can edit VAP 1 on either radio, with the `set` command, you cannot `clear` it. Attempting to do so will result in an error message that offers you the alternative of resetting VAP 1 to its default configuration.

The `VAP` submenu can be accessed only from AP mode (refer to Section 6.1.1 for more detail), and you can return to AP mode with the `AP` command.

In VAP mode the standard `quit` and `reboot` commands remain available. Changes to Bridge radio virtual interfaces always require you to reboot, as shown in the example output throughout this section.

6.4.4 Bridge Passwords in the CLI

Two passwords apply to the Bridge GUI, one for the *admin* (administrator) account, and one for the *operator* (view-only) account. The Bridge CLI has only an administrator account.

6.4.4.1 Changing Bridge GUI Passwords in the CLI

Which GUI password is set depends upon the *username* argument: **admin** sets the administrator password, **operator**, the view-only password. Use the set passwd command, as follows:

```
[GW]> set passwd web {admin|operator}
Enter Current Password:<oldpassword>
Enter     New Password:<newpassword>
Re-enter  New Password:<newpassword>
```

NOTE: Passwords should be a minimum of eight characters long and contain a mix of upper and lowercase letters and numerals.

The default Bridge GUI *admin* password is admin. The default *operator* password is operator.

GUI passwords must be at least eight characters long.

The set passwd command is valid only in GW (gateway) mode (refer to Section 6.1.1 for more detail).

NOTE: Usernames are predetermined for all Fortress Bridge interface options; they cannot be changed.

6.4.4.2 Changing the Bridge CLI Password

Use the set passwd command to change the CLI password, as follows:

```
[GW]> set passwd cli sysadm
Changing password for sysadm
Enter the new password (minimum of 5, maximum of 8 characters)
Please use a combination of upper and lower case letters and numbers.
Enter new password:<newpassword>
Re-enter new password:<newpassword>
Password changed.
```

The default CLI password is sysadm.

The set passwd command is valid only in GW (gateway) mode (refer to Section 6.1.1 for more detail).

6.4.5 Security Settings in the CLI

Security settings on the Fortress Bridge include encryption algorithm, re-keying interval, Access ID, operating mode, enabling/disabling SSH and the Bridge GUI, and system passwords.

Except for system passwords, all security settings can be viewed through the CLI.

Security settings are configured through the set command, using various options, as described in the following subsections.

6.4.5.1 Encryption Algorithm in the CLI

The encryption algorithm determines how the Bridge encodes data.

All of the Bridge's Secure Clients must be configured to use the same encryption algorithm as the Bridge. For information on setting encryption algorithms on Secure Clients, refer to your Fortress Secure Client user guide.

View the encryption algorithm (and the re-keying interval) in effect on the Bridge with `show crypto`:

```
[GW] > show crypto
CryptoEngine:AES256
ReKeyInterval:4
```

The `show crypto` command is valid only in GW (gateway) mode (refer to Section 6.1.1 for more detail).

The encryption algorithm that the Fortress Bridge and its Clients will use is set with `set crypto`, as follows:

```
[GW] > set crypto [-e aes128|aes192|aes256]
```

The default encryption algorithm is AES256.

The `set crypto` command is valid only in GW (gateway) mode (refer to Section 6.1.1 for more detail).

NOTE: You can combine on a single command line the `set crypto` arguments that configure the encryption algorithm and the re-key interval.

6.4.5.2 Re-Keying Interval in the CLI

The re-keying interval is the length of time between new keys issued by the Fortress Bridge. View the re-keying interval (and the encryption algorithm) in effect on the Bridge with `show crypto`:

```
[GW] > show crypto
CryptoEngine:AES256
ReKeyInterval:4
```

The `show crypto` command is valid only in GW (gateway) mode (refer to Section 6.1.1 for more detail).

The re-keying interval in effect between the Fortress Bridge and its Clients is set, in values between 1 and 24 hours, with `set crypto` command, as follows:

```
[GW] > set crypto [-t <hrs>]
```

The default re-keying interval is 4 hours.

The `set crypto` command is valid only in GW (gateway) mode (refer to Section 6.1.1 for more detail).

6.4.5.3 Data Compression in the CLI

View the compression setting in effect on the Bridge with the `show` command.

```
[GW] > show compression
on
```

Configure data compression on the Bridge with the `set` command:

```
[GW] > set compression {on|off}
```

Compression is turned on by default.

Be advised that Bridges in a point-to-point/multipoint configuration must be configured to use the same compression setting, or they will be unable to communicate with one another.

The `show` and `set compression` commands are valid only in GW (gateway) mode (refer to Section 6.1.1 for more detail).

6.4.5.4 Access ID in the CLI

The Access ID is a 16-digit hexadecimal ID that provides network authentication for the Fortress Security System.

All of the Bridge's Secure Clients must be configured to use the same Access ID as the Bridge. For information on setting encryption algorithms on Secure Clients, refer to your Fortress Secure Client user guide.

Use `set accessid` to change the Access ID, as follows:

```
[GW] > set accessid {<16digithexid>|default}
```

The default Access ID is represented by16 zeros.

The `show accessid` and `set accessid` commands are valid only in GW (gateway) mode (refer to Section 6.1.1 for more detail).

CAUTION: For security reasons, the Access ID in effect on the Bridge cannot be displayed. *Make a note of the new Access ID:* you will need it to configure the Bridge's Secure Clients, as well as to change the Access ID on the Bridge.

6.4.5.5 Operating Mode in the CLI

The Fortress Bridge can be operated in either of two modes: *Normal* (the default) or *FIPS*.

You can view the current operating mode on the Bridge with `show fips`:

```
[GW] > show fips
On
```

Change operating modes with the `set fips` command. To set the operating mode to *FIPS*:

```
[GW] > set fips on
```

Return the Fortress Bridge to *Normal* operating mode (the default) with:

```
[GW] > set fips off
```

The `show fips` and `set fips` commands are valid only in GW (gateway) mode (refer to Section 6.1.1 for more detail).

6.4.5.6 WAN Port Encryption in the CLI

By default, the Bridge's WAN port is in the encrypted zone of the Bridge-secured network. It can be configured to be in the network's unencrypted zone.

You can view the current WAN port setting with `show wanport`:

```
[GW] > show wanport
Encrypted
```

Reconfigure the WAN port's encrypted/unencrypted zone status with the `set wanport` command. To place the WAN port in the unencrypted network zone:

```
[GW] > set wanport -encrypt n
```

Return the WAN port to the encrypted zone with:

```
[GW] > set wanport -encrypt y
```

The `show wanport` and `set wanport` commands are valid only in GW (gateway) mode (refer to Section 6.1.1 for more detail).

6.4.5.7 SSH Access to the CLI

CAUTION: If you want to be able to access the Bridge CLI after outdoor installation, you must enable SSH (secure shell) during pre-configuration of the Bridge.

Secure Shell (SSH) is disabled on the Fortress Bridge by default.

You can view the current SSH setting with `show ssh`:

```
[GW] > show ssh
Off
```

To enable SSH, log on to the CLI (via a direct connection to the Bridge's **Console** port, as described in Section 6.1.2) and enter:

```
[GW] > set ssh on
```

To disable SSH:

```
[GW] > set ssh off
```

NOTE: Disabling SSH prevents remote access to the CLI from the network. With SSH disabled you can access the CLI only over a direct connection to the Bridge's **Console** port.

You can disable SSH from a remote terminal session, and continue that session normally. Access will be denied, however, the next time you try to access the CLI remotely.

The `show ssh` and `set ssh` commands are valid only in GW (gateway) mode (refer to Section 6.1.1 for more detail).

6.4.5.8 Disabling the Bridge GUI in the CLI

Bridge GUI access is enabled on the Fortress Bridge by default.

You can view the current GUI access setting with `show gui`:

```
[GW] > show gui
On
```

If you want to limit access to the Fortress Bridge exclusively to the CLI, you can disable the Bridge GUI, as follows:

```
[GW] > set gui off
```

To re-enable the Bridge GUI, enter:

```
[GW] > set gui on
```

The `show gui` and `set gui` commands are valid only in GW (gateway) mode (refer to Section 6.1.1 for more detail).

6.4.5.9 Blackout Mode in the CLI

To Bridge's front-panel LEDs are enabled by default. You can disable them, placing the Fortress Bridge in blackout mode.

You can view the current blackout mode with show blackout:

```
[GW] > show blackout
Off
```

If you want to disable the front-panel LEDs, turn blackout mode on, as follows:

```
[GW] > set blackout on
```

To re-enable the front-panel LEDs, enter:

```
[GW] > set blackout off
```

The `show blackout` and `set blackout` commands are valid only in GW (gateway) mode (refer to Section 6.1.1 for more detail).

6.4.6 System Date and Time in the CLI

View Bridge date and time settings with the `show clock` command:

```
[GW] > show clock
Wkday Month DAY HR:MIN:SEC TimeZone YEAR
```

Set system date and time on the Fortress Bridge, using the twenty-four-hour clock and numerical date, through the `set clock` command, as follows:

```
[GW] > set clock
[OK]
[GW] > set clock -h 15 -m 10 -s 00 -M 5 -D 19 -Y 2006
```

The `set clock` command returns the Bridge's current date and time values, which you can edit and re-enter: use the left/right arrow keys to navigate displayed fields, backspace over current values to overwrite them. When you finish typing in new values, strike **Enter**↵ to save them.

Alternatively, you can run `set clock` non-interactively with valid switches and arguments, as shown below.

```
[GW] > set clock [-h <hrs>] [-m <mins>] [-s <secs>] [-M <M>] [-D <D>] [-Y <YYYY>]
```

The `show clock` and `set clock` commands are valid only in GW (gateway) mode (refer to Section 6.1.1 for more detail).

6.4.7 Restoring Default Settings in the CLI

Return all of the Fortress Bridge's configuration settings to their factory default values with `reset`, confirming your intention at the query, as follows:

```
[GW] > reset
Warning: Reset to the default configuration?[Y|N] y
Reboot is required. [Y|N]?
```

NOTE: The `reset` command ends all active sessions on the Fortress Bridge.

As shown in the example output, changing resetting the Bridge to its factory defaults requires that you reboot the Bridge. To do so, enter `y` at the prompt.

The `reset` command is valid only in GW (gateway) mode (refer to Section 6.1.1 for more detail).

6.4.8 Non-802.1X Authentication Settings in the CLI

6.4.8.1 Non-802.1X Authentication Server Settings

The Bridge can be configured to authenticate users and devices locally through its internal RADIUS server or to use an external RADIUS server for user authentication.

Use `show auth` to display the current user authentication configuration:

```
[GW] > show auth
Type:Local
FailoverTimeout:0
```

Configure the Bridge to use its internal RADIUS server to authenticate users with `set auth`, as follows:

```
[GW] > set auth local
```

Configure the Bridge interactively to authenticate users through an external RADIUS server with `set auth`, as follows:

```
[GW]> set auth external
IPserver:123.45.67.89
[OK] set Server IP
AuthKey:s3cr4ts5r6v7rk8y
[OK] set Authentication Key
```

The default RADIUS shared key is **`fortress`**.

The RADIUS shared key can also be set non-interactively with:

```
[GW]> set auth -key <sharedkey>
```

The `-key` switch does not apply to internal (local) user authentication settings.

Disable RADIUS authentication on the Fortress Bridge with:

```
[GW]> set auth off
```

The `show auth` and `set auth` commands are valid only in GW (gateway) mode (refer to Section 6.1.1 for more detail).

6.4.8.2 Non-802.1X EAP Retry Interval Setting

When you are using an external non-802.1X RADIUS server with the Bridge, you can tune the retransmission time for EAP (Extensible Authentication Protocol) packets being sent to the server and the EAP clients for which the Bridge is acting as the authenticator.

View the Bridge's EAP retry interval the `show` command:

```
[GW]> show eapretryint
EAP retry interval in seconds 18
```

The Bridge's EAP retry mechanism has a fixed, six-second cycle, but the number of cycles allowed to elapse between EAP retries is configurable.

Configure the EAP retry interval with the `set` command, in whole-second values equal to or greater than six:

```
[GW]> set eapretryint 6
[OK] set EAP retry Interval to 6
```

You can enter values for the EAP retry interval that are not evenly divisible by six, but because the mechanism has a fixed six-second cycle, the Bridge will round the value to the nearest value that is evenly divisible by six:

```
[GW]> set eapretryint 25
[OK] set EAP retry Interval to 24
```

The default EAP retry interval setting is 18 seconds.

The `show eapretryint` and `set eapretryint` commands are valid only in GW (gateway) mode (refer to Section 6.1.1 for more detail).

6.4.9 802.1X Authentication Settings in the CLI

6.4.9.1 802.1X Authentication Server Settings

Support for 802.1X authentication on the Fortress Bridge, whether for wired or wireless devices, requires the use of an external 802.1X authentication service. Those WPA and WPA2 Security Suite settings that do *not* use PSK (pre-shared key mode), also require the use of an 802.1.X authentication server. (Possible VAP Security Suite settings are described in detail in Section 3.3.4.5; viewing and changing current settings through the Bridge CLI is described in Section 6.4.3.1.)

If you are using the `external` option for *non*-802.1X authentication (described in Section 6.4.8, above), the 802.1X authentication service can run on the same external server, but you must configure the server separately for each function.

Because 802.1X authentication is used by both wired and wireless devices connecting to the Fortress Bridge, the server can be configured in either the Bridge CLI's GW (Gateway) mode or its AP (access point) mode. Although the two modes use different command arguments to access 802.1X server settings, they apply to the same 802.1X service. (Refer to Section 6.1.1 for more detail on Bridge CLI user modes.)

In AP mode, use the `radius` argument with the show command to view the server settings:

```
[AP]> show radius
[RADIUS Info]
    Server IP: 127.0.0.1
  Server Port: 1812
Server Secret: password
```

In AP mode, use the `set` command with just the `radius` argument to configure the 802.1X server interactively. The Bridge CLI presents one field at a time, with the current setting displayed in parentheses. You can either enter a new value for a given field or strike **Enter**↵ to leave the value unchanged and go on to the next field.

```
[AP]> set radius
RADIUS server IP (127.0.0.1): 123.45.6.78
[OK]
Reboot is required when changing RADIUS server address
RADIUS server port (1812):
RADIUS server secret (password): drowssaPw3n
[OK]
Reboot is required when changing RADIUS server secret
Reboot is required. [Y|N]?
```

Alternatively, in AP mode, you can use the `set radius` command with valid switches and arguments to change 802.1X server settings:

```
[AP]> set radius -server <serverIPaddr> -port <port#> -secret <sharedkey>
```

In GW mode, use the `show` command with the `8021X` argument to view the server settings:

```
[GW]> show 8021X
Lan1:off
Lan2:off
Lan3:off
Lan4:off
Lan5:off
Lan6:off
Lan7:off
Lan8:off
AuthServer:127.0.0.1
AuthPort:1812
```

The last two lines of output display the current 802.1X server settings. The LAN port settings shown are described in the next section (6.4.9.2).

In GW mode, use the `set` command with just the `8021X` argument to configure the 802.1X server interactively. The Bridge CLI presents one field at a time, and you can either backspace over the existing value for a given field and enter a new value or strike **Enter**↵ to leave the value unchanged and go on to the next field.

```
[GW]> set 8021X
lan1[on|off]:off
lan2[on|off]:off
lan3[on|off]:off
lan4[on|off]:off
lan5[on|off]:off
lan6[on|off]:off
lan7[on|off]:off
lan8[on|off]:off
AuthServerIP:123.45.6.78
[OK]
AuthServerPort:1812
AuthServerSharedKey:drowssaPw3n
[OK]
Reboot is required. [Y|N]?
```

The last three input prompts present the current 802.1X server settings. The LAN port setting prompts are described in the next section (6.4.9.2).

Alternatively, in GW mode, you can use the `set 8021X` command with valid switches and arguments to change 802.1X server settings:

```
[GW]> set 8021X -ip <serverIPaddr> -p <port#> -key <sharedkey>
```

Reconfiguring 802.1X authentication settings requires that you reboot the Bridge in order to effect your changes.

The `radius` argument is exclusive to AP mode. The `8021X` argument is exclusive to GW mode. (Refer to Section 6.1.1 for more detail on Bridge CLI administrative modes.)

6.4.9.2 Internal LAN Switch Port 802.1X Settings

You can individually configure each of the ports of the Bridge's internal LAN switch to require that a connected device is an 802.1X supplicant successfully authenticated by the 802.1X authentication server configured for the Bridge (Section 6.4.9).

View current LAN port settings with the `show` command:

```
[GW]> show 8021X
Lan1:off
Lan2:off
Lan3:off
Lan4:off
Lan5:off
Lan6:off
Lan7:off
Lan8:off
AuthServer:127.0.0.1
AuthPort:1812
```

The `Lan` numbers shown correspond to the Bridge's front-panel switch port labeling. By default, the 802.1X authentication requirement is turned `off` for all eight ports.

Use the `set` command with just the `8021X` argument to configure the 802.1X server interactively. The Bridge CLI presents one field at a time, and you can either backspace over the existing value for a given field and enter a new value or strike **Enter**↵ to leave the value unchanged and go on to the next field.

Alternatively, you can use the `set 8021X` command with valid arguments to change 802.1X LAN port settings:

```
[GW]> set 8021X [lan1|2|3|4|5|6|7|8] [on|off]
```

Changing LAN port settings requires you to reboot the Bridge to effect your changes.

The `show 8021X` and `set 8021X` commands are valid only in GW (gateway) mode (refer to Section 6.1.1 for more detail).

6.5 Administration in the Bridge CLI

6.5.1 Trusted Devices in the CLI

View configured Trusted Devices with `show td`:

```
[GW]> show td
NAME            IP              MAC                 PORT
guests          123.45.6.7      11:22:33:44:55:66   80
audit           123.67.8.9      33:44:55:66:77:88   80,443
print1          234.56.7.8      22:33:44:55:66:77   23
Total TD: 3
```

Use the `add` and `del` (delete) commands to manage Trusted Devices for the Bridge-secured WLAN, as described in the following sections.

The commands that configure and delete Trusted Devices are valid only in GW (gateway) mode (refer to Section 6.1.1 for more detail).

6.5.1.1 Adding Trusted Devices in the CLI

Add Trusted Devices with the `add td` command, as follows:

```
[GW] > add td {-n <name>} {-ip <IPaddr>} {-m <MACaddr>} {-p any|<port1,port2,…>}
```

in which *name* is a descriptive identifier for the Trusted Device, *IPaddr* is the Trusted Device's network address, and *MACaddr* its MAC address. The *-p* switch specifies, by number, the port(s) accessible through the Trusted Device (comma delimited, without spaces), or that `any` port is accessible through the Trusted Device.

NOTE: Trusted Devices must be assigned static IP addresses.

Maximize network security by specifying the narrowest possible port access for Trusted Devices.

CAUTION: Specifying that **any** port can access a TD can pose a ***significant*** security risk.

You must configure a name and IP and MAC addresses for a Trusted Device when you add it to the Bridge configuration.

You can leave out `-p` (port sets) argument to establish default values for these settings. Trusted Devices have no ports open by default.

6.5.1.2 Deleting Trusted Devices in the CLI

Delete a single Trusted Device or all Trusted Devices from Fortress Bridge management with the `del td` command, as follows:

```
[GW] > del td {<name>|all}
```

6.5.2 SNMP Settings in the CLI

View the current SNMP configuration with `show snmp`:

```
[GW] > show snmp
Status:off
Contact:you@yourdomain
Location:Home
ROCommunity:public
RWCommunity:private
```

NOTE: You cannot configure SNMP management on a Fortress Bridge in *FIPS* operating mode. Refer to Section 3.6.1 for more information about Bridge operating modes and to Section 6.4.5.5 for details on changing it.

Enable SNMP (v1,2) management of the Fortress Bridge with the `enable` command:

The Fortress MIB is included on the CD that shipped with the Bridge and is also available from: **https://www.fortresstech.com/support/products_updates.asp**.

```
[GW] > set snmp on
```

Disable SNMP on the Fortress Bridge with the `disable` command:

```
[GW] > set snmp off
```

Configure the Fortress Bridge for use with SNMP (v1,2) with the `set` commands:

```
[GW] > set snmp -c <contact@domain.com> -l <locationName> -ro <roCmntyName> -rw <rwCmntyName>
Set Contact:OK
Set Location:OK
Set RO Community:OK
Set RW Community:OK
```

in which *contact* is the e-mail address to which SNMP event notifications will be sent, *locationName* identifies the Fortress Bridge, *roCmntyName* identifies the SNMP read-only community, and *rwCmntyName* identifies the SNMP read-write community.

You can include spaces in the location and SNMP community names by enclosing the input string in quotation marks.

The `show snmp` and `set snmp` commands are valid only in GW (gateway) mode (refer to Section 6.1.1 for more detail).

6.5.3 Viewing the Software Version in the CLI

Display the firmware version currently running on the Fortress Bridge with the command:

```
[GW] > about
Fortress Interface Shell. Version:2.6.0.2500Y
```

The `about` command is valid in either AP (access point) mode or GW (gateway) mode (refer to Section 6.1.1 for more detail).

6.5.4 Restarting the Bridge in the CLI

The `reboot` command does not power cycle the Bridge.

Restart the Fortress Bridge's cryptographic processor with `reboot`, confirming your intention at the query, as follows:

```
[GW] > reboot
Confirm: Reboot device now? [Y|N] y
The system is going down NOW !!
Sending SIGTERM to all processes.
stopping watchdog
Sending SIGKILL to all processes.
Please stand by while rebooting the system.
Restarting system.
```

NOTE: The `reboot` command ends all active sessions on the Fortress Bridge.

You can observe the Bridge stop its processor (as shown above). You can also observe the Fortress Bridge rebooting.

The `reboot` command is valid in AP (access point) mode, its VAP (virtual access point) submenu, or in GW (gateway) mode (refer to Section 6.1.1 for more detail).

6.6 Monitoring and Diagnostics in the CLI

6.6.1 Viewing a Summary Overview of the Bridge

Obtain a basic overview of the Bridge configuration—including hostname, Device ID, encryption, network address, and the current settings for SSH and GUI access to the Bridge and user authentication—with the command:

```
[GW]> show device
Hostname:Fswab
DeviceID:4389C1B376B1AFDD
CryptoEngine:AES256
IP(Private):172.24.1.27
Ssh:Off
Gui:On
Auth:Off
Fips:On
```

The `show device` command is valid only in GW (gateway) mode (refer to Section 6.1.1 for more detail).

6.6.2 Viewing System Uptime in the CLI

The show uptime command displays the number of days, hours and minutes that the Fortress Bridge has been operating since its last boot:

```
[GW]> show uptime
18 days 5 hr 33 min
```

The `show uptime` command is valid only in GW (gateway) mode (refer to Section 6.1.1 for more detail).

6.6.3 Partners Tracking in the CLI

View information about devices in the Bridge's encrypted zone, including Secure Clients and other Fortress Bridges with `show partners`:

```
[GW]> show partners
 MAC|DeviceId|State|Username|SessionID|IP|vlanID|computerName|activityCount
00:14:8C:08:24:80|65C2D9BC070E2494|03||0|172.19.180.20|0||1474
00:06:5B:AD:B0:13|1379ECAF24002154|03||0|172.19.179.20|0||1830
00:14:8C:08:21:40|1379ECAF24002154|03||0|172.19.179.20|0||996
00:14:8C:08:21:42|1379ECAF24002154|03||0|172.19.179.20|0||2104
```

6.6.4 Host Tracking in the CLI

View the MAC addresses of devices in the Bridges unencrypted zone—as well as the MAC addresses of each of the Bridge's physical and virtual interfaces)—with `show clients`:

NOTE: The term, *Client*, normally refers to devices running the Fortress Secure Client and located in the Bridge's unencrypted zone. The usage here is obsolete.

```
[GW]> show clients
-----------------------  Start of ClientMacDB::List-----------------------
Client1's mac:00:00:aa:8d:a2:e0     Client2's mac:00:00:aa:93:a1:a3
Client3's mac:00:01:6c:cc:ab:3e     Client4's mac:00:01:6c:e9:76:49
Client5's mac:00:01:e6:7e:ae:d2     Client6's mac:00:02:3f:75:1a:25
Client7's mac:00:02:a5:02:b8:fb     Client8's mac:00:08:83:cf:31:eb
Client9's mac:00:09:6b:c2:2f:68     Client10's mac:00:0d:60:89:2f:4a
Client11's mac:00:0d:60:cd:e8:40    Client12's mac:00:0f:01:00:01:a8
Client13's mac:00:10:c6:cd:ba:0d    Client14's mac:00:11:25:14:31:d1
Client15's mac:00:11:25:15:12:42    Client16's mac:00:11:25:d5:a3:08
Client17's mac:00:13:20:84:40:95    Client18's mac:00:13:20:d5:e2:de
Client19's mac:00:13:21:cc:64:d2    Client20's mac:00:14:8c:08:03:40
Client21's mac:00:15:58:09:51:7e    Client22's mac:00:15:62:91:a8:21
Client23's mac:00:15:62:91:a8:42    Client24's mac:00:16:35:01:7a:47
Client25's mac:00:16:41:15:68:63    Client26's mac:00:20:4a:67:9f:aa
-----------------------  End of ClientMacDB::List-----------------------
 Total of 13 Clients in the Database
```

Hosts (labeled *Client*) are numbered in the order they were added to the database, following the Bridge's internal interfaces, and are listed by their MAC addresses. Below the list, a count of the entries in the database is given.

You can flush the database of host (labeled Client) MAC address with the del command:

```
[GW] > del clients
[OK]
[GW] > show clients
------------------------  Start of ClientMacDB::List-----------------------
  {empty}
------------------------  End of ClientMacDB::List-----------------------
 Total of 0 Clients in the Database
```

The `show clients` and `del clients` commands are valid only in GW (gateway) mode (refer to Section 6.1.1 for more detail).

6.6.5 AP Associations in the CLI

View information about devices currently connected through the Bridge's internal radios with `show associations`:

```
[AP] > show associations
                                      Rate  Level               802.11  802.11
Radio VAP MAC                Channel  (M)   (dBM) Suite         Auth    Encryption
----- --- ------------------ -------  ----- ----- ------------- ------- ----------
1     4   00:20:A6:58:05:DB 1        11    -43   Shared-WEP    shared  wep
2     1   02:14:8C:08:24:82 52       54    -50   Fortress      open    none
2     1   02:14:8C:08:04:82 52       54    -43   Fortress      open    none
2     1   02:14:8C:08:21:42 52       54    -44   Fortress      open    none
```

The radio, VAP (virtual access point) and channel through which the associated device is connected are given, as well dynamic readings of the connection's data rate (in megabits per second) and signal level (in decibels referenced to milliwatts). In addition, you can view the Security Suite setting configured for the associated device's VAP, with its 802.11 authentication and encryption types.

The `show associations` command is valid only in AP (access point) mode (refer to Section 6.1.1 for more detail).

6.6.6 Viewing the System Log in the CLI

View the system log with the show command:

```
[GW] > show log
11/20/2006 17:43:50  Debug  CLIENT_MAC_DB: Add New client Mac=00:10:13:23:72:ab
11/20/2006 17:42:25  Info   ROAMING (1): 00148c081f80 Mac has moved to the eth0 side:
dest=ffffffffffff, ip=806
11/20/2006 17:42:25  Info   Reseting internals for gateway roaming.  State=3
11/20/2006 17:42:25  Debug  CLIENT_MAC_DB: Add New client Mac=00:14:8c:08:1f:80
11/20/2006 17:41:13  Info   ClientMacDB::CleanUp:  Purged 1 old clients out of 21
11/20/2006 17:19:48  Debug  CLIENT_MAC_DB: Add New client Mac=00:16:6f:0e:1f:a5
11/20/2006 17:17:42  Debug  CLIENT_MAC_DB: Add New client Mac=00:06:5b:ae:07:51
11/20/2006 16:39:38  Debug  Session ID = 1998424547
11/20/2006 16:39:38  Info   Generating new keys
11/20/2006 16:39:38  Info   Rebuilt local keys (version=1998424547)
--More--
```

6.6.7 Pinging a Device

You can `ping` devices from the Bridge's CLI. The Bridge pings three times and then displays the ping statistics.

```
[GW] > ping 123.45.6.78
PING 123.45.6.78 (123.45.6.78) from 123.45.6.89 : 56(84) bytes of data.
64 bytes from 123.45.6.78: icmp_seq=1 ttl=128 time=18.3 ms
64 bytes from 123.45.6.78: icmp_seq=2 ttl=128 time=23.0 ms
64 bytes from 123.45.6.78: icmp_seq=3 ttl=128 time=23.0 ms
--- 123.45.6.78 ping statistics ---
3 packets transmitted, 3 received, 0% loss, time 2025ms
rtt min/avg/max/mdev = 18.318/21.490/23.098/2.243 ms
```

The `ping` command is valid in either AP (access point) mode or GW (gateway) mode (refer to Section 6.1.1 for more detail).

6.6.8 Tracing a Packet Route

You can run `traceroute` from the Bridge's CLI:

```
[GW] > traceroute 123.45.6.78
traceroute to 123.45.6.78 (123.45.6.78), 30 hops max, 38 byte packets
 1  123.45.6.78 (123.45.6.78)  1.001 ms  5.474 ms  9.954 ms
```

The `traceroute` command is valid in either AP (access point) mode or GW (gateway) mode (refer to Section 6.1.1 for more detail).

6.7 WLAN Wireless Extension Tools

The Bridge CLI calls a select set of Linux® Wireless Extension Tools for WLAN configuration beyond the basic radio settings configured through the Bridge's native `set radio` command (described in Section 6.4.3).

These commands are intended exclusively for use by experienced network administrators familiar with them. If you have no experience with these tools, you should familiarize yourself with using Linux Wireless Extension Tools to configure the MADWiFi/Atheros® wireless driver. If you have Web access, you can refer to:

http://madwifi.org/users-guide/node2.html

WARNING: Some of the Linux Wireless Extension Tools available through the Bridge CLI can, if used improperly, damage your network configuration and even render the Bridge temporarily inoperable. Do not use these commands unless you are familiar with them—and then only at your own risk.

You can obtain a list of Wireless Extension Tools available through the Bridge CLI `help` system with:

```
[AP] > wlan
Description: executes WLAN utility commands
Usage: wlan [commands] [args]. Possible commands:
  80211stats
  athstats
  athchans
  athctrl
  athdebug
  iwconfig
  iwpriv
  wlanconfig
```

Usage and valid arguments for these commands can be displayed through their native `help` function, which is called with the `-h` argument, as follows:

```
[AP]> wlan wlanconfig -h
usage: wlanconfig wlanX create wlandev wifiX
            wlanmode [sta|adhoc|ap|monitor] [bssid | -bssid]
[nosbeacon]
usage: wlanconfig wlanX destroy
```

6.7.1 Creating a Wireless Extension Tools Script

Configuration changes made with the `iwconfig` and `iwpriv` WLAN Wireless Extension Tools are held in dynamic memory and do not persist through reboots of the Bridge. You can, however, create a script of these commands that will be run as part of the Bridge's bootstrap process.

When run with the write (`-w`) or append (`-a`) or arguments, the `script` command supplies an input line on which you can enter `iwconfig` and `iwpriv` commands with valid arguments.

Entering a script created with the `-w` argument saves the new script (overwriting the current script, if one exists). Entering a script created with the `-a` argument adds the new command(s) and argument(s) to an existing script (without overwriting it).

NOTE: Wireless Extension Tool scripts are included in Fortress Bridge backup files; restore operations therefore overwrite the existing script with the one in the backup file.

```
[AP]> script -w
Enter commands(iwpriv|iwconfig [args]) you want to run at boot time:
```

The `script` command with the `-x` argument executes the command(s) in the script.

```
[AP]> script -x
```

The `script` command returns no output when it successfully executes, but an error message *will* result if it fails.

Linux Wireless Extension Tools `scripts` commands can only be executed in AP (access point) mode (refer to Section 6.1.1 for more detail).

You can view any existing script by entering the `script` command without arguments.

```
[AP]> script
```

Linux Wireless Extension Tools are only available in AP (access point) mode (refer to Section 6.1.1 for more detail).

6.8 Secure Automatic Configuration

When deploying a point-to-point or point-to-multipoint network of Fortress Bridges that will be connected through the internal Radio 2 interface of each Bridge, you can preconfigure the network nodes automatically.

NOTE: You cannot use the SAC function with versions of the Fortress Bridge earlier than 2.6.1.

When a network of Bridges has been initially deployed in this way, you can also use the secure automatic configuration (SAC) utility to effect network-wide configuration changes from the root Bridge, as well as to automatically configure a new Bridge to be added to the existing network.

The Bridges in a point-to-point/multipoint network must run the same Bridge software version.

6.8.1 Preconfiguring a New Network Deployment with SAC

All of the Bridges to be included in the new network must be at their factory-default settings. (Section 6.4.7 describes restoring the Bridge's default settings from the Bridge CLI; Section 3.9 describes the same function in the Bridge GUI.)

6.8.1.1 Connecting the Bridges for Preconfiguration

1. Position the Bridges so that they operate only within their safe temperature range (14º–122º F/⁻10º–50º C).
2. Connect an 802.11a-capable antenna to antenna port 2 (**ANT2**) of each Bridge.
3. Connect the **WAN** ports of all of the Bridges in the deployment to an isolated Ethernet switch or hub (i.e., a switch or hub not connected to any existing LAN).
4. Connect the Bridges' external +48V DC power supplies to their front-panel **+48V DC** power inlets, and plug each power supply into a properly rated AC power outlet with the cord provided.
5. Connect the **Console** port of the Bridge you want to function as the SAC master Bridge (and the root Bridge in the network) directly to the serial terminal of the computer you will use to preconfigure the network.

NOTE: An RJ-45-to-DB9 adapter—included with each Bridge—is required to connect the Bridge's serial **Console** port to a DB9 terminal connection. Pin outs for these adapters are given in Table 7.1 on page 116.

6.8.1.2 Automatically Preconfiguring Network Bridges

The Bridge through which you invoke the initial SAC command automatically becomes both the root Bridge in the network and the master Bridge through which all subsequent network SAC functions must be performed.

Once a SAC master Bridge is established, you cannot designate a different Bridge as the master Bridge.

The `set sac start` command, which initiates the automatic configuration process, can be entered with or without the arguments that specify configurable parameters.

When issued without arguments, `set sac start` leaves Bridge security settings at their default values, while automatically generating appropriate SAC network parameters for all of the Bridges in the network, as shown in Table 6.1.

NOTE: The SAC master Bridge must be the root Bridge in the network. If you change its *Bridge Mode* setting to *Non-Root*, you will no longer be able to successfully execute SAC commands from the SAC master Bridge.

Table 6.1. Bridge Settings Resulting from SAC when None Are Specified

setting type	parameter	SAC behavior	value after SAC
security settings	Access ID	leave at default	0000000000000000 (16 zeros)
	encryption algorithm		AES-256
	re-key interval		4 hours
	operating mode		Normal (FIPS off)
SAC network parameters	IP address	generate automatically	auto-generated
	Radio 1 & 2 SSIDs		
	Radio 1 & 2 channels		

Allow all of the Bridges to boot before proceeding with SAC: front-panel **Stat1** and **Stat2** LEDs and the lower LEDs for both radios light solid green, while the upper LEDs for both radios and the WAN port link/activity (**Lnk/Act**) LED flash green intermittently.

1. Open a terminal application on the computer connected to the SAC master Bridge's **Console** port and (using the settings given in Section 6.1.2) open a session with the master Bridge.
2. Log in to the Bridge CLI of the master Bridge, using **sysadm** as both the login ID and password.
3. At the command prompt, `[GW]>`

   - If you want member Bridges' basic security settings to be left at their default values and SAC network parameters to be automatically generated for the Fortress network (as shown in Table 6.1), enter **set sac start** without arguments.

   or

   - If you want to specify some or all SAC-configurable parameters, enter the command with the appropriate switches and arguments, as follows:

```
[GW]> set sac start [-a <accessId>] [-e AES128|AES192|AES256] [-t <rekeyint>] [-fips off|on]
[-sa <rad2ssid>] [-ca <rad2chnl>] [-sg <rad1ssid>] [-cg <rad1chnl>] [-ipnw <IPaddr>|<resIPnw>]
```

The first line above shows security-setting switches and arguments. The `-a` switch configures the Access ID, for which you must enter a 16-digit hexadecimal value. Use the `-e` switch to enter one of the valid encryption algorithms and the `-t` switch to configure the re-key interval, in whole hours between `1` and `24`.

If you use the `-fips on` argument to place network Bridges in FIPS operating mode (described in Section 3.6.1), you will not be able to configure the network through subsequent `set sac start` commands until you have manually reconfigured each Bridge to use *Normal* operating mode (i.e., `set fips off`). FIPS-mandated restrictions do not allow configuration through SAC.

The second line of SAC input (above) shows SAC network-parameter switches and arguments. The `-sa` and `-ca` switches configure Radio 2's SSID and channel setting, respectively. The `-sg` and `-cg` switches configure the same settings for Radio 1.

You can use the `-ipnw` switch to establish a specific IP address for the master/root Bridge's management interface and automatically generate IP addresses within the same subnet for the rest of the network

NOTE: You can observe SAC events in the master Bridge's system log at any point in the SAC process with `show log`. Strike the **Ctrl-c** key, to return to the `[GW]>` command prompt.

Bridges. Alternatively, you can specify only a subnet and allow SAC to automatically generate all member IP addresses within that subnet, including that of the root/master Bridge.

The IP or subnet address you enter must fall within one of these reserved ranges:

- `10.0.0.0—10.255.255.255`
- `172.16.0.0—172.31.255.255`
- `192.168.0.0—192.168.255.255`

For example, the command below establishes the network Access ID, leaves the rest of the security settings at their defaults, configures an SSID and channel setting for each radio, and specifies a subnet for the deployment:

```
[GW]> set sac start -a 0f0e0d0c0b0a0b0c -sa r2s1s2i3d4 -ca 161 -sg r1s0s9i8d7 -cg 11 -ipnw 172.24.0.0
[OK] Started SAC process successfully
```

When the SAC process starts, you can observe the master/root Bridge's front-panel **Stat1** LED flash amber, while its **Stat2** LED lights solid amber. As each slave/non-root Bridge receives the SAC parameters, its **Stat1** and **Stat2** LEDs flash amber in unison.

4. Check the status of the SAC process with the `show sac` command:

```
[GW]> show sac
SwabSerialNum:24656196
SwabConfigID:19082
SwabSACRole:SAC_MASTER
SwabSACState:SAC_STOP_4SWAB
SwabSACVer:SAC_VER_PEGASUS_ARCH1
*********SACPeerInformation*********
SeriallNum|IpAddress|CfgID|PeerNum|PeerSACStatus|PeerSACState|PeerSACVer
24743196|172.24.0.3|0|1|SAC_PEER_CONFIRMED|SAC_FINISH_4PEER|SAC_VER_PEGASUS_ARCH1
24773196|172.24.0.4|0|2|SAC_PEER_CONFIRMED|SAC_FINISH_4PEER|SAC_VER_PEGASUS_ARCH1
```

The master Bridge confirms the `SAC_PEER` status of each new slave Bridge and displays `SAC_FINISH` for each of them that has successfully received SAC parameters.

5. Confirm that all of the slave/non-root Bridges in the network are recognized as SAC Peers with `show sp`:

```
[GW]> show sp
Peer1=>Serial_Number:24743196
Peer2=>Serial_Number:24773196
```

6. When the master Bridge shows `SAC_FINISH` for all slave Bridges and you have confirmed that the SAC Peer list is complete, save the network configuration with `set sac stop`:

```
[GW] > set sac stop
SAC Stop Initiated. May take some time to complete...
Stopped SAC process successfully
Reboot_Of_Master(SrlNum:24656196)_Required_For_NewConfiguration(CfgId:19082)_To_Take_Into_Effect
Reboot_Of_SACPeer(SrlNum:24743196)_Required_For_Configuration_Change_From(OldCfgId:0)_To(NewCfgI
d:19082_To_Take_Into_Effect
Reboot_Of_SACPeer(SrlNum:24773196)_Required_For_Configuration_Change_From(OldCfgId:0)_To(NewCfgI
d:19082)_To_Take_Into_Effect
```

7 Disconnect all of the Bridges' WAN ports from the switch/hub used to connect them for the initial SAC operation.

8 Power cycle each network Bridge by disconnecting and then reconnecting its external +48V DC power supply.

9 When all Bridges have rebooted, confirm the network configuration with `show sac`:

```
[GW] > show sac
SwabSerialNum:24656196
SwabConfigID:19082
SwabSACRole:SAC_MASTER
SwabSACState:SAC_INIT4SWAB
SwabSACVer:SAC_VER_PEGASUS_ARCH1
*********SACPeerInformation*********
SeriallNum|IpAddress|CfgID|PeerNum|PeerSACStatus|PeerSACState|PeerSACVer
24773196|172.24.0.4|19082|2|SAC_PEER_CONFIRMED|SAC_COMPLETE_4PEER|SAC_VER_PEGASUS_ARCH1
24743196|172.24.0.3|19082|1|SAC_PEER_CONFIRMED|SAC_COMPLETE_4PEER|SAC_VER_PEGASUS_ARCH1
```

The matching configuration IDs (`ConfigID`/`CfgID 19082`, above) indicate that the networked Bridges are all members of the same SAC group.

10 Confirm that all SAC group members are present on the network with `show partners`:

```
[GW] > show partners
 MAC|DeviceId|State|Username|SessionID|IP|vlanID|computerName|activityCount
02:14:8C:08:24:82|E4106192950F2494|01||0|172.24.0.4|0||56
00:14:8C:08:2C:C2|557C81E5D6072CD4|01||0|172.24.0.3|0||56
```

The configured Fortress Bridge network is ready to be deployed.

SAC commands are valid only in Gateway mode (refer to Section 6.1.1 for more detail).

6.8.2 Reconfiguring Network Settings with SAC

Only Bridges in Normal (non-FIPS) operating mode can be configured through SAC.

Once a network has been configured through SAC, you can use the SAC function to change any of the SAC-configurable parameters of the Fortress Bridges forming the network.

Because the channel setting and SSID of *Radio 2* in all network nodes must match, you can use the `show radio` and `show vap` commands on any network Bridge to view the current values of these SAC-configurable settings (refer to sections 6.4.3 and 6.4.3.1, respectively).

NOTE: When SAC network nodes use Radio 1 in AP mode, their SSIDs and channel settings should not match, even though they can be set globally with SAC. Use the `show radio` and `show vap` commands from the Bridge CLIs of individual network nodes to view these SAC-configurable settings.

Similarly, the encryption algorithm and re-key interval in effect on the network can be viewed with `show crypto` (sections 6.4.5.1 and 6.4.5.2, respectively).

The Access ID cannot be displayed for security purposes (but it must match across all network Bridges).

Use the `show network` command on the master/root Bridge to view its IP address (Section 6.4.1), and the `show sac` command to view the IP addresses of slave/non-root Bridges.

The same switches and arguments used to preconfigure the network through SAC (as explained in Section 6.8.1) are valid for reconfiguring the network.

Two additional switches modify the behavior of the SAC operation itself; these are shown in the third line of input below:

```
[GW] > set sac start [-a <accessId>] [-e AES128|AES192|AES256] [-t <rekeyint>] [-fips off|on]
[-sa <rad2ssid>] [-ca <rad2chnl>] [-sg <radio1ssid>] [-cg <radio1chnl>] [-ipnw <IPaddr>|<resIPnw>]
[-autogen yes|no] [-allowall yes|no]
```

When you set automatic generation (`-autogen`) to `yes`, the `set sac start` command automatically generates any of the SAC-configurable network settings (as shown in Table 6.1) that you do not explicitly specify in the command.

NOTE: As required for preconfiguration (Section 6.8.1, above), `-autogen` and `-allowall` default to `yes` when you first invoke `set sac start`. The defaults of these switches for subsequent `set sac start` invocations is `no`.

After the first invocation of `set sac start` (Section 6.8.1), the default `-autogen` setting is `no`, which causes only those network parameters that you specify to be changed from their current settings.

When you set allow all (`-allowall`) to `yes`, the master/root Bridge broadcasts the entire set of SAC parameters to any Fortress Bridge within range of the master/root Bridge. When `-allowall` is set to `no`, the master Bridge sends SAC parameters to only those Bri7dges on its SAC Peer list.

Fortress recommends that `-allowall` be left at its default setting of `no` when the `set sac command` is executed in any uncontrolled environment, particularly in a wireless environment.

CAUTION: Setting `-allowall` to `yes` in an uncontrolled environment poses a significant security risk.

For example, the command below changes the Radio 2 SSID on all Bridges in the SAC group:

```
[GW] > set sac start -sa caisiNET01
[OK] Started SAC process successfully
```

After executing `set sac start`, use `show sac` to confirm that the configuration change is `COMPLETE` for each SAC peer.

NOTE: Whenever the configuration changes, the configuration ID (`ConfigID`) also changes.

```
[GW] > show sac
SwabSerialNum:24656196
SwabConfigID:42550
SwabSACRole:SAC_MASTER
SwabSACState:SAC_START_4SWAB
SwabSACVer:SAC_VER_PEGASUS_ARCH1
*********SACPeerInformation*********
```

```
SeriallNum|IpAddress|CfgID|PeerNum|PeerSACStatus|PeerSACState|PeerSACVer
24773196|172.24.0.4|19082|2|SAC_PEER_CONFIRMED|SAC_COMPLETE_4PEER|SAC_VER_PEGASUS_ARCH1
24743196|172.24.0.3|19082|1|SAC_PEER_CONFIRMED|SAC_COMPLETE_4PEER|SAC_VER_PEGASUS_ARCH1
```

To save the new configuration, enter `set sac stop`:

```
[GW] > set sac stop
SAC Stop Initiated. May take some time to complete...
Stopped SAC process successfully
Reboot_Of_Master(SrlNum:24656196)_Required_For_NewConfiguration(CfgId:42550)_To_Take_Into_Effect
Reboot_Of_SACPeer(SrlNum:24773196)_Required_For_Configuration_Change_From(OldCfgId:19082)_To(New
CfgId:42550)_To_Take_Into_Effect
Reboot_Of_SACPeer(SrlNum:24743196)_Required_For_Configuration_Change_From(OldCfgId:19082)_To(New
CfgId:42550)_To_Take_Into_Effect
```

As the output informs you, you must reboot the Bridges in the network for the new configuration to take effect.

SAC commands are valid only in Gateway mode (refer to Section 6.1.1 for more detail).

6.8.3 Adding and Deleting Network Bridges with SAC

6.8.3.1 Adding a New SAC Network Bridge

Once a network has been configured through SAC, you can use the SAC function to add a new Fortress Bridge to the network.

1. Position the new Bridge so that it operates only within its safe temperature range (14º–122º F/-10º–50º C).
2. Connect an 802.11a-capable antenna to antenna port 2 (**ANT2**) of the new Bridge.
3. Connect the **WAN** port of the new Bridge to the **WAN** port of any node in the SAC network.
4. Connect the new Bridge's external +48V DC power supply to its front-panel **+48V DC** power inlet, and plug the power supply into a properly rated AC power outlet with the cord provided.
5. Connect the new Bridge's **Console** port directly to the serial terminal of the computer you will use to preconfigure the new Bridge.
6. Open a terminal application on the computer connected to the new Bridge's **Console** port and (using the settings given in Section 6.1.2) open a session with the new Bridge.
7. Log in to the CLI of the new Bridge, using **`sysadm`** as both the login ID and password.
8. Preconfigure the new Bridge to use the same Access ID and encryption algorithm already in effect on the Fortress Bridge network with these commands:

NOTE: An RJ-45-to-DB9 adapter—included with each Bridge—is required to connect the Bridge's serial **Console** port to a DB9 terminal connection. Pin outs for these adapters are given in Table 7.1 on page 116.

```
[GW] > set accessid <16digithexid>

[GW] > set crypto [-e aes128|aes192|aes256][-t <hrs>]
```

9. Use `show sac` to determine—and then make a note of—the serial number of the new Bridge:

```
[GW]> show sac
SwabSerialNum:24743196
SwabConfigID:0
SwabSACRole:SAC_SLAVE
SwabSACState:SAC_INIT4SWAB
SwabSACVer:SAC_VER_PEGASUS_ARCH1
```

10 Log off the new Bridge's CLI and disconnect the **Console** port cable.

11 Log onto the Bridge CLI of the master/root Bridge and add the new Bridge's serial number to the master Bridge's SAC Peer list, with the `add` command:

```
[GW]> add sp 24743196
[OK]
```

If you are adding multiple Bridges, enter their serial numbers separated by commas, without spaces.

12 Execute the `set sac start` command:

```
[GW]> set sac start
[OK] Started SAC process successfully                    er 62(t-45.2(a)4.7he n(w ma)-268(r)-1.6rid)-268ge,r 6
```

When the SAC process starts, you can observe the master/root Bridge's front-panel **Stat1** LED flash amber and its **Stat2** LED light solid amber. As the new Bridge receives the SAC parameters, its **Stat1** and **Stat2** LEDs flash amber in unison.

132

NOTE:

1 Tc0 Tw[([GW)6.7(]>)]TJ/F2 1 Tf8.5985 0 0 9.48 104.343601.02 Tm-0.0069 Tc-0.007 Tw[shr

16 Disconnect the WAN ports of the new and master Bridges.

17 Power cycle the new Bridge.

The new Bridge is ready to be deployed on the network.

6.8.3.2 Deleting a Bridge from a SAC Network

You can view the current list of SAC Peers from the master/root Bridge's CLI with `show sp`:

```
[GW]> show sp
Peer1=>Serial_Number:24773196
Peer2=>Serial_Number:24743196
```

You can determine the serial number of a particular SAC Peer by executing `show sac` from the CLI of the Bridge in question:

```
[GW]> show sac
SwabSerialNum:24773196
SwabConfigID:16284
SwabSACRole:SAC_SLAVE
SwabSACState:SAC_INIT4SWAB
SwabSACVer:SAC_VER_PEGASUS_ARCH1
```

Use the `del` command—from the master/root Bridge's CLI—to delete a Bridge from the master/root Bridge's SAC Peer list and from the SAC network:

```
[GW]> del sp <serialnumber>
```

where *<serialnumber>* is the serial number of the Bridge you want to remove from the network.

SAC commands are valid only in Gateway mode (refer to Section 6.1.1 for more detail).

Chapter 7
Specifications

7.1 Hardware Specifications

7.1.1 Performance

unencrypted throughput:	up to 23 Mbps
encrypted throughput:	up to 10 Mbps

7.1.2 Physical

form factor:	compact, rugged desktop chassis
dimensions:	2.3" H x 8.75" W x 6.6" D (5.8 cm×22.2 cm×16.8 cm)
weight:	3.5 lbs. (1.6 kg), approximate
connections:	nine RJ-45 10/100 Mbps Ethernet ports one RJ-45 serial port two USB ports one 48V DC power input port two N-type antenna ports (female): **ANT1** radio configured as 802.11a/b/g tri-band port **ANT2** radio configured as high-gain 802.11a port (5.7–5.8 GHz)
power supply:	external +48V AC-to-DC adapter *or* WAN port power over Ethernet (PoE)
system indicators:	eight front-panel system LEDs (G/Y): *Status1* (**Stat1**), *Status2* (**Stat2**), *Cleartext* (**Clr**), *Failover* (**Fail**), *two LEDs for wireless* **Radio2**, *two LEDs for wireless* **Radio1** nine pairs integrated port *link/activity* & *power* LEDs

7.1.3 Environmental

maximum AC draw:	13 Watts (57 Watts in reserve for future per-port power sourcing)
maximum heat dissipation:	44.3 BTU/hr
cooling:	fanless heat sink chassis
operating temperature:	14º–122º F (-10º–50º C)
operating relative humidity (non-condensing):	5%–95%
storage temperature:	-4º–158º F (-20º–70º C)

7.1.4 Compliance

safety:	UL60950-1, IEC60529 (CB test), UL (NEMA) 3/3S/4 “raintight”
emissions:	CE, FCC Class A
immunity:	EN61000-3, EN61000-4
vibration:	MIL-STD 810F 514 / SC-18 (pending)

7.1.5 Logical Interfaces

The physical connections described in Section 7.1.2 are identified as logical interfaces, as defined by FIPS 140-2, in the table below:

Logical Interface	Physical Interface
data input:	nine RJ-45 10/100 Mbps Ethernet ports two N-type antenna ports (female): **ANT1** radio configured as 802.11a/b/g tri-band port **ANT2** radio configured as high-gain 802.11a port (5.7–5.8 GHz
data output:	nine RJ-45 10/100 Mbps Ethernet ports two N-type antenna ports (female): **ANT1** radio configured as 802.11a/b/g tri-band port **ANT2** radio configured as high-gain 802.11a port (5.7–5.8 GHz
control input:	nine RJ-45 10/100 Mbps Ethernet ports one RJ-45 serial port one 48V DC power input port two N-type antenna ports (female): **ANT1** radio configured as 802.11a/b/g tri-band port **ANT2** radio configured as high-gain 802.11a port (5.7–5.8 GHz) front-panel, recessed, warm-power reset control
status output:	nine RJ-45 10/100 Mbps Ethernet ports one RJ-45 serial port one 48V DC power input port two N-type antenna ports (female): **ANT1** radio configured as 802.11a/b/g tri-band port **ANT2** radio configured as high-gain 802.11a port (5.7–5.8 GHz) eight front-panel system LEDs nine pairs integrated port *link/activity* & *power* LEDs
power:	external +48V AC-to-DC adapter *or* WAN port power over Ethernet (PoE)

7.2 RJ-45-to-DB9 Console Port Adapter

An RJ-45-to-DB9 adapter (included with each Bridge) is required in order to connect the Bridge’s **Console** port to a DB9 terminal connection.

Figure 7.1 below shows the pin numbers for the two connectors. With the RJ-45 connector facing you and oriented with the tab receptacle up, pins are numbered from left to right, as shown. With the DB9 connector facing you and oriented with

the wide side up, pins are numbered from right to left, top to bottom.

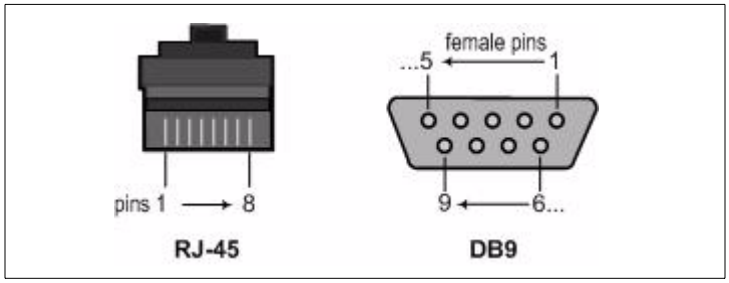


Figure 7.1 RJ-45 and DB9 Pin Numbering

Table 7.1 shows the adapter pin-outs.

Table 7.1. RJ-45-to-DBP Adapter Pin-Outs

RJ-45 pin	DB9 pin	standard color
1	-	grey
2	4	brown
3	3	yellow
4	-	green
5	5	red
6	2	black
7	6	orange
8	8	blue

Chapter 8
Troubleshooting

Problem	Solution
You are unable to access the Bridge GUI.	Verify the Bridge's physical connection: • from an Ethernet port on a computer or a network switch to one of the Bridge's unencrypted internal LAN ports. —or— • from a computer running the Fortress Secure Client in the Bridge's encrypted zone.
	Verify the browser link: • the computer you are using to access the Bridge GUI is in the same subnet as—or has a network route to—the Bridge's IP address. • you are using *https* (hypertext transfer protocol with Secure Socket Layer), rather than simple http to connect to the Bridge GUI. • you are using the correct IP address and subnet mask to connect (the default is 192.168.254.254, subnet mask 255.255.255.0). • if you just changed Bridge's IP address, you have closed the browser window you last used to access the Bridge GUI and opened a new browser window to access its new address.
	Verify the Bridge GUI's accessibility: • the Bridge GUI has not been disabled in the Bridge CLI. • no one is logged on to the Bridge CLI. • the Bridge's IP address has not changed.
You are unable to access the Bridge CLI.	• Verify that your serial application is using the correct settings: bps=38400, data bits=8, parity=none, stop bits=1, flow control=none • If you are connecting directly to the Bridge's **Console** port, verify the physical connections. • If you are connecting remotely, verify that SSH has been enabled through the **Console** port. (SSH is disabled by default.)

Problem	Solution
The Bridge is not allowing traffic to pass.	Verify the Bridge's physical connections: • from the Bridge's **Unencrypted** port to the LAN. • from the Bridge's **Encrypted** port to the WLAN. • in AF7500 & AF2100, verify the CAT5e cable type (*crossover* for direct host/AP connections; *straight* for connections to switches/hubs).
	Verify that auto-negotiation is enabled on all devices directly connected to the Bridge, including switches, hubs and APs.
	Reset connections (clear the Secure Client database). If this does not resolve the problem, restart/reboot the Bridge's cryptographic processor.
	Verify the underlying network configuration: temporarily remove the Bridge and verify that network traffic passes normally.
A Secure Client device cannot communicate with the Bridge.	Verify that the Secure Client is configured to use the same Access ID and encryption algorithm as the Bridge.
	Reset connections (clear the Secure Client database) on the Bridge. If this does not resolve the problem, restart/reboot the Bridge's cryptographic processor.
	Reset connections on the Secure Client (refer to your Fortress Secure Client user guide for instruction).
	In devices using a NIC to communicate with the WLAN through a Cisco® AP, verify that Cisco AP packet encapsulation mode on the AP is set to *RFC 1042*.
After the Bridge is restarted, some Secure Clients do not immediately resume processing.	On each affected Secure Client, reset all connections (refer to your Fortress Secure Client user guide for instruction).
In a point-to-point/multipoint deployment, Secure Clients receive excessive login prompts.	Disable the *Restart Session Login Prompt* on all non-root Bridges in the network (on *SECURITY SETTINGS* under *AUTHENTICATION SETTINGS*).
An upgrade process simply fails to complete, or fails with the message: *Failed to decrypt*.	Restart/reboot the Bridge, and retry the upgrade procedure. If the upgrade continues to fail, contact Fortress Technical Support.

Index

Numerics

A

B

C

D

E

F

G

H

I

L

M

N

O

P

R

S

T

U

more...

V

W

Glossary

3DES	Triple Data Encryption Standard—a FIPS-approved NIST standard for data encryption using 192-bits (168-bit encryption, 24 parity bits) for protecting sensitive (unclassified) U.S. government (and related) data. NIST amended and re-approved 3DES for FIPS in May, 2004.
802.11	The IEEE standard that specifies technologies for WLANs.
802.1X user authentication	An IEEE standard for port-based network access control, providing user authentication and authorization to devices attached to a LAN port (or preventing access from that port if authentication fails).
802.16	The IEEE standard that specifies technologies for fixed broadband wireless MANs that use a point-to-multipoint architecture, also called WiMAX, WirelessMAN™ or the Air Interface Standard.
Access ID	In Fortress Technologies products, a user-defined, 16-digit hexadecimal value that provides network authentication for all devices authorized to communicate over a Fortress-secured network. Network authentication is one of the components of Multi-factor Authentication™.
access point (AP)	A device that transmits and receives data between a wired LAN and a WLAN. APs connect multiple users and wireless devices within a defined area. Multiple APs increase the coverage area: as devices move out of range of one AP, they automatically connect to a neighboring AP.
AES	Advanced Encryption Standard—a FIPS-approved NIST standard for 128/192/256-bit data encryption for protecting sensitive (unclassified) U.S. government (and related) data; also referred to as the *Rijndael algorithm*. NIST FIPS-approved AES in November, 2001.
administrator password	In Fortress Technologies products, a password that guards against unauthorized modifications to the system or its components.
APIPA	Automatic Private IP Addressing—a Microsoft feature that allows a DHCP client unable to acquire an address from a DHCP server to automatically configure itself with an IP address from a reserved range (169.254.0.1 through 169.254.255.254). The client uses the self-configured IP address until a DHCP server becomes available.
ARP	Address Resolution Protocol—describes how IP addresses are converted into physical, DLC addresses, (ex., MAC addresses).
ATM	Asynchronous Transfer Mode—a technology for transferring data over a network in packets or cells of a fixed size.
BPM	In FIPS, bypass mode—state in which cleartext is allowed to pass on an encrypted interface
bridge	A network device that connects two networks or two segments of the same network.
Bridge	Refer to *Fortress Secure Wireless Access Bridge*.

Bridge GUI	The browser-based graphical user interface through which the Fortress Secure Wireless Access Bridge is configured and managed, locally or remotely.
CCITT	Comite Consultatif Internationale de Telegraphie et Telephonie, former name of the ITU-T.
client	In the Fortress Controller FISh (command-line) interface and front-panel LCD, devices on the encrypted (WLAN) side of the network and running the Fortress Secure Client. In the Fortress Gateway FISh (command-line) interface, devices on the unencrypted (LAN) side of Gateway. In client-server architecture, an application that relies on another, shared application (server) to perform some of its functions, typically for an end-user device.
Client	Refer to *Fortress Secure Client*.
controller	A device that controls data transfer between a computer and a peripheral device.
Controller	Refer to *Fortress Security Controller*.
Controller GUI	The browser-based graphical user interface through which the Fortress Security Controller is configured and managed, locally or remotely.
Crypto Officer password	A FIPS-defined term—sometimes, *Crypto password*—the a*dministrator password* in Fortress devices in FIPS-enabled operating mode.
Data Link Layer	Refer to *DLC*.
DES	Data Encryption Standard—formerly, a FIPS-approved NIST standard for data encryption using 64 bits (56-bit encryption, 8 parity bits). NIST withdrew its FIPS-approval for DES on May 19, 2005.
device authentication	In Fortress Technologies products, the means by which MaPS/ACS controls network access at the level of individual devices, tracking them via their generated Device IDs and providing the network administrator tools to explicitly allow and disallow them on the network; one of the factors in Fortress's Multi-factor Authentication™.
Device ID	In Fortress Technologies products, a 16-digit hexadecimal value generated for, and unique to each, Fortress controller device and Secure Client device on the Fortress-secured network. Device IDs are used for *device authentication* and are neither modifiable nor transferable.
DHCP	Dynamic Host Configuration Protocol—an Internet protocol describing a method for flexibly assigning device IP addresses from a defined pool of available addresses as each networked device comes online, through a client-server architecture. DHCP is an alternative to a network of fixed IP addresses.
Diffie-Hellman key establishment	A protocol by which two parties with no prior knowledge of one another can agree upon a shared secret key for symmetric key encryption of data over an insecure channel. Also, *Diffie-Hellman-Merkle key establishment*; *exponential key exchange*.
DLC	Data Link Control—the second lowest network layer in the OSI Model, also referred to as the *Data Link Layer*, *OSI Layer 2* or simply *Layer 2*. The DLC layer contains two sublayers: the MAC and LLC layers.
DMZ	Demilitarized Zone—in IT, a computer (or subnet) located between the private LAN and a public network, usually the Internet.
DoD	Department of Defense
EAP	Extensible Authentication Protocol—defined by RFC 2284, a general protocol for user authentication. EAP is implemented by a number of authentication services, including RADIUS.
EAP-MD5	An EAP security algorithm developed by RSA Security® that uses a 128-bit generated number string, or hash, to verify the authenticity of a data transfers.
EAP-TLS	EAP-Transport Layer Security—a Point-to-Point Protocol (PPP) extension supporting mutual authentication, integrity-protected cipher suite negotiation, and key exchange between two endpoints, within PPP.
EAP-TTLS	EAP-Tunneled TLS—An EAP-TLS protocol developed by Funk and Certicom that uses TLS to establish a secure connection between a client and server.

failover	A device or system configuration in which two, identical components are installed for a given function so that if one of them fails the redundant component can carry on operations without any substantial interruption of service. Also, an instance in which an active component becomes inoperative and *fails over* operations to its partner.
FIPS	Federal Information Processing Standards—issued by NIST, FIPS mandate how IT, including network security, is implemented by the U.S. government and associated agencies.
FIPS operating mode	In Fortress Technologies products, the operating mode that complies with FIPS 140-2.
FISh	Fortress Interface Shell—formerly, the command-line interface for configuring and managing a Fortress controller device through a direct physical connection or a serial terminal application.
Fortress ACS	Fortress Access Control Server—a Fortress Technologies client-server application that predates MaPS and provides centralized management of the Fortress-secured network.
Fortress controller device	The collective noun for Fortress network devices that secure communications between wireless devices and a LAN, or between devices within a LAN, or between two WLANs/LANs in a point-to-point or -multipoint configuration—comprising Fortress Security Gateways, Fortress Security Controllers and Fortress Secure Wireless Access Bridges.
Fortress MaPS™	Fortress Management and Policy Server—a client-server application that provides centralized management of the Fortress-secured network, as well as device and user authentication (through MaPS or in conjunction with an existing authentication server). MaPS runs as a service and is managed from the MaPS Console.
Fortress Secure Client	A software client module for securing network communications on laptops, PDAs, tablet PCs, and industrial equipment such as barcode scanners and portable terminals.
Fortress Secure Client Bridge	Also, *Fortress SCB* or *SCB*—a hardware device for providing wireless connectivity and securing network communications on wired devices such as portable medical equipment and point-of-sale (POS) terminals.
Fortress Security Controller	Sometimes, *Fortress Controller*—A network device for securing, at Layer 2 of the OSI Model, communications between wireless devices and a LAN, or between devices within a LAN, or between two WLANs/LANs in a point-to-point or -multipoint configuration.
Fortress Security Gateway	Sometimes, *Fortress Secure Gateway* or *Fortress Gateway*—A network device for securing, at Layer 2 of the OSI Model, communications between wireless devices and a LAN, or between devices within a LAN, or between two WLANs/LANs in a point-to-point or -multipoint configuration.
Fortress Security System	The deployment of Fortress controller devices, MaPS (or ACS), and Fortress Secure Clients and/or Secure Client Bridges working together to secure a network. The minimum configuration for the Fortress Security System is a controller device and one or more Secure Clients.
Fortress Secure Wireless Access Bridge	Also, *Fortress Bridge*—an network device that can act as an access point, wireless bridge and/or LAN switch, as well as provide a DSL/cable/satellite link, while securing, at Layer 2 of the OSI Model, communications between wireless devices and a LAN, or between devices within a LAN, or between two WLANs/LANs in a point-to-point or -multipoint configuration.
frame	In Fortress Technologies GUIs, a portion of a larger screen or dialog, graphically set apart from other elements on the screen and providing the interface for a specific feature or function set. In IT, a packet of data transmitted/received.
gateway	In IT, a node on a network, usually a router, that provides a connection to another network.
Gateway	Refer to *Fortress Security Gateway*.
Gateway GUI	The browser-based graphical user interface through which the Fortress Gateway is configured and managed, locally or remotely.

groups	An association of network objects (users, devices, etc.). Groups are typically used to allocate shared resources and apply access policies.
GUI	Graphical User Interface
guest	In Fortress Technologies, a guest user as configured in MaPS. Alternatively, in the Fortress Controller, devices given access on the encrypted (WLAN) side of the network as Trusted Devices, access points, or guests.
host	In Fortress Technologies, devices on the unencrypted (LAN) side of the network.
HTTP	Hypertext Transfer Protocol—used to transmit and receive all data over the World Wide Web.
IANA	Internet Assigned Number Authority—the organization that assigns Internet Protocol (IP) addresses and port numbers.
ICMP	Internet Control Message Protocol —supports packets containing error, control, and informational messages. The **`ping`** command uses ICMP to test an Internet connection.
IDS	Intrusion Detection System—monitors network activity to identify suspicious patterns that may indicate a network or system attack and supports automated and/or manual real-time responses.
IEEE	Institute of Electrical and Electronics Engineers—a nonprofit technical professional association that develops, promotes, and reviews standards within the electronics and computer science industries.
IETF	Internet Engineering Task Force—the primary standards organization for the Internet.
IP	Internet Protocol—defines a method for transmitting data, in packets, from one computer to another over a network, one of the two primary protocols implemented in TCP/IP networks.
IPS	Intrusion Prevention System—allows network administrators to apply policies and rules to network traffic, as it is monitored by an intrusion detection system.
IPsec	Internet Protocol security—a set of protocols developed by the IETF to support secure exchange of packets at the IP layer, deployed widely to implement VPNs.
ISO	International Organization for Standardization, formerly the International Standards Organization—ISO still refers to standards (ex., ISO 9000); the whole name refers to the organization, sometimes appending the earlier initialization in parentheses.
IT	Information Technology
ITU-T	International Telecommunications Union-Telecommunication, Geneva-based international organization for telecommunications standards, formerly CCITT.
key establishment	An transaction through which two parties with no prior knowledge of one another can agree upon a shared secret key for symmetric key encryption of data over an insecure channel. Sometimes, key exchange
LAN	Local Area Network—a collection of computers located within a small geographic area (such as an office building) that shares a common communications infrastructure and network resources (i.e., printers, servers, etc.).
Layer 2	Refer to DLC.
LDAP	Lightweight Directory Access Protocol—a protocol used to access directories on a network, including the Internet. LDAP makes it possible to search compliant directories to locate information and resources on a network. LDAP is a streamlined version of the Directory Access Protocol, part of the X.500 standard for network directory services.
LLC	Logical Link Control—one of two sublayers of OSI Layer 2 (refer to *DLC*), in which frame synchronization, flow control and error checking takes place.
MAC	Media Access Control—one of two sublayers of the OSI Model's DLC, at which data access and transmission permissions are controlled.
MAC address	Media Access Control address—a unique number that identifies a device, used to properly direct network traffic to the device.
MaPS™	Refer to Fortress MaPS.

MaPS Console	In Fortress's MaPS, a Java-based, configuration client interface for the Fortress Management and Policy Server, through which all MaPS functions are accessed.
MaPS object	In Fortress's MaPS, any entity on the secure network, including Fortress controller devices, Secure Client devices, users, and network resources.
MAN	Metropolitan Area Network—a collection of interconnected computers within a town or city.
MIB	Management Information Base—SNMP-compliant information that an SNMP agent stores about itself and sends in response to SNMP server requests (PDUs).
MobileLink™	In GE Medical Systems *Information Technologies*, a proprietary method for wireless transmission of serial output.
MITM	Man in the Middle attack—a network security breach in which an attacker is able to intercept, read, insert and modify messages between two parties without their knowing that the link between them has been compromised.
Multi-factor Authentication™	In Fortress Technologies products, the combination of network authentication (through the network Access ID), device authentication (through the Device ID), and user authentication (through user credentials), that guards the network against unwanted access. (Device authentication can be implemented only on a MaPS-managed network.)
multiplexing	The practice of transmitting multiple signal types over a single connection.
NetBIOS	Network Basic Input/Output System—an API that originally provided basic I/O services for a PC-Network and that has been variously adapted and augmented to support current LAN/WLAN technologies.
network authentication	In Fortress Technologies products, the requirement that all devices must authenticate with the correct *Access ID* in order to connect to the Fortress-secured network; one of the factors in Fortress's Multi-factor Authentication™.
network resource	In Fortress's MaPS, one of a special class of MaPS object on the wired LAN that provides a service or function, such as e-mail or printing, to devices and users on the WLAN.
NIAP	National Information Assurance Partnership—a collaboration between NIST and the National Security Agency (NSA), in response to the Computer Security Act of 1987 (PL 100-235), to promote sound security requirements for IT products and systems and appropriate measures for evaluating them.
NIST	National Institute of Standards and Technology, the U.S. Government agency responsible for FIPS.
NTLM	Windows NT LAN Manager—a user authentication protocol developed by Microsoft®.
operating mode	In Fortress Technologies products, the way in which access controls and cryptographic processing are implemented on the Fortress-secured network.
OSI Model	Open System Interconnection Model—an ISO standard that defines a networking framework for implementing data transfer and processing protocols in seven layers. (Also see, *DLC*.)
PAN	Personal Area Network
partner	In Fortress Technologies, devices in communication with the Fortress controller device, including redundant controller devices, access points and any configured Trusted Devices, as well as the controller device's Secure Clients.
PDU	Protocol Data Unit—often synonymous with *packet*, a unit of data and/or control information as defined by an OSI layer protocol
PKI	Public Key Infrastructure (PKI), a system of digital certificates and other registration authorities that authenticate the validity of each party involved in an Internet transaction; sometimes, trusted hierarchy.
policy	In Fortress's MaPS, the means by which access to the secure network and its resources are controlled for users, devices and groups.
PPP	Point-to -Point Protocol—a method for communicating TCP/IP traffic over serial point-to-point connections.

RSA SecurID®	An authentication method created and owned by RSA Security.
RADIUS	Remote Authentication Dial-In User Service—an authentication server design that issues challenges to connecting users for their usernames and passwords and authenticates their responses against a database of valid usernames and passwords; described in RFC 2865.
RF	Radio Frequency
RFC	Request for Comments—a document proposing an Internet standard that has been accepted by the IETF as potentially developing into an established Internet standard.
SCB	Refer to *Fortress Secure Client Bridge*.
Secure Client	Refer to *Fortress Secure Client*.
Secure Client Bridge	Refer to *Fortress Secure Client Bridge*.
Secure Client device	In Fortress Technologies products, a device such as a laptop, PDA, tablet PC, or barcode scanner, that has the Fortress Secure Client installed and configured to permit the device to communicate on the Fortress-secured network.
Secure/Security Gateway	Refer to *Fortress Security Gateway*.
SFP	Small Form Pluggable—shorthand for fiber optic Small Form Pluggable transceiver.
SHA	Secure Hash Algorithm
SLIP	Serial Line Internet Protocol—a method for communicating over serial lines, developed for dial-up connections.
SMTP	Simple Mail Transfer Protocol—describes a method for transmitting e-mail between servers.
SNMP	Simple Network Management Protocol—a set of protocols for simplifying management of complex networks. The SNMP server sends requests (PDUs) to network devices, and SNMP-compliant devices (SNMP agents) respond with data about themselves (stored in MIBs).
SNMP agent	Any network device running the SNMP daemon and storing a MIB, a client of the SNMP server.
SSH®	Secure Shell®, sometimes, Secure Socket Shell—a protocol, developed by SSH Communication Security®, for providing authenticated and encrypted logon, file transfer and remote command execution over a network.
state	In Fortress Technologies products, the exact stage of key negotiation between a Secure Client and the Fortress controller device through which it connects.
SWLAN	Secure Wireless Local Area Network
symmetric key encryption	A class of cryptographic algorithm in which a shared secret between two or more parties is used to maintain a private connection between or among them.
TCP	Transmission Control Protocol—defines a method for reliable (i.e., in order, with integrity checking) delivery of data packets over a network, one of the two primary protocols implemented in TCP/IP networks.
TCP/IP	Transmission Control Protocol/Internet Protocol—the basic, two-part communication protocol in use on the Internet (refer to IP and TCP).
TLS	Transport Layer Security—a two-part protocol that defines secure data transmission between client/server applications communicating over the Internet. TLS Record Protocol uses data encryption to secure data transfer, and the TLS Handshake Protocol allows the client and server to authenticate each other and negotiate the encryption method to use before exchanging data.
Trusted Device	In Fortress Technologies products, a device that does not have the Secure Client installed but is allowed network access through a policy created for it in MaPS or rules defined for it on the Fortress controller device.
trusted hierarchy	Refer to PKI.

UDP	User Datagram Protocol—defines a method for “best effort” delivery of data packets over a network that, like TCP, runs on top of IP but, unlike TCP, does not guarantee the order of delivery or provide integrity checking.
user authentication	The practice of requiring users to enter their assigned user IDs and established passwords and of checking the validity of these credentials before allowing them to connect to the network.
user password	The password a user must enter in order to access a network or system that requires user authentication.
VLAN	Virtual Local Area Network—a collection of computers configured through software to behave as though they are members of the same network, even though they may be physically connected to separate subnets.
VoIP	Voice over IP, sometimes VOI (Voice over Internet)
VPN	Virtual Private Network—a private network of computers connected, entirely or in part, by public phone lines.
WEP	Wired Equivalent Privacy—security protocol for WLANs, defined in the 802.11b standard but subsequently found to be vulnerable to attack. WPA is intended to supplant WEP in current and future 802.11 standards.
Wi-Fi®	Wireless Fidelity—used generically to refer to any type of 802.11 network (referred originally to the narrower 802.11b specification for WLANs).
WiMAX	Worldwide Interoperability for Microwave Access—the IEEE 802.16 specification for fixed, broadband, wireless MANs that use a point-to-multipoint architecture, defining bandwidth use in the licensed frequency range of 10GHz–66GHz and the licensed and unlicensed frequency range of 2GHZ–11GHz.
WIDS	Wireless Intrusion Detection System
WLAN	Wireless Local Area Network. A local area network that allows mobile users network access through radio waves rather than cables.
WPA	Wi-Fi Protected Access—a specification for implementing security on Wi-Fi networks using 802.1x and EAP to restrict network access, and TKIP encryption to secure data transfer. WPA is designed to replace the weaker WEP on WEP-enabled network devices and in current and future 802.11 standards.