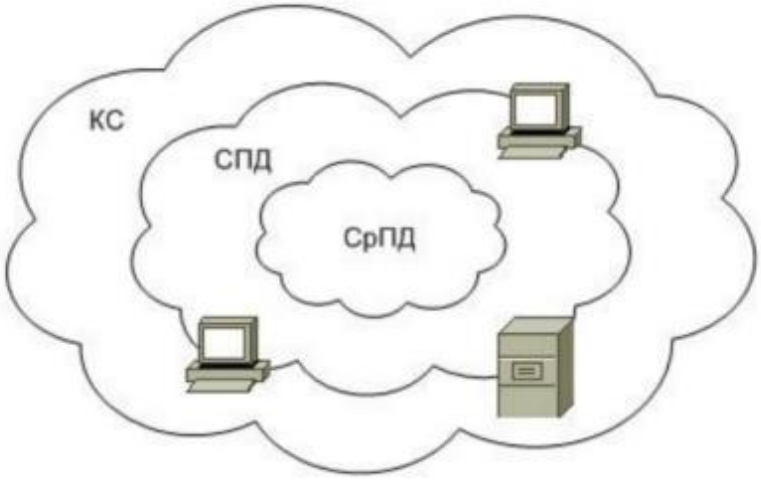
1. Понятие компьютерной сети

Под компьютерной сетью (КС) понимают совокупность различных технических средств (то есть самих компьютеров и другого оборудования), предназначенная для передачи компьютерной информации (то есть файлов и сообщений) на относительно большие расстояния (то есть за пределы компьютеров) Любую КС можно рассматривать с двух точек зрения: программной и аппаратной
В основе любой КС лежит так называемая сеть передачи данных (СПД), которая может задействовать различные среды передачи данных (СрПД) Иногда в составе СПД выделяют базовую (опорную) СПД Все устройства в составе СПД можно разделить на две четко разделяющиеся группы: оконечные (находятся по периметру СПД) и посредники (составляют ядро СПД)
Весь трафик в СПД традиционно разделяют на три базовых типа: обычные компьютерные данные (data), голос (voice) и видео (video) Каждый тип обладает характерными особенностями СПД, поддерживающие пересылку разнородного трафика, в нотации Cisco называются конвергированными (converged networks) Особенности трафика обеспечиваются так называемым качеством обслуживания (Quality of Service, QoS)
Традиционные виды компьютерных данных без исключения, по умолчанию, обслуживаются по принципу «Все делается для доставки пакетов, но при этом ничего не гарантируется» (best efforts), что, по сути, является отсутствием QoS Гарантии «возникают» при работе с голосом и видео
Таким образом, компьютерные сети представляют собой сложные системы, включающие в себя различные технические средства и технологии для эффективной передачи и обработки данных, голоса и видео Эти сети обеспечивают качественное обслуживание (QoS) для разнородного трафика, что особенно важно для голосовой и видео связи



2. Классификация компьютерных сетей

Введение: Классификация компьютерных сетей включает в себя множество типов, которые различаются по масштабам, назначению и способам взаимодействия. Сети классифицируются по различным параметрам и стандартизируются международными, европейскими и американскими организациями.
Основная часть: С одной стороны, выделяют:
1. Local Area Networks (LANs) - локальные КС (ЛКС)
2. Wide Area Networks (WANs) - глобальные КС (ГКС)
3. Metropolitan Area Networks (MANs) - городские КС
4. Personal Area Networks (PANs) - личные КС
5. Remote Access Services (RASes) - КС для подключения удаленных пользователей (teleworkers)
6. Data Center Networks - КС центров обработки данных
7. Home Networks - домашние КС
8. Industrial Networks - промышленные КС

С другой стороны, выделяют:
1. Intranets - внутренние КС предприятий и организаций
2. Internets - КС публичного доступа

Локальные сети (LAN) выделяют территориально, охватывая территорию не более кампуса и предполагая определенные технологии. Глобальные сети (WAN) выделяют технологически и могут охватывать произвольную территорию. Городские сети (MAN) являются промежуточными между LAN и WAN. Личные сети (PAN) позволяют подключать периферийные устройства к компьютеру. RAS существует в контексте WAN. Домашние, промышленные и сети центров обработки данных являются специализированными вариантами LAN. Внутренние сети (Intranets) выделяют по ведомственной принадлежности пользователей, а публичные сети (Internets) интегрированы в одноименную сеть. Внутренние сети (Intranets) обычно имеют связь с Интернетом.
Кроме того, сети могут быть изолированными (isolated) или открытыми для прослушивания (open). С точки зрения организации взаимодействия, компьютерные сети могут быть сильносвязанными или слабосвязанными. В сильносвязанной сети существует хост-ЭВМ и терминал (хост-терминальная модель). В слабосвязанной сети существует сервер и клиент (клиент-серверная модель).

3. Стандарты компьютерных сетей

Введение: Стандарты компьютерных сетей определяют правила и соглашения, которые применяются при создании локальных сетей и организации передачи данных. Эти стандарты могут быть международными, европейскими и американскими, и они помогают формализовать требования в предметной области.

Основная часть: Стандарты компьютерных сетей делятся на:

1. Международные (например, ISO/IEC)
2. Европейские (например, EN)
3. Американские (например, ANSI/TIA/EIA)

Стандарты формализуют определенные требования и могут носить предварительный или временный характер, включать дополнения и списки обнаруженных ошибок, а также

устаревать или заменяться другими стандартами. Реализация стандарта представляет собой его практическое или теоретическое воплощение. Сертификация позволяет определить факт соответствия стандарту.

В 1980 году при IEEE был создан специальный комитет по стандартизации компьютерных сетей, результатом работы которого стало множество стандартов 802.x. Наибольший интерес представляют:

1. 802.3 – Ethernet
2. 802.11 – Wi-Fi
3. 802.16 – WiMax

Стандарты Ethernet по пропускной способности делятся на три группы:

1. Ethernet - до 10 Mbit/s включительно
2. Fast Ethernet - 100 Mbit/s
3. Gigabit Ethernet – 1, 10, 100, 40, 25, Gbit/s и Multigigabit

Организации, работающие со стандартизацией компьютерных сетей:

- Международная организация по стандартизации (ISO)
- Институт инженеров электротехники и радиоэлектроники (IEEE)
- Американский национальный институт стандартов (ANSI) и др.

В локальных КС за разработку сетевых стандартов отвечает комитет 802 под эгидой IEEE. Наиболее известными подкомитетами являются:

- IEEE 802.1 – разработка стандартов межсетевого взаимодействия и управления сетевыми устройствами.
- IEEE 802.3 – разработка стандартов для проводных сетей стандарта Ethernet, использующих метод множественного доступа с контролем несущей частоты и обнаружением коллизий (CSMA/CD).
- IEEE 802.11 – разработка стандартов и правил функционирования устройств в беспроводных локальных сетях (Wi-Fi).

Вывод: Стандарты компьютерных сетей обеспечивают структурированность и согласованность в процессе создания и управления сетями, что позволяет эффективно использовать различные технологии и методы для передачи данных.

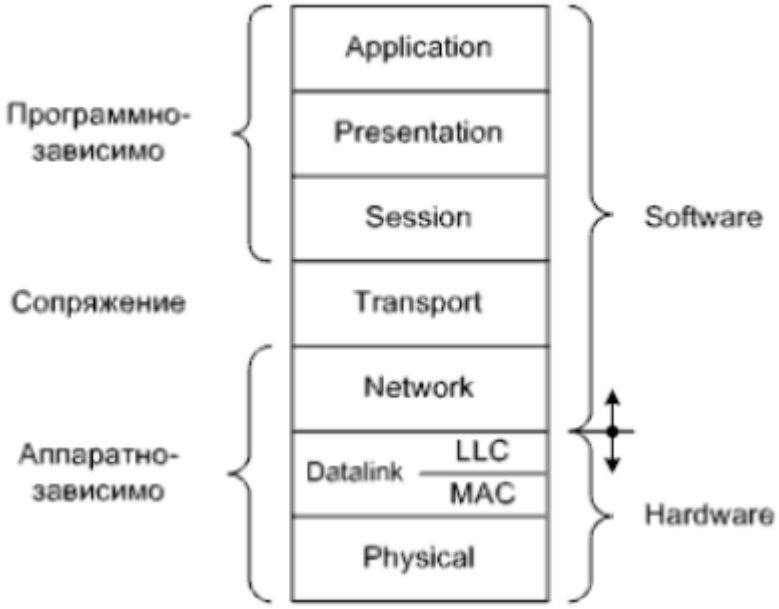
4. Наиболее распространенные модели компьютерных сетей

Введение: Наиболее распространенные модели компьютерных сетей включают в себя различные архитектуры, разработанные для стандартизации и упрощения взаимодействия между системами. Среди них выделяются модели OSI, TCP/IP и иерархическая модель от Cisco.

Основная часть: Из всех моделей КС наиболее фундаментальной является открытая модель взаимодействия систем - Open System Interconnection (OSI), разработанная ISO. OSI – модель,

определяющая разные уровни взаимодействия систем, дает им стандартные имена и указывает, какую работу должен делать каждый уровень.

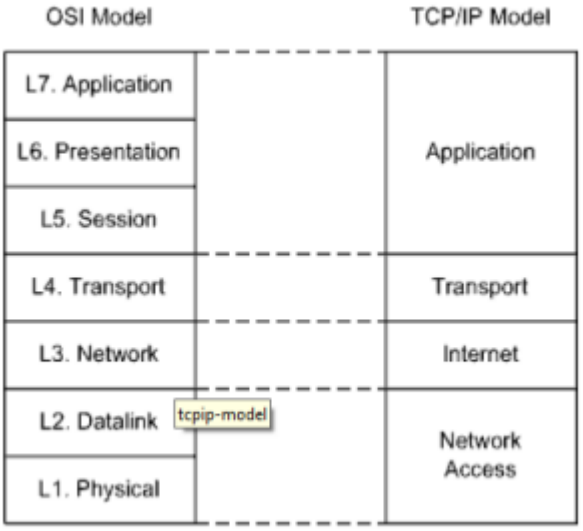
Модель включает 7 уровней.



На вершине иерархии находится человек, но абонентами КС являются взаимодействующие программы. Взаимодействие в рамках модели OSI может быть вертикальным (обеспечивает работу между соседними уровнями на одном устройстве) и горизонтальным (обеспечивает связь программ и процессов на различных устройствах).

- Интерфейс - это правила взаимодействия между пространственно совмещенными соседними уровнями модели OSI.
- Протокол - это правила взаимодействия между пространственно разнесенными одинаковыми уровнями модели OSI.

Ещё одна модель связана с семейством протоколов TCP/IP. Её сопоставление с моделью OSI на следующем рисунке.



Компания Cisco разработала собственную иерархическую сетевую модель (Cisco hierarchical network model), которую рекомендует использовать в корпоративных сетях разного масштаба. Модель включает 3 уровня:

1. Access – доступ
2. Distribution (иногда aggregation) – распределение
3. Core – ядро

Уровень доступа предназначен для обеспечения подключений к КС оконечных пользователей. Особое внимание здесь уделяют предоставлению пользователям требующихся им ресурсов. Уровень распределения предназначен для обеспечения взаимодействия в пределах групп пользователей. Особое внимание здесь уделяют резервированию соединений. Уровень ядра предназначен для обеспечения высокоскоростной связи между относительно удаленными группами пользователей. Особое внимание здесь уделяют характеристикам трафика. На всех уровнях значительное место отведено разграничению трафика с целями защиты пользователей друг от друга и защиты КС от пользователей. В настоящее время самая популярная из пропагандируемых Cisco архитектур – Cisco Borderless Network.

Вывод: Модели компьютерных сетей, такие как OSI, TCP/IP и иерархическая модель Cisco, предоставляют стандарты и структуры для эффективного взаимодействия между системами. Они помогают организовать и оптимизировать работу сетей, обеспечивая качественную и безопасную передачу данных.

5. Физический уровень модели OSI

Введение: Физический и канальный уровни модели OSI являются основополагающими в обеспечении передачи данных и их целостности. Каждый из них выполняет свои специфические функции и включает определенные компоненты.

Основная часть: Физический уровень модели OSI На физическом (physical) уровне формализуют подключение того либо иного сетевого устройства к СрПД. В пространстве

физический уровень охватывает «точку» подключения. Специфическими понятиями физического уровня являются:

1. Среда
2. Разъём (физический порт)
3. Несущая (частота)
4. Модуляция
5. Сигнал

Фундаментальная задача уровня заключается в передаче сигнала. Для передачи сигнала используется несущая и её модуляция. Несущая – частота гармонических электрических (электромагнитных) колебаний, служащих переносчиком информации при её передаче посредством модуляции этих колебаний сигналами, соответствующими передаваемому сообщению. Модуляция – процесс изменения одного или нескольких параметров несущего высокочастотного колебания в соответствии с изменением параметров передаваемого сигнала. Сигнал – материальное воплощение сообщения для использования при передаче, обработке и хранении информации. Функции физического уровня реализуются на всех устройствах, подключенных к сети. Со стороны компьютера функции физического уровня выполняются сетевым адаптером или последовательным портом. Физический уровень определяет такие виды сред передачи данных, как оптоволокно, витая пара и т.д. Стандартными типами сетевых интерфейсов, относящимися к физическому уровню, являются: RS-232 и RS-485.

Функции физического уровня модели OSI:

- Побитовая доставка
- Физическое кодирование (способ представления данных в виде импульсов)
- Адресация на основе уникальных MAC-адресов
- Предоставление протокола множественного доступа

6. Канальный уровень модели OSI

Канальный уровень предназначен для обеспечения взаимодействия сетей на физическом уровне и контроля ошибок, которые могут возникнуть. Полученные с физического уровня данные, представленные в битах, он упаковывает в кадры, проверяет их на целостность и, если нужно, исправляет ошибки (либо формирует повторный запрос поврежденного кадра) и отправляет на сетевой уровень. Канальный уровень может взаимодействовать с одним или несколькими физическими уровнями, контролируя и управляя этим взаимодействием.

На канальном (datalink) уровне формализуют взаимодействие станций в пределах сегмента. Специфическими понятиями канального уровня являются:

1. Сегмент сети
2. Физическая и логическая топология сегмента
3. Пакет (кадр)
4. Бит- и байт-стаффинг
5. Адресация в пределах сегмента
6. Канальный код
7. Код проверки целостности сегмента (кадра)

8. Алгоритм доступа к моноканалу

Канальный уровень разделяют на два подуровня:

1. MAC (Media Access Control) – контроль доступа к СрПД
2. LLC (Logical Link Control) – контроль логического соединения

На подуровне MAC, более низком, выполняется взаимодействие с физическим уровнем, то есть средозависимые операции, такие как формирование и распознавание пакетов, адресация, канальное кодирование и другие. На подуровне LLC, более высоком, выполняется взаимодействие с сетевым уровнем, то есть средонезависимые операции, такие как разбиение данных на пакеты, сборка данных из пакетов, определение соответствующей подсистемы сетевого уровня и другие. На этом уровне работают коммутаторы, мосты и другие устройства. Эти устройства используют адресацию второго уровня (канальный уровень).

Протоколы канального уровня:

- IEEE 802.3 (Ethernet)
- IEEE 802.11
- IEEE 802.2 (определяет управление логическим каналом (LLC) как верхнюю часть уровня канала передачи данных модели OSI)

Вывод: Физический и канальный уровни модели OSI являются ключевыми компонентами в обеспечении передачи данных и контроля их целостности. Они играют важную роль в построении эффективных и надежных сетевых систем, обеспечивая структурированное взаимодействие и стандартизацию сетевых процессов.

7. Сетевой уровень модели OSI

Введение: Сетевой уровень модели OSI играет важную роль в обеспечении маршрутизации и передачи данных между различными сетевыми сегментами. Этот уровень отвечает за логическую адресацию и управление трафиком, что позволяет данным находить путь от отправителя к получателю через сложные сети.

Основная часть: На сетевом (network) уровне формализуют маршрутизацию пакетов данных через сеть. Специфическими понятиями сетевого уровня являются:

1. IP-адресация
2. Маршрутизация
3. Пакет (datagram)
4. Интерфейс и маршрут
5. Протоколы маршрутизации

Основные функции сетевого уровня модели OSI:

- Логическая адресация: предоставление уникальных IP-адресов для устройств в сети.

- Маршрутизация: определение оптимального пути для передачи данных от отправителя к получателю через сеть.
- Управление трафиком: контроль потока данных и предотвращение заторов в сети.
- Фрагментация и сборка данных: разбиение больших пакетов на меньшие фрагменты для передачи и последующая сборка на уровне получателя.
- Контроль ошибок и восстановление данных: проверка целостности данных и исправление ошибок при необходимости.

Примеры протоколов сетевого уровня: IP (Internet Protocol), ICMP (Internet Control Message Protocol), IGMP (Internet Group Management Protocol).

Вывод: Сетевой уровень модели OSI обеспечивает маршрутизацию и передачу данных между различными сетевыми сегментами, выполняя ключевые функции логической адресации, управления трафиком и контроля ошибок. Этот уровень является основой для создания сложных и эффективных сетевых инфраструктур, обеспечивая надежное и безопасное соединение между устройствами в сети.

8. Транспортный и сеансовый уровни модели OSI

Введение: Транспортный и сеансовый уровни модели OSI обеспечивают ключевые функции для передачи данных и управления сессиями между приложениями в сети. Эти уровни позволяют программам использовать сетевое оборудование и управляют процессами передачи данных.

Основная часть: Транспортный уровень модели OSI: Транспортный уровень позволяет перейти от оборудования к программам. На транспортном (transport) уровне формализуют использование программным обеспечением сетевого оборудования, то есть как отдельно взятым программам предоставляется «транспорт». Специфическими понятиями транспортного уровня являются:

1. Пакет (сегмент сообщения)
2. Программный порт
3. Логическое соединение
4. Надежность доставки
5. Алгоритм борьбы с заторами СПД

Основные функции транспортного уровня OSI:

- Обнаружение ошибок, частичная их ликвидация
- Подтверждение передачи
- Восстановление передачи после отказов и неисправностей
- Разбиение данных на блоки определенного размера
- Управление передачей по сети и обеспечение целостности данных

Пример протоколов: TCP, UDP.

Сеансовый уровень модели OSI: Сеансовый или сессионный (session) уровень позволяет предоставить доступ к транспорту всем программам в многозадачном окружении. Кроме собственно сессии, имеются ещё два основных специфических понятия сеансового уровня:

1. Программный порт
2. Алгоритм мультиплексирования программ

В практических реализациях сеансовый уровень выражен слабо и обычно совмещается с транспортным. На сеансовом уровне определяется, какой будет передача между двумя прикладными процессами:

- Полудуплексной (процессы будут передавать и принимать данные по очереди)
- Дуплексной (процессы будут передавать данные и принимать их одновременно)

Основные функции сеансового уровня OSI:

- Установление и завершение на сеансовом уровне соединения между взаимодействующими приложениями
- Синхронизация сеансовых соединений
- Установление на прикладном процессе меток, позволяющих после отказа либо ошибки восстановить его выполнение от ближайшей метки
- Прекращение сеанса без потери данных
- Передача особых сообщений о ходе проведения сеанса

Вывод: Транспортный и сеансовый уровни модели OSI обеспечивают надежную и эффективную передачу данных между приложениями, а также управление сессиями. Эти уровни играют важную роль в создании стабильных и функциональных сетевых соединений.

9. Прикладной уровень и уровень представления модели OSI

Введение: Прикладной уровень и уровень представления модели OSI обеспечивают взаимодействие между пользователем и сетью, а также преобразование и управление данными для передачи по сети.

Основная часть: Прикладной уровень модели OSI: Прикладной (application) уровень призван решать конкретные пользовательские задачи с помощью КС. Он предназначен для решения таких задач, как:

1. Пересылка файлов между компьютерами
2. Пересылка электронных писем
3. Поддержка удаленных текстовых и графических терминалов, в том числе для администрирования
4. Пересылка мультимедийных документов
5. Обмен мгновенными сообщениями
6. Совместная разработка чего-либо

Специфических понятий прикладного уровня великое множество, и они зависят от решаемых задач. К протоколам прикладного уровня относятся: HTTP, FTP, RDP.

Уровень представления модели OSI: Уровень представления обеспечивает преобразование протоколов и кодирование/декодирование данных. Запросы приложений, полученные с прикладного уровня, на уровне представления преобразуются в формат для передачи по сети, а полученные из сети данные преобразуются в формат приложений. На этом уровне может осуществляться сжатие/распаковка или шифрование/дешифрование, а также перенаправление запросов другому сетевому ресурсу, если они не могут быть обработаны локально.

Уровень представления (presentation) позволяет адаптировать прикладную информацию в форму, приемлемую для передачи по КС, то есть является прослойкой между программами и транспортом. Основными задачами уровня представления являются:

1. Кодирование информации (включая возможное сжатие) с целью обеспечения её защиты при пересылке по открытым для прослушивания сетям.
2. Шифрование информации с целью обеспечения её защиты при пересылке по открытым для прослушивания сетям.

Поскольку обычно уровень представления «привязан» к прикладному уровню, в реализациях эти уровни часто совмещаются.

Вывод: Прикладной уровень и уровень представления модели OSI обеспечивают эффективное взаимодействие пользователя с сетью, а также безопасность и преобразование данных для их передачи. Эти уровни играют ключевую роль в обеспечении функциональности и безопасности сетевых приложений.

10. Семейство протоколов TCP/IP

Введение: Семейство протоколов TCP/IP является основой для передачи данных в современных сетях и охватывает различные уровни взаимодействия.

Основная часть: Разделение протоколов по уровням:

- Прикладной уровень и уровень представления: FTP, Telnet, SMTP, DNS, HTTP.
- Транспортный и сеансовый: TCP, UDP.
- Сетевой уровень: IMCP, RIP, OSPF, IP, ARP, RARP.
- Физический и канальный: Ethernet, Token Ring, FR.

Основные из них:

- FTP
- Telnet
- SMTP, POP, IMAP
- HTTP

Протоколы: Протокол FTP предназначен для пересылки файлов между двумя удаленными станциями. FTP разрабатывался одним из первых, но до сих пор занимает значимое место в сети Internet. FTP базируется на клиент-серверной модели и использует транспорт TCP.

Протокол Telnet реализует концепцию NVT (Network Virtual Terminal), уходящую корнями в UNIX-системы. Telnet базируется на клиент-серверной модели и использует транспорт TCP. Задействуется одно соединение.

Протокол SMTP используют для передачи электронной почты в почтовый ящик – от пользовательской станции (отправителя) к почтовому серверу и от одного почтового сервера к другому.

Протокол POP используют для приема электронной почты из почтового ящика – от почтового сервера к пользовательской станции (получателя).

Протокол IMAP также предназначен для приема электронной почты, но, в сравнении с POP, предоставляет комплексный функционал работы с почтовым ящиком.

Протокол HTTP предназначен для пересылки гипертекста между двумя удаленными станциями. HTTP-сообщениями являются различные web-страницы, написанные на языке HTML и его расширениях, но протокол пригоден и для пересылки других данных.

Вывод: Семейство протоколов TCP/IP охватывает различные уровни сетевого взаимодействия и обеспечивает передачу данных, взаимодействие приложений и управление сессиями. Эти протоколы являются основой для функционирования современных сетей и обеспечивают надежную и эффективную работу.

11. Эволюция COM-портов и их место в современных ПК

Введение: Эволюция COM-портов ПК отражает развитие технологий и их значение в истории вычислительной техники. COM-порты играли важную роль в ранних компьютерах и продолжают находить применение в современных системах.

Основная часть:

1. **Семидесятые годы XX века:** Компания Intel разработала два контроллера последовательного порта: 8250 (UART) и 8251 (USART). Эти контроллеры были рассчитаны на подключение по шине X-Bus и использовались в первых ПК на базе процессора 8086 с системной шиной ISA. Микросхемы UART и USART устанавливались на плату специального адаптера и подключались к материнской плате ПК через разъем системной шины. В это время возникла традиция устанавливать последовательные порты парами (COM1 и COM2).
2. **Времена доминирования процессоров 80286:** Происходило развитие контроллеров. В СССР был создан аналог 8251 под названием КР580ВВ51А. На Западе развитие получила микросхема 8250, которая была усовершенствована до UART 16550 разработки National Semiconductor. 16550 стала стандартной микросхемой на длительное время благодаря более высокой пропускной способности (до 115200 baud) и возможности буферизации (две очереди FIFO по 16 байт).
3. **Интеграционные процессы:** Привели к появлению мультикарт – плат расширения с интегрированными контроллерами последовательного порта (2x16550), параллельного порта, игрового порта, НГМД и НЖМД, которые подключались к системной шине (обычно ISA).

4. **Интеграция чипа Multi I/O:** Для ПК на базе поздних Intel486 была характерна интеграция чипа Multi I/O на материнскую плату.
5. **Период процессоров Pentium:** Сформировалась базовая структура материнской платы ПК, состоящая из четырех основных БИС. Контроллеры последовательного порта (2x16550) стали частью интегрированной периферии и не претерпели значительных изменений.
6. **Современное состояние:** С 2005 года традиционный последовательный интерфейс ПК считается устаревшим (legacy) и часто исключается из состава интегрированной периферии.

Вывод: Эволюция COM-портов показывает, как изменялись технологии и требования пользователей. Несмотря на то, что COM-порты считаются устаревшими, они продолжают находить применение в специфических задачах и устройствах.

12. Структура COM-портов ПК

Введение: COM-порты на аппаратном уровне представляют собой сложные устройства, обеспечивающие взаимодействие между различными компонентами ПК и периферийными устройствами.

Основная часть: На аппаратном уровне приемник и передатчик работают параллельно, используя отдельные физические цепи. Для подключения по стандарту RS-232 используют девятиконтактные разъемы DE-9. Передатчик и приемник COM-порта представляют собой сдвиговые регистры, которые записывают данные в регистр передатчика параллельно, а затем последовательно сдвигают их в линию под воздействием тактовых импульсов.

В структуру COM-порта входит:

- Шина данных
- Приемный и передающий буфер
- Программируемый бод-генератор для тактирования
- Множество регистров (информационные, служебные, управляющие)

Вывод: COM-порты обеспечивают надежную и эффективную передачу данных между устройствами, играя ключевую роль в коммуникации между компонентами ПК и внешними устройствами.

13. Цепи RS-232 и их использование

Цепи RS-232 и их использование

Введение: Цепи RS-232 выполняют важные функции в организации передачи данных и управления информационным потоком между устройствами.

Основная часть: Традиционное назначение цифровых цепей RS-232:

1. SOUT (Serial Output) - выход передатчика
2. SIN (Serial Input) - вход приемника
3. RTS (Request to Send) - сигнал-запрос от UART к модему о передаче байта
4. CTS (Clear to Send) - сигнал-подтверждение от модема к UART о готовности принять байт для передачи
5. DSR (Data Set Ready) - сигнал от модема к UART о готовности к взаимодействию
6. DTR (Data Terminal Ready) - сигнал от UART к модему о готовности к взаимодействию
7. DCD (Data Carrier Detect) - сигнал от модема к UART об обнаружении данных
8. RI (Ring Indicator) - сигнал от модема к UART об обнаружении входящего телефонного звонка

Служебные цепи RS-232 позволяют организовать контроль информационного потока (flow control), предотвращая переполнение приемника и приостанавливая быстрый передатчик. Практически все служебные цепи напрямую связаны с регистрами управления и состояния UART 16550, что позволяет реализовать алгоритмы контроля программно, например, в драйверах операционных систем.

Вывод: Цепи RS-232 играют важную роль в обеспечении эффективной передачи данных и управлении информационным потоком между устройствами, обеспечивая надежную работу компьютерных систем и периферийных устройств.

14. Ассинхронный режим работы com-порта

Введение: Асинхронный режим работы COM-порта обеспечивает передачу данных с использованием минимальной неделимой единицы, называемой байтом. Этот режим позволяет надежно передавать данные, обеспечивая синхронизацию между передатчиком и приемником.

Основная часть: Атомарной единицей, с которой работает как UART, так и USART, является байт, причем один байт может содержать от 5 до 8 битов. По умолчанию линия находится в состоянии логической единицы. При наличии байта для передачи передатчик переводит линию в состояние логического нуля, то есть передает старт-бит, что сигнализирует приемнику о начале передачи данных. Стоп-бит необходим для гарантированного возврата линии в исходное состояние (логическая единица) после передачи данных. Старт-бит всегда один, а стоп-битов может быть один, полтора либо два.

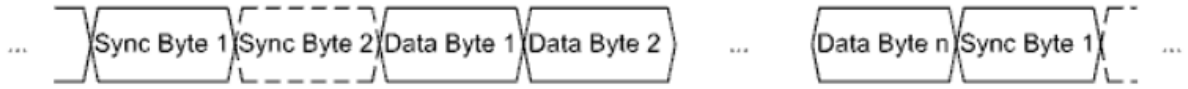
Для проверки целостности данных может использоваться бит паритета. Бит паритета формируется в зависимости от настроек проверки, обеспечивая четное или нечетное количество единиц или нулей в данных. Например, если включена проверка единиц на четность (even), то бит паритета формируется таким образом, чтобы общее число единиц было четным. Ошибки отслеживаются приемником.

Вывод: Асинхронный режим работы COM-порта обеспечивает надежную передачу данных, используя старт-бит, стоп-бит и бит паритета для синхронизации и проверки целостности данных. Этот режим широко используется для связи между различными устройствами.

15. Синхронный режим работы com-порта

Введение: Синхронный режим работы COM-порта позволяет передатчику и приемнику работать в синхронном режиме, обеспечивая постоянную передачу данных и их синхронизацию.

Основная часть: При простое передатчик заполняет линию специальными байтами синхронизации, тем самым настраивая приемник. Все поступающие байты передаются без обрамления. Ошибки отслеживаются приемником. При обнаружении ошибок, возникающих из-за фазовых сдвигов, приемник должен каким-либо дополнительным способом приостановить передатчик, чтобы тот вновь заполнил линию байтами синхронизации.



Вывод: Синхронный режим работы COM-порта обеспечивает постоянную передачу данных и их синхронизацию, используя специальные байты синхронизации и механизмы обнаружения и исправления ошибок.

16. Тактирование com-порта

Введение: Тактирование COM-порта является важным аспектом его функционирования, обеспечивая синхронизацию передачи данных и управление частотой передачи.

Основная часть: Тактирование сдвиговых регистров UART 16550 осуществляется с помощью встроенного программируемого бод-генератора (baud generator). Бод-генератор представляет собой программируемый делитель частоты. Выходная частота бод-генератора Fout определяется по формуле:

$$Fout=Fin/16\cdot DL$$

где Fin — входная частота, DL — шестнадцатибитная константа, старшая и младшая части которой хранятся в двух регистрах UART (DLL и DLM).

На вход бод-генератора поступает меандр, получаемый от внешнего кварцевого резонатора, который тактирует и сам автомат UART. Частота тактирования автомата UART по крайней мере в 16 раз больше Fout. Для правильного расчета DL необходимо точно знать Fin. В

современных Super I/O эта частота может достигать 48 MHz. При делении частоты BIOS конфигурирует UART, приводя Fin к классическому значению 1,843 MHz. При DL = 1 (нулевое значение DL использовать не рекомендуется), Fout = 115200 Hz.

Вывод: Тактирование COM-порта с использованием бод-генератора обеспечивает синхронизацию и управление частотой передачи данных. Правильная настройка частоты важна для надежной и эффективной работы COM-порта.

17. Архитектура COM-портов ПК

Введение: Архитектура COM-портов ПК играет ключевую роль в обеспечении взаимодействия между устройствами и процессором. Для стандарта RS-232 зарезервированы определенные порты и аппаратные прерывания.

Основная часть: В стандартной архитектуре для RS-232 зарезервированы следующие порты в адресном пространстве ввода-вывода процессора: 3F8-3FF и 2F8-2FF в шестнадцатеричной системе счисления. По этим адресам хранятся регистры портов, и предусмотрена возможность работы по прерываниям. Стандартными аппаратными прерываниями для COM1 и COM2 являются IRQ4 и IRQ3 соответственно, хотя их можно изменить.

Register Address Access (AEN = 0)		Abbreviation	Register Name	Access
Base +	DLAB			
0h	0	THR	Transmit Holding Register	WO
0h	0	RBR	Receiver Buffer Register	RO
0h	1	DLL	Divisor Latch LSB	R/W
1h	1	DLM	Divisor Latch MSB	R/W
1h	0	IER	Interrupt Enable Register	R/W
2h	—	IIR	Interrupt Identification Register	RO
2h	—	FCR	FIFO Control Register	WO
3h	—	LCR	Line Control Register	R/W
4h	—	MCR	Modem Control Register	R/W
5h	—	LSR	Line Status Register	R/W
6h	—	MSR	Modem Status Register	R/W
7h		SCR	Scratch Pad Register	R/W

Вывод: Понимание архитектуры COM-портов и зарезервированных портов и прерываний является важным для эффективного испол
ьзования и настройки этих интерфейсов в ПК.

18. Стандарты, близкие к RS-232

Введение: С развитием технологий были разработаны новые стандарты передачи данных, близкие к RS-232. RS-422 и RS-485 стали закономерным продолжением стандарта RS-232, обеспечивая улучшенные характеристики.

Основная часть: RS-422 и RS-485 можно рассматривать как развитие RS-232. Основные сравнительные характеристики этих стандартов приведены в таблице:

Характеристика	RS-232	RS-422	RS-485
Способ передачи сигнала	Изменение потенциала относительно земли	Дифференциальная пара	Дифференциальная пара
Направление передачи	Одностороннее, двустороннее	Одностороннее, двустороннее	Одностороннее, двустороннее
Максимальное количество передатчиков	1	1	32
Максимальное количество приемников	1	10	32
Ориентировочная максимальная пропускная способность	1 Mbit/s	10 Mbit/s	10 Mbit/s
Ориентировочное максимальное расстояние	15 m	1200 m	1200 m

Для передачи данных посредством интерфейса RS-485 требуются специальные трансиверы с гальванической развязкой, обеспечивающие дифференциальный способ передачи сигнала. Гальваническая развязка может быть либо трансформаторной, либо оптронной. В качестве среды передачи данных обычно используют витую пару и разъемы типа RJ.

Вывод: Стандарты RS-422 и RS-485 предоставляют улучшенные характеристики по сравнению с RS-232, включая большую пропускную способность и дальность передачи, что делает их подходящими для различных приложений.

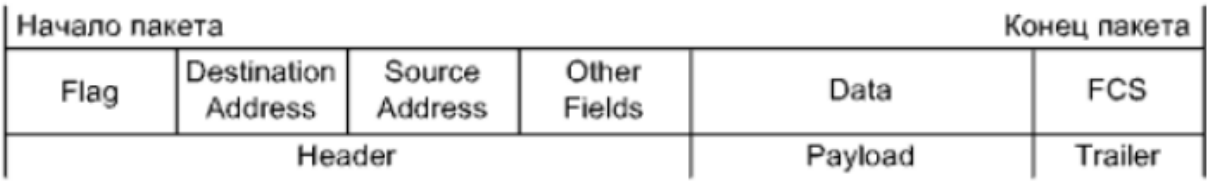
19. Структура типового пакета компьютерной сети

Введение: Структура типового пакета компьютерной сети включает в себя различные поля, которые играют важную роль в обеспечении правильной передачи данных и контроля их целостности.

Основная часть: Назначение полей пакета:

- Flag - флаг начала пакета
- Destination Address - адрес назначения
- Source Address - адрес источника
- Other Fields - прочие поля, включая специфические поля и флаги определенной реализации
- Data – данные, «полезное» наполнение пакета
- FCS (Frame Check Sequence) - контрольная сумма, позволяющая проверить целостность пакета

Часть пакета до начала данных называется заголовком (header), а часть после данных – хвостовиком (trailer). В байто-ориентированных реализациях длина пакета кратна восьми битам, то есть пакет состоит из октетов. Все поля пакета можно разделить на полезные и служебные. Полезная нагрузка заключается в данных, но данные могут носить служебный характер. В некоторых пакетах поле данных может отсутствовать. Количество дополнительного трафика, порождаемого служебными полями, оценивается как overhead.

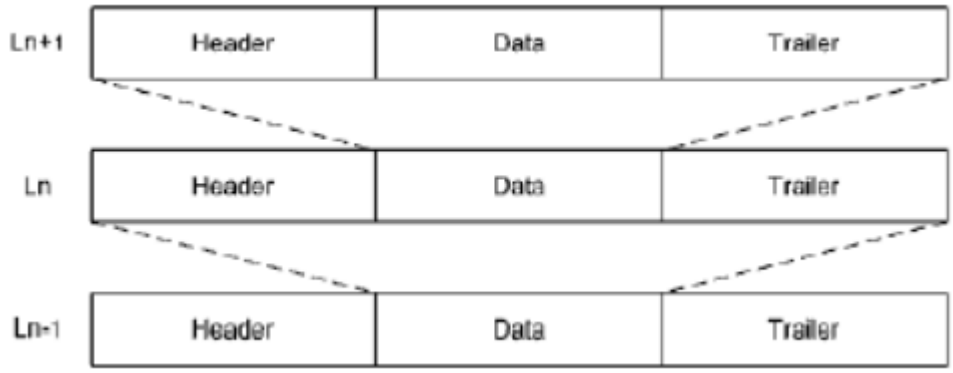


Вывод: Структура типового пакета компьютерной сети и назначение его полей обеспечивают надежную передачу данных и контроль их целостности, что является ключевым аспектом работы сетей

20. Инкапсуляция и ее проявления в компьютерных сетях

Введение: Инкапсуляция является важным процессом в компьютерных сетях, обеспечивающим эффективную передачу данных между уровнями сетевой модели. Этот процесс включает вкладывание пакета вышестоящего уровня в пакет нижестоящего уровня при подготовке к передаче.

Основная часть: Под инкапсуляцией понимают вкладывание пакета определенного вышестоящего уровня в поле данных пакета смежного нижестоящего уровня в процессе подготовки к передаче, то есть при продвижении сверху вниз. Под декапсуляцией понимают обратное действие после приема, то есть при продвижении снизу вверх.



Функционал любого из вышестоящих уровней "знает", какие нижестоящие ресурсы ему необходимы и чем он располагает. Поэтому процесс инкапсуляции не доставляет трудностей. Функционал нижестоящего уровня при разборе полученных пакетов заранее не знает, какой из вышестоящих подсистем передавать эти пакеты. Проблему решают введением в структуру пакета служебного поля, в котором записывается код протокола вышестоящего уровня.

Инкапсуляция также позволяет организовывать туннелирование, передавая пакеты одного протокола через пакеты другого протокола того же уровня. Если данные не помещаются в поле отведенной длины, используется фрагментация - разбивка данных на фрагменты и их передача цепочкой пакетов. Принимающая сторона выполняет дефрагментацию. Перемежение позволяет "распараллелить" пересылку пакетов или их фрагментов, задействуя несколько каналов, что особенно важно для низкоскоростных сред передачи данных.

Вывод: Инкапсуляция и декапсуляция являются ключевыми процессами в компьютерных сетях, обеспечивающими эффективную передачу и обработку данных. Эти процессы включают фрагментацию, туннелирование и перемежение, что делает сети более гибкими и эффективными.

21. Бит-стаффинг

Введение: Бит-стаффинг является методом кодирования данных, используемым для обеспечения уникальности флаговых последовательностей и предотвращения ошибок в передаче данных.

Основная часть: При бит-стаффинге совпадающая с флагом последовательность разбивается с помощью вставки дополнительного бита с соответствующим значением. Применение бит-стаффинга увеличивает длину пакета. Чтобы уменьшить связанные с бит-стаффингом издержки, следует минимизировать количество вставок, вставляя разбивающий бит после наиболее длинной уникальной подпоследовательности в флаговой последовательности.

Классическим флагом начала пакета является байт со значением 01111110 b (7Eh).

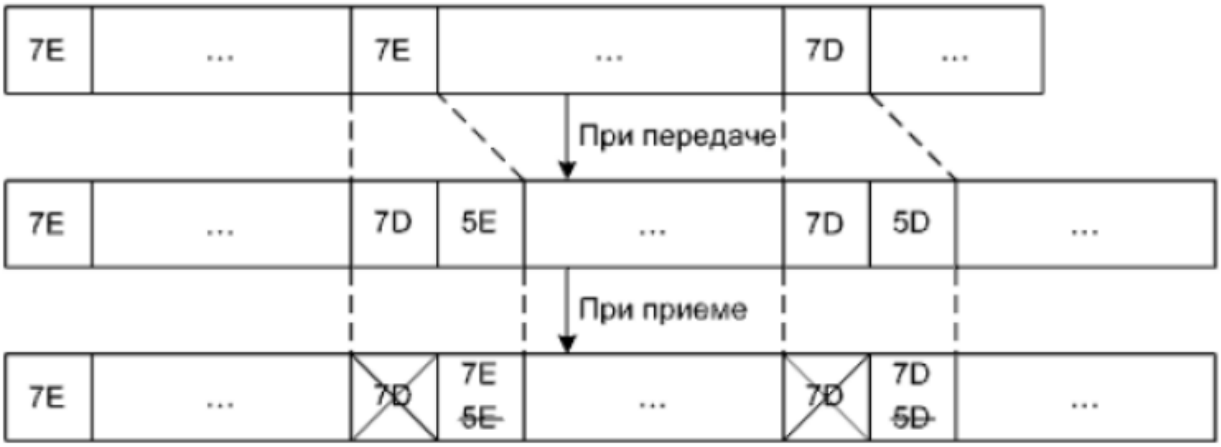
На передающей стороне после нуля и шести единиц всегда вставляется седьмая единица, а на принимающей стороне единица после нуля и шести единиц всегда удаляется. Бит-стаффинг используется при задействовании синхронных сред передачи данных.

Вывод: Бит-стаффинг является эффективным методом кодирования, позволяющим обеспечить уникальность флаговых последовательностей и избежать ошибок в передаче данных в синхронных средах передачи данных.

22. Байт-стаффинг

Введение: Байт-стаффинг является более сложным методом кодирования по сравнению с бит-стаффингом. Этот метод используется для обеспечения уникальности флаговых байтов и предотвращения ошибок в асинхронных средах передачи данных.

Основная часть: Алгоритмы байт-стаффинга манипулируют байтами, являются более сложными и затратными, но при программировании позволяют избежать битовых операций.



Единственным способом обеспечения уникальности флагового байта является замена совпадающего байта на другой выбранный байт. Принимающая сторона отличает замененный байт от незамененного с помощью ESC символа. Наличие ESC символа говорит станции-приемнику о замене, а следующий за ESC символ код замены позволяет определить, какая замена была осуществлена. Байт-стаффингу можно подвергать целые группы символов.

Байт-стаффинг применяют при задействовании асинхронных сред передачи данных.

Вывод: Байт-стаффинг является сложным, но эффективным методом кодирования, используемым для обеспечения уникальности флаговых байтов и предотвращения ошибок в асинхронных средах передачи данных, что позволяет реализовать надежную передачу данных.

23. Особенности линейного кодирования и классификация линейных кодов, применяемых в компьютерных сетях

Введение: Линейное кодирование используется для преобразования битовых последовательностей, чтобы обеспечить надежную передачу данных. Одной из основных причин разработки линейных кодов является проблема девиации несущей, возникающая при передаче данных.

Основная часть: Девиация несущей происходит, когда передатчик и приемник работают на разных частотах, что приводит к фазовым сдвигам и ошибкам передачи. Современные системы используют блоки фазовой автоподстройки частоты (ФАПЧ) для автоматической синхронизации. Все линейные коды направлены на преобразование битовых последовательностей таким образом, чтобы в линии постоянно происходили изменения, обеспечивая равномерное распределение нулей и единиц.

Классификация линейных кодов основывается на следующих факторах:

1. Кодирование уровнями либо переходами
2. Наличие инвертирования

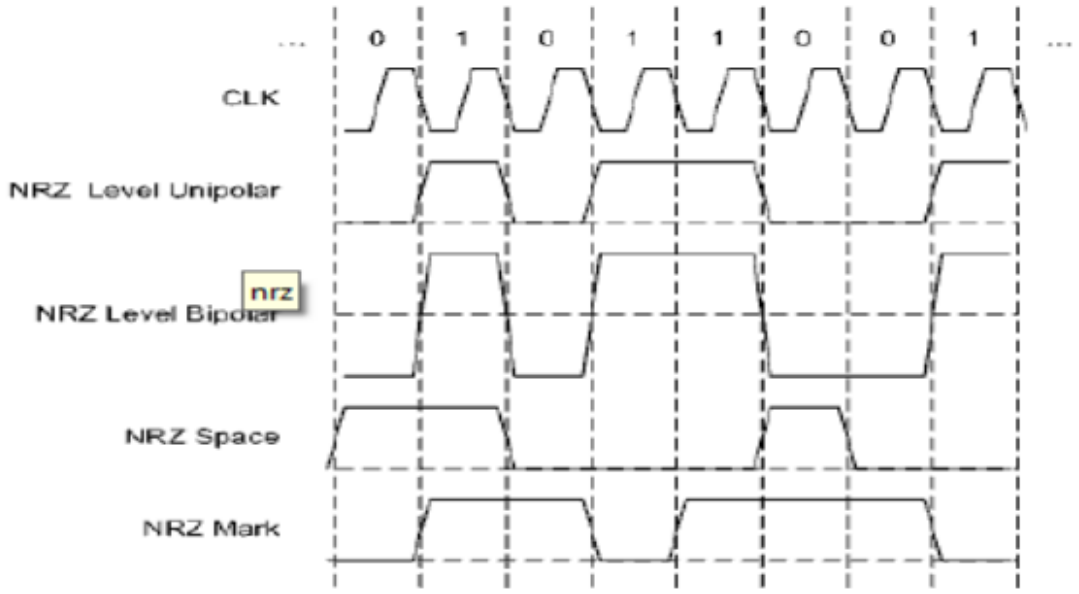
3. Однополярность либо многополярность
4. Наличие возврата к нулю
5. Наличие самосинхронизации
6. Наличие перестановки или подмены битов

Вывод: Линейное кодирование и классификация линейных кодов играют важную роль в обеспечении надежной передачи данных, решая проблемы девиации несущей и обеспечивая синхронизацию между передатчиком и приемником.

24. Линейные коды без возврата к нулю и с возвратом к нулю

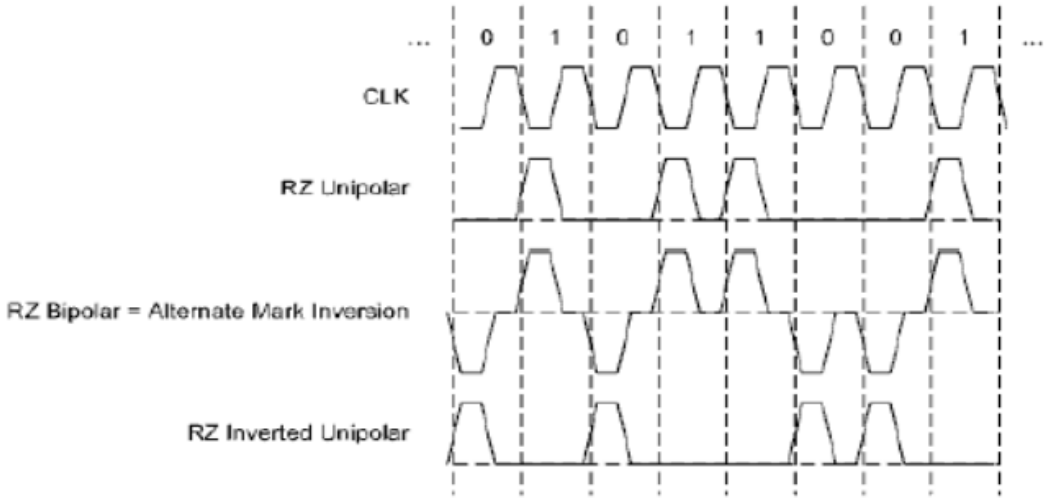
Введение: Линейные коды используются для кодирования данных в компьютерных сетях. Существуют коды без возврата к нулю (NRZ) и с возвратом к нулю (RZ).

Основная часть: NRZ коды изменяют уровни между тактами. В простых случаях логические уровни не преобразуются или инвертируются. Более сложные случаи включают space и mark варианты. Space-вариант: ноль во входной последовательности кодируется сменой уровня, единица - сохранением уровня. Mark-вариант: единицы приводят к переключению уровней. Space и mark инверсны друг другу. NRZ коды могут быть однополярными и двухполярными, и требуют дополнительной цепи для тактирования.



Примеры технологий с применением NRZ: RS-232, USB, HDLC.

RZ коды изменяют уровни между тактами, но на половине каждого такта происходит возврат к нулю. Двухполярные RZ коды обладают свойством самосинхронизации.



Примеры технологий с применением RZ: IrDA.

Вывод: NRZ и RZ коды обеспечивают различные способы кодирования данных, используемые в различных технологиях для передачи данных в компьютерных сетях.

25. Манчестерские и многоуровневые линейные коды

Введение: Манчестерские и многоуровневые линейные коды используются для кодирования данных, обеспечивая самосинхронизацию и надежную передачу данных в различных технологиях сетей.

Основная часть: Манчестерские коды выражаются в переходах между уровнями во время тактов, поэтому их иногда называют фазовыми кодами. Есть два «равноправных» варианта манчестерского кода:

1. Ноль во входной последовательности заменяется на переход от единицы к нулю, а единица заменяется на переход от нуля к единице.
2. Либо наоборот.

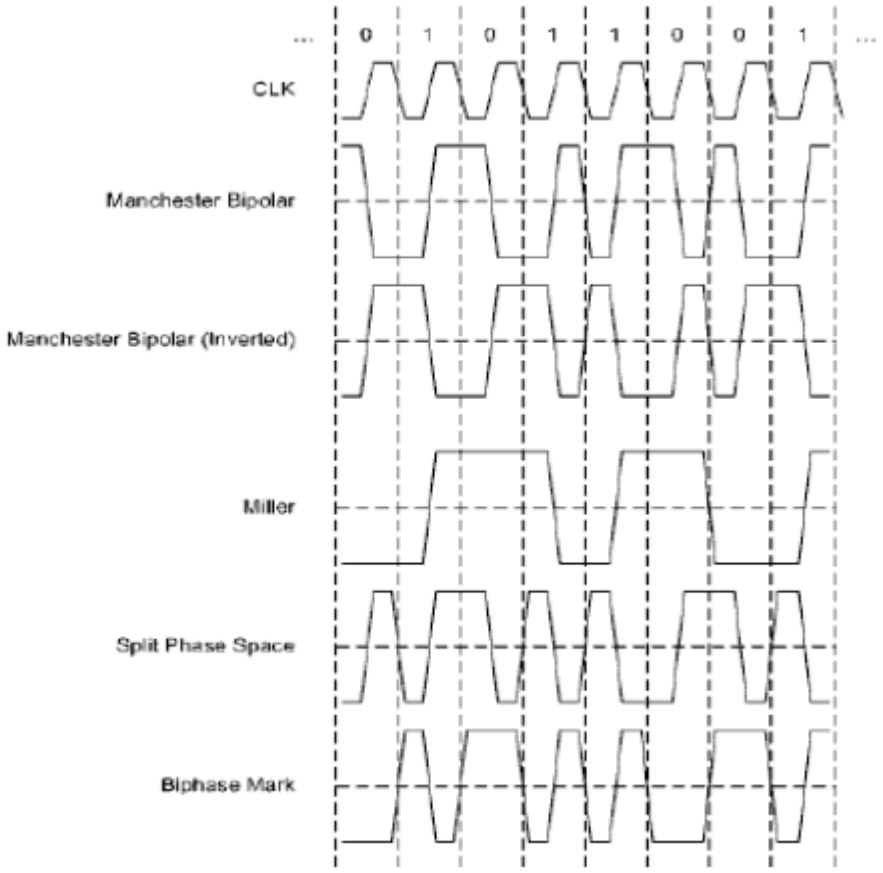
Манчестерские коды обладают свойством самосинхронизации.

Существуют несколько кодов, близких к манчестерским:

1. Код Миллера (Miller): Ноль соответствует отсутствию перехода во время такта, единица соответствует переходу во время такта, плюс между двумя нулями всегда выполняется смена уровня.
2. Split Phase код: Учитывает направление предыдущего перехода. При space-варианте ноль соответствует переходу во время такта в противоположном направлении,

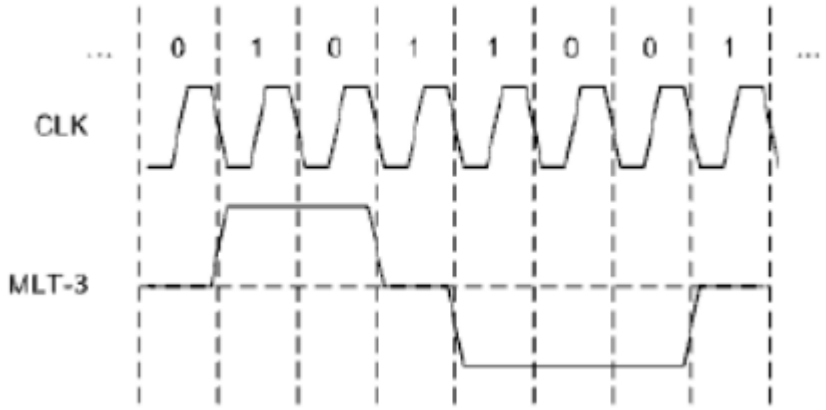
единица – в совпадающем направлении. При mark-варианте роли нулей и единиц инвертируются.

3. Biphase код: Кроме возможных переходов во время тактов, всегда выполняется смена уровня между тактами. При space-варианте ноль соответствует переходу во время такта, единица – отсутствию перехода. При mark-варианте роли нулей и единиц инвертируются.



Примеры технологий с применением манчестерских кодов: Ethernet, Token Ring, некоторые IR-технологии.

MLT коды выражаются в переключении между несколькими уровнями между тактами. Например, код MLT-3 имеет три уровня: -1, 0, +1. Кодирование может начинаться с нуля. Ноль в исходной последовательности кодируется сохранением текущего уровня, а единица – переходом к соседнему уровню (с сохранением направления, если это возможно).



Примеры технологий с применением MLT-кодов: Fast Ethernet, FDDI.

Вывод: Манчестерские и многоуровневые линейные коды обеспечивают самосинхронизацию и надежную передачу данных в различных сетевых технологиях, что делает их эффективными для использования в компьютерных сетях.

26. Блочные линейные коды

Введение: Блочные линейные коды используются для замены блоков битов из входной последовательности на большие блоки битов в выходной последовательности. Эти коды могут комбинироваться с другими линейными кодами и часто включают контрольные последовательности для управления данными.

Основная часть: Блочные коды выражаются в замене блоков битов из входной последовательности на большие (как правило) по размеру блоки битов в выходной последовательности. Блочные коды могут комбинироваться с вышеперечисленными кодами. В связи с избыточностью блочных кодов, во многих из них предусмотрены контрольные последовательности, которые, по сути, являются управляющими символами.

Первым примером может служить код 4b/5b, применяемый в Fast Ethernet и CDDI. Более сложным примером может служить код 8b/10b, применяемый в оптических вариантах Gigabit Ethernet. Биты входного блока обозначают как ABCDEFGH от младшего к старшему, выходного abcdefghij также от младшего к старшему. Входной блок разбивается на два подблока: x из пяти битов и y из трех битов. Поэтому выходной код представляет собой конкатенацию двух кодов 5b/6b и 3b/4b. Кроме блоков данных D, имеются контрольные блоки K, которые кодируют альтернативно. Таким образом, входной блок обозначают как Dx.y либо Kx.y. В код 8b/10b заложена гибкая система уравнивания количества нулей и количества единиц, заключающаяся в динамическом выборе блока для замены (одного из двух) исходя из текущего значения RD (Running Disparity). Предусмотрено два значения RD -1 и +1. При выборе текущего значения RD учитывается предыдущее значение RD и соотношение нулей и единиц во входном блоке (плюс есть исключения).

Вывод: Блочные линейные коды обеспечивают гибкость и надежность передачи данных, используя контрольные последовательности и динамическое уравнивание нулей и единиц. Эти коды широко применяются в современных сетевых технологиях.

27. Поля Галуа и их применение в компьютерных сетях

Введение: Поля Галуа (GF) используются в математике для операций над конечными множествами чисел. В компьютерных сетях поля Галуа применяются для обеспечения надежности и защиты данных.

Основная часть: Поле GF(p) из целых чисел 0, 1, p-1, порожденное в результате отображения f. Z/p->GF(p), где Z/p - факторкольцо множества целых чисел, в котором роль идеала играет простое число p, называют полем Галуа (Galois field) порядка p. При вычислениях с элементами поля Галуа используют целочисленную арифметику с приведением по соответствующему модулю.

Для практического применения полей Галуа в компьютерных системах необходимо перейти от скалярного представления к векторному. Расширенное поле Галуа GF(p^n) можно рассматривать как векторное пространство, где простое число p является характеристикой поля и соответствует количеству состояний разряда вектора, а n является степенью поля над его простым подполем и соответствует количеству разрядов вектора. Поскольку в обычных компьютерных системах разряды регистров бинарные, то наибольший интерес представляют поля GF(2^n).

Сложение бинарных векторов (совпадает с вычитанием) соответствует поразрядной операции xor. С умножением и делением дела обстоят сложнее. Скалярное произведение не подходит, так как его результат может выйти за пределы поля. Векторное произведение определено только для трехразрядных векторов. Полиномиальное представление также не решает проблему, так как произведение полиномов выводит за пределы поля. Для обеспечения конечности поля Галуа, полученный полином нужно привести путем деления на выбранный полином степени n. Выбранный для построения поля Галуа полином называют порождающим (образующим).

Деление векторов в математике не известно. После перехода на язык полиномов деление всегда должно быть безостаточным. Деление можно представить как умножение полинома на полином, обратный делителю. Для достижения цели порождающий полином должен быть неприводимым по модулю p.

Вывод: Поля Галуа обеспечивают математическую основу для операций с конечными множествами чисел, что позволяет применять их для кодирования и защиты данных в компьютерных сетях, обеспечивая надежность и целостность информации.

28. Модель помехоустойчивого канала связи и теорема Шеннона

Введение: Теорема Шеннона положила начало помехоустойчивому кодированию, утверждая, что любой дискретный канал связи имеет конечную пропускную способность и может использоваться для передачи информации с высокой степенью достоверности, несмотря на наличие помех.

Основная часть: Передаваемое сообщение разбивается на блоки фиксированного размера a из k битов a1, a2, … ak. Кодер выполняет функцию f, называемую схемой кодирования, и тем самым преобразует вектор a в вектор c из n битов c1, c2, … cn, называемый кодовым словом. В процессе пересылки кодового слова по каналу связи на него накладывается вектор ошибок e, в котором единичные биты соответствуют искажениям. После применения декодером схемы декодирования g получается вектор a', в идеале совпадающий с исходным вектором a.

Подобная схема кодирования является избыточной. На практике всегда ищут компромисс между степенью обеспечения достоверности при передаче и вычислительной сложностью кодов, что в первую очередь отражается на скорости декодирования. В компьютерных сетях множество кодовых слов получается из множества исходных слов как отображение из конечного поля GF(2^k) в конечное поле GF(2^n). При более простых схемах кодирования в кодовом слове сначала располагаются биты входного сообщения (информационные), а за ними - дополнительные проверочные биты a1, a2, … ak, битов c1, c2, … cn. В более сложных случаях проверочные биты чередуются с информационными.

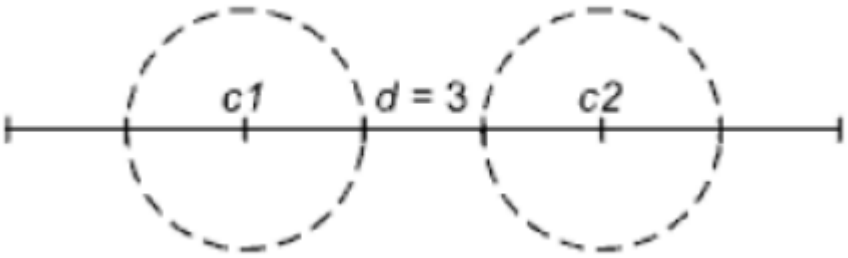
Вывод: Теорема Шеннона и модель помехоустойчивого канала связи обеспечивают основу для кодирования и передачи данных с высокой степенью достоверности, что является ключевым аспектом работы современных компьютерных сетей.

29. Линейные помехоустойчивые коды, включая коды Хэмминга и циклические коды

Введение: Перед выбором того или иного помехоустойчивого кода нужно определить, сколько бинарных ошибок код должен обнаруживать и сколько бинарных ошибок код должен исправлять. Эти параметры определяются расстоянием Хэмминга и весом Хэмминга.

Основная часть: Число координат (позиций), которыми два вектора x и y различаются, называется расстоянием Хэмминга – d(x,y). Число ненулевых позиций вектора x называют весом Хэмминга w(x). Расстояние Хэмминга показывает количество возникших ошибок. Для

увеличения корректирующей способности кода следует стремиться увеличивать расстояния между кодовыми словами. Минимальное расстояние dmin называют кодовым и оно является важной характеристикой помехоустойчивого кода. Согласно теореме, для того чтобы линейный код исправлял t ошибок, должно выполняться условие: dmin>=2t + 1. Для того чтобы линейный код обнаруживал t ошибок, должно выполняться условие dmin>=t + 1.



Бинарным кодом Хэмминга называют код длины n = 2^m – 1, m >=2 с проверочной матрицей H размером m × (2^m – 1), в которой столбцы соответствуют записи 1, 2 … 2^m-1 в двоичной системе счисления. Код Хэмминга позволяет исправлять одиночную ошибку и обнаруживать множественные ошибки.

Циклические коды являются подгруппой линейных кодов. Циклическим кодом называют линейный код, удовлетворяющий дополнительному условию: если вектор a0, a1 … an-1 является кодовым словом, то и его циклический сдвиг an-1, a0 … an-2 также является кодовым словом. Циклический код позволяет исправлять одну и более ошибок и обнаруживать множественные ошибки (в зависимости от параметров). Базовая идея циклического кодирования состоит в том, чтобы в качестве проверочных битов передавать остаток от деления информационных битов на некоторое выбранное число. После приема снова выполняется деление уже возможно искаженных информационных битов на то же самое число и сравниваются остатки. Если остатки совпадают, то данные с определенной вероятностью приняты без ошибок.

Деление выполняется по правилам арифметики полей Галуа, без учета переносов. Информационные биты соответствуют информационному полиному, делитель - порождающему полиному. Частное в процессе кодирования не используется и "отбрасывается". Для разнообразия остатков порождающий полином должен выбираться неприводимым полиномом. Существуют два подхода к реализации циклического кода на стороне приемника:

1. Согласно базовой идее, описанной выше.
2. На порождающий полином делится все принятое кодовое слово. Если ошибка не произошла, остаток будет нулевым. Оба подхода равноценны.

Вывод: Линейные помехоустойчивые коды, такие как коды Хэмминга и циклические коды, обеспечивают надежную коррекцию и обнаружение ошибок, что является ключевым аспектом обеспечения целостности и точности передачи данных в компьютерных сетях.

30. Классификация помехоустойчивых кодов

Введение: Помехоустойчивые коды классифицируются на основе различных методов кодирования и коррекции ошибок. Они играют важную роль в обеспечении надежности передачи данных.

Основная часть: Основные группы помехоустойчивых кодов:

1. Линейные коды, включая коды Хэмминга, циклические коды, БЧХ-коды (коды Боуза-Чоудхури-Хоквингема), РМ коды (коды Рида-Маллера), итеративные коды, коды на основе матриц Адамара, симплексные коды и некоторые другие.
2. Коды для контроля модульных и пакетных ошибок, включая РС-коды (коды Рида-Соломона), низкоплотные модульные коды, векторные модульные коды, итеративные модульные коды и некоторые другие.
3. Свёрточные коды.
4. Арифметические коды.
5. Низкоскоростные коды, включая коды максимальной длины, нелинейные коды, D-коды и некоторые другие.

Вывод: Классификация помехоустойчивых кодов охватывает широкий спектр методов и подходов, обеспечивающих надежность и целостность передачи данных в различных сетевых приложениях.

31. Классификация каналов в сети передачи данных

Введение: Каналы передачи данных классифицируются на основе направленности и метода использования. Эта классификация помогает определить, как данные передаются и разделяются в сети.

Основная часть: С точки зрения направленности, последовательный канал может функционировать в одном из трех режимов:

1. Симплексный – передача данных по каналу возможна только в одном направлении.
2. Полудуплексный – данные могут передаваться в обоих направлениях, но в один момент времени возможна передача только в одном направлении.
3. Полнодуплексный – данные могут передаваться в обоих направлениях одновременно.

Сейчас в КС доминируют полнодуплексные каналы.

Последовательный канал может быть:

1. Выделенным – зарезервирован за определенной парой станций абонентов.
2. Разделяемым – может использоваться несколькими станциями-абонентами.

Канал, который не может разделяться несколькими станциями-передатчиками одновременно, в отечественной литературе принято называть моноканалом. Во многих реализациях ситуация именно такая.

Вывод: Классификация каналов в сети передачи данных помогает определить способ и направленность передачи данных, а также их использование и разделение между станциями, что является важным аспектом организации сетевой коммуникации.

32. Логические и физические топологии LAN

Введение: Топология «возникает» на канальном уровне, когда речь идет об организации сегмента. Топологии делятся на различные типы в зависимости от структуры и способа соединения устройств.

Основная часть: Прежде всего, топологии делят на два типа:

1. Point-to-point - топология «точка к точке» связывает только две станции.
2. Multi-access (multipoint to multipoint) - топология с множественным доступом связывает более двух станций.

Эти два типа позволяют организовывать двунаправленные каналы между любым требующимся количеством абонентов, поэтому их реализуют наиболее часто. Применительно к однонаправленным каналам можно добавить еще два пункта:

1. Point-to-multipoint – иногда.
2. Multipoint-to-point – очень редко.

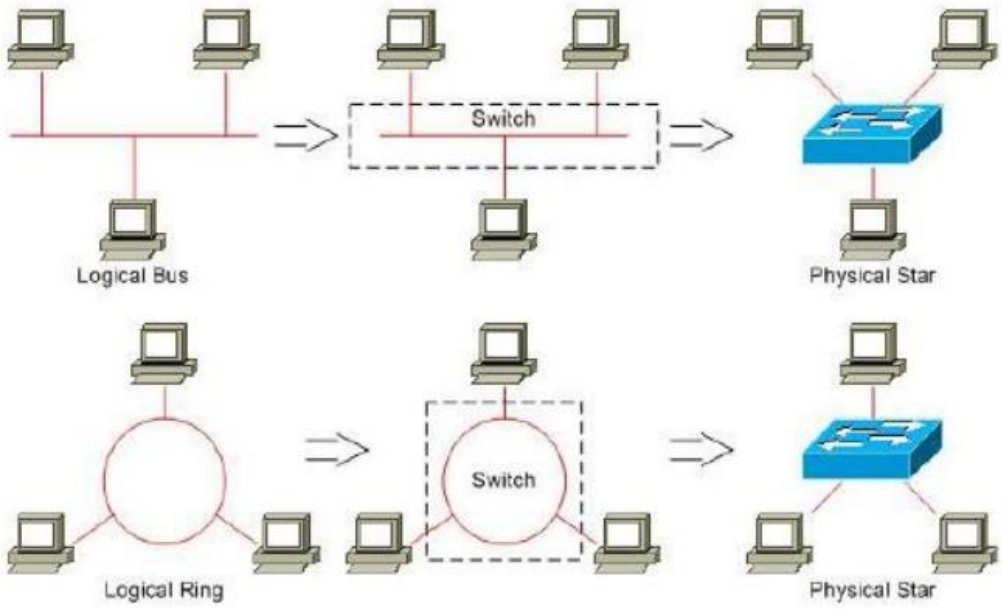
Менее двух станций в сегменте быть не может. Если топологически классифицировать аппаратные технологии, то есть еще два ракурса:

1. Физическая топология – отражает физические связи между устройствами.
2. Логическая топология – отражает логические связи между устройствами.

Характерными топологиями ЛКС (LAN) являются:

1. Шина – все компьютеры параллельно подключаются к одной линии связи. Информация от каждого компьютера передается всем остальным.
2. Кольцо – компьютеры последовательно соединены в кольцо. Передача в кольце производится всегда только в одном направлении. Каждый компьютер передает информацию только одному, следующему за ним.
3. Звезда – к одному центральному компьютеру присоединяются остальные периферийные компьютеры, причем каждый из них использует отдельную линию связи. Информация от периферийного компьютера передается только центральному компьютеру, от центрального – одному или нескольким периферийным.

Часто логическая топология не совпадает с физической. Примеры несоответствий между физической и логической топологиями.



Вывод: Логические и физические топологии LAN определяют способ соединения и взаимодействия устройств в сети, играя ключевую роль в организации сетевой инфраструктуры.

33. Логические и физические топологии WAN и RAS

Введение: Топология «возникает» на канальном уровне, когда речь идет об организации сегмента. Топологии делятся на различные типы в зависимости от структуры и способа соединения устройств.

Основная часть: Прежде всего, топологии делят на два типа:

1. Point-to-point - топология «точка к точке» связывает только две станции.
2. Multi-access (multipoint to multipoint) - топология с множественным доступом связывает более двух станций.

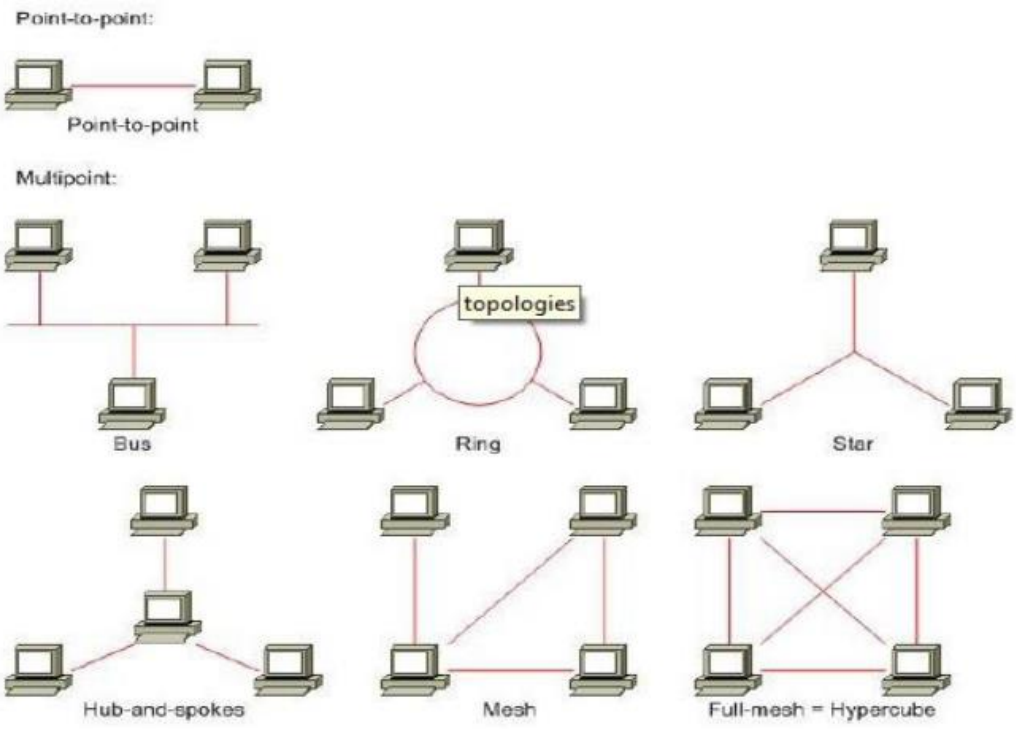
Эти два типа позволяют организовывать двунаправленные каналы между любым требующимся количеством абонентов, поэтому их реализуют наиболее часто. Применительно к однонаправленным каналам можно добавить еще два пункта:

1. Point-to-multipoint – иногда.
2. Multipoint-to-point – очень редко.

Менее двух станций в сегменте быть не может. Характерными топологиями ГКС (WAN) являются:

1. Сеть (произвольно связанная) (mesh)
2. Ступица со спицами (hub-and-spokes)
3. Полносвязная сеть (full-mesh)

Характерной RAS (Remote Access Server) топологией является point-to-point. Для ГКС-технологий существует только одна типичная топология (произвольно связанная сеть), остальные можно рассматривать как ее частные случаи.



Топологии КС с детализацией до станций и СрПД

Вывод: Логические и физические топологии WAN и RAS определяют способ соединения и взаимодействия устройств в сети, обеспечивая эффективное распределение ресурсов и доступ к удаленным серверам.

34. Особенности случайных методов доступа к моноканалу

Введение: Случайные методы доступа к моноканалу используются для управления передачей данных в сети, однако они могут столкнуться с проблемой коллизий между конкурирующими передатчиками.

Основная часть: Проблема заключается в «столкновениях» конкурирующих передатчиков. Если два или более передатчиков одновременно выдают сигналы в среду передачи данных (СрПД), возникает противоречие, называемое коллизией. Коллизия может быть как логической (информационный конфликт), так и физической (несовместимые физические процессы).

Классическим способом защиты оборудования от коллизий является гальваническая развязка (трансформаторная или оптронная). При попытках установить разные уровни наблюдаются эффекты «зануления» и «заединичивания». Коллизии затрагивают только станции, подключенные к одной СрПД (сегмент сети). Сегмент, в котором возможно возникновение коллизий, называется доменом коллизий.

Физические свойства СрПД не позволяют мгновенно передавать сигналы, поэтому коллизия распространяется по сегменту с конечной скоростью. Окно коллизий (collision window) - временной интервал, в течение которого станция гарантированно обнаруживает коллизию, равный удвоенному времени прохождения сигнала между двумя максимально удаленными станциями.

Существуют два подхода к проблеме коллизий:

1. Не допускать коллизии, используя детерминированные методы доступа к моноканалу.
2. Допускать коллизии и выходить из них, используя случайные методы доступа к моноканалу.

Во втором случае также можно выделить два подхода:

1. Не обращать внимание на причины коллизий, сосредоточившись на способах выхода из них.
2. Пытаться предотвращать коллизии, минимизируя их количество, и «тяжело» выходить из них, если они возникают.

Таким образом, все методы доступа к моноканалу делят на:

1. Случайные.
2. Детерминированные.

На эффективность случайных методов влияют следующие факторы:

1. Количество взаимодействующих станций.
2. Инертность среды передачи данных.
3. Длина кадра.
4. Частота синхронизации.

Вывод: Случайные методы доступа к моноканалу обеспечивают гибкость и возможность выхода из коллизий, однако их эффективность зависит от множества факторов, включая количество станций и характеристики среды передачи данных.

35. CSMA/CD (Ethernet)

Введение: CSMA/CD (Carrier Sense Multiple Access with Collision Detection) – это классический алгоритм множественного доступа с прослушиванием несущей и обнаружением коллизий, описанный в стандарте Ethernet (IEEE 802.3). Этот алгоритм является наглядным примером случайных методов доступа к моноканалу.

Основная часть: Задержка перед началом очередной попытки передачи после коллизии измеряется в так называемых слот таймах, количество которых является случайным целым числом rr (0 ≤\le rr ≤\le 2k2^k), где k=min⁡(n,10)k = \min (n, 10), а nn – номер попытки. После превышения счетчиком попыток порогового значения дальнейшие попытки считаются бесперспективными. Значение kk не может быть больше 10.

Качество диспетчеризации при обработке коллизий зависит от слот тайма, минимальной неделимой единицы времени при диспетчеризации. Он должен быть больше суммы удвоенного времени прохождения сигнала по сегменту и времени передачи jam-сигнала.

Механизм ускорения распределенного обнаружения коллизий, заложенный в стандарт, заключается в их «усилении». Каждая обнаружившая коллизию станция передает jam-сигнал. Этот сигнал позволяет другим станциям сразу «увидеть» коллизию и синхронизировать время начала отсчетов случайных задержек.

Вывод: CSMA/CD обеспечивает эффективное управление доступом к моноканалу, используя механизмы обнаружения и обработки коллизий, что делает его важным компонентом Ethernet.

36. Кадр Ethernet

Введение: Кадр Ethernet содержит ряд полей, определяющих структуру данных и обеспечивающих передачу информации по сети. Поля кадра важны для корректной передачи и проверки данных.

Основная часть: Поля Ethernet кадра:

1. Preamble – преамбула
2. SFD (Start Frame Delimiter) – разграничитель начала кадра
3. DA (Destination Address) – адрес назначения
4. SA (Source Address) – адрес источника

5. Length/Type – длина либо тип
6. Data – данные
7. Pad – наполнитель
8. FCS (Frame Check Sequence) – контрольная сумма
9. Extension – расширитель

Предусмотрены полудуплексный и полнодуплексный режимы, «поведение» в которых несколько различается. В качестве преамбулы выступают семь байтов со значением 10101010b, а в качестве SFD – байт со значением 10101011b. При сборке кадра учитываются ограничения на его длину. Ограничивается не только максимальная длина, а и минимальная. При недостаче в поле данных вслед за ним в кадр вставляются дополнительные октеты наполнители. Параметр MTU (Maximum Transmission Unit) определяет максимальный размер вкладываемых данных. Применительно к Ethernet, если значение поля Length/Type больше либо равно 1536 (600h), то указывает тип инкапсулируемых данных. При необходимости октеты расширители дополняют кадр до тайм-слота (только в полудуплексном режиме).

В качестве контрольного кода используется код CRC.

Вывод: Структура Ethernet кадра обеспечивает надежную передачу данных и их проверку, что является важным аспектом функционирования сетей Ethernet.

37. CSMA/CA (Wi-Fi)

Введение: CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance) – это алгоритм множественного доступа с прослушиванием несущей и избеганием коллизий, описанный в стандарте Wi-Fi (IEEE 802.11). Этот алгоритм является более сложным примером случайных методов доступа к моноканалу.

Основная часть: Случайная задержка измеряется в слот таймах, как и в Ethernet, но алгоритм другой. Количество слот таймов является случайным целым числом Random: 0 ≤\le Random ≤\le CW, где CW – так называемое окно состязаний (contention window), CWmin ≤\le CW ≤\le CWmax, и берётся из ряда 7, 15, 31 (2^n – 1). Типичные значения: CWmin =15, CWmax=1023.

Предусмотрены два счетчика попыток SRC (Short Retry Count) и LRC (Long Retry Count). Количество попыток ограничивается. Выбор значения зависит от физического уровня.

Для беспроводных каналов свойственны две проблемы:

1. Hidden node problem - проблема скрытой станции
2. Exposed node problem - проблема доступной станции

Все станции взаимодействуют в рамках одного канала. Проблема скрытой станции: станция C может ошибочно начать передачу станции B, так как не может «услышать», что станция A уже передает станции B (станция A «скрыта» от станции C). Проблема доступной станции:

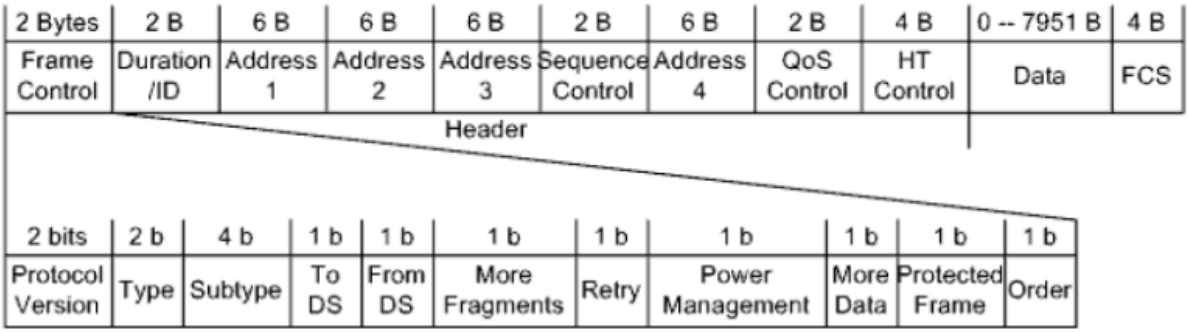
станция C, зная о взаимодействии станций A и B, не может передать станции D во время пассивности станции B, считая канал занятым ошибочно (станция C «доступна» для станции D).

Частично решить проблемы помогает опциональное расширение RTS/CTS.

Вывод: CSMA/CA обеспечивает эффективное управление доступом к моноканалу в беспроводных сетях, избегая коллизий и решая проблемы скрытых и доступных станций, что является важным аспектом функционирования Wi-Fi сетей.

38. Кадры Wi-Fi

Введение: Wi-Fi кадры содержат ряд полей, которые определяют структуру данных и обеспечивают правильную передачу информации по беспроводной сети. Эти поля важны для корректной работы сети и обеспечения качества обслуживания (QoS).



Основная часть: Поля Wi-Fi кадра включают:

1. Frame Control -- контроль кадра.
2. Duration/ID -- длительность-идентификатор (0 -- 32767 us при резервировании канала, трактовка зависит от наличия QoS).
3. Address 1 -- адрес 1.
4. Address 2 -- адрес 2.
5. Address 3 -- адрес 3.
6. Sequence Control -- контроль последовательности.
7. Address 4 -- адрес 4.
8. QoS Control -- контроль QoS.
9. HT Control (High Throughput) -- контроль интенсивной пересылки (при QoS).
10. Frame Body -- содержимое кадра (данные).
11. FCS (Frame Control Sequence) -- контрольная сумма.

Поля контроля кадра включают:

1. Protocol Version -- версия протокола (до сих пор равна нулю).

2. Type -- тип: 00b -- Management (управление), 01b -- Control (контроль), 10b -- Data (данные), 11b -- Reserved (зарезервировано).
3. Subtype -- подтип (в настоящее время определено около сорока подтипов).
4. To DS -- флаг направления в распределительную систему (проводную систему, связывающую беспроводные сегменты).
5. From DS -- флаг направления из распределительной системы.
6. More Fragments -- флаг наличия фрагментации.
7. Retry -- флаг повторной попытки передачи.
8. Power Management -- флаг режима энергосбережения.
9. More Data -- флаг наличия дополнительных данных (например, буферизированных данных для находящейся в режиме энергосбережения станции).
10. Protected Frame -- флаг защищенности кадра (шифрования).
11. Order -- флаг упорядоченности (при QoS).

Существуют три типа кадров: управление, контроль и данные. В зависимости от подтипа кадра в адресных полях могут комбинироваться до четырех из пяти возможных адресов:

1. BSSID (Basic Service Set Identifier) – идентификатор базовой зоны обслуживания (беспроводного сегмента).
2. SA (Source Address) – адрес источника.
3. DA (Destination Address) – адрес назначения.
4. TA (Transmitting station Address) – адрес станции передатчика (непосредственного).
5. RA (Receiving station Address) – адрес станции приемника (непосредственного).

Вывод: Поля Wi-Fi кадра обеспечивают структурированную и надежную передачу данных по беспроводной сети, а также поддержку QoS и других функций, необходимых для эффективной работы сети.

39. Особенности детерминированных методов доступа к моноканалу

Введение: Детерминированные методы доступа к моноканалу применяются при кольцевой топологии, где возможность возникновения коллизий менее выражена по сравнению с шинной топологией.

Основная часть: Концептуальная разница между случайными и детерминированными методами заключается в том, возникает ли случайность при «обращении» станции к моноканалу. Если станция имеет кадр для передачи и одновременно получает кадр из кольца, возникает вопрос о приоритете передачи.

Единственным способом преодоления логических коллизий является введение приоритетов. В то время как случайные методы основаны на генераторах случайных задержек, детерминированные методы основаны на системе приоритетов. Эта система может быть централизованной или распределенной.

Основные критерии классификации детерминированных методов:

1. Централизованное либо распределённое управление.
2. Алгоритм назначения приоритетов.
3. Топологические особенности.

На эффективность детерминированных методов влияют те же факторы, что и на случайные методы:

1. Количество взаимодействующих станций.
2. Частота синхронизации.
3. Длина кадра.

При сравнении детерминированных и случайных методов сложно сказать, какие из них лучше. Основные потери производительности при случайных методах возникают из-за задержек, а при детерминированных методах – из-за ретрансляции кадров. В среднем, детерминированные алгоритмы демонстрируют большую производительность, но оборудование для них более дорогостоящее.

Вывод: Детерминированные методы доступа к моноканалу, основанные на системе приоритетов, обеспечивают надежное управление передачей данных, особенно при кольцевой топологии. Их эффективность зависит от множества факторов, и они часто требуют более сложного и дорогостоящего оборудования.

40. Алгоритм Token Ring

Введение: Алгоритм Token Ring, описанный в стандарте IEEE 802.5, является наглядным примером детерминированных методов доступа к моноканалу. В Token Ring применяется централизованное управление, обеспечивающее надежную передачу данных в кольцевой топологии.

Основная часть: В Token Ring используется централизованное управление, что требует включения в кольцо по крайней мере одной управляющей станции (monitor station), наделенной особыми полномочиями и ответственной за инициализацию и контроль кольца. Станция монитор (monitor station) может быть основной (active monitor) или резервной (standby monitor).

Функции станции монитора включают:

1. Инициализацию подключившихся к кольцу станций.
2. Тактирование работы кольца на физическом уровне.
3. Контроль наличия и валидности маркера.
4. Предотвращение зацикливаний.

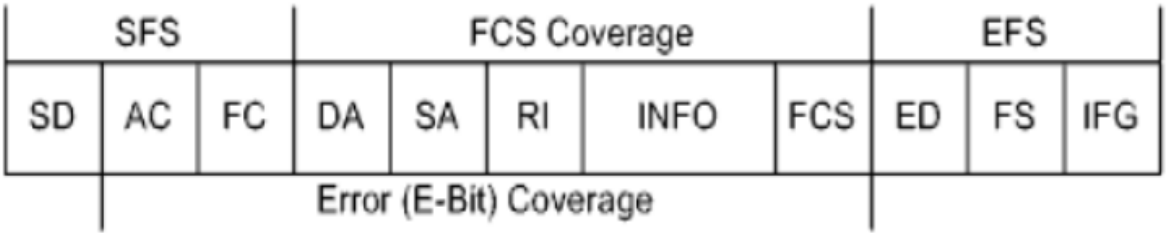
В Token Ring предусмотрены станции нескольких видов:

1. System managers - системные менеджеры.
2. Servers - различные серверы (configuration report servers, ring error monitors, ring parameter servers).
3. Data stations - информационные станции (обычные пользовательские станции).

В стандарте предусмотрены четыре вида передаваемых последовательностей:

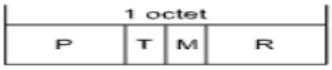
1. Token – маркер.
2. Frame – кадр.
3. Abort Sequence - прерывающая последовательность.
4. Fill - заполняющая последовательность.

Каждая станция должна распознавать маркеры, кадры и специальные последовательности. Формат кадров Token Ring включает основные поля:

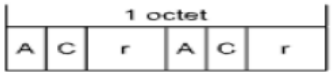


1. SD (Starting Delimiter) - начальный разделитель.
2. AC (Access Control) - контроль доступа.
3. FC (Frame Control) - контроль кадра.
4. DA (Destination Address) - адрес назначения.
5. SA (Source Address) - адрес источника.
6. RI (Routing Information) - информация о маршрутизации (может отсутствовать).
7. INFO (information) - данные (могут отсутствовать).
8. FCS (Frame Check Sequence) - контрольная сумма.
9. ED (Ending Delimiter) - конечный разделитель.
10. FS (Frame Status) - состояние кадра.
11. IFG (InterFrame Gap) - межкадровый интервал.

С точки зрения алгоритма контроля доступа наибольший интерес представляет одноименное поле, а также поле состояния кадра.



Где:
1) P (Priority bits) - текущий уровень приоритета
2) T (Token bit) - идентификатор маркера 0 маркер, 1 кадр
3) M (Monitor bit) - бит монитора
4) R (Reservation bits) - запрашиваемый уровень приоритета
Формат поля состояния кадра:



Где:
1) A (Address-recognized bit) - флаг распознания адреса (дублируется)
2) C (frame-Copied bit) - флаг копирования кадра (дублируется)
3) r (reserved) – зарезервировано

Механизм приоритетов Token Ring основан на связке двух полей P и R:

1. P (Priority bits) - текущий уровень приоритета.
2. R (Reservation bits) - запрашиваемый уровень приоритета.

Доступно восемь уровней приоритета. Можно выделить два режима взаимодействия:

1. Все станции имеют одинаковые приоритеты.
2. Станции могут иметь разные приоритеты.

Соблюдение правил гарантирует, что любая станция рано или поздно сможет передать кадр. Token Ring включает механизмы обеспечения надежности, такие как авто переконфигурирование и сигнализация об ошибках. Контрольный код – CRC. Скорость Token Ring – 4 или 16 Mbit/s (100 Mbit/s в поздних реализациях).

Вывод: Алгоритм Token Ring обеспечивает надежное управление доступом к моноканалу в кольцевой топологии, используя централизованное управление и механизм приоритетов. Он включает функции и механизмы для обеспечения надежности и корректной работы сети.

41. Реализации детерминированных методов доступа к моноканалу

Введение: Помимо Token Ring, существуют другие технологии, реализующие детерминированные методы доступа к моноканалу. Эти технологии обеспечивают различные способы организации доступа и передачи данных в сетях.

Основная часть:

1. Технология ARCNET (Attached Resource Computer NETwork):
    - Скорость: 2,5 Mbit/s
    - Логическая топология: однонаправленное кольцо
    - Физическая топология: шина или звезда
    - Первая широко используемая в ЛКС технология. В настоящее время устарела из-за распространения Ethernet.
2. Технология Token Bus (IEEE 802.4):
    - Скорость: 1, 5, 10, 20 Mbit/s
    - Логическая топология: однонаправленное кольцо
    - Физическая топология: шина
    - Алгоритм представляет собой адаптацию алгоритма Token Ring к шинной топологии. Почти не применялась и сильно устарела.
3. Технология FDDI (Fiber Distributed Data Interface), CDDI (Copper Distributed Data Interface):
    - Скорость: 100 Mbit/s, 200 Mbit/s
    - Логическая топология: однонаправленное кольцо с резервированием
    - Физическая топология: двойное кольцо с возможностью подключения деревьев через дополнительные сетевые устройства
    - Алгоритм представляет собой расширение алгоритма Token Bus. FDDI был вытеснен с рынка Fast Ethernet, но все еще ограниченно применяется.
4. Технология 100VG-AnyLAN:
    - Скорость: 100 Mbit/s
    - Логическая топология: дерево
    - Физическая топология: дерево с опциональным резервированием
    - Алгоритм представляет собой альтернативу Fast Ethernet (гибрид Ethernet и Token Ring). Технология не получила широкого распространения и исчезла с рынка.

Вывод: Реализации детерминированных методов доступа к моноканалу включают различные технологии, каждая из которых предлагает уникальные решения для передачи данных в сетях. Некоторые из них устарели и были вытеснены более современными технологиями, но они все же сыграли важную роль в истории сетевых технологий.

42. Адресация в компьютерных сетях и классификация адресов

Введение: Адресация в компьютерных сетях необходима для идентификации станций и обеспечения взаимодействия между ними. Адресация играет ключевую роль в пересылке пакетов между абонентами.

Основная часть: В форматах большинства пакетов присутствуют два адреса:

1. Адрес назначения (destination address)
2. Адрес источника (source address)

Адресация имеет ключевое значение в процессе пересылки пакетов между абонентами. Производительность СПД напрямую зависит от расположения адресов в пакете, поэтому

адреса располагают в самом начале пакета. Адрес назначения является более важным и анализируется системой передачи данных (СПД), поэтому он располагается раньше.

Многие топологии предполагают возможность приема пакета всеми станциями в пределах сегмента, вне зависимости от адреса назначения. Действия станций при этом включают «принятие», «анализ» и «обработку» пакета. Сравнение адреса назначения с собственным адресом позволяет станции распознать «свой» пакет. Адрес источника помогает определить абонента, создавшего пакет.

В каждом пакете должны присутствовать адреса канального уровня. В большинстве протоколов также предусмотрена адресация на сетевом и прикладном уровнях. Адреса канального уровня «зашиваются» в оборудование при производстве и считаются абсолютно уникальными. Такие адреса называют физическими. Адреса сетевого и прикладного уровней назначают пользователи и называют логическими.

Для взаимодействия сетевых процессов используются три уровня адресации:

1. Адрес подсети (subnet address) – для адресации подсети.
2. Адрес станции (node address) – для адресации станции в подсети.
3. Адрес программного порта (software port) – для адресации процесса в станции.

Диапазоны программных портов применительно к семейству TCP/IP

Port Number Range	Port Group
0 – 1023	Well Known
1024 – 49151	Registered
49152 – 65535	Private and Dynamic

Специально для компьютерных сетей разработаны четыре основных способа адресации:

1. Юникаст – пакет обрабатывается одной станцией.
2. Бродкаст (широковещательный) – пакет обрабатывается всеми станциями.
3. Мультикаст – пакет обрабатывается несколькими станциями.
4. Эникаст – пакет обрабатывается одной станцией из группы.

Мультикаст и эникаст адреса являются групповыми идентификаторами. Бродкаст, мультикаст и эникаст адреса не могут быть адресами источников, так как пакет может сгенерировать только одна станция. Эникаст адресация предполагает выбор станции на основе критерия, такого как время задержки.

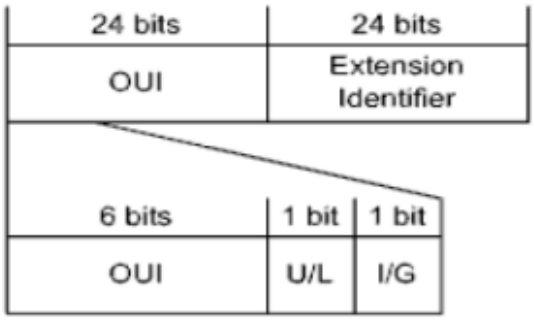
Вывод: Адресация в компьютерных сетях обеспечивает идентификацию станций и эффективное взаимодействие между ними. Существуют различные уровни и способы адресации, включая юникаст, бродкаст, мультикаст и эникаст, каждый из которых имеет свои особенности и применимость.

43. MAC-адреса

Введение: MAC-адреса (Media Access Control) являются уникальными идентификаторами сетевых устройств и контролируются IEEE Registration Authority (IEEE RA). Они используются для адресации на канальном уровне.

Основная часть: В стандартах IEEE определены три базовых формата MAC адресов: MAC-48, EUI-48 и EUI-64, где EUI (Extended Unique Identifier) означает расширенный уникальный идентификатор.

Формат EUI-48:



00-16-41-57-7D-48

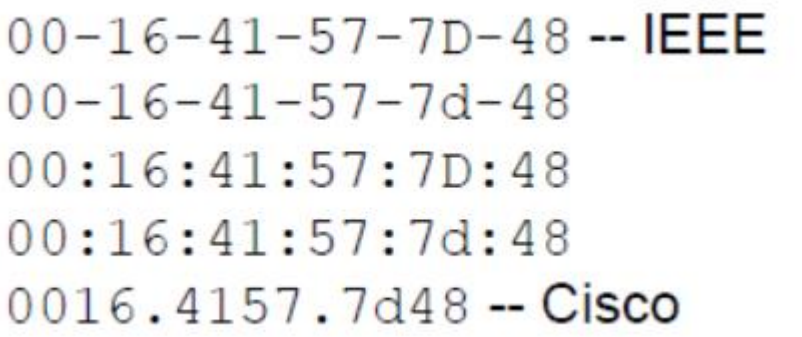
- Организационные уникальные идентификаторы (OUIs) выдаются централизовано, а уникальность оставшейся части адреса обеспечивают сами организации.
- Время валидности адресов – 100 лет. При администрировании может возникнуть необходимость подменить адрес, «зашитый» в оборудование, на другой. Этот новый адрес называют локальным административным адресом, признаком которого является единичное значение бита U/L.

Граница между OUI и Extension Identifier может проходить не только посередине адреса. Предусмотрены три варианта разрядности поля OUI:

1. MA-L (MAC Address - Large) – 24 бита (использовалась до 1 января 2014 г.)
2. MA-M (MAC Address Medium) – 28 битов (доступна после 1 января 2014 г.)
3. MA-S (MAC Address Small) – 36 битов (доступна после 1 января 2014 г.)

В каноническом представлении MAC-адрес сдвигается в канал начиная со старших разрядов.

По правилам IEEE MAC-адреса записываются в следующей нотации: XX-XX-XX-XX-XX-XX (где X – шестнадцатеричная цифра, верхний регистр), но часто используют альтернативные нотации.



Все юникаст-MAC-адреса имеют нулевое значение бита I/G. Групповые MAC-адреса формируются по особым правилам. В качестве бродкаст-MAC-адреса используется значение: FF-FF-FF-FF-FF-FF.

EUI-64 может использоваться не только для адресации, но и для идентификации устройств.

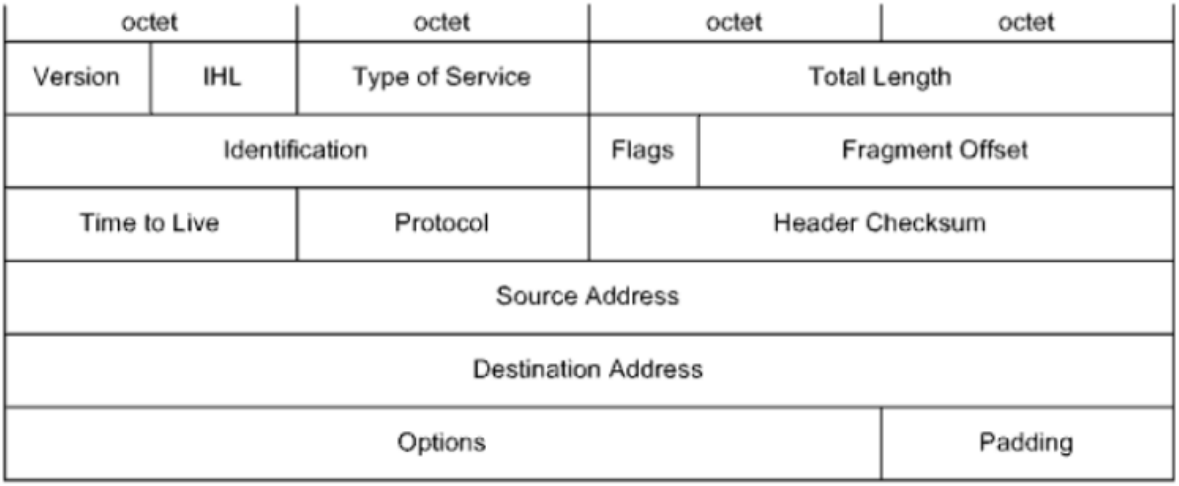
Примеры технологий с применением EUI-48: Ethernet, Wi-Fi, Token Ring. Примеры технологий с применением EUI-64: IPv6, FireWire.

Вывод: MAC-адреса являются уникальными идентификаторами сетевых устройств, обеспечивающими надежную адресацию на канальном уровне. Они используются в различных сетевых технологиях и имеют стандартизированные форматы и правила назначения.

44. Заголовок IPv4

Введение: В семействе TCP/IP за адресацию на сетевом уровне отвечает протокол IP. Заголовок протокола IPv4 (версии 4) имеет фиксированную структуру, обеспечивающую правильную передачу данных в сети.

Основная часть: Поля заголовка IPv4:



1. Version - версия (значение равно 4)
2. IHL (Internet Header Length) - длина заголовка (в 32-битных словах, минимальное значение равно 5)
3. Type of Service - тип сервиса (связано с QoS)
4. Total Length - общая длина данных (в байтах, не может превышать 65535 байтов)
5. Flags - флаги
6. Fragment Offset - смещение текущего фрагмента (в 64-битных словах, смещение первого фрагмента равно нулю)
7. Time to Live - «время жизни» (при каждой ретрансляции уменьшается, когда становится равным нулю, пакет уничтожается)
8. Protocol - протокол (инкапсулируемый в поле данных)
9. Header Checksum - контрольная сумма заголовка
10. Source Address - адрес источника
11. Destination Address - адрес назначения
12. Options - опции (связанные с безопасностью, размер вариативен)

Поле flags:

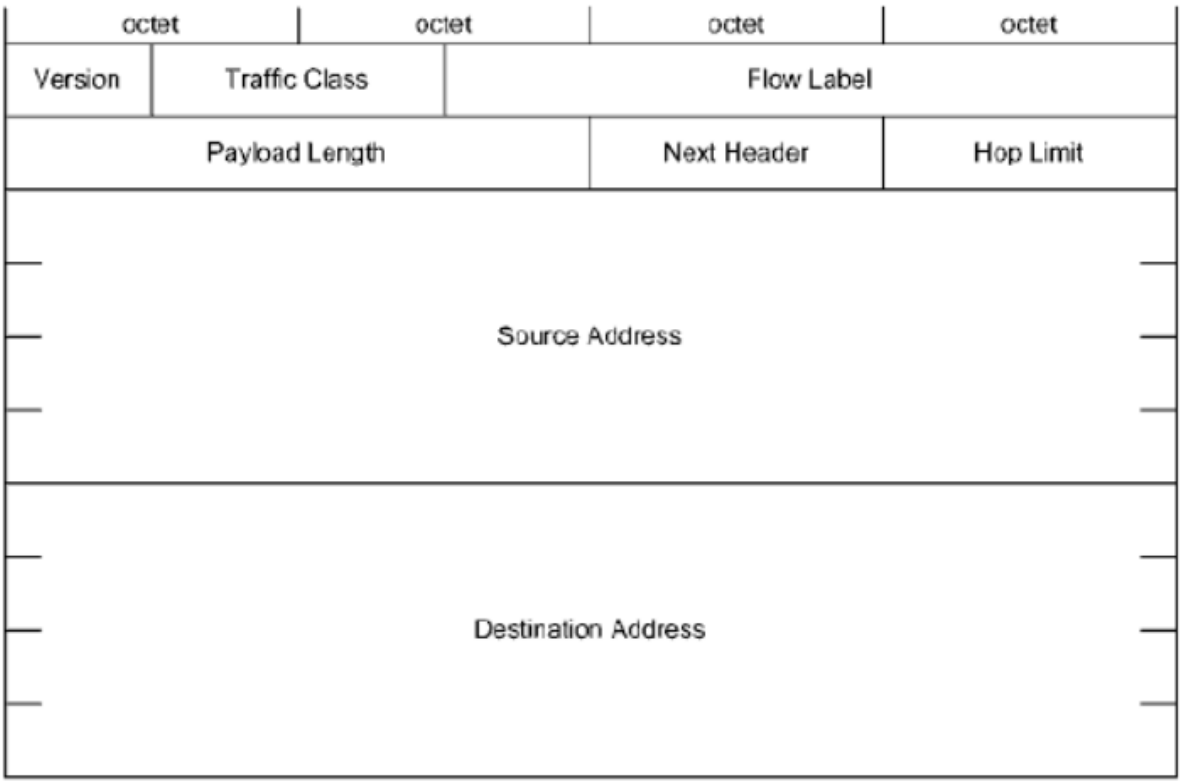
- DF (Don’t Fragment): 0 - пакет фрагментирован, 1 - пакет нефрагментирован
- MF (More Fragments): 0 - текущий фрагмент является последним, 1 - текущий фрагмент не является последним

Вывод: Фиксированная структура заголовка IPv4 обеспечивает надежную адресацию и передачу данных в сетях TCP/IP, а также включает механизмы фрагментации и контроля жизненного цикла пакетов.

45. Заголовок IPv6

Введение: Заголовок протокола IPv6 отличается гибкой структурой. Заголовки «каскадируются», что позволяет вставлять столько заголовков, сколько необходимо, обеспечивая гибкость и расширяемость.

Основная часть: Поля заголовка IPv6:



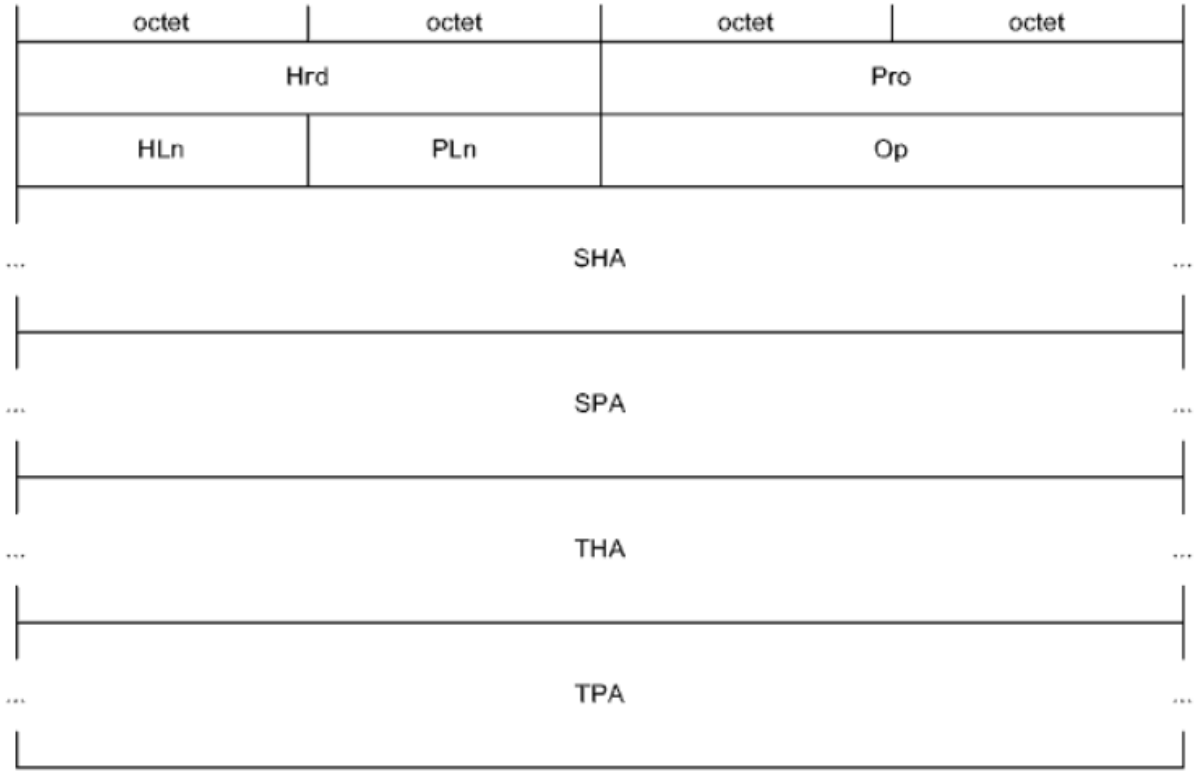
1. Version - версия (значение равно 6)
2. Traffic Class - класс трафика (связано с QoS)
3. Flow Label - метка потока (связано с QoS)
4. Payload Length - длина полезной нагрузки (в байтах, аналог поля Total Length)
5. Next Header - селектор следующего заголовка (аналог поля Protocol)
6. Hop Limit - ограничитель числа «прыжков» (аналог поля Time to Live)
7. Source Address - адрес источника
8. Destination Address - адрес назначения

Вывод: Гибкая структура заголовка IPv6 обеспечивает поддержку QoS и расширяемость, а также включает механизмы ограничения числа «прыжков» и инкапсуляции других заголовков, что делает IPv6 более адаптируемым и эффективным для современных сетевых приложений.

46. Протокол ARP

Введение: Группа протоколов под названием ARPs (Address Resolution Protocols) предназначена для восстановления соответствий между MAC-адресами и IP-адресами. Под прямым преобразованием, собственно ARP, понимают нахождение MAC-адреса по IP-адресу. Обратное преобразование выполняется по протоколу RARP (Reverse ARP).

Основная часть: Формат пакета ARP включает следующие поля:



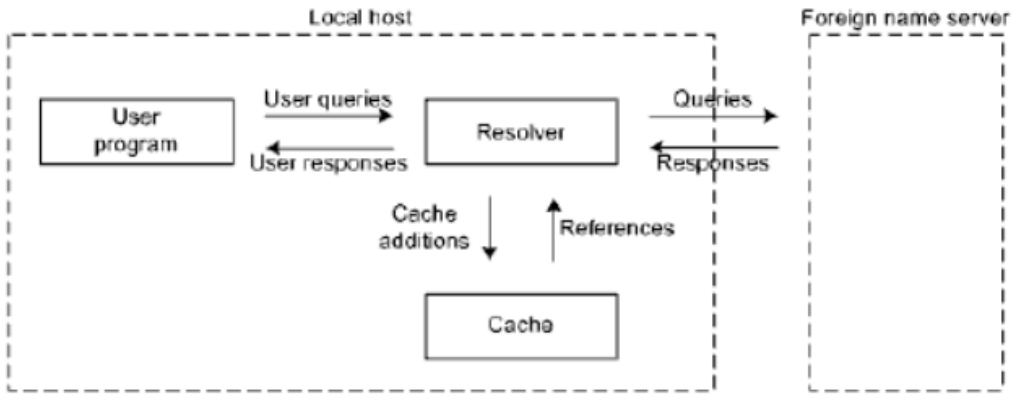
1. Hrd - тип оборудования (1 - Ethernet)
2. Pro - протокол (800h - IP)
3. HLn (Hardware address Length) - длина аппаратного (физического) адреса (в байтах, 6 - Ethernet)
4. PLn (Protocol address Length) - длина протокольного (логического) адреса (в байтах, 4 - IP)
5. Op (Opcode) - код операции: 1 – Request – запрос, 2 – Reply – ответ (и некоторые другие)
6. SHA (Sender Hardware Address) - аппаратный адрес запрашивающей станции
7. SPA (Sender Protocol Address) - протокольный адрес запрашивающей станции
8. THA (Target Hardware Address) - аппаратный адрес запрашиваемой станции
9. TPA (Target Protocol Address) - протокольный адрес запрашиваемой станции

Вывод: Протокол ARP обеспечивает прямое преобразование IP-адресов в MAC-адреса, что важно для правильного функционирования сетей. Обратное преобразование выполняется по протоколу RARP, обеспечивая всестороннюю адресацию в сетях.

47. Структура системы DNS

Введение: Протокол системы DNS (Domain Name System), описанный в RFCs 1034 и 1035, предназначен для восстановления соответствий между IP-адресами и адресами прикладного уровня. Под доменом в СПД понимают совокупность устройств, работающих в рамках единых правил.

Структура системы DNS:



Основная часть: Система DNS соответствует клиент-серверной модели и включает три основных компонента:

1. Адресное пространство доменных названий (domain name space) и записи о ресурсах (RRs - Resource Records).
2. Серверы названий (name servers).
3. Программы, отвечающие на запросы клиентов (resolvers).

Адресное пространство доменных названий имеет иерархическую древовидную структуру. Каждый узел дерева на некотором уровне иерархии обозначается DNS меткой (DNS label) длиной от 0 до 63 байтов, которая начинается с буквы и состоит из букв любого регистра, цифр и символа "-". Метка нулевой длины зарезервирована и является корнем дерева. При присоединении станции к домену ей присваивают метку. Доменное название строится из меток в соответствии с путем к корневой метке. Полная длина не может превышать 255 байтов. Доменное название может относиться как к отдельной станции, так и к ветви дерева (DNS домену). Доменное название может быть абсолютным или относительным. Внутреннее представление метки - один байт с указанием длины метки, за которым следуют байты метки. При интерпретации меток регистр букв не учитывается.

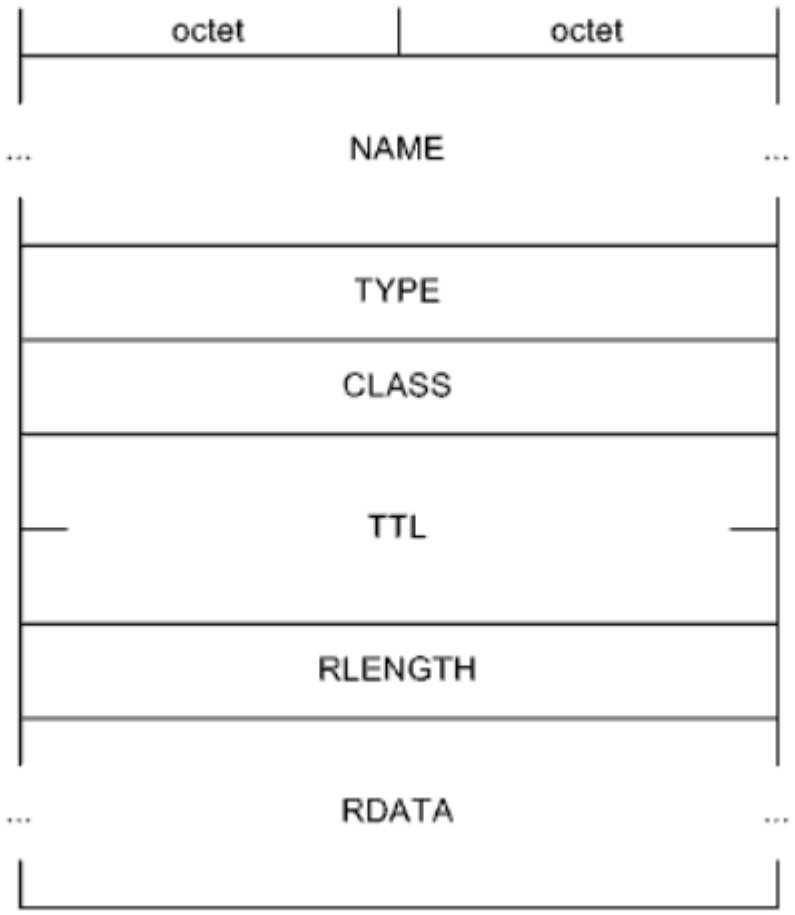
Записи доменных названий разделяются точками, и корневая метка находится крайней справа.

Вывод: Структура системы DNS обеспечивает иерархическую и логически организованную адресацию, что позволяет эффективно восстанавливать соответствия между IP-адресами и адресами прикладного уровня.

48. Сообщения DNS

Введение: Каждой станции или домену в системе DNS соответствует определенное количество Resource Records (RRs). Эти записи играют ключевую роль в процессах восстановления соответствий и передачи данных в DNS.

Основная часть: Формат DNS RR включает следующие поля:



1. NAME - доменное название, к которому относится RR.
2. TYPE - тип.
3. CLASS - класс (семейство протоколов).
4. TTL (Time To Live) - время жизни (валидности RR, в секундах).
5. RLENGTH (Resource LENGTH) - длина данных ресурса.

6. RDATA (Resource DATA) - данные ресурса (зависят от типа и класса).

Основные типы RRs:

1. A (A host address) - IP-адрес хоста.
2. NS (Name Server) - авторитетный сервер названий домена.
3. CNAME (Canonical NAME) - каноническое доменное название станции или домена.
4. SOA (Start of a zone of Authority) - оригинальные параметры зоны.
5. NULL - нулевая запись (произвольная информация).
6. PTR - указатель на доменное название станции (при обратных преобразованиях).
7. HINFO (Host INFO) - информация о станции (процессор и ОС).
8. MX (Mail eXchange) - доменное название почтового сервера в домене.
9. TXT (TeXT strings) - текстовые строки.
10. AAAA - IPv6-адрес хоста.
11. SRV (SeRVer selection) - описание сервиса.

Классы RRs:

1. IN - Internet.
2. CS - CSNET (устарел и аннулирован).
3. CH - Chaosnet (устарел).
4. HS - Hesiod (для БД, редкий).

Остальные значения классов зарезервированы

Примеры значений RRs класса IN:

A: `192.168.11.1.`

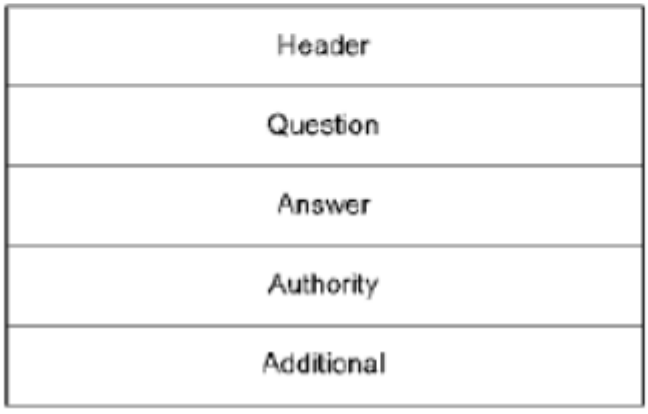
CNAME: `5-508-fileserv.bsuir.by.`

MX: `10 mail.bsuir.by.`

NS: `proxy1.bsuir.by.`

PTR: `5-508-fileserv.bsuir.by.`

Формат сообщения DNS:



Формат сообщения DNS включает следующие поля:

1. Header - заголовок.
2. Question - вопрос.
3. Answer - ответ.
4. Authority - авторитетный ответ.
5. Additional - дополнение.

Заголовок присутствует всегда, остальные поля вариативны.

Вывод: Сообщения DNS и Resource Records обеспечивают структурированное хранение и передачу данных, что является основой для функционирования системы DNS и восстановления соответствий между различными типами адресов.

49. Виртуальные соединения в сети передачи данных

Введение: Термин "соединение" является ключевым на транспортном уровне. Соединение подразумевает готовность абонентов передавать или принимать данные. Виртуальные соединения отличаются от физических соединений и используются для абстрагирования взаимодействий.

Основная часть: Виртуальные соединения (virtual connections) относятся к абонентам программ, которые физически соединены быть не могут. Соединения являются сугубо виртуальными. Нормальная готовность может рассматриваться в двух ракурсах:

1. Организация взаимодействия абонентов программ.
2. Настройка задействованного промежуточного оборудования.

В первом случае речь идет о виртуальных соединениях транспортного уровня, во втором – о виртуальных цепях (virtual circuits) сетевого или канального уровней. Виртуальные цепи бывают:

1. PVCs (Permanent Virtual Circuits) - выделенные виртуальные цепи.
2. SVCs (Switched Virtual Circuits) - коммутируемые виртуальные цепи.

Термин "виртуальный канал" может подходить как к виртуальным соединениям, так и к виртуальным цепям.

Вывод: Виртуальные соединения и цепи обеспечивают абстрагированное и гибкое взаимодействие между абонентами и настройку оборудования, что является важным аспектом эффективной работы сетей передачи данных.

50. Классификация оконных механизмов, используемых в сети передачи данных

Введение: Контроль доставки информационных пакетов может быть обеспечен различными методами, одним из которых является метод запросов подтверждений (requests/acknowledges). Для оптимизации обмена данными используется оконный метод, позволяющий передавать несколько пакетов до ожидания квитанций.

Основная часть: Выделяют два основных критерия классификации оконных методов. Исходя из количества пакетов, передаваемых в окне, оно может быть:

1. Статическим - неизменяемый размер окна заложен в протокол или устанавливается на весь сеанс обмена.
2. Динамическим - размер окна может изменяться (увеличиваться или уменьшаться) в процессе передачи сообщения.

Исходя из способа обработки очереди пакетов, окно может быть:

1. Фиксированным - перед формированием следующего окна текущее должно быть полностью «закрыто», то есть должны быть приняты все необходимые квитанции.
2. Скользящим - существует возможность сдвигать окно относительно последовательности пакетов.

При реализации оконного метода следует учитывать следующие дополнительные обстоятельства:

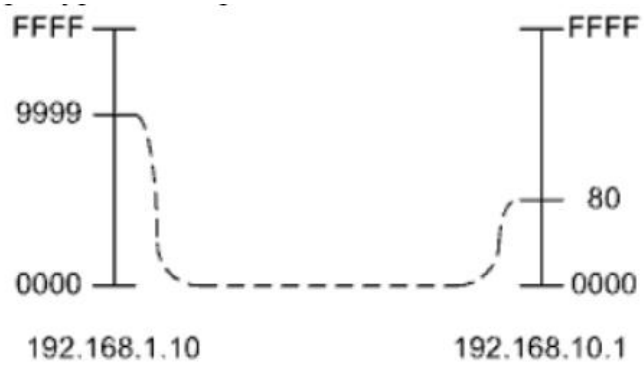
- Нужна нумерация пакетов в том или ином виде.
- Подтверждаться может как все окно, так и каждый из пакетов.
- Размером окна может управлять как передатчик, так и приемник.
- Размером окна можно управлять посредством служебных полей, в том числе и в информационных пакетах.
- Окно, с которым работает передатчик, может отличаться от окна, с которым работает приемник.
- Иногда важен порядок доставки пакетов.

Наиболее простым является статическое окно фиксированного размера. Основной его недостаток состоит в отсутствии возможности адаптации к изменениям в СПД. Динамическое окно позволяет успешно адаптироваться к изменениям в СПД: при увеличении загруженности окно целесообразно сужать, а при снижении – расширять. Скользящее окно, особенно в сочетании с динамическим, позволяет ускорить адаптацию к топологическим и другим изменениям в СПД.

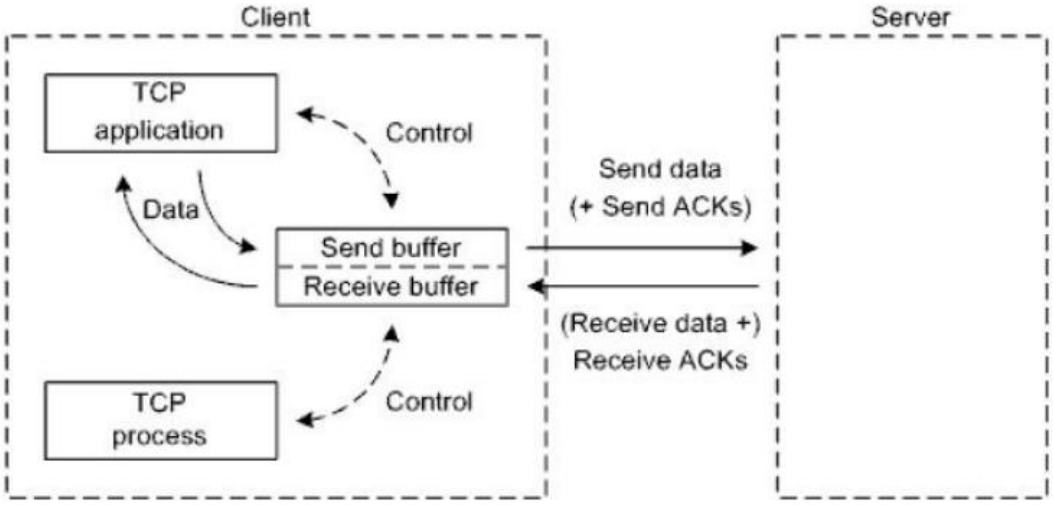
Вывод: Оконные методы обеспечивают эффективную передачу данных, улучшая контроль доставки и адаптацию к изменениям в сети. В зависимости от параметров и задач выбираются подходящие механизмы окон.

51. Структура системы TCP

Введение: TCP соответствует клиент-серверной модели. Сокет - это привязка к виртуальному каналу, соединяющему два взаимодействующих сетевых процесса, с учетом всех уровней адресации.



Структура соединения TCP:



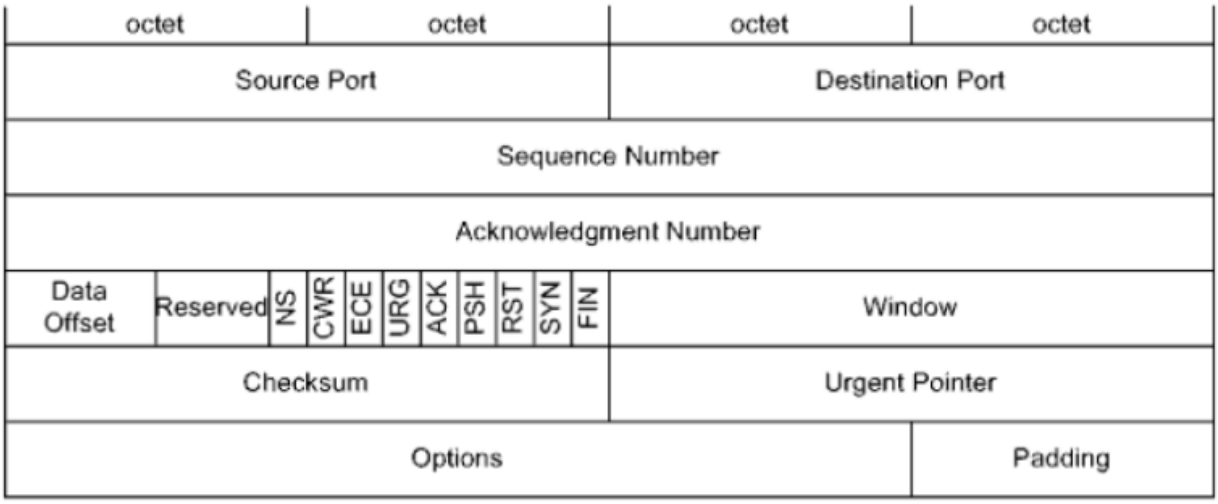
Основная часть: Применительно к каждому TCP соединению необходимо выделить приложение, производящее или потребляющее сетевые данные, и TCP процесс, предоставляющий коммуникационные услуги (например, драйвер ОС). Синхронизацию работы приложения и TCP процесса обеспечивает буферизация. TCP интерфейс состоит из примитивов для работы с буфером, позволяющих контролируемо записывать или считывать данные. Доступ к буферу имеет TCP процесс, который отслеживает наполнение буфера и организует прием или передачу данных, используя ресурсы нижних уровней.

Передаваемое сообщение разбивается на сегменты. Минимальной единицей данных в окне является октет (байт). Все байты сообщения нумеруются последовательными номерами (Sequence Numbers, SNs). Нумерация начинается с начального последовательного номера (Initial Sequence Number, ISN), который генерируется реализациями для лучшего управления соединениями. Сам ISN не включается в нумерацию байтов, то есть номер первого байта сообщения больше ISN на единицу. Номер сегмента соответствует SN первого байта данных в нем. Длина сегмента может варьироваться, но имеет ограничение. Важным параметром является MSS (Maximum Segment Size) – максимальная длина сегмента (по умолчанию 536 байтов).

Вывод: Структура системы TCP обеспечивает эффективное управление передачей данных, используя буферизацию и нумерацию байтов. Это позволяет организовать надежное и последовательное взаимодействие между приложениями и сетевыми процессами.

52. Заголовок TCP

Введение: Заголовок TCP (Transmission Control Protocol) содержит важные поля, необходимые для организации передачи данных и управления соединением в сетях. Поля заголовка TCP обеспечивают установление, поддержание и завершение соединения, а также контроль передачи данных.



Основная часть: Поля заголовка TCP включают:

1. Source Port - программный порт источника
2. Destination Port - программный порт назначения
3. Sequence Number (SN) - последовательный номер (сегмента)
4. Acknowledgment Number (AN) - подтверждающий номер
5. Data Offset - смещение данных (в 32-битных словах)
6. Reserved - зарезервировано (должно равняться нулю)
7. NS (Nonce Sum) – флаг - контрольная сумма для проверки правильности кодов явных уведомлений о заторах (связан с QoS, связан с IP заголовком)
8. CWR (Congestion Window Reduced) - флаг уменьшения окна затора при явном уведомлении о заторе
9. ECE (Explicit Congestion Notification Echo) - флаг подтверждения явного уведомления о заторе
10. URG (URGent Pointer field significant) - флаг значимости указателя на экстренные данные
11. ACK (ACKnowledgment field significant) - флаг значимости подтверждающего номера
12. PSH (PuSH Function) - флаг принудительной доставки данных (без буферизации)

13. RST (ReSeT the connection) - флаг разрыва соединения (из-за сбоя на одной из взаимодействующих сторон)
14. SYN (SYNchronize sequence numbers) - флаг синхронизации последовательных номеров
15. FIN (No more data from sender) - флаг последних данных
16. Window (W) - предлагаемое окно
17. Checksum - контрольная сумма
18. Urgent Pointer - указатель на экстренные данные
19. Options - опции (например, MSS)
20. Padding – наполнитель

Вывод: Заголовок TCP обеспечивает структуру и контроль передачи данных в сетях, позволяя устанавливать и поддерживать надежные соединения. Поля заголовка играют ключевую роль в управлении и организации сетевых взаимодействий.

53. Протокол TCP

Введение: Протокол TCP (Transmission Control Protocol) является основным протоколом транспортного уровня, обеспечивающим надежную доставку данных в сети. TCP использует оконные механизмы и флаги для управления соединениями и передачей данных.

Основная часть: Функционирование оконного механизма TCP базируется на использовании трех полей в заголовке сегмента SN, AN, W и трех флагов (из шести стандартизованных изначально) SYN, ACK, FIN. Установление TCP соединения, известное как «тройное рукопожатие» (three-way handshake), основывается на использовании флагов SYN и ACK. Несмотря на несимметричность процесса установления соединения, в дальнейшем оно используется в полнодуплексном режиме.

Полнодуплексность самого соединения достигается за счет того, что передаваемый в определенном направлении сегмент служит одновременно для транспортировки данных и связанных с ними служебных полей от передающей составляющей TCP процесса, а также подтверждений и связанных с ними других служебных полей от принимающей составляющей TCP процесса.

По правилу протокола, поле SN пересылаемого сегмента отражает собственный SN этого сегмента. В поле AN указывается SN ожидаемого сегмента, коим является следующий по порядку сегмент. При установлении соединения данные не пересылаются, поэтому в качестве SNs используют невключенные в нумерацию байтов сообщения ISNs, а в качестве ANs просто инкрементированные SNs.

Данные могут пересылаться только в одном направлении, то есть в симплексном режиме. В этом случае в направлении, попутном направлению пересылки данных, в качестве AN используется SN следующего по порядку несуществующего сегмента. ANs дублируются столько раз, сколько нужно. Аналогичные дублирования возникают при приостановке пересылки данных в определенном направлении.

Соединение всегда открывается в двух направлениях и должно быть закрыто в обоих направлениях. Для закрытия соединения сторона устанавливает флаг FIN в соответствующем сегменте. Размер предлагаемого окна в поле W может изменяться каждый раз для коррекции текущего окна передачи.

Проблема возможной потери сегментов решается с помощью тайм-аутов. Передающий TCP-процесс определяет потерю сегмента по отсутствию подтверждения в течение установленного интервала времени и передает сегмент повторно.

Вывод: Протокол TCP обеспечивает надежную передачу данных с использованием оконных механизмов, управления флагами и тайм-аутами. Установление и завершение соединения происходит по правилам «тройного рукопожатия», что гарантирует корректность и надежность сетевых взаимодействий.

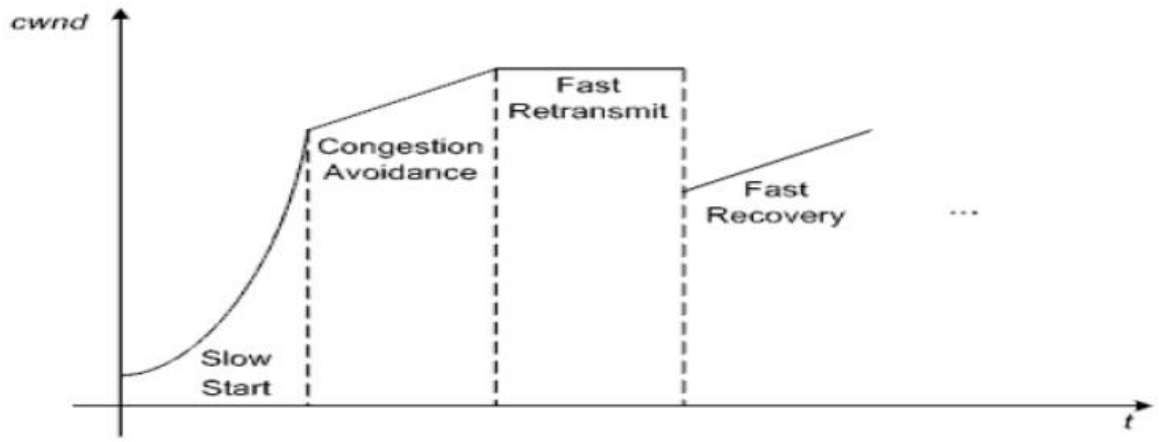
54. Усовершенствования протокола TCP

Введение: Для повышения эффективности и надежности TCP были предложены различные усовершенствования, направленные на решение известных проблем и улучшение производительности сети.

Основная часть: «Синдром глупого окна» («silly window syndrome») - проблема, заключающаяся в несоответствии текущего окна передачи состоянию приемника. Решение Нэгла позволяет бороться с этим синдромом, когда требуется часто отправлять небольшие сегменты с данными. Решение Кларка помогает, когда принимающей стороной часто анонсируется небольшое предлагаемое окно.

Стандартизированы четыре дополнения Ван Якобсона для борьбы с перегрузками:

1. Медленный старт (slow start): размер текущего окна передачи увеличивается плавно, пропорционально скорости получения подтверждений.
2. Избегание затора (congestion avoidance): сдерживание экспоненциального роста размера текущего окна передачи после преодоления порога.
3. Быстрая повторная передача (fast retransmit): при получении разупорядоченного сегмента с данными происходит повтор подтверждения с AN недостающего сегмента, а при получении трех одинаковых подтверждений - незамедлительный повтор сегмента.
4. Быстрое восстановление (fast recovery): после обнаружения затора переход сразу к избеганию коллизий, минуя стадию медленного старта.



Вывод: Усовершенствования протокола TCP, такие как решения Нэгла и Кларка, а также дополнения Ван Якобсона, направлены на улучшение производительности и надежности сети. Они решают проблемы, связанные с перегрузками и эффективностью передачи данных.

55. Протокол UDP и заголовок UDP

Введение: Протокол транспортного уровня UDP (User Datagram Protocol) реализует способ пересылки данных без гарантии доставки. Этот метод передачи данных часто называют дейтаграммным.

Основная часть: Поля заголовка UDP включают:

1. Source Port - программный порт источника
2. Destination Port - программный порт назначения
3. Length - длина дейтаграммы, включая заголовок (в байтах)
4. Checksum - контрольная сумма (подсчет включает заголовок и данные)

При вкладывании UDP дейтаграммы в IP пакет (IPv4 или IPv6) между заголовком UDP и IP вставляется дополнительный UDP псевдозаголовок, в котором дублируются некоторые значения из основного IP заголовка.

Вывод: Протокол UDP обеспечивает простой и быстрый способ передачи данных без гарантии доставки. Поля заголовка UDP позволяют идентифицировать источник и назначение данных, а также контролировать целостность передаваемой информации.

56. Классификация и характеристики сред передачи данных

Введение: Средства передачи данных (СрПД) играют важную роль в организации компьютерных сетей, обеспечивая различные способы передачи информации. Они классифицируются по типу и характеристикам, что помогает выбрать оптимальное решение для различных сетевых задач и условий.

Основная часть: Все исконно используемые в компьютерных сетях средства передачи данных можно разделить на пять типов:

1. Коаксиальные кабели (coaxials) с различным волновым сопротивлением.
2. Экранированные и неэкранированные кабели на основе витых пар (twisted pairs) различных категорий.
3. Одно- и многорежимные (одно- и многомодовые) оптоволоконные кабели (fiber равно fibre).
4. Эфир (ether).
5. Телефонные пары (phone pairs).

Где:

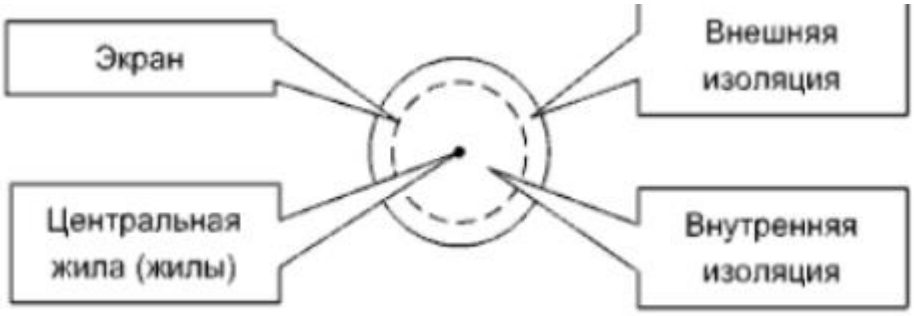
- 1, 2, 5 - «медь» (copper);
- 3 - «оптика» (optics);
- 1, 2, 3, 5 - проводные (wired) СрПД;
- 4 - беспроводные (wireless) СрПД.

Вывод: Классификация сред передачи данных помогает определить их характеристики и области применения, обеспечивая эффективную работу компьютерных сетей.

57. Среды передачи данных на основе коаксиальных кабелей

Введение: Коаксиальные кабели широко используются в различных областях, в том числе в телевидении, благодаря своим уникальным характеристикам.

Основная часть: Коаксиальные кабели имеют важное достоинство – возможность передавать множество сигналов одновременно. Внутри они выглядят следующим образом:



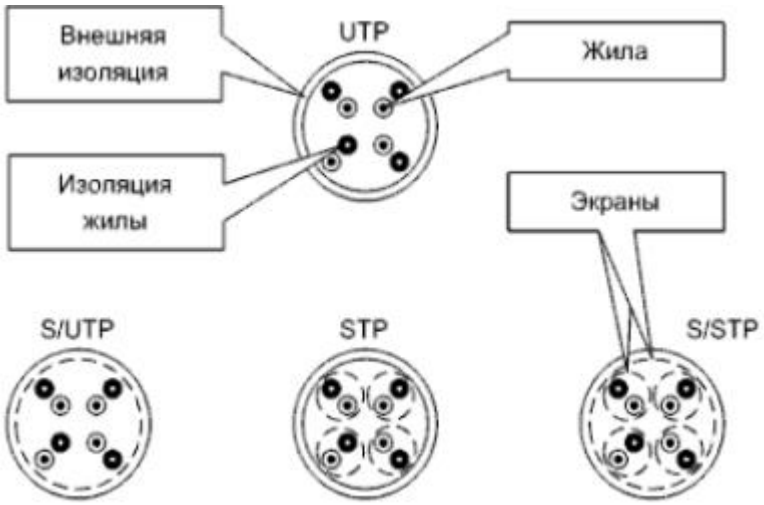
центральная жила, изоляция, оплетка и внешняя оболочка. Для формирования системы на таком кабеле нужны как минимум BNC (bayonet-neill-concelman) коннекторы, Т-соединители и пара терминаторов, один из которых заземляют. Коаксиальный кабель, в отличие от витой пары, устойчив к электромагнитным помехам и способен передавать сигналы на большие расстояния. Производители обычно выпускают коаксиальные кабели черного, реже серого цвета.

Вывод: Коаксиальные кабели обладают уникальными характеристиками, которые делают их идеальными для передачи множества сигналов одновременно и на большие расстояния, что делает их незаменимыми в телевидении и других областях.

58. Среды передачи данных на основе витых пар

Введение: Витые пары широко используются в сегментах компьютерных сетей благодаря своей универсальности и эффективности.

Основная часть: В сегментах КС широко используются четыре вида витых пар:



- TP – twisted pair
- S – shielded
- U – unshielded

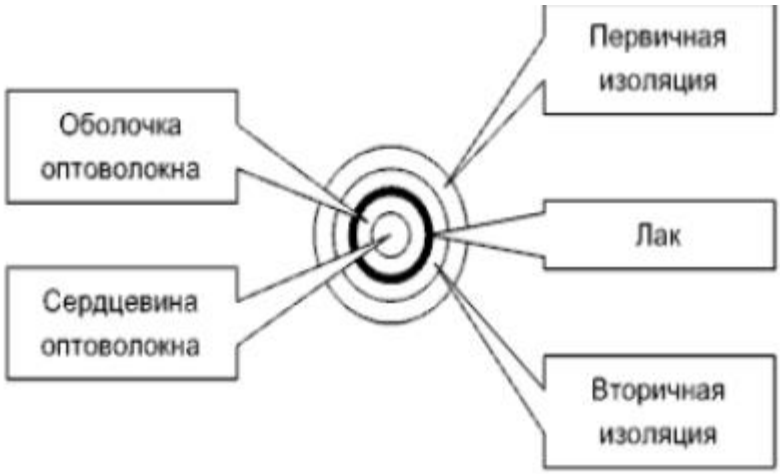
Витая пара состоит из 8 кабелей (бело-оранжевый, оранжевый, бело-зелёный, синий, бело-синий, зелёный, бело-коричневый, коричневый), которые разводятся по стандарту 568-B под RJ-45. Обычно на витой паре доступны по два асинхронных канала передачи и приёма данных. В типовых случаях витой парой соединяют разноранговое сетевое оборудование. Цвета самих кабелей в витой паре не оговорены, обычно они привязаны к палитре RAL и имеют серый цвет. Другие цвета говорят о более высоком качестве.

Вывод: Витые пары являются важной средой передачи данных в компьютерных сетях, обеспечивая надежное и эффективное соединение для различных видов сетевого оборудования.

59. Среды передачи данных на основе оптоволоконных кабелей

Введение: Оптоволоконные кабели играют важную роль в передаче данных на больших расстояниях и с высокой скоростью благодаря уникальным свойствам световодов.

Основная часть: Рабочими компонентами оптоволоконных кабелей являются световоды, изготовленные из оптоволокна, т.е. особого кварцевого стекла. Световод – это оптический волновод, состоящий из сердцевины и оболочки.



Большое количество изоляции обусловлено хрупкостью кабеля. В стандартах предусмотрены 8 видов световодов: OM1, OM2, OM3, OM4, OM5 – многорежимные, OS1, OS2, OS1a – однорежимные.

Также существует множество видов оптоволоконных кабелей. Оптоволоконные соединения делятся на несъемные (сплавные, механические) и съемные (контактные и линзовые).

Вывод: Оптоволоконные кабели обеспечивают высокоскоростную передачу данных на большие расстояния, что делает их важным компонентом современных сетевых систем

60. Физический уровень Ethernet

Введение: Физический уровень Ethernet определяет электрические или оптические свойства соединений между устройствами в сети, обеспечивая основу для передачи данных.

Основная часть: Физический уровень Ethernet включает:

1. Несколько интерфейсов физических сред.
2. Несколько порядков величины.
3. Скорости от 1 Мбит/с до 400 Гбит/с.

Ключевые стандарты Ethernet:

- 10BASE5 (1983) – «толстый» коаксиальный кабель 50 Ω (до 500 m).
- 10BASE2 (802.3a, 1985) – «тонкий» коаксиальный кабель 50 Ω (до 185 m).
- 10BASE-T (802.3i, 1990) – две телефонные витые пары (до 100 m).
- 10BASE-FL (802.3j, 1993) – два многорежимных световода (до 500 m).
- 100BASE-TX (802.3u, 1995) – две неэкранированные или экранированные витые пары категории 5 (до 100 m).
- 100BASE-FX (802.3u, 1995) – два многорежимных световода (до 2 km).

- 1000BASE-SX (802.3z, 1998) – два многорежимных световода (до 275 m – 62,5 um, до 550 m – 50 um).
- 1000BASE-LX (802.3z, 1998) – два однорежимных (до 5 km) или многорежимных световода (до 550 m).
- 1000BASE-T (802.3ab, 1999) – четыре неэкранированные или экранированные витые пары категории 5 (до 100 m).
- 2.5GBASE-T (802.3bz, 2016) – четыре неэкранированные или экранированные витые пары категории 5e (до 100 m).
- 5GBASE-T (802.3bz, 2016) – четыре неэкранированные или экранированные витые пары категории 5e (до 100 m).
- 10GBASE-SR (802.3ae, 2002) – два многорежимных световода (до 33 m – 62,5 um, до 400 m – 50 um).
- 10GBASE-LR (802.3ae, 2002) – два однорежимных световода (до 10 km).
- 10GBASE-ER (802.3ae, 2002) – два однорежимных световода (до 30 km).
- 10GBASE-T (802.3an, 2006) – четыре неэкранированные (до 55 m) или экранированные (до 100 m) витые пары категории 6, либо четыре витые пары категории 6A (до 100 m).

Вывод: Физический уровень Ethernet обеспечивает основу для передачи данных между устройствами, поддерживая различные скорости и интерфейсы для удовлетворения потребностей сетевых систем.

61. Структурированные кабельные системы и их модели

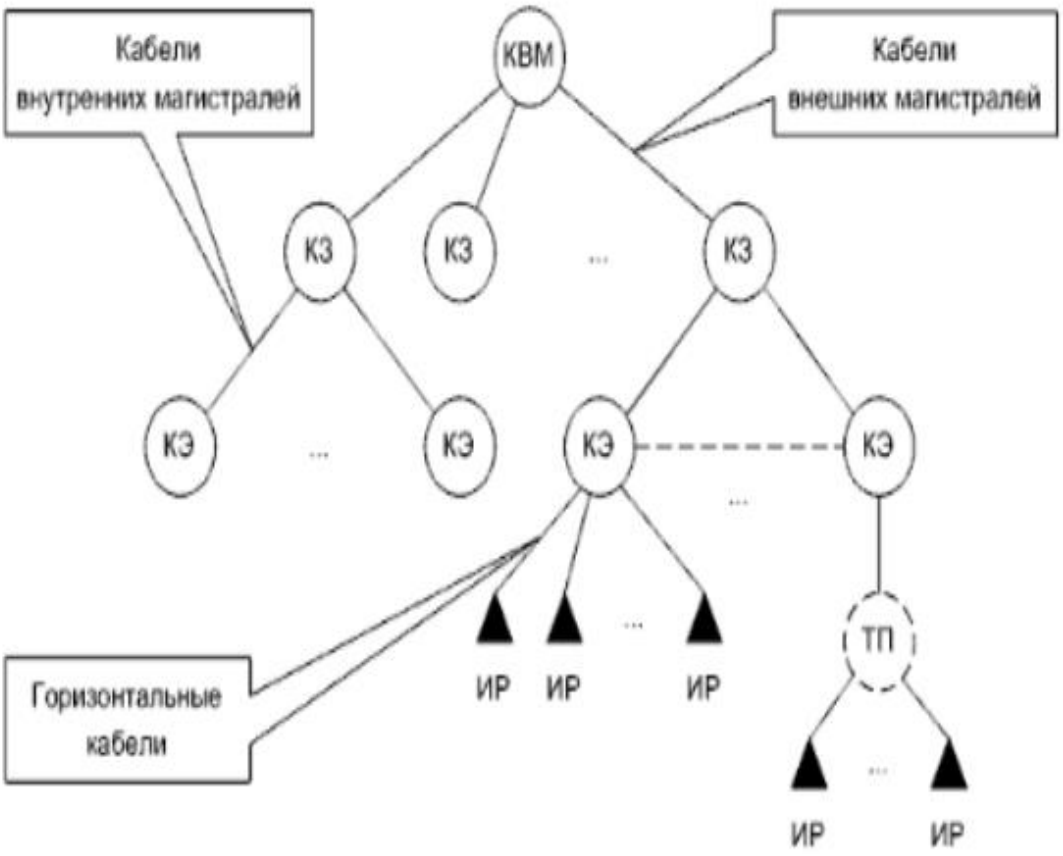
Введение: Структурированная кабельная система (СКС) – это упорядоченная совокупность телекоммуникационных и силовых кабелей, различного оборудования, а также специализированных помещений.

Основная часть: Основой для построения СКС служит древовидная топология, узлами которой является сетевое оборудование определённого типа. Помещения в СКС бывают:

1. Кроссовые (вспомогательное, активное и пассивное сетевое оборудование).
2. Аппаратные (кроме кроссового, может быть расположено серверное оборудование).

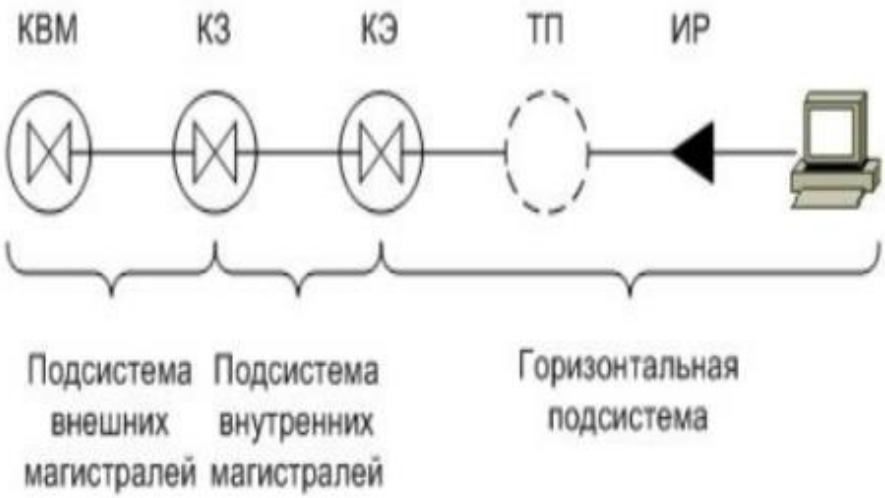
СКС включает три подсистемы:

1. Подсистема внешних магистралей (main, campus) – основа связи между компактно расположенными зданиями.
2. Подсистема внутренних магистралей (building) – связывает этажи одного здания.
3. Горизонтальная подсистема (horizontal) – связывает оборудование в пределах одного этажа.

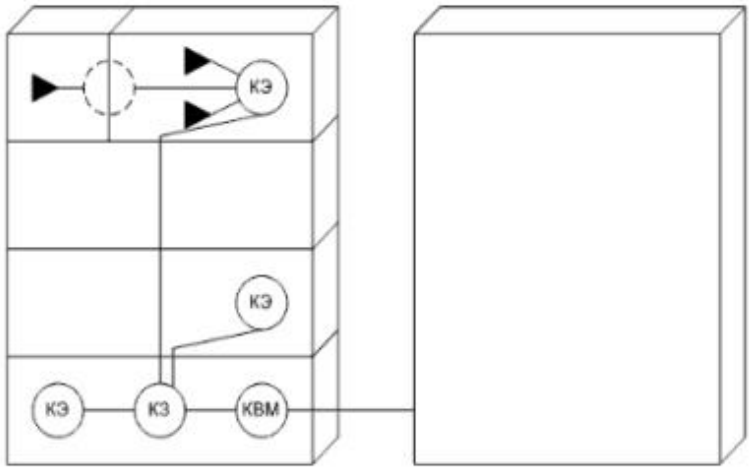


Основная модель СКС:

- КВМ – кроссовая внешних магистралей.
- КЗ – кроссовая здания.
- КЭ – кроссовая этажа.
- ИР – информационная розетка (для рабочего места).
- ТП (пунктирной линией) – точка перехода.



Горизонтальная модель СКС



Функциональная модель СКС здания

Горизонтальная и функциональная модели СКС здания также включают подобные компоненты.

Вывод: Структурированные кабельные системы обеспечивают упорядоченную и эффективную организацию сетевой инфраструктуры, используя древовидную топологию и различные подсистемы для связи между различными уровнями и сегментами сети.

62. Питание и заземление в структурированных кабельных системах

Введение: В структурированных кабельных системах (СКС) необходимо уделить внимание заземлению и питанию по нескольким причинам, связанным с безопасностью и надежностью работы сетевого оборудования.

Основная часть: Основные причины заземления и питания в СКС:

1. Предотвращение поражения людей электрическим током.
2. Защита кабельных трактов и сетевого оборудования от выхода из строя/помех.
3. Обеспечение возможности прохождения сигналов для некоторых видов сетевого оборудования.

Согласно стандарту TIA-607, в дополнение к основному контуру заземления здания или сооружения создают дополнительный, телекоммуникационный контур заземления (контур рабочего заземления).

Модель заземления включает:

- ГРЩ – главный распределительный щит здания.
- ШТЗ – шина телекоммуникационного заземления.
- ОШТЗ – основная ШТЗ.
- ЩС – щит силовой.
- РП – рабочее место.
- ТО – телекоммуникационное оборудование.

Для защиты от электрических зарядов в атмосфере применяют специальные устройства – газоразрядники.

Вывод: Заземление и питание в СКС обеспечивают безопасность и надежность работы сетевого оборудования, предотвращают поражение электрическим током и защищают оборудование от повреждений.

63. Пожарная безопасность структурированных кабельных систем

Введение: Структурированные кабельные системы (СКС) охватывают здание полностью, поэтому важно уделять особое внимание их пожарной безопасности.

Основная часть: Согласно американским стандартам NEC, предусмотрены 4 уровня пожарной безопасности (от высших к низшим):

1. Plenum – кабели, которые можно располагать как угодно (в plenum-области).
2. Riser – кабели, которые можно прокладывать в кабельных шахтах.
3. General purpose – кабели, которые можно прокладывать везде, кроме plenum-областей.
4. Residential – кабели, на прокладку которых нанесены определённые ограничения (например, только для жилых помещений).

В состав маркировки кабелей обычно вводят дополнительные обозначения материала оболочек:

- PVC – Поливинилхлорид (ПВХ).
- PE (PolyEthylene) – полиэтилен.
- FR (Flame retardant) – огнестойкий.
- CST – бронирован гофрированной стальной лентой и др.

Вывод: Пожарная безопасность в СКС обеспечивается соблюдением стандартов и использованием кабелей, соответствующих различным уровням пожарной безопасности, что предотвращает распространение огня и обеспечивает защиту здания.

64. Технология PoE

Введение: Относительно недавно производители сетевого оборудования начали разрабатывать технологии, позволяющие запитывать относительно маломощные Ethernet-устройства через информационные кабели, такие как витая пара. Эти технологии получили название PoE (Power over Ethernet).

Основная часть: Постепенно были введены два общепринятых стандарта: 802.3f и 802.3at, но до сих пор производители используют собственные проприетарные технологии, например, Cisco Universal Power over Ethernet.

В структуру PoE входят следующие блоки:

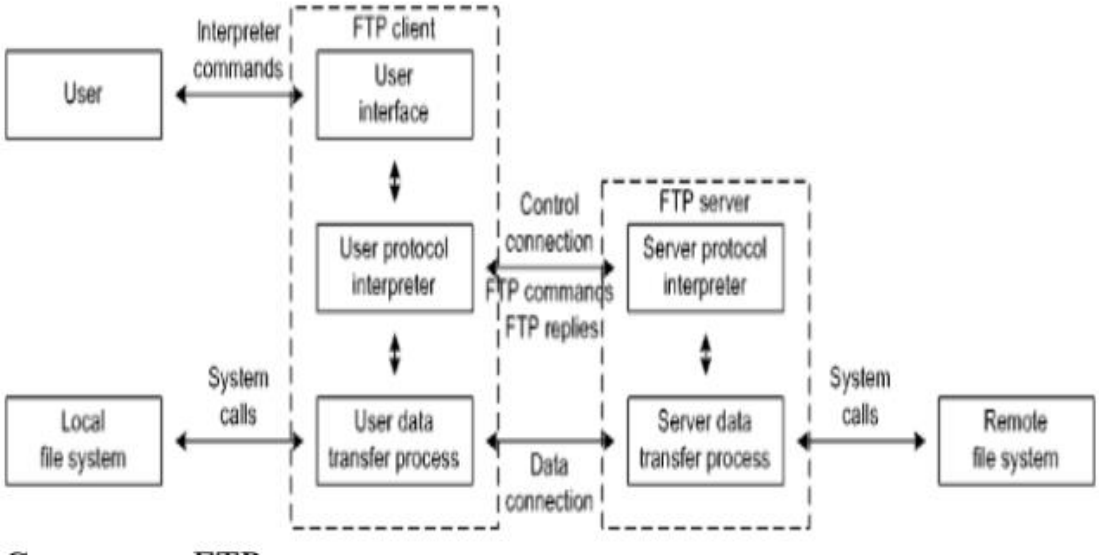
1. PSE (Power Sourcing Equipment) – вводит питающее напряжение в кабель.
2. PD (Powered Device) – питается от этого напряжения.

PSE может располагаться как на одном конце, так и на обоих концах кабеля. Либо оно может быть PoE-инжектором, который «вклинивается» в кабель и вводит напряжение. PoE обычно используется для небольших PD.

Вывод: Технология PoE предоставляет удобное решение для запитывания маломощных Ethernet-устройств через информационные кабели, упрощая установку и эксплуатацию сетевого оборудования.

65. Структура системы FTP

Введение: FTP (File Transfer Protocol) используется для передачи файлов между клиентом и сервером. FTP-клиент обслуживает запросы пользователя и работает на локальной станции, а FTP-сервер работает на удаленной станции и обслуживает запросы FTP-клиента.



Основная часть: Структура FTP-системы включает протокольные интерпретаторы и процессы пересылки данных как в составе сервера, так и в составе клиента. FTP-сервер представляет собой непрерывно выполняющуюся программу, ожидающую запросы от FTP-клиентов. Эта программа может быть реализована в виде демона UNIX или сервиса Windows.

FTP использует два соединения, что отличает его от многих других протоколов. Для него зарезервированы два программных порта: 20 – FTP Data (информационное соединение) и 21 – FTP (управляющее соединение).

Вывод: FTP обеспечивает эффективную передачу файлов между клиентом и сервером, используя два соединения и зарезервированные порты для информационного и управляющего соединений.

66. Протокол FTP и режимы обмена по протоколу FTP

Введение: FTP относится к протоколам прикладного уровня, ориентированным на пользователя. Он должен предоставлять функционально полный интерфейс для управления передачей файлов.

Основная часть: Классический интерфейс FTP представляет собой интерпретатор командной строки, активируемый вводом команды ftp. В качестве аргументов принимаются IP-адрес FTP-серверов и номер порта, если он отличается от стандартного. FTP использует два программных порта: 20 – FTP Data и 21 – FTP (управляющее соединение).

FTP поддерживает три режима пересылки сообщений:

1. Stream – файл пересылается как непрерывный поток байт. <EOF> - конец пересылки.
2. Block – файл пересылается в виде последовательности блоков, каждый из которых имеет заголовок с количеством байт. Этот способ редкий.

3. Compressed – файл пересылается в сжатом простейшими алгоритмами виде. Этот способ также редкий.

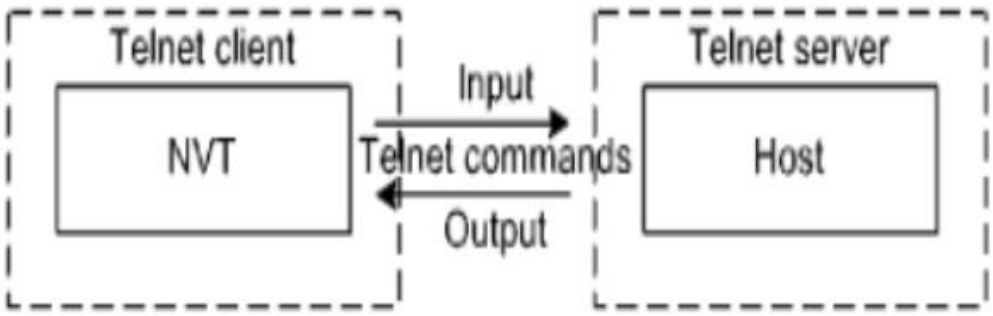
Также FTP поддерживает два режима работы: активный и пассивный.

Вывод: Протокол FTP предоставляет пользователям различные режимы пересылки сообщений и работы, что делает его гибким и универсальным инструментом для передачи файлов.

67. Структура и особенности системы Telnet

Введение: Telnet базируется на клиент-серверной модели и использует протокол TCP для удаленного управления устройствами через сеть.

Основная часть: Telnet использует одно соединение, стандартный номер программного порта Telnet-сервиса – 23.



Структура telnet-системы

Основная задача Telnet – обеспечение корректной транспортировки символов потока и ввода-вывода между NVT (network virtual terminal) и хостом. Для этого используется буферизация, чтобы не нагружать СПД. По умолчанию набранные символы отсылаются моментально, а в режиме linemode – при нажатии Enter.

Главный недостаток Telnet – полная незащищенность соединения от несанкционированного доступа. Данные и текст пересылаются в виде открытого текста (включая пароли, номера телефонов и т.д.). Впоследствии на смену Telnet пришел SSH (secure shell), который обеспечивает защищенное соединение.

Вывод: Telnet обеспечивает удаленное управление устройствами через сеть, но из-за незащищенности соединения был заменен более безопасным протоколом SSH.

68. Электронные письма и почтовые ящики

Введение: Сообщениями протоколов электронной почты являются электронные письма (emails), которые обеспечивают обмен сообщениями между пользователями через сети.

Основная часть: Электронные письма имеют текстовую природу и состоят из конверта (envelope) и содержимого (content). Содержимое включает заголовок (header) и основной текст (body). Структура электронных писем регламентируется стандартами (например, RFC 822, RFC 5322).

Для обеспечения прав и обязанностей, связанных с электронными письмами, предусмотрены механизмы DKIM (DomainKeys Identified Mail) Signatures (RFC 6376) и SPF (Sender Policy Framework) (RFC 7208). Изначально допускалась только 7-битная кодировка US-ASCII.

Почтовый ящик (mailbox) является ключевым понятием системы электронной почты. Он может быть расположен на почтовых серверах (MXes - Mail eXchanges) или на пользовательских станциях, и может быть как локальным, так и удаленным от пользователя.

Вывод: Электронные письма и почтовые ящики обеспечивают обмен сообщениями и их хранение, предоставляя пользователям удобный и функциональный инструмент для общения через сети.