

3. КАНАЛЬНЫЙ УРОВЕНЬ

3.1. Назначение канального уровня

Канальный уровень (Data Link Layer – DLL) пересылает данные от узла к узлу в пределах одного физического канала связи [2, 3, 7]. Протоколы канального уровня получают пакеты данных от сетевого уровня, инкапсулируют их в кадры и передают кадры на физический уровень. Канальный уровень в модели OSI стоит на втором месте над физическим уровнем, соответственно, канальный уровень называют также Layer 2, или сокращенно L2.

Обратимся к рис. 3.1. Представим себе, что все узлы, показанные на рисунке, могут обмениваться данными. За доставку данных между различными узлами отвечают службы нескольких уровней модели OSI. В частности, канальный уровень передаёт кадры внутри физических сегментов, обозначенных на рисунке как «Сегмент 1», «Сегмент 2», «Сегмент 3», «Сегмент 4». Указанные сегменты могут быть совершенно разнородными. Например, «Сегмент 1» может быть образован витыми парами, узлы в «Сегменте 2» обмениваются данными при помощи радиоволн, «Сегмент 3» и «Сегмент 4» – оптоволоконные. В каждом из сегментов могут использоваться свои собственные протоколы канального уровня.

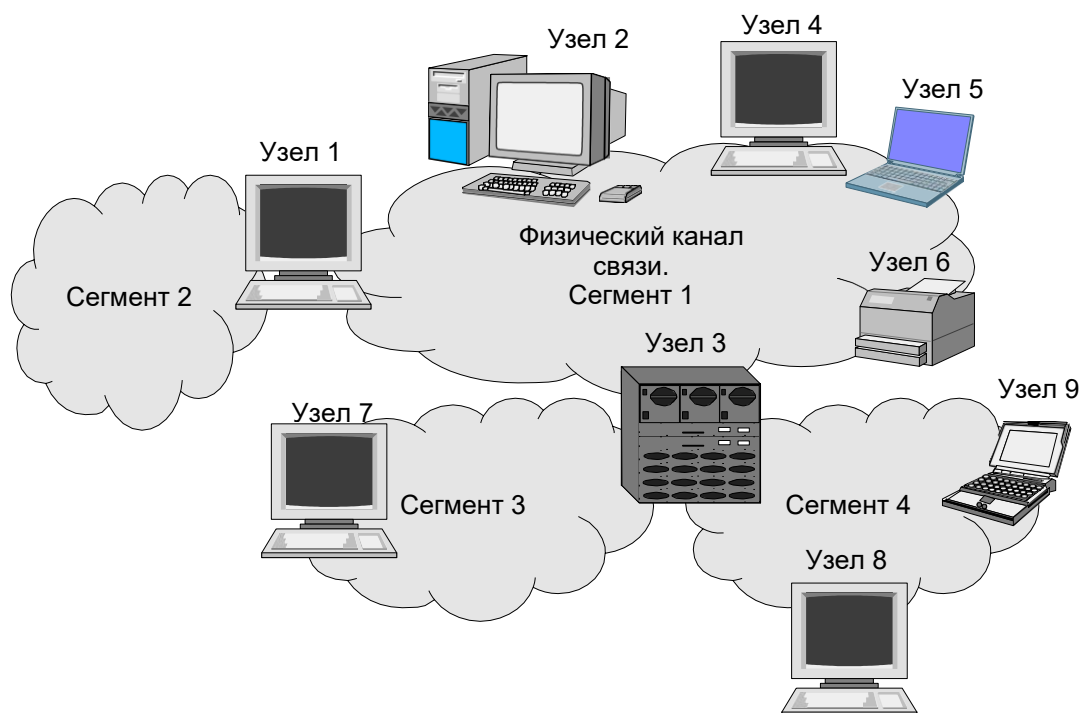


Рис. 3.1. Пример локальной вычислительной сети

Важно отметить, что с точки зрения служб канального уровня, все узлы являются равноправными, не важно, какую именно роль выполняет каждый из узлов. Узел 3 может быть, например, маршрутизатором, Узел 6 – принтером; на первом узле установлена ОС Free BSD, а на пятом – Windows. Канальный уровень ничего об этом «не знает».

Узлы подключаются к каналу передачи данных при помощи сетевых адаптеров (рис. 3.2). Каждый адаптер имеет уникальный сетевой адрес.

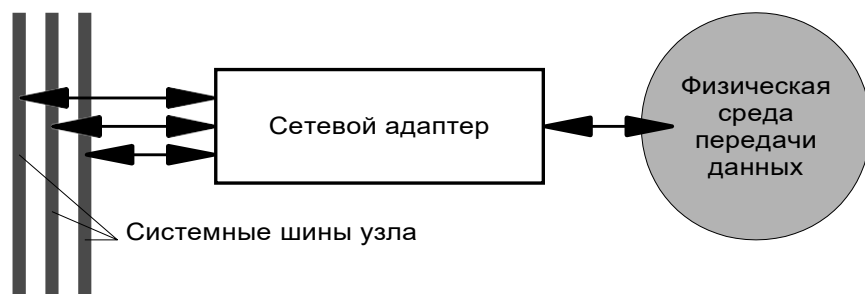


Рис. 3.2. Подключение сетевого адаптера

Канальный уровень формирует кадр данных, состоящий в общем случае из физического адреса получателя, физического адреса отправителя, пакета данных, контрольной суммы (рис. 3.3) [3, 7].

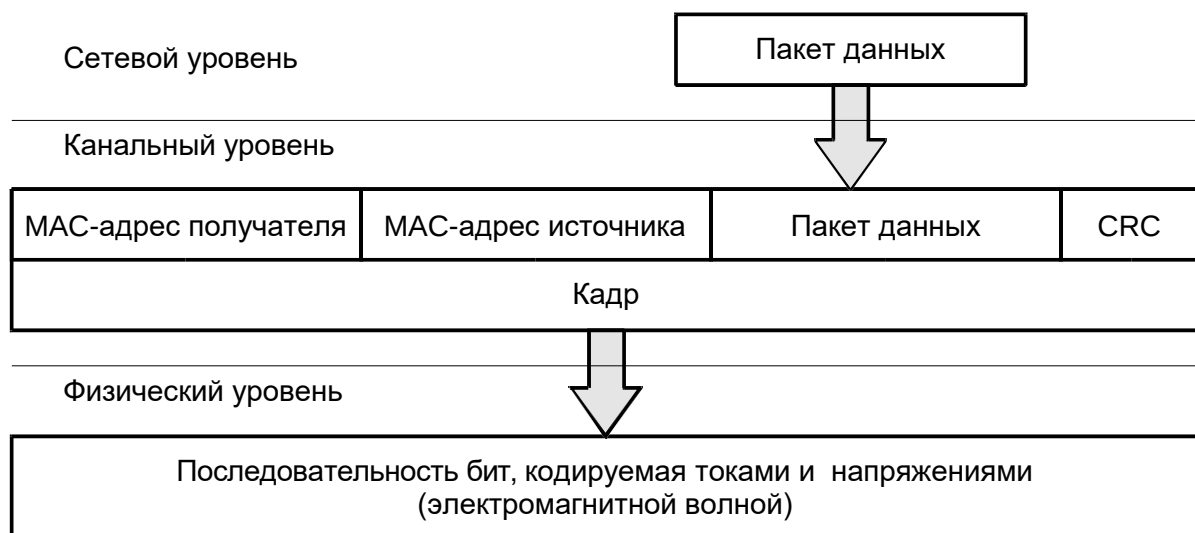


Рис. 3.3. Инкапсуляция данных в кадр

Некоторые протоколы канального уровня отвечают за безошибочную пересылку пакета данных в пределах физического сегмента сети,

поэтому в ряде случаев предусматривается повторная посылка ошибочного кадра. Следует отметить, что целостность данных канальным уровнем поддерживается только локально. Например, информация в Интернет при движении от сервера к пользователю может пройти множество разнородных сетей. Целостность данных при этом гарантирует транспортный уровень.

Протоколы канального уровня строятся исходя из особенностей физической передачи данных и тесно связаны с протоколами физического уровня. Услуги канального уровня в большинстве случаев реализуются аппаратно непосредственно сетевым адаптером. Адаптер является полуавтономным устройством. Он самостоятельно выполняет действия по организации передачи пакетов сетевого уровня от узла к узлу. В качестве среды передачи широко используются витая пара, оптоволокно, радиоэфир (см. п. 2.3).

Часто несколько узлов используют единую физическую среду для передачи данных. При этом каждый узел «слышит» посылки любого другого узла. Понятно, что если посылать данные будут несколько узлов одновременно, то все попытки что-то передать будут обречены на провал. Таким образом канальный уровень должен также обеспечить доступ к физической среде передачи данных. Соответствующие протоколы выделяют в отдельный подуровень управления доступом к среде (Media Access Control – MAC).

3.2. Задачи канального уровня

Протоколы канального уровня решают следующие задачи [1, 3, 7]:

А Формирование кадров. Структура кадра зависит от конкретного используемого протокола.

А Управление доступом к физической среде передачи данных. Сложность данной задачи варьируется от простейшего случая дуплексной связи двух узлов до обеспечения взаимодействия узлов в радиоэфире.

А Обнаружение ошибок при передаче данных. Иногда протоколы канального уровня обеспечивают также исправление ошибок. Следует отметить, что надёжная доставка данных канальным уровнем работает локально, то есть только в пределах одной физической сети.

А Управление потоками данных. Например, с целью предотвращения переполнения входного буфера сетевого адаптера.

3.3. Примеры технологий и стандартов канального уровня

Типовыми примерами стандартов канального уровня являются следующие [3, 7]:

Ethernet (группа стандартов IEEE 802.3)

Технология Ethernet (буквальный перевод «сеть в эфире») на сегодняшний день наиболее широко используется при организации локальных сетей ЭВМ. В качестве физической среды передачи данных может быть использован коаксиальный кабель, витая пара, оптическое волокно.

Wi-Fi (Группа стандартов IEEE 802.11)

Набор стандартов IEEE 802.11 включают в себя протоколы, ориентированные на построение беспроводных сетей. Адаптеры такой сети оборудованы радиопередатчиком и радиоприёмником. Сетевое оборудование, построенное по стандартам IEEE 802.11, распространяется под торговой маркой «Wi-Fi».

PPP

Протокол PPP (Point to Point Protocol) – протокол соединения двух узлов. Содержит целое семейство протоколов, применяемых при соединении двух узлов. В числе прочих включает протоколы проверки пароля и протоколы управления линией связи.

ARP

Протокол ARP (Address Resolution Protocol) – протокол разрешения адресов. Предназначен для получения сетевыми адаптерами таблиц соответствия сетевых адресов (MAC) IP-адресам. ARP позволяет узнать, какому узлу принадлежит тот или иной IP-адрес. Существует также реверсивный протокол разрешения адресов, позволяющий по известному MAC получить IP-адрес.

CSMA, CSMA/CD, CSMA/CA

Технология CSMA (Carrier Sense Multiple Access) – множественный доступ с контролем несущей, CSMA/CD (Carrier Sense Multiple Access / Collision Detection) – множественный доступ с контролем несущей с обнаружением коллизий, CSMA/CA (Carrier Sense Multiple Access / Collision Avoidance) – множественный доступ с контролем несущей с предотвращением коллизий кадров. Данные технологии применяются для организации совместной работы с временным разделением множества узлов, подключенных к одной физической среде.

3.4. Технологии CSMA, CSMA/CD, CSMA/CA

Каким образом можно разделить пропускную способность единой физической среды между отдельными узлами? Отметим, что хотелось бы добиться следующих характеристик передачи данных. Пусть R (бит в секунду) – пропускная способность канала связи, образованного с использованием данной среды. Пусть N – количество узлов, одновременно использующих физическую среду. При работе на передачу одного узла, он должен целиком использовать пропускную способность R . При одновременной работе на передачу $M \leq N$ узлов, на каждый узел должна приходиться пропускная способность канала R/M .

Вспомним существующие в многоканальных системах связи следующие способы разделения каналов:

- 1) частотное;
- 2) временное;
- 3) по форме сигнала (кодовое разделение);
- 4) по характеристикам электромагнитной волны (включая разделение по поляризации и по направлению распространения);
- 5) комбинированное, например, частотно-временное разделение;

Частотное разделение каналов вполне оправдано и принципиально необходимо в радиоэфире. Здесь нужно позаботиться об электромагнитной совместимости сети связи. Передатчики должны излучать радиосигналы только в пределах ограниченной полосы частот, а приёмники – принимать радиосигналы только в этой полосе. Использование частотного разделения в физических средах, образованных такими направляющими системами, как двухпроводная линия связи или витая пара, целесообразно в тех случаях, когда на этих средах функционирует разнородное оборудование (например, аналоговая телефонная связь плюс DSL-модем).

В случае подключения к витой паре нескольких равноправных узлов (с точки зрения канального уровня модели OSI), наиболее приемлемо временное разделение, которое может быть осуществлено с помощью трёх технологий:

1. Технология Demand Priority Access – доступ по приоритету запроса. Используется топология «звезда». Применение кабелей с несколькими витыми парами позволяет реализовать полнодуплексный режим связи. Управление доступом к физической среде осуществляется концентратором, который опрашивает узлы и получает запросы

на передачу данных. В запросе указывается приоритет данных. Концентратор на основе анализа приоритетов выполняет соединение между узлом-источником и узлом получателем.

2. Технология Token Ring. Логически узлы объединены в кольцо. Соседний узел может передавать следующему в кольце специальный кадр, именуемый *маркером*. Узел, «владеющий» в данный момент маркером, монополюет среду передачи. Если узел имеет данные, подготовленные к отправке, он передаёт один или несколько кадров данных, потом пересылает маркер следующему узлу в кольце. Если узлу нечего передавать, то он просто пересылает маркер дальше по кольцу.

Выгоды технологии Token Ring очевидны. Для сети, находящейся в исправном состоянии, имеется гарантированное максимальное время задержки передачи данных. Сложности возникают при отказе одного из узлов кольца. Также необходимы специальные протоколы включения узла в кольцо и отключения узла из кольца. Нужно обратить внимание на то, что если кольцо организовано физически (а не логически), надо принимать специальные меры для поддержания функционирования сети при выходе узла из строя. Накладные расходы на пересылку маркера также снижают эффективность технологии Token ring.

3. Технология CSMA (Carrier Sense Multiple Access) – множественный доступ с контролем «несущей». Рассмотрим эту технологию подробнее. На сегодняшний день широко используются две модификации – доступ с обнаружением коллизий (CSMA/CD) и доступ с предотвращением коллизий (CSMA/CA).

Идеи, положенные в основу технологии CSMA, просты. Во-первых, прежде чем начать передавать данные, узел прослушивает физическую среду. Передача начинается, только тогда, когда все остальные узлы «молчат». Во-вторых, узел не должен «монополизировать» физическую среду. «Сказал» сам – дай «сказать» другому. В-третьих, во время передачи узел также прослушивает среду, чтобы обнаружить *коллизию* – наложение физических сигналов от нескольких узлов. При наличии коллизии передаваемые данные искажаются и передачу необходимо повторить.

Почему вообще возникают коллизии, если узел прослушивает среду, прежде чем начать передачу? На рис. 3.4 показано, как распространяется сигнал в физической среде передачи, если передаёт только один узел (в данном случае – первый).

Видно, что распространение сигнала занимает конечное время. На рис. 3.4 также показан межкадровый интервал IFG – Inter Frame Gap, в течение которого другие узлы могут начать передачу.

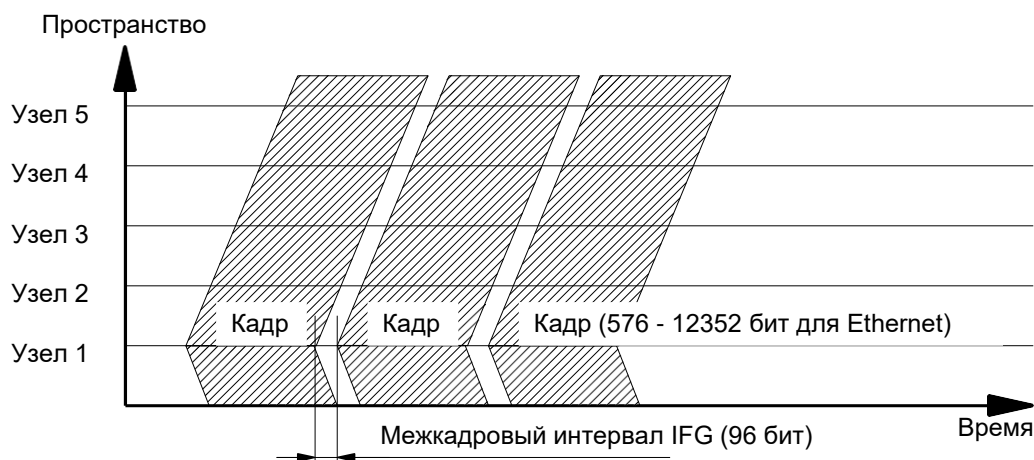


Рис. 3.4. Распространение данных в физической среде передачи [8]

Далее обратимся к рис. 3.5. В момент времени t_1 передачу начал первый узел, в момент времени t_2 четвёртый узел прослушал среду передачи и также начал передавать. В момент t_3 коллизия возникла возле четвёртого узла, в момент t_4 коллизия возникла возле первого узла. Кадры, передаваемые первым и четвёртым узлом, будут потеряны.

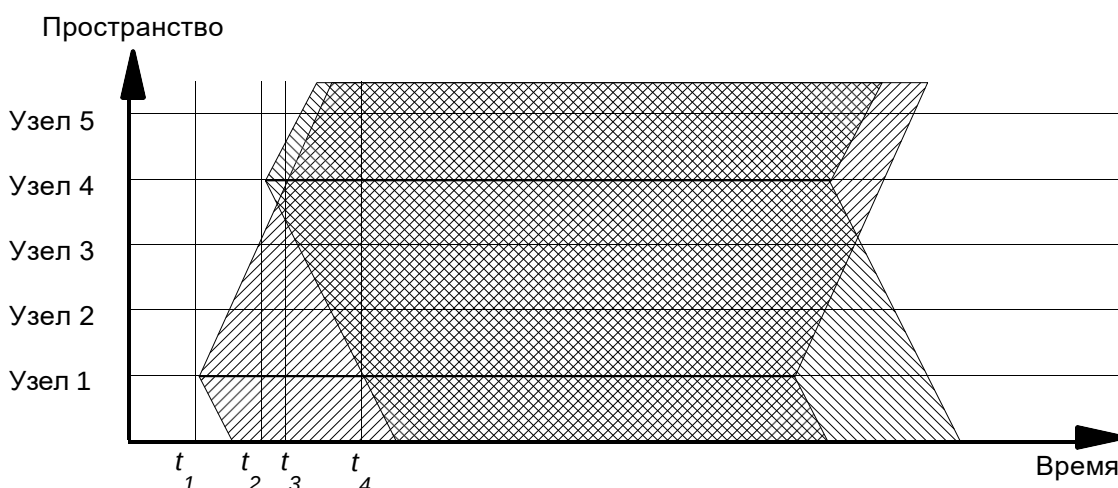


Рис. 3.5. Возникновение коллизии [8]

Для экономии времени и повышения эффективности использования разделяемой физической среды необходимо прервать передачу кадра почти сразу после обнаружения коллизии (рис. 3.6). Несколько

бит передаётся после обнаружения коллизии для того, чтобы остальные узлы также обнаружили, что среда занята и не пытались начать передачу.

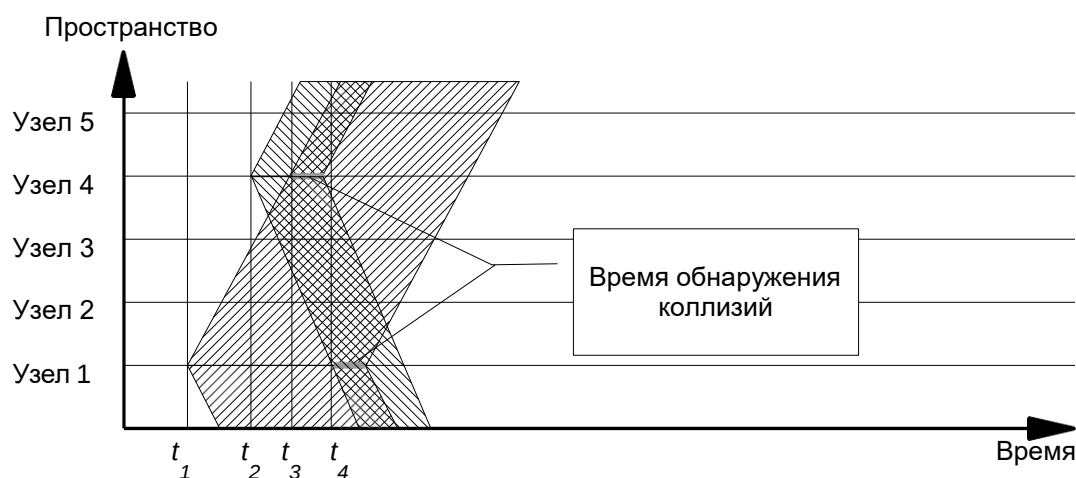


Рис. 3.6. Возникновение коллизии и прерывание передачи [8]

Что делать после коллизии узлу, который имеет непереданный кадр? Нужно немного подождать и опять попробовать начать передачу. Сколько ждать? После обнаружения коллизии узел переходит в фазу *экспоненциального отката*. Если коллизия для данного кадра была обнаружена впервые, то выбирается случайным образом число из ряда (0, 1), это число умножается на время, за которое может быть передано 512 бит (Time Slot – интервал времени). Узел сразу повторяет попытку передачи или ожидает один интервал.

После второй неудачи случайное число выбирается из ряда (0, 1, 2, 3). Узел может выждать до трёх интервалов. После третьей попытки имеется ряд (0, 1, 2, 3, 4, 5, 6, 7). И так далее. В десятой и последующих попытках случайное число выбирается из ряда (0 .. 1023). После 16-ти попыток сетевой адаптер извещает вышестоящий уровень OSI об ошибке сети. На рис. 3.7 представлен примерный алгоритм работы сетевого адаптера по технологии CSMA/CD.

Беспроводные сети (Wireless Networks – WLAN) имеют свои особенности. В нормально функционирующей сети, построенной с использованием направляющих систем, все узлы, входящие в физический сегмент, принимают сигналы друг друга. В радиосети это правило не выполняется, существует *проблема скрытого узла*. Рис. 3.8 иллюстрирует ситуации, при которых узел 2 способен обмениваться

данными с узлами 1 и 3, узлы же 1 и 3 не «слышат» друг друга. В первом случае это обусловлено наличием препятствия для распространения радиоволн.

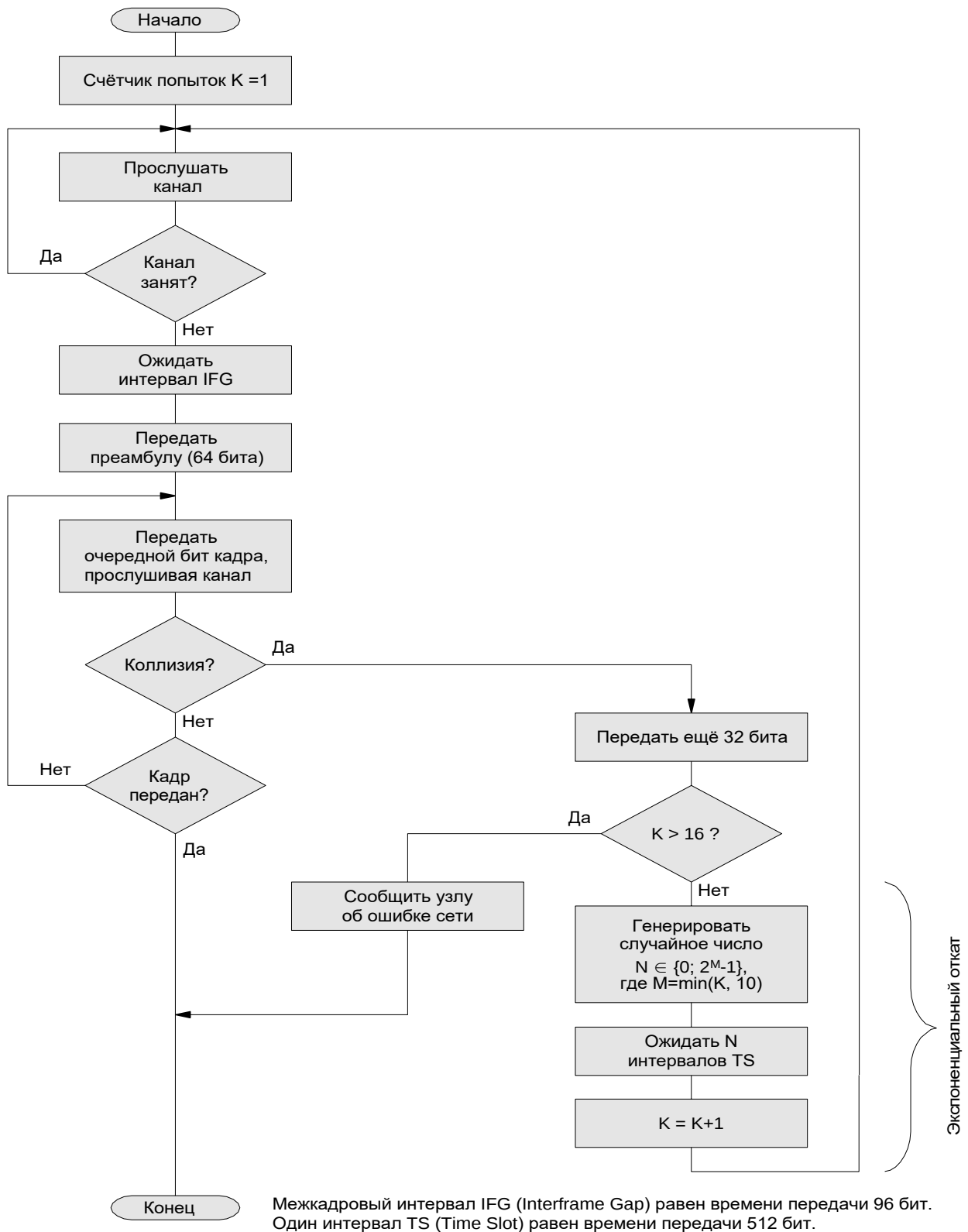


Рис. 3.7. Алгоритм работы сетевого адаптера по технологии CSMA/CD [2, 3]

Во втором – таким расстоянием между узлами 1 и 3, что мощность сигнала оказывается ниже порогового уровня, необходимого для работы приёмника.

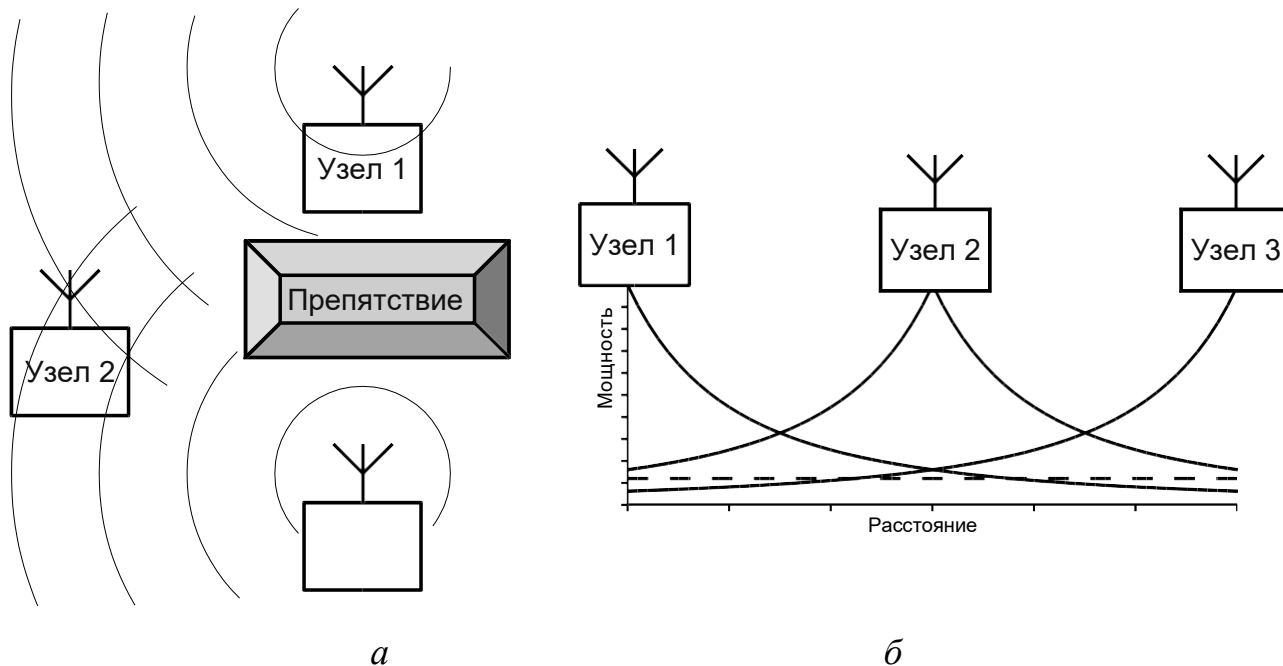


Рис. 3.8. Проблема скрытого узла [2, 3]:

а – при наличии препятствия для радиоволн;

б – с учетом падения мощности при удалении от передатчика

В сетях с радиодоступом применяется технология CSMA/CA (Carrier Sense Multiple Access / Collision Avoidance) – множественный доступ с контролем несущей с предотвращением коллизий кадров. Разберём диаграмму, изображённую на рис. 3.9.

Отметим, что в соответствии со стандартами беспроводных сетей, кадры содержат поле длительности. Таким образом узлы, принимающие передачу, могут определить время занятости канала.

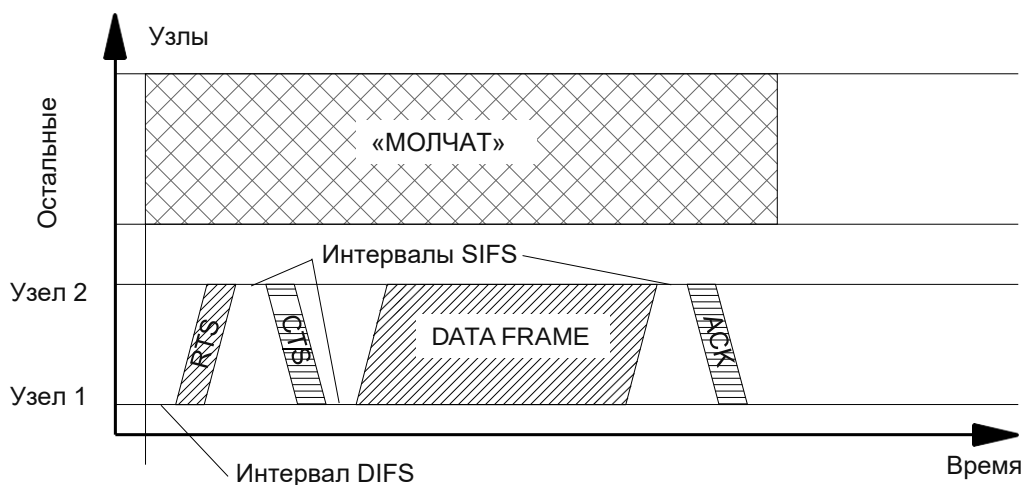


Рис. 3.9. Особенности передачи кадров в радиоэфире [2, 3]

Узел 1 «хочет» передать данные узлу 2. Узел 1 прослушивает эфир в течение интервала DIFS (Distributed coordination function Interframe Space) – межкадрового интервала для протокола распределённой функции координации. При наличии сигнала от других узлов, узел 1 откладывает передачу. Время паузы определяется как произведение случайного числа на длительность интервала Time Slot – стандартного интервала времени (табл. 3.1).

Таблица 3.1

Длительности межкадровых интервалов

Стандарт	Time Slot, мкс	DIFS, мкс	SIFS, мкс
IEEE 802.11b	20	50	10
IEEE 802.11a	9	34	16
IEEE 802.11g	9 или 20	28 или 50	10

Если в течение интервала DIFS узел 1 не обнаруживает мешающих сигналов, то он начинает передачу. Посылка каждого кадра выполняется через интервал времени SIFS (Short Interframe Space) – короткий межкадровый интервал.

Вначале узел 1 передаёт короткий кадр RTS (Request To Send) – запрос на отправку. Узел 2 отвечает коротким кадром CTS (Clear To Send) – разрешение отправки. Теперь узел 1 передаёт кадр данных. Если узел 2 принял данные и проверил CRC, то он отправляет кадр ACK (Acknowledgement Frame) – подтверждение. Явное подтверждение получения данных требуется, так как в сетях с радиодоступом нет гарантии, что узел 2 на протяжении всего кадра данных «слышит» узел 1. Кадры RTS/CTS и ACK не передаются в случае широковещательной посылки. Кадры RTS/CTS также не передаются, если размер кадра данных мал.

Передача кадров RTS/CTS в большинстве случаев позволяет предотвратить коллизии. Длительность кадров RTS/CTS мала, и вероятность коллизии во время их передачи минимальна. Узлы, находящиеся в окружении узла-получателя, принимают кадр CTS и ожидают указанный в поле длительности промежуток времени. Так решается проблема скрытого узла.

3.5. Технология Ethernet

Ethernet на сегодняшний день является самой популярной технологией построения локальных компьютерных сетей [2, 3, 7]. Группа

стандартов Ethernet описывает физические характеристики среды передачи данных, виды и параметры сигналов, характеристики физических интерфейсов. На канальном уровне определяются форматы кадров и протоколы доступа к физической среде передачи данных. Ethernet может использовать разные физические среды для распространения сигнала – коаксиальный кабель, витую пару, оптоволокно.

Ethernet базируется на технологии CSMA. Перед передачей кадра узел обязательно прослушивает «эфир», и только если канал свободен, – начинает передавать. Существует множество вариаций, обеспечивающих передачу данных со скоростями от 10 Мбит/с до 100 Гбит/с. Во всех случаях на канальном уровне используется *кадр Ethernet*.

Структура кадра Ethernet представлена на рис. 3.10. Заметим, что существует несколько разновидностей кадра, продвигаемых различными фирмами. Остановимся на кадре Ethernet II (DIX).

Прослушивание	Преамбула, 64 бита	MAC адрес получателя, 48 бит	MAC адрес источника, 48 бит	Тип кадра, 2 байта	Пакет данных, 46 - 1500 байт	CRC, 32 бита
	Кадр Ethernet II (DIX)					

Рис. 3.10. Структура кадра Ethernet

- Перед информационными полями кадра передаётся *преамбула*, представляющая собой фиксированную последовательность нулей и единиц:

[illegible]

Две последние единички указывают на то, что далее следует адрес получателя. Необходимость преамбулы связана с работой канала связи на физическом уровне. Во время приёма преамбулы сетевые адаптеры выполняют синхронизацию с частотой и фазой посылаемых битов. Пока происходит синхронизация, часть преамбулы может быть потеряна, но это никак не повлияет на правильный приём следующих бит в кадре.

- Поле «адрес получателя» содержит 48-разрядный MAC-адрес получателя. Кадр обрабатывает только тот сетевой адаптер, чей MAC-адрес указан в этом поле. Поле может содержать широковещательный адрес, тогда кадр обрабатывается всеми адаптерами. Также кадр с широковещательным адресом передаётся на все порты коммутаторов.

- Поле «адрес источника» содержит 48-разрядный MAC-адрес источника.

- Поле «тип кадра» указывает на протокол, инкапсулированный в кадре.

- Поле *данных* имеет переменную длину от 46 до 1500 байт. Значение 1500 байт – это максимальная единица передачи в сети Ethernet (MTU – Maximal Transfer Unit). В ряде случаев пакет данных имеет размер больший, чем 1500 байт. Тогда пакет разбивается вышестоящим протоколом на несколько частей. Если размер полезных данных меньше, чем 46 байт (это часто бывает в протоколе ARP), то оставшиеся байты заполняются произвольными данными.

- Поле *CRC* служит для проверки правильности приёма кадра.

Технология Ethernet продолжает бурно развиваться. В июне 2010 года утверждён стандарт IEEE 802.3ba, описывающий Ethernet со скоростями передачи до 100 ГБит/с (по четырём линиям со скоростями 25 ГБит/с). Максимальное расстояние между узлами при использовании одномодового оптоволокна составляет 10 км.

3.6. Сетевые адаптеры и физические адреса

Все узлы, вне зависимости от их типа и выполняемых ими функций, взаимодействуют с физической средой передачи данных посредством сетевых адаптеров. Адаптер физически является набором электронных компонентов (микросхем), связанным с системными шинами узла с одной стороны, и физической средой передачи данных – с другой.

Сетевой адаптер принимает и передаёт физические сигналы, распространяющиеся в среде передачи данных. Это могут быть немодулированные послышки в двухпроводной линии, модулированные сигналы в двухпроводной линии, радиосигналы, световые импульсы в оптоволокне.

Адаптер является полуавтономным устройством. Получив пакет данных от узла (с точки зрения модели OSI – от вышестоящего протокола в стеке), адаптер самостоятельно выполняет инкапсуляцию пакета в кадр и передачу кадра в канал связи. Получив кадр из канала связи, адаптер проверяет (если это определено протоколом) целостность кадра, извлекает пакет данных и передаёт этот пакет узлу, формируя аппаратное прерывание [2, 7].

Важно отметить, что большинство протоколов канального уровня не подразумевают надёжную передачу данных. Сетевой адаптер, получив «испорченный» кадр с неверной контрольной суммой, просто

отбрасывает его, не извещая о потере кадра вышестоящий уровень. Таким образом вышестоящие протоколы обязательно должны контролировать целостность данных.

Сетевой адаптер «ничего не знает» о правильной последовательности пакетов. Адаптер принимает кадры и передаёт содержащиеся в них пакеты в той последовательности, в которой кадры приходят на вход адаптера. Пакеты данных могут идти по разным маршрутам и перемешиваться. Протоколы вышестоящего уровня должны контролировать правильную последовательность пакетов.

В разделяемой среде передачи данных адаптеры принимают все кадры, распространяющиеся в этой среде. При этом каждый адаптер имеет уникальный физический адрес и обрабатывает кадры, предназначенные только для него. Физический адрес также называют МАС-адресом. Конечно, пользователь может в большинстве случаев изменить физический адрес адаптера, и теоретически возможно подключение к одной физической среде нескольких адаптеров с одинаковыми физическими адресами, однако это нарушит нормальную работу большинства протоколов канального уровня.

Структура МАС-адреса показана на рис. 3.11. МАС-адрес содержит 48 бит. Записывать МАС-адреса принято в шестнадцатеричной нотации.

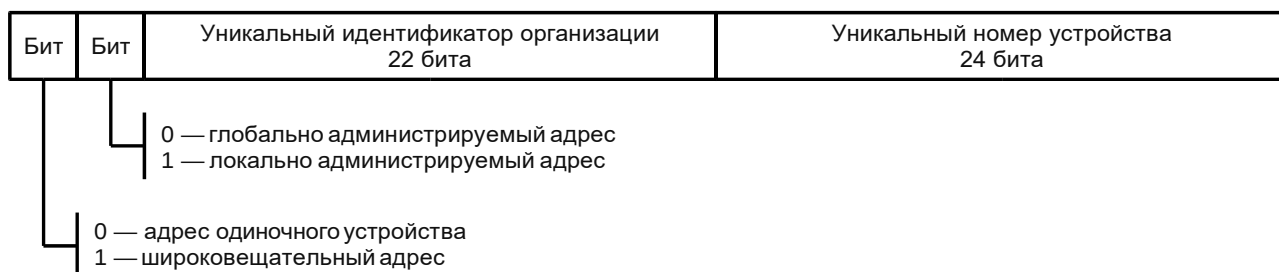


Рис. 3.11. Структура МАС-адреса [3]

Если старший бит адреса установлен в единицу, то это *широковещательный адрес*. Кадры с таким адресом должны принимать и обрабатывать все сетевые адаптеры. В качестве широковещательного чаще всего используется адрес FF:FF:FF:FF:FF:FF. Если старший бит адреса установлен в ноль, то это адрес одиночного устройства. Кадры с таким адресом обрабатываются только соответствующим адаптером.

Если второй по старшинству бит адреса установлен в единицу, то это *локально администрируемый адрес*, то есть адрес, установленный локальным программным обеспечением (операционной системой) или пользователем (посредством соответствующих утилит). Если второй

по старшинству бит адреса установлен в ноль, то это *глобально администрируемый адрес*, то есть уникальный адрес, установленный производителем адаптера.

Для MAC-адреса, установленного производителем, старшие 24 бита (три байта) являются *уникальным идентификатором организации* OUI – Organizationally Unique Identifier. Каждая фирма-производитель получает от института IEEE свои уникальные идентификаторы.

Рассмотрим, например, адрес 00:18:AF:82:83:07. Обратившись к одному из сайтов <http://www.networkcenter.info/inform/mac>, http://www.coffer.com/mac_find или к официальной страничке IEEE <http://standards.ieee.org/develop/regauth/oui/public.html>, можно выяснить, что в данном случае производителем адаптера (или микросхемы, на которой базируется адаптер) является компания «Samsung Electronics Co., Ltd».

Оставшиеся 24 бита в случае MAC-адреса производителя являются уникальным номером устройства.

Итак, изначально каждый сетевой адаптер имеет уникальный адрес. Может возникнуть вопрос, зачем нужна многоуровневая система адресации – IP-адреса, MAC-адреса? Не достаточно ли только «плоской» системы физических адресов?

Во-первых, над канальным уровнем может работать не только IP, но и другие протоколы. Во-вторых, представьте себе, что требуется замена адаптера, при этом информация о новом физическом адресе должна быть доступна всем устройствам, выполняющим маршрутизацию в глобальной сети. Это потребует больших накладных расходов. Ещё хуже представляется ситуация с широковещательными рассылками. А что будет, если вышедшей из строя адаптер начнёт непрерывно посылать широковещательные пакеты?

Казалось бы, что можно обойтись совсем без MAC-адресов, ведь тогда каждый адаптер в физическом сегменте сети будет обрабатывать каждый кадр и передавать его на верхний уровень. Но это значительно снизит производительность вычислительных систем. Кроме того, использование в кадрах физических адресов позволяет использовать такие устройства, как коммутаторы.

3.7. Концентраторы, коммутаторы, маршрутизаторы

Физические линии связи между компьютерами могут быть построены с использованием таких технологий, как коаксиальный ка-

бель, витая пара, оптоволокну, радиодоступ. Рассмотрим наиболее широко распространённую в настоящее время технологию витой пары. Для соединения трёх и более узлов в сеть требуется промежуточное устройство (рис. 3.12).

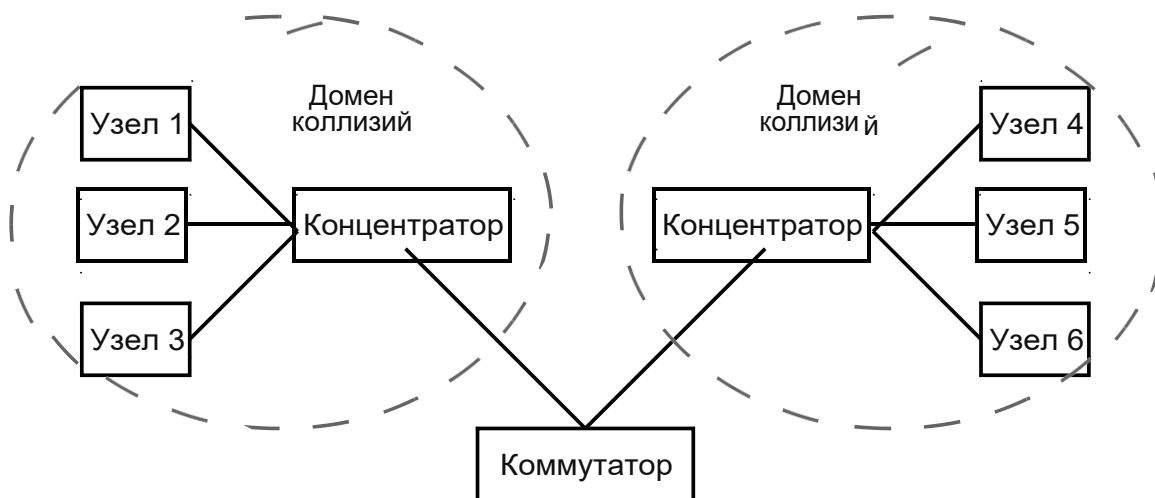


Рис. 3.12. Топология сети с концентраторами и коммутатором [7]

Концентратор (Hub) работает на физическом уровне. Двоичные сигналы, приходящие на любой порт концентратора, воспроизводятся на остальных портах. Таким образом, все узлы, подключённые к концентратору, входят в один *домен коллизий*.

В отличие от концентратора, коммутатор (Switch) работает на канальном уровне. Кадры передаются только на тот интерфейс (разъём для подключения витой пары, оптоволоконной линии, аудиоантенны), к которому подключен узел назначения. Таким образом домены коллизий локализуются. Коммутатор формирует очередь кадров на каждом интерфейсе и использует протокол CSMA. Наличие буферов на интерфейсах коммутатора позволяет согласовывать сегменты сети, использующие разные скорости передачи данных и разные сетевые технологии физического уровня.

Коммутатор (Switch) и мост (Bridge) являются очень близкими устройствами. Мост использует центральный процессор для обработки поступающих кадров, а в коммутаторе применяется коммутационная матрица. На сегодняшний день мосты практически не используются. Коммутаторы и мосты имеют большее время задержки распространения кадров, чем концентраторы, так как они анализируют кадры.

Коммутатор является самообучающимся устройством. Для того, чтобы определять, на какой интерфейс следует передать очередной

кадр, коммутатор формирует специальную таблицу, в которую записываются номер интерфейса, MAC-адрес подключенного к интерфейсу адаптера, а также время (табл. 3.2).

Таблица 3.2

Фрагмент таблицы коммутатора

MAC-адрес	Интерфейс коммутатора	Время
00:24:1D:84:41:62	1	08:05:00
00:0E:A6:21:12:4D	1	08:35:03
00:11:1B:78:B4:12	3	08:35:04

В момент включения коммутатора таблица пуста. Все входящие кадры передаются на все интерфейсы. По мере поступления кадров на очередной интерфейс коммутатор считывает адрес узла-отправителя и заполняет таблицу. Каждая запись имеет конечное время жизни. Если тот или иной адаптер в течение длительного периода не обнаруживает своей активности, запись из таблицы исключается. Таким образом таблица поддерживается в актуальном состоянии. Необходимо обратить внимание на то, что широковещательные пакеты передаются на все интерфейсы. Коммутатор имеет ограниченные возможности защиты от «широковещательного шторма».

Коммутатор осуществляет функции *фильтрации* и *продвижения* кадров. Пусть на интерфейс 1 коммутатора (см. табл. 3.2) приходит кадр, адресованный узлу 00:0E:A6:21:12:4D. Коммутатор отыскивает соответствующий адрес в таблице и определяет, что кадр надо игнорировать, таким образом выполняется фильтрация. Пусть на интерфейс 1 приходит кадр, адресованный узлу 00:11:1B:78:B4:12, такой кадр будет передан на интерфейс 3, выполняется продвижение.

Таблицы маршрутизации часто создаются вручную. Однако иерархическая система адресов позволяет ограничивать распространение широковещательных пакетов. Гибкая настройка маршрутизации также позволяет оптимизировать передачу трафика по нескольким каналам (об этом – в гл. 4).

Структура сети (см. рис. 3.12) имеет тот недостаток, что при выходе из строя коммутатора сеть распадется на несвязанные сегменты. Для повышения надёжности необходимо предусмотреть резервные пути, включив ещё несколько коммутаторов (рис. 3.13).

В такой топологии возникает проблема заикливания и размножения кадров. Для предотвращения этих эффектов используется протокол *STP – Spanning Tree Protocol IEEE 802.1D (протокол связующего дерева)*. Коммутаторы обмениваются друг с другом специальными кадрами BDPDU – Bridge Protocol Data Units и виртуально отключают некоторые интерфейсы так, чтобы исключить циклические пути.

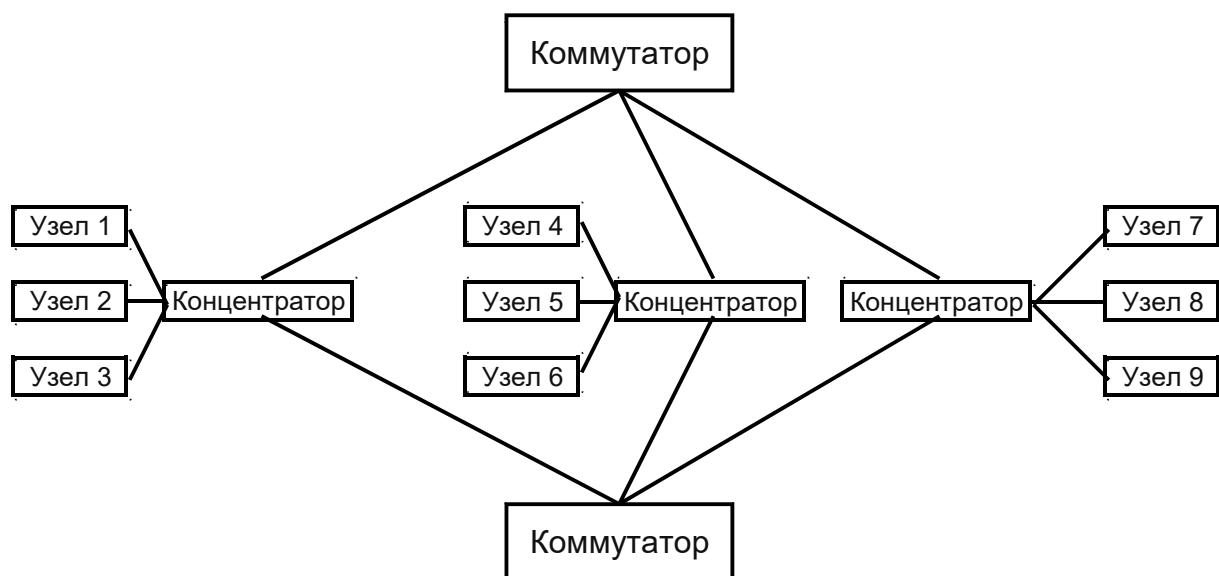


Рис. 3.13. Топология сети с резервными путями [3, 7]

Алгоритм построения связующего дерева включает следующие действия:

- выбирается *корневой коммутатор*. Корневым становится устройство с наименьшим BrigeID (приоритет и MAC-адрес коммутатора);
- прочие коммутаторы находят кратчайший путь до корневого и соответствующий интерфейс назначают *корневым*;
- для каждого сегмента сети определяется кратчайший путь до корневого интерфейса, соответствующие интерфейсы становятся *назначенными*;
- все интерфейсы, кроме корневых и назначенных, отключаются;
- рассылка кадров BDPDU выполняется с определённой периодичностью (по умолчанию, две секунды), при необходимости строится новое связующее дерево.

На основе коммутаторов можно строить *виртуальные сети* (VLAN – Virtual LAN). Виртуальной сетью называется группа узлов,

трафик которых изолирован от трафика других узлов. Организация нескольких виртуальных сетей позволяет гибко управлять правами доступа к ресурсам сети и изолировать широковещательные шторма. Виртуальные сети могут пересекаться (например, несколько групп узлов могут иметь доступ к одному серверу). Виртуальные сети объединяются при помощи маршрутизаторов или коммутаторов третьего уровня.

3.8. Помехоустойчивое кодирование на канальном уровне

На сегодняшний день большинство средств передачи и хранения данных используют тот или иной метод помехоустойчивого кодирования. Широко распространённым вариантом является *циклический избыточный код* (CRC – Cyclic Redundancy Code) [1, 5, 8].

Поле CRC (рис. 3.14) содержится в каждом кадре данных и позволяет с высокой достоверностью выявлять ошибки, возникающие при передаче кадра через физическую среду. Поле CRC обеспечивает достоверную передачу информации только в пределах физического сегмента сети.

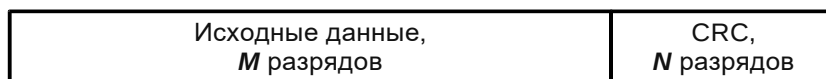


Рис. 3.14. Данные и циклический избыточный код

Адаптер, обрабатывающий предназначенные для него кадры, проверяет их корректность. Если ошибок не обнаружено, пакет данных, содержащийся в кадре, передаётся на сетевой уровень. В том случае, когда происходит дальнейшая транспортировка этих пакетов (например, маршрутизатором), формируется новый кадр и вычисляется новый избыточный код.

Если адаптер обнаруживает ошибку, кадр может быть просто отброшен. Таким образом, задача надёжной доставки данных от узла-отправителя до узла-получателя в пределах одного физического сегмента сети, и тем более, в нескольких сетях, выполняется протоколами сетевого уровня.

Коротко рассмотрим основы построения циклического избыточного кода.

Пусть $D(x)$ – полином, соответствующий исходным данным, N – количество разрядов CRC. Полином $G(x)$ степени N будем называть *порождающим*. Циклический избыточный код $R(x)$ находится как остаток от деления $D(x)$ на $G(x)$:

$$R(x) = D(x)x^N \cdot \text{mod } G(x), \quad (3.1)$$

где $D(x)x^N$ – исходное сообщение, к которому дописаны N нулей в конце;

mod – операция вычисления остатка от деления полиномов.

Корректность полученного кадра можно проверить, разделив последовательность $D(x) R(x)$ на порождающий полином $G(x)$. В случае отсутствия ошибок остаток должен быть равен нулю.

В разных стандартах используются разные порождающие полиномы, что вносит некоторую путаницу. Возможна ситуация, когда оборудование, произведённое разными фирмами, не способно взаимодействовать друг с другом из-за того, что используются отличающиеся алгоритмы вычисления CRC в служебных кадрах.

Группа стандартов IEEE 802.3 использует порождающий полином $x^{32} + x^{26} + x^{23} + x^{22} + x^{16} + x^{12} + x^{11} + x^{10} + x^8 + x^7 + x^5 + x^4 + x^2 + x + 1$.

Такой циклический избыточный код позволяет обнаруживать однократные ошибки (ошибки в одном бите кадра), двукратные и трёхкратные ошибки для кадров размером до 1500 байт, а также все ошибки с нечётным числом ошибочных битов.

3.9. Протоколы ARP, RARP

Связь физических адресов (MAC-адресов) сетевых адаптеров и IP-адресов узлов сети обеспечивает протокол ARP (Address Resolution Protocol) – протокол разрешения адресов. Каждый узел ведёт таблицу соответствия MAC-адреса сетевому адресу [3, 7]. Пример записей в памяти узла в табл. 3.3.

Таблица 3.3

Фрагмент таблицы ARP-модуля

IP-адрес	MAC-адрес	Время
10.7.21.1	00:24:1D:84:41:62	08:05:00
10.7.125.293	00:0E:A6:21:12:4D	08:35:03
10.7.212.91	00:11:1B:78:B4:12	08:35:04

Пусть узлу с IP-адресом 10.7.121.121 требуется передать данные на узел 10.7.121.122. Если адрес получателя уже есть в таблице, то соответствующие данные передаются сетевому адаптеру, который формируется кадр с MAC-адресами получателя и отправителя. В этот кадр инкапсулируется пересылаемый пакет.

Если нужный IP-адрес в таблице не найден, то узел посылает ARP-запрос. В кадре в качестве MAC-адреса получателя указывается широковещательный адрес FF:FF:FF:FF:FF:FF, тип кадра указывает на протокол ARP, пакет данных содержит IP-адрес отправителя и IP-адрес получателя (рис. 3.15).

Адрес получателя: FF:FF:FF:FF:FF:FF	Адрес источника: 74:F0:6D:07:80:36	Протокол: ARP	Пакет данных: цель 10.7.121.122, источник 10.7.121.121	CRC
--	---------------------------------------	------------------	--	-----

запрос «Кто имеет IP 10.7.121.122? Спрашивает узел 74:F0:6D:07:80:36»

Адрес получателя: 74:F0:6D:07:80:36	Адрес источника: 00:24:1D:84:41:62	Протокол: ARP	Пакет данных: цель 10.7.121.121, источник 10.7.121.122	CRC
--	---------------------------------------	------------------	--	-----

ответ «Мой IP 10.7.121.122. Отвечает узел 00:24:1D:84:41:62»

Рис. 3.15. Кадры с запросом и ответом по протоколу ARP

Все адаптеры локальной сети обрабатывают широковещательный запрос и передают его на сетевой уровень. Если один из узлов обнаруживает, что запрошен его MAC-адрес, формируется ответный пакет, аналогичный полученному, только вместо широковещательного MAC-адреса указывается адрес узла-получателя.

Узлы обрабатывают все ARP-запросы, формируя таблицу адресов. Записи в таблице имеют конечное время жизни (как правило, 20 мин.), таким образом таблица поддерживается в актуальном состоянии.

Существует также обратный протокол RARP (Reverse ARP), позволяющий определить IP-адрес по известному MAC-адресу.

3.10. Семейство протоколов PPP

PPP (Point to Point Protocol) – протокол передачи от точки к точке [3, 7]. Семейство PPP включает множество стандартов. Инициализацию и завершение сеанса связи выполняет протокол LCP (Link Control Protocol) – протокол управления каналом. Диаграмма, иллюстрирующая фазы работы протокола PPP, показана на рис. 3.16.

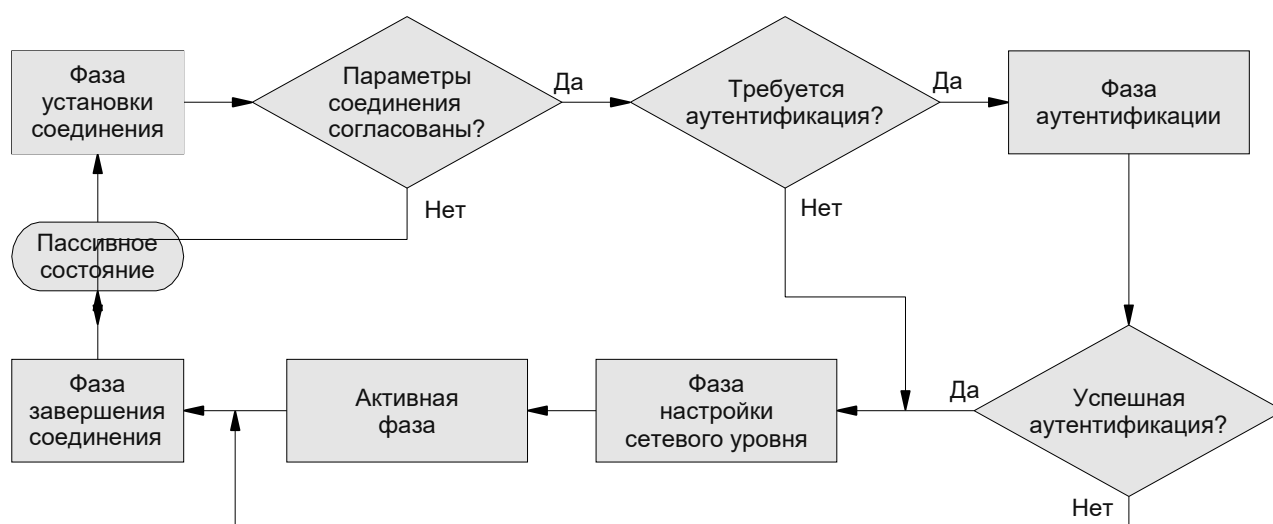


Рис. 3.16. Фазы работы протокола PPP

Так как протокол PPP рассчитан на связь только двух узлов, то можно использовать физически раздельные линии (например, различные витые пары) для передачи в двух направлениях. Таким образом коллизии полностью исключены и возможно дуплексное соединение.

Формат кадра протокола PPP представлен на рис. 3.17. Кадр начинается и заканчивается байтом флага 01111110 (0x7E). Поле адреса может содержать только одно значение 11111111 (0xFF), управляющее поле – 00000011 (0x03). Поле протокола указывает на протокол, инкапсулированный в поле данных. Поле CRC служит для обнаружения ошибок передачи. Так как поле адреса и управляющие поля не несут информации, в процессе установки соединения может быть указан формат кадра без этих полей.

Флаг, 1 байт 0x7E	Адрес, 1 байт 0xFF	Управление, 1 байт 0x03	Протокол, 2 байта	Данные, переменная длина	CRC, 2 - 4 байта	Флаг, 1 байт 0x7E
Кадр протокола PPP						

Рис. 3.17. Формат кадра протокола PPP

Если байт 01111110 (0x7E) встречается в поле данных, то заменяется последовательностью 01111101 01011110 (0x7D 0x5E). Если в поле данных встречается байт 01111101 (0x7D), то заменяется на 01111101 01011101 (0x7D 0x5D). Помимо этого, все байты со значениями меньше, чем 0010000 (0x20) также подменяются двухбайтовыми последовательностями. В частности, байт 00000001 (0x01) передаётся как 01111101 00100001 (0x7D 0x21). Протокол PPP используется для модемных соединений, а модемы могут воспринять байты со значениями от 00000000 (0x00) до 00011111 (0x1F) как управляющие последовательности.

Интернет-провайдерами России для предоставления доступа к Всемирной сети широко используются протоколы PPPoE и PPTP. Протокол PPPoE (Point-to-point protocol over Ethernet) – протокол передачи от точки к точке через Ethernet выполняет инкапсуляцию кадров PPP в кадры Ethernet. PPPoE также предоставляет услуги аутентификации, шифрования, сжатия данных. Протокол PPTP (Point-to-Point Tunneling Protocol) – протокол передачи от точки к точке с использованием тоннеля выполняет инкапсуляцию кадров PPP в IP-пакеты.

Одним из протоколов аутентификации является CHAP (Challenge Handshake Authentication Protocol) – протокол аутентификации с запросом и рукопожатием. Протокол CHAP используется для периодической проверки аутентичности узла с использованием трёхшаговой процедуры. Аутентификация выполняется после фазы установки соединения и состоит из следующих шагов:

- сервер посылает запрос клиенту;
- клиент, используя данные в запросе и пароль, вычисляет хеш-функцию, значение которой передаёт серверу;
- сервер вычисляет хеш-функцию и сравнивает значение с полученным от клиента. Если значения совпадают, то аутентификация считается успешной, в противном случае соединение должно быть завершено.

Через случайный интервал времени сервер может повторить запрос аутентификации. При помощи протокола CHAP возможна также взаимная аутентификация двух узлов. Вначале первый узел посылает запрос второму, после завершения процедуры второй узел посылает запрос первому.

Недостатком протокола CHAP является необходимость хранить пароль в открытом виде на каждом из узлов.

Выводы по главе 3

Канальный уровень модели OSI:

- обеспечивает доставку кадров с инкапсулированными пакетами данных в пределах физического сегмента сети от узла к узлу;
- решает задачу разделения физической среды передачи данных между узлами, подключенными к этой среде;
- обеспечивает локальную (в пределах сегмента сети) целостность кадров;
- в ряде случаев решает задачу аутентификации узлов.

В табл. 3.4 приведены некоторые широко используемые стандарты Ethernet и Wi-Fi, в которые входят спецификации канального уровня.

Таблица 3.4

Некоторые стандарты Ethernet и Wi-Fi

Стандарт	Физическая среда	Скорость	Максимальное расстояние между узлами	Максимальное число узлов в сегменте	Максимальная длина сети
1	2	3	4	5	6
10BASE-5	Коаксиальный кабель, толщина 9 мм, Z = 50 Ом	10 Мбит/с	500 м	100	2,5 км
10BASE-2	Коаксиальный кабель, толщина 5 мм, Z = 50 Ом	10 Мбит/с	185 м	30	925 м
10BASE-T	Витая пара категории 3	10 Мбит/с	100 м	1024	500 м
10BASE-F	Оптический кабель	10 Мбит/с	До 2 км	2	
100BASE-TX	Витая пара категории 5	100 Мбит/с	100 м	1024	205 м
100BASE-FX	Оптический кабель (многомодовый)	100 Мбит/с	До 2 км	1024	
100BASE-LX10	Оптический кабель (одномодовый)	100 Мбит/с	До 10 км	2	
1000BASE-T	Витая пара категории 5	1 Гбит/с	100 м	2	
1000BASE-SX	Оптический кабель (многомодовый)	1 Гбит/с	До 550 м	2	
1000BASE-LX	Оптический кабель (одномодовый)	1 Гбит/с	До 5 км	2	

1000BASE-LH	Оптический кабель (одномодовый)	1 Гбит/с	До 100 км	2	
10GBASE-T	Витая пара категории 6	10 Гбит/с	100 м	2	
10GBASE-SR	Оптический кабель (многомодовый)	10 Гбит/с	До 300 м	2	

Окончание табл. 3.4

1	2	3	4	5	6
10GBASE-LR	Оптический кабель (одномодовый)	10 Гбит/с	До 25 км	2	
100GBASE-LR4	Оптический кабель (одномодовый)	100 Гбит/с	До 10 км	2	
IEEE 802.11b	Радиочастоты в области 2.4 ГГц	До 11 Мбит/с	До 30 м	-	До 8 км (направленные антенны)
IEEE 802.11g	Радиочастоты в области 2.4 ГГц	До 20 Мбит/с	До 30 м	-	До 8 км (направленные антенны)
IEEE 802.11n	Радиочастоты в области 2.4 ГГц и в области 5 ГГц	До 300 Мбит/с			

Вопросы для самопроверки

1. Опишите особенности технологии CSMA.
2. Пусть задержка распространения сигнала в канале связи между двумя узлами составляет τ . Пропускная способность канала связи – R . Два узла одновременно начинают передачу кадра длительностью L . Произойдёт ли коллизия, если $\tau < L/R$? Объясните, почему.
3. Зачем в начале кадра Ethernet передаётся преамбула?
4. Почему ARP-запросы посылаются в широковещательном кадре? Почему ARP-ответы посылаются в кадре с MAC-адресом получателя?
5. Многие функции сетевого адаптера могут выполняться программно центральным процессором узла. Каковы преимущества и недостатки передачи этих функций от адаптера к узлу?
6. Как обеспечивается уникальность MAC-адресов?
7. В чём заключается процедура экспоненциального отката в технологии CSMA? Для чего эта процедура нужна?

8. Рассмотрите структуру локальной сети в вашем компьютерном классе. Определите размер домена коллизий.
9. Какие функции выполняет кадр явного подтверждения АСК в сетях с радиодоступом?
10. Каковы функции коммутатора в сети Ethernet?