Канальный уровень 4

14 мая 2026 г.

Практическое использование протоколов канального уровня

Для связи компьютеров в пределах одного здания широко применяются локальные сети, однако большинство глобальных сетей построено на линиях «точка-точка». Здесь рассмотрим три наиболее распространенных случая использования протоколов канального уровня в двухточечных каналах интернета.

Первый случай — передача пакетов по оптоволоконным каналам SONET. Такие каналы широко применяются, например, для соединения маршрутизаторов, установленных в разных концах сети провайдера.

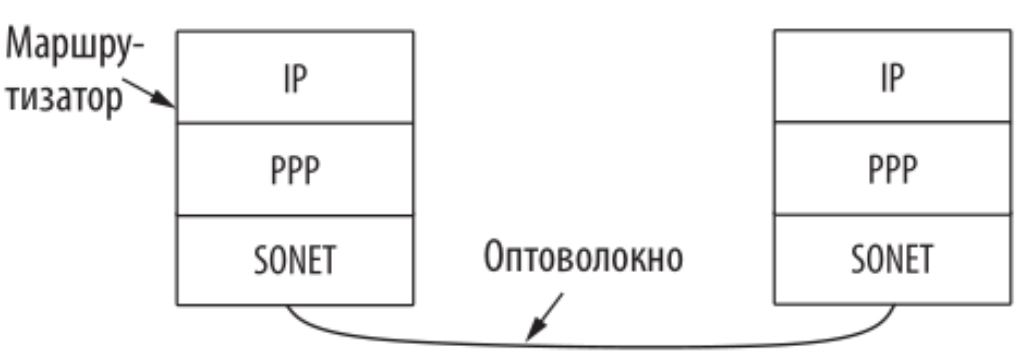
Вторым примером является использование каналов ADSL в пределах локального абонентского шлейфа телефонной сети.

Наконец, мы обсудим применение каналов DOCSIS в пределах локального шлейфа кабельной сети — с их помощью к интернету подключаются миллионы отдельных пользователей и компаний.

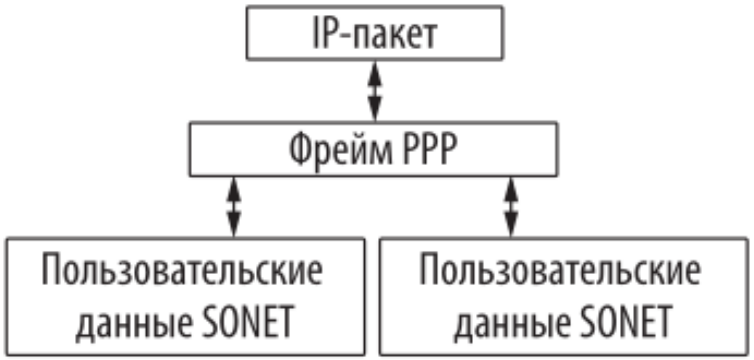
Для пересылки пакетов используется стандартный протокол двухточечного соединения PPP (Point-to-Point Protocol).

SONET, с которым мы познакомились ранее — это протокол физического уровня, наиболее часто используемый в оптоволоконных каналах, которые составляют магистраль различных коммуникационных сетей, включая телефонную. SONET обеспечивает строго определенную скорость передачи данных (например, 2,4 Гбит/с в канале OC-48). Поток битов организован в виде пакетов фиксированного размера, которые посылаются каждые 125 мкс, независимо от наличия в них пользовательских данных.

Чтобы передавать пакеты по таким каналам, необходим некоторый механизм формирования фреймов, способный отличать возникающие иногда пакеты от непрерывного потока битов, в котором они передаются. Для этого на IP- маршрутизаторах работает протокол PPP, как показано на илл


Маршру-
тизатор
IP
PPP
SONET
Оптоволокно
IP
PPP
SONET

(а)

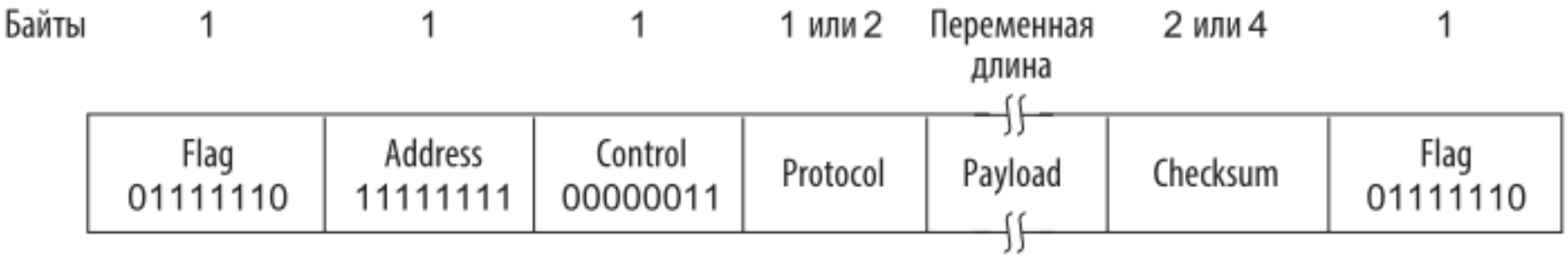

IP-пакет
Фрейм PPP
Пользовательские данные SONET
Пользовательские данные SONET

(б)

Благодаря широкому набору опций, PPP предлагает три основные функции:

- Метод формирования фреймов, однозначно обозначающий конец одного фрейма и начало следующего. Формат фреймов также обеспечивает обнаружение ошибок.
- Протокол управления каналом **LCP** (Link Control Protocol), позволяющий устанавливать соединения, тестировать их, договариваться о параметрах использования и снова отключать их, когда они не нужны.
- Способ договориться о параметрах сетевого уровня независимо от используемого в нем протокола. Данный метод состоит в том, что для каждого поддерживаемого сетевого уровня имеется свой сетевой протокол управления **NCP** (Network Control Protocol).

Формат фрейма PPP показан на илл. Все PPP-фреймы начинаются со стандартного флагового байта протокола HDLC 0x7E (01111110). Если этот байт встречается в поле Payload, он предваряется управляющим байтом 0x7D, а следующий за ним представляет собой экранированный байт, сложенный по модулю 2 со значением 0x20 (при этом переключается пятый бит).


Байты
1
1
1
1 или 2
Переменная длина
2 или 4
1
Flag 01111110
Address 11111111
Control 00000011
Protocol
Payload
Checksum
Flag 01111110

байт-стаффинг

Например, 0x7D 0x5E — это управляющая последовательность для флагового байта 0x7E. Это означает, что начало и конец фрейма можно найти, просто просканировав содержимое на наличие байта 0x7E. Больше он нигде встречаться не будет. Правило удаления заполняющих битов при получении — найти значение 0x7D, удалить его, а следующий байт сложить по модулю 2 со значением 0x20.

После стартового фрейма идет поле Address (Адрес), которому всегда присваивается двоичное значение 11111111; это означает, что все станции должны принимать этот фрейм. Использование такого значения позволяет избежать необходимости назначать адреса передачи данных.

За полем адреса следует поле Control (Управляющее поле), его значение по умолчанию равно 00000011. Это число означает ненумерованный фрейм.

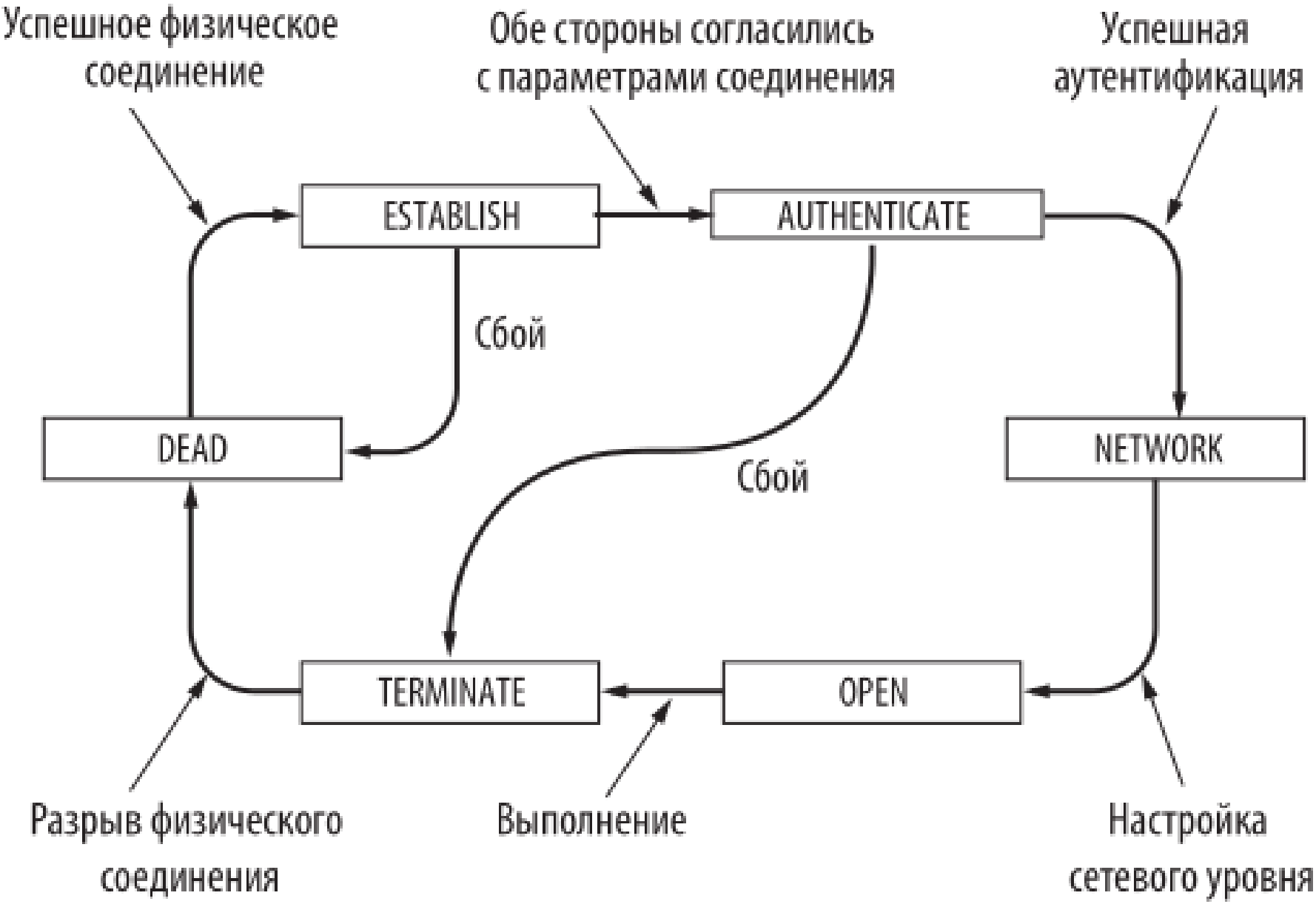
Так как по умолчанию поля Address и Control являются константами, протокол LCP позволяет двум сторонам договориться о возможности пропустить оба поля и сэкономить таким образом по 2 байта на фрейм.

Четвертое поле фрейма PPP — Protocol (Протокол). Оно определяет тип пакета, который содержится в поле Payload. Номера, начинающиеся с бита 0, отведены для IP версий 4 и 6, а также других протоколов сетевого уровня, таких как IPX и AppleTalk. С бита 1 начинаются коды, используемые в конфигурационных протоколах PPP, включая LCP и различные NCP для каждого поддерживаемого протокола сетевого уровня. Размер поля Protocol по умолчанию составляет 2 байта, однако путем переговоров с помощью LCP он может быть уменьшен до одного байта.

Поле Payload может быть переменной длины, вплоть до некоторого оговоренного максимального значения. Если размер не определен во время установки соединения при помощи LCP, то по умолчанию используется длина 1500 байт. При необходимости данные пользователя могут дополняться специальными символами.

Следом за Payload располагается поле Checksum (Контрольная сумма). В обычном состоянии оно занимает 2 байта, но в случае необходимости по договоренности может занимать четыре. Четырехбайтная контрольная сумма фактически представляет собой 32-битный код CRC.

Перед тем как передавать фреймы PPP по линии SONET, необходимо установить и настроить соединение PPP. Этапы, через которые проходит линия связи при ее установлении, использовании и разъединении


Успешное физическое соединение
Обе стороны согласились с параметрами соединения
Успешная аутентификация
ESTABLISH
AUTHENTICATE
Сбой
DEAD
NETWORK
Сбой
TERMINATE
OPEN
Разрыв физического соединения
Выполнение
Настройка сетевого уровня

Изначально линия в состоянии DEAD (отключена), то есть соединения на физическом уровне не существует. После создания физического соединения линия переходит в состояние ESTABLISH (установление соединения).

В этот момент начинаются переговоры о параметрах с помощью протокола LCP.

Узлы PPP обмениваются пакетами LCP (они содержатся в поле Payload фрейма PPP). Это необходимо для выбора из перечисленных выше параметров PPP. Инициирующий узел предлагает варианты, а отвечающие узлы либо соглашаются с ними, либо отвергают частично или полностью. Они также могут делать свои предложения.

При успешном результате переговоров линия переходит в фазу AUTHENTICATE (аутентификация). Теперь обе стороны по желанию могут проверить, кем является собеседник. После успешной аутентификации в фазе NETWORK (сеть) происходит обмен пакетами NCP для настройки сетевого уровня.

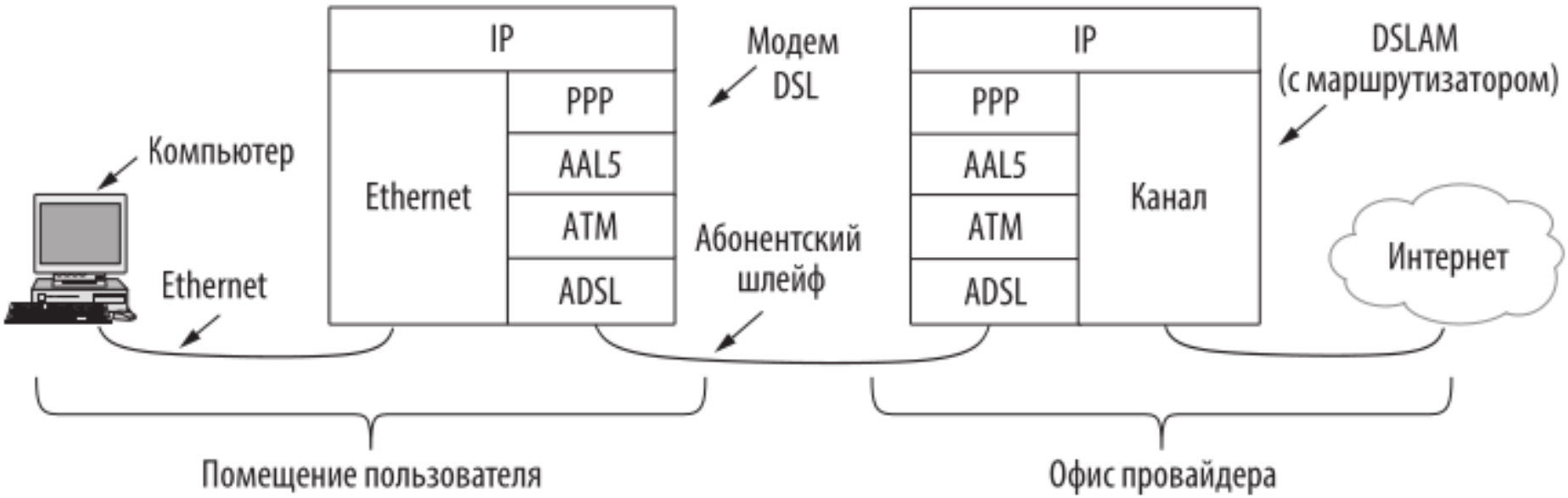
NCP отличается в зависимости от конкретного протокола сетевого уровня и поддерживает конфигурационные запросы, характерные только для него. Например, для IP наиболее важной задачей является назначение IP-адресов собеседникам на обоих концах линии.

Когда линия переходит в фазу OPEN (открыть), можно начинать передачу данных. Именно в этой фазе IP-пакеты пересылаются в PPP-фреймах по линии SONET.

Когда передача данных закончена, линия переходит к фазе TERMINATE (завершить), а затем снова в состояние DEAD (выключено), когда физическое соединение разрывается.

ADSL

ADSL (Asymmetric Digital Subscriber Line — асимметричная цифровая абонентская линия) соединяет миллионы домашних пользователей с интернетом на скоростях, равных нескольким мегабитам в секунду. Для этого используются те же телефонные провода, по которым предоставляются услуги традиционной телефонии.


IP
PPP
AAL5
ATM
ADSL
Ethernet
Модем DSL
Компьютер
Ethernet
Абонентский шлейф
IP
PPP
AAL5
ATM
ADSL
Канал
DSLAM (с маршрутизатором)
Интернет
Помещение пользователя
Офис провайдера

DSL модем отправляет биты по абонентскому шлейфу, адресуя их DSLAM (DSL Access Multiplexer — мультиплексор доступа DSL), установленному в местном офисе телефонной компании.

Домашний компьютер пользователя посылает IP-пакеты DSL-модему, используя ,например сеть Ethernet.

Затем DSL-модем отправляет IP-пакеты по абонентскому шлейфу на устройство DSLAM с помощью протоколов, которые мы рассмотрим далее.

На стороне DSLAM или подключенного к нему маршрутизатора (в зависимости от реализации) IP-пакеты извлекаются, поступают в сеть провайдера и достигают точки назначения в интернете.

Протоколы, работающие в соединении ADSL, начинаются с низшего, физического уровня. Он основаны на цифровой схеме модуляции, называемой ортогональным частотным мультиплексированием (также известным как дискретный многотональный сигнал).

Между ADSL и PPP находятся ATM и AAL5. Это новые протоколы, с которыми мы ранее не встречались. Протокол **асинхронной передачи данных ATM** (Asynchronous Transfer Mode)

ATM был разработан в начале 1990-х годов и широко рекламировался при первом запуске. Была обещана сетевая технология, которая решит все мировые телекоммуникационные проблемы, объединив голос, текстовые данные, кабельное телевидение, телеграф, почтовых голубей, связанные нитью консервные банки и все остальные способы передачи информации в единую интегрированную систему, способную удовлетворить любые требования пользователей. К сожалению, ожидания не оправдались.

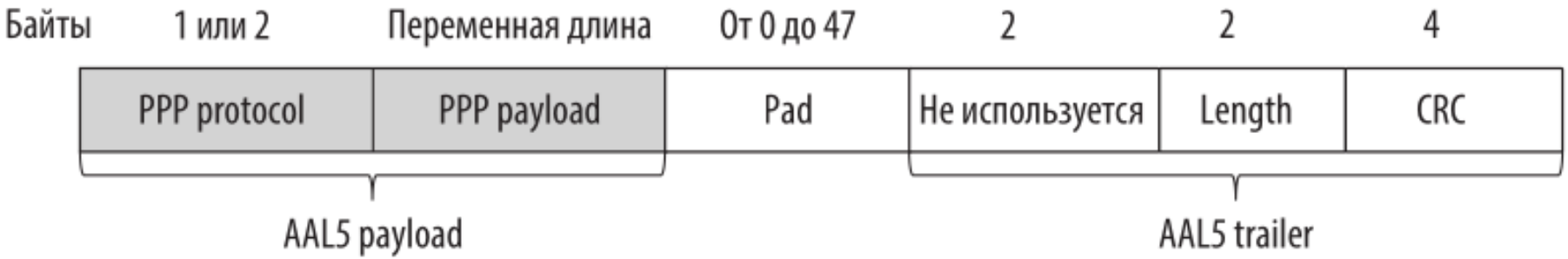
ATM представляет собой канальный уровень, основанный на пересылке ячеек (cells) информации фиксированной длины. «Асинхронная передача» означает, что нет необходимости отправлять ячейки постоянно, как это происходит с битами в синхронных линиях типа SONET.

Ячейки пересылаются только тогда, когда имеется готовая к передаче информация. ATM — это технология, ориентированная на установление соединения. В заголовок каждой ячейки встраивается идентификатор виртуального контура (virtual circuit), и устройства используют этот идентификатор для пересылки ячеек по маршрутам внутри установленных соединений.

Длина каждой ячейки составляет 53 байта: 48 байт пользовательских данных плюс 5 байт заголовка. Используя ячейки небольшого размера, ATM гибко разделяет полосу пропускания физического канала между разными пользователями. Это полезно, например, при одновременной передаче голоса и данных по одному каналу.

Для пересылки данных по сети ATM необходимо преобразовать их в последовательность ячеек. Преобразование выполняется на уровне адаптации протокола ATM путем сегментации и обратной сборки. Для разных служб, пересылающих различную информацию (от периодических голосовых сэмплов до пакетных данных), были определены несколько уровней адаптации. Основной, используемый для пакетных данных — это **уровень адаптации ATM 5** (ATM Adaptation Layer 5, AAL5).

Фрейм AAL5 показан на илл. Роль заголовка в нем исполняет трейлер (AAL5 trailer), содержащий сведения о длине (Length), а также 4-байтный код CRC для обнаружения ошибок. Разумеется, это тот же самый CRC, используемый протоколом PPP и сетями стандарта IEEE 802, такими как Ethernet.


Байты
1 или 2
Переменная длина
От 0 до 47
2
2
4
PPP protocol
PPP payload
Pad
Не используется
Length
CRC
AAL5 payload
AAL5 trailer

Помимо пользовательских данных (AAL5 payload), во фрейме AAL5 есть биты заполнения (Pad). Они дополняют общую длину, чтобы она была кратной 48 байтам. Таким образом, фрейм можно поделить на целое число ячеек. Хранить адреса внутри фрейма не нужно, так как идентификатор виртуального контура, имеющийся в каждой ячейке, не даст ей заблудиться и приведет к нужному получателю.

Итак, мы познакомились с протоколом ATM. Осталось только обсудить, как его задействует протокол PPP при ADSL-подключении. Это делается с помощью еще одного стандарта, который так и называется — PPP с использованием ATM (PPP over ATM, PPPoA).

В действительности данный стандарт нельзя назвать протоколом (поэтому на илл. его нет). Скорее это спецификация, описывающая, как одновременно применять протокол PPP и фреймы AAL5.

Пользовательские данные AAL5 содержат только два поля PPP: Protocol и Payload, как показано на илл.

Поле Protocol сообщает устройству DSLAM на другом конце линии, чем являются эти пользовательские данные: пакетом IP, LCP или другого протокола. Принимающая сторона знает, что ячейки содержат информацию PPP, так как виртуальный контур ATM настраивается соответствующим образом.

Для фрейма AAL5 механизмы формирования фрейма PPP не требуются, всю работу выполняют ATM и AAL5. Дополнительно создавать фреймы было бы попросту бессмысленно.

Код CRC протокола PPP также не нужен, поскольку AAL5 включает такой же CRC. Механизм выявления ошибок дополняет кодирование физического уровня, применяемое в каналах ADSL (код Рида — Соломона для исправления ошибок и 1-байтный CRC для распознавания оставшихся отклонений, не выявленных другими способами). Это куда более сложный механизм устранения ошибок, чем тот, что применяется при пересылке данных в сетях SONET.

Резюме

Задача канального уровня — преобразование необработанного потока битов, поступающего с физического уровня, в поток фреймов, которые могут использоваться сетевым уровнем.

Резюме

Канальный уровень может представлять этот поток с различной степенью надежности, начиная от служб без установки соединения и без подтверждения и заканчивая стабильными службами, ориентированными на установление соединения.

Резюме

Для формирования фреймов используются разнообразные методы, включая подсчет байтов, байт-стаффинг и бит-стаффинг.

Резюме

Протоколы канального уровня могут обеспечить контроль ошибок для обнаружения и исправления поврежденных и повторной передачи потерянных фреймов.

Резюме

Во избежание перегрузки медленного приемника быстрым отправителем применяется управление потоком.

Резюме

Коды с обнаружением и исправлением ошибок добавляют к сообщениям избыточную информацию с помощью ряда математических методов.

Резюме

Сверточные коды и коды Рида-Соломона широко используются для коррекции ошибок, при этом коды с низкой плотностью проверок четности приобретают все большую популярность. К кодам обнаружения ошибок, используемым на практике, относятся циклические избыточные проверки и контрольные суммы.

Резюме

Мы рассмотрели ряд протоколов, обеспечивающих надежную работу канального уровня за счет подтверждений и повторной передачи или, если взять более реалистичный пример, за счет запросов ARQ (Automatic Repeat reQuest).

Резюме

Начав с обсуждения идеальной среды передачи, где отсутствуют ошибки, и идеального приемника, который может обработать входящий поток любого размера, мы познакомились с управлением потоком, затем с контролем ошибок с помощью порядковых номеров и, наконец, с алгоритмом с остановкой и ожиданием.

Резюме

Затем мы перешли к алгоритму «раздвижного окна», позволяющему обмениваться данными в двух направлениях, и узнали о концепции вложенного подтверждения.

Резюме

В интернете в качестве основного протокола линий «точка-точка» используется PPP. Он предоставляет службу без установки соединения и без подтверждения. Для разделения фреймов применяются флаговые байты, а для распо знавания ошибок — коды CRC.

Резюме

С помощью этого протокола пакеты передаются по множеству типов соединений, включая каналы SONET в глобальных сетях и ADSL для домашних подключений. Для предоставления доступа в интернет по имеющейся сети кабельного телевидения используется протокол DOCSIS.