

RadioLAN Marketing Group, Inc.

Application Note

Subject: Encryption Installation User Setup Guide

RadioLAN users may encrypt all the data sent on their RadioLAN wireless networks to enhance the security of the network. RMG's SecureLINK software provides this encryption capability, and is available from your Authorized RMG Reseller.

SecureLINK is based upon RSA Software's public-key/private-key system and is available in 40-bit or 128-bit versions. Your RadioLAN product must be using one of the following minimum software revisions:

	40-bit encryption	128-bit encryption
Adapter Products (101, 130, 140, or 150)	Version 2.0	Version 2.32
Bridge Products (208, 408, 317, 347, or 357)	Version 2.0	Version 3.0

The latest version of the RadioLAN software is available for free for registered RadioLAN users on our website's downloads page.

Now we will look at how to install encryption on the RadioLAN wireless network.

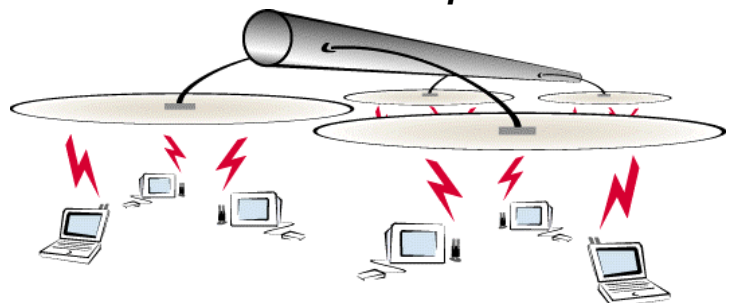
Preparation

Once the basic RadioLAN network is installed and setup, the user has the option to type in a code value to be used to compute a private encryption key. The user must also set encryption to be "on", to participate in the encrypted wireless network. Having encryption ability on a product does not automatically encrypt your data. The default setting is NOT to encrypt.

Like any network, the settings on one computer have impact on others. If you choose to enable encryption on your wireless network, all wireless users must have encryption. Each station must be set for the same code value and must be set to have encryption 'on' before communication can take place between stations. Users of the ISA CardLINK, PCI CardLINK, MobiLINK and BackboneLINK all must have their units enabled with encryption on to be able to communicate.

MobiLINK, ISA CardLINK, and PCI CardLINK Installation and Setup

In order to install the public and private keys, the RadioLAN CardLINK-equipped station must have RadioNET Manager software installed. RMG will have provided an



encryption key diskette with a **Feature Upgrade Key** code value linked to your MAC serial number. This is the private key for your RadioLAN device.

The **Feature Upgrade Keys** are delivered in two formats, a printed report listing the products serial number(s), product type and Software Upgrade Code to use for that product, and a diskette containing a text file for each product being upgraded.

Step 1. Run RadioNET Manager on the computer to be upgraded. Confirm the CardLINK product requires an upgrade by selecting the FEATURES tab in RadioNET Manager. If SecureLINK is already installed, you will see '40-bit encryption' or '128-bit encryption' listed. If there are no items listed, press the UPGRADE button to go to the next step.

Step 2. A window will open for you to enter the **Feature Upgrade Key** value. Use the KEY values on the report, or choose the correct diskette file to "cut and paste" the KEY Value into this field. Once the value is entered, exactly as provided, press the OK key to test the entry.

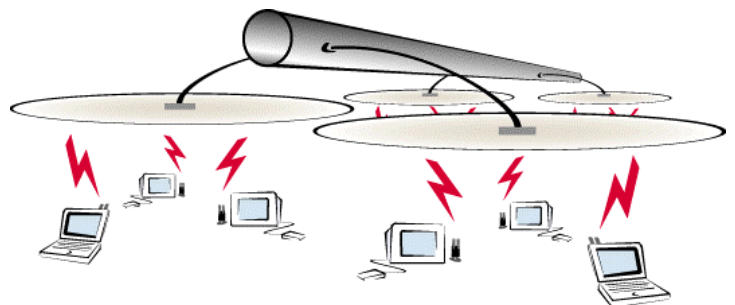
Step 3. The newly entered value is tested to verify it is correct for this specific CardLINK serial number. If successful, the new Encryption Feature is installed and available. If the KEY value is not correct, an error is returned and the Encryption Feature is not installed.

Once installed, you may use the RadioNET Manager to view the current encryption status, enter the encryption key, and turn on or turn off encryption. To view the encryption status; Run RadioNET Manager, and a small padlock is listed on the lower right of the window. If the padlock is RED and says "unlocked", your station is not being encrypted. If the padlock is GREEN and says "locked", the station data is being encrypted.

Step 4. We will now enter the 'public' encryption key. A public key can be any alphanumeric string that all users on the wireless network will share. To enter a public key, run RadioNET Manager and choose CONFIG->Network Parm's. Press Modify to open the Modify Network Parameters screen. Press the Encryption Key button to enter the Encryption Key value, once in the Encryption Key field, and a second time in the Confirm Encryption field. Click, OK. If your entered data match, your public key will be accepted and RadioNET Manager will return you to the previous screen.

To disable encryption, go to the "Modify Network Parameters", de-select the Encryption Enabled checkbox and then press OK. If you enable encryption and find no wireless stations in the node table (INFO button), you have either not enabled encryption on the other stations or the public key value you entered was not the same as entered on the other stations.

After installation of the private key, RadioNET Manager will display a column in the INFO->Station Info screen listing which stations are encrypted and which are not. This allows an administrator to know if a station is sending encrypted data.



BackboneLINK and Campus BridgeLINK Installation and Operation

To install the encryption option you must have management access to the BBL or CBL, and have the encryption key diskette with the **Feature Upgrade Key** code value linked to your MAC serial number. This is the private key for your RadioLAN device.

Step 1. Access the device to be upgraded and verify that the software revision level is adequate for the encryption level you are installing. Confirm the BackboneLINK product requires an upgrade by selecting the System Features on the left menu. If optional features are already installed, they will be listed. If there are no items listed, go to step 2.

Step 2. Type or “cut and paste” the proper KEY Value into the Software Upgrade KEY field. Once the value is entered exactly as provided, press the OK key to test the entry.

Step 3. The newly entered value is tested to verify it matches the serial number of this device. If it does, then the new Encryption Feature is installed and available. If the KEY value is not correct, an error is returned and the Encryption Feature is not installed.

Once installed, you may use the BackboneLINK Manager to view the current encryption status, enter the encryption key, and turn on or turn off encryption. The BackboneLINK Manager or Campus BridgeLINK Manager displays a small padlock on the upper right of the window. If the padlock is RED and shows “unlocked”, your station is not being encrypted. If the padlock is GREEN and shows “locked”, the station data is being encrypted.

Step 4. We will now enter the ‘public’ encryption key. A public key can be any alphanumeric string that all users on the wireless network will share. To enter the public encryption key, go to the BackboneLINK Manager main screen and select System Configuration->Data Encryption. Enter the key value twice, once in the ‘Encryption Key’ field, and a second time in the ‘Retype Encryption key’ field. Then check the ‘Data Encryption: Enabled’ check box, and press OK to change this configuration. If the data match, pressing OK will accept and temporarily save the values. To make this save permanent, go to the Configuration Changes screen, select ‘Save all Changes and Reset’, and press OK.

To disable encryption, go to the System Configuration->Data Encryption, de-select the ‘Enable Data Encryption’ field, and press OK. Then go to the ‘Configuration Changes’ screen, select ‘Save all Changes and Reset’, and press OK.

If you enable encryption and find no wireless stations in the Node Discovery table you have either not yet enabled encryption on the other stations or the KEY value you entered was not the same as entered on the other stations.

