

В данном уроке будут рассмотрены две заключительные темы данного курса:

- Маршрутизация Multicast
- IP версии 6

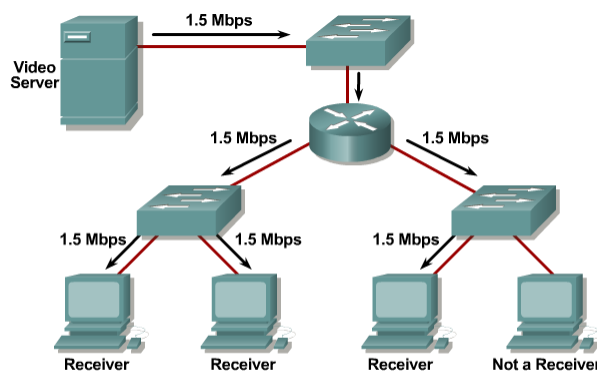
Современные мультимедийные приложения интегрируют звук, графику, анимацию, текст, видео. Такого типа приложения сегодня стали эффективным средством корпоративного общения. Однако, отправка таких мультимедийных данных в сети кампуса требует большой пропускной способности. IP Multicast является эффективным способом доставить мультимедийные данные для многих узлов в одном IP потоке. IP Multicast использует специальные стандарты адресации, а также методы для определения членов Multicast групп, отправителей и Multicast протоколов маршрутизации. Вы можете использовать Cisco IOS command line interface (CLI) для конфигурации IP multicast на устройствах Cisco.

Этот урок содержит детальный обзор технологий IP multicast и содержит следующие основные разделы:

1. Основные принципы Multicast
2. IGMP and Layer 2
3. Multicast Протоколы маршрутизации
4. Multicast настройка и проверка

### 1.1 Базовая концепция Multicast

Multicast можно использовать, чтобы отправить пакеты с данными многим получателям. К примеру мультимедийный сервер отправляет одну копию каждого пакета с единственным IP адресом назначения, этот пакет могут получить многие конечные узлы, если они готовы принимать и обрабатывать пакет, отправленный этот специальный адрес.



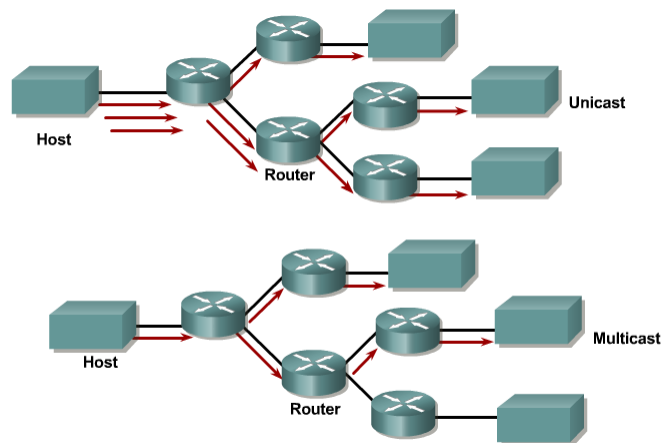
A multicast server sends out a single data stream to multiple clients using a special multicast address.

На рисунке видео-сервер передает единственный видео-поток к набору устройств, прослушивающих специфический групповой адрес. Используется только 1.5 Mbps пропускной способности сети, несмотря на число получателей. Посылая пакеты данных ко многим получателям, эти пакеты не дублируются для каждого получателя но отправляются единственным потоком, где конечные роутеры увеличивают количество этих пакетов для получателей, когда это необходимо. При этом роутеры обрабатывают меньше пакетов, нежели при обычной unicast передаче данных, потому что они получают только единственную копию пакета. Поскольку конечные роутеры выполняют увеличение количества пакетов для доставки их получателям, отправитель, или источник группового вещания, не нуждается в знании unicast адресов всех получателей.

Некоторые сетевые технологии (например, webcasting) используют “push” метод, чтобы доставить одни и те же данные ко многим пользователям. Вместо пользователя, кликающего по линкам, для получения данных, данные доставляется автоматически. Пользователям только один раз придется подписаться на канал, чтобы получить данные; после этого, данные периодически отправляются к пользователю. Проблема с webcast есть, это транспортировка которая все еще выполняющееся с использованием unicast.

### 1.2 Unicast против Multicast

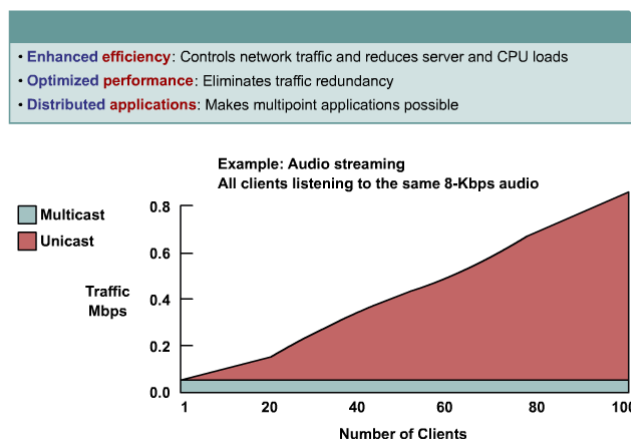
При передаче unicast посылается множество копии данных, одна копия для каждого получателя.



Unicast пример на рисунке показывает передачу, в которой три копии данных отправляются от узла, и сеть отправляет каждый пакет отдельно к трем получателям. Узел, может, отправлять данные только одному получателю за один раз, потому что придется создать различные пакеты с разными адресами назначения для каждого получателя. При групповой передаче, данные отправляются в единственной копии для многих получателей. Данные отправленные многим получателям потому, что получатели заранее подписались на них. Пример, показанный на рисунке, показывает передачу данных от узла, и это ОДНА копия данных, сеть передает эти данные в единственной копии, и только на последнем роутере размножает их. Каждый пакет существует только в единственной копии на любом участке сети. Ближайшие к клиенту роутеры повторяют и передают пакет с данными через несколько интерфейсов, если в этом есть необходимость.

### 1.3 Преимущества и недостатки Multicast

Multicast передача обеспечивает много преимуществ по сравнению с unicast в случае передачи одной-ко-многим или многие-ко-многим.



- Расширенная эффективность: сетевая пропускная способность используется эффективнее, потому что множественные потоки данных заменяются единственной передачей.
- Оптимизированная производительность: меньше копий данных, требующих отправки и обработки.
- Распределенные приложения: распределенные приложения не будут работать с unicast, потому что unicast передача не масштабируется (уровень трафика и количество клиентов можно считать по пропорции 1:1).

Есть другие преимущества:

- При эквивалентной отправки группового трафика, отправитель использует меньше производительности и пропускную способность.
- Групповые пакеты не требуют высокой пропускной способности как unicast пакеты, и они прибывают к получателям почти одновременно.
- Multicast дает целый ряд новых приложений, которые не возможны при unicast (например, видео по запросу [VoD]).

Существуют также некоторые недостатки multicast, которые должны быть рассмотрены. Большинство multicast приложений основаны на User Datagram Protocol (UDP). Это дает возможность избавиться от некоторых нежелательных последствий, по сравнению с аналогичными unicast приложениями использующими TCP.

Multicast на основе UDP:

- Самая быстрая доставка, но иногда пакет пропадает. Многие многоадресные приложений, работающие в режиме реального времени (например, видео и аудио), могут быть затронуты этими потерями. Кроме того, запрос повторной передачи данных в таком случае не представляется возможным.
- В результате большого количества потерь данных голос становится прерывистым, теряются слова, это может сделать содержание непонятным
- В случае передачи видео, большое количество потерь пакетов приводит к тому, что человеческий глаз видит "артефакты" в изображении. Тем не менее, некоторые алгоритмы сжатия могут серьезно пострадать даже от незначительных потерь пакетов, это приводит к тому что видео становится прерывистым или останавливается на несколько секунд.
- Отсутствие контроля перегрузок при работе UDP может привести к плохо контролируемой перегрузке сети.
- Повторяющиеся пакеты иногда могут быть получены из-за изменений Multicast топологии сети. Приложение должно ожидать случайно дублировавшиеся пакеты и должным образом обрабатывать их.
- Несвоевременная доставка пакетов может также произойти и в ходе изменения топологии сети или других сетевых событий, которые влияют на поток Multicast трафика.
- UDP не имеет механизмов надежности, поэтому вопросы надежности должны быть решены в рамках применения Multicast силами приложений
- Проблема ограничения Multicast трафика только выбранной группе получателей, иными словами, появляется возможность перехвата трафика посторонними узлами
- Использование некоторых коммерческих приложений становится невозможным, когда вопросы надежности и безопасности не решены (например, финансовые данные).

#### 1.4 Multicast приложения

Существуют различные типы многоадресных приложений. Вот три наиболее распространенные модели:

- One-to-many (Один-ко-многим) - когда один отправитель посылает данные ко многим получателям, такого рода приложений могут быть использованы для аудио и видео распределения, объявлений, мониторинга и так далее. Если один-ко-многим приложению потребуется обратная связь с получателями, оно становится многие-ко-многим.
- Many-to-many (Многие-ко-многим) - где хост может быть отправителем и получателем, или случаи, где два или более получателей также выступают в качестве отправителей. При этом получение данных из нескольких источников повышает сложность приложений и создает различные проблемы в области управления.
- Many-to-one (Многие-к-одному)- где многие получатели передают данных на одного отправителя, используется финансовыми приложениями. Другие виды использования: сбор данных, аукционов и голосования.

Много новых многоадресных приложений появляются и спрос на них растет.

К примеру:

- Live TV and radio broadcast to the desktop
- Corporate broadcast
- Distance learning
- Multicast file transfer data and file replication
- Training
- Video conferencing
- Video-on-demand
- Whiteboard/collaboration
- Real-time data delivery-financial

#### 7.1.5 Multicast IP адресация

Роутеры отличают трафик Multicast от Unicast, используя зарезервированный класс D IP адресов.

|         |   |   |   |   |                    |
|---------|---|---|---|---|--------------------|
| 28 Bits |   |   |   |   |                    |
| Class D | 1 | 1 | 1 | 0 | Multicast Group ID |

Рис. 1  
Рис. 2

| Class D First Octet |   |   |   |     |   |   |   | Multicast Addresses         |
|---------------------|---|---|---|-----|---|---|---|-----------------------------|
| 1                   | 1 | 1 | 0 | 0   | 0 | 0 | 0 | 224.0.0.0 – 224.255.255.255 |
| 1                   | 1 | 1 | 0 | 0   | 0 | 0 | 1 | 225.0.0.0 – 225.255.255.255 |
| 1                   | 1 | 1 | 0 | 0   | 0 | 1 | 0 | 226.0.0.0 – 226.255.255.255 |
| 1                   | 1 | 1 | 0 | ... |   |   |   | 227.0.0.0 – 227.255.255.255 |
| 1                   | 1 | 1 | 0 | ... |   |   |   | 237.0.0.0 – 237.255.255.255 |
| 1                   | 1 | 1 | 0 | 1   | 1 | 1 | 0 | 238.0.0.0 – 238.255.255.255 |
| 1                   | 1 | 1 | 0 | 1   | 1 | 1 | 1 | 239.0.0.0 – 239.255.255.255 |

Сетевые устройства могут быстро определить класс D IP адресов посмотрев на первые 4 старших бита, которые всегда равны 1110. Последующие 28 бит в адресе класса D есть адрес группы (рис.1). Так что диапазон multicast IP адресов от 224.0.0.0 до 239.255.255.255 (рис.2). Адресное пространство multicast IP адресов разделено на следующие группы:

| Description                 | Range                        |
|-----------------------------|------------------------------|
| Reserved link local address | 224.0.0.0 to 224.0.0.255     |
| Globally scoped addresses   | 224.0.1.0 to 238.255.255.255 |
| Limited scope addresses     | 239.0.0.0 to 239.255.255.255 |

Локальные области действия адреса (Reserved link local):

- Резервированы Internet Assigned Numbers Authority (IANA) для сетевых протоколов.
- Адресное пространство от 224.0.0.0 до 224.0.0.255
- Multicast в этом диапазоне никогда не пересекает границ маршрутизаторов. Вне зависимости от TTL, поэтому TTL обычно устанавливают равное в 1

| Address    | Description  |
|------------|--|
| 224.0.0.1  | All multicast systems on a subnet                              |
| 224.0.0.2  | All multicast routers on a subnet                              |
| 224.0.0.4  | All Distance Vector Multicast Routing Protocol (DVMRP) routers |
| 224.0.0.5  | All OSPF routers   |
| 224.0.0.6  | All OSPF designated routers (DRs)                              |
| 224.0.0.9  | All RIPv2 routers  |
| 224.0.0.10 | All EIGRP routers  |
| 224.0.0.13 | All PIMv2 routers  |

Globally scoped addresses:

- Выделяются динамически через интернет
- Диапазон адресов от 224.0.0.0 до 238.255.255.255
- Диапазон 224.2.x.x используется приложениями Multicast Backbone (Mbone). Mbone это множество маршрутизаторов интернета которые поддерживают IP multicasting для различных публичных и частных аудио и видео программ. Mbone был организован IETF.

Limited (administratively) scoped addresses:

- Резервирован для использования в частных доменах, также как частное адресное пространство IP, которое используется внутри одной организации, адреса ограниченной или административной области действия, ограничены одной локальной группой или организацией.
- Адресное пространство в диапазоне от 239.0.0.0 до 239.255.255.255
- Организации могут использовать адреса ограниченной области для локальных multicast приложений, которые не будут маршрутизироваться через интернет.

Внутри автономной системы или домена, адреса этой области могут быть далее разделены на диапазоны. Это разделение называется разделением адресов на области и позволяет повторно использовать адреса внутри меньших доменов. Административно разделенное multicast адресное пространство делится на следующие области:

- Локальную область организации 239.192.0.0 по 239.251.255.255
- Локальная область сайта (239.255.0.0/16, также 239.252.0.0/16, 239.253.0.0/16, и 239.254.0.0/16 также зарезервировано)

## 1.6 Multicast адресация второго уровня

Как маршрутизаторы или коммутаторы определяют соответствие multicast IP-адреса к мас-адресу? Обычные сетевые интерфейсы в сегменте LAN получают только пакеты предназначенные для их встроенного мас-адреса. Тем не менее не существует эквивалента ARP для мультикаст адресов вместо этого IANA выделила специальный идентификатор OUI что бы определять multicast мас-адреса. Multicast мас-адреса всегда начинаются с бита 0x01 в первом октете, точнее префикс 0x01005e (+следующий младший бит который тоже равен 0) зарезервирован для определения соответствия IP- multicast к мас-адресу. Полный диапазон multicast мас-адресов: 0100.5e00.0000 по 0100.5e7f.ffff.(Рис.1)

Рис.1

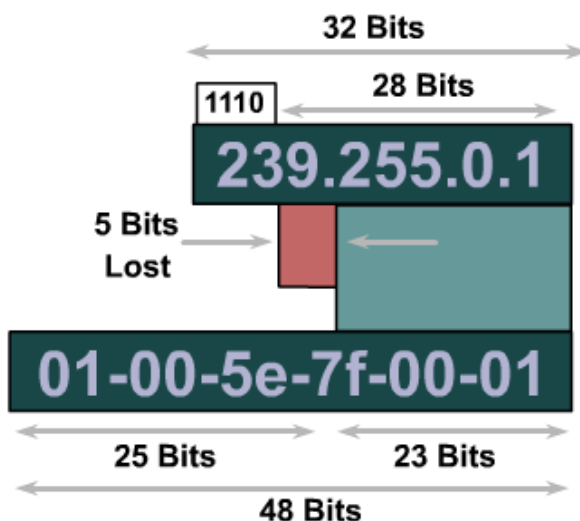
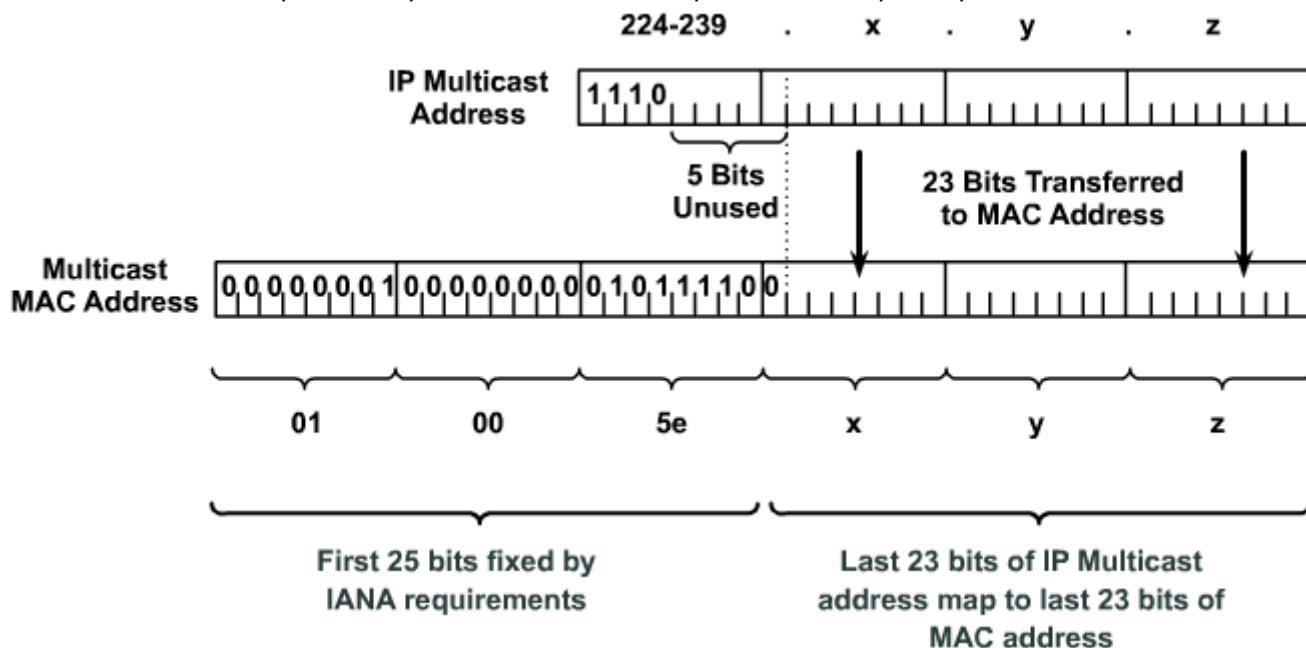


Рис.2

Таким образом первые 25 бит мас-адреса имеют фиксированное значение а следующие



23 бита соответствуют последним 23 битам IP-адреса multicast группы. (рис.2)

Что бы осуществить перевод multicast IP-адреса в mac-адрес записываем последние 23 бита multicast IP-адреса в младшие 23 бита mac-адреса. В multicast IP-адресе есть 28 уникальных битов (всего 32, первые 4 всегда 1110), а в mac-адрес транслируется только 23 бита таким образом 5 бит в IP-адресе не используются и не включаются в mac-адрес. Значит есть 5 бит которые перекрываются (не используется).

|                    |                    |                    |                    |                    |
|--------------------|--------------------|--------------------|--------------------|--------------------|
| <b>224.10.0.1</b>  | <b>225.10.0.1</b>  | <b>226.10.0.1</b>  | <b>227.10.0.1</b>  | <b>228.10.0.1</b>  |
| <b>229.10.0.1</b>  | <b>230.10.0.1</b>  | <b>231.10.0.1</b>  | <b>232.10.0.1</b>  | <b>233.10.0.1</b>  |
| <b>234.10.0.1</b>  | <b>235.10.0.1</b>  | <b>236.10.0.1</b>  | <b>237.10.0.1</b>  | <b>238.10.0.1</b>  |
| <b>239.10.0.1</b>  | <b>224.138.0.1</b> | <b>225.138.0.1</b> | <b>226.138.0.1</b> | <b>227.138.0.1</b> |
| <b>228.138.0.1</b> | <b>229.138.0.1</b> | <b>230.138.0.1</b> | <b>231.138.0.1</b> | <b>232.138.0.1</b> |
| <b>233.138.0.1</b> | <b>234.138.0.1</b> | <b>235.138.0.1</b> | <b>236.138.0.1</b> | <b>237.138.0.1</b> |
| <b>238.138.0.1</b> | <b>239.138.0.1</b> |                    |                    |                    |

Рис.3

В результате 2 или более разных multicast IP-адресов могут отображаться на один и тот же mac-адрес. Например 224.1.1.1 и 225.1.1.1 отображает на один mac-адрес. Если пользователь 1 подписался на группу А с IP-адресом 224.1.1.1 и пользователь 2 подписался на группу В 225.1.1.1 то они оба будут получать потоки А и В на канальном уровне. Тем не менее на 3 уровне они оба будут видеть только потоки их multicast группы, (так как их multicast IP-адреса разные). Это дает нам возможность иметь 32 различных multicast IP-адреса, которые будут соответствовать одному multicast mac-адресу. Например: все multicast IP-адреса на рис. 3 получают один mac-адрес 01-00-5e-0a-00-01. Сетевые администраторы должны принимать это во внимание когда назначают multicast IP-адреса.

### 1.7 Multicast сессии

Когда запускается multicast приложение на узле получателе, это приложение должно знать к каким multicast группам подключаться. Это приложение должно узнать все доступные сессии или потоки которые обычно соответствуют одной или более IP multicast группам.

Есть несколько способов, как приложение может узнать о multicast сессиях:

- Приложение вступает в общеизвестную, заранее заданную multicast группу; в которой анонсируются доступные сессии
- Приложение связывается с соответствующим сервером каталога
- Приложение запускается с web страницы, на которой доступные сессии отображаются как URL. Можно также использовать e-mail.
- Пользователь сам настраивает приложение для прослушивания определенной multicast сессии, вручную вводя IP- multicast адрес в приложение.

Приложение session directory (SD) (каталог сессий) работает путеводителем и показывает multicast содержимое (контент), клиентское приложение запускается на PC и показывает пользователю какой контент доступен. Это приложение использует каталог или Session Description Protocol (SDP) или Session Announcement Protocol (SAP) чтобы узнать какой контент доступен.

Примечание: И приложения SD и SDP иногда называются SDR или sdr в документации cisco SDP/SAP называются sdr.

Само приложение SD служит для анонсирования доступных сессий и помогает созданию новых сессий. Изначально приложение SD было переработано в приложение SDP (которое в этом курсе называется SDR), приложение SDR позволяет следующее использование:

- Описание сессий и их анонсирование
- Транспортировка анонсов сессии через общеизвестные multicast группы

224.2.127.254

- Создание новых сессий

На получателе SDR узнает про доступные группы и сессии, если пользователь кликает на иконке multicast потока в списке SRD, то он пытается подключиться к этой multicast группе.

На отправителе SDR создает новые сессии и избегает конфликтов IP-адресов. Отправитель во время создания сессии связывается с соответствующим кешем SDR (отправитель также получатель) и выбирает один из неиспользуемых multicast IP-адресов,



когда сессия создана отправитель начинает анонсировать ее вместе со всей информацией, необходимой получателю чтобы успешно вступить в сессию.

RFC 3266, который определяет SDP, определяет стандартный набор переменных которые описывают сессию, большинство таких переменных унаследованы от SDR. Сам транспорт не определен в RFC. Есть несколько механизмов пересылки пакетов описывающих сессии через multicast сеть:

- SAP определен в RFC2974 переносит информацию о сессии
- SIP определен в RFC2543 это сигнальный протокол для интернет конференций, телефонии, уведомления о присутствии, событиях и мгновенных сообщений.
- RTSP определен RFC2326 в основном служит управляющим протоколом в мультимедийной среде RTSP позволяет VCR-like управление то есть (select, forward, rewind, pause, stop, and so on) а также передает информацию о сессии
- E-mail (in Multipurpose Internet Mail Extensions [MIME] формате) также передает SDR пакеты описывающие сессии
- WEB - страницы дают описание сессии в стандартном SDR формате

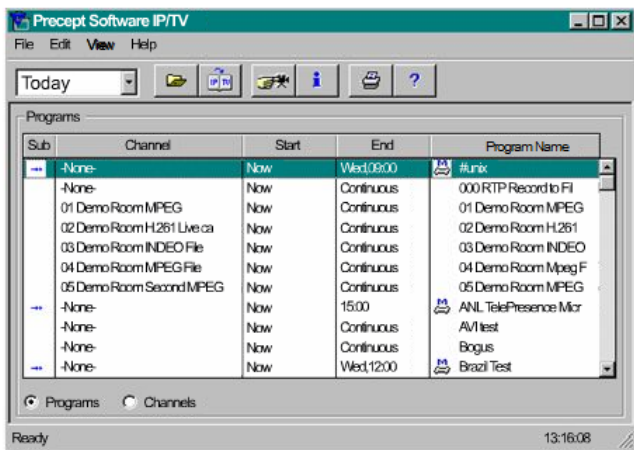


Рисунок показывает механизм работы SDR на примере Cisco IP TV. Cisco IP-TV в основном использует три компоненты: сервер (источник), контент менеджер (сервер каталога) и просмотрщик(получатель)

Получатель производит одно из двух следующих действий:

- Связаться с контент менеджером (напрямую через unicast) и получить список доступных программ (сессий, потоков) от него
- Прослушивать периодически объявления SAPR

Cisco IP-TV использует SAP для доставки сессий SDR просмотрщику (получателю). Используется стандартная формат SDR для описания сессии.

## 2. IGMP и 2 уровень

### 2.1 Введение в IGMPv2

Протокол IGMP вводит требования для определения процесса вступления в multicast группу и выхода из нее. Понимание этого протокола является фундаментальным при определении multicast группы. На данный момент существует 3 версии IGMP.

Без контроля, многоадресные пакеты затопляют сеть как неизвестные одноадресные кадры которые Ethernet коммутаторы распространяют через все порты. IGMP snooping и Cisco Group Management Protocol (CGMP) решает эту проблему.

IGMP это протокол взаимодействия узла и маршрутизатора который используется, когда узлы хотят вступить в multicast группу. В IGMP v.1 Маршрутизаторы посылают периодические запросы на участие в multicast группах на multicast адрес 224.0.0.1. Узлы посылают уведомление об участии в группе на multicast адрес той группы в которую они хотят войти. При этом узлы молча покидают группу, не сообщая об этом маршрутизатору.

Большинство изменений между IGMP v.1 и IGMP v.2 направлены на решение проблем с задержкой на вступление и выход из группы, и решение проблем с неоднозначной адресацией в оригинальной спецификации протокола.

Вот некоторые важные изменений:

- Запросы, специфичные для группы
- Сообщение о выходе из группы
- Механизм выбора запрашивающего узла, того кто будет посылать пакеты
- Таймер ответа на запрос

Запросы специфические для группы которые были добавлены в IGMP v.2 позволяют маршрутизаторам запрашивать информацию о членстве в одной группе вместо всех групп, этот оптимизированный способ узнать остались ли члены в группы без необходимости спрашивать о членстве во всех группах. Разница между специфическими для группы запросами и запросами на членство состоит в том что запросы на членство рассылаются multicast для всех узлов на IP адрес 224.0.0.1 в то время как запросы специфические для группы multicast рассылаются только на multicast адрес группы.

Сообщения о выходе из группы позволяют узлам сказать маршрутизатору что они выходят из группы, (покидают группу). Эта информация уменьшает задержку на выход из группы в сегменте, если тот член группы который покидает эту группу является последним членом из этой группы. Стандарт определяет время, когда сообщение запроса о выходе из группы должно быть послано. Интервал времени ответа (The query-interval response) на запрос был добавлен чтобы контролировать разброс ответов, это время устанавливается в запросе, чтобы указать узлам (членам группы) сколько времени у них есть чтобы ответить на запрос о членстве. При этом IGMP2 обратно совместим с IGMP1

## 2.2 Сообщения на добавление и удаление в IGMPv2 группы

Члены желающие вступить в multicast группу не должны ждать запроса о членстве в группе чтобы в нее вступить. Они отправляют специальное сообщение, чтобы показать свой интерес в членстве. Этот процесс уменьшает задержку на вступления для конечной системы если других членов такой группы на текущий момент нет в этом сетевом сегменте.

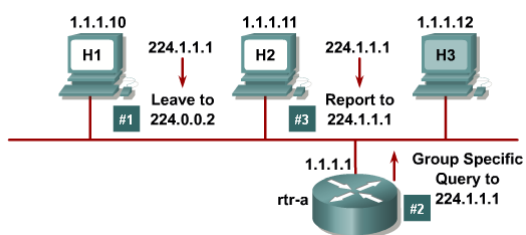
После того как узел H2 отправил запрос о членстве в группе для группы 224.1.1.1 группа 224.1.1.1 становится активной на интерфейсе маршрутизатора Ethernet 0. Используя команду show ip igmp group можно увидеть следующий список:

- группа 224.1.1.1 была активна на этом интерфейсе в течении 1 часа 3 минут
- группа 224.1.1.1 станет просроченной и будет удалена через 2 минуты и 31 секунду если не придет новых IGMP ответов о членстве в этой группе в течении этого времени
- последний узел который рапортовал о членстве в этой группе это 1.1.1.11 H2

Когда в одном сетевом сегменте Ethernet присутствует 2 или более IGMP маршрутизаторов тот который обладает наибольшим IP адресом становится выбранным. В IGMP v1 узлы покидают группу пассивно, они не указывают явно, что уходят из группы, они просто перестают посылать отчеты о членстве. В IGMP v2 они должны явно послать сообщение о выходе из группы

В IGMP v 2 когда маршрутизатор получает сообщение о выходе из группы он отвечает на это событие посылая специфический для группы запрос на ту группу из которой уходит узел чтобы увидеть есть ли в сети еще узлы заинтересованные в получении трафика этой группы этот процесс позволяет уменьшить общую задержку на выход из группы.

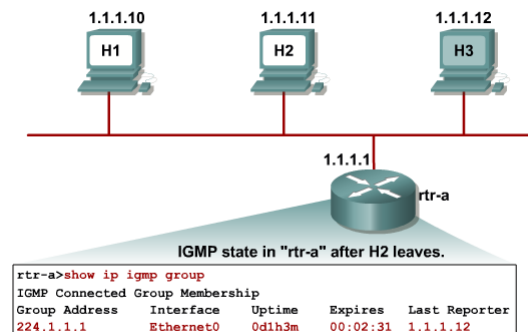
На следующем рисунке: узлы H2 и H3 - члены multicast группы 224.1.1.1 в какой то момент узел H2 решает выйти из группы и объявляет об этом, посылая сообщение о выходе из группы для multicast группы 224.0.0.2.



Маршрутизатор слышит это сообщение о выходе из группы и посылает специфический для группы запрос чтобы увидеть есть ли еще члены этой группы в сетевом сегменте. Узел H3 не вышел из multicast группы 224.1.1.1 так что он отвечает обычным ответом. Этот ответ показывает маршрутизатору что надо дальше отправлять multicast трафик для 224.1.1.1 потому что как минимум один член этой группы еще существует.



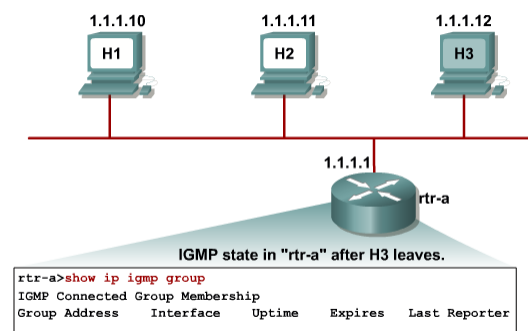
На следующем рисунке: можно видеть что multicast группа 224.1.1.1 все еще активна тем ни менее информация об IGMP показывает что узел H3 последний узел который отправлял сообщение о членстве в группе IGMP.



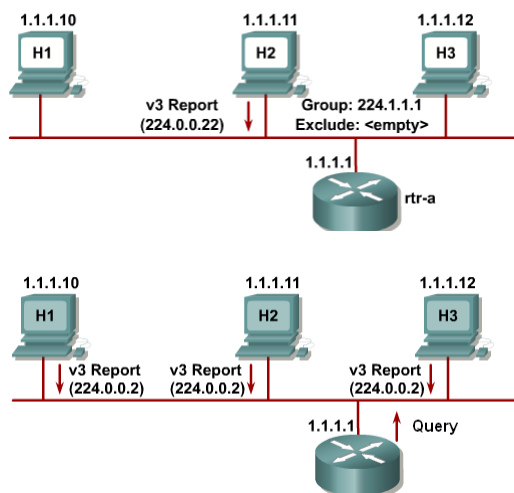
После получение сообщения о выходе из группы от H3 маршрутизатор посылает специфический для группы запрос чтобы узнать кто то еще присутствует или нет.

Так как узел H3 был последним членом группы 224.1.1.1 он не получает в ответ ни одного отчета о членстве в группе 224.1.1.1 и членство в группе пропадает по тайм-ауту, типично на это уходит от 1 до 3 секунд с того момента как узел посылает сообщение о выходе и до тех пор пока специфический для группы запрос не вылетит по тайм-ауту тогда multicast трафик перестанет отправляться для этой группы.

На следующем рисунке: все узлы вышли из группы 224.1.1.1 на интерфейсе Ethernet 0. Этот статус показан выводом команды show ip igmp group



## 2.3 Введение в IGMPv3



Главное изменение ведения в IGMP v3 определенного в RFC 3376 это разрешить узлам показывать, что они хотят получать трафик только от конкретного источника в multicast группе. IGMPv3 добавляет возможность фильтровать multicast пакеты основываясь на источнике multicast. Это улучшение делает утилизацию ресурсов маршрутизатора более эффективной.

Рисунок показывает IGMP v3 в действии. Узел 3 отправляет объединенное сообщение с явным запросом на вступление на подключение к данному источнику из списка источников. IGMP v3 использует список источников для фильтрации что позволяет системе рапортовать об интересе о получение пакетов только от конкретного источника или от всех источников которые посылают на определенный multicast адрес в определенную группу. Multicast протоколы маршрутизации могут использовать эту информацию

чтобы избежать доставки multicast пакетов от определенных источников в сети где нет заинтересованных получателей. В IGMP v3 отчеты посылаются на адрес 224.0.0.22 в место 224.0.0.2

## 2.4 Совместимость IGMPv2 и IGMPv3

```
R1# show ip igmp interface
FastEthernet0/0 is up, line protocol is up
Internet address is 192.168.1.1/24
IGMP is enabled on interface
Current IGMP host version is 2
Current IGMP router version is 2
IGMP query interval is 60 seconds
IGMP querier timeout is 120 seconds
IGMP max query response time is 10 seconds
Last member query count is 2
Last member query response interval is 1000 ms
Inbound IGMP access group is not set
IGMP activity: 2 joins, 0 leaves
Multicast routing is enabled on interface
Multicast TTL threshold is 0
Multicast designated router (DR) is 192.168.1.1 (this system)
IGMP querying router is 192.168.1.1 (this system)
Multicast groups joined by this system (number of users):
  224.0.1.40(1)
```

Используйте команду `show ip igmp interface` для того чтобы определить какая версия IGMP активна на интерфейсе.

В примере, IGMP версия указана в строке которая выглядит как "current igmp host version is 2 и current igmp router version is 2"

## 2.5 Multicast в оборудовании 2 уровня, коммутатор



Для большинства коммутаторов 2-го уровня multicast трафик обычно рассматривается как трафик с неизвестным MAC адресом получателя или широковещательный кадр. Таким образом этот кадр будет разослан каждому порту внутри Vlan. Это поведение допустимо для неизвестного и широковещательного трафика, но как сказано ранее, IP multicast узлы могут вступать и быть заинтересованными только в конкретных multicast группах. На большинстве коммутаторов 2 уровня такой трафик отправляется через все порты в результате тратится пропускная способность и в сетевых сегментах и на конечных узлах.

Итого, есть проблема : Коммутаторы 2 уровня рассылает широковещательно multicast трафик.

- Обычно Коммутаторы 2 уровня рассматривает multicast трафик как неизвестный или широковещательный и должны разослать его через все порты
- В статических записях иногда может быть указано какой порт должен получать от каких групп multicast трафик
- Динамическая конфигурация этого содержимого облегчает администрирование

Один из методов используемых на коммутаторах Cisco Catalyst это разрешить администратору вручную настроить коммутатор, ассоциировать multicast MAC адрес с различными портами. Например: администратор настраивает порты 5,6,7 так что только они получают multicast трафик предназначенный для multicast группы. Этот метод работает, но плохо масштабируется. IP узлы работающие с multicast трафиком динамически вступают и выходят из группы используя IGMP чтобы оповестить об этом multicast маршрутизатор. Динамическая конфигурация таблиц коммутации на коммутаторах более эффективна и облегчает администрирование.

## 2.6 Multicast методы 2 уровня

Множество различных решений было разработано для улучшения поведения коммутаторов, когда они получают multicast кадры, например:

CGMP Cisco Group Management Protocol и IGMP Snooping. CGMP это протокол Cisco который работает между multicast маршрутизатором и коммутатором, этот протокол позволяет Cisco multicast маршрутизаторам информировать коммутаторы о той информации которую они получили в IGMP пакетах после того как они увидели IGMP сообщения посланные узлами.

С помощью IGMP Snooping коммутатор должен просмотреть каждый multicast пакет для того чтобы определить содержит ли он информацию о IGMP и соответствующим образом обновить свою таблицу MAC-адресов. Реализация IGMP Snooping на дешевых коммутаторах со слабыми CPU может серьезно ударить по производительности, когда данные пересылаются на больших скоростях. Решением этой проблемы является внедрение IGMP Snooping на высокоуровневых коммутаторах со специальными платами ASICs, которые могут производить проверки IGMP пакетов аппаратно. CGMP это лучшее решение для дешевых коммутаторов без специализированного аппаратного обеспечения для обработки multicast.

## 2.7 Cisco Group Management Protocol (CGMP)

CGMP является наиболее распространенным многоадресным коммутационным решением, и оно было впервые реализовано в оборудовании компании Cisco.



CGMP – базируется на модели клиент-сервер, в которой роутер считается CGMP сервером, а коммутатор – клиентом. Есть программные компоненты, работающие на обоих устройствах и роутер транслирует IGMP сообщения в CGMP команды, которые затем обрабатываются коммутатор, для заполнения своей таблицы коммутации второго уровня корректными записями multicast адресов. Основой CGMP – является то, что multicast роутер видит все IGMP пакеты и информирует коммутатор, когда конкретный узел входит или покидает multicast группу. Роутеры используют зарезервированные для CGMP multicast MAC-адреса для отправки управляющих пакетов CGMP коммутатору, а коммутатор использует эту информацию чтобы настраивать свою таблицу коммутации.

Когда маршрутизатор получает управляющий пакет IGMP, он создаёт пакет CGMP который содержит тип запроса (вступление или выход), multicast MAC-адрес второго уровня и конкретный MAC-адрес клиента.

Этот пакет посылается на общеизвестный CGMP multicast MAC-адрес, который выглядит как: 0100.1CDD.DDDD, который прослушивается всеми CGMP коммутаторы. CGMP Control Message интерпретируется, и создаются надлежащая запись на коммутаторе, в контент-адресной памяти (content-addressable memory CAM), там находится таблица ограничивающая передачу Multicast трафика для этой группы.

### **Solution 1: Cisco Group Management Protocol (CGMP)**

- Runs on switches and routers.
- CGMP packets sent by routers to switches at a multicast MAC address:
  - 0100.0cdd.dddd
- CGMP packet contains:
  - Type field: Join or Leave
  - MAC address of the IGMP client
  - Multicast MAC address of the group
- Switch uses CGMP packet information to add or remove an entry for a particular multicast MAC address.

## 2.8 IGMP Snooping

Второе решение для multicast свичинга это IGMP Snooping .



Как понятно из названия технологии, коммутаторы начинают понимать IGMP и прослушивают полностью все переговоры между маршрутизаторами. Для осуществления этого нужно, чтобы коммутатор идентифицировал и изучал копию всех IGMP пакетов которые проходят между маршрутизаторами и узлами, это следующие IGMP пакеты:

- IGMP отчеты о членстве
- IGMP запросы на выход из группы.

Если не уделять должного внимания тому, как реализован IGMP Snooping, возможно коммутатору понадобится просматривать все multicast пакеты 2-го уровня чтобы определить IGMP пакеты. Это действие может наносить серьезный урон производительности коммутатора. Правильный дизайн требует присутствия специального аппаратного обеспечения (Layer 3 ASICs) чтобы избежать этой проблемы, это будет на прямую влиять на стоимость коммутатора. Коммутаторы должны поддерживать сетевой уровень чтобы избежать серьезных проблем с производительностью из-за IGMP snooping.

#### **Solution 2: IGMP snooping**

- Switches become "IGMP" aware.
- IGMP packets are intercepted by the CPU or by special hardware ASICs.
- The switch must examine contents of IGMP messages to determine which ports want what traffic:
  - IGMP membership reports
  - IGMP leave messages
- Effect on switch:
  - Must process all Layer 2 multicast packets
  - Administration load increased with multicast traffic load
  - Requires special hardware to maintain throughput

### 3.1 Протоколы маршрутизации, использующие Multicast

Деревья распространения multicast определяют путь от источника к получателям, через который проходит multicast трафик.

Существует 2 типа распределения multicast трафика

- Деревья источника (Source trees )
- Разделяемые деревья (Shared trees )

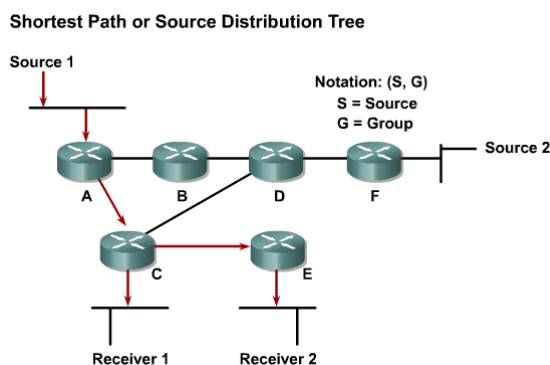
При использовании дерева источника, отдельное дерево строится для каждого источника, от каждого источника ко всем членам его группы. Так как дерево от источника использует самый короткий путь к его получателям оно также называется shortest path tree SPT (Дерево Кратчайшего Пути). Каждая пара источник/группа требует информацию о состоянии, при использовании групп с очень большим количеством источников или сетей в которых есть очень большое количество групп с большим количеством источников в каждой группе, использование деревьев от источника может серьезно нагрузить память роутера. Source trees также часто называют Source base trees или Source root trees что переводится как деревья основанные на источнике или деревья с источником в корне (когда источник будет корнем дерева). Протоколы использующие "Разделяемые деревья" создают пути передачи multicast которые полагаются на центральный роутер, который служит точкой встречи между multicast источником и получателем (rendezvous point RP). Источники изначально посылают multicast пакеты этому роутеру (RP), который затем направляет эту информацию через разделяемое дерево всем членам группы. Использование разделяемых деревьев менее эффективен чем SPT

потому что пути между источниками и получателями не обязательно самые короткие но при этом они менее требовательные к роутеру в плане использования памяти и нагрузки процессора.

В принципе существует 2 типа работы multicast протоколов маршрутизации: плотного и не плотного режима (dense mode and sparse mode):

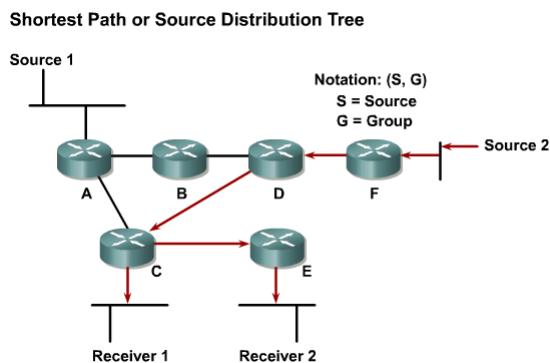
- dense mode. “Плотные” протоколы (протоколы плотного режима) широковещательно рассылают multicast трафик во все части сети и периодически удаляют потоки из тех сегментов где нет получателей, используя механизм периодического затопления и очистки.
- sparse mode. “Не плотные” протоколы (протоколы не плотного режима) используют явный механизм включения когда деревья распространения строятся по требованию с помощью специальных, явных, сообщений о включении в дерево которые посылаются роутерами которые на прямую подключены к получателям.

### 3.2 Распределенное дерево Multicast

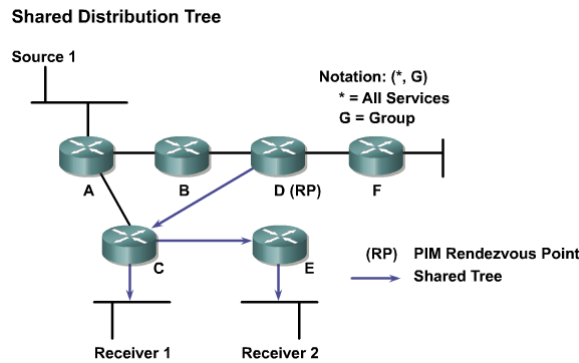


Картинка выше показывает SPT между источником (Source) 1 и получателем (Receiver) 1 и 2. На ней четко видно что путь от источника к получателям проходит через роутеры A, C, и E – это путь с наименьшей стоимостью, то есть по сути выбранной метрикой.

Пакеты передаются в соответствии с парой адресов источника и группы (Отправитель,Группа). Состояние продвижения пакетов ассоциированное с SPT, называют – нотацией (S,G) – которые произносятся как \*S запятая G\*. Где S – это IP адрес источника (Source) , а G – это адрес multicast группы (Group) рассылки.

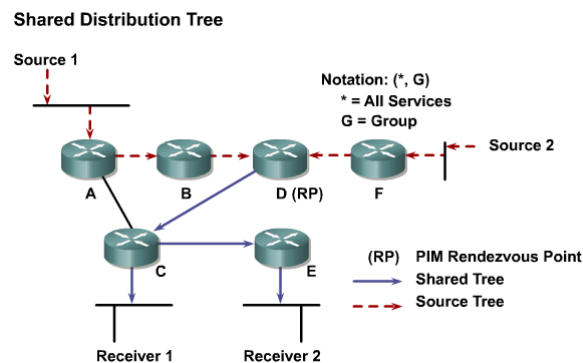


Картинка выше показывает другой пример SPT, на которой источник(source) 2 активен и посылает multicast пакеты получателям(receiver) 1 и 2. Для этого строится отдельное дерево SPT, в этот раз с источником 2 как корнем SPT. Основная концепция здесь в том что, отдельное дерево SPT - строиться для каждого источника S посылающего пакеты в группу G.



Картинка выше показывает общее распределение деревьев, роутер D является корнем этого разделяемого дерева, которое строится от роутера D к роутерам C, E чтобы достичь получателя (Receiver) 1 и 2. В PIM (Protocol Independent Multicast), независимо от multicast протокола, корнем разделяемого дерева является RP.

Пакеты направляются вниз по разделяемому дереву к получателям. Состояние перенаправления по умолчанию для разделяемого дерева, записывается в нотации (\*,G). Где звёздочка – это подстановочная запись, она может быть заменена на что угодно, то есть обозначающая любой источник а G – это адрес multicast группы.



На картинке выше, источник 1 и 2 посылают multicast пакеты на RP через SPT, а от RP – multicast пакеты направляются через, разделяемое дерево рассылки к получателям (receiver) 1 и 2.

### 3.3 Идентификация деревьев распространения Multicast

Записи о распространении multicast, которая появляется в таблице распространения multicast (то есть в таблице маршрутизации multicast), читается следующим образом:

- (S,G) От источника S посылающего в группу G. Такие записи обычно присутствуют для SPT, но могут так же появляться для разделяемого дерева.
- (\*,G) - от любого источника посылающего в группу G, такие записи обычно отображают разделяемые деревья но также создаются в Cisco роутерах для существующих (S,G) записей.

Записи о состоянии SPT – используют больше памяти роутера, потому что создаётся отдельная запись для каждой «пары источник и группа получатель», но трафик отправляется по более оптимальному пути для каждого получателя, таким образом минимизируя задержку в передачи пакета. Деревья разделяемого распределения - используют меньше памяти роутера, но не предоставляют самые оптимальные пути от источника к получателю, таким образом вводят дополнительную задержку в доставку пакета.

Примечание:

MFT (Multicast Forward Table) – таблица маршрутизации multicast

MFE (Multicast Forward Entries) – запись в таблицу маршрутизации multicast, эта таблица, содержится отдельно от таблицы MFT. Если есть пакеты с multicast получателем – то они просматриваются отдельно.

### 3.4 Маршрутизация IP Multicast

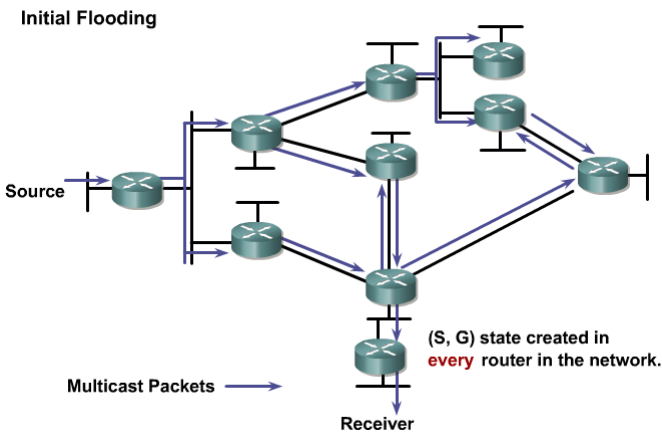
В unicast маршрутизации когда роутер получает пакет, решение о том куда отправить пакет зависит от адреса получателя пакета. В multicast маршрутизации, решение о том куда



отправить пакет, зависит от того откуда пришел multicast пакет. Multicast роутеры должны знать источник пакета, а не его получателя. С учетом multicast, IP-адрес источника определяет - известного отправителя, а IP-адрес получателя определяет - группу неизвестных получателей. Multicast маршрутизаторы используют механизм, называемый RPF (Reverse Path Forwarding) перенаправление по обратному пути, что бы избежать возникновения петель в маршрутизации, а также обеспечить самый короткий путь от источника к получателям.

### 3.5 Protocol-Independent Multicast: PIM-DM

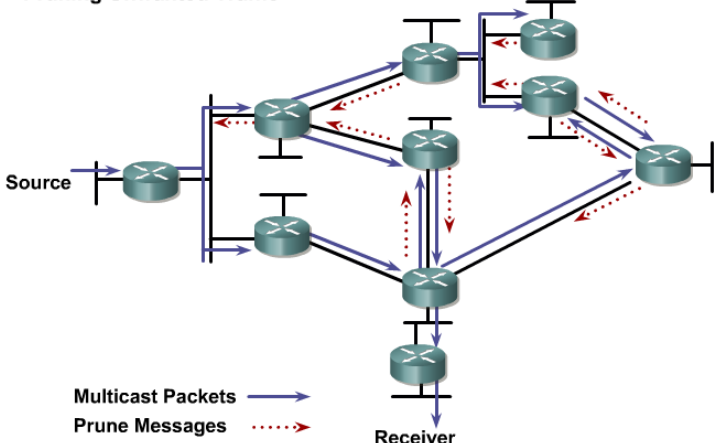
PIM dens mod, то есть PIM плотного режима ( PIM-DM ) изначально затопляет трафиком все не RPF-интерфейсы где есть другой PIM-DM сосед (другой такой маршрутизатор) или на прямую подключенный член группы.



На картинке: multicast трафик, который посылается от источника, флудит во всю сеть. Каждый маршрутизатор получает трафик через свой RPF-интерфейс и отправляет этот трафик всем своим PIM-DM соседям.

В результате этого процесса некоторый трафик попадает на маршрутизаторы не через RPF-интерфейсы, например как с 2-мя маршрутизаторами в центре картинки или с 2-мя в верхнем правом углу. Пакеты получены не через RPF-интерфейс отбрасываются. Эти RPF-потоки являются нормальными при механизме изначального затопления информацией и затем корректируются нормальным механизмом очистки (PIM-DM pruning mechanism).

Pruning Unwanted Traffic



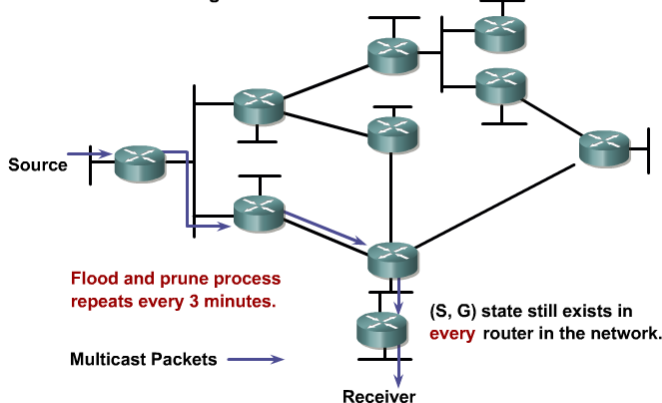
На картинке: отправляются сообщения PIM-DM очистки, чтобы остановить нежелательный трафик, они отображены пунктирными стрелочками.

Сообщения об очистке также отправляются и через не RPF-интерфейсы, чтобы отказаться от данного потока multicast трафика через этот интерфейс так как он попадает на интерфейс не через самый короткий возможный путь к источнику, примеры сообщения очистки которые посылаются через RPF-интерфейс можно увидеть на маршрутизаторах в центре и крайнем с права на картинке.

Сообщения об ошибке посылаются через RPF-интерфейс только в том случае если нету далее по потоку никакого

маршрутизатора то есть далее ему некому передавать multicast трафик.

Results After Pruning



Картинка: показывает тот SPT который получился в результате очистки сети от ненужного, незатребованного multicast трафика.

Несмотря на то что поток multicast трафика более не достигает всех маршрутизаторов сети состояния (S, G) остаются, на всех на них и будет оставаться до тех пор пока источник не перестанет отправлять пакеты. В PIM-DM строк жизни сообщения об очистке истекает через 3 минуты, после этого периода multicast трафик снова флудит для всех маршрутизаторов (снова затопливает всю сеть). Этот периодический механизм flood-and-prune (затопления и очистки) он является нормальным для сетей которые используют PIM-DM и его обязательно учитывать при проектирование сытей с использованием PIM-

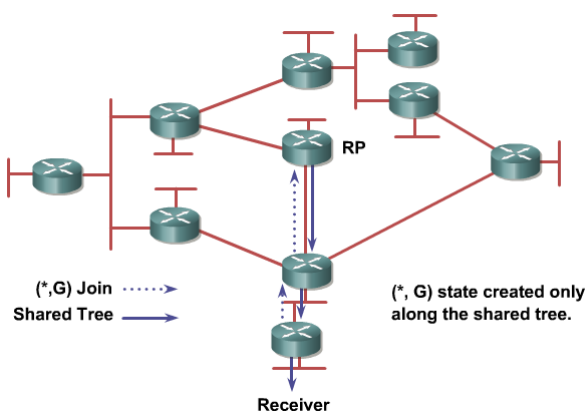
DM.

### 3.6 Protocol-Independent Multicast: Describing PIM-SM

PIM sparse mode (PIM-SM) – то есть PIM “не плотного” режима описан в RFC2362. Также как в PIM-DM, PIM-SM тоже абсолютно независим от использования unicast протокола. PIM-SM использует разделяемые деревья распространений, но он также может переключиться в режим использования деревьев SPT. PIM-SM базируется на модели явного уведомления (явного запроса), таким образом трафик отправляется в те части сети которые его требуют (которым он нужен). PIM-SM использует ARP чтобы скоординировать перенаправления multicast трафика от источника к получателю. Отправители регистрируются на RP и отправляют единственную копию multicast информации через него к зарегистрированным получателям. Члены группы соединяются в разделяемые деревья ихними локально выбранными роутерами (Designated Router DR). В корне разделяемого дерева, которое таким образом строится, всегда находится RP. PIM-SM хорошо подходит для широко масштабируемых внедрений и в “плотном” и в “не плотном” режиме групп в enterprise сети. Он представляет из себя оптимальный выбор для всех производственных сетей вне зависимости от их размера и плотности членов групп multicast рассылки.

Существует множество оптимизаций и улучшений к PIM включая следующие:

- двухсторонний режим передачи PIM который разработан специально для приложений многие-ко-многим то есть приложений связи many-to-many это такие приложения в которых множество узлов отправляет multicast трафик друг другу.
- source specific multicast (SSM) multicast специфический для источника который представляет из себя вариант PIM-SM который строится только на source-specific SPTs, то есть с определенным источником SPT и не требует активного RP для source-specific groups, то есть для групп со специфическим источником (диапазон адресов 232/8).

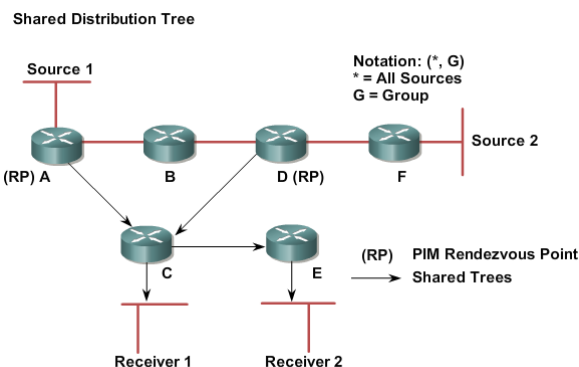


На картинке: активный получатель (receiver) подключился к multicast группе G. Последний маршрутизатор (last-hop router) знает IP адрес RP маршрутизатора для групп G и посылает сообщения о подключении (\*,G) к этой группе на RP.

Вот это вот сообщения (\*,G) путешествует от хоп-к-хопу в направлении RP и таким образом по дороге оно строит цепочку, ветку разделяемого дерева, которое расширяется от RP к последнему маршрутизатору в цепочке, к которому напрямую подключен получатель.

В этом месте, то есть в этой точке трафик для группы G спокойно путешествует по разделяемому дереву к получателю.

#### 7.3.7 PIM Sparse-Dense-Mode (PIM в разреженно плотном режиме)



Картинка показывает два multicast источника. Для максимальной эффективности можно внедрить множества RP и каждый RP расположить в оптимальном месте. Эта конструкция является сложной для настройки, управления и устранения неполадок, с ручной конфигурацией RPS.

PIM sparse-dense mode поддерживает автоматический выбор RP для каждого multicast. То есть для каждого потока, например роутер A на картинке может быть RP для источника 1, а роутер E может быть RP для источника 2.

Для PIM sparse-dense mode это является рекомендуемым решением от Cisco для IP Multicast. Поскольку PIM-DM плохо масштабируется и имеет повышенные требования к ресурсам маршрутизатора, PIM-SM предлагает очень ограниченные возможности по настройке RP. Если невозможно найти RP автоматически для multicast группы, и ни один не настроен вручную, PIM sparse-dense mode будет работать в “плотном” режиме. Таким образом для нормальной работы PIM в “не плотном” режиме вам нужно разработать и внедрить автоматическое обнаружение RP.

#### 4.1 Разрешение использования в разреженном и разреженно-плотном режиме

Для того чтобы внедрить простой PIM-SM и PIM разреженно-плотной режим используются следующие команды:

**router(config) #**

```
ip multicast-routing
```

- Enables multicast routing.

**router(config-if) #**

```
ip pim { sparse-mode | sparse-dense-mode }
```

- Enables PIM SM on an interface. Sparse-dense-mode enables mixed sparse/dense groups.

**router(config) #**

```
ip pim send-rp-announce {interface type} scope {ttl}  
group-list {acl}  
ip pim send-rp-discovery {interface type} scope {ttl}
```

- Configures the ability of a group of routers to be and discover RPs dynamically.

- Глобальная команда конфигурации `ip multicast-routing` включает поддержку IP-multicast на маршрутизаторе.
- Команда интерфейса `ip pim sparse-mode` включает роботу PIM-SM на выбранном интерфейсе. `ip pim sparse-dense-mode` включает интерфейс маршрутизатора в работу PIM-SM для групп в разреженном режиме (для которых известен RP) и в плотном режиме для всех прочих групп.
- Глобальная команда `ip pim send-rp-announce {interface type} scope {ttl} group-list {acl}` используется для того чтобы сделать маршрутизатор RP. Этот маршрутизатор посылает авто-RP сообщение 224.0.1.39, таким образом он анонсирует себя как кандидата на RP для групп в том диапазоне который описан в {acl}.
- Глобальная команда `ip pim send-rp-discovery {interface type} scope {ttl}` настраивает маршрутизатор как агент соответствия RP mapping. Он будет прослушивать IP-адрес 224.0.1.39 и посылать сообщение соответствия RP для группы на 224.0.1.40. Другие PIM маршрутизаторы прослушивают 224.0.1.40 чтобы автоматически определить RP.
- Команда `ip pim spt-threshold {rate | infinity}` контролирует переключение из режима разделяемых деревьев в SPT в разреженном режиме. Использование ключевого слова `infinity` позволяет не выполнять переключение никогда.

Примечание:

Рекомендуемый метод настройки интерфейса для работы в режиме PIM-SM это использование команды `ip pim sparse-dense-mode`. Этот метод позволяет автоматическое обнаружение RP, позволяет использование маршрутизаторов начальной загрузки (BSR), или статически определение RP, это позволяет уменьшить усилия на конфигурацию.

#### 4.2 Исследование таблицы маршрутизации multicast

Команда `show ip mroute` самая полезная команда для определения состояния multicast источников и групп с точки зрения выбранного маршрутизатора. (картинка 1)

router#

```
show ip mroute [group-address] [summary] [count] [active kbps]
```

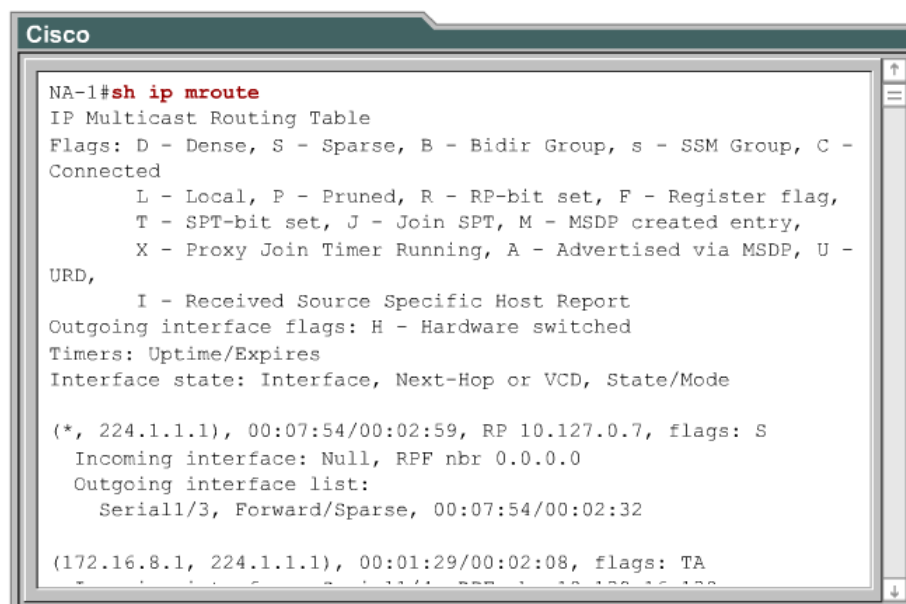
**Displays the contents of the IP multicast routing table:**

- **summary:** Displays a one-line, abbreviated summary of each entry in the IP multicast routing table.
- **count:** Displays statistics about the group and source, including number of packets, packets per second, average packet size, and bits per second.
- **active:** Displays the rate at which active sources are sending to multicast groups. The default is 4 kbps.

Вывод этой команды показывает часть дерева распределения multicast вместе с входящим интерфейсом и списком исходящих интерфейсов. Доступны следующие опции:

- **summary:** показывает одну сокращенную строку для каждой записи multicast таблицы маршрутизации
- **count:** показывает статистику о группе и источнике включая количество пакетов, количество пакетов в секунду, средний размер пакета, и количество битов в секунду.
- **active:** показывает скорость с которой активные источники посылают информацию в multicast группу. Активные источники это те которые посылают со скоростью показанной в kbps. По умолчанию 4 Кб/сек.

Вывод команды `show ip mroute` показан на картинке 2, там показана multicast таблица маршрутизации при использовании PIM-SM:



```
Cisco
NA-1#sh ip mroute
IP Multicast Routing Table
Flags: D - Dense, S - Sparse, B - Bidir Group, s - SSM Group, C -
Connected
      L - Local, P - Pruned, R - RP-bit set, F - Register flag,
      T - SPT-bit set, J - Join SPT, M - MSDP created entry,
      X - Proxy Join Timer Running, A - Advertised via MSDP, U -
URD,
      I - Received Source Specific Host Report
Outgoing interface flags: H - Hardware switched
Timers: Uptime/Expires
Interface state: Interface, Next-Hop or VCD, State/Mode

(*, 224.1.1.1), 00:07:54/00:02:59, RP 10.127.0.7, flags: S
  Incoming interface: Null, RPF nbr 0.0.0.0
  Outgoing interface list:
    Serial1/3, Forward/Sparse, 00:07:54/00:02:32

(172.16.8.1, 224.1.1.1), 00:01:29/00:02:08, flags: TA
```

- **(\*, G) :** Таймеры, адрес RP для данной группы, список флагов для данной группы (S -sparse-разрежений режим)
  - Входящий интерфейс это интерфейс направлений в сторону RP, если он Null, то этот маршрутизатор является RP для этой группы. Если ваш аргумент Reverse Path Forwarding (RPF), отправление по обратному пути, это адрес следующего маршрутизатора в направлении к RP. Если он 0.0.0.0 то этот маршрутизатор сам является RP для заданной группы.
  - Список исходящих интерфейсов (OIL), те по которым идет рассылка совместно с ихними режимами и таймерами.

- (S, G) : таймеры и флаги для этой записи при этом T- показывает что используется SPT; A- показывает что он должен объявляться через Multicast Source Discovery Protocol [MSDP].
  - Входящий интерфейс это интерфейс в направлении источника S. RPF сосед это адрес следующего маршрутизатора в направлении источника если он 0.0.0.0 то источник напрямую подключен к нам.
  - Список OIL это список исходящих интерфейсов с их режимами и таймерами

#### 4.3 Обнаружение PIM соседей

##### 4.4

Когда PIM-SM настроен, первый шаг проверки интерфейса с PIM, это проверка правильно ли определены соседи PIM. (картинка 1)

**router#**

```
show ip pim interface [type number] [count]
```

- Displays information about interfaces configured for PIM

**router#**

```
show ip pim neighbor [type number]
```

- Lists the PIM neighbors discovered by the Cisco IOS software

**router#**

```
mrinfo [hostname | address]
```

- Queries which neighboring multicast routers are peering with the local router or router specified

Для проверки можно использовать следующие команды:

- show ip pim interface: показывает информацию про PIM-интерфейсы.
- show ip pim neighbor: показуэт обнаруженных PIM -соседей .
- mrinfo: показывает информацию о multicast маршрутизаторах которые подключены к локальному маршрутизатору.

Команда show ip pim interface показывает следующую информацию (картинка 2):

```
R1# show ip pim interface detail
```

| Address      | Interface       | Ver/<br>Mode | Nbr<br>Count | Query<br>Intvl | DR<br>Prior | DR          |
|--------------|-----------------|--------------|--------------|----------------|-------------|-------------|
| 192.168.1.1  | Loopback1       | v2/S         | 0            | 30             | 1           | 192.168.1.1 |
| 172.16.13.1  | FastEthernet0/0 | v2/S         | 1            | 30             | 1           | 172.16.13.3 |
| 172.16.102.1 | Serial0/0/0     | v2/S         | 1            | 30             | 1           | 0.0.0.0     |
| 172.16.103.1 | Serial0/0/1     | v2/S         | 1            | 30             | 1           | 0.0.0.0     |

- Address: IP адрес интерфейса.
- Interface: тип и количество PIM-интерфейсов.
- Ver/Mode: PIM версия (1 or 2) на интерфейсе и режим (dense mode, sparse mode, or sparse-dense mode).
- Nbr Count: количество соседей на этом соединении.
- Query Intvl: частота послания PIM hellos и запросов (по умолчанию 30 секунд).
- DR Prior: Приоритет использованный при выборе DR. Если все маршрутизаторы на канале multicast имеют одинаковой приоритет (по умолчанию равен 1) будет выбран наибольший IP адрес
  - DR: IP адрес DR маршрутизатора. (на подключениях точка-точка DR отсутствует и будет показан адрес 0.0.0.0.)

Команда show ip pim neighbor показывает следующую информацию: (картинка 3)



## Cisco

```
R1# show ip pim neighbor
```

```
PIM Neighbor Table
```

```
Mode: B - Bidir Capable, DR - Designated Router, N - Default DR Priority,  
S - State Refresh Capable
```

| Neighbor Address | Interface       | Uptime/Expires    | Ver | DR Prio/Mode |
|------------------|-----------------|-------------------|-----|--------------|
| 172.16.13.3      | FastEthernet0/0 | 00:02:29/00:01:42 | v2  | 1 / DR S     |
| 172.16.102.2     | Serial0/0/0     | 00:02:30/00:01:40 | v2  | 1 / S        |
| 172.16.103.3     | Serial0/0/1     | 00:02:29/00:01:43 | v2  | 1 / S        |

- Neighbor Address: IP адрес PIM-соседа.
- Interface: интерфейс на котором мы получили PIM hello (PIM query в PIMv1)
- Uptime: время активности PIM соседа.
- Expires: таймаут активности PIM соседа. Получение PIM hello или query сбрасывает этот таймер.
- Ver: Версия PIM (1 или 2) которую использует сосед.
- DR Priority: Если сосед поддерживает эту опцию то показывается число, если нет то не показывается.

Пример: вывода команды `mrinfo` показывает информацию о подключенных маршрутизаторах, поддерживающих multicast трафик, и соединенных с R1.

## Cisco

```
R1# mrinfo
```

```
172.16.13.1 [version 12.4] [flags: PMA]:  
  192.168.1.1 -> 0.0.0.0 [1/0/pim/querier/leaf]  
  172.16.13.1 -> 172.16.13.3 [1/0/pim]  
  172.16.102.1 -> 172.16.102.2 [1/0/pim]  
  172.16.103.1 -> 172.16.103.3 [1/0/pim]
```

#### 4.4 Проверка информации про RP

#### 4.5

Маршрутизатор должен знать и иметь доступ к RP для определенной multicast группы и этот RP должен работать в режиме PIM-SM. К дополнению использования multicast ping вы можете использовать следующие команды для решения проблем с доступностью RP (картинка 1).

```
router(config) #
```

```
show ip pim rp [group-name | group-address | mapping]
```

- Display active rendezvous points (RPs) that are cached with associated multicast routing entries
- **Mapping**—displays all group-to-RP mappings that the router is aware of

```
router(config) #
```

```
show ip rpf {address | name }
```

- Displays how IP multicast routing does Reverse Path Forwarding (RPF)
- **Address**—IP address of a source of an RP

- **show ip pim rp**: если запущен без аргументов показывает RP информацию о активных группах. Если указан групповой адрес или имя группы, позывается только RP информация о выбранной группе.

- **show ip pim rp mapping**: показывает содержимое кеша соответствий групп к RP. Этот Кеш показывает какой RP соответствует какому диапазону групп, и наполняется с помощью auto-RP или механизмом BSR, а также с помощью статического назначения RP. Очень важно проверить эту информацию чтобы убедиться что маршрутизатор обладает верной информацией о соответствии RP к сетевым multicast группам в соответствии с действующей сетевой технологией и нормальной работой сети.

- **show ip rpf**: Показывает RPF информацию для RP или для источника.

```
Cisco
R1# show ip pim rp
Group: 226.26.26.26, RP: 10.100.3.3, v2, v1, uptime
00:53:51, expires 00:02:03
Group: 225.25.25.25, RP: 10.100.1.1, v2, v1, next RP-
reachable in 00:01:10
```

```
Cisco
R1# show ip pim rp mapping
PIM Group-to-RP Mappings
This system is an RP (Auto-RP)
This system is an RP-mapping agent (Serial0/0/0)

Group(s) 225.25.25.25/32
  RP 10.100.1.1 (?), v2v1
    Info source: 10.100.1.1 (?), elected via Auto-RP
    Uptime: 00:54:25, expires: 00:02:34
Group(s) 226.26.26.26/32
  RP 10.100.3.3 (?), v2v1
    Info source: 10.100.3.3 (?), elected via Auto-RP
    Uptime: 00:53:57, expires: 00:01:58
  RP 10.100.1.1 (?), v2v1
    Info source: 10.100.1.1 (?), via Auto-RP
    Uptime: 00:54:25, expires: 00:02:32
```

Команда **show ip pim rp** показывает весь список активных групп и их ассоциации с RP (картинка 2). Эта форма команды является устаревшей поскольку она показывает очень ограниченную информацию, потому предпочитается использовать **show ip pim rp mapping** (картинка 3), потому что она дает более обширную информацию и с кеша например следующее:

- IP адрес маршрутизатора который распространял информацию - когда источник информации локальный маршрутизатор, при ручной RP конфигурации, или когда источник автоматически получает информацию

- Механизм с помощью которого эта информация была получена.(автоматический RP, BSR, или статическая конфигурация)

- Или этот маршрутизатор работает как RP-кандидат, BSR или агент соответствия

```
Cisco
(toward the RP)
NA-2#show ip rpf 10.127.0.7
RPF information for NA-1 (10.127.0.7)
  RPF interface: Serial1/3
  RPF neighbor: ? (10.127.0.241)
  RPF route/mask: 10.127.0.7/32
  RPF type: unicast (ospf 1)
  RPF recursion count: 0
  Doing distance-preferred lookups across tables

(toward the source)
NA-2#show ip rpf 10.139.17.126
RPF information for ? (10.139.17.126)
  RPF interface: Serial0/0
  RPF neighbor: ? (10.139.16.134)
  RPF route/mask: 10.139.17.0/25
  RPF type: unicast (ospf 1)
  RPF recursion count: 0
```

Команда `show ip rpf` показывает соответствие RPF информации с адресом источника (картинка 4). Указаний адрес не обязательно должен быть активным источником. Это может быть простой IP адрес или адрес RP. Указывать адрес RP очень удобно для получения RPF информации о разделяемом дереве.

“RPF interface” это интерфейс в направлении источника или RP в то время как “RPF neighbor” это адрес следующего маршрутизатора в направлении к источнику (RP)

“RPF type” указывает на источник информации RPF. Например unicast показывает что информация была получена с unicast таблицы маршрутизации (в этом случае от Open Shortest

Path First Protocol [OSPF]) Другие типы RPF могут использовать Distance Vector Multicast Routing Protocol (DVMRP), Multiprotocol Border Gateway Protocol (BGP) расширения для IP multicast, или статической. Информация о RPF очень важна для multicast маршрутизации, и необходимо быть особо внимательным когда вы просматриваете информацию PIM-SM потому что существует возможность существования разделенных деревьев и SPT.

#### 4.5 Проверка состояния группы

Если multicast трафик не доходит до получателей, необходимо проверить членство IGMP групп на крайних маршрутизаторах. Команда `show ip igmp interface` показывает информацию о выбранном интерфейсе, а команда `show ip igmp groups` список локальных групп известных маршрутизатору (картинка 1).

**router#**

```
show ip igmp interface [type number]
```

- Displays multicast-related information about an interface

**router#**

```
show ip igmp groups [group-address | type number]
```

- Displays the multicast groups that are directly connected to the router and that were learned via IGMP

Включение PIM режима на интерфейсе также включает работу IGMP на этом интерфейсе. Интерфейс может быть настроен для работы в плотном, разреженном, или разрежено-плотном режиме. Режим определяет как маршрутизатор наполняет свои multicast таблицы маршрутизации, и как будут перенаправляться multicast пакеты, которые были получены от непосредственно подключенных к нему локальных сетей. Для реализации IP multicast маршрутизации вам необходимо

```
Cisco
R1# show ip igmp interface
FastEthernet0/0 is up, line protocol is up
Internet address is 192.168.1.1/24
IGMP is enabled on interface
Current IGMP host version is 2
Current IGMP router version is 2
IGMP query interval is 60 seconds
IGMP querier timeout is 120 seconds
IGMP max query response time is 10 seconds
Last member query count is 2
Last member query response interval is 1000 ms
Inbound IGMP access group is not set
IGMP activity: 2 joins, 0 leaves
Multicast routing is enabled on interface
Multicast TTL threshold is 0
Multicast designated router (DR) is (system)
IGMP querying router is 192.168.1.1
```

включить PIM в одном из этих режимов.

На картинке 2 и 3 показан простой вывод для этих команд.

```
Cisco
R1# show ip igmp groups
IGMP Connected Group Membership
Group Address Interface Uptime Expires Last Reporter Group Accounted
229.7.7.7 FastEthernet0/0 00:02:19 00:02:19 192.168.1.3
224.0.1.40 FastEthernet0/0 00:02:22 00:02:22 192.168.1.1
```

#### 4.6 Настройка маршрутизатора для включения в multicast группу

В некоторых случаях необходимо настроить маршрутизатор таким образом чтобы multicast трафик проходил по сегменту где нет ни одного члена заданной группы и нет узла который мог бы информировать о членстве в заданной группе используя IGMP. Вы можете настроить маршрутизаторы Cisco таким образом чтобы они были членами multicast групп, что может быть полезным для определения multicast доступности в сети. Если устройство является членом группы и поддерживает протокол который пересылается в группу оно может ответить на запрос (например посланный командой ping). Устройство также отвечает на IGMP эхо запросы посылаемые в группу членом которой она является.

Ниже описаны два способа направить multicast трафик в сегмент сети. Эти команды очень часто используются в лабораторных работах где нету настоящих multicast серверов и получателей.

- `ip igmp join-group`: (картинка 1 )маршрутизатор принимает multicast пакеты в дополнение к их перенаправлению. Прием multicast пакетов предотвращает от использования механизма fast switching.

- `ip igmp static-group`: Маршрутизатор не принимает пакеты но перенаправляет их. Соответственно этот метод использует механизм fast switching. Исходящий интерфейс появляется в IGMP Кеше, но сам маршрутизатор не является членом группы, как можно видеть по отсутствующему флагу L(local) в записях multicast таблицы маршрутизации.

| Command   | Purpose                  |
|---|--------------------------|
| <code>ip igmp join-group<br/>group-address</code> | Joins a multicast group. |

(Картинка 2) показывает простой пример настройки маршрутизатора для включения его в multicast группу и включения IGMP используя команду `ip igmp join-group` в режиме конфигурирования.

```
Cisco
R1# conf t
R1(config)# interface fastethernet 0/0
R1(config-if)# ip igmp join-group 229.7.7.7

*Nov  3 20:54:57.114: IGMP(0): WAVL Insert group: 229.7.7.7
interface: FastEthernet0/0Successful
*Nov  3 20:54:57.114: IGMP(0): Send v2 Report for 229.7.7.7
on FastEthernet0/0
*Nov  3 20:54:57.114: IP: s=192.168.1.1 (local), d=229.7.7.7
(FastEthernet0/0), len 28, sending broad/multicast
```

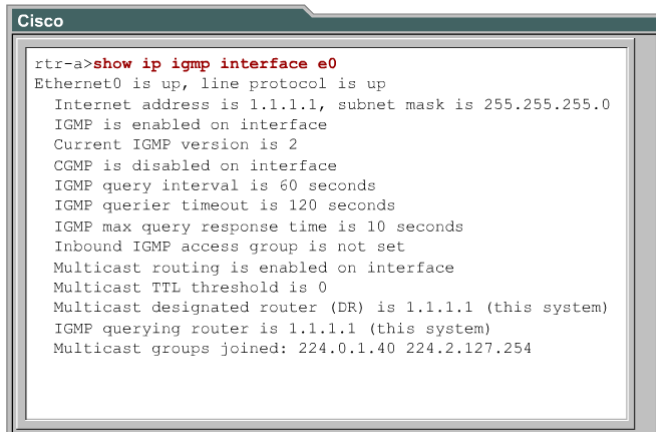
#### 4.7 Настройка маршрутизатора статически подключенного к группе

Чтобы настроить маршрутизатор как статически подключенный член группы и разрешить fast switching, используется команда `ip igmp static-group` показанная на (картинке 1).

| Command   | Purpose   |
|---|---|
| <code>ip igmp static-group<br/>group-address</code> | Configures the router as a statically connected member of a group |

Для того чтобы получить информацию о multicast группах напрямую подключенных к маршрутизатору информация о которых была получена с помощью IGMP используется команда `show ip igmp interface`. Эта команда дает возможность узнать такую информацию:

- Настройка интерфейса для multicast и IGMP
- Версия IGMP что используется на интерфейсе
- IGMPv2 предпочитаемой запросчик для сети с множественным доступом
- Избранный маршрутизатор Multicast
- Обледененные multicast группы на текущем маршрутизаторе

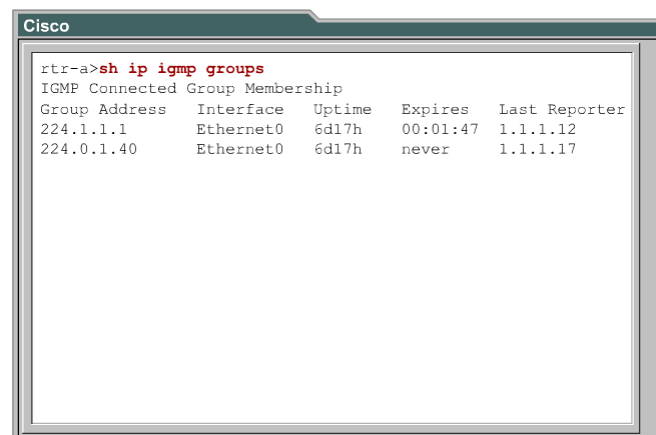


```
Cisco
rtr-a>show ip igmp interface e0
Ethernet0 is up, line protocol is up
Internet address is 1.1.1.1, subnet mask is 255.255.255.0
IGMP is enabled on interface
Current IGMP version is 2
CGMP is disabled on interface
IGMP query interval is 60 seconds
IGMP querier timeout is 120 seconds
IGMP max query response time is 10 seconds
Inbound IGMP access group is not set
Multicast routing is enabled on interface
Multicast TTL threshold is 0
Multicast designated router (DR) is 1.1.1.1 (this system)
IGMP querying router is 1.1.1.1 (this system)
Multicast groups joined: 224.0.1.40 224.2.127.254
```

На картинке 2 маршрутизатор сам включается в следующее 2 группы:

- 224.0.1.40 group: Auto RP, избранно автоматически маршрутизатором
- 224.2.127.254 group: SDR, настроено командой `ip sdr listen`

Для того чтобы получить информацию о multicast группах напрямую подключенных к маршрутизатору информация о которых была получена с помощью IGMP используется команда `show ip igmp groups`.



```
Cisco
rtr-a>sh ip igmp groups
IGMP Connected Group Membership
Group Address  Interface  Uptime    Expires   Last Reporter
224.1.1.1      Ethernet0  6d17h     00:01:47  1.1.1.12
224.0.1.40     Ethernet0  6d17h     never     1.1.1.17
```

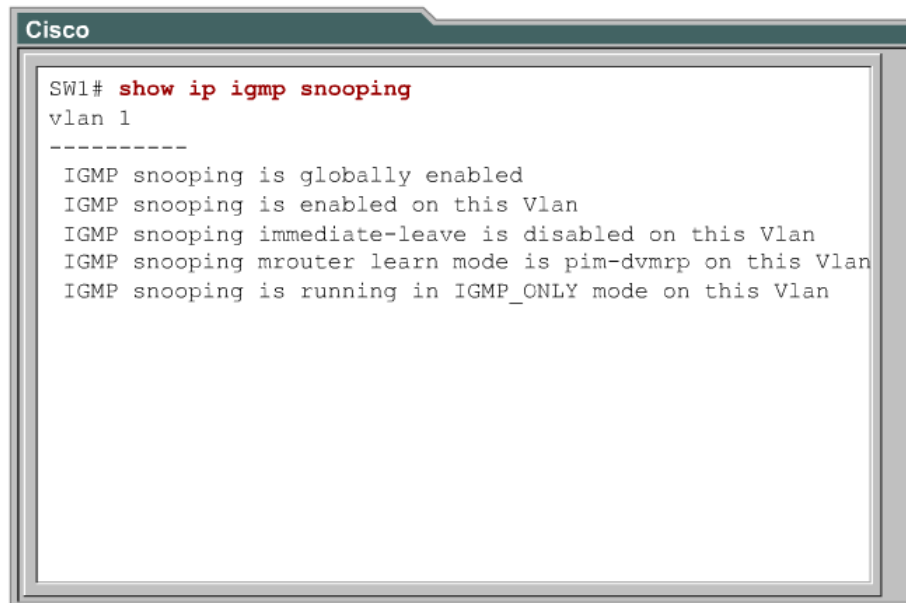
На (картинке 3) маршрутизатор распознает следующее 2 multicast группы:

- Группа 224.1.1.1 активна на интерфейсе Ethernet0 в течении 6 дней и 17 часов. Таймаут этой группы истечёт через 1 минуту и 47 секунд и будет удалена если IGMP Host не подтвердит свое членство в этой группе до этого времени. Последним узлом что подтвердил свое членство в группе был 1.1.1.12
- Группа 224.0.1.40 (auto RP) в эту группу автоматически входят все Cisco маршрутизаторы , и в ней нет ограничений во времени существования.

#### 4.8 Проверка IGMP Snooping

Для проверки IGMP snooping на коммутаторе используется команда `show ip igmp snooping`, она выводит информацию о настройке IGMP snooping для всех или указанного VLAN на коммутаторе (картинка 1).

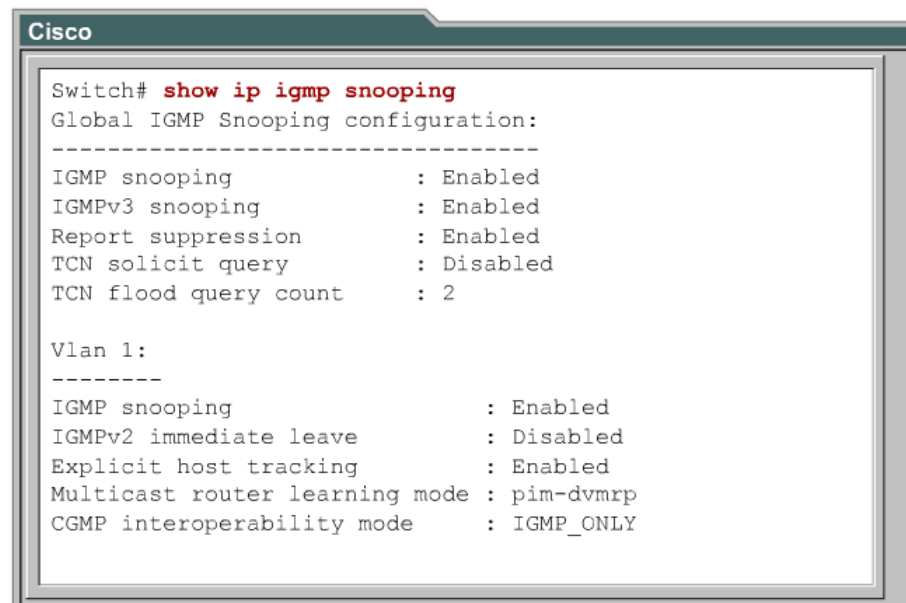




```
Cisco
SW1# show ip igmp snooping
vlan 1
-----
IGMP snooping is globally enabled
IGMP snooping is enabled on this Vlan
IGMP snooping immediate-leave is disabled on this Vlan
IGMP snooping mrouter learn mode is pim-dvmrp on this Vlan
IGMP snooping is running in IGMP_ONLY mode on this Vlan
```

IGMP snooping по умолчанию включена глобально и для каждого VLAN на коммутаторе SW1. В этом случае IGMP snooping идентифицирует порт коммутатора как порт multicast маршрутизатора только в том случае если он видит сообщение PIM или DVMRP отправление в направлении коммутатора на данном порту.

(Картинка 2) показывает простой пример вывода команды show ip igmp snooping на коммутаторе Catalyst 4000. Этот формат вывода будет отличаться для разных моделей Catalyst коммутаторов.



```
Cisco
Switch# show ip igmp snooping
Global IGMP Snooping configuration:
-----
IGMP snooping                : Enabled
IGMPv3 snooping              : Enabled
Report suppression           : Enabled
TCN solicit query            : Disabled
TCN flood query count        : 2

Vlan 1:
-----
IGMP snooping                : Enabled
IGMPv2 immediate leave       : Disabled
Explicit host tracking        : Enabled
Multicast router learning mode : pim-dvmrp
CGMP interoperability mode    : IGMP_ONLY
```

Вы также можете использовать команду show mac-address-table multicast для того чтобы посмотреть таблицу MAC адресов для VLAN на которых включен IGMP snooping. (картинка 3 )

```
SW1# show mac-address-table multicast
```

| Vlan | Mac Address    | Type | Ports               |
|------|----------------|------|---------------------|
| ---- | -----          | ---- | -----               |
| 1    | 0100.5e00.0128 | IGMP | Fa0/1               |
| 1    | 0100.5e07.0707 | IGMP | Fa0/1, Fa0/3, Fa0/5 |

## Основы IPv6

### 1.1 Введение в IPv6

Для возможности дальнейшего увеличения и хорошей масштабируемости вашей сети необходимо преодолеть достаточно серьезную проблему: ограничения на количество доступных IP адресов. Протокол IP версии 6 (IPv6) позволяет решить эту проблему увеличив пространство адресов, а так же более функционального заголовка IP-пакета. IPv6 может обеспечить улучшенную иерархическую структуру адресов по сравнению с IP-адресами v4. Одно из ключевых преимуществ увеличенного адресного пространства это возможность отказаться от технологии NAT (Network Address Translation Трансляция Сетевых Адресов) в сетях большого размера. Поддержка протокола IPv6 в маршрутизатор Cisco начинается с операционной системы *Cisco IOS Software Release 12.2(2)T* и более поздние. Поскольку на сегодняшний день большая часть сети Интернет использует IP-адреса v4, произвести быстрый и полный переход на IP-адреса v6 не возможно. Поэтому переход будет происходить постепенно с одновременным использованием IP-адресов v4 и v6. Длина IP-адресов v6 составляет 128бит. Такое количество адресов позволяет каждому жителю планеты предоставить отдельный IP-адрес. Это окончательно решит проблему нехватки адресов.

### 1.2 Свойства IPv6

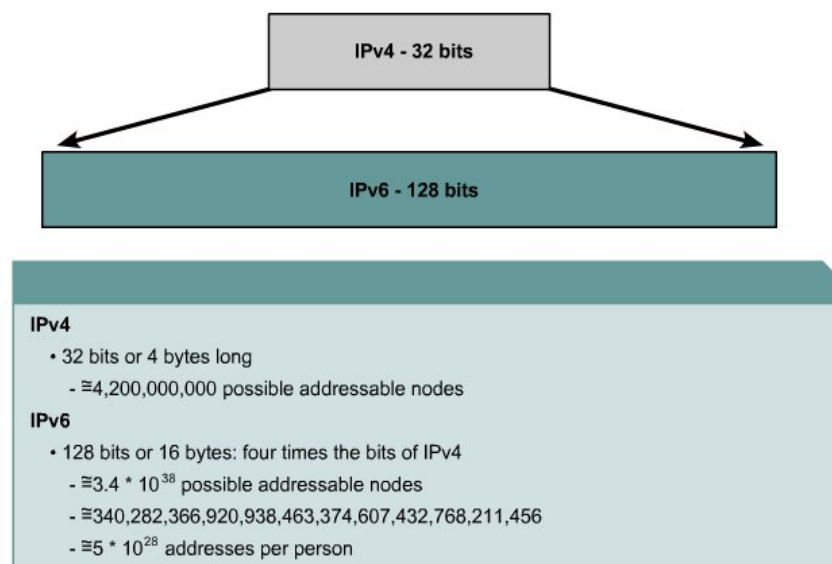
IPv6 является очень сильной заменой протокола IPv4 он предлагает такие нововведения:

- **Увеличенное адресное пространство:** Позволяет увеличить размер и гибкость сети; повысить оптимизацию таблиц маршрутизации; упростить работу одновременно с несколькими ISP провайдерами; использовать автоматическую настройку сетевых интерфейсов на основе MAC-адресов; упростить соединения частных и публичных сегментов сети.
- **Упрощенный (более короткий) заголовок:** Позволяет увеличить скорость маршрутизации пакетов; отсутствие широковещательной рассылки пакетов и как следствие широковещательных штормов; отсутствие контрольной суммы; возможность добавление расширений к заголовку; возможность классификации трафика без просмотра заголовка транспортного уровня.
- **Мобильность и безопасность:** поддержка стандарта Mobile IP который позволяет мобильным устройствам переключаться между протоколами IPv4 и IPv6 без разрыва соединения (мобильное устройство должно поддерживать этот стандарт); встроенная поддержка технологии IPsec которая осуществляет функцию шифрование по умолчанию при обмене данными между IPv6 узлами сети.
- **Гибкий переход:** сетевой интерфейс может поддерживать работу одновременно с двумя протоколами IPv4 и IPv6; поддержка туннеля 6to4 который позволяет в пакетах IPv4 передавать пакеты IPv6;

### 1.3 Увеличенное адресное пространство

Количество адресов по сравнению с IPv4 увеличено в 4 раза и составляет 128 бит. Однако как и в любой другой адресной схеме не все адреса доступны для использования. На сегодняшний день в протоколе IPv4 нехватка адресного пространства временно была решена с помощью технологии Трансляции сетевых адресов (NAT). А приоритизация трафика с помощью технологии QoS.

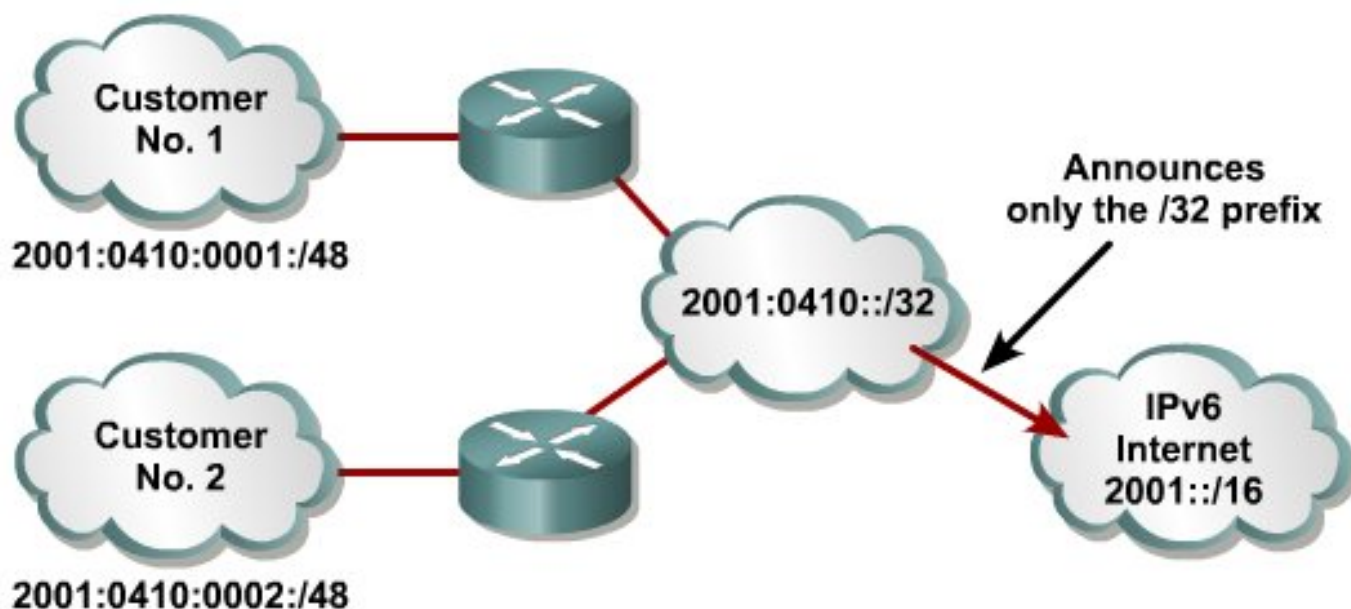
Технология IPv6 позволяет назначить реальный адрес большому числу личных устройств пользователя: коммуникаторам, мобильным телефонам, домашним медиа-центрам и т.д. Что



позволит этим устройствам работать в сети без технологий трансляции или временного назначения адреса. В связи с увеличенным размером IP-адреса были увеличены поля заголовка отвечающие за адреса отправителя и получателя. Их суммарный размер стал составляет 256 бит в сравнение с 64 битами для заголовка IPv4.

*Примечание: Более подробно об особенностях адресации IPv6 можно прочитать в RFC 3513*

Увеличенное адресное пространство упрощает ISP провайдерам раздачу адресов и оптимизацию маршрутных таблиц. Это можно сделать объединив все реальные адреса пользователей в одну IP-сеть без различных технологий трансляции или временной выдачи IP-адреса.



## 2.1 Архитектура IPv6 адресов

IPv4 Header

|                     |          |                 |              |                 |
|---------------------|----------|-----------------|--------------|-----------------|
| Version             | IHL      | Type of Service | Total Length |                 |
| Identification      |          |                 | Flags        | Fragment Offset |
| Time to Live        | Protocol | Header Checksum |              |                 |
| Source Address      |          |                 |              |                 |
| Destination Address |          |                 |              |                 |
| Options             |          |                 | Padding      |                 |

IPv6 Header

|                     |               |             |           |  |
|---------------------|---------------|-------------|-----------|--|
| Version             | Traffic Class | Flow Label  |           |  |
| Payload Length      |               | Next Header | Hop Limit |  |
| Source Address      |               |             |           |  |
| Destination Address |               |             |           |  |

Заголовок IP-пакета v4 состоит из 12 основных полей длина которых составляет 20 байт. Размер заголовка может быть больше за счет необязательного поля переменной длины Options. Заголовок IP-пакета v6 состоит только из пяти полей. Остальные поля не требуются.

Поскольку в протоколе IPv4 предусмотрена процедура фрагментации пакетов это приводит к значительному увеличению служебной информации в заголовке IP-пакета. Маршрутизаторы которые работают по протоколу IPv6 не выполняют фрагментацию, что приводит к уменьшению служебной информации в заголовке IP-пакета. Вместо фрагментации маршрутизаторы работающие по протоколу IPv6 определяют MTU(maximum transmission unit, доступный максимальный размер пакета ) до конечной цели в рамках конкретной сессии.

На начальном этапе исходное IPv6 устройство пытается отправить пакет размером который был указан одним из верхних уровней (транспортным или приложений). В случае получения в ответ ICMP-сообщения о том что пакет слишком велик, выполняется отправка пакета MTU-discover уменьшенного размера до тех пор, пока его размер не будет удовлетворять

всем промежуточным устройствам. После этого новое значение MTU устанавливается для всей сессии.

Кроме того в ICMP-сообщении о том что пакет слишком велик может содержаться предлагаемый размер MTU. Для каждой сессии определяется свое значение MTU. Информация о MTU сохраняется в кэше на основании IP-адреса получателя. Если выполняется маршрутизация от источника то определение MTU может выполняться на основании адреса отправителя.

Поскольку топология сети может периодически изменяться то процедура определения MTU для каждой сессии позволит определять наиболее оптимальное значение MTU. В случае если устройство получает ICMP-сообщения о том что пакет слишком велик в нем будет содержаться рекомендуемое значение MTU которое будет обязательно меньше текущего.

По умолчанию каждое устройство работающее по протоколу IPv6 выполняет определение MTU каждые 5 минут для возможности его увеличения. После этого вышестоящие уровни будут использовать значение MTU полученное от сетевого уровня.

Если вышестоящие уровни не согласны использовать MTU полученное от сетевого уровня, то IPv6 может выполнить фрагментацию исходного пакета, однако промежуточные устройства этого делать не могут.

На канальный уровень ложится задача по расчету контрольной суммы и выявления ошибок для каждого пакета. Поскольку на канальном уровне эти функции реализованы достаточно надежно они были убраны из функций сетевого уровня. А в случае необходимости данную функцию могут выполнять протоколы транспортного уровня.

## 2.2 Сравнение заголовков IPv4 и IPv6.

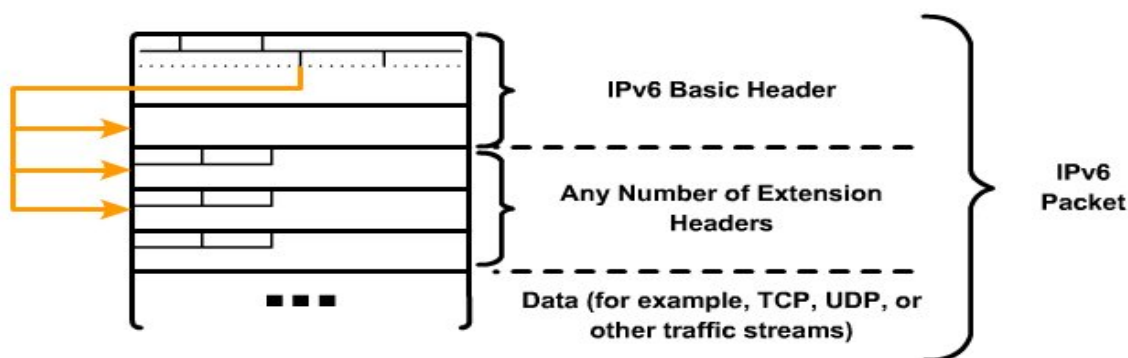
Длина IPv6-заголовка составляет 40байт, длина IPv4-заголовка 20байт. Количество полей меньше, а длина каждого слова составляет 64бита, для более быстрой обработки новыми процессорами. Длина IP-адреса составляет 128бит что 4 раза длиннее чем у IPv4.

IPv6-заголовок содержит такие поля:

- **Version(Версия)** — длина поля составляет 4бита и указывает версию протокола IP.
- **Traffic Class(Класс трафика)** — длина поля 8 бит. Назначение поля соответствует полю ToS пакета IPv4. Позволяет выполнять приоритезацию трафика.
- **Flow Label(метка потока)** — длина поля 20бит. Используется для оптимизации процесса коммутации с помощью маркировке потоков данных.
- **Payload Length (Размер пакета)** — указывается полный размер IP-пакета;
- **Next Header (Следующий заголовок)** — указывает какому протоколу транспортного уровня предназначен IP-пакет;
- **Hop Limit (Лимит хопов)** — указывает максимальное число хопов (промежуточных маршрутизаторов) через которые может пройти IP-пакет;
- **Source Address (адрес отправителя)** — длина поля 16 байт. Указывается IP-адрес узла отправителя;
- **Destination Address (адрес получателя)** — длина поля 16 байт. Указывается IP-адрес узла получателя;
- **Extension Headers (поля расширений)** — необязательные поля переменной длины.

## 2.3 Поля расширения IPv6

Существует большое количество полей расширений. В случае если в одном пакете используется одновременно дополнительных полей расширений они должны следовать в следующем порядке:



- IPv6 header — основной заголовок пакета;
- Hop-by-hop options header — добавляется в случае использования Resource Reservation Protocol [RSVP] и Multicast Listener Discovery version 1 [MLDv1]. По умолчанию данное поле установлено в 0 и обрабатывается каждым промежуточным маршрутизатором.
- Destination options header (используется только в случае применения следующего заголовка) - Этот заголовок обрабатывается первым получателем, адрес которого указан в поле адреса назначения основного заголовка получателями, перечисленными в заголовке маршрутизации (Routing);
- Routing header — используется для маршрутизации от источника;
- Fragment header — используется для фрагментации пакета;
- Authentication header and Encapsulating Security Payload header — используется для IPsec аутентификации;
- Upper-layer header — указывается протокол транспортного уровня которому нужно передать пакет.

## 2.4 Определение адресного пространства

Длина IPv6-адреса составляет 128 бит. Адрес разделен на 8 сегментов по 16 бит. Каждый сегмент записывается в 16 системе счисления в диапазоне от 0x000 до 0xFF F разделенных двоеточием. Буквы A, B, C, D, E, F не чувствительны к регистру.

Особенности использования IPv6-адресов:

- Если впереди числа находится 0, его можно исключить (09C0 = 9C0)
- Если сегмент адреса или несколько сегментов подряд содержит только 0, то их можно заменить на ::
- Если весь адрес состоит из 0, то адрес можно заменить ::

```
- 2031:0000:130F:0000:0000:09C0:876A:130B
- 2031:0:130f::9c0:876a:130b
- 2031::130f::9c0:876a:130b ← Incorrect

- FF01:0:0:0:0:0:0:1 → FF01::1

- 0:0:0:0:0:0:0:1 → ::1
- 0:0:0:0:0:0:0:0 → ::
```

Использование «:» позволяет значительно сократить длину адреса и повысить удобство его использования.

*Примечание: Если в адресе содержится несколько сегментов состоящих только из 0, то можно только один сегмент заменить на ::*

## 2.5 Типы IPv6 адресов

Структура IPv6 адресов описана в RFC 3513 и в RFC 4291. Эти документы описывают 3 типа адресов:

- Unicast адреса
- Multicast адреса
- Anycast адреса

### Unicast адреса

Unicast адреса предназначены для идентификации конкретного устройства в сети. Пакет отправленный на Unicast адрес доставляется на идентифицируемый с помощью адреса интерфейс. Существует 2 типа Unicast адресов:

- **Link-local unicast address (локальный Unicast адрес)** — может использоваться только в рамках локальной сети (аналог автономных адресов IPv4);
- **Global unicast address (глобальный Unicast адрес)** — может использоваться в сетях любого размера (аналог реальных адресов IPv4).

Каждый интерфейс должен иметь минимум 1 локальный Unicast адрес. Однако интерфейс может иметь одновременно несколько адресов всех трех типов.



## Multicast адреса

Поскольку в IPv6 не используются широковещательные адреса, то вместо них применяются Multicast адреса. Этот тип адресов позволяет подставлять пакеты с данными одновременно нескольким сетевым интерфейсам. Для этого используются Multicast группы, которые позволяют отправлять данные ограниченной группе узлов. Количество Multicast адресов IPv6 значительно превышает количество Multicast адресов IPv4.

## Anycast адреса

В протоколе IPv6 появился новый тип адресов - Anycast адреса. Anycast адрес может ссылаться одновременно на несколько интерфейсов одного узла. Пакет отправленный на Anycast адрес будет доставлен на ближайший интерфейс узла определенный с помощью протокола маршрутизации. Anycast адрес не может использоваться в качестве адреса отправителя.

В протоколе IPv6 зарезервированно несколько специальных IP-адресов:

**::/128** - может использоваться только при разработке программного обеспечения;

**::1/128** — Локальный адрес кольцевого интерфейса. Используется для обращения к самому себе (Аналог 127.0.0.1 в IPv4).

**2001:db8::/32** - Везде, где приводятся примеры IPv6-адресов, следует использовать адреса этого диапазона.

**fe80::/10** - локальный префикс, указывает, что адрес является действительным только внутри местной физической сети. Это аналог автоконфигурации IP адреса 169.254.0.0/16 в IPv4.

**ff00::/8** - многоадресный префикс используется для Multicast рассылки

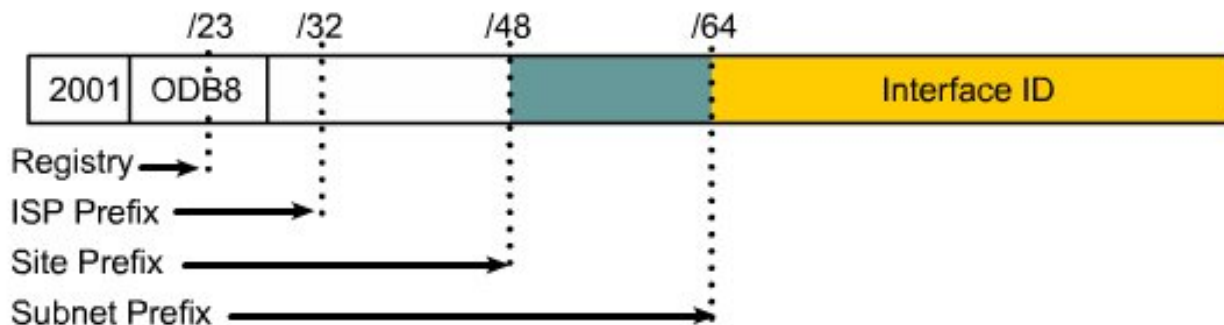
## 2.6 Глобальные Unicast и Anycast адреса.

Глобальные Unicast и Anycast адреса используют одинаковый формат. Anycast адреса используют часть адресного пространства Unicast адресов. Эти адреса рассматриваются как Unicast адреса устройств которые не настраивались для использования Anycast адресов. Когда один Unicast назначен нескольким интерфейсам одного узла он автоматически становится Anycast адресом. Пакет отправленный на Anycast адрес доставляется на ближайший интерфейс узла. Отправитель формирует пакет, в качестве адреса получателя указывает Anycast адрес и отправляет пакет ближайшему маршрутизатору. Отправитель на основании Anycast адреса может контролировать маршрут по которому следует пакет.

Anycast может использоваться в случае если пользователь подключен одновременно к нескольким ISP, т.е. имеет одновременно несколько подключений к сети Internet. Пользователь может использовать Anycast адрес для всех своих подключений. Таким образом отправитель сможет определить кратчайший путь до пользователя. Другой пример использования Anycast адресов это возможность подключения локальной сети одновременно к нескольким ISP через разные маршрутизаторы. Маршрутизаторам назначается единый Anycast адрес, а промежуточные устройства сами будут определять кратчайший путь до локальной сети.

IPv6 глобальный Unicast адрес по своему назначению полностью соответствует IPv4 глобальному Unicast адресу. Структура адресов позволяет иметь общие префиксы для оптимизации таблиц маршрутизации как в рамках сегментов сетей организаций так и в рамках сегментов сетей провайдеров. Глобальный Unicast адрес состоит из двух сегментов: идентификатор сети и идентификатор интерфейса.

IPv6 Unicast адреса охватывают все доступное адресное пространство за исключением диапазона FF00::/8 который используется для Multicast адресов. Текущая выдача Unicast адресов осуществляется организацией Internet Assigned Numbers Authority (IANA) из диапазона 2000::/3 который является 1/8 частью всего адресного пространства.



Сетевая часть адреса состоит из двух префиксов: 48 бит — глобальный префикс маршрутизации и 16 бит идентификатор сети. В соответствии со стандарт RFC 2374 глобальный префикс маршрутизации имеет иерархическую структуру и состоит из двух частей: Top Level Aggregator and Next-Level Aggregator. Поскольку некоторые существующие сети используют старую архитектуру 16 битное поле Subnet prefix может использоваться внутри организации для

построения их собственно иерархической системы подсетей. Каждой организации доступно 65536 подсетей.

### 3. Динамические IPv6 адреса

#### 3.1 Определение адресов интерфейса хоста.

Адрес IPv6 состоит из двух частей:

- Префикс подсети – представляет собой сеть к которой подключен интерфейс. Префикс подсети имеет фиксированную длину в 64 bit.

- Локальный идентификатор (иногда называю token), который уникально идентифицирует хост в локальной сети. Локальный идентификатор имеет фиксированную длину 64 bit и создается динамически в зависимости от используемой технологии и инкапсуляции. Например если в качестве технологии выступает Ethernet то локальный идентификатор создается из EUI-48 MAC адреса устройства. В IPv6 адресе 64 bit локальный идентификатор является уникальным в пределах локальной сети, другими словами в пределах среды передачи в которой для передачи пакетов между узлами используется только канальный уровень. Функции префикса подсети в IPv6 такие же как и в IPv4.

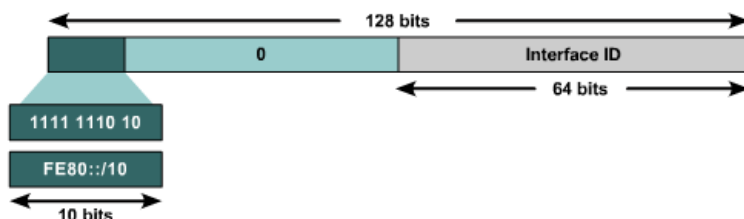
#### 3.2 Локальные адреса (Link-local address)

Локальные адреса уникальны в пределах локальной сети и не могут быть переданы за ее пределы. Маршрутизаторы не пересылают пакеты которые содержат в себе локальные адреса, потому что они не проверены на уникальность за пределами локальной сети. Локальные адреса создаются динамически и содержат link-local prefix **FE80::/10** и 64 bit идентификатор интерфейса. Процесс создания такого адреса называется - автоконфигурация без запоминания состояния (**stateless autoconfiguration**) .

Локальный адрес используется для:

- Автоматической конфигурации адреса интерфейса
- При определении соседей
- Определении маршрутизаторов
- Используется многими протоколами маршрутизации

Структура Link-local адреса представлена на рисунке.



#### 3.3 Автоконфигурация без запоминания состояния (**Stateless Autoconfiguration**)

Автоконфигурация без запоминания состояния (**Stateless Autoconfiguration**)- свойство IPv6 позволяющее хостам автоматически конфигурировать интерфейсы без использования серверов DHCP и ручной настройки. Используя автоматическую конфигурацию любое устройство IPv6 может самостоятельно создать свой IPv6 адрес и после проверки его уникальности в пределах сети использовать его для выхода в сеть.

Для систем подключающихся к сети использующей технологию Ethernet процесс автоматического создания адреса делится на несколько этапов:

1. На первом этапе создается уникальный идентификатор Ethernet интерфейса. Для этого используется EUI-48 MAC адрес который модифицируется с использованием алгоритма описанного в IEEE EUI-64. Например: Имеется исходный MAC адрес 00-0C-29-C2-52-FF после преобразования адреса в соответствии со стандартом EUI-64 получим : 00-0C-29-**FF-FE**-C2-52-FF. Если IPv6 адрес будет локальным то уникальный идентификатор будет иметь такой вид: 000C:29FF:FEC2:52FF. Если же IPv6 адрес будет глобальным то правильный формат идентификатора будет: 020C:29FF:FEC2:52FF.

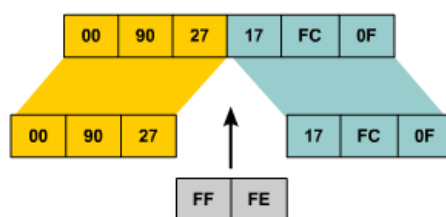
2. На втором этапе к 64 bit идентификатору который определили на 1 этапе добавляется link-local префикс **fe80::/64** для создания 128 bit локального (link-local) адреса. Например **fe80::20c:29ff:fec2:52ff** полученный адрес назначается интерфейсу и помечается как «предварительный» («tentative»).

3. Перед тем как адрес будет окончательно назначен интерфейсу необходимо проверить его уникальность в пределах сети, этот процесс называется duplicate address detection DAD (определение дублирующихся адресов). Адрес может быть не уникален, если в сети присутствует два устройства с одинаковыми MAC адресами, а значит перед тем как применить адрес необходимо проверить его уникальность. Для проверки уникальность хост посылает ICMPv6 запрос обнаружения «соседнего» узла, в котором в качестве адреса источника указан неопределенный адрес «:::», а в качестве адреса назначения «предварительный» («tentative») адрес который был создан на втором этапе. Если на этот запрос не последовало ответа то адрес считается уникальным и может быть назначен интерфейсу. Если ответ на запрос пришел. Значит адрес не уникален и не может быть применен, в таком случае требуется ручная настройка интерфейса.

4. На этом этапе снимается метка «предварительный» с адреса и он назначается интерфейсу. Теперь можно использовать интерфейс для обмена данными с другими узлами сети.

### 3.4. Преобразование MAC адреса по стандарту EUI-64 в IPv6 идентификатор.

MAC адрес (IEEE 802) имеет длину 48 bit размер же идентификатора IPv6 составляет 64 bit. Стандарт EUI-64 определяет процедуру преобразования 48 bit MAC адреса в 64 bit идентификатор, для этого посередине MAC адреса вставляется 0xFFFFE и получается 64 bit значение которое и становится IPv6 идентификатором. Например преобразуем MAC адрес 00-90-27-17-FC-0C используя стандарт EUI-64, для этого по середине вставим значение 0xFFFFE и в результате получим вот такой идентификатор IPv6 0090:27FF:FE17:FC0C



#### Universal/Local (U/L)

Седьмой бит в идентификаторе IPv6 показывает, кем управляется адрес и называется **Universal/Local (U/L) bit**.

- Если U/L бит установлен в 0 (local) то адрес является локальным и управляется администратором сети. И может быть изменен путем изменения MAC адреса.
- Если U/L бит установлен в 1 (Universal) то в этом случае адрес управляется IEEE через ISP.

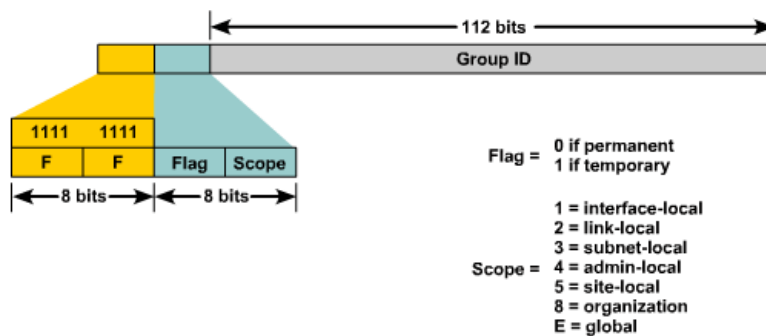
#### Individual/Group (I/G)

Восьмой бит в идентификаторе IPv6 определяет является ли адрес индивидуальным (unicast) или групповым (multicast) и называется **Individual/Group (I/G) bit**. Если бит установлен в 0 то адрес является индивидуальным, если же он установлен в 1 то адрес групповой.

### 3.5 Групповые рассылки (Multicasting) в IPv6.

Групповой адрес назначается группе интерфейсов, пакеты посланные на групповой адрес принимаются всеми интерфейсами участвующими в групповой рассылке. Один и тот же интерфейс может находится в нескольких группах. Multicasting в IPv6 важен, так как IPv6 поддерживает множество функций связанных именно с групповыми рассылками.

Групповой адрес имеет следующий формат:



• Начинается IPv6 multicast адрес с префикса **FF00::/8**. Второй октет префикса содержит флаг, указывающий на то, является ли групповой адрес постоянным (permanent) или временным (temporary). После флага остальные семь бит занимают параметр scope указывающий на область действия группового адреса.

• Если flag установлен в 0, то групповой адрес является постоянным, значение флага 1 указывает на то что адрес временный.

• Параметр scope может принимать следующие значения:

**1** - зона действия адреса loopback интерфейс

**2** - зона действия адреса unicast link-local

**3** - зона действия адреса локальная подсеть subnet-local

**4** - локальная административная зона

**5** - зона действия адреса site-local

**8** - Организация является зоной действия адреса (диапазон в котором объединяются несколько site-local зон)

**E** - область действия адреса глобальная сеть.

Например адрес **FF02::/16** - постоянный групповой адрес с link-local областью действия

• Завершает multicast адрес Group ID имеющий длину 112 bit

Адреса групповая рассылка наиболее часто используются в IPv6 и заменяют собой широковещательную. В адресах групповой рассылки отсутствует TTL (Time to Live) а область действия указывается внутри самого адреса групповой рассылки.

### 3.6. Постоянные групповые адреса.

В IPv6 существует зарезервированный диапазон постоянных групповых адресов, начинается он с адреса **FF00::** и заканчивается **FF0F::**. Ниже приведено несколько примеров адресов из этого диапазона которые назначаются и отслеживаются IANA.

• **FF02::1** - все узлы в локальной сети (область действия Link-local)

• **FF02::2** - все маршрутизаторы в локальной сети.

• **FF02::9** - все маршрутизаторы в локальной сети поддерживающие IPv6 RIP

• **FF05::101** - все сервера NTP в пределах сайта (область действия site-local)

### 3.7. Anycast адреса

IPv6 anycast адрес является глобальным адресом индивидуальной рассылки, который назначен на более чем один интерфейс. Когда пакет посылают на адрес anycast, он направляется к "самому близкому" интерфейсу, имеющему такой же адрес. В глобальных сетях «самый близкий» интерфейс будет определяться с помощью протокола маршрутизации по самой короткой дистанции. В локальных сетях самый близкий интерфейс соответствует самому близкому соседу который будет найден.

Следующие характеристики свойственны anycast адресу:

• Anycast адреса распределяются из адресного пространства адресов индивидуальной (unicast) рассылки, поэтому anycast адрес практически не отличим от unicast адреса и должен быть явно сконфигурирован при настройке интерфейсов.

• В 1993 была предложена идея anycast в IP. Для IPv6 anycast определен как способ послать пакет в самый близкий интерфейс, который является членом anycast группы.

• Адрес anycast не должен использоваться как адрес источника в пакета IPv6.

### 3.8. Мобильность IPv6

Мобильность - очень важная функция в современных сетях. Мобильный IP - стандарт IETF, доступный и для IPv4 и для IPv6. Мобильный IP дает возможность перемещаться мобильным устройствам без обрыва текущего подключения. В IPv6 мобильность встроенная функция, что означает, что любой узел IPv6 может использовать возможность перемещения между точками доступа в сети без дополнительных модификаций протокола. В IPv4 в отличие от IPv6, мобильность - новая функция, которую необходимо добавлять в протокол.

Заголовки маршрутизации IPv6 делают Мобильным IPv6 намного более эффективный для конечных узлов чем Мобильный IPv4. Мобильность использует всю гибкость протокола IPv6.

Мобильность реализованная в IPv6 отличается от мобильности IPv4 следующими свойствами:

- Адресное пространство IPv6 допускает создание Мобильной сети любого размера.
- Модель мобильного IPv6 включает в себя опции которые уже заложены в протоколе, такие как определение соседей, автоматическое конфигурирование и т.д.
- Во многих случаях используется мобильная оптимизация маршрута, позволяющая избежать использование маршрутизатора и пересылать пакеты соседним узлам непосредственно. Такая поддержка оптимизации маршрута является фундаментальной частью протокола IPv6.
- Мобильные узлы работают с другими узлами, которые не поддерживают мобильность (также как и в мобильности которая реализована в IPv4).

#### 4. Описание маршрутизации в IPv6.

IPv6 поддерживается следующими протоколами маршрутизации:

- **Статическая маршрутизация.** Используется и конфигурируется точно также как и в IPv4. Требования, которые специфические для IPv6 описаны в RFC 2461
- **RIPng.** Routing Information Protocol next generation RIPng описан в RFC 2080. Дистанционно векторный протокол имеющий такие же основные свойства как и предыдущие версии RIP. Количество хопов не больше 15, использование split horizon и poison reverse для предотвращения появления маршрутных петель.

Особенности использования IPv6 заключаются в следующем:

Для транспорта используется IPv6

Апдейты посылаются на порт 521

Для апдейтов используется мультикастовый адрес FF02::9

- **OSPFv3.** Реализация протокола для IPv6 включает в себя следующие отличительные особенности:

Базируется на OSPFv2

Работает поверх IPv6

Аутентификация (может использоваться IPSec)

Включена поддержка адресации IPv6

- **IS-IS.** Принципы работы сохранились такие же как и для версии под IPv4. Для IPv6 Добавлены следующие специфические опции:  
Два новых Type, Length, Value (TLV) атрибута  
Поддержка адресации IPv6 для интерфейсов  
Новый протокол ID

**EIGRP.** Enhanced Interior Gateway Routing Protocol (EIGRP), может быть использован, для маршрутизации IPv6. При этом, если EIGRP используется для маршрутизации IPv4, то протокол будет работать исключительно с адресами IPv4. А EIGRP используемый для работы с IPv6 адресами будет работать исключительно только с ними. Таким образом версии EIGRP работающие с IPv4 и с IPv6 настраиваются по отдельности. Сам же процесс конфигурации EIGRP для IPv4 и IPv6 одинаков.

#### Сравнение OSPFv2 и OSPFv3

Протоколы OSPFv2 и OSPFv3 очень похожи между собой, ряд функций присутствуют и в одном и в другом протоколе. Для сравнения схожие функции перечислены ниже:

- Одинаковые механизмы определения соседей и установления отношений соседства между ними
  - Механизмы обмена LSA пакетами одинаковы для OSPFv2 и OSPFv3
  - OSPFv3 использует для своей работы те же типы пакетов что и OSPFv2. Такие как hello packets, database description (database description packet), link-state request (LSR), link-state update (LSU), и LSA
- Основные отличия OSPFv2 и OSPFv3:
- OSPFv3 включается на интерфейсах. Включение OSPF на интерфейсе автоматически создает процесс OSPF и соответствующую команду в конфигурационном файле;
  - Анонсируются все сети настроенные на интерфейсе;
  - Идентификатор маршрутизатора должен быть настроен вручную. Правила выбора идентификатора аналогичны правилам для OSPFv2, однако, если на маршрутизаторе не настроен адрес IPv4, то идентификатор должен быть настроен вручную;
  - Новые типы LSA. Добавлены два новых типа LSA — Link LSA и Intra-Area Prefix LSA;
  - Области распространения LSA. Кроме существующих областей распространения в OSPFv2 — зона и автономная система, добавилась область — канал (области распространения LSA указаны в описании соответствующих LSA);
  - Несколько сущностей (instances) могут быть в пределах канала;
  - Пакеты OSPF отправляются с link-local адреса (за исключением virtual link);
  - Аутентификации в самом OSPFv3 нет. Протокол использует аутентификацию IPv6;

## Типы LSA для IPv6

**Объявление о состоянии канала (LSA)** — единица данных, которая описывает локальное состояние маршрутизатора или сети. Множество всех LSA, описывающих маршрутизаторы и сети, образуют базу данных состояния каналов (LSDB). Ниже приведена таблица типов LSA для OSPFv2 и OSPFv3.

| OSPFv2 |                          | OSPFv3 |                       |
|--------|--------------------------|--------|-----------------------|
| Тип    | Название                 | Тип    | Название              |
| 1      | Router LSA               | 1      | Router LSA            |
| 2      | Network LSA              | 2      | Network LSA           |
| 3      | Network Summary LSA      | 3      | Inter-Area Prefix LSA |
| 4      | ASBR Summary LSA         | 4      | Inter-Area Router LSA |
| 5      | AS-External LSA          | 5      | AS-External LSA       |
| 7      | NSSA External LSA        | 7      | Type-7 LSA            |
| 8      | Нет соответствующего LSA | 8      | Link LSA              |
| 9      | Нет соответствующего LSA | 9      | Intra-Area Prefix LSA |

Описание типов LSA:

**Router LSA** — объявление о состоянии каналов маршрутизатора. Эти LSA распространяются всеми маршрутизаторами. Распространяются только в пределах одной зоны.

**Network LSA** — объявление о состоянии каналов сети. Распространяется DR в сетях со множественным доступом. Network LSA не создается для сетей в которых не выбирается DR. Распространяются только в пределах одной зоны.

**Inter-Area Prefix LSA** — Отправляется ABR и описывает межзональные маршруты для маршрутизаторов в других зонах. Распространяются только в пределах одной зоны.

**Inter-Area Router LSA** — Отправляется ASBR для сообщения о его местонахождении. Распространяются только в пределах одной зоны.

**AS External LSA** — объявления о состоянии внешних каналов автономной системы. Объявление распространяется пограничным маршрутизатором автономной системы в пределах всей автономной системы.



**Type-7 LSA** — объявления о состоянии внешних каналов автономной системы в NSSA зоне. Это объявление может передаваться только в NSSA зоне. На границе зоны пограничный маршрутизатор преобразует type 7 LSA в type 5 LSA.

**Link LSA** — анонсирует link-local адрес и префикс(ы) маршрутизатора всем маршрутизаторам разделяющим канал (link). Отправляется только если на канале присутствует более чем один маршрутизатор. Распространяются только в пределах канала (link).

**Intra-Area Prefix LSA** — ставит в соответствие:

- список префиксов IPv6 и маршрутизатор, указывая на Router LSA,
- список префиксов IPv6 и транзитную сеть, указывая на Network LSA.

Распространяются только в пределах одной зоны.

LSA типы 8,9 добавлены в IPv6 версии протокола OSPF.

## 5. Внедрение и проверка OSPFv3.

### 5.1. Настройка OSPFv3 в IPv6.

Большинство команд OSPFv3 аналогичны командам OSPFv2. В большинстве случаев достаточно заменить **ip** на **ipv6** или добавить **ipv6** к команде. Например, для назначения адреса интерфейсу вместо команды **ip address**, используется команда **ipv6 address**. Для просмотра таблицы маршрутизации IPv6 необходима команда **show ipv6 route**. При этом конфигурация OSPFv3 это не подрежим или подкоманда **router ospf**. Например, вместо использования команды **network area** для идентификации сетей обслуживаемых OSPFv3, интерфейсы на прямую конфигурируются так, что IPv6 сети являются частью сети OSPFv3.

Следующие шаги описывают конфигурацию OSPF для IPv6:

Шаг 1. Спланируйте и создайте стратегию внедрения OSPF в Вашей сети IPv6.

Шаг 2. Включите однонаправленную маршрутизацию IPv6 командой **ipv6 unicast-routing**.

Шаг 3. Включите IPv6 на интерфейсах используя команду **ipv6 ospf area**.

Шаг 4. (Опционально) Настройте специфические параметры OSPFv3 на интерфейсах, такие как область, приоритет маршрутизатора, стоимость пути.

Шаг 5. (Опционально) Настройте специфические параметры маршрутизации: приоритет, объединение маршрутов итд.

#### Таб. 1.

- Схожесть с OSPFv2
- использование команд схожих с командами OSPFv2
- Прямая конфигурация интерфейсов
- нет необходимости использовать команду **network**
- Родной режим IPv6 в маршрутизаторе
- IPv6 не подрежим команды **router ospf**

#### Таб. 2.

| Команда              | Описание  |
|----------------------|---|
| ipv6 unicast-routing | включает пересылку<br>однаправленных датаграмм IPv6 |

### 5.2. Включение OSPFv3 на интерфейсе.

Большая часть конфигурации OSPFv3 производится на интерфейсе. Рисунок 1 показывает простую настройку адреса IPv6, области OSPF, приоритета маршрутизатора и стоимости пути.

#### Рис.1.

```
Router(config-if)#ipv6 address 4ffe:aaaa:2::2/64
Router(config-if)#ipv6 ospf 1 area 0
Router(config-if)#ipv6 ospf priority 25
Router(config-if)#ipv6 ospf cos
Router(config-if)#ipv6 ospf cost 25
Router(config-if)#
```

Таблица 3 приводит описание этих команд.

#### Таб. 3.



| Шаг | Команда или действие  | Цель   |
|-----|---|--|
| 1   | Router(config)# <b>interface</b> <i>type number</i>                                       | Определяет тип и номер интерфейса, переводит маршрутизатор в режим конфигурации интерфейса.  |
| 2   | Router(config-if)# <b>ipv6 address</b> <i>address/prefix-length [eui-64]</i>              | Конфигурирует IPv6 адрес и включает функционирование IPv6 на интерфейсе. Параметр <b>eui-64</b> принуждает маршрутизатор заполнить 64 бита низкого порядка в адресе используя <b>eui-64</b> ID интерфейса. |
| 3   | Router(config-if)# <b>ipv6 ospf</b> <i>process-id area area-id [instance instance-is]</i> | Включает OSPF для интерфейса сконфигурированного в режиме IPv6   |
| 4   | Router(config-if)# <b>ipv6 ospf priority</b> <i>priority number</i>                       | Указание приоритета используется при выборах Designated Router.  |
| 5   | Router(config-if)# <b>ipv6 ospf cost</b> <i>cost</i>                                      | Стоимость отправки пакета на интерфейс выражается в метрике состояния связи.   |

### 5.3. Тонкая настройка OSPFv3.

Тонкая настройка проводится из режима конфигурации маршрутизации. Для перехода в режим конфигурации маршрутизации используйте команду **ipv6 router ospf process-id**. Эта команда включает ospf на маршрутизаторе. Параметр *process ID* идентифицирует уникальный процесс OSPFv3.

Для маршрутизаторов использующих только IPv6 параметр *router ID* должен быть определен при конфигурировании OSPFv3 как адрес IPv4. Для этого используется команда **router-id router-id**. OSPFv3 использует 32 битный номер в качестве *router ID*. *Router ID* выражается в десятичной нотации разделенной точками, таким образом позволяя легко накладывать сеть OSPFv3 на сеть OSPFv2. Рисунок 2 показывает простую конфигурацию *router ID*.

**Рис. 2.**

```
Router(config)#ipv6 unicast-routing
Router(config)#ipv6 router ospf 1
Router(config-rtr)#router
Router(config-rtr)#router-id 255.255.255.255
```

Если на маршрутизаторе настроен IPv4, то по умолчанию *router ID* выбирается так же как и в OSPFv2. Самый высокий IP адрес сконфигурированный на интерфейсе loopback становится *router ID*. Если интерфейсов loopback не сконфигурировано, то выбирается самый высокий адрес любого другого интерфейса.

### 5.4. Объединение маршрутов OSPFv3.

Рисунок 3 показывает состояние маршрутов OSPFv3 до объединения.

**Рис. 3.**

```
OI 2002:1DB9:0:0:7::/64 [110/25]
via FE90::B8AA::CCFF:FE00:6F00, FastEthernet 0/0
OI 2002:1DB9:0:0:8::/64 [110/25]
via FE90::B8AA::CCFF:FE00:6F00, FastEthernet 0/0
OI 2002:1DB9:0:0:9::/64 [110/50]
via FE90::B8AA::CCFF:FE00:6F00, FastEthernet 0/0
```

Для совмещения и объединения маршрутов на границе области используйте команду **area area-id range ipv6-prefix/prefix-length [advertise | not-advertise] [cost cost]**. Рисунок 4 демонстрирует простой пример применения этой команды.

**Рис. 4.**

```
Router(config)#ipv6 router ospf 2|
Router(config-rtr)#area range 1 2002:1DB9:://48
```

Стоимость объединенного маршрута будет равна стоимости самого «дешевого» маршрута из тех, которые были использованы для объединения. Например маршруты из рисунка 3 объединяются в маршрут на рисунке 5.

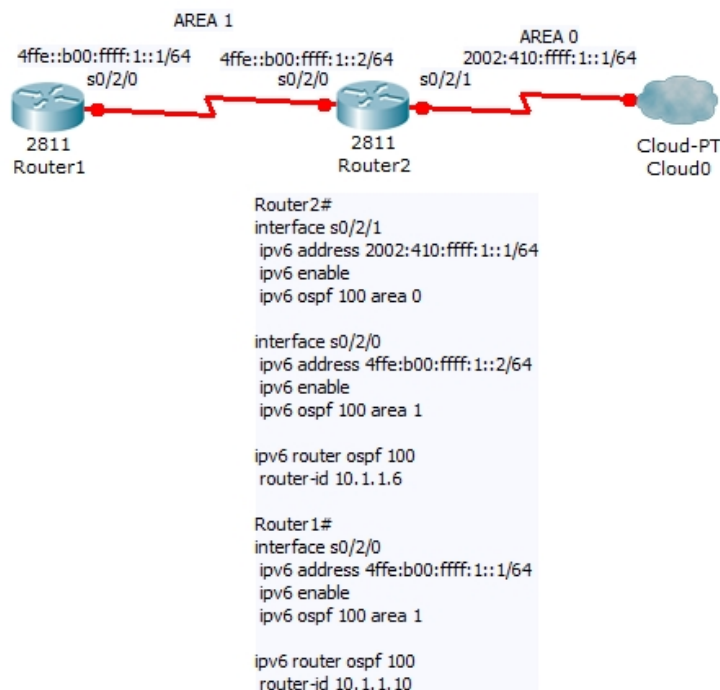
**Рис. 5.**

OI 2002:1DB9::/48 [110/50]  
via FE90::B8AA::CCFF:FE00:6F00, FastEthernet 0/0

### 5.5. Пример конфигурации OSPFv3.

Рисунок 6 демонстрирует сеть OSPF состоящую из 2-х маршрутизаторов обслуживающих области 0 и 1 соответственно. Команда **ipv6 ospf 100 area 0** динамически создает процесс "ipv6 router ospf 100" так же как и команда **ipv6 ospf 100 area 1**.

**Рис. 6.**



### 5.6. Проверка конфигурации OSPFv3.

Существует несколько общих команд группы **show** для OSPFv3, включая **show ipv6 ospf [process-id] [area-id] interface [interface]**. Эта команда генерирует информацию об интерфейсах настроенных на работу с OSPF, как показано на рисунке 7.

**Рис. 7.**

```
Router#show ipv6 ospf interface s0/2/0
Serial0/2/0 is up, line protocol is up
Link Local Address FE80::240:BFF:FEDD:7C01 , Interface ID 3
Area 0, Process ID 100, Instance ID 0, Router ID 255.255.255.255
Network Type POINT-TO-POINT, Cost: 64
Transmit Delay is 1 sec, State POINT-TO-POINT,
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
Hello due in 00:00:02
Index 1/1, flood queue length 0
Next 0x0(0)/0x0(0)
Last flood scan length is 1, maximum is 1
Last flood scan time is 0 msec, maximum is 0 msec
Suppress hello for 0 neighbor(s)
```

**clear ipv6 ospf [process-id] {process | force-spf | redistribution | counters [neighbor [neighbor-interface | neighbor-id]]}** вызывает SPF рекалькуляцию и распространение Базы Информации о Маршрутизации (RIP).

**show ipv6 ospf [process-id] [area-id]** отображает общую информацию об OSPF процессе, как это показано на рисунке 8.

**Рис. 8.**

```

Router#sh ipv6 ospf 100
Routing Process "ospfv3 100" with ID 255.255.255.255
SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs
LSA group pacing timer 240 secs
Interface flood pacing timer 33 msecs
Retransmission pacing timer 66 msecs
Number of external LSA 0. Checksum Sum 0x000000
Number of areas in this router is 0. 0 normal 0 stub 0 nssa
Reference bandwidth unit is 100 mbps

```

Таблица 4 показывает некоторые поля и описание результата работы команды **show ipv6 ospf**.

**Таб. 4.**

| Поле  | Описание   |
|---|--|
| Routing process "ospfv3 1" with ID 172.16.3.3 | Идентификатор процесса - process ID, идентификатор OSPF маршрутизатора |
| LSA group pacing timer                        | Сконфигурированный LSA group pacing таймер (в секундах)                |
| Interface flood pacing timer                  | Сконфигурированный LSA group flood таймер (в миллисекундах)            |
| Retransmission pacing timer                   | Сконфигурированный Retransmission pacing таймер (в миллисекундах)      |
| Number of areas                               | Номера областей маршрутизатора, адресов областей итд.                  |

### 5.7. Проверка соседей OSPFv3.

Что бы отобразить информацию о соседях в OSPF поинтерфейсно, используйте команду **show ipv6 ospf neighbor** в режиме пользователя или в привилегированном режиме.

Команда **show ipv6 ospf neighbor detail** выводит детальную информацию о соседях как показано на рисунке 9.

**Рис. 9.**

```

Router#sh ipv6 ospf neighbor
Neighbor ID    Pri   State           Dead Time   Interface ID  Interface
10.1.1.6       1    FULL/-          00:00:37    3             Serial0/2/0
Router#sh ipv6 ospf neighbor deta
Router#sh ipv6 ospf neighbor detail
Neighbor 10.1.1.6, interface address FE80::260:47FF:FEB5:8D01
  In the area 1 via interface Serial0/2/0
  Neighbor priority is 1, State is FULL, 7 state changes
  DR is 0.0.0.0 BDR is 0.0.0.0
  Options is 0x10
  Dead timer due in 00:00:33
  Neighbor is up for 00:01:06
  Index 1/1, retransmission queue length 0, number of retransmission 0
  First 0x0(0)/0x0(0) Next 0x0(0)/0x0(0)
  Last retransmission scan length is 0, maximum is 0
  Last retransmission scan time is 0 msec, maximum is 0 msec
Router#

```

Таблица 5 отображает информацию о полях и их описании для команды **show ipv6 ospf neighbor**.

**Таб. 5.**

| Поле                   | Описание  |
|------------------------|---|
| Neighbor ID, neighbor  | ID маршрутизатора соседа                            |
| In the area            | Область и интерфейс, через которые был изучен сосед |
| Pri; neighbor priority | Приоритет и состояние соседа                        |

|                                 |   |
|---------------------------------|---|
| State                           | Состояние OSPF  |
| State changes                   | Количество изменения состояния с момента изучения соседа  |
| Options                         | Содержание параметров поля options пакета Hello. (Только внешний бит, e-bit, значение которого 0 или 2: значение 2 указывает что область не является ограниченной, а 0 указывает на ограниченную область) |
| Dead timer due in               | Ожидаемое время через которое IOS объявит соседа мертвым  |
| Neighbor is up for              | Время в часах минутах и секундах, с момента перехода соседа в двухсторонний режим   |
| Index                           | Местонахождение соседа в ретрансмиссионной очереди области и АС   |
| Retransmission queue length     | Количество элементов в ретрансмиссионной очереди  |
| Number of retransmission        | Количество отправок пакета обновления в течении рассылки  |
| First                           | Адреса памяти, в которых находятся детали рассылки  |
| Next                            | Адреса памяти, в которых находятся детали рассылки  |
| Last retransmission scan length | Номер LSA в последнем ретрансмиссионном пакете  |
| Maximum                         | Максимальное количество LSA посланных в ретрансмиссионных пакетах   |
| Last retransmission scan time   | Время, затраченное на создание последнего ретрансмиссионного пакета   |
| Maximum                         | Максимальное время потраченное на создание ретрансмиссионного пакета  |

### 5.8. Проверка базы данных (БД) OSPFv3.

Для просмотра информации касающейся БД OSPF конкретного маршрутизатора используйте команду **show ipv6 ospf database** в режиме пользователя или привилегированном режиме. Различные формы этой команды предоставляют информацию о разных состояниях OSPF.

Рисунок 10 показывает результат работы команды **show ipv6 ospf database**. Таблица 6 показывает описание полей вывода команды **show ipv6 ospf database**.

**Рис. 10.**

```
Router#show ipv6 ospf database
      OSPF Router with ID (10.1.1.10) (Process ID 100)

      Router Link States (Area 1)

ADV Router   Age      Seq#      Link count Bits
10.1.1.10    232     0x80000002 1
10.1.1.6     232     0x80000002 1

      Link (Type-8) Link States (Area 1)

ADV Router   Age      Seq#      Link ID
10.1.1.10    242     0x80000002 3
10.1.1.6     242     0x80000002 3

      Intra Area Prefix Link States (Area 1)

ADV Router   Age      Seq#      Link ID   Ref-lstypе   Ref-LSID
10.1.1.10    242     0x80000001 2         0x2001       0
10.1.1.6     242     0x80000001 2         0x2001       0
Router#|
```

**Таб. 6.**

| Поле       | Описание                      |
|------------|-------------------------------|
| ADV Router | ID advertising маршрутизатора |

|            |   |
|------------|---|
| Age        | Возраст состояния связи   |
| Seq#       | Номер последовательности состояния связи (определяет старые и дублирующиеся адреса) |
| Link ID    | ID номер интерфейса   |
| Ref-lstype | Тип ссылки состояния связи  |

## 6. Использование IPv6 и IPv4.

### 6.1. Механизм трансляции из IPv6 в IPv4.

Трансляция из IPv4 в IPv6 не требует обновления на всех nodes одновременно. Большинство механизмов перехода включают мягкую интеграцию IPv4 в IPv6. Существуют способы позволяющие узлам IPv4 взаимодействовать с IPv6 узлами. Эти механизмы могут быть применены в различных ситуациях.

Две основных техники трансляции из IPv4 в IPv6 следующие:

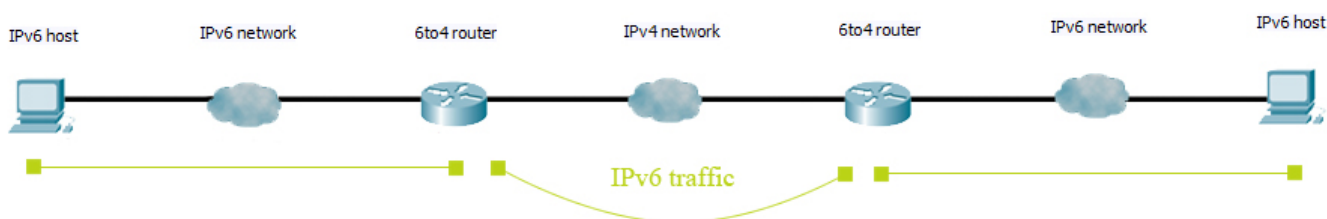
- Двойной стек
- Туннель IPv6 поверх IPv4

Для коммуникации между сетями построенными на IPv4 и IPv6, адреса IPv4 могут быть инкапсулированы в адреса IPv6.

Рисунок 1 показывает примеры механизмов интеграции и трансляции. Маршрутизаторы 6to4 автоматически инкапсулируют трафик IPv6 в пакеты IPv4.

**Рис. 1.**

Трансляция позволяет достичь следующего:



Нет необходимости одновременного обновления всех компонентов сети;  
Доступны разные алгоритмы трансляции:

- двойной стек
- тунелирование 6to4

что дает мягкую интеграция IPv4 и IPv6;

Узлы IPv4 и IPv6 могут взаимодействовать друг с другом.

### 6.2. Двойной стек Cisco IOS.

### 6.3.

Большинство IOS Cisco готово к использованию IPv6. Как только на интерфейсе были сконфигурированы IPv6 и IPv4, интерфейс становится двустековым и может пересылать IPv6 и IPv4 трафик. Использование IPv6 в маршрутизаторах Cisco требует использования команды режима глобальной конфигурации **ipv6 unicast-routing**. Эта команда включает пересылку пакетов IPv6. (Рис. 2.)

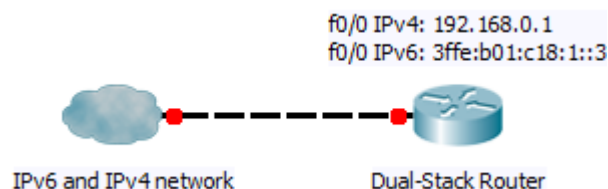
**Рис. 2.**

```

Router>enab
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#ipv6 unicast-routing
Router(config)#interface fastethernet 0/0
Router(config-if)#ip address 192.168.0.1 255.255.255.0
Router(config-if)#ipv6 address 3ffe:b01:c18:1::4/127
Router(config-if)#no shutdown

%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up
Router(config-if)#

```

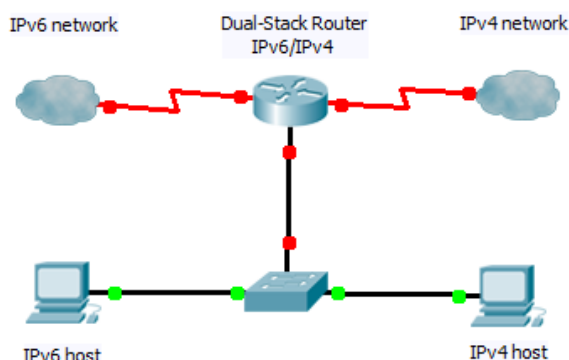


Все интерфейсы, которые пересылают трафик IPv6 должны иметь IPv6 адреса. Команда `ipv6 address` позволит назначить адрес IPv6 на интерфейс.

Метод двойного стека это метод интеграции, когда нод подключается одновременно к сети IPv4 и IPv6, и поэтому имеет 2 стека. (Рис 3.) Такая конфигурация может быть настроена как на один, так и на несколько интерфейсов. Относительно двухстековости можно заключить следующее:

- Двустековый нод выбирает, какой стек использовать на основании адреса назначения. Предпочтение всегда отдается стеку IPv6. Двустековый режим интеграции, в котором узлы имеют оба стека - IPv4 и IPv6, будет одним из самых распространенных. Устаревшие IPv4 приложения, как и раньше будут использовать старый стек, новые приложения получают преимущества обоих стеков.
- Новый API создан для поддержки обоих типов адресации - IPv4 и IPv6, а так же поддержки DNS запросов. Этот API заменяет `gethostbyname` и `gethostbyaddr` запросы. Таким образом новые приложения смогут использовать оба стека как IPv4 так и IPv6. При этом старые приложения реализованные в новом API смогут работать с стеком IPv4.
- Накопленный опыт в портировании приложений IPv4 на IPv6 стек свидетельствует о необходимости внесения минимальных изменений в исходный код. Эта техника хорошо известна и опробована в прошлом при переходе с одного протокола на другой. Это дает возможность постепенно переходить на новый стек.

**Рис. 3.**

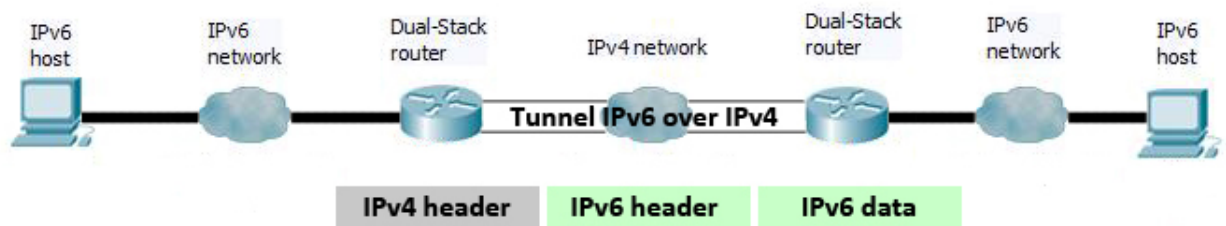


### 6.3. Туннели.

Туннели часто используются для покрытия несовместимой функциональности существующих сетей. Туннелирование трафика IPv6 в IPv4 требует наличие пограничного маршрутизатора, для инкапсуляции пакетов IPv6 в пакеты IPv4, а так же маршрутизатора с другой стороны туннеля для декапсуляции этого трафика. (Рис. 4.)



**Рис. 4.**



Эта технология позволит подключить области с IPv6 без необходимости конвертации всей сети в IPv6.

Туннелирование интеграционный метод, в котором пакет IPv6 инкапсулируется в пакет другого протокола – в частности IPv4.

Этим методом инкапсуляции является протокол 41 IPv4, который имеет следующие характеристики:

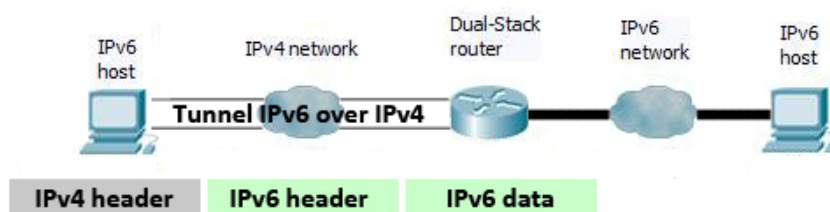
- Заголовок IPv4 без опций + заголовок IPv6 + полезная нагрузка;
- Продуманный двойной стек, который не требует конвертации IPv6 для подключения областей IPv6;
- Увеличенный размер MTU на 20 октетов;
- Сложность в диагностике и устранении неисправностей.

При своих преимуществах и недостатках туннелирование не является законченным решением. Конечная цель – полный переход на IPv6.

#### **6.4. Изолированный двустековый узел.**

Инкапсуляция может быть произведена пограничным маршрутизатором между узлами, или между узлом и роутером. Пример на рисунке 5 показывает изолированный двустековый узел, использующий инкапсулирующий туннель для связи с пограничным маршрутизатором сети IPv6. При этом туннелирование не будет работать, если промежуточный узел не поддерживает или не работает с протоколом 41 IPv4.

**Рис. 5.**



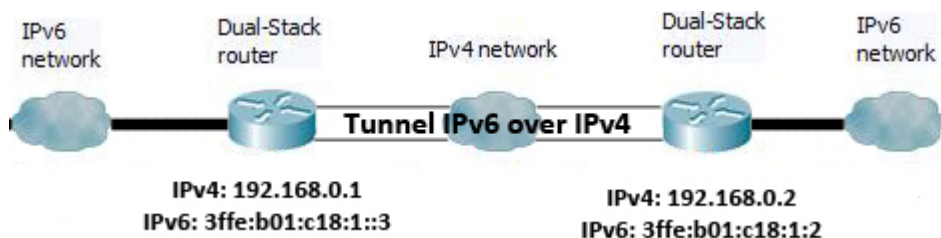
#### **6.5. Конфигурирование туннеля.**

При ручной конфигурации туннеля, необходимо настроить как IPv4 так и IPv6 адреса. При этом адреса должны быть статическими. Такую конфигурацию необходимо применить на каждом конце туннеля.

Пограничные маршрутизаторы должны быть двустековыми. Конфигурация роутеров должна быть статической, маршрутизация должна быть соответствующе сконфигурирована для пересылки пакетов IPv6. Концы туннеля могут быть нумерованными, однако это существенно затруднит устранение неисправностей. При этом, практика резервирования адресов для концов туннеля известная из IPv4 больше не является решением.

**Рис. 6.**

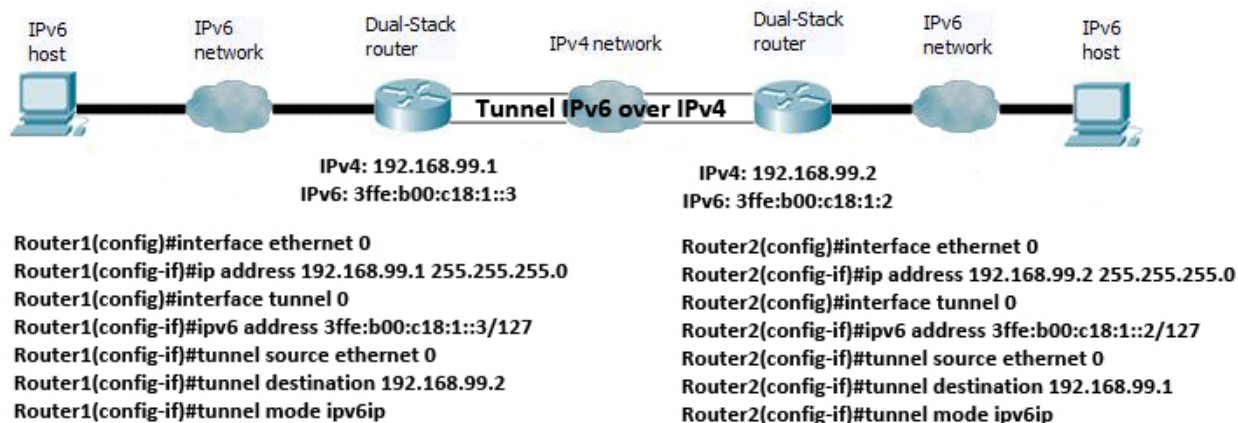




## 6.6. Пример конфигурации туннеля.

Пример на рисунке 7 показывает, как вручную сконфигурировать туннель для IPv6.

Рис. 7.



Каждый узел на концах туннеля должен поддерживать оба протокола – IPv4 и IPv6.

Команда включающая туннелирование – **tunnel mode ipv6ip**. Она указывает на использование протокола IPv6 как «пассажира», а протокола IPv4 как транспортного и инкапсулирующего.

При этом существует несколько механизмов автоматического туннелирования. Среди них следующие:

- **6to4** – использует реверсивный префикс 2002::/16 и позволяет подключить изолированные области IPv6;
- **ISATAP (Intra-Site Automatic Tunnel Addressing Protocol)** – точка-множество точек, позволяет соединить системы внутри области.

Другой известный механизм трансляции – Teredo (еще известный как Shipworm). Этот механизм туннелирует IPv6 пакеты внутри пакетов IPv4 по протоколу UDP.

## 6.7. Туннелирование IPv6 в IPv4 (6to4 tunneling).

Автоматическое туннелирование 6to4 позволяет изолированным IPv6 сетям подключаться через сети IPv4 к удаленным сетям IPv6. Основное отличие автоматического туннелирования 6to4 от ручного заключается в использовании технологии точка-множество точек, а не точка-точка. В 6to4 маршрутизаторы не конфигурируются в пары, т.к. они видят инфраструктуру IPv4 как виртуальный не широковещательный канал с множественным доступом. Адрес IPv4 встроенный в адрес IPv6 используется для того чтобы найти удаленный конец автоматического туннеля.

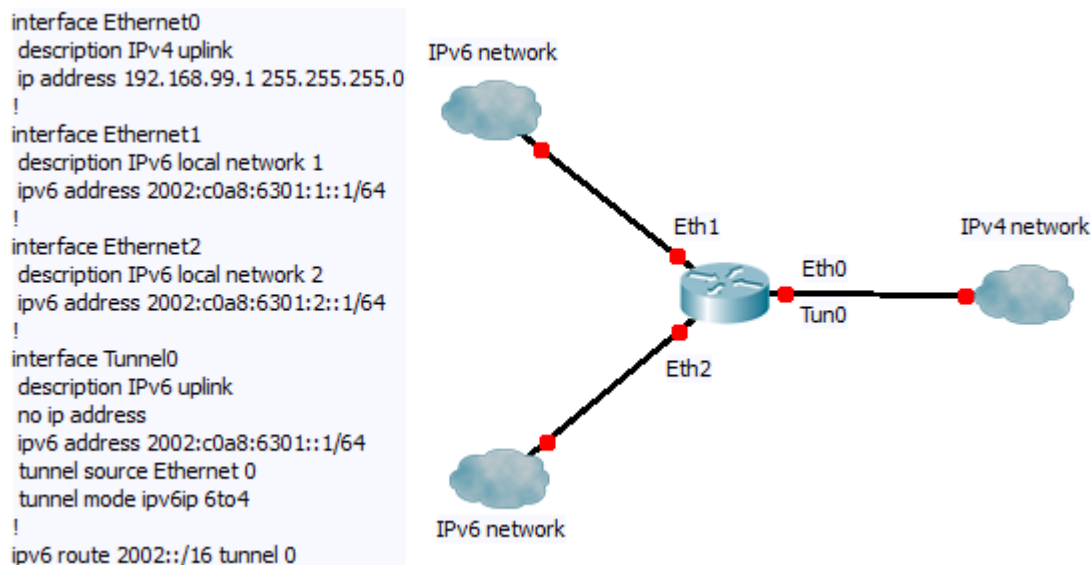
Автоматический туннель 6to4 конфигурируется на пограничном маршрутизаторе сети IPv6 изолированной сети, который создает по пакетный туннель через инфраструктуру IPv4 в другую сеть IPv6. Адрес назначения туннеля извлекается из IPv6 адреса который использует префикс 2002::/16, формат которого имеет вид 2002:IPv4 адрес пограничного маршрутизатора::/48. Пограничные маршрутизаторы туннеля 6to4 должны поддерживать оба

стека IPv4 и IPv6. 6to4 туннель может быть сконфигурирован между пограничными маршрутизаторами, или между пограничным роутером и узлом.

Самый простой сценарий внедрения туннелей 6to4, это межсетевое соединение областей IPv6 подключенный к общей сети IPv4 (это может быть как глобальная сеть, так и корпоративная магистраль). Основное требование – каждая область должна иметь уникальный глобальный адрес IPv4; Cisco IOS будет использовать этот адрес для создания уникального префикса 6to4/48 IPv6. Для работы приложений соответствующие записи в системе DNS необходимы как для данного, так и для других типов туннелей.

На рисунке 8 показана схема конфигурирования автоматического туннеля 6to4.

**Рис. 8.**



Общие шаги конфигурирования:

1. **enable**
2. **configure terminal**
3. **interface tunnel** *tunnel-number*
4. **ipv6 address** *ipv6-prefix/prefix-length* [*eui-64*]
5. **tunnel source** {*ip-address* | *interface-type interface-number*}
6. **tunnel mode ipv6ip 6to4**
7. **exit**
8. **ipv6 route** *ipv6-prefix/prefix-length* **tunnel** *tunnel-number*

## 6.8. NAT-PT трансляция.

Network Address Translation—Protocol Translation технология применяемая для трансляции IPv6 в IPv4 и позволяющая взаимодействовать IPv6 устройствам только с IPv4 устройствами и наоборот.

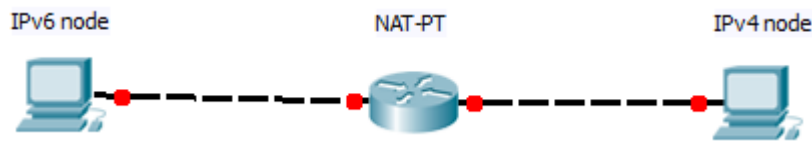
Обязательным условием для настройки NAT-PT является конфигурация интерфейсов маршрутизатора производящего трансляцию с IPv4 и IPv6 адресами.

Ограничения NAT-PT:

- NAT-PT не поддерживается Cisco Express Forwarding
- NAT-PT предоставляет ограниченную поддержку Application Layer Gateway (ICMP, FTP, DNS)
- Имеет те же самые ограничения что и IPv4 NAT

Следующее изображение демонстрирует топологию использования NAT-PT

**Рис. 9.**



При этом конечные узлы должны быть сконфигурированы только на использование одного стека – IPv6 или IPv4.

Не смотря на то, что IPv6 предоставляет конечным пользователям более эффективную систему, полный переход на IPv6 произойдет не сразу. На период модернизации необходимо обеспечить взаимодействие между узлами работающими по протоколу IPv6 и узлами использующими протокол IPv4. Основным преимуществом такой трансляции является отсутствие необходимости проводить реконфигурацию конечных узлов. Настройки производятся только на маршрутизаторе. Основное отличие NAT-PT от туннелирования – это то, что NAT-PT используется только для соединения узлов типа IPv6 to IPv4. Для соединений типа IPv6 to IPv4 to IPv6 необходимо использовать туннелирование, во избежание двойной трансляции. При этом не рекомендуется использовать NAT-PT на узлах с двойным стеком. Они так же предназначены для работы в режиме туннеля.

NAT-PT реализует три механизма трансляции:

- Статическая
- Динамическая
- Трансляция портов или перегрузка (PAT)

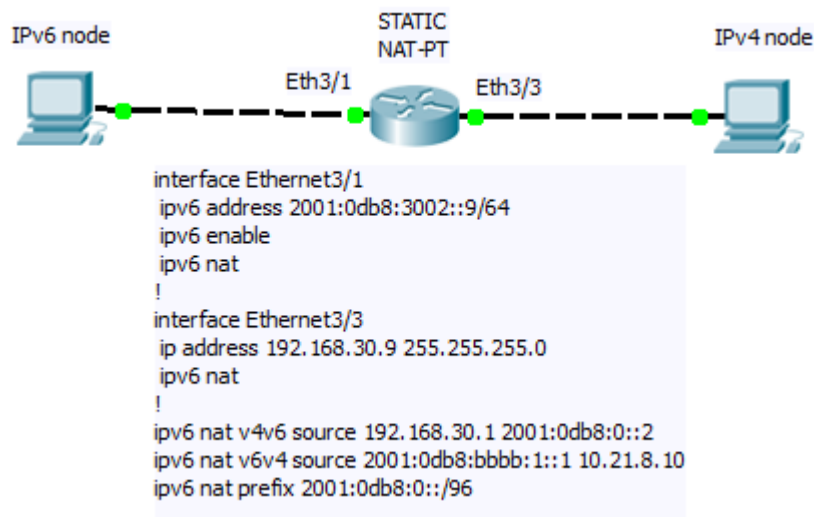
**Статическая трансляция** привязывает один IPv6 адрес к одному IPv4 адресу. При реализации нескольких соединений придется настраивать большое количество трансляций. Поэтому статическая трансляция используется для подключений между одиночными узлами, либо для организации доступа к узлу в сети IPv4 – например к внешнему DNS серверу.

**Динамическая трансляция** позволяет создать множественные привязки адресов используя пул адресов из которого будут браться адреса для трансляции. Количество адресов в пуле будет определять максимальное количество сессий трансляции. Все трансляции записываются в динамическую базу трансляций.

**PAT** позволяет использовать один адрес IPv4 для множества сессий благодаря мультиплексированию по портам, позволяя тем самым нескольким IPv6 пользователям пользоваться одним IPv4 адресом.

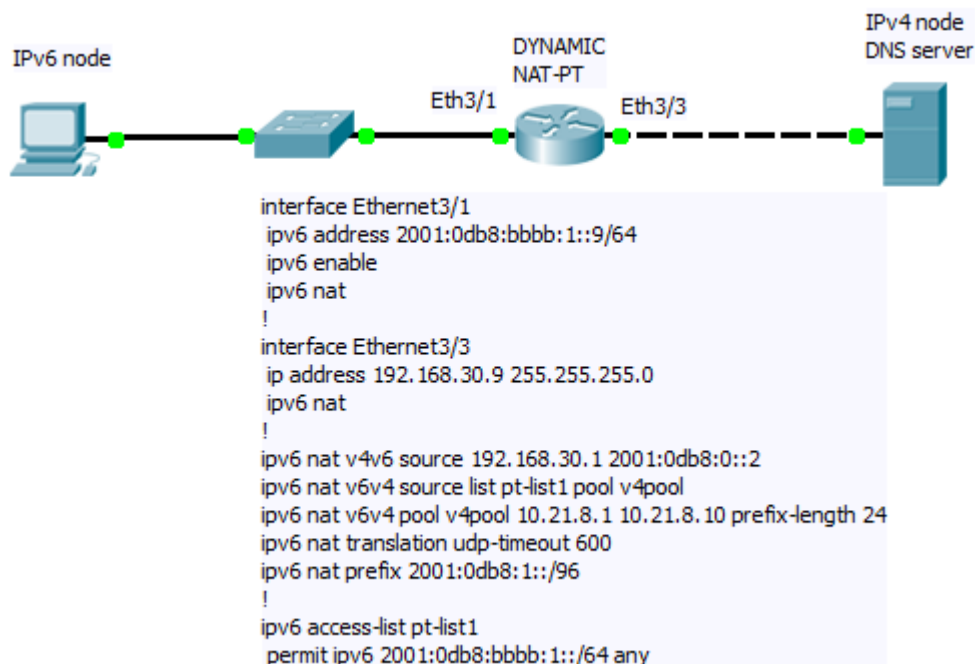
Рисунки 10, 11 показывают примеры конфигурации NAT-PT.

**Рис. 10**

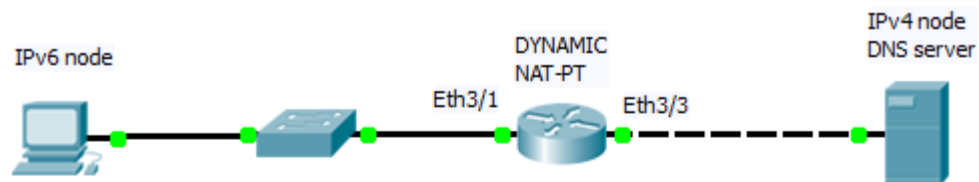


В примере динамической трансляции происходит трансляция доступа к DNS серверу находящемуся в зоне IPv4, при этом создается пул для трансляции с названием v4pool и диапазоном адресов 10.21.8.1-10.21.8.10, а так же настраивается список доступа pt-list1 позволяющий получить доступ из сети IPv6 в любое место. Т.е. имеет место трансляция для доступа области IPv6 в область IPv4. Для реализации PAT необходимо лишь добавить overload в конце команды ipv6 nat. Например: ipv6 nat v6v4 source list pt-list1 pool v4pool overload.

**Рис. 11.**



А это альтернативный вариант трансляции позволяющий сделать обратную процедуру – доступ области IPv4 к области IPv6.



```

interface Ethernet3/1
ipv6 address 2001:0db8:bbbb:1::9/64
ipv6 enable
ipv6 nat
!
interface Ethernet3/3
ip address 192.168.30.9 255.255.255.0
ipv6 nat
!
ipv6 nat v4v6 source list 72 pool v6pool
ipv6 nat v4v6 pool v6pool 2001:0db8:0::1 2001:0db8:0::2 prefix-length 128
ipv6 nat v6v4 source 2001:0db8:bbbb:1::1 10.21.8.0
ipv6 nat prefix 2001:0db8:0::/96
!
access-list 72 permit 192.168.30.0 0.0.0.255

```