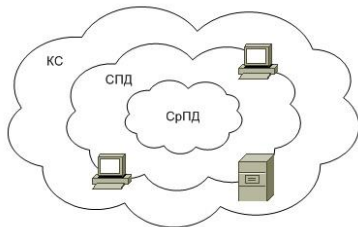


1. Понятие компьютерной сети.

Под компьютерной сетью понимают совокупность различных технических средств (то есть самих компьютеров и другого оборудования), предназначенная для передачи компьютерной информации на относительно большие расстояния (за пределы компьютеров).

В основе лежит сеть передачи данных (СПД), которая может задействовать различные среды передачи данных (СрПД). СрПД соответствует физ. уровню. Модели OSI.



Группы устройств в СПД:

- Оконечные – находятся по периметру СПД
- Посредники – составляют ядро СПД

Типы трафика в СПД:

- Обычные компьютерные данные
- Голос
- Видео

Особенности трафика обеспечиваются Quality of Service (обычно актуально для голоса и видео).

2. Классификация компьютерных сетей.

КС бывают:

- PAN – персональные (подключение устройств к ПК/телефону)
- LAN – локальные (охватывают территорию не более кампуса (eduroam))
- MAN – городские (по всему городу. Тв, передача новостей)
- WAN – глобальные (континент или более)
- RAN – Remote access. Подключение удалённого пользователя.
- Home networks
- Datacenters networks
- Industrial networks

С другой стороны,

- Intranets – внутренние КС предприятий и организация
- Internets – публичные сети.

Могут быть:

- Изолированными – закрытыми для прослушивания
- Открытыми для прослушивания

С точки зрения взаимодействия:

- Сильносвязанными
- Слабосвязанными

Также могут делиться территориально, по стандартизации (EN – Europe, ANSI – America, ISO – международные) и по скорости передачи (Ethernet – 10 Mb/s, Fast Ethernet – 100 Mb/s, Gigabit Ethernet – 1, 10, 100, 40, 25 Gb/s, Multigigabit)

3. Стандарты компьютерных сетей.

Все стандарты разбиваются на три группы: EN – Европейские, ANSI – Американские, ISO – международные. Стандарты лишь формализуют определённые требования к компьютерной сети. Могут носить предварительный (preliminary) или временный (interim) характер. Могут включать дополнения (annexes) и списки обнаруженных ошибок (errata). Также могут замещаться другими стандартами (obsolete).

802.X – серия стандартов, посвящённая КС. Сейчас наиболее популярны и интересны:

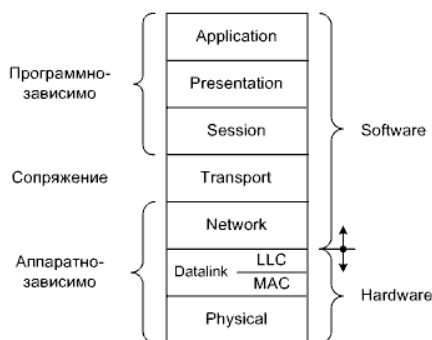
- 802.3 – Ethernet
- 802.11 – WiFi
- 802.16 – WiMax

Данные стандарты поддерживаются вплоть до 80-х годов.

4. Наиболее распространённые модели компьютерных сетей.

Наиболее распространённая – модель взаимодействия систем (open system interconnection), разработанная ISO.

Модель включает 7 уровней (физический, канальный, сетевой, транспортный, сессии, представления, приложения). На верхушке находится человек, но пользователями уровней всё так же являются программы.



Взаимодействие в OSI может быть вертикальным и горизонтальным.

- Интерфейс – взаимодействие между соединениями на одном уровне (горизонтальное)
- Протокол – взаимодействие между разными уровнями OSI (вертикальное).

Также существует модель TCP/IP. Связана с одноимённым протоколом.

OSI Model		TCP/IP Model
L7. Application	-----	Application
L6. Presentation		
L5. Session		
L4. Transport	-----	Transport
L3. Network		Internet
L2. Datalink	-----	Network Access
L1. Physical		

Главная отличительная особенность – Network-access и application-уровни.

Cisco также на основе многолетнего опыта разработала собственную иерархическую модель.

Три уровня:

- 1) Access – уровень доступа (подключение к КС конечных пользователей)
- 2) Distribution – уровень распределения (обеспечение взаимодействия в пределах групп пользователей)

3) Core – ядра (обеспечение высокоскоростной связи)

5. Физический уровень модели OSI.

На физическом уровне формализуют подключение сетевого устройства к КС. В пространстве представляется точкой подключения к КС. Специфические понятия: среда, разъём (физ. порт), несущая частота, модуляция, сигнал. Описывает способы передачи бит (а не пакетов!), через физические линии связи.

6. Канальный уровень модели OSI.

На канальном уровне формализуют взаимодействие между узлами (станциями), находящимися в одном сегменте сети.

Специфические понятия канального уровня:

- Сегмент – множество станций (любое устройство, принимающее трафик), объединённых одной СРПД, которые видят друг друга непосредственно.
- Физ. и лог. топология сегмента
- Бит- байт- стаффинг
- Пакет (кадр)
- Канальный код
- Код проверки целостности
- Алгоритм доступа к моноканалу

Канальный уровень разделяют на два подуровня:

- MAC (Media Access Control) – контроль доступа к СРПД.
- LLC (Logical Link Control) – контроль логического соединения.

На подуровне MAC осуществляется взаимодействие с физическим уровнем, такие как формирование и распознавание пакетов, адресация, канальное кодирование.

На LLC осуществляется взаимодействие с сетевым уровнем, такие как разбиение на пакеты, сборка данных из пакетов, определение подсистемы и другие.

7. Сетевой уровень модели OSI.

Сетевой уровень позволяет «выйти» за пределы сегмента. Предназначается для определения пути передачи данных.

На сетевом уровне формализуют построение полноценной КС, охватывающей произвольное количество сегментов.

Специфическими понятиями сетевого уровня являются:

- пакет (собственно пакет);
- адресация в пределах всей КС;
- маршрутизация.

8. Транспортный и сеансовый уровни модели OSI.

Транспортный уровень позволяет перейти от оборудования к программам. На нём формализуют использование ПО сетевым оборудованием, т.е. как отдельно взятым программам использовать «транспорт». Предназначен для доставки данных

Спец. понятия: пакет (сегмент сообщения), программный порт, логическое соединение, надёжность доставки, алгоритм борьбы с заторами в СПД.

Уровень сессии позволяет предоставлять программам доступ к транспорту в промежутках длительного времени (сессии).

Кроме сессии есть ещё два основных понятия: программный порт, алгоритм мультиплексирования программ. В практических реализациях обычно совмещён с транспортным.

9. Прикладной уровень и уровень представления модели OSI

Уровень представления (presentation) адаптирует прикладную информацию в форму, пригодную для передачи по КС, т.е. это прослойка между программами и транспортом. Основные понятия: кодирование информации с целью обеспечения правильной интерпретации в последующем, шифрование информации с целью защиты при пересылке по открытым для прослушивания сетям.

Прикладной уровень (application) является интерфейсом обмена между приложением и компьютерной сетью. Специфических понятий множество, и они зависят от решаемой задачи, например, пересылка файлов, мгновенная пересылка голоса и видео, пересылка сообщений и т.д.

10. Семейство протоколов TCP/IP

Протоколы TCP/IP обозначают все, что связано с протоколами TCP и IP. В состав семейства входят протоколы UDP, IP, TCP, SMTP, SNMP, TELNET, FTP и многие другие.

Application	FTP	Telnet	SMTP	DNS	HTTP	...
Presentation						
Session						
Transport	TCP			UDP		
Network	ICMP	RIP	OSPF	...		
	IP					
	ARP			RARP		
Datalink	Ethernet		Token Ring	FR	...	
Physical						

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

В 70-х годах компания Intel разработала два контроллера последовательного типа в составе периферии для 8086. Один из них получил название 8250, UART (Universal asynchronous receiver/transmitter). Были рассчитаны на подключение к шине X-Bus.

Во времена 80286 были созданы несколько UART, самый успешный из которых стал 16550 от National Semiconductor (max baud rate from 9600 to 115200). В СССР развивался свой аналог, но распространения он не получил.

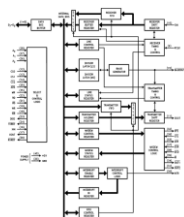
Дальше получили распространение мультикарты, вследствие чего сформировался Multi I/O (доп. плата).

Во времена Pentium стали Super I/O, которая впаивалась на мат. плату.

В настоящее время данные порты считают устаревшими и исключают из состава периферии. В настоящем интерфейс называется RS-232.

12. Структура COM-портов ПК

На аппаратном уровне приемник и передатчик работают параллельно т.е. по отдельным физическим цепям полностью независимо друг от друга. Для физического подключения по стандарту RS-232 используют девятиконтактные разъемы DE-9. Передатчик и приемник COM-порта представляют из себя сдвиговые регистры: данные, предварительно записанные в регистр передатчика параллельно, последовательно сдвигаются в линию под воздействием тактовых импульсов.



Стоит запомнить, но я не смогу.

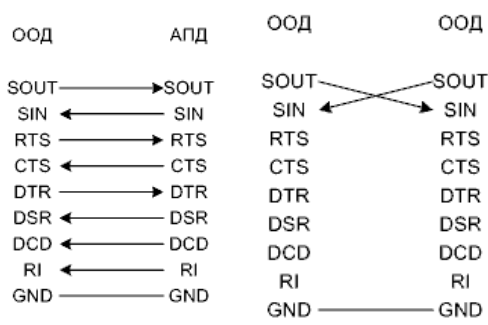
13. Цепи RS-232 и их использование

Всего существует 9 цифровых цепей RS-232:

- SOUT – serial output (выход приёмника)
- SIN – serial input (вход приёмника)
- RTS – ready to send (сигнал-запрос о передаче байта)
- CTS – clear to send (сигнал-подтверждение о готовности принять байт)
- DSR – data set ready (сигнал от модема к порту о готовности)
- DTR – data terminal ready (сигнал от порта к модему о готовности)
- DCD – data carrier detect (сигнал от модема к порту об обнаружении данных)
- RI – ring indicator (сигнал о входящем звонке)
- GND – ground (уровень земли, или нуля)

Данные цепи позволяют налаживать связь между оборудованием по принципу модем-порт и по принципу порт-порт (нуль-модемное соединение).

Реализации бывают полностью программные (XON/XOFF) и полуаппаратные (RTS/CTS). Все реализации предполагают обратную связь с приёмником.



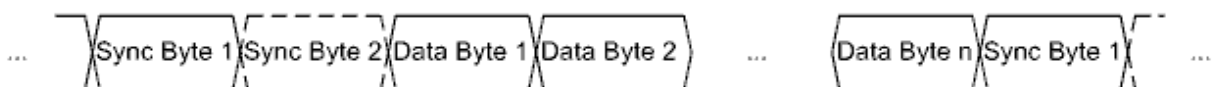
14. Асинхронный режим работы COM-порта

В асинхронном режиме синхронизируется обмен каждого информационного байта. Порт-отправитель посылает стартовый бит, который сигнализирует, что следует начать отлов первого информационного бита. Скорость передачи меньше, чем в синхронном режиме.



15. Синхронный режим работы COM-порта.

В синхронном режиме синхронизируется весь информационный обмен, т.е. вставляются байты синхронизации при простое канала. Не приходится вставлять байты начала и конца сообщения.



Минимальная адресуемая ячейка для UART – байт. Причём байт может быть от 5 до 8 бит.

16. Тактирование COM-порта

Так как по сути COM-порт – это сдвиговый регистр, то ему нужны какие-то импульсы тактирования. Тактирование данных портов осуществляется непрерывно и происходит с помощью встроенного программируемого бод-генератора. Бод-генератор представляет собой программируемый делитель частоты. Частота F_{out} осуществляется по формуле $F_{out} = F_{in} / (16 * DL)$, где DL – шестнадцатититная

константа, старшая и младшая часть которой хранятся в двух регистрах UART (DLL и DMM). Частота тактирования измеряется в бодах.

17. Архитектура COM-портов ПК

В стандартной архитектуре для RS-232 зарезервированы следующие порты в адресном пространстве ввода-вывода процессора: 3F8-3FF и 2F8-2FF в шестнадцатеричной с.с. По данным адресам хранятся регистры портов. При этом предоставлена возможность работы по прерываниям. Стандартными аппаратными прерываниями COM1 и COM2 являются IRQ4 и IRQ3 соответственно (также 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

18. Стандарты, близкие к RS-232

Так как RS-232 формировался как интерфейс для разноранговых устройств, т.е., как интерфейс для подключения периферии. Объединять более двух устройств по данному интерфейсу было невозможным. Вследствие, продолжением стали два стандарта: RS-422 и RS-485. В отличие от RS-232 они передавали на дальние расстояния и на больших скоростях за счёт использования дифференциальной пары вместо изменения потенциала относительно земли.

19. Структура типового пакета компьютерной сети

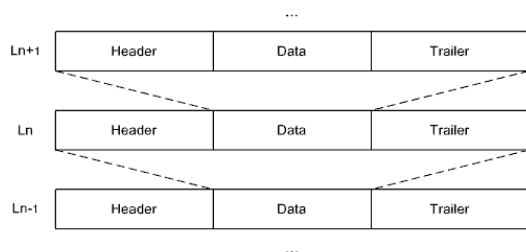
Начало пакета				Конец пакета	
Flag	Destination Address	Source Address	Other Fields	Data	FCS
Header				Payload	Trailer

- Flag – флаг начала пакета.
- DA – адрес назначения.
- SA – адрес отправителя.
- Other fields – специфические поля определённой реализации.
- Data – полезная нагрузка.
- FCS (frame checksum) – контрольная сумма, проверяющая целостность пакета.

Часть пакета, расположенной до полезной нагрузки принято называть header-ом. После – trailer-ом.

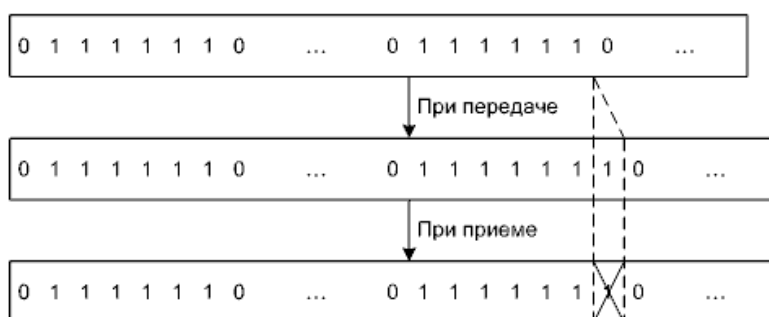
20. Инкапсуляция и ее проявления в компьютерных сетях

Под инкапсуляцией в КС подразумевают вкладывание пакета, определённого вышестоящего уровня в поле данных пакета нижестоящего уровня в процессе подготовки к передаче, т.е. при продвижении сверху вниз.



21. Битстаффинг

Когда пакет данных передаётся – его начало и конец обозначается флагом начала и конца (обычно это символ «~»), или следующая последовательность из бит: 01111110). Но такая последовательность может присутствовать и в сообщении. Битстаффинг решает эту проблему вставкой дополнительного бита (0 или единицы, как задано в системе), после последовательности из 6 единиц (т.е. мы насильно заменяем следующий бит на бит стаффинга). Пример, с битом стаффинга «1»:



22. Байтстаффинг

При байтстаффинге происходит такая же ситуация, как и при битстаффинге. При передаче пакет имеет флаг начала и конца. При обнаружении в поле полезной нагрузки пакета байта, совпадающего с байтом флага, происходит замена данного байта на некоторый другой (например, «~» на «8»). Но тогда будет проблема. Что если мы встретим заменённый символ в последовательности (в нашем случае «8»). Для этого вставляется ESC-байт. Наличие ESC-символа говорит о факте замены, а следующий за ESC-символом символ – код замены позволяет определить какая замена была осуществлена.

Пример:



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

Линейное кодирование – адаптация битовых последовательностей к возможностям физического уровня с целью обеспечения или улучшения технических характеристик. Слово «линейное» происходит от понятия физической линии.

Все линейные коды направлены на преобразование битовых последовательностей, чтобы в линии всегда происходили изменения, и, соответственно, чтобы шанс помех был меньше.

Коды классифицируются по следующим признакам:

- Кодирование уровнями или переходами
- Наличие инвертирования
- Однополярность или многополярность
- Наличие «возврата к нулю»
- Наличие самосинхронизации
- Наличие перестановки или подмены битов

Всего есть 5 основных способов кодирования:

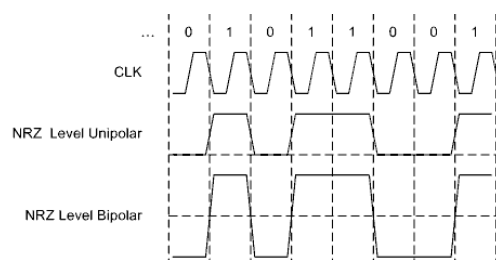
- NRZ (non-return zero) – коды без возврата к нулю
- RZ (return zero) – коды с возвратом к нулю
- Manchester code – манчестерские
- MLT (Multi-level transmit) – многоуровневые коды
- Block codes – блочные коды

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

NRZ-коды выражаются изменением уровней между тактами. В простых случаях, логические уровни или не преобразуются вообще или инвертируются. В более сложных – уровень инвертируется при приходе нуля (space) или единицы (mark).

Область применения: RS-232, RS-485, USB

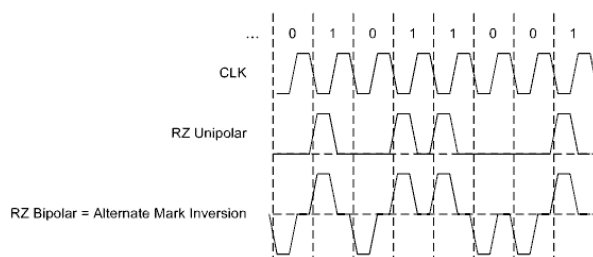
Пример:



RZ-коды выражаются переходом к нулю (gnd) на каждой половине такта. Двухполярные RZ-коды обладают самосинхронизацией (0 в них выражается как -1, и после перехода в логический уровень нуля (-1В) сигнал переходит в землю (0В)).



Область применения: IrDA

Пример:



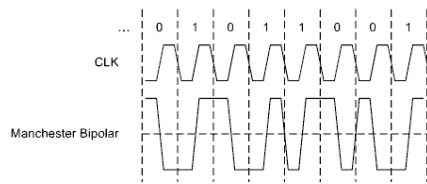
25. Манчестерские и многоуровневые линейные коды

Манчестерские уровни выражаются в переходах между уровнями во время тактов. Так как 0 будет

выглядеть в манчестерском коде вот так: , а единица вот так:  из этого можно предположить, что данные коды обладают свойством самосинхронизации (так как нуль всё равно всегда будет подниматься изначально вверх, а потом спадать вниз. Единица, соответственно, наоборот).

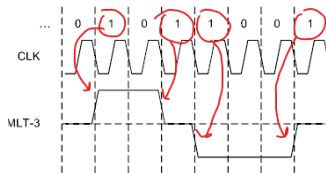
Манчестерский код широко используется в стандартах Ethernet, Token Ring.

Пример:



Многоуровневые коды выражаются в переключении между несколькими уровнями между тактами. Например, MLT-3 имеет три уровня: 1, 0, -1. Переключение происходит по единице, что означает переход на соседний уровень. Используется в Fast Ethernet.

Пример:



26. Блочные линейные коды

Блочные коды выражаются в замене блоков битов из входной последовательности на бóльшие блоки битов. Блочные коды могут комбинироваться со всеми кодами, оперирующими битами. В связи с избыточностью, во многих предусмотрены контрольные последовательности. Из минусов таких кодов стоит выделить лишь большое количество необходимой памяти для хранения таблицы. Из плюсов – кодирование и декодирование становится лёгким.

27. Поля Галуа и их применение в компьютерных сетях

В помехоустойчивом кодировании очень важное место занимают поля Галуа.

В помехоустойчивом кодировании все операции выполняются по, так называемой, арифметике Галуа. Т.е. результатом любой арифметической операции будет являться элемент из данного поля. Поля задаются целым числом. Пример: GF (Galua field) от 5 будет равно: GF(5) = 0, 1, 2, 3, 4. Пример сложения: $0 + 1 = 1$, $4 + 1 = 0$, $4 + 3 = 2$. Умножение: $4 * 2 = 3$. И т.д. (операции делаем по модулю).

Для бинарных же векторов арифметика намного сложнее. Сложение тут будет представляться операцией xor GF(4): ($1 + 1 = 0$, $2 + 2 = 0$, $3 + 1 = 2$). Умножение – умножением полиномы GF(8): (например, $5 = 101 = x^2 * 1 + x * 0 + 1 * 1$, $7 = 111 = x^2 * 1 + x * 1 + 1 * 1$. $5 * 7 = (x^2 + 1) * (x^2 + x + 1) = x^4 + x^3 + x^2 + x^2 + x + 1 = x^4 + x^3 + x + 1 = 11011 = 27$). $x^2 + x^2$ складываются по xor (получается 0). Далее, так как результат не входит в используемое поле, необходимо использовать порождающий полином (выбирается самостоятельно). В качестве полинома используется неприводимое (простое) число. Используем $x^3 + x + 1 = 1011 = 11$. Вернёмся к умножению. Теперь складываем порождающий полином и результат умножения (всё ещё по модулю): $(x^4 + x^3 + x + 1) + (x^3 + x + 1) = x^4$.

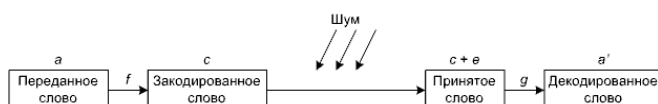
Деление можно представить, как умножение полинома-делимого на полином, обратный делителю.

28. Модель помехоустойчивого канала связи и теорема Шеннона

Помехоустойчивое кодирование – кодирование, предназначенное для проверки целостности и восстановления ошибочных битов.

Начало данному кодированию положила теорема Шеннона. Она утверждает, что любой дискретный канал связи имеет конечную пропускную способность и этот канал может быть задействован для передачи информации со сколь угодно большой степенью достоверности, несмотря на наличие помех. (любой канал может быть максимально помехоустойчивым)

Модель такого канала связи:



Сообщение разбивается на блоки битов фиксированного размера a , кодер выполняет функцию f (в код вставляются биты проверки), поступает шум, после пересылки декодер декодирует по функции g слово a' , которое, в идеале, должно получаться таким же, как и a .

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

Так как помехоустойчивое кодирование выполняется по системе линейных уравнений, помехоустойчивые коды называются линейными. Особенностью являются дополнительные проверочные символы (обычно биты).

Код Хэмминга – самокорректирующийся и самоконтролирующийся код, который позволяет исправить одну ошибку и обнаружить множественные ошибки. Сообщение кодируется с помощью вставки дополнительных битов.

Циклические коды – линейные коды, которые позволяют исправить одну и более ошибок и обнаружить множество (в зависимости от реализации). Главная идея – передавать в качестве проверочных битов остаток от деления на некоторое выбранное число. После передачи выполняется деление возможно искажённых битов на то же самое число и остатки сравниваются. Если остатки совпадают – то данные, скорее всего, переданы без ошибок.

На практике используется арифметика Галуа (без учёта переносов).

30. Классификация помехоустойчивых кодов

Две главные группы это:

- Коды, обнаруживающие ошибки (позволяют только обнаружить ошибку)
- Коды, исправляющие ошибки (позволяют обнаружить и исправить ошибки)

Также коды делятся на:

- Линейные коды – коды, проверочные биты которых образуются вследствие линейной системы уравнений.
- Нелинейные – которые образуются различными другими путями.

Могут делиться на:

- Блочные – сообщение разбивается на блоки.
- Непрерывные – неразделяемая последовательность символов.

(можно было добавить Сверточные коды, Арифметические коды, Низкоскоростные коды, но по ним не нашёл информации).

31. Классификация каналов в сети передачи данных

С точки зрения направленности, канал может функционировать в одном из трёх режимов:

- Симплексном – передача возможна только в одном направлении
- Полудуплексном – передача может осуществляться в двух направлениях, но в один момент времени может передаваться лишь в одну сторону
- Полнодуплексный – передача может осуществляться в обе стороны одновременно.

На данный момент в КС доминируют полнодуплексные каналы.

Также последовательный канал может быть:

- Выделенным – зарезервирован определённой парой станций-абонентов
- Разделяемый – может разделяться несколькими абонентами

32. Логические и физические топологии LAN

Топологии возникают на канальном уровне, при организации сегмента. Прежде всего выделяют две самые частые реализации:

- Point-to-point – связывает только две станции
- Multi-access – связывает более двух станций (множественный доступ).

Также могут добавляться:

- Point-to-multipoint – используется иногда
- Multipoint-to-point – очень редко

В плане топологий различают физическую (отражает физические связи) и логическую (отображает логику взаимодействия). Часто физическая не совпадает логической.

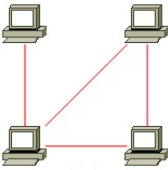
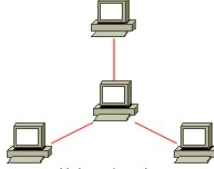
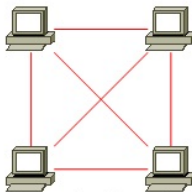
Логические топологии в LAN:

- Шина
- Кольцо
- Звезда

Причём физически топологии шины, кольца и звезды совпадают (коммутатор посередине, все остальные узлы связаны с ним). Также сегмент может иметь гибридную топологию.

33. Логические и физические топологии WAN и RAS.

Логические топологии WAN:

- Сеть (mesh): 
- Ступица-со-спицами (hub-and-spokes): 
- Полная связь (full mesh): 

Данные сегменты также могут иметь гибридную топологию

Логической топологией для RAS (remote access server) является point-to-point, по логичным причинам.

34. Особенности случайных методов доступа к моноканалу

Если в СрПД два или более передатчика, находящихся в равных условиях одновременно выдают сигналы, то возникает противоречие (коллизия).

Коллизия может быть физической (несовместимые физические процессы), при этом система выйдет из строя, так и логической (информационный конфликт). Обычно коллизия возникает при попытке установить различные физические уровни. Сегмент, в котором возможно возникновение коллизии называется доменом коллизии. Понятие коллизии относится не только к сигналу, но и к пакету!

Способы борьбы с коллизиями:

- Не допускать коллизий вообще (детерминированный доступ к моноканалу, Token ring)
- Допускать коллизии и каким-то образом выходить из них (CSMA/CD).

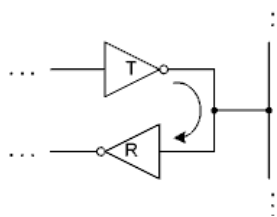
Во втором случае могут быть два подхода:

- Не обращать внимание на причины возникновения коллизии, а делать упор на выходе из них
- Пытаться предотвращать коллизии, а если возникают, то «тяжело» выходить из них

Таким образом методы доступа к моноканалу делятся на детерминированные и случайные.

Все случайные методы основаны на использовании генератора случайных чисел, который позволяет делать случайные задержки при попытке доступа к моноканалу, а значит, с определённой вероятностью избегать коллизии.

Ключевая особенность – выход передатчика и входа приёмника станции – одна цепь

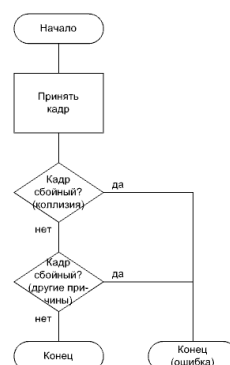


35. CSMA/CD (Ethernet)

Данный метод является наглядным методом доступа к моноканалу. Carrier Sense Multiple Access / Collision Detection – множественный доступ с прослушиванием несущей / обнаружением коллизии. Всего включает две схемы:



Передача кадра



Принятие кадра

Ключевой особенностью являются следующие моменты:

- Обнаружение коллизии.
В этом случае передатчик должен передать JAM-сигнал (сигнал для обнаружения станциями коллизий и для синхронизации времени начала случайных задержек), инкрементировать счётчик попыток, и, если он не переполнен, выждать случайную задержку (измеряется в слот-таймах), которая определяется по номеру попытки ($T_{rand} = 2^k$, где k – случайно сгенерированное число в диапазоне от 0 до tryNumber).
- Обнаружение поздней коллизии или переполнение счётчика попыток
В этом случае уже ничего не поделать, и передатчик должен отправить сообщение об ошибке.

Слот-тайм является минимальной неделимой единицей времени и подбирается с учётом многих параметров (как минимум должен быть больше окна коллизии + времени передачи JAM-сигнала)

Окно коллизии – промежуток времени, при котором любая станция гарантированно обнаруживает коллизию. Равен удвоенному времени прохождения сигнала между двумя максимально удалёнными станциями.

36. Кадр Ethernet

7 B	1 B	6 B	6 B	2 B	46 -- 1500 Bytes		4 B	?
Preamble	SFD	DA	SA	Length/ Type	Data	Pad	FCS	Extension

Поля:

- Preamble – преамбула. Преамбула используется в качестве синхронизирующей последовательности для интерфейсных цепей и способствует декодированию битов. (10101010b)
- SFD (Start Frame Delimiter) – разграничитель начала кадра
- DA (Destination Address) – адрес назначения
- SA (Source Address) – адрес источника
- Length/Type – длина либо тип
- Data – данные
- Pad – наполнитель. Необязательное поле. При недостатке в поле данных вслед за ним в кадр вставляются дополнительные октеты-наполнители (значения стандартом не регламентируются)
- FCS (Frame Check Sequence) – контрольная сумма. FCS используется для обнаружения ошибок в данных, содержащихся в кадре.

Данный заголовок имеет фиксированную длину, но производители Ethernet-оборудования предусмотрели нестандартные увеличения заголовка вплоть до 9000 байт (jumbo-кадры).

37. CSMA/CA (Wi-Fi)

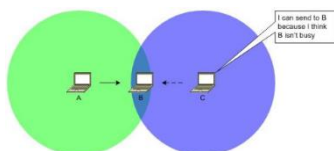
CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance) множественный доступ с прослушиванием несущей и избеганием коллизий.

Случайная задержка измеряется в слот-таймах, но алгоритм другой. Количество слот-таймов (времени задержки после коллизии) является целым числом: $0 \leq \text{Random} \leq \text{CW}$, где CW – так называемое окно состязаний (contention window), $\text{CW}_{\min} \leq \text{CW} \leq \text{CW}_{\max}$, и берётся из ряда 7, 15, 31 ($2^n - 1$). Типичные значения: $\text{CW}_{\min} = 15$, $\text{CW}_{\max} = 1023$.

Также предусмотрены счётчики попыток (SRC – short retry counter, LRC – long retry counter). Количество попыток также ограничивается.

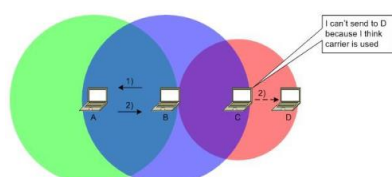
Также для беспроводных каналов появляются две проблемы: Hidden node problem (проблема скрытой станции) и Exposed node problem (проблема доступной станции). Эти проблемы возникнут, если не учесть окно коллизий (промежуток времени, при котором любая станция гарантированно обнаруживает коллизию. Равен удвоенному времени прохождения сигнала между двумя максимально удалёнными станциями).

Проблема скрытой станции:



Станция С может посылать сообщение вместе со станцией А станции В, потому что не будет знать о существовании станции А.

Доступной станции:



Станция С не может отправлять сообщение станции D, так как видит, что станции В посылает сообщение станция А, и она думает, что канал занят

Данные проблемы можно частично решить путём добавления сигналов RTS (ready to send) / CTS (clear to send).

38. Кадры Wi-Fi

В отличие от Ethernet, в Wi-Fi используется 3 типа кадров:

- Кадр данных (как и в ethernet)
- Кадр контроля (служебные кадры, необходимые для корректной работы, к примеру, ACK, RTS, CTS)
- Кадры управления (например, подключение к Wi-Fi или аутентификация)

Данный тип определяется в поле контроля кадра (Frame Control)

2 Bytes	2 B	6 B	6 B	6 B	2 B	6 B	2 B	4 B	0 – 11454 B	4 B
Frame Control	Duration /ID	Address 1	Address 2	Address 3	Sequence Control	Address 4	QoS Control	HT Control	Frame Body	FCS
Header										
2 bits	2 b	4 b	1 b	1 b	1 b	1 b	1 b	1 b	1 b	1 b
Protocol Version	Type	Subtype	To DS	From DS	More Fragments	Retry	Power Management	More Data	Protected Frame	Order

Поля контроля кадров:

- Protocol version
- Type (00 – управление, 01 – контроль, 10 – данные, 11 – зарезервировано)
- Subtype – просто подтип (в настоящее время более 40 видов)
- To DS – флаг направления в распределительную систему (bool)
- From DS – флаг направления из системы (bool)
- More Fragments – флаг наличия фрагментации
- Retry – флаг повторной попытки
- Power management – флаг режима энергосбережения
- More Data – флаг доп. данных (например, буферизированных, находящихся на станции)
- Protected Frame – защищённость кадра
- Order – флаг упорядочивания (при QoS)

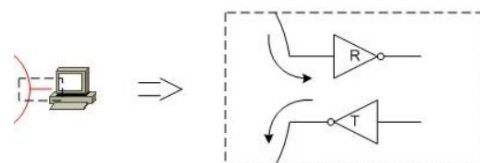
Поля пакета (только те, которые не следуют из их названия):

- Duration / ID - длительность-идентификатор (0 – 32767 us)
- HT Control – контроль интенсивной пересылки (high throughput)
- Frame Body – данные (содержимое кадра)

39. Особенности детерминированных методов доступа к моноканалу

Кольцо можно рассматривать как своеобразный моноканал, один такт которого соответствует полный или частичный «обход» кадром всех станций.

Ключевая особенность – что кольцевую (как и моноканальную) топологию можно представить следующим образом:



Т.е. каждый приёмник соединён с передатчиком предыдущей станции

При такой технологии никаких физических коллизий не должно быть, но существует особый тип логических коллизий.

Проблема: станция имеет собственный кадр для передачи к ней приходит кадр, который необходимо продвигать дальше. Какой из этих кадров стоит продвигать?

Частичное решение: введение буферов. Но возлагать на обычную станцию пользователя роль сетевого моста – нецелесообразно.

Полное решение: введение уровней уровни приоритетов. Благодаря этому возникает задача распределённых приоритетов. При этом не обойтись без арбитра (token, маркер). Это будет специальный служебный кадр, который будет давать приоритет станции.

40. Алгоритм Token Ring

В данном алгоритме применяется централизованное управление. В кольце должна быть минимум одна станция-монитор, которая призвана инициализировать кольцо и следить за её работоспособностью.

Несмотря на то, что Token Ring предполагает некоторое распараллеливание, обобщённо алгоритм можно представить, как бесконечно циркулирующий, под действием станции-монитора маркер (токен), который анализируется всеми станциями и к которому при необходимости «цепляются» данные.

В данном алгоритме предусмотрены четыре вида последовательностей:

- Token – маркер
- Frame – кадр
- Abort sequence - прерывающая последовательность
- Fill – заполняющая последовательность

Несмотря на то, что в стандарт заложена комплексная система приоритетов, некоторые «тонкости» оставлены на реализации.

Главное – чтобы в алгоритме были поля P и R, где P – поле текущего приоритета, а R – поле запрашиваемого приоритета. Каждое из полей может иметь значение от 000b до 111b. При отсутствии маркера, станция-монитор создаёт и запускает токен с нулевыми значениями этих полей. С помощью этого токена и реализуется предоставление права на передачу сообщения.

Далее:

- Если у станции есть сообщения на передачу, оно захватывает токен и выставляет поле T (is token) в единицу (значит, что кадр – не является токеном), преобразует маркер в кадр и отправляет сообщение.
- Если нету сообщений – посылает токен дальше.

Если на станцию приходит сообщение, адресованное не ей – она передаёт его дальше по кругу. Если станции приходит сообщение, адресованное ей – она изменяет поле C (значит, что прочитано и скопировано) и отправляет дальше в кольцо. Причём удалять этот кадр из кольца сможет только станция, которая его создала. Станция посылает маркер после того, как получит сообщение-подтверждение от станции, которой было адресовано сообщение.

Также существует опция раннего освобождения маркера, при котором станция не ждёт подтверждения от станции, которой оно отправляет сообщение.

Владение токеном ограничено и контролируется таймером ТНТ (token holding timer)

41. Реализации детерминированных методов доступа к моноканалу

Кроме Token Ring есть ещё ряд технологий:

- ARCNET – первая технология ЛКС, массово использовалась до Ethernet. В настоящее время считается устаревшей. Имела скорость 2,5 Мб/с и физ. топологию шины и лог., кольца. Алгоритмом использовался Token Ring без приоритетов.
- Token Bus – разработана параллельно с Token Ring. Благодаря плохому масштабированию (подключению новых пользователей) и постоянных сбоях почти не использовалась, но была стандартизирована на 802.4. Физическая топология: шина, логическая: однонаправленное кольцо. Скорость: 1, 5, 10, 20 Mb/s.
- FDDI (Fiber Distribution Data Interface) – разработана с целью передачи информации на дальние расстояния. Физ. топология двойного кольца (два параллельных) лог. топология однонаправленное кольцо с резервированием.

- 10VG-AnyLAN – разработана как альтернатива Fast Ethernet, продвигалась как гибрид Ethernet и Token Ring. Имела скорость в 100 Mb/s, и физическую и логическую топологию дерева.

42. Адресация в компьютерных сетях и классификация адресов

В качестве двух обязательных адресов используются:

- Адрес назначения
- Адрес источника

Адресация «привязана» к протоколу, а протокол – к уровню модели сети, на котором происходит адресация. В каждом пакете должны быть, как минимум, адреса канального уровня. Такие адреса часто «вшиваются» в сетевое оборудование, и разработчик никак не может на них повлиять. Такую адресацию называют физической. Кроме того, адресация может быть иерархической – т.е. выражаться в разделении адресов на типы.

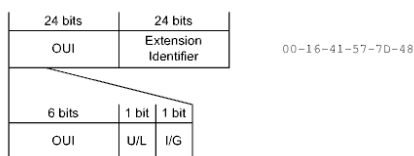
Для компьютерных сетей есть четыре типа адресов:

- Юникаст – пакет с таким адресом назначения должен быть обработан одной конкретной станцией
- Бродкаст – пакет должен быть обработан всеми станциями
- Мультикаст – пакет должен быть обработан несколькими станциями из множества
- Эникаст – пакет должен быть обработан одной станцией из множества (наиболее сложная адресация)

43. MAC-адреса

MAC-адреса должны быть уникальны и контролируются IEEE RA (Registration Authority). MAC-48 можно считать аналогом EUI-48, т.к. изначально это было общим понятием.

Формат таких адресов:



- OUI – Organization Unique Identifier (выдают централизованно, уникальность остальной части – проблема организации)
- U/L – Universal/Local
- I/G – Individual/Group
- Extension identifier – идентификатор-наполнитель.

Время валидности адресов – 100 лет.

Также известны три вида MAC-адресов: MA-L (24) MA-M (28) MA-L (36 битов).

По правилам данные адреса записывают в формате:

XX-XX-XX-XX-XX-XX.

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

Cisco: 0016.4157.7d48

Все Unicast-адреса должны иметь нулевые значения битов I/G

В качестве бродкаст-адреса принято использовать значение FF-FF-FF-FF-FF-FF

44. Заголовок IPv4

octet		octet		octet		octet	
Version	IHL	Type of Service		Total Length			
Identification				Flags	Fragment Offset		
Time to Live		Protocol		Header Checksum			
Source Address							
Destination Address							
Options						Padding	

Поля:

- Version – версия (значение равно 4)
- IHL (internet header length) – длина заголовка в 32-битных словах, минимальное значение 5
- Type of Service – тип QoS
- Total Length – общая длина данных в байтах
- Identification – идентификатор начала
- Flags – флаги
 - DF – don't fragment – 0 - пакет фрагментирован, 1 - не фрагментирован
 - MF – more fragments – 0 - текущий фрагмент является последним, 1 - не последним.
- Fragment Offset – смещение фрагмента относительно прошлых (в 64-битных словах).
- Time to live – время жизни, уменьшающееся при каждой ретрансляции
- Protocol – протокол (инкапсулируемый в поле данных)
- Header checksum – контрольная сумма заголовка
- Source address – адрес источника
- Destination address – адрес назначения.
- Option – опции (например вариативность размера)

45. Заголовок IPv6

octet	octet	octet	octet
Version	Traffic Class	Flow Label	
Payload Length		Next Header	Hop Limit
Source Address			
Destination Address			

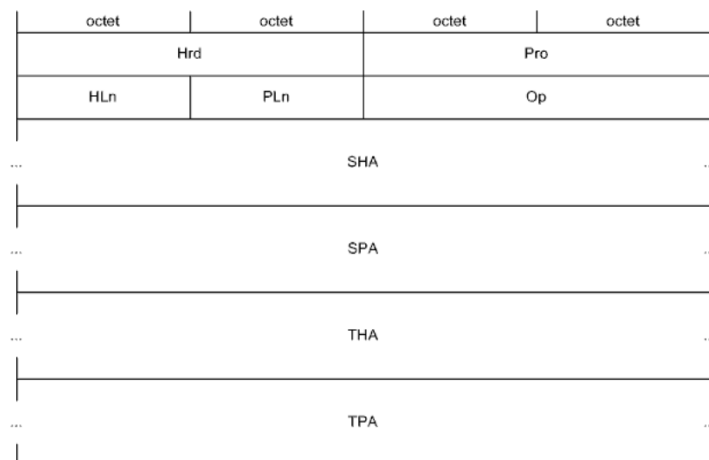
Поля:

- Version – версия (6)
- Traffic class – тип трафика (связан с QoS)
- Flow label – метка потока (связана с QoS)
- Payload length – длина полезной нагрузки в байтах (аналог Total length)
- Next header – селектор следующего заголовка
- Hop limit – ограничитель числа «прыжков» между станциями (аналог Time to Live)

46. Протокол ARP

Группа протоколов ARP (Address resolution protocol) предназначена для восстановления соответствий между MAC-адресами и IP-адресами.

Под прямым преобразованием (соответственно, ARP-преобразованием) понимают нахождение MAC-адреса по IP-адресу. Обратное преобразование выполняется по протоколу RARP (Reverse ARP).

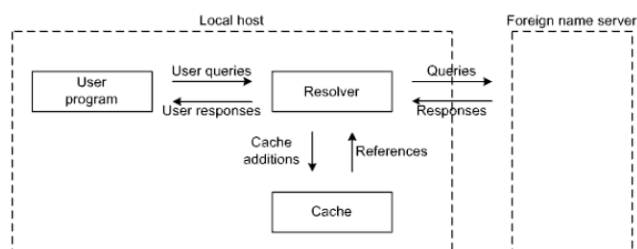


- Hrd (hardware) – тип оборудования
- Pro (protocol) – протокол
- HLn – Hardware address length
- PLn – protocol address length
- Op (Opcode) – код операции (1 – Request, 2 – Reply, и другие)
- SHA – sender hardware address
- SPA – sender protocol address
- THA – target hardware address
- TPA – target protocol address

47. Структура системы DNS

Протокол системы DNS (Domain Name System) предназначен для восстановления между IP-адресами и адресами прикладного уровня.

Под доменом в СПД понимают совокупность устройств, работающих в рамках неких единых правил. Некоторые служебные протоколы, в том числе DNS нельзя сопоставить с моделью OSI, хотя исходя из инкапсуляции, данный протокол можно отнести к прикладному уровню.



клиентов (resolvers)

Структура DNS соответствует клиент-серверной модели и включает три основных компонента:

- Адресное пространство доменных имён и записи о ресурсах (Resource Records). Каждой станции соответствует некоторое кол-во RR.
- Сервера названий (name servers)
- Программы, отвечающие на запросы

Адресное пространство имён имеет иерархическую древовидную структуру. Каждый узел дерева обозначают DNS-меткой, длиной от 0 до 63 байт. Метка нулевой длины зарезервирована и должна начинать древо. Доменное название строится из меток в соответствии с путём к корневой ветке. Полная длина не должна превышать 255 байтов. Может быть абсолютным (содержащим все метки до корня) или относительным (не все). Согласно нотации метки разделяют точками и корневая является крайней справа. Под прямым преобразованием понимают нахождение IP по доменному названию.

Сервера названий делят на: авторитетные (первоисточники информации о некоторых частях) и вспомогательные (работающие на основании сведений от первоисточников).

48. Сообщения DNS

Header
Question
Answer
Authority
Additional

Формат сообщения DNS

- Header – заголовок (есть всегда, все остальные поля вариативны)
- Question – запрос
- Answer – ответ
- Authority – авторитетный ответ
- Additional – дополнение

octet				octet			
ID							
QR	Opcode	AA	TC	RD	RA	Z	ADCD RCODE
QDCOUNT							
ANCOUNT							
NSCOUNT							
ARCOUNT							

Формат заголовка DNS

- ID – Identifier
- QR (Query/Response) – флаг запроса-ответа (0 – Query, 1 – Response)
- Opcode – код операции
- AA – Authoritative answer
- Z – нулевой бит
- RCODE (Response code) – код ответа
- QDCOUNT (Query DNS count) – количество RRs в поле Query (обычно один)
- ANCOUNT (Answer count) – количество RRs в поле Answers
- NSCOUNT (Name server count) – количество RRs в поле Authority
- ARCOUNT (Additional records count) – количество RRs в поле Additional

(Остальные поля не добавлял, потому что считаю не особо важными)