WIKIPEDIA

Internet Group Management Protocol

The **Internet Group Management Protocol** (**IGMP**) is a communications protocol used by hosts and adjacent routers on IPv4 networks to establish multicast group memberships. IGMP is an integral part of IP multicast and allows the network to direct multicast transmissions only to hosts that have requested them.

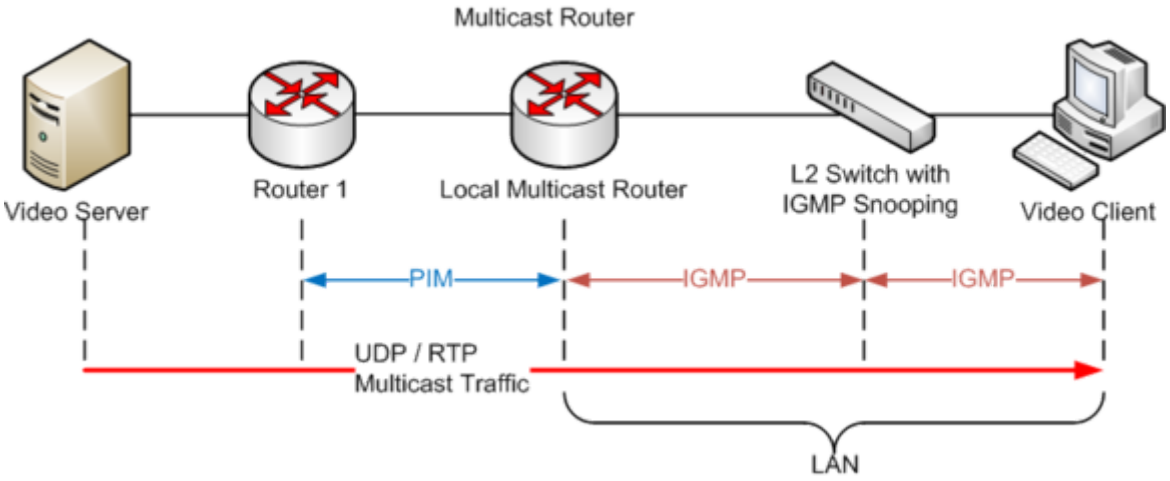
IGMP can be used for one-to-many networking applications such as online streaming video and gaming, and allows more efficient use of resources when supporting these types of applications.

IGMP is used on IPv4 networks. Multicast management on IPv6 networks is handled by Multicast Listener Discovery (MLD) which is a part of ICMPv6 in contrast to IGMP's bare IP encapsulation.

Contents

Architecture

A network designed to deliver a multicast service using IGMP might use this basic architecture:



IGMP operates between a host and a local multicast router. Switches featuring IGMP snooping derive useful information by observing these IGMP transactions. Protocol Independent Multicast (PIM) is then used between the local and remote multicast routers, to direct multicast traffic from hosts sending multicasts to hosts that have registered through IGMP to receive them.

IGMP operates on the network layer, just the same as other network management protocols like ICMP.[1]

The IGMP protocol is implemented on a particular host and within a router. A host requests membership to a group through its local router while a router listens for these requests and periodically sends out subscription queries. A single router per subnet is elected to perform this querying function. Some multilayer switches include an IGMP querier capability to allow their IGMP snooping features to work in the absence of an IP multicast capability in the larger network.

IGMP is vulnerable to some attacks,[2][3][4][5] and firewalls commonly allow the user to disable it if not needed.

Versions

There are three versions of IGMP.[6] IGMPv1 is defined by RFC 1112 (https://tools.ietf.org/html/rfc1112), IGMPv2 is defined by RFC 2236 (https://tools.ietf.org/html/rfc2236) and IGMPv3 was initially defined by RFC 3376 (https://tools.ietf.org/html/rfc3376) and has been updated by RFC 4604 (https://tools.ietf.org/html/rfc4604) which defines both IGMPv3 and MLDv2. IGMPv2 improves IGMPv1 by adding the ability for a host to signal desire to leave a multicast group. IGMPv3 improves IGMPv2 by supporting source-specific multicast[7] and introduces membership report aggregation.

These versions are backwards compatible. A router supporting IGMPv3 can support clients running IGMPv1, IGMPv2 and IGMPv3. IGMPv1 uses a query-response model. Queries are sent to 224.0.0.1. Membership reports are sent to the group's multicast address. IGMPv2 accelerates the process of leaving a group and adjusts other timeouts. Leave-group messages are sent to 224.0.0.2. A group-specific query is introduced. Group-specific queries are sent to the group's multicast address. A means for routers to select an IGMP querier for the network is introduced. IGMPv3 introduces source-specific multicast capability. Membership reports are sent to 224.0.0.22.

Messages

There are several types of IGMP messages:

General membership queries
: Sent by multicast routers to determine which multicast addresses are of interest to systems attached to the network(s) they serve to refresh the group membership state for all systems on its network.

Group-specific membership queries
: Used for determining the reception state for a particular multicast address

Group-and-source-specific queries
: Allow the router to determine if any systems desire reception of messages sent to a multicast group from a source address specified in a list of unicast addresses

Membership reports
: Sent by multicast receivers in response to a membership query or asynchronously when first registering for a multicast group

Leave group messages
: Sent by multicast receivers when specified multicast transmissions are no longer needed at the receiver

IGMP messages are carried in bare IP packets with IP protocol number 2.[8]:§4 Similar to the Internet Control Message Protocol, there is no transport layer used with IGMP messaging.

IGMPv2 messages

IGMPv2 packet structure[9]:§2

bit offset	0–7	8–15	16–31
0	Type	Max Resp Time	Checksum
32	Group Address		

Where:

Type
Indicates the message type as follows

IGMP message type values

Message	Type value
Membership Query	0x11
IGMPv1 Membership Report	0x12
IGMPv2 Membership Report	0x16
IGMPv3 Membership Report	0x22
Leave Group	0x17

Max Resp Time
Specifies the required responsiveness of replies to a Membership Query (0x11). This field is meaningful only in Membership Query; in other messages it is set to 0 and ignored by the receiver. The field specifies time in units of 0.1 second (a field vale of 10 specifies 1 second). Larger values reduce IGMP traffic burstiness and smaller values improve protocol responsiveness when the last host leaves a group.[9]:§2.2

Group Address
This is the multicast address being queried when sending a Group-Specific or Group-and-Source-Specific Query. The field is zeroed when sending a General Query.

The message is sent using the following IP destination addresses:

IGMPv2 destination address[9]:§9

Message Type	Multicast Address
General Query	All hosts (224.0.0.1)
Group-Specific Query	The group being queried
Membership Report (all IGMP versions)	The group being reported
Leave Group	All routers (224.0.0.2)

IGMPv3 membership query

IGMPv3 membership query[8]:§4.1

bit offset	0–3	4	5–7	8–15	16–31
0	Type = 0x11			Max Resp Code	Checksum
32	Group Address				
64	Resv	S	QRV	QQIC	Number of Sources (N)
96	Source Address [1]				
128	Source Address [2]				
	. . .				
	Source Address [N]				

Where:

Max Resp Code
: This field specifies the maximum time (in 1/10 second increments) allowed before sending a responding report. If the number is below 128, the value is used directly. If the value is 128 or more, it is interpreted as an exponent and mantissa.

Checksum
: This is the 16-bit one's complement of the one's complement sum of the entire IGMP message.

Group Address
: This is the multicast address being queried when sending a Group-Specific or Group-and-Source-Specific Query. The field is zeroed when sending a General Query.

Resv
: This field is reserved. It should be zeroed when sent and ignored when received.

S (Suppress Router-side Processing) Flag
: When this flag is set, it indicates to receiving routers that they are to suppress the normal timer updates.

QRV (Querier's Robustness Variable)
: If this is non-zero, it contains the Robustness Variable value used by the sender of the query. Routers should update their Robustness Variable to match the most recently received query unless the value is zero.

QQIC (Querier's Query Interval Code)
: This code is used to specify the Query Interval value (in seconds) used by the querier. If the number is below 128, the value is used directly. If the value is 128 or more, it is interpreted as an exponent and mantissa.

Number of Sources (N)
: This field specifies the number of source addresses present in the query. For General and Group-Specific Queries, this value is zero. For Group-and-Source-Specific Queries, this value is non-zero, but limited by the network's MTU.

Source Address [i]
: The Source Address [i] fields are a vector of n IP unicast addresses, where n is the value in the Number of Sources (N) field.

Implementations

The FreeBSD,[note 1] Linux[note 2] and Windows operating systems support IGMP at the host side.

See also

- Internet Group Management Protocol with Access Control

Notes

1. IGMPv3 was added to FreeBSD in version 8.0.
2. IGMPv3 was added in the Linux 2.5 kernel series.

References

1. Forouzan, Behrouz A. (2012). *Data Communications and Networking* (5th ed.). New York, NY: McGraw-Hill. p. 658. ISBN 0073376221.
2. Spoofed IGMP report denial of service (http://www.securityfocus.com/bid/5020/info) vulnerability.
3. "Fragmented IGMP Packet May Promote "Denial of Service" Attack" (https://web.archive.org/web/20050213091318/http://support.microsoft.com/default.aspx?scid=kb;en-us;238329&sd=tech). Dec 20, 2004. Archived from the original (http://support.microsoft.com/default.aspx?scid=kb;en-us;238329&sd=tech) on 2005-02-13.
4. IGMP Security Problem Statement and Requirements (http://www.securemulticast.org/GSEC/gsec3_ietf53_SecureIGMP1.pdf#search=%22igmp%20attacks%22) Archived (https://web.archive.org/web/20061013122139/http://www.securemulticast.org/GSEC/gsec3_ietf53_SecureIGMP1.pdf) 2006-10-13 at the Wayback Machine.
5. "Vulnerability in TCP/IP Could Allow Denial of Service (MS06-007, 913446))" (https://web.archive.org/web/20070205172614/https://www.microsoft.com/technet/security/Bulletin/MS06-007.mspx). February 14, 2006. Archived from the original (http://www.microsoft.com/technet/security/Bulletin/MS06-007.mspx) on 2007-02-05.
6. *IP Multicast Routing Configuration Guide* (https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3750x_3560x/software/release/15-2_2_e/multicast/configuration_guide/b_mc_1522e_3750x_3560x_cg/b_mc_3750x_3560x_chapter_011.html), Cisco, pp. 25–28, retrieved 2017-05-27
7. "Internet Group Management Protocol Overview" (https://web.archive.org/web/20101110115314/http://www.javvin.com/protocolIGMP.html). Javvin. Archived from the original (http://www.javvin.com/protocolIGMP.html) on 2010-11-10. Retrieved 2010-11-18.
8. *Internet Group Management Protocol, Version 3* (https://tools.ietf.org/html/rfc3376). doi:10.17487/RFC3376 (https://doi.org/10.17487%2FRFC3376). RFC 3376 (https://tools.ietf.org/html/rfc3376).
9. *Internet Group Management Protocol, Version 2* (https://tools.ietf.org/html/rfc2236). doi:10.17487/RFC2236 (https://doi.org/10.17487%2FRFC2236). RFC 2236 (https://tools.ietf.org/html/rfc2236).