MAC адрес. Формат кадра.

Технология Token Ring. Для чего MSAU. Что такое маркерный доступ. Основные скорости передачи. Приоритеты.

Технология FDDI. Зачем двойное кольцо. Размер сети. Скорость передачи.

1. **Доступ к среде CSMA/CD. Технология Ethernet. Что такое двойной экспоненциальный откат. Что такое коллизия. Почему есть ограничение на минимальный размер кадра.**

В сетях Ethernet используется метод доступа к среде передачи данных, называемый методом коллективного доступа с опознаванием несущей и обнаружением коллизий (CSMA/CD).

Этот метод используется исключительно в сетях с общей шиной. Все компьютеры такой сети имеют непосредственный доступ к общей шине, поэтому она может быть использована для передачи данных между любыми двумя узлами сети. Простота схемы подключения – один из факторов, определивших успех стандарта Ethernet. Говорят, что кабель, к которому подключены все станции, работает в режиме коллективного доступа (MA).

Все данные, передаваемые по сети, помещаются в кадры определенной структуры и снабжаются уникальным адресом станции назначения. Затем кадр передается по кабелю. Все станции, подключенные к кабелю, могут распознать факт передачи кадра, и та станция, которая узнает собственный адрес в заголовках кадра, записывает его содержимое в свой внутренний буфер, обрабатывает полученные данные и посылает по кабелю кадр-ответ. Адрес станции-источника также включен в исходный кадр, поэтому станция-получатель знает, кому нужно послать ответ.

При описанном подходе возможна ситуация, когда две станции одновременно пытаются передать кадр данных по общему кабелю. Для уменьшения вероятности этой ситуации непосредственно перед отправкой кадра передающая станция слушает кабель (то есть принимает и анализирует возникающие на нем электрические сигналы), чтобы обнаружить, не передается ли уже по кабелю кадр данных от другой станции. Если опознается несущая (CS), то станция откладывает передачу своего кадра до окончания чужой передачи, и только потом пытается вновь его передать. Но даже при таком алгоритме две станции одновременно могут решить, что по шине в данный момент времени нет передачи, и начать одновременно передавать свои кадры. Говорят, что при этом происходит коллизия, так как содержимое обоих кадров сталкивается на общем кабеле, что приводит к искажению информации.

Чтобы корректно обработать коллизию, все станции одновременно наблюдают за возникающими на кабеле сигналами. Если передаваемые и наблюдаемые сигналы отличаются, то фиксируется обнаружение коллизии (CD). Для увеличения вероятности немедленного обнаружения коллизии всеми станциями сети, ситуация коллизии усиливается посылкой в сеть станциями, начавшими передачу своих кадров, специальной последовательности битов, называемой jam-последовательностью.

После обнаружения коллизии передающая станция обязана прекратить передачу и ожидать в течение короткого случайного интервала времени, а затем может снова сделать попытку передачи кадра.

Из описания метода доступа видно, что он носит вероятностный характер, и вероятность успешного получения в свое распоряжение общей среды зависит от загруженности сети, то есть от интенсивности возникновения в станциях потребности передачи кадров.

Метод CSMA/CD определяет основные временные и логические соотношения, гарантирующие корректную работу всех станций в сети:

* Между двумя последовательно передаваемыми по общей шине кадрами информации должна выдерживаться пауза в 9.6 мкс; эта пауза нужна для приведения в исходное состояние сетевых адаптеров узлов, а также для предотвращения монопольного захвата среды передачи данных одной станцией.
* При обнаружении коллизии станция выдает в среду специальную 32-х битную последовательность (jam-последовательность), усиливающую явление коллизии для более надежного распознавания ее всеми узлами сети.
* После обнаружения коллизии каждый узел, который передавал кадр и столкнулся с коллизией, после некоторой задержки пытается повторно передать свой кадр. Узел делает максимально 16 попыток передачи этого кадра информации, после чего отказывается от его передачи. Величина задержки выбирается как равномерно распределенное случайное число из интервала, длина которого экспоненциально увеличивается с каждой попыткой. Такой алгоритм выбора величины задержки снижает вероятность коллизий и уменьшает интенсивность выдачи кадров в сеть при ее высокой загрузке.

Четкое распознавание коллизий всеми станциями сети является необходимым условием корректной работы сети Ethernet. Если какая-либо передающая станция не распознает коллизию и решит, что кадр данных ею верно передан, то этот кадр данных будет утерян, так как информация кадра исказится из-за наложения сигналов при коллизии, он будет отбракован принимающей станцией. Конечно, скорее всего искаженная информация будет повторно передана каким-либо протоколом верхнего уровня, например, транспортным или прикладным, работающим с установлением соединения и нумерацией своих сообщений. Но повторная передача сообщения протоколами верхних уровней произойдет через гораздо более длительный интервал времени (десятки секунд) по сравнению с микросекундными интервалами, которыми оперирует протокол Ethernet. Поэтому, если коллизии не будут надежно распознаваться узлами сети Ethernet, то это приведет к заметному снижению полезной пропускной способности данной сети.

Все параметры протокола Ethernet подобраны таким образом, чтобы при нормальной работе узлов сети коллизии всегда четко распознавались. Именно для этого минимальная длина поля данных кадра должна быть не менее 46 байт (что вместе со служебными полями дает минимальную длину кадра в 72 байта или 576 бит). Длина кабельной системы выбирается таким образом, чтобы за время передачи кадра минимальной длины сигнал коллизии успел бы распространиться до самого дальнего узла сети. Поэтому для скорости передачи данных 10 Мб/с, используемой в стандартах Ethernet, максимальное расстояние между двумя любыми узлами сети не должно превышать 2500 метров.

С увеличением скорости передачи кадров, что имеет место в новых стандартах, базирующихся на том же методе доступа CSMA/CD, например, Fast Ethernet, максимальная длина сети уменьшается пропорционально увеличению скорости передачи. В стандарте Fast Ethernet она составляет 210 м, а в гигабитном Ethernet ограничена 25 метрами.

Независимо от реализации физической среды, все сети Ethernet должны удовлетворять двум ограничениям, связанным с методом доступа:

* максимальное расстояние между двумя любыми узлами не должно превышать 2500 м;
* в сети не должно быть более 1024 узлов.

Кроме того, каждый вариант физической среды добавляет к этим ограничениям свои ограничения, которые также должны выполняться.

Уточним основные параметры операций передачи и приема кадров Ethernet, кратко описанные выше.

Станция, которая хочет передать кадр, должна сначала с помощью MAC-узла упаковать данные в кадр соответствующего формата. Затем для предотвращения смешения сигналов с сигналами другой передающей станции, MAC-узел должен прослушивать электрические сигналы на кабеле и в случае обнаружения несущей частоты 10 МГц отложить передачу своего кадра. После окончания передачи по кабелю станция должна выждать небольшую дополнительную паузу, называемую межкадровым интервалом, что позволяет узлу назначения принять и обработать передаваемый кадр, и после этого начать передачу своего кадра.

Одновременно с передачей битов кадра приемно-передающее устройство узла следит за принимаемыми по общему кабелю битами, чтобы вовремя обнаружить коллизию. Если коллизия не обнаружена, то передается весь кадр, поле чего MAC-уровень узла готов принять кадр из сети либо от LLC-уровня.

Если же фиксируется коллизия, то MAC-узел прекращает передачу кадра и посылает jam-последовательность, усиливающую состояние коллизии. После посылки в сеть jam-последовательности MAC-узел делает случайную паузу и повторно пытается передать свой кадр.

В случае повторных коллизий существует максимально возможное число попыток повторной передачи кадра, которое равно 16. При достижении этого предела фиксируется ошибка передачи кадра, сообщение о которой передается протоколу верхнего уровня.

Для того, чтобы уменьшить интенсивность коллизий, каждый MAC-узел с каждой новой попыткой случайным образом увеличивает длительность паузы между попытками. Временное расписание длительности паузы определяется на основе усеченного двоичного экспоненциального алгоритма отсрочки. Пауза всегда составляет целое число так называемых интервалов отсрочки.

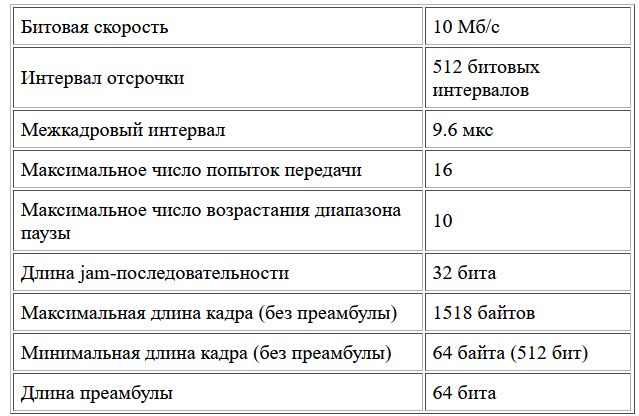
Интервал отсрочки – время, в течение которого станция гарантированно может узнать, что в сети нет коллизии. Это время тесно связано с другим важным временным параметром сети – окном коллизий. Окно коллизий равно времени двукратного прохождения сигнала между самыми удаленными узлами сети – наихудшему случаю задержки, при которой станция еще может обнаружить, что произошла коллизия. Интервал отсрочки выбирается равным величине окна коллизий плюс некоторая дополнительная величина задержки для гарантии:

интервал отсрочки = окно коллизий + дополнительная задержка

В стандартах 802.3 большинство временных интервалов измеряется в количестве межбитовых интервалов, величина которых для битовой скорости 10 Мб/с составляет 0.1 мкс и равна времени передачи одного бита.

Величина интервала отсрочки в стандарте 802.3 определена равной 512 битовым интервалам, и эта величина рассчитана для максимальной длины коаксиального кабеля в 2.5 км. Величина 512 определяет и минимальную длину кадра в 64 байта, так как при кадрах меньшей длины станция может передать кадр и не успеть заметить факт возникновения коллизии из-за того, что искаженные коллизией сигналы дойдут до станции в наихудшем случае после завершения передачи. Такой кадр будет просто потерян.

Время паузы после N-ой коллизии полагается равным L интервалам отсрочки, где L - случайное целое число, равномерно распределенное в диапазоне [0, 2N]. Величина диапазона растет только до 10 попытки, а далее диапазон остается равным [0, 210], то есть [0, 1024].



Учитывая приведенные параметры, нетрудно рассчитать максимальную производительность сегмента Ethernet в таких единицах, как число переданных пакетов минимальной длины в секунду. Количество обрабатываемых пакетов Ethernet в секунду часто используется при указании внутренней производительности мостов и маршрутизаторов, вносящих дополнительные задержки при обмене между узлами. Поэтому интересно знать чистую максимальную производительность сегмента Ethernet в идеальном случае, когда на кабеле нет коллизий и нет дополнительных задержек, вносимых мостами и маршрутизаторами.

Так как размер пакета минимальной длины вместе с преамбулой составляет 64+8 = 72 байта или 576 битов, то на его передачу затрачивается 57.6 мкс. Прибавив межкадровый интервал в 9.6 мкс, получаем, что период следования минимальных пакетов равен 67.2 мкс. Это соответствует максимально возможной пропускной способности сегмента Ethernet в 14880 п/с.

1. **Технология WiFi**

Wi-Fi — технология беспроводной локальной сети с устройствами на основе стандартов IEEE 802.11 (набор стандартов связи для коммуникации в беспроводной локальной сетевой зоне частотных диапазонов 0,9; 2,4; 3,6; 5 и 60 ГГц.). Логотип Wi-Fi является торговой маркой Wi-Fi Alliance. Под аббревиатурой Wi-Fi (от английского словосочетания Wireless Fidelity, которое можно дословно перевести как «беспроводная точность») в настоящее время развивается целое семейство стандартов передачи цифровых потоков данных по радиоканалам. Основными диапазонами Wi-Fi считаются 2.4 ГГц (2412 МГц-2472 МГц) и 5 ГГц (5160-5825 МГц). Сигнал Wi-Fi может передаваться на километры даже при низкой мощности передачи, но для приема Wi-Fi-сигнала с обычного Wi-Fi-маршрутизатора на далеком расстоянии нужна антенна с высоким коэффициентом усиления (например, параболическая антенна или Wi-Fi-пушка).

Любое оборудование, соответствующее стандарту IEEE 802.11, может быть протестировано в Wi-Fi Alliance и получить соответствующий сертификат и право нанесения логотипа Wi-Fi.

Принцип работы:

1. Проводится интернет-кабель.
2. Кабель подключается к роутеру, с помощью которого создается локальная сеть. Без него пользоваться вайфай невозможно.
3. К роутеру по беспроводной сети подключаются различные устройства: ноутбуки, смартфоны, телевизоры и т.д. Создается локальная сеть с выходом в интернет.

Вайфай не равен интернету. Технология создает локальную сеть, в которой разные устройства могут обмениваться данными без выхода во Всемирную сеть. При подключении к провайдеру устройства этой сети получают доступ в интернет.

Отсюда вывод: Wi-Fi сеть – это локальная сеть из устройств, подключенных по беспроводной технологии к маршрутизатору, который и обеспечивает для них выход в интернет. Количество подключаемых устройств ограничивается техническими параметрами роутера.

1. **Доступ к среде CSMA/CA**

CSMA/CA — это сетевой протокол, в котором:

* используется схема прослушивания несущей волны;
* станция, которая собирается начать передачу, посылает jam signal (сигнал затора);
* после продолжительного ожидания всех станций, которые могут послать jam signal, станция начинает передачу фрейма;
* если во время передачи станция обнаруживает jam signal от другой станции, она останавливает передачу на отрезок времени случайной длины и затем повторяет попытку.

CSMA/CA отличается от CSMA/CD тем, что коллизиям подвержены не пакеты данных, а только jam-сигналы. Отсюда и название «Collision Avoidance» — предотвращение коллизий (именно пакетов данных).

Избегание коллизий используется для того, чтобы улучшить производительность CSMA, отдав сеть единственному передающему устройству. Эта функция возлагается на «jamming signal» в CSMA/CA. Улучшение производительности достигается за счёт снижения вероятности коллизий и повторных попыток передачи. Но ожидание jam signal создаёт дополнительные задержки, поэтому другие методики позволяют достичь лучших результатов. Избегание коллизий полезно на практике в тех ситуациях, когда своевременное обнаружение коллизии невозможно — например, при использовании радиопередатчиков.

CSMA/CA – основной метод доступа к разделяемой среде, который используется в Wi-Fi. На практике, он работает почти всегда, но теоретически он не решает проблему скрытой и засвеченной станции. Поэтому в Wi-Fi можно использовать другой метод доступа к среде, который называется MACA. Однако этот метод доступа опциональный и используется очень редко. Достоинство метода заключается в том, что он позволяет решить проблему скрытой и засвеченной станций.

В чем состоит протокол MACA? Перед тем как передавать кадры с данными, компьютер должен отправить короткое управляющие сообщение, которое называется RTS. В этот запрос включается размер данных, который компьютер хочет передать и получатель в ответ, если он готов принимать данные, отправляет такое же короткое управляющие сообщение, которое называется сеть CTS. И опять же в это сообщение включается размер данных, которые компьютер готов принять. Другие компьютеры, которые получили сообщение CTS ждут, когда закончится передача данных, они знают сколько времени потребуется на передачу данных, так как размер данных включен в сообщение CTS, и знают сколько времени нужно на передачу подтверждения.

1. **Difs, sifs, pifs интервалы**

<https://intuit.ru/studies/courses/1004/202/lecture/5238?page=1>

1. **Фреймы ACK, RST, CST**

Фрейм Запрос на Отправку (Request to Send (RTS) frame)

Функция RTS/CTS является опциональной и разработана для уменьшения количества коллизий при пересылке фреймов, когда присутствуют скрытые устройства c Wi-Fi, имеющие ассоциацию с той же точкой доступа (пример: в зоне покрытия точки доступа есть мощная капитальная стена и два смартфона с двух сторон прекрасно слышат эту точку, но не слышат друг друга). Мобильные устройства отправляют RTS фрейм к другому устройству, как первую фазу в двухшаговом процессе, необходимом до отправки фрейма данных. По сути RTC/CTS это механизм отправки вектора NAV, который оповещает все устройства в зоне покрытия точки о том сколько времени будет передаваться фрейм и т.п.

Фрейм подтверждения Чистоты Радиоканала для Отправки (Clear to Send (CTS) frame)

Мобильное устройство (или точка доступа) c WiFi отвечает на фрейм RTS фреймом CTS, подтверждая тем самым для запрашивающего устройства чистоту канала для отправки фрейма данных. Фрейм CTS включает параметр времени, на которое все другие устройства (включая скрытые устройства) не должны передавать какие-либо фреймы в течении периода, который требуется запрашивающему устройству на передачу его фрейма. Данная функция минимизирует коллизии даже при наличии скрытых устройств и ведет к увеличению общей пропускной способности точки доступа при правильной имплементации.

Фрейм Подтверждение (Acknowledgement (ACK) frame)

После получения фрейма данных устройство-получатель c WiFi запускает процесс проверки фрейма на ошибки. Если ошибок не обнаружено, то устройство-получатель будет отправлять фрейм Подтверждение к устройству-отправителю c WiFi. Если устройство-отправитель не получило фрейм Подтверждение после определенного периода времени, то отправитель должен перепослать фрейм заново (в сети стандарта WiFi 802.11 все юникастовые фреймы данных должны быть подтверждены, иначе устройство-отправитель будет перепосылать их заново, снижая тем самым производительность системы).

Все остальные фреймы: <https://komway.ru/texnologii/wi-fi/wi-fi-frames-management-control-data>

1. **Проблемы сокрытой и засвеченной станции**

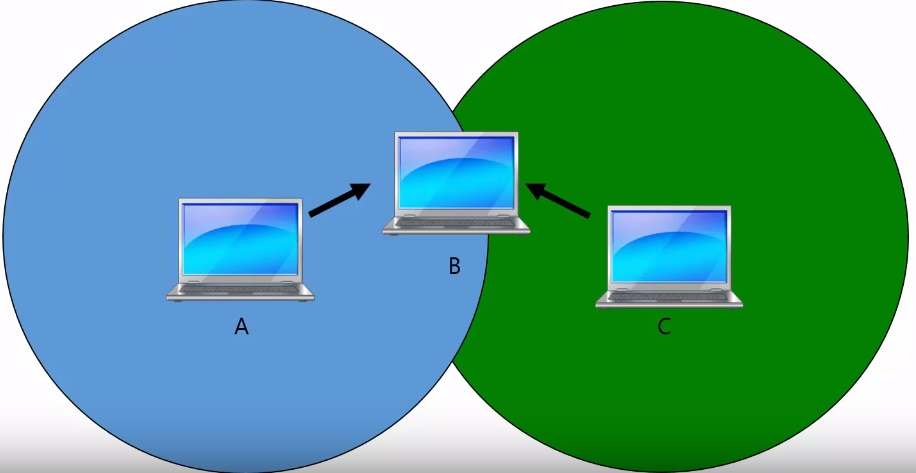
Во-первых, вероятность ошибки передачи данных в беспроводной среде гораздо выше, чем в проводной.

Во-вторых, в беспроводной среде, мощность сигнала, который мы передаем гораздо больше, чем мощность того сигнала, который мы принимаем.

В-третьих, если параметры Ethernet, в частности длина сети специально подобраны так, чтобы сигнал доходил до всех компьютеров, то в Wi-Fi этого обеспечить нельзя. Диапазон работы передатчиков в беспроводной среде ограничен, и поэтому не все компьютеры в сети Wi-Fi могут принимать передаваемые данные. Это приводит к ряду проблем, наиболее известные из которых эта проблема скрытой и засвеченной станции.

Проблема «скрытой» станции

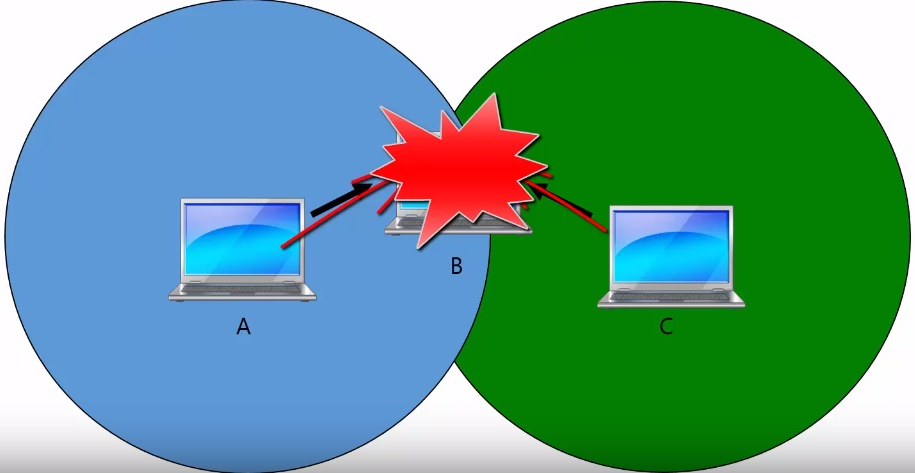
Предположим, что у нас есть три компьютер. Компьютер А и компьютер С хотят передавать данные компьютеру В.



Кругами показаны области действия передатчиков. Сигнал от компьютера А доходит до компьютера В, но не доходит до компьютера С. В Wi-Fi точно также, как и в Ethernet, компьютеры перед тем, как передавать данные, проверяют несущую частоту и смотрят не передает ли кто-то еще данные. И если среда свободна, только в этом случае происходит передача.

Но так как Wi-Fi-зона действия передатчика существенно ограничена, то может произойти следующая ситуация. Компьютер А хочет передать данные компьютеру В. Он проверил, что никто данные не передаёт, и начал передавать данные.

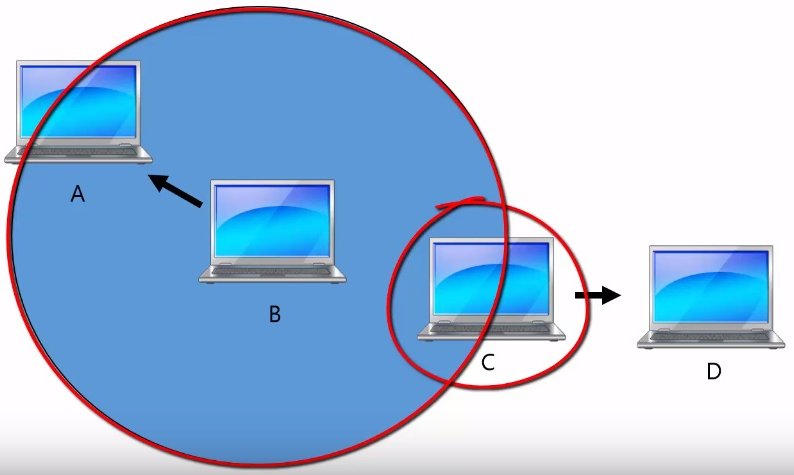
В то же самое время, компьютер С тоже решил передать данные компьютеру В. Но компьютер С находится за зоной действия передатчика от компьютера А. Поэтому там, где находится компьютер С, беспроводная среда свободна, и он решил, что передавать данные можно.



Однако, когда эти данные дошли до компьютера В, они столкнулись с теми данными, которые передавал компьютер А. Произошла коллизия и компьютер В не может принять данные ни от одного компьютера.

Проблема «засвеченной» станции

Проблема засвеченной станции, наоборот, приводит к тому, что компьютер не передаёт данные, хотя может это сделать. Предположим, что у нас есть четыре компьютера. Компьютер В хочет передавать данные компьютеру А, а компьютер С хочет передавать данные компьютеру D.



Компьютер D находится вне зоны действия передатчика компьютера B, поэтому компьютер C может смело передавать данные компьютеру D, однако сам компьютер C находится в зоне действия передатчика компьютера B, поэтому он считает, что среда занята и ждёт, когда компьютер B закончит передачу.

Решение «скрытой» станции

Компьютер A перед тем, как передать данные компьютеру B, высылает сообщение RTS и говорит, что хочет передать 1500 байт. Компьютер B в ответ передает управляющее сообщение CTS и это сообщение получает не только компьютер А, но и компьютер С, который находится вне зоны действия передатчика компьютера А.

Компьютер C понимает, что сейчас другой компьютер, сигнал от которого он не видит, будет передавать данные размером 1500 байт, поэтому он ждёт, когда передача закончится.

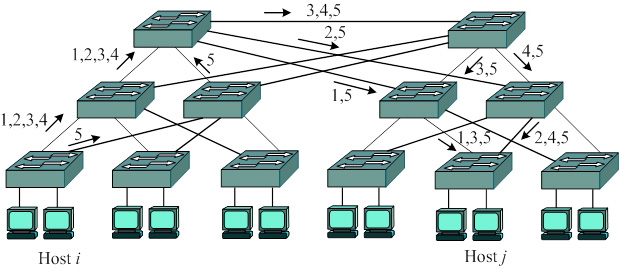
В это время компьютер А может смело передавать данные компьютеру В и быть уверенным, что коллизии не произойдет.

Решение «засвеченной» станции

Компьютер В и компьютер С передают сообщения RTS: компьютер B компьютеру A, а компьютер C компьютеру D. Так как компьютер D находится вне зоны действия передатчика компьютера B, то он считает, что среда свободна и передает компьютеру C сообщение CTS. Компьютер A также передает сообщение CTS компьютеру B. После этого компьютер B и компьютер C могут передавать данные одновременно.

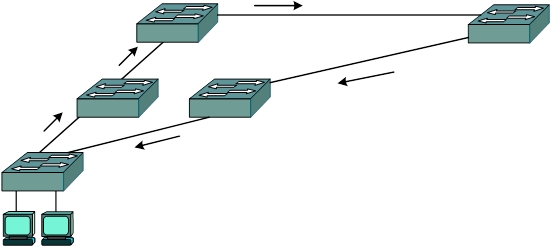
1. **Алгоритм STA**

Многоуровневая схема сети характеризуется избыточными устройствами и соединениями, что обеспечивает высокую надежность. Однако избыточные соединения могут приводить к образованию маршрутных петель, что, в свою очередь, может привести к зацикливанию передаваемых пакетов, широковещательному шторму и падению сети.



От узла Host i до Host j существует 5 различных путей.

Множество путей могут образовывать маршрутные петли, приводящие к зацикливанию кадров в какой-либо петле.



Поэтому к топологии сети предъявляются два противоположных требования:

1. с одной стороны, для повышения надежности необходимы избыточные устройства и маршруты (соединения);
2. с другой стороны, топология сети должна быть древовидной, т.е. не должна иметь маршрутных петель.

Для разрешения этих противоречивых требований был разработан протокол охватывающего (покрывающего) дерева STP, который при наличии избыточных физических соединений прокладывает логические маршруты так, чтобы топология сети была древовидной.

Алгоритм STA, реализующий протокол STP, автоматически выключает избыточные маршруты, образующие маршрутные петли. Избыточные соединения могут быть автоматически активизированы при выходе из строя соединений основного маршрута.

Таким образом, коммутаторы используют алгоритм STA, чтобы перевести в резервное состояние избыточные пути, которые не соответствуют иерархической древовидной топологии. Запасные избыточные пути задействуются, если основные выходят из строя. Протокол STP используется для создания логической иерархии без петель, т.е. при наличии физических петель, логические петли отсутствуют.

При этом топология сети будет древовидной и каждый конечный узел будет характеризоваться единственным путем до главного или корневого коммутатора К. Причем, расстояние от каждого узла до корневого коммутатора будет минимальным.

Алгоритм STA определяет активную конфигурацию сети за три этапа:

1. Сначала в сети определяется корневой мост, от которого строится дерево. Корневой мост может быть выбран автоматически или назначен администратором. При автоматическом выборе корневым становится мост с меньшим значением МАС-адреса его блока управления.
2. Для каждого моста определяется корневой порт – порт, который имеет по сети кратчайшее расстояние до корневого моста (точнее, до любого из портов корневого моста).
3. Для каждого сегмента сети выбирается так называемый назначенный порт – порт, который имеет кратчайшее расстояние от данного сегмента до корневого моста.

После определения корневых и назначенных портов каждый мост блокирует остальные порты, которые не попали в эти два класса портов.

1. **Широковещательный шторм**

Проблема возникновения широковещательного шторма известна практически любому сетевому инженеру или системному администратору. Суть её заключается в том, что в сети распространяется огромное количество широковещательных пакетов, перегружающих каналы и ресурсы сетевого оборудования, что в итоге приводит к сбою в работе сети. Чаще всего причиной шторма является коммутационная петля, которая может быть организована случайно или злонамеренно. В более редких случаях причиной может являться неисправное или неправильно настроенное оборудование, подключаемое к сети.

Эффективная проработка архитектуры сети на стадии проектирования позволит избежать возникновения широковещательного шторма. Можно использовать совместно настройки VLAN, STP и Broadcast Storm Control:

1. VLAN позволяет ограничить распространение шторма внутри одного широковещательного домена. Таким образом, хосты в соседних VLAN, а также каналы, где отсутствует проблемный VLAN, остаются незатронутыми;
2. STP не только защищает сеть в случае возникновения петли, но и позволяет извлечь из этого пользу – дополнительные соединения будут использоваться как резервные каналы в случае отказа основных. Более того, совместно с привязкой к настройкам VLAN, протокол STP позволит организовать распределение трафика по разным каналам между коммутаторами;
3. Broadcast Storm Control – позволяет ограничить максимальную пропускную способность для широковещательного трафика на портах коммутатора.

Наиболее эффективной защитой будет обладать сеть, в которой использованы каждая из перечисленных технологий. Особенно это актуально на границе сети – в портах, куда включается оборудование конечных пользователей или организован стыке другими сетями.

1. **Интеллектуальный коммутатор**

Кроме своего основного назначения – повышения пропускной способности связей – коммутатор позволяет строить изолированные на логическом уровне сегменты сети, потоки информации которых не пересекаются, а также контролировать эти потоки и управлять ими. Этими функциями наделен так называемый интеллектуальный (управляемый) коммутатор.

Организация логически изолированных сетевых сегментов получила название технологии виртуальных локальных сетей (VLAN).

Виртуальной сетью называется группа компьютеров сети, образующих сегмент, трафик которого полностью изолирован от компьютеров других сегментов сети. В то же время внутри виртуальной сети кадры передаются по технологии коммутации, то есть на тот порт, который связан с адресом назначения кадра.

Технология виртуальных сетей позволяет гибко реконфигурировать сеть (менять ее топологию) программным путем, не прибегая к физической реконструкции сети.

Виртуальные сети могут пересекаться, если один или несколько компьютеров входят в состав более чем одной виртуальной сети.

1. **Работа коммутатора в режиме конвейерной передачи кадра**

Коммутаторы могут работать в нескольких режимах, при изменении которых меняются задержка и надежность. Для обеспечения максимального быстродействия коммутатор может начинать передачу кадра сразу, как только получит МАС-адрес узла назначения. Такой режим получил название сквозной коммутации или коммутации «на лету» (конвейерная). Он обеспечивает наименьшую задержку при прохождении кадров через коммутатор. Однако в этом режиме невозможен контроль ошибок, поскольку поле контрольной суммы находится в конце кадра. Следовательно, этот режим характеризуется низкой надежностью.

Во втором режиме коммутатор получает кадр целиком, помещает его в буфер, проверяет поле контрольной суммы и затем пересылает адресату. Если получен кадр с ошибками, то он отбрасывается коммутатором. Поскольку кадр перед отправкой адресату назначения запоминается в буферной памяти, такой режим коммутации получил название коммутации с промежуточным хранением или буферизацией. Таким образом, в этом режиме обеспечивается высокая надежность, но низкая скорость коммутации.

Промежуточное положение между сквозной коммутацией "на лету" и буферизацией занимает режим коммутации свободного фрагмента. В этом режиме читаются первые 64 байта, которые включают заголовок кадра и поле данных минимальной длины. После этого начинается передача кадра до того, как будет получен и прочитан весь кадр целиком. При этом производится верификация адресации и информации LLC-протокола, чтобы убедиться, что данные будут правильно обработаны и доставлены адресату.

Когда используется режим сквозной коммутации "на лету", порты устройств источника и назначения должны иметь одинаковую скорость передачи. Такой режим называется симметричной коммутацией. Если скорости не одинаковы, то кадр должен запоминаться перед тем, как будет передаваться с другой скоростью. Такой режим называется асимметричной коммутацией, при этом должен применяться режим с буферизацией.

Асимметричная коммутация обеспечивает связь между портами с разной полосой пропускания. Данный режим является характерным, например, для потока данных между многими клиентами и сервером, при котором многие клиенты могут одновременно соединяться с сервером. Поэтому на это соединение должна быть выделена широкая полоса пропускания.

1. **MEN (metropolitan ethernet networks)**

Городская вычислительная сеть (Metropolitan area network, MAN) (от англ. «сеть крупного города») объединяет компьютеры в пределах города, представляет собой сеть, по размерам меньшую, чем WAN, но большую, чем LAN.

Самым простым примером городской сети является система кабельного телевидения. Она стала правопреемником обычных антенных сетей в тех местах, где по тем или иным причинам качество эфира было слишком низким. Общая антенна в этих системах устанавливалась на вершине какого-нибудь холма, и сигнал передавался в дома абонентов через кабельные сети.

Когда Интернет стал привлекать к себе массовую аудиторию, операторы кабельного телевидения поняли, что, внеся небольшие изменения в систему, можно сделать так, чтобы по тем же каналам в неиспользуемой части спектра передавались (причём в обе стороны) цифровые данные. С этого момента кабельное телевидение стало постепенно превращаться в MAN.

MAN — это не только кабельное телевидение. Недавние разработки, связанные с высокоскоростным беспроводным доступом в Интернет, привели к созданию других MAN, которые описаны в стандарте IEEE 802.16, описывающем широкополосные беспроводные ЛВС.

MAN (Metropolitan Area Network) — опорная сеть провайдера. То есть точки, связанные скоростными каналами. Расстояние — от 1 до 10 км. Это ещё не WAN, но точно MAN-решения.

MAN применяется для объединения в одну сеть группы сетей, расположенных в разных зданиях. В диаметре такая сеть может составлять от 5 до 50 километров.

Как правило, MAN не принадлежит какой-либо отдельной организации, в большинстве случаев её соединительные элементы и прочее оборудование принадлежит группе пользователей или же провайдеру, кто берёт плату за обслуживание. Об уровне обслуживания заранее договариваются и обсуждают некоторые гарантийные обязательства.

MAN часто действует как высокоскоростная сеть, чтобы позволить совместно использовать региональные ресурсы (подобно большой LAN). Это также часто используется, чтобы обеспечить общедоступное подключение к другим сетям, используя связь с WAN.