Link Local Bridging

- Feature History for Link Local Bridging, on page 1
- Information About Link Local Bridging , on page 1
- Use Case for Link Local Bridging, on page 2
- Guidelines and Restrictions for Link Local Bridging, on page 2
- Enabling Link Local Bridging Per Policy Profile (GUI), on page 2
- Enabling Link Local Bridging Per Policy Profile (CLI), on page 3
- Verifying Link Local Bridging, on page 3

Feature History for Link Local Bridging

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

This feature is available in all the releases subsequent to the one in which it is introduced in, unless noted otherwise.

Table 1: Feature History for Link Local Bridging

Release	Feature	Feature Information
Cisco IOS XE Bengaluru 17.6.1	Link Local Bridging	The Link Local Bridging feature allows you to manage link-local traffic in intercontroller and intracontroller roaming scenarios.

Information About Link Local Bridging

In Cisco IOS XE Bengaluru 17.5.1 and earlier releases, client packets were forwarded through the access VLAN of a client. The client also received all the IPv4 or IPv6 packets from its assigned access VLAN.

When an L3 client roamed from one controller to another controller, the point-of-presence (PoP) remained with the first controller, also known as the anchor controller or the home controller, and the point-of-attachment (PoA) moved to the second controller, also known as the foreign controller or the visited controller. In this anchor-foreign scenario, the client packets were tunneled back to the anchor controller to be forwarded on the access VLAN of the client.

Similarly, in case of L3 intracontroller roaming, when the feature Roaming Across Policy Profile is enabled, the client access VLAN is maintained, regardless of the policy profile VLAN. In such a scenario, the PoA becomes the destination policy profile VLAN.

A roaming wireless client is served better by the local services present near its PoA rather than discovering services present at its PoP. Therefore, from Cisco IOS XE Bengaluru 17.6.1 onwards, the intracontroller and intercontroller roaming scenarios described above, can now be managed with the help of the Link Local Bridging feature. Link Local Bridging is disabled by default.

Use Case for Link Local Bridging

If you have a local mode deployment, and L3 roaming is used to manage roaming clients across physical locations, the Link Local Bridging feature helps you to discover services, for example, using mDNS, which are physically close to the wireless client.

Guidelines and Restrictions for Link Local Bridging

- The Link Local Bridging feature is supported in local-mode or FlexConnect central switching.
- Only mDNS bridge mode is supported with Link Local Bridging.
- Guest profiles are not supported.
- Wired Guest LAN, Remote LAN (RLAN), and Inter-Release Controller Mobility (IRCM) are not supported.
- Mesh and IP Source Guard (IPSG) is not supported when the Link Local Bridging feature is enabled.
- Enabling Link Local Bridging on the anchor controller and disabling it on the foreign controller is not supported, even if roaming is successful.
- Access VLAN and bridge VLAN should be operational, for the Link Local Bridging feature to work.
- Link Local Bridging must be enabled across policy profiles for the same SSID.
- Wireless multicast-over-multicast (**wireless multicast** *multicast IP address*) must be configured, before enabling the Link Local Brigding feature. Therefore, the **wireless multicast link-local** command is enabled by default when wireless multicast is enabled.

Enabling Link Local Bridging Per Policy Profile (GUI)

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **Policy**.

Step 2 Click **Add**.
The **Add Policy Profile** window is displayed.

Step 3 In the **Add Policy Profile** page, in the **General** tab, enter the name of the policy profile.

Step 4 In the **Advanced** tab, check the **Link-Local Bridging** check box to enable link-local bridging on the policy profile.

Note When link-local bridging is enabled, Export Anchor will be disabled and Central Switching will be enabled automatically.

Step 5 Click **Apply to Device**.

Enabling Link Local Bridging Per Policy Profile (CLI)

To enable link local bridging per policy profile, follow these steps.

Before you begin

Ensure that wireless multicast-over-multicast and wireless multicast link-local are enabled.

Note From Cisco IOS XE Bengaluru 17.6.1, the wireless multicast link-local setting is enabled by default as soon as multicast is enabled. This means that all the downstream multicast link-local frames will be forwarded to wireless clients. In the Cisco IOS XE Bengaluru 17.5.x and the earlier releases, only mDNS multicast link-local frames were forwarded.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless profile policy** *profile-name* **Example:** `Device(config)# wireless profile policy wireless-profile1`	Creates policy profile for the WLAN.
Step 3	**link-local-bridging** **Example:** `Device(config-wireless-policy)# link-local-bridging`	Enables link local bridging per policy profile.

Verifying Link Local Bridging

To verify the configuration status of Link Local Bridging, use the following command:

```
Device# show wireless profile policy detailed policy1
Policy Profile Name                : policy1
```

```
Description                          :
Status                               : ENABLED
VLAN                                 : 81
Multicast VLAN                       : 0
OSEN client VLAN                     :
Multicast Filter                     : DISABLED
QBSS Load                            : ENABLED
Passive Client                       : DISABLED
ET-Analytics                         : DISABLED
StaticIP Mobility                    : DISABLED
WLAN Switching Policy
  Flex Central Switching             : ENABLED
  Flex Central Authentication        : ENABLED
  Flex Central DHCP                  : ENABLED
  Flex NAT PAT                       : DISABLED
.
.
.
  ----------------------------------------------------------
mDNS Gateway
  mDNS Service Policy name           : default-mdns-service-policy
User Defined (Private) Network              : Disabled
User Defined (Private) Network Unicast Drop  : Disabled
Policy Proxy Settings
  ARP Proxy State                    : DISABLED
  IPv6 Proxy State                   : None
Airtime-fairness Profile
  2.4Ghz ATF Policy                  : default-atf-policy
  5Ghz ATF Policy                    : default-atf-policy
Link-local bridging                  : ENABLED
```

To verify if Link Local Bridging VLAN is included, use the following command:

```
Device# show wireless client mac 7xxx.3xxx.3xxx detail
Client MAC Address : 7xxx.3xxx.3xxx
.
.
.
Link-local bridging VLAN: 3
.
.
.
WiFi Direct Capabilities:
  WiFi Direct Capable           : No
```

To verify if link local multicast traffic is enabled, use the following command:

```
Device# show wireless multicast
Multicast                              : Disabled
AP Capwap Multicast                    : Unicast
Wireless Broadcast                     : Disabled
Wireless Multicast non-ip-mcast        : Disabled
Wireless Multicast link-local          : Enabled
```