ARP Responses for Default Gateway IP Address Point to Wireless Clients

Contents

[Summary](#)

[Conditions](#)

[Root Cause](#)

[Workaround](#)

[Fix](#)

Summary

Customers reported, in 2019, that, intermittently in a given subnetwork, Address Resolution Protocol (ARP) responses for the default gateway's IP address point to some specific wireless clients rather than to the router. This could lead to either client or network-wide connectivity problems for other devices on the same VLAN/subnetwork.

Conditions

- The incorrect ARP responses point to MAC addresses that belong to Apple macOS devices which are running 10.14 or earlier
- Devices running 2019-vintage Android are associated to the same subnetwork
- The access points to which the macOS devices are associated are AP-COS (1800/2800/3800/4800/1540/1560/9100 series), in FlexConnect Local Switching, or SDA, mode, not Cisco IOS® APs.
- The access points have FlexConnect Proxy ARP (ARP caching) enabled
    - By default, FlexConnect ARP caching is enabled in AP-COS 8.3 and above
    - 8.2 is not susceptible, because it did not support AP-COS FlexConnect ARP caching
- This problem can affect deployments with AireOS or 9800 series Wireless LAN Controllers, or with Mobility Express

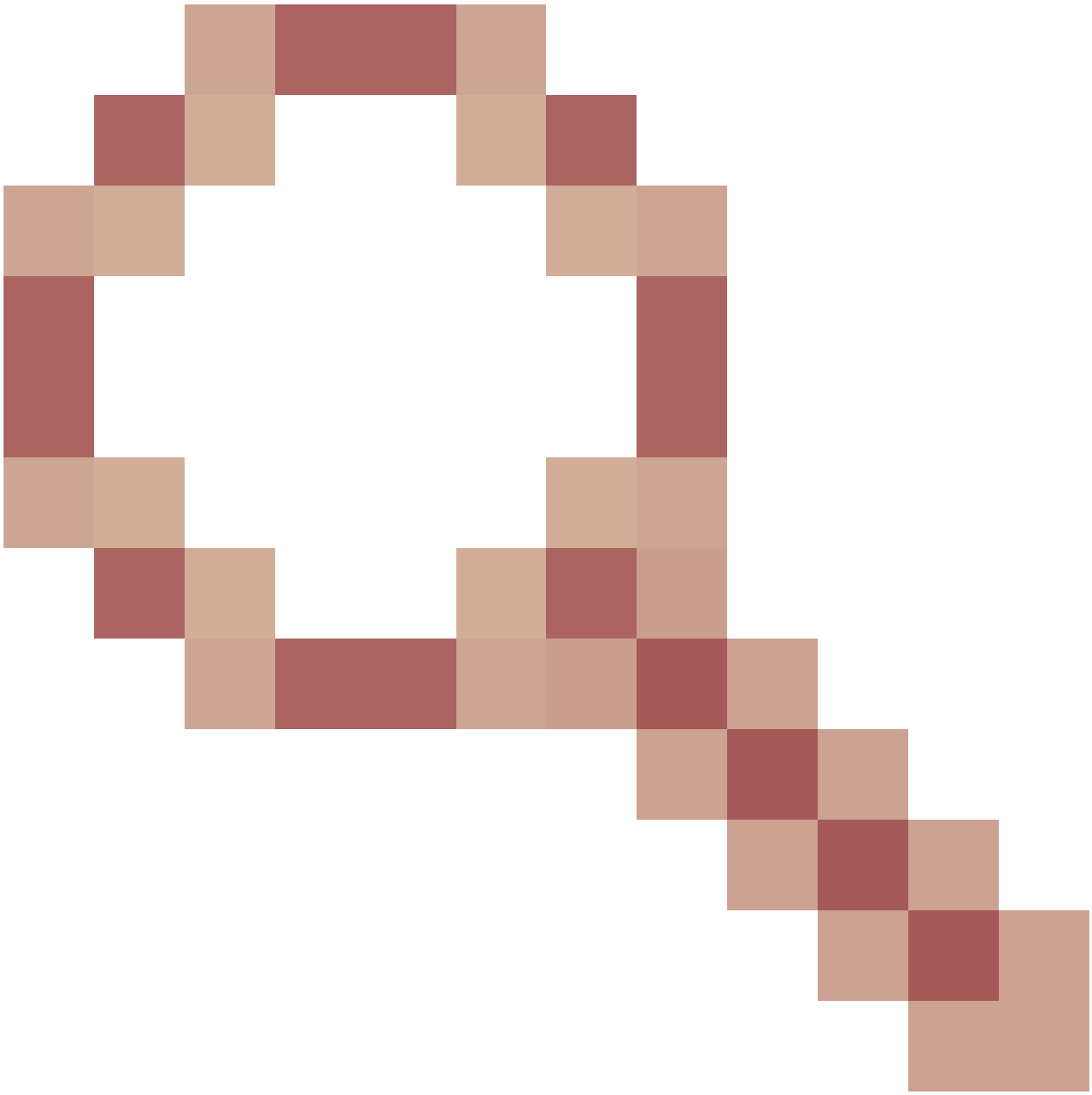
Root Cause

- This is not a malicious attack, but triggered by an interaction between the macOS device while in sleeping mode, and specific broadcast traffic generated by Android devices.
    - The macOS behavior is fixed in 10.15 and above
- AP-COS APs, while in FlexConnect or SDA mode, provide Proxy ARP (ARP caching) services by default. Due to their address learning design, they will modify table entries based on this traffic leading to default gateway ARP entry modification.

Workaround

Disable FlexConnect Proxy ARP (ARP caching).

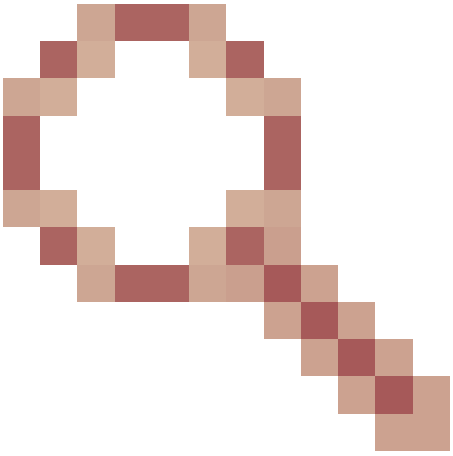
- If running FlexConnect with AireOS or Mobility Express, use the command **config flexconnect arp-caching disable**
    - this command works with 8.10, 8.9, 8.8, 8.5.151.0, and 8.5 escalation (8.5.140.13 or above)
    - if using earlier 8.5 code, this command does not work (CSCvp73371



), so upgrade to 8.5.151.0 or above

- if using 8.3 code, upgrade to 8.3MR5 escalation (8.3.150.3 or above, available from TAC) to get the CSCvp73371 fix

- if using SDA Fabric mode with AireOS, use the command **config flexconnect arp-caching disable**
  - this command works with 8.10, 8.9.111.0, 8.8.125.0 and 8.5.151.0

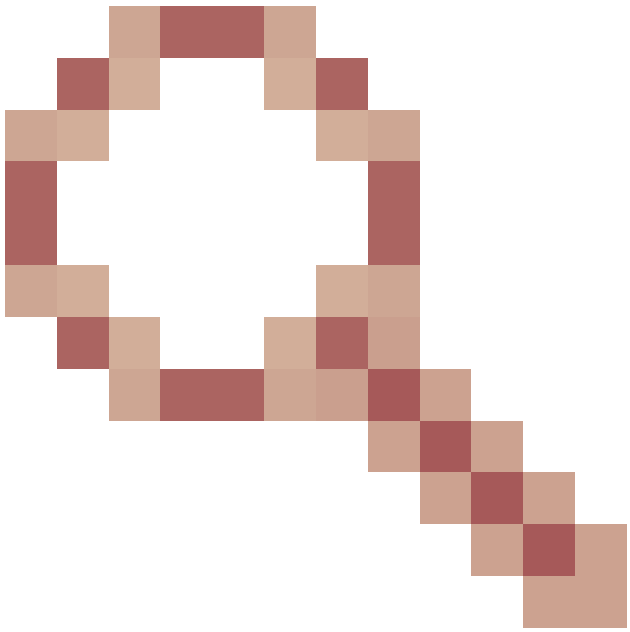


  - if using earlier 8.5 or 8.8 code, this command does not work (CSCvk79850), so upgrade to 8.5.151.0 / 8.8.125.0 / 8.10 or above

- If running FlexConnect with a 9800 series controller, use the command **no arp-caching** under **wireless profile flex**

By disabling FlexConnect Proxy ARP, ARP requests for wireless clients will be broadcast over the air, rather than answered by the APs. This will increase battery consumption somewhat for wireless handheld devices such as Cisco 8821 phones.

Fix



If running FlexConnect with AireOS 8.10.120.0 or above (CSCvp42721
), or IOS-XE 17.2.1 or above, and if no clients need to use static addressing, then:

- make sure that, at each location, all APs are in the same non-default FlexConnect group
- configure DHCP Required on the WLAN
- use the command **config flexconnect arp-caching enable** (AireOS)/**arp-caching** (IOS-XE)

This will prevent clients from using IP addresses other than the ones assigned by DHCP.