

# 与无线局域网控制器(WLCs)和接入点(CAPWAP)配置示例的组播

## Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[在无线局域网控制器\(WLCs\)的组播](#)

[在不同的WLC的广播工作情况](#)

[监听在WLC的IGMP](#)

[漫游无线的组播](#)

[指南为使用组播模式](#)

[网络设置](#)

[Configure](#)

[配置组播的无线网络](#)

[配置客户端的WLAN](#)

[通过GUI配置组播模式](#)

[通过CLI配置组播模式](#)

[配置组播的有线网络](#)

[验证并且排除故障](#)

[Related Information](#)

## Introduction

本文档介绍了有关如何配置组播的无线 LAN 控制器 (WLC) 和轻量接入点 (LAP) 并与启用组播的有线网络进行通信的示例。

## Prerequisites

## Requirements

尝试进行此配置之前，请确保满足以下要求：

- APs和Cisco WLCs的配置的基础知识。
- 知识如何配置基本的路由和组播在有线网络。

## Components Used

本文档中的信息基于以下软件和硬件版本：

- 运行固件版本8.5的Cisco 3504 WLC
- Cisco 3702系列膝部

- 有Intel的(R)双波段无线AC 8265适配器微软视窗10无线客户端
- 运行Cisco IOS软件版本12.2(18)的Cisco 6500交换机
- 运行Cisco IOS Software Release 16.3.7的两Cisco 3650系列交换机

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, make sure that you understand the potential impact of any command.

## 组播在无线局域网控制器(WLCs)

如果您的网络支持信息包组播，您能配置控制器用途为了同时传输在CAPWAP的组播信息包到所有或几接入点的组播方法。控制器在两个模式进行组播：

- 单播模式-在此模式下，控制器单播对每个AP的每个组播信息包被关联对控制器。此模式是效率低的，但是也许需要在不支持组播的网络。
- 组播模式-在此模式下，控制器发送组播信息包到CAPWAP组播组。此方法在控制器处理器减少在头顶上并且转移信息包复制工作到您的网络，比单播方法效率更高。当您使用不同的VLAN/Subnet AP和WLC然后时组播路由是必须在纸的反面支持转发downlink CAPWAP组播信息包从WLC到AP。

当您enable (event)组播模式和控制器从有线LAN时收到一个组播信息包，控制器封装信息包使用CAPWAP并且转发信息包到组地址CAPWAP的组播。控制器总是使用管理接口发送组播信息包。在组播组的接入点收到信息包并且转发它到所有BSSIDs被映射对客户端接收组播数据流的接口。从接入点方面，组播看来是广播到所有Ssid。

### 在不同的WLC的广播工作情况

默认情况下，WLC不会转发任何广播包(例如Upnp数据流)，除非广播转发是启用的。发出从WLC CLI为了enable (event)广播的此命令：

```
config network broadcast enable
```

或者enable (event)它与GUI：

The screenshot shows the Cisco WLC GUI configuration page for a controller. The 'General' tab is selected, and the 'Broadcast Forwarding' option is highlighted with a red circle and set to 'Enabled'. Other settings like 'LAG Mode on next reboot' and 'AP Multicast Mode' are also visible. The 'Apply' button is circled in red in the top right corner.

| Setting                      | Value                       |
|------------------------------|-----------------------------|
| Name                         | wifi-cisco-main-ct8510-prim |
| 802.3x Flow Control Mode     | Disabled                    |
| LAG Mode on next reboot      | Enabled                     |
| <b>Broadcast Forwarding</b>  | <b>Enabled</b>              |
| AP Multicast Mode            | Unicast                     |
| AP IPv6 Multicast Mode       | Unicast                     |
| AP Fallback                  | Enabled                     |
| CAPWAP Preferred Mode        | ipv4                        |
| Fast SSID change             | Disabled                    |
| Link Local Bridging          | Disabled                    |
| Default Mobility Domain Name | wifi-cisco-main             |
| RF Group Name                | wifi-cisco-main             |

广播使用在WLC被配置的**组播模式**，即使组播没有打开。这是因为您不能设置IP地址或模式，除非您enable (event)组播在GUI。所以，如果组播模式是单播，并且广播打开，这是模式广播用途(广播数据流被复制在WLC和单播对每个AP)。如果设置组播模式组播与组播地址，则请播放用途此模式(每个广播包通过组播组被发送到APs)。

**Note:**直到版本7.5，用于CAPWAP组播的端口号是12224。从版本7.6向前，用于CAPWAP的端口号更改到5247。

与AAA覆盖的组播从无线局域网控制器版本4.2支持及以后。必须enable (event) IGMP监听在控制器的您使组播与AAA覆盖工作。

## 监听在WLC的IGMP

WLC支持监听的IGMP更好导向组播信息包。当此功能是启用的时，控制器采集从客户端的IGMP报告，处理报告，在检查第3层组播地址和VLAN号以后创建唯一组播组标识(MGIDs)从IGMP报告，并且发送IGMP报告到基础设施交换机。控制器发送与源地址的这些报告作为从客户端收到报告的接口地址。

控制器然后更新在AP的接入点MGID表与客户端MAC地址。当控制器收到一个特定组播组的时组播数据流，寄它给所有APs。然而，只那些有活动客户端监听或被预订该组播组发送在该特定的WLAN的组播数据流的APs。IP信息包转发与为入口VLAN和目的地组播组是唯一的MGID。第2层组播信息包转发与为入口接口是唯一的MGID。

控制器技术支持组播监听为IPv6组播的监听程序发现(MLD) v1。此功能记录并且提供IPv6组播流到要求他们的客户端。为了支持IPv6组播，您必须enable (event)全局组播模式。

**Note:**当您禁用全局组播模式时，控制器仍然转发IPv6 ICMP组播消息，例如路由器公告，并且DHCPv6请求，和这些对于IPv6是必需的工作。结果，启动在控制器的全局组播模式不影响ICMPv6和DHCPv6消息。这些消息，不论全局组播模式是启用的，永远将转发。

当监听的IGMP是失效的时，下列是真的：

- 当发送组播数据到接入点时，控制器总是使用第2层MGID。被创建的每个接口分配一个层2个MGID。例如，管理接口有MGID 0，并且被创建的第一个动态接口分配MGID 8，增加，当每个动态接口被创建。
- 自客户端的IGMP信息包转发到路由器。结果，router igmp表用客户端的IP地址更新作为最后申报人。

当监听的IGMP是启用的时，下列是真的：

- 控制器总是使用第3层MGID所有第3层组播数据流被发送到接入点。对于所有第2层组播数据流，它继续对使用第2层MGID。
- 从无线客户端的IGMP报告信息包由控制器消耗或吸收，生成客户端的一次查询。在路由器发送IGMP查询后，控制器发送IGMP报告用其接口IP地址作为组播组的监听程序IP地址。结果，router igmp表用控制器IP地址更新作为组播监听程序。
- 当听组播组时的客户端从一个控制器漫游到另一个，第一个控制器传达监听的客户端所有组播组信息给第二个控制器。结果，第二个控制器能立即创建客户端组播组信息。第二个控制器发送IGMP报告到客户端监听的所有组播组的网络。在组播数据无缝的转移的此进程帮助到客户端。

注意：

- MGIDs是控制器特定。来自在两个不同的控制器的同样VLAN的同样组播组信息包可以被映射到两不同MGIDs。
- ，如果第2层组播是启用的，单个MGID分配到来自接口的所有组播地址。
- 组播组的最大数量每个控制器的VLAN支持的是100。

## 漫游无线的组播

一个组播客户端的一个主要挑战无线环境的是维护其组播组成员，当移动关于WLAN。从AP对AP移动在无线连接的丢包能的客户端的组播应用导致中断。互联网组管理协议(IGMP)播放在动态组成员信息维护的一重要的角色。

IGMP基本理解是重要了解什么发生在客户端的组播会话，当漫游关于网络时。在第2层漫游的事例，会话被维护，因为外国AP，若被设定适当地，已经属于组播组，并且数据流没有被以隧道传输到网络的一个不同的定位点。第3层漫游的环境如此是复杂，并且，从属在什么隧道模式您在您的控制器配置了，从无线客户端的IGMP发送的消息可以受影响。在控制器的默认移动性隧道模式是不对称的。这意味着对客户端的回程数据流被发送到锚点WLC然后转发到外国WLC，相关的客户端连接驻留。转发出局信息包外国WLC接口。在对称移动性隧道模式，Inbound与Outbound数据流被建立隧道到锚点控制器。

如果监听的客户端漫游到在一个不同的子网的一个控制器，组播信息包被建立隧道到客户端的锚点控制器避免反向路径过滤(RPF)检查。锚点然后转发组播信息包到基础设施交换机。

## 指南为使用组播模式

- Cisco无线网络解决方案使用一些IP地址范围特定目的，并且您应该记住这些范围，当您配置一个组播组时：224.0.0.0通过224.0.0.255 -后备的链路本地地址224.0.1.0通过238.255.255.255 -全局scoped地址239.0.0.0通过239.255.x.y /16 - Limited范围地址
- 当您enable (event)在控制器的组播模式，您必须也配置组地址CAPWAP的组播。使用IGMP，APs预订CAPWAP组播组。
- APs在监控模式下，嗅探器模式或者恶意探测器模式不加入组地址CAPWAP的组播。
- 在控制器配置的CAPWAP组播组应该是不同的为不同的控制器。
- CAPWAP APs传输组播信息包一致被配置的必须的数据速率。由于组播帧没有被重新传输在MAC控制层，信元的边缘的客户端也许不能成功接受他们。如果可靠的接收是目标，应该传输组播帧以低数据速率，通过禁用更高的必须的数据速率。如果为高数据传输比组播帧需要技术支持，收缩信元大小和禁用所有较低的数据速率，或者使用媒体流也许是有用的。根据您的需求，您能采取这些行动：如果需要传输与最极大的可靠性的组播数据，并且，如果没有对巨大组播带宽的需要，然后请配置一个基本速率，是足够低到达无线信元的边缘。如果需要传输组播数据以某一数据速率为了达到有些吞吐量，您能配置该费率作为最高的基本速率。您能也设置nonmulticast客户端覆盖的一个更低的基本速率。配置媒体流。
- 组播模式不在intersubnet移动性事件间运行例如客户隧道。它，然而，在第3层间运行漫游。
- 对于CAPWAP，控制器丢包组播发送的数据包到UDP控制和数据端口5246和5247，分别。所以，您也许要考虑不使用这些端口号以在您的网络的组播应用。Cisco建议您在[此WLC协议表里](#)不使用作为是列出的任何组播UDP端口控制器使用的UDP端口。
- Cisco建议在您的网络的所有组播应用没有使用作为CAPWAP组播被配置的组播地址组地址在控制器。
- 为了使组播工作在Cisco 2504 WLC，您必须配置组播IP地址。
- Cisco弹性7500系列WLCs不支持组播模式。
- Cisco弹性7510 WLCs不支持监听的IGMP和的MLD。
- Cisco 8510 WLCs：如果IPv6技术支持在与中央交换客户端的FlexConnect APs需要您必须enable (event)组播单播。您能从组播模式变成组播单播模式，只有当全局组播是失效的，意味着不支持监听的IGMP或的MLD。FlexConnect APs不与组播多播组产生关联。FlexConnect APs不支持监听的IGMP或的MLD。监听的IGMP和的MLD在组播组播模式下仅允许本地传送方式APs。由于监听的VideoStream需要IGMP或MLD，VideoStream功能在本地传送方式APs仅

运作，如果组播组播模式和监听是启用的。

- Cisco Mobility Express控制器不支持AP组播模式。
- Cisco建议您不使用广播单播或在控制器的组播单播模式设置APs被加入的地方超过50。
- 当曾经本地和FlexConnect AP模式时控制器的组播支持为另外平台有所不同。影响组播转发的参数是：控制器平台。在控制器的全局AP组播模式配置。AP的模式-本地，FlexConnect中央交换。对于本地交换，它没有送信/受信到/从控制器的信息包，因此不重要在控制器组播模式被配置。 **Note:**只有当他们在中央交换了WLANs，FlexConnect APs将参加CAPWAP组播组。与本地仅交换的WLANs的弹性APs不参加CAPWAP组播组。
- 有效对版本8.2.100.0，从控制器下载某些旧的配置由于在此版本引入的组播和IP地址验证是不可能的。全局组播的平台支持和组播模式在下面的表里列出。表1.全局组播和组播模式的平台支持

## 网络设置

所有设备和设置在图表中表示：

设备需要为基本IP连接和enable (event)组播被配置在网络。所以，用户能从纸的反面发送和接收组播数据流到无线边反之亦然。

本文使用这些IP地址WLC、AP和无线客户端：

```
config network broadcast enable
```

## Configure

为了配置此设置的设备，这些需要执行：

- [配置组播的无线网络](#)
- [配置组播的有线网络](#)

## 配置组播的无线网络

在您配置在WLCs前的组播，您必须配置基本操作的WLC和注册APs到WLC。本文档假设已配置WLC进行基本操作，并且已在WLC中注册LAP。如果您是尝试设置WLC以对LAP执行基本操作的新用户，请参阅[在无线LAN控制器\(WLC\)中注册轻量AP\(LAP\)](#)。

一旦膝部注册对WLC，请完成这些任务为了配置膝部和WLC此设置的：

1. [配置客户端的WLAN](#)
2. [Enable \(event\)以太网通过GUI组播模式](#)

## 配置客户端的WLAN

第一步是创建无线客户端能连接和接受对网络的访问的WLAN。完成这些步骤为了创建在WLC的一WLAN：

1. 要创建WLAN，请从控制器GUI中单击WLANs。

2. 要配置新的 WLAN，请单击 **New**。在本例中，WLAN被命名MulticastUsers，并且WLAN ID是1。

The screenshot shows the Cisco WLAN configuration interface. The top navigation bar includes 'MONITOR', 'WLANs', 'CONTROLLER', 'WIRELESS', 'SECURITY', and 'MANAGEMENT'. The 'WLANs' menu is highlighted. Below the navigation bar, the 'WLANs' section is visible, with a 'WLANs' sub-menu highlighted. The 'WLANs > New' configuration form is shown, with the following fields:

| Field        | Value          |
|--------------|----------------|
| Type         | WLAN           |
| Profile Name | MulticastUsers |
| SSID         | MulticastUsers |
| ID           | 1              |

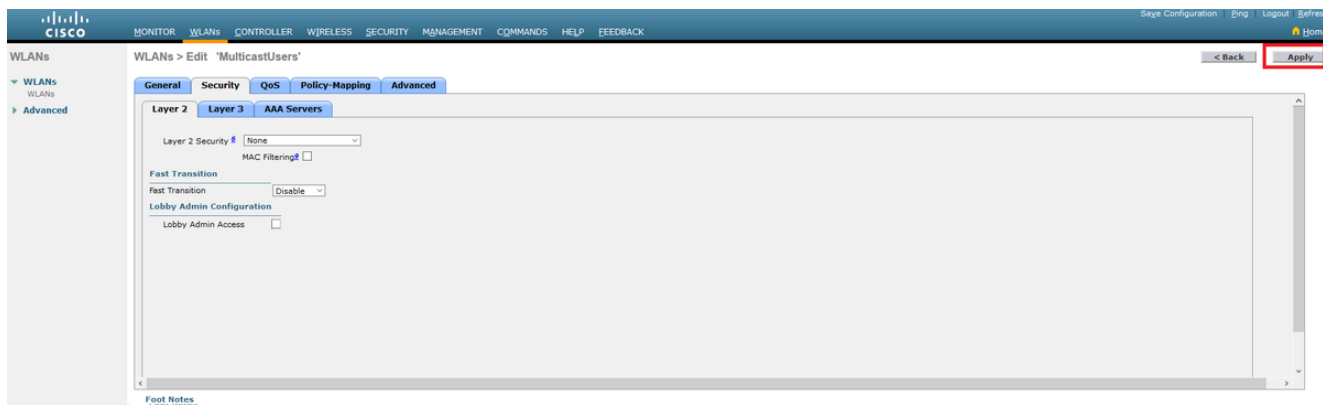
The 'Apply' button is highlighted in the bottom right corner.

3. 单击 **Apply**。
4. 在“WLAN”>“Edit”窗口中，定义特定于该 WLAN 的参数。
5. 对于WLAN，从接口名称字段请选择适当的接口。此示例映射MulticastUsers (192.168.47.0/24)接口对WLAN。
6. 选择其他参数，取决于设计需求。在本例中我们使用WLAN没有L2安全(请打开WLAN)。

The screenshot shows the Cisco WLAN configuration interface for editing the 'MulticastUsers' WLAN. The top navigation bar includes 'MONITOR', 'WLANs', 'CONTROLLER', 'WIRELESS', 'SECURITY', 'MANAGEMENT', 'COMMANDS', 'HELP', and 'FEEDBACK'. The 'WLANs' menu is highlighted. Below the navigation bar, the 'WLANs > Edit 'MulticastUsers'' configuration form is shown, with the following fields:

| Field                        | Value                                                                                                   |
|------------------------------|---------------------------------------------------------------------------------------------------------|
| Profile Name                 | MulticastUsers                                                                                          |
| Type                         | WLAN                                                                                                    |
| SSID                         | MulticastUsers                                                                                          |
| Status                       | <input checked="" type="checkbox"/> Enabled                                                             |
| Security Policies            | [WPA2][Auth(802.1X)]<br>(Modifications done under security tab will appear after applying the changes.) |
| Radio Policy                 | All                                                                                                     |
| Interface/Interface Group(G) | multicastusers                                                                                          |
| Multicast Vlan Feature       | <input type="checkbox"/> Enabled                                                                        |
| Broadcast SSID               | <input checked="" type="checkbox"/> Enabled                                                             |
| NAS-ID                       | none                                                                                                    |

The 'Interface/Interface Group(G)' field is highlighted in red. The 'Foot Notes' section at the bottom indicates: '1 Web Policv cannot be used in combination with IPsec'.



## 7. 单击 Apply。

使用CLI，发出这些命令为了配置在WLC的WLANs：

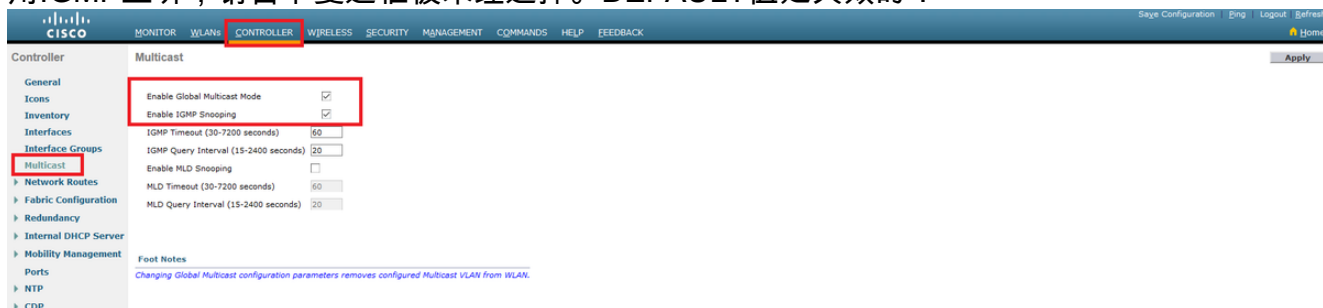
1. 发出**设置WLAN创建** `<wlan-id> <wlan-name>`命令为了创建一新的WLAN。对于WLAN id，从1请输入ID到16。对于wlan名称，请进入SSID至31个字母或数字字符。
2. 发出**设置WLAN enable (event)** `<wlan-id>`命令为了enable (event) WLAN。对于在本文的示例，命令是：

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

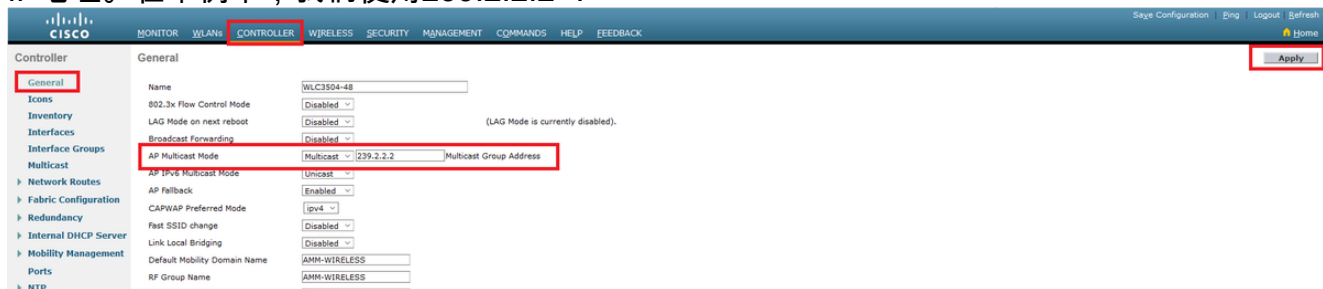
## 通过GUI配置组播模式

下一步是配置组播的WLC。完成这些步骤：

1. 选择**Controller>组播**打开组播页。
2. 选择**Enable (event)**全局组播Mode复选框配置发送组播信息包。默认值是禁用。
3. 如果希望对enable (event) IGMP监听，请选择**Enable (event) IGMP**监听的复选框。如果要禁用IGMP监听，请留下复选框被未经选择。DEFAULT值是失效的：



4. 选择**Controller>常规**对，并且对于AP从下拉菜单的组播模式请选择"Multicast"并且配置组播IP地址。在本例中，我们使用239.2.2.2：



## 5. 单击 Apply。

## 通过CLI配置组播模式

通过CLI发出这些命令为了enable (event)组播：

1. 从line命令，请发出**设置网络组播全局enable命令**。
2. 从line命令，请发出**设置网络组播模式组播<multicast-group-ip-address>命令**。对于在本文的示例，命令是：

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

在管理员enable (event)组播(默认情况下组播模式被禁用)后并且配置CAPWAP组播组，新的组播算法在这些方式之一中工作：

### 当组播组的来源在有线LAN：

一组播是启用的，并且CAPWAP配置组播组AP问题IGMP请求为了参加控制器CAPWAP组播组。这触发组播状态的正常设置在支持组播的路由器，在控制器和APs之间。组播组的IP原地址是控制器管理接口IP地址。

当控制器从任何第一跳跃路由器的时客户端收到一个组播信息包VLAN，传送信息包给CAPWAP组播组通过管理接口在最低的QoS级别。CAPWAP组播信息包的QoS位是硬编码的在最低级，并且不可能由用户更改。

支持组播的网络传送CAPWAP组播信息包到参加了CAPWAP组播组的其中每一个APs。支持组播的网络使用在路由器的正常组播机制复制信息包，当必要时，因此组播信息包到达所有APs。这解除从组播信息包的复制的控制器。

APs能收到其他组播信息包，但是处理来自控制器他们当前被加入仅的组播信息包。丢弃所有其他复制。如果超过一WLAN SSID被关联对VLAN从发送原始组播信息包，AP传输在每WLAN SSID的组播信息包(跟随对WLAN在CAPWAP报头的位图)。另外，如果该WLAN SSID在两无线电(802.11g和802.11a)，两无线电传输在WLAN SSID的组播信息包，如果有与它产生关联的客户端，即使那些客户端没有要求组播数据流。

### 当组播组的来源是无线客户端：

组播信息包是单播(CAPWAP被封装)从AP到控制器，类似于标准的无线客户端数据流。

控制器做两复制组播信息包。一复制被派出与到达的WLAN SSID产生关联的VLAN。此在接受组播流和路由器的有线LAN的enable (event)接受器得知新的组播组。信息包的第二复制CAPWAP被封装和被发送到CAPWAP组播组，以便无线客户端能接收组播流。

## 配置组播的有线网络

为了配置此设置的有线网络，您需要配置基本的路由和enable (event)组播路由的L3核心交换机：

所有组播协议可以用于有线网络。本文使用PIM-DM作为组播协议。参考[Cisco IOS IP组播配置指南](#)关于能使用组播在有线网络的不同的协议的详细信息。

### 挖出果核交换机配置

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

默认情况下，因为监听的IGMP在Cisco交换机，被启用配置在L2接入交换机没有必要。



# 验证并且排除故障

Use this section to confirm that your configuration works properly.

为了验证配置，您需要从来源W1发送组播数据流和检查组播数据流是否流经有线网络并且到达有线和无线组成员(C1)。

如果IP组播在您的网络，正确地配置请执行此任务为了测试。

检查在核心交换机和IGMP会员wth的组播路由show ip mroute命令并且显示ip igmp会员。 前一个示例的输出显示得这里。

```
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

您能也使用show ip mroute count命令为了保证组播路由适当地运作：

```
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
```

从这些输出，您能看到从来源W1的组播通信流和由组成员接受。

## Related Information

- [企业移动性8.5设计指南](#)
- [在无线局域网控制器配置示例的VLAN](#)
- [无线 LAN 控制器和轻量接入点基本配置示例](#)
- [IP组播：白皮书](#)
- [无线产品支持](#)
- [Technical Support & Documentation - Cisco Systems](#)