IGMP v3

Internet Group Management Protocol, Version 3

References : draft-ietf-idmr-igmp-v3-08.txt

Abstract

This document specifies Version 3 of the Internet Group Management Protocol, IGMPv3. IGMP is the protocol used by IPv4 systems to report their IP multicast group memberships to neighboring multicast routers. Version 3 of IGMP adds support for "source filtering", that is, the ability for a system to report interest in receiving packets *only* from specific source addresses, or from *all but* specific source addresses, sent to a particular multicast address. That information may be used by multicast routing protocols to avoid delivering multicast packets from specific sources to networks where there are no interested receivers.

Table of contents

Introduction

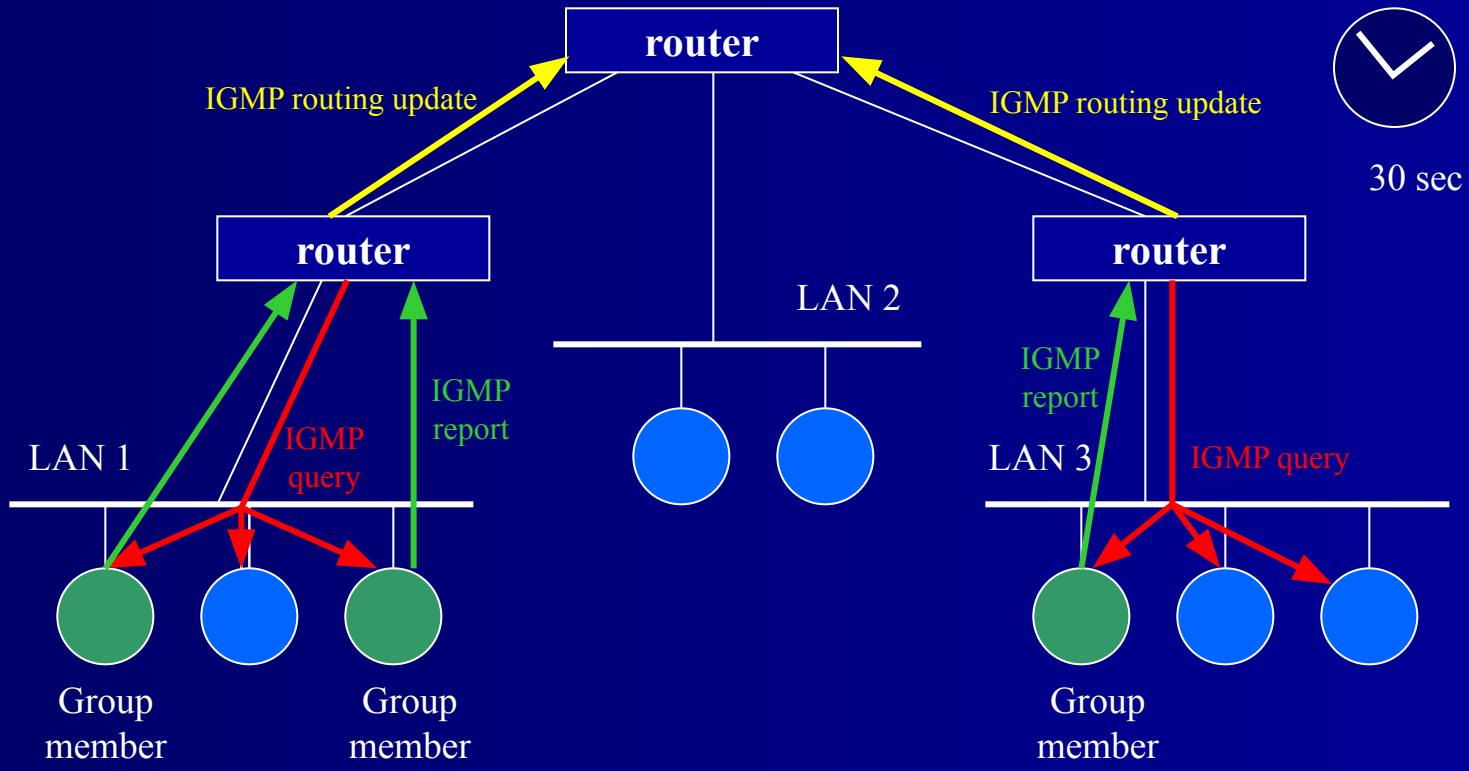
The Internet Group Management Protocol (IGMP) is used by IPv4 systems (hosts and routers) to report their IP multicast group memberships to any neighboring multicast routers. Note that an IP multicast router may itself be a member of one or more multicast groups, in which case it performs both the "multicast router part" of the protocol (to collect the membership information needed by its multicast routing protocol) and the "group member part" of the protocol (to inform itself and other, neighboring multicast routers of its memberships).

IGMP is also used for other IP multicast management functions, using message types other than those used for group membership reporting.

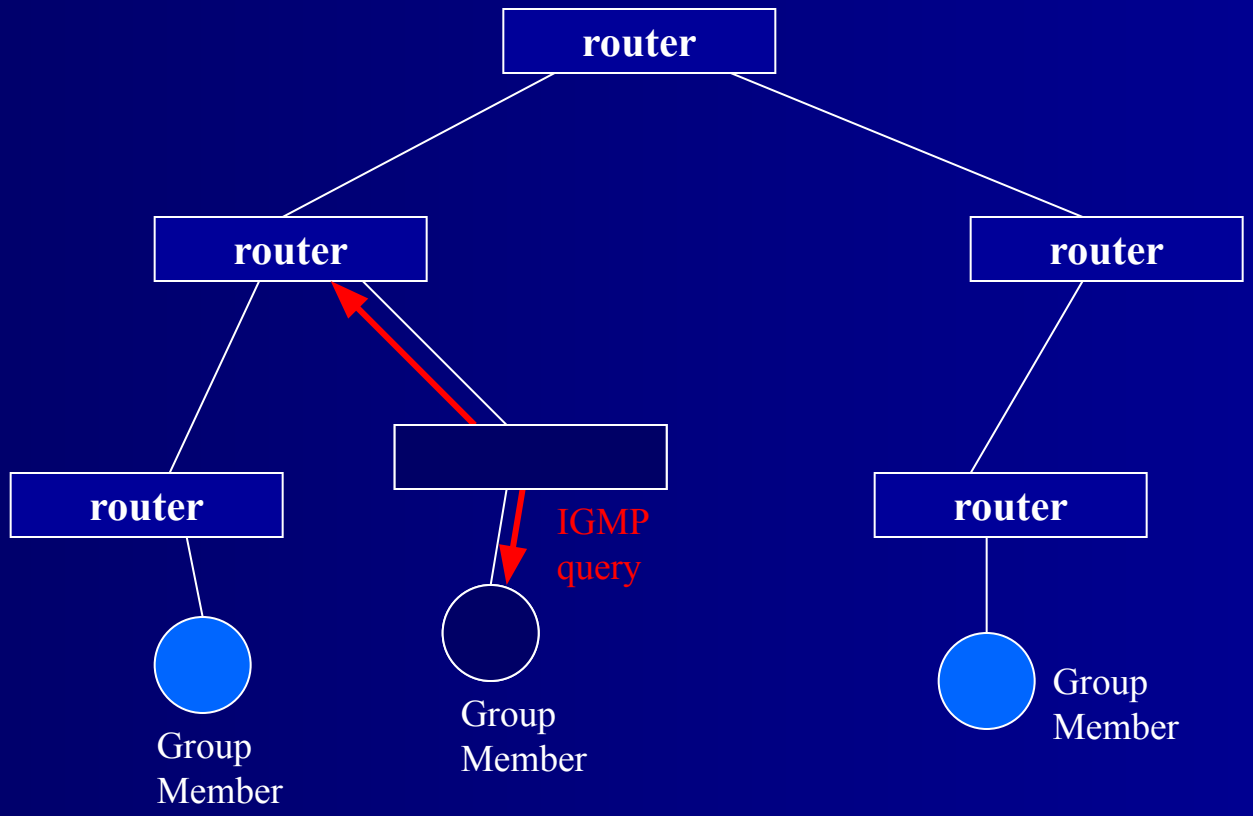
IGMP through versions

- **Version 1**, specified in [RFC-1112], was the first widely-deployed version and the first version to become an Internet Standard.
- **Version 2**, specified in [RFC-2236], added support for "low leave latency", that is, a reduction in the time it takes for a multicast router to learn that there are no longer any members of a particular group present on an attached network.
- **Version 3** adds support for "source filtering", that is, the ability for a system to report interest in receiving packets *only* from specific source addresses, or from *all but* specific source addresses, sent to a particular multicast address.

IGMP v1 - Behaviour



IGMP v1 - Pruning



IGMP v2 - enhancements

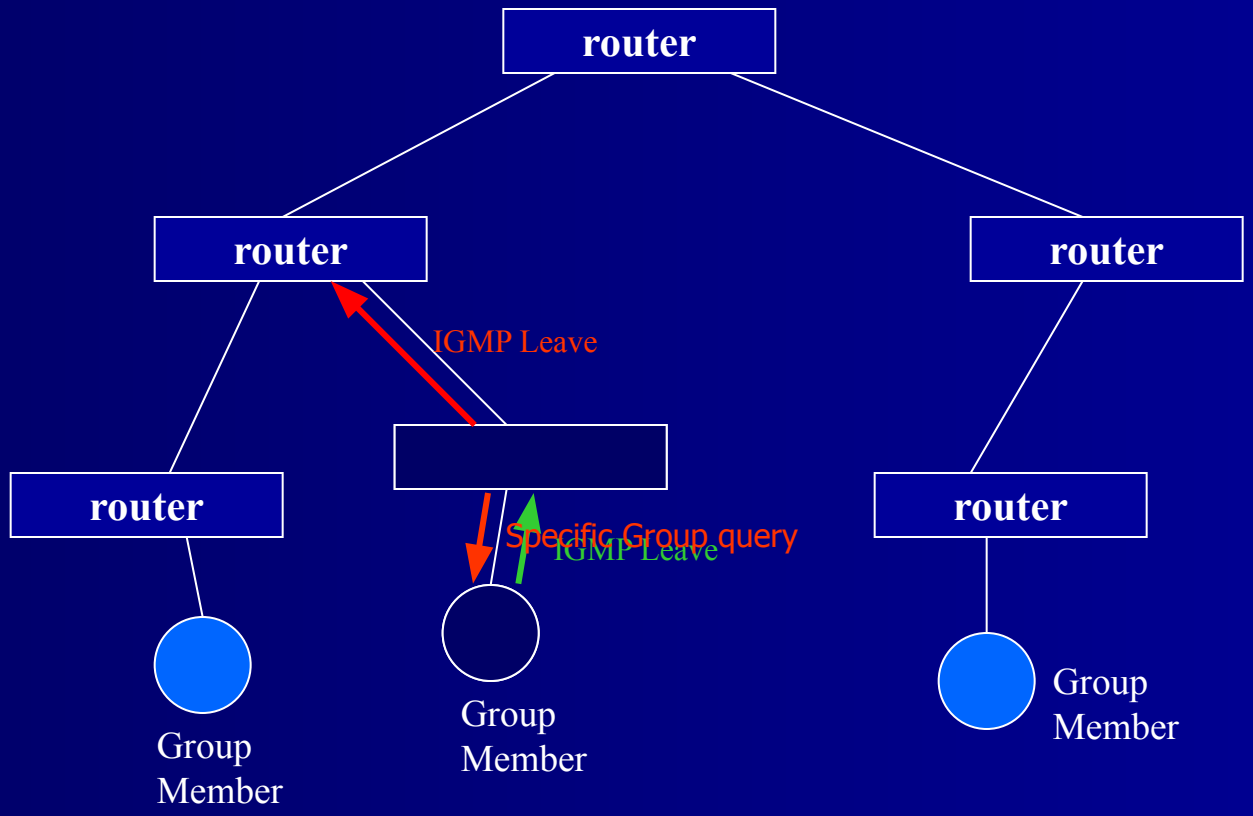
IGMP v2 introduces a procedure for the election of the router querier for each LAN. In the version 1 this was done by different routing policies.

Group-Specific Query – Added to permit queries form a router to a specific group and not to *all-host* address in the subnet (224.0.0.1).

Leave-Group – for a reduction in the time it takes for a multicast router to learn that there are no longer any members of a particular group present on an attached network. Sent to *all-routers* (224.0.0.2)

When a router receives the Leave-Group message, it uses the Group-Specific Query to verify if the sender was the last one in the group.

IGMP v2 - Pruning



IGMP v3 - features

- MUST be interoperable with v1 and v2
- Source-filtering
  - Only from a source
  - All but a source

IGMP v3 - API

Within an IP system, there is (at least conceptually) an Application Programming Interface or API used by upper-layer protocols or application programs to ask the IP layer to enable and disable reception of packets sent to specific IP multicast addresses. In order to take full advantage of the capabilities of IGMPv3, a system's IP API must support the following operation

```
IPMulticastListen (   socket,
                      interface,
                      multicast-address,
                                filter-mode,
                      source-list )
```

IGMP v3 - API parameters

"**socket**" is an implementation-specific parameter used to distinguish among different requesting entities.

"**interface**" is a local identifier of the network interface on which reception of the specified multicast address is to be enabled or disabled. (e.g., an Ethernet interface)

"**multicast-address**" is the IP multicast address to which the request pertains. If reception of more than one multicast address on a given interface is desired, IPMulticastListen is invoked separately for each desired multicast address.

"**filter-mode**" may be either INCLUDE or EXCLUDE.

"**source-list**" is an unordered list of zero or more IP unicast addresses from which multicast reception is desired or not desired, depending on the filter mode.

IGMP v3 - API compatibility

Previous versions of IGMP did not support source filters and had a simpler API consisting of Join and Leave operations to enable and disable reception of a given multicast address (from *all* sources) on a given interface.

The **Join** operation is equivalent to

IPMulticastListen (socket, interface, multicast-address, EXCLUDE, {})

and the **Leave** operation is equivalent to:

IPMulticastListen (socket, interface, multicast-address, INCLUDE, {})

where {} is an empty source list.

IGMP v3 - API example

For example, suppose one application or process invokes the following operation on socket s1:

IPMulticastListen (s1, i, m, INCLUDE, {a, b, c})

requesting reception on interface i of packets sent to multicast address m, *only* if they come from source a, b, or c.
Suppose another application or process invokes the following operation on socket s2:

IPMulticastListen (s2, i, m, INCLUDE, {b, c, d})

Thus, in this example, the reception state of interface i for multicast address m has filter mode INCLUDE and source list {a, b, c, d}.

IGMP v3 - Message format

IGMP messages are encapsulated in IPv4 datagrams, with an IP protocol number of 2. Every IGMP message is sent with an IP Time-to-Live of 1, and carries an IP Router Alert option [RFC-2113] in its IP header.

There are two IGMP message types of concern to the IGMPv3 protocol:

Type Number (hex)	Message Name
0x11	Membership Query
0x22	Version 3 Membership Report

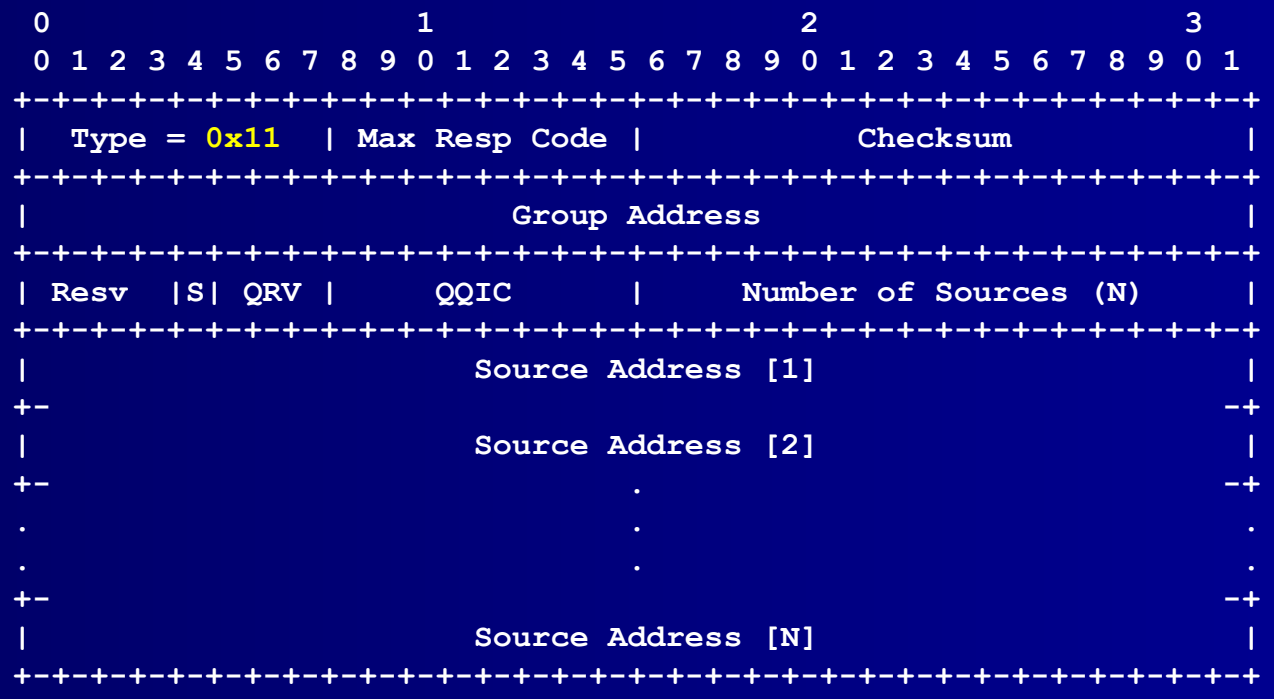
IGMP v3 - Message format

An implementation of IGMPv3 MUST also support the following three message types, for interoperation with previous versions of IGMP

0x12	Version 1 Membership Report	[RFC-1112]
0x16	Version 2 Membership Report	[RFC-2236]
0x17	Version 2 Leave Group	[RFC-2236]

IGMP v3 - Message format

Membership Query Message



IGMP v3 - Message format

Membership Query Message

The Max Resp Code field specifies the maximum time allowed before sending a responding report. Allow IGMPv3 routers to tune the "leave latency".

The Group Address field is set to zero when sending a General Query, and set to the IP multicast address being queried when sending a Group-Specific Query or Group-and-Source-Specific Query

The Querier's Query Interval Code field specifies the [Query Interval] used by the querier.

The Number of Sources (N) field specifies how many source addresses are present in the Query.

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.

IGMP v3 - Message format

Membership Query Message

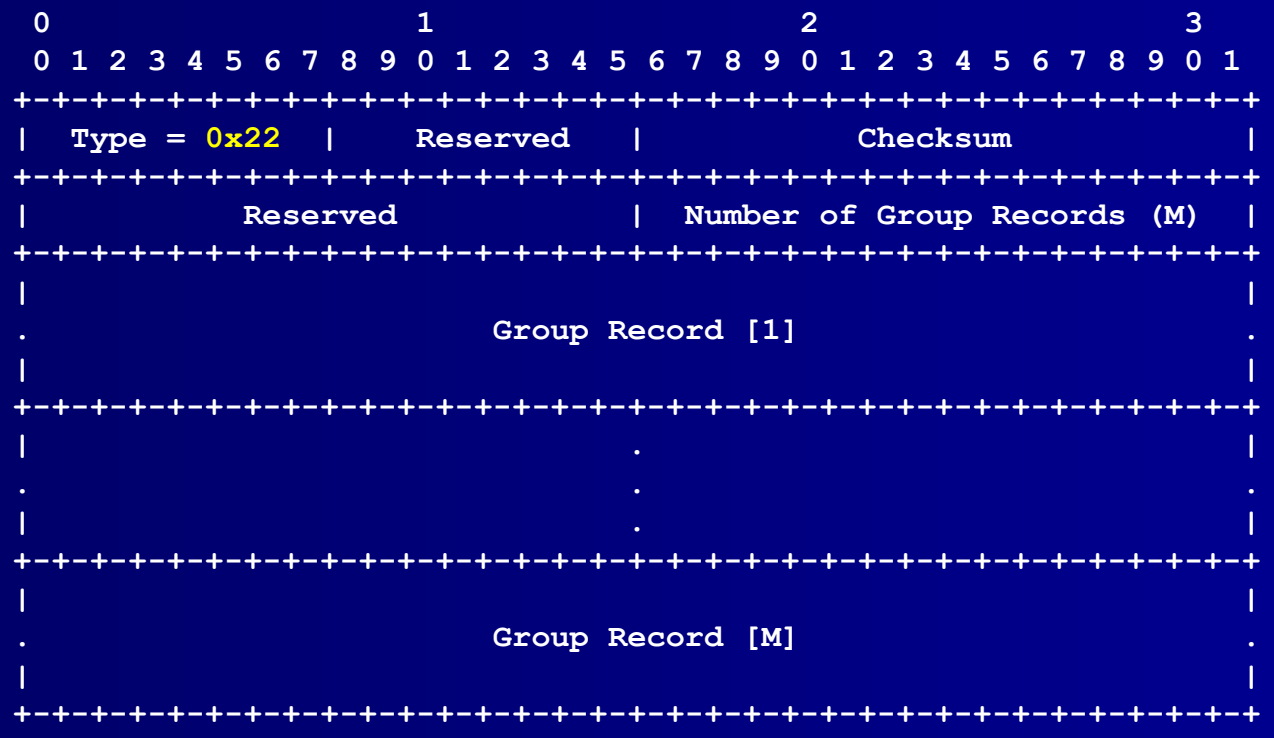
There are three variants of the Query message:

1. A "General Query"
2. A "Group-Specific Query"
3. A "Group-and-Source-Specific Query"

In IGMPv3, General Queries are sent with an IP destination address of 224.0.0.1, the all-systems multicast address. Group-Specific and Group-and-Source-Specific Queries are sent with an IP destination address equal to the multicast address of interest.

IGMP v3 - Message format

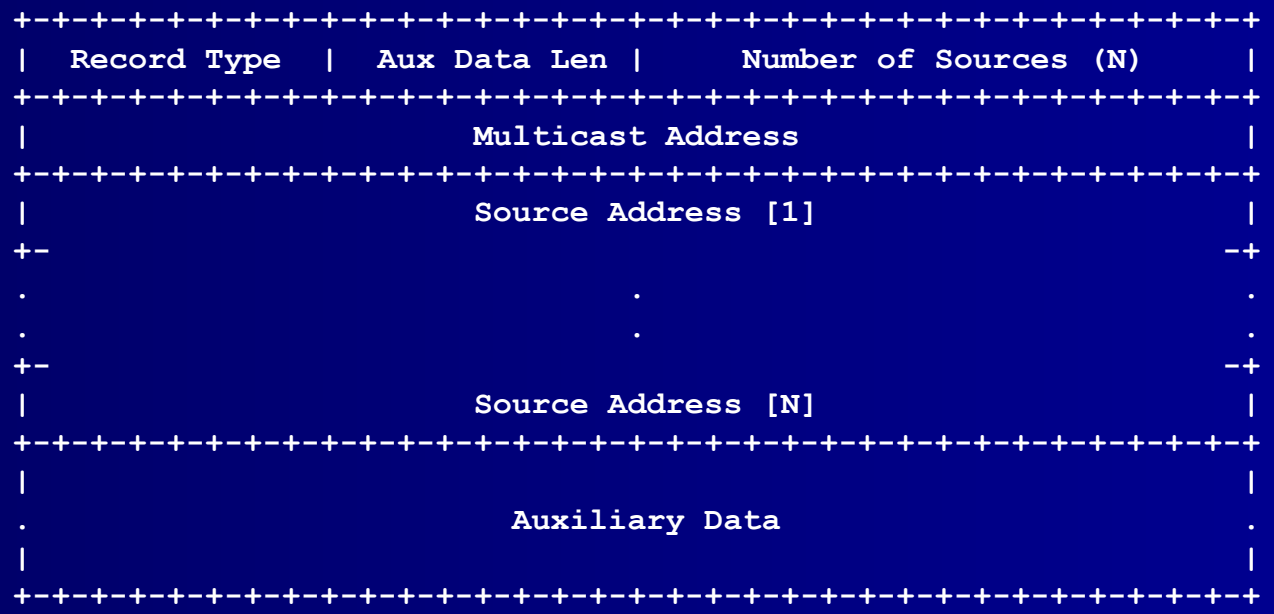
Membership Report Message



IGMP v3 - Message format

Membership Report Message

Each Group Record has the following internal format:



IGMP v3 - Message format

Membership Report Message

There are a number of different types of Group Records that may be included in a Report message:

- **A "Current-State Record"** (in response to a Query)
  1. MODE_IS_INCLUDE INCLUDE()
  2. MODE_IS_EXCLUDE EXCLUDE()

- **A "Filter-Mode-Change Record"** (when the filter mode change)
  3. CHANGE_TO_INCLUDE_MODE TO_IN()
  4. CHANGE_TO_EXCLUDE_MODE TO_EX()

- **A "Source-List-Change Record"** (when the source list change)
  5. ALLOW_NEW_SOURCES ALLOW()
  6. BLOCK_OLD_SOURCES BLOCK()

IGMP v3 - Message format

Membership Report Message

Version 3 Reports are sent with an IP destination address of 224.0.0.22, to which all IGMPv3-capable multicast routers listen. A system that is operating in version 1 or version 2 compatibility modes sends version 1 or version 2 Reports to the multicast group specified in the Group Address field of the Report.

IGMP v3 - The protocol

(for group members)

The all-systems multicast address, 224.0.0.1, is handled as a special case. On all systems -- that is all hosts and routers, including multicast routers -- reception of packets destined to the all-systems multicast address, from all sources, is permanently enabled on all interfaces on which multicast reception is supported. No IGMP messages are ever sent regarding the all-systems multicast address.

There are two types of events that trigger IGMPv3 protocol actions on an interface:

- A change of the interface reception state, caused by a local invocation of *IPMulticastListen*.
- Reception of a *Query*.

IGMP v3 - The protocol

(for group members)

Action on Change of Interface State

A change of interface state causes the system to immediately transmit a State-Change Report from that interface. The type and contents of the Group Record(s) in that Report are determined by comparing the filter mode and source list for the affected multicast address before and after the change, according to the table below.

Old State	New State	State-Change Record Sent
INCLUDE (A)	INCLUDE (B)	ALLOW (B-A), BLOCK (A-B)
EXCLUDE (A)	EXCLUDE (B)	ALLOW (A-B), BLOCK (B-A)
INCLUDE (A)	EXCLUDE (B)	TO_EX (B)
EXCLUDE (A)	INCLUDE (B)	TO_IN (B)

IGMP v3 - The protocol

(for group members)

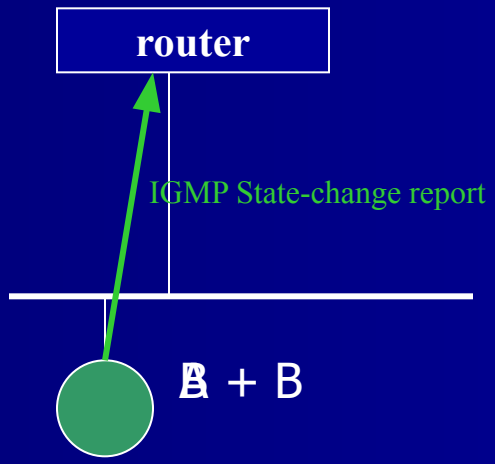
Action on Change of Interface State

To cover the possibility of the State-Change Report being missed by one or more multicast routers, it is retransmitted [Robustness Variable] – 1 more times, at intervals chosen at random from the range (0, [Unsolicited Report Interval]).

IPMulticastListen (s1, i, m, INCLUDE, {A})

IPMulticastListen (s2, i, m, INCLUDE, {B})

IPMulticastListen (s1, i, m, INCLUDE, {})



IGMP v3 - The protocol
(for group members)

Interface Filter State -- EXCLUDE

if ***any*** such record has a filter mode of EXCLUDE, then the filter mode of the interface record is EXCLUDE, and the source list of the interface record is the intersection of the source lists of all socket records in EXCLUDE mode, minus those source addresses that appear in any socket record in INCLUDE mode.

from socket s1: (i, m, EXCLUDE, {a, b, c, d})
from socket s2: (i, m, EXCLUDE, {b, c, d, e})
from socket s3: (i, m, INCLUDE, {d, e, f})

then the corresponding interface record on interface i is:

(m, EXCLUDE, {b, c})

IGMP v3 - The protocol

(for group members)

Interface Filter State -- INCLUDE

if ***all*** such records have a filter mode of INCLUDE, then the filter mode of the interface record is INCLUDE, and the source list of the interface record is the union of the source lists of all the socket records. For example, if the socket records for multicast address m on interface i are:

from socket s1: (i, m, INCLUDE, {a, b, c})
from socket s2: (i, m, INCLUDE, {b, c, d})
from socket s3: (i, m, INCLUDE, {e, f})

then the corresponding interface record on interface i is:

(m, INCLUDE, {a, b, c, d, e, f})

IGMP v3 - The protocol

(for group members)

Action on Reception of a Query

When a system receives a Query, it does not respond immediately. Instead, it delays its response by a random amount of time, bounded by the Max Resp Time value derived from the Max Resp Code in the received Query message. A system may receive a variety of Queries on different interfaces and of different kinds (e.g., General Queries, Group-Specific Queries, and Group-and- Source-Specific Queries), each of which may require its own delayed response.

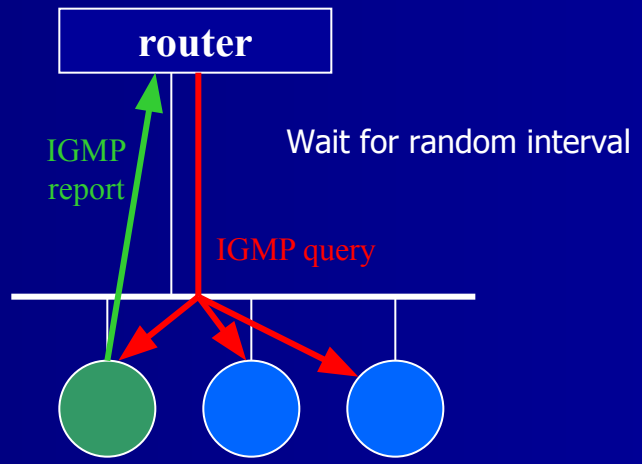
Before scheduling a response to a Query, the system must first consider previously scheduled pending responses and in many cases schedule a combined response.

IGMP v3 - The protocol
(for group members)

Action on Reception of a Query

Therefore, the system must be able to maintain the following state:

- A timer per interface for scheduling responses to General Queries.
- A per-group and interface timer for scheduling responses to Group-Specific and Group-and-Source-Specific Queries.
- A per-group and interface list of sources to be reported in the response to a Group-and-Source-Specific Query.



IGMP v3 - The protocol

(for multicast routers)

The purpose of IGMP is to enable each multicast router to learn, for each of its directly attached networks, which multicast addresses are of interest to the systems attached to those networks. IGMP version 3 adds the capability for a multicast router to also learn which *sources* are of interest to neighboring systems, for packets sent to any particular multicast address. The information gathered by IGMP is provided to whichever multicast routing protocol is being used by the router, in order to ensure that multicast packets are delivered to all networks where there are interested receivers.

NOTE: Multicast routers may also themselves become members of multicast groups, and therefore also perform the group member part of IGMPv3

IGMP v3 - The protocol

(for multicast routers)

If a multicast router has more than one interface to the same network, it only needs to operate this protocol over one of those interfaces. On each interface over which this protocol is being run, the router MUST enable reception of multicast address 224.0.0.22, from all sources.

Multicast routers need to know only that *at least one* system on an attached network is interested in packets to a particular multicast address from a particular source; a multicast router is not required to keep track of the interests of each individual neighboring system.

IGMPv3 is backward compatible with previous versions of the IGMP protocol. In order to remain backward compatible with older IGMP systems, IGMPv3 multicast routers MUST also implement versions 1 and 2 of the protocol.

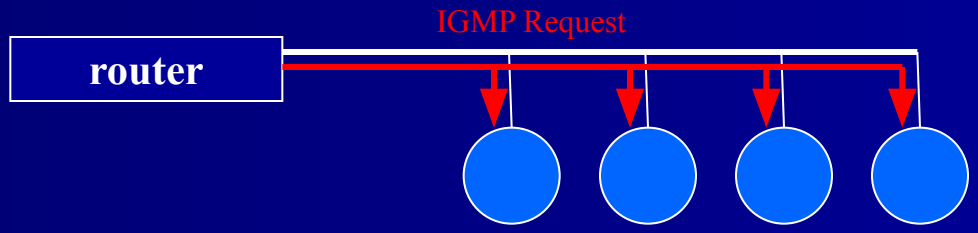
IGMP v3 - The protocol

(for multicast routers)

Conditions for IGMP Queries

- **Periodic request for membership**

Multicast routers send General Queries periodically to request group membership information from an attached network.
These queries are used to build and refresh the group membership state of systems on attached networks. Systems respond to these queries by reporting their group membership state (and their desired set of sources) with Current-State Group Records in IGMPv3 Membership Reports.

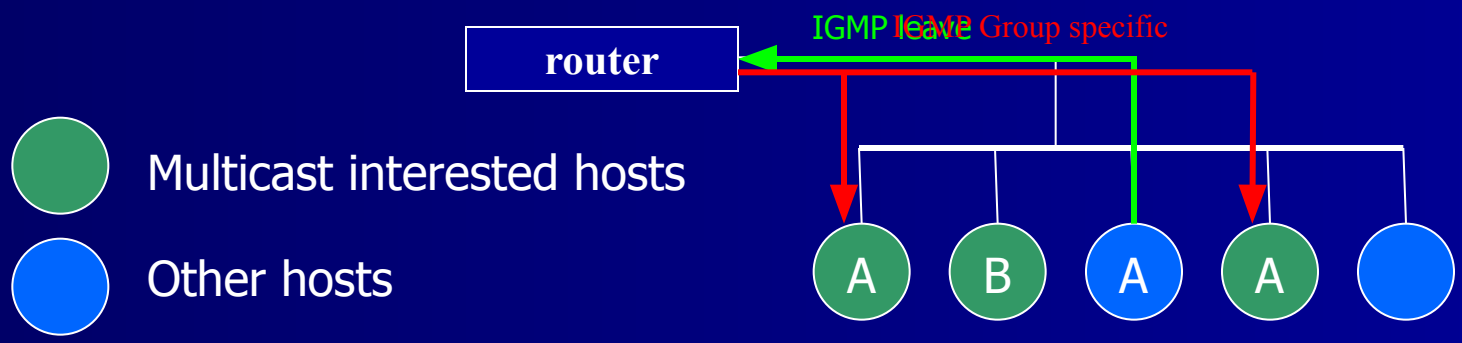


IGMP v3 - The protocol

(for multicast routers)

- **Group Specific Query**

To enable all systems on a network to respond to changes in group membership, multicast routers send specific queries. A Group- Specific Query is sent to verify there are no systems that desire reception of the specified group or to "rebuild" the desired reception state for a particular group. Group-Specific Queries are sent when a router receives a State-Change record indicating a system is leaving a group.



IGMP v3 - The protocol

(for multicast routers)

- **Group and Source Specific Query**

A Group-and-Source Specific Query is used to verify there are no systems on a network which desire to receive traffic from a set of sources. Group-and-Source Specific Queries list sources for a particular group which have been requested to no longer be forwarded. This query is sent by a multicast router to learn if any systems desire reception of packets to the specified group address from the specified source addresses.

IGMP v3 - The protocol
(for multicast routers)

IGMP State Maintained by Multicast Routers

Multicast routers implementing IGMPv3 keep state per group per attached network. This group state consists of:

- a filter-mode,
- a list of sources,
- and various timers.

For each attached network running IGMP, a multicast router records the desired reception state for that network.
That state conceptually consists of a set of records of the form:

(multicast address, group timer, filter-mode, (source records))

IGMP v3 - The protocol

(for multicast routers)

Definition of Router Filter-Mode

To reduce internal state, IGMPv3 routers keep a filter-mode per group per attached network. This filter-mode is used to condense the total desired reception state of a group to a minimum set such that all systems' memberships are satisfied. This filter-mode may change in response to the reception of particular types of group records or when certain timer conditions occur.

Conceptually, when a group record is received, the router filter-mode for that group is updated to cover all the requested sources using the least amount of state. As a rule, once a group record with a filter-mode of EXCLUDE is received, the router filter-mode for that group will be EXCLUDE.

IGMP v3 - The protocol

(for multicast routers)

Action on Reception of Reports

Reception of Current-State Records

When receiving Current-State Records, a router updates both its group and source timers. In some circumstances, the reception of a type of group record will cause the router filter-mode for that group to change.

Reception of Filter-Mode and Source-List Change Records

When a change in the global state of a group occurs in a system, the system sends either a Source-List-Change Record or a Filter-Mode-Change Record for that group. As with Current-State Records, routers must act upon these records and possibly change their own state to reflect the new desired membership state of the network.

IGMP v3 - The protocol
(for multicast routers)

Action on Reception of Queries

- **Timer Updates**

- **Querier Election**

  IGMPv3 elects a single querier per subnet using the same querier election mechanism as IGMPv2, namely by IP address.

If a router receives an older version query, it MUST use the oldest version of IGMP on the network.

IGMP v3 - Interoperation with older version

IGMP version 3 hosts and routers interoperate with hosts and routers that have not yet been upgraded to IGMPv3. This compatibility is maintained by hosts and routers taking appropriate actions depending on the versions of IGMP operating on hosts and routers within a network.

The IGMP version of a Membership Query message is determined as follows:

IGMPv1 Query: length = 8 octets AND Max Resp Code field is zero

IGMPv2 Query: length = 8 octets AND Max Resp Code field is non-zero

IGMPv3 Query: length >= 12 octets

IGMP v3 - Interoperation with older version

Group Member Behavior

In the Presence of Older Version Queriers

In order to be compatible with older version routers, IGMPv3 hosts MUST operate in version 1 and version 2 compatibility modes. IGMPv3 hosts MUST keep state per local interface regarding the compatibility mode of each attached network. A host's compatibility mode is determined from the Host Compatibility Mode variable which can be in one of three states: IGMPv1, IGMPv2 or IGMPv3. This variable is kept per interface and is dependent on the version of General Queries heard on that interface as well as the *Older Version Querier Present timers* for the interface.

IGMP v3 - Interoperation with older version

Multicast Router Behavior

In the Presence of Older Version Queriers

IGMPv3 routers may be placed on a network where at least one router on the network has not yet been upgraded to IGMPv3.

If any older versions of IGMP are present on routers, the querier MUST use the lowest version of IGMP present on the network.
When in IGMPv1 mode, routers MUST send Periodic Queries with a Max Resp Code of 0 and truncated at the Group Address field (i.e. 8 bytes long), and MUST ignore Leave Group messages.
When in IGMPv2 mode, routers MUST send Periodic Queries truncated at the Group Address field (i.e. 8 bytes long)

IGMP v3 - Interoperation with older version

Multicast Router Behavior

In the Presence of Older Version Group Members

IGMPv3 routers may be placed on a network where there are hosts that have not yet been upgraded to IGMPv3. In order to be compatible with older version hosts, IGMPv3 routers MUST operate in version 1 and version 2 compatibility modes.

In order to switch gracefully between versions of IGMP, routers keep an IGMPv1 *Host Present timer* and an IGMPv2 Host Present timer per group record.

IGMP v3 - Interoperation with older version

Multicast Router Behavior

When Group Compatibility Mode is IGMPv3, a router acts using the IGMPv3 protocol for that group.

When Group Compatibility Mode is IGMPv2, a router acts in IGMPv2 compatibility mode, treating all IGMPv3 messages mentioning a group as membership in that group, except IS_INC({}) and TO_INC({}), which are treated as IGMPv2 Leave messages. ALLOW() and BLOCK() messages are ignored.

When Group Compatibility Mode is IGMPv1, a router acts in IGMPv1 compatibility mode, treating IGMPv3 messages as above but adittionally ignoring IGMPv2 Leave messages.

IGMP v3 - Timers

Most of these timers are configurable. If non-default settings are used, they MUST be consistent among all systems.

Robustness Variable

The Robustness Variable allows tuning for the expected packet loss on a network. If a network is expected to be lossy, the Robustness Variable may be increased. IGMP is robust to (Robustness Variable - 1) packet losses. The Robustness Variable MUST NOT be zero, and SHOULD NOT be one. Default: 2

Query Interval

The Query Interval is the interval between General Queries sent by the Querier. Default: 125 seconds.

IGMP v3 - Timers

Query Response Interval

The Max Response Time used to calculate the Max Resp Code inserted into the periodic General Queries. Default: 100 (10 seconds)

The number of seconds represented by the [Query Response Interval] must be less than the [Query Interval].

Group Membership Interval

The Group Membership Interval is the amount of time that must pass before a multicast router decides there are no more members of a group or a particular source on a network. This value MUST be ((the Robustness Variable) * (the Query Interval)) + (one Query Response Interval).

IGMP v3 - Timers

Other Querier Present Interval

The Other Querier Present Interval is the length of time that must pass before a multicast router decides that there is no longer another multicast router which should be the querier.

Last Member Query Interval

The Last Member Query Interval is the Max Response Time used to calculate the Max Resp Code inserted into Group-Specific Queries sent in response to Leave Group messages. It is also the Max Response Time used in calculating the Max Resp Code for Group-and-Source-Specific Query messages. Default: 10 (1 second)
This value may be tuned to modify the *"leave latency"* of the network.

IGMP v3 - Timers

Older Version Querier Present Timeout

The Older Version Querier Interval is the time-out for transitioning a host back to IGMPv3 mode once an older version query is heard. When an older version query is received, hosts set their Older Version Querier Present Timer to Older Version Querier Interval.
This value MUST be ((the Robustness Variable) * (the Query Interval in the last Query received)) + (one Query Response Interval).

Older Host Present Interval

The Older Host Present Interval is the time-out for transitioning a group back to IGMPv3 mode once an older version report is sent for that group. When an older version report is received, routers set their Older Host Present Timer to Older Host Present Interval.

IGMP v3 - Configuring Timers

This section is meant to provide advice to network administrators on how to tune these settings to their network.
Ambitious router implementations might tune these settings dynamically based upon changing characteristics of the network.

Robustness Variable

The Robustness Variable tunes IGMP to expected losses on a link. IGMPv3 is robust to (Robustness Variable - 1) packet losses, e.g. if the Robustness Variable is set to the default value of 2, IGMPv3 is robust to a single packet loss but may operate imperfectly if more losses occur. On lossy subnetworks, the Robustness Variable should be increased to allow for the expected level of packet loss. However, increasing the Robustness Variable increases the leave latency of the subnetwork.

IGMP v3 - Configuring Timers

Query Interval

The overall level of periodic IGMP traffic is inversely proportional to the Query Interval. A longer Query Interval results in a lower overall level of IGMP traffic. The Query Interval MUST be equal to or longer than the Max Response Time inserted in General Query messages.

Max Response Time

The burstiness of IGMP traffic is inversely proportional to the Max Response Time. A longer Max Response Time will spread Report messages over a longer interval. However, a longer Max Response Time in Group-Specific and Source-and-Group-Specific Queries extends the leave latency

IGMP v3 - Security

IPSEC in Authentication Header mode [AH] may be used to protect against remote attacks by ensuring that IGMPv3 messages came from a system on the LAN (or, more specifically, a system with the proper key). When using IPSEC, the messages sent to 224.0.0.1 and 224.0.0.22 should be authenticated using AH.

- Symmetric key for the entire LAN
- Asymmetric key for hosts and routers

This solution only directly applies to Query and Leave messages in IGMPv1 and IGMPv2, since Reports are sent to the group being reported and it is not feasible to agree on a key for host-to-router communication for arbitrary multicast groups.

IGMP v3 - Security

Query Message

A forged Query message from a machine with a lower IP address than the current Querier will cause Querier duties to be assigned to the forger. If the forger then sends no more Query messages, other routers' Other Querier Present timer will time out and one will resume the role of Querier. A DoS attack on a host could be staged through forged Group-and-Source-Specific Queries.

- Routers SHOULD NOT forward Queries. This is easier for a router to accomplish if the Query carries the Router-Alert option.
- Hosts SHOULD Ignore v3 Queries without the Router-Alert option.

IGMP v3 - Security

Current-State Report messages

A forged Version 1 Report Message may put a router into "version 1 members present" state for a particular group, meaning that the router will ignore Leave messages. This can cause traffic to flow to groups with no members for up to [Group Membership Interval].

A forged Version 2 Report Message may put a router into "version 2 members present" state for a particular group, meaning that the router will ignore IGMPv3 source-specific state messages. This can cause traffic to flow from unwanted sources for up to [Group Membership Interval].

SOLUTION: ignore this Reports but only if compatibility mode don't care.

IGMP v3 - Security

State-Change Report messages

A forged State-Change Report message will cause the Querier to send out Group-Specific or Source-and-Group-Specific Queries for the group in question. This causes extra processing on each router and on each member of the group, but can not cause loss of desired traffic. There are two defenses against externally forged State-Change Report messages:

- Ignore the State-Change Report message if you cannot identify the source address of the packet
- Ignore State-Change Report messages without Router Alert options [RFC-2113], and require that routers not forward State-Change Report messages.

IGMP v3 - References

[RFC-1112] "Host Extensions for IP Multicasting"

[RFC-2113] "IP Router Alert Option"

[RFC-2119] "Key words for use in RFCs to Indicate Requirement Levels"

[RFC-2236] "Internet Group Management Protocol, Version 2

[RFC-2402] "IP Authentication Header"

"Internet Group Management Protocol, Version 3", Work in progress, draft-ietf-idmr-igmp-v3-08.txt, November 2001