Network Working Group
Request for Comments: 3376
Obsoletes: 2236
Category: Standards Track

B. Cain
Cereva Networks
S. Deering
I. Kouvelas
Cisco Systems
B. Fenner
AT&T Labs - Research
A. Thyagarajan
Ericsson

October 2002

Протокол управления группами Internet (IGMP), версия 3

Internet Group Management Protocol, Version 3

Статус документа

Этот документ задаёт проект стандартного протокола Internet для сообщества Internet и служит приглашением к дискуссии в целях развития и совершенствования. Текущее состояние стандартизации и статус протокола можно узнать из документа Internet Official Protocol Standards (STD 1). Документ может распространяться без ограничений.

Аннотация

В этом документе описана версия 3 протокола управления группами Internet - IGMPv3[1]. Протокол IGMP используется системами IPv4 для информирования соседних групповых маршрутизаторов о своих группах IP. В третьей версии IGMP добавлена поддержка фильтрации по источнику (source filtering), позволяющая системе сообщить о своей заинтересованности в получении группового трафика, направленного по данному групповому адресу, **только** от указанных отправителей или от всех, **кроме** указанных. Эта информация может применяться протоколами групповой маршрутизации для предотвращения доставки групповых пакетов от указанных отправителей в сети, где нет заинтересованных получателей.

Данных документ отменяет действие RFC 2236.

Оглавление

1. Введение....2
2. Сервисный интерфейс для запроса получения IP Multicast....3
3. Состояние восприятия группового трафика в системе....3
3.1. Состояние сокета....3
3.2. Состояние интерфейса....4
4. Форматы сообщений....5
4.1. Запрос о принадлежности к группе....5
4.1.1. Max Resp Code....5
4.1.2. Checksum....5
4.1.3. Group Address....5
4.1.4. Resv (резерв)....5
4.1.5. Флаг S (подавление обработки Router-Side)....6
4.1.6. QRV....6
4.1.7. QQIC....6
4.1.8. Number of Sources (N)....6
4.1.9. Source Address [i]....6
4.1.10. Дополнительные данные....6
4.1.11. Варианты запросов....6
4.1.12. Адреса получателей для запросов....6
4.2. Сообщение Version 3 Membership Report....7
4.2.1. Reserved....7
4.2.2. Checksum....7
4.2.3. Number of Group Records (M)....7
4.2.4. Group Record....7
4.2.5. Record Type....7
4.2.6. Aux Data Len....7
4.2.7. Number of Sources (N)....8
4.2.8. Multicast Address....8
4.2.9. Source Address [i]....8

[1]Internet Group Management Protocol.

4.2.10. Auxiliary Data....8
4.2.11. Дополнительные данные....8
4.2.12. Типы записей Group Record....8
4.2.13. IP-адреса источников для сообщений Report....9
4.2.14. IP-адреса получателей для сообщений Report....9
4.2.15. Нотация для записей Group Record....9
4.2.16. Размер Membership Report....9
5. Описание протокола для членов группы....9
5.1. Действия при смене состояния интерфейса....10
5.2. Действия при получении запроса....10
6. Описание протокола для групповых маршрутизаторов....11
6.1. Условия для запросов IGMP....12
6.2. Состояние IGMP, поддерживаемое групповыми маршрутизаторами....12
6.2.1. Определение Router Filter-Mode....12
6.2.2. Определение групповых таймеров....13
6.2.3. Определение таймеров источника....13
6.3. Правила пересылки IGMPv3....13
6.4. Действия при получении сообщений....13
6.4.1. Получение записей Current-State....13
6.4.2. Получение записей Filter-Mode-Change и Source-List-Change....14
6.5. Переключение режима фильтрации....15
6.6. Действия при получении запросов....15
6.6.1. Обновление таймеров....15
6.6.2. Выбор запрашивающего....15
6.6.3. Создание и отправка запросов....15
6.6.3.1. Создание и отправка запросов для группы....15
6.6.3.2. Создание и отправка запросов для группы и источника....15
7. Взаимодействие с ранними версиями IGMP....16
7.1. Различия версий запросов....16
7.2. Поведение членов группы....16
7.2.1. При наличии запросов прежних версий....16
7.2.2. При наличии членов групп со старой версией....16
7.3. Поведение группового маршрутизатора....16
7.3.1. Присутствие запрашивающих со старой версией....16
7.3.2. Присутствие членов групп со старой версией....17
8. Список таймеров и счётчиков, значения по умолчанию....17
8.1. Переменная Robustness....17
8.2. Интервал между запросами....18
8.3. Интервал между откликами....18
8.4. Интервал принадлежности к группе....18
8.5. Интервал присутствия других запрашивающих....18
8.6. Интервал стартового запроса....18
8.7. Счётчик стартовых запросов....18
8.8. Интервал запроса последнего участника....18
8.9. Счётчик запросов последнего участника....18
8.10. Время запроса последнего участника....18
8.11. Интервал незапрошенных отчётов....18
8.12. Тайм-аут присутствия запрашивающего старой версии....18
8.13. Интервал присутствия старых хостов....19
8.14. Настройка таймеров....19
8.14.1. Переменная Robustness....19
8.14.2. Интервал между запросами....19
8.14.3. Максимальное время отклика....19
9. Вопросы безопасности....19
9.1. Обманные сообщения Query....19
9.2. Обманные сообщения Current-State Report....20
9.3. Обманные сообщения State-Change Report....20
9.4. Использование IPSEC....20
10. Взаимодействие с IANA....20
11. Благодарности....20
12. Нормативные документы....21
13. Дополнительная литература....21
Приложение A. Обоснования....21
A.1 Необходимость сообщений State-Change....21
A.2 Отмена отправки отчётов. хостами....21
A.3 Переключение режима фильтрации с EXCLUDE на INCLUDE....21
Приложение B. Изменения по сравнению с IGMPv2....22

1. Введение

Протокол IGMP используется системами IPv4 (хостами и маршрутизаторами) для передачи соседним групповым маршрутизаторам сведений о принадлежности к их группам IP. Отметим, что групповые маршрутизаторы IP сами по себе могут быть членами multicast-групп и в этом случае выступают в протоколе, как участники маршрутизации (multicast router part) для сбора сведений о принадлежности к группам, используемых протоколом групповой маршрутизации, и члены групп (group member part) для информирования самого себя и других соседних маршрутизаторов о принадлежности к группам.

IGMP используется также для других функций управления групповой адресацией IP с применением сообщений, типы которых отличаются от сообщений о принадлежности к группам. В этом документе рассматриваются лишь функции и сообщения, связанные с принадлежностью к группам.

Этот документ задаёт версию 3 протокола IGMP. Версия 1, описанная в [RFC-1112], была первой широко распространённой версией, получившей статус стандарта Internet. В версии 2, заданной [RFC-2236], была добавлена поддержка low leave latency, т. е. снижения времени, в течение которого групповой маршрутизатор может принимать решение об отсутствии членов конкретной группы в подключённой сети. В версии 3 добавлена поддержка фильтрации источников, позволяющая системе указать свою заинтересованность в получении группового трафика **только** от указанных отправителей, как требуется для поддержки [SSM[1]], или от всех отправителей **кроме** указанных, передаваемого по указанному групповому адресу. Версия 3 предполагает совместимость с версиями 1 и 2.

Механизм MLD[2] аналогичным способом используется системами IPv6. MLD версии 1 [MLD] реализует функциональность IGMP версии 2, а MLD версии 2 [MLDv2] - функциональность IGMP версии 3.

Ключевые слова **необходимо** (MUST), **недопустимо** (MUST NOT), **требуется** (REQUIRED), **нужно** (SHALL), **не нужно** (SHALL NOT), **следует** (SHOULD), **не следует** (SHOULD NOT), **рекомендуется** (RECOMMENDED), **возможно** (MAY), **необязательно** (OPTIONAL) в данном документе должны интерпретироваться в соответствии с [RFC-2119]. В переводе эти слова выделяются **полужирным** шрифтом.

2. Сервисный интерфейс для запроса получения IP Multicast

В IP-системах имеется (по крайней мере, концептуально) служебный интерфейс, используемый протоколами вышележащих уровней для запросу на уровне IP разрешения или запрета приёма пакетов, направленных на указанный групповой адрес IP. Для полного использования возможностей IGMPv3 этот интерфейс должен поддерживать операцию:

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

где:

- **socket** – зависящий от приложения параметр, используемый для идентификации запрашиваемых в системе объектов (например, программ или процессов), примером могут служить системные вызовы BSD Unix.
- **interface** - локальный идентификатор сетевого интерфейса, для которого разрешается или запрещается восприятие указанного группового адреса. Интерфейс может быть физическим (например, Ethernet) или виртуальным (например, оконечная точка виртуального соединения Frame Relay или «туннеля» IP-in-IP). Реализация может разрешать специальное значение unspecified (не задано) в качестве параметра interface - в этом случае запрос будет применяться к основному (primary) или используемому по умолчанию (default) интерфейсу системы (возможно, организованному в системной конфигурации). Если восприятие группового адреса желательно для нескольких интерфейсов, IPMulticastListen вызывается для каждого из них.
- **multicast-address** - групповой адрес IP или группа, к которой относится запрос. Если на данном интерфейсе желательно принимать более одного адреса, IPMulticastListen вызывается для каждого из таких адресов.
- **filter-mode** - режим фильтрации. Параметр может принимать значение INCLUDE (включить) или EXCLUDE (исключить). В режиме INCLUDE получение пакетов на заданный групповой адрес запрашивается **только** с адресов IP, указанных параметром source-list. В режиме EXCLUDE получение пакетов на данный групповой адрес желательно от всех отправителей, **кроме** указанных параметром source-list.
- **source-list** - неупорядоченный (возможно, пустой) список индивидуальных адресов IP с которых желательно или не желательно (в соответствии с фильтром) принимать групповой трафик**.** Реализация **может** вносить ограничения на размер списка, но **недопустимо** ограничивать его значением меньше 64. При достижении предельного размера списка адресов служебный интерфейс **должен** возвращать сообщение об ошибке.

Для данной комбинации сокета, интерфейса и группового адреса в каждый момент времени может действовать только один режим фильтрации и список источников. Однако фильтр и список источников можно сменить последующими запросами IPMulticastListen для того же сокета, интерфейса и группового адреса. Каждый последующий запрос полностью отменяет предыдущие установки для указанного сокета, интерфейса и группового адреса.

В предыдущей версии IGMP фильтрация источников не поддерживалась и был простой сервисный интерфейс с операциями Join и Leave для разрешения и запрета приёма по указанному групповому адресу (из **всех** источников) для данного интерфейса. Эквивалентные операции в новом сервисном интерфейсе приведены ниже.

Операции Join эквивалентен запрос

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

Операции Leave эквивалентен запрос

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

где {} указывает пустой список источников.

Пример API, поддерживающего описанный выше служебный интерфейс, приведён в [FILTER-API].

3. Состояние восприятия группового трафика в системе

3.1. Состояние сокета

Для каждого сокета, который был указан в вызовах IPMulticastListen системе желательно сохранять запись о состоянии. Концептуально такая запись о состоянии сокета может иметь вид:

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

Состояние сокета меняется при каждом вызове IPMulticastListen для сокета, как показано ниже:

[1]Source-Specific Multicast.
[2]Multicast Listener Discovery - обнаружение прослушивающих групповой трафик устройств.

- если запрошен режим фильтрации INCLUDE **и** список источников пуст, при наличии элемента для запрошенного интерфейса и группового адреса этот элемент удаляется; при отсутствии такого элемента запрос игнорируется;

- если запрошен режим фильтрации EXCLUDE **или** запрошенный список источников не пуст, при наличии элемента для запрошенного интерфейса и группового адреса он изменяется в соответствии с запрошенным режимом фильтрации и списком источников; если такого элемента нет, он создаётся с использовании заданных в запросе параметров.

3.2. Состояние интерфейса

В дополнение к состояниям приёма группового трафика на уровне сокетов система также должна поддерживать или рассчитывать такое состояние для каждого из своих интерфейсов. Концептуально состояние представляет собой набор записей вида:

```
(multicast-address, filter-mode, source-list)
```

Для данного интерфейса существует не более одной записи на multicast-адрес. Состояние на уровне интерфейса выводится из состояний на уровне сокета, но может отличаться от него, когда разные сокеты используют разные режимы фильтрации и/или списки групповых адресов для того же группового адреса и интерфейса. В качестве примера предположим, сто приложение или процесс вызывает для сокета s1 операцию

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

запрашивающую приём на интерфейсе i пакетов, переданных по групповому адресу m, исходящих **только** с адресов a, b и c. Предположим, что другое приложение или процесс вызывает для сокета s2 операцию

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

запрашивающую приём на том же интерфейсе i пакетов, переданных по тому же групповому адресу m, исходящих **только** с адресов b, c и d. Для удовлетворения требований на обоих сокетах интерфейсу i нужно принимать пакеты, направленные по адресу m от любого из источников a, b, c и d. Таким образом, в этом примере состояние интерфейса i для группового адреса m имеет фильтр INCLUDE и список источников {a, b, c, d}.

После того, как групповой пакет был воспринят с интерфейса уровнем IP, он доставляется процессу или приложению, прослушивающему конкретный сокет, заданный состоянием восприятия группового трафика [и, возможно, другими условиями типа номера порта транспортного уровня, к которому привязан сокет]. В рамках приведённого выше примера если пакет приходит на интерфейс i и направлен по групповому адресу m от источника a, он будет доставлен на сокет s1, но не на сокет s2. Отметим, что сообщения IGMP Query и Report не фильтруются по источнику и всегда должны обрабатываться хостами и маршрутизаторами.

Фильтрация пакетов в зависимости от состояния приёма группового трафика на сокете является новой функцией этого служебного интерфейса. Прежний сервисный интерфейс [RFC1112] не использовал фильтрации по состоянию сокета. Присоединение сокета просто присоединяло хост к группе через данный интерфейс и пакеты, направленные в данную группу, доставлялись всем сокетам, независимо от их реального присоединения.

Общее правило порождении состояния интерфейса из состояния сокета состоит в создании записи для группового адреса на интерфейсе для каждой различающейся пары (интерфейс - групповой адрес) во всех состояниях сокета. Для совпадающих пар (интерфейс - групповой адрес) выполняются следующие действия:

- если **любая** из таких записей включает фильтр EXCLUDE, для интерфейса тоже устанавливается фильтр EXCLUDE, а список источников для интерфейсной записи будет пересечением списков источников во всех записях сокетов с фильтром EXCLUDE с исключением из него всех списков источников из записей сокета с фильтром INCLUDE. Например, если записи сокетов для группового адреса m и интерфейса i:

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

  соответствующая запись для интерфейса i будет:

  ```
  ( m, EXCLUDE, {b, c} )
  ```

  Если добавится четвёртый сокет

  ```
  s4:  ( i, m, EXCLUDE, {} )
  ```

  интерфейсная запись примет вид:

  ```
  ( m, EXCLUDE, {} )
  ```

- если **все** записи имеют фильтр INCLUDE, для интерфейсной записи также устанавливается режим INCLUDE, а список источников для интерфейсной записи будет объединением списков источников из записей сокетов. Например, если сокеты для группового адреса m на интерфейсе i имеют вид

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

  запись для интерфейса i будет

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

- Реализациям **недопустимо** использовать интерфейсную запись EXCLUDE для представления группы, если все сокеты для этой группы используют фильтр INCLUDE. Если при расчёте состояния для интерфейса достигнут предел доступных системных ресурсов, запросившему операцию приложению **должно** возвращаться сообщение об ошибке.

Приведённые выше правила порождения состояния для интерфейса используются вновь, если вызов IPMulticastListen изменяет состояние сокета путём добавления или изменения записи для состояния сокета. Отметим, что изменение состояния сокета не обязательно влечёт за собой изменение состояния для интерфейса.

4. Форматы сообщений

Сообщения IGMP инкапсулируются в дейтаграммы IPv4 с номеров протокола IP 2. Каждое сообщение IGMP, описанное в этом документе, передаётся со значениями IP TTL = 1, IP Precedence = Internetwork Control (например, ToS 0xc0) и опцией IP Router Alert [RFC-2113] в заголовке IP. Типы сообщений IGMP, зарегистрированы IANA [IANA-REG], как описано в [RFC-3228].

В данном документе описаны два типа сообщений IGMP, относящихся к IGMPv3.

Номер типа (шестнадцатеричный)	***Имя сообщения***
0x11	Membership Query - запрос на включение в группу
0x22	Version 3 Membership Report - отчёт о принадлежности (версия 3)

Реализации IGMPv3 **должны** также поддерживать перечисленные ниже сообщения для обеспечения взаимодействия с предыдущими версиями IGMP (см. раздел 7):

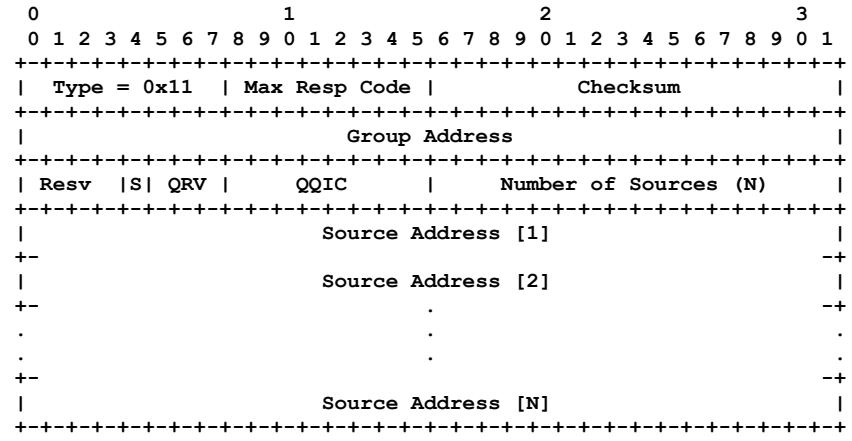
0x12	Version 1 Membership Report - отчёт о принадлежности (версия 1) [RFC-1112]
0x16	Version 2 Membership Report - отчёт о принадлежности (версия 2) [RFC-2236]
0x17	Version 2 Leave Report - отчёт о выходе (версия 2) [RFC-2236]

Нераспознанные типы сообщений **должны** отбрасываться без уведомления. Новые версия или расширения IGMP, протоколов групповой маршрутизации и т. п. могут использовать дополнительные типы сообщений.

В этом документе (если явно не указано иное) термины Query и Report обозначают сообщения IGMP Membership Query и IGMP V3 Membership Report, соответственно.

4.1. Запрос о принадлежности к группе

Сообщения Membership Query передаются групповыми маршрутизаторами IP для запроса состояния приёма группового трафика на соседних интерфейсах. Формат запроса показан ниже.



4.1.1. Max Resp Code

Поле Max Resp Code задаёт максимальное время, задержки с отправкой отклика. Реальное значение разрешённой задержки определяется значением Max Resp Time, которое представляется в десятых долях секунды и определяется на основе Max Resp Code, как показано ниже:

если Max Resp Code < 128, Max Resp Time = Max Resp Code;

если Max Resp Code >= 128, Max Resp Code представляется десятичным значением с плавающей запятой в формате:


```
Max Resp Time = (mant | 0x10) << (exp + 3)
```

Малые значения Max Resp Time позволяют маршрутизаторам IGMPv3 подобрать leave latency (задержка между моментом выхода из группы последнего хоста и моментом, когда протокол маршрутизации уведомляется об отсутствии в группе кого-либо). Большие значения (особенно > 128) позволяют регулировать всплески трафика IGMP в сети.

4.1.2. Checksum

Поле контрольной суммы представляет собой 16-битовое дополнение до 1 суммы дополнений до 1 для всего сообщения IGMP (данные пакеты IP). При расчёте контрольной суммы само значение поля Checksum предполагается нулевым. На приёмной стороне контрольная сумма должна проверяться до начала обработки сообщения [RFC-1071].

4.1.3. Group Address

Поле Group Address содержит значение 0 для сообщений General Query и запрашиваемый групповой адрес IP для сообщений Group-Specific Query и Group-and-Source-Specific Query (см. параграф 4.1.9).

4.1.4. Resv (резерв)

Поле Resv устанавливается в 0 при передаче и игнорируется на приёмной стороне.

4.1.5. Флаг S (подавление обработки Router-Side)

Установленный флаг S указывает всем промежуточным групповым маршрутизаторам, что выполнять обычные обновления таймеров, которые происходят при получении запросов, для этого случая не нужно. Однако этот флаг не отменяет выбор запрашивающего и обычную (host-side) обработку запроса, которая может потребоваться на маршрутизаторах, являющихся членами группы.

4.1.6. QRV

Если поле QRV[1] отлично от 0, оно содержит значение [Robustness Variable], используемое запрашивающим (т. е., отправителем запроса). Если значение [Robustness Variable] у запрашивающего превышает 7 (максимум для поля QRV), устанавливается QRV = 0. Маршрутизаторы используют значение QRV из наиболее свежего запроса в качестве значения переменной [Robustness Variable], если это поле отлично от 0. При нулевом значении QRV получатели используют принятое по умолчанию (см. параграф 8.1) или заданное статически значение [Robustness Variable].

4.1.7. QQIC

Поле QQIC[2] указывает [Query Interval], используемый запрашивающим. Реальный интервал3 QQI задаётся в секундах и определяется на основе кода QQIC, как показано ниже

если QQIC < 128, QQI = QQIC

если QQIC >= 128, QQIC представляется действительным числом с плавающей запятой в форме

```
    0 1 2 3 4 5 6 7
   +-+-+-+-+-+-+-+-+
   |1| exp | mant  |
   +-+-+-+-+-+-+-+-+
QQI = (mant | 0x10) << (exp + 3)
```

Групповые маршрутизаторы, не являющиеся инициатором текущего запроса, устанавливают своё значение [Query Interval] в соответствии с QQI на основе наиболее свежего запроса, если значение QQI не равно 0. В последнем случае используется принятое по умолчанию значение [Query Interval], как указано в параграфе 8.2.

4.1.8. Number of Sources (N)

Поле Number of Sources (N) указывает число адресов источников, присутствующих в запросе. Это поле имеет значение 0 в запросах General и Group-Specific, а в запросах Group-and-Source-Specific отлично от 0. Число адресов ограничено значением MTU в сети, через которую передаётся сообщение Query. Например в сетях Ethernet значение MTU равно 1500, заголовок IP с опцией Router Alert занимает 24 октета, поля IGMP вместе с Number of Sources (N) - ещё 12 октетов и для адресов источников остаётся 1464 октета, что позволяет включить 366 адресов (1464/4).

4.1.9. Source Address [i]

Поле Source Address [i] представляет собой вектор из n индивидуальных адресов IP, где значение n задано полем Number of Sources (N).

4.1.10. Дополнительные данные

Если поле Packet Length в заголовке IP принятого запроса указывает на присутствие дополнительных октетов данных, реализация IGMPv3 **должна** учитывать эти данные при вычислении контрольной суммы и сравнении с полем IGMP Checksum, в противном случае эти данные **должны** игнорироваться. При передаче сообщений Query реализациям IGMPv3 **недопустимо** включать в пакет дополнительные октеты сверх описанных здесь.

4.1.11. Варианты запросов

Имеется три вариант сообщений Query:

1. Запросы общего назначения (General Query) передаются групповыми маршрутизаторами для определения полного состояния приёма группового трафика на соседних интерфейсах (т.е, интерфейсах, подключённых к сети, в которую передаётся запрос). В General Query поля Group Address и Number of Sources (N) равны 0.
2. Запросы для группы (Group-Specific Query) передаются групповыми маршрутизаторами для определения состояния приёма применительно к **одному** групповому адресу на соседних интерфейсах. В Group-Specific Query поле Group Address содержит интересующий групповой адрес, а поле Number of Sources (N) - 0.
3. Запросы для группы и источника (Group-and-Source-Specific Query) передаются групповыми маршрутизаторами для определения наличия среди соседних интерфейсов желающего принимать пакеты, направленные по указанному групповому адресу любым из источников в вписке. В запросах Group-and-Source-Specific поле Group Address содержит интересующий адрес, а поля Source Address [i] - список интересующих источников.

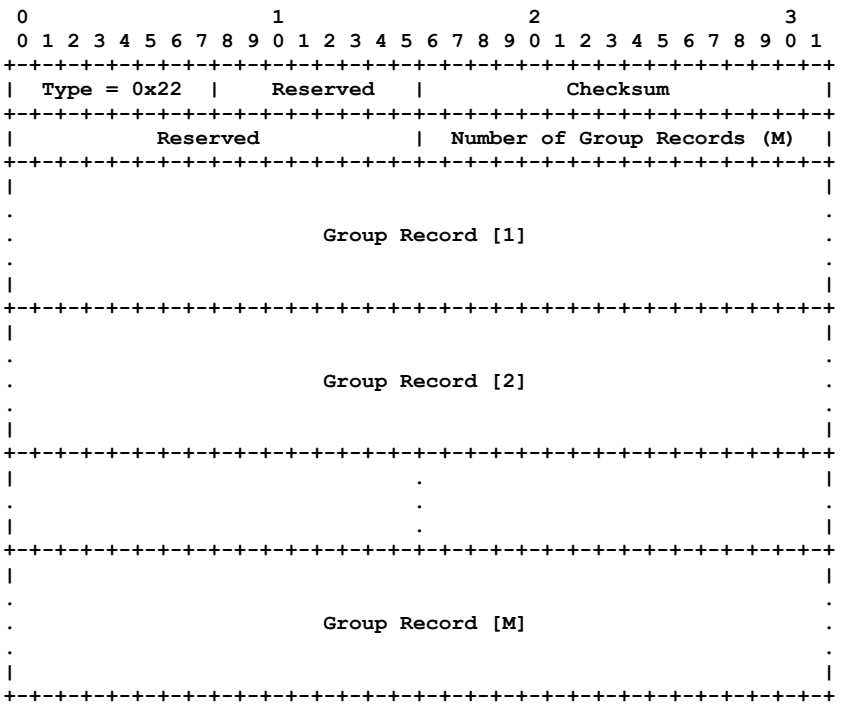
4.1.12. Адреса получателей для запросов

Общие запросы в IGMPv3 передаются с использованием IP-адреса получателя 224.0.0.1 (групповой адрес для всех систем. Запросы Group-Specific и Group-and-Source-Specific передаются по интересующему групповому адресу, Однако система должна воспринимать и обрабатывать все сообщения Query, где поле IP Destination Address содержит **любой** из адресов (индивидуальных и групповых) интерфейса, на котором принят запрос.

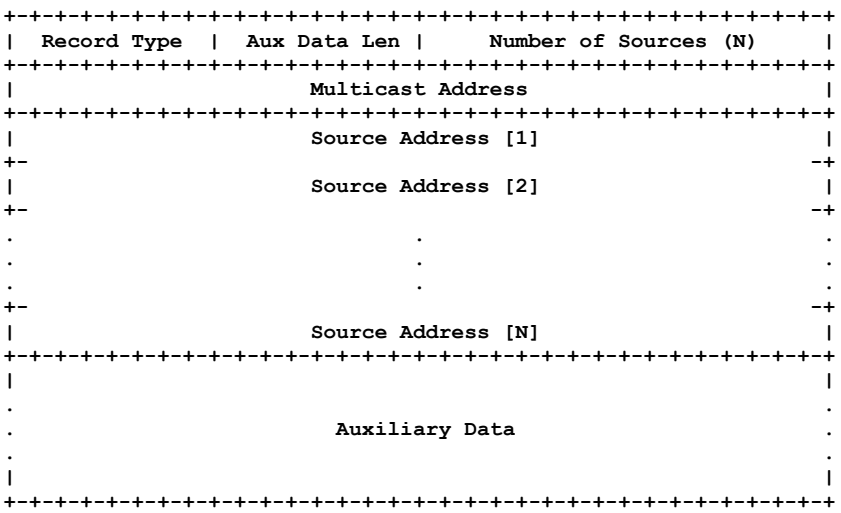
[1]Querier's Robustness Variable - значение отказоустойчивости запрашивающего.
[2]Querier's Query Interval Code - код интервала между запросами.

4.2. Сообщение Version 3 Membership Report

Сообщения Version 3 Membership Report передаются IP-системами для информирования соседних маршрутизаторов о текущем состоянии приёма группового трафика на своих интерфейсах или изменении этого состояния. Формат отчёта показан ниже.



Каждое поле Group Record имеет показанный ниже формат.



4.2.1. Reserved

Резервное поле устанавливается в 0 при передаче и игнорируется на приёмной стороне.

4.2.2. Checksum

Поле контрольной суммы представляет собой 16-битовое дополнение до 1 суммы дополнений до 1 для всего сообщения IGMP (данные пакеты IP). При расчёте контрольной суммы само значение поля Checksum предполагается нулевым. На приёмной стороне контрольная сумма должна проверяться до начала обработки сообщения.

4.2.3. Number of Group Records (M)

Поле Number of Group Records (M) задаёт число записей Group Record в данном отчёте.

4.2.4. Group Record

Каждая запись Group Record представляет собой блок полей с информацией принадлежности отправителей к одной из multicast-групп на интерфейсе, с которого передаётся сообщение Report.

4.2.5. Record Type

См. параграф 4.2.12.

4.2.6. Aux Data Len

Поле Aux Data Len указывает размер поля Auxiliary Data данной записи Group Record в 32-битовых словах. Нулевое значение поля говорит об отсутствии дополнительных данных.

4.2.7. Number of Sources (N)

Поле Number of Sources (N) задаёт число адресов отправителей в данной записи Group Record.

4.2.8. Multicast Address

Поле Multicast Address содержит групповой адрес IP, к которому относится данная запись Group Record.

4.2.9. Source Address [i]

Поле Source Address [i] представляет собой массив из n индивидуальных адресов IP, где n задаётся полем Number of Sources (N).

4.2.10. Auxiliary Data

При наличии поля Auxiliary Data оно служит для передачи дополнительной информации, относящейся к этой записи Group Record. Описываемый в этом документе протокол IGMPv3 не определяет каких-либо дополнительных данных. Следовательно, рекомендациям IGMPv3 **недопустимо** включать какие-либо дополнительные данные (т. е., **должно** устанавливаться Aux Data Len = 0) в передаваемые записи Group Record, а на приёмной стороне такие данные **должны** игнорироваться. Значение и представление полей Auxiliary Data может быть определено в последующих версиях протокола IGMP или его расширений.

4.2.11. Дополнительные данные

Если поле Packet Length в заголовке IP принятого сообщения Report говорит о наличии дополнительных октетов данных после финальной записи Group Record, реализации IGMPv3 **должны** включать эти октеты в расчёт IGMP Checksum, игнорируя их впоследствии. При передаче сообщений Report реализации IGMPv3 **недопустимо** включать какие-либо данные после финальной записи Group Record.

4.2.12. Типы записей Group Record

Существует множество типов различных записей Group Record, которые могут включаться в сообщения Report.

- Записи Current-State (текущее состояние) передаются системой в ответ на принятое интерфейсом сообщение Query. Такие записи говорят о текущем состоянии приёма на данном интерфейсе применительно к одному групповому адресу. Поле Record Type записи Current-State может принимать одно из двух значений, приведённых ниже.

Значение	*Имя и описание*
1	MODE_IS_INCLUDE - указывает, что на интерфейсе для указанного адреса установлен фильтр INCLUDE. Поля Source Address [i] в данной записи Group Record содержат список источников для указанного группового адреса на данном интерфейсе (если список не пуст).
2	MODE_IS_EXCLUDE - указывает, что на интерфейсе для указанного адреса установлен фильтр EXCLUDE. Поля Source Address [i] в данной записи Group Record содержат список источников для указанного группового адреса на данном интерфейсе (если список не пуст).

- Запись Filter-Mode-Change передаётся системой в тех случаях, когда локальный вызов IPMulticastListen приводит к изменению режима фильтрации (например, с INCLUDE на EXCLUDE или наоборот) в записи состояния интерфейса для конкретного группового адреса. Запись включается в сообщения Report, передаваемые с интерфейса, для которого произошло изменение. Поле Record записей Filter-Mode-Change может принимать одно из двух приведённых ниже значений.

3	CHANGE_TO_INCLUDE_MODE - показывает, что на интерфейсе для указанного группового адреса режим фильтрации изменён на INCLUDE. Поля Source Address [i] в данной записи Group Record содержат список источников для указанного группового адреса на данном интерфейсе (если список не пуст).
4	CHANGE_TO_EXCLUDE_MODE - показывает, что на интерфейсе для указанного группового адреса режим фильтрации изменён на EXCLUDE. Поля Source Address [i] в данной записи Group Record содержат список источников для указанного группового адреса на данном интерфейсе (если список не пуст).

- Запись Source-List-Change передаётся системой, в которой локальный вызов IPMulticastListen приводит к изменению списка источников, не совпадающему со сменой режима фильтрации, в интерфейсной записи для конкретного группового адреса. Такая запись включается в сообщение Report, передаваемое интерфейсом, где произошли изменения. Поле Record Type записи Source-List-Change может иметь одно из значений:

5	ALLOW_NEW_SOURCES - показывает, что поля Source Address [i] в данной Group Record содержат список дополнительных источников, которые система хочет принимать при передаче ими пакетов на указанный групповой адрес. Если изменение внесено в список фильтра INCLUDE, адреса добавляются в имеющийся список, если для фильтра задан режим EXCLUDE, добавленные адреса удаляются из списка.
6	BLOCK_OLD_SOURCES - показывает, что поля Source Address [i] в данной Group Record содержат список дополнительных источников, которые система не хочет больше принимать при передаче ими пакетов на указанный групповой адрес. Если изменение внесено в список фильтра INCLUDE, адреса удаляются из имеющегося списка принимаемых источников, если для фильтра задан режим EXCLUDE, адреса добавляются в список исключений.

  Если изменение списка источников приводит одновременно к добавлению новых источников и блокировке имеющихся, передаются две записи Group Record для одного группового адреса - одна запись имеет тип ALLOW_NEW_SOURCES, другая - BLOCK_OLD_SOURCES.

Термин State-Change используется для обозначения записи Filter-Mode-Change или Source-List-Change.

Нераспознанные типы записей **должны** игнорироваться без уведомления.

4.2.13. IP-адреса источников для сообщений Report

Отчёты IGMP передаются с корректным для подсети получателя IP-адресом источника. Адрес отправителя 0.0.0.0 может использоваться системами, которые ещё не имеют адреса IP. Отметим, что адрес 0.0.0.0 может одновременно использовать множество систем в ЛВС. Маршрутизаторы **должны** воспринимать отчёты с адресом отправителя 0.0.0.0.

4.2.14. IP-адреса получателей для сообщений Report

Сообщения Report версии 2 передаются по групповому адресу получателя 224.0.0.22, который прослушивают все поддерживающие IGMPv3 групповые маршрутизаторы. Система, работающая в режиме совместимости с версией 1 или 2, передаёт отчёты версии 1 или 2 по групповому адресу, указанному полем Group Address в сообщении Report. Кроме того, система **должна** воспринимать и обрабатывать все сообщения 2 версии 1 и 2, где поле IP Destination Address указывает на **любой** (индивидуальный или групповой) из интерфейсов системы, получившей сообщение Report.

4.2.15. Нотация для записей Group Record

В оставшейся части этого документа для обозначения содержимого Group Record, относящегося к конкретному групповому адресу используется показанная ниже нотация.

IS_IN (x) - тип MODE_IS_INCLUDE, адреса источников x;

IS_EX (x) - тип MODE_IS_EXCLUDE, адреса источников x;

TO_IN (x) - тип CHANGE_TO_INCLUDE_MODE, адреса источников x;

TO_EX (x) - тип CHANGE_TO_EXCLUDE_MODE, адреса источников x;

ALLOW (x) - тип ALLOW_NEW_SOURCES, адреса источников x;

BLOCK (x) - тип BLOCK_OLD_SOURCES, адреса источников x,

где x может быть:

- заглавной буквой (например, A) для обозначения множества источников;
- выражением (например, A+B), где A+B задаёт объединение множеств A и B, A*B указывает пересечение множеств A и B, A-B означает исключение элементов множества B из множества A.

4.2.16. Размер Membership Report

Если множество записей Group Record в отчёте. не помещается в размеры одного сообщения Report (определяется MTU в сети, через которую сообщение будет передано), записи Group Record передаются в нескольких сообщениях Report.

Если одна запись Group Record содержит множество адресов источников, которое не помещается в размер записи одного сообщения Report, для типов MODE_IS_EXCLUDE и CHANGE_TO_EXCLUDE_MODE запись делится на множество Group Record, содержащих отдельные подмножества адресов источников, и эти записи передаются в отдельных сообщениях Report. Для типов MODE_IS_EXCLUDE и CHANGE_TO_EXCLUDE_MODE, передаётся одна запись Group Record, содержащая столько адресов источников, сколько позволяет размер, а оставшиеся адреса просто не передаются; хотя выбор передаваемых адресов может быть произвольным, предпочтительно передавать одно и то же подмножество в каждом последующем отчёте., а не выбирать разные подмножества для сообщений.

5. Описание протокола для членов группы

Протокол IGMP является асимметричным и отдельно задаёт поведение членов групп (хостов и маршрутизаторов, получающих групповой трафик) и групповых маршрутизаторов. В этом параграфе описана та часть IGMPv3, которая относится ко всем членам групп. Отметим, что входящий в группу multicast-маршрутизатор выполняет требования обеих частей IGMPv3, получая сообщения IGMP от себя и своих соседей и отвечая на эти сообщения. Относящаяся к групповым маршрутизаторам часть IGMPv3 описана в разделе 6.

Поддерживающая протокол система выполняет описанные в этом разделе требования на всех своих интерфейсах, принимающих групповой трафик даже при подключении нескольких таких интерфейсов к одной сети.

Для обеспечения взаимодействия с системами, использующими ранние версии IGMP, поддерживается переменная MulticastRouterVersion для каждого интерфейса, на котором принимается групповой трафик. В этом параграфе описано поведение входящих в группы систем на интерфейсах которых задано MulticastRouterVersion = 3. Алгоритм определения MulticastRouterVersion и поведение для других (не 3) версий описано в разделе 7.

Групповой адрес all-systems (224.0.0.1) требует специальной обработки. На всех системах (хосты и маршрутизаторы, включая групповые) получение пакетов, направленных по адресу all-systems из любого источника постоянно разрешено на всех интерфейсах, где разрешается приём группового трафика. Никаких сообщений IGMP, относящихся к групповому адресу all-systems, не передаётся.

Существует два типа событий, которые вызывают действия протокола IGMPv3 на интерфейсе:

- изменение состояния приёма на интерфейсе, вызванное локальным вызовом IPMulticastListen;
- приём сообщения Query.

(сообщения IGMP, не являющиеся запросами, игнорируются без уведомления, за исключением случаев, когда их обработка требуется для совместимости с ранними версиями IGMP).

В последующих параграфах описаны действия для каждого из двух упомянутых случаев. В этих описаниях имена таймеров и счётчиков приводятся в квадратных скобках. Принятые по умолчанию значения таймеров и счётчиков приведены в разделе 8.

5.1. Действия при смене состояния интерфейса

Вызов IPMulticastListen может привести к смене состояния приёма группового трафика на интерфейсе в соответствии с правилами, приведёнными в параграфе 3.2. Каждое такое изменение воздействует на интерфейсную запись для одного группового адреса.

Изменение состояния на интерфейсе заставляет систему незамедлительно передать с этого интерфейса сообщение State-Change Report. Тип и содержимое Group Record в этом сообщении определяется путём сравнения режима фильтрации и списка источников для затронутого группового адреса до изменения и после его, как показано в таблице ниже. Если до изменения на интерфейсе не было состояния для данного группового адреса (создание интерфейсной записи) или состояние исчезло после изменения (удаление интерфейсной записи), «не существующее» состояние трактуется, как фильтр INCLUDE с пустым списком источников.

Старое состояние	***Новое состояние***	***Переданная запись***
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)

Если рассчитанный список источников в ALLOW или BLOCK записи State-Change Record пуст, такая запись не включается в сообщение Report.

На случай пропуска записи State-Change Report одним или множеством групповых маршрутизаторов она повторяется [Robustness Variable] - 1 раз со случайными интервалами из диапазона (0, [Unsolicited Report Interval]).

Если до завершения повторных передач сообщения State-Change Report произошла новая смена состояния, рассчитываются новые изменения и незамедлительно передаётся новое сообщение State-Change Report.

Расчёт содержимого нового отчёта для передачи показан ниже. Как и для первого сообщения сравнивается состояние интерфейса для затронутой группы до и после позднейшего изменений. Записи отчёта, показывающие различия, строятся в соответствии с приведённой выше таблицей. Однако эти записи не передаются в сообщении непосредственно, а объединяются с содержимым ожидающего отчёта для создания нового сообщения State-Change. Правила слияния описаны ниже.

Передача слитого сообщения State-Change Report прерывает повтор передачи предшествующих сообщений State-Change Report для того же группового адреса и начинает первую из [Robustness Variable] передач новых сообщений State-Change Report.

При каждом включении источника в разные отчёты, созданные как описано выше, для этого источника нужно поддерживать состояние повтора передачи пока хостом не будет передано [Robustness Variable] сообщений State-Change. Это делается для того, чтобы последовательные смены состояний не нарушали устойчивость протокола.

Если вызвавшая новый отчёт смена состояния интерфейса является изменением режима фильтрации, следующие [Robustness Variable] сообщений State-Change Report будут включать запись Filter-Mode-Change. Это применимо даже для тех случаев, когда в течение этого периода произошли изменения списка источников. Хост поддерживает состояние повтора для группы, пока не будут переданы [Robustness Variable] сообщений State-Change. Когда было передано [Robustness Variable] сообщений State-Change с записями Filter-Mode-Change после смены режима фильтрации и смена списка источников для интерфейса вызывает дополнительные отчёты, следующее сообщение State-Change будет включать записи Source-List-Change.

При каждой передаче State-Change Report содержимое сообщения определяется, как описано ниже. Если в отчёт следует включать запись Filter-Mode-Change, тогда при режиме фильтрации на интерфейсе INCLUDE в сообщение включается запись TO_IN, в остальных случаях - TO_EX. Если же в отчёт следует включать записи Source-List-Change, следует включать запись ALLOW и BLOCK. Содержимое упомянутых записей показано в таблице.

Запись	***Включённые источники***
TO_IN	Все из текущего состояния интерфейса, для которых должна выполняться пересылка.
TO_EX	Все из текущего состояния интерфейса, которые должны блокироваться.
ALLOW	Все с состоянием повторной передачи, что должно пересылаться.
BLOCK	Все с состоянием повторной передачи, что должно блокироваться.

Если рассчитанный список источников для записи ALLOW или BLOCK пуст, такая запись не включается в сообщение State-Change.

> Примечание. При передача первого сообщения State-Change отсутствующий отчёт для слияния может рассматриваться, как отчёт об изменении состояния с пустыми записями ALLOW и BLOCK (ни для одного источника нет состояния повтора передачи).

5.2. Действия при получении запроса

Получив сообщение Query, система не реагирует на него незамедлительно. Отклик задерживается не некоторое случайное время, ограниченное значением Max Resp Time, которое определяется из Max Resp Code в полученном запросе. Система может получать на разных интерфейсах разные запросы (например, General Query, Group-Specific Query, Group-and-Source-Specific Query), каждый из которых может потребовать своей задержки с откликом.

Перед планированием отклика на сообщение Query система должна сначала принять во внимание ожидающие отклики - во многих случаях планируемый отклик можно будет объединить с ожидающим. Следовательно, система должна поддерживать следующие параметры состояния:

- таймеры для интерфейсов при планировании откликов на General Query;
- таймеры для групп и интерфейсов при планировании откликов на запросы Group-Specific и Group-and-Source-Specific;
- списки источников для групп и интерфейсов, включаемые в отклики на Group-and-Source-Specific Query.

При получении нового сообщения Query с опцией Router-Alert на интерфейсе и система имеет состояние для оповещения, задержка с откликом выбирается случайным образом из диапазона (0, [Max Resp Time]), где значение Max Resp Time выводится из Max Resp Code в принятом сообщении Query. После этого используются приведённые ниже правила для определения планирования и типа сообщения Report. Правила применяются до обнаружения первого соответствия.

1. При наличии ожидающего отклика на предшествующий запрос General, запланированного раньше выбранной задержки, планировать дополнительный отклик не требуется.

2. Если получен запрос General, используется таймер интерфейса для планирования отклика на него по истечении заданного времени. Все ожидающие предшествующие отклики на General Query отбрасываются.

3. Если получен запрос Group-Specific или Group-and-Source-Specific и нет ожидающих откликов на предшествующие запросы для данной группы, используется таймер группы для планирования отклика. Если получен запрос Group-and-Source-Specific, список источников из него записывается для использования при генерации отклика.

4. Если имеется ожидающий отклик на предшествующий запрос для данной группы и новый запрос является Group-Specific Query или записанный список связанных с группой источников пуст, список источников для группы очищается и планируется один отклик с использованием таймера группы. Новый отклик планируется для передачи по истечении меньшего из двух сроков - оставшееся время ожидания и выбранная задержка.

5. Если получен запрос Group-and-Source-Specific и для этой группы имеется ожидающий отклик с непустым списком источников, список источников для данной группы дополняется списком из полученного запроса и планируется один отклик с использованием таймера группы. Новый отклик планируется для передачи по истечении меньшего из двух сроков - оставшееся время ожидания и выбранная задержка.

Когда отсчёт таймера для ожидающего отклика завершается, система передаёт через соответствующий интерфейс одно или множество сообщений Report содержащих одну или множество записей Current-State Record (см. параграф 4.2.12), как описано ниже:

1. Если отсчёт завершился для таймера интерфейса (т. е., в ожидании находится отклик на General Query), передаётся одна запись Current-State Record для каждого группового адреса, по отношению к которому у данного интерфейса имеется состояние восприятия, как описано в параграфе 3.2. Current-State Record передаёт групповой адрес и связанный с ним режим фильтрации (MODE_IS_INCLUDE или MODE_IS_EXCLUDE), а также список источников. Записи Current-State Record помещаются в отдельные сообщения Report (насколько позволяет размер).

2. Использование этого наивного алгоритма может приводить к значительным всплескам трафика в тех случаях, когда система входит в большое число групп. Вместо использования одного интерфейсного таймера реализациям рекомендуется распределять передачу таких сообщений Report в интервале (0, [Max Resp Time]). Отметим, что такие реализации **должны** предотвращать возникновение проблемы ack-implosion (взрыв подтверждений) (т. е., **недопустима** передача сообщений Report сразу же при получении General Query).

   Если завершился отсчёт для таймера группы и список сохранённых источников для группы пуст (т. е., имеется ожидающий отклик на Group-Specific Query), тогда (и только тогда) при наличии на интерфейсе состояния приёма для данного группового адреса передаётся одна запись Current-State Record для этого адреса. Запись Current-State содержит групповой адрес, связанный с ним режим фильтрации (MODE_IS_INCLUDE или MODE_IS_EXCLUDE) и список источников.

3. Если завершился отсчёт для таймера группы и список сохранённых источников для группы не пуст (т. е., имеется ожидающий отклик на Group-and-Source-Specific Query), тогда (и только тогда) при наличии на интерфейсе состояния приёма для данного группового адреса содержимое записи Current-State Record в отклике определяется из состояния интерфейса и ожидающего отклика, как показано в таблице ниже:

Набор источников в состоянии интерфейса	***записи ожидания отклика***	***записи текущего состояния***
INCLUDE (A)	B	IS_IN (A*B)
EXCLUDE (A)	B	IS_IN (B-A)

Если в полученной записи Current-State Record набор адресов отправителей будет пустым, отклик не передаётся.

В заключении, после генерации всех требуемых сообщений Report списки источников, связанные с группами, для которых передавались отчёты, очищаются.

6. Описание протокола для групповых маршрутизаторов

Целью IGMP является обеспечение каждому групповому маршрутизатору возможности узнать для всех подключённых непосредственно сетей групповые адреса, представляющие интерес для находящихся в этих сетях систем. IGMP версии 3 добавляет для групповых маршрутизаторов возможность узнать какие источники интересуют соседние системы для пакетов, направленных по любому конкретному групповому адресу. Собранная IGMP информация предоставляется используемому маршрутизатором протоколу групповой маршрутизации для того, чтобы групповые пакеты были доставлены во все сети, где есть заинтересованные получатели.

В этом разделе описана часть протокола IGMPv3, выполняемая групповыми маршрутизаторами. Эти маршрутизаторы сами могут быть членами multicast-групп и, следовательно, будут выполнять связанную с членами групп часть IGMPv3, описанную в разделе 5.

Групповой маршрутизатор исполняет описанный в этом разделе протокол для каждой из подключённых непосредственно к нему сетей. Если групповой маршрутизатор имеет несколько интерфейсов в одну сеть, достаточно исполнять этот протокол на одном из таких интерфейсов. На каждом интерфейсе, где используется протокол, маршрутизатор **должен** разрешить восприятие пакетов, направленных по групповому адресу 224.0.0.22, из всех источников (и **должен** исполнять групповую часть IGMPv3 для данного адреса на этом интерфейсе).

Групповому маршрутизатору нужно знать лишь, что **хотя бы одна** система в подключённой сети заинтересована в пакетах, направленных по конкретному групповому адресу из конкретного источника; ему не требуется отслеживать интересы каждой из соседних систем (см. дополнительное обсуждение в Приложении A.2, п. 1).

IGMPv3 обеспечивает совместимость с более ранними версиями протокола IGMP. Для этого групповые маршрутизаторы IGMPv3 **должны** также реализовать версии протокола 1 и 2 (см. раздел 7).

6.1. Условия для запросов IGMP

Групповые маршрутизаторы периодически отправляют запросы General Query для получения данных о принадлежности к группам из подключённых сетей. Эти запросы используются для создания и обновления состояния принадлежности к группам систем в подключённых сетях. Системы отвечают на такие запросы сообщениями со своим статусом присутствия в группах (и желаемыми наборами источников) в записях Current-State Group Record сообщений IGMPv3 Membership Report.

Как член multicast-группы, система может выражать свою заинтересованность в получении или отказе от получения трафика из конкретных источников. При изменении желаемого состояния восприятия в системе, она сообщает об этих изменениях, используя записи Filter-Mode-Change и/или Source-List-Change. Такие записи указывают явное изменение состояния для группы в системе в части списка источников или режима фильтрации. Когда участие в группе прерывается для системы или получение трафика от конкретного источника становится нежелательным, групповой маршрутизатор должен запросить других участников группы или прослушивающих тот же источник прежде, чем удалить группу (или источник) и отсечь соответствующий трафик.

Для обеспечения всем системам в сети возможности отвечать на изменения принадлежности к группам групповые маршрутизаторы передают специальные запросы. Group-Specific Query передаётся для того, чтобы убедиться в отсутствии систем, желающих принимать конкретную группу, или перестроить состояние восприятия для конкретной группы. Запросы Group-Specific передаются в тех случаях, когда маршрутизатор получает запись State-Change, указывающую выход системы из группы.

Запросы Group-and-Source Specific служат для проверки отсутствия в сети систем, желающих получать трафик из указанного набора источников. Group-and-Source Specific указывают источники для конкретной группы, относительно которых был запрошен отказ от пересылки. Такие запросы передаются групповыми маршрутизаторами для того, чтобы определить наличие систем, желающих получать пакеты по указанному групповому адресу из заданного списка источников. Запросы Group-and-Source Specific передаются только в ответ на получение записей State-Change и никогда не передаются в ответ на записи Current-State. Более подробно запросы описаны в параграфе 4.1.11.

6.2. Состояние IGMP, поддерживаемое групповыми маршрутизаторами

Групповые маршрутизаторы, поддерживающие IGMPv3 сохраняют состояния по группам и подключённым сетям. Состояние для группы включает режим фильтрации, список источников и разные таймеры. Для каждой подключённой сети, где используется IGMP, групповой маршрутизатор сохраняет желаемое состояние восприятия, которое представляет собой набор записей виде:

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

Каждая запись для источника (source record) имеет форму:

```
(source address, source timer)
```

Если желательны все источники в данной группе, сохраняется пустая запись источников с режимом фильтрации EXCLUDE. Это показывает, что хосты данной сети желают пересылки всех источников для данной группы. В IGMPv3 это служит эквивалентов включения в группу IGMPv1 или IGMPv2.

6.2.1. Определение Router Filter-Mode

Для снижения числа внутренних состояний маршрутизаторы IGMPv3 хранят режимы фильтрации по группам и подключённым сетям. Эти режимы используются для сжатия общего желаемого состояния приёма группы до минимального набора, который удовлетворит все входящие в группу системы. Режим фильтрации может меняться в ответ на получение отдельных типов записей от групп или по событиям, связанным с таймерами. В последующих параграфах используется термин router filter-mode для обозначения режима фильтрации применительно к конкретной группе. В параграфе 6.4 описаны изменения режима фильтрации при получении записей от групп.

Концептуально при получении записи от группы режим фильтрации для данной группы меняется так, чтобы включались все запрошенные источники с применением минимального числа состояний. Как правило, при получении от группы записи с режимом фильтрации EXCLUDE маршрутизатор будет использовать для данной группы фильтр EXCLUDE.

Когда в маршрутизаторе для группы установлен фильтр EXCLUDE, запись со списком источников содержит два типа источников. Первый набор включает источники, которые конфликтуют с желаемым состоянием восприятия - для этого типа должна обеспечиваться пересылка на том или ином маршрутизаторе сети. Второй набор включает источники, для которых хосты запросили отказ от пересылки. В Приложении A описаны причины хранения этого набора при фильтрации в режиме EXCLUDE.

Когда в маршрутизаторе для группы установлен фильтр INCLUDE, запись со списком источников представляет собой список источников, которые группа желает принимать. Это общий набор желаемых источников для данной группы. Для каждого источника в списке должна обеспечиваться пересылка на том или ином маршрутизаторе сети.

Поскольку переданная групповая запись с режимом фильтрации EXCLUDE будет вынуждать маршрутизатор сменить свой режим фильтрации на EXCLUDE, требуется механизм для возврата маршрутизаторов в режим INCLUDE. Если все системы из группы с режимом EXCLUDE прекратили присылать отчёты, на маршрутизаторе желательно вернуть для этой группы режим INCLUDE. Переход происходит по групповому таймеру, как описано в параграфе 6.5.

6.2.2. Определение групповых таймеров

Групповой таймер используется только для групп в режиме EXCLUDE и представляет время, когда режим фильтрации (filter-mode) для данной группы будет заменён на INCLUDE. Групповые таймеры организуются по группам и подключённым сетям. Групповые таймеры обновляются в соответствии с получаемыми групповыми записями.

Отсчёт группового таймера завершается, когда в маршрутизаторе для группы установлен фильтр EXCLUDE и в подключённой сети не остаётся больше получателей с режимом EXCLUDE. В этот момент маршрутизатор переходит в режим фильтрации INCLUDE. Описание действий при таком переходе приведено в параграфе 6.5.

В таблице ниже показаны роли группового таймера. В параграфе 6.4 подробно описана установка группового таймера по типам получаемых групповых записей.

Режим фильтрации	*Значение таймера*	*Действия и описание*
INCLUDE	Timer >= 0	Все участники группы в режиме INCLUDE.
EXCLUDE	Timer > 0	По крайней мере один участник в режиме EXCLUDE.
EXCLUDE	Timer == 0	В группе больше нет участников. По завершении отсчёта таймеров на источниках запись Group Record удаляется.

6.2.3. Определение таймеров источника

Таймеры источников организуются по записям для источников и декрементируются до достижения нулевого значения. Обновляются эти таймеры в соответствии с типом и режимом фильтрации получаемых групповых записей. Таймер (для конкретной группы) всегда обновляется при наличии данного источника в полученной записи для этой группы. В параграфе 6.4 описана организация таймера источника по типам групповых записей.

Запись для источника с запущенным таймером и режимом фильтрации для группы INCLUDE говорит о наличии одной или множества систем (с режимом фильтрации INCLUDE), которые желают принимать этот источник. Если для группы с режимом фильтрации INCLUDE отсчёт таймера источника завершается, маршрутизатор считает, что трафик от этого источника больше не нужен в подключённой сети и удаляет соответствующую запись для источника.

Таймеры источников трактуются иначе в тех случаях, когда на маршрутизаторе для группы используется режим фильтрации EXCLUDE. Если для записи источника имеется запущенный таймер и на маршрутизаторе для группы установлен режим фильтрации EXCLUDE, это означает, что источник является желанным по крайней мере для одной системы. Следовательно, маршрутизатору нужно пересылать пакеты от этого источника в сеть. В Приложении A описаны причины сохранения состояния для источников, по отношению к которым была запрошена пересылка, несмотря на режим EXCLUDE.

Если отсчёт таймера завершается с режимом фильтрации для группы EXCLUDE, маршрутизатор информирует протокол маршрутизации об отсутствии в сети получателей для данного источника.

При режиме фильтрации EXCLUDE для группы записи источников удаляются только по завершения отсчёта группового таймера. В параграфе 6.описаны действия, которые следует выполнять в зависимости от значения таймера для источника.

6.3. Правила пересылки IGMPv3

Когда групповой маршрутизатор получает от источника дейтаграммы, направленные в конкретную группу, этот маршрутизатор принимает решения о пересылке дейтаграмм в подключённые к нему сети. Ответственность за принятие такого решения лежит на используемом протоколе групповой маршрутизации и следует ему использовать данные IGMPv3 для того, чтобы все источники/группы, желаемые в той или иной подсети, пересылались в данную подсеть. Например, если для группы G задан режим фильтрации EXCLUDE, маршрутизатор может продолжать пересылку исключённых пакетов в транзитную подсеть.

Приведённая ниже таблица описывает предложения по пересылке, направляемые IGMP протоколу маршрутизации для трафика от источника, направленного в ту или иную группу. Указаны также действия, предпринимаемые по завершению отсчёта таймера источника на основе режима фильтрации для группы.

Режим фильтрации	*Значение таймера*	*Действия*
INCLUDE	Timer > 0	Предложить пересылку трафика от источника.
INCLUDE	Timer = 0	Предложить прекратить пересылку трафика от источника и удалить его запись. Если в группе не остаётся записей для источников, удалить запись группы.
INCLUDE	Нет источников	Предложить не пересылать трафик.
EXCLUDE	Timer > 0	Предложить пересылку трафика от источника.
EXCLUDE	Timer == 0	Предложить не пересылать трафик от источника (**не удалять** запись).
EXCLUDE	Нет источников	Предложить пересылку трафика от источника.

6.4. Действия при получении сообщений

6.4.1. Получение записей Current-State

При получении записей Current-State маршрутизатор обновляет свои таймеры для группы и источника. В некоторых случаях получение групповой записи будет вынуждать маршрутизатор изменить режим фильтрации для данной группы. В приведённой ниже таблице показаны действия по отношению к состоянию и таймера, которые может вызывать в маршрутизаторах получение записей Current-State.

Для описания обновлений таймера источника используются специальные обозначения - запись вида (A, B) будет представлять общее число источников для отдельной группы, где

A - множество записей источников, для которых значения таймеров > 0 (хоты бы 1 хост запросил пересылку);

B - множество записей источников, для которых значения таймеров = 0 (источники, для которых IGMP будет предлагать отказ от пересылки).

Отметим, что два множества записей используется только в режиме фильтрации для группы EXCLUDE на маршрутизаторе. Если на маршрутизаторе установлен для группы режим фильтрации INCLUDE, используется одно множество для описания источников, по отношению к которым запрошена пересылка (например, simply (A)).

В последующих таблицах для нескольких переменных используются сокращённые обозначения (они подробно описаны в разделе 8). Переменная GMI[1] указывает интервал, по истечении которого членство в группе прекращается. Переменная LMQT[2] указывает общее время, прошедшее после Last Member Query Count повторов. Значение LMQT представляет «задержку выпуска» или разницу между моментом передачи информации об изменении членства в группе и изменением сведений, предоставляемых протоколу маршрутизации.

В колонке «Действия» таблиц состояний маршрутизатора используются обозначения вида A=J, которые указывают, что множество записей источников A должно установить для своих таймеров значение J. Действие Delete A указывает удаление множества записей источников A. Group Timer=J означает, что в Group Timer для группы следует установить значение J.

Состояние маршрутизатора	*Полученный отчёт*	*Новое состояние*	*Действия*
INCLUDE (A)	IS_IN (B)	INCLUDE (A+B)	(B)=GMI
INCLUDE (A)	IS_EX (B)	EXCLUDE (A*B,B-A)	(B-A)=0 Delete (A-B) Group Timer=GMI
EXCLUDE (X,Y)	IS_IN (A)	EXCLUDE (X+A,Y-A)	(A)=GMI
EXCLUDE (X,Y)	IS_EX (A)	EXCLUDE (A-Y,Y*A)	(A-X-Y)=GMI Delete (X-A) Delete (Y-A) Group Timer=GMI

6.4.2. Получение записей Filter-Mode-Change и Source-List-Change

Когда в системе происходит глобальное изменение состояния группы, данная система передаёт для этой группы запись Source-List-Change или Filter-Mode-Change. Как и в случае с записями Current-State, маршрутизаторы должны реагировать на получение такой информации и могут изменять своё состояние в соответствии с новым желаемым состоянием принадлежности к группам в сети.

Маршрутизаторы должны запрашивать источники, для которых запрошен отказ от пересылки в группу. Когда маршрутизатор отправляет или получает запрос для конкретного набора источников, он снижает значения таймеров для этих источников до значения Last Member Query Time (в секундах). Если в ответ на запросы получены групповые записи, которые показывают заинтересованность в получении трафика из соответствующих источников, таймеры для этих источников обновляются.

Аналогично, при запросе маршрутизатора для конкретной группы, он снижает значение таймера для этой группы до Last Member Query Time секунд. Если в заданном интервале получена какая-либо групповая запись с режимом EXCLUDE, таймер для соответствующей группы обновляется и протоколу маршрутизации передаётся предложение сохранять пересылку для данной группы без прерывания.

В течение периода запроса (т. е., Last Member Query Time секунд) компонента IGMP в маршрутизаторе продолжает предлагать протоколу маршрутизации пересылать трафик, связанный с группами и источниками, указанными в запросе. Если в течение Last Member Query Time секунд не будет получена запись с выражением интереса для указанных в запросе групп или источников, маршрутизатор может «отсечь» группу или источники от сети.

В приведённой ниже таблице указаны изменения в состояниях групп и действия при получении записей Filter-Mode-Change или Source-List-Change. Указаны также запросы, передаваемые при получении тех или иных отчётов.

При описании передаваемых запросов используется обозначение Q(G) для запроса Group-Specific применительно к группе G, Q(G,A) для запроса Group-and-Source Specific применительно к группе G и списку источников A. Если в результате действия (например, A*B) список источников становится пустым, запроса после операции не передаётся.

Для обеспечения отказоустойчивости протокола запросы, передаваемые перечисленными в таблице действиями, требуется передавать [Last Member Query Count] раз в течение каждого интервала [Last Member Query Interval].

Если в момент планирования нового запроса ещё имеются ожидающие повторной передачи запросы для той же группы, новый запрос может быть объединён с имеющимся. Кроме того, получение отчёта хоста для группы с ожидающими запросами может оказывать влияние на содержимое этих запросов. Построение и поддержка состояний очередей ожидания описаны в параграфе 6.6.3.

Состояние маршрутизатора	*Полученный отчёт*	*Новое состояние*	*Действия*
INCLUDE (A)	ALLOW (B)	INCLUDE (A+B)	(B)=GMI
INCLUDE (A)	BLOCK (B)	INCLUDE (A)	Send Q(G,A*B)
INCLUDE (A)	TO_EX (B)	EXCLUDE (A*B,B-A)	(B-A)=0 Delete (A-B) Send Q(G,A*B) Group Timer=GMI
INCLUDE (A)	TO_IN (B	INCLUDE (A+B)	(B)=GMI Send Q(G,A-B)
EXCLUDE (X,Y)	ALLOW (A)	EXCLUDE (X+A,Y-A)	(A)=GMI
EXCLUDE (X,Y)	BLOCK (A)	EXCLUDE (X+(A-Y),Y)	(A-X-Y)=Group Timer Send Q(G,A-Y)

[1]Group Membership Interval.
[2]Last Member Query Time.

EXCLUDE (X,Y)	TO_EX (A)	EXCLUDE (A-Y,Y*A)	(A-X-Y)=Group Timer Delete (X-A) Delete (Y-A) Send Q(G,A-Y) Group Timer=GMI
EXCLUDE (X,Y)	TO_IN (A)	EXCLUDE (X+A,Y-A)	(A)=GMI Send Q(G,X-A) Send Q(G)

6.5. Переключение режима фильтрации

Групповой таймер служит механизмом переключения из режима фильтрации на маршрутизаторе из EXCLUDE в INCLUDE.

Когда отсчёт группового таймера завершается в режиме фильтрации EXCLUDE, маршрутизатор считает, что в подключённых сетях не осталось систем с режимом фильтрации EXCLUDE. Когда на маршрутизаторе установлен для группы режим фильтрации EXCLUDE и отсчёт группового таймера завершается, маршрутизатор переключает режим фильтрации для группы на INCLUDE.

Маршрутизатор использует записи для источников с запущенными таймерами источников в качестве своего состояния для переключения в режим фильтрации INCLUDE. Если есть хотя бы одна запись для источника со значением таймера источника больше 0 (т. е., с запрашиваемой пересылкой), маршрутизатор переключается в режим фильтрации INCLUDE, используя такие записи для источников. Записи для источников с нулевым значением таймера (из предыдущего режима EXCLUDE) удаляются.

Например, если состояние маршрутизатора для группы EXCLUDE(X,Y) и для этой группы завершается отсчёт таймера, маршрутизатор переключается в режим фильтрации INCLUDE с состоянием INCLUDE(X).

6.6. Действия при получении запросов

6.6.1. Обновление таймеров

Когда маршрутизатор передаёт или принимает запрос со сброшенным флагом Suppress Router-Side Processing, он должен обновить свои таймеры в соответствии с корректными значениями тайм-аутов для запрашиваемой группы или источников. В таблице показаны действия при передаче или приёме запроса Group-Specific или Group-and-Source Specific Query со сброшенным флагом Suppress Router-Side Processing.

Запрос	***Действие***
Q(G,A)	Значение Source Timer для источников A снижается до LMQT.
Q(G)	Значение Group Timer снижается до LMQT.

При получении или передаче маршрутизатором запросов с установленным флагом Suppress Router-Side Processing этот маршрутизатор не обновляет значения своих таймеров.

6.6.2. Выбор запрашивающего

IGMPv3 выбирает одного запрашивающего на подсеть, используя такой же механизм выбора, как IGMPv2, а именно - адрес IP. Когда маршрутизатор получает запрос с меньшим адресом IP, он устанавливает для таймера Other-Querier-Present значение Other Querier Present Interval и перестаёт отправлять запросы в сеть, если ранее уже был выбран запрашивающий. По завершении отсчёта таймера Other-Querier Present следует возобновить передачу General Query.

Если маршрутизатор получает более старую версию запроса, он **должен** использовать для этой сети более старую версию IGMP. Рассмотрение вопросов совместимости разных версий IGMP приведено в разделе 7.

6.6.3. Создание и отправка запросов

6.6.3.1. Создание и отправка запросов для группы

Когда в таблице указано действие Send Q(G), значение для таймера группы должно быть уменьшено до LMQT. В этом случае маршрутизатор должен незамедлительно отправить специфичный для группы запрос и запланировать [Last Member Query Count - 1] его повторов за каждый [Last Member Query Interval] в течение [Last Member Query Time].

При передаче специфичного для группы запроса, если значение таймера для группы больше LMQT, бит Suppress Router-Side Processing устанавливается в каждом сообщении.

6.6.3.2. Создание и отправка запросов для группы и источника

Когда запрашивающий встречает действие Send Q(G,X) в таблице 6.4.2, должны выполняться приведённые ниже операции для каждого источника X группы G со значением таймера больше LMQT:

- установить число повторов для каждого источника [Last Member Query Count];
- снизить значение таймера до LMQT.

Маршрутизатор должен незамедлительно передать специфичный для группы и источника запрос, а также запланировать передачу [Last Member Query Count - 1] повторов за каждый [Last Member Query Interval] в течение [Last Member Query Time]. Содержимое этих запросов рассчитывается, как показано ниже.

При создании специфичного для группы и источника запроса для группы G, передаются два отдельных сообщения с запросами. В первом сообщении устанавливается бит Suppress Router-Side Processing и содержатся все источники с состоянием повтора и таймерами больше LMQT. Во втором сообщении бит Suppress Router-Side Processing сброшен и содержатся все источники с состоянием повтора и таймерами не более LMQT. Если в любом из этих двух сообщений не содержится ни одного источника, передача такого сообщения не происходит.

Примечание. Если передача специфичного для группы запроса запланирована на одно время с передачей специфичного для группы и источников запроса для той же группы, передача специфичного для группы и источников сообщения с установленным битом Suppress Router-Side Processing может быть отменена.

7. Взаимодействие с ранними версиями IGMP

Хосты и маршрутизаторы IGMP версии 3 могут взаимодействовать с хостами и маршрутизаторами, ещё не обновлёнными до IGMPv3. Такая совместимость обеспечивается действиями хостов и маршрутизаторов с учётом версий IGMP, используемых на хостах и маршрутизаторах в сети.

7.1. Различия версий запросов

Версия IGMP для сообщений Membership Query определяется следующим образом:

```
IGMPv1 Query: размер 8 октетов и поле Max Resp Code имеет значение 0
IGMPv2 Query: размер 8 октетов и поле Max Resp Code имеет ненулевое значение
IGMPv3 Query: размер не менее 12 октетов
```

Запросу, не соответствующие ни одному из приведённых выше вариантов (например, с размером 10 октетов), **должны** отбрасываться без уведомления.

7.2. Поведение членов группы

7.2.1. При наличии запросов прежних версий

Для совместимости с маршрутизаторами старых версий хосты IGMPv3 **должны** работать в режимах совместимости с версиями 1 и 2. Хосты IGMPv3 **должны** сохранять поинтерфейсное состояние для режима совместимости в каждой из подключённых сетей. Режим совместимости на хосте определяется из переменной Host Compatibility Mode, которая может принимать три значения - IGMPv1, IGMPv2 или IGMPv3. Значения переменной хранятся для отдельно для каждого интерфейса и зависят от версии сообщений General Query, принимаемых этим интерфейсом, а также таймеров Older Version Querier Present для этого интерфейса.

Для беспроблемного переключения с одной версии IGMP на другую хосты сохраняют оба таймера IGMPv1 Querier Present и IGMPv2 Querier Present для каждого интерфейса. Для таймера IGMPv1 Querier Present устанавливается значение Older Version Querier Present Timeout (в секундах) при получении запроса IGMPv1 Membership Query. Для таймера IGMPv2 Querier Present устанавливается значение Older Version Querier Present Timeout (в секундах) при получении запроса IGMPv2 General Query.

Режим совместимости Host Compatibility Mode на интерфейсе меняется при получении запроса более старой версии (по сравнению с текущим режимом) или по завершению отсчёта таймера. При завершении отсчёта IGMPv1 Querier Present хост переключается в режим совместимости с IGMPv2, если у него запущен таймер IGMPv2 Querier Present. Если работающего таймера IGMPv2 Querier Present нет, хост переключается в режим совместимости IGMPv3. При завершении отсчёта таймера IGMPv2 Querier Present хост переключается в режим совместимости IGMPv3.

Значение переменной Host Compatibility Mode определяется наиболее старой версией запроса General, принятой за последние Older Version Querier Present Timeout секунд. Установка Host Compatibility Mode определяется таблицей.

Режим совместимости хоста	***Состояние таймера***
IGMPv3 (по умолчанию)	Таймеры IGMPv2 Querier Present и IGMPv1 Querier Present не запущены
IGMPv2	Таймер IGMPv2 Querier Present запущен, а IGMPv1 Querier Present не запущен
IGMPv1	IGMPv1 Querier Present запущен

Если хост получает запрос, требующий обновления таймеров Querier Present и соответствующей смены режима совместимости, менять режим следует незамедлительно.

В режиме совместимости IGMPv3 хост использует на данном интерфейсе протокол IGMPv3. В режиме совместимости IGMPv2 хост использует на интерфейсе только протокол IGMPv2. В режиме совместимости IGMPv1 хост использует на интерфейсе только протокол IGMPv1.

Маршрутизатор IGMPv1 будет передавать сообщения General Query с Max Resp Code = 0. Это значение **должно** интерпретироваться, как 100 (10 секунд).

Маршрутизатор IGMPv2 будет передавать сообщения General Query с желаемым значением Max Resp Code (диапазон значений Max Resp Time является линейным, а описанный в параграфе 4.1.1 экспоненциальный алгоритм не применяется).

При смене хостом режима совместимости он сбрасывает все ожидающие отклики и таймеры повтора передачи.

7.2.2. При наличии членов групп со старой версией

Хост IGMPv3 может быть размещён в сети, где имеются хосты, ещё не обновлённые до IGMPv3. Хост **может** позволить замену записи IGMPv3 Membership Record на Version 1 Membership Report или Version 2 Membership Report.

7.3. Поведение группового маршрутизатора

7.3.1. Присутствие запрашивающих со старой версией

Маршрутизаторы IGMPv3 могут размещаться в сетях, где имеется хотя бы один маршрутизатор, не обновленный до IGMPv3. В этом случае применяются следующие правила:

- Если в маршрутизаторах присутствуют более старые версии IGMP, запрашивающий **должен** использовать меньшую из версий IGMP, представленных в сети. Это требование должно быть реализовано на административном уровне - маршрутизаторы, желающие быть совместимыми с IGMPv1 и IGMPv2, **должны** иметь конфигурационную опцию для работы в режиме совместимости IGMPv1 или IGMPv2. При работе в режиме IGMPv1 маршрутизаторы **должны** передавать сообщения Periodic Query с Max Resp Code = 0,

усечённые по полю Group Address (т. е., размером 8 байтов), а также **должны** игнорировать сообщения Leave Group. Им также **следует** выдавать предупреждения при получении запросов IGMPv2 или IGMPv3, но частота генерации таких предупреждений **должна** быть ограничена. При работе в режиме IGMPv2 маршрутизаторы **должны** передавать сообщения Periodic Query, усечённые по полю Group Address (т. е., размером 8 байтов) и им также **следует** генерировать предупреждения при получении запросов IGMPv3 (частота таких предупреждений **должна** быть ограничена). Они также **должны** заполнять поля Max Resp Time с Max Resp Code (т. е., описанный в параграфе 4.1.1 экспоненциальный алгоритм не используется).

- Если маршрутизатор не настроен явно на использование IGMPv1 или IGMPv2 и получает сообщение IGMPv1 Query или IGMPv2 General Query, ему **следует** зафиксировать предупреждение. Частота таких предупреждений **должна** быть ограничена.

7.3.2. Присутствие членов групп со старой версией

Маршрутизаторы IGMPv3 могут размещаться в сетях с хостами, ещё не обновлёнными до IGMPv3. Для обеспечения совместимости со старыми версиями маршрутизаторы IGMPv3 **должны** работать в режиме совместимости с версией 1 или 2. Маршрутизаторы IGMPv3 сохраняют режимы совместимости по группам. Режим для группы определяется из переменной Group Compatibility Mode, которая может принимать одно из трёх значений: IGMPv1, IGMPv2, IGMPv3. Переменная хранится для групповой записи и зависит от версии сообщения Membership Report, принятого для данной группы, и таймера Older Version Host Present для этой группы.

Для беспроблемного переключения между версиями IGMP маршрутизатор поддерживает для каждой групповой записи таймеры IGMPv1 Host Present и IGMPv2 Host Present. Для таймера IGMPv1 Host Present устанавливается значение Older Version Host Present Timeout (в секундах) при получении IGMPv1 Membership Report. Для таймера IGMPv2 Host Present устанавливается значение Older Version Host Present Timeout (в секундах) при получении IGMPv2 Membership Report.

Режим Group Compatibility Mode для групповой записи меняется при получении отчёта более старой (по сравнению с текущим режимом) версии или по завершению отсчёта таймеров. Когда завершается отсчёт таймера IGMPv1 Host Present, маршрутизатор меняет режим Group Compatibility на IGMPv2, если запущен таймер IGMPv2 Host Present. Если запущенного таймера IGMPv2 Host Present нет, маршрутизатор меняет режим Group Compatibility на IGMPv3. При завершении отсчёта таймера IGMPv2 Host Present и отсутствии запущенного таймера IGMPv1 Host Present маршрутизатор меняет режим Group Compatibility на IGMPv3. Отметим, что при возврате для группы режима IGMPv3 требуется некоторое время на восстановление данных состояния, связанного с источниками. Специфичная для источников информация будет определяться следующим запросом General Query, но источники, которые следует блокировать, не будут блокироваться в течение интервала [Group Membership Interval] после него.

Значение переменной Group Compatibility Mode определяется версией наиболее старого отчёта из числа принятых за последний интервал Older Version Host Present Timeout (в секундах). Выбор значения Group Compatibility Mode показан в таблице.

Режим совместимости группы	***Состояние таймера***
IGMPv3 (по умолчанию)	Таймеры IGMPv2 Host Present и IGMPv1 Host Present не запущены
IGMPv2	Таймер IGMPv2 Host Present запущен, а IGMPv1 Host Present не запущен
IGMPv1	Таймер IGMPv1 Host Present запущен

Если маршрутизатор получает отчёт, требующий обновить таймеры Host Present и, соответственно, поменять режим совместимости, ему **следует** переключить режим совместимости незамедлительно.

В режиме совместимости для группы (Group Compatibility Mode) IGMPv3 маршрутизатор использует для данной группы протокол IGMPv3.

В режиме совместимости IGMPv2 маршрутизатор транслирует сообщения IGMPv2 в эквиваленты IGMPv3:

Сообщение IGMPv2	***Эквивалент IGMPv3***
Report	IS_EX({})
Leave	TO_IN({})

Сообщения IGMPv3 BLOCK игнорируются, как и списки источников в сообщениях TO_EX() (т. е., любое сообщение TO_EX() трактуется, как TO_EX({})).

В режиме совместимости IGMPv1 маршрутизатор транслирует сообщения IGMPv1 и IGMPv2 в их эквиваленты IGMPv3:

Сообщение IGMP	***Эквивалент IGMPv3***
v1 Report	IS_EX({})
v2 Report	IS_EX({})

В дополнение к игнорированию сообщений IGMPv3 BLOCK и списков источников в TO_EX(), как в режиме совместимости IGMPv2, игнорируются сообщения IGMPv2 Leave и IGMPv3 TO_IN().

8. Список таймеров и счётчиков, значения по умолчанию

Многие из упомянутых здесь таймеров являются настраиваемыми. Если используются отличные от принятых по умолчанию настройки, они **должны** быть согласованными между всеми системами на одном канале. В описаниях ниже скобки используются для группировки выражений.

8.1. Переменная Robustness

Переменная Robustness обеспечивает возможность тонкой настройки в соответствии с ожидаемой частотой потери пакетов в сети. Если предполагается высокий уровень потерь, значение Robustness можно увеличить. Протокол IGMP устойчив к потере (Robustness - 1) пакетов. Для переменной Robustness **недопустимо** устанавливать значение 0 и **не следует** использовать значение 1. По умолчанию используется значение 2.

8.2. Интервал между запросами

Параметр Query Interval определяет интервал между сообщениями General Query, передаваемыми запрашивающим (Querier). По умолчанию используется интервал 125 секунд.

Меняя [Query Interval], администратор может регулировать число сообщений IGMP в сети. При увеличении интервала запросы IGMP будут передаваться реже.

8.3. Интервал между откликами

Значение Max Responder Time используется для расчёта кода Max Resp Code, включаемого в периодические сообщения General Query. По умолчанию используется значение 100 (10 секунд).

Меняя [Query Responder Interval], администратор может настроить уровень всплесков для сообщений IGMP в сети. Большие значения будут снижать уровень всплесков трафика, поскольку отклики хостов будут распределены по более длинным интервалам. Число секунд, определяемое значением [Query Responder Interval], должно быть меньше [Query Interval].

8.4. Интервал принадлежности к группе

Значение Group Membership Interval определяет интервал, по истечении которого групповой маршрутизатор может принять решение об отсутствии членов в группе или прослушивающих конкретный источник в сети.

Это значение **должно** быть равно ((Robustness) * (Query Interval)) + (Query Responder Interval).

8.5. Интервал присутствия других запрашивающих

Значение Other Querier Present Interval определяет интервал, по истечении которого групповой маршрутизатор может принять решение об отсутствии других групповых маршрутизаторов, которым следует быть запрашивающими. Это значение **должно** быть равно ((Robustness) * (Query Interval)) + (½ Query Responder Interval).

8.6. Интервал стартового запроса

Значение Startup Query Interval определяет интервал между сообщениями General Query передаваемыми запрашивающим (Querier) при старте. По умолчанию используется значение 1/4 от Query Interval.

8.7. Счётчик стартовых запросов

Счётчик Startup Query Count показывает число стартовых запросов, разделённых интервалами Startup Query Interval. По умолчанию равно значению переменной Robustness.

8.8. Интервал запроса последнего участника

Параметр Last Member Query Interval определяет значение Max Responder Time, используемое для расчёта кода Max Resp Code, помещаемого в запросы Group-Specific Query, которые передаются в ответ на сообщения Leave Group. Он же определяет значение Max Responder Time, используемое при расчёте кода Max Resp Code для сообщений Group-and-Source-Specific Query. По умолчанию используется значение 10 (1 секунда).

Отметим, что для LMQI > 128 (12,8 сек.) может быть представлен ограниченный набор значений, соответствующих последовательным значениям Max Resp Code. При преобразовании заданного конфигурацией времени в Max Resp Code рекомендуется использовать, по возможности, точное значение или следующее меньшее значение, если запрошенное не имеет точного представления.

Это значение можно подстраивать для изменения «задержки» в сети. Меньшие значения уменьшают время обнаружения потери последнего участника группы или источника.

8.9. Счётчик запросов последнего участника

Значение Last Member Query Count определяет число запросов Group-Specific, передаваемых до того, как маршрутизатор примет решение об отсутствии локальных членов группы. Это же значение определяет число запросов Group-and-Source-Specific, передаваемых до того, как маршрутизатор примет решение об отсутствии получателей для конкретного источника. По умолчанию используется значение переменной Robustness.

8.10. Время запроса последнего участника

Last Member Query Time определяется произведением Last Member Query Interval и Last Member Query Count. Само значение не является настраиваемым, но его можно подобрать, меняя значения сомножителей.

8.11. Интервал незапрошенных отчётов.

Значение Unsolicited Report Interval определяет временной интервал между повторами изначальных отчётов. о принадлежности к группе. По умолчанию - 1 секунда.

8.12. Тайм-аут присутствия запрашивающего старой версии

Older Version Querier Interval определяет тайм-аут для возврата хоста в режим IGMPv3 после того, как он получил запрос старой версии. При получении такого запроса хосты устанавливают для своего таймера Older Version Querier Present Timer значение Older Version Querier Interval.

Это значение **должно** определяться выражением (Robustness) * (Query Interval из последнего запроса) + (Query Responder Interval).

8.13. Интервал присутствия старых хостов

Older Host Present Interval определяет тайм-аут для возврата группы в режим IGMPv3 после того, как для этой группы был передан отчёт старой версии. При получении такого отчёта маршрутизаторы устанавливают для своего таймера Older Host Present Timer значение Older Host Present Interval.

Это значение **должно** определяться выражением (Robustness) * (Query Interval) + (Query Responder Interval).

8.14. Настройка таймеров

В этом разделе приводятся рекомендации для сетевых администраторов по настройке описанных выше параметров в их сетях. Некоторые реализации маршрутизаторов могут устанавливать эти параметры динамически в соответствии с изменением характеристик сети.

8.14.1. Переменная Robustness

Переменная Robustness позволяет настроить IGMP в соответствии с ожидаемым уровнем потерь в канале. IGMPv3 сохраняет устойчивость при потере (Robustness - 1) пакетов. Например, если для переменной Robustness используется принятое по умолчанию значение 2, IGMPv3 будет устойчив к потере 1 пакета, но может работать не эффективно при более высоком уровне потерь. В подсетях со значительными потерями значение Robustness следует увеличивать с учётом ожидаемого уровня потери пакетов. Однако при увеличении значения переменной Robustness для подсети увеличивается время реакции на прекращение прослушивания источника или группы последним участником.

8.14.2. Интервал между запросами

Общий уровень периодического трафика IGMP обратно пропорционален значению Query Interval. Увеличение интервала между запросами снижает суммарный трафик IGMP. Значение Query Interval **должно** быть на меньше значения поля Max Responder Time, помещаемого в сообщения General Query.

8.14.3. Максимальное время отклика

Всплески трафика IGMP обратно пропорциональны значению Max Responder Time. Увеличение Max Responder Time будет увеличивать интервалы между сообщениями Report, однако при больших Max Responder Time в запросах Group-Specific и Source-and-Group-Specific будет возрастать время реакции на прекращение прослушивания источника или группы последним участником. Ожидаемая частота передачи сообщений Report может быть рассчитана путём деления ожидаемого числа передающих сообщения Report на величину Max Responder Time. Значение Max Responder Time может рассчитываться динамически с использованием ожидаемого числа отправителей отчётов. для данного запроса в соответствии с приведённой таблицей.

Тип запроса	*Ожидаемое число рапортующих*
General Query	Все системы в подсети.
Group-Specific Query	Все системы в подсети, которые выразили заинтересованность в группе
Source-and-Group-Specific Query	Все системы в подсети, которые выразили заинтересованность в источнике и группе

Маршрутизатор не обязан рассчитывать число рапортующих или динамически подстраивать Max Responder Time.

9. Вопросы безопасности

Рассматриваются воздействия поддельных сообщений каждого типа и описывается применение IPSEC AH для аутентификации сообщений, если она желательна.

9.1. Обманные сообщения Query

Обманное сообщение Query от машины, чей адрес IP меньше адреса текущего запрашивающего будет приводить к передаче функций Querier этой машине. Если обманщик больше не передаёт сообщений Query, отсчёт таймера Other Querier Present на другом маршрутизаторе будет завершён через какое-то время и роль Querier будет возвращена. В течение срока действия обмана, если обманщик игнорирует сообщения Leave, трафик может поступать в пустые группы вплоть до [Group Membership Interval].

С помощью обманных запросов Group-and-Source-Specific может быть организована DoS-атака на хост. Атакующий может узнать о принадлежности конкретного хоста к группам с помощью обычного запроса. После этого он может отправить большое число запросов Group-and-Source-Specific, каждый из которых включает большое число источников и большое значение Maximum Responder Time. Хост будет сохранять и поддерживать источники, указанные во всех этих запросах, пока не будет передан отложенный отклик. Это может приводить к значительному расходу памяти и ресурсов процессора для объединения записанных источников со списками источников, включёнными в последующие запросы.

Для защиты от таких DoS-атак реализация хоста может ограничивать число запросов Group-and-Source-Specific в расчёте на принадлежность к группе в течение интервала времени и/или записывать только ограниченное число источников.

Обманные запросы из локальной сети легко отследить. Для защиты от внешних запросов ниже даны 3 рекомендации:

- маршрутизаторам **не следует** пересылать запросы; это проще обеспечить при наличии в запросах опции Router-Alert;
- хостам **следует** игнорировать запросы версий 2 и 3 без опции Router-Alert;
- хостам **следует** игнорировать сообщений General Query версий 1, 2 и 3, отправленные на групповой адрес, отличающийся от 224.0.0.1 (все системы).

9.2. Обманные сообщения Current-State Report

Обманные сообщения Report могут создавать у групповых маршрутизаторов ложные представления о наличии членов в группах, где реально никого нет. Обманные сообщения Report из локальной сети не имеют смысла, поскольку включение в группу не является привилегированной операцией и локальные пользователи могут добиться того же результата без применения обманных сообщений. Обманные сообщения Report из внешних источников представляют некоторую опасность. Ниже приведены два способа борьбы с такими сообщениями.

- Игнорировать сообщения Report, если адрес отправителя не относится к сети, связанной с принявшим пакет интерфейсом. Это приводит к тому, что сообщения Report от мобильных хостов без адресов из локальной сети будут игнорироваться. Сообщения Report с адресом отправителя 0.0.0.0 **следует** воспринимать во всех случаях.

- Игнорировать сообщения Report без опции Router Alert [RFC-2113] и требовать, чтобы маршрутизаторы не пересылали сообщений Report (это не является требованием обобщённой фильтрации на пути пересылки, поскольку в пакетах уже имеется опция Router Alert). Это решение не обеспечивает совместимости с реализациями IGMPv1 и ранними версиями IGMPv2, где не требуется опция Router Alert.

Обманное сообщение Report версии 1 может перевести маршрутизатор в состояние «присутствуют члены с версией 1» для конкретной группы, в результате чего маршрутизатор будет игнорировать сообщения Leave. Это может привести к передаче трафика в пустые группы на время до [Group Membership Interval]. Для решения этой проблемы можно ввести на маршрутизаторах конфигурационный параметр, обеспечивающий возможность полного игнорирования сообщений версии 1. Это решение будет блокировать автоматическую совместимость с хостами версии 1, поэтому его следует использовать лишь в ситуациях, где быстрый выход из группы имеет критически важное значение.

Обманное сообщение Report версии 2 может перевести маршрутизатор в состояние «присутствуют члены с версией 2» для конкретной группы, в результате чего маршрутизатор будет игнорировать сообщения IGMPv3 Source-Specific State. Это может вызывать потоки трафика из нежелательных источников в интервале времени до [Group Membership Interval]. Для решения этой проблемы можно ввести на маршрутизаторах конфигурационный параметр, обеспечивающий возможность полного игнорирования сообщений версии 2. Это решение будет блокировать автоматическую совместимость с хостами версии 2, поэтому его следует использовать лишь в ситуациях, где фильтрация источников имеет критически важное значение.

9.3. Обманные сообщения State-Change Report

Обманные сообщения State-Change Report могут заставить запрашивающего (Querier) передавать запросы Group-Specific или Source-and-Group-Specific для соответствующей группы. В результате на каждом маршрутизаторе и у всех членов группы будут выполняться ненужные операции, но нужный трафик теряться не будет. Для защиты от обманных сообщений State-Change Report имеется два способа, описанных ниже.

- Игнорировать сообщения State-Change Report, если адрес их отправителя не относится к сети, связанной с принявшим пакет интерфейсом. В этом случае сообщения State-Change Report от мобильных хостов без адреса в локальной подсети будут игнорироваться. Сообщения State-Change Report с адресом отправителя 0.0.0.0 **следует** воспринимать на любом интерфейсе.

- Игнорировать сообщения State-Change Report без опций Router Alert [RFC-2113] и требовать от маршрутизаторов отказа от пересылки сообщений State-Change Report (это не является требованием обобщённой фильтрации на пути пересылки, поскольку в пакетах уже есть опция Router Alert).

9.4. Использование IPSEC

В дополнение к описанным выше мерам может применяться IPSEC в режиме Authentication Header [AH] для защиты от удалённых атак. Этот метод позволяет убедиться в том, что сообщения IGMPv3 приходят от систем из ЛВС (точнее, от систем с правильным ключом). При использовании IPSEC сообщения, отправляемые по адресам 224.0.0.1 и 224.0.0.22 следует аутентифицировать с помощью AH. Применительно к ключам существует два варианта:

1. Использование симметричного алгоритма цифровой подписи с одним ключом для всей ЛВС (или отдельным ключом для каждой группы). Это позволяет убедиться в том, что пакет отправлен системой, имеющей нужный ключ. Однако системы, имеющие верный ключ, могут отправлять и обманные сообщения, точная аутентификация на уровне отдельных отправителей не представляется возможной. Кроме того, в этом случае требуется запрет IPSec Replay Protection (защита от повторного использования пакетов).

2. При разработке подходящего стандарта управления ключами можно использовать асимметричные алгоритмы цифровой подписи. Все системы должны знать открытые ключи всех маршрутизаторов, а маршрутизаторы - открытые ключи всех систем. Это требует множества операций по управлению ключами, но обеспечивает возможность аутентификации отдельного отправителя. Например, в результате использования такой защиты хост не сможет отправлять обманные сообщения, поскольку это будет разрешено только маршрутизаторам.

Описанное здесь решение напрямую применимо лишь к сообщениям Query и Leave в IGMPv1 и IGMPv2, поскольку сообщения Report передаются в группу, к которой они относятся, и не представляется возможным согласовать ключи для взаимодействия между хостами и маршрутизаторами для произвольных multicast-групп.

10. Взаимодействие с IANA

Для всех типов IGMP, описанных в этом документе, значения уже выделены в [IANA-REG].

11. Благодарности

Авторы благодарны Ran Atkinson, Luis Costa, Toerless Eckert, Dino Farinacci, Serge Fdida, Wilbert de Graaf, Sumit Gupta, Mark Handley, Bob Quinn, Michael Speer, Dave Thaler и Rolland Vida за их комментарии и предложения.

Отдельные фрагменты этого документа заимствованы из [RFC-1112] и [RFC-2236].

12. Нормативные документы

[AH] Kent, S. and R. Atkinson, "IP Authentication Header", RFC 2402, November 1998.

[IANA-REG] http://www.iana.org/assignments/igmp-type-numbers

[RFC-1112] Deering, S., "Host Extensions for IP Multicasting", STD 5, RFC 1112, August 1989.

[RFC-2113] Katz, D., "IP Router Alert Option," RFC 2113, February, 1997.

[RFC-2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC-2236] Fenner, W., "Internet Group Management Protocol, Version 2", RFC 2236, November 1997.

[RFC-3228] Fenner, B., "IANA Considerations for IPv4 Internet Group Management Protocol (IGMP)", BCP 57, RFC 3228, February 2002.

13. Дополнительная литература

[RFC-1071] Braden, R., Borman, D. and C. Partridge, "Computing the Internet checksum", RFC 1071, September 1988.

[FILTER-API] Thaler, D., B. Fenner, and B. Quinn, "Socket Interface Extensions for Multicast Source Filters", Work in Progress[1].

[SSM] Bhattacharyya, S., et. al., "An Overview of Source-Specific Multicast (SSM)", Work in Progress[2].

[MLD] Deering, S., Fenner, W. and B. Haberman, "Multicast Listener Discovery (MLD) for IPv6", RFC 2710, October 1999.

[MLDV2] Vida, R., L. Costa, S. Fdida, S. Deering, B. Fenner, I. Kouvelas, and B. Haberman, "Multicast Listener Discovery Version 2 (MLDv2) for IPv6", Work in Progress[3].

Приложение A. Обоснования

A.1 Необходимость сообщений State-Change

IGMPv3 задаёт два типа отчётов. о принадлежности к группам (Membership Report) - Current-State и State Change. В этом параграфе приведены обоснования использования обоих типов отчётов.

Маршрутизаторам требуется различать сообщения Membership Report, переданные в ответ на запросы от них и переданные в результате смены состояния на интерфейсе. Отчёты о принадлежности к группам, передаваемые в ответ на сообщения Membership Query служат главным образом для обновления имеющегося на маршрутизаторе состояния и само состояние при этом обычно не меняется. Передаваемые в ответ на смену состояния на интерфейсе сообщения Membership Report требуют от маршрутизаторы выполнения тех или иных действий (см. параграф 6.4).

Если не будет возможности различать эти два типа отчётов., маршрутизатор будет вынужден трактовать все сообщения Membership Report, как возможные смены состояния и это приведёт к избыточной нагрузке на маршрутизатор, а также увеличит уровень трафика IGMP в сети.

A.2 Отмена отправки отчётов. хостами

В IGMPv1 и IGMPv2 хост будет прекращать отправку ожидающих отчётов. о принадлежности к группам, если увидит подобный отчёт от другого члена группы в своей сети. В IGMPv3 такая возможность была удалена. Ниже приведены причины отказа.

1. У маршрутизаторов может возникать потребность в отслеживании на своих интерфейсах статуса принадлежности к группам на уровне хостов. Это позволяет маршрутизаторам реализовать быстрый выход из групп (например, для многоуровневых систем контроля насыщения multicast-трафика), а также отслеживать принадлежность к группам в целях учёта услуг.
2. Подавление сообщений Membership Report недостаточно хорошо работает в ЛВС на основе мостов. Многие мосты и коммутаторы уровня 2 и 3, поддерживающие отслеживание IGMP (IGMP snooping), не пересылают сообщения IGMP в другие сегменты ЛВС для предотвращения «подавления отчётов.». Отказ от такого подавления упростит работу таких устройств.
3. Отказ от подавления отчётов. о принадлежности к группам снизит число обрабатываемых хостами сообщений и, следовательно, упростит реализацию машины состояний.
4. В IGMPv3 один отчёт о принадлежности к группам содержит записи для множества multicast-групп в целях снижения числа передаваемых сообщений. В предыдущих версиях IGMP отчёт для каждой группы передавался в отдельном сообщении.

A.3 Переключение режима фильтрации с EXCLUDE на INCLUDE

При наличии в сети для одной группы хостов с режимами фильтрации EXCLUDE и INCLUDE маршрутизатор должен использовать режим EXCLUDE (см. параграф 6.2.1). В режиме EXCLUDE маршрутизатор пересылает трафик от всех источников, за кроме тех, которые указаны в списке исключений. Если хостов с режимом фильтрации EXCLUDE больше нет, маршрутизатору желательно переключиться в режим INCLUDE без прерывания трафика остающихся получателей.

Одним из способов решения этой задачи является отслеживание маршрутизаторами всех источников, желаемых для хостов с режимом фильтрации INCLUDE, даже в тех случаях, когда сам маршрутизатор работает в режиме

[1]Работа опубликована в RFC 3678. *Прим. перев.*
[2]Работа опубликована в RFC 3569. *Прим. перев.*
[3]Работа опубликована в RFC 3810. *Прим. перев.*

фильтрации EXCLUDE. Если отсчёт таймера для группы завершается в режиме EXCLUDE, это означает, что в сети больше нет хостов с режимом EXCLUDE (иначе отчёты о принадлежности к группе от таких хостов обновляли бы таймер для группы). Маршрутизатор может аккуратно переключиться в режим фильтрации INCLUDE, сохранив источники, для которых в настоящее время выполняется пересылка, в своём списке источников.

Приложение B. Изменения по сравнению с IGMPv2

Хотя основным отличием IGMPv3 является добавление фильтрации источников, имеется ещё ряд отличий от RFC 2236, перечисленных ниже.

- Состояния поддерживаются для группы и списка источников, а не просто для группы, как в IGMPv2.
- Взаимодействие с системами IGMPv1 и IGMPv2 определено, как операции с состоянием IGMPv3.
- Изменён сервисный интерфейс IP для поддержки спецификаций списков источников.
- Запрашивающий включает свои значения Robustness и Query Interval в пакеты Query для синхронизации этих переменных на системах, не являющихся Querier.
- Max Responder Time в сообщениях Query меняется экспоненциально в диапазоне от 25,5 секунд до 53 минут для использования на каналах с очень большим числом систем.
- Хост повторяет сообщения о смене состояния для повышения отказоустойчивости.
- Определены дополнительные разделы данных для будущих расширений.
- Пакеты отчётов. передаются по адресу 224.0.0.22 для обеспечения коммутаторам уровня 2 возможности «перехвата».
- Пакеты отчётов. могут содержать множество групповых записей с целью снижения числа передаваемых пакетов.
- «Подавление» хостов больше не применяется с целью упрощения реализаций и обеспечения возможности явного отслеживания принадлежности к группам.
- Новый флаг Suppress Router-Side Processing (S) в сообщениях Query решает проблему отказоустойчивости в присутствии IGMPv2.

Адреса авторов

Brad Cain
Cereva Networks

Steve Deering
Cisco Systems, Inc.
170 Tasman Drive
San Jose, CA 95134-1706
Phone: +1-408-527-8213
EMail: deering@cisco.com

Bill Fenner
AT&T Labs - Research
75 Willow Rd.
Menlo Park, CA 94025
Phone: +1-650-330-7893
EMail: fenner@research.att.com

Isidor Kouvelas
Cisco Systems, Inc.
170 Tasman Drive
San Jose, CA 95134-1706
Phone: +1-408-525-0727
EMail: kouvelas@cisco.com

Ajit Thyagarajan
Ericsson IP Infrastructure

Перевод на русский язык
Николай Малых
nmalykh@protokols.ru

Полное заявление авторских прав

Подтверждение

Финансирование функций RFC Editor обеспечено Internet Society.