Configure Wireless Multicast on 5760 and 3850 Series WLCs

Contents

[Introduction](#)
[Prerequisites](#)
[Requirements](#)
[Components Used](#)
[Configure](#)
[Multicast Flow on NGWC](#)
[Verify](#)
[Troubleshoot](#)
[Important Considerations](#)

Introduction

This document describes how to configure wireless multicast on the Cisco 5760 and 3850 Series Wireless LAN Controllers (WLCs), which support both *multicast with unicast* and *multicast with multicast* delivery mechanisms.

Prerequisites

Requirements

Cisco recommends that you have basic knowledge of multicast implementation on the Cisco 5760 and 3850 Series WLCs.

Components Used

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

- Cisco 5760 Series WLC
- Cisco 3850 Series WLC
- Cisco 3602 Series Access Point (AP).

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Configure

Complete these steps in order to enable multicast on the Next Generation Wiring Closet (NWGC)

platforms:

1. Enter the **wireless multicast** command in order to enable multicast on the controller:

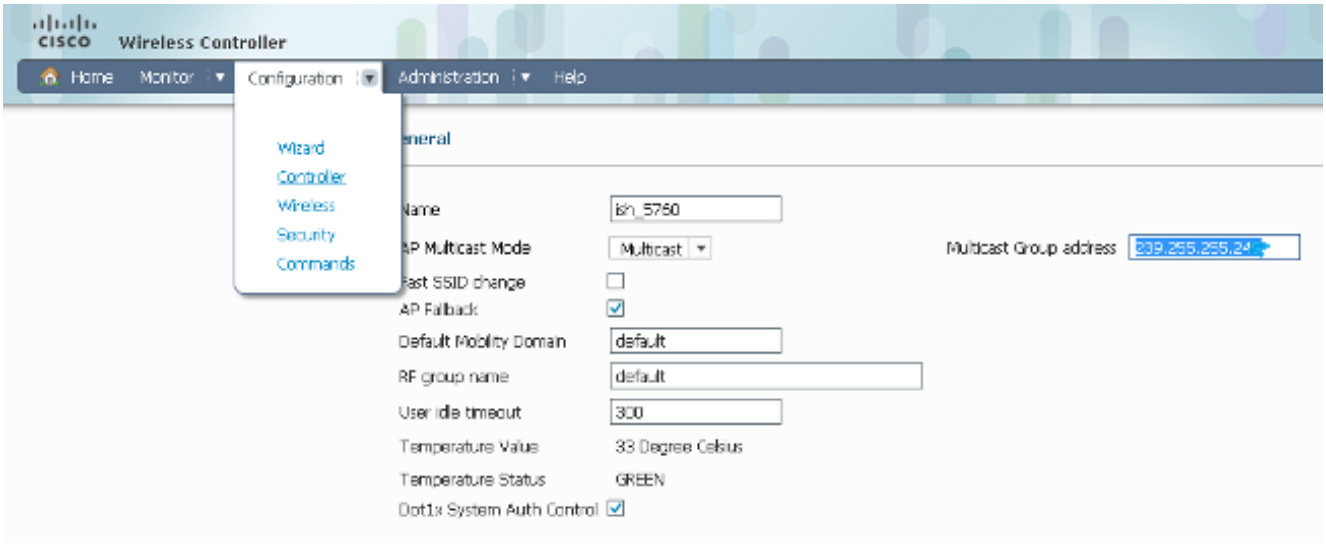
```
ish_5760(config)#wireless multicast
```

Note: This command by default enables the *multicast with unicast* delivery mechanism.

2. If you must change the delivery mechanism to *multicast with multicast*, then enter this command:

```
ish_5760(config)#ap capwap multicast 239.255.255.250
```

Note: This command configures the multicast group to which all of the Control and Provisioning of Wireless Access Points (CAPWAP) APs join, which optimizes the switch so that it sends a multicast CAPWAP message that reaches all of the APs. This process is different when unicast mode is used, as the switch would then be required to send unicast messages to all of the CAPWAP APs. This helps to minimize the system load on the controller.Optionally, you can navigate to **Configuration > Controller** from the GUI in order to configure this information, as shown here:



3. Enter these commands in order to enable Internet Group Management Protocol (IGMP) snooping on the controller (enabled by default):

```
ip igmp snooping

ip igmp snooping querier
```

Note: The **ip igmp snooping querier** command configures the controller so that it periodically checks whether a client still listens to the multicast traffic.

Multicast Flow on NGWC

These steps outline the flow of the multicast traffic on the NGWCs when the previous configuration is implemented:

1. The controller intercepts the IGMP packets that are sent by the wireless clients.

2. If the client entry for that multicast *group-vlan-source* combination exists, then the controller updates the IGMP timers.

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

3. The IGMP packet is forwarded upstream.

4. The MGID entry is sent to the AP, along with the client association information so that the client can receive the multicast traffic.

5. Based on the delivery mechanism (multicast with unicast/multicast), the controller forwards the traffic to the AP appropriately. **Note**: If the delivery mechanism is multicast, then Datagram Transport Layer Security (DTLS) encryption and Quality of Service (QoS) marking are not applied.
6. The AP then forwards the traffic to each client, as required.

Verify

Complete these steps in order to verify that your configuration works properly:

1. Enter the **show wireless multicast** command in order to verify whether multicast has been enabled correctly:

```
ish_5760#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
```

2. Enter the **show capwap sum** command in order to verify the CAPWAP information:

```
ish_5760#show capwap sum

Name Src Src Dest Dst Dtls MTU Xact
IP Port IP Port En
```

```
---- ----------- ---- ------------ ----- ---- ----- ---
Ca1  172.16.15.1 5247 239.10.10.11 5247  No   1449  1
Ca19 172.16.15.1 5247 172.17.1.54  52451 Yes  1380  3
```

Note: As shown in the output, the **Ca1** interface is used for AP multicast mode. The **Ca1** interface has a *DTLS* value of **No**, while the **Ca19** interface has a *DTLS* value of **Yes**.

3. Enter the **show capwap detail** or the **show capwap summary** in order to verify the number of APs that have joined the multicast group:

```
CAPWAP Tunnels General Statistics:
Number of Capwap Data Tunnels = 2
Number of Capwap Mobility Tunnels = 0
Number of Capwap Multicast Tunnels = 1


Name APName Type PhyPortIf Mode McastIf
------ --------------------------------
Ca2 ish_3502_lw_2 data  -  multicast Ca0
Ca1 ish_ap       data  - multicast Ca0
Ca0 -     mcas - unicast     -


Name SrcIP               SrcPort     DestIP DstPort DtlsEn MTU
--- ---------------     -------     ------  ------- ------ ---
Ca2 10.105.132.138 5247 10.106.55.133   39237   No     1464
Ca1 10.105.132.138 5247 10.106.15.135   38899   No     1464
Ca0  10.105.132.138 5247  239.255.255.249 5247    No      1464


Name IfId               McastRef
---   ------------------ --------
Ca2   0x0098BA0000000041 0
Ca1   0x00BC2C800000003D 0
Ca0   0x008B53C000000001  2
```

Note: The last line of this output points to the CAPWAP tunnel interface that was created for the multicast traffic, and the **McastRef** shows the number of APs that have joined the group. This information is helpful when you must check whether an AP that does not receive the multicast traffic has joined the multicast group.

4. Enter the **show int capwap 0** command in order to verify that the tunnel interface shows the destination address as the multicast group address:

```
ish_5760#show int capwap 0
Capwap0 is up, line protocol is up
Hardware is Capwap
MTU 1464 bytes, BW 10000000 Kbit/sec, DLY 0 usec,
reliability 255/255, txload 1/255, rxload 1/255
Encapsulation UNKNOWN, loopback not set
Keepalive set (10 sec)
Carrier delay is 0 msec
Tunnel iifid 39217105861607425, Tunnel MTU 1464
Tunnel source 10.105.132.138:5247, destination 239.255.255.249:5247
```

5. Enter the **show wireless multicast group summary** command in order to verify whether an MGID entry is created for the multicast group that the client attempts to join (**239.255.255.250** is used in this example):

```
ish_5760#show wireless multicast group summary
IPv4 groups
-------------
MGID   Source   Group             Vlan
---------------------------------------
4160   0.0.0.0 239.255.255.250   32
```

6. Enter this command in order to verify whether the client in question has been added to the MGID table:

```
ish_5760#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
```

7. Enter this command in order to verify whether the MGID entry has been added on the AP for this client:

```
ish_ap#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 when you attempt to determine whether the AP properly forwards the packets to the client.

8. Enter the **show ip igmp snooping igmpv2-tracking** command in order to view all of the client-multicast group mappings. This provides a snapshot of the clients that are connected and the groups that they have joined. Here is a sample output:

```
ish_5760#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.
```

9. Enter this command in order to verify the MGID from the controller:

```
ish_5760#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)
------------------------------------------------------------
```

Troubleshoot

Here is a list of **debug** commands that you can use in order to troubleshoot configuration issues from the controller:

- **debug ip igmp 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 multicast**
- **debug platform multicast error**
- **debug platform multicast event**
- **debug platform l2m-igmp/l2m-mld/l2multicast/l3multicast**
- **debug l2mcast wireless ios error**
- **debug l2mcast wireless ios mgid**
- **debug l2mcast wireless ios spi**

  Note: Ensure that you only use the relevant multicast **debug** commands in order to avoid performance issues.

Here is an example **show debug** command output:

```
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

Nova Platform:
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
```

Here is an example output that shows the MGID creation on the controller:

```
*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
```

Once the entry is created on the Cisco IOS® side, this is passed to the Wireless Control Module (WCM) process, which verifies before it 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
```

Here is a list of **debug** commands that you can use in order to troubleshoot configuration issues from the AP:

- **debug capwap mcast fwd**
- **debug capwap mcast query**

Here is an example **debug** command output:

```
*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**: While the MGID entry is added, the VLAN ID shows as **0** in the previous output. However, even though the entry is deleted, it shows the correct VLAN mapping.

Here is a list of **show** commands that you can use further analysis from the controller:

- **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**

Here is a list of **show** commands that you can use further analysis from the AP:

- **show capwap mcast mgid all**
- **show capwap mcast mgid id <id>**

Important Considerations

Here are some important considerations and limitations in regards to the configuration that is described in this document:

- The number of multicast groups to which each client can listen is limited to 16. Once the client sends the *Join* request with the 17th group, the creation occurs on the Cisco IOS side, but the WCM side sends a *Deny* message to the Cisco IOS. The latter then deletes that group.
- Currently, only IGMP Version 2 (V2) is supported. If a client uses IGMP Version 3 (V3), then the MGID creation does not occur on the controller. For this reason, in the source, group, and VLAN, the source address is always **0.0.0.0**.
- The number of L3 MGIDs that are supported on the NGWC range from 4,160 to 8,191. Since an MGID entry is a combination of the multicast address and the VLAN, there can be only 4,000 such combinations. This might be a limitation in large environments.
- The *Bonjour* feature across VLANs is not supported. This is because the IP address 224.0.0.251 is a link-local multicast address. The Cisco 5760 and 3850 Series WLCs, like any other catalyst switch, does not snoop link-local addresses. For this reason, you will see this error message appear:

```
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.
```