

# 配置在5760和3850系列WLCs的无线组播

## 目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[配置](#)

[组播在NGWC的流](#)

[验证](#)

[故障排除](#)

[重要考虑事项](#)

## 简介

本文描述如何配置在Cisco 5760和3850系列无线局域网控制器(WLCs)的无线组播，支持与单播的组播并且用组播交付机制组播。

## [先决条件](#)

### [要求](#)

Cisco建议您有组播实施基础知识在Cisco 5760和3850系列WLCs的。

### 使用的组件

本文档中的信息基于以下软件和硬件版本：

- Cisco 5760系列WLC
- Cisco 3850系列WLC
- Cisco 3602系列接入点(AP)。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

## 配置

完成这些步骤为了启用在下一代配线间(NWGC)平台的组播：

1. 输入**无线multicast命令**为了启用在控制器的组播：

`ish_5760(config)#wireless multicast`**注意**：默认情况下此命令启用**组播用单播**交付机制。

2. 如果必须更换交付机制**组播与组播**，则请输入此命令：

`ish_5760(config)#ap capwap multicast 239.255.255.249`**注意**：此命令配置所有无线接入点的组播组(CAPWAP) AP加入控制和供应，优化交换机，以便传送到所有AP的组播CAPWAP信息。此进程不同的，当使用时单播模式，因为交换机然后将要求传送单播信息到所有CAPWAP AP。这帮助最小化在控制器的系统负载。随意地，您能导航到从GUI的**Configuration>控制器**为了配置此信息，如显示此处：

3. 输入这些命令为了启用在控制器的互联网组管理协议(IGMP)窥探默认情况下(启用)：

```
ip igmp snooping
```

```
ip igmp snooping querier
```

**注意**：ip igmp snooping querier命令配置控制器，以便周期地证实客户端是否仍然听组播数据流。

## 在NGWC的组播流

当先前配置实现时，这些步骤概述组播数据流的流在NGWCs的：

1. 控制器截断由无线客户端发送的IGMP信息包。
2. 如果该组播组VLAN来源组合的客户端条目存在，则控制器更新IGMP计时器。

如果这是一个新的条目，则WLC创建根据(来源，组，VLAN)元组(MGID)的组播组标识符，与范围在1和4,095之间Layer2的(L2)或在4,160和8,191之间第3层的(L3)。

3. IGMP信息包是转发的上行。
4. MGID条目发送对AP，与客户端关联信息一起，以便客户端能收到组播数据流。
5. 基于交付机制(与单播/组播的组播)，控制器寄流量给AP适当地。**注意**：如果交付机制是组播，则数据报传输传送层安全(DTL)加密和服务质量(QoS)标记没有应用。
6. AP然后寄流量给每个客户端，如所需求。

## 验证

完成这些步骤为了验证您的配置适当地工作：

1. 输入**显示无线multicast命令**为了验证组播是否正确地启用：

```
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. 输入显示capwap总和命令为了验证CAPWAP信息：

```
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注意：如输出所显示，Ca1接口使用AP组播模式。而Ca19接口有DTL值是，Ca1接口有DTL值没有。

## 3. 输入显示capwap详细信息或显示capwap摘要为了验证加入组播组的AP数：

```

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
<b>Ca0</b>	<b>10.105.132.138</b>	<b>5247</b>	<b>239.255.255.249</b>	<b>5247</b>	<b>No</b>	<b>1464</b>

```

Name IfId McastRef
-----
Ca2 0x0098BA0000000041 0
Ca1 0x00BC2C800000003D 0

```

```
Ca0 0x008B53C000000001
```

2注意：此输出最后一行指向为组播数据流创建的CAPWAP隧道接口，并且McastRef显示加入组的AP数。此信息是有用，当不收到组播数据流的您必须证实时AP是否加入组播组。

## 4. 输入show int capwap 0命令为了验证隧道接口显示目的地址作为组播组地址：

```

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. 输入summary命令显示无线的组播组为了验证MGID条目是否为组播组创建客户端尝试加入(239.255.255.250用于此示例) :

```
ish_5760#show wireless multicast group summary
IPv4 groups
```

```
-----
MGID   Source   Group           Vlan
-----
4160   0.0.0.0   239.255.255.250 32
```

6. 输入此命令为了验证有问题的客户端是否被添加了到MGID表 :

```
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. 输入此命令为了验证MGID条目是否在此客户端的AP被添加了 :

```
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 **注意** : 考虑在已接收和已传输数据包的计数器。此信息是有用的, 当您尝试确定时AP是否适当地转发数据包给客户端。

8. 输入show ip igmp snooping igmpv2-tracking命令为了查看所有客户端组播组映射。他们加入的这提供连接客户端的快照和组。以下为示例输出 :

```
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. 输入此命令为了验证从控制器的MGID :

```
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 bcst 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)
```

-----

## 故障排除

这是的调试指令列表您能使用为了排除故障从控制器的配置问题 :

- 监听的debug ip igmp
- debug ip igmp监听的239.255.255.250
- debug ip igmp探测询问器
- debug ip igmp监听无线ios客户端跟踪
- debug ip igmp监听无线ios事件
- debug ip igmp监听无线ios错误

- debug ip igmp监听无线ap详细信息
- debug ip igmp监听无线ap错误
- debug ip igmp监听无线ap事件
- debug ip igmp监听无线ap消息
- 调试平台组播
- 调试平台组播错误
- 调试平台组播事件
- 调试平台l2m-igmp/l2m-mld/l2multicast/l3multicast
- 调试l2mcast无线ios错误
- 调试l2mcast无线ios mgid
- 调试l2mcast无线ios spi

注意：保证您只使用相关组播调试指令为了避免性能问题。

这是示例show debug命令输出：

```

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

这是显示在控制器的MGID创建的示例输出：

```
*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: (l2mcastn_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
```

一旦条目在Cisco IOS创建支持，这通过对无线控制模块(WCM)进程，验证，在添加条目前：

```
*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
```

这是的调试指令列表您能使用为了排除故障从AP的配置问题：

- 调试capwap mcast fwd

- 调试capwap mcast查询

这是示例debug命令的输出：

```
*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 .!!
```

注意：当MGID条目被添加时，VLAN ID显示作为0在上一个输出中。然而，即使条目删除，它显示正确VLAN映射。

这是列表表示命令，您能使用从控制器的进一步分析：

- 显示无线客户端摘要
- 显示wcdb数据库全部
- 显示无线组播组摘要
- 显示无线组播组<ip> VLAN <id>
- 显示无线组播源<ip>组<ip> VLAN <id>
- show ip igmp snooping无线mgid
- show ip igmp snooping igmpv2-tracking

这是列表表示命令，您能使用从AP的进一步分析：

- 显示capwap mcast mgid全部
- 显示capwap mcast mgid id <id>

## 重要考虑事项

这是一些重要考虑事项和限制关于在本文描述的配置：

- 每个客户端能侦听组播组的数量被限制到16。一旦客户端发送与第17组的加入请求，创建在Cisco IOS发生支持，但是WCM侧传送拒绝信息对Cisco IOS。后者然后删除该组。
- 目前，支持仅IGMP版本2 (V2)。如果客户端使用IGMP版本3 (V3)，则MGID创建在控制器不发生。为此，在来源、组和VLAN，源地址总是0.0.0.0。
- 从4,160的NGWC范围支持到8,191 L3 MGIDs的数量。因为MGID条目是组播地址和VLAN的组



合，只可以有4,000个这样组合。这也许是在大环境的一个限制。

- 不支持在VLAN间的*Bonjour*功能。这是因为IP地址224.0.0.251是链路本地组播地址。Cisco 5760和3850系列WLCs，类似其他Catalyst交换机，不监听链路本地地址。为此，您将看到此错误消息出现：

```
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.
```