Configuring Wireless Multicast on Wireless LAN Controllers

This document describes how to configure wireless multicast, which supports multicast with unicast delivery mechanism, on Cisco Catalyst 3850 Series Switches with WLCs.

Prerequisites

We recommend that you have a basic knowledge of the multicast implementation on Cisco Catalyst 3850 Series Switches with WLC.

Supported Platforms and Releases

The information in this document is based on the following software and hardware versions:

- Cisco Catalyst 3850 Series Switch with WLC
- Cisco 3602 Access Point (AP)

Note The information in this document refers to devices in a specific lab environment. Descriptions of the devices is provided with default configuration values. If you are on a live network, you must understand the potential impact of all the commands.

Configuring Multicast on Converged Access Platforms

To enable multicast on the Converged Access platforms, perform the following tasks:

Step 1 To enable multicast on Cisco Catalyst 3850 Series Switches with WLC, use the **wireless multicast** command in global configuration mode.

```
Device(config)# wireless multicast
```

Note By default, this command enables the multicast with unicast delivery mechanism.

Step 2 To enable Internet Group Management Protocol (IGMP) snooping on Cisco WLC (enabled by default), use the **ip igmp snooping** command in global configuration mode:

```
Device(config)# ip igmp snooping
Device(config)# ip igmp snooping querier
```

Note The **ip igmp snooping querier** command configures Cisco WLC to periodically monitor whether a client still interacts with multicast traffic.

Configuring Multicast Flow on Converged Access

The following steps outline the multicast traffic flow on the Converged Access. Refer to the Configuring Multicast on Converged Access Platforms section for configuration details.

Step 1 Cisco WLC intercepts the IGMP packets sent by wireless clients.

If there is an existing entry for the multicast group-vlan-source combination client, Cisco WLC updates the IGMP timers.

If this is a new entry, Cisco WLC creates a Multicast Group Identifier (MGID) based on the tuple (source, group, and VLAN) with a multiple range, either between 1 and 4,095 for Layer 2 (L2) or between 4,160 and 8,191 for Layer 3 (L3).

Step 2 The IGMP packet is forwarded as an upstream.

Step 3 The MGID entry is sent to an AP along with the associated client information, to receive the multicast traffic on a client.

Step 4 Cisco WLC forwards the traffic to the AP appropriately, if the delivery mechanism is multicast with unicast .

Note If the delivery mechanism is multicast, Datagram Transport Layer Security (DTLS) encryption and Quality of Service (QoS) marking are not applicable.

Step 5 The AP then forwards the traffic to each client, as per the requirement.

Verifying the Wireless Multicast Configuration on Wireless LAN Controller

To verify the configuration, perform the following steps:

Step 1 To verify whether multicast is enabled properly, use the **show wireless multicast** command in EXEC mode:

```
Device# show wireless multicast
Multicast: Enabled
AP Capwap Multicast: Multicast
AP Capwap Multicast group Address: 239.255.255.249
AP Capwap Multicast QoS Policy Name: unknown
AP Capwap Multicast QoS Policy State: None
Wireless Broadcast: Disabled
Wireless Multicast non-ip-mcast: Disabled

Vlan Non-ip-mcast Broadcast MGID
--------------------------------
1         Enabled Enabled Disabled
10        Enabled Enabled Enabled
24        Enabled Enabled Enabled
25        Enabled Enabled Enabled
26        Enabled Enabled Enabled
32        Enabled Enabled Enabled
```

Step 2 To verify whether an MGID entry is created for the multicast group the client attempts to join (239.255.255.250 is used as an example), use the **show wireless multicast group summary** command in EXEC mode:

```
Device# show wireless multicast group summary
IPv4 groups
-------------
MGID   Source   Group             Vlan
--------------------------------------
4160   0.0.0.0  239.255.255.250    32
```

Step 3 To verify whether the required client is added to the MGID table, use the **show wireless multicast group** command in EXEC mode:

```
Device# show wireless multicast group 239.255.255.250 vlan 32
Source : 0.0.0.0
Group : 239.255.255.250
Vlan : 32
MGID : 4160

Number of Active Clients : 1
Client List
-------------
```

```
Client MAC      Client IP      Status
---------------------------------------
1410.9fef.272c  192.168.24.50  MC_ONLY
```

Step 4 To verify whether the required MGID entry is added to the AP for this client , use the **show capwap mcast mgid** command in EXEC mode:

```
Device# show capwap mcast mgid id 4160

L3 MGID = 4160 WLAN bitmap = 0x0001
Slot map/tx-cnt: R0:0x0000/0 R1:0x0001/1499
Clients per Wlan
Wlan: 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16

!! This shows the number of clients per slot, per Service Set
   Identification (SSID) on the AP.

Normal Mcast Clients R0: 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
Normal Mcast Clients R1: 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
rx pkts = 1499 drp pkts = 0
tx packets:
wlan : 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15
slots0 : 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
slots1 : 1499 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0

Normal Mcast Clients:
Client: 1410.9fef.272c --- Qos User Priority: 0
```

Note Consider the counters on the received and transmitted packets. This information is useful to determine whether the AP properly forwards the packets to the client.

Step 5 To view all the client-multicast group mappings, use the **show ip igmp snooping igmpv2-tracking** command in EXEC mode. This command provides an overview of the connected clients and the joined groups.

```
Device# show ip igmp snooping igmpv2-tracking

Client to SGV mappings
----------------------

Client: 192.168.24.50 Port: Ca1
Group:  239.255.255.250  Vlan: 32 Source: 0.0.0.0 blacklisted: no

!! If the client has joined more than one multicast group, all the group entries will be shown here
 one after the other.

SGV to Client mappings
----------------------

Group:  239.255.255.250 Source: 0.0.0.0 Vlan: 32
Client: 192.168.24.50 Port: Ca1 Blacklisted: no

!! If there is more than one client entry, these will be shown here.
```

Step 6 To verify the MGID from Cisco WLC, use the **show ip igmp snoop wireless mgid** command in EXEC mode:

```
Device# show ip igmp snoop wireless mgid
```

```
Total number of L2-MGIDs = 33

Total number of MCAST MGIDs = 0

Wireless multicast is Enabled in the system
Vlan bcast nonip-mcast mcast mDNS-br mgid Stdby Flags
1 Enabled Disabled Enabled Enabled Enabled 0:1:1:1
100 Enabled Disabled Enabled Enabled Disabled 0:1:1:0
115 Enabled Disabled Enabled Enabled Disabled 0:1:1:0
517 Enabled Disabled Enabled Enabled Disabled 0:1:1:0
518 Enabled Disabled Enabled Enabled Disabled 0:1:1:0
519 Enabled Disabled Enabled Enabled Enabled 0:1:1:1
520 Enabled Disabled Enabled Enabled Enabled 0:1:1:1
521 Enabled Disabled Enabled Enabled Enabled 0:1:1:1
522 Enabled Disabled Enabled Enabled Enabled 0:1:1:1
523 Enabled Disabled Enabled Enabled Enabled 0:1:1:1
524 Enabled Disabled Enabled Enabled Enabled 0:1:1:1
525 Enabled Disabled Enabled Enabled Enabled 0:1:1:1
526 Enabled Disabled Enabled Enabled Enabled 0:1:1:1
527 Enabled Disabled Enabled Enabled Enabled 0:1:1:1
528 Enabled Disabled Enabled Enabled Enabled 0:1:1:1
529 Enabled Disabled Enabled Enabled Enabled 0:1:1:1
530 Enabled Disabled Enabled Enabled Enabled 0:1:1:1
531 Enabled Disabled Enabled Enabled Enabled 0:1:1:1
1002 Enabled Enabled Enabled Enabled Disabled 0:0:1:0
1003 Enabled Enabled Enabled Enabled Disabled 0:0:1:0
1004 Enabled Enabled Enabled Enabled Disabled 0:0:1:0
1005 Enabled Enabled Enabled Enabled Disabled 0:0:1:0

Index MGID (S, G, V)
--------------------------------------------------------
```

Troubleshooting Wireless Multicast Configuration on Wireless LAN Controller Issues

To troubleshoot the configuration issues from Cisco WLC, use the following commands:

debug ig ipmp snooping

debug ip igmp snooping 239.255.255.250

debug ip igmp snooping querier

debug ip igmp snoop wireless ios client-tracking

debug ip igmp snoop wireless ios events

debug ip igmp snoop wireless ios error

debug ip igmp snoop wireless ap detail

debug ip igmp snoop wireless ap error

debug ip igmp snoop wireless ap event

debug ip igmp snoop wireless ap message

debug platform l2m-igmp

debug l2mcast wireless ios error

debug l2mcast wireless ios mgid

debug l2mcast wireless ios spi

debug l2mcast wireless ios ipc

debug l2mcast wireless ios broadcast

Note To avoid performance issues, ensure that you use the relevant multicast debug commands.

The following is an output for the **show debug** command:

```
Device# show debug

NG3K Wireless:
 NG3K WIRELESS Error DEBUG debugging is on
L3 Multicast platform:
 NGWC L3 Multicast Platform debugs debugging is on
L2M IGMP platform debug:
 NGWC L2M IGMP Platform debugs debugging is on
 NGWC L2M IGMP SPI debugs debugging is on
 NGWC L2M IGMP Error debugs debugging is on
IP multicast:
 IGMP debugging is on for 239.10.10.11
IGMP tracking:
 igmpv2 tracking debugging is on
L2MC Wireless:
 L2MC WIRELESS SPI EVENTS debugging is on
 L2MC WIRELESS REDUNDANCY EVENTS debugging is on
 L2MC WIRELESS ERROR debugging is on
IGMP Wireless:
 IGMP SNOOP wireless IOS Errors debugging is on
 IGMP SNOOP wireless IOS Events debugging is on

 igmp/snooping/wireless/ap/event debugging is on
 multicast/event debugging is on
 igmp/snooping/wireless/ap/message/rx debugging is on
 igmp/snooping/wireless/ap/message/tx debugging is on
 wireless/log debugging is on
 l2multicast/error debugging is on
 igmp/snooping/wireless/ap/error debugging is on
 multicast/error debugging is on
 multicast debugging is on
 l2multicast/event debugging is on
 wireless/platform debugging is on
 igmp/snooping/wireless/ap/detail debugging is on
```

The following sample output displays MGID creation on the Cisco WLC:

```
*Sep 7 00:12:11.029: IGMPSN: Received IGMPv2 Report for group 239.255.255.250 received
 on Vlan 32, port Ca1
*Sep 7 00:12:11.029: IGMPSN: group: Received IGMPv2 report for group 239.255.255.250
 from Client 192.168.24.50  received on Vlan 32, port Ca1
*Sep 7 00:12:11.029: (l2mcast_tracking_is_client_blacklisted) Client: 192.168.24.50
 Group: 239.255.255.250 Source: 0.0.0.0 Vlan: 32 Port: Ca1
*Sep 7 00:12:11.029: (l2mcsn_process_report) Allocating MGID for Vlan: 32 (S,G):
 :239.255.255.250
*Sep 7 00:12:11.029: (l2mcast_wireless_alloc_mcast_mgid) Vlan: 32 Source: 0.0.0.0
 Group: 239.255.255.250
*Sep 7 00:12:11.030: (l2mcast_wireless_alloc_mcast_mgid) Hash entry added!
*Sep 7 00:12:11.030: (l2mcast_wireless_track_and_inform_client) Protocol: IGMPSN
```

```
 Client-address: 192.168.24.50 (S,G,V): 0.0.0.0 239.255.255.250 32 Port: Ca1, MGID:
 4160 Add: Add
*Sep 7 00:12:11.030: (l2mcast_get_client_params) Client Addr: 192.168.24.50 Client-id:
 40512055681220617 Mcast-vlan: 32(l2mcast_wireless_inform_client) Protocol: IGMPSN
 Client-address: 192.168.24.50 (S,G,V): 0.0.0.0 239.255.255.250 32 Port: Ca1, iifid =
 0x9667C000000004 MGID: 4160 Add: Add
*Sep 7 00:12:11.030: (l2mcast_wireless_inform_client) Sent INFORM CLIENT SPI
*Sep 7 00:12:11.030: (l2mcast_wireless_track_and_inform_client)
 l2mcast_wireless_inform_client passed
*Sep 7 00:12:11.032: %IOSXE-7-PLATFORM: 1 process wcm: IGMP has sent the
 WCM_INFORM_CLIENT with ^I client_id = 40512055681220617/8fed8000000009 ^I capwap id =
 42335320837980164 ^I mac_addr = 1410.9fef.272c ^I num_entry = 1
```

The entry created on the Cisco IOS is passed to the Wireless Control Module (WCM) process. The WCM process verifies and adds the entry.

```
*Sep 7 00:12:11.032: %IOSXE-7-PLATFORM: 1 process wcm: i = 0, source = 0.0.0.0 group =
 239.255.255.250  client_ip = 192.168.24.50 vlan = 32, mgid = 4160 add = 1
*Sep 7 00:12:11.032: %IOSXE-7-PLATFORM: 1 process wcm: in igmp_wcm_client_join_callback
 source = 0.0.0.0 group = 239.255.255.250 client_ip = 192.168.24.50 vlan = 32
 client_mac = 1410.9fef.272c mgid = 4160
*Sep 7 00:12:11.032: %IOSXE-7-PLATFORM: 1 process wcm: apfMswtp_iifid = 9667c000000004
 capwap_if_id = 9667c000000004
*Sep 7 00:12:11.032: %IOSXE-7-PLATFORM: 1 process wcm: rrc_manual_mode = 0
 rrc_status = 2
*Sep 7 00:12:11.032: %IOSXE-7-PLATFORM: 1 process wcm: locking mgid Tree in file
 bcast_process.c line 491
*Sep 7 00:12:11.033: %IOSXE-7-PLATFORM: 1 process wcm: allocateL3mgid: mgid entry AVL
 search key dump:
*Sep 7 00:12:11.033: %IOSXE-7-PLATFORM: 1 process wcm: 00000000: 00 00 00 00 ef 01 01
 01 00 08 ff ff ff ff ff ff ................^M 00000010: ff ff ff ff ff ff ff ff ff ff
 ff ff ff ff ff ff ................^M 00000020: ff ff ..^M
*Sep 7 00:12:11.033: %IOSXE-7-PLATFORM: 1 process wcm: mcast_group_client_lookup:
 Lookup failed for client with mac 1410.9fef.272c
*Sep 7 00:12:11.033: %IOSXE-7-PLATFORM: 1 process wcm: unlocking mgid Tree in file
 bcast_process.c line 624
*Sep 7 00:12:11.033: %IOSXE-7-PLATFORM: 1 process wcm: spamLradSendMgidInfo: ap =
 0C85.25C7.9AD0 slotId = 1, apVapId = 1, numOfMgid = 1 join = 1 isL2Mgid = 0,
 mc2ucflag = 0, qos = 0
*Sep 7 00:12:11.033: %IOSXE-7-PLATFORM: 1 process wcm: mscbApMac = 0c85.25c7.9ad0
 client_mac_addr = 1410.9fef.272c slotId = 1 vapId = 1 mgid = 4160 numOfSGs = 2,
 rrc_status = 2
```

To troubleshoot configuration issues from the AP, use the following commands:

debug capwap mcast fwd

debug capwap mcast query

The following is a sample output of the **debug** commands:

```
*Sep 7 06:00:38.099: CAPWAP MCAST: capwapDecodeMgidPayload: mgidTypeStr L3 IGMP MGID
 ADD,mgidType 53,mgid=4160,mgid operation=1
*Sep 7 06:00:38.099: CAPWAP MCAST: capwapAddMgidEntry: slotId= 1, client_mac=
 1410.9fef.272c, mgid= 4160, wlanid= 0, mc2ucflag= 0, priority= 0, downpriority= 0
 L3 mgid flag = L3 IGMP MGID .
*Sep 7 06:00:38.099: CAPWAP MCAST: allocateMgidEntry: mgid = 4160, isL3Mgid=1
*Sep 7 06:00:38.099: CAPWAP MCAST: capwap_bss_mgid_enable:MGID 4160 enable -
 Slot=1 WLAN=1
*Sep 7 06:00:38.099: CAPWAP MCAST: L3 IGMP MGID ADD MGID = 4160 SUCCESSFUL.!!
```

Note

- When an MGID entry is added, the VLAN ID displayed in the output is 0.
- The output displays the correct VLAN mapping even after the MGID entry is deleted.

Use the following commands for further analysis from Cisco WLC:

show wireless client summary

show wcdb database all

show wireless multicast group summary

show wireless multicast group <ip> vlan <id>

show wireless multicast source <ip> group <ip> vlan <id>

show ip igmp snooping wireless mgid

show ip igmp snooping igmpv2-tracking

Use the following commands for further analysis from the AP:

show capwap mcast mgid all

show capwap mcast mgid id <id>

Note

- The number of multicast groups to which each client can be associated is limited to 16. When the client sends a join request for a possible 17th group, the group is created on the Cisco IOS. But, on the WCM, a deny message is sent to Cisco IOS. The Cisco IOS then deletes that group.
- Currently, only IGMP V2 is supported. If a client uses IGMP V3, MGID is not created on the on the Cisco WLC. For this reason, the source address in the source, group, and VLAN is always 0.0.0.0.
- The number of L3 MGIDs supported on the Converged Access range from 4,160 to 8,191. Because an MGID entry is a combination of the multicast address and VLAN, there can only be 4,000 such combinations. This can be a limitation in large environments.
- The Bonjour feature is not supported across VLANs. This is because of the IP address 224.0.0.251, which is a link-local multicast address. Cisco Catalyst 3850 Series Switches with WLCs do not snoop link-local addresses like other Catalyst switches. Therefore, you will see the following error message:

```
IGMPSN: group: Received IGMPv2 report for group 224.0.0.251 from Client 192.168.24.94
received on Vlan 32, port Ca93 with invalid group address.
```