Disabling IP Learning in Local Mode

Disabling IP learning in local mode

A disabling IP learning in local mode feature is a WLAN security mechanism that

- uses the **no ip mac-binding** command to prevent device tracking for clients
- prevents IP Theft errors by ensuring that multiple clients do not register the same IP address, and
- allows downstream broadcast ARP traffic to reach wireless clients in the VLAN when ARP broadcast is enabled and IP MAC binding is disabled.

IP learning prevention in local mode scenarios

Describes how the controller handles IP address conflicts and ARP broadcast traffic in local mode.

Key points about IP learning prevention:

- In local mode central switching, multiple clients may have an allocated or registered IP address.
- If the controller detects more than one client using the same IP address, it discards one client as an IP Theft event, which may result in client exclusion.
- To allow downstream broadcast ARP traffic to reach wireless clients in the VLAN, enable ARP broadcast and disable IP MAC binding.
- The controller replicates broadcast ARP packets to all APs belonging to the controller when Multicast over Multicast (MOM) is disabled.
- To avoid replication, enable MOM.

Note This feature is applicable only for IPv4 addresses.

Restrictions for disabling IP learning in local mode

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 clients 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.

Disable IP learning in local mode (CLI)

Configure the wireless policy profile to disable IP learning in local mode, ensuring proper client IP address handling and ARP broadcast support.

This task is performed when you need to prevent IP address learning for wireless clients in local mode, typically to support downstream ARP broadcast traffic and avoid MAC binding issues.

Procedure

Step 1 Enter global configuration mode.

Example:

```
Device# configure terminal
```

Step 2 Configure the wireless profile policy.

Example:

```
Device(config)# wireless profile policy profile-policy-name
```

Step 3 Disable the wireless policy profile.

Example:

```
Device(config-wireless-policy)# shutdown
```

Disabling the policy profile results in associated AP and client rejoining.

Step 4 Disable IP learning in local mode.

Example:

```
Device(config-wireless-policy)# no ip mac-binding
```

Step 5 Enable the wireless policy profile.

Example:

```
Device(config-wireless-policy)# no shutdown
```

Step 6 Exit wireless policy configuration mode.

Example:

```
Device(config-wireless-policy)# exit
```

Step 7 Configure a VLAN and enter VLAN configuration mode.

Example:

```
Device(config-vlan-config)# vlan configuration vlan-id
```

To allow downstream broadcast ARP traffic to reach the wireless client in the VLAN, enable ARP broadcast and disable IP MAC binding.

Step 8 Enable ARP broadcast on the VLAN.

Example:

```
Device(config-vlan-config)# arp broadcast
```

Step 9 Return to privileged EXEC mode.

Example:

```
Device(config-vlan-config)# end
```

IP learning is disabled in local mode, allowing ARP broadcast traffic to reach wireless clients and preventing MAC binding issues.

Verify MAC entries database

Use the **show wireless device-tracking database mac** command to verify MAC address details stored in the device 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
```

ARP broadcast verification

To verify the ARP broadcast, use the following command.

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