Test your device's IGMP snooping implementation with Agilent's multi-port Packets and Protocols Application.

Multicasting is the process of sending data to a certain group of hosts on a network. The Internet Group Membership Protocol (IGMP) is a protocol used by hosts to report their multicast group memberships to multicast routers. This protocol is used in a variety of applications such as web TV and desktop conferencing.
Generally, a Layer-2 switch will flood traffic out of all ports for which the destination address is unknown. This means that multicast traffic will be flooded throughout the switch's broadcast domain, and can therefore cause a lot of bandwidth to be unnecessarily consumed if only a few hosts are interested in receiving the data.

IGMP snooping is a process whereby a Layer-2 switch passively listens (or "snoops") the Layer-3 IGMP traffic to determine which ports are interested in receiving certain multicast traffic. The switch listens for IGMP Query, Report and Leave protocol messages. If desired, IGMP snooping can be configured on a per-VLAN basis. Traffic will be dynamically forwarded only to those ports that want to receive the multicast transmission. This can significantly reduce the amount of multicast traffic passing through a Layer-2 network, thus better utilizing the available bandwidth.

This application note explains how to use N2X to test IGMP snooping implementation in your Enterprise networks and devices.

Testing with Agilent N2X

Agilent N2X is the industry’s most comprehensive test solution for testing the development and deployment of network services for converging network infrastructures. Service providers, network equipment manufacturers (NEMs) and component manufacturers can verify service attributes of entire networks end-to-end, while also isolating problems down to individual networking devices and subsystems.

Agilent N2X incorporates the strength of the RouterTester 900 to deliver unparalleled test realism to verify the ultimate performance, scalability and resilience of carrier grade services and infrastructure.

The N2X Packets and Protocols application enables N2X to verify the traffic forwarding performance, protocol scalability and services delivering capabilities of switching and routing devices across the enterprise, metro/edge and core.

A powerful and flexible PDU builder makes it easy to build streams of Layer-2 Layer-7 Protocol Data Units (PDUs) containing multiple encapsulations and even proprietary formats. With the PDU builder, you can define a packet length distribution and common header type, and then edit any field, including the payload. You can also set a field modifier to vary a header field's values, creating a separate flow or measurable stream for each one. This tool reduces the time needed to generate multi-encapsulated traffic types thereby allowing you to get more out of your testing time.

Users can also generate and analyze more streams per port than any other tester available (up to 32,768 transmit and receive streams per port), making it easy to scale your tests beyond the maximum performance parameters of your network or device. Your test can include 256 test ports per system, with 15 traffic profiles and up to 1023 - 4095 stream groups per port, depending on the port type. In total, the Traffic Generation and Analysis application can generate and measure statistics on 32,768 streams per port, using either four separate measurements over 32,768 streams or twelve measurements over 4,096 streams.
Testing IGMP Snooping

The following test procedure describes how to test your Layer-2 device's IGMP Snooping implementation.

Figure 1 below shows three N2X ports being used to test IGMP Snooping implementation. One port will be used to simulate a multicast server (or multicast router), transmitting traffic to multicast group addresses. The other two ports will simulate hosts, one of which is joining multicast groups with IGMP. When IGMP snooping is enabled, we expect traffic to be received only at the first destination test port.

![Diagram of test configuration](image)

**Figure 1: Test configuration for verifying IGMP snooping implementation**

**Test Steps**

**Step 1: Select test modules and ports.**
Configure three Ethernet test ports; one of these ports will be a multicast server (N2X source port), while the other two ports will be hosts.

**Step 2: Ensure that IGMP snooping is disabled on the DUT.**
Step 3: Enable IGMP emulation on the first destination test port.
This port will simulate a multicast host. Then enable IGMP to join certain multicast groups on this port (i.e. send IGMP Report messages). Please refer to Figure 2 and 3.

![Image of IGMP emulation session on N2X](image1.png)

The IP addresses are irrelevant, since the DUT is a Layer-2 device. If desired, the IGMP sessions can run over VLANs. Either IGMPv2 or IGMPv3 can be used, depending on the DUT’s implementation.

**Figure 2: Define an IGMP emulation session on N2X**

![Image of IGMP group membership profiles](image2.png)

These groups are being joined. In this example, the host is joining 2 groups.

**Figure 3: Simulate a multicast group to become a member**
Step 4: Transmit multicast traffic from the source tester port.
This port is simulating a multicast server. The destination addresses for this traffic should match the multicast groups being joined by the destination test port 1. Please refer to Figure 4.

Please note; when setting a Multicast address for Ethernet interfaces, it is important to set the MAC layer address correctly so that Layer-2 switches can recognize the multicast traffic.
IP multicast frames all use MAC addresses beginning with:
0x0100.5Exx.xxxx
where xx.xxxx is the last 23-bits of the IGMP multicast group address.

A PDU is created with IPv4 over Ethernet II.

The Destination IP addresses must match the multicast groups being joined by the host.

Either a List or an Incrementing range of MAC addresses can be specified. Use Increment if the multicast groups are contiguous.

The proper destination MAC addresses are specified based on the IGMP Group addresses.

VLAN tags may be specified if the subinterfaces are being used on the DUT.

Figure 4: Multicast traffic definition using N2X's powerful PDU builder
Step 5: Verify that the traffic is received on both of the destination tester ports.
This will verify the proper operation of a Layer-2 switch as it floods that traffic to all ports in the absence of IGMP snooping.

Step 6: Enable IGMP snooping on the Layer-2 DUT.

Step 7: Re-send the IGMP join messages from the simulated multicast host.
This will cause the DUT to learn which of its ports are connected to multicast hosts.

Step 8: Confirm proper operation of IGMP snooping.
The multicast traffic should be received on the first destination port, but not on the second port. Please refer to Figure 5.

**Figure 5: Verify IGMP snooping implementation**

### Additional Test Scenarios

After testing the basic IGMP snooping operation as described above, you may want to consider some of the following tests:

- Enabling subinterfaces (through multiple VLANs) on N2X and DUT.
- Scaling the number of multicast groups that are being tested.
- Testing both IGMPv2 and IGMPv3 groups.
Agilent N2X Test Advantages

- Full IGMP protocol emulation for both IGMPv2 and IGMPv3 (the full host state machine is implemented).
- Up to 6 levels of VLAN tags are supported, allowing easy setup of multiple VLAN tags.
- Ability to scale the number of multicast groups being joined to tens of thousands, hence stress testing the IGMP snooping implementation.
- N2X supports 32k traffic streams per port, allowing for granular QoS and operational measurements on each of these streams.
- If the DUT requires, N2X can become an IGMP Querier through the transmission of Query PDUs on the N2X source port (i.e. multicast router).
- N2X also supports the PIM-SM and MSDP protocols for a complete multicast test solution.

Conclusion

As highlighted in this application note, IGMP snooping is a process whereby a Layer-2 switch passively listens to (or "snoops") Layer-3 IGMP traffic for IGMP Queries, Reports and Leave protocol messages. This process can significantly reduce the amount of multicast traffic passing through a Layer-2 switch, as traffic is forwarded only to ports interested in receiving the specified traffic.

Using Agilent's N2X solution, users can simply and effectively test IGMP Snooping.

The N2X solution set offers a powerful and versatile platform to address the evolving test needs of enterprise, metro/edge and core routing and switching devices.