0.1 Wireless Support

Note: This equipment has been approved for mobile operation, and requires a minimum of 20 cm (7.9 inches) of space between the antenna(s) and each person's body (excluding extremities of hands, wrists, and feet) during wireless modes of operation.

The maximum antenna gain should not exceed 6 dBi.

Wireless connections use radiofrequencies through air waves instead of electrical signals through cables. A cellular wireless connection allows free physical movement within the broadcast radius of a cell's wireless access point (AP)—for example, a cell tower. Each wireless AP provides a direct or indirect cabled connection to the core of the wireless network.

The BANDIT chassis can hold an expansion module for connection to a cellular wireless network. The BANDIT's expansion port can hold a card for access to one of the following wireless networks. (The card installed depends on the wireless carrier and network you wish to use; you order a GSM or CDMA card according to the technology the carrier uses.)

- Code Division Multiple Access (CDMA) wireless network
- Global System for Mobile Communications (GSM) wireless network

A wireless network card supports the BANDIT as a wireless terminal. The card supports a wireless connection to a wireless access point (AP), such as a cell tower. (The BANDIT does not act as a gateway or AP for other wireless devices. That is, it does not provide a connection through which other terminal wireless devices, such as a cellphone or a wireless laptop computer, can reach a wireless network.)

You can set the BANDIT up to provide a connection between a cabled network and a wireless network. All features of the BANDIT are available for wireless and wired connections.

Figure 0-1 illustrates the BANDIT's wireless and wired connections. The BANDIT can send a transmission through a wireless carrier or through a wired network.

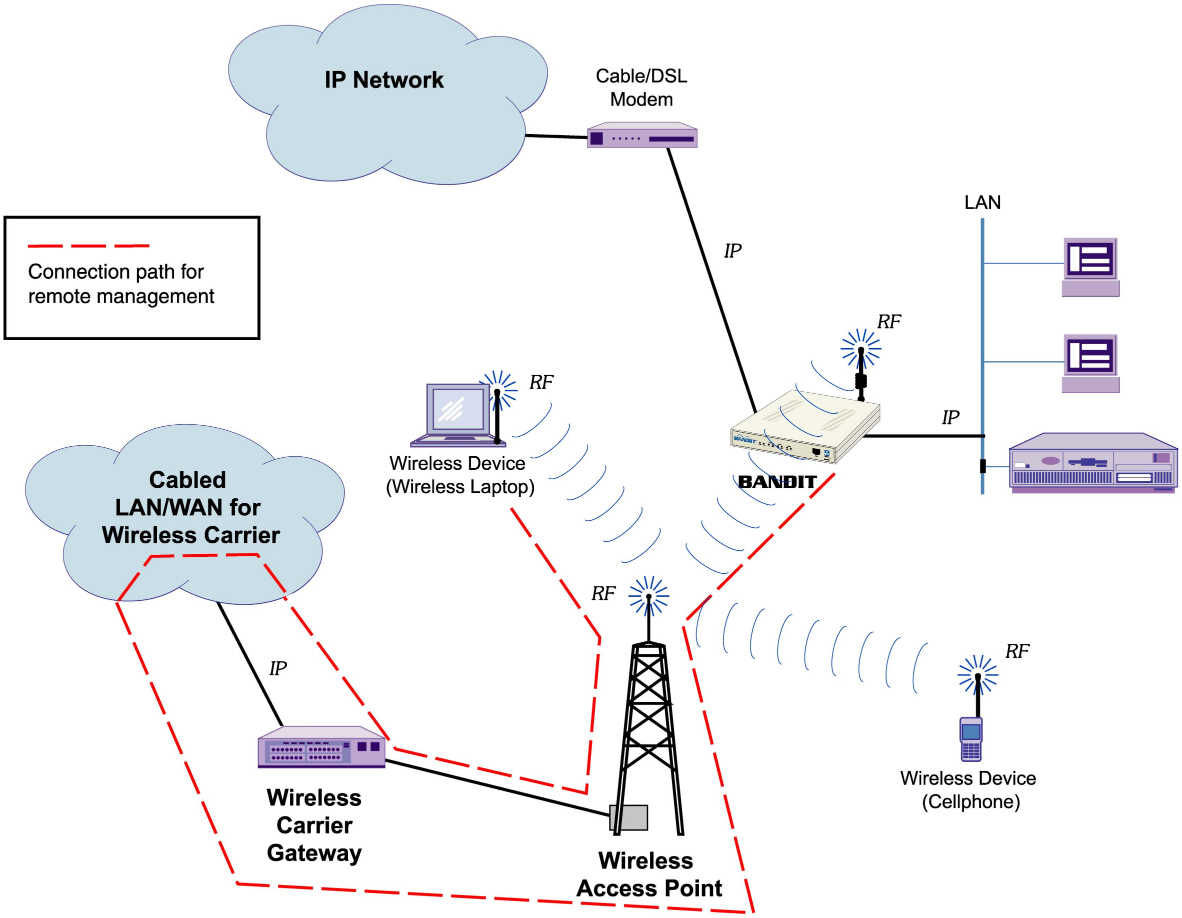
IP Network
Cable/DSL Modem
Connection path for remote management
LAN
IP
RF
IP
Wireless Device (Wireless Laptop)
RF
BANDIT
Cabled LAN/WAN for Wireless Carrier
IP
RF
RF
Wireless Device (Cellphone)
Wireless Carrier Gateway
Wireless Access Point

Figure 0-1. BANDIT Connections to Wireless Carrier, to Wired LAN, and to Wired IP Network

Note: A remote terminal can be set up to manage the BANDIT, from any location over any network. For example, a wireless laptop can manage the BANDIT remotely, if you configure the BANDIT's firewall to accept the connection. As in any other remote connection, the wireless laptop's packets go through the wireless carrier's network to be routed to the BANDIT (see Figure 0-1).

Figure 0-2 shows a BANDIT wireless card's faceplate with a mini-meg connector port for an antenna. Figure 0-3 shows a wireless module, with antenna, installed in the BANDIT chassis.

Note: The standard antenna for the BANDIT's wireless modules has 0 db (no gain). Contact your Encore Networks sales representative if you would like an optional antenna that has a +3 dB gain.

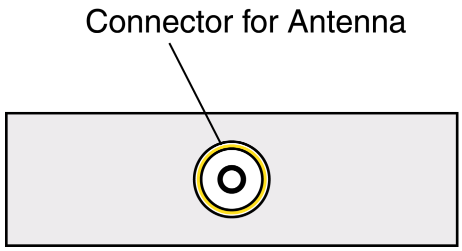

Figure 0-2. Wireless Module Faceplate

?? Picture currently unavailable

Figure 0-3. BANDIT Using Wireless Module, with Antenna Connected to Module

Warning: It is extremely important to set up security measures, including firewall protection, for each wireless device. Use the BANDIT's firewall for wireless connections to protect the BANDIT and its connection to the wireless network. See Section 0.1.1, *The BANDIT's Wireless Firewall*.

The BANDIT uses spoofing to handle legacy protocols that are sensitive to delay. It receives packets from the sender and replies with acknowledgment packets as if it were the remote terminal at the end of the connection; at the same time, the BANDIT sends the received data across the wireless network to the real remote terminal. The same process occurs in reverse when the remote terminal sends reply packets.

Note: When you order a CDMA wireless card for the BANDIT, the carrier-specific software is loaded on the wireless card before shipment.

A GSM carrier provides a Subscriber Identity Module (SIM) to insert into the GSM wireless card.

See the following sections:

- Section 0.1.1, *The BANDIT's Wireless Firewall*
- Section 0.1.2, *The CDMA Wireless Card*
- Section 0.1.3, *The GSM Wireless Card*

0.1.1 The BANDIT's Wireless Firewall

It is extremely important to set up security measures, including firewall protection, for each wireless device. Use the following procedure to configure a firewall to protect the BANDIT and its connection to the wireless network.

How to Configure the BANDIT's [Wireless??] Firewall

1 ?? To be added.

0.1.2 The CDMA Wireless Card

CDMA uses spread-spectrum technology.

Table 0-1 lists the specifications for the BANDIT's CDMA wireless expansion module.

Table 0-1. Specifications for CDMA Wireless Card (*1 of 2*)

Specification	CDMA Module
Power supply's maximum voltage	4.2 VDC

Table 0-1. Specifications for CDMA Wireless Card (2 of 2)

Specification	CDMA Module
Number of ports	One wireless port
Wireless interface	CDMA 2000 (IS-2000)
Data rate per port	Up to 153 kbps
Throughput	Up to 153 kbps
Dimensions (L x W x H)	2.3 in. x 1.3 in. x 0.2 in. (58 mm x 32.6 mm x 3.9 mm)
Weight	0.005 lb. (11 g)
Operating temperature	-22°F to 140°F (-30°C to 60°C)
Storage temperature	-40°F to 185°F (-40°C to 85°C)
Band of Operating Frequencies	(Dual band) Band class 0: Tx 824–849 MHz, Rx 869–894 MHz Band class 1: Tx 1850–1910 MHz, Rx 1930–1990 MHz

0.1.2.1 Activating the CDMA Card in the Carrier Network

The CDMA module is activated for use before shipment. However, you must activate the module for use in the carrier's network. Use one of the following procedures, depending on the carrier you have selected.

- *How to Activate the CDMA Card for the Sprint Network*
- *How to Activate the CDMA Card for the Verizon Network*

How to Activate the CDMA Card for the Sprint Network

Note: Before you activate the module in the network, make sure the module has already been properly provisioned for the Sprint network. (This was done before the BANDIT device was shipped to you.)

?? Procedure to be added.

How to Activate the CDMA Card for the Verizon Network

Note: Before you activate the module in the Verizon network, make sure the module has already been properly provisioned for the Verizon network. (This was done before the module was shipped to you.)

?? Procedure to be added.

0.1.2.2 Configuring the CDMA Wireless Card

Use the following procedure to configure the CDMA wireless connection in your network.

How to Configure the CDMA Wireless Port

1. ?? To be added.

0.1.3 The GSM Wireless Card

GSM is based on TDMA technology. The GSM card supports General Packet Radio Service (GPRS) for data transfer.

Table 0-2 lists the specifications for the BANDIT's GSM wireless expansion module.

Table 0-2. Specifications for GSM Wireless Card (1 of 2)

Specification	GSM Module
Power supply's maximum voltage	4.5 VDC
Number of ports	One wireless port
Wireless interface	GSM
Data rate per port	Up to 144 kbps
Throughput	Up to 144 kbps
Dimensions (L x W x H)	2.3 in. x 1.3 in. x 0.2 in. (58.4 x 32.2 x 3.9 mm)
Weight	0.005 lb. (11 g)
Operating temperature	-22°F to 140°F (-30°C to 60°C)

Table 0-2. Specifications for GSM Wireless Card (2 of 2)

Specification	GSM Module
Storage temperature	-40°F to 185°F (-40°C to 85°C)
Band of Operating Frequencies	E-GSM 900: Rx 925–960 MHz, Tx 880–915 MHz DCS 1800: Rx 1805–1880 MHz, Tx 1710–1785 MHz GSM 850: Rx 869–894 MHz, Tx 824–849 MHz PCS 1900: Rx 1930–1990 MHz, Tx 1850–1910 MHz

0.1.3.1 Activating the GSM Card in the Carrier Network

Before shipment, the carrier's SIM is placed into the GSM module, and the module is activated for use. However, you must activate the module for use in the carrier's network. Use one of the following procedures, depending on the carrier you have selected.

- *How to Activate the GSM Card for the Cingular/AT&T Wireless Network*
- *How to Activate the GSM Card for the T-Mobile GPRS Network*

How to Activate the GSM Card for the Cingular/AT&T Wireless Network

?? Procedure to be added.

How to Activate the GSM Card for the T-Mobile GPRS Network

?? Procedure to be added.

0.1.3.2 Configuring the GSM Wireless Card

Use the following procedure to configure the GSM wireless connection in your network.

How to Configure the GSM Wireless Port

1 ?? To be added.

0.1.3.3 The GSM Card’s Subscriber Identity Module

The GSM card supports a removable Subscriber Identity Module (SIM, also known as a GSM smartcard), to identify the user to the GSM network.

When you order your wireless BANDIT, you specify which carrier and network you will use. The vendor will install the Subscriber Identity Module that has the selected GSM carrier’s chip.

The BANDIT is not a traveling device, so you will not need SIMs for different countries. However, if you change GSM providers, the GSM card will need a SIM from the new provider. To change the SIM, use the following procedure.

How to Install or Replace the SIM in the BANDIT’s GSM Card

Warning: Follow all precautions against electrostatic discharge (ESD) when removing or installing modules in a BANDIT device. (For example, wear an ESD wrist-strap to protect the unit from ESD.) Allow only qualified service personnel to install and maintain this equipment.

To prevent electrical shock, do not power on the equipment until all cables are connected.

Caution: If you replace the SIM, you must also restart the BANDIT software and reconfigure the expansion port and any tables, paths, or other items using that port.

If you change hardware without reconfiguring the software to reflect the hardware change, the BANDIT may behave unpredictably.

1. Unplug the BANDIT device’s power supply.
2. Disconnect all network connections.
3. If this is a BANDIT Plus chassis with a connecting cable to a Remote Data Unit (RDU), disconnect that cable from the chassis.
4. If necessary, disconnect the grounding wire from the VPN device’s chassis.

5 If this is a BANDIT Plus chassis, loosen the retaining screws holding the chassis to the equipment rack, and remove the chassis from the rack.

6 Place the chassis on a flat, stable surface.

7 Do the following:

a Remove the screws from the bottom of the chassis. (There are four screws on the bottom of a VSR-30, original BANDIT, or BANDIT IP chassis. There are six screws along the periphery of the bottom of a BANDIT Plus chassis.)

b If this is a BANDIT Plus, remove the screws along the periphery of the top of the chassis.

8 Do one of the following:

a Lift the top off the VSR-30, original BANDIT, or BANDIT IP chassis (Figure 0-4).

b Slide the front faceplate and chassis bottom of the BANDIT Plus forward, out of the chassis frame (Figure 0-5).

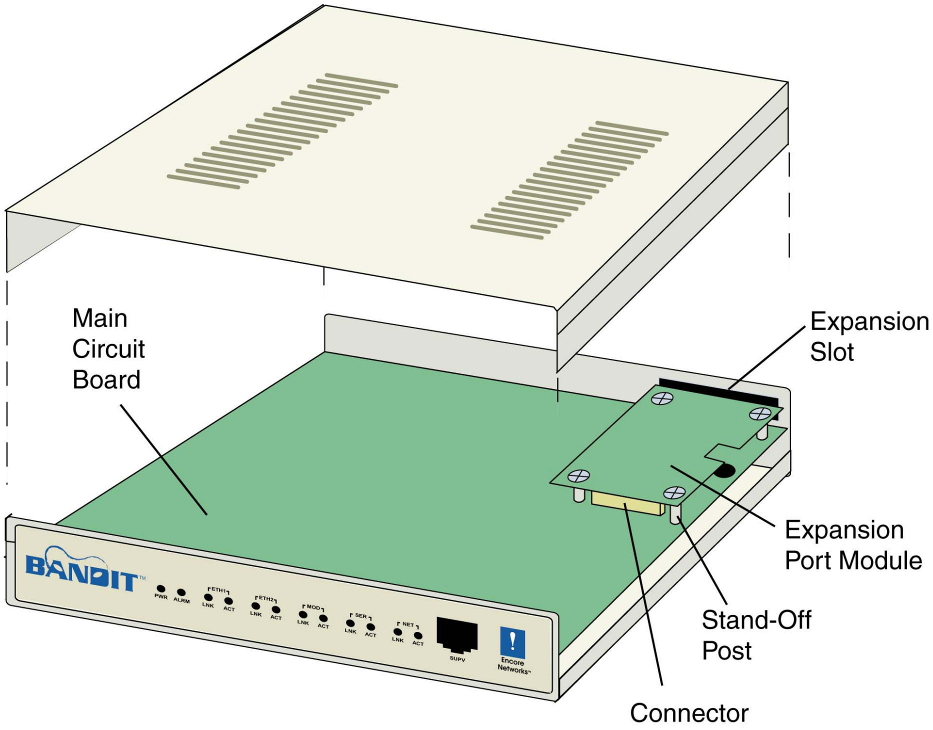

Figure 0-4. Lifting the Top Off the Original BANDIT or Bandit IP Chassis

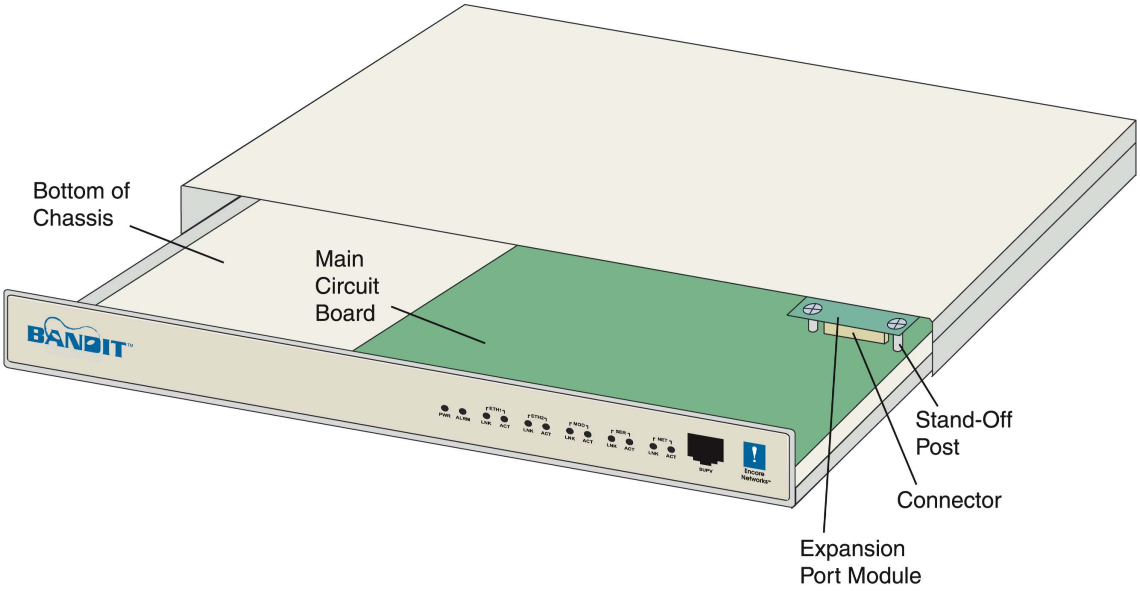

Figure 0-5. Sliding the Front Faceplate and Chassis Bottom of the BANDIT Plus or VSR-1200 Forward

9 Loosen the screws holding the current GSM in place on the main circuit board. Leave the GSM's cables connected to the BANDIT.

10 Lift the GSM and turn it over. The SIM is on the underside of the GSM card.

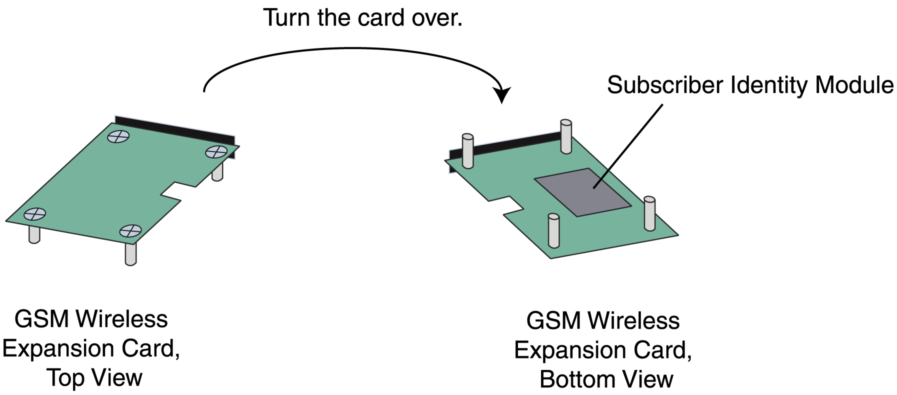
Turn the card over.
Subscriber Identity Module
GSM Wireless Expansion Card, Top View
GSM Wireless Expansion Card, Bottom View

Figure 0-6. SIM Location on GSM Card

11 Remove the old SIM from the GSM card, and install the new SIM on the GSM card.

12 Place the GSM back into the BANDIT device. The module attaches to a connector on the VPN device's main circuit board. Make sure the connector socket on the module aligns properly with the connector on the circuit board.

13 Once the module is seated into the connector, secure the module into place by tightening screws in the stand-off posts on the main circuit board.

14 Do one of the following:

a Place the top back onto the VSR-30, original BANDIT, or BANDIT IP chassis.

b Slide the BANDIT Plus chassis back together.

15 Do the following:

a If this is a BANDIT Plus, tighten the screws on the top of the chassis.

b Tighten the screws on the bottom of the VPN device's chassis.

16 If this is a BANDIT Plus, mount it back into its rack.

17 Reconnect the grounding wire to the VPN device's chassis.

18 If this is a BANDIT Plus that uses an RDU, reconnect its cable to the RDU.

19 Reconnect the VPN device's network connections.

20 Reconnect the device's power supply.

21 Open the BANDIT software and reconfigure the port you replaced. You must also reconfigure any paths, tables, or other items that use the port.

22 After you have reconfigured the port and its dependent items, save (write) the configuration and reset the BANDIT device.