

# Multicast with Wireless LAN Controllers (WLCs) and Lightweight Access Points (LAPs) Configuration Example

Document ID: 81671

---

## Introduction

## Prerequisites

Requirements

Components Used

Conventions

## Multicast in Wireless LAN Controllers (WLCs)

Multicast Behavior in Different WLC Software Versions

Wireless Multicast Roaming

Guidelines for Using Multicast Mode

## Network Setup

Configure

Configure the Wireless Network for Multicasting

Configure the Wired Network for Multicasting

## Verify and Troubleshoot

## Related Information

---

## Introduction

This document provides a configuration example on how to configure Wireless LAN Controllers (WLCs) and Lightweight Access Points (LAPs) for multicasting and communication with a multicast enabled wired network.

## Prerequisites

### Requirements

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

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

### Components Used

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

- Cisco 4400 WLC that runs firmware release 4.0
- Cisco 1000 Series LAPs
- Cisco 802.11a/b/g Wireless Client Adapter that runs firmware release 2.6
- Cisco 2500 Router that runs Cisco IOS® Software Release 12.4(2)
- Two Cisco 3500 XL Series Switches that run Cisco IOS Software Release 12.0(5)WC3b

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.

## Conventions

Refer to Cisco Technical Tips Conventions for more information on document conventions.

## Multicast in Wireless LAN Controllers (WLCs)

Before Cisco Unified Wireless Network Software Release 3.2, when IP multicast was enabled, the controller delivered multicast packets to wireless LAN (WLAN) clients by making copies of the multicast packets, then forwarded the packets through a unicast Lightweight Access Point Protocol (LWAPP) tunnel to each access point (AP) connected to the controller. Each multicast frame received by the controller from a VLAN on the first hop router was copied and sent over the LWAPP tunnel to each of the APs connected to it.

The controller might need to generate up to 300 copies of each multicast packet, which depends on the number of APs. This mechanism is inefficient, and places a large processing burden on the controller. This floods the network with a large number of duplicate unicast packets.

In Cisco Unified Wireless Network Software Releases 3.2 and later, the multicast performance of the Cisco Unified Wireless Network has been optimized. These releases introduce a more efficient way to deliver multicast traffic from the controller to the APs. Instead of using unicast to deliver each multicast packet over the LWAPP tunnel to each AP, an LWAPP multicast group is used to deliver the multicast packet to each AP. This allows the routers in the network to use standard multicast techniques to replicate and deliver multicast packets to the APs. For the LWAPP multicast group, the controller becomes the multicast source and the APs become the multicast receivers. For the multicast performance feature, the APs accept Internet Group Management Protocol (IGMP) queries only from the router and multicast packets with a source IP address of the controller with which they are currently associated.

If your network supports packet multicasting, you can configure the multicast method that the controller uses. The controller performs multicasting in two modes:

- **Unicast mode** In this mode, the controller unicasts every multicast packet to every AP associated to the controller. This mode is inefficient but might be required on networks that do not support multicasting.
- **Multicast mode** In this mode, the controller sends multicast packets to an LWAPP 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.

You can enable multicast mode using the controller GUI or CLI.

## Multicast Behavior in Different WLC Software Versions

Before WLC firmware release 4.0.206.0, multicast packet forwarding enabled either in unicast or multicast mode, also enabled broadcast packet forwarding. In WLC firmware release 4.0.206.0, broadcast and multicast traffic must be enabled separately. Broadcast is disabled by default. Issue this command from the WLC CLI in order to enable broadcast:

```
config network broadcast enable
```

Also, broadcast uses the **multicast mode** that is configured on the WLC, even if multicast is not turned on. If you want to enable broadcast without enabling multicast, you perform this via the CLI but not through the GUI. This is because you cannot set the IP address or the mode unless you enable multicast in the GUI. Therefore, if multicast mode is unicast and broadcast is turned on, this is the mode broadcast uses (broadcast

traffic is replicated and unicast to each AP). If multicast mode is set to multicast with a multicast address, then broadcast uses this mode (each broadcast packet is sent via the multicast group to the APs).

```
config network multicast mode multicast
                                Or
config network multicast unicast
```

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.

In controller software release 4.2, IGMP snooping is introduced 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 checking 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.

**Note:** IGMP snooping is not supported on the 2000 series controllers, the 2100 series controllers, or the Cisco Wireless LAN Controller Network Module for Cisco Integrated Services Routers.

Multicast applications have known performance limitations on the 2100 series controllers and the Cisco Wireless LAN Controller Network Module for Cisco Integrated Services Routers. Cisco is working to address these limitations in a future production code release. In the meantime, Cisco recommends that you use the 4400 series or WiSM controllers for multicast intensive applications.

**Note:** Multicast is not supported on APs that are connected directly to the local port of a 2100 series controller.

Refer to the *Cisco Unified Wireless Multicast Design* chapter of the Enterprise Mobility design guide for more information on multicast with WLCs.

This document provides a configuration example that illustrates how to configure multicasting on WLCs in order to connect to a multicast enabled wired network.

## 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. Internet Group Management Protocol (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 about 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 traffic are tunneled to the anchor controller.

## Guidelines for Using Multicast Mode

Use these guidelines when you enable multicast mode on your network:

- The Cisco Unified Wireless Network solution uses some IP address ranges for specific purposes. Keep these ranges in mind when you configure a multicast group:

Although not recommended, any multicast address can be assigned to the LWAPP multicast group; this includes the reserved link local multicast addresses used by OSPF, EIGRP, PIM, HSRP, and other multicast protocols.

Cisco recommends that multicast addresses be assigned from the administratively scoped block 239/8. IANA has reserved the range of 239.0.0.0–239.255.255.255 as administratively scoped addresses for use in private multicast domains. See the note for additional restrictions. These addresses are similar in nature to the reserved private IP unicast ranges, such as 10.0.0.0/8, defined in RFC 1918. Network administrators are free to use the multicast addresses in this range inside of their domain without fear of conflict with others elsewhere in the Internet. This administrative or private address space must be used within the enterprise and its leave or entry blocked from the autonomous domain (AS).

**Note:** Do not use the 239.0.0.X address range or the 239.128.0.X address range. Addresses in these ranges overlap with the link local MAC addresses and flood out all switch ports, even with IGMP snooping turned on.

Cisco recommends that enterprise network administrators further subdivide this address range into smaller geographical administrative scopes within the enterprise network to limit the "scope" of particular multicast applications. This prevents high-rate multicast traffic from leaving a campus (where bandwidth is plentiful) and congesting the WAN links. It also allows for efficient filtering of the high bandwidth multicast from reaching the controller and the wireless network. For more information on multicast address guidelines, refer to Guidelines for Enterprise IP Multicast Address Allocation.

- When you enable multicast mode on the controller, you must configure an LWAPP multicast group address on the controller. APs subscribe to the LWAPP multicast group using Internet Group Management Protocol (IGMP).
- Cisco 1100, 1130, 1200, 1230, and 1240 APs use IGMP versions 1, 2, and 3. However, Cisco 1000 Series APs use only IGMP v1 to join the multicast group.
- Multicast mode works only in Layer 3 LWAPP mode.
- APs in monitor mode, sniffer mode, or rogue detector mode do not join the LWAPP multicast group address.
- When you use controllers that run version 4.1 or earlier, you can use the same multicast address on all the controllers. If you use controllers that run version 4.2 or later, the LWAPP multicast group configured on the controllers must be different for each controller used on the network.
- If you use controllers with version 4.1 or earlier, the multicast mode does not work across intersubnet mobility events, such as guest tunneling, site-specific VLANs, or interface override that uses RADIUS. The multicast mode does work in these subnet mobility events when you disable the Layer 2 IGMP snooping/CGMP features on the wired LAN.

In later versions, that is, 4.2 or later, the multicast mode does not operate across intersubnet mobility events, such as guest tunneling. It does, however, operate with interface overrides that use RADIUS (but only when IGMP snooping is enabled) and with site-specific VLANs (access point group VLANs).

- The controller drops any multicast packets sent to the UDP port numbers 12222, 12223, and 12224. Make sure the multicast applications on your network do not use those port numbers.
- Multicast traffic is transmitted at 6 Mbps in an 802.11a network. Therefore, if several WLANs attempt to transmit at 1.5 Mbps, packet loss occurs. This breaks the multicast session.

## Network Setup

In this setup, the wired network is comprised of the three routers, R1, R2 and R3, that run OSPF between them.

The wired hosts connect to the network through a Layer 2 switch which is connected to Router R1. The wireless network connects to the network through Router R3, as shown in the diagram.

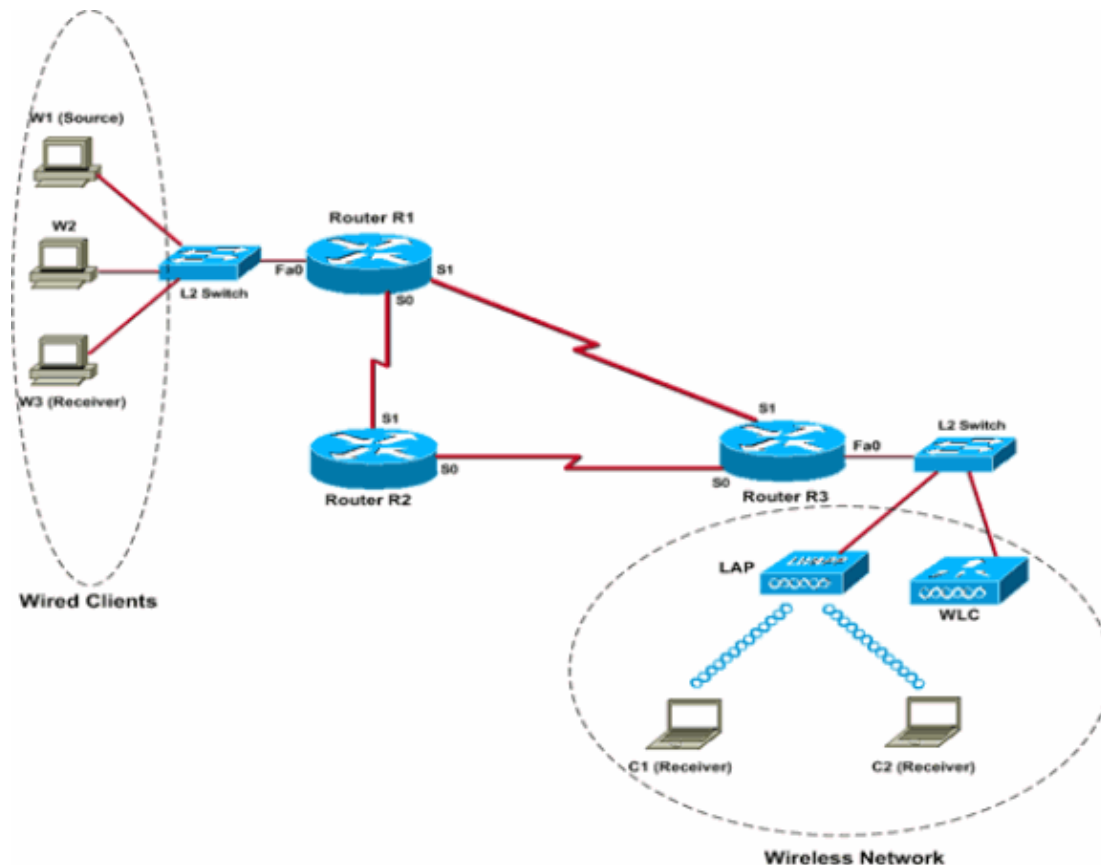
The devices need to be configured for basic IP connectivity and enable multicasting in the network. Therefore, users can send and receive multicast traffic from the wired side to the wireless side and vice versa.

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

```

WLC Management Interface IP address: 172.16.1.30/16
WLC AP Manager Interface IP address: 172.16.1.31/16
LAP IP address: 172.16.1.50/16
Wireless Client C1 IP address: 172.16.1.75/16
Wireless Client C2 IP address: 172.16.1.76/16
Wired Client W1 IP address: 192.168.0.20/16
Wired Client W2 IP address: 192.168.0.30/16
Wired Client W3 IP address: 192.168.0.40/16

```



## 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 LAPs 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).

**Note:** Do not use the 239.0.0.X or the 239.128.0.X address ranges. Addresses in these ranges overlap with the link local MAC addresses and flood all switch ports, even with IGMP snooping enabled. Refer to the Layer 2 Multicast Addresses section of IP Multicast Technology Overview for more information on overlapping multicast MAC addresses.

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

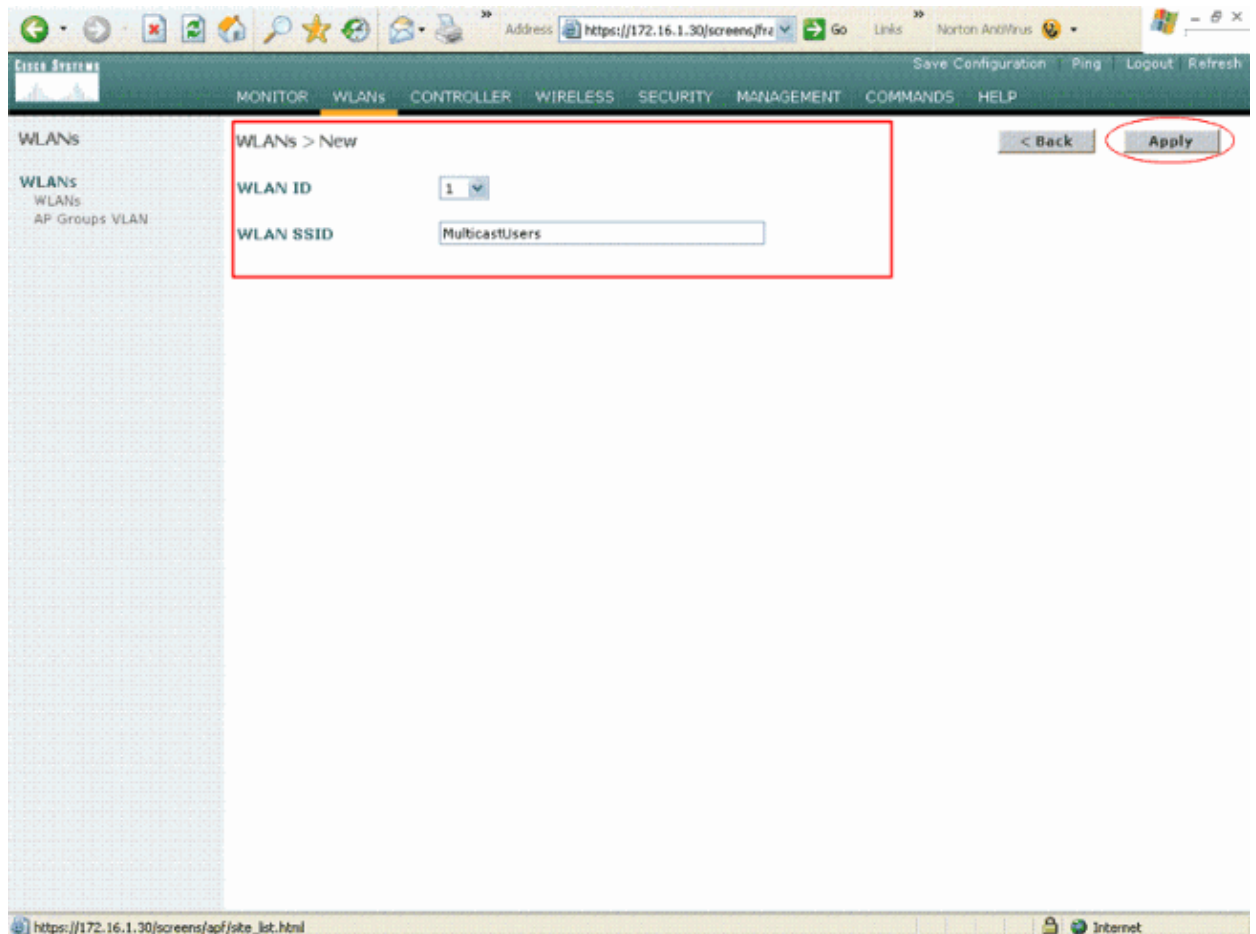
1. Configure the WLAN for Clients
2. Enable Ethernet Multicast Mode via the GUI

#### Configure the WLAN for Clients

The first step is create a WLAN to which 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.

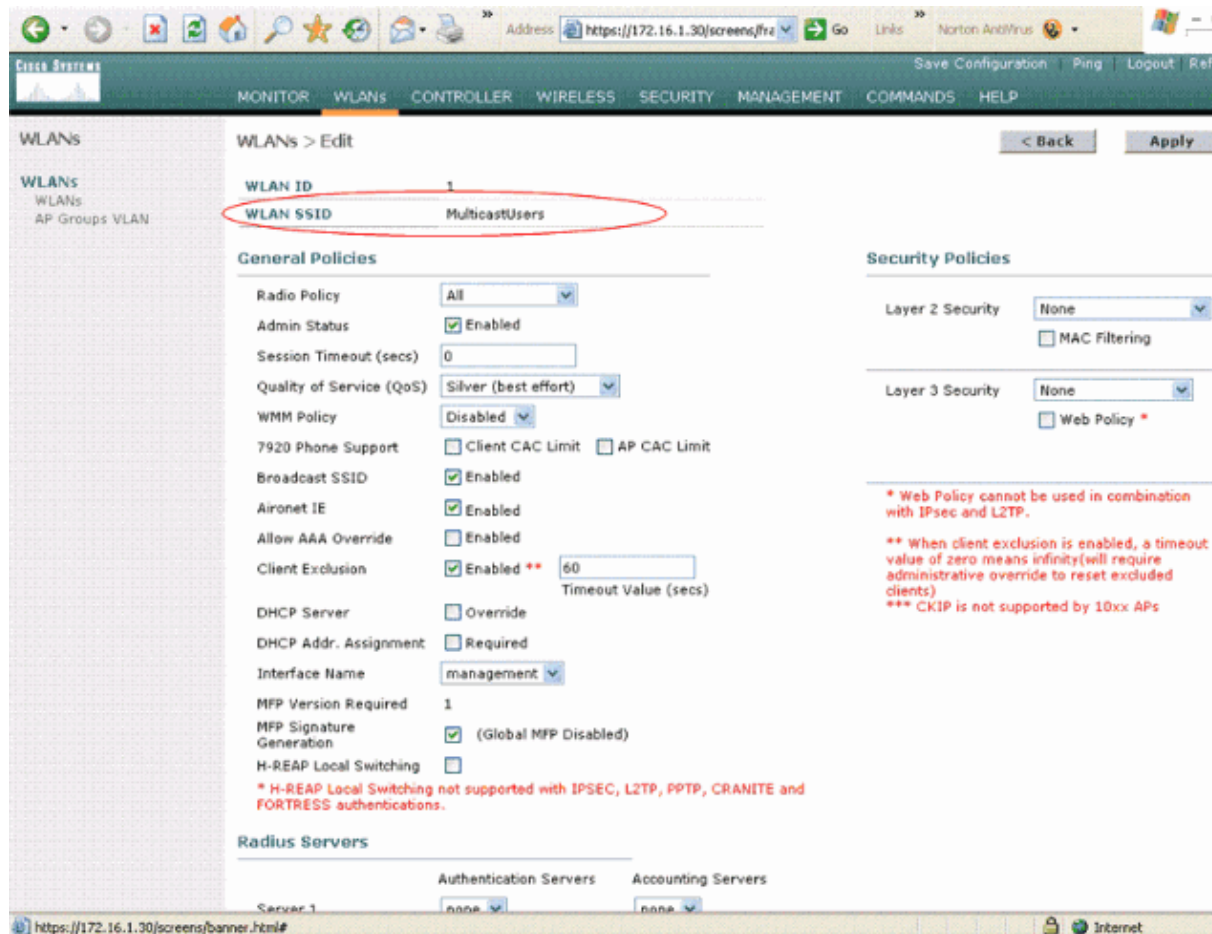
a. For the WLAN, choose the appropriate interface from the Interface Name field.

This example maps the management interface to the WLAN.

b. Select the other parameters, which depends on the design requirements.

The default values are used in this example.

c. Click **Apply**.



**Note:** In this example, Layer 2 Security methods to authenticate wireless users are not used. Therefore, choose **None** in the Layer 2 Security field. By default, the Layer 2 Security option is 802.1x.

**Note:** Instead of mapping the WLAN (SSID) to the management interface, dynamic interfaces can also be configured on the WLC to segment the wireless users and the WLAN can be mapped to the dynamic interfaces. Refer to VLANs on Wireless LAN Controllers Configuration Example for information on how to configure dynamic interfaces on WLCs.

Issue these commands in order to configure the WLANs on WLC using 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:

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

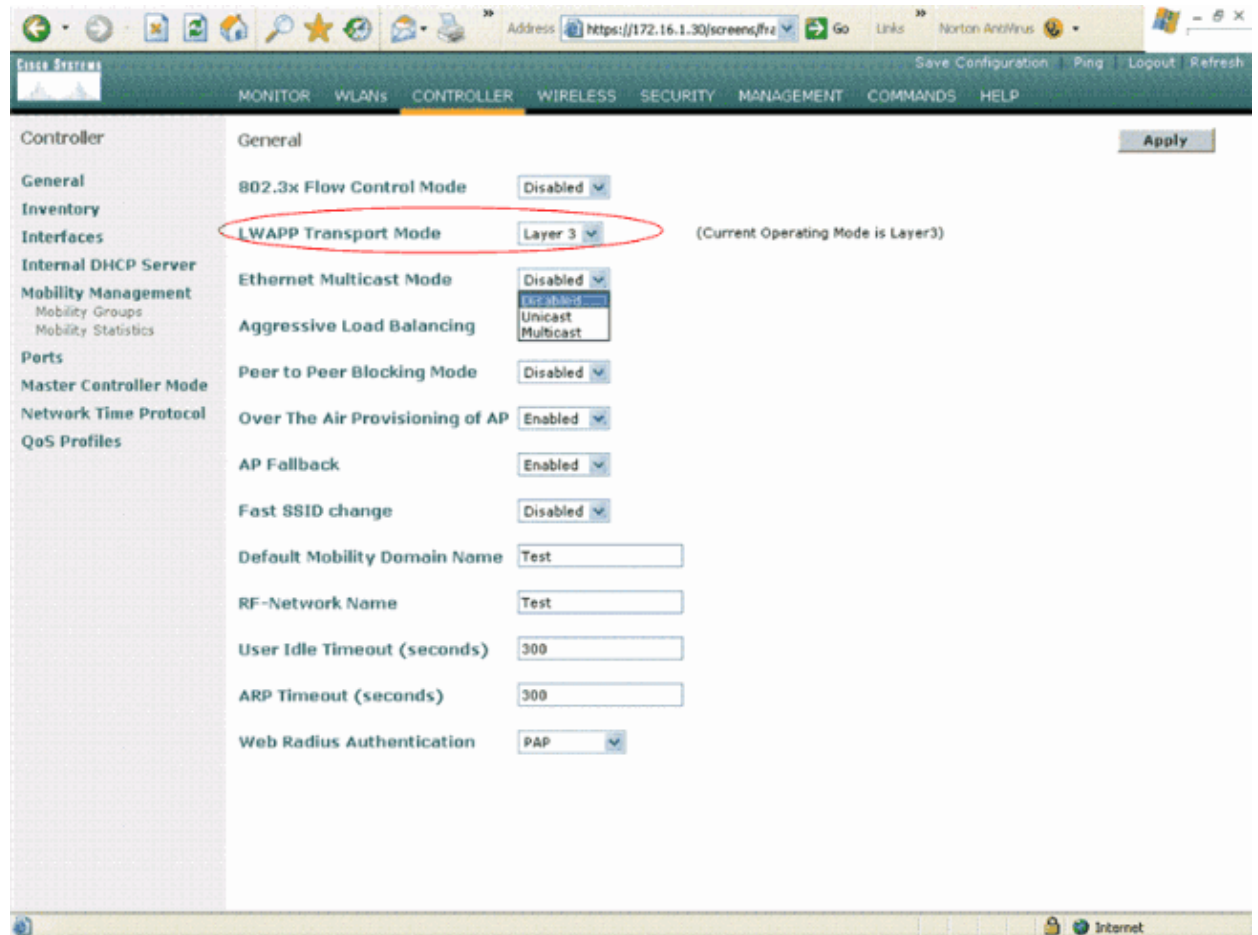
## Enable Ethernet Multicast Mode via the GUI

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

1. From the controller general web page, ensure that the LWAPP transport mode is set to **Layer 3**.



The multicast performance feature works only in this mode.



**Note:** When multicast is enabled as **multicast unicast**, packets are replicated for each AP; this can be processor intensive, so use it with caution. Multicast enabled as **multicast multicast** uses the user assigned multicast address to do a more traditional multicast out to the APs.

2. From the drop-down menu for the Ethernet Multicast Mode, choose **Multicast** and enter a Multicast Group Address.

In this example, the address is 239.255.1.60.



### 3. Click **Apply**.

**Note:** The WLC 4100 does not support multicast mode. Multicast is only done in unicast mode. This means that the controller has to replicate the multicast packet for each AP and unicast the multicast packet to each of the APs.

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

- a. From the command line, issue the **config network multicast global enable** command.
- b. From the command line, issue 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 239.255.1.60
```

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

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

The LWAPP APs download the controller LWAPP multicast group address during the normal join process (at boot time) to the controller. After an AP joins a controller and downloads its configuration, the AP issues an IGMP request in order to join the controller LWAPP 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, not the AP-manager IP address used for Layer 3 mode.

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

The multicast-enabled network delivers the LWAPP multicast packet to each of the APs that have joined the LWAPP 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 to the VLAN from where the original multicast packet was sent, the AP transmits the multicast packet over each WLAN SSID (following to the WLAN bitmap in the LWAPP 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 (LWAPP-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 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 LWAPP-encapsulated

and is sent to the LWAPP 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 routers for basic connectivity and enable multicasting in the wired network.

As mentioned earlier, OSPF is used as the unicast routing protocol.

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

These are the configurations for Routers R1, R2 and R3:

Router R1
<pre>RouterR1#show run Building configuration...  Current configuration : 836 bytes ! version 12.2 service timestamps debug uptime service timestamps log uptime no service password-encryption ! hostname RouterR1 ! ! ip subnet-zero ! ip multicast-routing  !--- Enables IP Multicasting on the network.  ! ! ! interface Ethernet0  ip address 192.168.0.1 255.255.0.0  ip pim dense-mode  !--- Enables PIM-Dense Mode Multicast Protocol on the interface.   ip cgmpp  !--- Enables Cisco Group Management Protocol (CGMP) on the interface !--- connected to the Layer 2 switch.  ! interface Serial0  description Connected to RouterR2  ip address 10.2.3.2 255.255.255.0  ip pim dense-mode  !--- Enables PIM-Dense Mode Multicast Protocol on the interface.  ! interface Serial1  description Connected to RouterR3  ip address 10.2.4.1 255.255.255.0</pre>

```

ip pim dense-mode

!--- Enables PIM-Dense Mode Multicast Protocol on the interface.

!
interface Serial2
  no ip address
  shutdown
!
interface Serial3
  no ip address
  shutdown
!
interface BRI0
  no ip address
  encapsulation hdlc
  shutdown
!
router ospf 1

!--- Configures OSPF as the unicast routing protocol.

  log-adjacency-changes
  network 10.0.0.0 0.255.255.255 area 0
  network 192.168.0.0 0.0.255.255 area 0
  !
ip classless
ip http server
!
!
!
line con 0
line aux 0
line vty 0 4
!
end

```

## Router R2

```

RouterR2#show run
Building configuration...

Current configuration : 616 bytes
!
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname RouterR2
!
!
ip subnet-zero
!
ip multicast-routing

!--- Enables IP Multicasting on the network.

!
!
!
interface Ethernet0
  no ip address
  shutdown
!

```

```

interface Serial0
  description Connected to RouterR3
  ip address 10.2.2.2 255.255.255.0
  ip pim dense-mode

!--- Enables PIM-Dense Mode Multicast Protocol on the interface.

!
interface Serial1
  description Connected to RouterR1
  ip address 10.2.3.1 255.255.255.0
  ip pim dense-mode

!--- Enables PIM-Dense Mode Multicast Protocol on the interface.

!
router ospf 1

!--- Configures OSPF as the unicast routing protocol.

  log-adjacency-changes
  network 10.0.0.0 0.255.255.255 area 0
!
ip classless
ip http server
!
!
!
line con 0
line aux 0
line vty 0 4
!
end

```

### Router R3

```

RouterR3#show run
Building configuration...

Current configuration : 711 bytes
!
version 12.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname RouterR3
!
!
ip subnet-zero
!
ip multicast-routing

!--- Enables IP Multicasting on the network.

!
!
!
interface Ethernet0
  ip address 172.16.1.1 255.255.0.0
  ip pim dense-mode

!--- Enables PIM-Dense Mode Multicast Protocol on the interface.

ip cgmp

```

```

!--- Enables Cisco Group Management Protocol (CGMP) on the interface
!--- connected to the Layer 2 switch.

!
interface Serial0
  description Connected to RouterR2
  ip address 10.2.2.1 255.255.255.0
  ip pim dense-mode

!--- Enables PIM-Dense Mode Multicast Protocol on the interface.

!
interface Serial1
  description Connected to RouterR1
  ip address 10.2.4.2 255.255.255.0
  ip pim dense-mode

!--- Enables PIM-Dense Mode Multicast Protocol on the interface.

!
router ospf 1

!--- Configures OSPF as the unicast routing protocol.

  log-adjacency-changes
  network 172.16.0.0 0.0.255.255 area 0
  network 10.0.0.0 0.255.255.255 area 0
!
ip classless
ip http server
!
!
!
!
line con 0
line aux 0
line vty 0 4
!
end

```

For Layer 2 switches, no configuration is required for multicasting. All IOS-based Layer 2 switches have CGMP enabled by default. Therefore, the switches automatically process the CGMP messages from routers.

## Verify and Troubleshoot

Use this section to confirm that your configuration works properly.

The Output Interpreter Tool (registered customers only) (OIT) supports certain **show** commands. Use the OIT to view an analysis of **show** command output.

In order to verify the configuration, you need to send multicast traffic from the source W1 and check if multicast traffic flows through the wired network and reaches the wired and wireless group members, W2, C1 and C2.

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

If all the multicast-capable routers are members of a multicast group, pinging that group causes all routers to respond, which can be a useful administrative and debugging tool.

Another reason to have a router join a multicast group is when other hosts on the network have an Interior Gateway Routing Protocol (IGRP) configuration that prevents them from correctly answering IGMP queries. When you have the router join the multicast group, this causes upstream routers to maintain multicast routing table information for that group and keep the paths for that group active. In order to configure a router to be part of the multicast group, issue this command from the interface configuration mode:

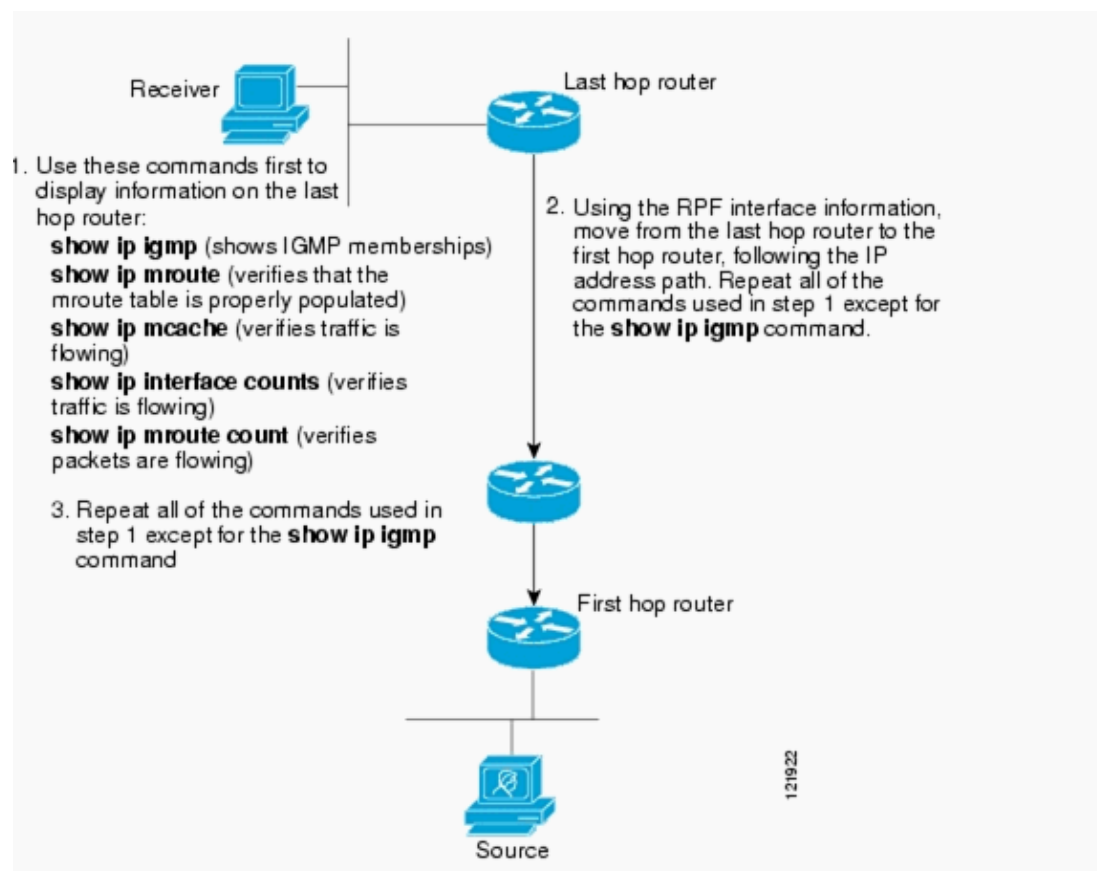
```
ip igmp join-group <group-address>  
Example: Router(config-if)#ip igmp join-group 239.255.1.60
```

Here is the output of the ping from Router R3:

```
RouterR3#ping 239.255.1.60  
  
Type escape sequence to abort.  
Sending 1, 100-byte ICMP Echos to 239.255.1.60, timeout is 2 seconds:  
  
Reply to request 0 from 10.2.2.2, 40 ms  
Reply to request 0 from 10.2.3.1, 84 ms  
Reply to request 0 from 10.2.4.1, 44 ms
```

## Locating a Faulty Hop

Perform this task in order to monitor and diagnose a basic IP multicast configuration. You can use this procedure when a receiver and a source do not operate as expected.



Here are the outputs of the **show ip igmp membership** and **show ip mroute count** commands for the example configuration. These outputs were taken from Router R3.

```
RouterR3#sh 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
Channel/Group-Flags:
/ - Filtering entry (Exclude mode (S,G), Include mode (*,G))
Reporter:
<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
*,224.0.1.40          10.2.2.1         1d21h     stop  2LA    Se0
*,239.255.1.60        172.16.1.1       1d06h     02:17 1LA    Et0

```

```
RouterR3#sh ip mroute count
```

```
IP Multicast Statistics
```

```
5 routes using 3094 bytes of memory
```

```
2 groups, 1.50 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: 239.255.1.60, Source count: 3, Packets forwarded: 6860,
```

```
Packets received: 7087
```

```
Source: 172.16.1.30/32, Forwarding: 304/1/147/0, Other: 304/0/0
```

```
Source: 172.16.1.75/32, Forwarding: 6329/8/57/3, Other: 6329/0/0
```

```
Source: 192.168.0.20/32, Forwarding: 227/1/69/0, Other: 454/227/0
```

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

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

---

## Related Information

- [Enterprise Mobility](#)
  - [VLANs on Wireless LAN Controllers Configuration Example](#)
  - [Wireless LAN Controller and Lightweight Access Point Basic Configuration Example](#)
  - [IP Multicast: White Papers](#)
  - [Wireless Support Page](#)
  - [Technical Support & Documentation – Cisco Systems](#)
- 

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2009 – 2010 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

---

Updated: Feb 04, 2009

Document ID: 81671

---