Configuring and Validating Key Controller (Wireless Security)

• Configuring and Validating Key Controller (Wireless Security), on page 1

Configuring and Validating Key Controller (Wireless Security)

To support wireless security to standard WPA protocols, a key rotation strategy has been implemented on IW9167E.

The key controller protocol can be described as a packet exchange between two devices, in which different stages of the process correspond to different states of each device, and the algorithm flow is controlled by a set of timers scheduled periodically to generate new PTK/GTK (Pairwise Transient Key/Group Transient Key) for packet encryption. The more often keys are updated, the less information is leaked in case of attack.

Configuring Key Controller from CLI

To configure a key controller, use the following CLI commands.

1. To enable AES (Advanced Encryption Standard) on radio use the following CLI command.

   ```
   Device# configure dot11Radio <interface> crypto aes enable
   ```

2. To enable key controller use the following CLI command.

   ```
   Device #configure dot11Radio <interface> crypto key-control enable
   ```

3. To enable key rotation use the following CLI command.

   ```
   Device# configure dot11Radio <interface> crypto key-control key-rotation enable
   ```

4. To set key rotation timer use the following CLI command.

   ```
   Device# configure dot11Radio <interface> crypto key-control key-rotation 3600
   ```

Note AES disabled by default. Config should be the same on all devices.

Validating Key Controller from CLI

To validate a key controller, use the following show commands.

show key controller config:

```
Device# show dot11Radio X crypto
AES encryption: enabled
AES key-control: enabled
Key rotation: enabled
Key rotation timeout: 3600(second)
```