Konfigurieren von Wireless Multicast auf WLCs der Serien 5760 und 3850

Inhalt

Einführung

Dieses Dokument beschreibt die Konfiguration von Wireless Multicast auf den Cisco Wireless LAN Controllern der Serien 5760 und 3850 (WLCs), die sowohl *Multicast mit Unicast* als auch *Multicast mit Multicast*-Bereitstellungsmechanismen unterstützen.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über grundlegende Kenntnisse der Multicast-Implementierung bei den Cisco WLCs der Serien 5760 und 3850 zu verfügen.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- Cisco WLC der Serie 5760
- Cisco WLC der Serie 3850
- Cisco Access Points der Serie 3602 (AP)

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Konfigurieren

Gehen Sie wie folgt vor, um Multicast auf den NWGC-Plattformen (Next Generation Wiring Closet) zu aktivieren:

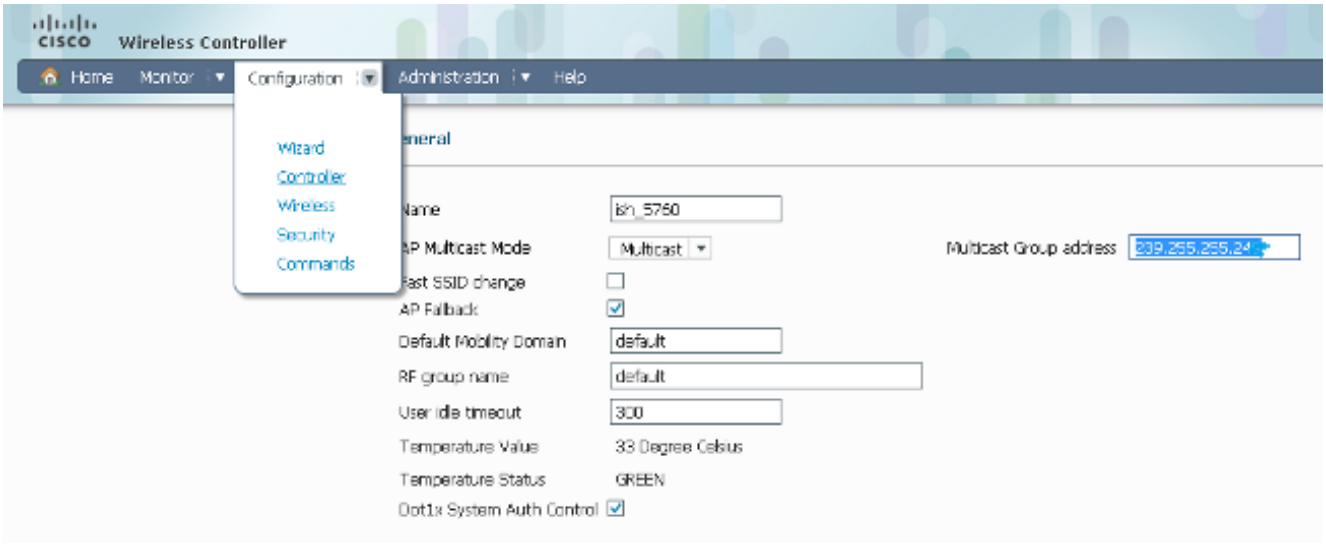
1. Geben Sie den **Wireless Multicast**-Befehl ein, um Multicast auf dem Controller zu aktivieren:

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

   Hinweis: Dieser Befehl aktiviert standardmäßig den *Multicast*-Bereitstellungsmechanismus *mit Unicast*.
2. Wenn Sie den Bereitstellungsmechanismus in *Multicast mit Multicast* ändern müssen, geben Sie den folgenden Befehl ein:

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

   Hinweis: Mit diesem Befehl wird die Multicast-Gruppe konfiguriert, der alle CAPWAPs (Control and Provisioning of Wireless Access Points) angehören. Durch diese Konfiguration wird der Switch so optimiert, dass er eine Multicast-CAPWAP-Nachricht sendet, die alle APs erreicht. Dieser Prozess unterscheidet sich, wenn der Unicast-Modus verwendet wird, da der Switch dann Unicast-Nachrichten an alle CAPWAPs senden muss. Dadurch kann die Systemlast auf dem Controller minimiert werden.Optional können Sie über die Benutzeroberfläche zu **Configuration > Controller** navigieren, um diese Informationen zu konfigurieren, wie hier gezeigt:



3. Geben Sie folgende Befehle ein, um IGMP-Snooping (Internet Group Management Protocol) auf dem Controller zu aktivieren (standardmäßig aktiviert):

   ```
   ip igmp snooping

   ip igmp snooping querier
   ```

   Hinweis: Der Befehl **ip igmp snooping querier** konfiguriert den Controller so, dass er regelmäßig überprüft, ob ein Client den Multicast-Datenverkehr weiterhin überwacht.

Multicast-Fluss bei NGWC

In diesen Schritten wird der Multicast-Datenverkehr auf den NGWCs bei der Implementierung der vorherigen Konfiguration beschrieben:

1. Der Controller fängt die IGMP-Pakete ab, die von den Wireless-Clients gesendet werden.

2. Wenn der Clienteintrag für diese Multicast-*Gruppe*-*VLAN*-*Quelle*-Kombination vorhanden ist, aktualisiert der Controller die IGMP-Timer.

   Wenn es sich um einen neuen Eintrag handelt, erstellt der WLC einen Multicast Group Identifier (MGID) basierend auf dem (Quelle, Gruppe, VLAN)-Tupel, dessen Bereich entweder zwischen 1 und 4.095 für Layer 2 (L2) oder zwischen 4.160 und 8.191 für Layer 3 (L3) liegt.

3. Das IGMP-Paket wird Upstream weitergeleitet.

4. Der MGID-Eintrag wird zusammen mit den Client-Zuordnungsinformationen an den AP gesendet, damit der Client den Multicast-Datenverkehr empfangen kann.

5. Basierend auf dem Bereitstellungsmechanismus (Multicast mit Unicast/Multicast) leitet der Controller den Datenverkehr entsprechend an den Access Point weiter. **Hinweis**: Wenn der Bereitstellungsmechanismus Multicast ist, werden die DTLS-Verschlüsselung (Datagram Transport Layer Security) und die QoS-Markierung (Quality of Service) nicht angewendet.
6. Der Access Point leitet den Datenverkehr dann nach Bedarf an jeden Client weiter.

Überprüfen

Gehen Sie wie folgt vor, um zu überprüfen, ob Ihre Konfiguration ordnungsgemäß funktioniert:

1. Geben Sie den Befehl **show wireless multicast** ein, um zu überprüfen, ob Multicast korrekt aktiviert wurde:

```
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. Geben Sie den Befehl **show capwap sum** ein, um die CAPWAP-Informationen zu überprüfen:

```
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
```

Hinweis: Wie in der Ausgabe gezeigt, wird die **Ca1-**Schnittstelle für den AP-Multicast-Modus verwendet. Die **Ca1-**Schnittstelle hat den Wert **Nein** für *DTLS*, während die **Ca19**-Schnittstelle den *Wert Ja* hat.

3. Geben Sie die **show capwap detail** oder die **show capwap summary ein**, um die Anzahl der APs zu überprüfen, die der Multicast-Gruppe beigetreten sind:

```
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
```

Hinweis: Die letzte Zeile dieser Ausgabe verweist auf die CAPWAP-Tunnelschnittstelle, die für den Multicast-Datenverkehr erstellt wurde, und die **McRef** zeigt die Anzahl der Access Points, die der Gruppe beigetreten sind. Diese Informationen sind hilfreich, wenn Sie überprüfen müssen, ob ein WAP, der den Multicast-Datenverkehr nicht empfängt, der Multicast-Gruppe beigetreten ist.

4. Geben Sie den Befehl **show int capwap 0 ein**, um zu überprüfen, ob die Tunnelschnittstelle die Zieladresse als Multicast-Gruppenadresse anzeigt:

```
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. Geben Sie den Befehl **show wireless multicast group summary** ein, um zu überprüfen, ob ein MGID-Eintrag für die Multicast-Gruppe erstellt wird, der der Client beitreten möchte (**239.255.255.250** wird in diesem Beispiel verwendet):

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

6. Geben Sie diesen Befehl ein, um zu überprüfen, ob der betreffende Client der MGID-Tabelle hinzugefügt wurde:

```
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. Geben Sie diesen Befehl ein, um zu überprüfen, ob der MGID-Eintrag dem Access Point für diesen Client hinzugefügt wurde:

```
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
```

Hinweis: Berücksichtigen Sie die Zähler für die empfangenen und übertragenen Pakete. Diese Informationen sind nützlich, wenn Sie ermitteln möchten, ob der Access Point die Pakete ordnungsgemäß an den Client weiterleitet.

8. Geben Sie den Befehl **show ip igmp snooping igmpv2-tracking ein**, um alle Client-Multicast-Gruppenzuordnungen anzuzeigen. Diese enthält einen Snapshot der Clients, die verbunden sind, sowie der Gruppen, denen sie beigetreten sind. Hier eine Beispielausgabe:

```
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. Geben Sie diesen Befehl ein, um die MGID vom Controller zu überprüfen:

```
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)
-----------------------------------------------------------
```

Fehlerbehebung

Im Folgenden finden Sie eine Liste von **Debug-**Befehlen, die Sie verwenden können, um Konfigurationsprobleme vom Controller zu beheben:

- **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**
- **debuggen ip igmp snoop wireless ios events**
- **debuggen ip igmp snoop wireless ios fehler**
- **debuggen ip igmp snoop wireless ap detail**
- **debuggen ip igmp snoop wireless ap fehler**
- **debuggen ip igmp snoop wireless ap event**
- **debuggen ip igmp snoop wireless ap meldung**
- **Debug-Plattform Multicast**
- **Multicast-Fehler der Debug-Plattform**
- **Debug-Plattform-Multicast-Ereignis**
- **Debug-Plattform l2m-igmp/l2m-mld/l2multicast/l3multicast**
- **debug l2mcast wireless ios fehler**
- **debug l2mcast wireless ios mgid**
- **debug l2mcast wireless ios spi**

  Hinweis: Stellen Sie sicher, dass Sie nur die relevanten Multicast-**Debug-**Befehle verwenden, um Leistungsprobleme zu vermeiden.

Im Folgenden finden Sie ein Beispiel für die Ausgabe des **Debug-**Befehls:

```
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
```

Die folgende Beispielausgabe zeigt die MGID-Erstellung auf dem 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
```

Nachdem der Eintrag auf der Cisco IOS®-Seite erstellt wurde, wird er an den WCM-Prozess (Wireless Control Module) übergeben, der überprüft, bevor der Eintrag hinzugefügt wird:

```
*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
```

Im Folgenden finden Sie eine Liste von **Debug-**Befehlen, mit denen Sie Konfigurationsprobleme vom Access Point aus beheben können:

- **Debug Capwap mcast fwd**
- **Debug Capwap-mcast-Abfrage**

Im Folgenden finden Sie ein Beispiel für **die** Ausgabe eines **Debugbefehls**:

```
*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 .!!
```

> **Hinweis**: Beim Hinzufügen des MGID-Eintrags wird die VLAN-ID in der vorherigen Ausgabe **als 0** angezeigt. Obwohl der Eintrag gelöscht wird, wird die richtige VLAN-Zuordnung angezeigt.

Im Folgenden finden Sie eine Liste von **show**-Befehlen, die Sie für weitere Analysen vom Controller verwenden können:

- **Zusammenfassung der Wireless-Clients anzeigen**
- **show wcdb database all**
- **Zusammenfassung der Wireless-Multicast-Gruppe anzeigen**

- **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**

Im Folgenden finden Sie eine Liste von **show**-Befehlen, die Sie für weitere Analysen vom Access Point verwenden können:

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

Wichtige Überlegungen

Im Folgenden sind einige wichtige Überlegungen und Einschränkungen hinsichtlich der Konfiguration aufgeführt, die in diesem Dokument beschrieben wird:

- Die Anzahl der Multicast-Gruppen, denen jeder Client zuhören kann, ist auf 16 begrenzt. Sobald der Client die *Join*-Anforderung mit der 17. Gruppe sendet, wird die Join-Anforderung auf der Seite von Cisco IOS erstellt, die WCM-Seite sendet jedoch eine *Deny*-Nachricht an Cisco IOS. Letztere löscht diese Gruppe.
- Derzeit wird nur IGMP Version 2 (V2) unterstützt. Wenn ein Client IGMP Version 3 (V3) verwendet, erfolgt die Erstellung der MGID nicht auf dem Controller. Aus diesem Grund ist die Quelladresse in der Quelle, Gruppe und im VLAN immer **0.0.0.0**.
- Die Anzahl der L3-MGIDs, die vom NGWC zwischen 4.160 und 8.191 unterstützt werden. Da ein MGID-Eintrag eine Kombination aus der Multicast-Adresse und dem VLAN ist, können nur 4.000 solcher Kombinationen vorhanden sein. Dies kann in großen Umgebungen eine Einschränkung darstellen.
- Die *Bonjour*-Funktion für VLANs wird nicht unterstützt. Dies liegt daran, dass die IP-Adresse 224.0.0.251 eine lokale Multicast-Adresse ist. Die Cisco WLCs der Serien 5760 und 3850 führen wie alle anderen Catalyst Switches keine Link-Local-Adressen aus. Aus diesem Grund wird die folgende Fehlermeldung angezeigt:

```
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.
```