Configuring IP-MAC Address Binding

Information About Configuring IP-MAC Address Binding

In the controller software Release 5.2 or later releases, the controller enforces strict IP address-to-MAC address binding in client packets. The controller checks the IP address and MAC address in a packet, compares them to the addresses that are registered with the controller, and forwards the packet only if they both match. In previous releases, the controller checks only the MAC address of the client and ignores the IP address.

You must disable IP-MAC address binding to use an access point in sniffer mode if the access point is associated with a 5500 series controller, a 2500 series controller, or a controller network module. To disable IP-MAC address binding, enter the **config network ip-mac-binding disable**.

WLAN must be enabled to use an access point in sniffer mode if the access point is associated with a 5500 series controller, a 2500 series controller, or a controller network module. If WLAN is disabled, the access point cannot send packets.

Note   If the IP address or MAC address of the packet has been spoofed, the check does not pass, and the controller discards the packet. Spoofed packets can pass through the controller only if both the IP and MAC addresses are spoofed together and changed to that of another valid client on the same controller.

Configuring IP-MAC Address Binding (CLI)

Step 1   Enable or disable IP-MAC address binding by entering this command:
config network ip-mac-binding {**enable** | **disable**}

The default value is enabled.

Note   You might want to disable this binding check if you have a routed network behind a workgroup bridge (WGB).

Note You must disable this binding check in order to use an access point in sniffer mode if the access point is joined to a Cisco 5500 Series Controller.

Step 2 Save your changes by entering this command:
save config

Step 3 View the status of IP-MAC address binding by entering this command:
show network summary

Information similar to the following appears:

```
RF-Network Name............................. ctrl4404
Web Mode.................................... Disable
Secure Web Mode............................. Enable
Secure Web Mode Cipher-Option High.......... Disable
Secure Web Mode Cipher-Option SSLv2......... Disable
...
```
IP/MAC Addr Binding Check .... Enabled
```
...<?Line-Break?><?HardReturn?>
```