Multicast in a Cisco CAPWAP Deployment

Understanding multicast within a CAPWAP deployment is necessary to deploy the Vocera "Broadcast to" command, Push to Talk session (PTT) and "Panic" functions. With Vocera broadcast function, a badge can inform the Vocera server that the badge needs to communicate to several devices. This communication to several badges will occur through the use of a multicast address. The Vocera server forwards the request to the target badges, requesting them to join the intended multicast address. The Vocera server does not play any further role in the communication. The source badge sends traffic to the intended multicast address. As the target recipients subscribed to the multicast flow, they receive the multicast traffic and the messages it contains. In this topology, the multicast packet is first receive by a controller (coming from the sending badge), and must be relayed to the wireless cells where the target recipients reside. This document later covers the essential steps to enable multicast within the controller-based solution. There are currently two delivery methods that the CAPWAP controller uses to deliver multicast to the clients:

- Unicast-Multicast Delivery Method
- Multicast-Multicast Delivery Method

This chapter includes the following topics:

- Unicast-Multicast Delivery Method, page 1
- Multicast-Multicast Delivery Method, page 2
- Router and Switch Multicast Configuration, page 3
- Enable IP Multicast Routing, page 3
- Enable PIM on an Interface, page 3
- Switch VLAN IGMP Snooping, page 4

Unicast-Multicast Delivery Method

The unicast-multicast delivery is a legacy method, where the Wireless LAN Controller creates a copy of every multicast packet and forwards it to every access point. When a client sends a multicast join to the wireless LAN, the access point forwards this join through the CAPWAP tunnel to the controller. The controller bridges this multicast join onto its directly connected local area network connection that is the default VLAN for the associated WLAN of the client. When an IP multicast packet arrives from the network to the controller, the controller replicates this packet with a CAPWAP header for each access point. When the source of the multicast
is also a receiver within the wireless domain, this packet is also duplicated and forwarded back to the same client who sent this packet. This is not the preferred method of multicast delivery within the Cisco Wireless solution. The unicast delivery method works with small deployments. However, due to the considerable overhead on the Wireless LAN Controller (WLC), this is never the recommended multicast delivery method.

**Figure 1: CAPWAP Multicast-Unicast**

If AP Group VLANs are configured, and an IGMP join is sent from a client through the controller, it is placed on the default VLAN of the WLAN that the client is on. Therefore, the client might not receive this multicast traffic unless the client is a member of this default broadcast domain.

---

**Note**

If AP Group VLANs are configured, and an IGMP join is sent from a client through the controller, it is placed on the default VLAN of the WLAN that the client is on. Therefore, the client might not receive this multicast traffic unless the client is a member of this default broadcast domain.

---

**Multicast-Multicast Delivery Method**

The multicast-multicast delivery method does not require the controller to replicate each multicast packet received. The controller is configured for an un-used multicast group address that each access point becomes a member of. With Figure 3, the multicast group defined from the WLC to the access point is 239.0.0.65. When a client sends a multicast join to the WLAN, the access point forwards this join through the CAPWAP tunnel to the controller. The controller can forward this link-layer protocol onto its directly connected local area network connection that is the VLAN for the associated WLAN of the client. The controller can transparently relay multicast client packets to the wired infrastructure (in which case the infrastructure sees the wireless client as the multicast client), or act as a proxy (in which case the infrastructure sees the controller as the multicast client). In both cases, the router that is local to the controller then adds this multicast group address to that interface for forwarding ((*,G)) entry. With Figure 3, the example multicast join was sent to the multicast group 230.230.x.y, which is the default multicast address used by Vocera badges. When the network forwards multicast traffic, the multicast address of 230.230.x.y is forwarded to the controller. The controller then encapsulates the multicast packet into a CAPWAP multicast packet addressed to the multicast group address (example here is 239.0.0.65) that is configured on the controller and forwards to the network. Each access point on the controller receives this packet as a member of the controller's multicast group. The access point then forwards the client's/server's multicast packet (example here is 230.230.x.y) to the...
WLAN/SSID identified within the CAPWAP multicast packet, on each radio having a client for this multicast traffic. The access points that do not have clients for this multicast flow drop the multicast frame.

**Figure 2: CAPWAP Multicast-Multicast**

![CAPWAP Multicast-Multicast Diagram]

**Router and Switch Multicast Configuration**

This document is not a network multicast configuration guide. Refer to Configuring IP Multicast Routing for a complete implementation story. This document covers the basics to enable multicast within your network environment.

**Enable IP Multicast Routing**

IP multicast routing allows the Cisco IOS® software to forward multicast packets. The `ip multicast-routing` global configuration command is required to allow multicast to function in any multicast enabled network. The `ip multicast-routing` command should be enabled on all routers within your network between the WLC(s) and their respective access points.

```bash
Router(config)#ip multicast-routing
```

**Enable PIM on an Interface**

This enables the routing interface for Internet Group Management Protocol (IGMP) operation. The Protocol Independent Multicast (PIM) mode determines how the router populates its multicast routing table. The example provided here does not require the rendezvous point (RP) to be known for the multicast group and therefore sparse-dense-mode is the most desirable given the unknown nature of your multicast environment. This is not a multicast recommendation to be configured to work although the Layer 3 interface directly connected to your controller should be PIM enabled for multicast to function. All interfaces between your WLC(s) and their respective access points should be enabled.

```bash
Router(config-if)#ip pim sparse-dense-mode
```
Switch VLAN IGMP Snooping

Roaming and multicast are not defined with a set of requirements to verify that multicast traffic can follow a subscribed user. Although the client badge is aware that it has roamed, it does not forward another IGMP join to make sure that the network infrastructure continues to deliver the multicast (Vocera broadcast) traffic to the badge. However, the controller is aware of the roaming event, and immediately sends a general IGMP query to any client that just roamed and requires multicast forwarding. The client then responds with the IGMP group that they are a member of and this is bridged to the wired network as described earlier in this document. When a client roams to a controller that does not have Layer 2 connectivity, or a Layer 3 roam, synchronous routing is added for multicast source packets. When a client, who has completed a Layer 3 roam sources a multicast packet from the wireless network, the foreign controller encapsulates this packet in the Ethernet over IP (EoIP) in IP tunnel to the anchor controller. The anchor controller then forwards that to the wireless clients locally associated as well as bridges this back to the wired network where it is routed using normal multicast routing methods.

IGMP snooping allows a switched network with multicast enabled to limit traffic to those switchports that have users who want multicast to be seen while pruning the multicast packets from switchports that do not wish to see the multicast stream. In a Vocera deployment, because the controller takes care of forwarding to the wired infrastructure all IGMP messages for all wireless clients needing multicast traffic, you can enable CGMP or IGMP snooping on the upstream switchport to the controller. This prevents multicast messages from flooding to the controller port when they are not needed. Vocera badges use IGMPv2 by default.

Refer to Configuring IGMP Snooping for more information.

```
Router(config)#interface vlan 150
Router(config-if)#ip igmp snooping
```