Configuring Wireless Multicast

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for Configuring Wireless Multicast

- The IP multicast routing must be enabled and the PIM version and PIM mode must be configured. The default routes should be available in the device. After performing these tasks, the device can then forward multicast packets and can populate its multicast routing table.
- To participate in IP multicasting, the multicast hosts, routers, and multilayer switches must have IGMP operating.
- When enabling multicast mode on the switch, a CAPWAP multicast group address should also be configured. Access points listen to the CAPWAP multicast group using IGMP.

Restrictions for Configuring Wireless Multicast

The following are the restrictions for configuring IP multicast routing:

- Access points in monitor mode, sniffer mode, or rogue detector mode do not join the CAPWAP multicast group address.
- The CAPWAP multicast group configured on the switch should be different for different switches.
- Multicast routing should not be enabled for the management interface.

Information About Wireless Multicast

If the network supports packet multicasting, the multicast method that the switch uses can be configured. The switch performs multicasting in two modes:

- Unicast mode—The switch unicasts every multicast packet to every access point associated to the switch. This mode is inefficient but might be required on networks that do not support multicasting.
- Multicast mode—The switch sends multicast packets to a CAPWAP multicast group. This method reduces overhead on the switch processor and shifts the work of packet replication to the network, which is much more efficient than the unicast method.

When the multicast mode is enabled and the switch receives a multicast packet from the wired LAN, the switch encapsulates the packet using CAPWAP and forwards the packet to the CAPWAP multicast group address. The switch always uses the management VLAN for sending multicast packets. Access points in the multicast group receive the packet and forward it to all the BSSIDs mapped to the VLAN on which clients receive multicast traffic.

The switch supports all the capabilities of v1 including Multicast Listener Discovery (MLD) v1 snooping but the v2 and v3 capabilities are limited. This feature keeps track of and delivers IPv6 multicast flows to the clients that request them. To support IPv6 multicast, global multicast mode should be enabled.

Internet Group Management Protocol (IGMP) snooping is introduced to better direct multicast packets. When this feature is enabled, the switch snooping gathers IGMP reports from the clients, processes them, creates unique multicast group IDs (MGIDs) based on the Layer 3 multicast address and the VLAN number, and sends the IGMP reports to the IGMP querier. The switch then updates the access point MGID table on the access point with the client MAC address. When the switch receives multicast traffic for a particular multicast group, it forwards it to all the access points, but only those access points 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 VLAN.

MGID is a 14-bit value filled in the 16-bit reserved field of wireless information in CAPWAP header. The remaining 2 bits should be set to zero.

Related Topics

Configuring Wireless Multicast-MCMC Mode (CLI), on page 3
Configuring Wireless Multicast-MCUC Mode (CLI), on page 4

Information About Multicast Optimization

Multicast used to be based on the group of the multicast addresses and the VLAN as one entity, MGID. With the VLAN group, duplicate packets might increase. Using the VLAN group feature, every client listens to the multicast stream on a different VLAN. As a result, the switch creates different MGIDs for each multicast address and VLAN. Therefore, in a worst case situation, the upstream router sends one copy for each VLAN, which results in as many copies as the number of VLANs in the group. Because the WLAN remains the same for all clients, multiple copies of the multicast packet are sent over the wireless network. To suppress the duplication of a multicast stream on the wireless medium between the switch and the access points, the multicast optimization feature can be used.

Multicast optimization enables you to create a multicast VLAN that can be used for multicast traffic. One of the VLANs in the switch can be configured as a multicast VLAN where multicast groups are registered. The clients are allowed to listen to a multicast stream on the multicast VLAN. The MGID is generated using the mulicast VLAN and multicast IP addresses. If multiple clients on different VLANs of the same WLAN are listening to a single multicast IP address, a single MGID is generated. The switch makes sure that all multicast streams from the clients on this VLAN group always go out on the multicast VLAN to ensure that the upstream router has one entry for all the VLANs of the VLAN group. Only one multicast stream hits the VLAN group even if the clients are on different VLANs. Therefore, the multicast packets that are sent out over the network is just one stream.

Related Topics

Configuring IP Multicast VLAN for WLAN (CLI), on page 11

How to Configure Wireless Multicast

Configuring Wireless Multicast-MCMC Mode (CLI)

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **wireless multicast**
4. **ap capwap multicast ipaddr**
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Switch# configure terminal`	Enters global command mode.

Step 3	**wireless multicast**
	
	Example:
	`Switch(config)# wireless multicast`
	
	`Switch(config)# no wireless multicast`
		Enables the multicast traffic for wireless clients. The default value is disable. Add **no** in the command to disable the multicast traffic for wireless clients.

Step 4	**ap capwap multicast ipaddr**
	
	Example:
	`Switch(config)# ap capwap multicast 231.1.1.1`
	
	`Switch(config)# no ap capwap multicast 231.1.1.1`
		Enables the forwarding mode in multicast. Add **no** in the command to disable the multicast mode.

Step 5	**end** **Example:** `Switch(config)# end`	Exits the configuration mode. Alternatively, press **Ctrl-Z** to exit the configuration mode.

Related Topics

Information About Wireless Multicast, on page 2

Configuring Wireless Multicast-MCUC Mode (CLI)

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **wireless multicast**
4. **no ap capwap multicast** *ipaddr*
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable**	Enables privileged EXEC mode.

	Command or Action	Purpose
	Example: `Switch> enable`	• Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Switch# configure terminal`	Enters global command mode.
Step 3	**wireless multicast** **Example:** `Switch(config)# wireless multicast`	Enables the multicast traffic for wireless clients and enables mDNS bridging. The default value is disable. Add **no** in the command to disable the multicast traffic for wireless clients and disable mDNS bridging.
Step 4	**no ap capwap multicast** *ipaddr* **Example:** `Switch(config)# no ap capwap multicast 231.1.1.1`	Enables forwarding mode in multicast. Add **no** in the command to disable the multicast mode.
Step 5	**end** **Example:** `Switch(config)# end`	Exits the configuration mode. Alternatively, press **Ctrl-Z** to exit the configuration mode.

Related Topics

Information About Wireless Multicast, on page 2

Configuring IPv6 Snooping (CLI)

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ipv6 mld snooping**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable**	Enables privileged EXEC mode.

	Command or Action	Purpose
	Example: `Switch> enable`	• Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Switch# configure terminal`	Enters global command mode.
Step 3	**ipv6 mld snooping** **Example:** `Switch(config)# ipv6 mld snooping`	Enables MLD snooping.

Configuring IPv6 Snooping Policy (CLI)

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ipv6 snooping policy** *policy-name*
4. **security-level guard**
5. **device-role node**
6. **protocol** {**dhcp** | **ndp**}

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Switch# configure terminal`	Enters global command mode.

	Command or Action	Purpose
Step 3	**ipv6 snooping policy** *policy-name* **Example:** `Switch(config)# ipv6 snooping policy mypolicy`	Configures an IPv6 snooping policy with a name.
Step 4	**security-level guard** **Example:** `Switch(config-ipv6-snooping)# security-level guard`	Configures security level to inspect and drop any unauthorized messages.
Step 5	**device-role node** **Example:** `Switch(config-ipv6-snooping)# device-role node`	Configures the role of the device, which is a node, to the attached port.
Step 6	**protocol** {**dhcp** | **ndp**} **Example:** `Switch(config-ipv6-snooping)# protocol ndp`	Sets the protocol to glean addresses in DHCP or NDP packets.

Configuring Layer 2 Port as Multicast Router Port (CLI)

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ipv6 mld snooping vlan** *vlan-id* **mrouter interface Port-channel** *port-channel-interface-number*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Switch# configure terminal`	Enters global command mode.

	Command or Action	Purpose
Step 3	**ipv6 mld snooping vlan** *vlan-id* **mrouter interface Port-channel** *port-channel-interface-number* **Example:** `Switch(config)# ipv6 mld snooping vlan 2 mrouter interface Port-channel 22`	Configures a Layer 2 port as a Multicast router port. The VLAN is the client VLAN.

Configuring RA Guard (CLI)

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ipv6 nd raguard policy** *policy-name*
4. **trusted-port**
5. **device-role** {**host** | **monitor** | **router** | **switch**}

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Switch# configure terminal`	Enters global command mode.
Step 3	**ipv6 nd raguard policy** *policy-name* **Example:** `Switch(config)# ipv6 nd raguard policy myraguardpolicy`	Configures a policy for RA Guard.
Step 4	**trusted-port** **Example:** `Switch(config-nd-raguard)# trusted-port`	Sets up a trusted port.

	Command or Action	Purpose
Step 5	**device-role** {**host** | **monitor** | **router** | **switch**} **Example:** `Switch(config-nd-raguard)# device-role router`	Sets the role of the device attached to the port.

Configuring Non-IP Wireless Multicast (CLI)

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **wireless multicast non-ip**
4. **wireless multicast non-ip** *vlanid*
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Switch# configure terminal`	Enters global command mode.

Step 3	**wireless multicast non-ip**
	
	Example:
	`Switch(config)# wireless multicast non-ip`
	
	`Switch(config)# no wireless multicast non-ip`
		Enables non-IP multicast in all VLANs. Default value is **enable**. Wireless multicast must be enabled for the traffic to pass. Add **no** in the command to disable the non-IP multicast in all VLANs.

Step 4	**wireless multicast non-ip** *vlanid*
	
	Example:
	`Switch(config)# wireless multicast non-ip 5`
	
	`Switch(config)# no wireless multicast non-ip 5`
		Enables non-IP multicast per VLAN. Default value is **enable**. Both wireless multicast and wireless multicast non-IP must be enabled for traffic to pass. Add **no** in the command to disable the non-IP multicast per VLAN.

	Command or Action	Purpose
Step 5	**end** **Example:** `Switch(config)# end`	Exits the configuration mode. Alternatively, press **Ctrl-Z** to exit the configuration mode.

Configuring Wireless Broadcast (CLI)

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **wireless broadcast**
4. **wireless broadcast vlan** *vlanid*
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Switch# configure terminal`	Enters global command mode.

Step 3	**wireless broadcast**
	
	Example:
	`Switch(config)# wireless broadcast`
	
	`Switch(config)# no wireless broadcast`
		Enables broadcast packets for wireless clients. Default value is disable. Enabling **wireless broadcast** enables broadcast traffic for each VLAN. Add **no** in the command to disable broadcasting packets.

Step 4	**wireless broadcast vlan** *vlanid*
	
	Example:
	`Switch(config)# wireless broadcast vlan 3`
	
	`Switch(config)# no wireless broadcast vlan 3`
		Enables broadcast packets for single VLAN. Default value is **enable**. Wireless broadcast must be enabled for broadcasting. Add **no** in the command to disable the broadcast traffic for each VLAN.

	Command or Action	Purpose
Step 5	**end** **Example:** `Switch(config)# end`	Exits the configuration mode. Alternatively, press **Ctrl-Z** to exit the configuration mode.

Configuring IP Multicast VLAN for WLAN (CLI)

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **wlan** *wlan_name*
4. **shutdown**
5. **ip multicast vlan** {*vlan_name vlan_id*}
6. **no shutdown**
7. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Switch# configure terminal`	Enters global command mode.
Step 3	**wlan** *wlan_name* **Example:** `Switch(config)# wlan test 1`	Enters the configuration mode to configure various parameters in the WLAN.
Step 4	**shutdown** **Example:** `Switch(config-wlan)# shutdown`	Disables WLAN.

	Command or Action	Purpose

Step 5	**ip multicast vlan** {*vlan_name vlan_id*}
	
	Example:
	`Switch(config-wlan)# ip multicast vlan 5`
	
	`Switch(config-wlan)# no ip multicast vlan 5`
		Configures multicast VLAN for WLAN. Add **no** in the command to disable the multicast VLAN for WLAN.

Step 6	**no shutdown** **Example:** `Switch(config-wlan)# no shutdown`	Enables the disabled WLAN.
Step 7	**end** **Example:** `Switch(config)# end`	Exits the configuration mode. Alternatively, press **Ctrl-Z** to exit the configuration mode.

Related Topics

Information About Multicast Optimization, on page 3

Monitoring Wireless Multicast

Table 1: Commands for Monitoring Wireless Multicast

Commands	Description
show wireless multicast	Displays the multicast status and IP multicast mode, each VLAN's broadcast and non-IP multicast status. Also displays the mDNS bridging state.
show wireless multicast group summary	Displays all (Source, Group and VLAN) lists and the corresponding MGID value.
show wireless multicast [**source** *source*] **group** *group* **vlan** *vlanid*	Displays details of the given (S,G,V) and shows all of the clients associated with it and their MC2UC status .
show ip igmp snooping wireless mcast-spi-count	Displays statistics of the number of multicast SPIs per MGID sent between IOS and the Wireless Controller Module.
show ip igmp snooping wireless mgid	Displays the MGID mappings.

Commands	Description
show ip igmp snooping igmpv2-tracking	Displays the client-to-SGV mappings and SGV-to-client mappings.
show ip igmp snooping querier vlan *vlanid*	Displays IGMP querier information for the specified VLAN.
show ip igmp snooping querier detail	Displays detailed IGMP querier information of all the VLANs.
show ipv6 mld snooping querier vlan *vlanid*	Displays MLD querier information for the specified VLAN.
show ipv6 mld snooping wireless mgid	Displays MGIDs for IPv6 multicast group.

Where to Go Next for Wireless Multicast

You can configure the following:

- IGMP
- PIM
- SSM
- IP Multicast Routing
- Service Discovery Gateway

Additional References

Related Documents

Related Topic	Document Title
For complete syntax and usage information for the commands used in this chapter.	*IP Multicast Routing Command Reference (Catalyst 3650 Switches)*
Platform-independent configuration information	• *IP Multicast: PIM Configuration Guide, Cisco IOS XE Release 3SE (Catalyst 3650 Switches)* • *IP Multicast: IGMP Configuration Guide, Cisco IOS XE Release 3SE (Catalyst 3650 Switches)* • *IP Multicast: Multicast Optimization Configuration Guide, Cisco IOS XE Release 3SE (Catalyst 3650 Switches)*

Error Message Decoder

Description	Link
To help you research and resolve system error messages in this release, use the Error Message Decoder tool.	https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi

Standards and RFCs

Standard/RFC	Title
—	

MIBs

MIB	MIBs Link
All supported MIBs for this release.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/support