Configure Multicast with AireOS Wireless LAN Controllers (WLCs)

Contents

Introduction

Prerequisites

- Requirements
- Components Used

Multicast in WLCs

- Broadcast Behavior in Different WLC
- IGMP Snooping on WLC
- Wireless Multicast Roaming
- Guidelines to Use the Multicast Mode

Network Setup

Configure

- Configure the Wireless Network for Multicasting
  - Configure the WLAN for Clients
  - Configure Multicast Mode via the GUI
  - Configure Multicast Mode via the CLI
- Configure the Wired Network for Multicasting

Verify and Troubleshoot

Related Information

Introduction

This document describes how to configure Wireless LAN Controllers (WLCs) and Lightweight Access Points (LAPs) for multicast.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Basic knowledge of the configuration of APs and Cisco WLCs
- Knowledge of how to configure basic routing and multicasting in a wired network

Ensure that you meet these requirements before you attempt this configuration.

Components Used

The information in this document is based on these software and hardware versions:

- Cisco 3504 WLC that runs Firmware Release 8.5

- Cisco 3702 Series LAPs
- Microsoft Windows 10 Wireless Client with Intel(R) Dual Band Wireless-AC 8265 adapter
- Cisco 6500 switch that runs Cisco IOS® Software Release 12.2(18)
- Two Cisco 3650 Series Switches that run Cisco IOS Software Release 16.3.7

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. If your network is live, ensure that you understand the potential impact of any command.

Multicast in WLCs

If your network supports packet multicasting, you can configure the multicast method that the controller uses in order to transport the multicast packets over Control And Provisioning of Wireless Access Points (CAPWAP) to all or several access points at the same time. The controller performs multicasting in two modes:

- Unicast mode - In this mode, the controller unicasts every multicast packet to every AP associated with the controller. This mode is inefficient, but can be required on networks that do not support multicasting.
- Multicast mode - In this mode, the controller sends multicast packets to a CAPWAP multicast group. This method reduces overhead on the controller processor and shifts the work of packet replication to your network, which is much more efficient than the unicast method.

- When you use a different VLAN/Subnet for AP and WLC, Multicast routing is mandatory on the wired side to support forwarding the downlink CAPWAP Multicast packet from WLC to AP.

When you enable multicast mode and the controller receives a multicast packet from the wired LAN, the controller encapsulates the packet with the use of CAPWAP and forwards the packet to the CAPWAP multicast group address. The controller always uses the management interface to send multicast packets. Access points in the multicast group receive the packet and forward it to all the BSSIDs mapped to the interface on which clients receive multicast traffic. From the access point perspective, the multicast appears to broadcast to all SSIDs.

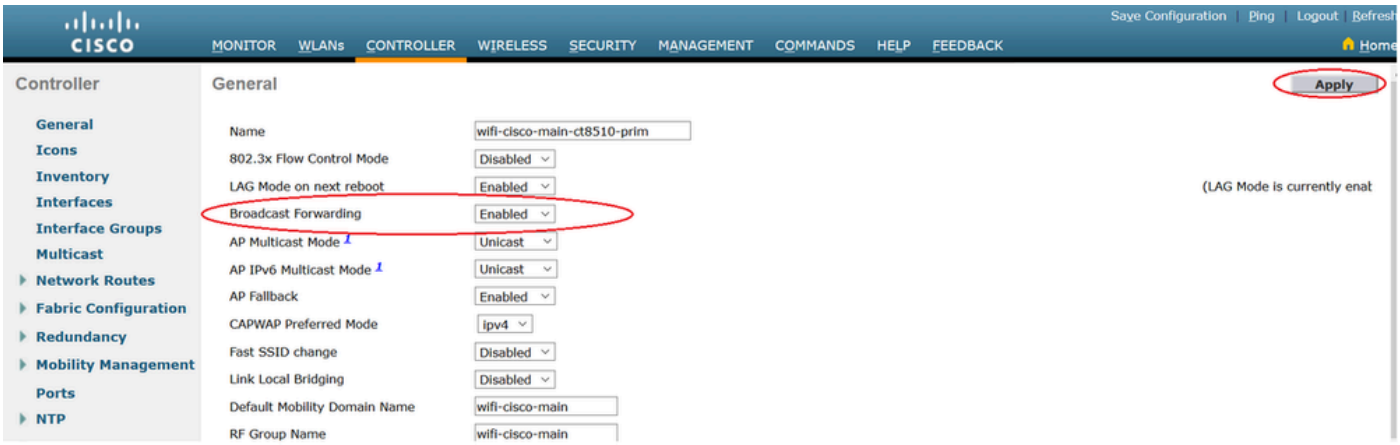
Broadcast Behavior in Different WLC

By default, the WLC does not forward any broadcast packets (such as Upnp traffic) unless broadcast forwarding is enabled. Issue this command from the WLC CLI in order to enable broadcast:

<#root>

```
config network broadcast enable
```

Or enable it with the GUI:



Broadcast uses the **multicast mode** that is configured on the WLC, even if multicast is not turned on. This is because you cannot set the IP address or the mode unless you enable multicast in the GUI. Therefore, if the multicast mode is unicast and the broadcast is turned on, this is the mode the broadcast uses (broadcast traffic is replicated at the WLC and unicast to each AP). If multicast mode is set to multicast with a multicast address, then the broadcast uses this mode (each broadcast packet is sent via the multicast group to the APs).

Note: Until Release 7.5, the port number used for CAPWAP multicast was 12224. From Release 7.6 onwards, the port number used for CAPWAP is changed to 5247.

Multicast with AAA override is supported from Wireless LAN Controller release 4.2 and later. You have to enable IGMP snooping on the controller to make multicast work with AAA override.

IGMP Snooping on WLC

Internet Group Management Protocol (IGMP) snooping is supported on WLC to better direct multicast packets. When this feature is enabled, the controller gathers IGMP reports from the clients, processes the reports, creates unique multicast group IDs (MGIDs) from the IGMP reports after it checks the Layer 3 multicast address and the VLAN number, and sends the IGMP reports to the infrastructure switch. The controller sends these reports with the source address as the interface address on which it received the reports from the clients.

The controller then updates the access point MGID table on the AP with the client MAC address. When the controller receives multicast traffic for a particular multicast group, it forwards it to all the APs. However, only those APs that have active clients listening or subscribed to that multicast group send multicast traffic on that particular WLAN. IP packets are forwarded with an MGID that is unique for an ingress VLAN and the destination multicast group. Layer 2 multicast packets are forwarded with an MGID that is unique for the ingress interface.

The controller supports Multicast Listener Discovery (MLD) v1 snooping for IPv6 multicast. This feature keeps track of and delivers IPv6 multicast flows to the clients that request them. In order to support IPv6 multicast, you must enable Global Multicast Mode.

Note: When you disable the Global Multicast Mode, the controller still forwards the IPv6 ICMP multicast messages, such as router announcements and DHCPv6 solicits, as these are required for IPv6 to work. As a result, when the Global Multicast Mode is enabled on the controller, it does not impact the ICMPv6 and the DHCPv6 messages. These messages are forwarded irrespective of whether or not the Global Multicast Mode is enabled.

When IGMP snooping is disabled, this is true:

- The controller always uses Layer 2 MGID when it sends multicast data to the access point. Every interface created is assigned one Layer 2 MGID. For example, the management interface has an MGID of 0, and the first dynamic interface created is assigned an MGID of 8, which increments as each dynamic interface is created.
- The IGMP packets from clients are forwarded to the router. As a result, the router IGMP table is updated with the IP address of the clients as the last reporter.

When IGMP snooping is enabled, this is true:

- The controller always uses Layer 3 MGID for all Layer 3 multicast traffic sent to the access point. For all Layer 2 multicast traffic, it continues to use Layer 2 MGID.
- IGMP report packets from wireless clients are consumed or absorbed by the controller, which generates a query for the clients. After the router sends the IGMP query, the controller sends the IGMP reports with its interface IP address as the listener IP address for the multicast group. As a result, the router IGMP table is updated with the controller IP address as the multicast listener.
- When the client that is listening to the multicast groups roams from one controller to another, the first controller transmits all the multicast group information for the listening client to the second controller. As a result, the second controller can immediately create the multicast group information for the client. The second controller sends the IGMP reports to the network for all multicast groups to which the client was listening. This process aids in the seamless transfer of multicast data to the client.
- The WLC mostly works in IGMPv1 and v2. APs use IGMPv2 to join the CAPWAP multicast group. When wireless clients send igmpv3 reports, they are translated and forwarded as igmpv2 by the WLC towards the wired network. From then on answers are expected in IGMPv2. This means wireless clients can use IGMPv3 but wired network IGMPV3 features are not supported by the WLC.



Note: The MGIDs are controller specific. The same multicast group packets that come from the same VLAN in two different controllers can be mapped to two different MGIDs. If Layer 2 multicast is enabled, a single MGID is assigned to all the multicast addresses that come from an interface. The maximum number of multicast groups supported per VLAN for a controller is 100.

Wireless Multicast Roaming

A major challenge for a multicast client in a wireless environment is to maintain its multicast group membership when moved about the WLAN. Drops in the wireless connection that move from AP to AP can cause a disruption in the multicast application of a client. IGMP plays an important role in the maintenance of dynamic group membership information.

A basic comprehension of IGMP is important to understand what happens to the multicast session of a client when it roams the network. In a Layer 2 roaming case, sessions are maintained simply because the foreign AP, if configured properly, already belongs to the multicast group, and traffic is not tunneled to a different anchor point on the network. Layer 3 roaming environments are a little more complex in this manner, and, dependent upon what tunneling mode you have configured on your controllers, the IGMP messages sent from a wireless client can be affected. The default mobility tunneling mode on a controller is asymmetrical. This means that return traffic to the client is sent to the anchor WLC and then forwarded to the foreign WLC, where the associated client connection resides. Outbound packets are forwarded out the foreign WLC interface. In symmetrical mobility tunneling mode, both inbound and outbound traffics are tunneled to the anchor controller.

If the listening client roams to a controller in a different subnet, the multicast packets are tunneled to the

anchor controller of the client to avoid the reverse path filtering (RPF) check. The anchor then forwards the multicast packets to the infrastructure switch.

Guidelines to Use the Multicast Mode

- The Cisco Wireless network solution uses some IP address ranges for specific purposes, and you must keep these ranges in mind when you configure a multicast group:
  - 224.0.0.0 through 224.0.0.255 - Reserved link-local addresses
  - 224.0.1.0 through 238.255.255.255 - Globally scoped addresses
  - 239.0.0.0 through 239.255.x.y/16 - Limited scope addresses
- When you enable multicast mode on the controller, you must also configure a CAPWAP multicast group address. APs subscribe to the CAPWAP multicast group with the use of IGMP.
- APs in monitor mode, sniffer mode, or rogue detector mode do not join the CAPWAP multicast group address.
- The CAPWAP multicast group configured on the controllers must be different for different controllers.

CAPWAP APs transmit multicast packets at one of the configured mandatory data rates.

Because multicast frames are not retransmitted at the MAC layer, clients at the edge of the cell can fail to receive them successfully. If reliable reception is a goal, multicast frames must be transmitted at a low data rate, by disabling the higher mandatory data rates. If support for high data rate multicast frames is required, it can be useful to shrink the cell size and disable all lower data rates, or to use Media Stream.

Depending on your requirements, you can take these actions:

- If you need to transmit multicast data with the greatest reliability and if there is no need for great multicast bandwidth, then configure a single basic rate, that is low enough to reach the edges of the wireless cells.

- If you need to transmit multicast data at a certain data rate in order to achieve a certain throughput, you can configure that rate as the highest basic rate. You can also set a lower basic rate for coverage of nonmulticast clients.
- Configure Media Stream.

- The multicast mode does not operate across intersubnet mobility events such as guest tunneling. It does, however, operate across Layer 3 roams.
- For CAPWAP, the controller drops multicast packets sent to UDP control and data ports 5246 and 5247, respectively. Therefore, you can consider not to use these port numbers with the multicast applications on your network. Cisco recommends that you do not use any Multicast UDP ports listed in this WLC protocols table as being UDP ports used by the controller.
- Cisco recommends that any multicast applications on your network do not use the multicast address configured as the CAPWAP multicast group address on the controller.
- For multicast to work on Cisco 2504 WLC, you have to configure the multicast IP address.
- Multicast mode is not supported on Cisco Flex 7500 Series WLCs.
- IGMP and MLD snooping are not supported on Cisco Flex 7510 WLCs.
- For Cisco 8510 WLCs:
  - You must enable multicast-unicast if IPv6 support is required on FlexConnect APs with central switching clients.
  - You can change from multicast mode to multicast-unicast mode only if global multicast is disabled, which means IGMP or MLD snooping is not supported.
  - FlexConnect APs do not associate with a multicast-multicast group.
  - IGMP or MLD snooping is not supported on FlexConnect APs. IGMP and MLD snooping are allowed only for local mode APs in multicast-multicast mode.

    - Because VideoStream requires IGMP or MLD snooping, the VideoStream feature works only on local mode APs if the multicast-multicast mode and snooping are enabled.
- Cisco Mobility Express Controller does not support AP multicast mode.
- Cisco recommends that you do not use Broadcast-Unicast or Multicast-Unicast mode on controller setup where there are more than 50 APs joined.
- While you use Local and FlexConnect AP mode, the controller multicast support differs for different platforms.

The parameters that affect Multicast forwarding are:

- Controller platform.
- Global AP multicast mode configuration at the controller.
- Mode of the AP - Local, FlexConnect central switching.
- For Local switching, it does not send/receive the packet to/from the controller, so it does not matter which Multicast mode is configured on the controller.

> **Note**: FlexConnect APs join the CAPWAP multicast group only if they have centrally switched WLANs. Flex APs with only locally switched WLANs do not join the CAPWAP multicast group.

- Effective with Release 8.2.100.0, it is not possible to download some of the earlier configurations from the controller because of the Multicast and IP address validations introduced in this release. The platform support for global multicast and multicast mode are listed in this table.

Table 1. Platform Support for Global Multicast and Multicast Mode

Platform	Global Multicast	Multicast Mode	Supported
Cisco 5520, 8510, and 8540 Controllers	Enabled	Unicast	No
Enabled	Multicast	Yes	
Disabled	Unicast	No multicast support (configuration supported)	
Disabled	Multicast	No multicast support (configuration supported)	
Cisco Flex 7510 Controller	Global Multicast cannot be enabled. Only Unicast mode is supported. Also, AP-Multicast mode cannot be changed to Multicast-Multicast.		
Cisco 2504 Controller	Only Multicast mode is supported.		
Cisco vWLC	Multicast is not supported; only Unicast mode is supported.		
Cisco 3504 Controller and Cisco 5508 Controller	Enabled	Unicast	Yes
Enabled	Multicast	Yes	
Disabled	Unicast	Yes	
Disabled	Multicast	No	

Network Setup

All devices and setup are shown in the diagram:

The devices need to be configured for basic IP connectivity and enable multicasting in the network. Therefore, users can send and receive multicast traffic from the wired side to the wireless side and vice versa.

This document uses these IP addresses for the WLC, AP, and wireless clients:

```
WLC Management Interface IP address: 10.63.84.48/23
LAP IP address: 172.16.16.0/23
Wireless Client C1 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
```

Configure

In order to configure the devices for this setup, these need to be performed:

- Configure the Wireless Network for Multicasting
- Configure the Wired Network for Multicasting

Configure the Wireless Network for Multicasting

Before you configure multicasting on WLCs, you must configure the WLC for basic operation and register the APs to the WLC. This document assumes that the WLC is configured for basic operation and that the LAPs are registered to the WLC. If you are a new user trying to set up the WLC for basic operation with LAPs, refer to Lightweight AP (LAP) Registration to a Wireless LAN Controller (WLC).

Once the LAPs are registered to the WLC, complete these tasks in order to configure the LAPs and WLC for this setup:

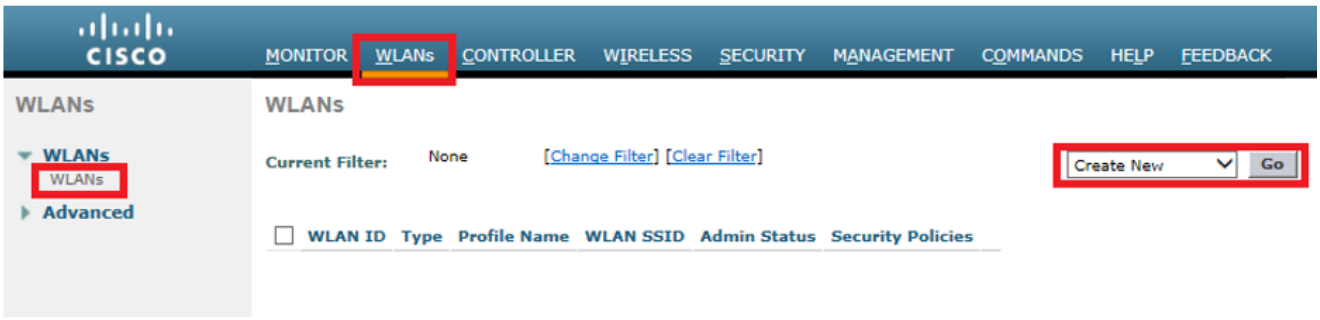
1. Configure the WLAN for Clients
2. Enable Ethernet Multicast Mode via the GUI

Configure the WLAN for Clients

The first step is to create a WLAN that the wireless clients can connect to and receive access to the network. Complete these steps in order to create a WLAN on the WLC:

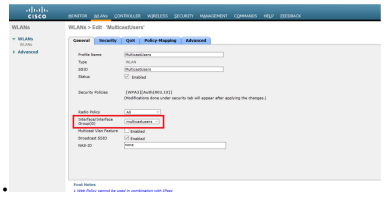
1. Click **WLANs** from the controller GUI in order to create a WLAN.
2. Click **New** in order to configure a new WLAN.

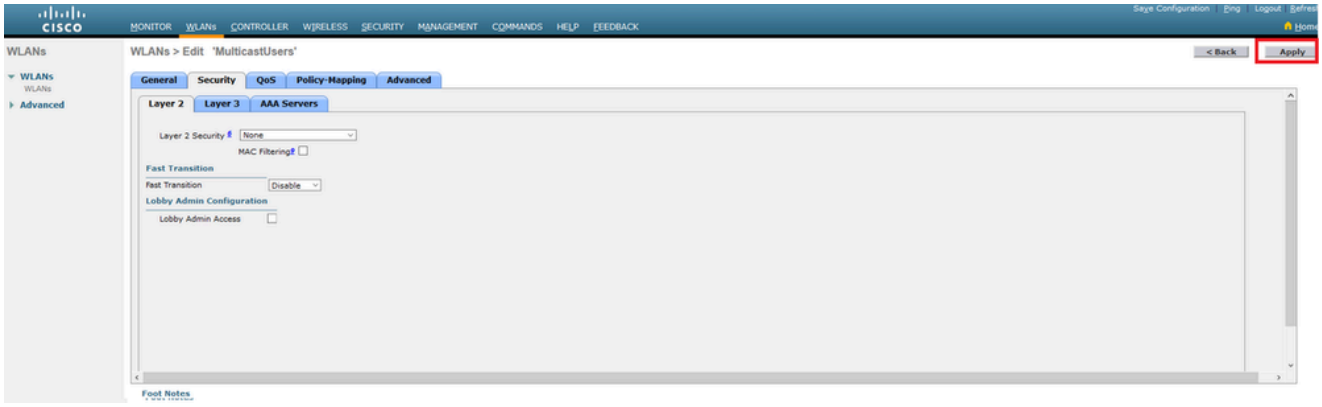
In this example, the WLAN is named **MulticastUsers** and the WLAN ID is 1:



3. Click **Apply**.
4. In the **WLAN > Edit Window**, define the parameters specific to the WLAN.
5. For the WLAN, choose the appropriate interface from the **Interface Name** field.

   This example maps the MulticastUsers (192.168.47.0/24) interface to the WLAN.
6. Choose the other parameters, which depend on the design requirements.

   In this example, you can use WLAN with no L2 Security (Open WLAN). 



7. Click **Apply**.

Issue these commands in order to configure the WLANs on WLC with the use of the CLI:

1. Issue the **config wlan create <wlan-id> <wlan-name>** command in order to create a new WLAN. For wlan-id, enter an ID from 1 to 16. For wlan-name, enter an SSID up to 31 alphanumeric characters.
2. Issue the **config wlan enable <wlan-id>** command in order to enable a WLAN.

   For the example in this document, the commands are:

   <#root>

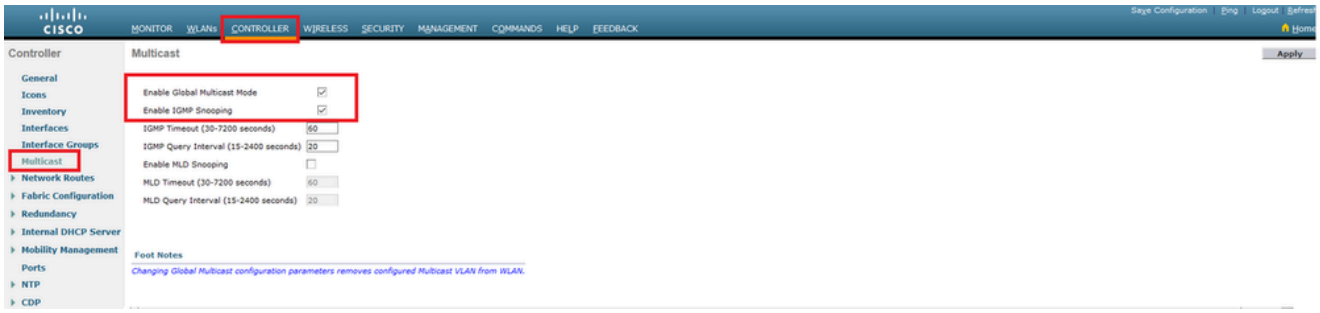
   config wlan create 1 MulticastUsers

```
config wlan enable 1
```

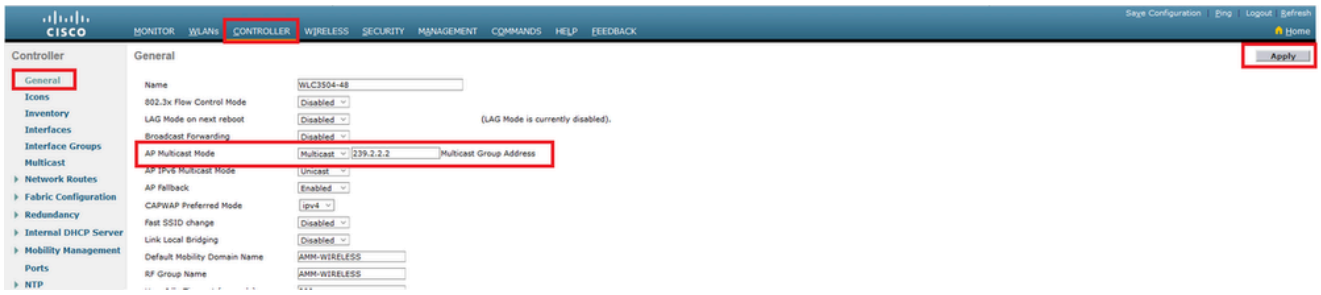
Configure Multicast Mode via the GUI

The next step is to configure the WLC for multicasting. Complete these steps:

1. Navigate to **Controller** > **Multicast**. This opens the Multicast page.
2. Choose the **Enable Global Multicast Mode** check box to configure the WLC to forward multicast packets. The default value is disabled.
3. If you want to enable IGMP snooping, choose the **Enable IGMP snooping** check box. If you want to disable IGMP snooping, leave the check box unselected. The default value is disabled:



4. Navigate to **Controller > General.** For AP Multicast Mode from the drop-down menu, choose Multicast and configure the multicast IP address. In this example, 239.2.2.2 is used:



5. Click **Apply**.

Configure Multicast Mode via the CLI

Issue these commands in order to enable multicast through the CLI:

1. From the command line, run the **config network multicast global enable** command.
2. From the command line, run the **config network multicast mode multicast <multicast-group-ip-address>** command.

   For the example in this document, the commands are:

```
config network multicast global enable config network multicast mode multicast 239.2.2.2
```

After the administrator enables multicast (multicast mode is disabled by default) and configures the CAPWAP multicast group, the new multicast algorithm works in one of these ways:

When the source of the multicast group is on the wired LAN:

One Multicast is enabled and the CAPWAP multicast group is configured. The AP issues an IGMP request in order to join the controller CAPWAP multicast group. This triggers the normal setup for the multicast state in the multicast-enabled routers, between the controller and APs. The source IP address for the multicast group is the controller management interface IP address.

When the controller receives a multicast packet from any of the client VLANs on the first hop router, it transmits the packet to the CAPWAP multicast group via the management interface at the lowest QoS level. The QoS bits for the CAPWAP multicast packet are hard-coded at the lowest level and cannot be changed by the user.

The multicast-enabled network delivers the CAPWAP multicast packet to each of the APs that have joined the CAPWAP multicast group. The multicast-enabled network uses the normal multicast mechanisms in the routers to replicate the packet along the way, as needed so that the multicast packet reaches all APs. This relieves the controller from the replication of multicast packets.

APs can receive other multicast packets, but process only the multicast packets that come from the controller to which they are currently joined. Any other copies are discarded. If more than one WLAN SSID is associated with the VLAN from where the original multicast packet was sent, the AP transmits the multicast packet over each WLAN SSID (along with the WLAN bitmap in the CAPWAP header). In addition, if that WLAN SSID is on both radios (802.11g and 802.11a), both radios transmit the multicast packet on the WLAN SSID if there are clients associated with it, even if those clients did not request the multicast traffic.

When the source of the multicast group is a wireless client, the multicast packet is unicast (CAPWAP-encapsulated) from the AP to the controller, similar to standard wireless client traffic.

The controller makes two copies of the multicast packet. One copy is sent out to the VLAN associated with the WLAN SSID on which it arrived. This enables receivers on the wired LAN to receive the multicast stream and the router to learn about the new multicast group. The second copy of the packet is CAPWAP-encapsulated and is sent to the CAPWAP multicast group so that wireless clients can receive the multicast stream.

Configure the Wired Network for Multicasting

In order to configure the wired network for this setup, you need to configure the L3 Core switch for basic routing and enable multicast routing.

Any multicast protocol can be used in the wired network. This document uses PIM-DM as the multicast protocol. Refer to the Cisco IOS IP Multicast Configuration Guide for detailed information on the different protocols that can be used for multicasting in a wired network.

Core Switch Configuration
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 configuration is needed on the L2 access switch since IGMP snooping is enabled by default on Cisco Switches.

Verify and Troubleshoot

Use this section to confirm that your configuration works properly.

In order to verify the configuration, you need to send multicast traffic from source W1 and check if multicast traffic flows through the wired network and reaches the wired and wireless group members (C1).

Perform this task in order to test if IP multicast is configured correctly in your network.

Check multicast routing on the Core switch and IGMP memberships with the commands **show ip mroute** and **show ip igmp membership** . The output from the previous example is shown here:

<#root>

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




<#root>

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 Vl16 !--- AP membership to CAPWAP multicast address.
*,224.0.1.40 10.63.84.1 1d01h 02:38 2LA Vl84
*,
```

239.100.100.100 192.168.47.10

```
 00:01:45 02:56 2A Vl47 !--- Wireless Client C1 to Stream multicast address .
*,239.255.255.250 192.168.48.11 00:05:03 02:58 2A Vl48
*,239.255.255.250 10.63.85.163 21:19:25 02:40 2A Vl84
```

You can also use the command **show ip mroute count** in order to ensure that multicast routing works properly:

<#root>

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
```

From these outputs, you can see that multicast traffic flows from source W1 and is received by the group members.

Related Information

- Enterprise Mobility 8.5 Design Guide
- VLANs on Wireless LAN Controllers Configuration Example
- Wireless LAN Controller and Lightweight Access Point Basic Configuration Example
- IP Multicast: White Papers
- Cisco Technical Support & Downloads