

## Understanding IGMP Snooping

This Application Note relates to the following Dell PowerConnect™ product(s):

- PowerConnect 33xx switches

### Abstract

This Application Note explains how a feature called IGMP snooping can significantly reduce traffic from streaming media and other bandwidth-intensive IP multicast applications. This document introduces the IGMP protocol and provides step-by-step instructions for configuring Dell PowerConnect 33xx switches to use IGMP snooping.

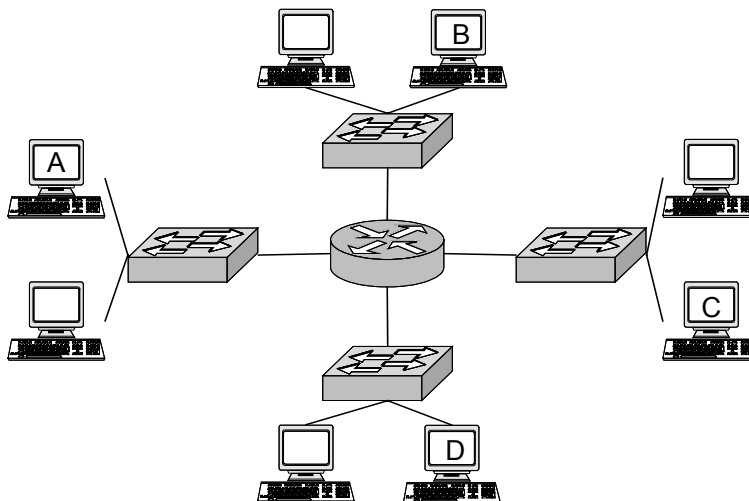
### Applicable Network Scenarios

By default, layer 2 devices such as Dell PowerConnect 33xx switches treat IP multicast traffic in the same manner as broadcast traffic – namely, by forwarding frames received on one interface to all other interfaces. This may create excessive traffic on the network and degrade the performance of hosts attached to the switches. Every frame received by each host generates an interrupt that the host must process, robbing cycles that might instead be used by applications.

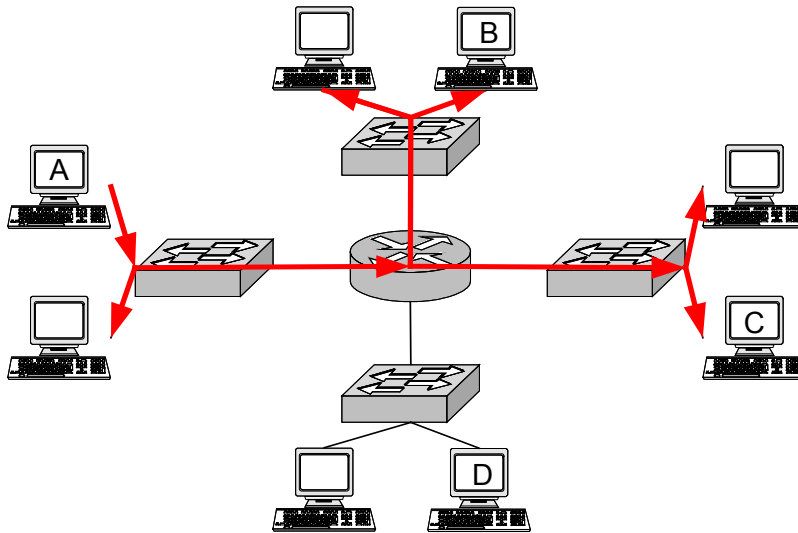
Layer 3 devices have less of a problem with rampant broadcast and multicast traffic because of their ability to segment networks and forward traffic only to actual destination interfaces.

With Internet Group Management Protocol (IGMP) snooping, Layer 2 devices also can make intelligent multicast forwarding decisions by examining the contents of each frame's Layer 3 IP header.

Consider the example of a heterogeneous Layer 2 and Layer 3 network that does not use IGMP snooping. The figure below shows a simple network in which eight hosts connect to four Layer 2 switches. The switches in turn connect to one router in the middle.

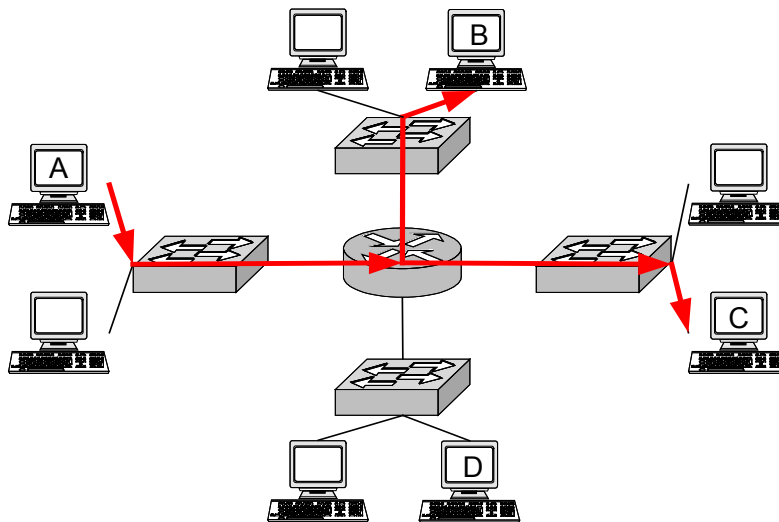


Now suppose Host A is an IP multicast transmitter and Hosts B and C are multicast receivers in the same group as Host A. The router will correctly forward IP multicast traffic only to those segments with registered receivers (Hosts B and C). However, the Layer 2 switches will flood the traffic to all hosts on all interfaces.



The larger the network grows, the greater the performance impact of this extraneous multicast traffic.

Now we can see what happens with the addition of IGMP Snooping on the Layer 2 devices. Just as desired, only hosts that are group receivers actually receive multicast traffic.



## Technology Background

The Internet Engineering Task Force (IETF) defined IGMP as a means of associating *groups* of IP multicast transmitters and receivers. Each member host of an IP multicast is either a transmitter or a receiver.

A station that wishes to become a receiver sends an IGMP “group join” message to that group’s transmitter. Each Layer 3 device that forwards an IGMP join message records the group ID and source

interface in its multicast forwarding table. When the transmitter sends IP multicast traffic, the Layer 3 device will then forward the traffic only to those interfaces from which it has received join messages. Thus, the Layer 3 device forwards IP multicast traffic only to those hosts that have requested it.

Applications that use IP multicast, such as those involving streaming media, automatically handle IP multicast group membership. Users do not have to manually send IGMP messages.

Over time, the IETF has defined three versions of IGMP:

**IGMPv1:** [IETF Request for Comments 1112 \(RFC 1112\)](#) defines the original version of IGMP. RFC 1112 defines the join message that hosts use to join an IP multicast group. However, IGMPv1 does not define a method for hosts to leave a multicast group. With IGMPv1, routers must use a timer to determine which hosts are still members of the group.

**IGMPv2:** [RFC 2236](#) defines “group leave” messages that enable IP multicast-aware devices to keep current information on group membership.

**IGMPv3:** [RFC 3376](#) represents a major revision of IGMP. Instead of the one-transmitter/many-receiver model of IGMP versions 1 and 2, hosts using IGMPv3 specify lists of transmitters to listen to.

IGMP snooping, as the name implies, is a method by which Layer 2 devices can “listen in” on IGMP conversations between hosts and routers. When a switch hears a group join message from a host, it notes which switch interface it heard the message on, and adds that interface to the group. Similarly, when a Layer 2 switch hears a group leave message or a response timer expires, the switch will remove that host’s switch interface from the group.

IP multicast traffic has some special characteristics. Destination IP addresses for multicast traffic fall within the range of 224.0.0.1 through 239.255.255.255 (although some addresses within this range are reserved). Destination Ethernet addresses for multicast traffic begin with 01:00:5E and end with the low-order 23 bits of the destination IP address.

## Proposed Solution

### Overview

Configuring IGMP snooping is a simple two-step process on Dell PowerConnect 33xx switches. First you must enable IGMP snooping, and then you enable filtering of multicast traffic. Two examples are given here:

- Enabling IGMP snooping globally for all interfaces on a Dell PowerConnect 3348 switch
- Enabling IGMP snooping for interfaces of a selected VLAN on a Dell PowerConnect 3348 switch

While it is possible to restrict the scope of IGMP snooping by enabling it only on selected VLANs, it is a much more common practice to enable IGMP snooping on all switch interfaces.

Note that at least one Layer 3 device must exist in the network for IP multicast and IGMP snooping to work. Layer 2 switches by themselves cannot support IP multicast service.

### Step-By-Step Instructions

1. To enable IGMP snooping for all switch interfaces, enter the following commands from the console:

```
Dell-3348> enable
Dell-3348# configure
Dell-3348(config)# ip igmp snooping
Dell-3348(config)# bridge multicast filtering
```

```
Dell-3348(config)# end
Dell-3348# copy running-config startup-config
```

This sequence puts the switch in executive mode; enters into configuration mode; enables IGMP snooping globally; enables selective forwarding of multicast traffic; exits configuration mode; and saves the running configuration.

2. To enable IGMP snooping for a given VLAN (we use VLAN ID 100 in this example), enter the following commands from the console:

```
Dell-3348> enable
Dell-3348# configure
Dell-3348(config)# int vlan 100
Dell-3348(config-if)# ip igmp snooping
Dell-3348(config-if)# bridge multicast filtering
Dell-3348(config-if)# end
Dell-3348# copy running-config startup-config
```

This sequence puts the switch in executive mode; enters into configuration mode; selects VLAN 100 for configuration; enables IGMP snooping on VLAN 100; enables selective forwarding of multicast traffic; exits configuration mode; and saves the running configuration.

### Conclusion

As described above, IGMP snooping can provide a simple yet effective means of reducing unwanted traffic from the network. With IGMP snooping enabled globally, a Dell PowerConnect switch will forward IP multicast traffic only to interfaces with group members attached.

This Application Note is for informational purposes only, and may contain typographical errors and technical inaccuracies. The content is provided as is, without express or implied warranties of any kind. Information in this document is subject to change without notice.

Trademarks used in this text: Dell, the DELL logo, and PowerConnect are trademarks of Dell Inc. Other trademarks and trade names may be used in this document to refer to either the entities claiming the marks and names or their products. Dell Inc. disclaims any proprietary interest in trademarks and trade names other than its own. © 2004 Dell Inc. All rights reserved.