IP Мультивещание

Принципы IP Мультивещания и приложения, IGMP,

DVRMP, MOSPF, PIM-SM, PIM-DM, MBone, RTP/RTPC

Содержание

- **IP мультивещание**
  - RFC 1112
  - IGMPv1, IGMPv2, IGMPv3
  - IGMP Snooping
- **IP Multicast Маршрутизация**
  - DVMRP
  - PIM-DM
  - PIM-SM
  - MOSPF
  - CBT
- **MBone**
- **Multicast Приложения**
- **RTP/RTPC**

IP-Multicast Сервис-Модель Резюме

- **IP-Multicast архитектура согласно RFC 1112:**
  - Отправители, посылающие пакеты по IP multicast адресу
  - Приёмники, желающие принять участие в этом IP multicast адресе
    - ✓ регистрируются как участники группы для multicast адреса через IGMP
  - Маршрутизаторы, договаривающиеся как доставлять multicast трафик от отправителей к получателям
    - ✓ построение распределённых деревьев, дублирование пакетов
    - ✓ на самом деле выполняется multicast протоколами маршрутизации

IP-мультивещание

- **Различие только между точка-точка IP пакетом и multicast IP пакетом**
  - адрес группы в поле назначения
- **IP адреса класса D используются как групповые адреса multicast-группы**
  - класс D адреса: 1110xxxx.xxxxxxxx.xxxxxxxx.xxxxxxxx
  - поэтому 2^{28} = 268.435.456 возможных групп
  - класс D диапазон: от 224.0.0.0 до 239.255.255.255

IANA диапазоны multicast адресов

- Локальные адреса
  - ✓ **224.0.0.0 - 224.0.0.255** зарезервированы для сетевых протоколов локальных сетей
  - ✓ Пакеты с такими адресами никогда не проходят через роутер
  - ✓ Пакеты не выходят за пределы своего сегмента LAN (TTL = 1)
- Глобальные адреса
  - ✓ **224.0.1.0 – 238.255.255.255**
  - ✓ Используются для многоадресной передачи между сетями
  - ✓ Некоторые зарезервированы для известных приложений
    - ➢ Например, 224.0.1.1 – протокол NTP
- Ограниченного радиуса действия
  - ✓ **239.0.0.0 – 239.255.255.255**
  - ✓ административно ограниченные адреса не выходят за пределы AS или других областей
- Статические (RFC2770)
  - ✓ 233.0.0.0/8 диапазон закреплен за организациями, имеющими свой номер AS
  - ✓ Номер AS внедряется во второй и третий байты этого диапазона

IP Multicast Адреса

- **Некоторые хорошо известные multicast адреса**
  - определены IANA (RFC 1700)
    - ✓ 224.0.0.1 … все системы подсети, поддерживающие многоадресные рассылки
    - ✓ 224.0.0.2 … все маршрутизаторы в этой подсети, поддерживающие многоадресные рассылки
    - ✓ 224.0.0.4 … все DVMRP маршрутизаторы
    - ✓ 224.0.0.5 … все OSPF маршрутизаторы
    - ✓ 224.0.0.6 … все назначенные OSPF маршрутизаторы
    - ✓ 224.0.0.9 … все RIPv2 маршрутизаторы
    - ✓ 224.0.0.10 … все eIGRP маршрутизаторы
    - ✓ 224.0.0.11 … все мобильные агенты
    - ✓ 224.0.1.1 … NTP Протокол сетевого времени
    - ✓ 224.0.1.14 … IETF-2-AUDIO
    - ✓ 224.0.1.15 … IETF-2-VIDEO

Групповые L2 адреса в Broadcast Сетях

- **В broadcast сетях IP multicast-пакет может быть послан**
  - или по L2 OSI RM широковещательному (Broadcast) адресу
    - ✓ все станции будут получать multicast-пакет в этой сети
    - ✓ FF-FF-FF-FF-FF-FF (IEEE 802 LAN)
  - или по L2 OSI RM групповому (multicast) адресу
    - ✓ только группа станций будет получать multicast-пакет
    - ✓ необходима привязка L3 IP multicast адреса к L2 multicast адресу (аппаратному адресу)
    - ✓ multicast-приёмники группы должны быть запрограммированы слушать этот “аппаратный” адрес

Класс D IP-адрес → LAN Multicasts Адрес

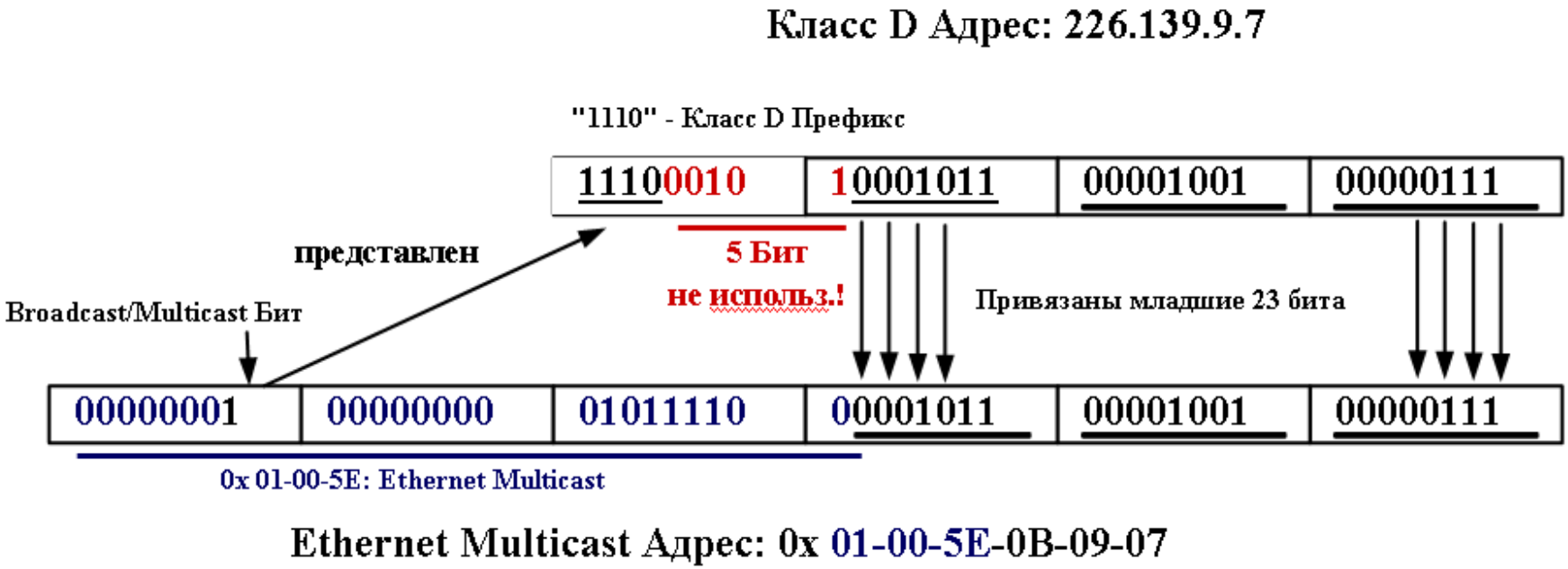
- **IP-адрес класса D имеет изменяемую часть - 28 бит**
- **IANA владеет блоком MAC-адресов Ethernet (поле vendor code) начиная с 01:00:5E**
  - Половина этого блока предназначена для групповых адресов
    - ✓ Т.е. 23 младших бита адреса соответствуют групповым IP-адресам
    - ✓ 24 бит = 0
  - ИТАК:
    - ✓ 00-00-5E… (трактовка IEEE, Ethernet)
    - ✓ **01-00-5E** … Ethernet multicast (I/G бит = 1) – первые три байта (24 бита) - зарезервированное значение OUI-идентификатора для multicast адресов
- **Аналогичная ситуация с другими технологиями**
  - 00-00-7A (Маркерное Кольцо (Token Ring))
  - 10-00-7A … Token Ring Multicast (I/G бит = 1) – аналогично….

Класс D IP-адрес → LAN Multicasts Адрес

- **23 младших бита класса D привязываются**
  - к младшим 23 битам Ethernet multicast адреса
  - 01-00-5E-00-00-00
    - ✓ 24-бит MAC-адреса устанавливается равным нулю
- **указано в RFC 1112**

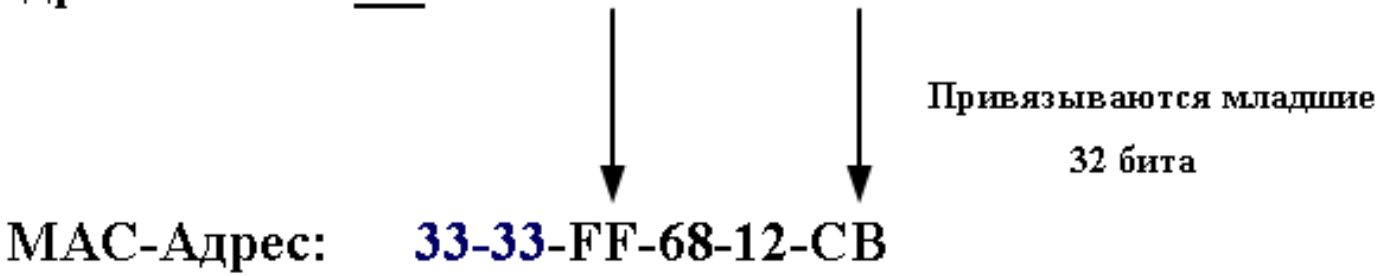
Класс D → LAN Multicasts Адрес

- **Пример**
  - Привязка Класс D IP-адреса к Ethernet Multicast Адресу
    - ✓ Статическая привязка, нет ARP
    - ✓ IANA резервирует диапазон 01:00:5E:00:00:00 – 01:00:5E:7F:FF:FF



Класс D → LAN Multicasts Адрес

- **5 битов IP-адреса не могут быть привязаны к MAC-адресу**
- **Возникает 32:1 неопределённость адреса**
  - 32 различные IP-Multicast-группы имеют один и тот же multicast MAC-адрес
  - Приложение вынуждено принимать во внимание IP-Address, и осуществлять фильтрацию нежелательных многоадресных кадров
  - Сетевым администраторам необходимо помнить правило 32:1 и избегать наложений многоадресных групп
- **IPv6-Multicast Адрес:** **0x FF02:0:1:FF68:12CB**



Реализация IP Multicast

- **RFC 1112 “расширения хоста для IP мультивещания”**
  - определяет компоненты multicast-архитектуры и задачи компонентов
    - ✓ модель реализации IP-хоста
      - IP сервисный интерфейс
      - IP модуль
      - сервисный интерфейс локальной сети
      - модуль локальной сети
    - ✓ задачи multicast-отправителя
    - ✓ задачи multicast-получателя
    - ✓ задачи multicast-маршрутизатора
    - ✓ протокол “хост – маршрутизатор”
      - Межсетевой Протокол Управления Группами (IGMP)

RFC 1112 Основные факты

- **IP мультивещание - это передача IP пакета к группе хостов**
  - такая же надёжность как у правильной unicast IP датаграммы
- **Каждая группа определяется одним адресом класса D**
- **Группы могут быть любого размера, участники могут находиться в любом месте в Интернете**
- **Принадлежность хоста к группе является динамической**
  - хосты могут присоединяться и покидать группы в любое время
- **Группа может быть постоянной или временной**
  - постоянные используют зарезервированные “хорошо известные” IP адреса
  - временные могут использовать все остальные IP адреса, которые не зарезервированы
- **Multicast-отправители не должны быть участниками групп**

RFC 1112 Основные факты (прод.)

- **Хост передаёт IP multicast пакеты**
  - как мультивещание в локальной сети, которое непосредственно достигает всех соседних участников группы получателей
  - по умолчанию TTL=1 (большее значение может быть запрошено приложением)
  - multicast пакеты, которые должны достигнуть удалённых участников, должны быть отправлены с TTL больше, чем 1
  - TTL может использоваться для управления объёмом multicast-трафика
- **хост, желающий multicast-трафик**
  - должен присоединиться к группе, подготовив интерфейс локальной сети для получения соответствующих мультивещаний локальной сети
  - должен сообщить свою принадлежность к группе локальному multicast-роутеру IGMP сообщениями

RFC 1112 Основные факты (прод.)

- **Отправление IP multicast пакетов осуществляется multicast-роутером**
- **Multicast-роутеры будут отправлять все полученные IP multicast пакеты с значением TTL большим, чем 1**
  - ко всем другим сетям, имеющим участников группы получателей
- **Multicast-роутеры присоединены к сетям участникам, которые доступны в пределах TTL**
  - Для завершения доставки передачей IP multicast пакета как мультивещания в локальной сети
- **Метод multicast маршрутизации**
  - определён в других RFCs

Содержание

- **IP мультивещание**
  - RFC 1112
  - IGMPv1, IGMPv2, IGMPv3
  - IGMP Snooping
- **IP Multicast Маршрутизация**
  - DVMRP
  - PIM-DM
  - PIM-SM
  - MOSPF
- **MBone**
- **Multicast Приложения**
- **RTP/RTPC**

IGMPv1 (RFC 1112)

- **Межсетевой Протокол Управления Группами (IGMP)**
  - IGMP – Internet Group Management Protocol
    - ✓ Для динамической регистрации отдельных хостов в многоадресной группе локальной сети
      - ➢ Посылая IGMP-сообщения на свой локальный multicast роутер
  - версия (1) определена в RFC 1112
    - ✓ только хост по отношению к роутеру
    - ✓ расширение IGMP для связи роутер - роутер в других документах (RFCs)
  - работает по широковещательным LANs и точка-точка
  - IGMP для IP мультивещаний это неотъемлемая часть IP, как ICMP для IP unicasts
  - IGMP сообщения инкапсулируются в IP пакеты
    - ✓ IP номер протокола = 2
    - ✓ адреса назначения - multicast адрес
      - ➢ 224.0.0.1 ...все системы в этой подсети

IGMP v1 формат

0	4	8	16 31
Версия	**Тип**	**Не используется**	**Контрольная сумма**
Групповой адрес (Groupaddr)			

- **Версия = 1**
- **Два типа IGMP-сообщений**
  - Тип = 1 Запрос Принадлежности (host membership **Query**)
    - ✓ Периодически запрашивает Роутер
    - ✓ При отсутствии ответа на три последовательных IGMP-запроса роутер отключает группу и прекращает передачу адресованного этой группе трафика
  - Тип = 2 Ответ о Принадлежности (host membership **Report**)
    - ✓ отвечает Хост
- **Контрольная сумма - стандартная IP контрольная сумма**
- **Групповой адрес - адрес группы получателей**
  - все нули (0.0.0.0) в Запросах (**Query**)
  - Groupaddr в Ответах (**Report**)

IGMP v1 процедуры

- **В каждой широковещательной сети**
  - Только один multicast-роутер генерирует запросы “query”
    - ✓ выбор query-роутера выходит за рамки RFC 1112
- **Выбранный multicast-роутер**
  - периодически отправляет IGMP-сообщения “Запрос Принадлежности”, используя multicast IP адрес 224.0.0.1 с TTL = 1 (Polling)
  - принимает IGMP-сообщения “Ответ о Принадлежности” в ответ на IGMP-запросы
- **IGMP Report-сообщения посылаются multicast хостами**
  - Когда устройство намеревается принять многоадресный поток (незатребованный ответ)
    - ✓ обновляются данные роутеров о принадлежностях к группе, имеющихся в локальных присоединённых сетях
    - ✓ с адресом назначения идентичным сообщённому группе
  - Ответ на запрос принадлежности, отправленный роутером
- **multicast-роутер должен слушать все multicast-адреса**

IGMP v1 процедуры (продолжение)

- **Хост, желающий получать multicast-трафик определённой группы (Groupaddr)**
  - Конфигурирует локальный сетевой интерфейс для получения multicast
    - ✓ 224.0.0.1
    - ✓ класс D для групп (224.x.x.x - 239.255.255.255)
- **Хост, получив IGMP сообщения “Запрос Принадлежности”**
  - запускает “таймер задержки ответа” для каждой группы, к которой он подключен
  - Значение “таймера задержки ответа” - произвольно выбранное (случайное)
- **Хост, когда “таймер задержки ответа” для группы X истекает**
  - Формирует IGMP сообщение “Ответ о Принадлежности”” с TTL= 1
  - IP-адрес назначения в IP-пакете = “групповой адрес” в передаваемом IGMP-сообщении “Ответ о Принадлежности”
  - MAC-адрес назначения – групповой MAC-адрес
    - ✓ Формируется по групповому L3 адресу, который включается как в IP-, так и IGMP-заголовок. Решается проблема неоднозначности (32:1)

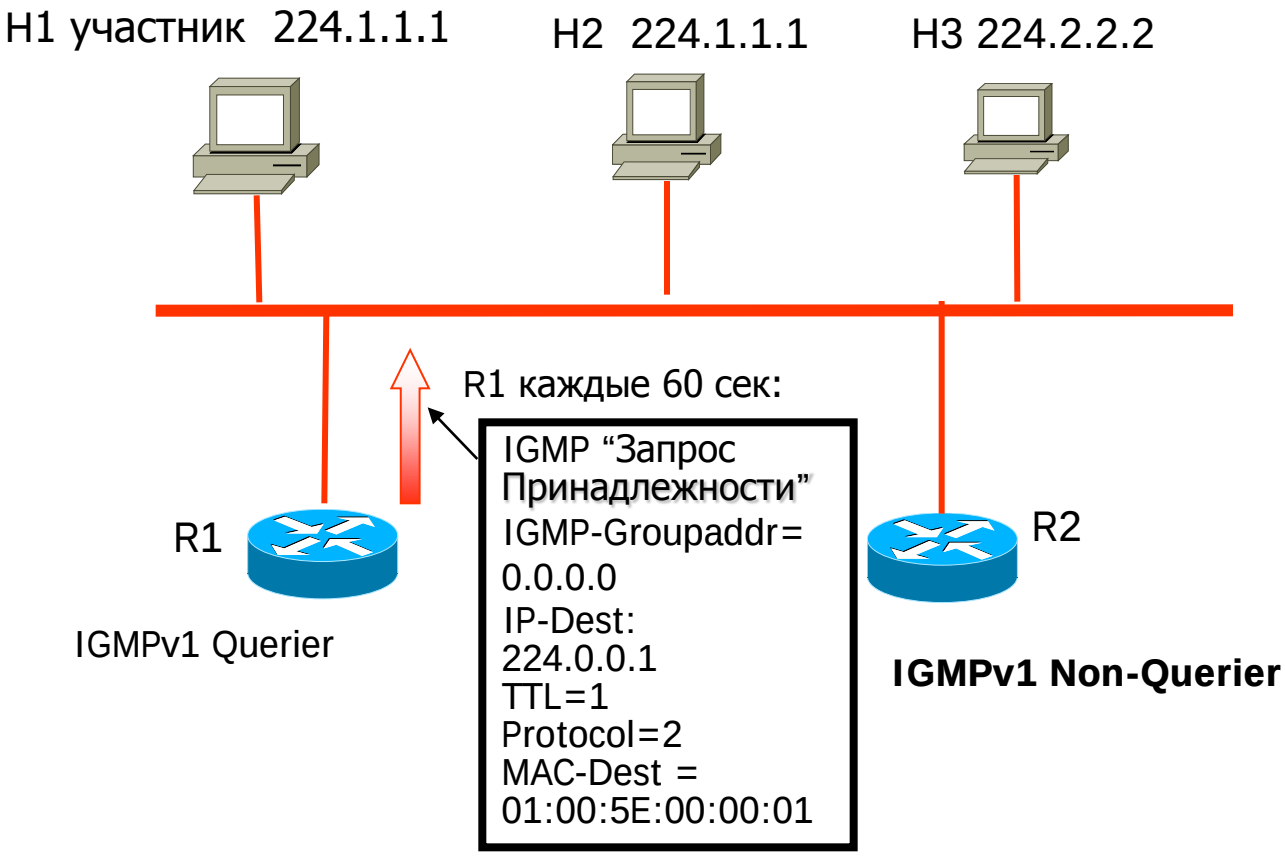
IGMP v1 процедуры (продолжение)

- **Другие участники группы X**
  - Услышав ответ других станций обнуляют таймеры, подавляя создание ответа
  - Такая методика предотвращает лавинную передачу ответов (IGMP Reports) в сегменте сети
- **В нормальном случае, только одно IGMP Report сообщение в группе будет послано в ответ на запрос**
- **Если хост хочет присоединиться к новой группе**
  - один или два IGMP сообщения “Ответ о Принадлежности” передаются немедленно, вместо ожидания IGMP “Запрос Принадлежности”
- **IGMP таймеры**
  - “Query Таймер” (таймер запросов) = обычно 60 - 90 сек (min 60 сек)
  - “Report Таймер задержки” (таймер задержки ответов) = 0 - 10 сек (max 10 сек), случайное число

IGMPv1 Процесс Запрос – Ответ I

Позволяет роутеру определять, какие multicast группы активны

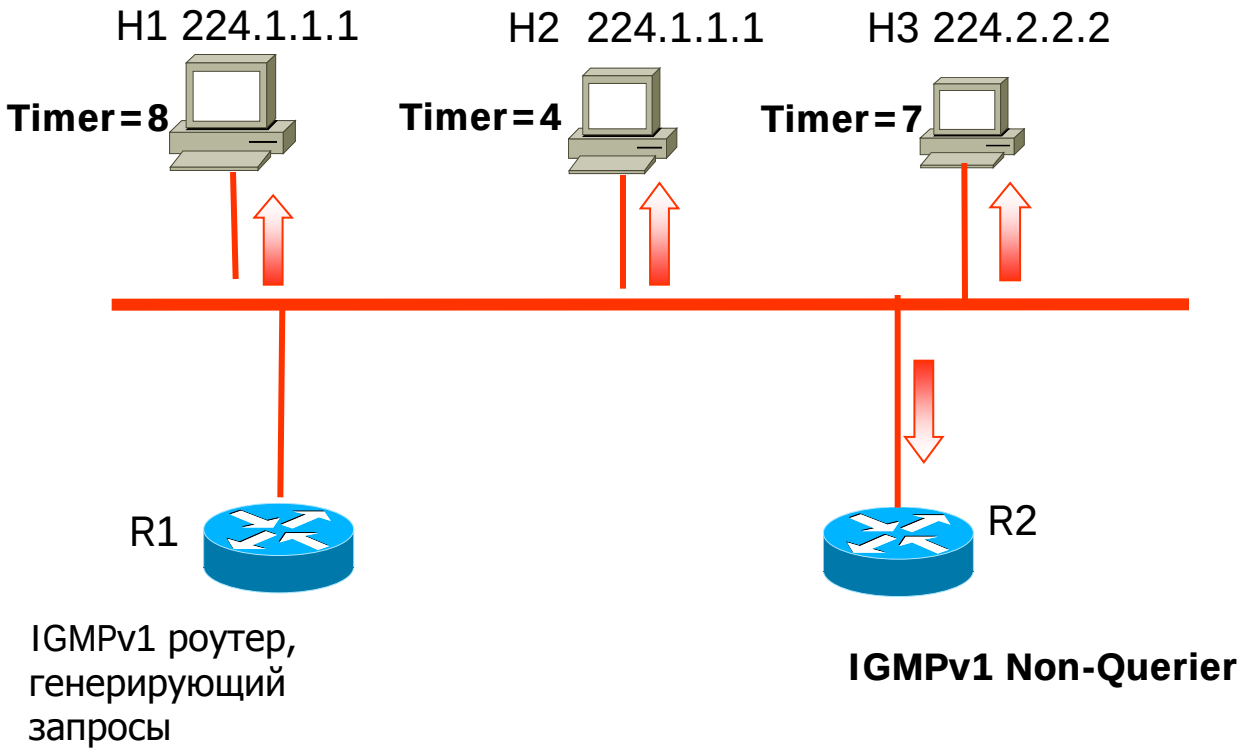
Хосты уже слушают multicast группы, они хотят трафик (и слушают 224.0.0.1 – все системы в этой подсети)



IGMPv1 Процесс Запрос – Ответ II

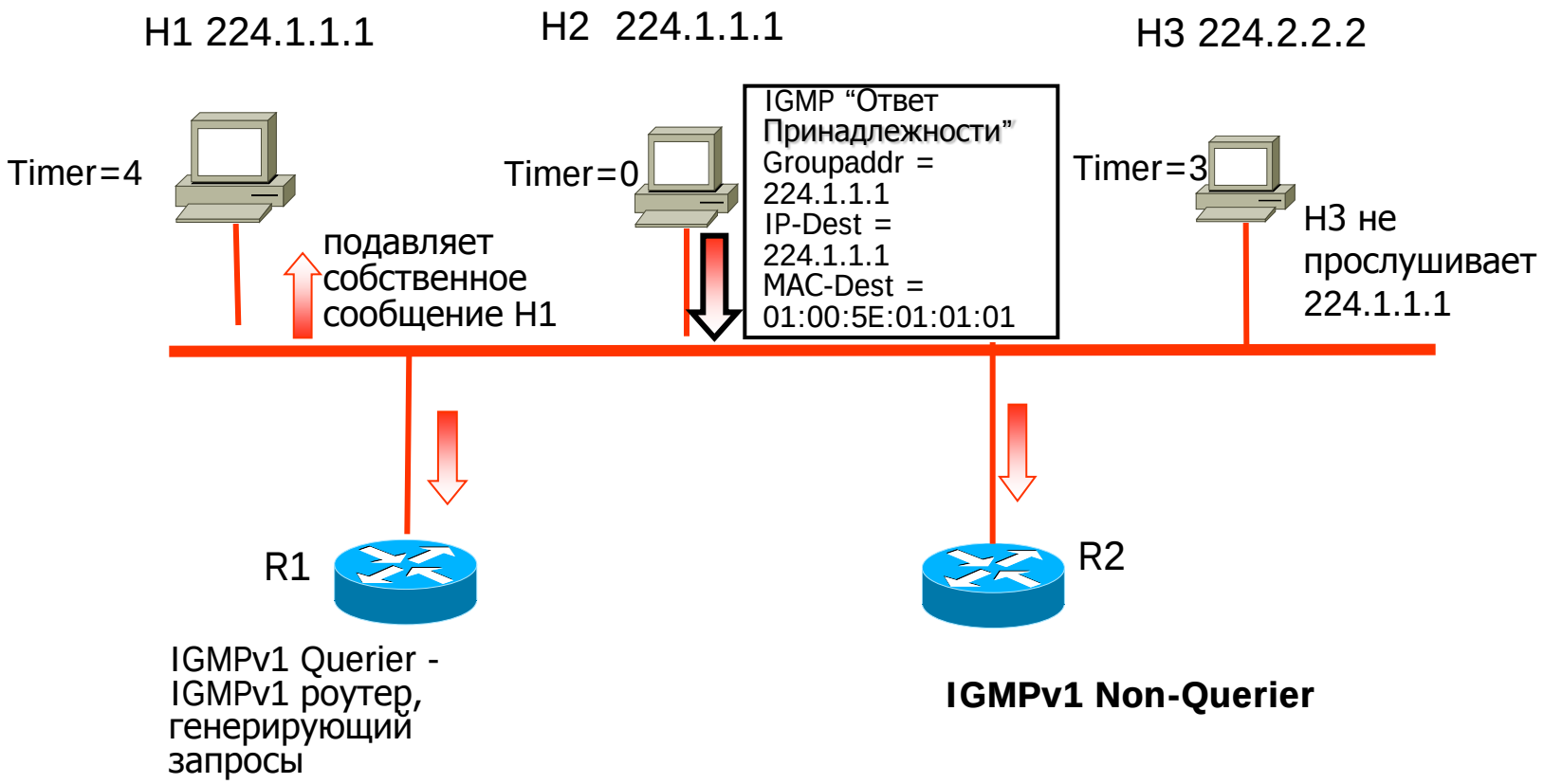
Для предотвращения "Взрыва-ответов" с идентичной информацией

- Каждый хост, получив запрос, устанавливает “таймер ответа” (случайное число от 0 до 10)
- Хост отвечает, когда таймер достигнет 0 и никто ранее не ответил
- Этот “Report подавляющий механизм” помогает уменьшить трафик



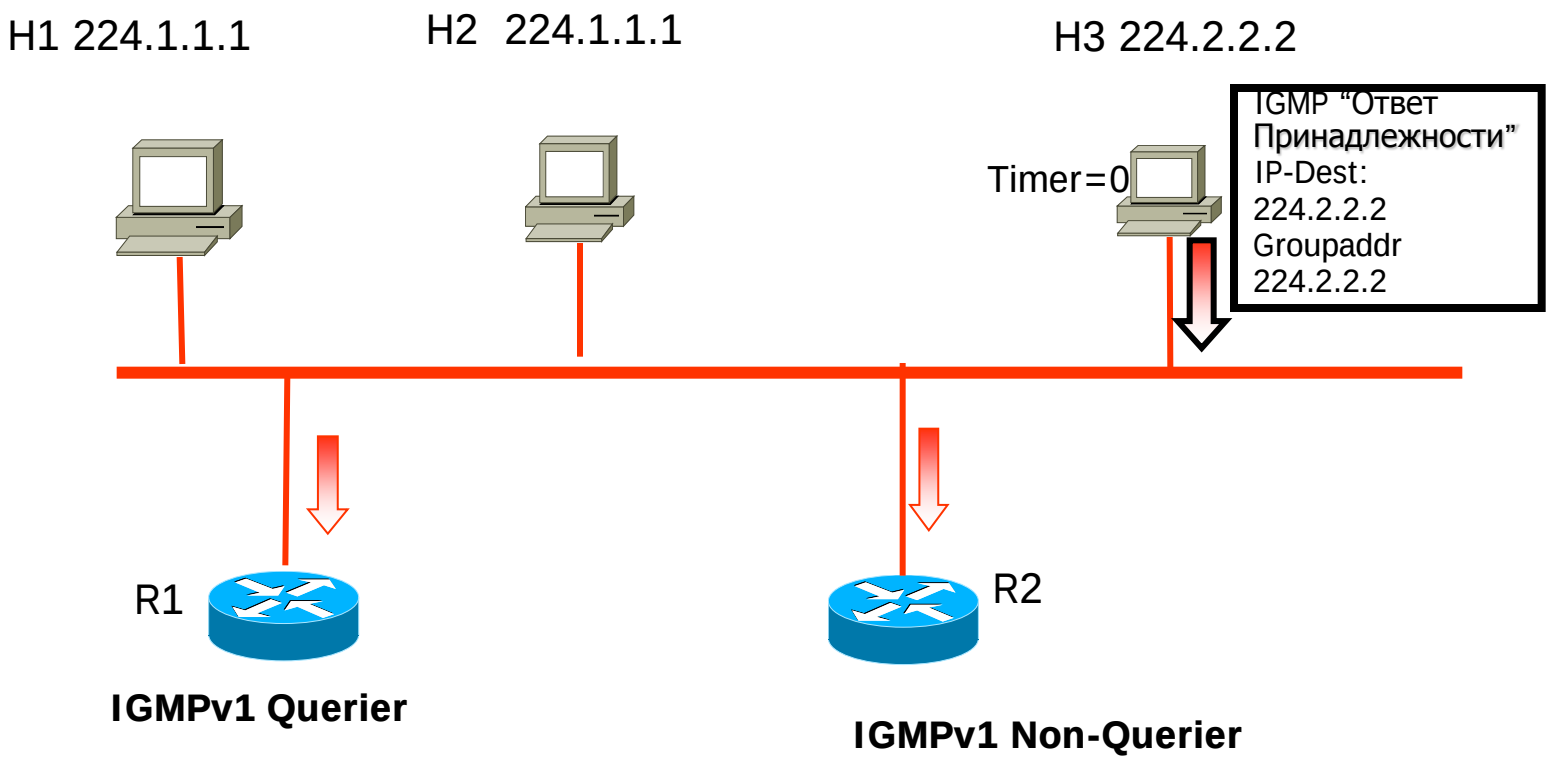
IGMPv1 Процесс Запрос – Ответ III

4 Секунды спустя:



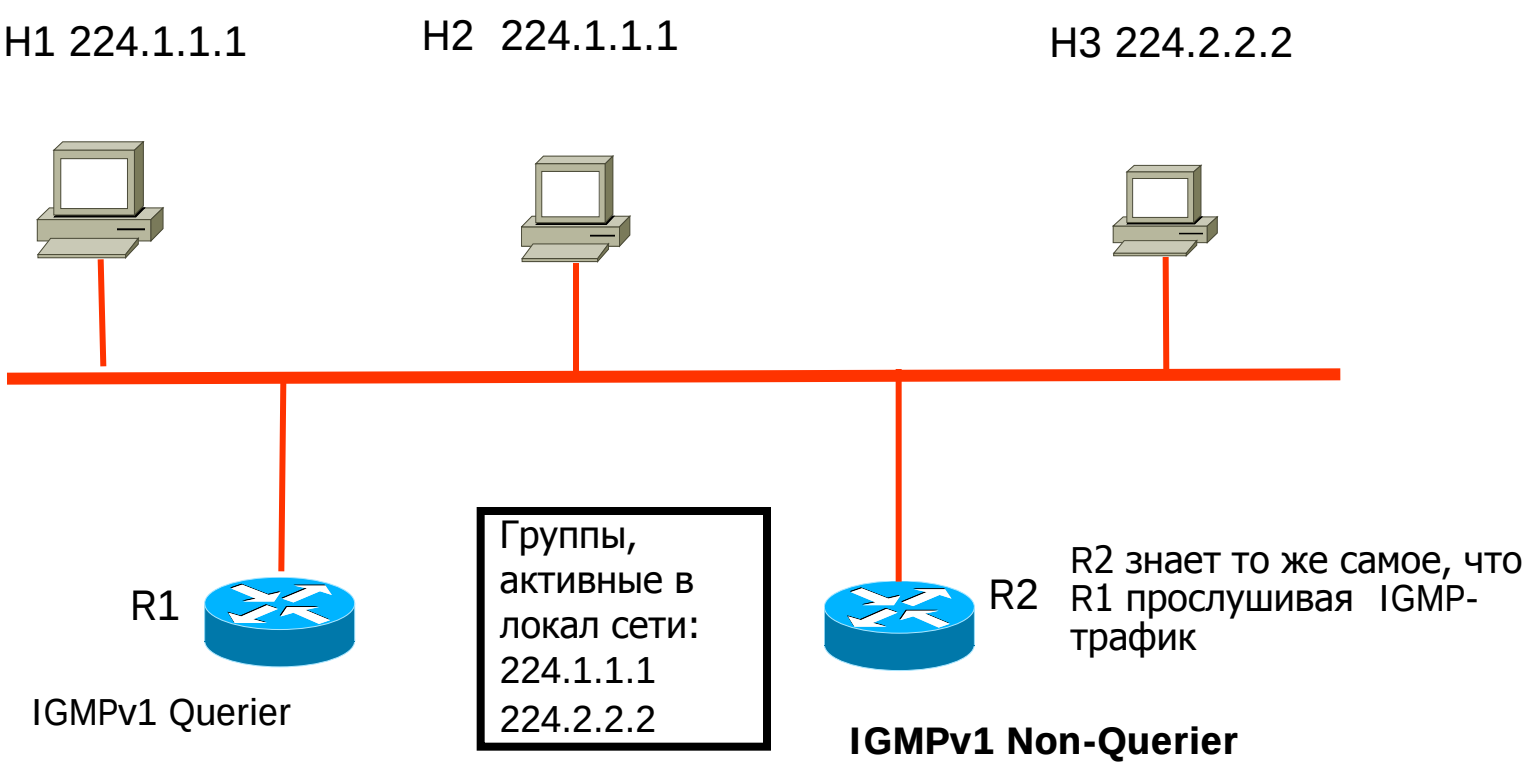
IGMPv1 Процесс Запрос – Ответ IV

3 Секунды спустя:



IGMPv1 Процесс Запрос – Ответ V

Заключительная картинка:

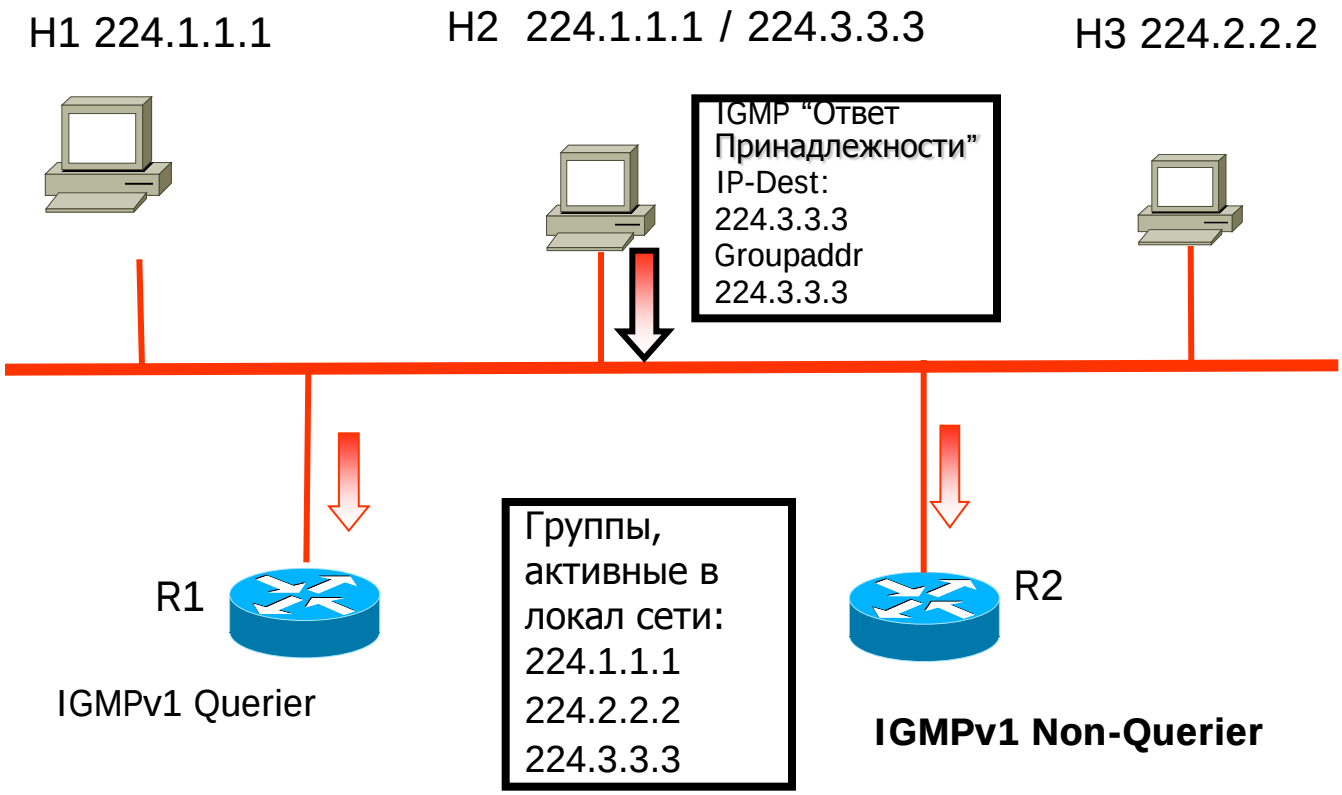


Примечание: В IGMPv1 R1 не известно кол-во слушателей.

Только группы, которые активны

IGMPv1 Процесс подключения (Join-сообщение)

- **Если хост первоначально подключается к multicast группе, то посылается Незатребованный ответ (Unsolicited Report):**



IGMP v1 процесс отключения

- **Роутер прекращает передачу Multicast-трафика для определённой группы в подсети, если в течении 3-х отчетных интервалов не принимаются отчеты / ответы (membership reports) для этой группы**
- **Обычный тайм-аут это 3 Query интервала**
  - ~ 3 минуты

НЕДОСТАТКИ:

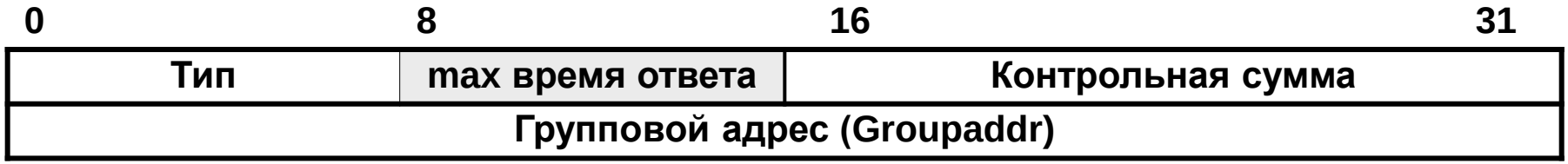
- **Долгая задержка отключения**
- **Может вызывать неприятности**
  - Представьте приложение с высокой пропускной способностью видео
  - Пользователь это "Channel-surfing"
  - Каждый раз, когда пользователь покидает группу, трафик для этой группы доставляется в подсеть в течение 3 минут

РЕШЕНИЕ: IGMPv2

IGMP v2

- **RFC 2236 (IGMP v2)**
  - Усовершенствование процесса подключения к группе и выхода из нее
- **Обратная совместимость с версией 1**
- **Отличия от версии 1**
  - новые сообщения и процедуры, чтобы уменьшить задержки, связанные с выходом из группы
    - ✓ Покинуть группу (Leave Group) сообщение
      - посылается хостом всем маршрутизаторов по адресу 224.0.0.2
    - ✓ Специальный Групповой Запрос
      - Посылается роутером, чтобы обнаружить, последний ли участник группы вышел ???
      - Устанавливает небольшое (меньшее) значение параметра “max время ответа” для получения как можно быстрее ответа и следовательно, прекращения multicast трафика
  - стандартный метод выбора запрашивающего роутера (querier)
    - ✓ Роутер с “меньшим” IP адресом становится “Query роутером”

IGMP v2 формат



- **Четыре типа IGMPv2-сообщений ()**
  - Тип 0x11 = Membership Query (Запрос принадлежности)
    - ✓ Общий Запрос (поле Groupaddr = 0.0.0.0) перенесено от v1
    - ✓ Специальный Групповой Запрос (поле Groupaddr = определяет группу)
  - Тип 0x12 = v1-Membership Report (Ответ о принадлежности по v1)
  - Тип 0x16 = v2-Membership Report (Ответ о принадлежности по v2)
  - Тип 0x17 = Leave Group (Покинуть группу)
- **Макс. время ответа**
  - используется только в Membership Query для задания максимально допустимого времени для “таймера задержки ответа”
  - в долях - 1/10 секунды

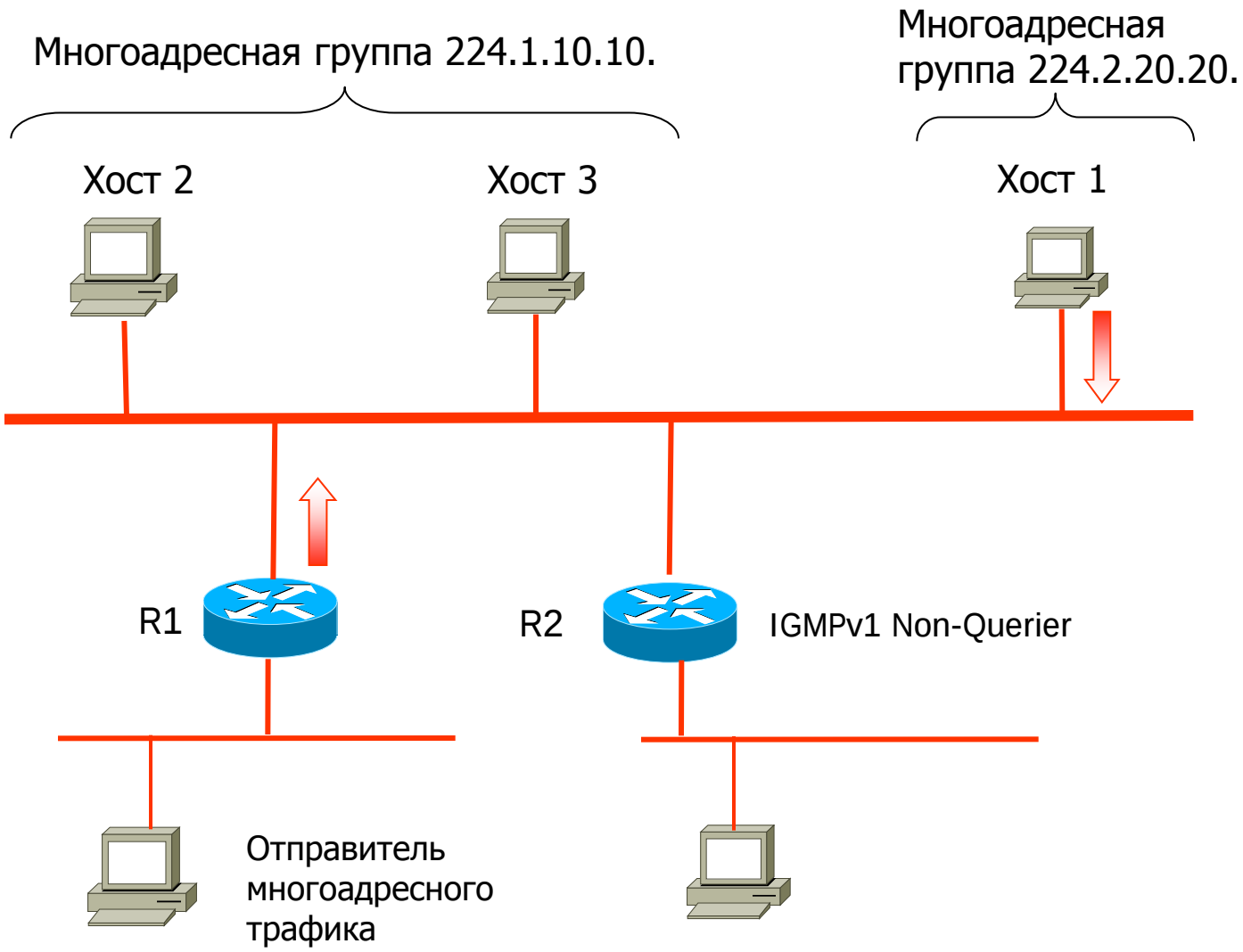
IGMPv2 процедуры

- **IGMPv2 роутер поддерживает список всех хостов сегмента сети, входящих в группу**
  - Называется многоадресным multicast-роутером
  - Формирует списки (многоадресные таблицы) для каждой группы хостов
  - Корректирует список группы если от хоста приходит “незатребованный ответ” о выходе из группы
  - Если пришло “сообщение о выходе” от последнего хоста в группе, роутер посылает “специальный групповой запрос”, для уточнения состава группы
  - Если не будет ответа на “специальный групповой запрос”, Роутер прерывает multicast-поток в сегмент сети для этой конкретной группы
- **Поле “max время ответа” позволяет увеличить значение задержки**
  - Диапазон “max время ответа” = 0 - 25 с (max=25)
  - По умолчанию = 10 с
  - Увеличение времени ответа позволяет сгладить всплески ответов в сегменте при большом количестве групп

IGMPv2 процедуры

- **Для совместимости (одновременной работы) IGMPv2 и IGMPv1**
  - Общие Query (Запросы) и Report (ответы) v1 перешли в v2
  - Замечание:
    - ✓ в IGMPv1 Query поле Groupaddr = 0,
      - ➢ следствие - участники всех групп отвечают по таймеру (0-10 с)
    - ✓ в IGMPv2 Query поле Groupaddr = “конкретный адрес группы”
      - ➢ Другие группы игнорируют это запрос
  - Возможный ситуации с совместимостью v2 и v1
    - ✓ Роутер поддерживает IGMPv2, хосты IGMPv1
      - ➢ Все будет работать по схеме IGMPv1
    - ✓ Роутер поддерживает IGMPv2, часть хостов поддерживает IGMPv2
      - ➢ Все будет работать по схеме IGMPv1 (самим догадаться почему ???)
    - ✓ Если в сегменте сети один роутер IGMPv1, другой – IGMPv2, последний должен быть переведен в режим поддержки v1
      - ➢ Поскольку в двух версиях используются разные методики выбора генерирующего запросы роутера

IGMPv2 пояснения (доработать…)

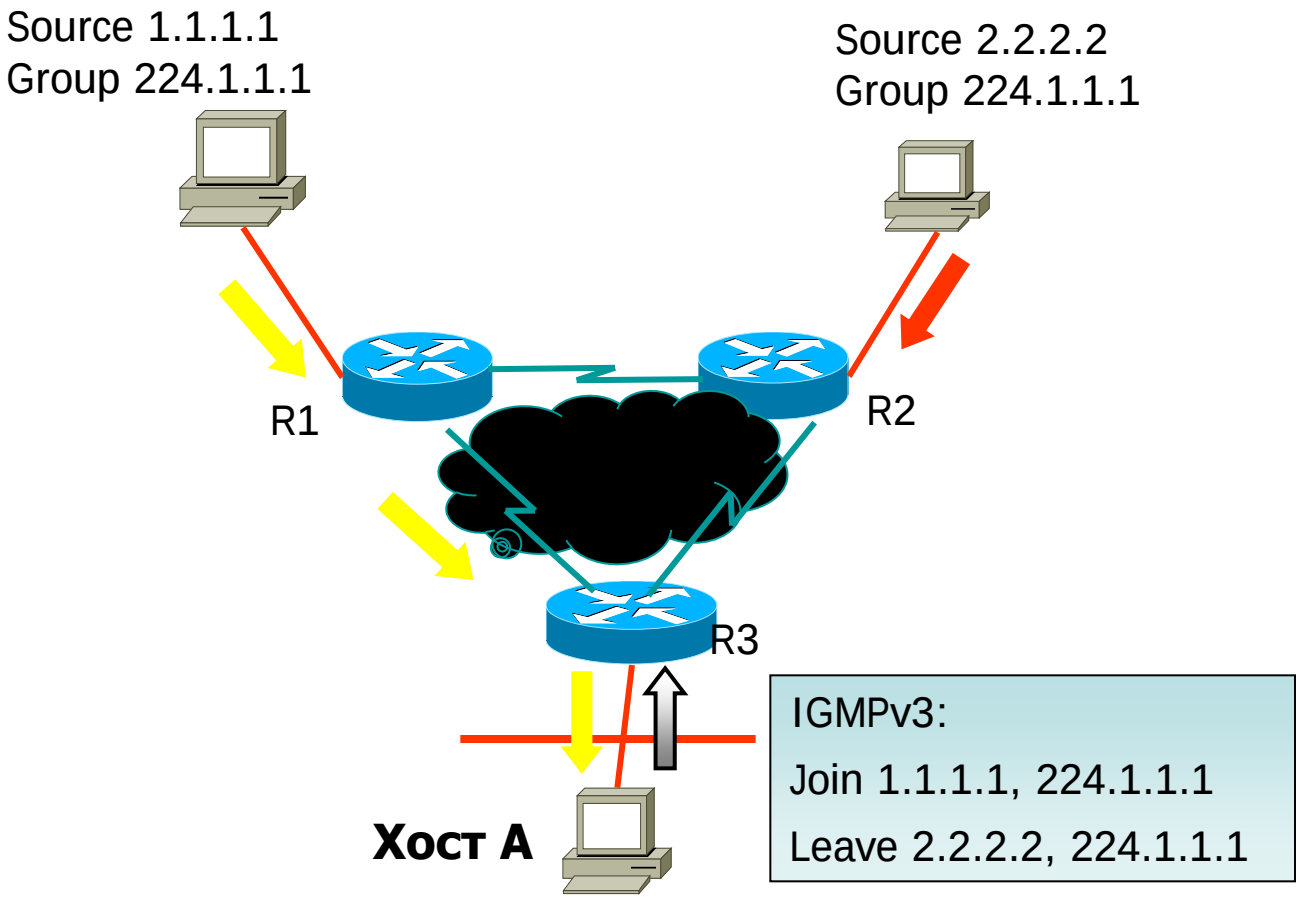


IGMP v3 (МГФ доработать)

- **RFC 3376**
- **добавляет "фильтрацию источника"**
  - способность сообщить об участии в получении пакетов только от определённых source-адресов или от всех, (но определённые source-адреса отправляют multicast адресу)
  - уменьшает опасность “Отказа Сервис Атакой”
    - ✓ продолжающаяся multicast-сессия может быть нарушена посылкой junk-data к той же multicast группе
    - ✓ этот источник может быть "отключен"

IGMPv3 Фильтрация Источника

Хост А хочет принимать (Join - подключится**) от S=1.1.1.1 ,**
но не от S=2.2.2.2 (Leave - покидать)



IGMP и IPv6

- **IGMP функции непосредственно Интегрированы в IPv6 (ICMPv6)**
- **Все хосты IPv6 должны поддерживать multicasting**
- **В IPv4, поддержка multicasting и IGMP не обязательна**

Содержание

- IP мультивещание
  - RFC 1112
  - IGMPv1, IGMPv2, IGMPv3
  - IGMP Snooping
- IP Multicast Маршрутизация
  - DVMRP
  - PIM-DM
  - PIM-SM
  - MOSPF
- MBone
- Multicast Приложения
- RTP/RTPC

IGMP Snooping (IGMP Прослушивание)

- **Проблема: L2, Flooding Multicast Кадров**
  - Обычно L2 Switches рассматривают Multicast трафик как Неизвестный или Широковещательный и должны "flood" кадр к каждому порту
    - ✓ особенно проблематично, когда плоская иерархия с множеством участников broadcast домена
  - Проблема полосы пропускания
  - Только участники групп должны получать multicast трафик
  - Как коммутаторы могут знать?
  - Решения:
    1. Ручная статическая конфигурация MAC-таблицы коммутации коммутатора
    2. CGMP - Cisco Group Multicast Protocol
       - MAC связь между Switch и Router – определено производителем
    3. IGMP Snooping (IGMP-прослушивание)

Статическая конфигурация MAC-таблицы

- Ручками сетевых администраторов

Фирменный протокол CGMP

- **CGMP (Cisco Group Multicast Protocol) – фирменный протокол CISCO**
  - Хост отправляет IGMP-ответы (например, со своим MAC-source= 00:60:08:93:DB:C1) о подключении к группе 224.1.10.10
  - CGMP совместимый роутер отправляет коммутатору информацию о MAC-source, запросившем многоадресный трафик 01:00:5E:01:0A:0A (224.1.10.10)
  - Коммутатор модифицирует таблицу коммутации
    - ✓ Ищет unicast-адрес 00:60:08:93:DB:C1 и к порту, на котором находится этот хост, добавляет адрес группы (01:00:5E:01:0A:0A)
    - ✓ Теперь, все кадры с MAC-dist = 01:00:5E:01:0A:0A будут направлены в этот порт, без распространения их в другие порты
- **Особенности.**
  - Функционирование CGMP не требует изменений в хостах
  - Функционирование CGMP затрагивает только коммутаторы (Catalist) и роутеры (Cisco)

Протокол CGMP иллюстрация

- **Коммутаторы классически самообучаются**
- **Роутер (Cisco) по протоколу CGMP сообщает коммутаторам (Catalist) о**
  - MAC unicast-адресе подключенному MAC-multicast-группе
- **Подробности опущены (МГФ)**

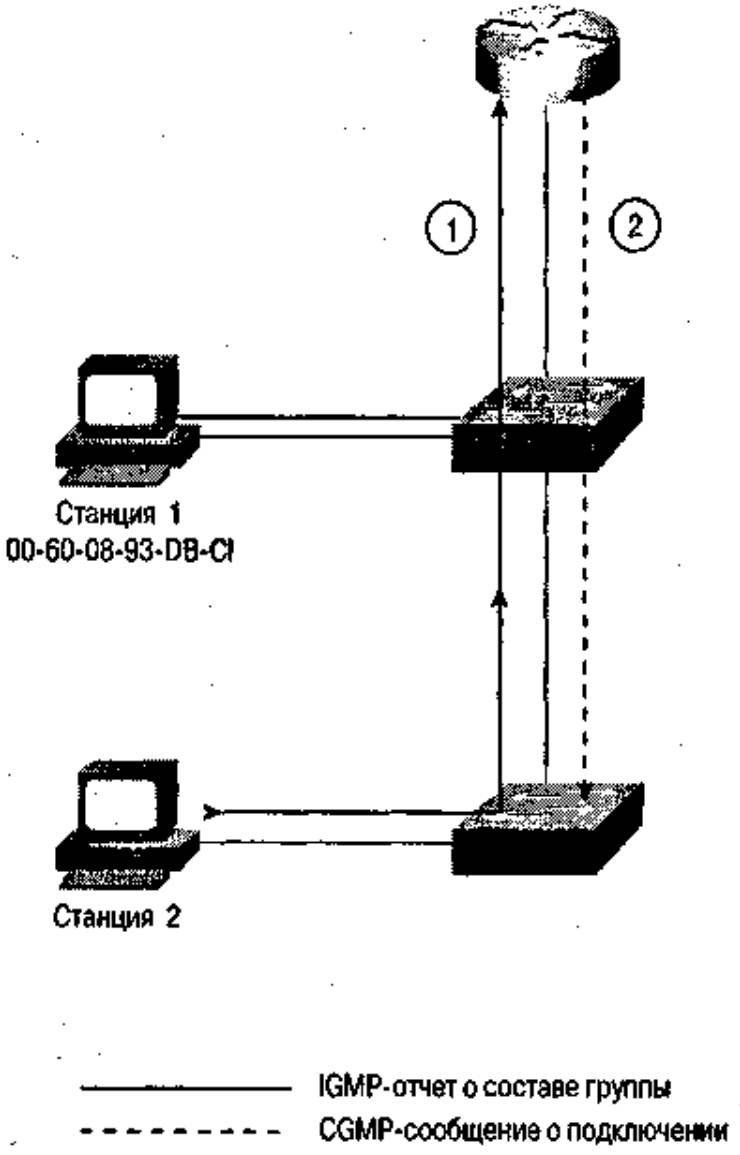


Рис. 13.11. Пример работы протокола CGMP

IGMP Snooping (Отслеживание)

Коммутатор становится знающим "IGMP"

- Multicast коммутатор – должен проверять содержимое IGMP сообщений,
  Routing Protocol, чтобы определить какие порты и какой хотят трафик
  - IGMP Membership Reports
  - IGMP Leave Сообщения

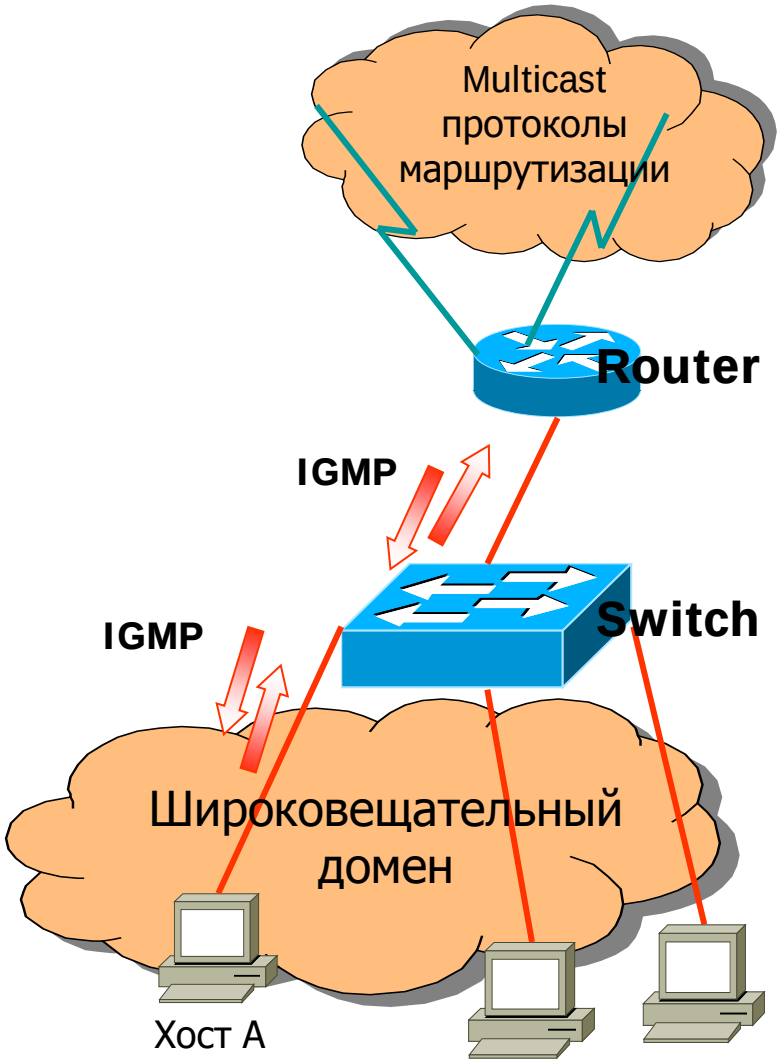
Влияние

– должен обрабатывать ВСЕ Multicast пакеты L2

IGMP пакеты имеют Class-D destination и Multicast MAC адреса, подобно любому другому multicast трафику

Что хорошо

- Возможно использование оборудования разных фирм,
- это оборудование должно поддерживать IGMP Snooping



Содержание

- IP мультивещание
  - RFC 1112
  - IGMPv1, IGMPv2, IGMPv3
  - IGMP Snooping
- IP Multicast Маршрутизация
  - DVMRP
  - PIM-DM
  - PIM-SM
  - MOSPF
- MBone
- Multicast Приложения
- RTP/RTPC

IP Multicast Маршрутизация (вспомним!!!)

- **Роутеры, которые поддерживающие multicast трафик, создают связные деревья, по которым передается многоадресный IP-трафик**
- **Два типа связных дерева**
  - Деревья от источника
    - ✓ Корень дерева – источник multicast–трафика
    - ✓ Листья дерева - приемники multicast–трафика
    - ✓ Дерево использует кратчайшие маршруты
      - ➢ Называют такое дерево - дерево кратчайших маршрутов (shortest path tree, SPT)
      - ➢ Описывают SPT парой (S,G), где S – IP-адрес источника, а G – групповой адрес приемника
  - Деревья общего доступа
    - ✓ Корень дерева – точка рандеву (RP)
    - ✓ Источник отправляет трафик корню, откуда он передается вниз по дереву общего пользования всем приемникам
      - ➢ Описывают дерево парой (*,G), где * – IP-адреса источников, а G – групповые адреса приемников

IP Multicast Маршрутизация (вспомним!!!)

- **Роутеры, которые поддерживающие multicast трафик, создают связные деревья, по которым передается многоадресный IP-трафик**
  - большинство протоколов multicast-маршрутизации формируют маршрут не от отправителя к получателю, а в обратном направлении http://www.intuit.ru/department/network/pami/9/1.html
  - Дерево рассылки должно быть построено так, чтобы поток отправителя как можно дольше не разветвлялся. Желательно, чтобы разветвления происходили как можно ближе к получателю
  - Это соображение проиллюстрировано на рис. 9.2. На рисунке условно, в виде сетки маршрутизаторов показан фрагмент сети Интернет. Прямоугольником отмечен передатчик, а в нижней части кружочками приемники – члены группы. Маршруты от передатчика к приемникам можно проложить индивидуально (выделены жирными линиями), а можно и "коллективно". От передатчика до маршрутизатора следует один поток для всех приемников. Такое решение приводит к минимизации сетевой загрузки, ведь всем приемникам посылаются одни и те же пакеты. Чем позже их пути разойдутся, тем лучше. Именно этот алгоритм и реализует протокол PIM. Точки разветвления потоков на рис. 9.2 отмечены крестами (RP).

DVMRP

- **Distance Vector Multicast Routing Protocol**
  - первая версия
    - ✓ определена в RFC 1075 (экспериментальный RFC)
  - действующая версия, сейчас используется в MBONE
    - ✓ определена в draft-ietf-idmr-dvrmp-v3-04.txt
- **DVMRP содержит два компонента**
  - обычный дистанционно-векторный протокол маршрутизации
    - ✓ Строит DVMRP таблицы маршрутизации для всех источников multicast трафика
      - ➢ reverse path расстояния (дистанция)
    - ✓ Использует для связи IGMP расширения
  - урезанный RPF (reverse path forwarding – обратная передача) с отсечением (pruning) и прививанием / подключением (grafting)
    - ✓ чтобы посылать multicast-пакеты по усечённым broadcast деревьям, избегая ненужных ветвей дерева

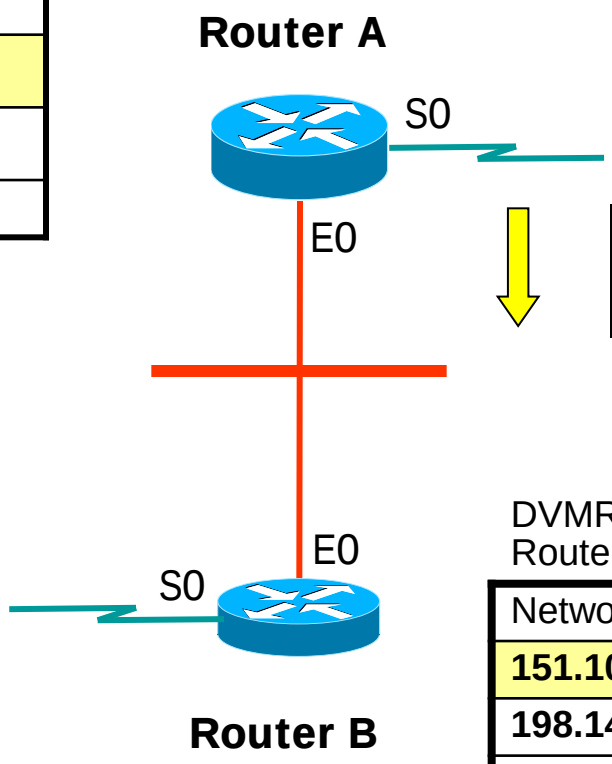
DVMRP

- DVMRP **multicast протокол маршрутизации необходим дополнительно к unicast протоколу маршрутизации**
  - Процесс multicast маршрутизации идёт параллельно с unicast маршрутизацией
  - путь от источника S к multicast роутеру вычисляется и хранится в **multicast таблице маршрутизации**,
    - ✓ используется очень похожий на RIP подход
    - ✓ соседи посылают друг другу сообщения о маршрутах к известным сетям и сохраняют эту информацию в отдельной маршрутной таблице DVMRP
    - ✓ по получении рекламируемого маршрута с hop-count (числом) большим, чем 32 (poison reverse – отравленный реверс), роутер понимает что это им же рекламируемый соседу маршрут (расщепление горизонта) и отсекает его
    - ✓ аналогично создаются усечённые broadcast деревья ко всем хостам

DVMRP- построение RP таблицы маршрутизации

DVMRP таблица маршрутизации
Router A

Network	Intf	Metric
151.10.0.0/16	**S0**	**3**
204.1.16.0/24	**S0**	**10**



Router A посылает
Route Report

151.10.0.0/16	**3**
204.1.16.0/24	**10**

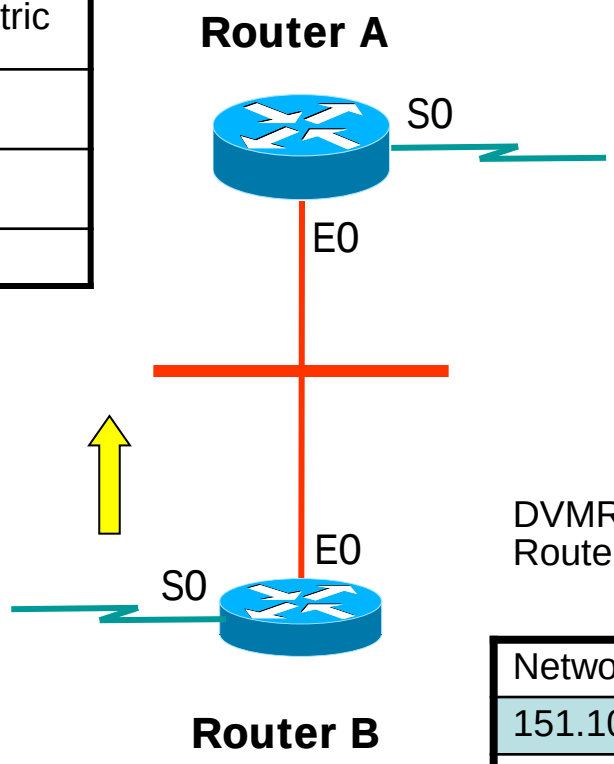
DVMRP таблица маршрутизации
Router B

Network	Intf	Metric
151.10.0.0/16	**S0**	**7**
198.14.2.0/24	**S0**	**3**

DVMRP- построение RP таблицы маршрутизации

DVMRP таблица маршрутизации Router A

Network	Intf	Metric
151.10.0.0/16	**S0**	**3**
204.1.16.0/24	**S0**	**10**
198.14.2.0/24	E0	4



Router B обновляет свою таблицу отсылая сообщение о маршруте. **Добавлением 32 (бесконечность**) к сетям входящим в E0, Router A знает, что Router B ожидает multicast-трафик для этих сетей

151.10.0.0/16	**36**
204.1.16.0/24	**43**
198.14.2.0/24	**3**

DVMRP таблица маршрутизации Router B

Network	Intf	Metric
151.10.0.0/16	E0	4
198.14.2.0/24	**S0**	**3**
204.1.16.0/24	E0	11

DVMRP

- **DVMRP свойственная проблема flooding первого пакета и периодического flooding по всей сети**
  - Напоминание: flooding необходим, чтобы выполнить отсечение и прививки (называется обновить состояния) для любых взаимосвязей источника/группы
- **возможно присоединение ранее отсечённых ветвей**
- **DVMRP не является протоколом, который хорошо масштабируется**
  - слишком много информации о состоянии
  - максимальное hop-count (число хопов) 32
  - периодический flooding для обновления маршрутов

Содержание

- IP мультивещание
  - RFC 1112
  - IGMPv1, IGMPv2, IGMPv3
  - IGMP Snooping
- IP Multicast Маршрутизация
  - DVMRP
  - PIM-DM
  - PIM-SM
  - MOSPF
- MBone
- Multicast Приложения
- RTP/RTPC

PIM - **Protocol Independent Multicast**

- **PIM (Protocol Independent Multicast - независимая от протокола многоадресная рассылка)**
  - ✓ называется так, потому что не зависит от IP-протокола unicast маршрутизации (EIGRP, OSPF, BGP или статические маршруты)
  - ✓ Называется “многоадресный протокол маршрутизации”
  - ✓ Однако вместо построения полностью независимой Multicast таблицы маршрутизации, он использует для обратной передачи одноадресную (Unicast) таблицу маршрутизации, т.е.
    - ➢ **Использует** для многоадресной рассылки **unicast таблицы маршрутизации**
    - ➢ **Не посылает и не принимает обновлений многоадресных маршрутов**
- Это решение для multicast маршрутизации предложено рабочей группой IDMR (Inter-Domain Multicast Routing)
- акцентируется на создании маршрутизации для всего Internet
  - ✓ например, занимается проблемами подобных взрыву ответов (состояний), вызванного большим числом групп

PIM

- **два варианта PIM для различной плотности участников**
  - **PIM-DM** (PIM Dense Mode) – плотный режим
    - ✓ PIM-DM указан в draft-ietf-idmr-pim-dm-05.txt
    - ✓ плотные группы имеют большое кол-во участников в большом кол-ве мест
    - ✓ Доставка Multicast трафика по всей сети методом выталкивания
  - **PIM-SM** (PIM Sparse Mode) – разряженный режим
    - ✓ PIM-SM V1 определен в RFC 2117, V2 в RFC 2362
    - ✓ Разряженные группы имеют только несколько участников в небольшом кол-ве мест
    - ✓ Доставка многоадресного трафика осуществляется методом втягивания. Трафик передается только в те сети, где есть активные хосты, пославшие явный запрос на получение данных
    - ✓ Для распространения информации об активных хостах используется дерево общего доступа
    - ✓ Трафик может оставаться в пределах дерева общего доступа или перейти на оптимизированной дерево от источника

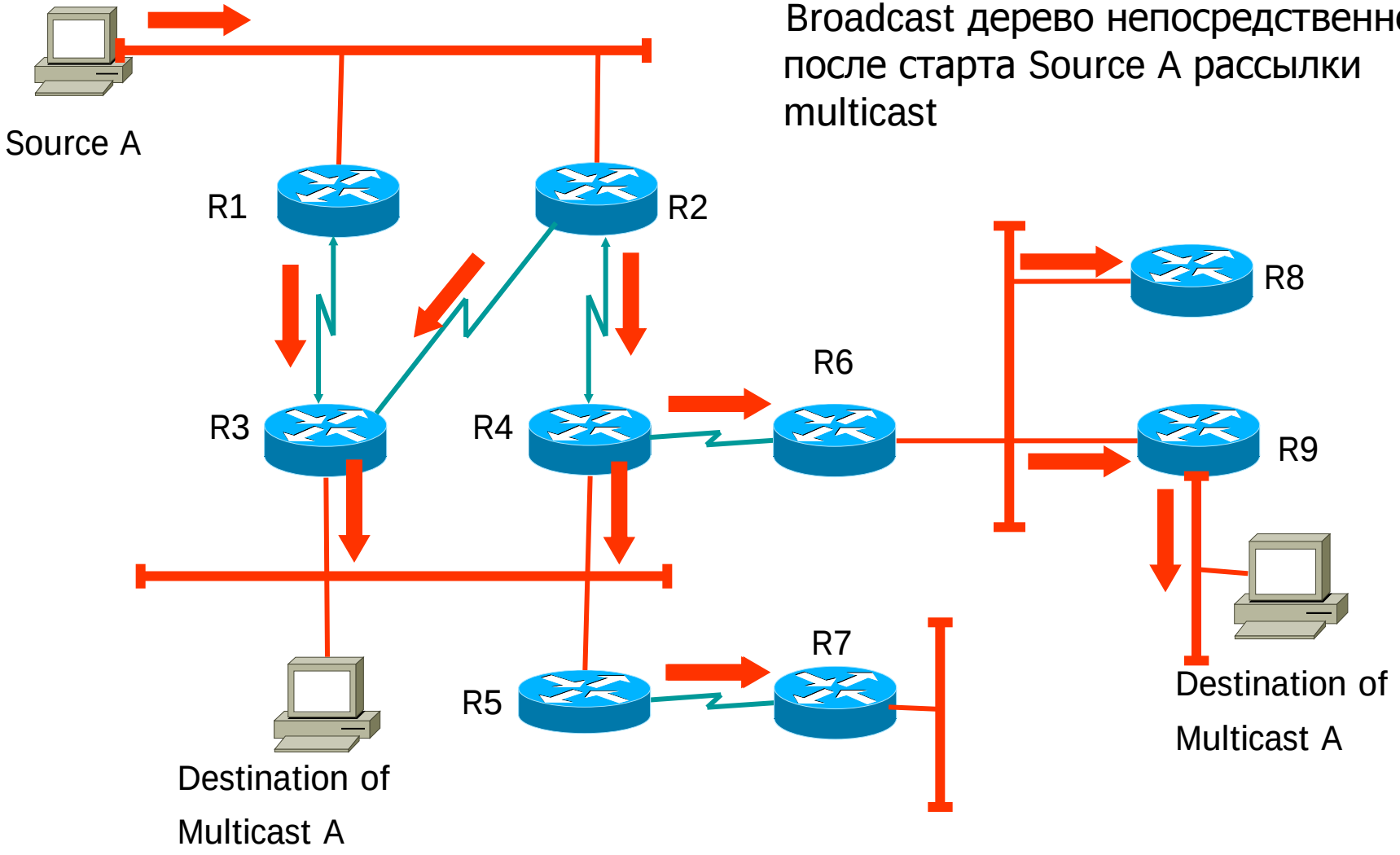
PIM-DM (PIM Dense Mode)

- **Плотный режим PIM**
  - Основан на RPF (reverse path forward) принципе и методе отсечения
  - Вначале PIM-DM распространяет multicast трафик по всей сети
    - ✓ этот процесс называется **flooding первого пакета**,
    - ✓ Роутеры, не имеющие соседей, расположенных в направлении передачи трафика, не передают нежелательный трафик (отсечение)
  - Такой процесс (распространение многоадресного трафика по всей сети) повторяется каждые 3 минута
    - ✓ этот процесс называется **периодический flooding**
  - Механизм распространения и отсечения трафика реализуется посредством **накопления роутером "информации о состоянии"** формируемой **на основе реального multicast трафика**
    - ✓ В трафике содержится информация об источнике и группе
    - ✓ Роутеры , расположенные в направлении передачи, могут создать собственные многоадресные таблицы передачи
    - ✓ PIM-DM поддерживает только деревья источника: структура (S, G)
    - ✓ PIM-DM не использует деревья общего доступа: структура (*, G)

PIM-DM (PIM Dense Mode)

- **Плотный режим PIM (продолжение)**
  - строит дерево маршрутов аналогично DVMRP
    - ✓ похож на DVMRP, но никакой дополнительный multicast протокол маршрутизации не используется
  - полагается на наличие нормального unicast routing протокола
  - unicast routing protocol будет рассчитывать путь от роутера до назначенных сетей (источника multicast-трафика)
  - в отличие от усечённых broadcast деревьев DVMRP, PIM-DM строит broadcast деревья
    - ✓ деревья строятся на лету, когда идёт затопление первым пакетом
    - ✓ будет отправлен только первый полученный пакет
    - ✓ при получении такого же пакета на другом интерфейсе, распространение будет остановлено
  - метрика пути unicast таблицы маршрутизации будет использоваться для RPF алгоритма
    - ✓ RPF алгоритм рассмотрен ранее
  - не может работать с асимметричной метрикой
- **Нет update-сообщений (нет протокола), есть только “информации о состоянии”**

Пример 1: Multicas трафик



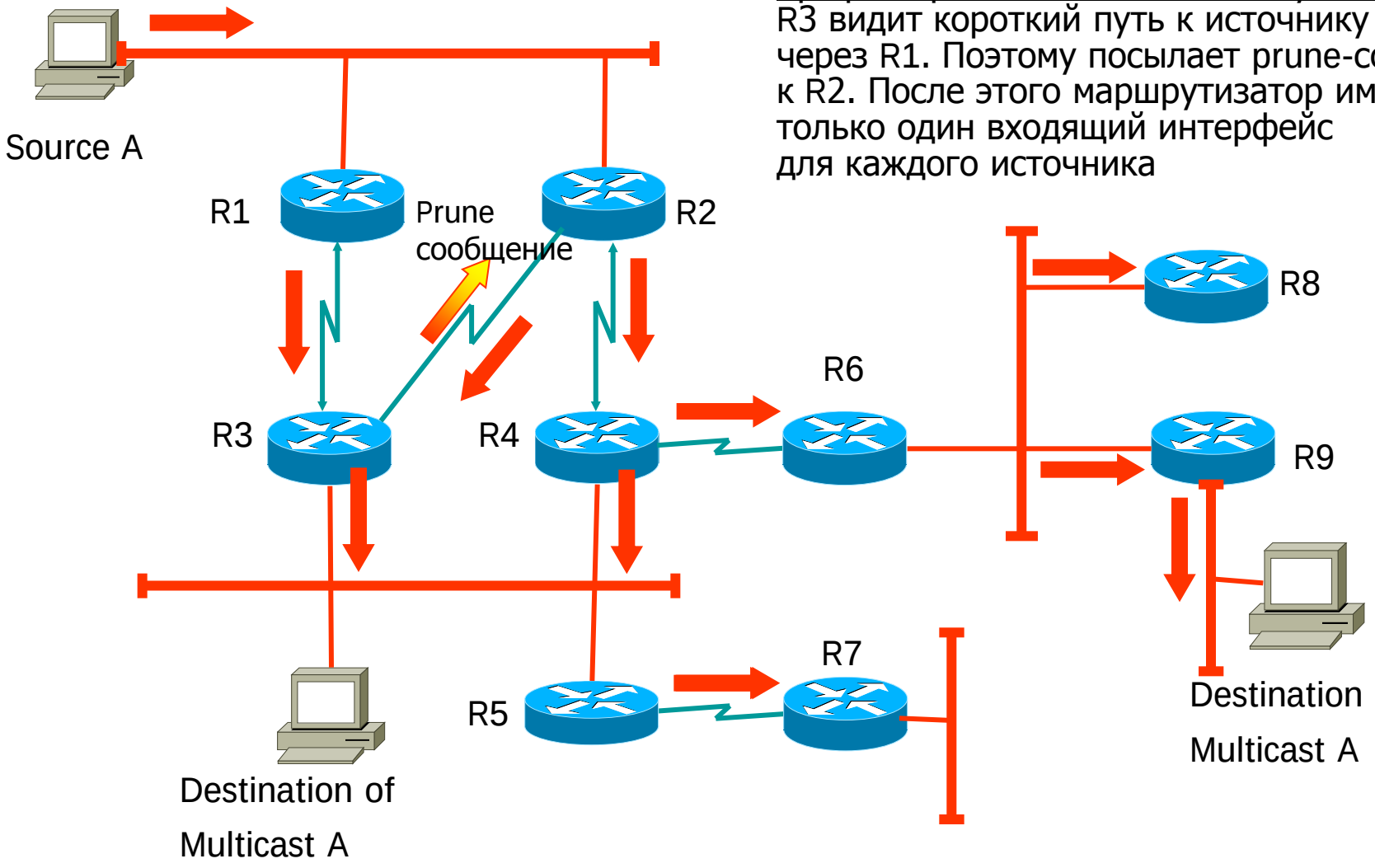
Broadcast дерево непосредственно после старта Source A рассылки multicast

PIM-DM

PIM – Плотный режим (продолжение)

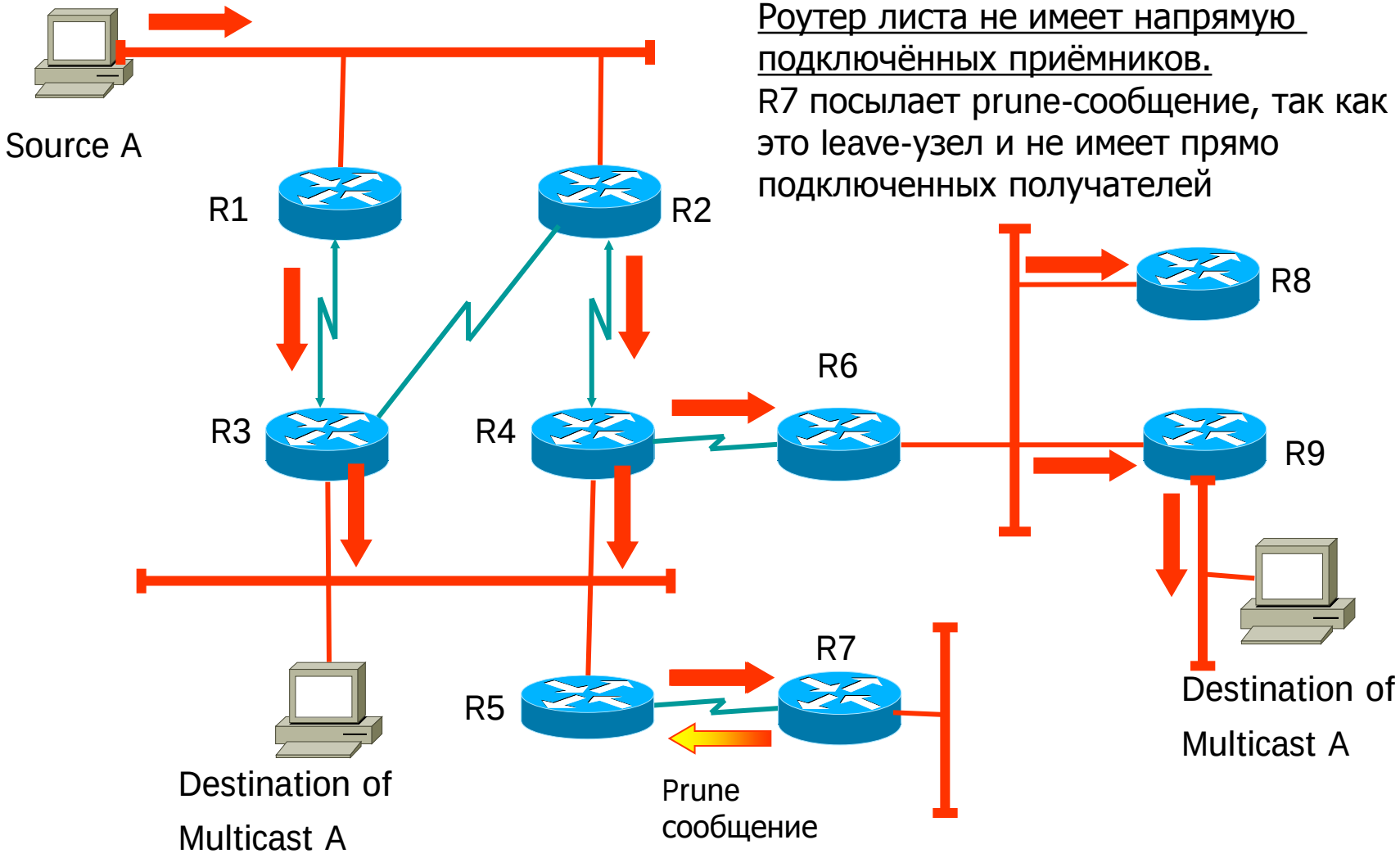
- крайне простой протокол / метод
  - ✓ сохранение (кэширование) prune-сообщений (source/group состояний)
  - ✓ в случае нехватки памяти, отсечение (prune) сводится к минимуму, до недавно используемого контекста
- специальные процедуры, чтобы решить задачу отсечения в broadcast сетях и управления равными по стоимости мульти-путями
  - ✓ prune-сообщения посылаются ко всем PIM-роутерам по multicast адресу 224.0.0.13 (в пределах сегмента сети или точка-точка)
  - ✓ Роутер посылает prunes в следующих случаях
    - ➢ Трафик приходит не в RPF точку интерфейса
    - ➢ Роутер листа не имеет напрямую подключённых приёмников
    - ➢ Роутер в соединении точка-точка, который получил prune от соседа
    - ➢ Роутер в сегменте LAN, который получает prune от соседа на этом сегменте и никто не отвергает prune

Пример 1: pruning (отсечение)



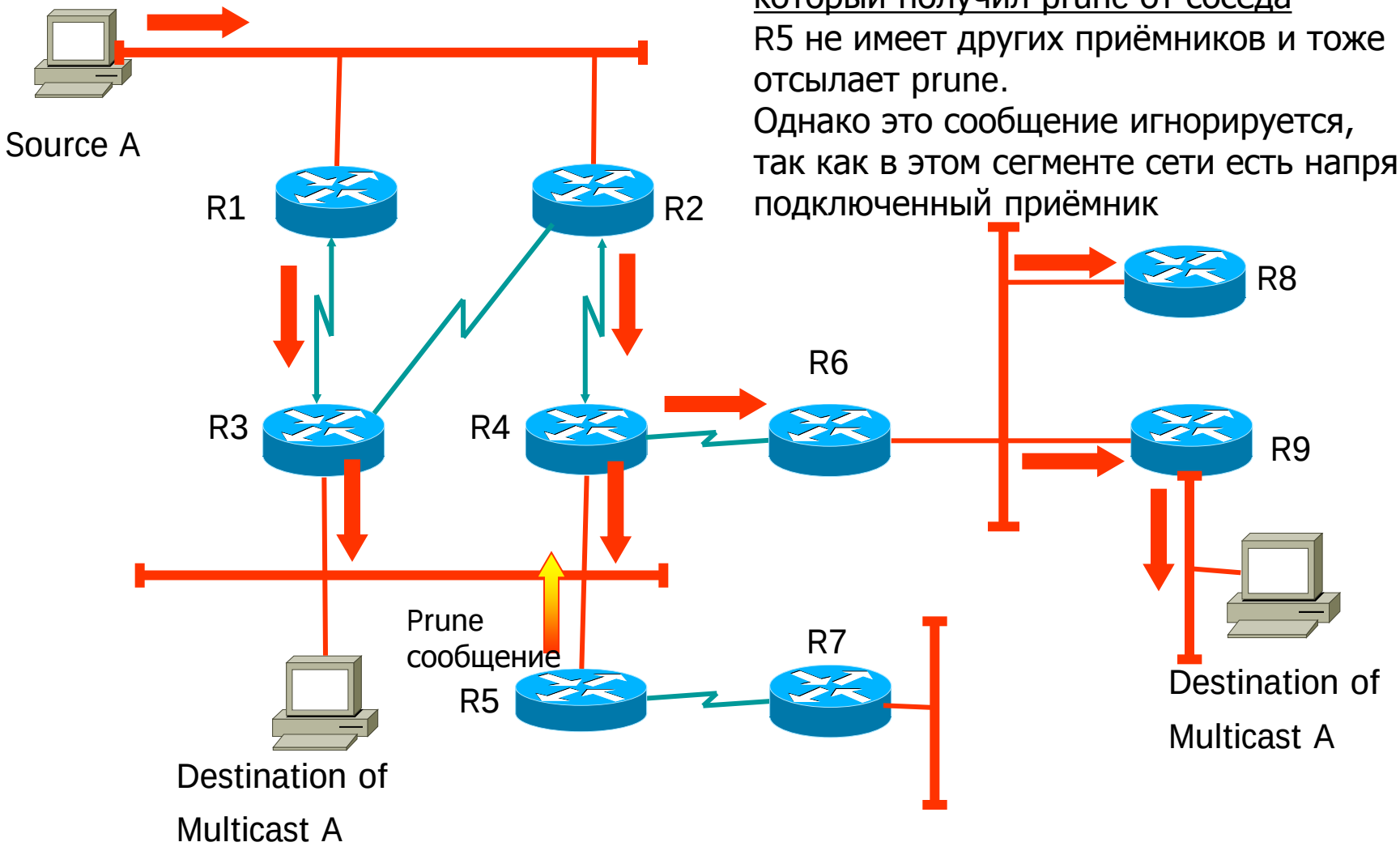
Трафик приходит не в RPF точку интерфейса
R3 видит короткий путь к источнику трафика через R1. Поэтому посылает prune-сообщение к R2. После этого маршрутизатор имеет только один входящий интерфейс для каждого источника

Пример 2: pruning (отсечение)



Роутер листа не имеет напрямую подключённых приёмников.
R7 посылает prune-сообщение, так как это leave-узел и не имеет прямо подключенных получателей

Пример 3: pruning (отсечение)



<u>Роутер в соединении точка-точка, который получил prune от соседа</u>
R5 не имеет других приёмников и тоже отсылает prune.
Однако это сообщение игнорируется, так как в этом сегменте сети есть напрямую подключенный приёмник

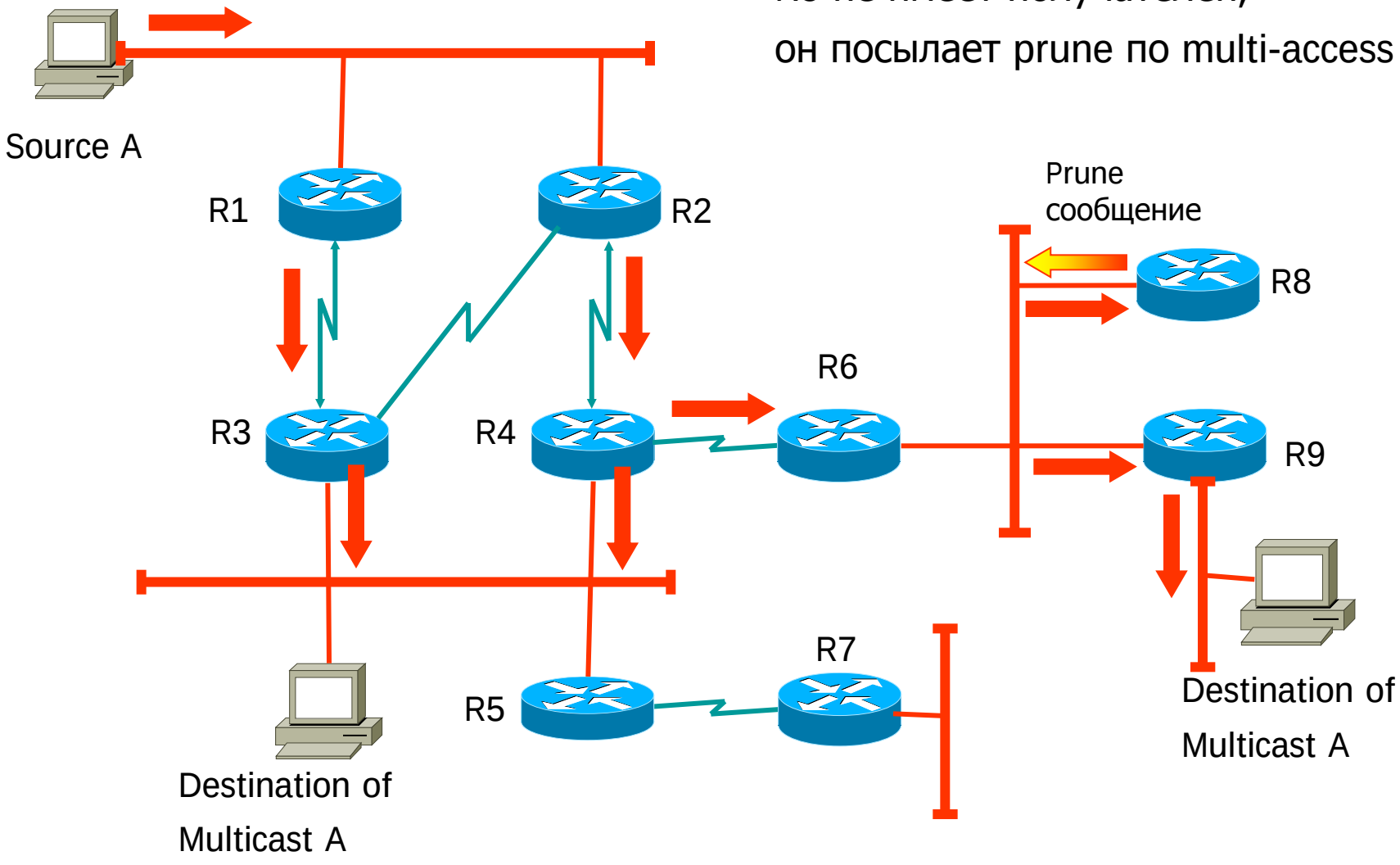
PIM-DM – Override the prune (Отмена отсечения)

PIM – Плотный режим (продолжение)

- В DVMRP маршрутизатор помнит всех своих соседей, поэтому получение prune от одного маршрутизатора в распределённых LAN не проблема
  - ✓ Multicast-трафик отправляется LAN интерфейсом до тех пор, пока все присоединённые маршрутизаторы не пошлют prune-сообщение
- PIM-DM использует специальный алгоритм отмены отсечения
  - ✓ когда вышестоящий маршрутизатор получает prune-сообщение от разделяемого медиа-сегмента, то запускается **prune-delay таймер** (обычно >3сек)
    - ➢ Т.е сразу не отключается трафик
  - ✓ Поскольку prune-сообщения посылаются к all-PIM routers, значит каждый маршрутизатор в сегменте получает prune-сообщения
  - ✓ это даёт возможность маршрутизаторам с активными получателями отправлять join-сообщение (244.0.0.13), чтобы отменить отсечение
  - ✓ это приводит к накоплению задержки

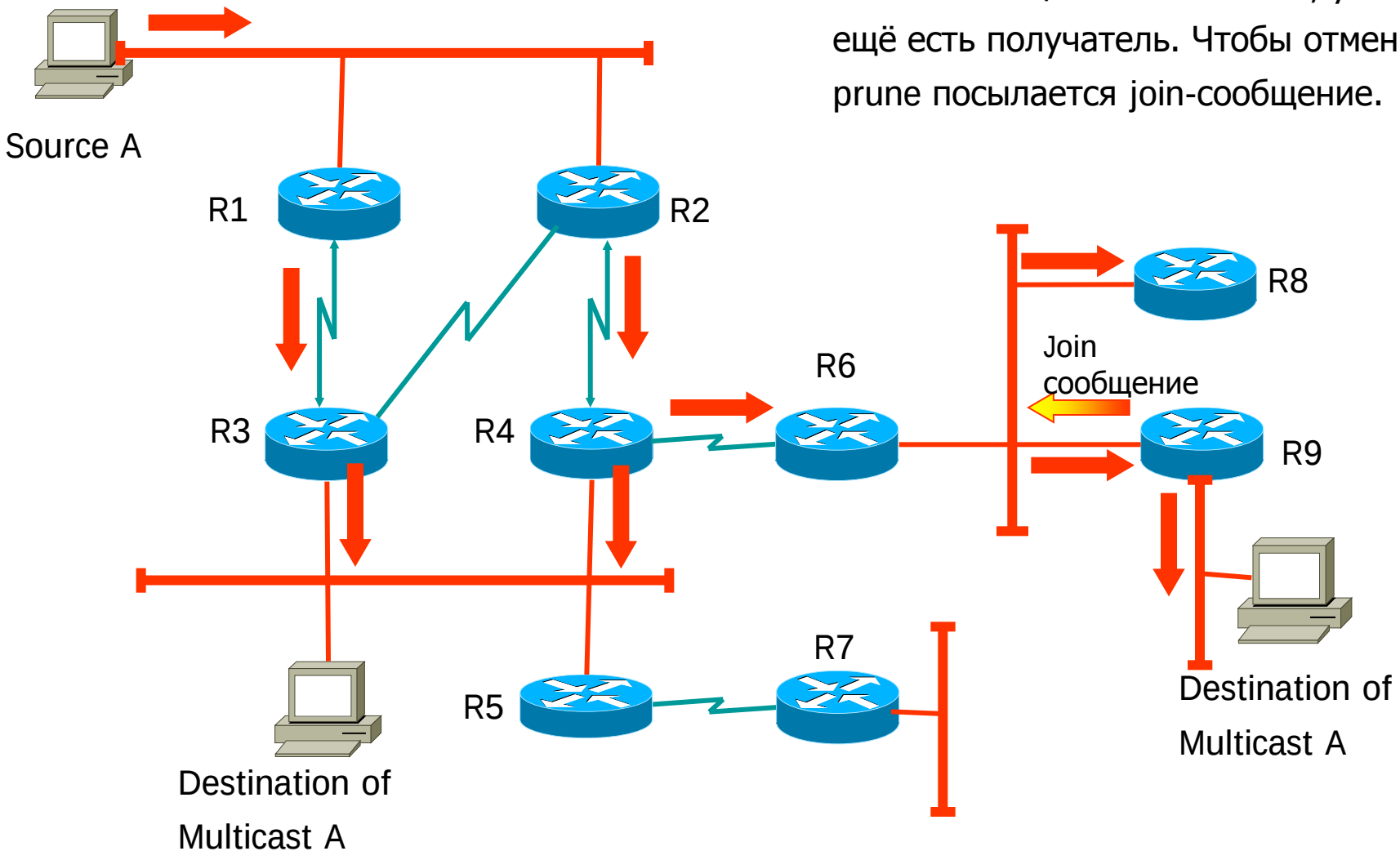
Пример 4: Override the prune (Отмена отсечения)

R8 не имеет получателей,
он посылает prune по multi-access link



Пример 5: Override the prune (Отмена отсечения)

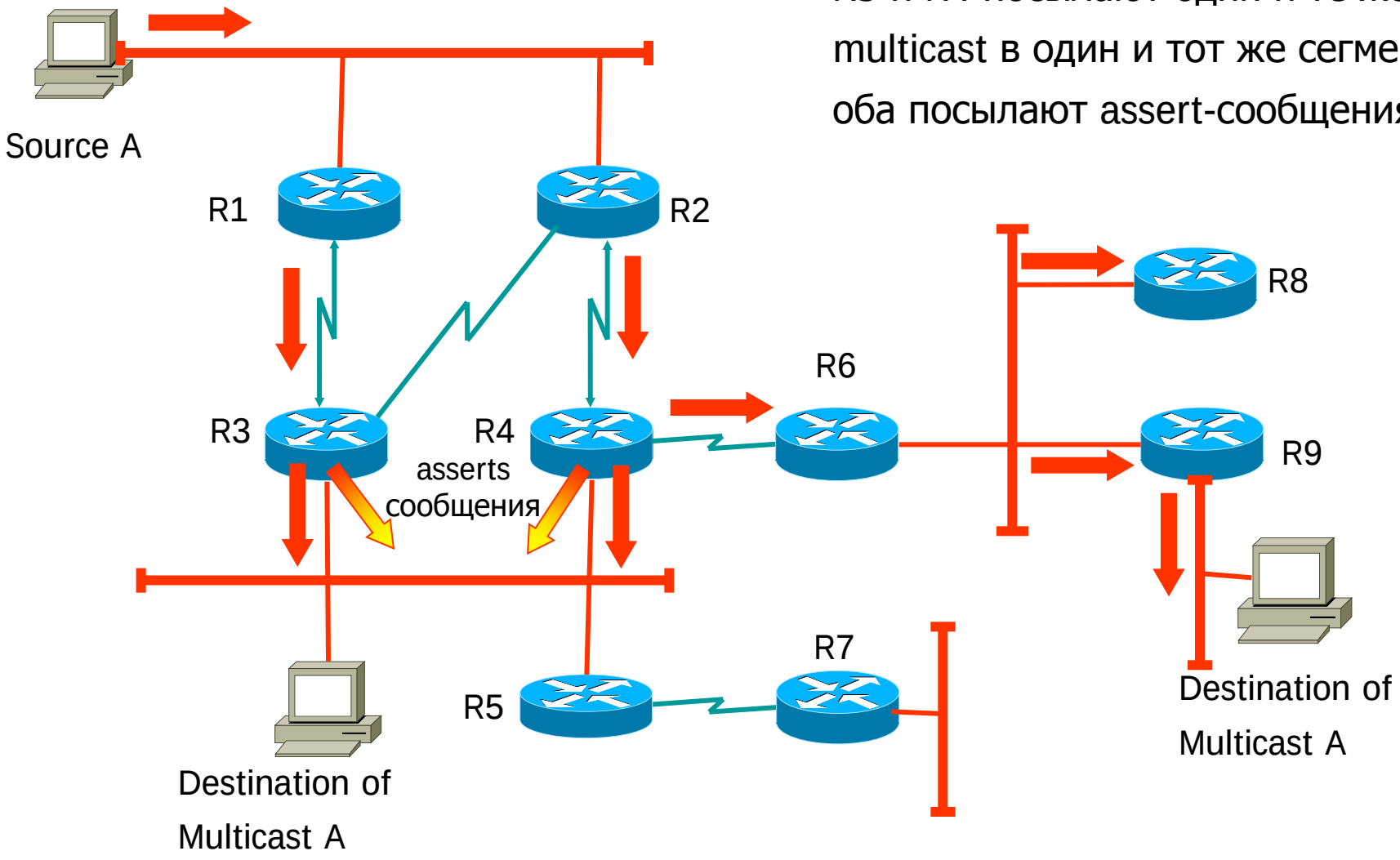
Но это сообщение слышит R9, у которого ещё есть получатель. Чтобы отменить prune посылается join-сообщение.



PIM-DM – **asserts-сообщения**

- PIM – Плотный режим (продолжение)
  - в отличие от DVRMP, который строит усечённые broadcast деревья, PIM-DM должен обрабатывать избыточные пути
  - это делается с использованием **assert-сообщений** (утверждающие-сообщения)
    - ✓ если роутер посылает multicast пакет из выходящего интерфейса, он посылает assert-сообщение (224.0.0.13), чтобы решить какой роутер будет следующим (next-hop)
    - ✓ сообщение содержит административные расстояния маршрутизаторов и метрики к источнику
    - ✓ если значения одинаковые, вышестоящий IP адрес побеждает

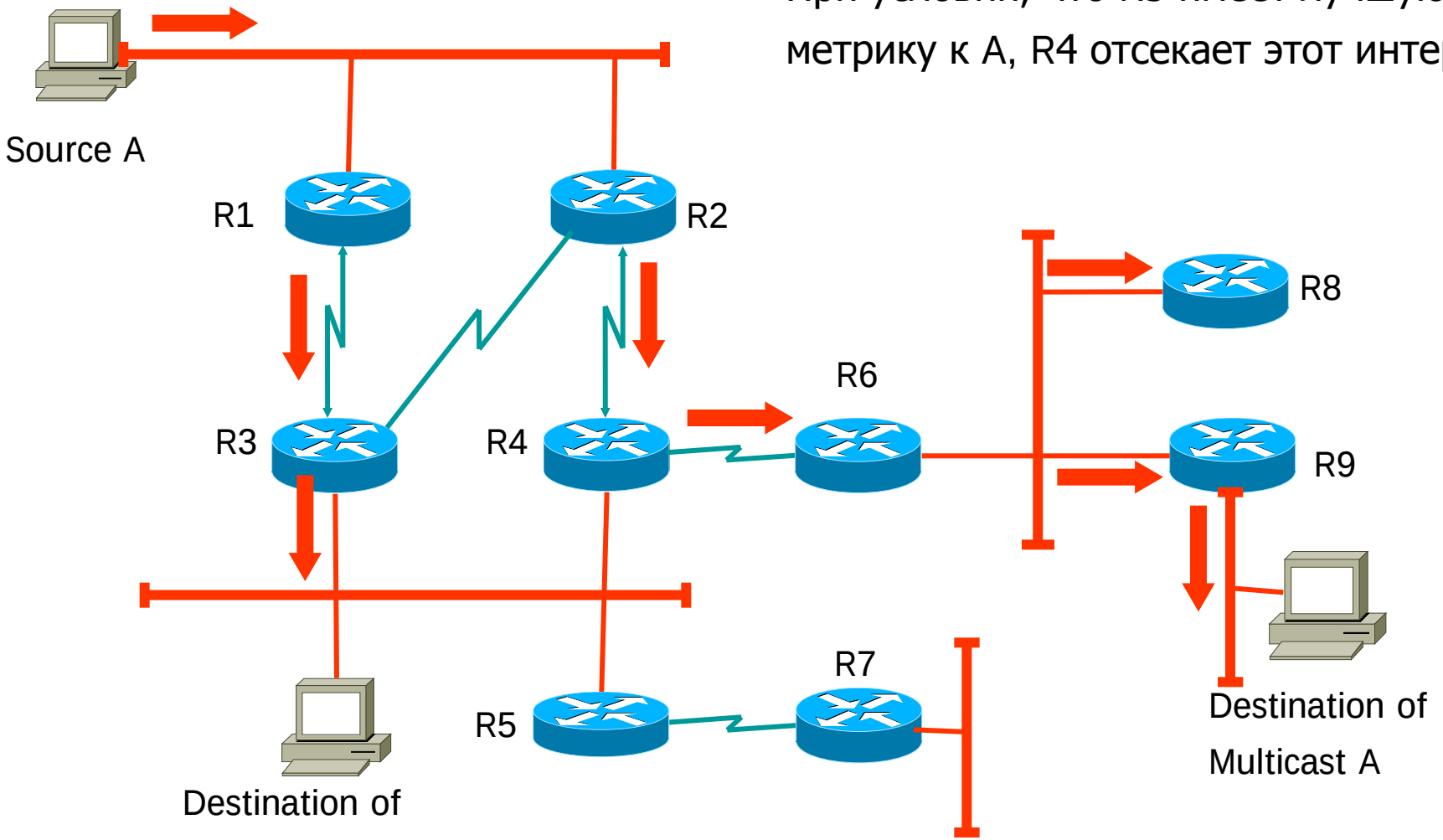
Пример 6: PIM-DM – **asserts-сообщения**



R3 и R4 посылают одни и те же multicast в один и тот же сегмент, оба посылают assert-сообщения

Пример 7: PIM-DM – **asserts-сообщения**

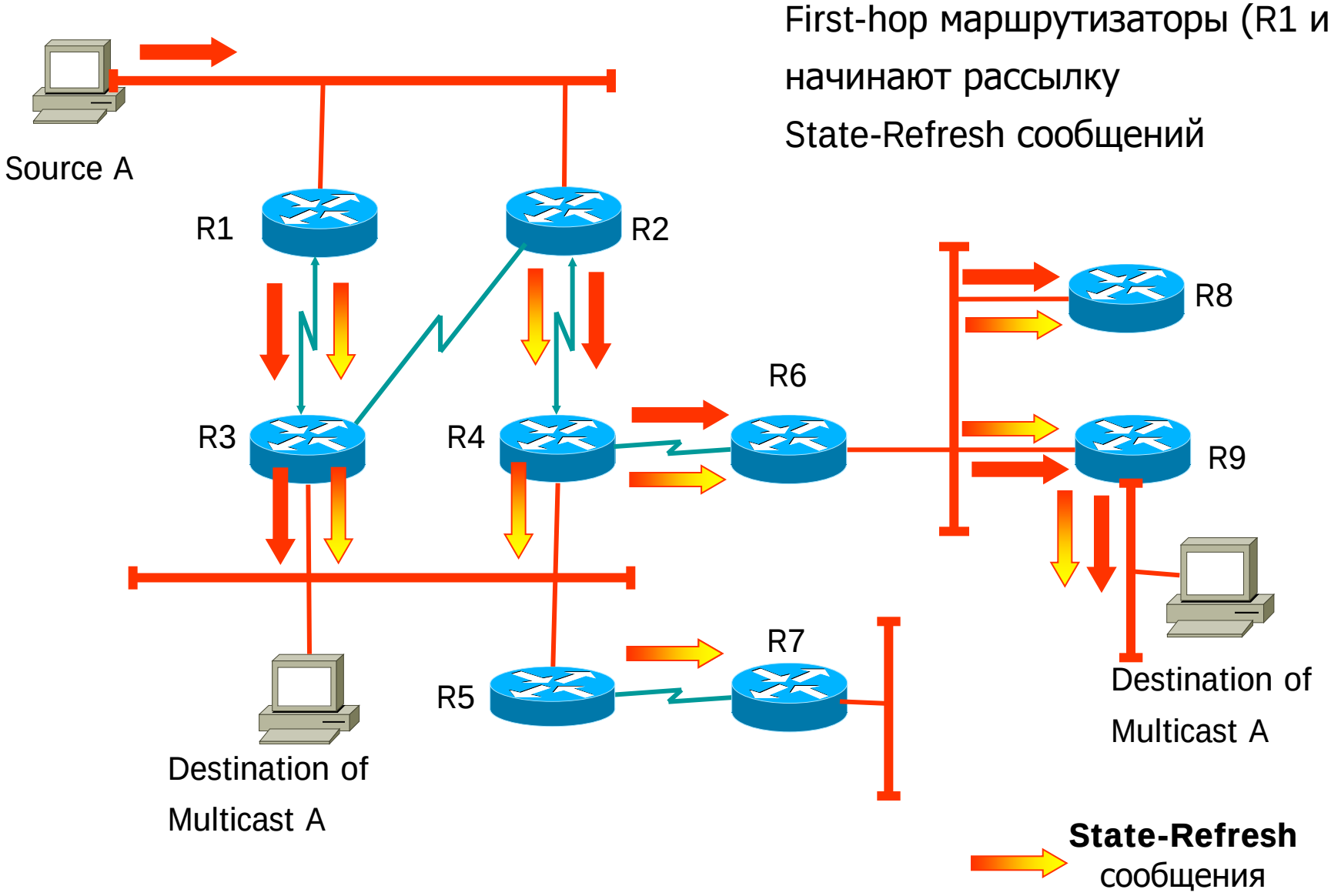
При условии, что R3 имеет лучшую метрику к A, R4 отсекает этот интерфейс



PIM-DM – State-Refresh

- PIM – Плотный режим (продолжение)
  - Каждое pruned-состояние имеет тайм-аут около 3 мин
  - Это значит, что каждые 3 минуты, multicast пакеты затопляются через все дерево
  - Чтобы решить эту проблему, IETF выдвинула интересное предложение, названное **state-refresh** (регенерация состояния)
    - ✓ если источник всё ещё посылает трафик, state-refresh сообщение вниз по broadcast дереву, сбрасывая таймер pruned-состояний
    - ✓ включением той же информации, что и в assert-сообщениях, эти состояния обновляются также

Пример 8: PIM-DM – State-Refresh



PIM-DM: Заключение

- PIM-DM лучше использовать в “быстрых” сетях, где периодический flooding не является проблемой
  - Если unicast сети хорошо структурированы, то PIM-DM масштабируется намного лучше, чем DVRMP
    - ✓ особенно, если полностью поддерживается state-refresh
  - Однако кол-во состояний маршрутизации может стать проблемой в сетях с множеством активных источников/групп

Содержание

- IP мультивещание
  - RFC 1112
  - IGMPv1, IGMPv2, IGMPv3
  - IGMP Snooping
- IP Multicast Маршрутизация
  - DVMRP
  - PIM-DM
  - PIM-SM
  - MOSPF
- MBone
- Multicast Приложения
- RTP/RTPC

Разряженный режим PIM (PIM-SM – PIM Sparse Mode)

- вариант метода SPT (дерево кратчайших маршрутов)
  - ✓ пакеты не “затопляют” всю сеть
  - ✓ multicasts пересылаются только участникам, которые явно присоединились к группе по (*, G) дереву
- отличия основного SPT метода
  - ✓ ядро называют точкой встречи (RP)
  - ✓ дерево не двунаправленное
  - ✓ RP может создать source based (S, G) дерево к Multicast источнику, чтобы избежать инкапсуляции / декапсуляции multicast-пакетов
    - ➢ напоминание: инкапсуляция выполняется first-hop маршрутизатором выбранного источника
  - ✓ маршрутизаторы могут строить source base деревья к Multicast источнику
    - ➢ поэтому название RP; группы временно собираются в RP перед тем, как они построит свои собственные деревья

PIM-SM

- **Подключение к группе (Joining works) очень похожа на SPT**
  - Хост посылает (*,G) join-сообщение его first-hop роутеру
    - ✓ если у роутера уже есть состояние для этой группы (пользователи группы), то он просто добавляет новый интерфейс к (*,G) состоянию входа
    - ✓ если роутер не имеет других приёмников этой группы, то он создаёт новый (*,G) вход и посылает join-сообщение вышестоящему, которым обрабатывается тот же путь
    - ✓ используя те же сообщения роутер может присоединить (S,G) дерево, меняя адрес RP на адрес источника
  - В отличие от других sparse-mode протоколов, PIM создаёт только soft-состояния (тихие-состояния)
    - ✓ поэтому состояния должны обновляться перед их тайм-аутом
    - ✓ маршрутизаторы должны посылать join-сообщения каждую минуту вышестоящему маршрутизатору так долго, пока есть состояние входов
      - ➢ список групп может обновляться одним join-сообщением

PIM-SM

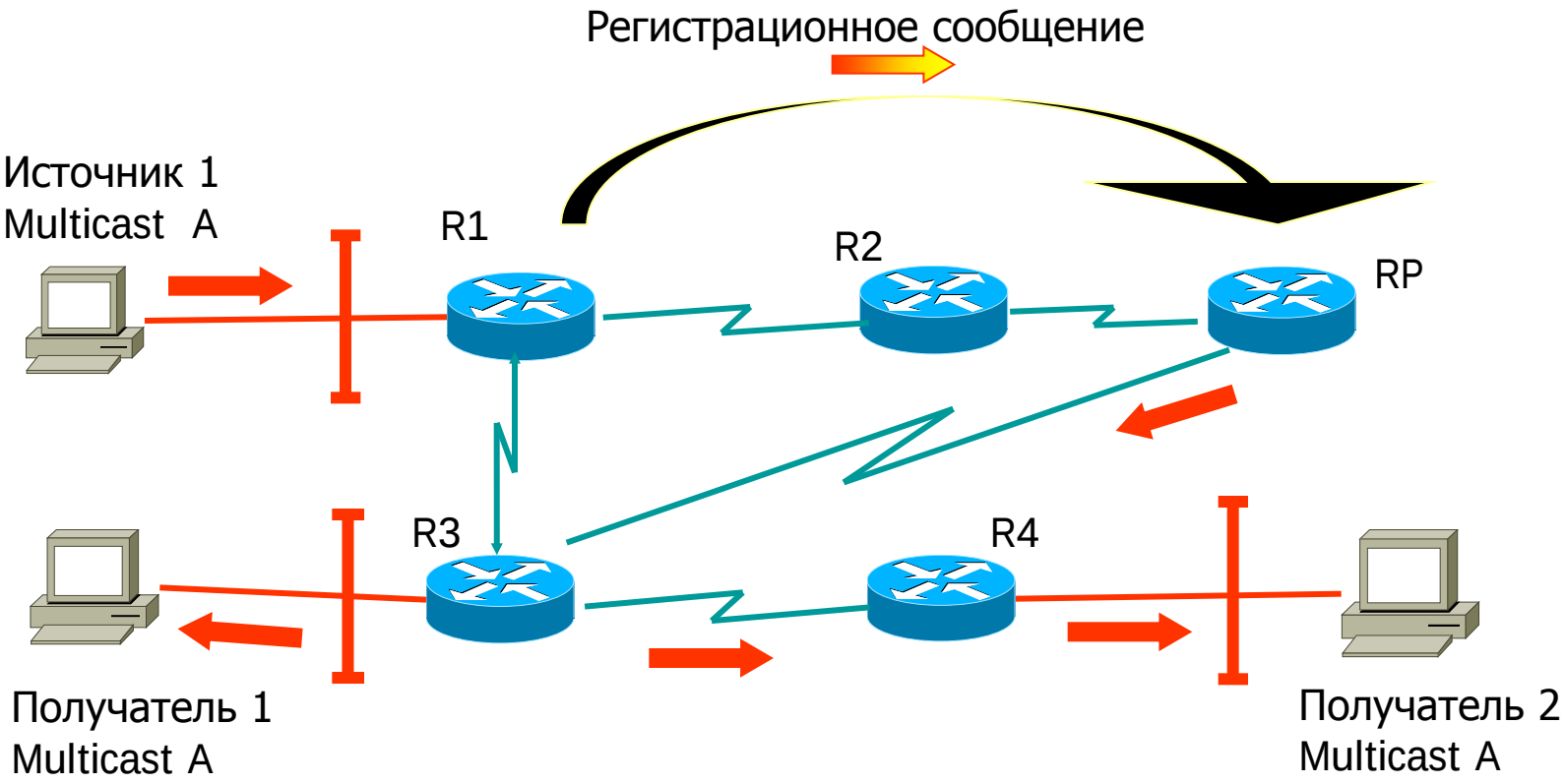
Регистрация источника

- В PIM-SM для получателей есть возможность присоединиться к группе, без отсылающего источника, и для источника начать multicast-рассылку без активных получателей
- Используются специальные регистрационные сообщения
  - ✓ эти сообщения уведомляют RP об активном источнике
  - ✓ и доставляют первые multicast-пакеты
- Когда источник начинает отправку трафика, то first-hop маршрутизатор инкапсулирует пакеты в сообщение регистрации, которое является unicast к RP
  - ✓ RP декапсулирует пакеты, чтобы переслать их группе
  - ✓ и посылает (S,G) join-сообщение к источнику, поэтому нормальный multicast-трафик в итоге достигнет RP

PIM-SM

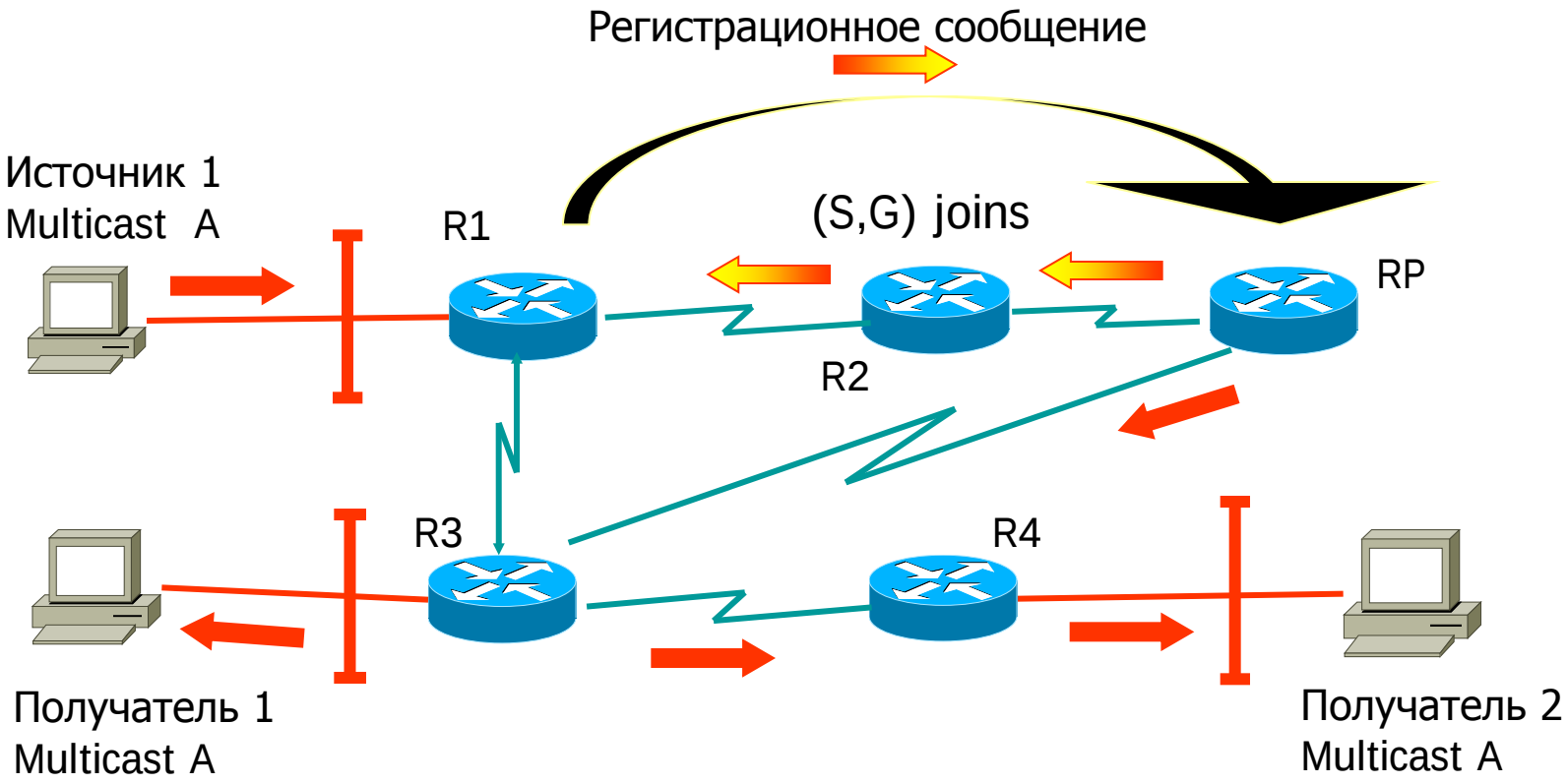
- Регистрация источника (продолжение)
  - Как только пакеты достигнут RP, будет послано сообщение остановки регистрации к источнику, заставляя first-hop маршрутизатор останавливать register-сообщения
    - ✓ RP будет посылать register-stop сообщения сразу же, если нет активных получателей в группе

PIM-SM: Регистрация



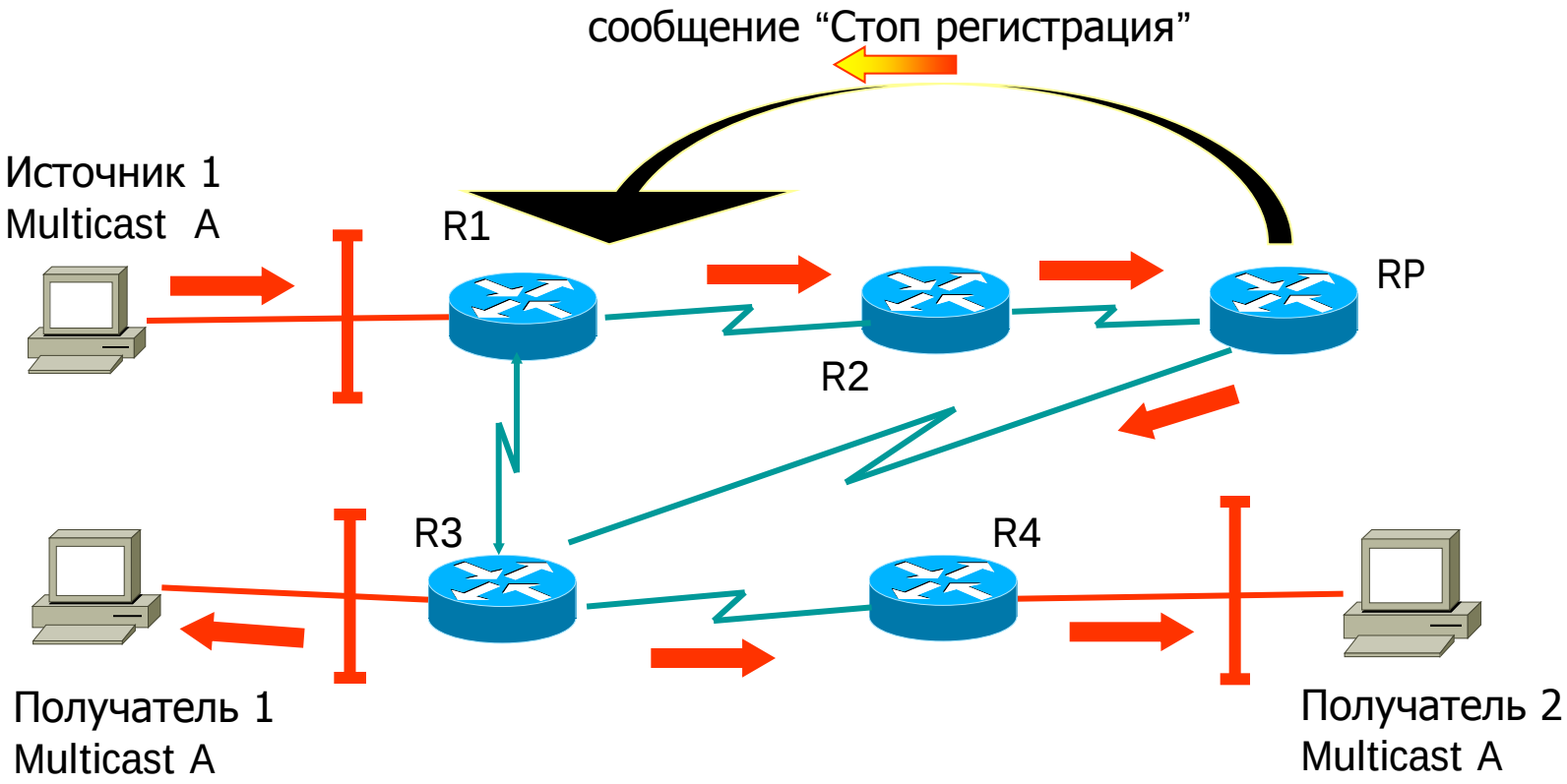
Источник 1 начинает multicast-рассылку. First-hop маршрутизатор инкапсулирует пакеты и unicasts к RP, который затем декапсулирует и передаст их по (*,G) дереву

PIM-SM: Регистрация



RP посылает (S,G) join сообщение “подключения к источнику”, чтобы создать SPT дерево от источника 1 к RP

PIM-SM: Регистрация

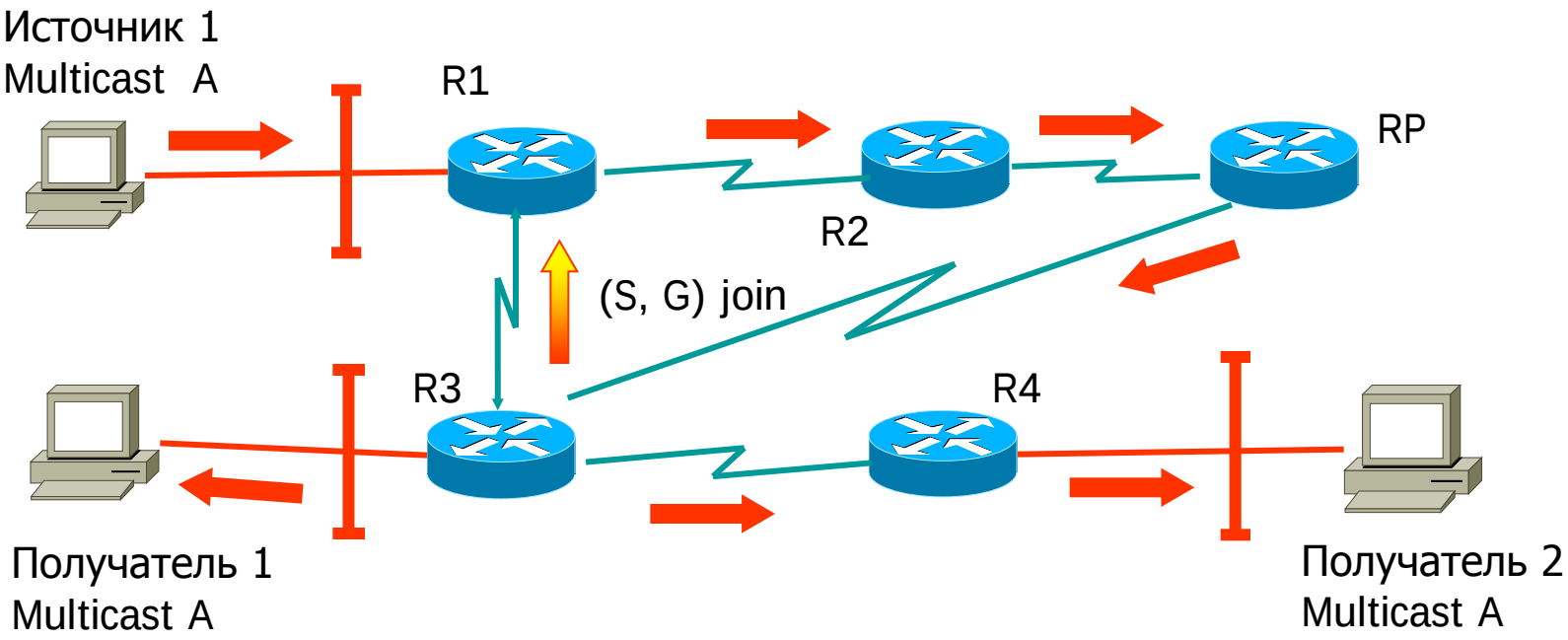


Получив (S,G) joins сообщение First-hop маршрутизатор теперь может послать multicast вниз по SPT к RP, который посылает в ответ register-stop сообщение, чтобы остановить registration-сообщения

PIM-SM: SPT Переключение

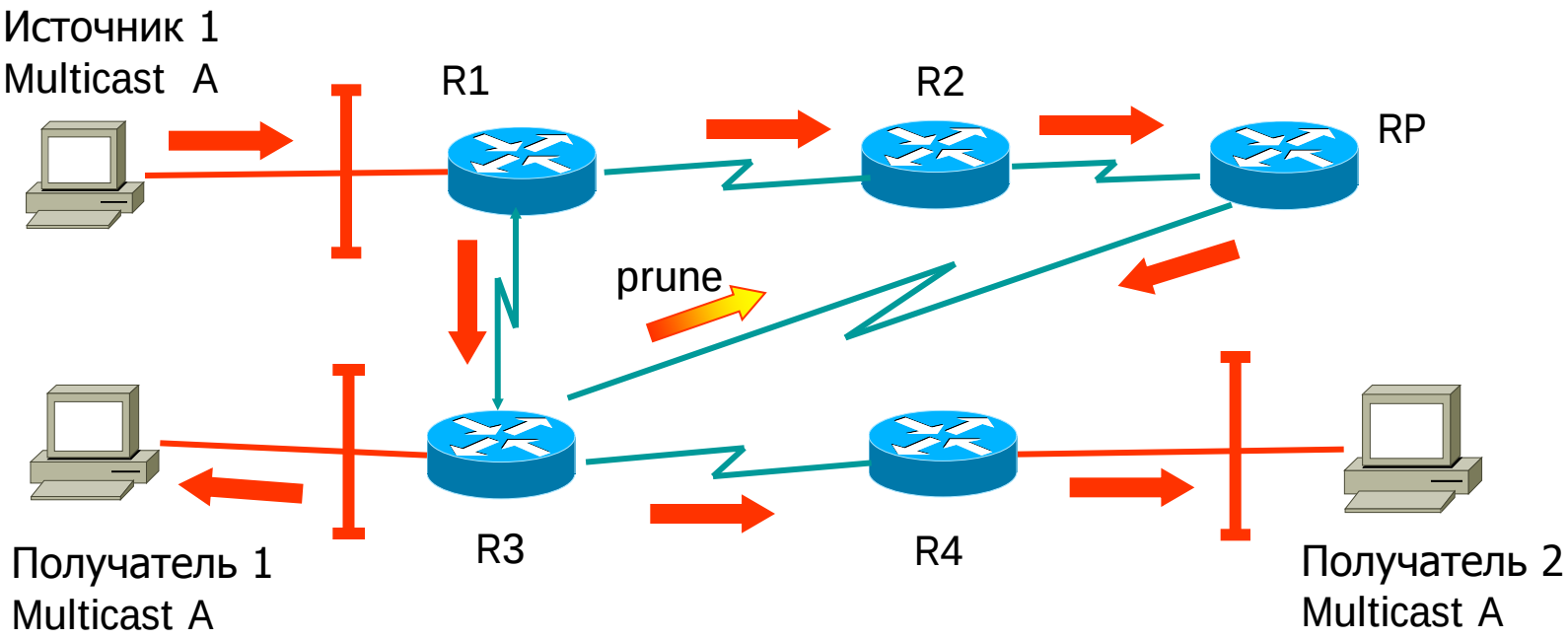
- **First-hop multicast маршрутизатор multicast приёмника, может вызвать формирование source based дерева (S, G)**
  - новое join-сообщение по кратчайшему пути к источнику и отсечённому к RP
  - эта особенность вызвана тем, что указанный SPT-порог полосы пропускания, превышается
    - ✓ в CISCO маршрутизаторах по умолчанию 0
  - любой промежуточный маршрутизатор может вызвать строительство source-based распределённого дерева
    - ✓ например, распознаётся если слишком много трафика от данного источника проходит по неоптимальному пути
    - ✓ помните: multicast маршрутизатор способен вычислить кратчайший путь к RP и следовательно к любому другому сетевому адресу

PIM-SM: SPT Переключение



First-hop маршрутизатор от получателя 1 отправляет (S,G) join к источнику

PIM-SM: SPT Переключение

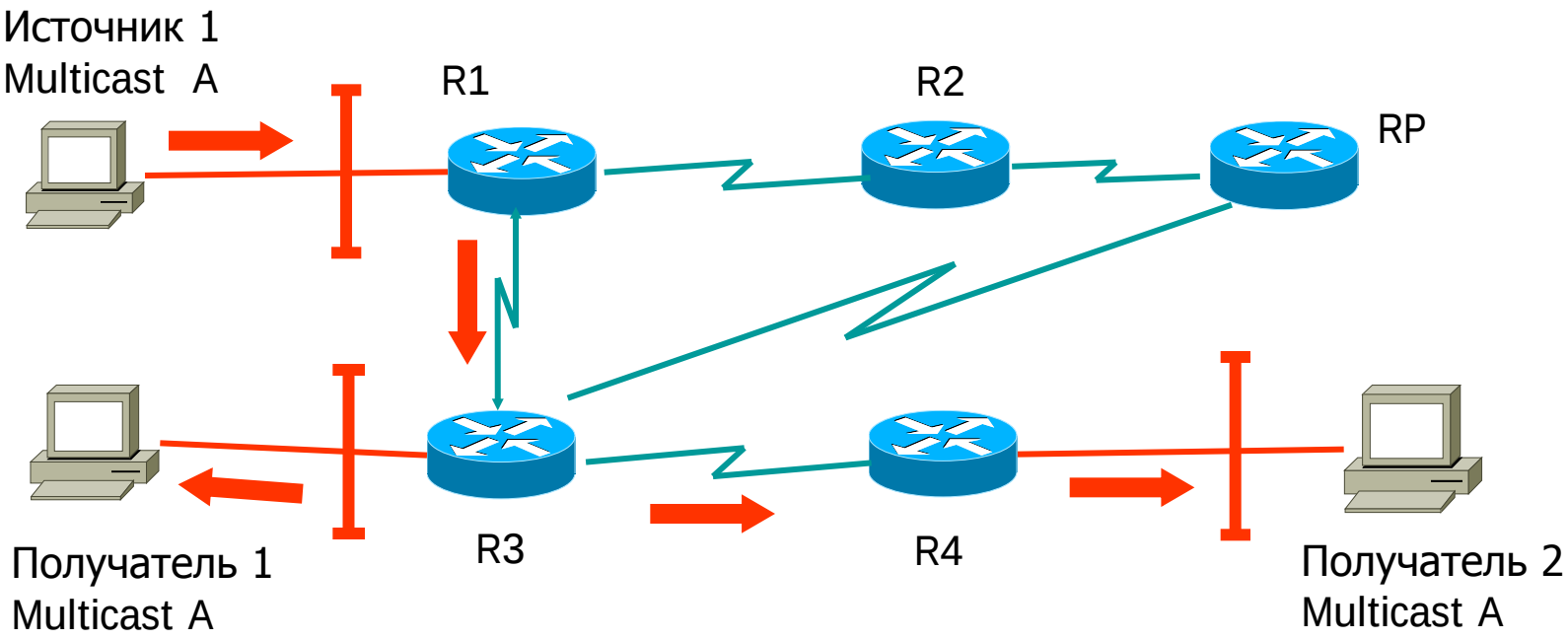


Join-сообщение будет следовать к источнику, строя SPT по путь.

Теперь есть два потока достигающих одного и того же маршрутизатора.

Посылается специальное prune-сообщение, которое направляется к RP

PIM-SM: SPT Переключение



Теперь в нашем примере RP не имеет других интерфейсов и тоже будет посылать отсечение к источнику. Приводя к результату, показанному выше на схеме

PIM – SM: Заключение

- **PIM-SM лучше подходит для multicast сетей, которые имеют потенциальных участников на окончаниях WAN связей**
- **Способность устанавливать SPT-порог, помогает инженерам конфигурировать там домен**
  - это помогает контролировать кол-во состояний, созданных мультивещанием внутри сети
    - ✓ Например, высокий порог приводит к топологии звезда
    - ✓ установка его очень низким уменьшает значимость RP с самого начала

Содержание

- IP мультивещание
  - RFC 1112
  - IGMPv1, IGMPv2, IGMPv3
  - IGMP Snooping
- IP Multicast Маршрутизация
  - DVMRP
  - PIM-DM
  - PIM-SM
  - MOSPF
- MBone
- Multicast Приложения
- RTP/RTPC

MOSPF

- **Multicast расширения к OSPF**
  - определён в RFC 1584
  - RFC 1585: MOSPF Анализ и Опыт
  - обеспечивает multicast-маршрутизацию в пределах AS
  - акцентируется на эффективном вычислении маршрута
- **MOSPF**
  - сетевая карта дополнена новым типом записи состояния канала → принадлежность группы LSA
    - ✓ создаётся multicast-маршрутизаторами, отвечающими за подсеть
    - ✓ получен в итоге пограничными маршрутизаторами
    - ✓ специальные соображения для путей с равной стоимостью
    - ✓ вместе с маршрутизатором и сетью LSA, SPT рассчитывается для каждого источника-сети / группы
      - ➢ Результат (S/m, G) дерево (источник/маска подсети, группа)

MOSPF (продолжение)

- RPF и prune вычисления
  - ✓ может быть сделано локально в памяти без flooding первого пакета или периодического flooding
- не требуется дополнительных multicast протоколов маршрутизации
  - ✓ полагается на нормальный unicast routing protocol OSPF
  - ✓ допускает симметричную метрику
- проблема вычисления кратчайшего пути до каждого источника
  - ✓ может загружать даже самые мощные CPU multicast маршрутизаторов
- поэтому вычисления по требованию
  - ✓ когда приходит первый пакет данного источника и группе
    - ➢ но для достаточного кол-ва активных источников, даже этого может быть достаточно, чтобы перегрузить CPU, особенно, если получатели часто самостоятельно включаются и выключаются

MOSPF – Межзонная маршрутизация

- **MOSPF Межзонная маршрутизация**
  - Для того, чтобы MOSPF мог работать между двумя зонами, ABR должен иметь возможность multicast
    - ✓ MABR
  - MABR будет собирать multicast информацию и посылать этот LSA в зону 0
    - ✓ замечание: зона 0 не будет пересылать информацию в других направлениях
  - этого метода достаточно, когда источники находятся в зоне 0
  - чтобы решить эту дилемму, MABR будет включать подстановочный бит в их маршрутизатор LSA, направленный к non-backbone зоне
    - ✓ это определяет MABR как участника для каждой multicast группы
    - ✓ они передадут информацию в зону 0, действуя как источник
  - Это приводит к нежелательному трафику, если нет “реальных” источников

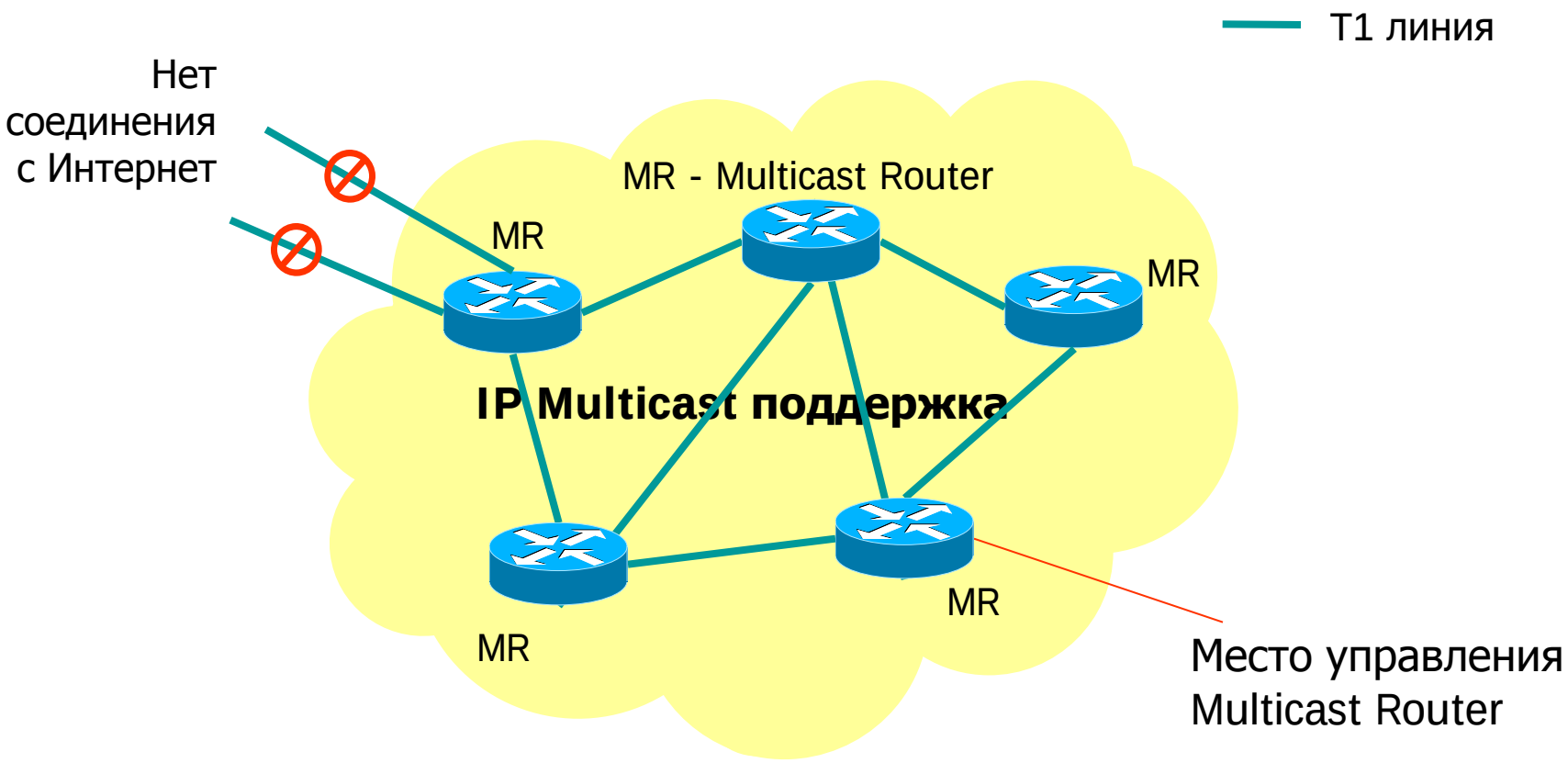
Содержание

- IP мультивещание
  - RFC 1112
  - IGMPv1, IGMPv2, IGMPv3
  - IGMP Snooping
- IP Multicast Маршрутизация
  - DVMRP
  - PIM-DM
  - PIM-SM
  - MOSPF
- MBone
- Multicast Приложения
- RTP/RTPC

История MBONE

- **DARTNet**
  - Правительство U.S. сформировало DARPA Testbed Network
    - ✓ утверждённое в начале 1990-ых
    - ✓ игровая площадка для исследователей, чтобы проверить и оценить новые средства и технологии, не затрагивая работы Интернета
    - ✓ первоначально составлена из T1 линий, соединяющих различные сайты
    - ✓ сайты используют Sun SPARCstations, выполняющий multicast маршрутизацию как DVMRP multicast routing daemon
    - ✓ следовательно DARTNet имел свой IP Multicast поддерживающийся между всеми сайтами
    - ✓ первое использование обеспечило аудио-мультивещание IETF собраний

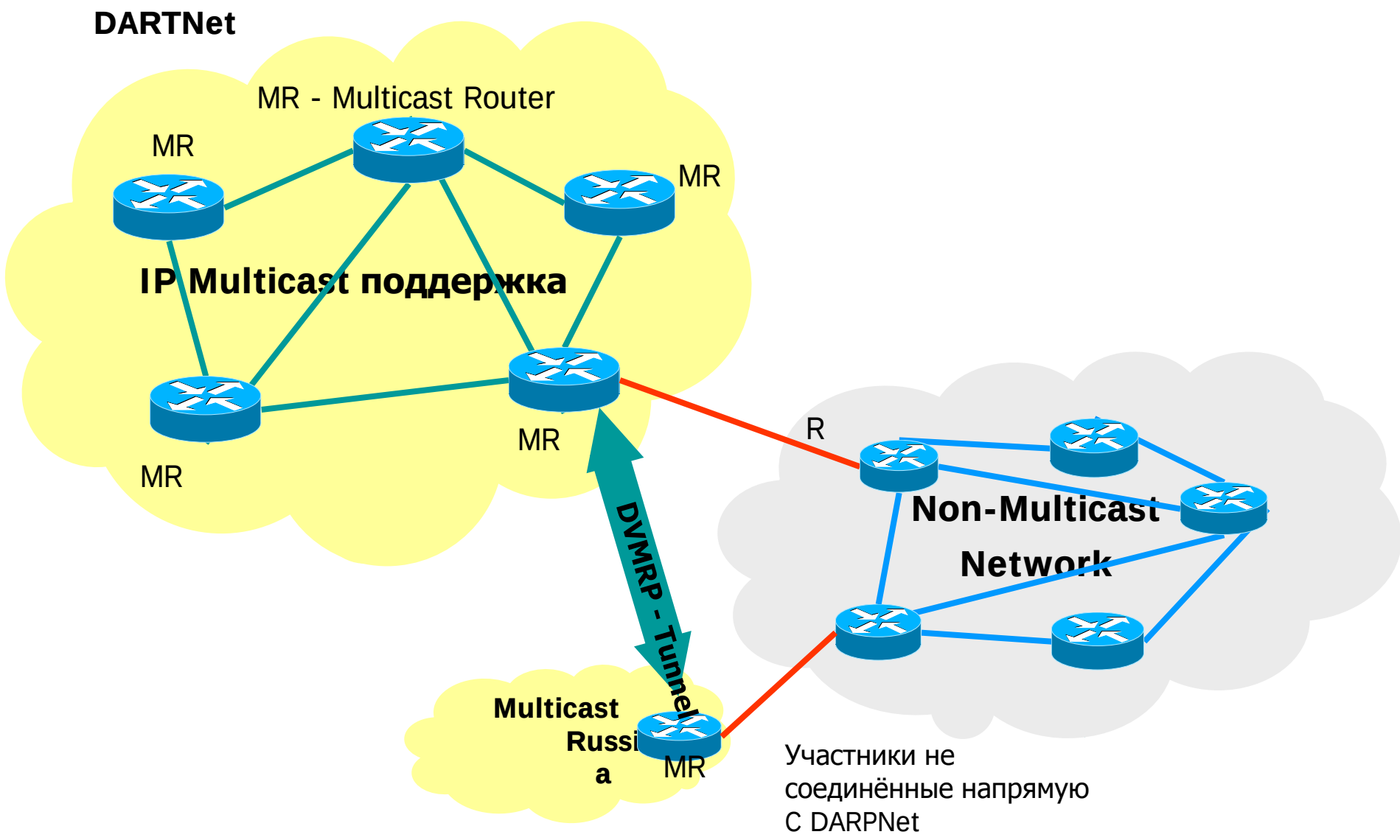
DARPA Test-bed Сеть (DARTNet)



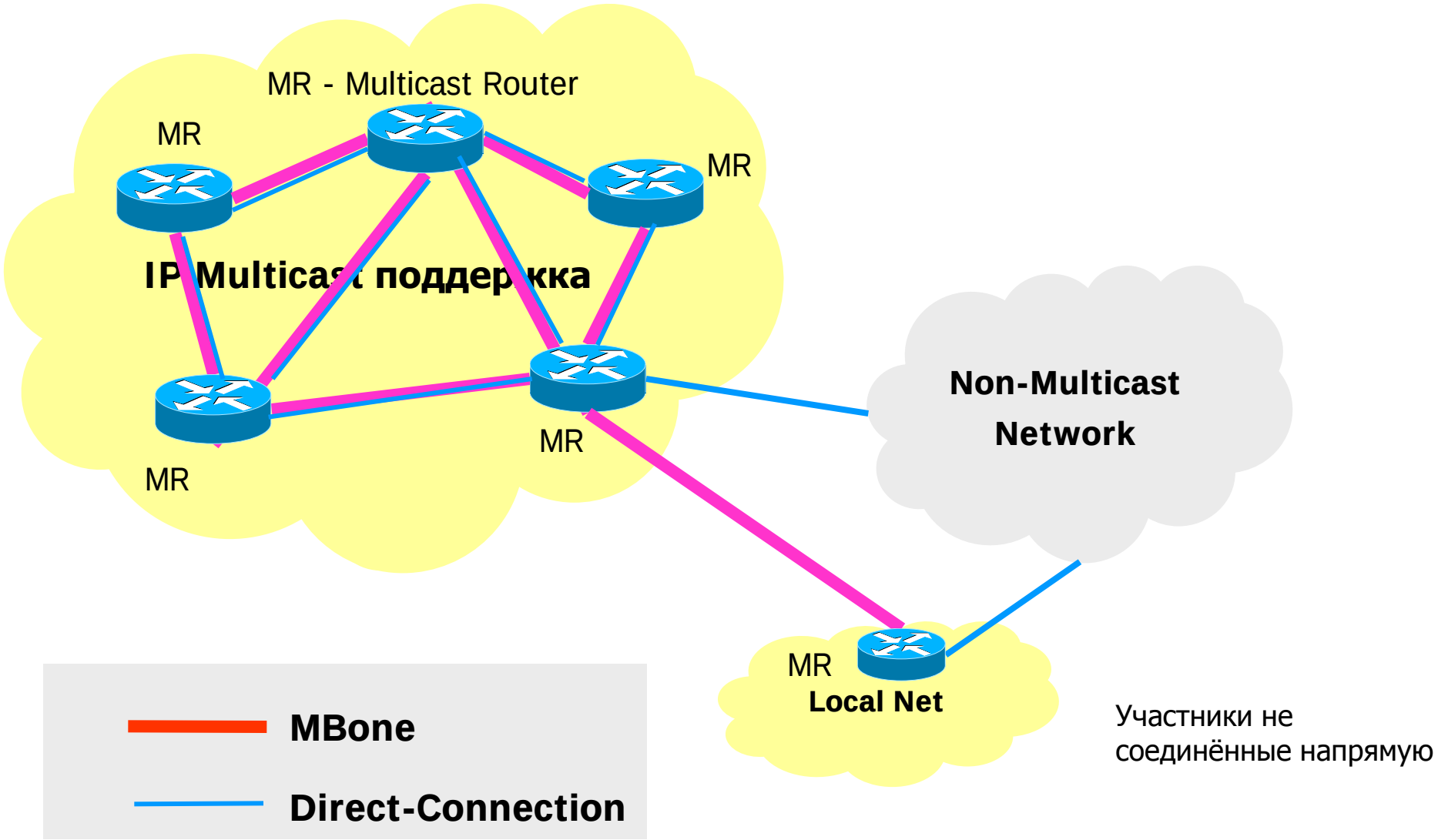
История MBONE (продолжение)

- **DARTNet продолжение / MBone**
  - В то время, 20 сайтов были присоединены к backbone
  - два года спустя, одновременные аудио и видео передачи распространялись более чем 500 участникам, расположенным в 15 странах
  - участники не были напрямую присоединены к DARTNet backbone
  - чтобы обеспечить multicast трафик в DARTNet опорную сеть, должны быть сформированы DVMRP тунели
  - эти туннельные подключения, обеспечивающие соединения с DARTNet (начальное multicast ядро сети) были вскоре названы MBone (Multicast Backbone)
  - сегодня MBone всё ещё работает, но возможность multicast соединения, включена во многих Интернет маршрутизаторах
  - продолжаются попытки интегрировать MBONE непосредственно в инфраструктуру Интернета

DVMRP - Tunneling



DVMRP - Tunneling → MBone

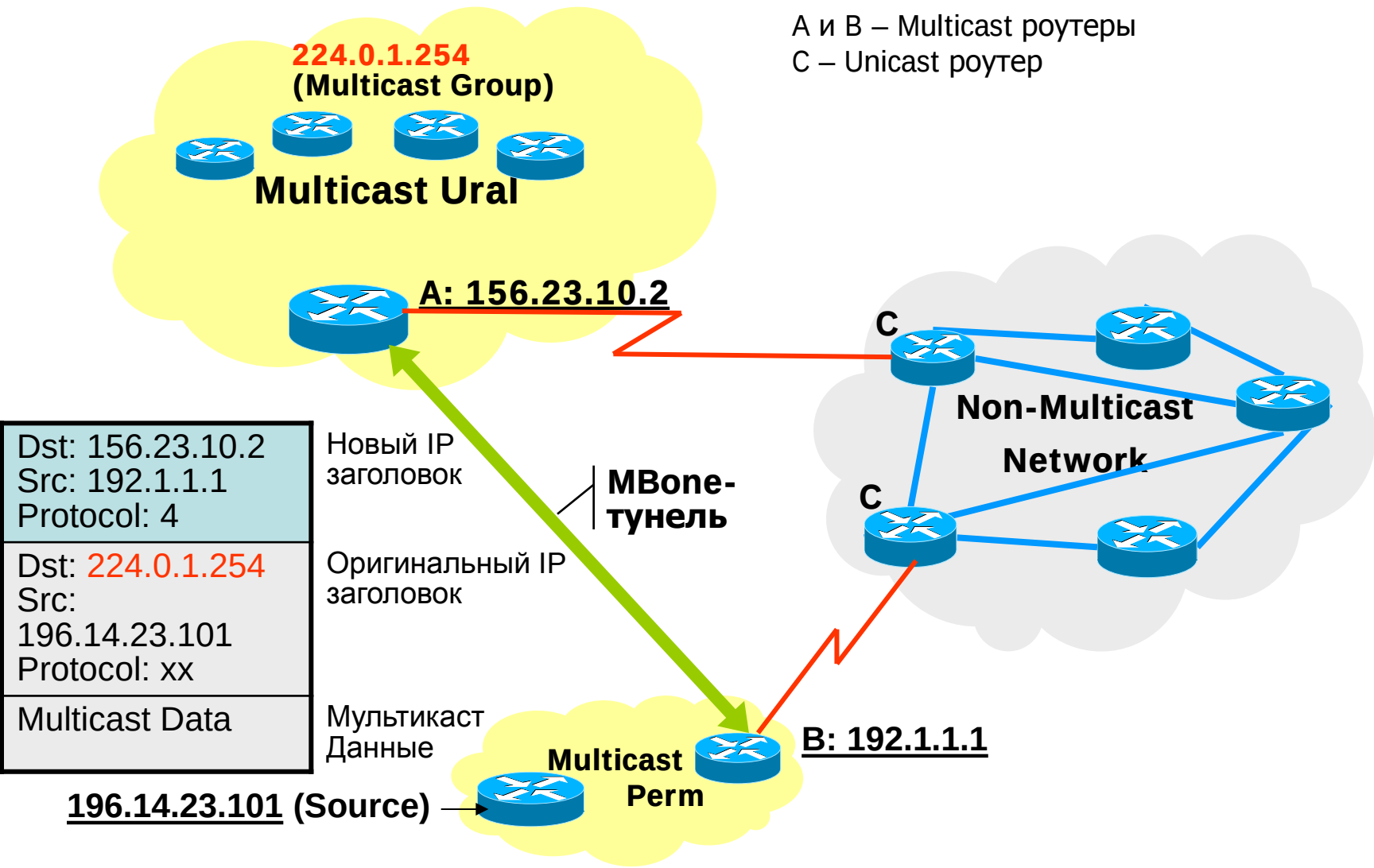


Участники не соединённые напрямую

MBONE Маршрутизация

- **Multicast Backbone сегодня**
  - структура
    - ✓ связанный набор multicast маршрутизаторов
    - ✓ виртуальная сеть с оверлеем на Интернет
    - ✓ оверлейная сеть использует свои multicast протоколы маршрутизации
  - multicast остров
    - ✓ состоит из multicast хостов и multicast маршрутизаторов
    - ✓ обеспечивает multicast сервис для проверки мультимедиа приложений
  - multicast острова подключены через туннели
    - ✓ multicast маршрутизаторы инкапсулируют пакеты в unicast пакеты
    - ✓ инкапсулированные пакеты передаются через стандартные Интернет маршрутизаторы
    - ✓ адрес назначения, содержащийся в unicast пакетах это конечная точка туннеля

MBONE Тунель

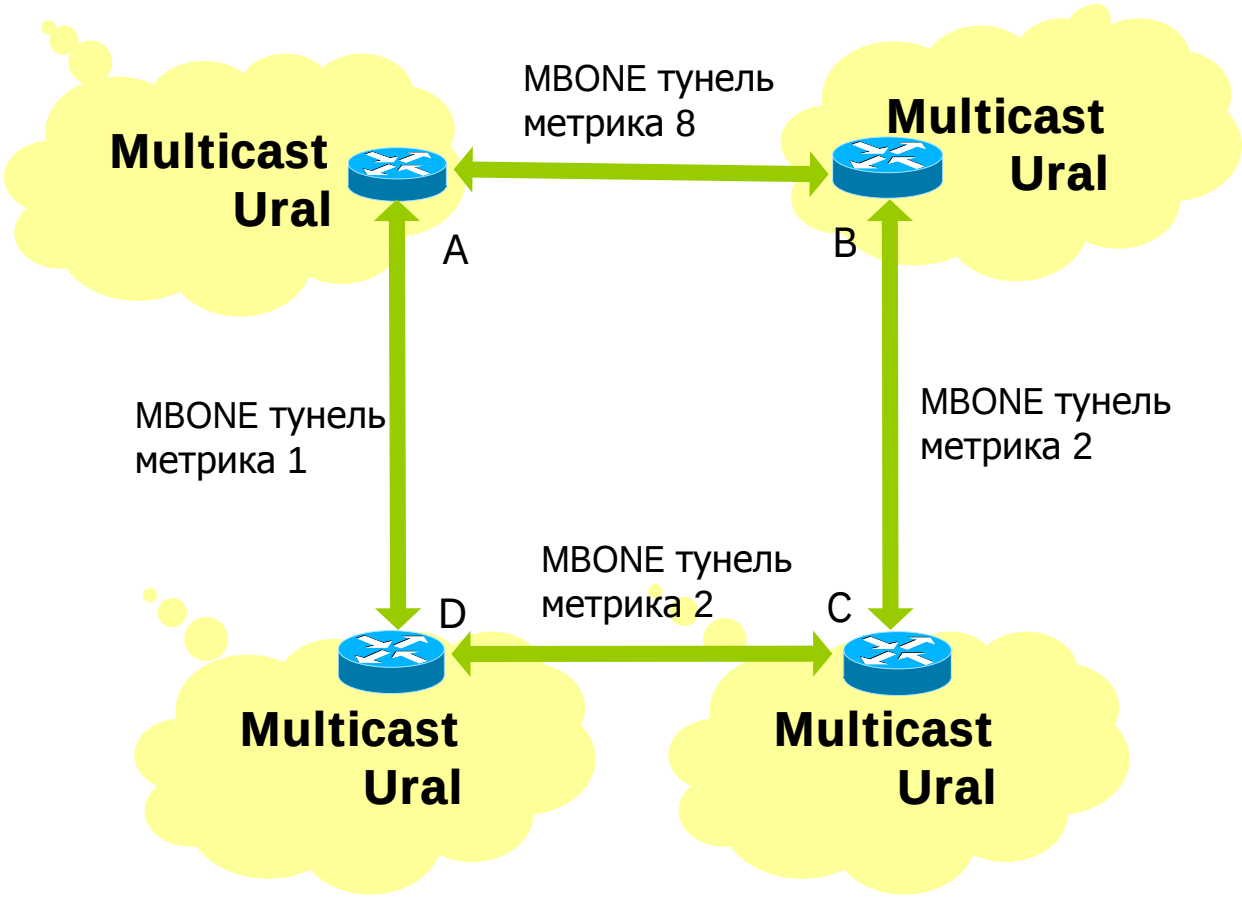


MBONE Маршрутизация (продолжение)

- **MBone туннели**
  - роутер в удалённом конце туннеля удаляет инкапсулированный заголовок и пересылает пакеты к принимающим устройствам
  - туннели связывают метрику с направлением передачи
    - ✓ параметр метрики используется как стоимость в multicast алгоритме маршрутизации
    - ✓ алгоритм маршрутизации использует значение метрики для выбора лучшего пути по сети (см. следующий слайд)
  - multicast пакеты посланные от роутера A к роутеру B не должны использовать непосредственно их соединяющий туннель
    - ✓ потому, что стоимость альтернативного пути, используемого маршрутизатором D и C равна 5 (1 + 2 + 2)
  - threshold параметры тоже ограничивают распространение multicast пакетов
  - устанавливается минимальный TTL для multicast пакета, пересылаемого по туннелю (TTL уменьшается на 1 каждым маршрутизатором)

MBONE метрика тунелей

A, B, C, D –Multicast роутеры



MBONE Будущее

- Большинство Интернет маршрутизаторов будет обеспечивать непосредственную поддержку для IP multicast
  - исключит потребность в multicast туннелях
  - текущая реализация MBone только временное решение
  - устареет, когда multicasting будет полностью поддерживаться в каждом Интернет маршрутизаторе

Содержание

- IP мультивещание
  - RFC 1112
  - IGMPv1, IGMPv2, IGMPv3
  - IGMP Snooping
- IP Multicast Маршрутизация
  - DVMRP
  - PIM-DM
  - PIM-SM
  - MOSPF
  - CBT
- MBone
- Multicast Приложения
- RTP/RTPC

Протокол CBT (RFC-2189)

- Протокол CBT (RFC-2189) реализует метод CBT так, как он ранее описан
- В протоколе CBT предусмотрена возможность взаимодействия с DVMRP

IP Multicast Приложения

Live TV and Radio Broadcast to the Desktop

Corporate Broadcasts

Distance Learning

Multicast File Transfer

Data and File Replication

Training

Video Conferencing

Video-On-Demand

Whiteboard/Collaboration

Real-Time Data Delivery - Financial

Session Information

- **SAP/SDP**
  - перед подключением к мультимедиа сессии, необходима информация о multicast адресе и порте этой сессии
  - кроме того ко времени, когда сессия станет активной, тип приложения должен быть известным
    - ✓ **Session Announcement Protocol SAP** - это протокол для объявления multicast конференций и сессий
      - SAP клиенты анонсируют их конференции и сессии периодически multicasting SAP пакетами, содержащими информацию о сессии
      - к соответствующему известному multicast адресу и порту
    - ✓ **Session Description Protocol SDP используется, чтобы шифровать информацию в сессии**
      - информация может быть произвольно зашифрована, чтобы избежать её прочтения неавторизованной стороной

Multicast Приложения

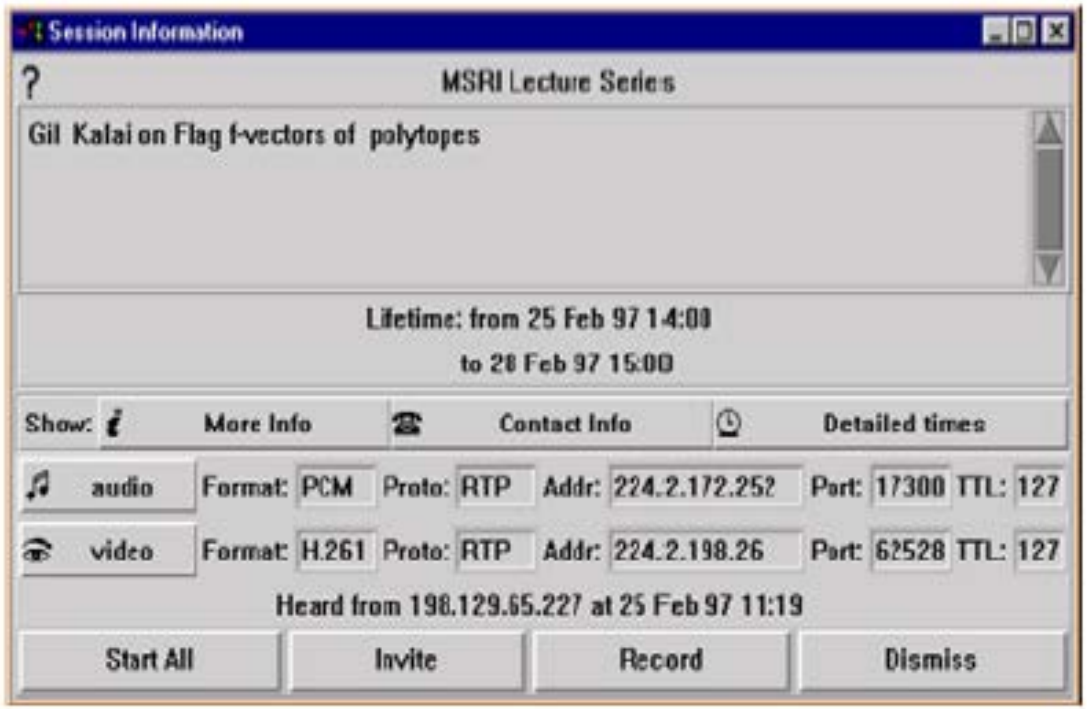
- **Могут быть поделены на 4 категории**
  - Мультимедиа конференции
  - Рассылка данных
  - Игры и моделирование
  - Мультивещание данных в реальном времени

Мультимедиа конференции

- Мультимедиа конференции
  - видео только одно из многих IP multicast приложений
  - многие средства были разработаны для работы по MBone
  - большинство широко используемых приложений для мультимедиа конференций являются MBone свободно распространяемыми приложениями
  - SDR (Session Directory Tool)
    - ✓ SDR слушает приходящие SAP пакеты
  - если есть активные multicast сессии в сети приложение шифрует информацию сессии, используя SDP
    - ✓ и показывает результаты на экране
  - теперь определённое приложение начинает использовать информацию о сессии
    - ✓ И мультимедиа конференция может начаться

Пример MBone Приложений (SDR)

Multicast Сессии



Приложение может начать использовать информацию сессии

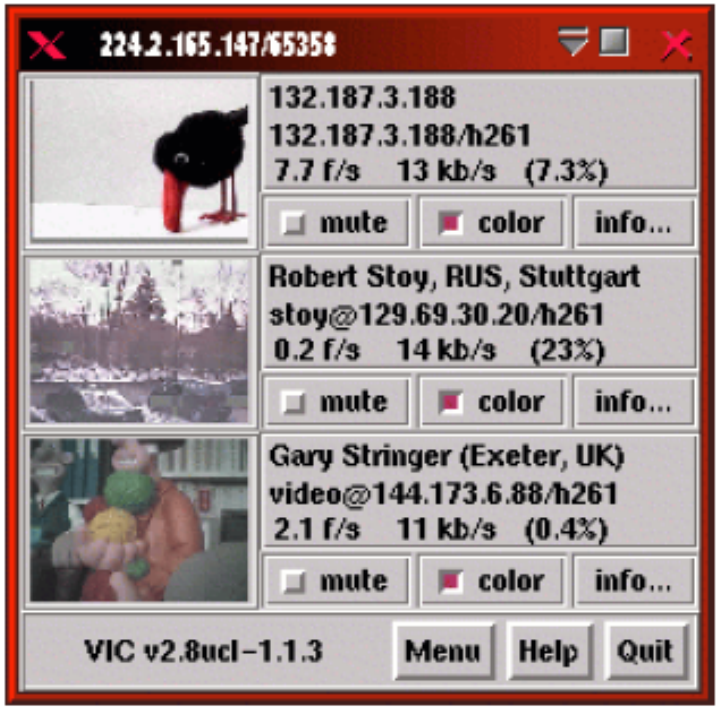
Мультимедиа конференции 2

- Мультимедиа конференции (продолжение)
  - VAT (MBone Multimedia Audio Tool)
  - VIC (MBone Multimedia Video Tool)
  - многие-ко-многим только аудио или аудио-видео связь
  - WB (Shared Whiteboard Tool)
  - электронная whiteboard, которую участники multicast сессии могут разделять
  - в отличие от аудио/видео используется надёжный multicast протокол
  - иначе участники не смогут увидеть те же самые вещи на их whiteboards
  - время повторной передачи потерянных аудио/видео пакетов было бы тоже большим

Пример MBone Приложений (VAT, VIC)

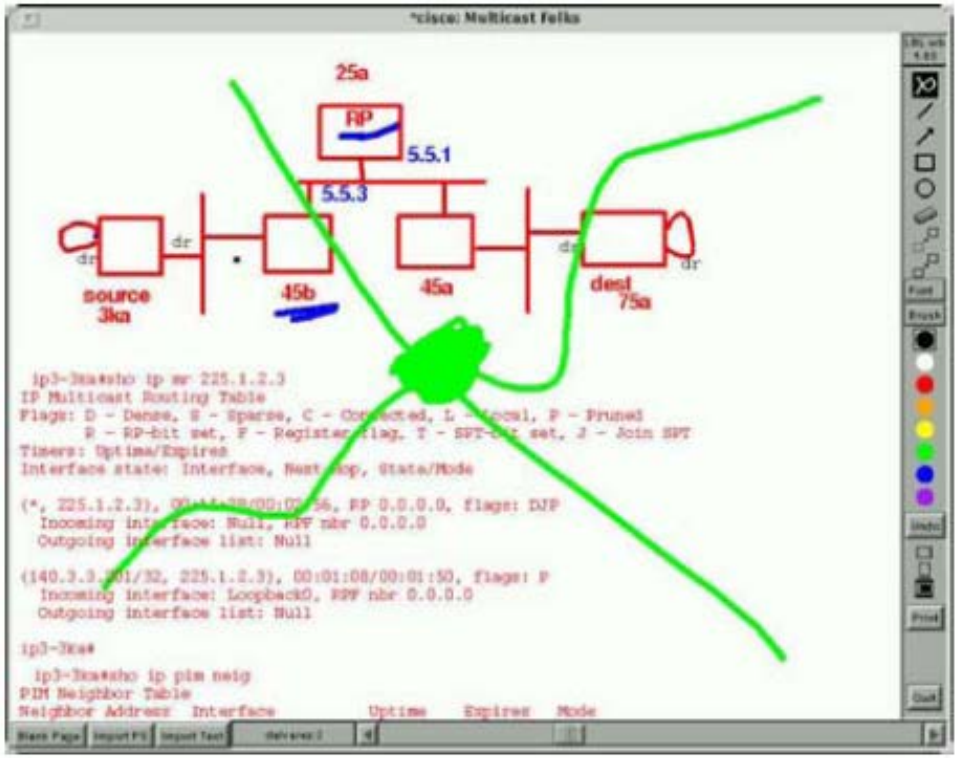
VAT:

VIC:



MBone средства есть тут: http://www-mice.cs.ucl.ac.uk/multimedia/software

Пример MBone Приложений (wb)



MBone средства есть тут: http://www-mice.cs.ucl.ac.uk/multimedia/software

Мультимедиа конференции 2

- **Мультимедиа конференции (продолжение)**
  - Существуют и коммерческие продукты
  - Активное использование приводит к большему потреблению пропускной способности
  - Только аудио конференция в паре с whiteboard приложением будет крайне мощной формой мультимедиа конференции, которая не потребляет много пропускной способности

Рассылка данных

- **Рассылка данных**
  - Дублирование данных другой multicast зоны становится очень популярным
  - MFTP (multicast форма ftp, “NAK только” протокол)
  - один или более файлов могут быть посланы одновременно с ftp группе узлов в сети, используя IP multicasting
  - например, центральный сайт может эффективно поместить обновлённые файлы данных в каждый областной офис

Игры и Моделирование

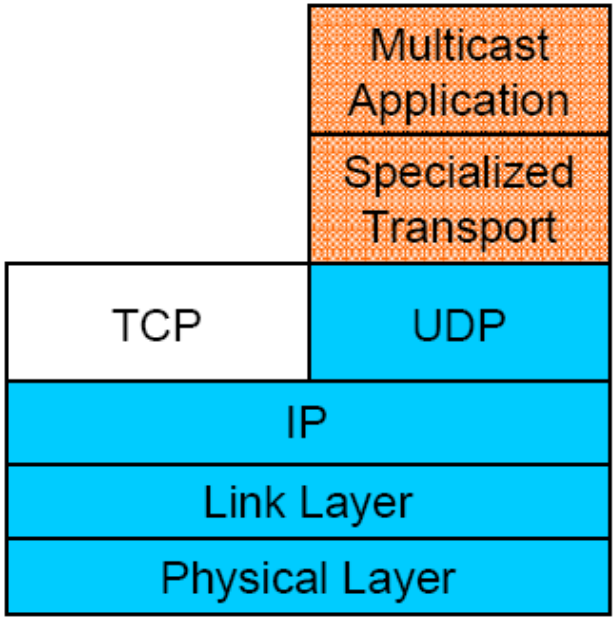
- **Игры и Моделированные**
  - приложения уже доступны
  - интеграция multicast сервисов позволяет приложениям масштабироваться к большому кол-ву пользователей
  - multicast группы могут представлять различные разделы игр и моделирования
  - все пользователи перемещаются от одного раздела к другому, они выходят и присоединяются к различным multicast группам

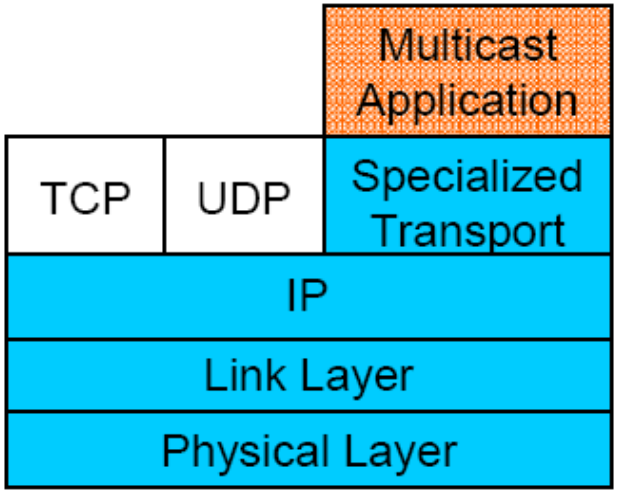
Мультивещание данных в реальном времени

- **Мультивещание данных в реальном времени**
  - приложения распространяют данные большому кол-ву пользователей в реальном времени
  - например, информация биржевого аппарата может быть доставлена рабочим станциям на торговый этаж
  - нужны специальные протоколы и приложения потому , что информация критична ко времени

Работа под UDP или IP

- Multicast приложения должны выполняться под UDP (например RTP;левая картинка) или непосредственно интерфейс IP, обеспечивающий их собственный транспортный слой (правая картинка)





Real-time Приложения основанные на RTP/RTPC

- **В дополнение к упомянутым MBone приложениям есть ещё другие, использующие RTP/RTCP**
  - Quick Time (Apple)
    - ✓ обеспечивает цифровое видео и медиа поток
  - Real Audio and Real Video (RealNetworks)
    - ✓ высококачественное аудио и видео поток
  - NetMeeting (Microsoft)
    - ✓ обеспечивает IP телефонию, white boarding, текстовые чаты и приложения и совместное использование файлов
  - CU-seeMe (CUseeMe Networks)
    - ✓ Программное обеспечение Интернет видео чат с поддержкойвидео, аудио, текста и whiteboard связи
  - IP/TV (Cisco Systems)
    - ✓ Живое видео, назначенное видео и видео по расписанию

Содержание

- IP мультивещание
  - RFC 1112
  - IGMPv1, IGMPv2, IGMPv3
  - IGMP Snooping
- IP Multicast Маршрутизация
  - DVMRP
  - PIM-DM
  - PIM-SM
  - MOSPF
- MBone
- Multicast Приложения
- RTP/RTPC

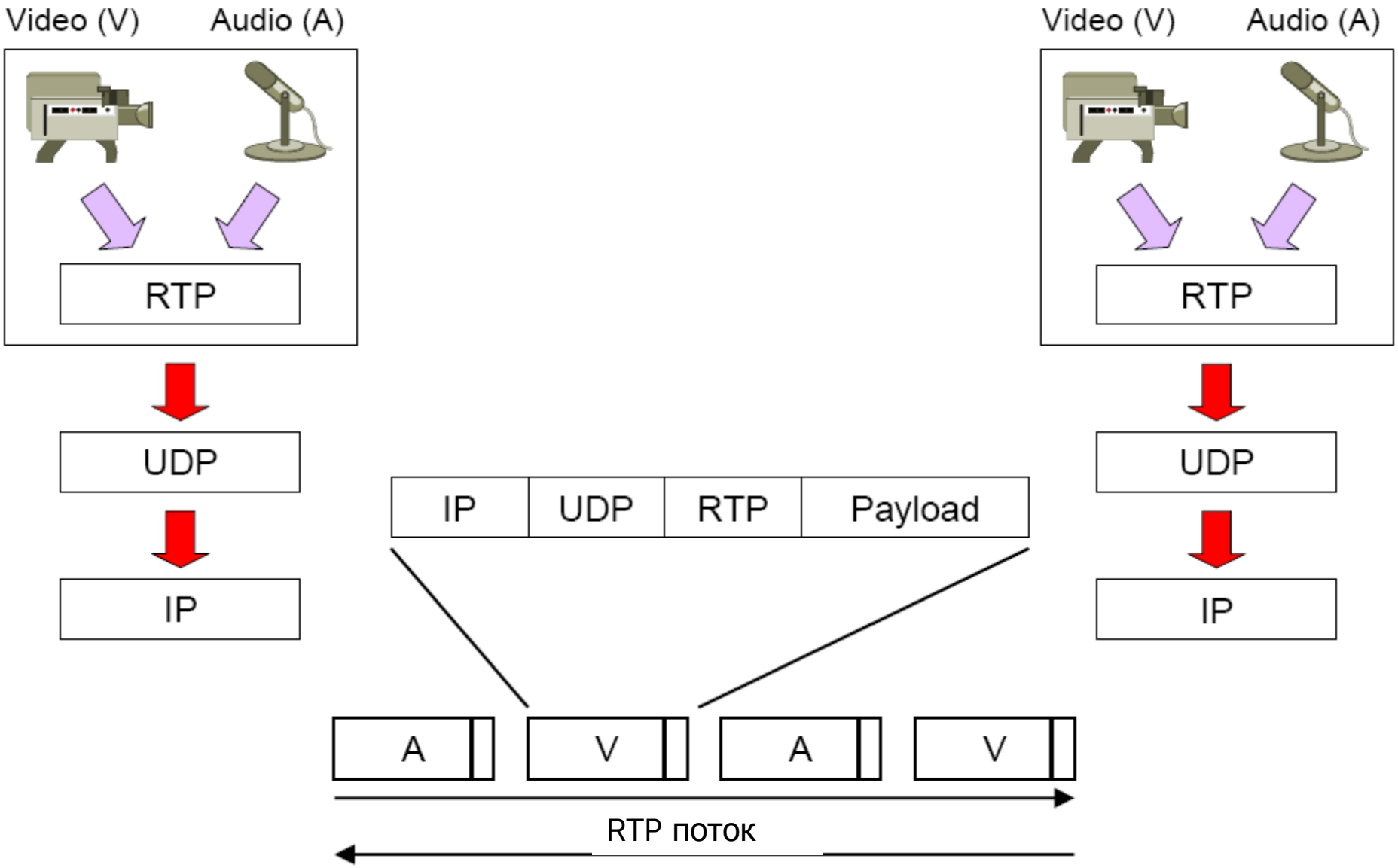
RTP и RTCP

- Чтобы использовать real-time сервисы в приложении, должны использоваться два протокола
  - Real-Time Transport Protocol (RTP) обеспечивающий транспортировку real-time пакетов данных
    - ✓ unicast и multicast передачи
    - ✓ чтобы, адаптировать новые real-time приложения, архитектуру преднамеренно оставляли неполной
    - ✓ позволяет легко адаптировать протокол к новым аудио и видео стандартам
  - RTP Control Protocol (RTCP) контролирует качество сервиса, обеспечивающегося в текущих RTP сессиях

RTP и RTCP

- **RTP**
  - осуществляет транспортные задачи должен, обеспечивает синхронизацию мультимедиа потоков данных
    - ✓ RTP может использоваться, чтобы отметить пакеты, связанные с индивидуальными видео и аудио потоками
    - ✓ позволяет потокам быть синхронными в принимающем хосте
    - ✓ следующий слайд показывает работу RTP в мультимедиа передаче
    - ✓ аудио и видео данные инкапсулируются в RTP пакеты,
    - ✓ если мультимедиа приложение не использует RTP сервисы Приёмник не сможет связать соответствующие аудио и видео пакеты
    - ✓ из-за перегрузки или изменяющихся условий работы в сети

RTP


Video (V)
Audio (A)
RTP
UDP
IP
Video (V)
Audio (A)
RTP
UDP
IP
IP
UDP
RTP
Payload
A
V
A
V
RTP поток

RTP и RTCP

- **RTP (продолжение)**
  - из-за проблем производительности RTP, многие функции не были включены
  - RTP протокол не содержит никаких механизмов, гарантирующих доставку или качества сервисных функций
  - стандарт не подтверждает доставку пакета в очереди предполагая, что сети надёжна и доставка пакетов идёт последовательно
  - не предотвращается возможность сетевой перегрузки
  - проектировщики приложений должны определить, являются ли эти сервисы приемлемыми

RTP Формат заголовка

первые 12 байт присутствуют в каждом RTP пакете

- V: версия RTP
- P: Заполнитель
  - ✓ Если P=1, пакет содержит один или более дополнительных октетов-заполнителей в конце поля данных (заполнители не являются частью поля данных). Последний октет заполнителя содержит число октетов, которые должны игнорироваться
  - ✓ Заполнитель нужен при использовании некоторых алгоритмов шифрования при фиксированном размере блоков или при укладке нескольких RTP-пакетов в один UDP
- X: Расширение
  - ✓ Если X=1, одно расширение заголовка следует за фиксированным заголовком
- CSRC count: число CSRC: 4 бита = $(0001 – 1111)_2 = (1 – 15)_{10}$
  - ✓ содержит количество csrc-идентификаторов, которые записаны в пакете.

RTP Формат заголовка

- M: маркер
  - ✓ позволяет существенным событиям быть отмеченными в потоке пакетов (frame boundaries)
    - ➢ Например, выделять в потоке пакетов существенные события, такие как границы кадра
  - ✓ Интерпретация маркера определяется профайлом.
    - ➢ Профайл может определить дополнительные маркерные биты или специфицировать отсутствие маркерных битов путем изменения числа битов в поле PT.

RTP Формат заголовка

- **поле** SSRC (**Synchronization Source**) - **Идентификатор Источника синхронизации** : все пакеты в потоке от одного источника содержат одинаковый SSRC идентификатор
  - ✓ Это допускает получателя к группе пакетов для воспроизведения.
- **Что такое Источник синхронизации (SSRC):**
  - ✓ Источник потока RTP-пакетов, определяется 32-битным числовым SSRC-идентификатором, который записывается в заголовок RTP-пакета и не зависит от сетевого адреса.
  - ✓ Все пакеты от источника синхронизации нумеруются и выполняется временная привязка. Эти данные используются принимающей стороной при воспроизведении.
  - ✓ Источниками синхронизации могут служить источники первичного сигнала (микрофоны или видеокамеры), а также RTP-смесители.

RTP Формат заголовка

- SSRC-идентификатор представляет собой случайное число, которое является уникальным для данной RTP-сессии.
- Участник сессии не должен использовать один и тот же SSRC-идентификатор для всех RTP-сессий мультимедийного набора.
- Если участник формирует несколько потоков в рамках одной RTP-сессии (например, от нескольких видеокамер), каждый участник должен быть снабжен уникальным SSRC-идентификатором.

RTP Формат заголовка

- **CSRC идентификаторы:** Содержит список источников для загрузки в текущий пакет. Это поле используется, когда микшер объединяет различные потоки пакетов. (см. далее в этой главе)
- **Что такое «Информационный источник CSRC (contributing source)»:** Источник потока RTP-пакетов, который вносит вклад в общий поток, формируемый RTP-смесителем/микшером. Смеситель вставляет список SSRC-идентификаторов, которые идентифицируют парциальные источники, в заголовок RTP-пакетов. Этот список называется CSRC-списком.
- Примером приложения может быть аудио-конференция, где смеситель отмечает всех говорящих, чей голос порождает исходящие пакеты. Это позволяет принимающей стороне идентифицировать говорящего, хотя все пакеты имеют один и тот же SSRC-идентификатор.

RTP Формат заголовка

- **RTP сервисы протокола**
  - ✓ RTP обеспечивает “end to end” транспортные услуги для приложений, передающих real-time данные
  - ✓ включены в RTP заголовок
- **PT (Payload Type) Идентификация типа полезной загрузки: 7 бит**
  - ✓ RTP может задержать части аудио или видео потоков
  - ✓ чтобы различать эти потоки, отправка приложения включает payload type identifier в RTP заголовке
  - ✓ идентификатор показывает, что для создания payload, использовалась специальная схема кодирования
  - ✓ принимающее приложение использует этот идентификатор, чтобы определить соответствующий алгоритм декодирования
- идентифицирует формат поля данных RTP-пакета и определяет интерпретацию его приложением. Могут быть определены дополнительные коды типа данных. Исходный набор кодов по умолчанию для аудио и видео задан в профайле Internet-draft draft-ietf-avt-profile, и может быть расширен в следующих редакциях стандарта assigned numbers (RFC-1700) [5].

RTP Формат заголовка

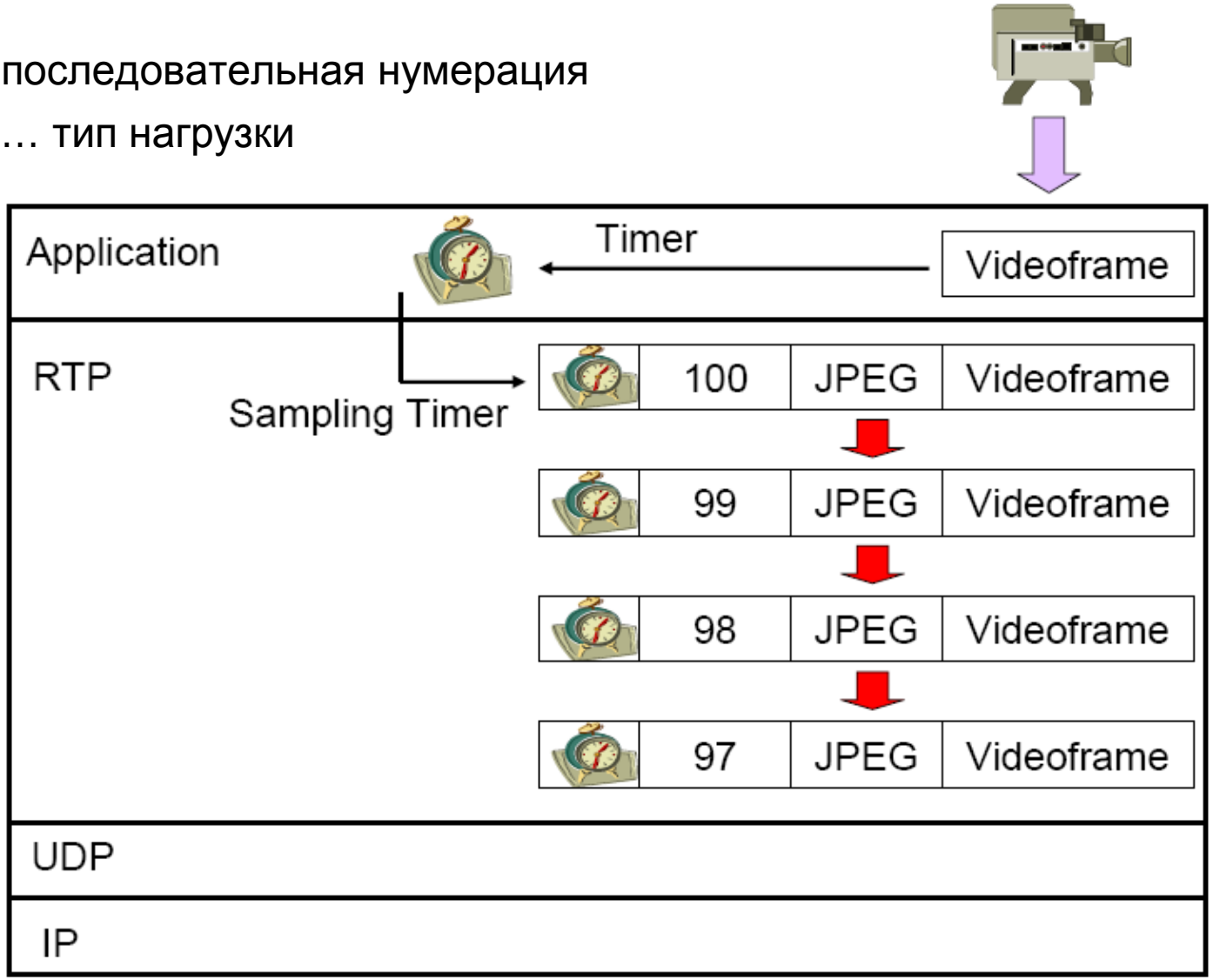
- RTP сервисы протокола (продолжение)
  - Последовательная нумерация (Sequence Number)
    - ✓ используются принимающим RTP хостом для восстановления исходного порядка передаваемых пакетов
    - ✓ получатель может обнаружить потерю пакета, используя информацию в этом поле
    - ✓ начальное значение кода является случайным. Алгоритм генерации таких кодов рассмотрен в [6].
  - Временная метка (Timestamping)
    - ✓ временные метки используются в RTP, чтобы синхронизировать пакеты от различных источников
    - ✓ timestamp представляет выборку (создание) времени первого октета в RTP пакете данных
    - ✓ возможно, что несколько RTP пакетов могут иметь одинаковые временные метки
    - ✓ например это может случиться, когда один видео кадр передаётся в множестве RTP пакетов

RTP Формат заголовка

- Временная метка (Timestamping) - продолжение
  - ✓ Временная метка соответствует времени стробирования для первого октета в информационном RTP-пакете.
  - ✓ Время стробирования должно быть получено от часов, показания которых увеличиваются монотонно и линейно, чтобы обеспечить синхронизацию и вычисление временного разброса.
  - ✓ Разрешающая способность часов должна быть достаточной для обеспечения приемлемой точности синхронизации (одного тика на видео кадр обычно не достаточно).
  - ✓ Частота часов зависит от формата данных и задается статически в профайле, в спецификации поля данных, или динамически средствами, выходящими за пределы спецификации протокола RTP.
  - ✓ Если RTP-пакеты генерируются периодически, используется временная привязка, определенная задающим генератором стробирования, а не показаниями системных часов.
  - ✓ Начальное значение временной метки является случайным. Несколько последовательных RTP-пакетов могут иметь идентичные временные метки, если логически они генерируются одновременно (например, относятся к и тому же видео кадру).

RTP Timestamping

- 100…последовательная нумерация
- JPEG… тип нагрузки



RTP и RTCP

- RTCP
  - чтобы управлять real-time доставкой, многие приложения требуют обратной связи о текущем быстродействии сети
    - ✓ первичная функция RTCP, обеспечить обратную связь о качестве RTP рассылки данных
    - ✓ RTCP основан на периодической передаче управляющих пакетов всем участникам в сессии
    - ✓ RTCP использует UDP соединение для связи
    - ✓ отделяются от UDP соединения, используя RTP протокол
  - RTCP архитектура определяет пять типов управляющей информации, использующейся, чтобы определить текущее быстродействие

RTP и RTCP

- Типы RTCP управляющей информации (прод.)
  - Сообщение отправителя:
    - ✓ отправляется источником RTP потока данных (в интервалах)
    - ✓ обеспечивает статистики передачи и приёма, наблюдаемую отправителем
    - ✓ посылается как multicast пакет, обрабатываемый всеми участниками RTP сессии
  - Сообщение получателя:
    - ✓ обеспечивают статистику приёма для участников, не являющихся активными отправителями
    - ✓ выпускаются если вышло временя и нет потоков данных
  - Сообщение описание источника:
    - ✓ используется RTP отправителем, чтобы обеспечить local capability информацией

RTP Трансляторы и Микшеры

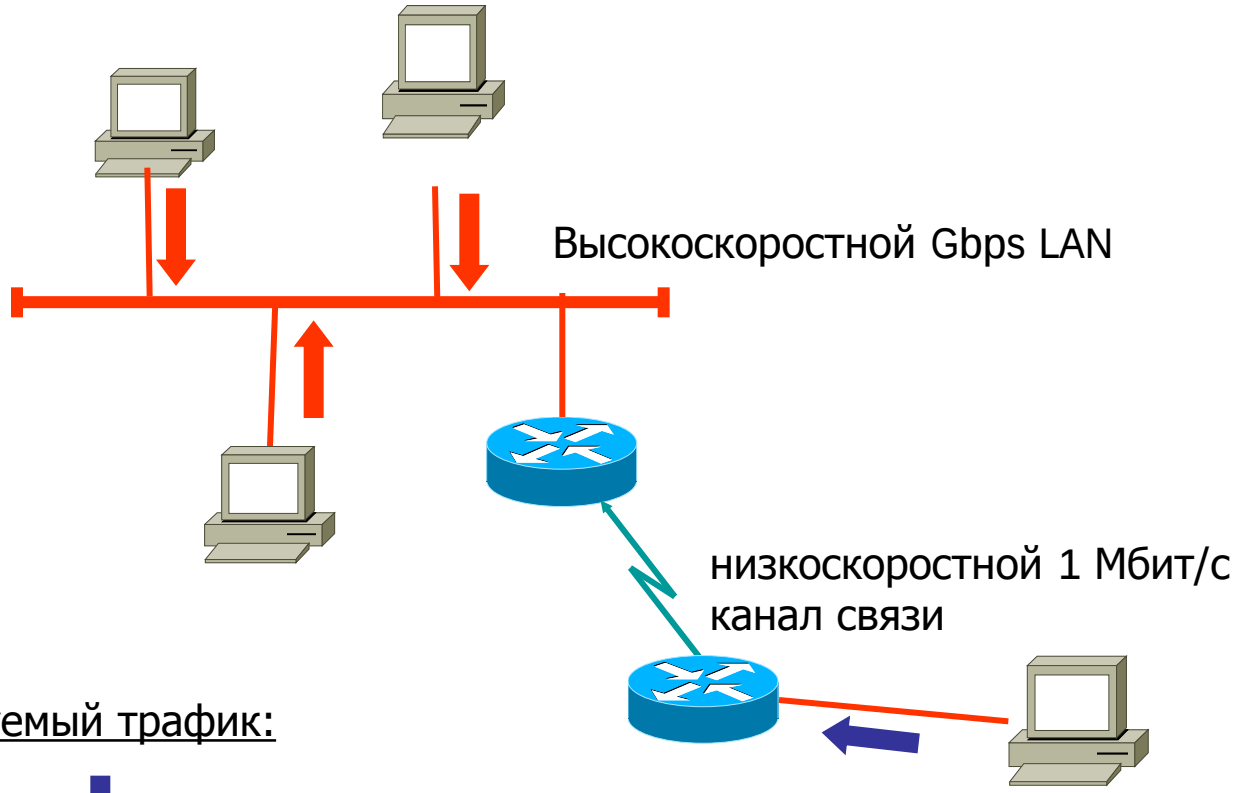
- **RTP протокол поддерживает использование трансляторов и микшеров, чтобы изменять поток RTP пакетов**
  - эти устройства используются, когда некоторым получателям мультимедиа сессии, необходимо получать данные в различных форматах
- **RTP трансляторы**
  - используются, чтобы изменить тип данных в RTP пакете
  - в примере, три videoconferencing рабочих станции обмениваются MPEG трафиком по high-speed LAN
  - каждая рабочая станция генерирует MPEG данные (1.5 Мбит/с)
  - другая станция связанная по низкоскоростному последовательному подключению хочет участвовать в видеоконференции

RTP Трансляторы и Микшеры

- **RTP транслятор (продолжение)**
  - полосы пропускания этих соединений не достаточно, чтобы поддерживать видео потоки
  - одно из решений этой проблемы, замена видео формата всех рабочих станций на формат, использующий меньший трафик (например, H.261 с 256 Kbps)
  - но уменьшение бит-рейта, ведёт к снижению качества видео
  - альтернативное решение - RTP устройства трансляции
  - Каждый индивидуальный MPEG видео поток конвертируется в H.261 видео поток с 256 Kbps, который может пересылаться через последовательную линию
  - три LAN прикреплённые станции продолжают использовать более качественный MPEG формат

Видеоконференция без трансляции

Видеоконференция с 4 станциями
(только связь LAN -> последовательная линия)

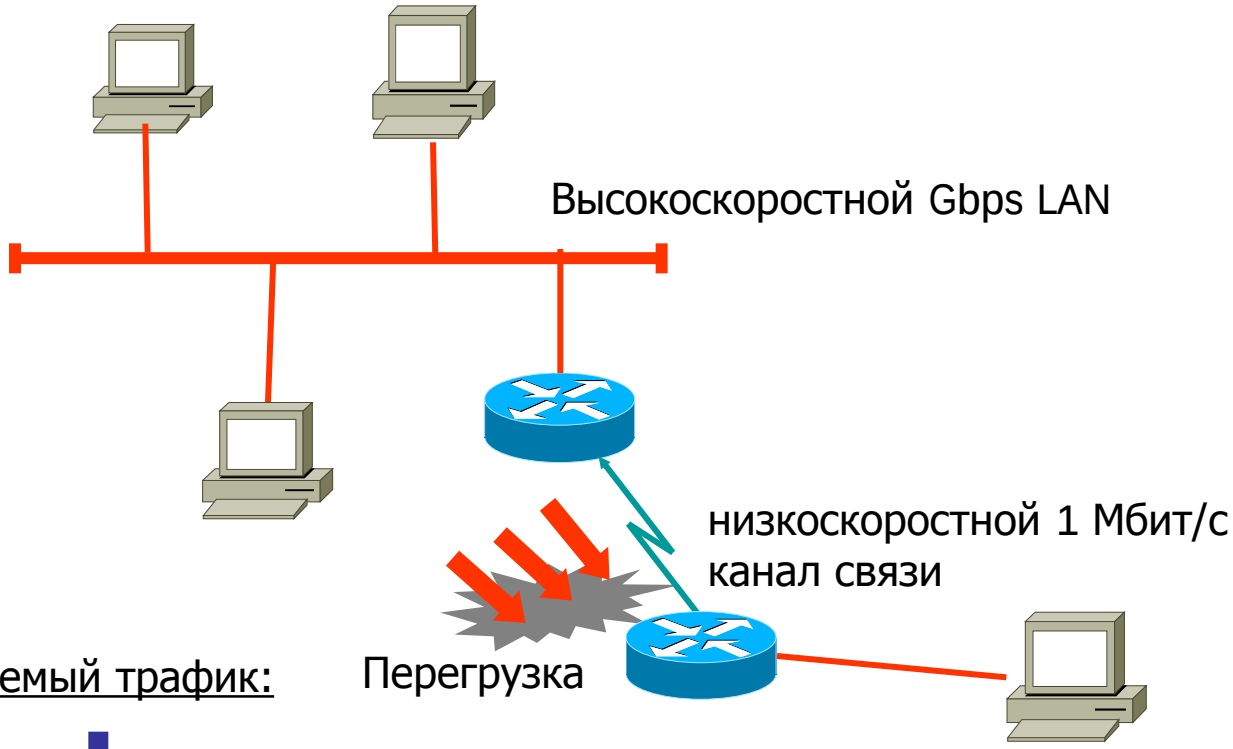


Генерируемый трафик:

… 1,5 Мбит/с … 256Кбит/с

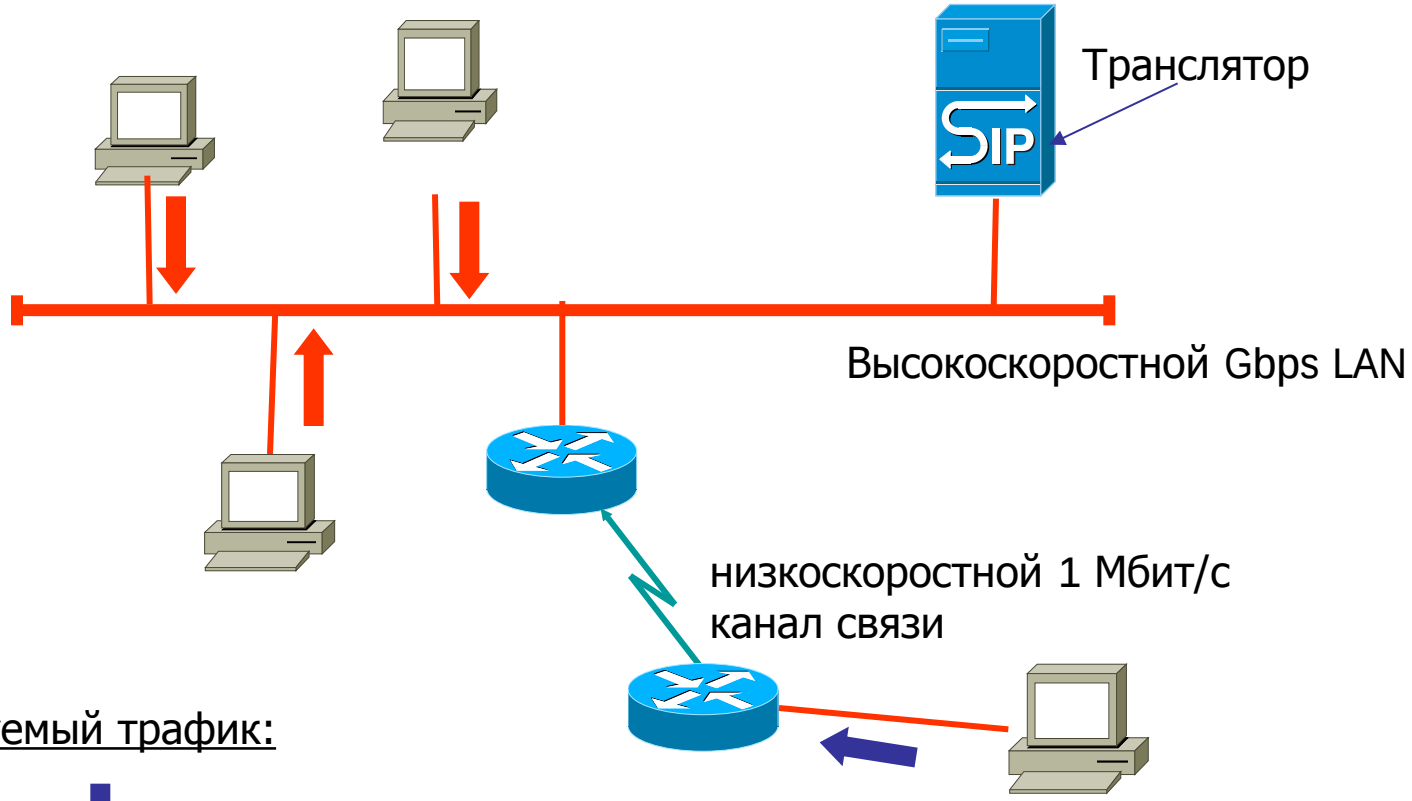
Видеоконференция без трансляции

Видеоконференция с 4 станциями
(только связь LAN -> последовательная линия)



Видеоконференция с TTP трансляцией

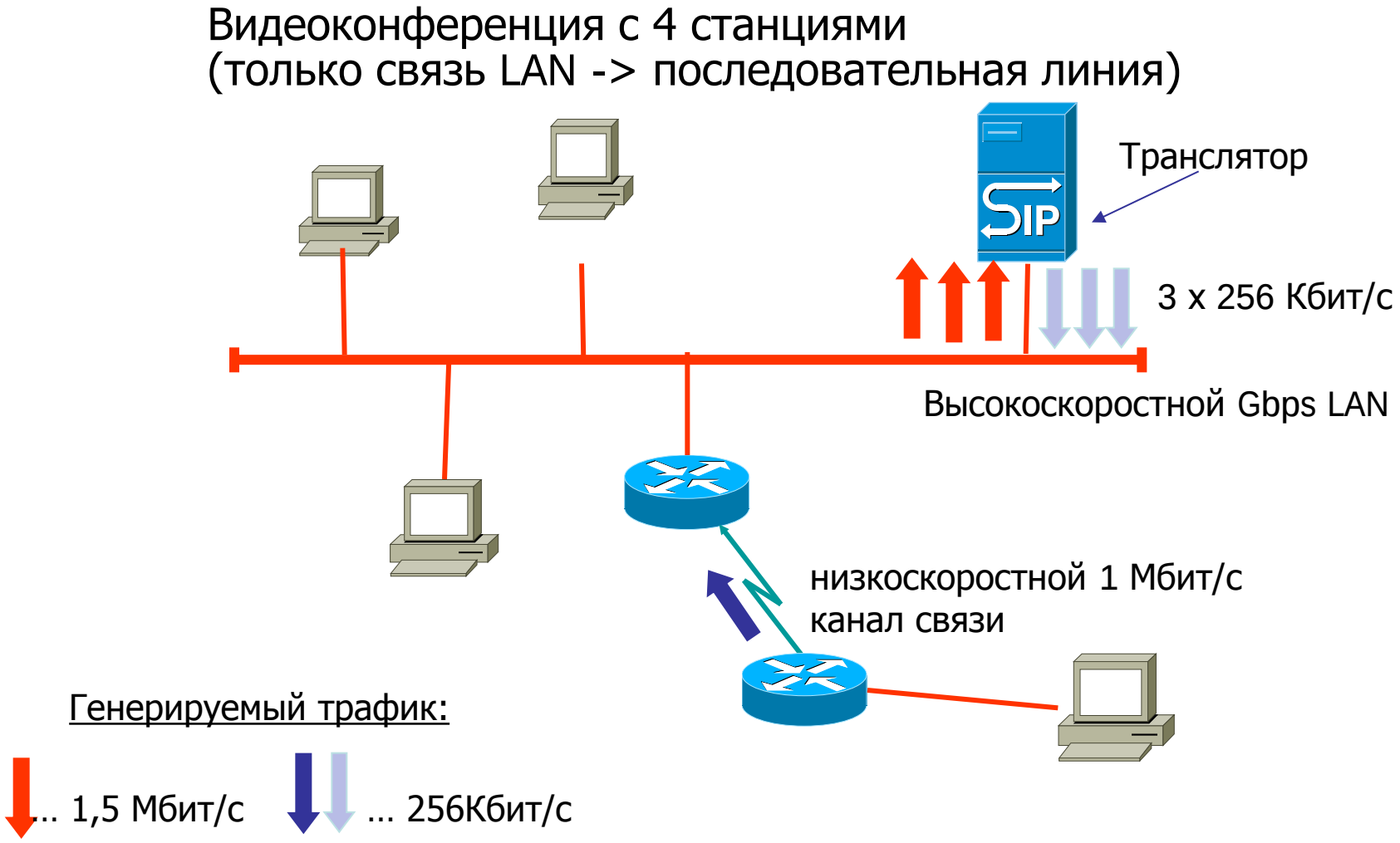
Видеоконференция с 4 станциями
(только связь LAN -> последовательная линия)



Генерируемый трафик:

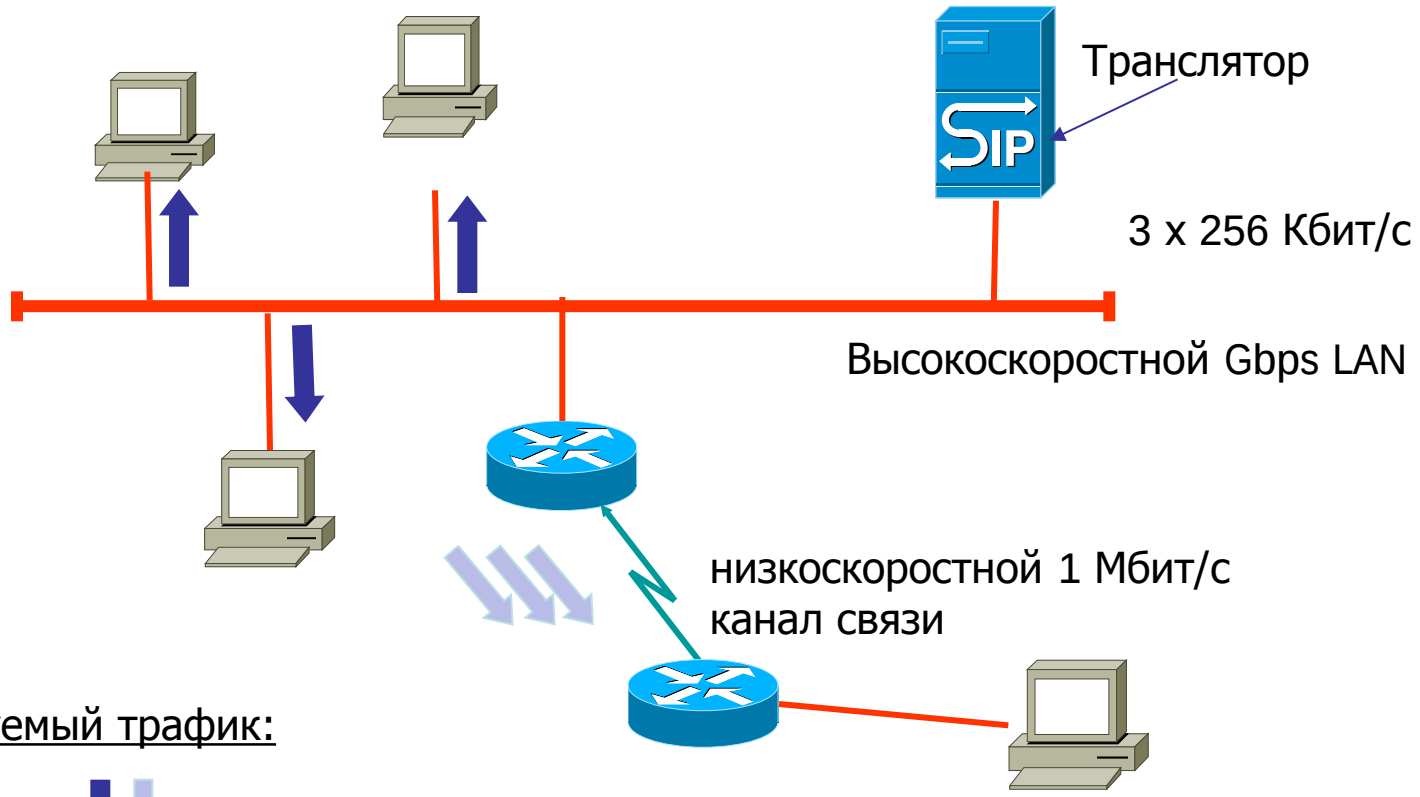
... 1,5 Мбит/с ... 256Кбит/с

Видеоконференция с TTP трансляцией



Видеоконференция с RTP трансляцией

Видеоконференция с 4 станциями
(только связь LAN -> последовательная линия)



RTP Трансляторы и Микшеры

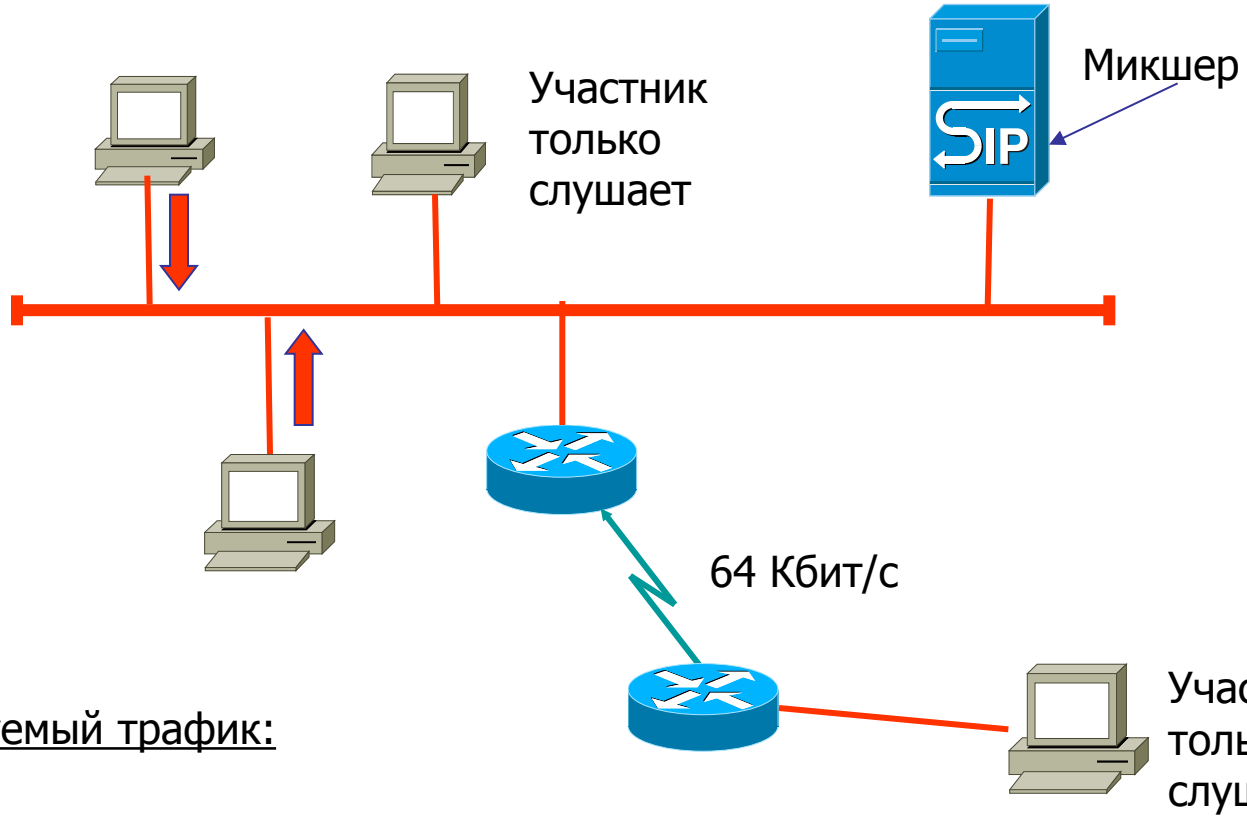
- **RTP трансляторы (продолжение)**
  - RTP трансляторы используются в брандмауэрах, которые не передают multicast пакетов
  - два транслятора на каждой стороне брандмауэра
  - один для безопасного туннелирования multicast пакета
  - второй передаёт информацию как multicast пакеты
- **RTP микшеры**
  - RTP микшеры используются, чтобы комбинировать несколько потоков данных в один RTP поток
  - эти устройства используют, чтобы поддерживать аудио передачу приложений, где одновременно только один или два спикера

RTP Трансляторы и Микшеры

- **RTP микшеры (продолжение)**
  - RTP микширование не используется в среде видео приложений
  - в примере, две audio conferencing станции производит PCM аудио потоки с бит-рейтом 64 Kbps
  - другие рабочие станции по низкоскоростным последовательным соединениям участвуют в видеоконференциях
  - пропускная способность этого подключения не достаточная, чтобы поддерживать 192 Kbps
  - RTP микшер объединяет два потока отправителя в один 64 Kbps поток
  - это позволяет новой станции присоединяться к конференции

RTP Микширование с 2 спикерами

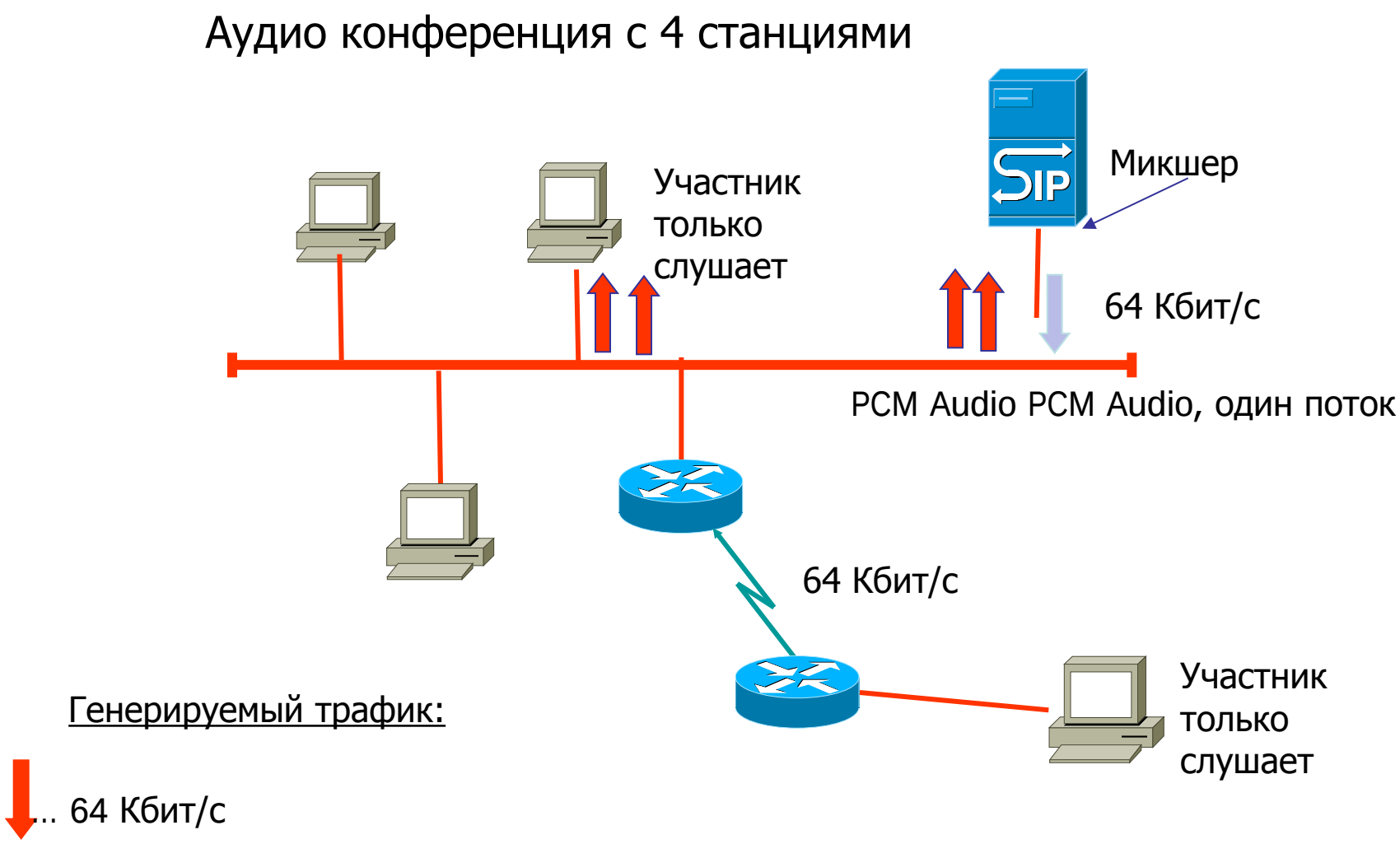
Аудио конференция с 4 станциями



Генерируемый трафик:

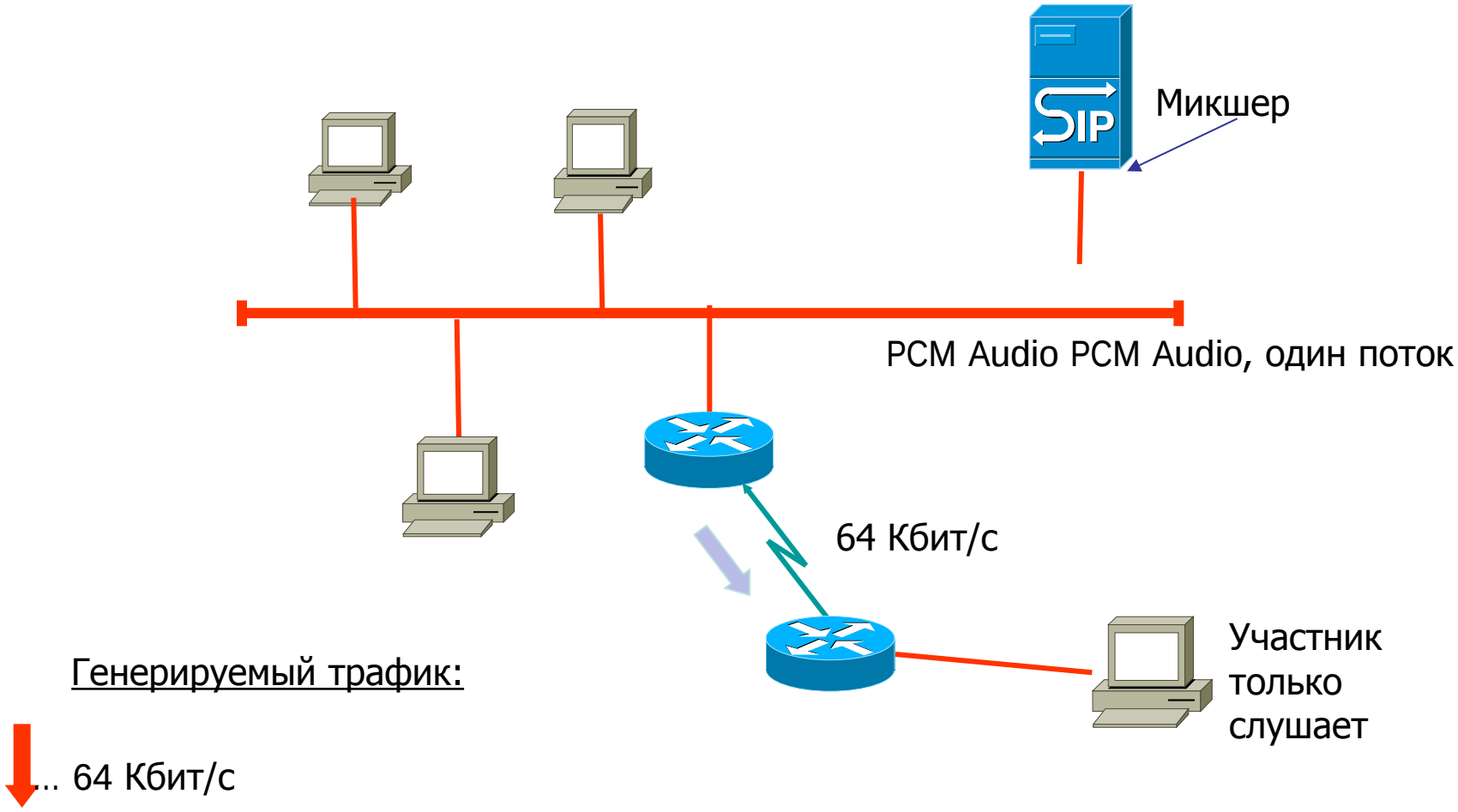
… 64 Кбит/с

RTP Микширование с 2 спикерами



RTP Микширование с 2 спикерами

Аудио конференция с 4 станциями



RTP Трансляторы и Микшеры

- **RTP микшеры (продожение)**
  - payload тип входящих и выходящих пакетов остаётся тем же
  - возможно сочетать RTP микширование и RTP трансляцию в одной среде
  - это может потребоваться если станция соединяется по низкоскоростному соединению
  - payload формат PCM потока, может быть изменён до более низкой пропускной способности

Источники

- http://abc.vvsu.ru/Books/ebooks_iskt/%DD%EB%E5%EA%F2%F0%EE%ED%ED%FB%E5%F3%F7%E5%E1%ED%E8%EA%E8/%D2%E5%EB%E5%EA%EE%EC%EC%F3%ED%E8%EA%E0%F6%E8%EE%ED%ED%FB%E5%20%F2%E5%F5%ED%EE%EB%EE%E3%E8%E8/Index/mcast.html
- **Протокол мультикастинг-маршрутизации DVMRP** http://book.itep.ru/4/4/mcst_21.html
- **Обзор IP-мультикастинга в среде многопротокольной коммутации по меткам (MPLS)** http://book.itep.ru/4/4/mcst_21.html
- **Путеводный вектор и другие (Кульгин)** http://sol.te.net.ua/www/routing/7/
- http://xgu.ru/wiki/IP_Multicast
- http://xgu.ru/wiki/PIM