6AOSCG0058-29B
December 2014

ADTRAN

Configuration Guide

Configuring IGMP Snooping

This configuration guide provides information and configuration support for Internet Group Management Protocol (IGMP) snooping. This guide provides an overview of IP multicast, IGMP, and IGMP snooping, as well as steps for configuring IGMP snooping using the ADTRAN Operating System (AOS) command line interface (CLI). Additionally, troubleshooting support for IGMP snooping is provided.

This guide consists of the following sections:

IGMP Snooping Overview

This section provides an overview of concepts and technology related to IGMP snooping. The following topics are covered:

IP Multicast

IP multicast has many applications, ranging from video and audio program delivery, music on hold for an IP private branch exchange (PBX), conferencing applications, and delivery of software updates, data, or other information to the multiple sites and devices. Unlike normal unicast traffic, which provides single, unit-to-unit communication, multicast provides single-to-many communication. In multicast communication, a single unit behaves as if it is communicating with a single endpoint, but that message is replicated to every member listening for that unit's stream. In a multicast-enabled network, the media server sends specific content in a single stream to a specific multicast IP address, much like a local broadcast TV station sends its content on a specific broadcast frequency. The network has multicast intelligence and is able to make copies of the stream as necessary to reach all active receivers. This provides two significant advantages:

1. There is never more than one instance of a particular content stream at any given point in the network.
2. The network will only copy and forward a stream to locations that have active receivers.

Figure 1 on page 3 depicts a multicast-enabled network in which **PC1**, **PC2**, **PC4**, **PC6,** and **PC7** have subscribed to the same broadcast. Using IGMP, the PCs have signaled to their local router that they wish to receive the broadcast stream by joining the multicast group. The satellite routers use a multicast routing protocol to signal other routers and the **Central Router** that they have subscribers for the multicast group. Each router in the network then understands if it is in the path toward the multicast group subscribers.

The **Media Server** is able to send a single copy of the stream to the multicast group's IP address. The **Central Router** receives the stream and sends a copy out all interfaces that have subscribers for that group. This process is repeated at each router until the stream arrives at each segment that has subscribers. Since there is never more than one copy of the stream on any given link, bandwidth is conserved. Notice that **PC1** and **PC2** are on the same broadcast domain. **Satellite Router 1** makes a single copy of the stream and transmits it into that broadcast domain, where it is received by both PCs.

The benefit of using a multicast address instead of a broadcast address is only devices running a process that uses a given multicast address need to listen for that address. Other devices are not interrupted when traffic is transmitted to a multicast address. With broadcast traffic, all attached devices are interrupted to listen to a broadcast packet.

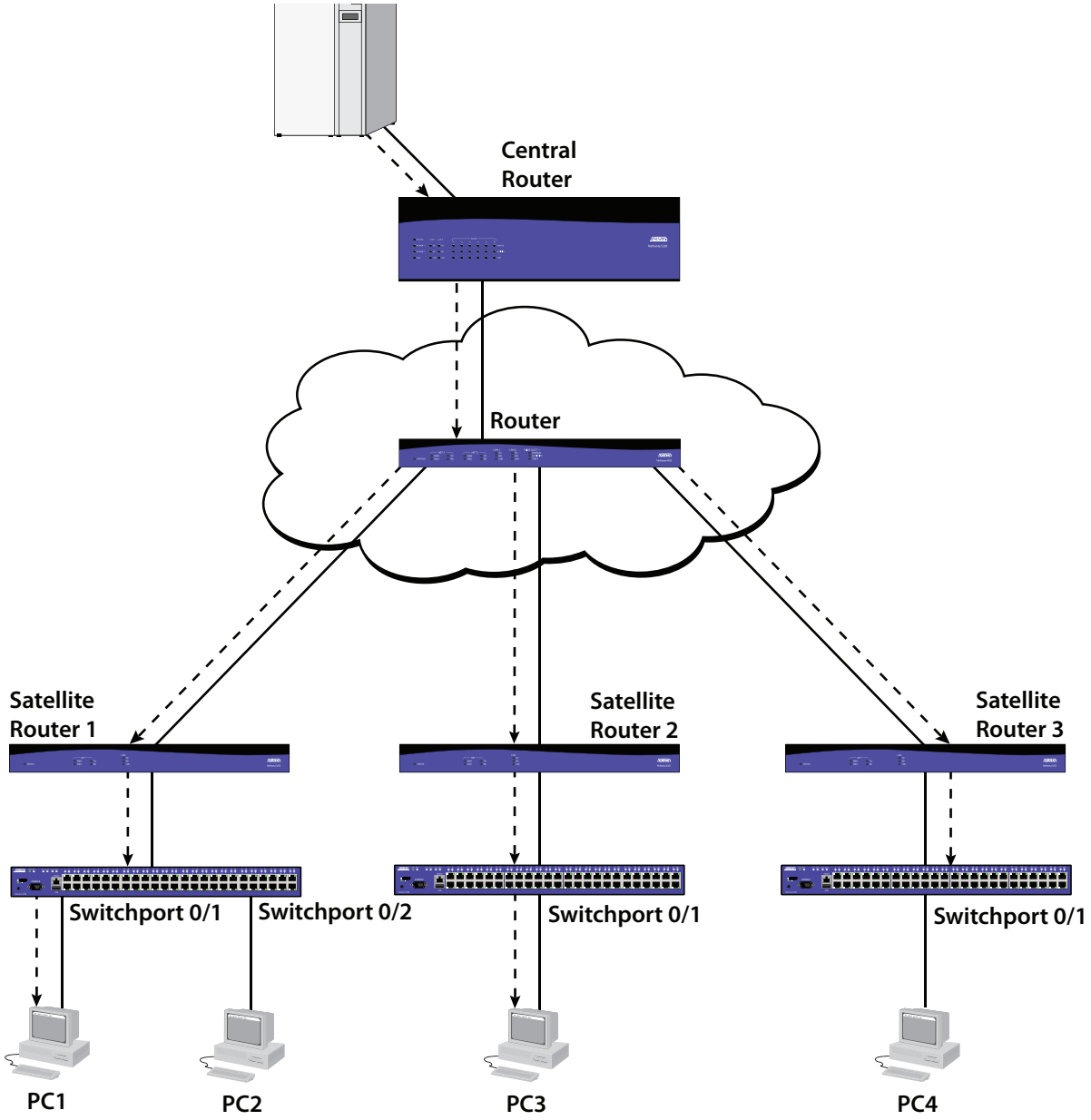

Figure 1. Multicast-Enabled Network

Internet Group Management Protocol

IGMP allows a device to notify a directly-connected multicast router that it wishes to join a specific multicast group and therefore receive packets sent to that multicast group address. It also allows a router to query attached segments (subnets) to determine whether any group members remain. If no remaining group members are detected, streams to that group are no longer forwarded to that segment. In IGMP version 1 (IGMPv1), when a device wishes to leave a group, it ceases to respond to the router's query. When no devices respond on a given segment, the router stops forwarding that group to that segment. This

causes some lag time between when the last device stops subscribing to a stream and when the router stops sending the stream. To reduce this lag time and make better use of network resources, IGMP version 2 (IGMPv2) introduced a group-specific leave message and process that expedites termination of a stream to an interface when the last member leaves.

IGMP Snooping

IGMP snooping takes advantage of IGMP packets flowing through a switch to reduce unnecessary flooding of multicast traffic. Since multicast traffic isn't automatically learned by switch hardware, the switch must flood the multicast traffic out all ports in the virtual local area network (VLAN) to ensure that a subscribed client receives the traffic. By using information learned by snooping IGMP packets, the device can build a multicast MAC address table and reduce the amount of flooding. This allows multicast traffic to be forwarded only to ports on which multicast subscribers or multicast routers have been learned.

Figure 2 depicts a multicast-enabled network consisting of a media server, a router, a switch, and hosts. **PC1** and **PC2** are located on **VLAN1**, and **PC3** and **PC4** are located on **VLAN2**. In the network, **PC1** and **PC4** have subscribed to the same multicast stream (as indicated by the dashed lines). The PCs have signaled to the **Router** using IGMP that they wish to receive the multicast stream by joining the multicast group. By snooping the IGMP packets sent from the PCs to the router, the **Switch** has learned which hosts want to receive the multicast stream, and is able to forward the stream to the appropriate hosts without flooding all hosts within the VLAN.

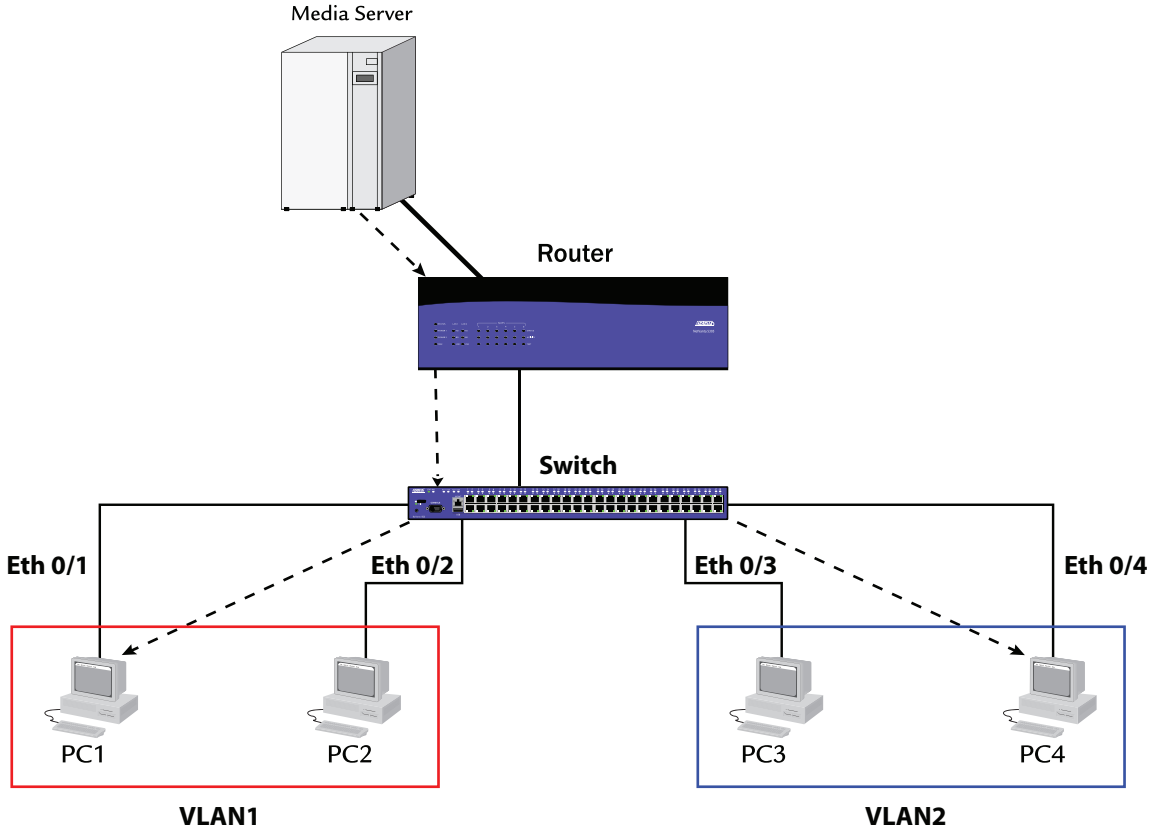

Figure 2. Multicast Network with IGMP Snooping

IGMP Querier

The function of an IGMP querier is to generate IGMP group membership queries to retrieve IGMP membership reports from active members and to allow updating of the group membership tables. Without an IGMP querier, the group membership tables used for IGMP snooping cannot be constructed and, consequently, snooping cannot operate.

Hardware and Software Requirements and Limitations

The IGMP snooping feature is available on AOS switches as outlined in the *Product Feature Matrix*, available online at https://supportforums.adtran.com.

The IGMP querier function is available on AOS switches as outlined in the *Product Feature Matrix*, available online at https://supportforums.adtran.com.

The IGMP querier function does not support the querier election protocol as described in Internet Engineering Task Force (IETF) RFC 2236. The querier ignores any other queriers on the LAN segment

Configuring IGMP Snooping

The following steps are required to configure IGMP snooping on an AOS device:

Step 1: Access the CLI

To access the CLI on your AOS unit, follow these steps:

1. Boot up the unit.
2. Telnet to the unit (**telnet** <*ip address*>), for example:

   telnet 10.10.10.1

> NOTE *If during the unit's setup process you have changed the default Internet Protocol (IP) address (**10.10.10.1**), use the configured IP address.*

3. Enter your user name and password at the prompt.

> NOTE *The AOS default user name is **admin** and the default password is **password**. If your product no longer has the default user name and password, contact your system administrator for the appropriate user name and password.*

4. Enter the Enable mode by entering **enable** at the prompt as follows:

   >enable

5. Enter your Enable mode password at the prompt.

> NOTE *The default Enable mode password is **password**. If your product no longer has the default Enable password, contact your system administrator for the appropriate password.*

6. Enter the unit's Global Configuration mode as follows:

   #configure terminal

   (config)#

Step 2: Enable IGMP Snooping

The commands required to enable IGMP snooping on a VLAN depend on the version of AOS running on your unit. Units running an AOS version earlier than R10.10.0, must first enable IGMP snooping globally before enabling IGMP snooping on a VLAN. Units running AOS R10.10.0 or later only have to enable IGMP snooping on the desired VLAN.

> NOTE *If a VLAN interface is configured for a VLAN receiving excessive multicast traffic, it is recommended that IGMP Snooping be enabled on that VLAN to reduce the processor load on the switch. Without enabling IGMP Snooping on a VLAN receiving excessive multicast traffic, a switch could become overburdened and behave erratically.*

To enable IGMP snooping globally, enter the **ip igmp snooping** command at the Global Configuration command prompt.

(config)**#ip igmp snooping**

To enable IGMP snooping on a specified VLAN on your unit, enter the **ip igmp snooping vlan** command at the Global Configuration command prompt.

(config)**#ip igmp snooping vlan** <*vlan id*>

Syntax	Description
<*vlan id*>	Specifies a valid VLAN ID on which to enable IGMP snooping. Range is **1** to **4095**.

The following example enables IGMP snooping on VLAN 1:

(config)**#ip igmp snooping vlan 1**

Step 3: Optional. Configure the IGMP Querier

Normally, the multicast router on the local network serves as the IGMP querier. However, when no multicast router exists in the VLAN to originate queries, the IGMP querier function can be enabled on the AOS unit to support multicast streams within a single VLAN.

When enabled, the IGMP querier sends IGMPv2 general membership queries every 125 seconds. Also, the queries will have a maximum response time field of 10 seconds.

The IGMP querier does not transmit group-specific membership queries.

To configure the IGMP querier, follow these steps:

1. From the Global Configuration command prompt, use the **ip igmp snooping querier vlan** command to enable the IGMP querier on the specified VLAN.

   (config)#**ip igmp snooping querier vlan** <*vlan id*> <*source address*>

Syntax	Description
<*vlan id*>	Specifies a valid VLAN ID on which the querier will be enabled. Range is **1** to **4094**.
<*source address*>	Specifies the source address used for IGMP query packets.

   The following example enables the IGMP querier on VLAN ID **1** with a source address of **10.10.10.1**:

   (config)**#ip igmp snooping querier vlan 1 10.10.10.1**

2. From the Global Configuration command prompt, use the **ip igmp snooping querier period** command to specify the interval at which the IGMP querier will send out IGMPv2 queries.

   (config)**#ip igmp snooping querier period** <*seconds*>

Syntax	Description
<*seconds*>	Specifies the number of seconds between sent queries. Range is **10** to **1000** seconds. The default is **125** seconds.

   The following example specifies a **10** seconds IGMP querier interval:

   (config)**#ip igmp snooping querier period 10**

Step 4: Optional. Configure the Default Multicast Router Interface

To add a static connection to a multicast router, use the **ip igmp snooping vlan mrouter interface** command at the Global Configuration command prompt.

(config)**#ip igmp snooping vlan** <*vlan id*> **mrouter interface** <*interface*>

Syntax	Description
<*vlan id*>	Specifies a valid VLAN ID. Range is **1** to **4095**.
<*interface*>	Specifies the port of the multicast router to be added to the list of multicast router interfaces. Specify an interface in the format *<interface type [slot/port | slot/port.subinterface id | interface id | interface id.subinterface id | ap | ap/radio | ap/radio.vap]>*. For example, for a switchport interface, use **switchport 0/1**; for a gigabit-switchport interface, use **gigabit-switchport 0/1**; for a port channel interface, use **port-channel 1**. Type **ip igmp snooping vlan** <*vlan id*> **mrouter interface ?** for a complete list of applicable interfaces.

The following example adds switchport interface 0/1 to the list of multicast router interfaces:

(config)**#ip igmp snooping vlan 1 mrouter interface switchport 0/1**

Step 5: Optional. Configure Static Multicast Group Members

To statically configure a Layer 2 interface as a member of a multicast group, use the **ip igmp snooping vlan static interface** command at the Global Configuration command prompt.

(config)**#ip igmp snooping vlan** <*vlan id*> **static** <*mac address*> **interface** <*interface*>

Syntax	Description
<*vlan id*>	Specifies a valid VLAN ID of the multicast group. Range is **1** to **4095**.
<*mac address*>	Specifies the multicast group's 48-bit medium access control (MAC) address. MAC addresses should be expressed in the following format xx:xx:xx:xx:xx:xx (for example, **00:A0:C8:00:00:01**).
<*interface*>	Specifies the interface of the multicast group member. Specify an interface in the format <*interface type [slot/port* | *slot/port.subinterface id* | *interface id* | *interface id.subinterface id* | *ap* | *ap/radio* | *ap/radio.vap]*>. For example, for a switchport interface, use **switchport 0/1**; for a gigabit-switchport interface, use **gigabit-switchport 0/1**; for a port channel interface, use **port-channel 1**. Type **ip igmp snooping vlan** <*vlan id*> **mrouter interface ?** for a complete list of applicable interfaces.

The following example configures the switchport interface 0/1 as a member of the multicast group with multicast MAC address **01:00:5E:01:01:01**:

(config)**#ip igmp snooping vlan 1 static 01:00:5E:01:01:01 interface switchport 0/1**

Step 6: Optional. Configure Handling of Unknown Multicast Frames

Beginning in R10.10.0, AOS units with IGMP snooping enabled drop unknown multicast frames by default. However, AOS units can be configured to flood VLAN ports with unknown multicast frames when IGMP snooping is enabled.

To enable flooding of unknown multicast frames, use the **ip igmp snooping flood-unknown** command at the Global Configuration prompt. The following example enables flooding of VLAN ports for unknown multicast frames:

(config)**#ip igmp snooping flood-unknown**

Step 7: Optional. Configure Immediate Leave

A port is removed from the IP multicasting group after the port fails to respond to a query. When enabled, the immediate leave option allows the AOS device to remove a port immediately after a host sends a leave message instead of waiting for a query to time out.

Immediate leave can be enabled on a per VLAN basis. Prior to configuring this setting, you must enable IGMP snooping on the VLAN as shown in *Step 2: Enable IGMP Snooping on page 6*.

To enable immediate leave, enter the **ip igmp snooping immediate-leave vlan** command at the Global Configuration command prompt.

(config)**#ip igmp snooping immediate-leave vlan** <*vlan id*>

Syntax	Description
<*vlan id*>	Specifies a valid VLAN ID on which to enable IGMP snooping. Range is **1** to **4095**.

The following example enables IGMP immediate leave on VLAN 1:

(config)**#ip igmp snooping immediate-leave vlan 1**

Troubleshooting

The following section describes **show** and **debug** commands associated with IGMP snooping. The **show** commands allow you to verify the IGMP snooping configuration on VLANs, and the **debug** commands display statistics and errors associated with IGMP snooping.

Show Commands

The **show ip igmp snooping** commands display configuration information for IGMP snooping. The command variations allow you to filter the type of IGMP snooping information displayed. You can choose to display the VLANs on which IGMP snooping is enabled or the ports associated with multicast routers. If no keywords are specified, all IGMP snooping information is displayed.

Command Variant	Description
show ip igmp snooping	Displays all IGMP snooping information.
show ip igmp snooping mrouter	Displays multicast router information for all VLANs.
show ip igmp snooping mrouter vlan <*vlan id*>	Displays multicast router information for a specified VLAN. Valid range for the <*vlan id*> variable is **1** to **4094**.
show ip igmp snooping vlan	Displays IGMP snooping information for all VLANs.
show ip igmp snooping vlan <*vlan id*>	Displays IGMP snooping information for the specified VLAN. Valid range for the <*vlan id*> variable is **1** to **4094**.

The following example shows IGMP snooping information for VLAN 1:

>enable
#show ip igmp snooping vlan 1
Vlan 1: IGMP snooping is enabled on this VLAN

The following example shows the multicast router ports associated with VLAN 200:

```
>enable
#show ip igmp snooping mrouter vlan 200
VLAN            Ports
----------------+ ---------------------------------
200             Gi0/2(static)
300             CPU(dynamic)
```

Debug Commands

The **debug ip igmp snooping** command enables debug messages for IGMP snooping errors and events. The **verbose** keyword can be appended to the end of the command to enable detailed debug messages.

Command Variant	Description
debug ip igmp snooping	Enables debug messages for IGMP snooping.
debug ip igmp snooping verbose	Enables detailed debug messages for IGMP snooping.

Turning on a large amount of debug information can adversely affect the performance of your unit.

The following example enables detailed debug messages for IGMP snooping:

```
>enable
#debug ip igmp snooping verbose
```

