Configuring Wireless Multicast

- Prerequisites for Configuring Wireless Multicast, on page 1
- Restrictions on Configuring Wireless Multicast, on page 1
- Information About Wireless Multicast, on page 2
- How to Configure Wireless Multicast, on page 6
- Verifying Wireless Multicast, on page 13
- Where to Go Next for Wireless Multicast, on page 13

Prerequisites for Configuring Wireless Multicast

- 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 forward multicast packets and 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 device, a CAPWAP multicast group address should also be configured. Access points listen to the CAPWAP multicast group using IGMP.

Restrictions on 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 should be different for different devices.
- Multicast routing should not be enabled for the management interface.

Restrictions for IPv6 Snooping

The IPv6 snooping feature is not supported on Etherchannel ports.

Restrictions for IPv6 RA Guard

- The IPv6 RA Guard feature does not offer protection in environments where IPv6 traffic is tunneled.
- This feature is supported only in hardware when the ternary content addressable memory (TCAM) is programmed.
- This feature can be configured on a switch port interface in the ingress direction.
- This feature supports host mode and router mode.
- This feature is supported only in the ingress direction; it is not supported in the egress direction.
- This feature is not supported on EtherChannel and EtherChannel port members.
- This feature is not supported on trunk ports with merge mode.
- This feature is supported on auxiliary VLANs and private VLANs (PVLANs). In the case of PVLANs, primary VLAN features are inherited and merged with port features.
- Packets dropped by the IPv6 RA Guard feature can be spanned.
- If the **platform ipv6 acl icmp optimize neighbor-discovery command** is configured, the IPv6 RA Guard feature cannot be configured and an error message will be displayed. This command adds default global Internet Control Message Protocol (ICMP) entries that will override the RA guard ICMP entries.

Information About Wireless Multicast

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

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

The flexconnect mode has two submodes: local switching and central switching. In local switching mode, the data traffic is switched at the AP level and the controller does not see any multicast traffic. In central switching mode, the multicast traffic reaches the controller. However, IGMP snooping takes place at the AP.

When the multicast mode is enabled and the device receives a multicast packet from the wired LAN, the device encapsulates the packet using CAPWAP and forwards the packet to the CAPWAP multicast group address. The device 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 device supports all the capabilities of IGMP v1, including Multicast Listener Discovery (MLD) v1 snooping, but the IGMP v2 and IGMP 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 device 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 device then updates the access-point MGID table on the corresponding access point with the client MAC address. When the device 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 the CAPWAP header. The remaining two bits should be set to zero.

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 device creates different MGIDs for each multicast address and the VLAN. Therefore, the upstream router sends a 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 the 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 device 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 device 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 device makes sure that all the 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.

IPv6 Global Policies

IPv6 global policies provide storage and access policy database services. IPv6 ND inspection and IPv6 RA guard are IPv6 global policies features. Every time an ND inspection or RA guard is configured globally, the policy attributes are stored in the software policy database. The policy is then applied to an interface, and the software policy database entry is updated to include this interface to which the policy is applied.

IPv6 RA Guard

The IPv6 RA Guard feature provides support for allowing the network administrator to block or reject unwanted or rogue RA guard messages that arrive at the network device platform. RAs are used by devices to announce themselves on the link. The IPv6 RA Guard feature analyzes these RAs and filters out RAs that are sent by unauthorized devices. In host mode, all RA and router redirect messages are disallowed on the port. The RA guard feature compares configuration information on the Layer 2 (L2) device with the information found in the received RA frame. Once the L2 device has validated the content of the RA frame and router redirect frame against the configuration, it forwards the RA to its unicast or multicast destination. If the RA frame content is not validated, the RA is dropped.

In the wireless deployment RAs coming on wireless ports are dropped as routers cannot reside on these interfaces.

Information About IPv6 Snooping

IPv6 Neighbor Discovery Inspection

The IPv6 Neighbor Discovery Inspection, or IPv6 "snooping," feature bundles several Layer 2 IPv6 first-hop security features, including IPv6 Address Glean and IPv6 Device Tracking. IPv6 neighbor discovery (ND) inspection operates at Layer 2, or between Layer 2 and Layer 3, and provides IPv6 features with security and scalability. This feature mitigates some of the inherent vulnerabilities for the neighbor discovery mechanism, such as attacks on duplicate address detection (DAD), address resolution, device discovery, and the neighbor cache.

IPv6 ND inspection learns and secures bindings for stateless autoconfiguration addresses in Layer 2 neighbor tables and analyzes ND messages in order to build a trusted binding table. IPv6 ND messages that do not have valid bindings are dropped. An ND message is considered trustworthy if its IPv6-to-MAC mapping is verifiable. This feature mitigates some of the inherent vulnerabilities for the neighbor discovery mechanism, such as attacks on duplicate address detection (DAD), address resolution, device discovery, and the neighbor cache.

When IPv6 ND inspection is configured on a target (which varies depending on platform target support and may include device ports, switch ports, Layer 2 interfaces, Layer 3 interfaces, and VLANs), capture instructions are downloaded to the hardware to redirect the ND protocol and Dynamic Host Configuration Protocol (DHCP) for IPv6 traffic up to the switch integrated security features (SISF) infrastructure in the routing device. For ND traffic, messages such as NS, NA, RS, RA, and REDIRECT are directed to SISF. For DHCP, UDP messages sourced from port 546 or 547 are redirected.

IPv6 ND inspection registers its "capture rules" to the classifier, which aggregates all rules from all features on a given target and installs the corresponding ACL down into the platform-dependent modules. Upon receiving redirected traffic, the classifier calls all entry points from any registered feature (for the target on which the traffic is being received), including the IPv6 ND inspection entry point. This entry point is the last to be called, so any decision (such as drop) made by another feature supersedes the IPv6 ND inspection decision.

IPv6 ND Inspection

IPv6 ND inspection learns and secures bindings for stateless autoconfiguration addresses in Layer 2 neighbor tables. IPv6 ND inspection analyzes neighbor discovery messages in order to build a trusted binding table database, and IPv6 neighbor discovery messages that do not have valid bindings are dropped. A neighbor discovery message is considered trustworthy if its IPv6-to-MAC mapping is verifiable.

This feature mitigates some of the inherent vulnerabilities for the neighbor discovery mechanism, such as attacks on duplicate address detection (DAD), address resolution, device discovery, and the neighbor cache.

IPv6 Device Tracking

IPv6 device tracking provides IPv6 host liveness tracking so that a neighbor table can be immediately updated when an IPv6 host disappears.

IPv6 First-Hop Security Binding Table

The IPv6 First-Hop Security Binding Table recovery mechanism feature enables the binding table to recover in the event of a device reboot. A database table of IPv6 neighbors connected to the device is created from information sources such as ND snooping. This database, or binding, table is used by various IPv6 guard

features to validate the link-layer address (LLA), the IPv4 or IPv6 address, and prefix binding of the neighbors to prevent spoofing and redirect attacks.

This mechanism enables the binding table to recover in the event of a device reboot. The recovery mechanism will block any data traffic sourced from an unknown source; that is, a source not already specified in the binding table and previously learned through ND or DHCP gleaning. This feature recovers the missing binding table entries when the resolution for a destination address fails in the destination guard. When a failure occurs, a binding table entry is recovered by querying the DHCP server or the destination host, depending on the configuration.

Recovery Protocols and Prefix Lists

The IPv6 First-Hop Security Binding Table Recovery Mechanism feature introduces the capability to provide a prefix list that is matched before the recovery is attempted for both DHCP and NDP.

If an address does not match the prefix list associated with the protocol, then the recovery of the binding table entry will not be attempted with that protocol. The prefix list should correspond to the prefixes that are valid for address assignment in the Layer 2 domain using the protocol. The default is that there is no prefix list, in which case the recovery is attempted for all addresses. The command to associate a prefix list to a protocol is **protocol** {**dhcp** | **ndp**} [**prefix-list** *prefix-list-name*].

IPv6 Device Tracking

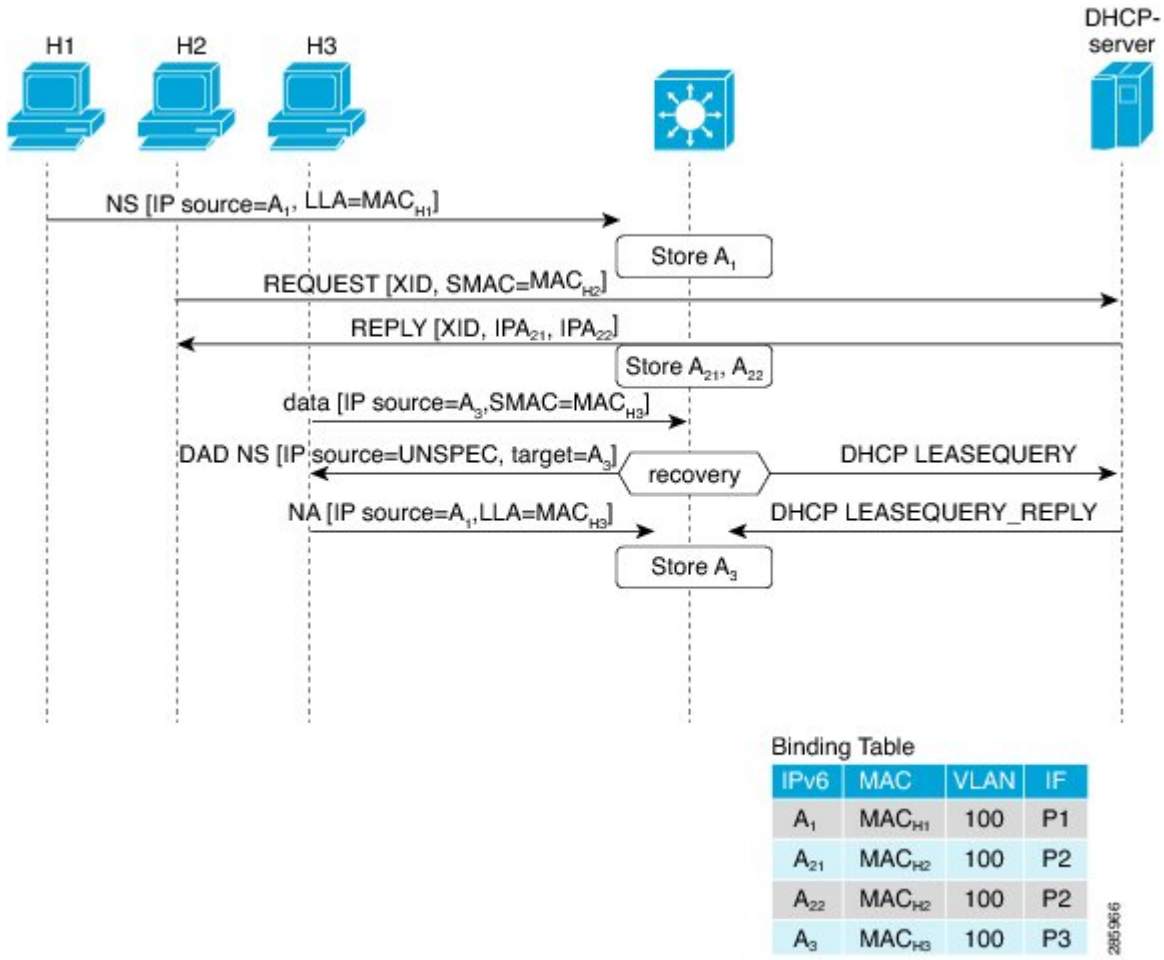
IPv6 device tracking provides IPv6 host liveness tracking so that a neighbor table can be immediately updated when an IPv6 host disappears.

IPv6 Address Glean

IPv6 address glean is the foundation for many other IPv6 features that depend on an accurate binding table. It inspects ND and DHCP messages on a link to glean addresses, and then populates the binding table with these addresses. This feature also enforces address ownership and limits the number of addresses any given node is allowed to claim.

The following figure shows how IPv6 address glean works.

Figure 1: IPv6 Address Glean



How to Configure Wireless Multicast

Configuring Wireless Multicast-MCMC Mode (CLI)

Procedure

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

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

Step 3	**wireless multicast**
	Example:
	`Device(config)# wireless multicast`
	`Device(config)# no wireless multicast`
		Enables multicast traffic for wireless clients. By default, multicast traffic is in disabled state. Use the **no** form of this command to disable the multicast traffic for wireless clients.

Step 4	**end** **Example:** `Device(config)# end`	Exits configuration mode. Alternatively, press **Ctrl-Z** to exit configuration mode.

Configuring Wireless Multicast-MCUC Mode (CLI)

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password, if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**wireless multicast** **Example:** `Device(config)# wireless multicast`	Enables the multicast traffic for wireless clients and enables mDNS bridging. By default, the feature is in disabled state. Use the **no** form of this command to disable the multicast traffic for wireless clients and disable mDNS bridging.
Step 4	**end** **Example:** `Device(config)# end`	Exits configuration mode. Alternatively, press **Ctrl-Z** to exit configuration mode.

Configuring IPv6 Snooping (CLI)

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password, if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**ipv6 mld snooping** **Example:** `Device(config)# ipv6 mld snooping`	Enables MLD snooping.

Configuring IPv6 Snooping Policy (CLI)

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password, if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**ipv6 snooping policy** *policy-name* **Example:** `Device(config)# ipv6 snooping policy mypolicy`	Configures an IPv6 snooping policy with a name.
Step 4	**security-level guard** **Example:** `Device(config-ipv6-snooping)# security-level guard`	Configures the security level to inspect and drop unauthorized messages, if any.

	Command or Action	Purpose
Step 5	**device-role node** **Example:** `Device(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:** `Device(config-ipv6-snooping)# protocol ndp`	Sets the protocol to glean addresses in either the DHCP or the NDP packets.

Configuring Layer 2 Port as Multicast Router Port (CLI)

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password, if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**ipv6 mld snooping vlan** *vlan-id* **mrouter interface Port-channel** *port-channel-interface-number* **Example:** `Device(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 IPv6 RA Guard (CLI)

Procedure

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

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**ipv6 nd raguard policy** *policy-name* **Example:** `Device(config)# ipv6 nd raguard policy myraguardpolicy`	Configures a policy for RA guard.
Step 4	**trusted-port** **Example:** `Device(config-nd-raguard)# trusted-port`	Sets up a trusted port.
Step 5	**device-role** {**host** | **monitor** | **router** | **switch**} **Example:** `Device(config-nd-raguard)# device-role router`	Sets the role of the device attached to the port.

Configuring Non-IP Wireless Multicast (CLI)

Procedure

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

Step 3	**wireless multicast non-ip**
	Example:
	`Device(config)# wireless multicast non-ip`
	`Device(config)# no wireless multicast non-ip`
		Enables non-IP multicast in all the VLANs. By default, the non-IP multicast in all the VLANs is in Disabled state. Wireless multicast must be enabled for the traffic to pass. Use the **no** form of this command to disable non-IP multicast in all the VLANs.

Step 4	**wireless multicast non-ip vlan** *vlanid* **Example:** `Device(config)# wireless multicast non-ip vlan 5`	Enables non-IP multicast per VLAN. By default, non-IP multicast per VLAN is in Disabled state. Both wireless multicast and wireless multicast non-IP must be enabled for

	Command or Action	Purpose
	`Device(config)# no wireless multicast non-ip vlan 5`	traffic to pass. Use the **no** form of this command to disable non-IP multicast per VLAN.
Step 5	**end** **Example:** `Device(config)# end`	Exits configuration mode. Alternatively, press **Ctrl-Z** to exit configuration mode.

Configuring Wireless Broadcast (CLI)

Procedure

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

Step 3	**wireless broadcast**
	Example:
	`Device(config)# wireless broadcast`
	`Device(config)# no wireless broadcast`
		Enables broadcast packets for wireless clients. By default, the broadcast packets for wireless clients is in Disabled state. Enabling **wireless broadcast** enables broadcast traffic for each VLAN. Use the **no** form of this command to disable broadcasting packets.

Step 4	**wireless broadcast vlan** *vlanid*
	Example:
	`Device(config)# wireless broadcast vlan 3`
	`Device(config)# no wireless broadcast vlan 3`
		Enables broadcast packets for single VLAN. By default, the Broadcast Packets for a Single VLAN feature is in Disabled state. Wireless broadcast must be enabled for broadcasting. Use the **no** form of this command to disable broadcast traffic for each VLAN.

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

Configuring IP Multicast VLAN for WLAN (CLI)

Procedure

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

Step 5	**ip multicast vlan** {*vlan_name vlan_id*}
	Example:
	`Device(config-wlan)# ip multicast vlan 5`
	`Device(config-wlan)# no ip multicast vlan 5`
		Configures multicast VLAN for WLAN. Use the **no** form of this command to disable the multicast VLAN for WLAN.

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

Verifying Wireless Multicast

Table 1: Commands for Verifying Wireless Multicast

Command	Description
show wireless multicast	Displays the multicast status and IP multicast mode, and each VLAN's broadcast and non-IP multicast status. Also displays the Multicast Domain Name System (mDNS) bridging state.
show wireless multicast group summary	Displays all (Group and VLAN) lists and the corresponding MGID values.
show wireless multicast [**source** *source*] **group** *group* **vlan** *vlanid*	Displays details of the specified (S,G,V) and shows all the clients associated with 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.
show ip igmp snooping igmpv2-tracking	Displays the client-to-SGV mappings and the SGV-to-client mappings.
show ip igmp snooping querier vlan *vlanid*	Displays the IGMP querier information for the specified VLAN.
show ip igmp snooping querier detail	Displays the detailed IGMP querier information of all the VLANs.
show ipv6 mld snooping querier vlan *vlanid*	Displays the MLD querier information for the specified VLAN.
show ipv6 mld snooping wireless mgid	Displays MGIDs for the IPv6 multicast group.

Where to Go Next for Wireless Multicast

You can configure the following:

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