AES Encryption Setup

Serial and TTL Radios

User Manual Addendum

Part Number: LAD0021AB
Revision: A
Last Updated: 10/04/2011

Safety Information

The products described in this manual can fail in a variety of modes due to misuse, age, or malfunction. Systems with these products must be designed to prevent personal injury and property damage during product operation and in the event of product failure.

Warning! DO NOT REMOVE OR INSERT DIAGNOSTICS CABLE WHILE CIRCUIT IS LIVE UNLESS THE AREA IS KNOWN TO BE FREE OF IGNITION CONCENTRATIONS OF FLAMMABLE GASES OR VAPORS.

Warranty

FreeWave Technologies warrants your FreeWave® Wireless Data Transceiver against defects in materials and manufacturing for a period of two years from the date of shipment. In the event of a Product failure due to materials or workmanship, FreeWave will, at its option, repair or replace the Product. The Product must be returned to FreeWave upon receiving a Return Material Authorization (RMA) for evaluation of Warranty Coverage.

In no event will FreeWave Technologies Inc., its suppliers, and its licensors be liable for any damages arising from the use of or inability to use this Product. This includes business interruption, loss of business information, or other loss which may arise from the use of this Product. Please be advised that OEM customer's warranty periods may vary.

Warranty Policy may **not apply**:

1. If Product repair, adjustments or parts replacements is required due to accident, neglect, unusual physical, electrical or electromagnetic stress.
2. If Product is used outside of FreeWave specifications.
3. If Product has been modified, repaired, or altered by Customer unless FreeWave specifically authorized such alterations in each instance in writing. This includes the addition of conformal coating.

Special Rate Replacement Option

A special rate replacement option is offered to non-warranty returns or upgrades. The option to purchase the replacement unit at this special rate is only valid for that RMA. The special replacement rate option expires if not exercised within 30 days of final disposition of RMA.

Restricted Rights

Any product names mentioned in this manual may be trademarks or registered trademarks of their respective companies and are hereby acknowledged. Information in this manual is subject to change without notice and is proprietary and confidential to FreeWave Technologies, Inc.

This manual is for use by purchasers and other authorized users of the FreeWave® Wireless Data Transceiver only.

No part of this manual may be reproduced or transmitted in any form or by any means, electronic or mechanical, or for any purpose without the express written permission of FreeWave Technologies, Inc.

FreeWave's Spread Spectrum Wireless Data Transceivers are designed and manufactured in the United States of America.

FreeWave Technologies Inc.
1800 South Flatiron Court
Boulder, CO 80301
Phone: 303.444.3862
Toll Free: 1.866.923.6168
Fax: 303.786.9948
www.freewave.com

Printed in the United States of America.

Document Revision History

Date	Rev Letter	Updates Made
10/4/2011	A	• Updated format to meet new FreeWave document standards. • Added hexadecimal information in the "Setting the Encryption Key" section. • Converted content to procedures.

About this Document

This document describes how to enable AES Encryption in FreeWave serial and TTL radios. Use this document in conjunction with the user manual for your specific radio to setup AES Encryption. If you are using MM2 series radios, or the TDMA protocol with your radio, see the following documents for information about AES Encryption on those devices:

- *AES Encryption & MM2 Wireless Modules*
- *Encryption Key Loading Using TDMA*

Prior to using this document, you should be familiar with programming radio parameter settings.

Contacting FreeWave Technical Support

For up-to-date troubleshooting information, check the Support page at www.freewave.com.

FreeWave provides technical support Monday through Friday, 7:30 AM to 5:30 PM Mountain Time (GMT -7). Call toll-free at 1.800.548.5616, factory direct after hours at 303.381.9200, or contact us through email at moreinfo@freewave.com.

Documentation Feedback

Your feedback is important to us! FreeWave Technologies, Inc. is committed to continually improving the quality of our documentation. If you have any comments or suggestions about this document, send them to us at techpubs@freewave.com. Please include the name of the manual or the manual's part number in your email.

AES Encryption Overiew

Protecting the confidentiality, integrity, and authenticity of your data communication is essential to maintaining a robust, reliable, and secure wireless infrastructure. FreeWave has incorporated a number of mechanisms to achieve these critical security objectives, including the use of AES Encryption. When available and enabled, AES Encryption adds a layer of 128-bit, 192-bit, or 256-bit encryption strength to the data before it is sent out via RF.

To set AES Encryption in a serial or TTL radio, you need to select the encryption strength and provide an encryption key.

Setting AES Encryption Strength

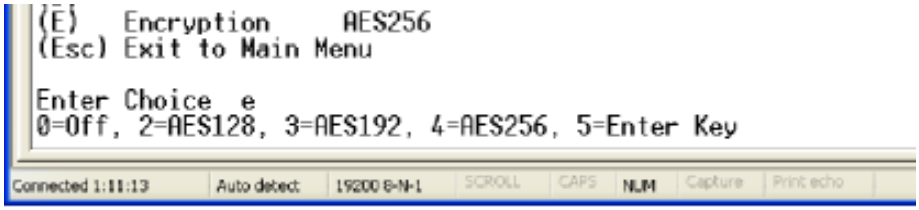
AES Encryption is available in various strengths. Your network, and the data you are sending determines the encryption strength you should use. The higher the encryption strength, the stronger the encryption; however, it can also take longer for the encryption and de-encryption to take place.

> **Important:** Every radio in the network must have matching encryption strengths and encryption keys for successful communication.

The encryption option is located within the Edit Radio Transmission Characteristics menu in the radio's Setup menu.

Note: Encryption settings are only available through HyperTerminal or Setup Terminal in Tool Suite. The encryption options are not available in the Tool Suite Transmission Characteristics tab.

1. Connect to the radio in Setup Mode and display the Setup Main menu in HyperTerminal or in Setup Terminal in Tool Suite.
2. From the Setup Main menu, select **(3) Edit Radio Transmission Characteristics**.
3. From the Radio Parameters menu, select **(E) Encryption** to display the encryption options.



4. Enter the number corresponding to the encryption strength you want to use:

Encryption Option	Description
0 = Off	Turns off AES encryption
2 = AES128	Enables AES encryption, 128-bit strength
3 = AES192	Enables AES encryption, 192-bit strength
4= AES256	Enables AES encryption, 256-bit strength

5. Select menu option **5** to enter the encryption key. For more information, see the next section.
6. Press **Esc** to return to the Radio Parameters menu, and press **Esc** again to return to the Setup Main menu.

Setting the AES Encryption Key

The encryption key is the piece of information used to encrypt and de-encrypt the data sent through your network. Even with encryption, your data is only as secure as the strength of the encryption key you use.

Keys should be random in nature and entered as hexadecimal values (0-F in two-character pairs). You can use any combination of characters for your password. For example, a combination of numbers that you know, or a sentence or phrase converted into hexadecimal format. Various string-to-hexadecimal converters are available on the Web or refer to the hexadecimal conversion chart on page 4.

Important: Every radio in the network must have matching encryption strengths and encryption keys for successful communication.

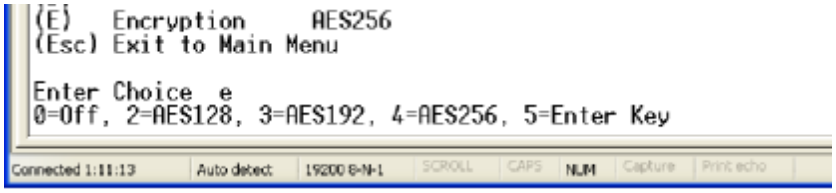
The encryption key option is located within the Edit Radio Transmission Characteristics menu in the radio's Setup menu.

Note: Encryption settings are only available through HyperTerminal or Setup Terminal in Tool Suite. The encryption options are not available in the Tool Suite Transmission Characteristics tab.

1. Connect to the radio in Setup Mode and display the Setup Main Menu in HyperTerminal or in Setup Terminal in Tool Suite.

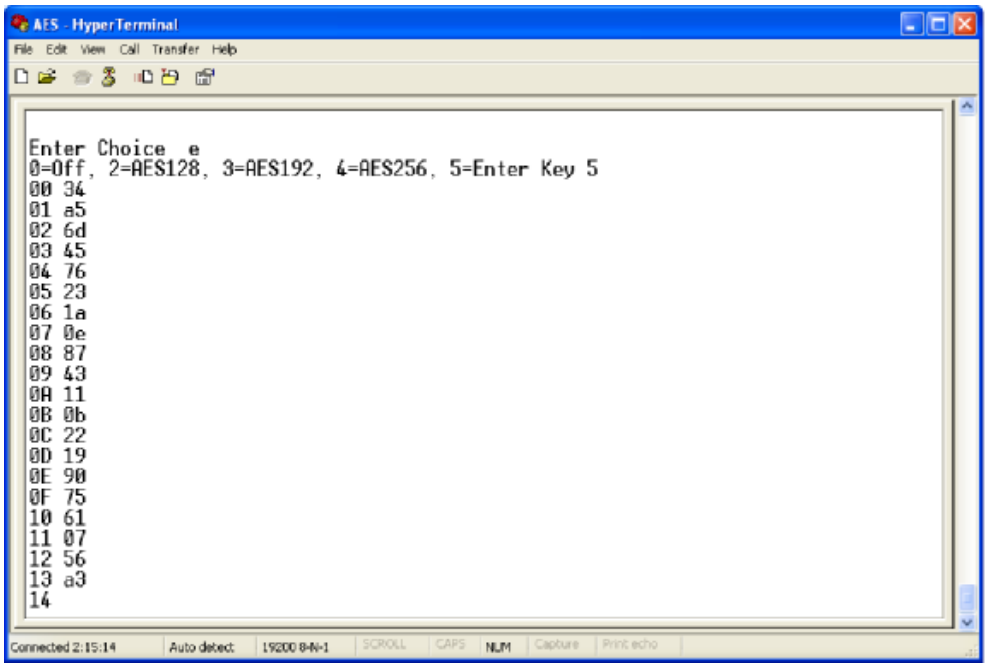
   Note: Encryption settings are only available through HyperTerminal or Setup Terminal in Tool Suite. The encryption options are not available in the Tool Suite Transmission Characteristics tab.

2. From the Setup Main menu, select **(3) Edit Radio Transmission Characteristics**.
3. From the Radio Parameters menu, select **(E) Encryption** to display the encryption options.



   The current encryption level displays next to the (E) Encryption menu option.

4. From the displayed options, select **5** to enter the encryption key.
5. Enter the encryption key in 2-character hexadecimal combinations in the lines provided.



   The **Enter Key** option always asks for all 32 lines of the encryption key. However, the encryption strength you select determines how many of the lines are required:

   - 128-bit encryption - Enter key information in rows 00 to 0F. The last 16 lines (10 to 1F) are ignored.

- 192-bit encryption - Enter key information in rows 00 to 17. The last 8 entries (18 to 1F) are ignored.
- 256-bit encryption - Enter key information in rows 00 to 1F. All lines are used.

6. Press **Esc** until you return to the Setup Main menu.

Hexadecimal Conversion Chart

Encryption keys should be random in nature and entered as hexadecimal values (0-F in two-character pairs). You can use any combination of characters for your password. For example, a combination of numbers that you know, or a sentence or phrase converted into hexadecimal format.

Various string-to-hexadecimal converters are available on the Web. A string-to-hexadecimal converter is a way to convert a phrase you are likely to remember. You can also use the table below to convert text to a hexadecimal string. For example, "Hi" converts to 4869 in hexadecimal.

Text	Encoded String	Text	Encoded String	Text	Encoded String
A	41	V	56	q	71
B	42	W	57	r	72
C	43	X	58	s	73
D	44	Y	59	t	74
E	45	Z	5a	u	75
F	46	a	61	v	76
G	47	b	62	w	77
H	48	c	63	x	78
I	49	d	64	y	79
J	4a	e	65	z	7a
K	4b	f	66	0	30
L	4c	g	67	1	31
M	4d	h	68	2	32
N	4e	i	69	3	33
O	4f	j	6a	4	34
P	50	k	6b	5	35
Q	51	l	6c	6	36
R	52	m	6d	7	37
S	53	n	6e	8	38
T	54	o	6f	9	39
U	55	p	70		


FreeWave®