

Configuración de multidifusión con controladores de LAN inalámbrica (WLC) y puntos de acceso (CAPWAP)

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Multidifusión en WLC](#)

[Comportamiento de Broadcast en Diferentes WLC](#)

[Detección de IGMP en WLC](#)

[Roaming de multidifusión inalámbrica](#)

[Pautas para Utilizar el Modo Multicast](#)

[Configuración de la red](#)

[Configurar](#)

[Configuración de la red inalámbrica para multidifusión](#)

[Configuración de WLAN para clientes](#)

[Configuración del modo multidifusión mediante la GUI](#)

[Configuración del modo multidifusión mediante la CLI](#)

[Configuración de la red por cable para multidifusión](#)

[Verificación y resolución de problemas](#)

[Información Relacionada](#)

Introducción

Este documento describe cómo configurar Wireless LAN Controllers (WLCs) y Lightweight Access Points (LAPs) para multicast.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Conocimiento básico de la configuración de AP y Cisco WLC
- Conocimientos sobre cómo configurar el routing y la multidifusión básicos en una red por cable

Asegúrese de cumplir estos requisitos antes de intentar esta configuración.

Componentes Utilizados

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

- Cisco 3504 WLC que ejecuta firmware versión 8.5
- Cisco 3702 Series LAP
- Cliente inalámbrico Microsoft Windows 10 con adaptador Intel(R) Wireless-AC 8265 de doble banda
- Switch Cisco 6500 que ejecuta Cisco IOS® Software Release 12.2(18)
- Dos switches Cisco serie 3650 que ejecutan la versión 16.3.7 del software Cisco IOS

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. Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Multidifusión en WLC

Si su red admite la multidifusión de paquetes, puede configurar el método de multidifusión que utiliza el controlador para transportar los paquetes de multidifusión a través de CAPWAP a todos o varios puntos de acceso al mismo tiempo. El controlador realiza la multidifusión en dos modos:

- Modo de unidifusión: en este modo, el controlador unidifusión cada paquete de multidifusión a cada AP asociado con el controlador. Este modo no es eficaz, pero puede ser necesario en redes que no admiten multidifusión.
- Modo de multidifusión: en este modo, el controlador envía paquetes de multidifusión a un grupo de multidifusión CAPWAP. Este método reduce la sobrecarga en el procesador del controlador y traslada el trabajo de replicación de paquetes a su red, que es mucho más eficiente que el método unicast. Cuando utiliza una VLAN/subred diferente para el AP y el WLC, el ruteo multicast es obligatorio en el lado cableado para soportar el reenvío del paquete de multidifusión CAPWAP del link descendente del WLC al AP.

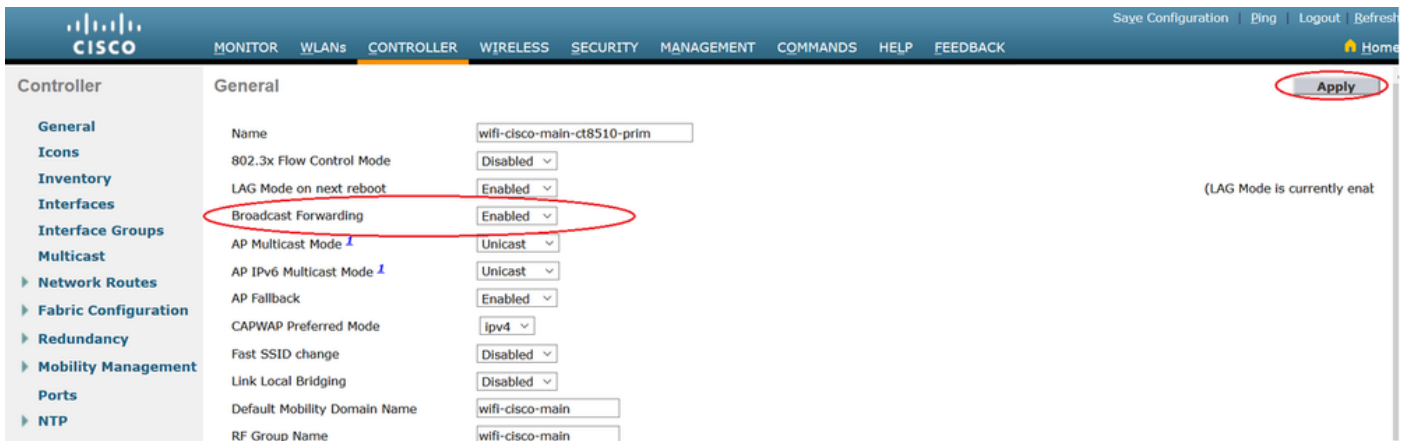
Cuando habilita el modo multicast y el controlador recibe un paquete multicast de la LAN cableada, el controlador encapsula el paquete con el uso de CAPWAP y reenvía el paquete a la dirección del grupo multicast CAPWAP. El controlador siempre utiliza la interfaz de administración para enviar paquetes multicast. Los puntos de acceso en el grupo multicast reciben el paquete y lo reenvían a todos los BSSID asignados a la interfaz en la que los clientes reciben tráfico multicast. Desde la perspectiva del punto de acceso, la multidifusión parece difundir a todos los SSID.

Comportamiento de Broadcast en Diferentes WLC

De forma predeterminada, el WLC no reenvía ningún paquete de difusión (como el tráfico Upnp) a menos que se habilite el reenvío de difusión. Ejecute este comando desde la CLI del WLC para habilitar la difusión:

```
config network broadcast enable
```

O habilitarlo con la GUI:



La difusión utiliza el **multicast mode** que se configura en el WLC, incluso si el multicast no está encendido. Esto se debe a que no puede establecer la dirección IP ni el modo a menos que habilite la multidifusión en la GUI. Por lo tanto, si el modo multicast es unicast y el broadcast está encendido, éste es el modo que el broadcast utiliza (el tráfico del broadcast se replica en el WLC y el unicast a cada AP). Si el modo multicast se configura en multicast con una dirección multicast, entonces el broadcast utiliza este modo (cada paquete de broadcast se envía a través del grupo multicast a los AP).

Nota: Hasta la versión 7.5, el número de puerto utilizado para la multidifusión CAPWAP era 12224. A partir de la versión 7.6, el número de puerto utilizado para CAPWAP se cambia a 5247.

La versión 4.2 y posteriores del Wireless LAN Controller admiten la multidifusión con anulación de AAA. Debe habilitar la indagación IGMP en el controlador para que la multidifusión funcione con la invalidación AAA.

Detección de IGMP en WLC

El snooping del protocolo de administración de grupos de Internet (IGMP) se admite en el WLC para dirigir mejor los paquetes de multidifusión. Cuando se habilita esta función, el controlador recopila los informes IGMP de los clientes, procesa los informes, crea ID de grupo multicast (MGID) únicos a partir de los informes IGMP después de verificar la dirección multicast de Capa 3 y el número de VLAN, y envía los informes IGMP al switch de infraestructura. El controlador envía estos informes con la dirección de origen como la dirección de interfaz en la que recibió los informes de los clientes.

El controlador luego actualiza la tabla MGID del punto de acceso en el AP con la dirección MAC del cliente. Cuando el controlador recibe tráfico multicast para un grupo multicast determinado, lo reenvía a todos los AP. Sin embargo, solamente los AP que tienen clientes activos que escuchan o suscribieron a ese grupo multicast envían tráfico multicast en esa WLAN particular. Los paquetes IP se reenvían con un MGID que es único para una VLAN de ingreso y el grupo multicast de destino. Los paquetes multicast de Capa 2 se reenvían con un MGID que es único para la interfaz de ingreso.

El controlador admite la detección de escucha multidifusión (MLD) v1 para multidifusión IPv6. Esta función realiza un seguimiento de los flujos de multidifusión IPv6 y los envía a los clientes que los solicitan. Para admitir la multidifusión IPv6, debe habilitar el modo de multidifusión global.

Nota: Cuando inhabilita el Modo de multidifusión global, el controlador reenvía los mensajes

de multidifusión ICMP IPv6, como anuncios de router y solicitudes DHCPv6, ya que son necesarios para que IPv6 funcione. Como resultado, cuando se habilita el Modo Multicast Global en el controlador, no afecta los mensajes ICMPv6 y DHCPv6. Estos mensajes se reenvían independientemente de si el modo de multidifusión global está activado o no.

Cuando la indagación IGMP está inhabilitada, esto es cierto:

- El controlador siempre utiliza MGID de capa 2 cuando envía datos multicast al punto de acceso. A cada interfaz creada se le asigna un MGID de capa 2. Por ejemplo, la interfaz de administración tiene un MGID de 0 y a la primera interfaz dinámica creada se le asigna un MGID de 8, que aumenta a medida que se crea cada interfaz dinámica.
- Los paquetes IGMP de los clientes se reenvían al router. Como resultado, la tabla IGMP del router se actualiza con la dirección IP de los clientes como el último informador.

Cuando la indagación IGMP está habilitada, esto es cierto:

- El controlador siempre utiliza MGID de capa 3 para todo el tráfico de multidifusión de capa 3 enviado al punto de acceso. Para todo el tráfico de multidifusión de capa 2, continúa utilizando MGID de capa 2.
- El controlador consume o absorbe los paquetes de informe IGMP de los clientes inalámbricos, lo que genera una consulta para los clientes. Después de que el router envía la consulta IGMP, el controlador envía los informes IGMP con su dirección IP de interfaz como la dirección IP del receptor para el grupo multicast. Como resultado, la tabla IGMP del router se actualiza con la dirección IP del controlador como receptor de multidifusión.
- Cuando el cliente que escucha los grupos multicast se traslada de un controlador a otro, el primer controlador transmite toda la información del grupo multicast para el cliente que escucha al segundo controlador. Como resultado, el segundo controlador puede crear inmediatamente la información del grupo multicast para el cliente. El segundo controlador envía los informes IGMP a la red para todos los grupos multicast a los que el cliente estaba escuchando. Este proceso ayuda en la transferencia sin problemas de datos de multidifusión al cliente.
- El WLC funciona principalmente en IGMPv1 y v2. Los AP utilizan IGMPv2 para unirse al grupo de multidifusión CAPWAP. Cuando los clientes inalámbricos envían informes igmpv3, el WLC los traduce y reenvía como igmpv2 hacia la red cableada. A partir de entonces, se esperan respuestas en IGMPv2. Esto significa que los clientes inalámbricos pueden utilizar IGMPv3 pero las funciones de IGMPv3 de la red cableada no son compatibles con el WLC.

Nota:

- Los MGID son específicos del controlador. Los mismos paquetes de grupo multicast que provienen de la misma VLAN en dos controladores diferentes se pueden asignar a dos MGID diferentes.
- Si la multidifusión de Capa 2 está habilitada, se asigna un único MGID a todas las direcciones de multidifusión que provienen de una interfaz.
- El número máximo de grupos de multidifusión admitidos por VLAN para un controlador es 100.

Roaming de multidifusión inalámbrica

Un desafío importante para un cliente de multidifusión en un entorno inalámbrico es mantener su pertenencia al grupo de multidifusión cuando se mueve por la WLAN. Las caídas en la conexión

inalámbrica que se mueven de AP a AP pueden causar una interrupción en la aplicación multicast de un cliente. IGMP desempeña un papel importante en el mantenimiento de la información de pertenencia a grupos dinámicos.

Una comprensión básica de IGMP es importante para entender qué sucede con la sesión de multidifusión de un cliente cuando se desplaza por la red. En un caso de roaming de Capa 2, las sesiones se mantienen simplemente porque el AP externo, si se configura correctamente, ya pertenece al grupo multicast, y el tráfico no se tuneliza a un punto de anclaje diferente en la red. Los entornos de roaming de Capa 3 son un poco más complejos de esta manera y, según el modo de tunelización que haya configurado en sus controladores, los mensajes IGMP enviados desde un cliente inalámbrico pueden verse afectados. El modo de tunelización de movilidad predeterminado en un controlador es asimétrico. Esto significa que el tráfico de retorno al cliente se envía al WLC de anclaje y luego se reenvía al WLC externo, donde reside la conexión del cliente asociado. Los paquetes salientes se reenvían fuera de la interfaz WLC externa. En el modo de tunelización de movilidad simétrica, los tráficos entrantes y salientes se tunelizan al controlador de anclaje.

Si el cliente de escucha se traslada a un controlador en una subred diferente, los paquetes multicast se tunelizan al controlador de anclaje del cliente para evitar la verificación de filtrado de trayectoria inversa (RPF). A continuación, el anclaje reenvía los paquetes de multidifusión al switch de infraestructura.

Pautas para Utilizar el Modo Multicast

- La solución de red inalámbrica de Cisco utiliza algunos intervalos de direcciones IP para fines específicos, y debe tener estos intervalos en cuenta al configurar un grupo de multidifusión:
224.0.0.0 a 224.0.0.255 - Direcciones locales de link reservadas
De 224.0.1.0 a 238.255.255.255: direcciones de ámbito global
De 239.0.0.0 a 239.255.x.y/16: direcciones de alcance limitado
- Cuando habilita el modo multicast en el controlador, también debe configurar una dirección de grupo multicast CAPWAP. Los AP se suscriben al grupo de multidifusión CAPWAP con el uso de IGMP.
- Los AP en el modo monitor, el modo sniffer, o el modo rogue del detector no se unen a la dirección del grupo multicast CAPWAP.
- El grupo de multidifusión CAPWAP configurado en los controladores debe ser diferente para los distintos controladores.

Los AP CAPWAP transmiten paquetes multicast a una de las velocidades de datos obligatorias configuradas.

Debido a que las tramas multicast no se retransmiten en la capa MAC, los clientes en el borde de la celda pueden fallar al recibirlas exitosamente. Si la recepción confiable es un objetivo, las tramas multicast deben transmitirse a una velocidad de datos baja, desactivando las velocidades de datos obligatorias más altas. Si se requiere compatibilidad con tramas de multidifusión de alta velocidad de datos, puede ser útil reducir el tamaño de celda y deshabilitar todas las velocidades de datos inferiores, o utilizar la secuencia multimedia.

En función de sus requisitos, puede realizar las siguientes acciones:

- Si necesita transmitir datos de multidifusión con la mayor fiabilidad y no necesita un gran ancho de banda de multidifusión, configure una única velocidad básica, lo suficientemente baja como para alcanzar los bordes de las celdas inalámbricas.

- Si necesita transmitir datos de multidifusión a una velocidad de datos determinada para lograr un rendimiento determinado, puede configurar esa velocidad como la velocidad básica más alta. También puede establecer una velocidad básica más baja para la cobertura de clientes no multidifusión.
- Configuración del flujo de medios.
- El modo multidifusión no funciona en los eventos de movilidad entre subredes, como la tunelización de invitados. Sin embargo, funciona en itinerancias de capa 3.
- Para CAPWAP, el controlador descarta los paquetes multicast enviados a los puertos de datos y control UDP 5246 y 5247, respectivamente. Por lo tanto, puede considerar no utilizar estos números de puerto con las aplicaciones multicast en su red. Cisco recomienda que no utilice ningún puerto UDP de multidifusión enumerado en [esta tabla de protocolos WLC](#) como puertos UDP utilizados por el controlador.
- Cisco recomienda que las aplicaciones de multidifusión de la red no utilicen la dirección de multidifusión configurada como dirección de grupo de multidifusión CAPWAP en el controlador.
- Para que la multidifusión funcione en el WLC de Cisco 2504, debe configurar la dirección IP de multidifusión.
- El modo de multidifusión no es compatible con los WLC de la serie Cisco Flex 7500.
- Las funciones de indagación IGMP y MLD no son compatibles con los WLC Cisco Flex 7510.
- Para Cisco 8510 WLC: Debe activar la unidifusión multidifusión si se requiere compatibilidad con IPv6 en los puntos de acceso de FlexConnect con clientes de switching central. Puede cambiar del modo multidifusión al modo multidifusión-unidifusión sólo si la multidifusión global está desactivada, lo que significa que no se admite la indagación IGMP o MLD. Los puntos de acceso FlexConnect no se asocian a un grupo de multidifusión multidifusión. El snooping de IGMP o MLD no se admite en los puntos de acceso de FlexConnect. La indagación IGMP y MLD se permite solamente para los AP del modo local en el modo multicast-multicast. Debido a que VideoStream requiere indagación IGMP o MLD, la función VideoStream sólo funciona en los AP de modo local si el modo multicast-multicast y la indagación están habilitados.
- Cisco Mobility Express Controller no admite el modo de multidifusión AP.
- Cisco recomienda que no utilice el modo de unidifusión de difusión o unidifusión de multidifusión en la configuración del controlador donde haya más de 50 AP unidos.
- Mientras utiliza el modo AP local y FlexConnect, la compatibilidad con multidifusión del controlador difiere según la plataforma.

Los parámetros que afectan al reenvío de multidifusión son:

- Plataforma del controlador.
- Configuración del modo multicast global AP en el controlador.
- Modo del punto de acceso: switching central FlexConnect local.
- Para la conmutación local, no envía/recibe el paquete hacia/desde el controlador, por lo que no importa qué modo de multidifusión esté configurado en el controlador. **Nota:** Los AP FlexConnect se unen al grupo de multidifusión CAPWAP solo si tienen WLAN conmutadas centralmente. Los AP Flex con solamente WLAN conmutadas localmente no se unen al grupo de multidifusión CAPWAP.
- A partir de la versión 8.2.100.0, no es posible descargar algunas de las configuraciones anteriores del controlador debido a las validaciones de dirección IP y multidifusión

introducidas en esta versión. En esta tabla se muestra la compatibilidad de plataforma para el modo de multidifusión global y multidifusión. Tabla 1. Compatibilidad de la plataforma para el modo de multidifusión global y multidifusión

Configuración de la red

Todos los dispositivos y la configuración se muestran en el diagrama:

Los dispositivos deben configurarse para la conectividad IP básica y activar la multidifusión en la red. Por lo tanto, los usuarios pueden enviar y recibir tráfico multidifusión desde el lado cableado al lado inalámbrico y viceversa.

Este documento utiliza estas direcciones IP para el WLC, el AP, y los clientes inalámbricos:

```
WLC Management Interface IP address: 10.63.84.48/23
LAP IP address: 172.16.16.0/23
Wireless Client Cl IP address: 192.168.47.17/24
Wired Client W1 IP address: 192.168.48.11/24
CAPWAP multicast IP address : 239.2.2.2
Stream multicast address : 239.100.100.100
```

Configurar

Para configurar los dispositivos para esta configuración, se deben realizar estas acciones:

- [Configuración de la red inalámbrica para multidifusión](#)
- [Configuración de la red por cable para multidifusión](#)

Configuración de la red inalámbrica para multidifusión

Antes de configurar la multidifusión en los WLC, debe configurar el WLC para el funcionamiento básico y registrar los AP al WLC. Este documento supone que el WLC se configura para el funcionamiento básico y que los LAPs se registran al WLC. Si usted es un nuevo usuario que intenta configurar el WLC para el funcionamiento básico con los LAPs, consulte [Registro ligero del AP \(LAP\) a un controlador del Wireless LAN \(WLC\)](#).

Una vez que los LAP se registran al WLC, complete estas tareas para configurar los LAP y el WLC para esta configuración:

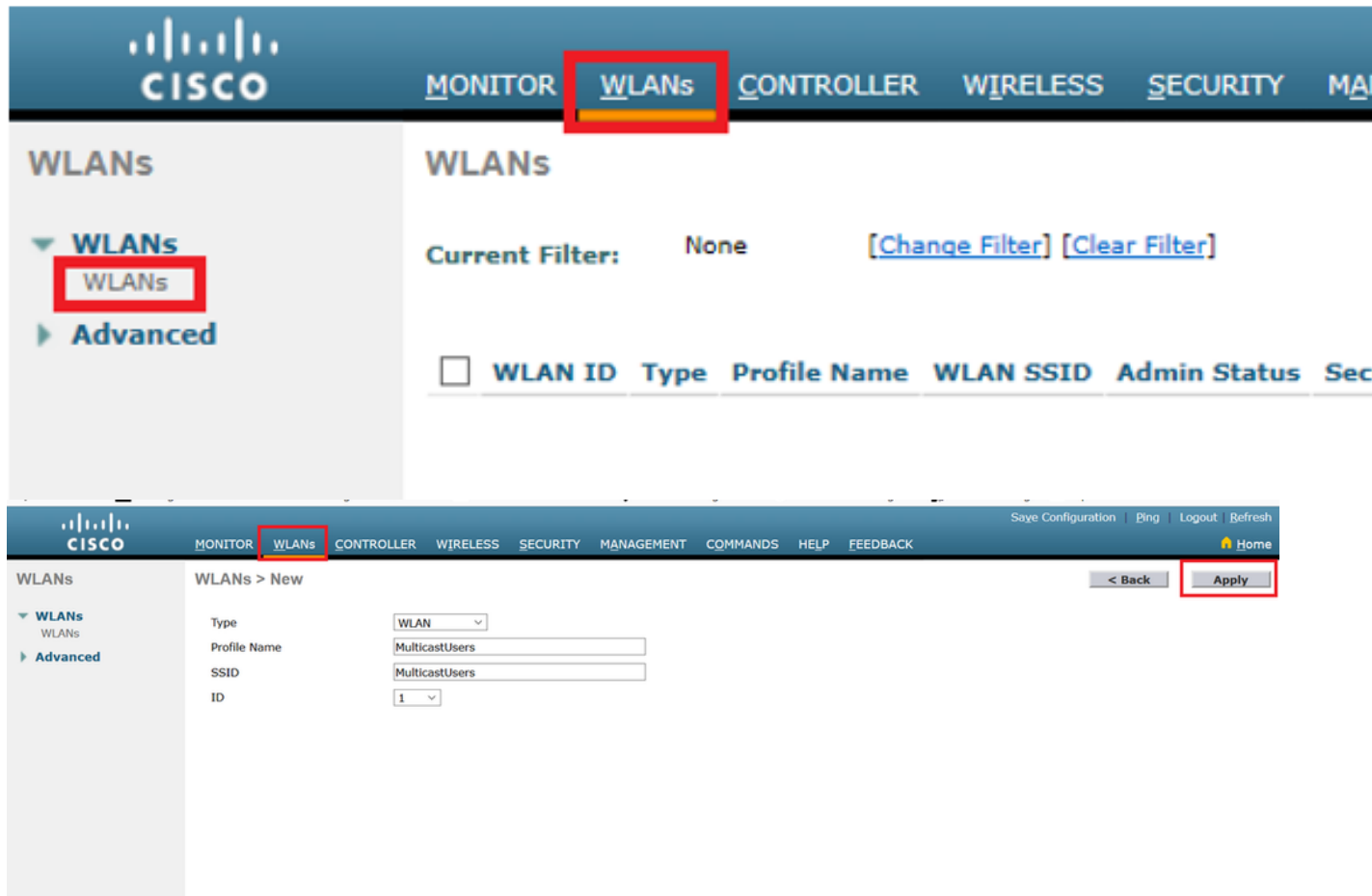
1. [Configuración de WLAN para clientes](#)
2. [Activación del modo multidifusión Ethernet mediante la GUI](#)

Configuración de WLAN para clientes

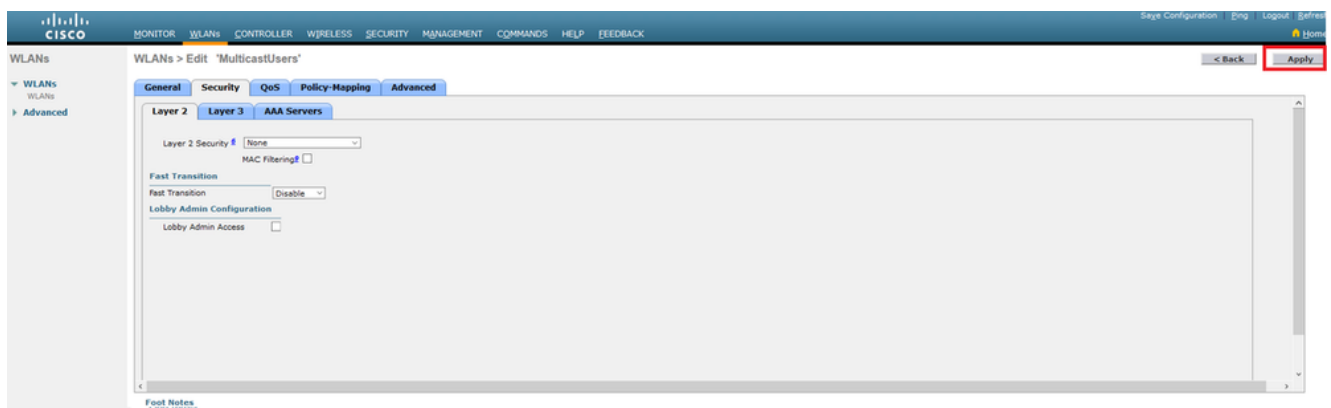
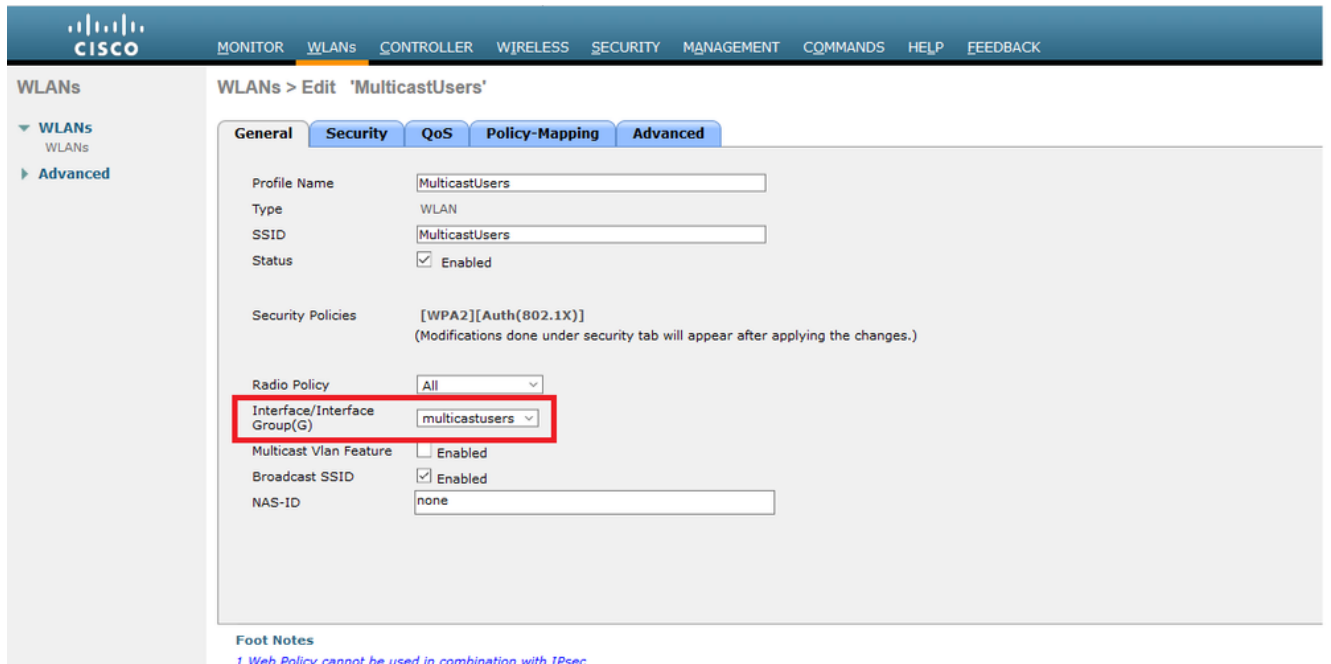
El primer paso es crear una WLAN a la que los clientes inalámbricos puedan conectarse y recibir acceso a la red. Complete estos pasos para crear una WLAN en el WLC:

1. Haga clic **WLANs** desde la GUI del controlador para crear una WLAN.

- Haga clic **New** para configurar una nueva WLAN.
En este ejemplo, la WLAN se denomina **MulticastUsers** y el ID de WLAN es 1.



- Haga clic **Apply**.
- En el **WLAN > Edit Window**, defina los parámetros específicos de la WLAN.
- Para la WLAN, elija la interfaz adecuada del **Interface Name** campo. Este ejemplo asigna la interfaz **MulticastUsers (192.168.47.0/24)** a la WLAN.
- Elija los demás parámetros, que dependen de los requisitos de diseño. En este ejemplo, puede utilizar **WLAN sin seguridad L2 (WLAN abierta)**.



7. Haga clic **Apply**.

Ejecute estos comandos para configurar las WLAN en el WLC con el uso de la CLI:

1. Ejecute el comando `config wlan create` para crear una nueva WLAN. Para wlan-id, introduzca un ID del 1 al 16. Para wlan-name, introduzca un SSID de hasta 31 caracteres alfanuméricos.
2. Ejecute el comando `config wlan enable` para habilitar una WLAN. Para el ejemplo de este documento, los comandos son:

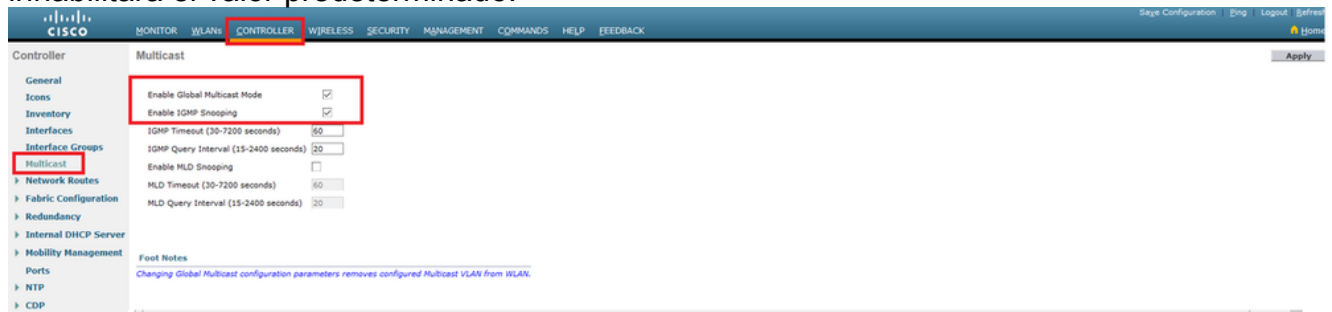
```
config wlan create 1 MulticastUsers
config wlan enable 1
```

Configuración del modo multidifusión mediante la GUI

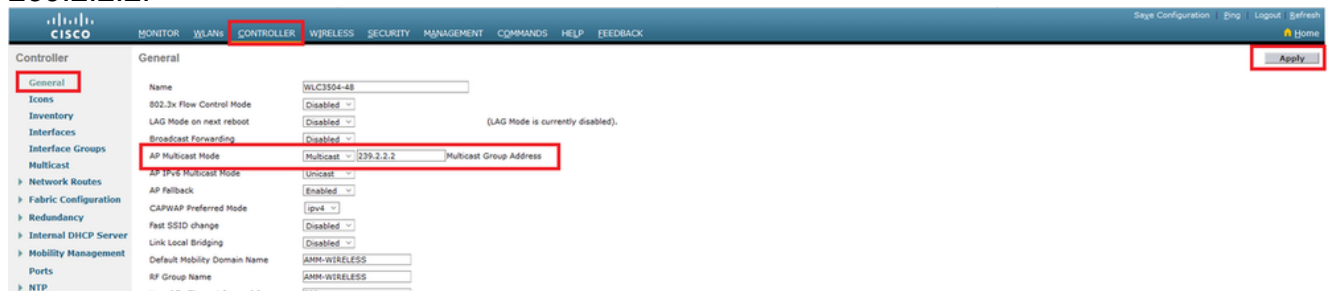
El siguiente paso es configurar el WLC para la multidifusión. Complete estos pasos:

1. Vaya a **Controller > Multicast**. Se abrirá la página Multidifusión.
2. Elija el **Enable Global Multicast Mode** para configurar el WLC para reenviar paquetes multicast. Se inhabilitará el valor predeterminado.
3. Si desea activar la indagación de IGMP, elija el **Enable IGMP snooping** casilla de verificación. Si desea desactivar la indagación IGMP, deje la casilla de verificación sin marcar. Se

inhabilitará el valor predeterminado:



4. Vaya a **Controller > General**. Para el modo de multidifusión AP en el menú desplegable, seleccione **Multicast** y configure la dirección IP de multidifusión. En este ejemplo, se utiliza **239.2.2.2**:



5. Haga clic **Apply**.

Configuración del modo multidifusión mediante la CLI

Ejecute estos comandos para habilitar la multidifusión a través de la CLI:

1. Desde la línea de comandos, ejecute el comando `config network multicast global enable` comando.
2. Desde la línea de comandos, ejecute el comando `config network multicast mode multicast <multicast-group-ip-address>` comando. Para el ejemplo de este documento, los comandos son:
`config network multicast global enable config network multicast mode multicast 239.2.2.2`

Una vez que el administrador habilita la multidifusión (el modo multidifusión está deshabilitado de forma predeterminada) y configura el grupo multidifusión CAPWAP, el nuevo algoritmo de multidifusión funciona de una de estas maneras:

Cuando el origen del grupo multicast está en la LAN cableada:

Se habilita una multidifusión y se configura el grupo de multidifusión CAPWAP. El AP emite una solicitud IGMP para unirse al grupo multicast CAPWAP del controlador. Esto activa la configuración normal para el estado multicast en los routers habilitados para multicast, entre el controlador y los AP. La dirección IP de origen para el grupo multicast es la dirección IP de la interfaz de administración del controlador.

Cuando el controlador recibe un paquete de multidifusión de cualquiera de las VLAN del cliente en el router del primer salto, transmite el paquete al grupo de multidifusión CAPWAP a través de la interfaz de administración en el nivel de QoS más bajo. Los bits de QoS para el paquete de multidifusión CAPWAP están codificados en el nivel más bajo y el usuario no puede cambiarlos.

La red habilitada para multidifusión entrega el paquete de multidifusión CAPWAP a cada uno de los AP que se han unido al grupo de multidifusión CAPWAP. La red habilitada para multidifusión

utiliza los mecanismos de multidifusión normales en los routers para replicar el paquete en el camino, según sea necesario para que el paquete de multidifusión llegue a todos los AP. Esto libera al controlador de la replicación de paquetes multicast.

Los AP pueden recibir otros paquetes multicast, pero procesar solamente los paquetes multicast que vienen del controlador al cual están actualmente unidos. Cualquier otra copia se descartará. Si más de un SSID WLAN está asociado con la VLAN desde donde se envió el paquete multicast original, el AP transmite el paquete multicast a través de cada SSID WLAN (junto con el mapa de bits WLAN en el encabezado CAPWAP). Además, si ese SSID WLAN está en ambas radios (802.11g y 802.11a), ambas radios transmiten el paquete multicast en el SSID WLAN si hay clientes asociados con él, incluso si esos clientes no solicitaron el tráfico multicast.

Cuando el origen del grupo de multidifusión es un cliente inalámbrico:

El paquete multicast es unicast (encapsulado CAPWAP) desde el AP al controlador, similar al tráfico de cliente inalámbrico estándar.

El controlador hace dos copias del paquete multicast. Se envía una copia a la VLAN asociada con el SSID WLAN en el que llegó. Esto permite que los receptores de la LAN cableada reciban la secuencia de multidifusión y que el router conozca el nuevo grupo de multidifusión. La segunda copia del paquete está encapsulada CAPWAP y se envía al grupo de multidifusión CAPWAP para que los clientes inalámbricos puedan recibir la secuencia de multidifusión.

Configuración de la red por cable para multidifusión

Para configurar la red con cables para esta configuración, debe configurar el switch principal L3 para el routing básico y habilitar el routing multidifusión.

En la red con cables se puede utilizar cualquier protocolo de multidifusión. Este documento utiliza PIM-DM como protocolo de multidifusión. Consulte la Guía de Configuración de IP Multicast de Cisco IOS para obtener información detallada sobre los diferentes protocolos que se pueden utilizar para la multidifusión en una red con cable.

Configuración del switch principal

```
ip multicast-routing !--- Enables IP Multicasting on the network. interface Vlan16
description AP Management VLAN
ip address 172.16.16.1 255.255.254.0
ip helper-address 10.63.84.5
ip pim dense-mode
!--- Enables PIM-Dense Mode Multicast Protocol on the interface.
interface Vlan47
description Wireless Client
ip address 192.168.47.1 255.255.255.0
ip helper-address 10.63.84.5
ip pim dense-mode !--- Enables PIM-Dense Mode Multicast Protocol on the interface. ! interface Vlan48
description Wired Client
ip address 192.168.48.1 255.255.255.0
ip helper-address 10.63.84.5
ip pim dense-mode !--- Enables PIM-Dense Mode Multicast Protocol on the interface. interface Vlan84
description Wireless Management VLAN
ip address 10.63.84.1 255.255.254.0
ip pim dense-mode ! end
```

No se necesita ninguna configuración en el switch de acceso L2 ya que la indagación IGMP está habilitada de forma predeterminada en los switches Cisco.

Verificación y resolución de problemas

Use esta sección para confirmar que su configuración funciona correctamente.

Para verificar la configuración, debe enviar tráfico multicast desde el origen W1 y verificar si el tráfico multicast fluye a través de la red cableada y llega a los miembros del grupo cableado e inalámbrico (C1).

Realice esta tarea para probar si la multidifusión IP está configurada correctamente en su red.

Verifique el ruteo multicast en el switch principal y las pertenencias a IGMP con los comandos **show ip mroute** y **show ip igmp membership**. Aquí se muestra el resultado del ejemplo anterior:

```
CORE1-R1#show ip mroute
IP Multicast Routing Table
Flags: D - Dense, S - Sparse, B - Bidir Group, s - SSM Group, C - Connected,
L - Local, P - Pruned, R - RP-bit set, F - Register flag,
T - SPT-bit set, J - Join SPT, M - MSDP created entry,
X - Proxy Join Timer Running, A - Candidate for MSDP Advertisement,
U - URD, I - Received Source Specific Host Report, Z - Multicast Tunnel
Y - Joined MDT-data group, y - Sending to MDT-data group
Outgoing interface flags: H - Hardware switched, A - Assert winner
Timers: Uptime/Expires
Interface state: Interface, Next-Hop or VCD, State/Mode

(*, 239.255.255.250), 21:19:09/00:02:55, RP 0.0.0.0, flags: DC
Incoming interface: Null, RPF nbr 0.0.0.0
Outgoing interface list:
Vlan48, Forward/Dense, 00:04:48/00:00:00
Vlan84, Forward/Sparse-Dense, 21:19:09/00:00:00

(*, 239.100.100.100), 00:01:58/stopped, RP 0.0.0.0, flags: DC
Incoming interface: Null, RPF nbr 0.0.0.0
Outgoing interface list:
Vlan47, Forward/Dense, 00:01:29/00:00:00
(192.168.48.11, 239.100.100.100), 00:01:58/00:02:58, flags: T
Incoming interface: Vlan48, RPF nbr 0.0.0.0, RPF-MFD
Outgoing interface list:
Vlan47, Forward/Dense, 00:01:29/00:00:00, H

(*, 224.0.1.40), 1d21h/00:02:54, RP 0.0.0.0, flags: DCL
Incoming interface: Null, RPF nbr 0.0.0.0
Outgoing interface list:
Vlan84, Forward/Sparse-Dense, 1d01h/00:00:00

(*, 239.2.2.2), 01:21:13/stopped, RP 0.0.0.0, flags: DC
Incoming interface: Null, RPF nbr 0.0.0.0
Outgoing interface list:
Vlan16, Forward/Dense, 00:33:10/00:00:00

(10.63.84.48, 239.2.2.2), 00:33:46/00:02:51, flags: T
Incoming interface: Vlan84, RPF nbr 0.0.0.0, RPF-MFD
Outgoing interface list:
Vlan16, Forward/Dense, 00:33:10/00:00:00, H
```

```
CORE1-R1#show ip igmp membership
```

Flags: A - aggregate, T - tracked
L - Local, S - static, V - virtual, R - Reported through v3
I - v3lite, U - Urd, M - SSM (S,G) channel
1,2,3 - The version of IGMP, the group is in

hannel/Group-Flags:

/ - Filtering entry (Exclude mode (S,G), Include mode (G))

Reporter:

<mac-or-ip-address> - last reporter if group is not explicitly tracked

<n>/<m> - <n> reporter in include mode, <m> reporter in exclude

Channel/Group Reporter Uptime Exp. Flags Interface

*,**239.2.2.2 172.16.16.17** 00:33:25 02:48 2A V116 !--- AP membership to CAPWAP multicast address.

*,224.0.1.40 10.63.84.1 1d01h 02:38 2LA V184

*,**239.100.100.100 192.168.47.10** 00:01:45 02:56 2A V147 !--- Wireless Client C1 to Stream multicast address .

*,239.255.255.250 192.168.48.11 00:05:03 02:58 2A V148

*,239.255.255.250 10.63.85.163 21:19:25 02:40 2A V184

También puede utilizar el comando **show ip mroute count** para garantizar que el ruteo multicast funcione correctamente:

```
CORE1-R1#show ip mroute count
```

```
IP Multicast Statistics
```

```
10 routes using 5448 bytes of memory
```

```
6 groups, 0.66 average sources per group
```

```
Forwarding Counts: Pkt Count/Pkts per second/Avg Pkt Size/Kilobits per second
```

```
Other counts: Total/RPF failed/Other drops(OIF-null, rate-limit etc)
```

```
Group: 239.255.255.250, Source count: 0, Packets forwarded: 0, Packets received: 0
```

```
Group: 239.100.100.100, Source count: 1, Packets forwarded: 1351, Packets received: 1491
```

```
Source: 192.168.48.11/32, Forwarding: 1351/14/1338/151, Other: 1491/0/140
```

```
Group: 224.0.1.40, Source count: 0, Packets forwarded: 0, Packets received: 0
```

```
Group: 239.2.2.2, Source count: 1, Packets forwarded: 3714, Packets received: 3726
```

```
Source: 10.63.84.48/32, Forwarding: 3714/28/551/163, Other: 3726/0/12
```

A partir de estos resultados, puede ver que el tráfico multicast fluye desde el origen W1 y es recibido por los miembros del grupo.

Información Relacionada

- [Guía de diseño de Enterprise Mobility 8.5](#)
- [Ejemplo de Configuración de VLANs en Controladores de LAN Inalámbrica](#)
- [Ejemplo de la configuración básica del controlador y del Lightweight Access Point del Wireless LAN](#)
- [Multidifusión IP: Informe Oficial](#)
- [Soporte Técnico y Documentación - Cisco Systems](#)

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).