Disabling Device Tracking to Support NAC Devices

Feature History for Disabling Device Tracking to Support NAC Devices

This table provides release and related information for the feature explained in this module.

Table 1: Feature History for Disabling Device-Tracking to Support NAC Devices

Release	Feature	Feature Information
Cisco IOS XE Cupertino 17.8.1	Disabling Device Tracking to Support NAC Devices	This feature helps to control the flow of traffic between wireless clients using network access control (NAC) device.

Information About Disabling Device Tracking to Support NAC Devices

The feature helps to control the flow of traffic between wireless clients using a network access control (NAC) device. The NAC device blocks the direct traffic between wireless clients using ARP spoofing.

Use the **no ip mac-binding** command for ARP spoofing from the NAC and disabling the wireless client device tracking.

Note This feature is applicable only for IPv4 addresses.

Restrictions for Disabling Device Tracking to Support NAC Devices

- The **wireless client ip deauthenticate** command works by referring to the IP table binding entries directly. It does not work for client whose IPs are not learnt.
- Layer 3 web authentication and other L3 policies are not supported.
- When IP Source Guard (IPSG) is enabled and multiple binding information is sent with the same address and preference level (such as DHCP, ARP, and so on) to Cisco Packet Processor (CPP), the CPP starts to ignore the later bindings after the first binding creation. Hence, you should not configure IPSG and **no ip mac-binding** together. If IPSG and **no ip mac-binding** are configured together then IPSG does not work.

Disabling Device Tracking for Wireless Clients (CLI)

Disable device tracking for wireless clients using commands.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless profile policy** *profile-policy-name* **Example:** `Device(config)# wireless profile policy test-profile-policy`	Configures the wireless profile policy.
Step 3	**shutdown** **Example:** `Device(config-wireless-policy)# shutdown`	Disables the wireless policy profile. **Note** Disabling policy profile results in associated AP and client to rejoin.
Step 4	**no ip mac-binding** **Example:** `Device(config-wireless-policy)# no ip mac-binding`	Disables the IP-MAC address binding.

	Command or Action	Purpose
Step 5	**no shutdown** **Example:** `Device(config-wireless-policy)# no shutdown`	Enables the wireless policy profile.
Step 6	**exit** **Example:** `Device(config-wireless-policy)# exit`	Returns to privileged EXEC mode.
Step 7	**vlan configuration** *vlan-id* **Example:** `Device(config)# vlan configuration 20`	Configures a VLAN and enters VLAN configuration mode.
Step 8	**arp broadcast** **Example:** `Device(config-vlan-config)# arp broadcast`	Enables ARP broadcast on VLAN.
Step 9	**end** **Example:** `Device(config-vlan-config)# end`	Returns to privileged EXEC mode.

Verifying ARP Broadcast

To verify the ARP broadcast, use the following command:

```
Device# show platform software arp broadcast
Arp broadcast is enabled on vlans:
20,50
```