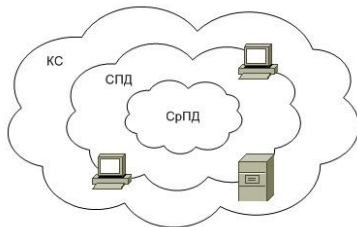


1. Понятие компьютерной сети.

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).

Практическим (или теоретическим) воплощением стандарта является так называемая реализация.

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

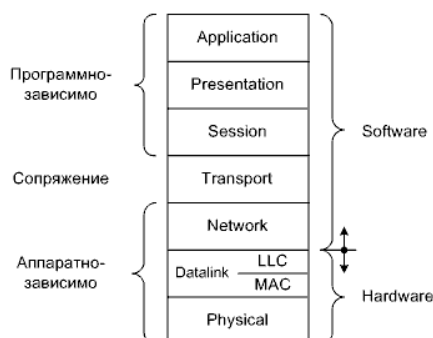
- 802.3 – Ethernet
- 802.11 – WiFi
- 802.16 – WiMax

Данные стандарты поддерживаются вплоть до 80-х годов.

4. Наиболее распространенные 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 вершине находится человек, но пользователями уровней всё так же являются программы.



Взаимодействие в OSI может быть вертикальным и горизонтальным.

- Интерфейс – взаимодействие между пространственно совмещёнными соседними уровнями OSI
- Протокол – взаимодействие между пространственно разнесёнными одинаковыми уровнями OSI (горизонтальное).

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

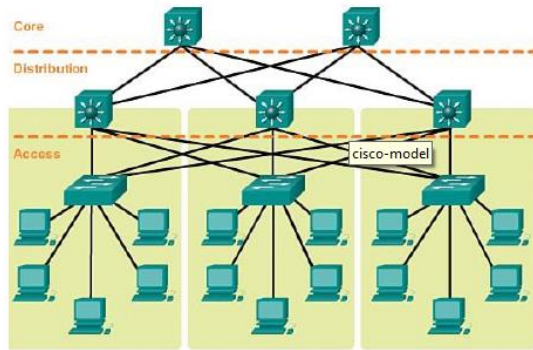
OSI Model		TCP/IP Model
L7. Application		Application
L6. Presentation		
L5. Session		
L4. Transport		Transport
L3. Network		Internet
L2. Datalink		Network Access
L1. Physical		

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. Примеры протоколов: Ethernet, Token Ring, Bluetooth.

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.

Примеры протоколов: PTP (point-to-point), Ethernet

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.

Протоколы: IPv4/6, ARP, RARP

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.

Протоколы: TCP, UDP

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.

Протоколы: HTTP, DNS, FTP, Telnet

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	TCP			UDP		
Transport						
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.

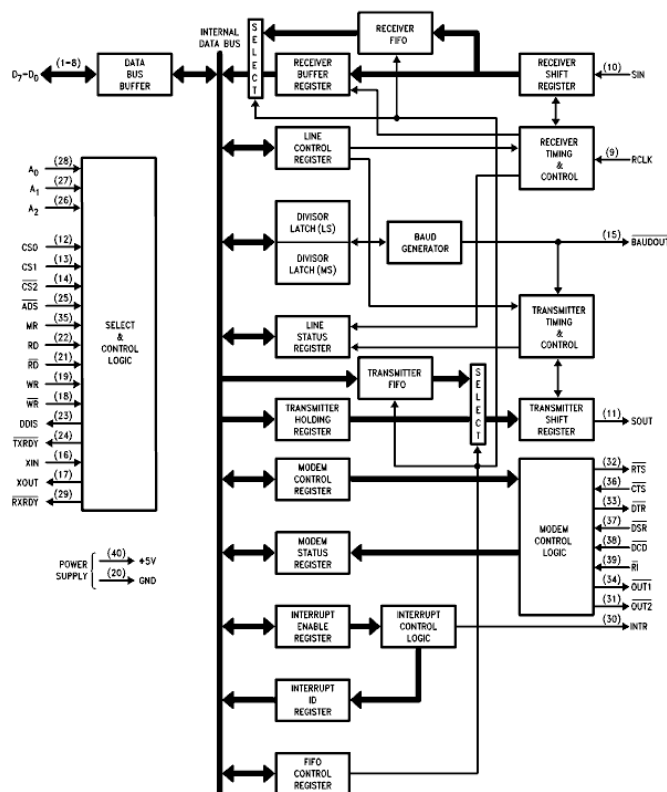
Дальше получили распространение мультикарты, вследствие чего сформировался Multi I/O (доп. плата).

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 интерфейсе 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.



Запомнить схему (Хотя бы примерно)

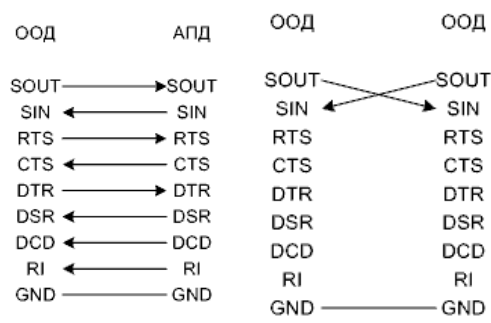
13. Цепи RS-232 и их использование

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.



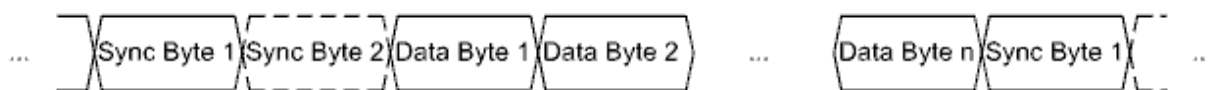
14. Асинхронный режим работы COM-порта

В асинхронном режиме синхронизируется обмен каждого информационного байта. По умолчанию линия находится в состоянии логической единицы, перед передачей линия выставляется в логический ноль (старт-бит), а после переходит в исходное состояние путем передачи стоп-бита (может быть один, полтора либо два). Скорость передачи меньше, чем в синхронном режиме. Ошибки отслеживаются приемником путем анализа бита четности.



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 – шестнадцатитрибитная константа, старшая и младшая часть которой хранятся в двух регистрах UART (DLL и DLM). 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

Запомнить как минимум за что какой регистр отвечает!

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.

Характеристика	RS-232	RS-422	RS-485
Способ передачи сигнала	Изменение потенциала относительно земли	Дифференциальная пара	Дифференциальная пара
Максимальное количество передатчиков	1	1	32
Максимальное количество приемников	1	10	32
Максимальная пропускная способность Мбит/с	1	10	10
Максимальное расстояние, м	15	1200	1200

19. Структура типового пакета компьютерной сети

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

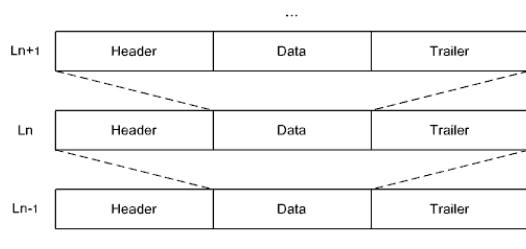
- Flag – флаг начала пакета.
- DA – адрес назначения.
- SA – адрес отправителя.
- Other fields – специфические поля определённой реализации.
- Data – полезная нагрузка.
- FCS (frame checksum) – контрольная сумма, проверяющая целостность пакета.

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. Например, пользователь посылает HTTP запрос на сервер, представляющий из себя HTTP заголовок и данные, после спуска по модели OSI до физического уровня, инкапсулированные данные для пересылки могут выглядеть так:

Ethernet заголовок | IPv4 заголовок | TCP заголовок | HTTP заголовок | пользовательские данные



Туннелирование – это вкладывание пакета одного протокола в пакеты другого протокола того же уровня

Фрагментация – разбиение данных на фрагменты, и передача цепочки пакетов. Применяется, если пакеты или данные некоторого уровня не помещаются в поле определённой длины в пакеты нижестоящего уровня.

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:

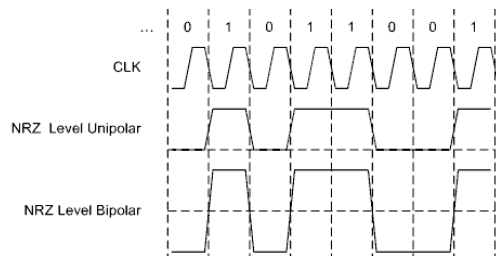
- NRZ (non-return zero) – коды без возврата к нулю
- RZ (return zero) – коды с возвратом к нулю
- Manchester code – манчестерские
- MLT (Multi-level transmit) – многоуровневые коды
- Block codes – блочные коды

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

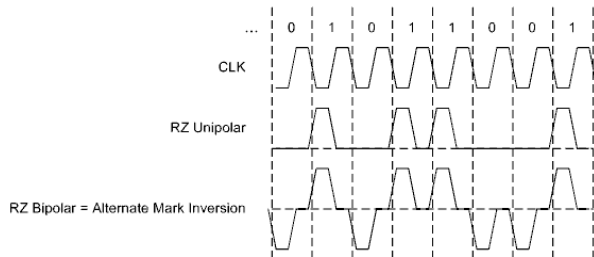
Пример:



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:



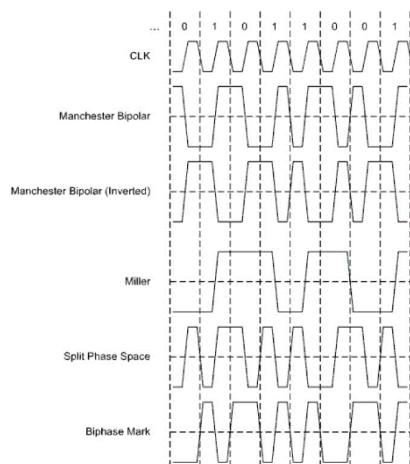
25. Манчестерские и многоуровневые линейные коды

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

выглядеть в манчестерском коде вот так вот: , 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:



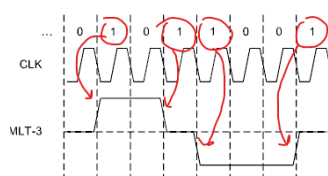
Миллер – смена уровня по единице.

Split phase space – смена уровня по нулю и каждый такт - переход

Biphase Mark – смена уровня по единице и такт единицы - переход

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 большие 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. Самыми популярными кодировками являются 4b/5b и 8b/10b применяемые в различных стандартах Ethernet: первый в Fast Ethernet, а второй в оптоволоконном Gigabit Ethernet.

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, $5 = 101 = x^2 * 1 + x * 0 + 1 * 1$, $7 = 111 = x^2 * 1 + x * 1 + 1 * 1$. $5 * 7 = (x^2 + 1) * (x^2 + x + 1) = x^4 + x^3 + x^2 + x + 1 = x^4 + x^3 + x + 1 = 11011 = 27$). $x^2 + x^2$ 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. После данной операции надо разделить полученное значение на неприводимый полином:

$$\begin{array}{r}
 + \quad x^4 + x^3 + x + 1 \\
 \quad x^4 + x^2 + x \\
 \hline
 + \quad x^3 + x^2 + 1 \\
 \quad x^3 + x + 1 \\
 \hline
 \quad x^2 + x
 \end{array}
 \quad \begin{array}{l}
 \left| \begin{array}{l} x^3 + x + 1 \\ x + 1 \end{array} \right. \\
 \hline
 \text{Остаток от} \\
 \text{деления}
 \end{array}$$

Складываем в делении потому что в бинарных полях Галуа сложение и вычитание является одной операцией xor.

В итоге результат – это наш остаток от деления

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 информационных битов на некоторое выбранное число. После приёма выполняется деление возможно искажённых битов на то же самое число и остатки сравниваются. Если остатки совпадают – то данные, скорее всего, переданы без ошибок.

Второй подход предполагает, что принятое слово делится на порождающий полином. Если ошибок не произошло, остаток будет равен нулю.

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 (Телевидение, Радио)
- Полудуплексном – передача может осуществляться в двух направлениях, но в один момент времени может передаваться лишь в одну сторону (Разговор по рации)
- Полнодуплексный – передача может осуществляться в обе стороны одновременно. (разговор по телефону)

На данный момент в КС доминируют полнодуплексные каналы.

Также последовательный канал может быть:

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

Причем канал, который не может разделяться несколькими станциями передатчиками одновременно, в отечественной литературе принято называть моноканалом.

Также есть:

- СПД с коммутацией пакетов – в структуру пакетов включают адреса источника и отправителя, и устройства-посредники определяют дальнейший путь на основе этого
- СПД с коммутацией каналов – сначала по запросу передатчика прокладывается путь к вызываемой станции, потом отправляется пакет

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, как пример – RAS
- 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 и кольца, к примеру, совпадают (коммутатор посередине, все остальные узлы связаны с ним). Также сегмент может иметь гибридную топологию.

Направленность каналов может «накладываться» на топологии. К примеру, кольцо может быть одно или двунаправленным. Можно написать примеры реализации (FDDI как двунаправленное кольцо)

33. Логические и физические топологии WAN и RAS.

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

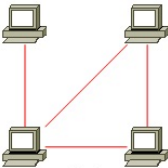
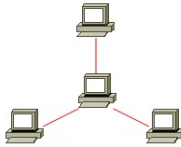
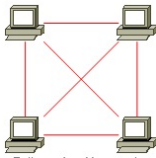
- Point-to-point – связывает только две станции, как пример – RAS
- Multi-access – связывает более двух станций (множественный доступ).

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 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 логическим 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).

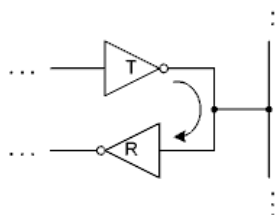
Во втором случае могут быть два подхода:

- 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 вход приёмника станции – одна цепь

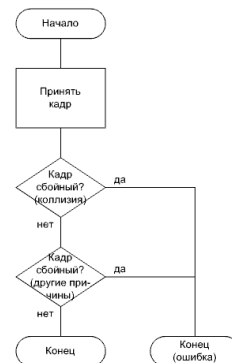


35. CSMA/CD (Ethernet)

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 ($T_{\text{rand}} = 2^k$, 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)

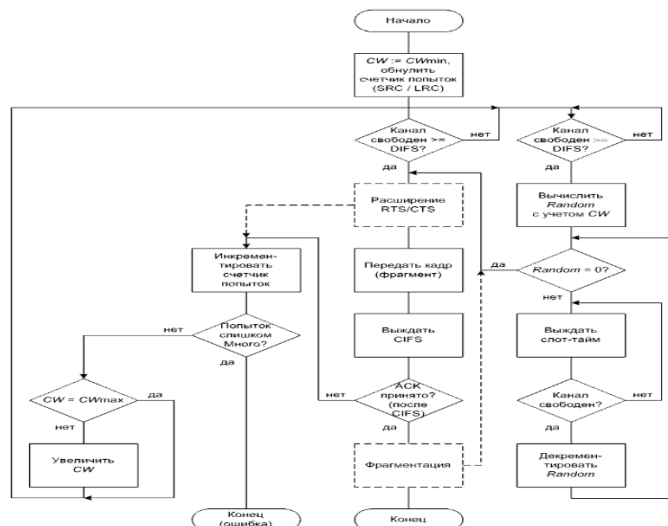
CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance) множественный доступ с прослушиванием несущей и избеганием коллизий.

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: $\text{CW}_{\min} = 15$, $\text{CW}_{\max} = 1023$.

В отличие от CSMA/CD после отправки кадра с сообщением, передающая сторона должна дождаться служебного кадра ACK. Если служебный кадр не пришел, то CW увеличивается, и станция начинает выжидать межкадровый интервал.

В CSMA/CA есть два времени для ожидания: межкадровый интервал и короткий межкадровый интервал. Станция, которая хочет переслать кадр, необходимо выждать межкадровый интервал, а станция, которая хочет переслать подтверждение (ACK), необходимо выждать короткий межкадровый интервал.

После выжидания обычного межкадрового интервала каждая станция, желающая отправить кадр, вычисляет RANDOM в соответствии с CW и начинает ждать. Станция перед отправкой кадра прождет минимум RANDOM слот-таймов, а если при этом линия будет занята, то число RANDOM уменьшаться не будет. В этом и проявляется collision avoidance в названии. 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).



Алгоритм

Можно упомянуть про проблемы скрытых и открытых станций.

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)

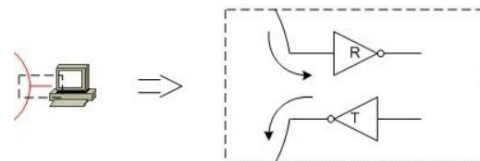
Поля пакета (только те, которые не следуют из их названия):

- 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)

Также существуют стековые станции, которые используются для манипуляций с приоритетом токена.

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 сбоев 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

Для того, чтобы станции-абоненты могли организовать взаимодействие, им необходимо некоторым образом выделять друг друга среди других станций. С целью идентификации станций им присваивают некоторые адреса. Таким образом, возникает адресация в СПД.

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:

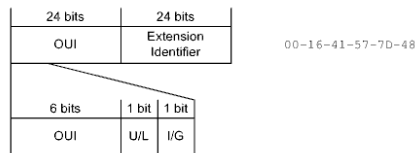
- Юникаст – пакет с таковым адресом назначения должен быть обработан одной конкретной станцией. WEB-страницы, HTTP-запросы
- Бродкаст – пакет должен быть обработан всеми станциями (ARP-запрос)
- Мультикаст – пакет должен быть обработан несколькими станциями из множества (IPTV)
- Эникаст – пакет должен быть обработан одной станцией из множества (наиболее сложная адресация) (Anycast DNS)

43. MAC-адреса

MAC-адрес – адрес канального уровня модели OSI, используется для уникальной идентификации сетевого оборудования. Уникальность MAC-адресов контролирует IEEE Registration Authority.

В стандартах IEEE определены три базовых формата MAC-адресов: MAC48, EUI-48 и EUI-64, где EUI (Extended Unique Identifier) -- расширенный уникальный идентификатор. MAC-48 можно считать синонимом EUI-48, хотя изначально это было более общее понятие.

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

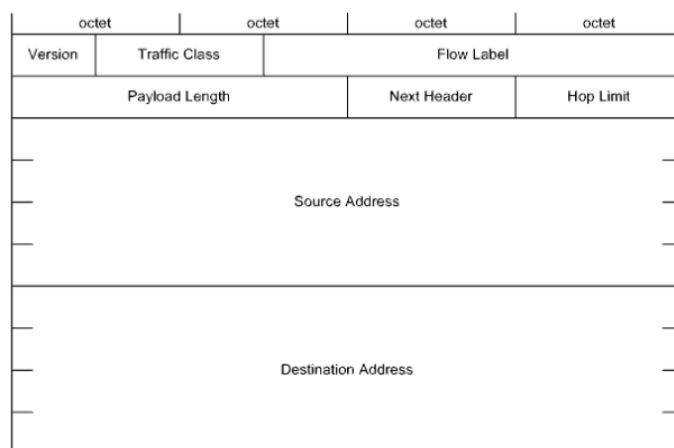
octet		octet		octet		octet	
Version	IHL	Type of Service		Total Length			
Identification				Flags	Fragment Offset		
Time to Live		Protocol		Header Checksum			
Source Address							
Destination Address							
Options						Padding	

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 – уникальный идентификатор пакета
- 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

Заголовок IPv6 гибкий: сколько заголовков нужно, столько и вставляется.



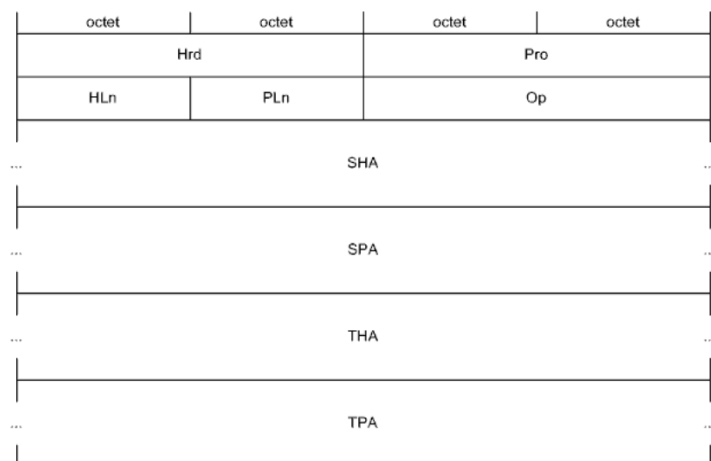
Поля:

- Version – версия (6) (4 бита)
- Traffic class – тип трафика (связан с QoS) (8 бит)
- Flow label – метка потока (связана с QoS) (20 бит)
- Payload length – длина полезной нагрузки в байтах (аналог Total length) (16 бит)
- Next header – селектор следующего заголовка (8 бит)
- Hop limit – ограничитель числа «прыжков» между станциями (аналог Time to Live) (8 бит)

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).



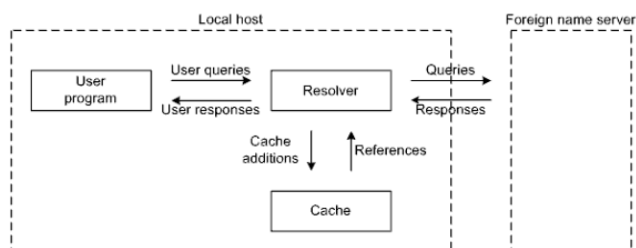
- Hrd (hardware) – тип оборудования (16 бит)
- Pro (protocol) – протокол (16 бит)
- HLn – Hardware address length (8 бит)
- PLn – protocol address length (8 бит)
- Op (Opcode) – код операции (1 – Request, 2 – Reply, и другие) (16 бит)
- SHA – sender hardware address (все адреса разделяются троеточиями т.к. переменной длины)
- 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	AD	CD	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
- 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)

49. Виртуальные соединения в сети передачи данных

Одним из ключевых терминов транспортного уровня является «соединение». Понятие соединения = понятие готовности. Если абоненты находятся в состоянии готовности, говорят, что они «соединены». Также следует выделять виртуальные соединения от физических. Виртуальные соединения – соединения между абонентами-программами.

Следует учитывать, что нормальная готовность может рассматриваться в двух ракурсах:

- Организация абонентов-программ
- Настройка задействованного промежуточного оборудования

В первом случае речь идёт о виртуальных цепях сетевого или канального уровней. Виртуальные цепи бывают:

- PVCs (Permanent virtual circuits) – выделенные виртуальные цепи
- SVCs (switched virtual circuits) – коммутируемые виртуальные цепи

Следует выделить, что термин «виртуальный канал» подходит, как и для виртуальных соединений, так и для виртуальных цепей.

Также стоит упомянуть способы организации взаимодействия, их всего два:

- Без гарантийной доставки – в СПД принимаются усилия для доставки сообщения, но ничего не гарантируется.
- С гарантийной доставкой – алгоритм работы транспортной службы гарантирует доставку пакетов. (запрос-подтверждение)

50. Классификация оконных механизмов, используемых в сети передачи данных

В случае, когда СПД загружена незначительно, алгоритм запросов-подтверждений становится слишком затратным на время, поэтому оптимизировать такой подход позволяет оконный режим, суть которого состоит в том, что до перехода к ожиданию квитанций передаётся не один, а несколько пакетов (окно).

Выделяют два основных критерия классификации оконных методов:

- Статический – неизменяемый размер окна, задающийся в протокол или устанавливающийся изначально на весь сеанс обмена (самое простое)
- Динамический – размер окна может меняться в процессе передачи сообщений (в зависимости от загрузки СПД, получения подтверждений и т.д. Сложнее)

Исходя из способа обработки очереди пакетов окно может быть:

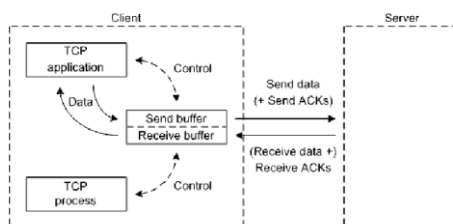
- Фиксированным – перед формированием нового окна, предыдущее должно быть полностью закрыто (простой вариант)
- Скользящим – существует возможность сдвигать окно относительно последовательности пакетов (сложный, но эффективный)

При реализации оконных методов стоит учитывать следующие обстоятельства:

- Нумерация пакетов должна присутствовать в том или ином виде
- Подтверждаться может как всё окно, так и каждый пакет
- Размером окна может управлять как передатчик, так и приёмник
- Размер окна управляется посредством служебных полей
- Окно, с которым работает передатчик может отличаться от окна, с которым работает приёмник

51. Структура системы TCP

TCP соответствует клиент-серверной модели. Сокет – это привязка к виртуальному каналу, соединяющему между собой два взаимодействующих сетевых процесса, с учётом всех уровней адресации.



Структура TCP-соединения

В TCP обязательно должно быть приложение, производящее и принимающее сетевые данные и специальный TCP-процесс, предоставляющий коммуникационные услуги (как драйвер ОС). Синхронизировать взаимодействие приложения и процесса можно лишь используя буфер. Приложение может читать и писать в буфер, в то время как процесс отслеживает наполнение и организует приём и передачу данных, используя ресурсы более низких уровней.

Предназначенное для передачи сообщение разбивается на сегменты, все байты сообщения последовательно нумеруются так называемыми последовательными номерами (SNs Sequence numbers). Нумерация начинается с начального последовательного номера (ISN – initial sequence number), который генерируется случайно. Принято, что ISN в нумерацию не включается, т.е. номер первого байта сообщения больше ISN на единицу! Номером сегмента является SN первого байта данных в нём. Длина сегмента должна иметь ограничение и контролироваться MSS (max segment size, по умолчанию 536 байт).

Передающее приложение «порциями» записывает части сообщения в буфер. Длина сообщения и длина буфера – вещи разные, и практически всегда различные. На другой стороне входящие сообщения записываются в буфер приёма в соответствии со своими номерами. Важно, чтобы размер окна не превышал размера входного буфера. Также важно, чтобы обмен сообщениями был с обеих сторон (как минимум MSG и ACK).

52. Заголовок TCP

octet				octet				octet				octet													
Source Port								Destination Port																	
Sequence Number																									
Acknowledgment Number																									
Data Offset		Reserved		NS		CWR		ECE		URG		ACK		PSH		RST		SYN		FIN		Window			
Checksum												Urgent Pointer													
Options												Padding													

Формат заголовка TCP

Поля:

- Source/Destination port – программный порт источника и назначения. (по 16 бит)
- Sequence number – номер сегмента (32 бита)
- ACK number – номер подтверждения (32 бита)

- Data offset – смещение данных (4 бита)
- Reserved – нули (3 бита)
 - NS (nonce sum) – флаг контрольной суммы для проверки кодов уведомлений о заторах
 - CWR (congestion window reduced) – флаг уменьшения окна затора при явном уведомлении
 - ECE (explicit congestion notification echo) – флаг подтверждения явного уведомления
 - URG (URGent pointer field significant) – флаг значимости указателя на экстренные данные
 - ACK – флаг подтверждающего номера
 - PSH (PuSH function) – флаг принудительной доставки данных (без записи в буфер)
 - RST (ReSeT connection) – флаг разрыва соединения (из-за сбоя на одной из сторон)
 - SYN (Synchronize sequence number) – флаг синхронизации последовательных номеров
 - FIN – флаг последних данных
- Window (W) – предлагаемое окно (16 бит)
- Checksum – контрольная сумма (16 бит)
- Urgent Pointer – указатель на экстренные данные (16 бит)
- Options – опционально (24 бита)
- Padding – наполнение (8 бит)

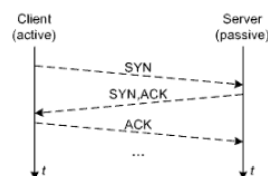
Функционирование базируется на использовании трёх полей в заголовке сегмента: SN, AN, W и трёх флагов SYN, ACK, FIN.

53. Протокол TCP

Протокол TCP – это большой, времязатратный протокол, что объясняется его механизмом подтверждения сообщений. Но взамен времени пользователь получает гарантию доставки сообщения. Т.е. мы будем отправлять сообщение, пока не достигнем до станции, и она не отправит нам ответное сообщение о приходе нашего.

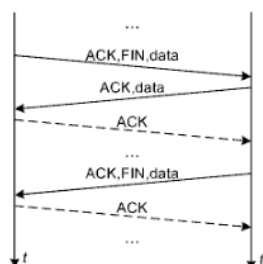
Протокол требует, чтобы перед отправкой сообщений станции были связаны (т.е. видели друг друга и установили виртуальное соединение).

Установление TCP-соединения выглядит как «тройное рукопожатие», основываясь на флагах SYN и ACK.



Функционирование протокола TCP базируется на использовании трёх полей в заголовке сегмента: SN, AN, W и флагов ACK, SYN, FIN.

После тройного рукопожатия станции начинают информационный обмен, который будет длиться, пока у обеих станций не закончатся сообщения.



Для закрытия соединения в своём направлении станция-отправитель отправляет сообщение FIN. Причём станция-получатель не обязана в этот же момент завершать обмен

Важно, что сервер должен отправлять клиенту сообщения с ACK по приходу любого сообщения или окна, в зависимости от реализации. Если же сообщение не дошло или пришло после таймаута – оно считается потерянным и отправляется заново.

54. Усовершенствования протокола TCP

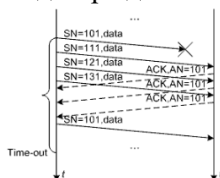
- TCP Cookie Transaction (TCPCT) – расширение для защиты серверов от атак типа «отказ в обслуживании»
- TCP Encrypt – расширение для кодировки на транспортном уровне. Предназначен для прозрачной работы.
- TCP Fast open – это расширение для ускорения открытия последовательных соединений TCP между двумя оконечными устройствами.

Также стала хорошо известна проблема, вошедшая под названием «синдром глупого окна» (SWS – silly window syndrome). Синдром возникает по разным причинам, и проявляется в том, что текущее окно передачи не соответствует состоянию приёмника, тем самым не позволяя его максимально «нагрузить» или наоборот «разгрузить» (например, в Telnet при нажатии клавиши отправляется 1 байт информации и 40-байтовый заголовок).

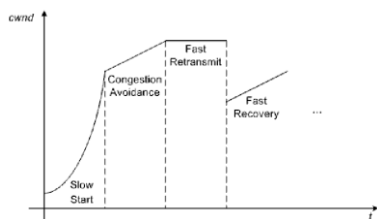
- Решение Нэгла: Объединение нескольких пакетов с небольшими сегментами данных в одно
- Решение Кларка: Запрещает принимающей стороне отправлять информацию о малом окне данных. Вместо этого отправитель ждёт, пока буфер не заполнится до большего размера.

Также существует четыре вида дополнений Ван Якобсона:

- Медленный старт – в начале передачи размер окна увеличивается не скачком, а плавно, пропорционально скорости получения подтверждений.
- Избегание затора – смысл в сдерживании экспоненциального роста размера текущего окна передачи после преодоления некоторого порога.
- Быстрая повторная передача – при получении разупорядоченного сегмента незамедлительный повтор подтверждения с AN недостающего сегмента с данными. При получении 3 таких подтверждений передатчик должен незамедлительно передать сегмент заново.



- Fast recovery – после обнаружения затора, переход сразу к избеганию коллизий, минуя стадию медленного старта



55. Протокол UDP и заголовок UDP

Данный протокол является протоколом транспортного уровня и реализует способ пересылки данных без гарантии доставки, часто называемый дейтаграммами (datagram)

octet	octet	octet	octet
Source Port		Destination Port	
Length		Checksum	

Поля:

Source Port -- программный порт источника.

Destination Port -- программный порт назначения.

Length -- длина дейтаграммы включая заголовок (в байтах).

Checksum -- контрольная сумма (псевдозаголовка, плюс заголовка, плюс данных).

Заголовок UDP. Все поля по 16 бит

При вкладывании UDP-дейтаграммы в IP-пакет, между UDP-заголовком и IP-заголовком вставляется дополнительный UDP-псевдозаголовок, в котором дублируются некоторые значения IP-заголовка.

56. Классификация и характеристики сред передачи данных

СрПД – это физическая среда, в которой передача данных происходит путём электрических сигналов. В настоящее время выделяют два типа соединения: кабельное и беспроводное. С точки зрения целевой области применения все кабели делят на:

- Кабели для внешней прокладки (outdoors) (на улице) – большое число проводов и высокая прочность
- Кабели для внутренней прокладки (indoor) (в помещении) – меньшие габариты и масса
- Оконечные кабели (cords) (для подключения рабочих мест) – простые и низкокачественные.

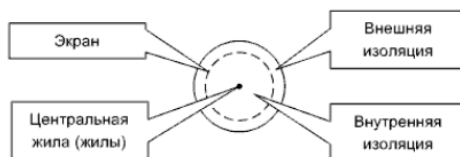
В простейшем случае кабель состоит из проводника и изоляции. Отдельно выделяют витые пары (twisted pair). Обычно в них свиты два провода, образующие дифференциальную пару.

Основные типы кабелей сейча это:

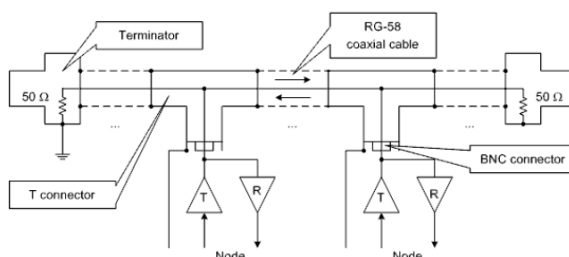
- Коаксиальный кабель – 185-200 м, 10 Мб/с
- Витая пара – 30-100 метров, 10-100 Мб/с
- Оптоволоконный кабель – 2 км, 10 Мб/с – 2 Гб/с

57. Среды передачи данных на основе коаксиальных кабелей

Широко используется в телевидении. Важное достоинство – передавать в один и тот же момент множество сигналов. Внутри выглядит следующим образом:



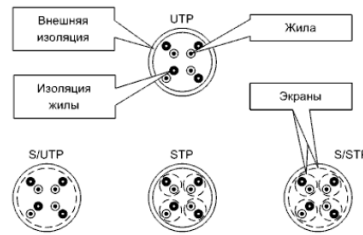
Для формирования системы на таком кабеле нужны как минимум BNC (bayonet-neill-concelman) коннекторы, T-соединители и пара терминаторов, один из которых заземляют.



Коаксиальный кабель, в отличие от витой пары, устойчив к электромагнитным помехам. И способен передавать сигналы на большие расстояния.

58. Среды передачи данных на основе витых пар

В сегментах КС широко используются четыре вида витых пар:

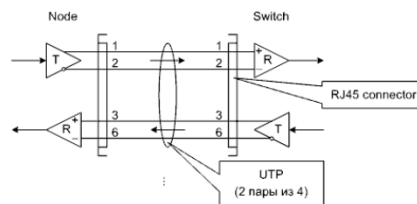


Где:

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

Сама витая пара состоит из 8 кабелей (бело-оранжевый, оранжевый, б-зелёный, синий, б-синий, зелёный, б-коричневый, коричневый), которые разводятся по стандарту 568-B под RJ-45, к примеру.

Обычно на витой паре доступны по два асинхронных канала передачи и приёма

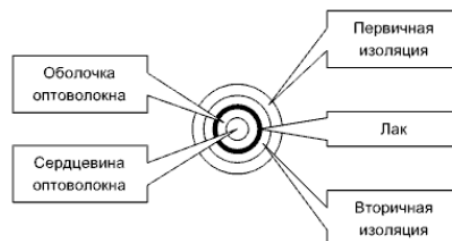


В типовых случаях витой парой соединяют разноранговое сетевое оборудование.

Цвета самих кабелей в витой паре не оговорены. Обычно привязаны к палитре RAL и имеют серый цвет. Другие цвета говорят о более высоком качестве.

59. Среды передачи данных на основе оптоволоконных кабелей

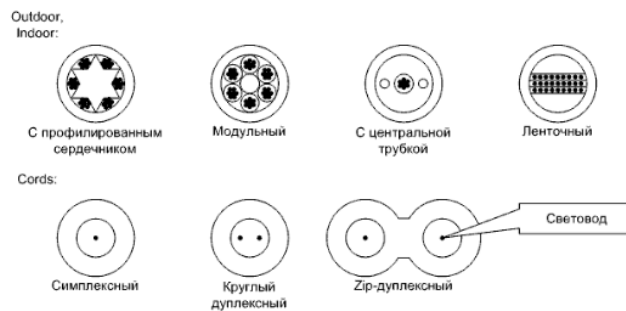
Рабочими компонентами оптоволоконных кабелей являются световоды изготовленные из оптоволокна, т.е. особого кварцевого стекла. Световод – это оптический волновод. Рабочий компонент – сердцевина.



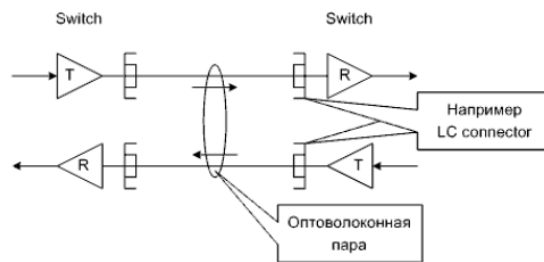
Большое количество изоляции обусловлено хрупкостью кабеля.

В стандартах также предусмотрены 8 видов светодиодов: OM1, OM2, OM3, OM4, OM5 – многомодовые, OS1, OS2, OS3 – одномодовые.

Также применяют множество видов оптоволоконных кабелей:



Типичная схема включения оптоволоконной пары:



Также оптоволоконные соединения делят на сплавные, механические (несъёмные) и контактные и линзовые (съёмные).

60. Физический уровень Ethernet

Физический уровень определяет электрические или оптические свойства физического соединения между устройством и сетью или между сетевыми устройствами. Он дополняется уровнем MAC и уровнем логических каналов.

Коаксиальный кабель	Витая пара	Оптоволокно
Ethernet 10 Mb/s		
10BASE-SE5	10BASE-T	10BASE-FL
10BASE-SE2		
Fast Ethernet (100 Mb/s)		
-	100BASE-TX	100BASE-FX
Gigabit Ethernet (1Gb/s)		
1000BASE-CX	1000BASE-T	1000BASE-SX 1000BASE-LX
Multigigabit		
-	2.5BASE-T 5BASE-T	-
Gigabit Ethernet (10Gb/s)		
10GBASE-CX4	10GBASE-T	10GBASE-SR 10GBASE-LR 10GBASE-ER

- 10BASE-SE5 – толстый коаксиальный кабель и внешние приёмопередатчики (SE2 – тонкий и внутренние приёмопередатчики)
- 10BASE-T – две телефонные витые пары
- 10BASE-FL – два многорежимных светода и источники излучения
- 100BASE-TX – две неэкранированные или экранированные витые пары
- 100BASE-FX – два многорежимных светода и источники излучения

- 1000BASE-T – четыре экранированные или неэкранированные витые пары категории 5
- 1000BASE-SX – два многорежимных светодиода и коротковолновые лазеры
- 1000BASE-LX – два одnoreжимных светодиода и длинноволновые лазеры
- 2.5BASE-T (5BASE-T) – четыре экранированные или неэкранированные витые пары категории 5е
- 10GBASE-T – четыре экранированные или неэкранированные витые пары категории 6 или 6А
- 10GBASE-SR/LR/ER – два многорежимных/одnoreжимных/одnoreжимных светодиода и коротковолновые/длинноволновые/экстрадлинноволновые лазеры.

Физический уровень Ethernet включает в себя:

- несколько интерфейсов физических сред
- несколько порядков величины
- скорости от 1 Мбит / с до 400 Гбит / с

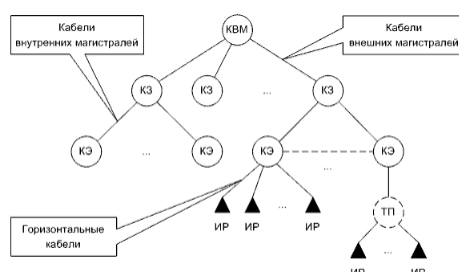
61. Структурированные кабельные системы и их модели

Структурированная кабельная система – это упорядоченная по тем или иным критериям совокупность телекоммуникационных и силовых кабелей, различного оборудования, а также соответствующих специализированных помещений. Основой для построения СКС служит древовидная топология, узлами которой служит сетевое оборудование определённого типа. Помещения в СКС бывают:

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

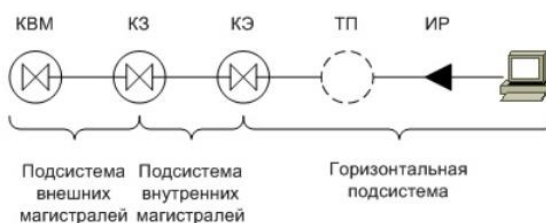
СКС включает в себя три подсистемы:

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

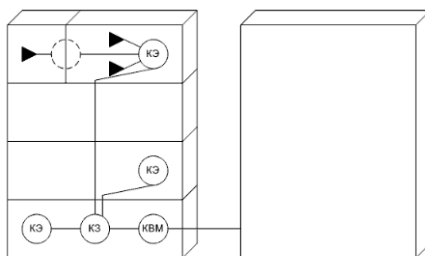


Основная модель СКС

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



Горизонтальная модель СКС



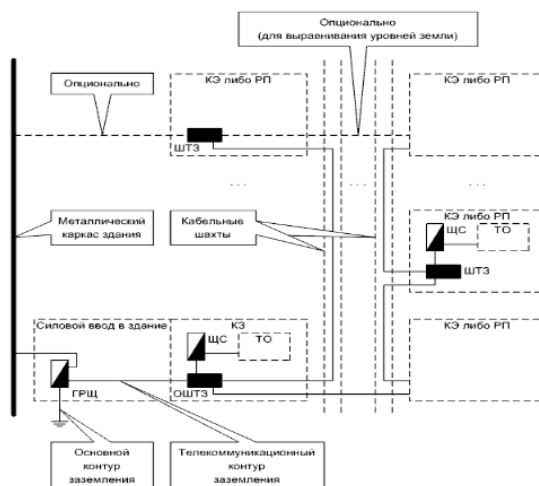
Функциональная модель СКС здания

62. Питание и заземление в структурированных кабельных системах

В СКС должно быть уделено внимание заземлению и питанию по следующим причинам:

- Предотвращение поражения людей электрическим током
- Защита кабельных трактов и сетевого оборудования от выхода из строя/помех
- Обеспечения возможности прохождения сигналов применительно некоторым видам сетевого оборудования.

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



Модель заземления

- 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.

Рекомендации стандартов по заземлению экранов кабелей:

- В аппаратных и кроссовых экраны должны заземляться по возможности на телекоммуникационный контур
- Экраны вертикальной подсистемы должны заземляться с обоих концов
- Экраны горизонтальной подсистемы достаточно заземлять с одного конца

63. Пожарная безопасность структурированных кабельных систем

Т.к. СКС охватывают здание полностью, серьёзное внимание должно быть уделено пожарной безопасности.

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

- Plenum – сюда относят кабели, которые можно располагать как угодно (при притоке воздуха, достаточного для поддержания горения, так называемая plenum-область)
- Riser – кабели, которые можно прокладывать в кабельных шахтах
- General purpose – кабели, которые можно прокладывать везде, кроме plenum-областей.
- Residential – кабели, на прокладку которых нанесены определённые ограничения (например, только для жилых помещений)

В состав маркировки кабелей обычно вводят дополнительные обозначения материала оболочек:

- PVC (PolyVinyl Chloride) – ПВХ
- PE (PolyEthylene) – полиэтилен
- PA (PolyAmide) – полиамид (нейлон)
- FR (Flame Retardant) – огнестойкий
- LS (Low Smoke) – низкое выделение дыма при горении
- NC (None Corrosive) – не подвержен коррозии
- UVR (Ultra Violet Resistant) – не подвержен влиянию ультрафиолетового излучения
- HF (Halogen Free) – не содержит галогенов

64. Технология PoE

Относительно недавно производители сетевого оборудования стали разрабатывать технологии, позволяющие запитывать относительно маломощные Ethernet-устройства через информационные кабели (например, через витую пару) – технологии под названием PoE (Power over Ethernet).

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

В структуру PoE входят ряд блоков:

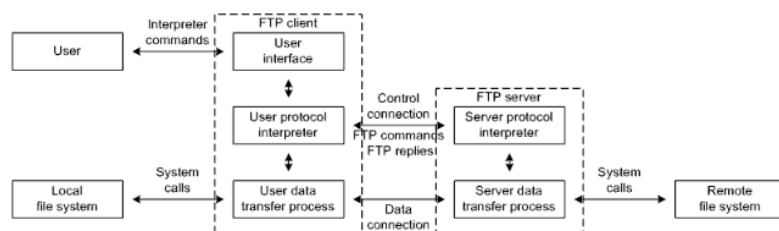
- PSE (Power Sourcing Equipment) – вводит питающее напряжение в кабель
- PD (Powered Device) – питается от этого напряжения

PSE может располагаться как на одном конце, так и на обоих. Либо может «вклиниваться» в кабель, т.е. быть PoE-injector-ом

Обычно используется для небольших PD.

65. Структура системы FTP

FTP-клиент обслуживает запросы пользователя и работает на локальной, по отношению к нему, станции. FTP-сервер работает на удалённой станции и обслуживает запросы FTP-клиента.



Структура FTP-системы

Как в составе сервера, так и в составе клиента выделяют протокольные интерпретаторы и процессы пересылки данных.

FTP-сервер представляет собой непрерывно выполняющуюся программу, ожидающую запросы от FTP-клиентов, выраженную в виде демона UNIX или сервиса Windows.

В отличие от многих протоколов FTP использует не одно, а два соединения, значит для него зарезервированы два программных порта: 20 – FTP Data (информационное соединение), 21 – FTP (управляющее соединение).

66. Протокол FTP и режимы обмена по протоколу FTP

FTP относят к протоколам прикладного уровня, ориентированным на пользователя. Это значит, что реализация FTP должна предоставить пользователю функционально полный интерфейс.

Взаимодействие по протоколу FTP базируется на модели запрос-ответ с применением тайм-аутов.

FTP-команда представляет из себя последовательность из 3-4 букв (режим не учитывается), за которыми могут следовать аргументы, разделяемые пробелом <SP>. Команда завершается символами возврата каретки и перевода строки <CRLF>.

Некоторые команды протокола FTP:

- USER <username> - имя пользователя
- PASS <password> - пароль, должна следовать после USER
- CWD <pathname> - сменить рабочий каталог удаленной ФС
- CDUP – перейти к родительскому каталогу
- QUIT – выход из удаленной системы
- PORT <host-port> - Совокупность IP-адреса и номера порта, необходимая для создания data connection (<h1>,<h2>,<h3>,<h4>,<p1>,<p2>)
- PASV – установить пассивный режим обмена
- TYPE <typecode> - файловое представление
- RETR <pathname> - загрузить файл с FTP-сервера (download)
- STOR <pathname> - загрузить файл на FTP-сервер (upload) (если файл с таким названием уже есть, то перезаписать)
- APPE <pathname> - загрузить файл на FTP-сервер с (upload) (если файл с таким названием уже есть, то данные дописываются в конец)
- DELE <pathname> - удалить файл или каталог на FTP-сервере
- RMD <pathname> - удалить каталог на FTP-сервере
- MKD <pathname> - создать каталог на FTP-сервере
- PWD – вывести на экран рабочий каталог
- LIST [<pathname>] – вывести список файлов удаленного каталога

Каждый FTP-запрос должен сопровождаться как минимум одним FTP-ответом.

FTP-ответ кодируется так:

Хyz <SP> <text> <CRLF>

Где хyz – целочисленный трехбайтный код

Коды предназначены для техники, а текст для людей.

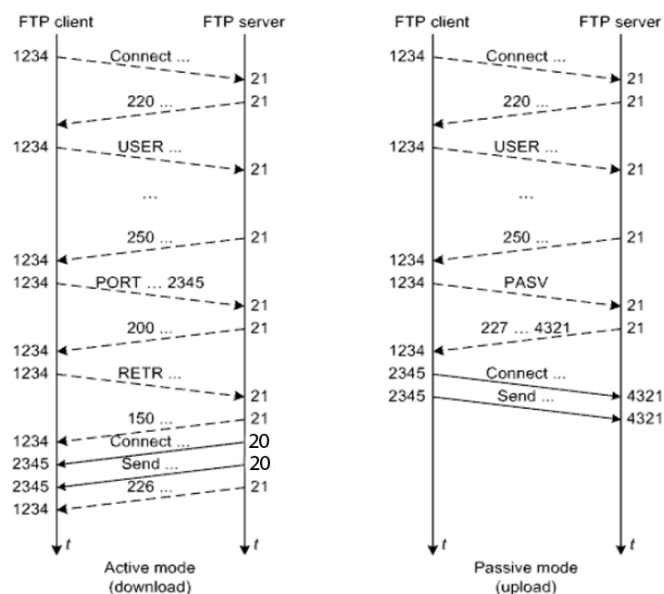
Х – идентифицирует статус завершения

Y – подробности

В зависимости от того, какая сторона является инициатором установления информационного соединения различают активный и пассивный режимы обмена. Активный режим более предпочтителен.

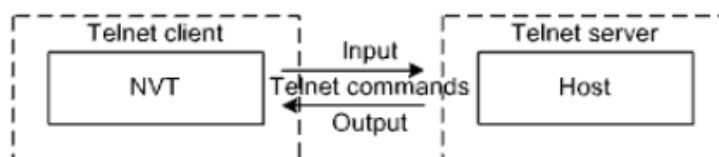
Отличие активного и пассивного режимов заключается в том, как создается информационное соединение: в активном режиме это происходит через команду PORT <p> от клиента к серверу, где <p> - динамически выделенный порт клиента, <p> <-> 20; в пассивном режиме клиент отправляет команду

PASV, ответом на которую является динамически выделенный порт сервера <p2>, после чего выделяется динамический порт клиента <p1> и происходит создание связи <p1> <-> <p2>.



67. Структура и особенности системы Telnet

Telnet базируется на клиент-серверной модели и использует протокол TCP. Задействуется 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. Используется буферизация, в том числе для того чтобы не нагружать СПД. По умолчанию набранные символы отсылаются моментально. В режиме linemode – при нажатии Enter.

Главный недостаток – полная незащищённость соединения от несанкционированного доступа. Данные и текст пересылается в виде открытого текста (в том числе пароли, номера телефонов и т.д.). На смену telnet пришёл SSH (secure shell). В нём идея абсолютно та же, но соединение защищено.

68. Электронные письма и почтовые ящики

Сообщениями протоколов электронной почты являются электронные письма. По аналогии с бумажным письмом, электронное письмо так же состоит из конверта (envelope) и содержимого (content). Содержимое, в свою очередь, состоит из заголовка и основного текста. Изначально в отношении всех компонентов электронного письма допускались только 7-мибитная кодировка US-ASCII.

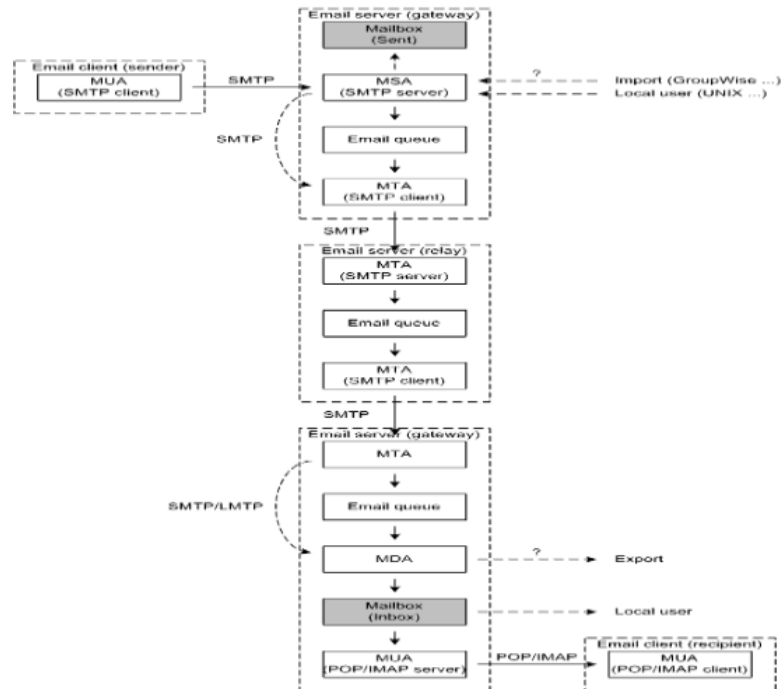
Значимое расширение электронной почты – MIME (Multipurpose Internet Mail Extension), позволяющее включать в основной текст сообщения различные мультимедийные данные, такие как text, video, audio, image, application, multipart (несколько типов).

Одно из ключевых понятий электронной почты является понятие почтового ящика (mailbox). Почтовые ящики могут быть выделены как на отдельных серверах, так и на пользовательских станциях.

При рассмотрении любой почтовой системы прежде всего выделяют следующие процессы:

- MTAs (mail transport agents) – доставляют письма между почтовыми серверами.

- MDAs (mail delivery agents) – помещают доставленные сообщения в ящики пользователей
- MUAs (mail user agents) – реализуют интерфейс пользователей с их почтовыми ящиками.
- MSAs (mail submission agents) – позволяют вводить письма разными способами

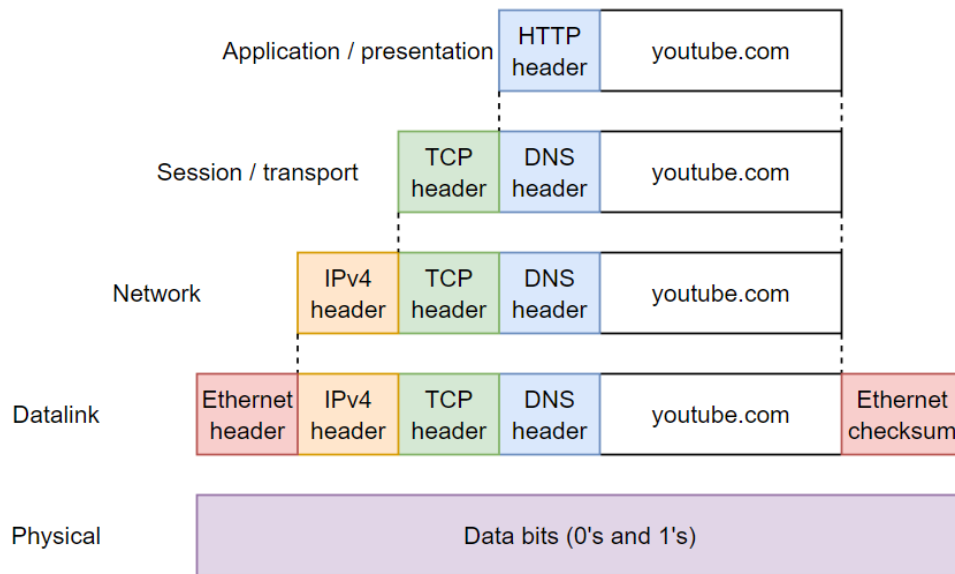


Обобщённая структура SMTP

Практика:

1. Инкапсуляция, туннелирование, фрагментация

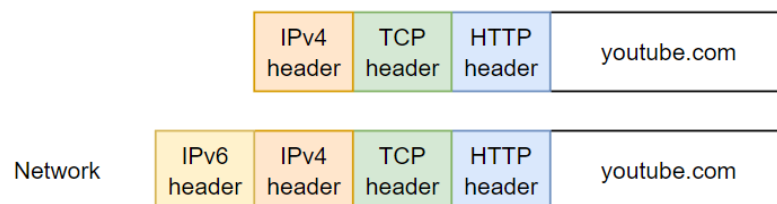
Пример: заходим на сайт YouTube.com:



Инкапсуляция

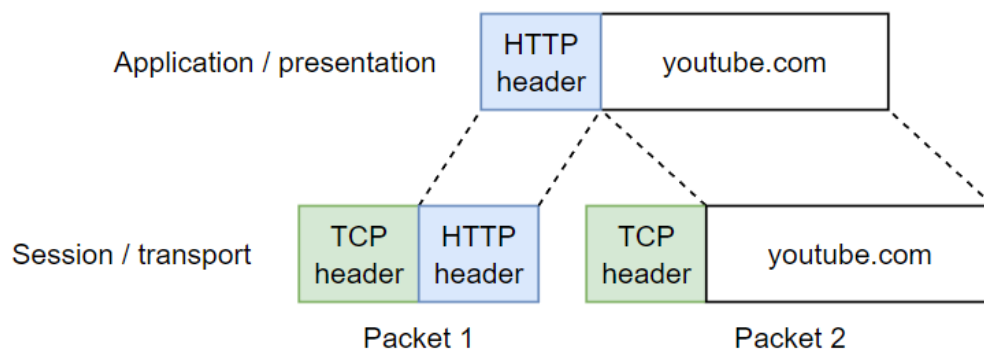
Т.е. мы вкладываем наше название в сообщения с более высоких уровней на более низкий.

Туннелирование:



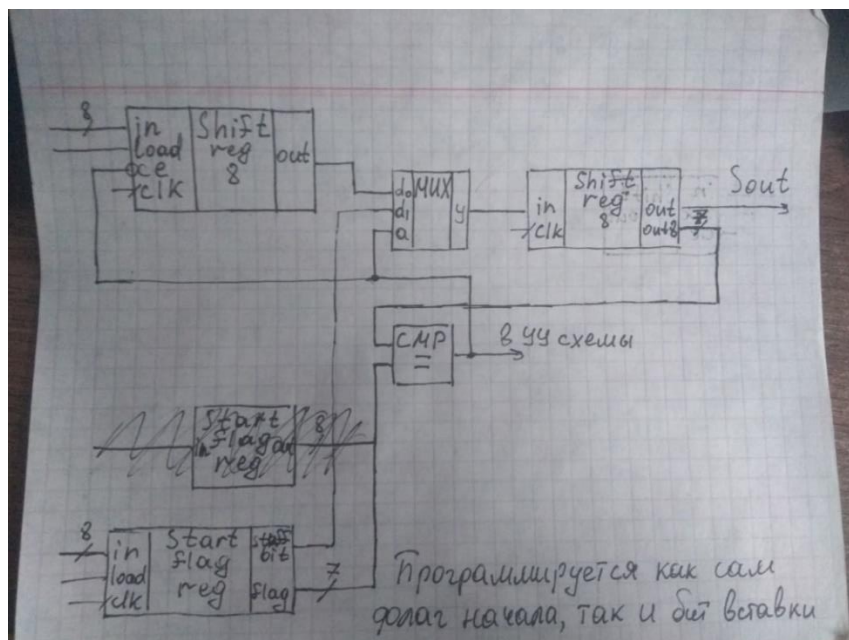
Просто вкладываем пакеты на одном уровне в ещё один пакет того же уровня

Фрагментация:



Разбиваем пакет на две части, если он не умещается в одну. Дефрагментация – обратный процесс. Собираем пакет из частей.

2. Алгоритмы и схемы бит- байт- стаффинга



Thanks Dmitriy Derugo

3. Линейные коды (кодирование)

24 вопрос. Примеры

4. Помехоустойчивые коды (расчёты)

Кодовое расстояние рассчитывается как минимально кол-во единиц в сумме всех чисел по модулю два.

Например, для кода:

$C = \{0000, 1001\}$ кодовое расстояние равно $1001 \oplus 0000 = 1001$, 2 единицы, т.е. кодовое расстояние = 2

$C = \{0001, 1011, 1000, 0111\}$ кодовое расстояние равно $d_c = \min p (b_x \oplus b_y) = \min (0001 \oplus 1011 = 1010, 0001 \oplus 1000 = 1001, 0001 \oplus 0111 = 0110, 1011 \oplus 1000 = 0011, 1011 \oplus 0111 = 1100, 1000 \oplus 0111 = 1111)$

Минимально – 2 единицы, т.е. кодовое расстояние = 2

Код обнаруживает не более $d_c - 1$ ошибок. Т.е. код с кодовым расстоянием $d_c = 3$ может обнаружить не более 2 ошибок

Код может исправить не более $E'(d_c - 1) / 2$ ошибок. Т.е. код с кодовым расстоянием 3 может исправить не более $3 - 1 / 2 = 1$ ошибки.

5. Код Хэмминга и циклический код (расчеты)

ХЭММИНГ:

Получающиеся коды (расчеты):

$$C = \{0110, 1011, 1111, 0001\};$$

$$d_c = \min_{\substack{1 \leq i \leq n \\ b_i \neq b_j, j \in C, b_i \neq b_j}} (b_i, b_j) = \min(1, 2, 3, \dots) = 1$$

$$k - \text{ко сепар.} : d_c \cdot d_c - 1 = 0$$

$$k - \text{ко исп.} : \frac{d_c}{2} = 0$$

Код Хэмминга и CRC:

8 9 10 4 12 13 14 15 16

Берут двучисл. код и делают контрольные биты.

Каждый контрольный бит: $k = \lceil \log_2 (\sum_{i=1}^m (m+1) \cdot i^{\lceil \log_2 (m+1) \rceil}) \rceil$, где m - кол-во

битов в сообщении (т.е. k где $m = 8$ равно: $\lceil \log_2 (8+1 \cdot \lceil \log_2 (8+1) \rceil) \rceil$

$$= \lceil \log_2 (8+1 \cdot 3) \rceil = \lceil \log_2 (12) \rceil = 4$$

$$\begin{array}{cccccccc} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ \times & \times & 0 & \times & 0 & 0 & \times & 0 & 0 & 0 & 0 \end{array}$$

Далее считаем каждый бит в битах, проверяющих битах (где 0 бита это 0, 1, 5, 5, 7...; где 1 это 12, 5, 6, 3, 10...). Первая проверка выполняется те разряды, номера которых в двоичном коде имеют в младшем разряде единицу (1х, 1х1, ...). Таковыми являются: 1, 3, 5, 7, 9...

Вторая проверка выполняется те разряды, номера которых в двоичном коде имеют во втором разряде единицу (1х, 1х1, 1х1х, ...). Таковыми являются: 2, 3, 6, 7.

Самая проверка выполняется как сумма по модулю 2 или же "⊕" для контрольных битов (изначально все контрольные биты = 0). Т.е. в коде 011011 биты будут начислены на позиции: 1х0х110х110 и бит 1 будет равен: 0⊕1⊕0⊕1=0

контрольные

биты:

$$0 \oplus 1 \oplus 0 \oplus 1 \oplus 0 = 0$$

Обратная проверка Хэмминга осуществляется повторным кодированием сообщения и сверкой контрольных битов. Например: 0110 - исходное сообщ. → в код Хэмминга: 1х10х110 = 1100110 - переданное сообщение;

1110 - полученное сообщение

1х1х110 - заново кодируем

0010110 - биты 1 и 2 не совпадают, значит

ошибка в 1+2 = 3 бите.

CRC

CRC НА ДРУГОЙ СТРАНИЦЕ

CRC

1) Следует (для упрощения) разбить сообщение в полиномиальную форму:

$$10110 = x + x \cdot 0 + x + x + x = x + x + x \quad \text{или} \quad 1101 = x^3 + x^2 + x^0 = x^3 + x^2 + 1$$

2) Определим значение минимального расстояния по формуле $d_{\min} = r + b + 1$, где r - кол-во обнаруживаемых ошибок; b - кол-во исправляемых ошибок. Доётся излагать по условию. Например, кол-во обнаруж. : 2, кол-во исправ. : 1;

~~$d_{\min} = 2 + 1 + 1 = 4$.~~ Например: нужно тогда код обнаружит двойные ошибки и обнаружит и исправит одиночные:

$$d_{\min} = 2 + 1 = 3 - \text{по первому условию}$$

$$d_{\min} = 1 + 1 + 1 = 3 - \text{по второму условию}$$

3) Выбираем циклический код с $k = d_{\min}$. Определим число контрол. разрядов:

$$(\text{предположим, для шифра 1101}): K = E \lceil \log_2(4 + 1 + E \lceil \log_2(5) \rceil) \rceil = E \lceil \log_2(8) \rceil = 3$$

Выбираем полином 3 степени, например, 11: $x^3 + x + 1 = 1011$.

Продолжение на другой странице

4) Умножаем сообщение на x^n , где n - степень полинома:

$$(x^3 + x^2 + 1) \cdot x^3 = x^6 + x^5 + x^3 = 1101000, \text{ Можно просто сдвинуть влево на степень полинома.}$$

5) Делим результат (4) пункта на необратимый полином (в нашем случае на 4):

$$11 = 1011$$

$$\begin{array}{r|l} 01101000 & 1011 \\ \underline{1011} & \\ 01100 & \\ \underline{1011} & \\ 01110 & \\ \underline{1011} & \\ 01010 & \\ \underline{1011} & \\ 0001 & \end{array}$$

↓
0001 - Полученный остаток укажем на единицу, чтобы добавить в выходные биты.

6) Складываем результат (4) пункта и полученный остаток:

$$F(x) = 1101000 + 001 = 1101001$$

7) На стороне приёма делим полученное сообщение на этот же полином:

$$\begin{array}{r|l} 1101001 & 1011 \\ \underline{1011} & \\ 01100 & \\ \underline{1011} & \\ 01110 & \\ \underline{1011} & \\ 01011 & \\ \underline{1011} & \\ 0000 & \end{array}$$

Т.к. остаток нулевой - ошибки не произошло.

8) Пример: если произошла ошибка - подсчитываем вес остатка (число единиц в нём)

Пример:

$$\begin{array}{r|l} 1101010 & 11011 \\ \underline{1011} & 1 \\ 01100 & \\ \underline{1011} & \\ 01100 & \\ \underline{1011} & \\ 01111 & \\ \underline{1011} & \\ 0100 & \end{array}$$

- вес = 1

а) Если вес равен или меньше ~~числа~~ числа исправляемых ошибок - то принимаем

код складываем по модулю 2 с остатком: $1101101 \oplus 100 = 1101001$ - прав. сообщ.

Продолжение на другой странице

б) Если все больше знаков ошибок - сдвигаем полученное сообщение влево, добавляя в свободные места "0" циклически. ~~И~~ сдвигаем сообщение влево.

Пример:

$$\begin{array}{r|l}
 1001001 & 1011 \\
 1011 & 1 \\
 \hline
 0010000 & \\
 1011 & \\
 \hline
 00(111) &
 \end{array}$$

Больше 1;

$1001001 \rightarrow 0010011$ в результате деления получили 101, но 101 не подходит, ~~и~~ сдвигаем еще на разряд: $0010011 \rightarrow 0100110$

$$\begin{array}{r|l}
 \oplus 0100110 & 1011 \\
 1011 & 1 \\
 \hline
 001010 & \\
 1011 & \\
 \hline
 0001 &
 \end{array}$$

Теперь суммируем по модулю 2: $\oplus \begin{array}{r} 0100110 \\ 001 \\ \hline 0100111 \end{array}$

и сдвигаем обратно на 2 разряда влево (циклически). Получаем:

1101001

Это и есть искомое сообщение.

6. Поля Галуа (математические операции)