Disabling IP Learning in Local Mode

- Information About Disabling IP Learning in Local Mode, on page 1
- Restrictions for Disabling IP Learning in Local Mode, on page 1
- Disabling IP Learning in Local Mode (CLI), on page 2
- Verifying MAC Entries from Database , on page 3
- Verifying ARP Broadcast, on page 3

Information About Disabling IP Learning in Local Mode

In Local mode central switching scenarios, multiple clients may have an allocated or registered IP address. If the controller detects more than one client attempting to use the same IP address, it will discard one of the clients as an IP Theft event, potentially resulting in client exclusion.

The Disabling IP learning in Local mode feature utilizes the **no ip mac-binding** command to ensure that device tracking is not done for clients, thus preventing the IP Theft error.

To allow downstream broadcast ARP traffic to reach the wireless client in the VLAN, you should enable ARP broadcast and disable IP MAC binding. The controller replicates this traffic packet to all the APs belonging to the controller when Multicast over Multicast (MOM) is disabled.

To avoid this replication, you will need to enable the MOM.

Note This feature is applicable only for IPv4 addresses.

Restrictions for Disabling IP Learning in Local Mode

- 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.
- The L3 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 IP and preference level (such as DHCP, ARP, and so on) to CPP, the CPP starts to ignore the later bindings after the first binding creation. Hence, you should not configure IPSG and disable IP MAC binding together. If IPSG and **no ip mac-binding** are configured together then IPSG does not work.

Disabling IP Learning in Local Mode (CLI)

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 IP learning in Local mode.
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-config)# vlan configuration 20`	Configures a VLAN and enters VLAN configuration mode. **Note** To allow downstream broadcast ARP traffic to reach the wireless client in the VLAN, you should enable ARP broadcast and disable IP MAC binding.
Step 8	**arp broadcast** **Example:** `Device(config-vlan-config)# arp broadcast`	Enables ARP broadcast on VLAN.

	Command or Action	Purpose

Step 9	**end**
	Example:
	`Device(config-vlan-config)# end`
		Returns to privileged EXEC mode.

Verifying MAC Entries from Database

To verify the MAC details from database, use the following command:

```
Device# show wireless device-tracking database mac
  MAC             VLAN  IF-HDL      IP

------------------------------------------------------------------------------------------

  6c96.cff2.889a  64    0x90000008  9.9.64.175
```

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
```