

# Configurar o Multicast wireless no 5760 e 3850 Series WLC

## Índice

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Configurar](#)

[Fluxo do Multicast em NGWC](#)

[Verificar](#)

[Troubleshooting](#)

[Considerações importantes](#)

## Introdução

Este documento descreve como configurar o Multicast wireless nos controladores do Wireless LAN do Cisco e Series (WLC), que apoiam o *Multicast com unicast* e o *Multicast com mecanismos de entrega do Multicast*.

## Pré-requisitos

### Requisitos

Cisco recomenda que você tem o conhecimento básico da aplicação do Multicast no Cisco e Series WLC.

### Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

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

As informações neste documento foram criadas a partir de dispositivos em um ambiente de

laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

## Configurar

Termine estas etapas a fim permitir o Multicast nas Plataformas do armário de fiação da próxima geração (NWGC):

1. Inscreva o **comando multicast wireless** a fim permitir o Multicast no controlador:

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

Nota: Este comando permite à revelia o *Multicast com* mecanismo de entrega do *unicast*.

2. Se você deve mudar o mecanismo de entrega ao *Multicast com Multicast*, a seguir incorpore este comando:

```
ish_5760(config)#ap capwap multicast 239.255.255.249
```

Nota: Este comando configura o grupo de transmissão múltipla a que todo o controle e abastecimento dos pontos de acesso Wireless (CAPWAP) AP se juntam, que aperfeiçoa o interruptor de modo que envie uma mensagem do Multicast CAPWAP que alcance todos os AP. Este processo é diferente quando o modo de Unicast é usado, porque o interruptor estaria exigido então para enviar mensagens do unicast a todo o CAPWAP AP. Isto ajuda a minimizar a carga de sistema no controlador. Opcionalmente, você pode navegar à **configuração > ao controlador do GUI** a fim configurar esta informação, como mostrado aqui:



3. Incorpore estes comandos a fim permitir a verificação do Protocolo de Gerenciamento do Grupo da Internet (IGMP) no controlador (permitido à revelia):

```
ip igmp snooping
```

```
ip igmp snooping querier
```

Nota: O comando **ip igmp snooping querier** configura o controlador de modo que verifique periodicamente se um cliente ainda escute o tráfego multicast.

## Fluxo do Multicast em NGWC

Estas etapas esboçam o fluxo do tráfego multicast no NGWCs quando a configuração precedente é executada:

1. O controlador intercepta os pacotes de IGMP que são enviados pelos clientes Wireless.
2. Se a entrada de cliente para essa combinação da grupo-VLAN-fonte do Multicast existe, então o controlador atualiza os temporizadores IGMP.  
  
Se esta é uma entrada nova, a seguir o WLC cria um identificador do grupo de transmissão múltipla (MGID) baseado (fonte, grupo, VLAN) na tupla, com a escala entre 1 e 4,095 para a camada 2 (L2) ou entre 4,160 e 8,191 para a camada 3 (L3).
3. O pacote de IGMP é enviado rio acima.
4. A entrada MGID é enviada ao AP, junto com a informação da associação de cliente de modo que o cliente possa receber o tráfego multicast.
5. Baseado no mecanismo de entrega (Multicast com unicast/Multicast), o controlador para a frente o tráfego ao AP apropriadamente. Nota: Se o mecanismo de entrega é Multicast, a seguir a criptografia da Segurança da camada de transporte de datagram (DTL) e a marcação do Qualidade de Serviço (QoS) não são aplicadas.
6. O AP então para a frente o tráfego a cada cliente, como necessário.

## Verificar

Termine estas etapas a fim verificar que sua configuração trabalha corretamente:

1. Inscreva o **comando multicast wireless da mostra** a fim verificar se o Multicast esteve permitido corretamente:

```
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. Incorpore o comando da **soma do capwap da mostra** a fim verificar a informação CAPWAP:

```
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 3Nota: Segundo as indicações da saída, a relação **Ca1** é usada para o modo do Multicast AP. A relação **Ca1** tem um valor *DTL do nenhum*, quando a relação **Ca19** tiver um valor *DTL de sim*.

3. Incorpore o **detalhe do capwap da mostra** ou o **sumário do capwap da mostra** a fim verificar o número de AP que se juntaram ao grupo de transmissão múltipla:

```
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 2Nota: A última linha desta saída aponta à interface de túnel CAPWAP que foi criada para o tráfego multicast, e o **McastRef** mostra o número de AP que se juntaram ao grupo. Esta informação é útil quando você deve verificar se um AP que não receba o tráfego multicast se junte ao grupo de transmissão múltipla.

4. Inscreva o **comando 0 do capwap int da mostra** a fim verificar que a interface de túnel mostra o endereço de destino como o endereço de grupo de transmissão múltipla:

```
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. Inscreva o **comando summary wireless do grupo de transmissão múltipla da mostra** a fim verificar se uma entrada MGID está criada para o grupo de transmissão múltipla a que o cliente tenta se juntar (**239.255.255.250** é usado neste exemplo):

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

6. Incorpore este comando a fim verificar se o cliente na pergunta esteve adicionado à tabela MGID:

```
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. Incorpore este comando a fim verificar se a entrada MGID esteve adicionada no AP para este cliente:

```
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
```

Nota: Considere os contadores na recebida e nos pacotes transmitido. Esta informação é útil quando você tenta determinar se o AP corretamente para a frente os pacotes ao cliente.

8. Incorpore o comando do **IGMP Snooping igmpv2-tracking da mostra IP** a fim ver todos os mapeamentos do grupo do cliente-Multicast. Isto fornecem um instantâneo dos clientes que são conectados e os grupos a que se juntou. Está aqui um exemplo de saída:

```
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. Incorpore este comando a fim verificar o MGID do controlador:

```
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)
```

```
-----
```

## Troubleshooting

Está aqui uma lista de **comandos debug** que você pode usar a fim pesquisar defeitos problemas de configuração do controlador:

- debugar o IGMP Snooping IP
- debugar o IGMP Snooping 239.255.255.250 IP
- debugar o formador de fila do IGMP Snooping IP
- debugar o cliente-seguimento ios do Sem fio da espião do igmp IP
- debugar eventos wireless ios da espião do igmp IP
- debugar o erro wireless ios da espião do igmp IP
- debugar o detalhe wireless ap da espião do igmp IP
- debugar o erro wireless ap da espião do igmp IP
- debugar o evento wireless ap da espião do igmp IP

- debugar a mensagem wireless ap da espião do igmp IP
- debugar o Multicast da plataforma
- debugar o erro do Multicast da plataforma
- debugar o evento do Multicast da plataforma
- debugar a plataforma l2m-igmp/l2m-mld/l2multicast/l3multicast
- debugar o erro wireless ios l2mcast
- debugar o mgid wireless ios l2mcast
- debugar o spi wireless ios l2mcast

Nota: Assegure-se de que você use somente os **comandos debug** relevantes do Multicast a fim evitar problemas de desempenho.

Está aqui um **comando show debug** do exemplo 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

```

Estão aqui umas saídas de exemplo que mostrem a criação MGID no controlador:

```

*Sep 7 00:12:11.029: IGMP SN: Received IGMPv2 Report for group 239.255.255.250 received
on Vlan 32, port Ca1
*Sep 7 00:12:11.029: IGMP SN: 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: (l2mcast_wireless_alloc_mcast_mgid) 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: IGMP SN
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: IGMP SN
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

```

Uma vez que a entrada é criada no lado do <sup>®</sup>do Cisco IOS, esta está passada ao processo wireless do módulo de controle (WCM), que verifica antes que adicione a entrada:

```

*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: mschApMac = 0c85.25c7.9ad0
client_mac_addr = 1410.9fef.272c slotId = 1 vapId = 1 mgid = 4160 numOfSGs = 2,
rrc_status = 2

```

Está aqui uma lista de comandos debug que você pode usar a fim pesquisar defeitos problemas de configuração do AP:

- debugar o mcast fwd do capwap
- debugar a pergunta do mcast do capwap

Está aqui um comando debug do exemplo:



```
*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 .!!
```

Nota: Quando a entrada MGID for adicionada, o ID de VLAN mostra como **0** na saída precedente. Contudo, mesmo que a entrada seja suprimida, mostra o mapeamento correto VLAN.

Está aqui uma lista de **comandos show** que você pode usar a análise mais aprofundada do controlador:

- mostre o sumário do cliente Wireless
- mostre o base de dados todo do wcdb
- mostre o sumário wireless do grupo de transmissão múltipla
- mostre a <ip> wireless do grupo de transmissão múltipla o <id> vlan
- mostre a <ip> wireless do grupo do <ip> do origem de transmissão múltipla o <id> vlan
- mostre o mgid do Sem fio do IGMP Snooping IP
- mostre o IGMP Snooping igmpv2-tracking IP

Está aqui uma lista de **comandos show** que você pode usar a análise mais aprofundada do AP:

- mostre o mgid todo do mcast do capwap
- mostre o <id> identificação do mgid do mcast do capwap

## Considerações importantes

Estão aqui algumas considerações e limitações importantes com respeito à configuração que é descrita neste documento:

- O número de grupos de transmissão múltipla que cada cliente pode escutar é limitado a 16. Uma vez que o cliente envia o pedido da *junta* com o 17o grupo, a criação ocorre no lado do Cisco IOS, mas o lado WCM envia uma mensagem da *negação ao* Cisco IOS. As supressões dos últimos então que agrupam.
- Atualmente, somente o Versão 2 do IGMP (V2) é apoiado. Se um cliente usa o Versão 3 do IGMP (V3), a seguir a criação MGID não ocorre no controlador. Por este motivo, na fonte, no grupo, e no VLAN, o endereço de origem é sempre 0.0.0.0.

- O número de L3 MGIDs que é apoiado na escala NGWC de 4,160 a 8,191. Desde que uma entrada MGID é uma combinação do endereço de multicast e do VLAN, pode haver somente 4,000 tais combinações. Esta pôde ser uma limitação em grandes ambientes.
- A característica de *Bonjour* através dos VLAN não é apoiada. Isto é porque o endereço IP 224.0.0.251 é um endereço de multicast do link local. O Cisco e Series WLC, como nenhum outro Catalyst Switch, não faz endereços locais de link da espiação. Por este motivo, você verá este Mensagem de Erro aparecer:

```
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.
```