Technical Note

Using RLX2-IHx Bridging Client on Cisco Wireless Infrastructure

Document Code: Using RLX2-IHx Bridging Client on Cisco Wireless Infrastructure_EL_01082019
Date: January 8, 2019
Revision: 1.0

Introduction

RLX2-IHx Bridging Client provides a way for non-wireless devices to connect to 3rd party wireless infrastructure when these devices are connected to its Ethernet port. However, customers that use RLX2-IHx Bridging Client on a Cisco wireless infrastructure may experience intermittent connectivity issues with Ethernet devices that are connected to the Bridging Client. The problem happens when the Bridging Client is connected to a Cisco access point that is configured to ***Local*** AP Mode (Figure 1). In this technical note, we will describe the problem and the solution.

Problem

When a Cisco access point is operating in Local AP Mode (a.k.a. centrally switched), all clients' traffic is processed by the Cisco wireless controller. In this mode, after a Bridging Client is connected to a Cisco access point, the Cisco wireless controller will learn the IP address of the Bridging Client by analyzing packets (e.g., ARP request, DHCP request, etc.) sent from the Bridging Client. Once an IP address of the Bridging Client is learned (it can be the IP address of one of the devices behind the Bridging Client or the Bridging Client itself), the Cisco wireless controller will bind the IP address to the MAC address of the Bridging Client (Figure 2). By default, Cisco wireless controllers act as proxy for all ARP requests, i.e., upon receiving an ARP request, the wireless controller responds with an ARP response instead of passing the request directly to the client. However, the controller will only respond if the target IP address of the ARP request is known, otherwise, the ARP request will be dropped. This means that ARP resolution from the

How to Contact Us

Asia Pacific
Regional Office
+60.3.7941.2888
support.ap@prosoft-technology.com

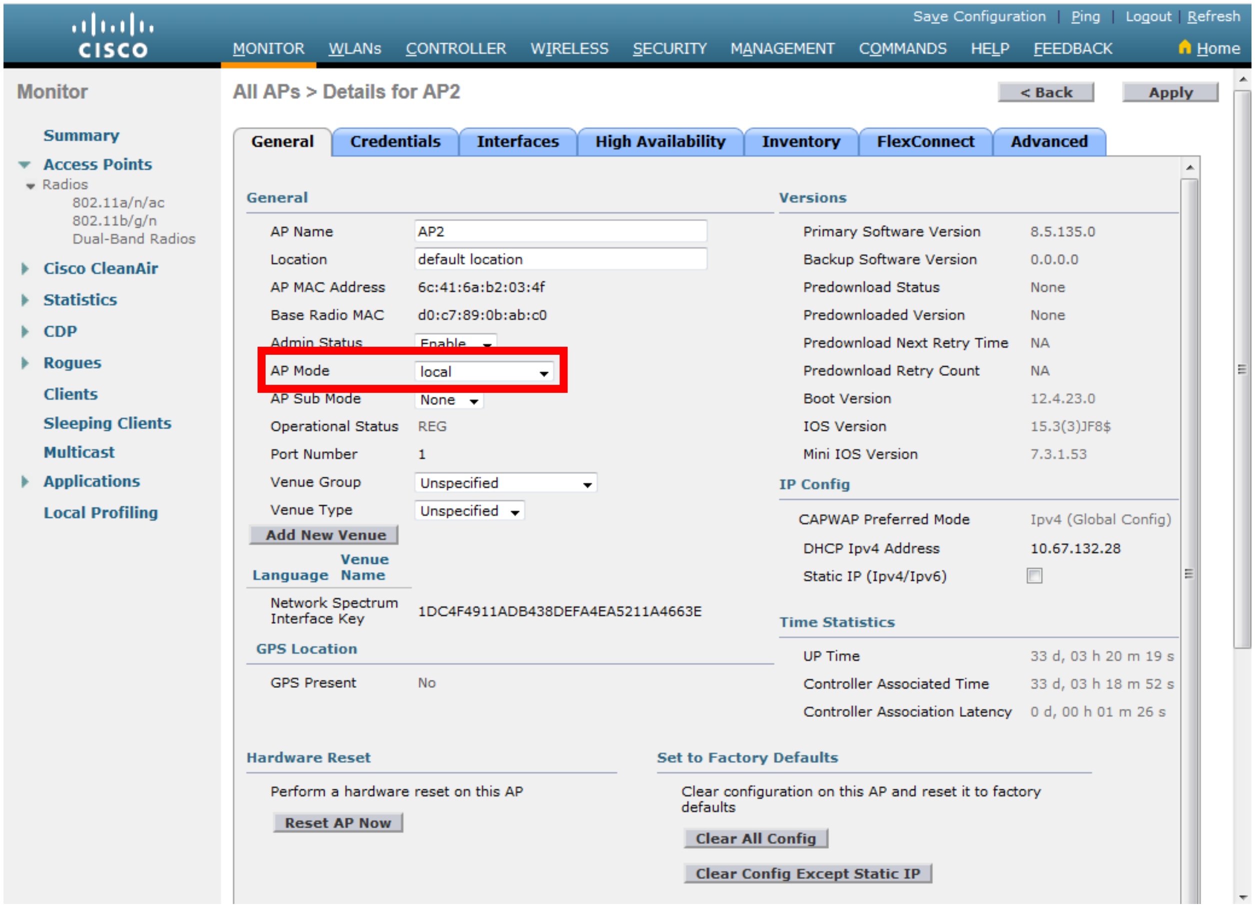
North Asia
(China, Hong Kong)
+86.21.5187.7337
support.ap@prosoft-technology.com

Europe/Middle East/Africa
Regional Office
+33.(0)5.34.36.87.20
support.emea@prosoft-technology.com

Latin America
Regional Office
+52.222.264.1814
support.la@prosoft-technology.com

North America
Corporate Office
+1.661.716.5100
support@prosoft-technology.com

infrastructure side will only work for one of the devices that are connected to the Bridging Client or the Bridging Client itself. Network traffic may not be able to start because of the ARP failures. Since the IP-to-MAC address mapping of a wireless client may change over time due to continuously (re-)learning by the wireless controller, the ARP resolution of a device may or may not work depending on which IP address is bound to the MAC address of the Bridging Client at that moment, thus showing intermittent behavior.



All APs > Details for AP2

General

AP Name: AP2
Location: default location
AP MAC Address: 6c:41:6a:b2:03:4f
Base Radio MAC: d0:c7:89:0b:ab:c0
Admin Status: Enable
AP Mode: local
AP Sub Mode: None
Operational Status: REG
Port Number: 1
Venue Group: Unspecified
Venue Type: Unspecified

Language | Venue Name

Network Spectrum Interface Key: 1DC4F4911ADB438DEFA4EA5211A4663E

GPS Location

GPS Present: No

Versions

Primary Software Version: 8.5.135.0
Backup Software Version: 0.0.0.0
Predownload Status: None
Predownloaded Version: None
Predownload Next Retry Time: NA
Predownload Retry Count: NA
Boot Version: 12.4.23.0
IOS Version: 15.3(3)JF8$
Mini IOS Version: 7.3.1.53

IP Config

CAPWAP Preferred Mode: Ipv4 (Global Config)
DHCP Ipv4 Address: 10.67.132.28
Static IP (Ipv4/Ipv6): □

Time Statistics

UP Time: 33 d, 03 h 20 m 19 s
Controller Associated Time: 33 d, 03 h 18 m 52 s
Controller Association Latency: 0 d, 00 h 01 m 26 s

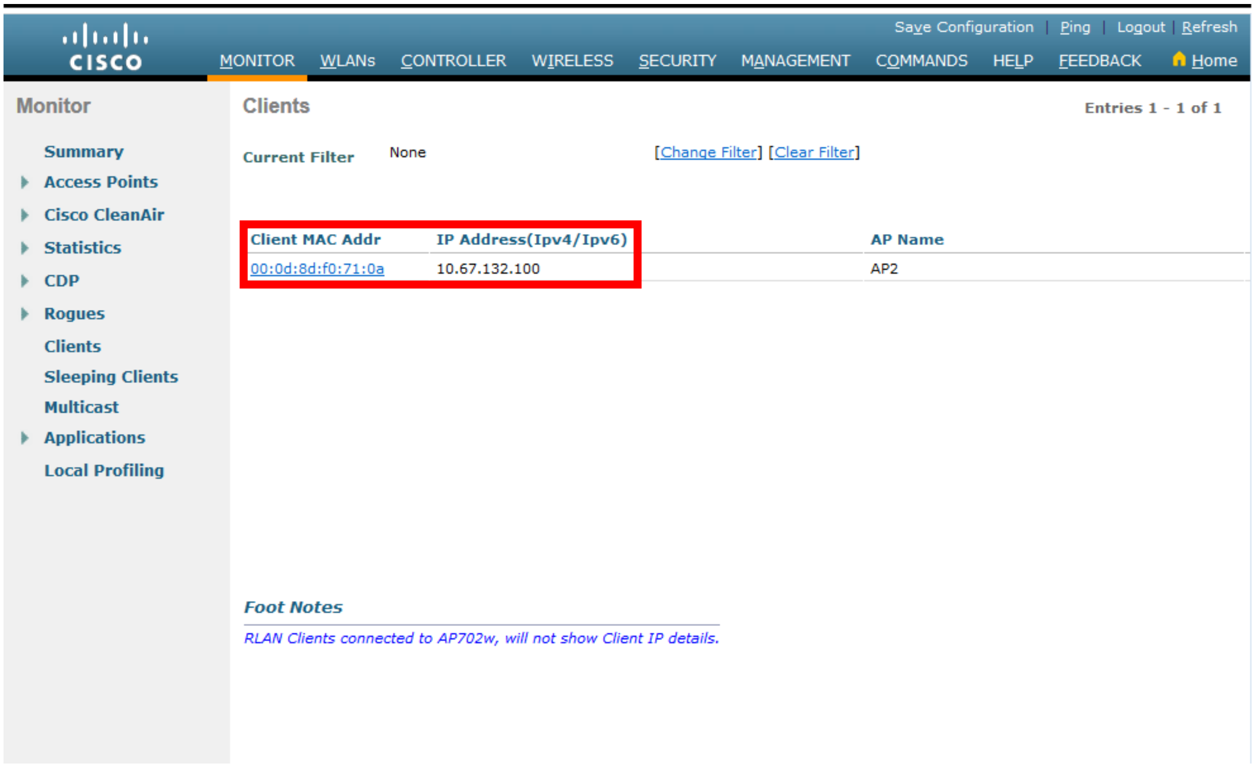
Hardware Reset

Perform a hardware reset on this AP

Set to Factory Defaults

Clear configuration on this AP and reset it to factory defaults

Figure 1 Cisco AP Mode configuration



Clients

Entries 1 - 1 of 1

Current Filter None

Client MAC Addr	IP Address(Ipv4/Ipv6)	AP Name
00:0d:8d:f0:71:0a	10.67.132.100	AP2

Foot Notes

RLAN Clients connected to AP702w, will not show Client IP details.

Figure 2 IP-to-MAC address mapping of wireless client

Solution

Currently, there is no way to disable the proxy ARP function in the Cisco wireless controller when an access point is configured in Local AP mode. To facilitate ARP resolution for all devices behind a Bridging Client, we have to configure the access points involved to operate in ***FlexConnect*** AP mode and enable ***FlexConnect Local Switching*** on the corresponding SSID.

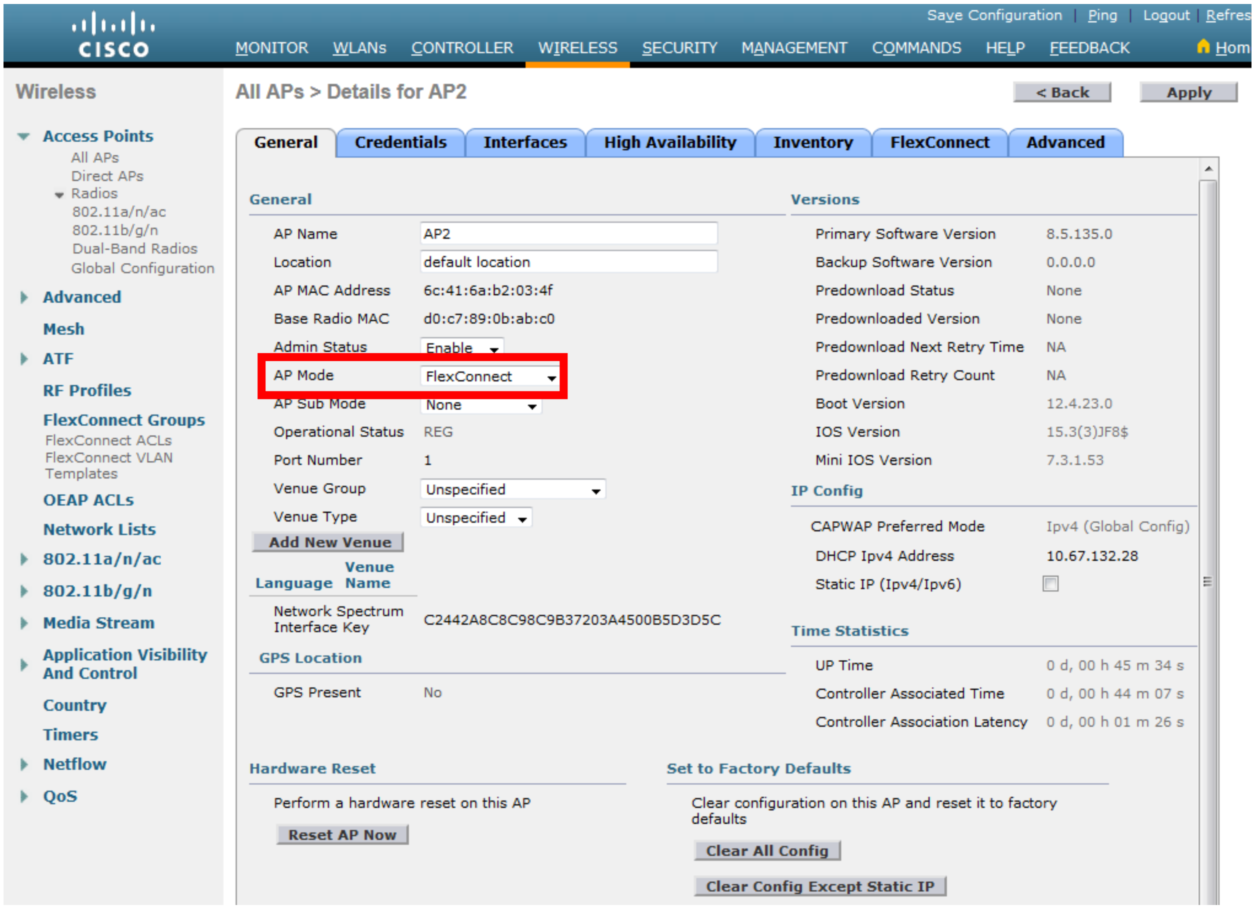
Configuring an access point to operate in FlexConnect AP mode (GUI)

Step 1 Choose **Wireless** to open the All APs page.

Step 2 Click the name of the desired access point. The All APs > Details page appears.

Step 3 Choose FlexConnect from the AP Mode drop-down list to enable FlexConnect for this access point (Figure 3).

Step 4 Click **Apply** to commit the change. The access point will reboot.



All APs > Details for AP2

General

AP Name	AP2
Location	default location
AP MAC Address	6c:41:6a:b2:03:4f
Base Radio MAC	d0:c7:89:0b:ab:c0
Admin Status	Enable
AP Mode	FlexConnect
AP Sub Mode	None
Operational Status	REG
Port Number	1
Venue Group	Unspecified
Venue Type	Unspecified

Language Venue Name

Network Spectrum Interface Key C2442A8C8C98C9B37203A4500B5D3D5C

GPS Location

GPS Present No

Versions

Primary Software Version	8.5.135.0
Backup Software Version	0.0.0.0
Predownload Status	None
Predownloaded Version	None
Predownload Next Retry Time	NA
Predownload Retry Count	NA
Boot Version	12.4.23.0
IOS Version	15.3(3)JF8$
Mini IOS Version	7.3.1.53

IP Config

CAPWAP Preferred Mode	Ipv4 (Global Config)
DHCP Ipv4 Address	10.67.132.28
Static IP (Ipv4/Ipv6)	□

Time Statistics

UP Time	0 d, 00 h 45 m 34 s
Controller Associated Time	0 d, 00 h 44 m 07 s
Controller Association Latency	0 d, 00 h 01 m 26 s

Hardware Reset

Perform a hardware reset on this AP

Set to Factory Defaults

Clear configuration on this AP and reset it to factory defaults

Figure 3 Configuring access point to FlexConnect AP mode

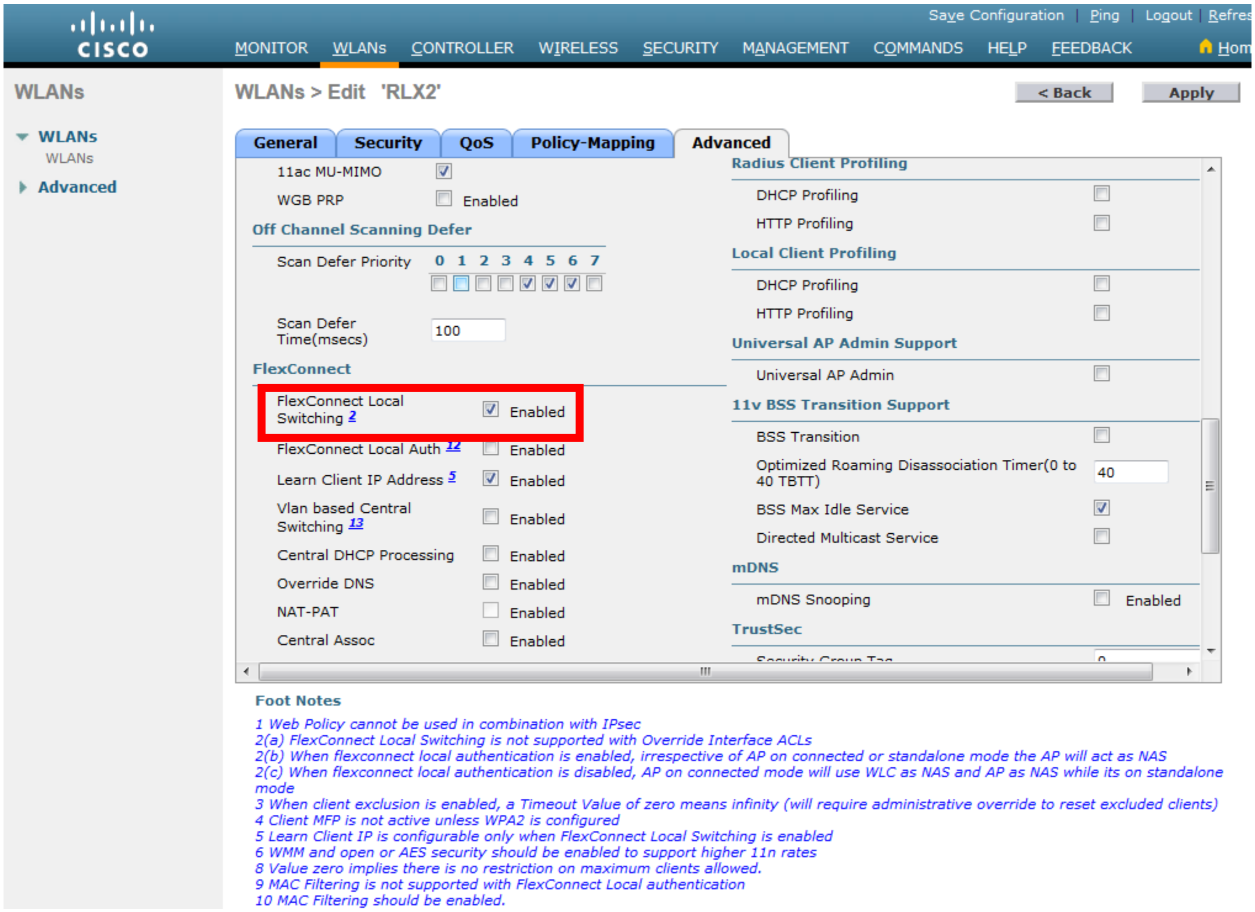
Configuring Local Switching on a SSID

Step 1 Choose **WLANs** to open the WLANs page.

Step 2 Click the WLAN ID of the desired SSID. The WLANs > Edit page appears.

Step 3 In the Advanced tab, select the **FlexConnect Local Switching** check box to enable local switching for the WLAN (Figure 4).

Step 4 Click **Apply** to commit the change.



WLANs > Edit 'RLX2'

11ac MU-MIMO ☑

WGB PRP □ Enabled

Off Channel Scanning Defer

Scan Defer Priority 0 1 2 3 4 5 6 7
□ □ □ □ ☑ ☑ ☑ □

Scan Defer Time(msecs) 100

FlexConnect

FlexConnect Local Switching [2] ☑ Enabled

FlexConnect Local Auth [12] □ Enabled

Learn Client IP Address [5] ☑ Enabled

Vlan based Central Switching [13] □ Enabled

Central DHCP Processing □ Enabled

Override DNS □ Enabled

NAT-PAT □ Enabled

Central Assoc □ Enabled

Radius Client Profiling

DHCP Profiling □

HTTP Profiling □

Local Client Profiling

DHCP Profiling □

HTTP Profiling □

Universal AP Admin Support

Universal AP Admin □

11v BSS Transition Support

BSS Transition □

Optimized Roaming Disassociation Timer(0 to 40 TBTT) 40

BSS Max Idle Service ☑

Directed Multicast Service □

mDNS

mDNS Snooping □ Enabled

TrustSec

Security Group Tag 0

Foot Notes

1 Web Policy cannot be used in combination with IPsec
2(a) FlexConnect Local Switching is not supported with Override Interface ACLs
2(b) When flexconnect local authentication is enabled, irrespective of AP on connected or standalone mode the AP will act as NAS
2(c) When flexconnect local authentication is disabled, AP on connected mode will use WLC as NAS and AP as NAS while its on standalone mode
3 When client exclusion is enabled, a Timeout Value of zero means infinity (will require administrative override to reset excluded clients)
4 Client MFP is not active unless WPA2 is configured
5 Learn Client IP is configurable only when FlexConnect Local Switching is enabled
6 WMM and open or AES security should be enabled to support higher 11n rates
8 Value zero implies there is no restriction on maximum clients allowed.
9 MAC Filtering is not supported with FlexConnect Local authentication
10 MAC Filtering should be enabled.

Figure 4 Enabling FlexConnect Local Switching