

## **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 Wi-Fi Protected Access (WPA) protocols, a key rotation strategy is implemented for Catalyst IW9167E. The key controller protocol is a packet exchange between two devices, in which different stages of the process correspond to different states of each device. The algorithm flow is controlled by a set of timers scheduled periodically to generate new Pairwise Transient Key/Group Transient Key for packet encryption. The more frequently keys are updated, the lesser amount of information is leaked in the event of an attack.

## **Configuring Key Controller from CLI**

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

1. To enable Advanced Encryption Standard (AES) 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

By default, AES mode is disabled. Configuration should be same on all devices.

## Validating Key Controller from CLI

To validate a key controller, use the following show command:

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