

Multicast inalámbrico de la configuración en el WLCs de las 5760 y 3850 Series

Contenido

[Introducción](#)

[prerrequisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Configurar](#)

[Flujo del Multicast en NGWC](#)

[Verificación](#)

[Troubleshooting](#)

[Consideraciones importantes](#)

Introducción

Este documento describe cómo configurar el Multicast inalámbrico en los reguladores del Wireless LAN de las Cisco y Series (WLCs), que soportan el *Multicast con el unicast* y el *Multicast con los mecanismos de entrega del Multicast*.

Prerrequisitos

Requisitos

Cisco recomienda que usted tiene conocimiento básico de la implementación del Multicast en el WLCs de las Cisco y Series.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- WLC de las Cisco 5760 Series
- WLC de las Cisco 3850 Series
- Punto de acceso de las Cisco 3602 Series.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Configurar

Complete estos pasos para habilitar el Multicast en las Plataformas del Wiring Closet de la última generación (NWGC):

1. Ingrese el **comando multicast sin hilos** para habilitar el Multicast en el regulador:

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

Nota: Este comando por abandono habilita el *Multicast con el mecanismo de entrega del unicast*.

2. Si usted debe cambiar el mecanismo de entrega al *Multicast con el Multicast*, después ingrese este comando:

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

Nota: Este comando configura al grupo de multidifusión a quien todo el control y aprovisionamiento de los grupos de acceso de red inalámbrica (CAPWAP) los AP se unen a, que optimiza el Switch de modo que envíe un mensaje del Multicast CAPWAP que alcance todos los AP. Este proceso es diferente cuando utilizan al modo unidifusión, pues el Switch entonces sería requerido para enviar los mensajes del unicast a todo el CAPWAP AP. Esto ayuda a minimizar la carga del sistema en el regulador. Opcionalmente, usted puede navegar a la **configuración > al regulador del GUI** para configurar esta información, como se muestra aquí:

3. Ingrese estos comandos para habilitar el snooping del Internet Group Management Protocol (IGMP) en el regulador (habilitado por abandono):

```
ip igmp snooping
```

```
ip igmp snooping querier
```

Nota: El comando **ip igmp snooping querier** configura el regulador de modo que marque periódicamente si un cliente todavía escucha el tráfico Multicast.

Flujo del Multicast en NGWC

Estos pasos delimitan el flujo del tráfico Multicast en el NGWCs cuando se implementa la configuración previa:

1. El regulador intercepta los paquetes IGMP que son enviados por los clientes de red inalámbrica.
2. Si existe la entrada del cliente para esa combinación de la grupo-VLAN-*fuentes del Multicast*, entonces el regulador pone al día los temporizadores IGMP.

Si esto es una nueva entrada, después el WLC crea un identificador del grupo de

multidifusión (MGID) basado en (fuente, grupo, VLA N) el tuple, con el rango entre 1 y 4,095 para la capa 2 (L2) o entre 4,160 y 8,191 para la capa 3 (L3).

3. El paquete IGMP se remite la conexión en sentido ascendente.
4. La entrada MGID se envía al AP, junto con la información de la asociación del cliente de modo que el cliente pueda recibir el tráfico Multicast.
5. De acuerdo con el mecanismo de entrega (Multicast con el unicast/Multicast), el regulador adelante el tráfico al AP apropiadamente. Nota: Si el mecanismo de entrega es Multicast, después el cifrado de la Seguridad de la capa de transporte de datagrama (DTL) y el marcado del Calidad de Servicio (QoS) no son aplicados.
6. El AP entonces adelante el tráfico a cada cliente, como sea necesario.

Verificación

Complete estos pasos para verificar que su configuración trabaja correctamente:

1. Ingrese el **comando multicast sin hilos de la demostración** para verificar si el Multicast se ha habilitado correctamente:

```
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. Ingrese el comando de la **suma del capwap de la demostración** para verificar la información 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: Tal y como se muestra en de la salida, la interfaz **Ca1** se utiliza para el modo del Multicast AP. La interfaz **Ca1** tiene un valor *DTL de ningún*, mientras que la interfaz **Ca19** tiene un valor *DTL de sí*.

3. Ingrese el **detalle del capwap de la demostración** o el **resumen del capwap de la demostración** para verificar el número de AP que se han unido a al grupo de multidifusión:

```
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: La línea más reciente de esta salida señala a la interfaz del túnel CAPWAP que fue creada para el tráfico Multicast, y el **McastRef** muestra el número de AP que se han unido a al grupo. Esta información es útil cuando usted debe marcar si un AP que no recibe el tráfico Multicast se ha unido a al grupo de multidifusión.

4. Ingrese el **comando 0 del capwap de la demostración internacional** para verificar que la interfaz del túnel muestra a la dirección destino como la dirección de grupo de multidifusión:

```
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. Ingrese el **comando summary sin hilos del grupo de multidifusión de la demostración** para verificar si una entrada MGID está creada para el grupo de multidifusión que el cliente intenta unirse a (**239.255.255.250** se utiliza en este ejemplo):

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

6. Ingrese este comando para verificar si han agregado al cliente en la pregunta a la tabla 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. Ingrese este comando para verificar si la entrada MGID se ha agregado en el 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 los contadores en haber recibido y los paquetes transmitidos. Esta información es útil cuando usted intenta determinar si el AP correctamente adelanta los paquetes al cliente.

8. Ingrese el comando del IGMP Snooping igmpv2-tracking del IP de la demostración para ver todos los mappings del grupo del cliente-Multicast. El proporciona una foto de los clientes que están conectados y los grupos que se han unido a. Éste es un ejemplo de salida:

```
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. Ingrese este comando para verificar el MGID del regulador:

```
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 Stdbby 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

Aquí está una lista de **comandos debug** que usted pueda utilizar para resolver problemas los problemas de configuración del regulador:

- **IGMP Snooping del IP del debug**
- **IGMP Snooping 239.255.255.250 del IP del debug**
- **querier del IGMP Snooping del IP del debug**
- **cliente-seguimiento IOS de la Tecnología inalámbrica del fisgón del igmp del IP del debug**
- **eventos inalámbricos IOS del fisgón del igmp del IP del debug**
- **error inalámbrico IOS del fisgón del igmp del IP del debug**
- **detalle inalámbrico ap del fisgón del igmp del IP del debug**
- **error inalámbrico ap del fisgón del igmp del IP del debug**
- **evento inalámbrico ap del fisgón del igmp del IP del debug**
- **mensaje inalámbrico ap del fisgón del igmp del IP del debug**
- **Multicast de la plataforma del debug**
- **error del Multicast de la plataforma del debug**
- **evento del Multicast de la plataforma del debug**

- plataforma l2m-igmp/l2m-mld/l2multicast/l3multicast del debug
- error inalámbrico IOS del debug l2mcast
- mgid inalámbrico IOS del debug l2mcast
- spi inalámbrico IOS del debug l2mcast

Nota: Asegúrese de que usted utilice solamente los **comandos debug** relevantes del Multicast para evitar los problemas de rendimiento.

Aquí está un **comando show debug** del ejemplo hecho salir:

```
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
```

Aquí está una salida de ejemplo que muestra la creación MGID en el regulador:

```
*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: (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: IGMP SN

Client-address: 192.168.24.50 (S,G,V): 0.0.0.0 239.255.255.250 32 Port: Cal, 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: Cal, 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

Una vez que la entrada se crea en el lado del [®]del Cisco IOS, esto se pasa al proceso inalámbrico del módulo de control (WCM), que verifica antes de que agregue la 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 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

Aquí está una lista de **comandos debug** que usted pueda utilizar para resolver problemas los problemas de configuración del AP:

- **mcast fwd del capwap del debug**

- **interrogación del mcast del capwap del debug**

Aquí está un resultado del comando de debug del ejemplo:

*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: Mientras que se agrega la entrada MGID, el VLAN ID muestra como 0 en la salida anterior. Sin embargo, aunque se borra la entrada, muestra la asignación correcta del VLAN.

Aquí está una lista de comandos **show** que usted pueda utilizar el análisis adicional del regulador:

- muestre el resumen del cliente de red inalámbrica
- muestre la base de datos toda del wcdb
- muestre el resumen inalámbrico del grupo de multidifusión
- muestre a <ip> inalámbrico del grupo de multidifusión el <id> vlan
- muestre a <ip> inalámbrico del grupo del <ip> del origen de multidifusión el <id> vlan
- muestre el mgid de la Tecnología inalámbrica del IGMP Snooping del IP
- muestre el IGMP Snooping igmpv2-tracking del IP

Aquí está una lista de comandos **show** que usted pueda utilizar el análisis adicional del AP:

- muestre el mgid todo del mcast del capwap
- muestre el <id> identificación del mgid del mcast del capwap

Consideraciones importantes

Aquí están algunas consideraciones y limitaciones importantes con respecto a la configuración que se describe en este documento:

- El número de grupos de multidifusión quienes cada cliente pueda escuchar se limita a 16. Una vez que el cliente envía la petición del *unido* con el 17mo grupo, la creación ocurre en el lado del Cisco IOS, pero el lado WCM envía un mensaje de la *negación al Cisco IOS*. Este último entonces borra a ese grupo.
- Actualmente, solamente se soporta el IGMP versión 2 (V2). Si un cliente utiliza el IGMP versión 3 (v3), después la creación MGID no ocurre en el regulador. Por este motivo, en la fuente, el grupo, y el VLAN, la dirección de origen es siempre 0.0.0.0.
- El número de L3 MGIDs que se soporta en el rango NGWC a partir del 4,160 a 8,191. Puesto que una entrada MGID es una combinación de la dirección Multicast y del VLAN, puede haber solamente 4,000 tales combinaciones. Esto pudo ser una limitación en los entornos grandes.
- La característica de *Bonjour* a través de los VLAN no se soporta. Esto es porque la dirección IP 224.0.0.251 es una dirección Multicast del local de la conexión. El WLCs de las Cisco y Series, como ningún otro switch de Catalyst, no hace las direcciones locales del link del

figón. Por este motivo, usted verá este mensaje de error 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.
```