FIPS Mode Support

WB45NBT and WB50NBT

Application Note *v1.0*

INTRODUCTION

The goal of this document includes the following:

- Explain how to enable FIPS Mode on the Laird WB45NBT and WB50NBT.
- Offer practical notes regarding FIPS mode support.

OVERVIEW

FIPS (Federal Information Processing Standard) is a National Institute of Standards and Technology (NIST) standard for data used in computer systems. Of the most interest to Wi-Fi systems is FIPS 140-2 which defines security requirements for cryptographic modules, or modules that provide security services such as encryption to provide data.

FIPS support is provided for the wireless interface by **openssl_fips-2.0** with the SDC supplicant and additional kernel and user space components.

The Laird WB45NBT and WB50NBT use an embedded FIPS 140-2-validated cryptographic module (openssl_fips-2.0) for cryptographic operations involving the wireless interface, specifically the supplicant for wireless authentication, and the driver for AES link encryption.

When running in FIPS mode, the WB45NBT/WB50NBT radios only use AES-CCMP-128 encryption. In FIPS mode, the supplicant restricts operation to WPA2-AES with EAP-TLS, and WPA2-PSK/AES.

If no encryption key has been established (such as during authentication), 802.1x/eapol authentication packets are transmitted and received unencrypted; all other transmit and receive data packets are discarded.

METHOD OF ENABLING FIPS MODE

To enable FIPS mode of operation for the wireless interface, follow these steps:

1. A FIPS compatible configuration profile must be used – either WPA2-AES/EAP-TLS, or WPA2-PSK/AES.
2. FIPS mode must be enabled and the wireless interface restarted:

```
# sdc_cli global set fips enable
Wireless restart required to activate fips mode
# wireless restart
```

Note: A reboot also restarts the wireless interface in the new mode.

Americas: +1-800-492-2320
Europe: +44-1628-858-940
Hong Kong: +852 2923 0610

To disable FIPS mode of operation for the wireless interface, follow these steps:

1. FIPS mode must be disabled, and the wireless interface restarted:

```
# sdc_cli global set fips disable
Wireless restart required to deactivate fips mode
# wireless restart
```

Note: A reboot restarts the wireless interface in the new mode.

To see the current mode of operation for the wireless interface, enter the following:

```
# sdc_cli global show fips
```

Four different states are possible:

- FIPS Mode: Disabled and Inactive
- FIPS Mode: Inactive – Enabled on next start
- FIPS Mode: Enabled and Active
- FIPS Mode: Active – Disabled on next start

If the status indicates *Disabled/Enabled on next start*, then the FIPS configuration was changed without issuing the wireless restart.

SOME PRACTICAL NOTES

The following are some practical notes regarding FIPS mode support:

- FIPS mode only works with WPA2-AES EAP-TLS, and WPA2-PSK/AES.
- Certificates must use a signature algorithm that is allowed in FIPS mode:
  - Signature Algorithm: md5WithRSAEncryption – fails – md5 is not allowed
  - Signature Algorithm: sha1WithRSAEncryption – successful
- PKCS#12 certificate files must use encoding methods allowed in FIPS mode (for openssl override the certpbe encoding – for example using *-certpbe PBE-SHA1-3DES*)
- If you attempt to use a configuration other than WPA2-AES/EAP-TLS and WPA2-PSK/AES and debug output is enabled, the following error messages are output:
  - *CFG: Disabled. Invalid WPA type for FIPS*
  - *CFG: Disabled. Invalid EAP type for FIPS*
- The private key can be encrypted or unencrypted. If the private key is encrypted, it must be of PKCS#8 format. If the private key starts with the following it is the old format (which uses MDS) and is not FIPS-compliant You may use OpenSSL to fix the certificate in these cases by converting it to PKCS12 and then back to PEM as follows:

```
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: DES-EDE3-CBC,2FA91DAE900C159E
```

- OpenSSL can be used to fix the certificate by converting to PKCS12 and then back to PEM using a script as follows:

```
openssl pkcs12 -export -out $1.p12 -inkey $1 -in $1 -passin pass:$2 -passout
pass:$2
```


Americas: +1-800-492-2320
Europe: +44-1628-858-940
Hong Kong: +852 2923 0610

```
openssl pkcs12 -in $1.p12 -out $1.new -passin pass:$2 -passout pass:$2
```

- Use the following to see if the drivers are in FIPS mode:

```
cat /sys/module/ath6kl_core/parameters/fips_mode
```

- Driver statistics are available in FIPS mode:

  egrep '[0-9]' /sys/module/ath6kl_laird/parameters/fips_stat*

- The supplicant is in FIPS mode if it has been executed with -F.
  To look for **-F** in the supplicant startup, run the following command:

```
ps | egrep sdcsupp
```

- If the FIPS module fails self-test (KAT/integrity failure), then the supplicant outputs an error message and exits.

Notes Regarding OpenSSL:

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (http://www.openssl.org/)

This product includes cryptographic software written by Eric Young. (eay@cryptsoft.com)

This product includes software written by Tim Hudson. (tjh@cryptsoft.com)

REVISION HISTORY

Version	Date	Notes	Approver
1.0	21 April 2016	Initial Release with WB50NBT added	Doug Smith