Лекция XIII. Уровень сетевых интерфейсов (Канальный уровень)

Курс читает Рогозин Н.О., кафедра ИУ-7

Введение

- В то время как сетевой уровень обеспечивает взаимодействие между хостами, канальный отвечает за процесс прохождения пакетов по отдельным каналам
- Передаваемое канальным уровнем сообщение называется кадром (frame)
- Одна из основных задач – определить, где начинается и заканчивается кадр в потоке данных
- Канальный уровень делится на MAC, реализуемый аппаратно, и LLC, реализуемый программно

Коммутация в локальной сети

- Коммутаторы локальной сети работают на канальном уровне и не различают сетевых адресов, не используют алгоритмы маршрутизации
- Для перенаправления пакетов в сети коммутаторов используются не сетевые адреса, а адреса канального уровня
- Существование двух уровней адресации (сетевой и канальный уровень) является необходимым

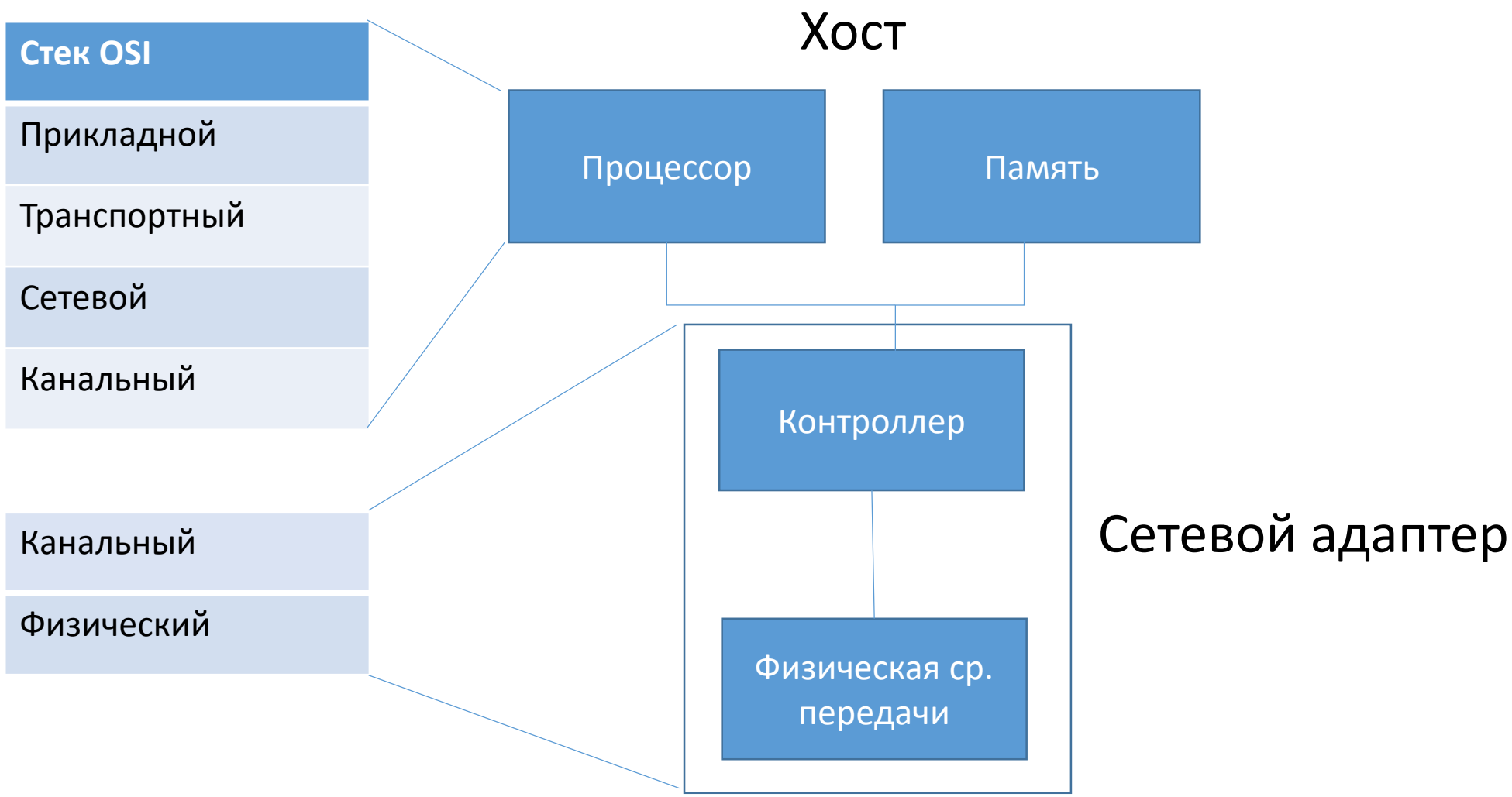
Типы каналов

- Два принципиально разных типа каналов: широковещательные и обычные двухточечные линии связи
- Двухточечная линия связи соединяет отправителя на одном конце линии и получателя на другом.
- Для двухточечных линий связи разработано множество протоколов канального уровня.
  - PPP (Point-to-Point Protocol — протокол передачи от точки к точке) и
  - HDLC (High-level DataLink Control) — высокоуровневый протокол управления каналом).
- Широковещательный канал может иметь несколько передающих и принимающих узлов, присоединенных к одному и тому же совместно используемому широковещательному каналу.
  - Ethernet, беспроводные локальные сети

Коммутатор

- Устройство, предназначенное для соединения нескольких узлов компьютерной сети в пределах одного или нескольких сегментов сети.
- Разработаны с использованием мостовых технологий и часто рассматриваются как многопортовые мосты.
- В отличие от концентратора, который распространяет трафик от одного подключённого устройства ко всем остальным, коммутатор передаёт данные только непосредственно получателю (исключение составляет широковещательный трафик всем узлам сети и трафик для устройств, для которых неизвестен исходящий порт коммутатора).

Функционал сетевого адаптера в стеке OSI



Принцип работы

- В памяти хранится таблица коммутации, в которой указывается соответствие MAC-адреса узла порту **коммутатора**. При включении коммутатора эта таблица пуста, и он работает в режиме обучения. В этом режиме поступающие на какой-либо порт данные передаются на все остальные порты коммутатора. При этом коммутатор анализирует фреймы (кадры) и, определив MAC-адрес хоста-отправителя, заносит его в таблицу на некоторое время.
- Впоследствии, если на один из портов коммутатора поступит кадр, предназначенный для хоста, MAC-адрес которого уже есть в таблице, то этот кадр будет передан только через порт, указанный в таблице.
- Если MAC-адрес хоста-получателя не ассоциирован с каким-либо портом коммутатора, то кадр будет отправлен на все порты, за исключением того порта, с которого он был получен. Со временем коммутатор строит таблицу для всех активных MAC-адресов, в результате трафик локализуется.

Виды кадров

- Информационные, содержащие данные конечных пользователей, (они формируются в компьютерах)
- Служебные, источником которых может быть любое устройство, использующее канальный уровень. Формируются, например, мостами для реализации алгоритма покрывающего дерева, маршрутизаторами при обмене маршрутной информацией, компьютерами при объявлении выполняемых ими сервисов.

Функции коммутатора

- **Формирование кадра** - включает размещение данных, поступивших с верхнего уровня, в поле данных кадра, а также формирование заголовка, то есть определение и занесение в соответствующие поля кадра контрольной суммы, MAC-адресов отправителя и получателя, отметки о типе протокола верхнего уровня, пакет которого упакован в поле данных кадра, и возможно некоторой другой информации.

Функции коммутатора

- **Анализ заголовка кадра** и **обработка кадра** на основании результатов проведенного анализа могут заключаться, например, в уничтожении кадра при несовпадении контрольной суммы, в принятии решения о передаче кадра в сеть при несовпадении адреса назначения с адресом данного узла и т.п.
- **Прием кадра из сети** и **отправка кадра в сеть** прежде всего связаны с получением доступа к передающей среде, эта процедура единообразным образом выполняется всеми устройствами сети, построенной с использованием общей базовой сетевой технологии. Как правило, принимаемые кадры помещаются в буфер, а при отправке - выбираются из буфера.

Режимы коммутации

- **С промежуточным хранением (Store and Forward).** Коммутатор читает всю информацию в кадре, проверяет его на отсутствие ошибок, выбирает порт коммутации и после этого посылает в него кадр.
- **Сквозной (cut-through).** Коммутатор считывает в кадре только адрес назначения и после выполняет коммутацию. Этот режим уменьшает задержки при передаче, но в нём нет метода обнаружения ошибок.
- **Бесфрагментный (fragment-free)** или ***гибридный***. Этот режим является модификацией сквозного режима. Передача осуществляется после фильтрации фрагментов коллизий (первые 64 байта кадра анализируются на наличие ошибки и при её отсутствии кадр обрабатывается в сквозном режиме).

Симметрия в коммутации

- Свойство симметрии при коммутации позволяет дать характеристику коммутатора с точки зрения ширины полосы пропускания для каждого его порта.
- **Симметричный коммутатор** обеспечивает коммутируемые соединения между портами с одинаковой шириной полосы пропускания, например, когда все порты имеют ширину пропускания 10 Мб/с или 100 Мб/с.
- **Асимметричный коммутатор** обеспечивает коммутируемые соединения между портами с различной шириной полосы пропускания, например, в случаях комбинации портов с шириной полосы пропускания 10 Мб/с или 100 Мб/с и 1000 Мб/с.

Симметрия в коммутации

- Асимметричная коммутация используется в случае наличия больших сетевых потоков типа клиент-сервер, когда многочисленные пользователи обмениваются информацией с сервером одновременно, что требует большей ширины пропускания для того порта коммутатора, к которому подсоединён сервер, с целью предотвращения переполнения на этом порте. Для того, чтобы направить поток данных с порта 100 Мб/с на порт 10 Мб/с без опасности переполнения на последнем, асимметричный коммутатор должен иметь буфер памяти.
- Асимметричный коммутатор также необходим для обеспечения большей ширины полосы пропускания каналов между коммутаторами, осуществляемых через вертикальные кросс-соединения, или каналов между сегментами магистрали.

Буфер памяти

- Для временного хранения фреймов и последующей их отправки по нужному адресу, коммутатор может использовать буферизацию. Буферизация может быть также использована в том случае, когда порт пункта назначения занят. Буфером называется область памяти, в которой коммутатор хранит передаваемые данные.
- Буфер памяти может использовать два метода хранения и отправки фреймов: буферизация по портам и буферизация с общей памятью.
- При **буферизации по портам** пакеты хранятся в очередях (queue), которые связаны с отдельными входными портами. Пакет передаётся на выходной порт только тогда, когда все фреймы, находившиеся впереди него в очереди, были успешно переданы. При этом возможна ситуация, когда один фрейм задерживает всю очередь из-за занятости порта его пункта назначения. Эта задержка может происходить даже в том случае, когда остальные фреймы могут быть переданы на открытые порты их пунктов назначения.

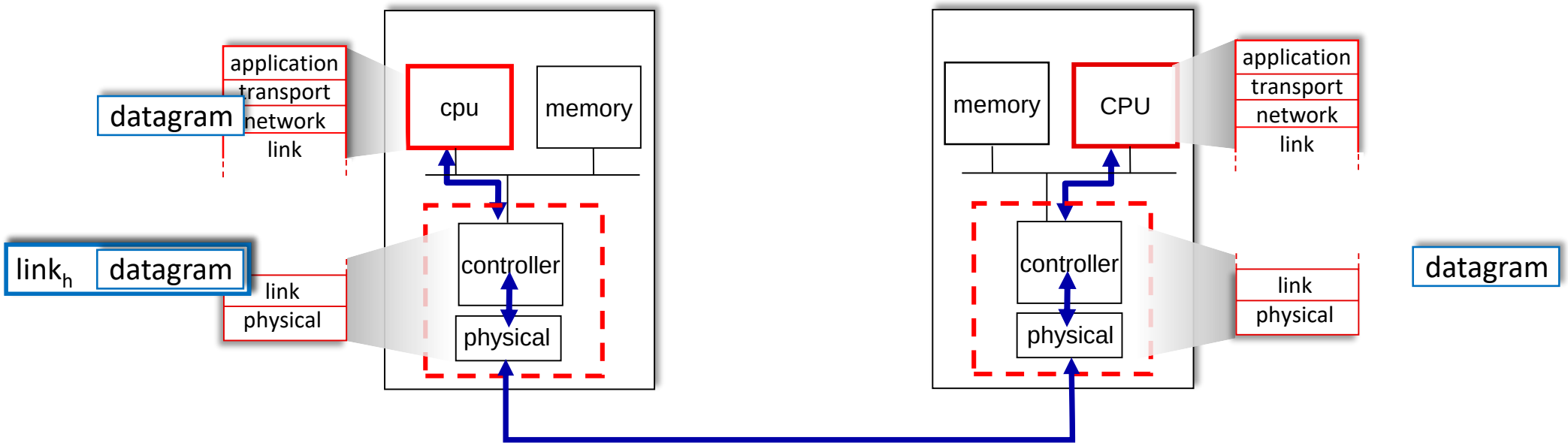
Буфер памяти

- При **буферизации в общей памяти** все фреймы хранятся в общем буфере памяти, который используется всеми портами коммутатора. Количество памяти, отводимой порту, определяется требуемым ему количеством. После этого фреймы, находившиеся в буфере, динамически распределяются по выходным портам. Это позволяет получить фрейм на одном порте и отправить его с другого порта, не устанавливая его в очередь.
- Коммутатор поддерживает карту портов, в которые требуется отправить фреймы. Очистка этой карты происходит только после того, как фрейм успешно отправлен.
- Размер фрейма ограничивается всем размером буфера, а не долей, предназначенной для конкретного порта. Это означает, что крупные фреймы могут быть переданы с меньшими потерями, что особенно важно при асимметричной коммутации, то есть когда порт с шириной полосы пропускания 100 Мб/с должен отправлять пакеты на порт 10 Мб/с.

Механизмы передачи фрейма

- Для того, чтобы передавать фреймы, коммутатор использует три базовых механизма:
- **Flooding** — фрейм, полученный на один из портов, передается на остальные порты коммутатора. Коммутатор выполняет эту операцию в двух случаях:
  - при получении широковещательного или multicast (если не настроена поддержка multicast) фрейма,
  - при получении unknown unicast фрейма. Это позволяет коммутатору доставить фрейм хосту (при условии, что хост достижим и существует), даже когда он не знает, где хост находится.
- **Forwarding** — передача фрейма, полученного на одном порту, через другой порт в соответствии с записью в таблице коммутации.
- **Filtering**— если коммутатор получает фрейм через определенный порт, и MAC-адрес получателя доступен через этот же порт (это указано в таблице коммутации), то коммутатор отбрасывает фрейм. То есть, коммутатор считает, что в этом случае хост уже получил этот фрейм, и не дублирует его.

Взаимодействие интерфейсов



Отправляющая сторона:

- инкапсулирует пакет в кадр
- добавляет биты контроля, выполняет надежную передачу, контроль потока и т.д.

Принимающая сторона:

- Ищет ошибки, выполняет надежный прием, контроль потока и т.д.
- извлекает пакет, передает вышележащему вроню

Подуровень LLC

- Отвечает за достоверную передачу кадров данных между узлами, а также реализует функции интерфейса с прилегающим к нему сетевым уровнем. Стандартные протоколы канального уровня часто различаются реализацией метода доступа к разделяемой среде, в то время как функции LLC-уровня гораздо меньше варьируются от одного стандарта к другому.
- Уровень LLC дает более высоким уровням возможность управления качеством услуг, предоставляемых канальным уровнем. Так передача данных на канальном уровне может быть выполнена дейтаграммным способом либо с установлением соединений, с подтверждением правильности приема либо без подтверждения.

Подуровень MAC

- Отвечает за прием кадра из сети и отправка его в сеть
- В локальных сетях используется разделяемая среда передачи данных, поэтому все протоколы канального уровня локальных сетей включают процедуру доступа к среде, которая и является главной функцией MAC-уровня.
- Кроме того, MAC-уровень должен согласовать дуплексный режим работы уровня LLC с полудуплексным режимом работы физического уровня. Для этого он буферизует кадры с тем, чтобы при получении доступа к среде, передать их по назначению.

MAC адрес

- уникальный шестибайтный номер, «прошитый» в сетевой плате при изготовлении.
- номер используется для идентификации отправителя и получателя фрейма; и предполагается, что при появлении в сети нового компьютера (или другого устройства, способного работать в сети) сетевому администратору не придётся настраивать этому компьютеру MAC-адрес вручную.
- каждый производитель получает в координирующем комитете IEEE Registration Authority диапазон из шестнадцати миллионов (2^{24}) адресов
- По трём старшим байтам MAC-адреса можно определить производителя.

Формат MAC адреса

- 48-разрядный (6 октетов) MAC-адрес, который разделён на четыре части

Формат MAC адреса

- Первые 3 октета содержат 24-битный уникальный идентификатор организации, или код MFG (Manufacturing, производителя), который производитель получает в IEEE. При этом используются только младшие 22 разряда (бита); 2 старшие имеют специальное назначение:
- **Первый бит (младший бит первого байта)** — указывает: для *одиночного (0)* или *группового (1)* адресата предназначен кадр;
- **Второй младший бит первого байта** — указывает, является ли MAC-адрес *глобально (0)* или *локально (1)* администрируемым.

Приемы обнаружения и исправления ошибок

- Канальный уровень получателя может передать сетевому уровню поврежденную дейтаграмму или не заметить повреждения какого-либо другого поля в заголовке кадра. Поэтому следует выбирать такую схему определения ошибок, при которой вероятность подобных событий мала.
- Как правило, чем изощреннее методы обнаружения и исправления ошибок (снижающие вероятность появления необнаруженных ошибок), тем больше издержки — требуется больше операций для вычисления контрольной суммы и больше времени для передачи дополнительной информации.

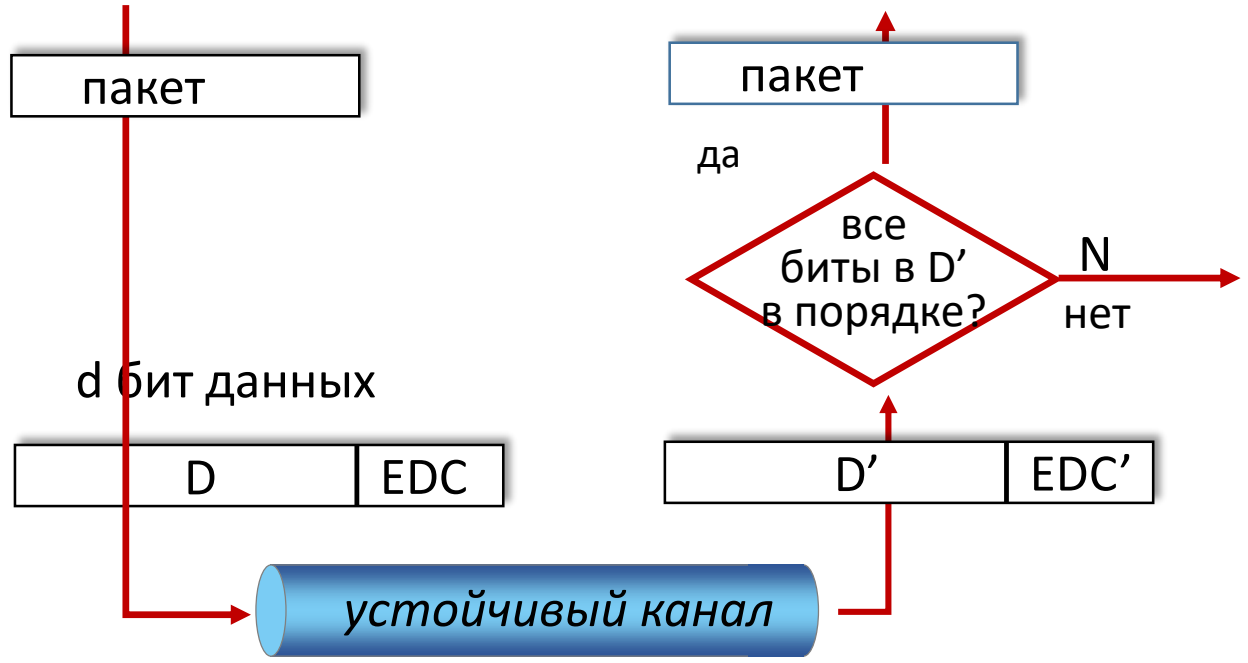
Приемы обнаружения и исправления ошибок

- Для выявления ошибок передачи данных по сети применяются коды двух типов:
  - **Коды обнаружения ошибок;**
  - **Корректирующие коды (допускающие исправление обнаруженных ошибок).**
- Кодирование заключается в добавлении к передаваемым информационным битам дополнительных контрольных битов.
- Контрольные биты при этом могут располагаться отдельно от информационных битов (как в коде CRC), либо вперемежку с информационными (код Хэмминга).

Обнаружение ошибок

EDC: обнаружение и корректировка бит

D: данные, защищенные обработкой



Обнаружение ошибок не надежно на 100%

- протокол может пропускать ошибки
- большее поле EDC дает большие возможности обнаружения и коррекции

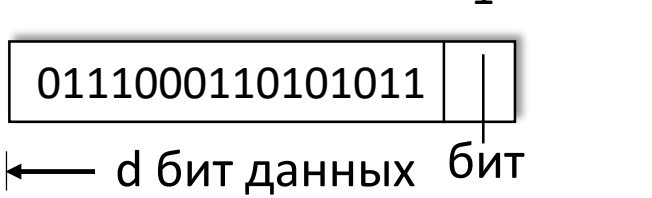
Контроль четности

D Разрядов данных	Бит четности
0 1 1 1 0 0 0 1 1 0 1 0 1 0 1 1	1

Контроль по паритету

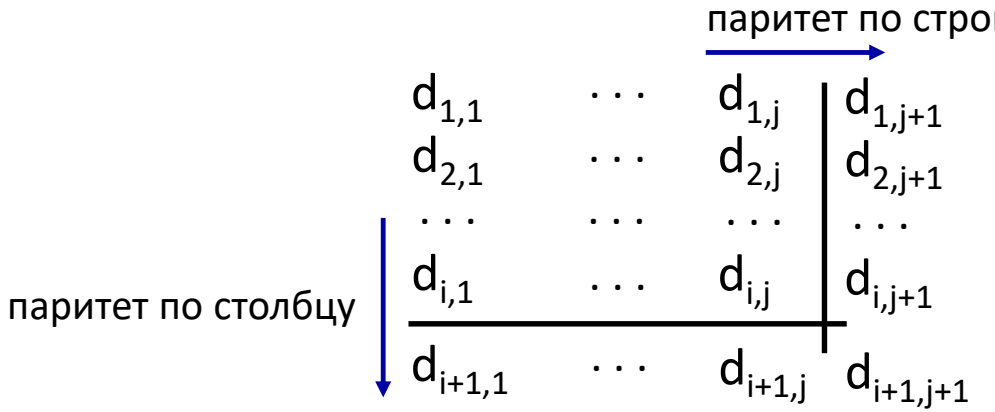
Паритет по строке :

- обнаруживает **единичные** ошибки



Паритет по строке и столбцу:

- обнаруживает и исправляет **единичные** ошибки



Паритет по четности:
установливается бит паритета так, чтобы число 1 было четным

нет ошибок:

1 0 1 0 1	1
1 1 1 1 0	0
0 1 1 1 0	1
1 0 1 0 1	0

обнаруженные и исправленные ошибки 1 бита

1 0 1 0 1	1
1 0 1 1 0	0
0 1 1 1 0	1
1 0 1 0 1	0

ошибка

ошибка

Вычисление контрольной суммы

- D-разрядов данных рассматривается как последовательность k-разрядных целых чисел
- Наиболее простой метод заключается в простом суммировании этих *k*-разрядных целых чисел и использовании полученной суммы в качестве битов определения ошибок.
- В протоколах TCP и UDP контрольная сумма вычисляется по всем полям (включая поля заголовка и данных).
- Не подходит для канального уровня, используется CRC

Контрольная сумма

Цель: Обнаружение ошибок в сегменте

Отправитель:

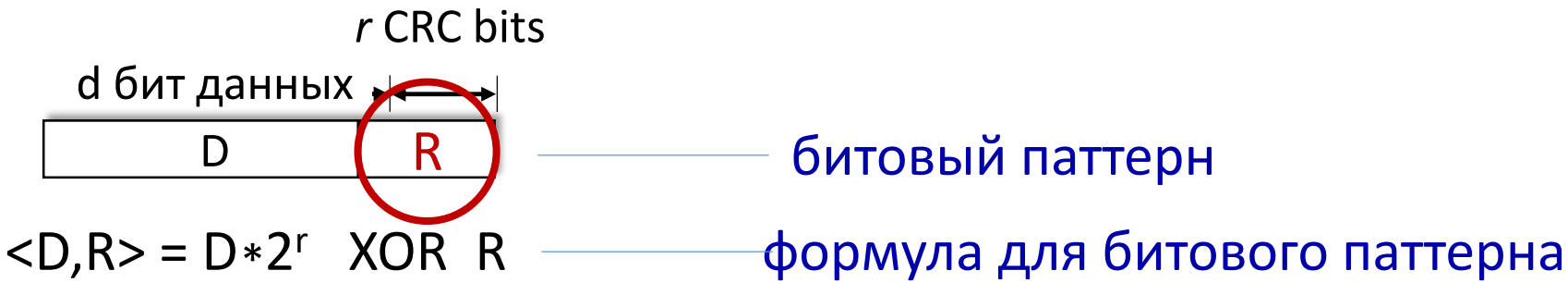
- Рассматривать содержимое UDP сегмента (поля заголовка UDP и IP адреса) как посл-ть 16 битн. чисел
- Контрольная сумма: дополнение содержимого сегмента
- Контрольная сумма помещается в поле контрольной суммы

Получатель:

- Вычислить сумму полученного сегмента
- Проверить, равна ли сумма полученной в пакете:
  - не равна - обнаружена ошибка
  - равна - ошибки нет

Cyclic Redundancy Check (CRC)

- Более совершенный способ контроля
- D: биты данных
- G: битовый паттерн для *r+1* бит



Цель: выбрать *r* CRC бит, R, таких что <D,R> в точности делятся на G (mod 2)

- получатель знает G, делит <D,R> на G. Если остаток ненулевой: ошибка
- может обнаружить все ошибки для r+1 бит
- широко используется на практике (Ethernet, 802.11 WiFi)

Cyclic Redundancy Check (CRC)

- CRC (Cyclic Redundancy Check - циклический избыточный контроль) является разновидностью так называемых хеш-функций.
- Хеш-функция является, по сути, остатком от деления двоичного многочлена, соответствующего информационным данным, на некий фиксированный порождающий многочлен.

CRC: Процедура

- Из файла берётся первое слово — это может быть битовый (CRC-1), байтовый (CRC-8) или любой другой элемент. Если старший бит в слове «1», то слово сдвигается влево на один разряд с последующим выполнением операции XOR с порождающим полиномом. Соответственно, если старший бит в слове «0», то после сдвига операция XOR не выполняется.
- После сдвига теряется старый старший бит, а младший бит освобождается — его значение устанавливается равным нулю.
- На место младшего бита загружается очередной бит из файла, и операция повторяется до тех пор, пока не загрузится последний бит файла. После прохождения всего файла, в слове остается остаток, который и является контрольной суммой.

Cyclic Redundancy Check (CRC): пример

Требование:

$D \cdot 2^r \ XOR \ R = nG$

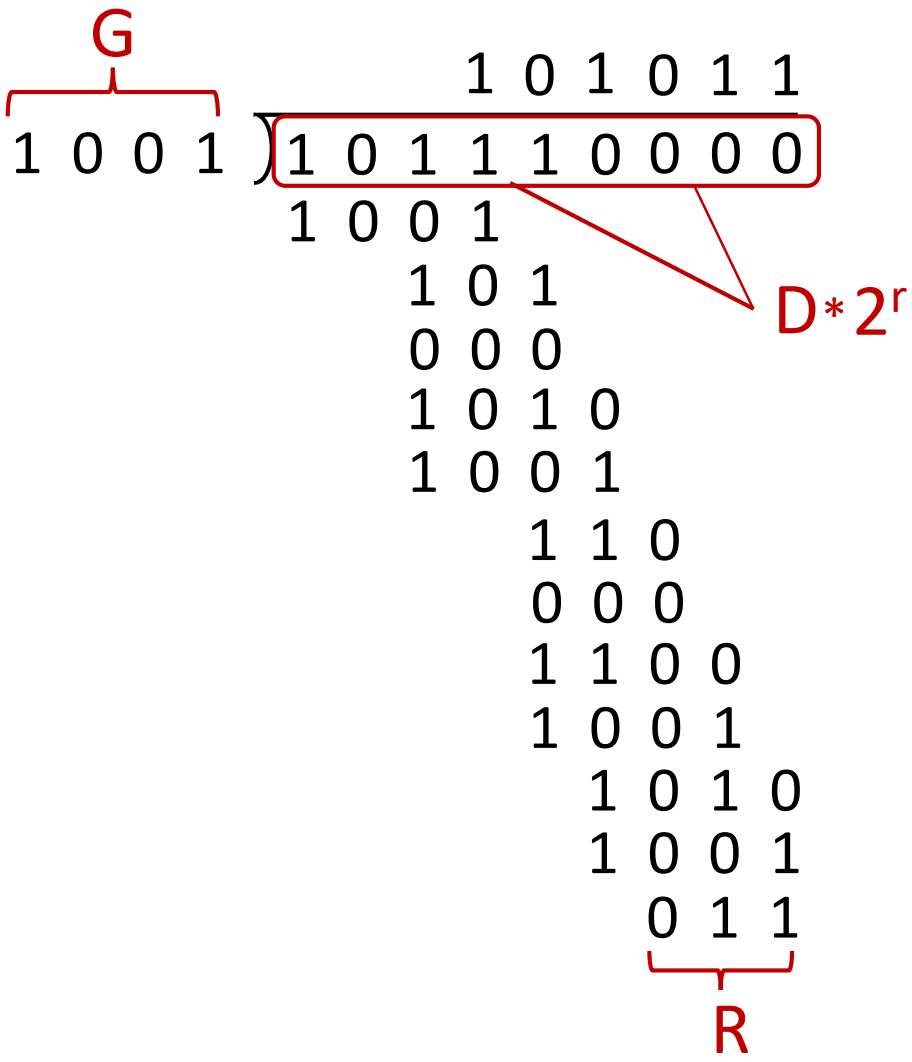
или:

$D \cdot 2^r = nG \ XOR \ R$

или:

при делении $D \cdot 2^r$ by G, остаток должен удовлетворять условию:

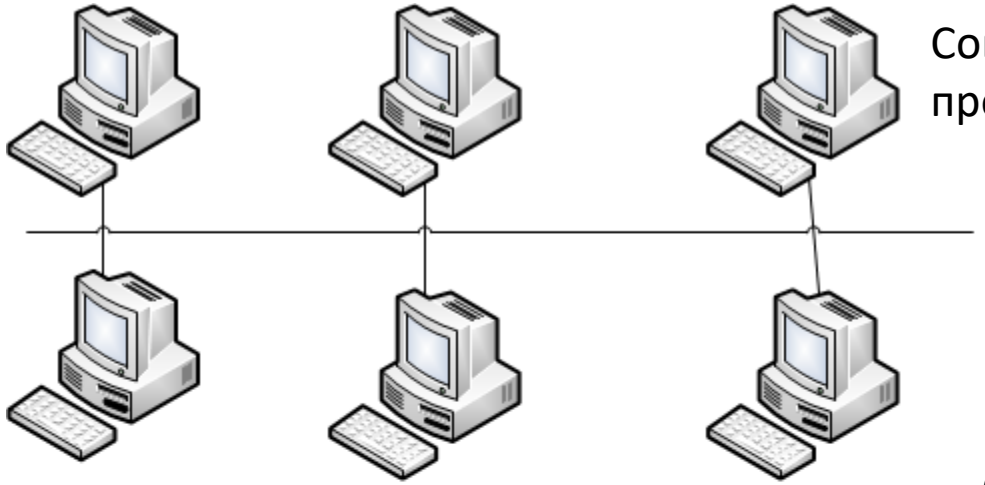
$$R = \text{остаток}\left[\frac{D \cdot 2^r}{G}\right]$$



Задача множественного доступа

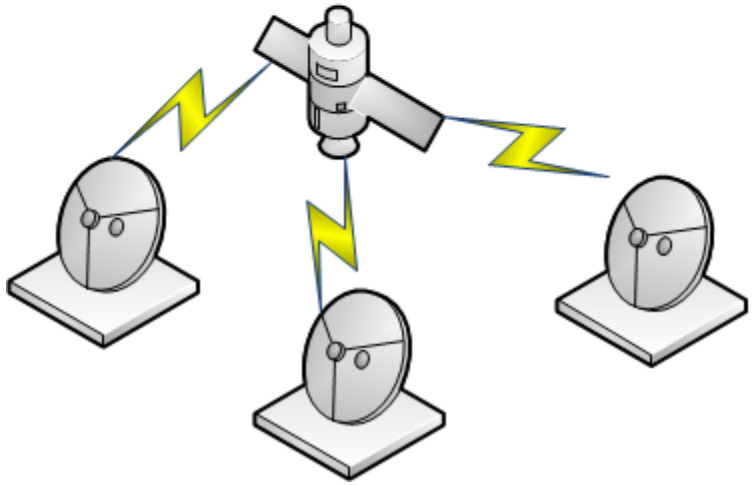
- Важная проблема заключается в координации доступа множества передающих и принимающих узлов к общему широковещательному каналу
- Набор правил для обмена данными называется протоколом множественного доступа
- протоколы множественного доступа применяются в сетях самых разных конфигураций, включая кабельные и беспроводные локальные сети, а также спутниковые сети.

Задача множественного доступа



Совместно используемая
проводная сеть (кабельная)

Совместно используемая
беспроводная сеть



Спутниковая связь

Коллизии

- Поскольку передавать кадры могут все узлы, возможна ситуация, когда одновременно начнут передачу несколько узлов.
- Когда такое происходит, каждый из узлов одновременно получает несколько кадров, то есть на принимающих узлах имеет место **коллизия** переданных кадров.
- Как правило, в случае коллизии принимающие узлы не могут корректно обрабатывать принятые кадры, так как сигналы таких кадров накладываются друг на друга.
- Таким образом, все вовлеченные в коллизию кадры теряются, а все время, пока они передавались, оказывается потраченным впустую.
- Очевидно, что наличие множества узлов, требующих частой передачи данных, означает высокую вероятность коллизий и низкий коэффициент использования канала.

Окно коллизий

- Важным аспектом коллизии является окно коллизий, представляющее собой интервал времени, необходимый для распространения сигнала по каналу и обнаружения его любой станцией сети.
- В наихудших для одноканальной сети условиях время, необходимое для обнаружения столкновения сигналов (коллизии), в два раза больше задержки распространения, так как сигнал, образовавшийся в результате коллизии, должен распространяться обратно к передающим станциям. Чтобы окно коллизии было меньше, такой способ доступа целесообразно применять в сетях с небольшими расстояниями между станциями, т.е. в локальных сетях. Кроме того, вероятность появления коллизий возрастает с увеличением расстояния между станциями сети.
- Коллизия является нежелательным явлением, так как приводит к ошибкам в работе сети и поглощает много канального времени для ее обнаружения и ликвидации последствий. Поэтому желательно реализовать некоторый алгоритм, позволяющий либо избежать коллизий, либо минимизировать их последствия.

Протоколы MAC-подуровня

три основных группы:

- разделение канала
  - разделить канал на части (слоты времени, частоты, код)
  - выделить каждому узлу
- *произвольный доступ*
  - канал не делится, допустимы коллизии
  - восстановление после коллизий
- поочередный доступ
  - узлы получают доступ по очереди, большее время для узлов с большим количеством пакетов к отправке

FDMA

- Каждому пользователю на время сеанса связи выделяется своя полоса частот Δf (частотный канал).
- Наиболее распространено использование метода FDMA в системах радио (Δf обычно составляет 9 кГц при амплитудной модуляции и 25–50 кГц при частотной модуляции) и телевещания (Δf — 8 МГц).
- Используется во всех аналоговых системах сотовой связи, при этом полоса частот Δf составляет 10–30 кГц. Основной недостаток метода FDMA — недостаточно эффективное использование полосы частот. Эффективность заметно повышается при переходе к более совершенным методам доступа.

WDM

- Также называется волновым мультиплексированием или спектральным уплотнением, напоминает хорошо известное мультиплексирование с частотным разделением каналов, но только выполняемое в оптической среде передачи. Развитием этой технологии стало «плотное» WDM (dense WDM, DWDM).
- Рост объема передаваемых данных постепенно привел к исчерпанию пропускной способности существующего оптического волокна, со всей остротой поставив вопрос ее увеличения. Увеличение скорости передачи данных по волоконной линии связи связана с рядом трудностей, поскольку проложенное волокно изначально не было рассчитано на высокие скорости передачи.

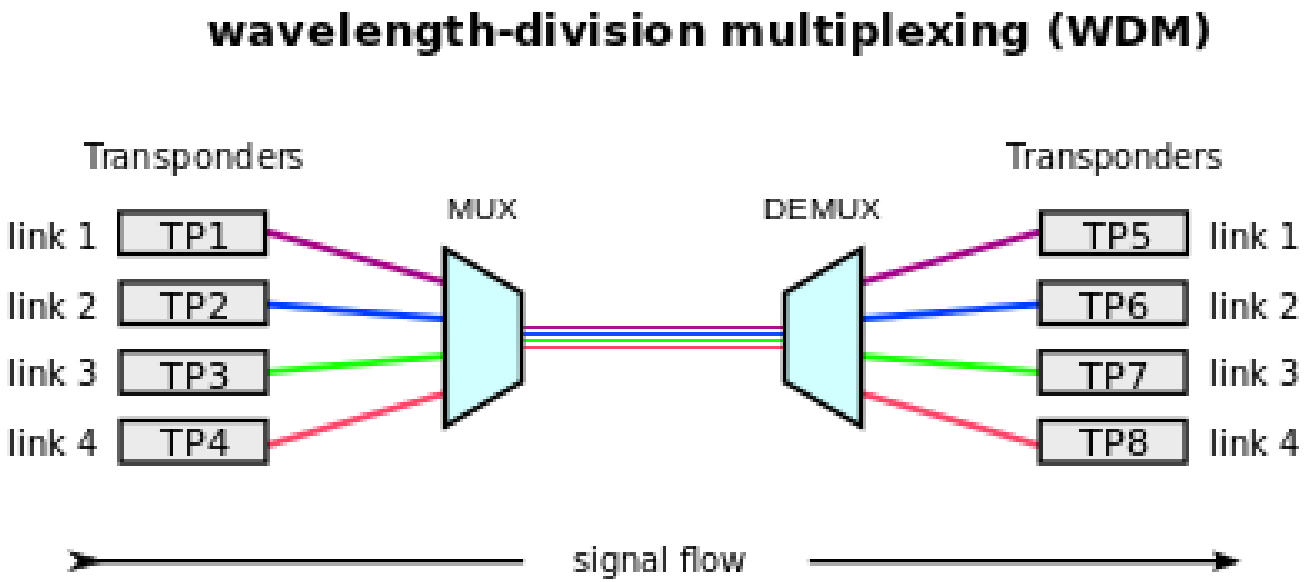
WDM

- Во-первых, при высоких скоростях существенную роль начинают играть отражения сигнала от мест соединения кабелей и поляризационная модовая дисперсия, вызванная отклонением поперечного сечения волокна от круговой формы.
- Для компенсации дисперсии прокладываются отрезки волоконно-оптического кабеля с дисперсией противоположного знака.
- Во-вторых, с ростом скорости передачи усиливается затуха- ние (рассеяние) светового потока и ухудшается чувствительность фотоприемника, то есть увеличивается минимальная мощность входного сигнала, при которой частота появления ошибок соответствует определенному пределу. Чтобы обеспечить достаточную мощность принимаемого сигнала, приходится устанавливать дополнительные усилители и регенераторы.

WDM

- Волновой мультиплексор объединяет сигналы с разными несущими из нескольких входных волокон и передает их по одному магистральному волокну.
- Мультиплексирование выполняется пассивными устройствами, функционирование которых основыва- ется на известных явлениях физической оптики — дисперсии, дифракции, интерференции.
- Обратную операцию реализует волновой демультиплексор: он выделяет одноканальные потоки из многоканального трафика и направляет их в отдельные волокна.

WDM


wavelength-division multiplexing (WDM)
Transponders
Transponders
MUX
DEMUX
link 1
TP1
link 2
TP2
link 3
TP3
link 4
TP4
TP5
link 1
TP6
link 2
TP7
link 3
TP8
link 4
signal flow

ALOHA

- Первая компьютерная сеть передачи данных с пакетной коммутацией, использовавшая в качестве среды доступа к ней беспроводную технологию. Была разработана и введена в эксплуатацию в 1968—1970-х годах группой учёных Гавайского университета под руководством Нормана Абрамсона в рамках исследовательского проекта THE ALOHA SYSTEM
- Необходимость возникла из-за особенностей местности на Гаваях (группа островов с гористым рельефом).

ALOHA

- В сети ALOHAnet для соединения компьютеров с главным вычислительным центром использовалось радиосоединение в дециметровом диапазоне волн. Было выделено два радиоканала шириной 100 КГц со скоростью передачи данных по ним 24 000 бод.
- Один радиоканал на частоте 407.350 МГц использовался для передачи данных от терминалов к центральному компьютеру в Гонолулу, а второй канал на частоте 413.475 МГц использовался для рассылки широковещательных сообщений от центрального компьютера терминалам (для этого возле центрального компьютера была установлена широковещательная антенна, а на удалённых островах — направленные антенны, не позволявшие принимать сообщения друг от друга — в системе ALOHA использовалась сетевая топология звезда).

Чистая ALOHA

- Первую версию *ALOHA random access* также называют чистой ALOHA (англ. *pure ALOHA*). При использовании этого метода доступа к каналу, пользовательские компьютеры начинают передавать центральному пакеты данных сразу же после появления предназначенной для пересылки информации. Если передача двух или большего числа станций совпадают по времени (хотя бы частично), то центральный компьютер не может корректно принять данные.
- Чтобы дать отправителям возможность обнаружить коллизию, центральный компьютер рассылает полученный пакет данных после приёма. Сравнивая переданный пакет и принятый, отправитель может понять, были ли его данные приняты корректно или с ошибками. Если данные были переданы некорректно, отправитель выжидает случайный интервал времени и совершает повторную попытку передачи.

Чистая ALOHA

- Этот подход является достаточно эффективным, когда действия пользователей не координируются и они посылают данные случайными по объему порциями, например с клавиатуры терминала.
- Протокол ALOHA будет работать хорошо, если число передач мало по сравнению с общим временем доступности канала

Слотированная ALOHA

- В 1972 году Лоуренс Робертс предложил другую версию системы ALOHA, названную слотированной ALOHA (англ. *slotted ALOHA*).
- Основным отличием слотированной ALOHA от чистой являлась идея разделения оси времени на дискретные интервалы равной длительности tau , названные слотами.
- Каждый терминал последовательно отмерял границы слотов.
- Для синхронизации границ слотов использовался специальный синхронизирующий сигнал, передаваемый с широковещательной антенны всем терминалам.
- При появлении предназначенных для передачи пакетов данных терминал задерживал передачу до начала следующего слота. Длительность слотов выбиралась так, чтобы за время одного слота терминал успел передать свой пакет данных и получить от центрального компьютера подтверждение успешной передачи.

Слотированная ALOHA

- Слотовая ALOHA требует установки общих (синхронизированных) таймеров на наземных станциях и спутнике.
- Таймеры синхронизируются для передачи графика в строго определенные периоды времени.
- Например, таймеры могут требовать, чтобы пакеты передавались только порциями в течение 20 мс (0,020 с). В данном при- мере интервал в 20 мс получается при использовании канала со скоростью передачи данных 50000 бит/с и пакетов длиной 1000 бит (1000/50000 = 0,20 с).
- Интервал в 20 мс называется длительностью пакета; это время, в течение которого пакет передается по каналу. Существует требование, чтобы все станции начинали передачу в начале слота (кванта времени). Пакет не может передаваться, если он требует для передачи более одного слота.

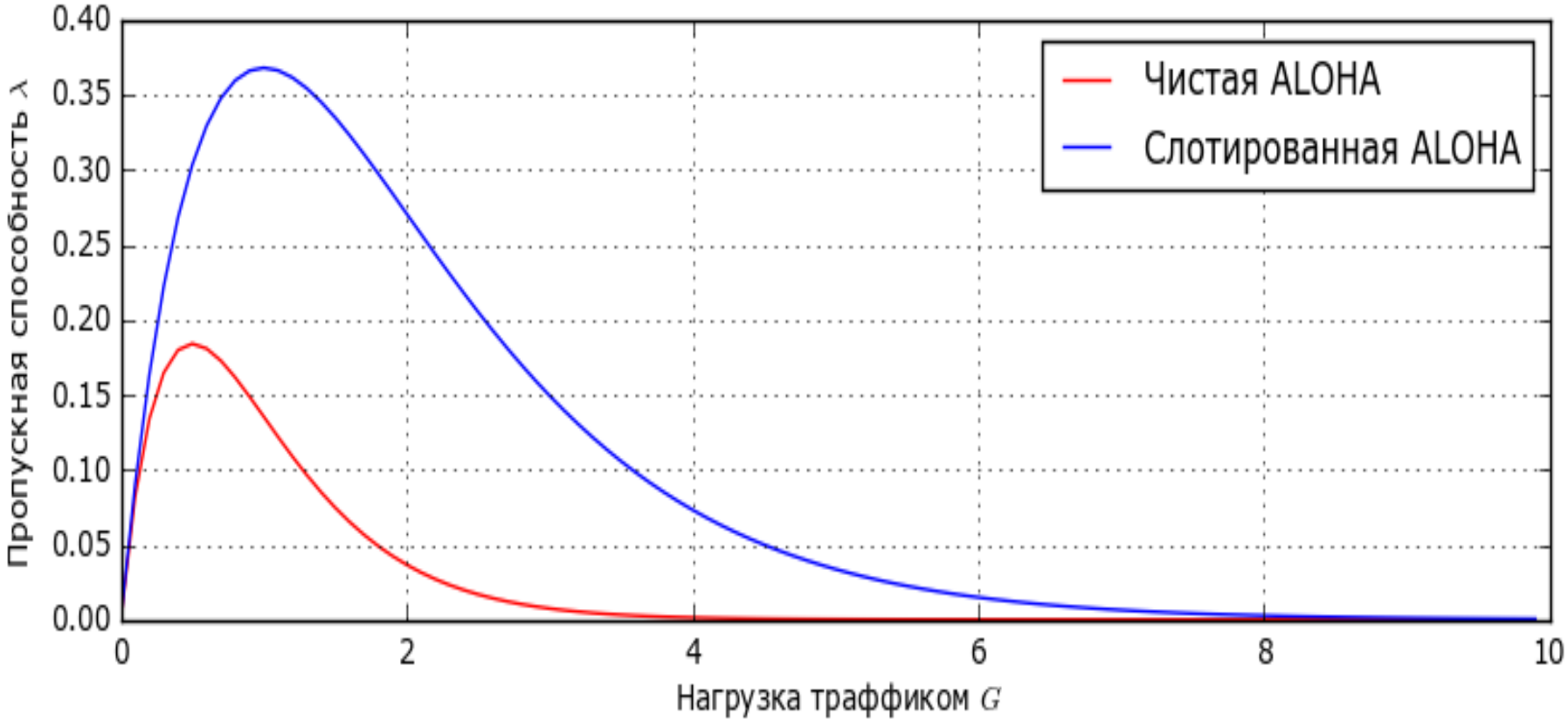
Слотированная ALOHA: эффективность

эффективность: кол-во успешно доставленных фреймов

- предположим, что: существует N узлов с множеством кадров для отправки, каждый передает данные в слот с вероятностью *p*
  - вероятность, что данный узел успешно использует слот = $p(1-p)^{N-1}$
  - вероятность, что любой узел успешно использует слот = $Np(1-p)^{N-1}$
  - макс. эффективность: найти p^* которое приводит к макс. $Np(1-p)^{N-1}$
  - fдля мно-ва узлов, найти предел $Np^*(1-p^*)^{N-1}$ при N $\rightarrow$inf:

макс. эффективность = 1/e = .37

Сравнение пропускной способности



CSMA

- Вероятностный сетевой протокол канального (MAC) уровня.
- Узел, желающий передать пакет данных, выполняет процедуру оценки чистоты канала, то есть слушает шумы в передающей среде в течение заранее определённого периода времени. Если передающая среда оценивается как чистая, узел может передать пакет данных. В противном случае, если выполняется другая передача, узел «отстраняется», то есть ждёт определённое количество времени, прежде чем опять предпринять процедуру отправки пакета.

CSMA

- На практике более распространена модификация этой технологии CSMA/CD, поддерживающая разпознавание коллизий.
- Существует также технология CSMA/CA, которая пытается избегать коллизии.
- Избегание коллизий важно, поскольку сеть CSMA/CD является равноранговой, в результате возникает соперничество за канал

CSMA/CD

1. Адаптер получает пакет от сетевого уровня, создает фрейм
2. Адаптер проверяет канал:
   свободен: начать передачу.
   занят: подождать, пока будет свободен, начать передачу
3. Адаптер передает весь фрейм без коллизий, передача закончена
4. Если адаптер фиксирует факт передачи данных в сети: прекратить, отправить jam последовательность
5. После прекращения
   - после n-ой коллизии, NIC выбирает случайное K $\{0,1,2, \ldots, 2^n-1\}$. NIC ждет $K \cdot 512$ бит, возвращается к шагу 2
   - больше коллизий - больше интервал ожидания

Протоколы поочередного доступа

- Протоколы ALOHA и CSMA не позволяют для каждого из *M* активных узлов передавать свои данные со скоростью *R/M* бит/с, где R - максимальной пропускной способностью канала бит/с.
- Это подвигло исследователей на создание нового класса протоколов — **протоколов поочередного доступа**.
- Как и в случае с протоколами произвольного доступа, их существуют десятки, и у каждого есть множество вариантов.

Протокол опроса

- При использовании протокола опроса один из узлов должен быть назначен главным (управляющим). Главный узел поочередно **опрашивает** все узлы. Например, сначала главный узел посылает сообщение узлу 1, сообщая ему, что он может передать некоторое максимальное количество кадров.
- После того как узел 1 передает несколько кадров, главный узел разрешает передать некоторое количество кадров узлу 2. (Главный узел может определить момент завершения передачи очередным узлом по отсутствию сигнала в канале.)
- Данная процедура продолжается бесконечно, при этом главный узел в цикле опрашивает все узлы.

Протокол опроса

- Протокол опроса устраняет коллизии и пустые кванты, от которых страдают протоколы произвольного доступа, эффективность протокола опроса значительно выше. Однако у протокола опроса есть несколько недостатков.
- Первый -определенное время тратится протоколом опроса на саму процедуру опроса, то есть на выдачу узлу разрешения на передачу. Например, если только один узел является активным, тогда он не сможет передавать со средней скоростью, равной полной пропускной способности канала, так как после отправки активным узлом разрешенного количества кадров главный узел будет опрашивать остальные узлы в каждом цикле.
- Второй - при выходе из строя главного узла вся деятельность канала прекращается.
- В качестве примеров протоколов опроса можно привести 802.15 и Bluetooth

Протокол с передачей маркера

- В этом протоколе главного узла не существует. Все узлы, присоединенные к широковещательному каналу, обмениваются небольшим специальным кадром, называемым **маркером** (токеном).
- Порядок обмена маркера фиксирован. Например, узел 1 всегда посылает маркер узлу 2, а узел 2 всегда посылает маркер узлу 3 и т. д.; а узел *N* всегда посылает маркер узлу 1. Получив маркер, узел удерживает его, только если у него есть данные для передачи; в противном случае он немедленно передает маркер следующему узлу.
- Если к моменту получения маркера у узла есть кадры для передачи, он отправляет некое максимальное количество кадров, после чего пересылает маркер следующему узлу.

Протокол с передачей маркера

- Передача маркера осуществляется децентрализованно и обладает высокой эффективностью.
- Но проблемы могут возникнуть и в данной схеме. Например, выход из строя одного узла может вывести из строя весь канал, а если какой-либо узел забудет передать маркер, потребуется специальная процедура вывода канала из тупиковой ситуации.
- За многие годы было разработано множество протоколов с передачей маркера, в частности, FDDI (протокол волоконно-оптического интерфейса передачи) и протокол IEEE 802.5 для передачи маркера по сети с кольцевой конфигурацией.

Протокол маркерное кольцо

- Протокол типа "*маркерное кольцо"* применяется в сетях с кольцевой топологией, которые относятся к типу сетей с последовательной конфигурацией, где широковещательный режим работы невозможен.
- В таких сетях сигналы распространяются через однонаправленные двухточечные пути между узлами.
- Узлы и однонаправленные звенья соединяются последовательно, образуя физическое кольцо.
- В отличие от сетей с шинной структурой, где узлы действуют только как передатчики или приемники и отказ узла или удаление его из сети не влияет на передачу сигнала к другим узлам, здесь при распространении сигнала все узлы играют активную роль, участвуя в ретрансляции, усилении, анализе и модификации приходящих сигналов.

DOCSIS

- Стандарт предусматривает передачу данных абоненту по сети кабельного телевидения с максимальной скоростью до 42 Мбит/с и получение данных от абонента со скоростью до 10,24 Мбит/с.
- Он призван сменить господствовавшие ранее решения на основе фирменных протоколов передачи данных и методов модуляции, несовместимых друг с другом, и должен гарантировать совместимость аппаратуры различных производителей.

DOCSIS

- Стандарт DOCSIS задействует мультиплексирование с частотным разделением (FDM) для разделения нисходящих (от CMTS к модему) и восходящих (от модема к CMTS) сетевых сегментов на множество частотных каналов.
- Ширина каждого нисходящего канала составляет 6 МГц, максимальная пропускная способность — около 40 Мбит/с на канал (хотя на практике такая частота передачи данных по кабельному модему достигается редко).
- Максимальная ширина восходящего канала составляет 6,4 МГц, а его максимальная пропускная способность — примерно 30 Мбит/с.
- Все восходящие и нисходящие каналы являются широковещательными.
- Кадры передаются по нисходящему каналу головной станцией и принимаются всеми кабельными модемами, подключенными к этому каналу.

DOCSIS

- Каждый интервал содержит последовательность мини-интервалов, в ходе которых кабельные модемы могут передавать информацию CMTS. CMTS явно выделяет конкретным кабельным модемам право на передачу информации в ходе тех или иных мини-интервалов.
- Для этого CMTS отправляет по нисходящему каналу специальное управляющее сообщение, называемое MAP, в котором указывает, какой кабельный модем (располагающий данными для отправки) может их передать в течение мини-интервала, приходящегося на период, обозначенный в MAP-сообщении.
- Поскольку мини-интервалы явно выделяются кабельным модемам, головная станция может гарантировать, что в ходе мини-интервала никаких коллизий не возникнет.

ARP [RFC 826]

- Когда одно из устройств пытается установить связь с другим, с известным IP-адресом, ему необходимо определить MAC-адрес получателя. Именно эту задачу решает протокол ARP
- Описание протокола было опубликовано в ноябре 1982 года в RFC 826. ARP был спроектирован для случая передачи IP-пакетов через кадры Ethernet. При этом общий принцип, предложенный для ARP, может, и был использован и для сетей других типов.
- Данные ARP вкладываются в протокол канального уровня и являются, по уровню вложения, протоколом 3го уровня, по функционалу остаются протоколом 2го уровня.

ARP-таблица

- Некоторые устройства хранят специальные ARP-таблицы, в которых содержится информация о MAC- и IP-адресах других устройств, подключенных к той же локальной сети. ARP-таблицы позволяют установить однозначное соответствие между IP- и MAC-адресами. Такие таблицы хранятся в определенных областях оперативной памяти и обслуживаются автоматически на каждом из сетевых устройств (см. таблицы ниже).
- В редких случаях приходится создавать ARP-таблицы вручную. Обратите внимание, что каждый компьютер в сети поддерживает свою собственную ARP-таблицу.

ARP-таблица

ifindex	Физический порт (интерфейс), соответствующий данному адресу;
Физический адрес	MAC-адрес, например Ethernet-адрес;
IP-адрес	IP-адрес, соответствующий физическому адресу;
тип адресного соответствия	1) вариант не стандартный и не подходит ни к одному из описанных ниже типов; 2) 2 - данная запись уже не соответствует действительности; 3) 3 - постоянная привязка; 4) 4 - динамическая привязка;

Интернет-адрес	Физический адрес	Тип
112.11.15.145	44-8B-5C-CB-E8-FD	динамический

ARP запись и TTL

- Ниже пример таблицы, где для каждой пары адресов в таблице **также содержится поле предписанного времени жизни (Time To Live, TTL**), в котором указывается, когда данная запись будет удалена из таблицы.
- В таблице не обязательно содержатся записи для всех узлов локальной сети. Записи для одних узлов могут быть удалены, так как время их жизни истекло, записи для других узлов вообще могут никогда не попасть в эту таблицу.
- Типичное значение времени жизни — 20 мин. с момента помещения записи в ARP-таблицу.

Интернет-адрес	Физический адрес	TTL
112.11.15.145	44-8B-5C-CB-E8-FD	13:36:00

Пример работы протокола

- Прикладная программа одного хоста отправляет сообщение другой. Прикладной программе IP-адрес места назначения обычно известен.
- Данный IP адрес ищется в ARP таблице в оперативной памяти.
- Если для требуемого IP-адреса в ней присутствует Ethernet-адрес, то формируется и посылается соответствующий пакет.
- Если же с помощью ARP-таблицы не удается преобразовать адрес, то выполняется следующее:
- Всем машинам в сети посылается пакет с ARP-запросом (с широковещательным Ethernet-адресом места назначения)
- Исходящий IP-пакет ставится в очередь.

Пример работы протокола

- Каждая машина, принявшая ARP-запрос, сравнивает собственный IP-адрес с IP-адресом в запросе. Если IP-адрес совпал, то прямо по Ethernet-адресу отправителя запроса посылается ответ, содержащий как IP-адрес ответившей машины, так и ее Ethernet-адрес.
- После получения ответа на свой ARP-запрос машина имеет требуемую информацию о соответствии IP и Ethernet-адресов, формирует соответствующий элемент ARP-таблицы и отправляет IP-пакет, ранее поставленный в очередь. Если же в сети нет машины с искомым IP-адресом, то ARP-ответа не будет и не будет записи в ARP-таблицу. Протокол IP будет уничтожать IP-пакеты, предназначенные для отправки по этому адресу.

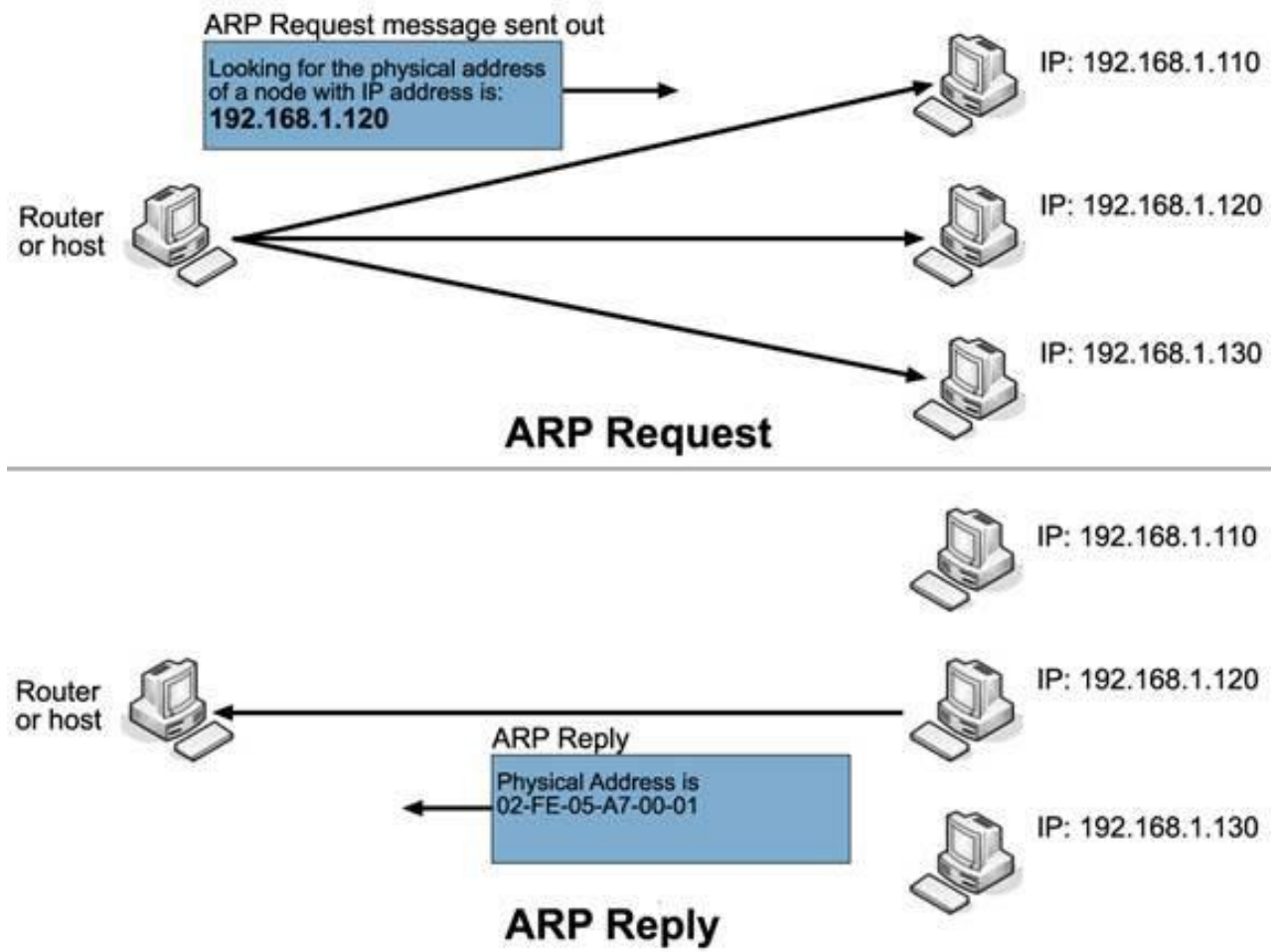
Пример работы протокола

- Когда система-источник получает такой ответ, она обновляет свою таблицу ARP и становится готовой к пересылке данных по локальной сети.
- Сообщение ARP помещается в поле данных кадра вслед за заголовком (заголовками) нижних уровней.
- Например, для Ethernet с кадрами DIX сообщение ARP следует за MAC-заголовком, а для сетей типа 802.3 или 802.5 — за MAC-заголовком, заголовком Logic Link Control (LLC) и подзаголовком Sub-Network Access Protocol (SNAP).
- Тип протокола для таких кадров (ARP через Ethernet) определяется кодом X'0806.

Пример работы протокола

- Некоторые реализации IP и ARP не ставят в очередь IP-пакеты на то время, пока они ждут ARP-ответов. Вместо этого IP-пакет просто уничтожается, а его восстановление возлагается на модуль TCP или прикладной процесс, работающий через UDP.
- Такое восстановление выполняется с помощью таймаутов и повторных передач. Повторная передача сообщения проходит успешно, так как первая попытка уже вызвала заполнение ARP-таблицы.
- Следует отметить, что каждая машина имеет отдельную ARP-таблицу для каждого своего сетевого интерфейса.

Пример работы протокола



Формат ARP-кадра

Формат пакета ARP

Формат ARP-кадра

- **Поле Hardware Type** : В поле данного типа помещается признак типа используемого протокола канального уровня. Протоколу Ethernet соответствует значение 1 данного поля.
- **Поле Protocol Type** : В поле данного типа помещается признак типа используемого протокола сетевого уровня. Протоколу IP соответствует значение 0800 данного поля.
- **Поля HLEN и PLEN** : Содержимое полей HLEN и PLEN определяет размер адреса канального и сетевого уровня соответственно. Наличие данных полей обеспечивает возможность использования протокола ARP для определения физического адреса в различных сетях второго и третьего уровня.

Коды оборудования

Код типа оборудования	Описание
1	Ethernet (10 Мбит/с)
2	Экспериментальный Ethernet (3 Мбит/с)
3	Радиолюбительская связь через X.25
4	Proteon ProNET маркерная кольцевая сеть (Token Ring)
5	Chaos (полнодуплексная надежная передача между процессами)
6	Сети IEEE 802
7	ARCNET

Формат ARP-кадра

- **Поле Operation :** В этом поле размещается признак типа информационного кадра ARP

Operation	Значение
ARP Request	1
ARP Response	2
RARP Request	3
RARP Response	4

- **Поля IP (Network Address)** В полях Target IP и Sender IP кадров ARP и RARP размещаются сетевые адреса станции назначения и передающей станции, соответственно.
- **Поля HA (Hardware Address)**

  В полях Target HA и Sender HA кадров ARP и RARP размещаются физические адреса станции назначения и передающей станции, соответственно.

ARP кэш

- На каждом хосте содержится ARP кэш (ARP cache).
- Записи в кэше могут быть двух видов: статические и динамические.
- Время жизни записи в кэше оставлено на усмотрение разработчика. По умолчанию может составлять от десятков секунд (например, 20 секунд) до четырёх часов
- ARP кэш хранит данные несколько минут после сеанса связи, затем данные о MAC адресе Получателя удаляются из кэша и перед выполнением очередного сеанса связи Отправитель будет вынужден опять отправить ARP запрос в сеть.
- Вывести на экран arp-таблицу:
  arp –a

ProxyARP

- Сети соединены через маршрутизатор, работающий в соответствии со смешанным протоколом ARP (функционально это IP-мост)
- Маршрутизатор знает, какая из машин принадлежит какой физической сети.
- Он перехватывает широковещательные ARP-запросы из сети 1, относящиеся к сети 2, и наоборот.
- Во всех случаях в качестве физического адреса маршрутизатор возвращает свой адрес. В дальнейшем, получая дейтограммы, он маршрутизирует их на физические адреса по их IP-адресам.

RARP

- Принцип работы RARP заключается в том, что бездисковая система может считать свой уникальный аппаратный адрес с интерфейсной платы и послать RARP запрос (широковещательный фрейм в сеть), где потребует кого-нибудь откликнуться и сообщить IP адрес (с помощью RARP отклика).
- Протокол (и сервер) RARP обеспечивает определение IP адреса по MAC адресу (например, при загрузке устройства, не имеющего возможности хранить свой собственный IP адрес), т.е. Выполняет функции обратные протоколу ARP. Уникальный MAC адрес обеспечивается изготовителем устройства.
- Клиент RARP посылает широковещательный кадр Ethernet с запросом, содержащим MAC адрес целевого узла. В ответ от сервера ожидается RARP пакет (unicast), содержащий соответствующий ему IP адрес. Ответ может быть получен непосредственно от RARP сервера или от посредника (proxy). В качестве посредника обычно выступает маршрутизатор. В сегменте сети может быть несколько RARP серверов, так что можно ожидать несколько ответов.

Особенности RARP

- Очевидно, что использование одной рабочей станции в качестве RARP – сервера не может обеспечить достаточной надежности. Станция, которая выполняет данную функцию в сети, может выйти из строя, или может быть слишком перегружена для того, чтобы вовремя ответить на RARP – запрос. Поскольку ответ на запрос не будет получен, запрос нужно повторять снова и снова. Единственным выходом из данной ситуации может быть резервирование RARP – сервера.
- Простое резервирование (например - дублирование) этих устройств может привести к возникновению дополнительных трудностей. К таким трудностям, в частности, относится возможность возникновения коллизий при одновременном ответе на RARP – запрос двумя RARP – серверами. Для разрешения этой проблемы должно быть проведено ранжирование серверов на первичный и вторичные.

Особенности RARP

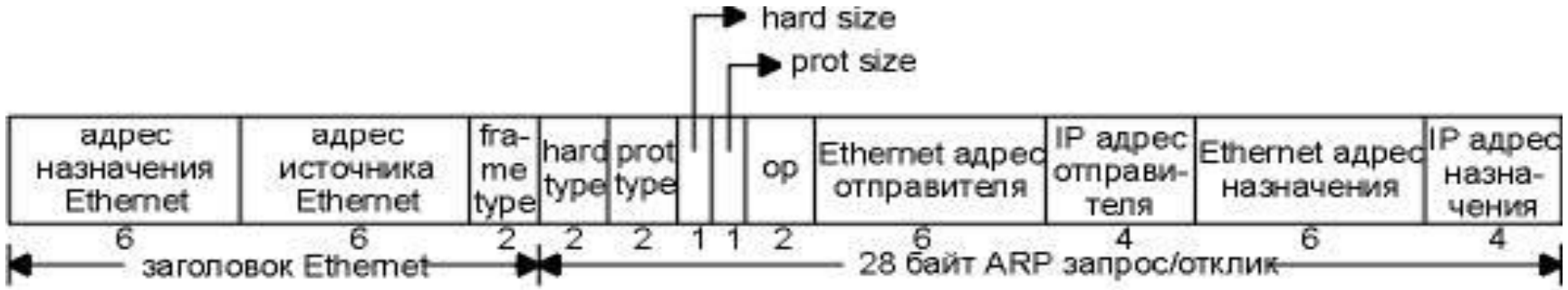
- Для предотвращения коллизий в данном случае может быть использовано две схемы:
- Задержка ответа вторичного RARP – сервера на такт
- Задержка ответа вторичного RARP – сервера на случайный отрезок времени

Особенности RARP

- При использовании первой схемы в сети может только один вторичный RARP–сервер, который отвечает на RARP–запрос только в том случае, если он был послан повторно. Очевидно, что использование данной схемы не позволяет избежать возникновения коллизии в том случае, когда первый запрос был потерян из-за временной перегрузки первичного RARP – сервера или вследствие возникновения проблем в канале передачи на физическом уровне.
- При использовании второй схемы в сети могут находиться несколько вторичных RARP–серверов. Каждый из этих вторичных серверов отвечает на RARP – запрос по прошествии интервала времени, величина которого определяется случайным образом. Очевидно, что в данном случае, вероятность возникновения коллизий при ответе вторичных серверов существенно уменьшается.

Формат пакета RARP

- Формат пакета RARP практически идентичен пакету ARP. Запрос RARP широковещательный, в нем содержится аппаратный адрес отправителя, при этом он спрашивает кого-либо послать ему его IP адрес. Отклик обычно персональный.



где,
hard size - размер аппаратного адреса
prot size - размер адреса протокола
frame type - тип фрейма
hard type - тип аппаратного адреса
prot type - тип адреса протокола
op - код операции

STP

- Сетевой протокол (или семейство сетевых протоколов) предназначенный для автоматического удаления циклов (петель коммутации) из топологии сети на канальном уровне в Ethernet-сетях.
- Основной задачей STP является устранение петель в топологии произвольной сети Ethernet, в которой есть один или более сетевых мостов, связанных избыточными соединениями.
- STP решает эту задачу, автоматически блокируя соединения, которые в данный момент для полной связности коммутаторов являются избыточными.

STP

- Протокол STP формализует сеть в виде графа, вершинами которого являются коммутаторы и сегменты сети.
- Сегмент — это связная часть сети, не содержащая коммутаторов (маршрутизаторов).
- Сегмент может быть разделяемым (во времена создания алгоритма STA это был единственный тип сегмента) и включать устройства физического уровня — повторители/концентраторы, существование которых коммутатор, будучи устройством канального уровня, «не замечает».

Метрика

- Величина, обратно пропорциональная пропускной способности сегмента.
- Условное время передачи бита сегментом.
- В текущей версии стандарта 802.1D-2004 используются такие значения метрик, которые расширяют диапазон скоростей сегментов до 10 Тбит/с (то есть с большим запасом относительно сегодняшнего уровня максимальной для Ethernet скорости в 100 Гбит/с), давая такому сегменту значение 2;
- Соответственно сегмент 100 Гбит/с получает значение 200, 10 Гбит/с — 2000, 1 Гбит/с - 20 000, 100 Мбит/с - 200 000, а 10 Мбит/с - 2 000 000.

BPDU

- Специальные пакеты, которыми периодически обмениваются коммутаторы для автоматического определения конфигурации дерева.
- Переносят данные об идентификаторах коммутаторов и портов, а также о расстоянии до корневого коммутатора. Существуют два типа сообщений, которые переносят пакеты BPDU:
  - Конфигурационные сообщения, называемые также сообщениями Hello (с интервалом 2 с), и сообщения с уведомлениями об изменении конфигурации.
  - Для доставки BPDU используется групповой адрес 01:80:C2:00:00:00, позволяющий организовать эффективный обмен данными.

STP

- Суть работы протокола заключается в том, что поддерживающие его коммутаторы сети Ethernet обмениваются друг с другом информацией «о себе».
- На основании определённых условий (обычно в соответствии с настройками) один из коммутаторов выбирается «корневым» (или «root»), после чего все остальные коммутаторы по алгоритму остовного дерева выбирают для работы порты, «ближайшие» к «корневому» коммутатору (учитывается количество посредников и скорость линий).
- Все прочие сетевые порты, ведущие к «корневому» коммутатору, блокируются. Таким образом образуется несвязное дерево с корнем в выбранном коммутаторе.

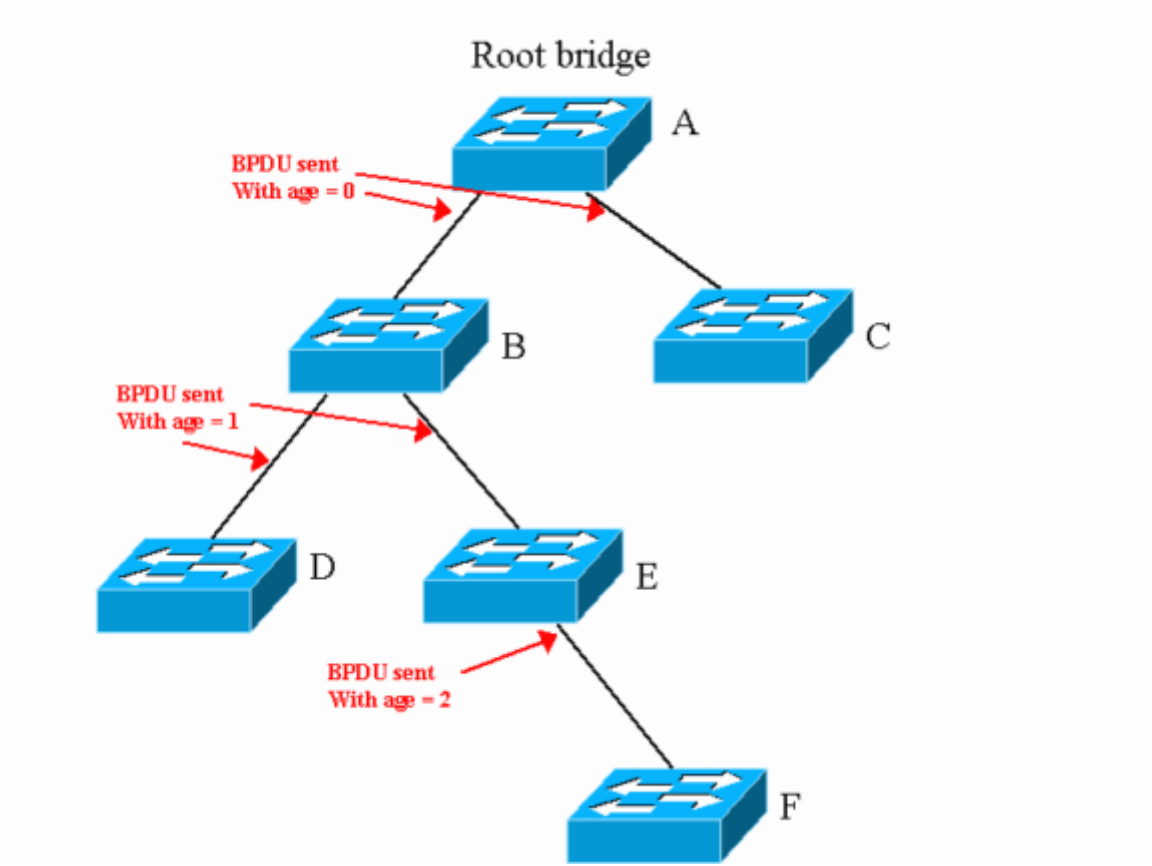
STP

- После включения коммутаторов в сеть, по умолчанию каждый коммутатор считает себя корневым (root).
- Каждый коммутатор начинает посылать по всем портам конфигурационные Hello BPDU пакеты раз в 2 секунды.
- Если мост получает BPDU с идентификатором моста (Bridge ID) меньшим, чем свой собственный, он прекращает генерировать свои BPDU и начинает ретранслировать BPDU с этим идентификатором. Таким образом в конце концов в этой сети Ethernet остаётся только один мост, который становится *корневым мостом* (root bridge).
- Остальные мосты ретранслируют BPDU корневого моста, добавляя в них собственный идентификатор и увеличивая счётчик стоимости пути (path cost).

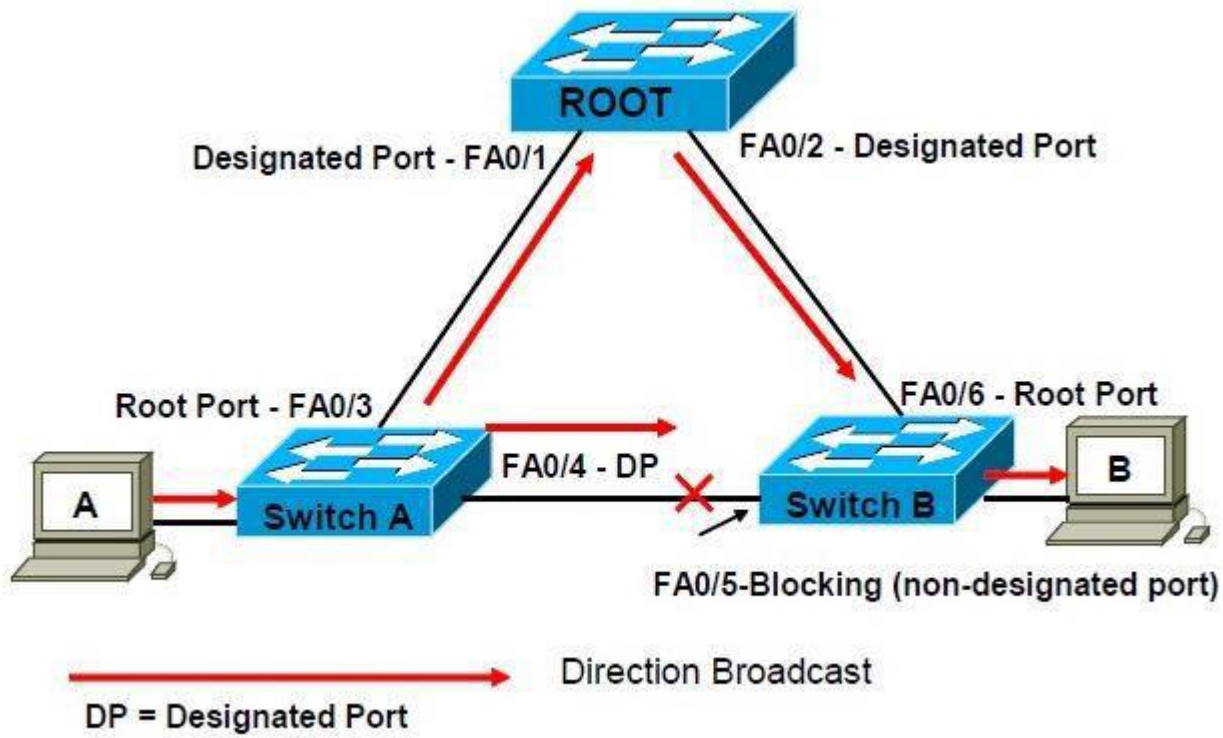
STP

- Для каждого сегмента сети, к которому присоединены два и более портов мостов, происходит определение designated port — порта, через который BPDU, приходящие от корневого моста, попадают в этот сегмент.
- После этого все порты в сегментах, к которым присоединены 2 и более портов моста, блокируются за исключением root port и designated port.
- Корневой мост продолжает посылать свои Hello BPDU раз в 2 секунды.

STP - схема работы



STP - схема работы



RSTP [IEEE 802.1w]

- Модификация, призванная сократить время реконфигурирования за счет усложнения алгоритма
- Основным недостатком протокола STP является его «медлительность»: в сетях с большим количеством коммутаторов время определения новой активной конфигурации может оказаться слишком большим.
- Если в сети используются заданные по умолчанию значения тайм-аутов, то переход на новую конфигурацию может занять свыше 50 секунд: 20 секунд понадобится на констатацию факта потери связи с корневым коммутатором (истечение таймера — единственный способ узнать об этом событии в стандартном варианте STA), еще 2x15 секунд нужно для перехода портов в состояние продвижения.

Тип сегмента

- Двухточечный сегмент. В коммутируемых сетях это единственный тип сегмента; для него у порта существует единственный порт-сосед.
- Разделяемая среда. Стандарт RSTP по-прежнему учитывает существование разделяемой среды, так как формально ее никто не отменял для скоростей ниже 10 Гбит/с.
- Тупиковая связь (edge port). Связь, соединяющая порт коммутатора с конечным узлом сети; по этому сегменту нет смысла ожидать прихода сообщений протокола RSTP. Тупиковая связь конфигурируется администратором.

Другие отличия

- Исключается стадия прослушивания. Коммутаторы не делают паузу в 15 секунд, для того чтобы зафиксировать соответствующую роль порта, например, корневого или назначенного. Вместо этого порты переходят в стадию обучения сразу же после назначения им роли корневого или назначенного порта.
- Сокращается период фиксации отказа в сети — вместо 10 периодов неполучения сообщений Hello он стал равен трем таким периодам, то есть 6 секунд вместо 20.

Другие отличия

- Введены новые роли портов — появились альтернативный (alternative) и резервный (backup) порты.
- **Альтернативный порт** — порт-дублер корневого порта коммутатора, то есть он начинает продвигать кадры в том случае, когда отказывает (либо перестает принимать сообщения Hello в течение трех периодов) корневой порт.
- **Резервный порт** является портом-дублером назначенного порта сегмента; однако такая роль порта имеет смысл только для сегментов, представляющих собой разделяемую среду.
- Альтернативные и резервные порты находятся в состоянии отбрасывания кадров, так как они не должны продвигать кадры до тех пор, пока их роль не изменится на роль корневого или назначенного порта. Как альтернативные, так и резервные порты выбираются одновременно с корневыми и назначенными портами.

Фильтрация трафика

- В локальной сети могут возникать ситуации, когда абсолютная доступность узлов нежелательна.
- Пример — сервер финансового отдела, доступ к которому желательно разрешить только с компьютеров нескольких конкретных сотрудников этого отдела.
- Доступ можно ограничить и на уровне ОС или системы управления базой данных самого сервера, но для надежности желательно иметь несколько эшелонов защиты и ограничить доступ еще и на уровне сетевого трафика.

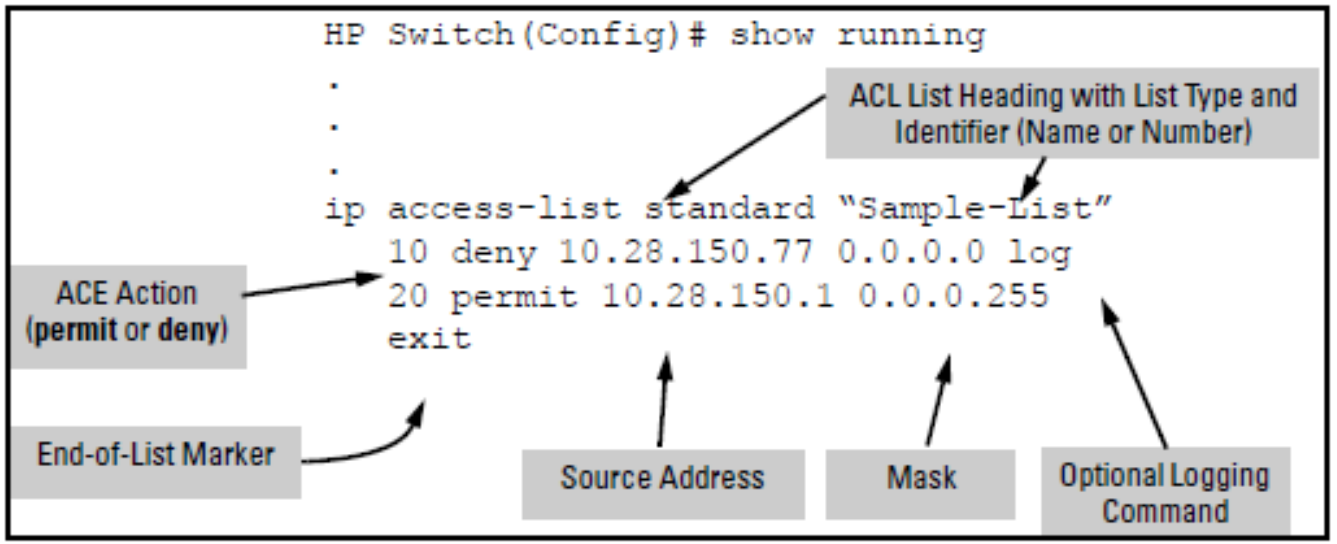
Фильтрация трафика

- **Пользовательский фильтр,** который также часто называют списком доступа (access list), предназначен для создания дополнительных барьеров на пути кадров, что позволяет ограничивать доступ определенных групп пользователей к отдельным службам сети.
- Пользовательский фильтр —это набор условий, которые ограничивают обычную логику передачи кадров коммутаторами.
- Наиболее простыми являются пользовательские фильтры на основе MAC-адресов станций.

Фильтрация трафика

- Иногда администратору требуется задать более тонкие условия фильтрации, например, запретить некоторому пользователю печатать свои документы на Windows-сервере печати, находящемся в чужом сегменте, а остальные ресурсы этого сегмента сделать доступными.
- Для реализации подобного фильтра нужно запретить передачу кадров, которые удовлетворяют следующим условиям: во-первых, имеют определенный MAC-адрес, во-вторых, содержат в поле данных пакеты SMB, в-третьих, в соответствующем поле этих пакетов в качестве типа сервиса указана печать.
- Коммутаторы не анализируют протоколы верхних уровней, такие как SMB, поэтому администратору приходится для задания условий фильтрации «вручную» определять поле, по значению которого нужно осуществлять фильтрацию.

Пример правил списка доступа



Виртуальные локальные сети (VLAN)

- Группа узлов сети, трафик которой, в том числе широковещательный, на канальном уровне полностью изолирован от трафика других узлов сети.

Назначение VLAN

При использовании пользовательских фильтров коммутатора возникают проблемы:

- Приходится задавать отдельные условия для каждого узла сети, используя при этом громоздкие MAC-адреса. Гораздо проще было бы группировать узлы и описывать условия взаимодействия сразу для групп.
- Невозможно блокировать широковещательный трафик. Широковещательный трафик может быть причиной недоступности сети, если какой-то ее узел умышленно или неумышленно с большой интенсивностью генерирует широковещательные кадры.

Назначение VLAN

- Основное назначение технологии VLAN состоит в облегчении процесса создания изолированных сетей, которые затем обычно связываются между собой с помощью маршрутизаторов.
- Такое построение сети создает мощные барьеры на пути нежелательного трафика из одной сети в другую.
- Любая крупная сеть должна включать маршрутизаторы, иначе потоки ошибочных кадров, например широковещательных, будут периодически «затапливать» всю сеть через прозрачные для них коммутаторы, приводя ее в неработоспособное состояние.

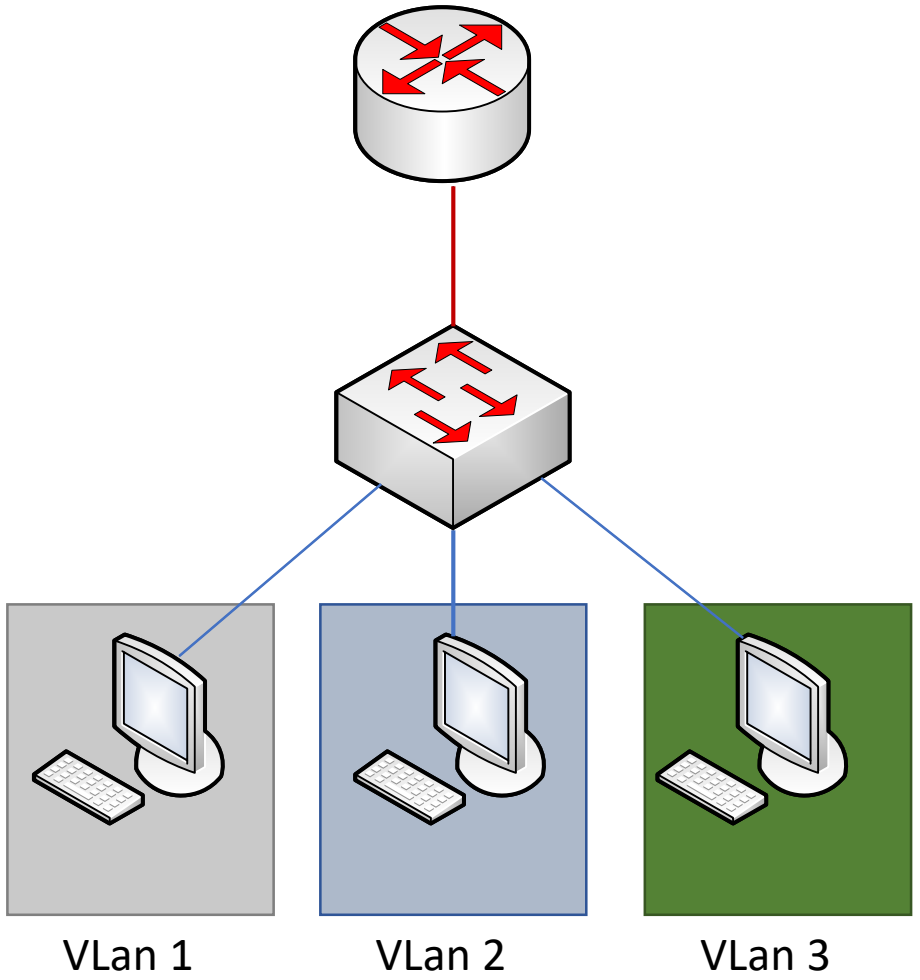
Необходимость VLAN

- До появления технологии VLAN для создания отдельной сети использовались либо физически изолированные сегменты коаксиального кабеля, либо не связанные между собой сегменты, построенные на повторителях и мостах.
- Затем эти сети связывались маршрутизаторами в единую составную сеть
- Изменение состава сегментов (переход пользователя в другую сеть, дробление крупных сегментов) при таком подходе подразумевает физическую перекоммутацию разъемов на передних панелях повторителей или на кроссовых панелях, что не очень удобно в больших сетях — это требует объемной физической работы, к тому же высока вероятность ошибки.

Виртуальные сети на базе одного коммутатора

- При создании виртуальных сетей на основе одного коммутатора обычно используется механизм группирования портов коммутатора.
- При этом каждый порт приписывается той или иной виртуальной сети. Кадр, пришедший от порта, принадлежащего, например, виртуальной сети 1, никогда не будет передан порту, который не принадлежит этой виртуальной сети.
- Порт можно приписать нескольким виртуальным сетям, хотя на практике так делают редко — пропадает эффект полной изоляции сетей.

Виртуальные сети на базе одного коммутатора



Виртуальные сети на базе одного коммутатора

- Второй способ образования виртуальных сетей основан на группировании MAC-адресов.
- Каждый MAC-адрес, который изучен коммутатором, приписывается той или иной виртуальной сети.
- При существовании в сети множества узлов этот способ требует от администратора большого объема ручной работы и по этой причине не получил распространения.

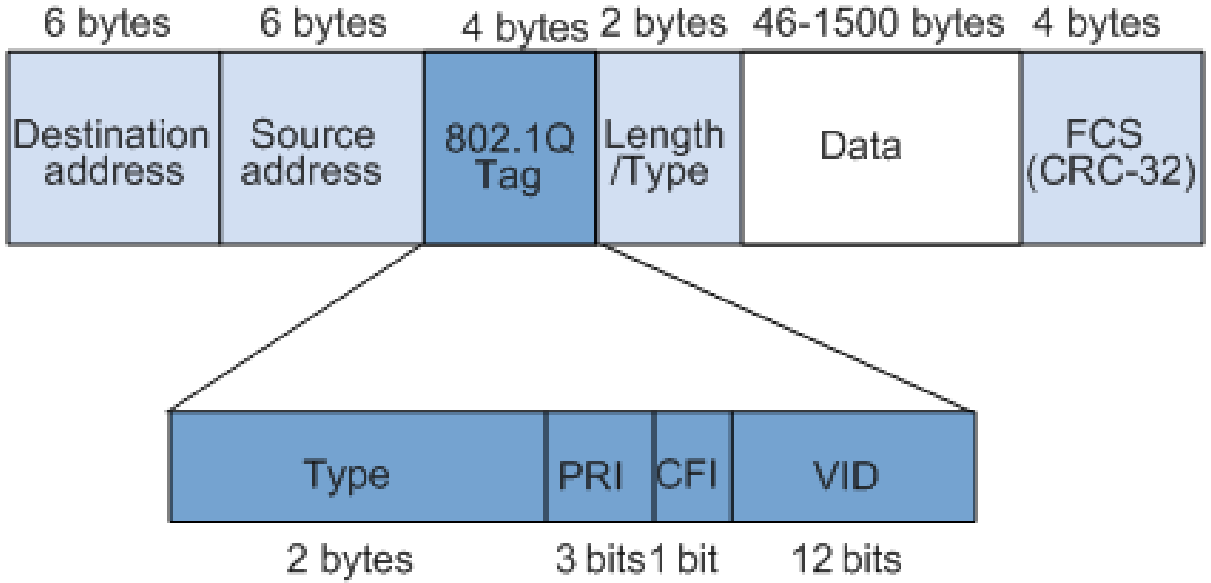
Виртуальные сети на базе нескольких коммутаторов

- Если узлы какой-либо виртуальной сети подключены к разным коммутаторам, то для подключения каждой такой сети на коммутаторах должна быть выделена специальная пара портов.
- В противном случае, если коммутаторы будут связаны только одной парой портов, информация о принадлежности кадра той или иной виртуальной сети при передаче из коммутатора в коммутатор будет утеряна.
- Таким образом, коммутаторы с группированием портов требуют для своего соединения столько портов, сколько виртуальных сетей они поддерживают.
- Порты и кабели используются в этом случае очень расточительно. Кроме того, при соединении виртуальных сетей через маршрутизатор для каждой виртуальной сети выделяются отдельные кабель и порт маршрутизатора, что также приводит к большим накладным расходам.

IEEE 802.1Q

- До принятия стандарта IEEE 802.1Q существовало много фирменных протоколов этого типа, но все они имели один недостаток — оборудование различных производителей при образовании VLAN оказывалось несовместимым.
- Вводит понятие **тега виртуальной локальной сети,** который состоит из поля TCI (Tag Control Information — управляющая информация тега) размером в 2 байта и предшествующего ему поля EtherType, которое является стандартным для кадров Ethernet и также состоит из 2 байтов.

Формат пакета тега 802.1Q



Формат пакета тега 802.1Q

- Тег VLAN не является обязательным для кадров Ethernet. Кадр, у которого имеется такой заголовок, называют помеченным (tagged frame).
- Коммутаторы могут одновременно работать как с помеченными, так и с непомеченными кадрами. Из-за добавления тега VLAN максимальная длина поля данных уменьшилась на 4 байта.
- Чтобы оборудование локальных сетей могло отличать и понимать помеченные кадры, для них введено специальное значение поля EtherType, равное 0x8100.
- Это значение говорит о том, что за ним следует поле TCI, а не стандартное поле данных. Обратите внимание, что в помеченном кадре за полями тега VLAN следует другое поле EtherType, указывающее тип протокола, данные которого переносятся полем данных кадра.

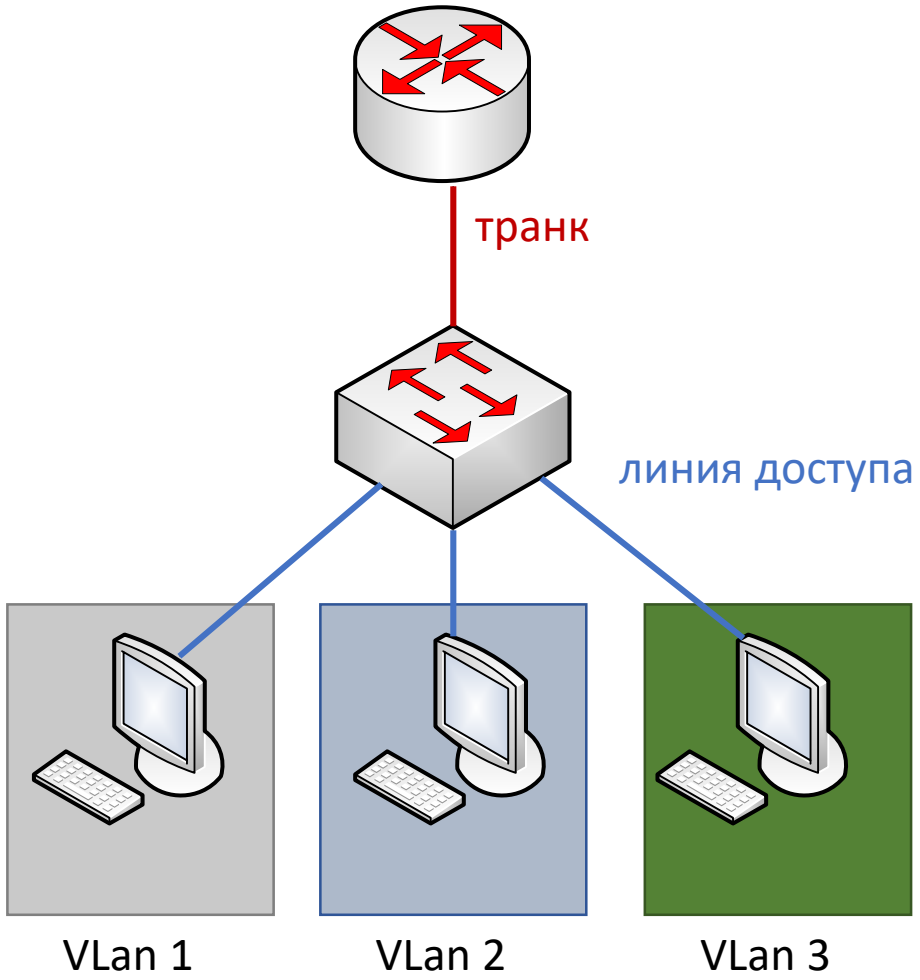
Формат пакета тега 802.1Q

- В поле TCI находится 12-битное поле номера (идентификатора) VLAN, называемого VID.
- Разрядность поля VID позволяет коммутаторам создавать до 4096 виртуальных сетей.
- Помимо этого, в поле TCI помещено трехбитное поле приоритета кадра.
- Однобитное поле CFI было введено с целью поддержания специального формата кадра Token Ring, для сетей Ethernet оно должно содержать значение 0. Пользуясь значением VID в помеченных кадрах, коммутаторы сети выполняют групповую фильтрацию трафика, разбивая сеть на виртуальные сегменты, то есть на VLAN.
- Для поддержки этого режима каждый порт коммутатора приписывается к одной или нескольким виртуальным локальным сетям, то есть выполняется группировка портов.
- Поле приоритета предназначено для согласованного обеспечения качества обслуживания (QoS) различных классов трафика. Всего может поддерживаться до 8 классов трафика (это определяется тремя битами поля)

Конфигурирование VLan

- Линия доступа связывает порт коммутатора (называемый в этом случае портом доступа) с конечным узлом (компьютером, мобильным устройством и т. п.), принадлежащим некоторой виртуальной локальной сети.
- Предполагается, что конечный узел работает с непомеченными кадрами, то есть структура VLAN для него прозрачна.
- Транк — это линия связи, которая соединяет между собой порты двух коммутаторов; в общем случае через транк передается трафик нескольких виртуальных сетей.

Конфигурирование VLan



Конфигурирование VLan

- Коммутаторы, поддерживающие технику VLAN, без специального конфигурирования по умолчанию работают как стандартные коммутаторы, обеспечивая соединения всех совсеми.
- В сети, образованной такими коммутаторами, все конечные узлы по умолчанию относятся к условной сети VLAN1 с идентификатором VID, равным 1.
- Все порты этой сети, к которым подключены конечные узлы, по определению являются портами доступа.
- Сеть VLAN1 можно отнести к виртуальным локальным сетям лишь условно, так как по ней передаются непомеченные кадры. Условная сеть VLAN также называется сетью VLAN, предлагаемой по умолчанию (default VLAN), или естественной (native VLAN).

Конфигурирование VLan

- Чтобы образовать в исходной сети виртуальную локальную сеть, нужно в первую очередь выбрать для нее значение идентификатора VID, отличное от 1, а затем, используя команды конфигурирования коммутатора, приписать к этой сети те порты, к которым присоединены включаемые в нее компьютеры.
- Порт доступа может быть приписан только к одной виртуальной локальной сети.
- Порты доступа получают от конечных узлов сети непомеченные кадры, маркируя их тегом VLAN, содержащим то значение VID, которое назначено этому порту.
- При передаче же помеченных кадров конечному узлу порт доступа удаляет тег виртуальной локальной сети.

Гибкое конфигурирование портов

- В этой схеме порте порты не делятся на транки и порты доступа, каждый порт может быть гибко сконфигурирован для специфической поддержки кадров VLAN в зависимости от потребностей сети.

Гибкое конфигурирование портов

- **Принимать только непомеченные кадры.** В этом случае режим соответствует режиму порта доступа.
- **Принимать только помеченные кадры.** При этом порту могут быть приписаны один или несколько номеров VLAN. Этот режим соответствует избирательному режиму работы транка. Помеченные кадры передаются без отбрасывания/добавления тега VLAN.
- **Принимать как помеченные, так и непомеченные кадры.** Непомеченные кадры всегда принадлежат естественной сети VLAN1 (некоторые модели коммутаторов позволяют администратору назначить естественной сети VLAN произвольный номер, отличный от 1). Порту может быть приписан один или несколько номеров VLAN.

Автоматизация конфигурирования VLan

- В сети, состоящей из большого количества коммутаторов и не разделенной на подсети маршрутизаторами, полностью ручное конфигурирование VLAN может приводить к ошибкам из-за несогласованности информации об активных сетях VLAN на различных коммутаторах, особенно если их конфигурируют разные администраторы.
- Существует несколько протоколов, позволяющих частично автоматизировать конфигурирование VLAN в сети.

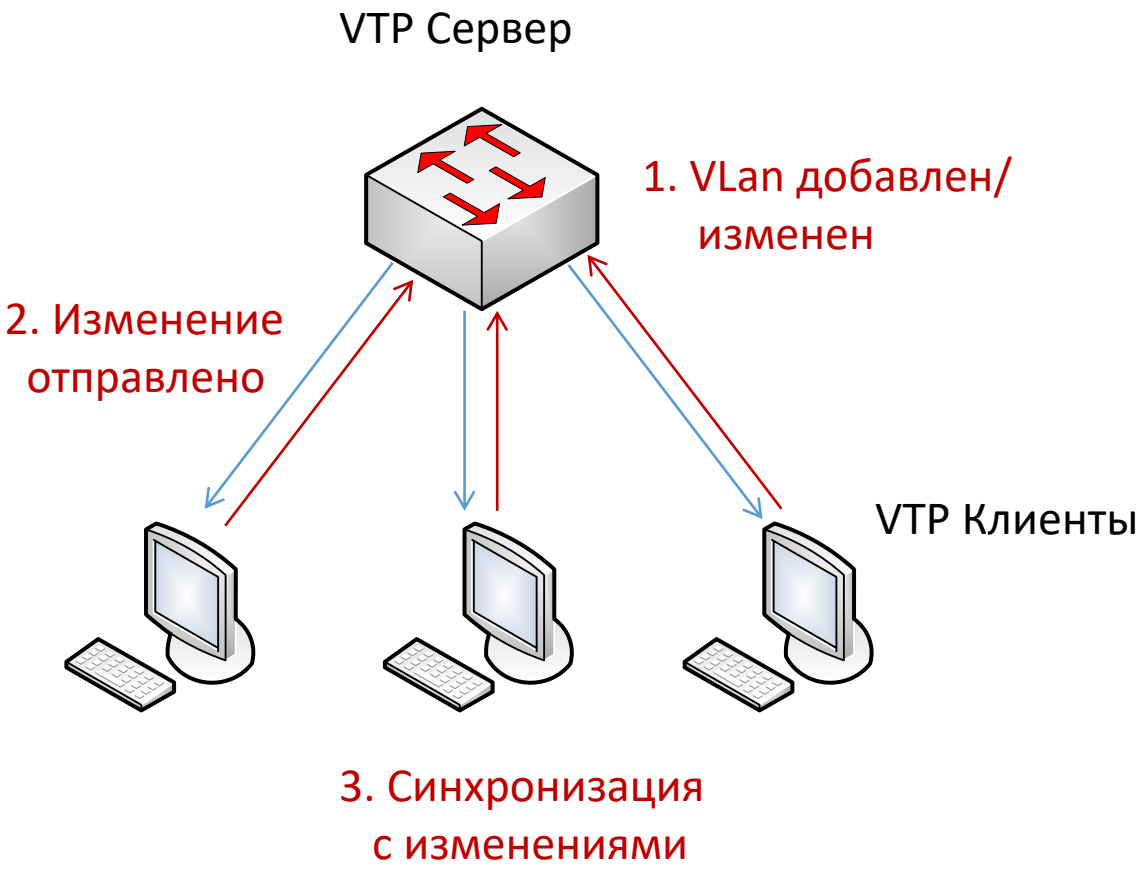
VTP

- Является проприетарным протоколом компании Cisco и работает только на ее коммутаторах.
- Коммутаторы Cisco поддерживают модель «транк — линии доступа», а протокол VTP позволяет по транковым связям передавать информацию о сетях VLAN, активизированных на одном из коммутаторов, другим коммутаторам сети.
- Поэтому достаточно добавить (или удалить) VLAN на одном из коммутаторов сети, после чего все остальные коммутаторы сети получат информацию о добавлении (удалении) VLAN с данным номером и произведут соответствующие изменения в своих конфигурационных записях.

VTP

- Для удобства администрирования больших сетей существует понятие домена — все сообщения протокола VTP воспринимаются коммутаторами только одного и того же домена (имя домена и его пароль конфигурируются на каждом коммутаторе вручную).
- Приписывание VLAN порту доступа по-прежнему выполняется вручную.
- Порты, работающие в режиме транка, приписывают номера VLAN к транку (работающему в избирательном режиме) динамически. Автоматически выполняется отсечение номера VLAN для транков некоторого домена, если в данном домене этот номер не приписан ни одному из его портов доступа (это свойство называется VTP pruning).

VTP


VTP Сервер
1. VLan добавлен/
изменен
2. Изменение
отправлено
VTP Клиенты
3. Синхронизация
с изменениями

GARP

- Является одним из двух по пулярных приложений протокола GARP (Generic Attribute Registration Protocol).
- Протокол GARP был разработан рабочей группой IEEE 802.1 для того, чтобы коммутаторы локальной сети могли сообщать друг другу (регистрировать в сети) различные атрибуты.

MRP (Multiple Registration Protocol)

- Протокол GARP обладал несколькими существенными недостатками — в больших сетях он порождал большое количество служебного трафика, кроме того, процесс установления новой конфигурации мог длиться слишком долго из-за нескольких обязательных тайм-аутов.
- Поэтому в 2007 году группа IEEE 802.1 заменила GARP протоколом MRP (Multiple Registration Protocol).
- Соответственно протокол MVRP заменил GVRP. За счет изменения формата сообщений и логики обмена ими служебный трафик был сокращен, а время установления новой конфигурации уменьшено.

MPLS

- Одна из самых перспективных транспортных технологий, объединяющих технику виртуальных каналов с функциональностью стека TCP/IP.
- Главное достоинство MPLS видится сегодня многим специалистам в способности предоставлять разнообразные транспортные услуги в IP-сетях, в первую очередь —услуги виртуальных частных сетей.
- Эти услуги отличаются разнообразием, они могут предоставляться как на сетевом, так и на канальном уровне.

MPLS

- Дейтаграммное продвижение реализуется протоколом IP — он работает точно так же, как и в традиционном IP-маршрутизаторе, при этом таблица маршрутизации может создаваться как вручную, так и протоколами маршрутизации стека TCP/IP.
- В то же время в этом коммуникационном устройстве, называемом маршрутизатором с коммутацией по меткам (Label Switch Router, LSR), имеется второй модуль продвижения, работающий в соответствии с техникой коммутации виртуальных каналов, который здесь называется модулем коммутации по меткам

MPLS

- Оба модуля продвижения управляются одним и тем же слоем управления LSR, куда наряду с традиционными протоколами IP-маршрутизации, такими как RIP, OSPF, IS-IS и BGP, входят и новые протоколы, называемые сигнальными.
- Сигнальные протоколы нужны для автоматического установления в сети виртуального пути, называемого в технологии MPLS путем коммутации по меткам (Label Switching Path, LSP).
- Наличие общего слоя управления позволяет LSR гибко использовать наличие двух модулей продвижения — одну часть потоков данных он может продвигать, применяя технику IP-продвижения, а другую — технику коммутации по меткам. Слой управления имеет информацию о топологии сети, необходимую для работы каждого уровня продвижения.

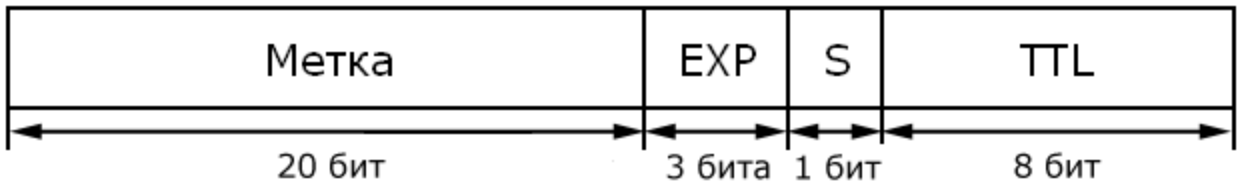
Класс эквивалентности продвижения (FEC)

- Forwarding Equivalence Class - группа IP-пакетов, имеющих одни и те же требования к условиям транспортировки (транспортному сервису).
- Все пакеты, принадлежащие к данному классу, продвигаются через MPLS-сеть по одному виртуальному пути LSP.

Примеры классов эквивалентности продвижения

- **На основании IP-адреса назначения.** Это наиболее близкий к принципам работы IP-сетей подход, который состоит в том, что для каждого префикса сети назначения, имеющегося в таблице LER-маршрутизации, создается отдельный класс FEC. Протокол LDP, полностью автоматизирует процесс создания классов FEC по этому способу.
- **В соответствии с требованиями инжиниринга трафика.** Классы выбираются таким образом, чтобы добиться баланса загрузки каналов сети.
- **В соответствии с требованиями VPN**. Для конкретной виртуальной частной сети клиента создается отдельный класс FEC.
- **По типам приложения.** Например, трафик IP-телефонии (RTP) составляет один класс FEC, а веб-трафик — другой.
- **По интерфейсу**, с которого получен пакет.
- **По MAC-адресу назначения кадра**, если это кадр Ethernet.

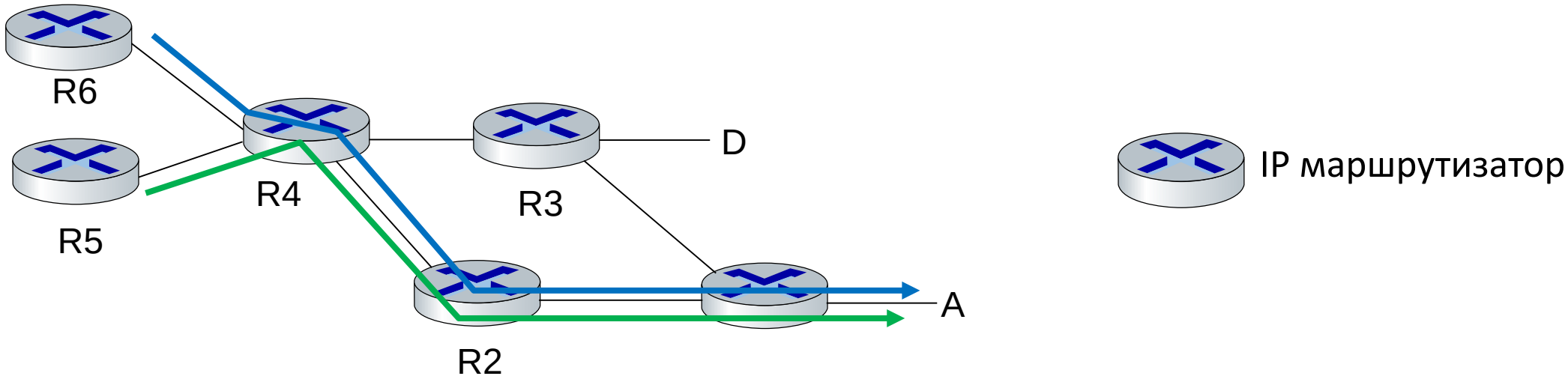
Формат заголовка MPLS



Формат пакета MPLS

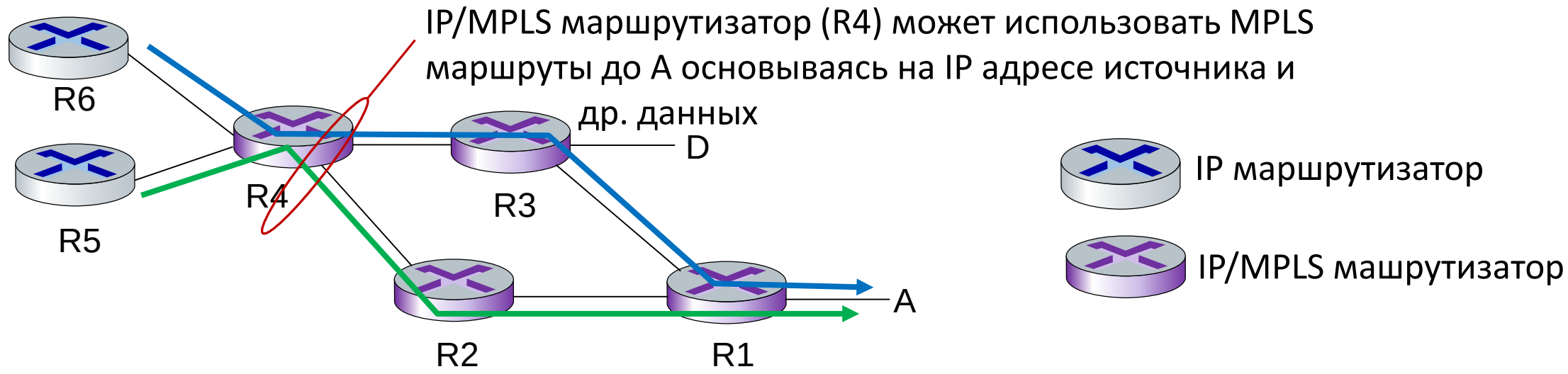
- **Метка (20 бит)**. Используется для выбора соответствующего пути коммутации по меткам.
- **Время жизни (TTL)**. Данное поле, занимающее 8 бит, дублирует аналогичное поле IP-пакета. Это необходимо для того, чтобы устройства LSR могли отбрасывать «заблудившиеся» пакеты только на основании информации, содержащейся в заголовке MPLS, не обращаясь к заголовку IP.
- **Класс услуги (Class of Service, CoS)**. Поле CoS, занимающее 3 бита, первоначально было зарезервировано для развития технологии, но в последнее время используется в основном для указания класса трафика, требующего определенного уровня QoS.
- **Признак дна стека меток.** Этот признак (S) занимает 1 бит.

MPLS и IP



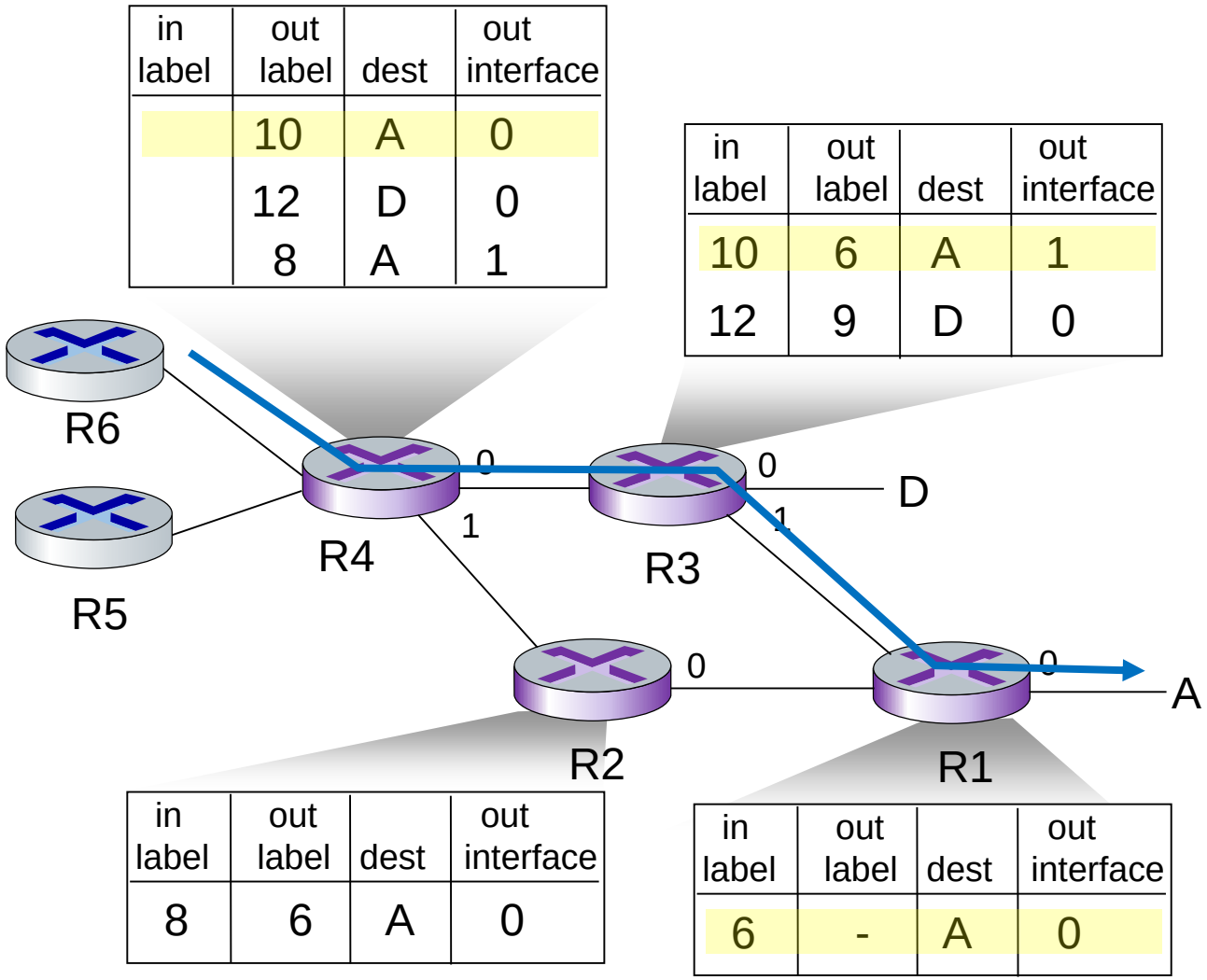
- IP маршрутизация: путь до целевого узла определяется только адресом целевого узла

MPLS и IP



- IP маршрутизация: путь до целевого узла определяется только адресом целевого узла
- MPLS маршрутизация: путь к целевому узлу может быть основан на адресе источника и адресе целевого узла
  - *быстрая перестройка:* предварительное вычисление резервных маршрутов в случае потери канала

MPLS


in label
out label
dest
out interface
10
A
0
12
D
0
8
A
1
in label
out label
dest
out interface
10
6
A
1
12
9
D
0
R6
R5
R4
R3
R2
R1
0
1
0
1
0
0
D
A
in label
out label
dest
out interface
8
6
A
0
in label
out label
dest
out interface
6
-
A
0

Ограничения коммутаторов

- Серьезные ограничения по-прежнему накладываются на топологию коммутируемой локальной сети.
- Требование отсутствия петель преодолевается с помощью техники STP и аналогов и агрегирования каналов лишь частично.
- STP не позволяет задействовать все альтернативные маршруты для передачи пользовательского трафика, а агрегирование каналов разрешает так делать только на участках сети между двумя соседними коммутаторами.
- Подобные ограничения не позволяют применять многие эффективные топологии, пригодные для передачи трафика.

Ограничения коммутаторов

- Логические сегменты сети, расположенные между коммутаторами, слабо изолированы друг от друга, а именно — не защищены от широковещательных штормов.
- Использование же механизма виртуальных сетей, реализованного во многих коммутаторах, хотя и позволяет достаточно гибко создавать изолированные по трафику группы станций, изолирует их полностью, то есть так, что узлы одной виртуальной сети не могут взаимодействовать с узлами другой виртуальной сети.

Ограничения коммутаторов

- В сетях, построенных на основе мостов и коммутаторов, достаточно сложно решается задача фильтрации трафика на основе данных, содержащихся в пакете.
- В таких сетях фильтрация выполняется только с помощью пользовательских фильтров, для создания которых администратору приходится иметь дело с двоичным представлением содержимого пакетов.

Ограничения коммутаторов

- Реализация транспортной подсистемы только средствами физического и канального уровней приводит к недостаточно гибкой одноуровневой системе адресации, в качестве адреса назначения используется MAC-адрес, жестко связанный с сетевым адаптером.

Ограничения коммутаторов

- У коммутаторов ограничены возможности по трансляции протоколов при создании гетерогенной сети.
- Они не могут транслировать протоколы WAN в протоколы LAN из-за различий в системе адресации этих сетей, а также различных значений максимального размера поля данных.

Использованные источники

- В. Олифер, Н. Олифер “Компьютерные сети. Принципы, технологии, протоколы”
- Д. Куроуз, К. Росс “Компьютерные сети. Нисходящий подход.”
- https://techhub.hpe.com/eginfolib/networking/docs/switches/RA/15-18/5998-8151_ra_2620_asg/content/ch10s05.html