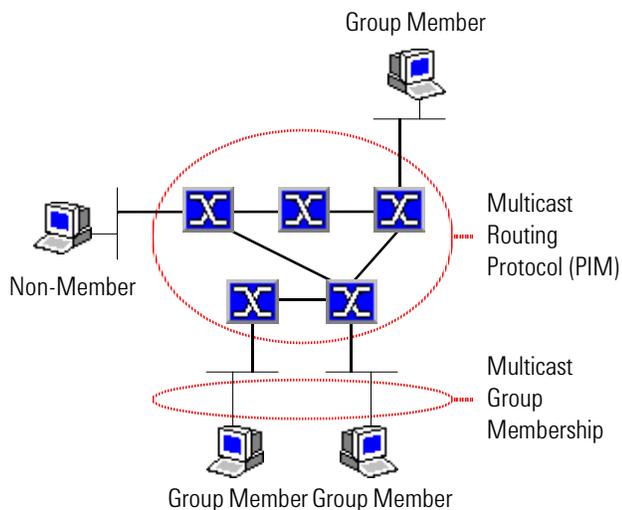


Application Note

IGMP (v3) Multicast Functional Testing



Introduction

Multicasting allows a host to send data packets across the Internet to a set of hosts that can be on different, geographically dispersed subnets. The source host sends data to a pseudo destination called a *multicast group*, and does so efficiently, using less bandwidth than unicast or broadcast traffic. Unlike unicast transmission, which would copy a packet to send it to multiple destinations, multicast sources send a packet only once.

Multicast-aware routers on the Internet use multicast *routing* protocols like PIM to deliver packets across the Internet to subnets that have hosts in the multicast group. These routers build and maintain distribution trees to forward multicast traffic.

Multicast routers connected to subnets use multicast *group membership* protocols like IGMP to discover which local hosts are members of which multicast groups, and to deliver multicasted packets to member hosts.

Current applications of multicasting include email distribution lists, routing information flooding, and web-based training seminars and voice/video conferences.



Test Challenges

Routers supporting IGMP Version 3 must correctly implement the following new features:

IGMP v3	IGMP v2
<ul style="list-style-type: none"> Source Specific Multicast (SSM): A host receives packets only from specified sources. Include/exclude filters are used to accept/deny traffic from sources. Membership reports can contain multiple multicast groups, up to the MTU of the interface. Leave a multicast group using a Membership report that includes no sources. Hosts can also respond to group-source-specific queries. 	<ul style="list-style-type: none"> The host simply received all packets sent to the multicast group. Membership reports can contain only one multicast group. Leave using a specific Leave message (which is no longer used in v3). Hosts can respond to group- or source-queries.

Other tests:

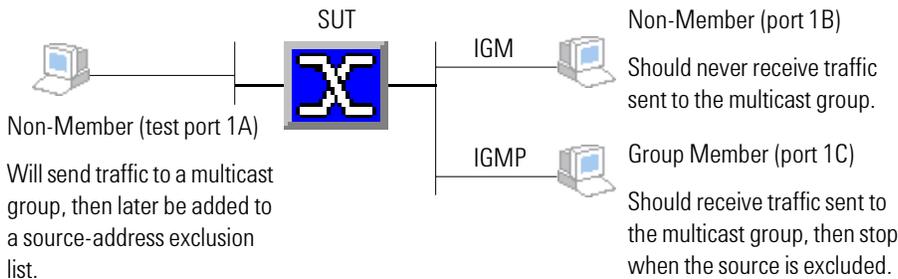
Whether enabling IGMP Version 3 maintains backwards compatibility with older IGMP versions.

Whether the performance of unicast traffic suffers while multicast traffic is being propagated.

Scaling to find the maximum number of multicast groups before packet loss or excess latency occurs.

Test Description

This note describes how to use a 4-port Gigabit Ethernet module to simulate 3 different hosts and test a SUT's implementation of IGMPv3 Source Specific Multicast and Include/Exclude filters:



Test Steps

1. Enable IGMPv3 on test ports (i.e. hosts) 1B and 1C.
2. Simulate a multicast group and enable test port 1C to become a member later.
3. Set up test port (i.e. host) 1A to send traffic to the multicast group.
4. Verify that port 1C receives multicast packets but port 1B does not.
5. Add port 1A's address to the excluded sources list for the multicast group, and verify that port 1C no longer receives multicast packets.

This note does not illustrate these test preamble steps:

Select test ports 1A, 1B, and 1C.

Configure the IP addresses of the test ports and their connected SUT interfaces.

Bring up the physical and link layers.

SUT Setup

Configure the SUT as follows:

Enable IGMP Version 3 on the SUT interfaces connected to ports 1B and 1C.

Enable PIM sparse or sparse-dense mode on the interfaces.

Note: On some routers you also need to distribute the Multicast cache to ensure that IGMP hosts receive traffic.

Multicast Addresses

Multicast groups are identified by a Class D IP address in the range 224.0.0.0 to 239.255.255.255. For details, see RFC 1112.

There are two types of reserved multicast addresses — those reserved for all multicast applications and those reserved from use by IGMP. With IGMPv3, these two lists now contain the same set of addresses:

- 224.0.0.0 — Base multicast address
- 224.0.0.1 — All systems on this subnet
- 224.0.0.2 — All routers on this subnet
- 224.0.0.4 — DVMRP routers
- 224.0.0.5 — OSPF routers
- 224.0.0.6 — OSPF designated routers
- 224.0.0.13 — PIM routers
- 224.0.0.14 — RSVP encapsulation
- 224.0.0.22 — IGMPv3 membership

Other address restrictions enforced by the tester:

A multicast address group's first and last address must be within the valid range and not contain reserved addresses.

Each multicast group pool must contain a unique set of addresses, which can overlap but not intersect (i.e. 1, 3, 5 and 2, 4, 6 overlap but do not intersect).

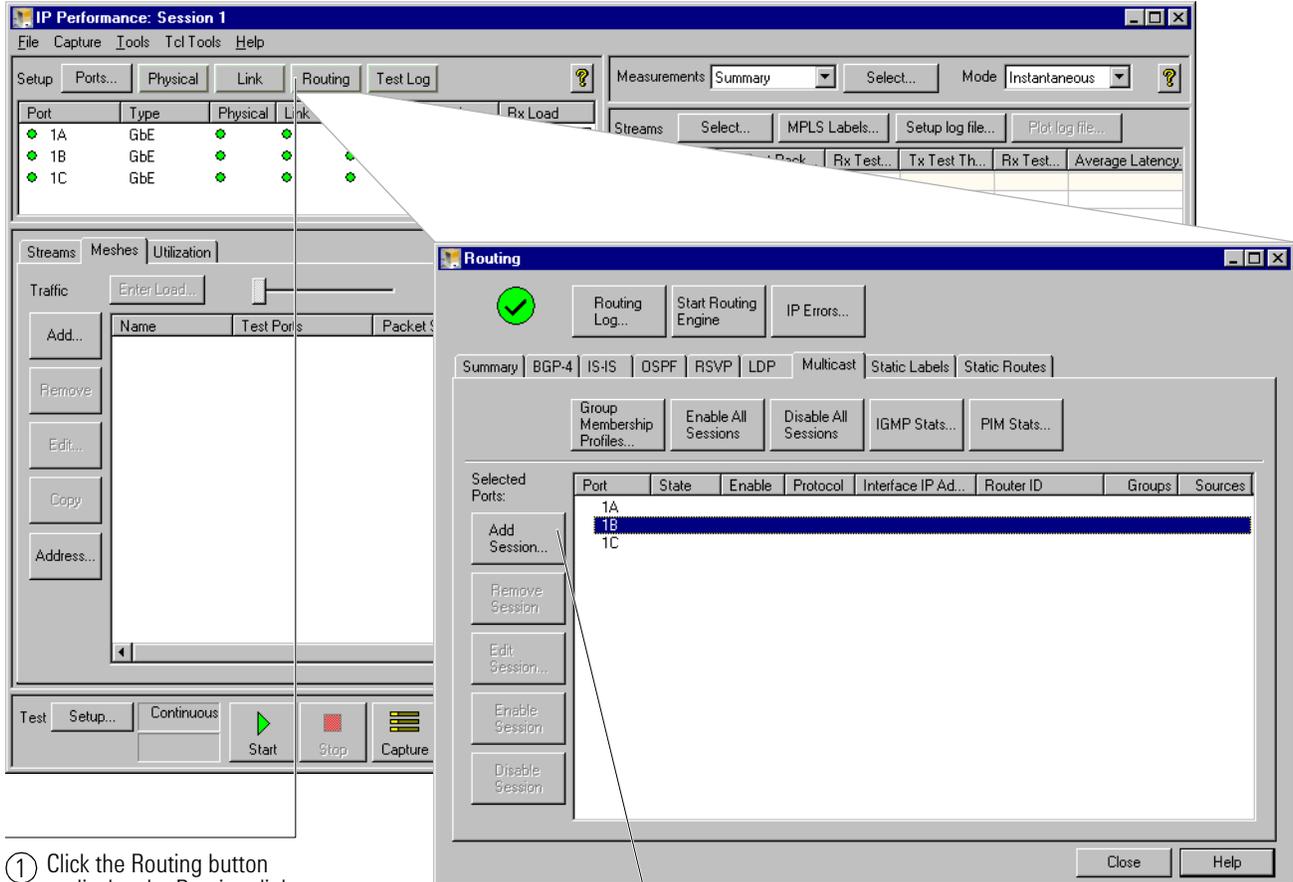
If two multicast group pools have an address in common, the two pools cannot be used by the same test port at the same time. If the first then the second pool is enabled, the tester considers the second pool invalid. However, if the first pool is disabled, the second is no longer considered invalid and can be enabled.

Note: You can use the tester API to remove an address from the reserved list, after which you can send multicast traffic to the address. This is useful for testing how the SUT handles traffic sent to restricted multicast addresses. When addresses are reserved they cannot be used by multicast traffic or IGMP. When they are unreserved they can be used by traffic, but not by IGMP. We recommend that you do not change the list of reserved addresses.

References

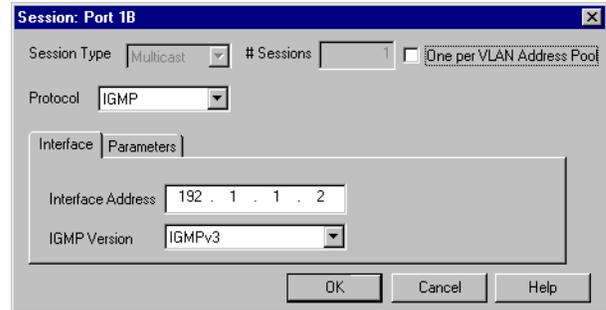
- RFC 1112: Host Extensions for IP Multicasting (IGMP Version 1)
- RFC 2236: IGMP Version 2
- draft-ietf-idmr-igmp-v3-nn.txt: IGMP Version 3
- draft-holbrook-ssm-arch-nn.txt: SSM for IP

Step 1: Enable IGMPv3 on test ports (i.e. hosts) 1B and 1C

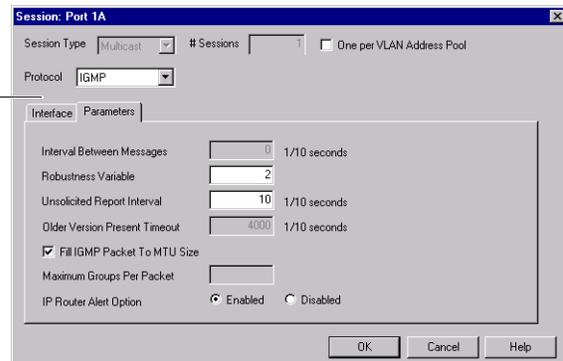


① Click the Routing button to display the Routing dialog.

② Click the Multicast tab, select port 1B, and click the Add Session button to display the Session dialog. Use this dialog to configure the test port (host) 1B's IGMP emulation. On the Interface tab, IGMPv3 is the default.



③ On the Parameters tab, adjust the default IGMP settings as needed. Click the Help button for details about a parameter.



④ Repeat to enable IGMPv3 on test port (host) 1C.

Step 2: Simulate a multicast group and enable test port 1C to become a member later

1 Back on the Routing dialog, click the Group Membership Profiles button.

2 On the Group Membership Profiles dialog, select port 1C and click Add Group Pool. On the IGMP Group Pool dialog, click Add Pools.

3 On the Multicast Group Pools dialog, click the Add button to define a new multicast group.

4 On the Multicast Group Pool dialog, define the multicast group address. You can define a "pool" of several addresses to scale the test and see how the SUT handles up to 100,000 different multicast groups. This test requires only one group.

5 Back on the IGMP Group Pool dialog, select the newly defined multicast group from the pulldown menu. Back on the Group Membership Profiles dialog, under port 1C, this multicast group is shown with a checkbox so that you can dynamically join and leave the group. By default, the filter mode is Exclude with no addresses in the group's source list.

Step 3: Set up test port (i.e. host) 1A to send traffic to the multicast group

The IP Performance window shows the Traffic area with an 'Add...' button. The Traffic Class Configuration dialog is open, showing 'My Multicast Traffic' as the Traffic Class Name. Under Traffic Distribution, 'Multicast' is selected. In the Source Ports section, '1B' is in the Available Ports list and '1A' is in the Selected Ports list. The Multicast Group is set to 'My Multicast Group'.

② In the Traffic area of the IP Performance window, select the Meshes tab, then click the Add button.

② On the Traffic Class Configuration dialog, select the port from which to send multicast traffic. Click on a port in the Available Ports list and click the Add button to send traffic from the selected test port.

③ On the Traffic Class Configuration dialog, select the multicast group to receive traffic. The default AGT_MULTICAST_GROUP cannot be used to receive traffic. Select a multicast group you configured on the previous page from the pull-down menu.

② Back on the IP Performance window's Traffic area, click the Address button.

⑤ Specify the source address to use in multicast packets. Select the multicast traffic stream, select the destination "route" at the bottom, then click the Edit Source button.

The Stream Addresses for Traffic Classes dialog shows a list of streams: 1A (1 address), 1B (0 addresses), and 1C (0 addresses). The selected stream is '1A -> My Multi...'. The Source Address is set to '192.168.1.2'. The Destination Route Pools section shows a table with one route: 230.0.0.0/32 with 1 route and 1 source address used.

⑥ Add a new source pool. Click Add Pools. On the Multicast Source Address Pools dialog, click Add. Then, on the Multicast Source Address Pool dialog, enter the source address(es) to use.

⑦ Back on the IP Performance window's Test area, click the Start button to start generating the multicast traffic and measuring statistics.

The Source Addresses for Multicast Traffic dialog shows a table with one source address pool: 'AGT_SOURCE_ADDRES...'. The Source Name is 'AGT_SOURCE_ADDRES...', the First Address is '192.168.1.1', the Last Address is '192.168.1.1', and the Num Addresses is '1'.

Step 4: Verify that port 1C receives multicast packets but port 1B does not

1 On the Routing dialog, click Start Routing Engine.

This begins the IGMP emulations on ports 1B and 1C. The button toggles to Stop Routing Engine. Each port's State should transition from Disabled to Enabled.

2 Click Group Membership Profiles.

3 Click the checkbox to join the group.

4 Port 1C should begin receiving multicast packets.

Routing Dialog:

Port	State	Enable	Protocol	Interface IP Ad...	Router ID	Groups	Sources
1A							
1B	1	Enabled	IGMPv3	192.2.1.2		0	0
1C	2	Enabled	IGMPv3	192.3.1.2		1	0

Group Membership Profiles Dialog:

Session	State	Protocol	Join	Groups	First	Last	Modifier	Filter	Sources	
1A										
1B	2	Disabled	IGMPv3	0					0	
1C	3	Disabled	IGMPv3	100	100	230.0.0.0	230.0.0.99	1/32	EXC...	1

IP Performance: Session 1 Dialog:

Port	Type	Physical	Link	Routing	Tx Load	Rx Load
1A	GbE	●	●	●		
1B	GbE	●	●	●		
1C	GbE	●	●	●		

Streams Table:

Ports/Streams	Tx Test Pack...	Rx Test...	Tx Test Th...	Rx Test...	Average Latency
All Ports	2403846	1201923			
Port 1A	2403846	0	1230.77	0.00	
Port 1B	0	0	0.00	0.00	
Port 1C	0	1201923	0.00	615.38	500000.0

Rx Test Packets Graph:

Time: 0:00:00:11

Rx Test Packets: 1,200,000

Graph showing a red bar at approximately 1,200,000 packets.

Agilent's RouterTester System

Agilent's RouterTester System offers a powerful and versatile test platform to address the evolving test needs of metro/edge platforms, core routers and optical switches. RouterTester provides Network Equipment Manufacturers and Service Providers with the industry's leading tools for wire speed, multiport traffic generation and performance analysis of today's networking devices.

Warranty and Support

Hardware Warranty

All RouterTester and QA Robot hardware is warranted against defects in materials and workmanship for a period of 3 years from the date of shipment.

Software Warranty

All RouterTester and QA Robot software is warranted for a period of 90 days. The applications are warranted to execute and install properly from the media provided. This warranty only covers physical defects in the media, whereby the media is replaced at no charge during the warranty period.

Software Updates

With the purchase of any new system controller Agilent will provide 1 year of complimentary software updates. At the end of the first year you can enroll into the Software Enhancement Service (SES) for continuing software product enhancements.

Support

Technical support is available throughout the support life of the product. Support is available to verify that the equipment works properly, to help with product operation, and to provide basic measurement assistance for the use of the specified capabilities, at no extra cost, upon request.

Ordering Information

To order and configure the test system consult your local Agilent field engineer.

United States:

Agilent Technologies
Test and Measurement Call Center
P.O. Box 4026
Englewood, CO 80155-4026
1-800-452-4844

Canada:

Agilent Technologies Canada Inc.
5150 Spectrum Way
Mississauga, Ontario
L4W 5G1
1-877-894-4414

Europe:

Agilent Technologies
European Marketing Organisation
P.O. Box 999
1180 AZ Amstelveen
The Netherlands
(31 20) 547-2323
United Kingdom
07004 666666

Japan:

Agilent Technologies Japan Ltd.
Measurement Assistance Center
9-1, Takakura-Cho, Hachioji-Shi,
Tokyo 192-8510, Japan
Tel: (81) 426-56-7832
Fax: (81) 426-56-7840

Latin America:

Agilent Technologies
Latin American Region Headquarters
5200 Blue Lagoon Drive, Suite #950
Miami, Florida 33126
U.S.A.
Tel: (305) 269-7500
Fax: (305) 267-4286

Asia Pacific:

Agilent Technologies
19/F, Cityplaza One, 1111 King's Road,
Taikoo Shing, Hong Kong, SAR
Tel: (852) 3197-7777
Fax: (852) 2506-9233

Australia / New Zealand:

Agilent Technologies Australia Pty Ltd
347 Burwood Highway
Forest Hill, Victoria 3131
Tel: 1-800-629-485 (Australia)
Fax: (61-3) 9272-0749
Tel: 0-800-738-378 (New Zealand)
Fax: (64-4) 802-6881

www.agilent.com/comms/RouterTester

