Вопросы

1. **Понятие компьютерной сети**
2. **Классификация компьютерных сетей**
3. **Стандарты КС**
4. **Наиболее распространенные модели КС**
5. **Физический уровень модели OSI**
6. **Канальный уровень модели OSI**
7. **Сетевой уровень модели OSI**
8. **Транспортный и сеансовый уровни модели OSI**
9. **Прикла дной уровень и уровень представления модели OSI**
10. **Семейство протоколов TCP/IP**
11. **Эволюция COM-портов и их место в современном ПК**
12. **Структура COM-портов ПК**
13. **Цепи RS-232 и их использование**
14. **Асинхронный режим работы COM-порта**
15. **Синхронный режим работы COM-порта**
16. **Тактирование COM-порта**
17. **Архитектура COM-портов ПК**
18. **Стандарты, близкие к RS-232**
19. **Структура типового пакета компьютерной сети**
20. **Инкапсуляция и ее проявления в компьютерных сетях**
21. **Бит-стаффинг**
22. **Байт-стаффинг**
23. **Особенности линейного кодирования и классификация линейных кодов, применяемых в КС**
24. **Линейные коды без возврата к нулю и с возвратом к нулю**
25. **Манчестерские и многоуровневые коды**
26. **Блочные линейные коды**
27. **Поля Галуа и их применение в компьютерных сетях**
28. **Модель помехоустойчивого канала связи и теорема Шеннона**
29. **Линейные помехоустойчивые коды, включая коды Хэмминга и циклические коды**
30. **Классификация помехоустойчивых кодов**

1. Понятие компьютерной сети

Компьютерная сеть (КС) – это совокупность различных технических средств (то есть самих компьютеров и другого оборудования), предназначенная для передачи компьютерной информации (то есть файлов и сообщений) на относительно большие расстояния (то есть за пределы компьютеров).

В основе любой КС лежит так *называемая сеть передачи данных* (СПД) – Data Communication Network (dcn), которая может задействовать различные *среды передачи данных* (СрПД).

Иногда в составе СПД выделяют базовую (опорную) СПД.

Все устройства в составе СПД можно разделить на две четко разделяющиеся группы:

1. Оконечные (end devices) – находятся по периметру СПД (компьютер, планшет, принтер)
2. Посредники (intermediary devices) – составляют ядро СПД. (маршрутизатор, коммутатор)

Весь трафик в СПД традиционно разделяют на три базовых типа:

1. Обычные компьютерные данные (data)
2. Голос (voice)
3. Видео (video)

2. Классификация компьютерных сетей

С одной стороны, выделяют:

1. Local Area Networks (LANs) – локальные КС (ЛКС), выделяют прежде всего территориально, охватывают территорию не более кампуса, но при этом подразумевает определённые технологии.

2. Wide Area Networks (WANs) – глобальные КС (ГКС), выделяют прежде всего технологически и, в общем случае, может охватывать произвольную территорию.

3. Metropolian Area Networks (MANs) – городские КС (русской нет), промежуточный вариант между LAN и WAN, по всему городу, тв, передача новостей

4. Personal Area Networks (PANs) – личные КС, позволяет подключить к компу периферийные устройства .

5. Remote Access Services (RASes) – КС для подключения удалённых пользователей (teleworkers), существует в контексте WAN/

6. Industrial Networks – промышленные КС, специализированный вариант LAN.

7. Datacenter Networks – КС центров обработки данных, специализированный LAN.

8. Home Networks - домашние КС, специализированный LAN.

С другой стороны:

1. Intranets – внутренние КС предприятий и организаций, обычно выделяют по ведомственной принадлежности пользователей.

2. Internets – КС публичного доступа

Кроме того, сети могут быть:

1. Изолированными – закрыты для прослушивания (isolated)

2. Открытыми для прослушивания (open)

С точки зрения организации взаимодействия КС могут быть:

1. Сильносвязанными – наличие хост-ЭВМ (host) (основной вычислительный компонент) с одной стороны и терминала (исключительно устройство для ввода и отображения информации, следовательно они без хоста бесполезны) с другой. Совокупность хоста и подключенных к нему терминалов принято называть рабочей станцией (workstation)

2. Слабосвязанными – наличие сервера (обслуживает запросы клиентов, пассивный элемент) с одной стороны и клиента (обслуживают запросы пользователей, активный элемент) с другой.

3. Стандарты КС

Все стандарты делят на:

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

Стандарты могут носить *предварительный* (preliminary) или *временный* (interim) характер. Могут включать *дополнения* (annexes) и *списки обнаруженных ошибок* (errata). Могут *устаревать или замещаться другими стандартами* (obsolete).

Практическим (или теоретическим) воплощением стандарта является так называемая реализация. Сертификация позволяет определить факт соответствия стандарту.

Множество стандартов IEEE 802.x. Сейчас наибольший интерес представляют:

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

Стандарты Ethernet по пропускной способности делят на три группы:

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

4. Наиболее распространённые модели КС

Модель OSI

(Open System Interconnection - открытая модель взаимодействия систем)

Из всех моделей КС является наиболее фундаментальной. Открытость системы позволяет третьим сторонам разрабатывать для этих систем различные аппаратные или программные средства расширения и модификации, а также создавать программно-аппаратные комплексы из продуктов разных производителей.

Модель включает семь уровней (физический, канальный, сетевой, транспортный, сеансовый, представления, прикладной)

Взаимодействие в рамках модели OSI может быть вертикальным (между уровнями) и горизонтальным (между одинаковыми моделями):

1. Интерфейс – это правила взаимодействия между пространственно совмещенными соседними уровнями модели OSI.

2. Протокол – правила взаимодействия между прастраснственно разнесенными одинаковыми уровнями модели OSI.

Модель TCP/IP

Связана с одноименным семейством протоколов. Включает три уровня:

1. Access – уровень доступа, предназначен для обеспечения подключения к КС оконечных пользователей. особое внимание предоставлению пользователям требующихся им ресурсов.

2. Distribution – уровень распределения предназначен для обеспечения взаимодействия в пределах групп пользователей. особое Внимание резервированию соединений.

3. Core – уровень ядра предназначен для обеспечения высокоскоростной связи между относительно удаленными группами пользователей. особое внимание характеристикам трафика

На всех уровнях значительное место отведено разграничению трафика с целями защиты пользователей друг от друга и защиты КС от пользователей. При этом всем, технологии могут быть различными.

5. Физический уровень модели OSI

На физическом уровне формализуют подключение того, либо иного сетевого устройства к СрПД. Соответственно в пространстве физ уровень охватывает точку подключения.

Фундаментальная задача физ уровня заключается в передаче сигнала.

Специфическими понятиями физ уровня является:

- среда
- разъем (физ порт)
- несущая (частота)
- модуляция
- сигнал

6. Канальный уровень OSI

На канальном уровне формализуют взаимодействие *станций* в пределах *сегмента*.

Станция (узел, англ. Node) - устройство, способное передавать и принимать сетевой трафик принято называть. (ПК, Сервер, маршрутизатор и т.д.)

Сегмент - множество станций, объединенных посредством одной СрПД, то есть видящих друг друга непосредственно.

Специфическими понятиями канального уровня являются:

- сегмент сети
- физ и лог топология сегмента
- пакет (кадр)
- бит- и байт-стаффинг
- адресация в пределах сегмента
- канальный код
- код проверки целостности пакета (кадра)
- алгоритм доступа к моноканалу

Канальный уровень разделяют на два подуровня:

1. MAC (Media Access Control) – контроль доступа к СрПД.

Выполняется взаимодействие с физ уровнем, то есть средозависимые операции, такие как формирование и распознавание пакетов, адресация, канальное кодирование и другие.

2. LLC (Logical Link Control) – контроль логического соединения.

Выполняется взаимодействие с сетевым уровнем, то есть средозависимые операции такие как разбиение данных на пакеты, сборка данных из пакетов, определение соответствующей подсистемы сетевого уровня и другие.

7. Сетевой уровень модели OSI

На сетевом уровне формализуют построение полноценной КС произвольного масштаба, охватывающей произвольное кол-во сегментов.

Сетевой уровень позволяет выйти за пределы сегмента.

Предназначается для определения пути передач данных.

Специфическими понятиями сетевого уровня являются:

- пакет
- адресация в пределах всей КС
- маршрутизация

8. Транспортный и сеансовый уровни модели OSI

На транспортном уровне формализуют использование программным обеспечением сетевого оборудования, то есть как отдельно взятым программам представляется «транспорт».

Транспортный уровень позволяет перейти от оборудования к программам.

Специфическими понятиями транспортного уровня:

- пакет (сегмент сообщения)
- программный порт
- логическое соединение
- надежность доставки
- алгоритм борьбы с заторами в СПД

Сеансовый уровень позволяет предоставлять всем программам доступ к транспорту в многозадачном окружении в промежутках длительного времени (сессии).

Специфические понятия сеансового уровня:

- сессия
- программный порт
- алгоритм мультиплексирования программ

В практических реализациях сеансовый уровень выражен слабо и обычно совмещается с транспортным.

9. Прикладной уровень и уровень представления OSI.

Уровень представления позволяет адаптировать прикладную информацию в форму, приемлемую для передачи по КС, то есть является прослойкой между программами и транспортом.

Основными задачами уровня представления являются:

-кодирование информации (включая возможное сжатие) с целью обеспечения ее правильной интерпретации в последующем

- шифрование информации с целью обеспечения ее защиты при пересылке по открытым для прослушивания сетям

Прикладной уровень призван решать конкретные пользовательские задачи с помощью КС.

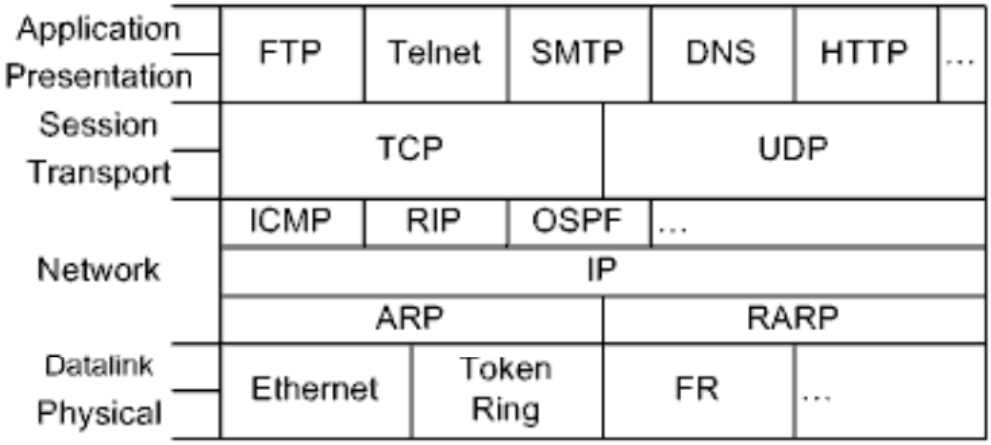
Примерами прикладных задач могут служить :

- пересылка файлов между компьютерами
- пересылка электронных писем
- поддержка удаленных текстовых и графических терминалов, в том числе для администрирования
- пересылка мультимедийных документов
- обмен мгновенными сообщениями
- совместная разработка чего-либо
- пересылки голоса и видео (не свойственно традиционным КС)

Часто эти уровни (представления и прикладной) в реализации совмещаются.

10. Семейство протоколов TCP/IP

Семейство протоколов tcp/ip описано в стандартах RFC (Request for comments).



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

В развитии COM-портов можно выделить следующие основные этапы:

В свое время (семидесятые годы 20 века) компания Intel разработала два контроллера последовательного порта (UART (8250) и USART(8251)).

Далее в течение длительного времени происходило усовершенствование UART и USART. Следует выделить UART 16550, которая на долгое время стала стандартной. В ней повысилась пропускная способность, появилась возможность буферизации (две очереди по 16 байт на стороне приемника и на стороне передатчика).

В дальнейшем интеграционные процессы привели к появлению мультикарт. (на чипе Multi I/O). Позже уже была характерна интеграция чипа Multi I/O на материнскую плату.

Во времена Pentium сформировалась действительная до сих пор структура ПК. В этой структуре появилася и чип Multi I/O только ввиду модификаций и улучшений он стал называться Super I/O.

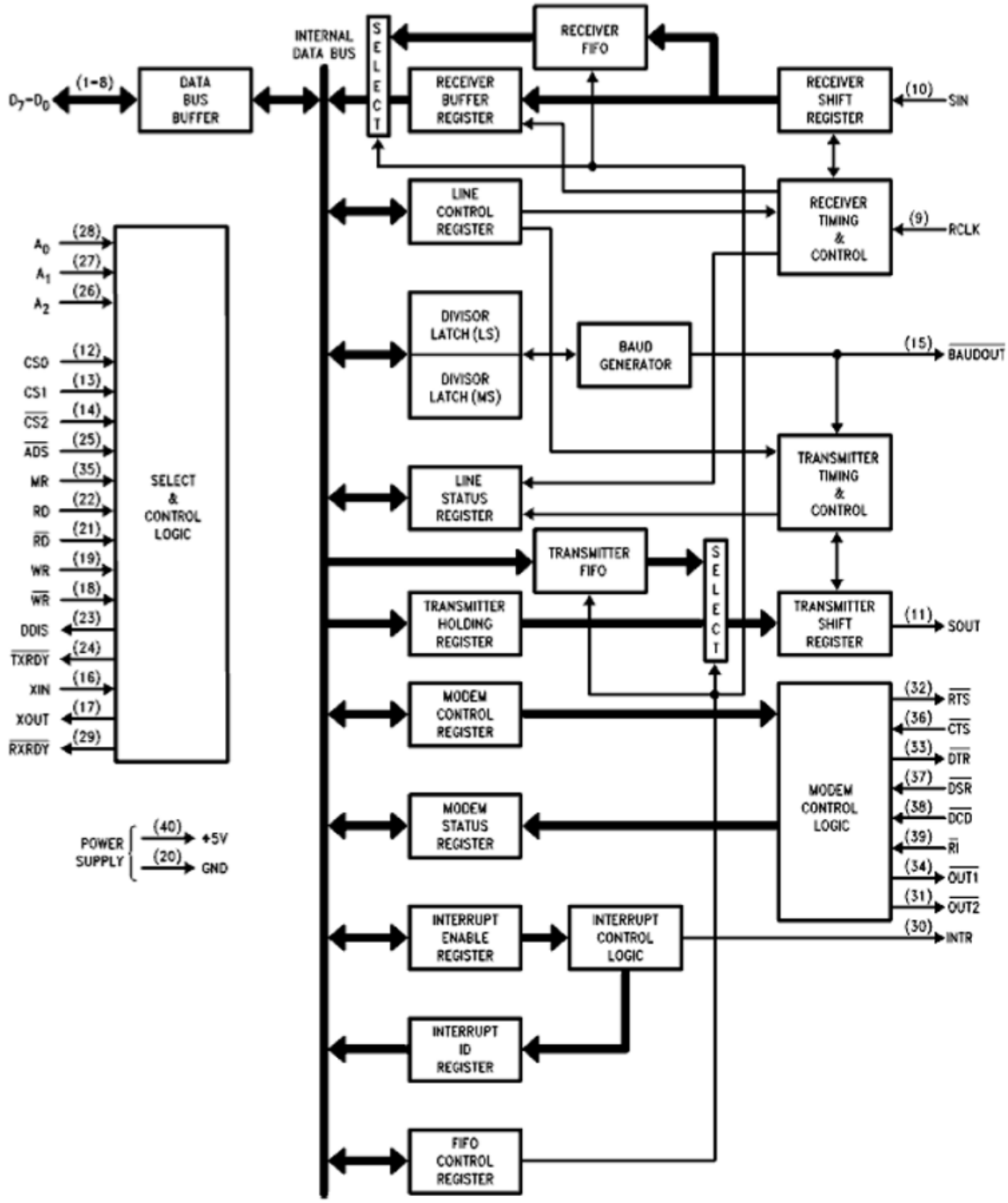
В настоящее время (приблизительно с 2005 года) традиционный последовательный интерфейс ПК считают устаревшим (legacy), часто исключают из состава интегрированной периферии - на материнских платах можно увидеть все реже.

Однако возобновлено производство мультикарт - новые версии представляют собой платы расширения с интерфейсом PCI.

Сейчас в качестве основного интерфейса подключения периферийных устройств к ПК рассматривается USB.

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.



13. Цепи RS-232 и их использование

- SOUT (Serial Output) – выход передатчика
- SIN (Serial Input) – вход приемника
- RTS (Request to Send) – сигнал-запрос от UART к модему о передаче байта
- CTS (Clear to Send) – сигнал подтверждение от модема к UART о готовности принять байт для передачи
- DSR (Data set ready) – сигнал от модема к UART о готовности к взамодействию
- DTR (Data Terminal Ready) – сигнал от UART к модему о готовности к взаимодействию
- DCD (Data Carrier Detect) – сигнал от модема к UART об обнаружении данных
- RI (Ring Indicator) – сигнал от модема к UART об обнаружении входящего телефонного звонка
- GND – ground (уровень земли или нуля)

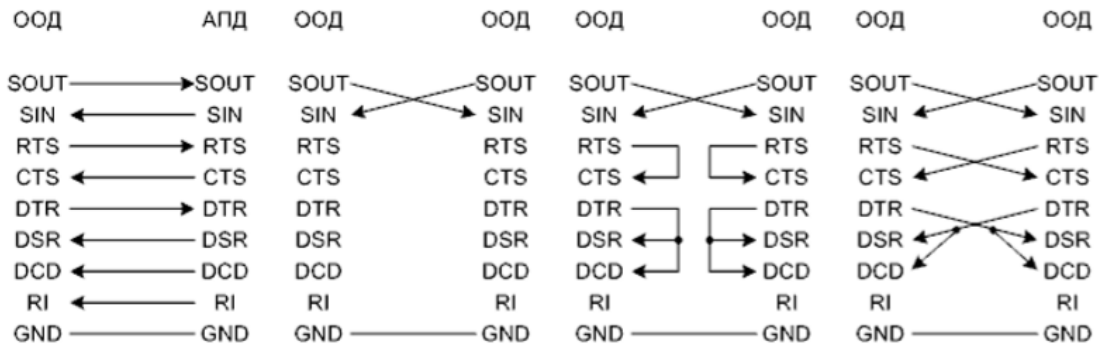
Служебные цепи RS-232 позволяют организовывать контроль информационного потока. Например, это позволяет избегать переполнения приемника, приостанавливая “быстрый” передатчик.

Два основных метода контроля передачи:

1. RTS/CTS – полуаппаратный
2. XON/XOFF – программный (приемник передает в обратном направлении спец байт XON (11h) для инициирования передачи и спец байт XOFF (13h) для остановки передачи)

В стандартной ситуации, ООД взаимодействуют между собой посредством АПД, причем с помощью так называемых “рукопожатий” с АПД. При этом подключение АПД к ООД осуществляют посредством “прямого” кабеля.

Для подключения двух ООД друг к другу непосредственно необходим один из вариантов нуль модемного (предполагает отсутствие модема) кросс-кабеля (поскольку цепи SIN и SOUT скрещивают).


ООД
АПД
SOUT
SIN
RTS
CTS
DTR
DSR
DCD
RI
GND
ООД
ООД
ООД
ООД
ООД
ООД

14. Асинхронный режим работы COM-порта

В асинхронном режиме синхронизируется обмен каждого информационного байта (5-8 бит).

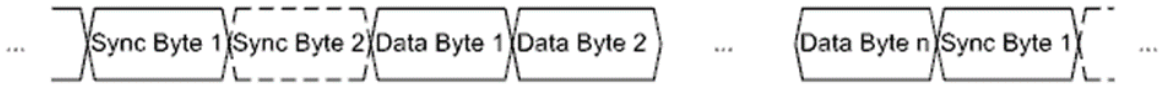
По умолчанию линия находится в состоянии логической единицы. При наличии байта для передачи передатчик переводит линию в состояние логического нуля, то есть передает старт-бит, что говорит приемнику о том, что на следующем такте нужно «ловить» первый информационный бита. Далее идет передача информационных битов. Для проверки целостности информационной части, если эта проверка включена, за информационной частью вставляется бит паритета. При этом действует правило дополнения. Например, если включена проверка единиц на четность (even), то бит паритета формируется таким образом, чтобы общее число единиц (в информационной части плюс бит паритета) было четным. Либо, если включена проверка нулей на нечетность (odd), то общее количество нулей должно быть нечетным Стоп-бит необходим для того, чтобы после передачи информационной последовательности гарантированно вернуть линию в исходное, то есть единичное состояние. Старт-бит всегда один, а стоп-битов может быть один, полтора либо два.

Скорость передачи меньше, чем в синхронном режиме.

Ошибки отслеживаются приемником.

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.



Простыми словами, когда ничего не передается, то просто передаются Sync байты.

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

Ошибки отслеживаются приемником.

16. Тактирование COM-порта

Так как по сути приемник и передатчик COM-порта – 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 – это программируемый делитель частоты, с помощью которого осуществляется тактирование порта.

$F_{out} = F_{in} / (16 * DL)$

- DL – шестнадцатибитная константа, старшая и младшая часть которой хранятся в двух регистрах UART (DLL и DLM)
- F_{in} – входная частота
- F_{out} – выходная частота

Частота тактирования измеряется в бодах (бит/с).

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).

Регистры UART:

1. THR (Transmit Holding Register) – регистр данных передатчика (точнее буферный регистр сдвигового регистра передатчика)

2. RBR (Receiver Buffer Register) – регистр данных приемника (точнее буферный регистр сдвигового регистра приемника).

3. DLL (Divisor Latch Least significant byte) – младшая часть константы деления бод-генератора.

4. DLM (Divisor Latch Most significant byte) – старшая часть константы деления бод-генератора.

5. IER (Interrupt Enable Register) – регистр разрешения прерываний.

6. IIR (Interrupt Identification Register) – регистр идентификации прерываний.

7. FCR (FIFO Control Register) – регистр управления очередями FIFO передатчика и приемника.

8. LCR (Line Control Register) – регистр управления линией.

9. MCR (Modem Control Register) – регистр управления модемом.

10. LSR (Line Status Register) – регистр состояния линии.

11. MSR (Modem Status Register) – регистр состояния модема.

12. SCR (Scratch Pad Register) – дополнительный регистр для временного хранения данных, не связанный с функционированием UART

18. Стандарты, близкие к RS-232

С точки зрения топологии, интерфейс RS-232 обладает одним существенным ограничением, которое закономерно вытекает из его природы. Он изначально задумывался как интерфейс между разноранговыми устройствами, то есть, по сути дела, как интерфейс для подключения периферийных устройств к компьютеру. Более двух устройств с помощью RS232 объединить невозможно.

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
Направление передачи	Одностороннее, двустороннее	Одностороннее, двустороннее	Одностороннее, двустороннее
Максимальное количество передатчиков	1	1	32
Максимальное количество приемников	1	10	32
Ориентировочная максимальная пропускная способность	1 Mbit/s	10 Mbit/s	10 Mbit/s
Ориентировочное максимальное расстояние	15 m	1200 m	1200 m

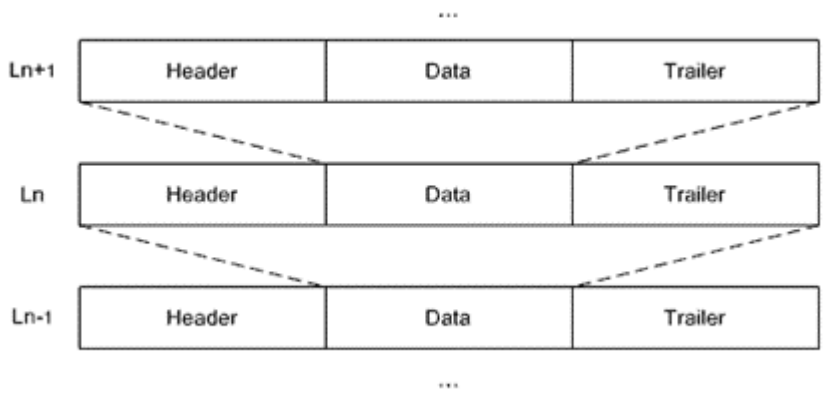
19. Структура типового пакета в компьютерных сетях

- 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

20. Инкапсуляция и ее проявления в компьютерных сетях

При продвижении информации между уровнями возникает необходимость в преобразованиях структур данных. Преобразования выражаются в *инкапсуляции* и *декапсуляции*.

Инкапсуляция – вкладывание пакета определенного вышестоящего уровня в поле данных пакета смежного нижестоящего уровня в процессе подготовки к передаче, то есть при продвижении сверху вниз.



Инкапсуляция имеет еще ряд проявлений. Если при выполнении инкапсуляции данные некоторого уровня не помещаются в поле отведенной длины, то можно прибегнуть к *фрагментации* (fragmentation) – разбить данные на фрагменты и передать цепочку пакетов. Принимающая сторона будет вынуждена выполнить *дефрагментацию* (defragmentation).

21. Бит-стаффинг

Бит-стаффинг – в бит ориентированных системах модификация следующей за флагом цифровой последовательности (добавлением перед передачей и стиранием после приема битов), которая решает проблему распознавания флага начала пакета.

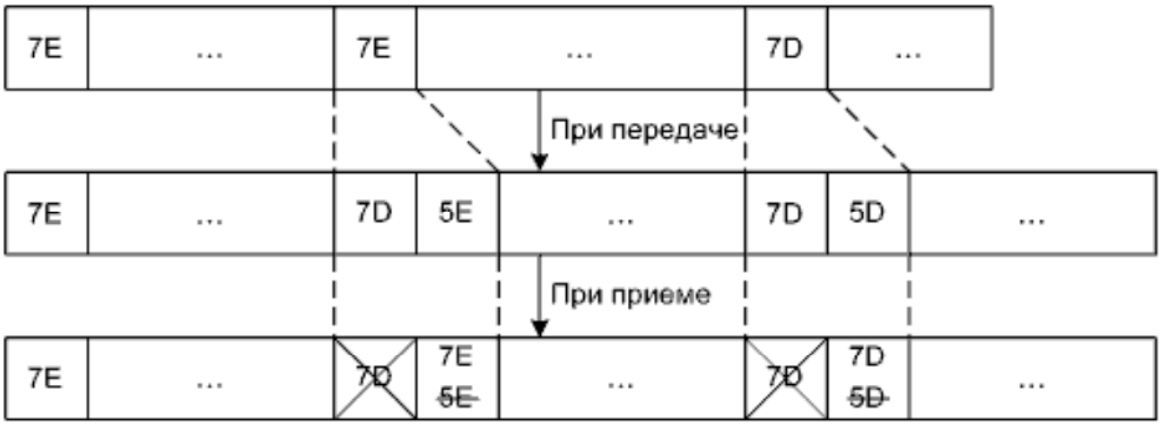
Проблема заключается в том, что последовательность, соответствующая флагу, может встретиться и после флага начала пакета. Следовательно, нужно обеспечить уникальность флаговой последовательности в пакете.

Применение бит-стаффинга приводит к увеличению длины пакета. Теоретически, с целью уменьшения связанных с бит-стаффингом «издержек», следует стремиться к минимизации количества вставок: разбивающий бит нужно вставлять после наиболее длинной уникальной подпоследовательности в флаговой последовательности.

Классическим флагом является 7Eh (01111110b). На передающей стороне после нуля и шести единиц всегда вставляется седьмая единица, а на принимающей стороне единица после нуля и шести единиц всегда удаляется.

22. Байт-стаффинг

Байт-стаффинг – в байт ориентированных системах модификация следующей за флагом цифровой последовательности (заменой байтов), которая решает проблему распознавания флага начала пакета.



Производятся следующие замены в последовательности после флага:

- Флаг = ESC-символ + Код замены флага
- Совпадения с ESC-символом = ESC-символ + Код замены ESC

В данной ситуации:

- флаг = 7E
- ESC-символ = 7D
- Код замены флага = 5E
- Код замены ESC = 5D

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.

Все линейные коды применяются для 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 способо в кодирования:

- NRZ (non-return–to-zero) – коды без возврата к нулю
- RZ (return-to-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

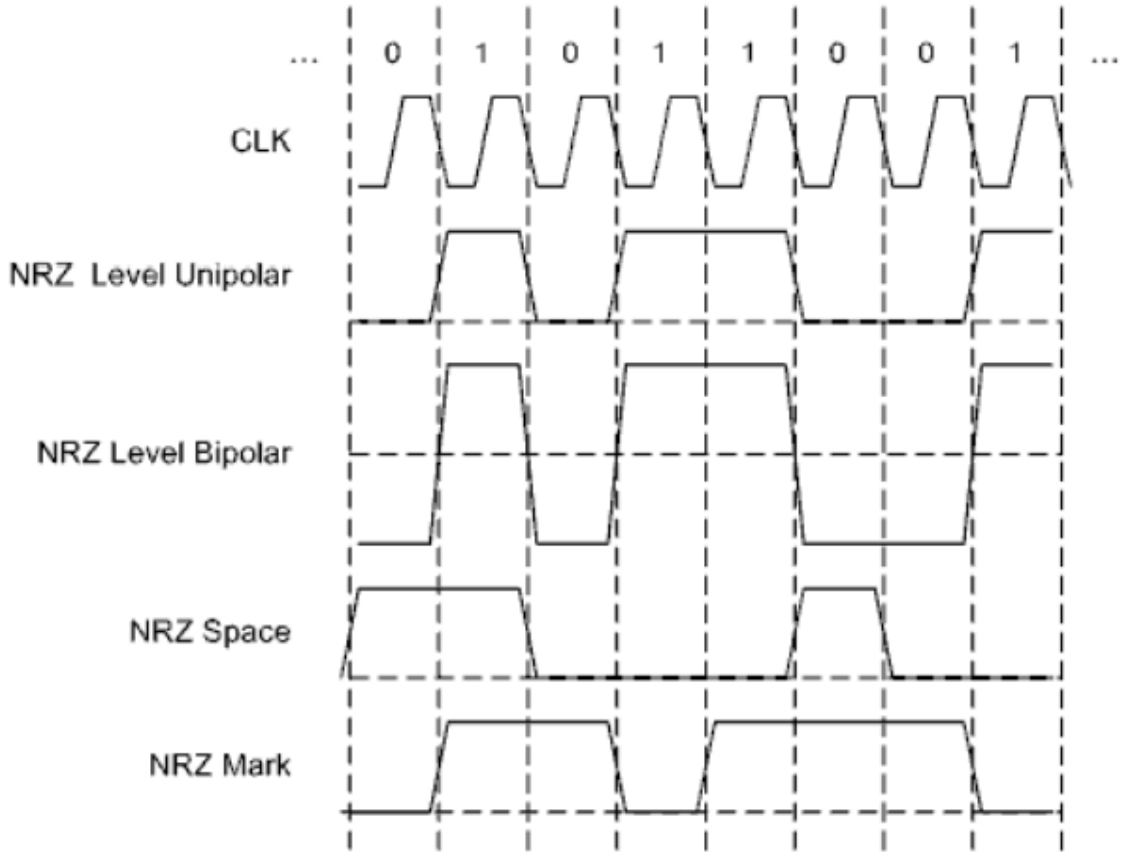
Применение: RS-232, USB, HDLC.

Изменение уровней между тактами.

Варианты NRZ-кодов:

- *Space*: 0 входной последовательности кодируется сменой текущего уровня, а 1 – сохранение текущего уровня.
- Mark: 1 входной последовательности кодируется сменой текущего уровня, а 0 – сохранение текущего уровня

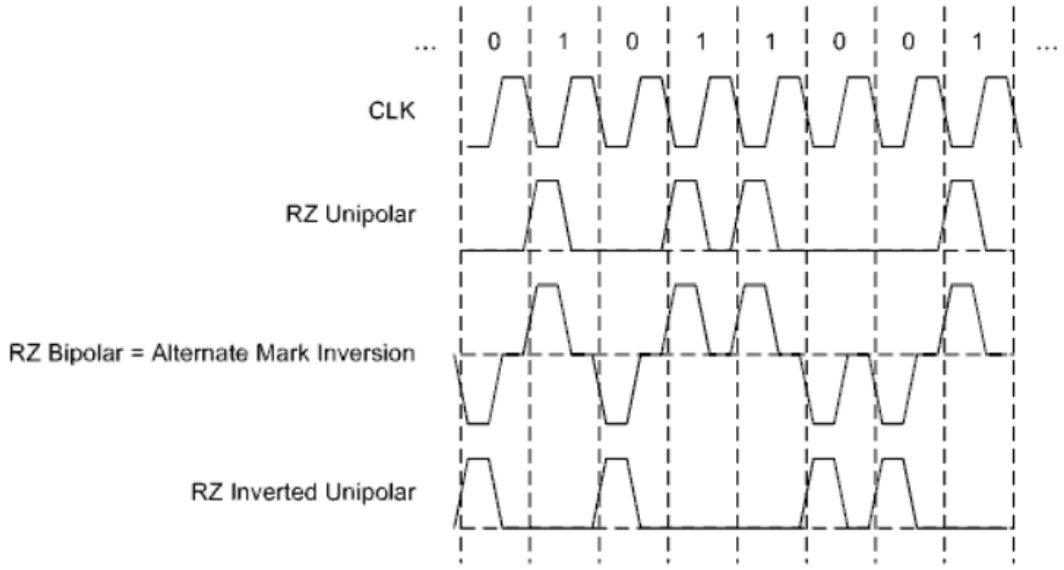
Могут быть однополярными и двуполярными.



RZ-коды

Применение: IrDA

Так же выражаются в изменении уровней между тактами, но на половине каждого такта всегда происходит возврат к нулю (земле). Двухполярные RZ-коды обладают свойством самосинхронизации.

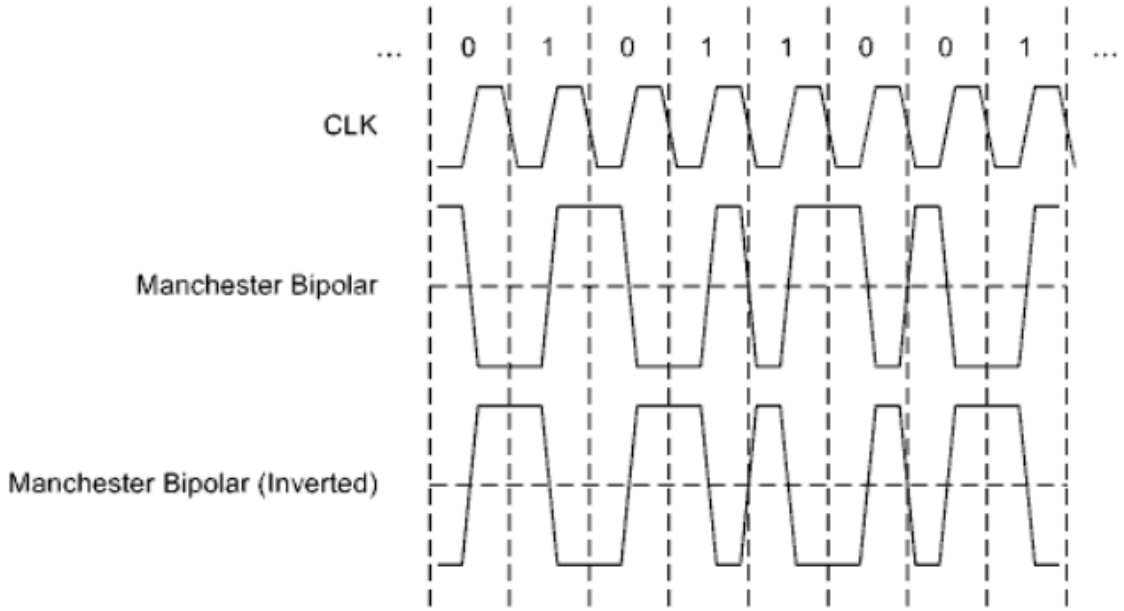

...
0
1
0
1
1
0
0
1
...
CLK
RZ Unipolar
RZ Bipolar = Alternate Mark Inversion
RZ Inverted Unipolar

25. Манчестерские и многоуровневые линейные коды

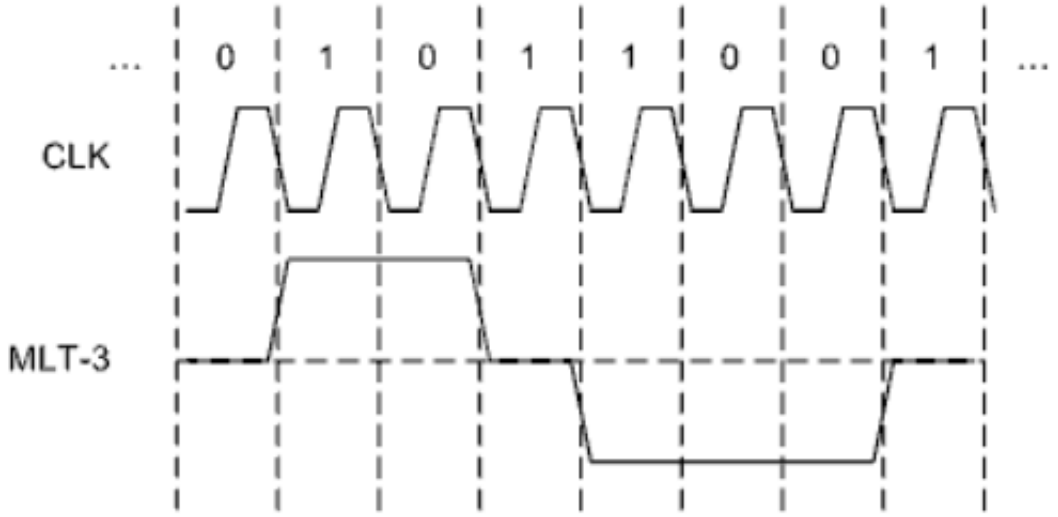
Манчестерские коды выражаются в переходах между уровнями во время тактов, поэтому их иногда называют фазовыми кодами.

Применение: Ethernet, Token Ring

Есть два «равноправных» варианта собственно манчестерского кода. Ноль во входной последовательности заменяется на переход от единицы к нулю, а единица заменяется на переход от нуля к единице. Либо наоборот. Манчестерские коды обладают свойствk’ /ом самосинхронизации.



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


...
0
1
0
1
1
0
0
1
...
CLK
MLT-3

26. Блочные линейные коды

Блочные коды выражаются в замене блоков битов из входной последовательности на большие (как правило) по размеру блоки битов в выходной последовательности. Блочные коды могут комбинироваться с другими линейными кодами. В связи с избыточностью блочных кодов, во многих из них предусмотрены контрольные последовательности, которые, по сути, являются управляющими символами. Первым примером может служить код 4b/5b, применяемый в Fast Ethernet и CDDI.

Таблица замены блоков битов кода 4b/5b

4b	5b
0000	11110
0001	01001
0010	10100
0011	10101
0100	01010
0101	01011
0110	01110
0111	01111
1000	10010
1001	10011
1010	10110
1011	10111
1100	11010
1101	11011
1110	11100
1111	11101

Более сложным примером может служить код 8b/10b, применяемый в оптических вариантах Gigabit Ethernet.

Биты входного блока обозначают как ABCDEFGH - от младшего к старшему, выходного abcdefghij - так же от младшего к старшему.

Входной блок разбивается на два подблока: x из пяти битов и y из трех битов. Поэтому выходной код представляет собой конкатенацию двух кодов: 5b/6b и 3b/4b.

Кроме собственного блока данных D, имеются контрольные блоки K, которые кодируются альтернативно.

В код 8b/10b заложена гибкая система уравнивания количества нулей и количества единиц.

27. Поля Галуа и их применение в компьютерных сетях

В помехоустойчивом кодировании все операции выполняются по, так называемой, арифметике Галуа.

Данная арифметика заключается в том, что результатом любой арифметической операции над элементами поля будет являться элемент из данного поля. Поля задаются целым числом.

Поля Галуа скалярного представления:

Поле $GF(p)$ из целых чисел 0, 1 ... p - 1, порожденное в результате отображения f: $\mathbf{Z}/p$ -> $GF(p)$, где $\mathbf{Z}/p$ -- факторкольцо множества целых чисел, в котором роль идеала играет простое число p, и $f([a]) = a$, называют *полем Галуа* (Galois field) порядка p.

При вычислениях с элементами поля Галуа используют целочисленную арифметику с приведением по соответствующему модулю.

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 = 3.0

Поля Галуа векторного представления:

Для практического применения полей Галуа в компьютерных системах необходимо перейти от скалярного представления к векторному.

Расширенное поле Галуа $GF(p^n)$ можно рассматривать как векторное пространство, где простое число p является характеристикой поля и соответствует количеству состояний разряда вектора, а n является степенью поля над его простым подполем и соответствует количеству разрядов вектора.

Поскольку в обычных компьютерных системах разряды регистров бинарные, то наибольший интерес представляют поля $GF(2^n)$.

Сложение бинарных векторов (совпадает с вычитанием) проблему не представляет и соответствует поразрядной операции хог.

Для операции произведения:

Для обеспечения конечности поля Галуа, полученный в результате произведения полином нужно привести. Это достигают путем деления на некий выбранный полином степени n. Ясно, что выбирать можно разные полиномы. Выбор другого полинома приведет к другим результатам умножения и, соответственно, к другому полю $GF(p^n)$.

Выбранный для построения поля Галуа полином называют *порождающим* (*образующим*).

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:

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 (схема кодирования), тем самым преобразует вектор a в c (кодовое слово), поступает шум, в процессе пересылке кодового слова по каналу связи на него накладывается вектор ошибок e, в котором единичные биты соответствуют искажениям, после применения декодером схемы декодирования g получается вектор a’, который, в идеале, должен получиться 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.

Алгоритм:

Прежде всего, необходимо вставить контрольные биты. Они вставляются в строго определённых местах — это позиции с номерами, равными степеням двойки. В нашем случае (при длине информационного слова в 16 бит) это будут позиции 1, 2, 4, 8, 16.

Теперь необходимо вычислить значение каждого контрольного бита. Значение каждого контрольного бита зависит от значений информационных бит (как неожиданно), но не от всех, а только от тех, которые этот контрольных бит контролирует. Для того, чтобы понять, за какие биты отвечает каждых контрольный бит необходимо понять очень простую закономерность: контрольный бит с номером N контролирует все последующие N бит через каждые N бит, начиная с позиции N.

Берём каждый контрольный бит и смотрим сколько среди контролируемых им битов единиц, получаем некоторое целое число и, если оно чётное, то ставим ноль, в противном случае ставим единицу.

На принимающей стороне необходимо убрать контрольные биты и заново применить алгоритм. Для того чтобы понять, что произошла ошибка нужно сравнить пришедшую закодированную последовательность с заново закодированной (отличаются = ошибка). Чтобы вычислить, где она произошла, нужно определить, какие контрольные биты не совпадают. Затем сложить их номера, чтобы получить позицию ошибки. Затем просто инвертировать бит в позиции, где произошла ошибка.

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 искаженных битов на то же самое число и

остатки сравниваются. Если остатки совпадают – то данные, скорее всего, переданы без ошибок.

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

Циклическим кодом называют линейный код, удовлетворяющий дополнительному условию: если вектор a0, a1, … a(n-1) является кодовым словом, то и его циклический сдвиг a(n-1), a0, …, a(n-2) так же является кодовым словом.

Циклический код позволяет исправлять одну и более ошибок и обнаруживать множественные ошибки (зависит от параметров).

Базовая идея циклического кодирования состоит в том, чтобы в качестве проверочных битов передавать остаток от деления информационных битов на некоторое выбранное число. После приема снова выполняется деление уже возможно искаженных информационных битов на то же самое число и сравнивается с остатком. Если остатки совпадают, то данные с определенной вероятностью приняты без ошибок.

На практике же деление выполняется по правилам арифметики полей Галуа, то есть без учета переносов.

Информационные биты, то есть делимое, соответствуют информационному полиному. Делитель соответствует порождающему (образующему) полиному. Частное не используется и отбрасывается. Для того чтобы максимально разнообразить остатки в качестве порождающего полинома должен выбираться неприводимый полином.

Существует два подхода к реализации циклического кода на стороне приемника:

1. Согласно базовой идеи, описанной выше
2. На порождающий полином делится все принятое кодовое слово. Если ошибок нет, то остаток будет равен 0.

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 (код Хэмминга, циклические коды, итеративные коды и другие)
- Коды для контроля модульных и пакетных ошибок (РС-коды, низкоплотные модульные коды, векторные модульные коды)
- Сверточные коды
- Арифметические коды
- Низкоскоростные коды (коды максимальной длины, нелинейные коды)

Могут делиться на:

- Блочные – сообщение разбивается на блоки
- Непрерывные – неразделенная последовательность символов

31. Классификация каналов в сети передачи данных

С точки зрения направленности, последовательный 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.

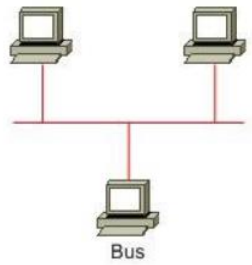
Также последовательный канал может быть:

- Выделенным – зарезервирован определенной парой станций-абонентов, также в отечественной литературе называется моноканалом.
- Разделяемый – может разделяться несколькими абонентами

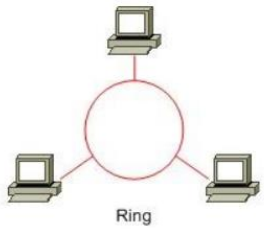
32. Логические и физические топологии LAN

Топологии в LAN:

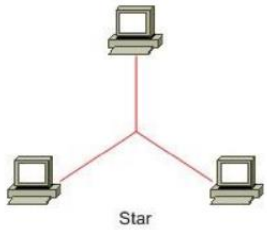
- Шина



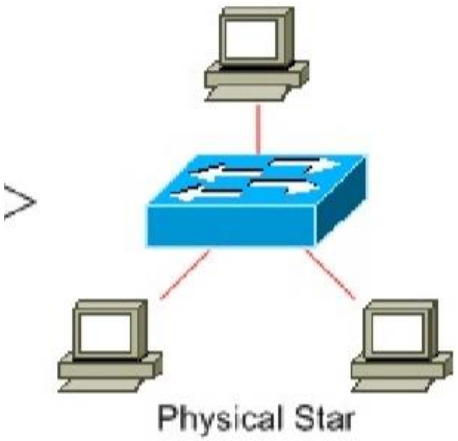
- Кольцо



- Звезда



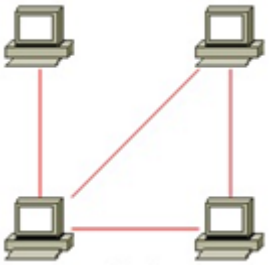
Причём физически топологии шины, кольца и звезды совпадают (коммутатор посередине, все остальные узлы связаны с ним). Также сегмент может иметь *гибридную* топологию.



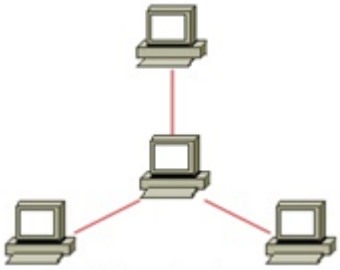
33. Логические и физические топологии WAN и RAS

Логические топологии WAN:

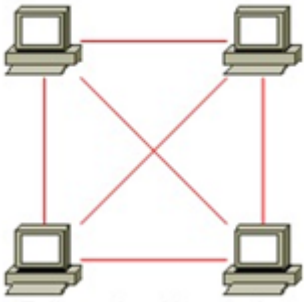
- Сеть (mesh)



- Ступица-со-спицами (hub-and-spokes)



- Полная связь (full mesh):



Топология RAS – 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 может выйти 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*.

Два подхода случайных методов доступа:

- 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

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

Ключевая особенность – выход передатчика и вход приемника станции – одна цепь

35. CSMA/CD (Ethernet)

CSMA/CD (Carrier Sense Multiple Access with Collision Detection) - множественный доступ с прослушиванием несущей и обнаружением коллизий, описанный в стандарте Ethernet (IEEE 802.3).

Передача очередного кадра

Прием очередного кадра

Задержка перед началом очередной попытки передачи после коллизии (backoff) измеряется в так называемых слот-таймах (slot time - минимальная единица времени при диспетчеризации и подбирается с учетом многих других параметров. По крайней мере, он должен быть больше суммы удвоенного времени прохождения сигнала по сегменту и времени переда jam-сигнала), количество которых является случайным целым числом r.

$$0 \le r \le 2^k ,$$

где

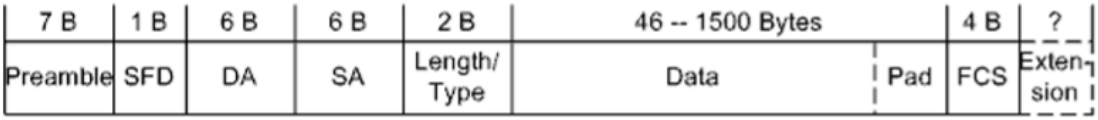
$$k = \min (n, 10) ,$$

где n - номер попытки.

После превышения счетчиком попыток некоторого порогового значения дальнейшие попытки считываются бесперспективными. Значение k не может быть больше 10.

Каждая обнаружившая коллизию станция передает специальный jam-сигнал некоторой длительности (значение стандартом не регламентируется). Jam-сигнал выполняет две важные функции. Во-первых, является признаком возникновения коллизии, что позволяет другим станциям сразу «увидеть» коллизию (столкнувшиеся передатчики, выставившие jam-сигнал, и так знают о коллизии). Во-вторых, позволяет синхронизировать время начала отсчетов случайных задержек.

36. Кадр Ethernet



Поля:
Preamble -- преамбула.
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.
FCS (Frame Check Sequence) -- контрольная сумма.
Extension -- расширитель.

37. CSMA/CA (Wi-Fi)

CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance) - множественный доступ с прослушиванием несущей и избеганием коллизий, описанный в стандарте Wi-Fi (IEEE 802.11).

Случайная задержка измеряется в слот-таймах, как и в Ethernet, но алгоритм другой. Количество слот-таймов является случайным целым числом Random:

$0 \le Random \le CW$,

где CW (contention window) -- так называемое окно состязаний:

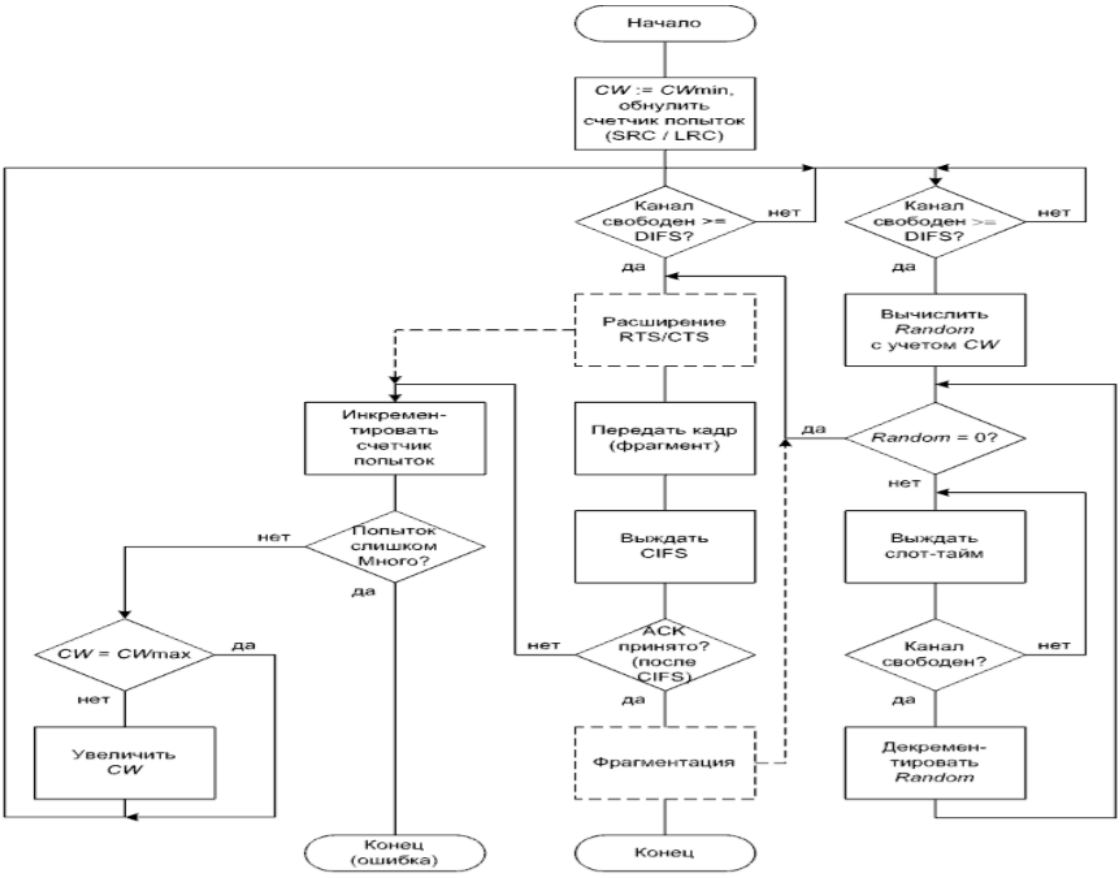
$CW_{min} \le CW \le CW_{max}$,

и берется из ряда: 7, 15, 31 ... (два в некоторой степени минус один).

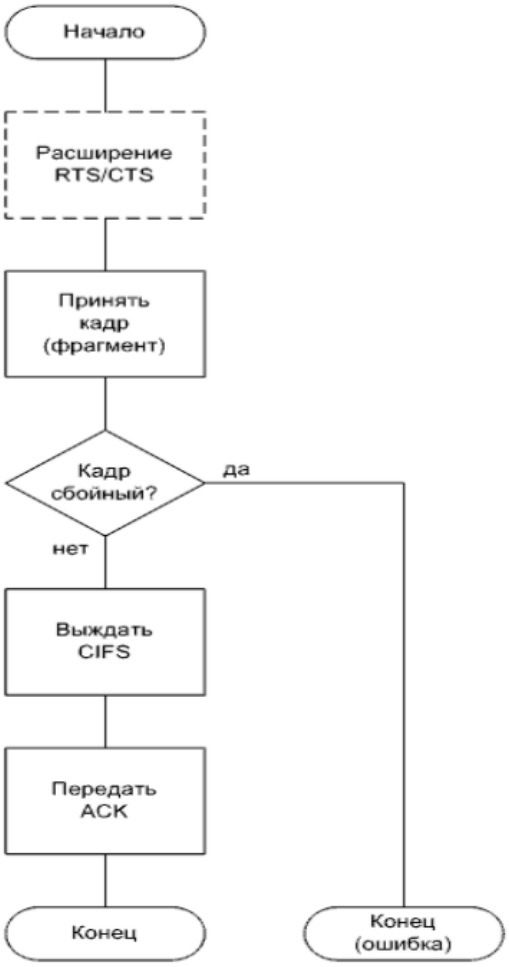
Крайние значения зависят от способа модуляции (типичное значение CWmin - 15, типичное CWmax - 1023).

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

Передача очередного кадра



Прием очередного кадра



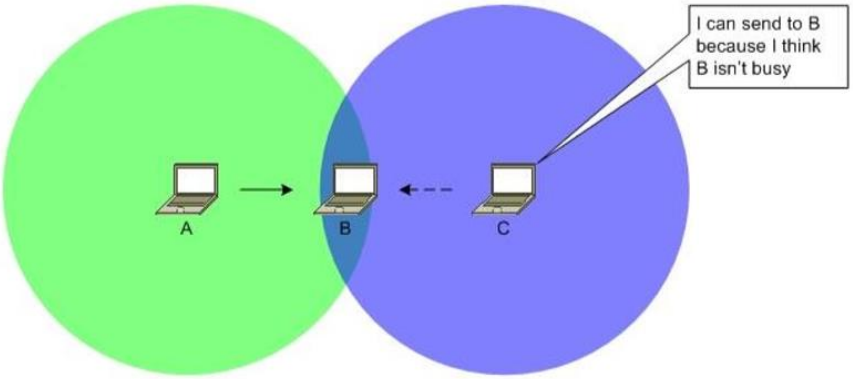
Для беспроводных каналов свойственны две проблемы, которые получили следующие названия:

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

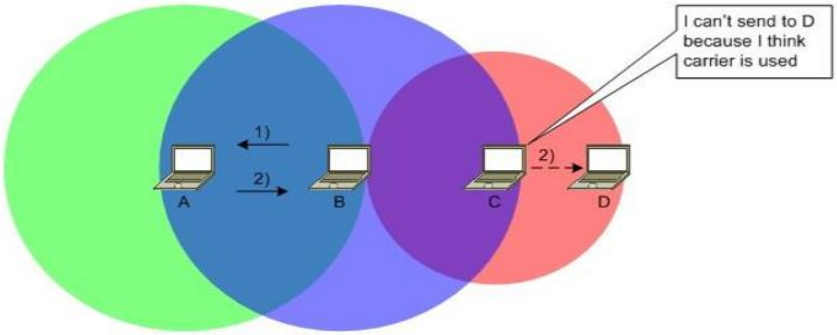
Предполагается, что все станции взаимодействуют в рамках одного канала.

Эти проблемы могут возникнуть и в проводных каналах, если не учесть окно коллизий.

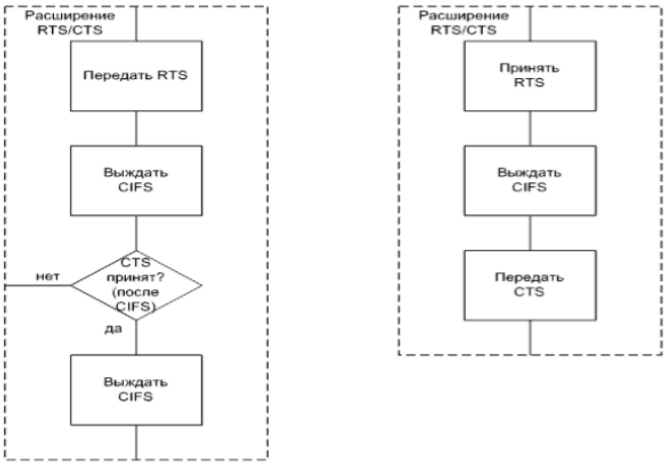
Проблему скрытой станции можно сформулировать так: станция С может ошибочно начать передачу станции В, так как не может “услышать” что станция А уже передает станции В (станция А “скрыта” от станции С).



Проблему доступной станции можно сформулировать так: станция C, зная о взаимодействие станция A и B, не может передать станции D во время пассивности станции B, а могла бы, поскольку считает канал занятым ошибочно (станция C “доступна” для станции D).



Частично решить проблемы помогает опциональное расширение RTS(ready to send)/CTS(clear to send).

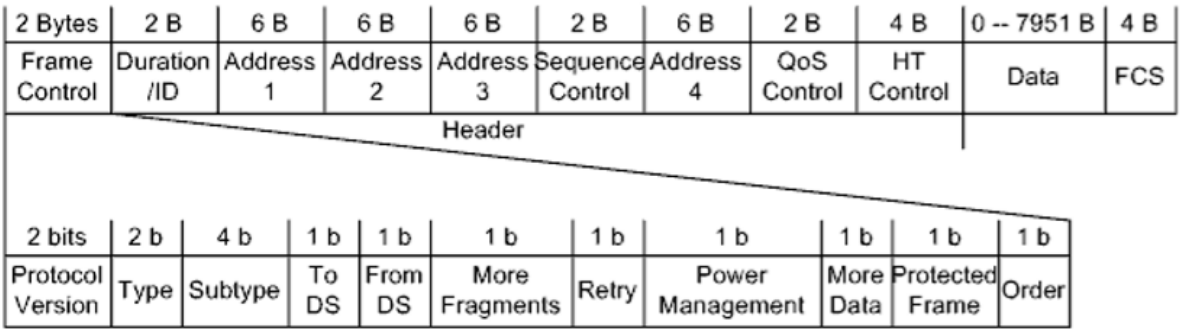


Алгоритм CSMA/CA (Wi-Fi). Расширение RTS/CTS

дописать!!!!!!!! (или нет)

38. Кадры Wi-Fi

Обобщенный формат кадра Wi-Fi



Поля:

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

Поля контроля кадра:

1. Protocol Version - версия протокола (до сих пор равна нулю)
2. Type - тип: 00 - Management - управление, 01 - Control - контроль, 02 - Data - данные, 11 - Reserved - зарезервировано.
3. Subtype - подтип (в настоящее время определено около сорока подтипов)
4. To DS - флаг направления в распределительную систему (проводную систему, связывающую беспроводные сегменты)
5. From DS - флаг направления из распределительной системы
6. More Fragments - флаг наличия фрагментации
7. Retry - флаг повторной попытки передачи
8. Power Management - флаг режима энергосбережения

9. More Data - флаг наличия доп данных (например, буферизованных данных для находящейся в режиме энергосбережения станции)

10. Protected Frame - флаг защищенного кадра (шифрования)

11. Order - флаг упорядоченности (при QoS)

В зависимости от подтипа кадра в адресных полях могут комбинироваться до четырех из пяти возможных адресов:

BSSID (Basic Service Set Identifier) - идентификатор так называемой базовой зоны обслуживания (то есть беспроводного сегмента)

SA (Source Address) - адрес источника

DA (Destination Address) - адрес назначения

TA (Transmitting station Address) - адрес станции-передатчика (непосредственного)

RA (Receiving station Address) - адрес станции-приемника (непосредственного)

39. Особенности детерминированных методов доступа к моноканалу

Все детерминированные методы завязаны на системе приоритетов в том или ином виде.

При использовании механизма приоритетов не обойтись без так или иначе выраженного арбитра. В качестве арбитра может выступать специальный служебный кадр, который в русскоязычной литературе обычно называют маркером (token).

Таким образом, основные критерии классификации детерминированных методов:

- централизованное либо распределенное управление
- алгоритм назначения приоритетов
- топологические особенности

На эффективность детерминированных методов наиболее существенное влияние оказывают те же факторы, что и в ситуациях со случайными методами:

- кол-во взаимодействующих станций
- частота синхронизации
- длина кадра.

40. Алгоритм Token Ring

В данном алгоритме применяется *централизованное управление*. В кольцо включается по крайней мере одна управляющей станция(в Token Ring – *станция-монитор)*, наделенная особыми полномочиями и призванная инициализировать кольцо и следить за его работоспособностью.

Кроме единственной *основной станции-монитора* (active monitor) в состав кольца может входить некоторое количество *резервных мониторов* (standby monitors)

Функции *станции монитора*:

1. Инициализация подключившихся к кольцу станций
2. Тактировать (на физическом уровне) работу кольца
3. Контролировать наличие и валидность маркера
4. Предотвратить зацикливание

В стандарте предусмотрены четыре вида передаваемых последовательностей:

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

Каждая из станций в любое время должна распознавать (и различать) маркеры, кадры и спец последовательности.

Главное – чтобы в алгоритме были поля контроля доступа P и R, где P – поле текущего приоритета, а R – поле запрашиваемого приоритета. Каждое из полей может иметь значение от 000b до 111b, то есть доступно восемь уровней приоритета. При отсутствии приоритетов станция-монитор создаёт и запускает токен с нулевыми значениями этих полей (назначение этих полей не проявляется). 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 (идентификатор маркера) в единицу, преобразует маркер в кадр и отправляет сообщение
- Если нету сообщений – посылает токен дальше

Приоритет автоматически достается станции, до который маркер дошел раньше

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 THT (token holding timer)

41. Реализации детерминированных методов доступа к моноканалу

1) Token Ring

2) Технология ARCNET (Attached Resource Computer NETwork) - первая технология ЛКС, массово использовалась до Ethernet. В настоящее время является сильно устаревшей. Скорость: 2,5 Mbit/s. Логическая топология: однонаправленное кольцо. Физическая топология: шина или звезда. Во втором случае требовалось дополнительное сетевое оборудование (пассивные или активные концентраторы). Алгоритм является аналогом упрощенного варианта алгоритма Token Ring (без системы приоритетов).

3) Технология Token Bus. Была стандартизирована как IEEE 802.4. Благодаря плохому масштабированию и сложности восстановления после сбоев, почти не применялась, только в промышленных сетях некоторых индустриальных компаний. Разработка давно остановлена, является сильно устаревшей. Скорость: 1, 5, 10, 20 Mbit/s. Логическая топология: однонаправленное кольцо. Физическая топология: шина. Алгоритм представлял собой адаптацию алгоритма Token Ring к шинной топологии.

4) Технология FDDI (Fiber Distributed Data Interface) разрабатывалась целенаправленно для поддержки оптических СрПД и позволяет значительно увеличить дальность передачи. Кроме собственно FDDI, еще был разработан аналогичный вариант для электрических СрПД под названием CDDI (Copper Distributed Interface). Скорость: 100 Mbit/s, 200 Mbit/s. Логическая топология: однонаправленное кольцо с резервированием, то есть два отдельных кольца (если оба кольца исправны, то они функционируют параллельно). Физическая топология: двойное кольцо, к которому с помощью дополнительного сетевого оборудования могут подключаться деревья (узлами дерева являются концентраторы, листьями -- станции, концентратор корень включается в двойное кольцо). Алгоритм представляет собой расширение алгоритма Token Bus.

5) Технология 100VG-AnyLAN. Идея заключается в получении по тем временам высокоскоростного гибрида между Ethernet и Token Ring, причем с сохранением совместимости с их кадрами. Скорость: 100 Mbit/s. Логическая топология: дерево. Физическая топология: дерево (с опциональным резервированием), формируемое с помощью дополнительного сетевого оборудования (узлами дерева являются повторители, листьями -- станции или мосты, с помощью мостов можно

подключать сегменты Ethernet или Token Ring). Метод доступа получил название Demand-priority. Основывается на программном автомате под названием MAC state machine.

42. Адресация в компьютерных сетях и классификация адресов

В качестве двух обязательных адресов используется:

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

Для компьютерных сетей ест ь четыре базовых типа адресов:

1) Юникаст – пакет с таковым адресом назначения должен быть обработан одной конкретной станцией
2) Бродкаст – пакет должен быть обработан всеми станциями
3) Мультикаст – пакет должен быть обработан несколькими станциями из множества
4) Эникаст – пакет должен быть обработан одной станцией из множества (наиболее сложная адресация)

Бродкаст-, мультикаст- и эникаст-адреса не могут быть адресами источников, так как отдельно взятый пакет может сгенерировать только одна станция.

В каждом пакете должны присутствовать по крайней мере адреса канального уровня. В большинстве же практических реализаций семейств протоколов, кроме адресации на канальном уровне, предусмотрена адресация на сетевом (в связке с транспортным) и прикладном уровне.

Адреса канального уровня «зашиваются» в сетевое оборудование при его производстве и поэтому повторяться не должны. Они не предполагают возможность пользовательского вмешательства и их считают абсолютно уникальными. Часто (в том числе Cisco) такую адресацию называют *физической* (physical). Адреса сетевого и прикладного уровней назначают пользователи. Часто (в том числе Cisco) такую адресацию называют *логической* (logical).

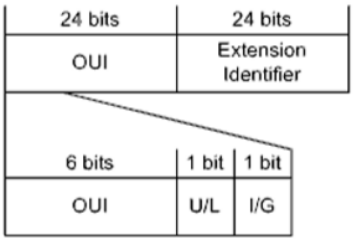
Кроме всего прочего, даже на одном уровне модели OSI адресация может быть *иерархической* (hierarchical), то есть предполагать определенную структуризацию соответствующего адресного пространства. Иерархичность выражается в количественном и качественном разделении адресов на типы

43. MAC-адреса

MAC-адрес — уникальный идентификатор, присваиваемый каждой единице активного сетевого оборудования или некоторым их интерфейсам в компьютерных сетях Ethernet.

MAC-адреса должны быть уникальны и контролируются IEEE RA (Registration Authority). В стандартах IEEE определены три базовых формата MAC-адресов: MAC-48, EUI-48 и EUI-64, где EUI (Extended Unique Identifier) -расширенный уникальный идентификатор. MAC-48 можно считать аналогом EUI-48, т.к. изначально это было общим понятием.

Формат EUI-48:



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

Поля:
OUI (Organizationally Unique Identifier) -- уникальный идентификатор организации (производителя).
U/L (Universal/Local) -- признак универсальности-локальности адреса.
I/G (Individual/Group) -- признак индивидуального-группового адреса.
Extension Identifier -- идентификатор-наполнитель.

OUIs выдают централизованно, уникальность оставшейся части должны обеспечить сами организации (любым способом по своему усмотрению).

Время валидности адресов (время, которое нужно выдержать перед повторным присвоением того же адреса другому устройству) определено как 100 лет.

Иногда, при администрировании, возникает необходимость подменить адрес, “зашитый” в оборудование, на некий другой. Этот новый адрес называют локальным административным адресом. Его признаком является единичное значение бита U/L. Согласовывать значение остальных битов не требуется, но в пределах сегмента адрес не должен повторяться.

Граница между OUI и Extension Identifier может проходить не только посредине адреса. В общем случае предусмотрены три варианта разрядности поля OUI: MA-L (MAC Address – Large – 24 бита), MA-M (Medium –28) MA-S (Small – 36 битов).

По правилам данные адреса записывают в формате:

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

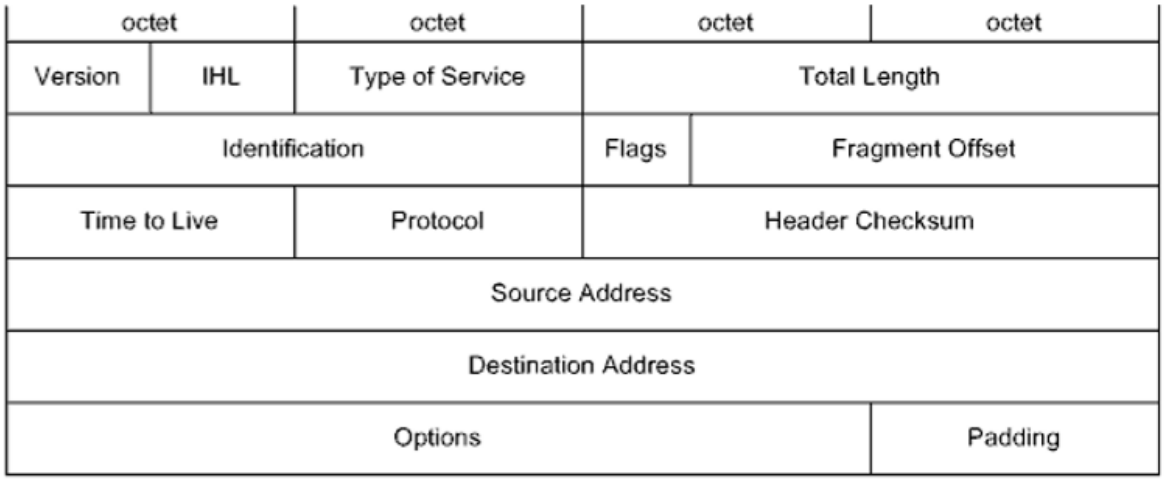
IEEE: 00-16-41-57-7D-48

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



Поля:

1) Version - версия (значение равно 4)
2) IHL (Internet Header Length) - длина заголовка (в 32-ух битных словах, минимальное значение 5)
3) Type of Service - тип сервиса (связано с QoS)
4) Total Length - общая длина данных (в байтах, не может превышать 65536 байтов)
5) Identification - уникальный идентификатор пакета (при фрагментации позволяет определить к какому пакету относится фрагмент)
6) Flags - флаги
7) Fragment Offset - смещение текущего фрагмента (в 64-ех битных словах, смещение первого фрагмента равна нулю)
8) Time to Live - “время жизни” (при каждой ретрансляции уменьшается, когда становится равным нулю пакет уничтожается)
9) Protocol - протокол (инкапсулирующий в поле данных)
10) Header Checksum - контрольная сумма заголовка
11) Source Address - адрес источника
12) Destination Address - адрес назначения
13) Options - опции (например, связанные с безопасностью, размер вариативен)

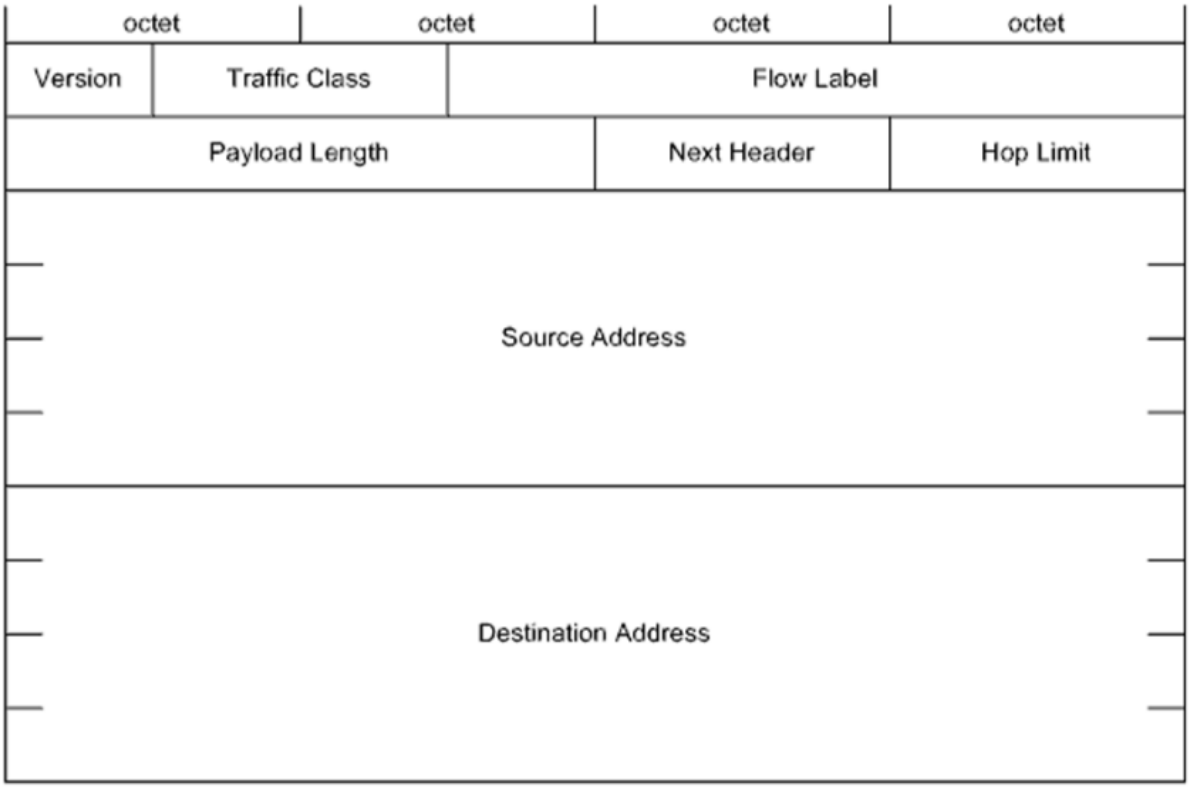
Флаги:

DF (Don’t Fragment): 0 - пакет фрагментирован, 1 - пакет нефрагментирован

MF (More Fragment): 0 - текущий фрагмент является последним, 1 - текущий фрагмент не является последним

45. Заголовок IPv6

Заголовок данного типа имеет гибкую структуру. Заголовки “каскадируются” - сколько заголовков нужно, столько и вставляется.



Поля:

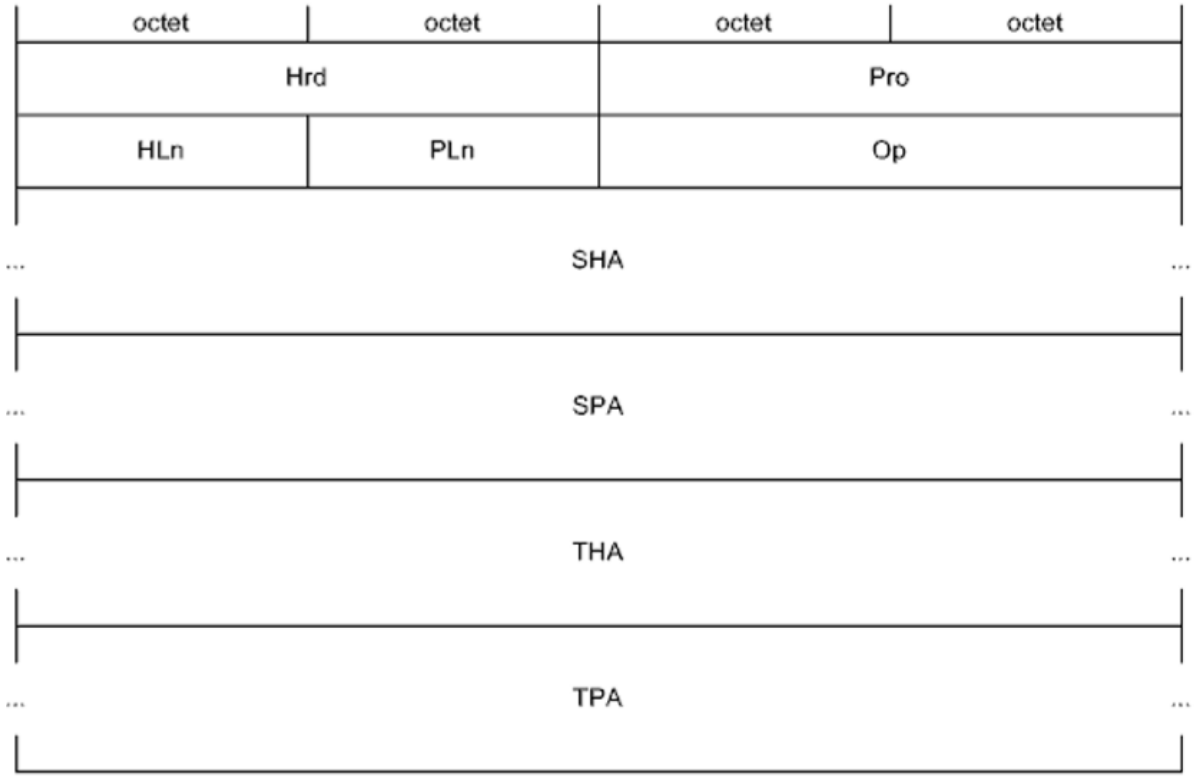
1) Version - версия (значение равно 6)
2) Traffic Class - класс трафика (связано с QoS)
3) Flow Label - метка потока (связано с QoS)
4) Payload Length - длина полезной нагрузки (в байтах, аналог поля Total Length)
5) Next Header - селектор следующего заголовка (в том числе, аналог поля Protocol)
6) Hop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

46. Протокол ARP

Группа протоколов под названием ARPs (Address Resolution Protocols) предназначена для восстановления соответствий между MAC-адресами и IP-адресами.

Под прямым преобразованием, собственно ARP (RFC 826), понимаю нахождение MAC-адреса по IP-адресу. Обратное преобразование выполняется по протоколу RARP (Reverse ARP).

Формат пакета ARP



Поля:

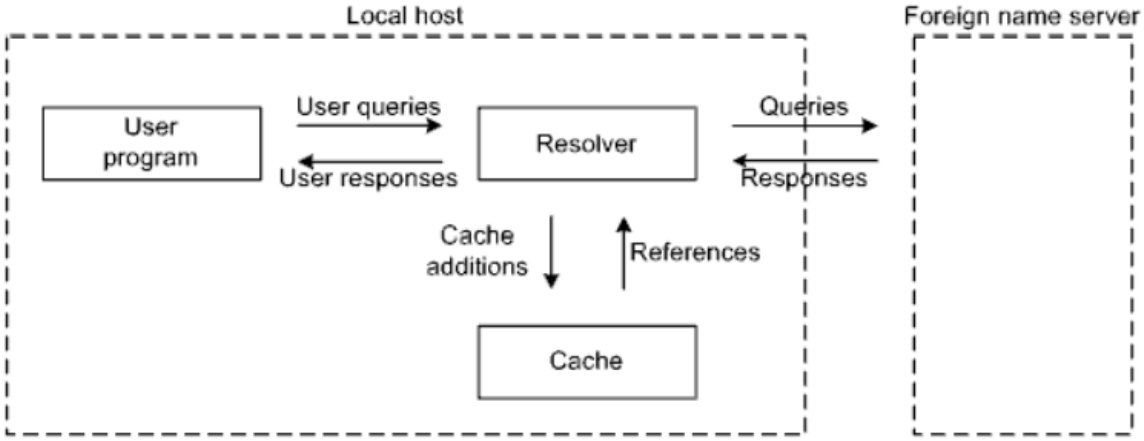
1) Hrd (Hardware) - тип оборудования (1 - Ethernet)
2) Pro (Protocol) - протокол (800h - IP)
3) HLn (Hardware address Length) - длина аппаратного (физического) адреса (в байтах, 6 - Ethernet)
4) PLn (Protocol address Length) - длина протокольного (логического) адреса (в байтах, 4 - IP)
5) Op (Opcode) - код операции: 1 - Request - запрос, 2 - reply - ответ (и некоторые другие)
6) SHA (Sender Hardware Address) - аппаратный адрес станции-отправителя (запрашивающий либо отвечающий на зарос)
7) SPA (Sender Protocol Address) - протокольный адрес станции-отправителя

8) THA (Target Hardware Address) - аппаратный адрес станции-получателя

9) TPA (Target Protocol Address) - протокольный адрес станции-получателя

47. Структура системы DNS

Протокол системы DNS – прикладной протокол предназначенный для установления соответствия между IP адресами и адресами прикладного уровня (с которыми работает пользователь).



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

1. Адресное пространство доменных названий (domain name space) и записи о ресурсах – RRs (Resource Records).

Адресное пространство доменных названий имеет иерархическую древовидную структуру.

Доменное название строится из меток – в соответствии с путем к корневой метке. Полная длина не может превышать 255 байтов. Может быть как абсолютным, то есть содержащим всю цепочку меток от станции до корневой метки, так и относительным, то есть содержащим только часть меток.

2. Серверы названий (name servers).

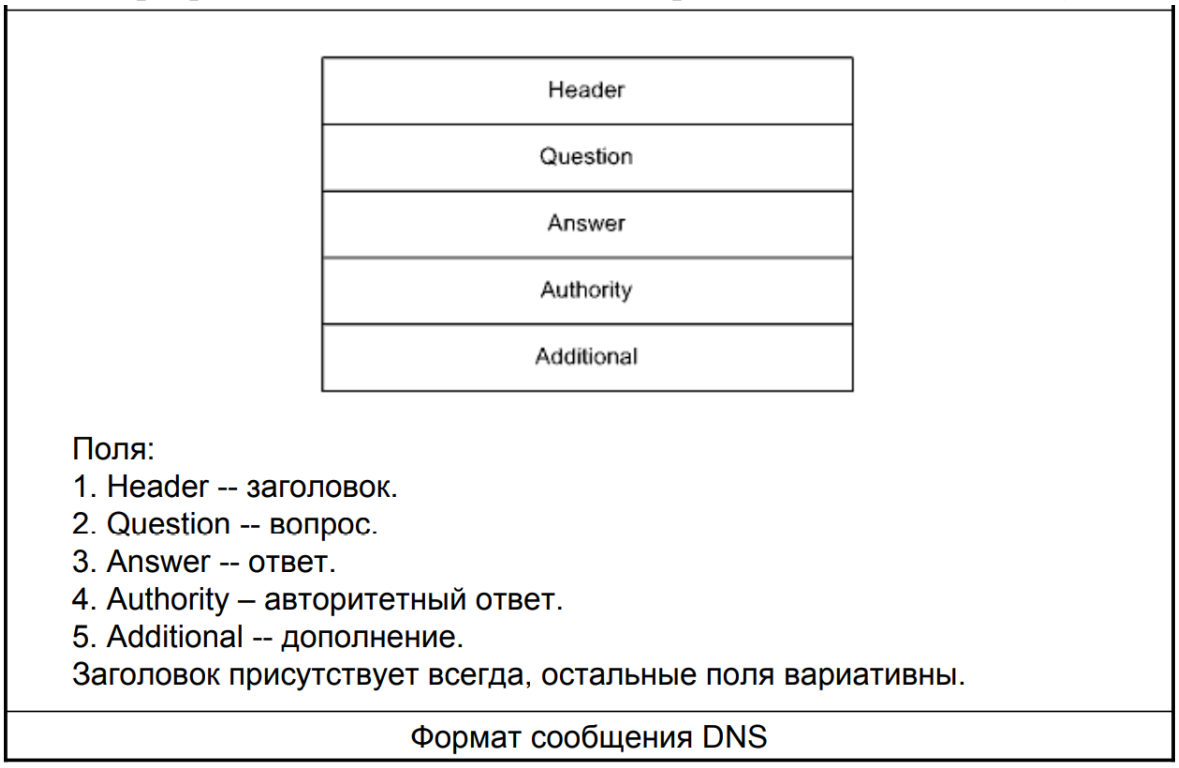
Серверы названий удерживают БД с записями о ресурсах. Их делят на авторитарные и вспомогательные. Также образуют иерархию

3. Программы, отвечающие на запросы клиентов (resolvers).

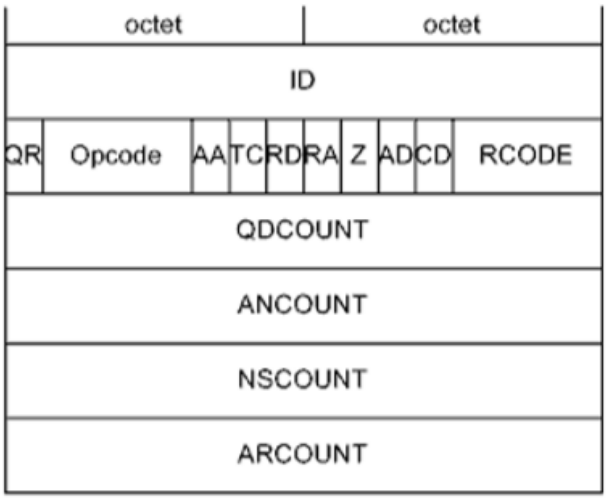
Каждый из этих компонентов «видит» систему DNS по-своему.

48. Сообщения DNS

Сообщения DNS – это запросы и ответы, которые отправляются и принимаются программами отвечающими на запросы клиентов (resolvers).



Формат сообщения DNS



Формат заголовка сообщения DNS

Поля:

1. ID(Identifier) - идентификатор (программы, сгенерировавшей запрос)

2. QR (Query/Response) - флаг запроса/ответа: 0 – query, 1 – response
3. opcode - код операции
4. AA (Authoritative answer) - флаг авторитетного ответа
5. TC (TrunCount) - флаг усеченного сообщения (при слишком длинном сообщение)
6. RD (Recursion Desired) - флаг желательной рекурсии (при обработке запроса)
7. RA (Recursion Available) - флаг поддержки рекурсии
8. Z (Zero) - нулевой бит (зарезервировано)
9. AD (Authenticated Data) - флаг криптографической верифицируемости ответа
10. CD (Checking Disabled) - флаг отсутствия необходимости в криптографической верификации ответа.
11. RCODE (Response code) - код ответа
12. QDCOUNT (Query DNS COUNT) - количество RRs в поле question (обычно один)
13. ANCOUNT(Answer Count) - количество RRs в поле Answer
14. NSCOUNT (Name Server Count) - кол-во элементов в поле Authority
15. ARCOUNT (Additional Records Count) - колво элементов в поле Additional

49. Виртуальные соединения в сети передачи данных

Соединение – нахождение абонентов в состоянии готовности к обмену данными.

Виртуальные соединения – это соединения, установленное между взаимодействующими абонентами-программами.

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

- Организация взаимодействия абонентов-программ
- Настройка задействованного промежуточного оборудования.

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

В свою очередь, виртуальные цепи бывают:

- PVCs (Permanent Virtual Circuits) -- выделенные виртуальные цепи
- SVCs (Switched Virtual Circuits) -- коммутируемые виртуальные цепи (в отечественной литературе иногда называют виртуальными вызовами).

Термин *виртуальный канал* (virtual channel) может в равной степени подходить как к виртуальным соединениям, так и к *виртуальным цепям*.

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

Выделяют два основных критерия классификации оконных методов.

1. Исходя из количества пакетов, передаваемых в окне, оно может быть:

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

2. Исходя из способа обработки очереди пакетов, окно может быть:

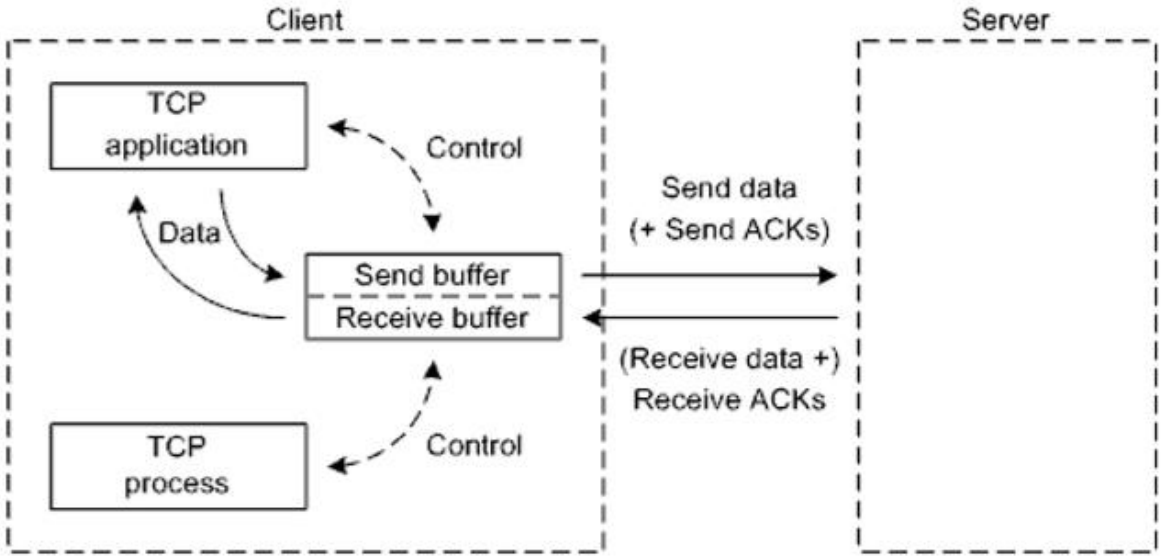
- Фиксированным (fixed) – перед формированием следующего окна текущее должно быть полностью «закрыто», то есть должны быть приняты все необходимые квитанции.
- Скользящим (sliding) – существует возможность сдвигать окно относительно последовательности пакетов.

При реализации оконного метода следует учитывать след дополнительные обстоятельства:

- нужна нумерация пакетов в том или ином виде
- подтверждаться может как все окно, так и каждый из пакетов
- размером окна может управлять как передатчик, так и приемник
- размером окна можно управлять посредством служебных полей, в том числе и в информационных пакетах
- окно, с которым работает передатчик, может отличаться от окна, с которым работает приемник
- иногда важен порядок доставки, пакетов

51. Структура системы TCP

TCP соответствуют клиент-серверной модели.



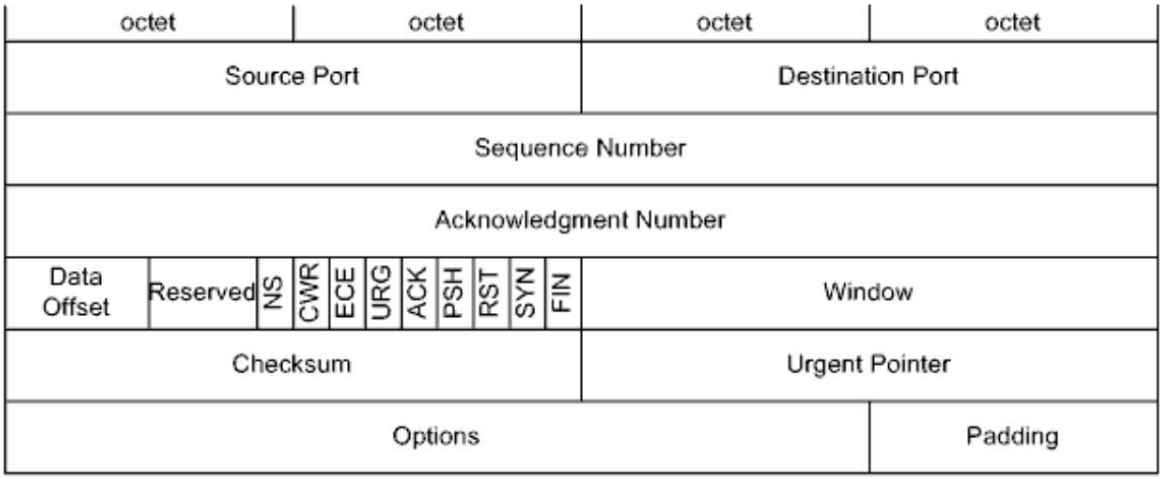
Применительно к каждому TCP-соединению нужно выделять приложение, производящее или потребляющее сетевые данные, и TCP-процесс, предоставляющий коммуникационные услуги (например, спец драйвер ОС). Синхронизировать работу приложения и TCP-процесса можно только с помощью буферизации.

TCP-приложение использует *TCP-интерфейс* для работы с *буффером*, чтобы контролировать запись или считывание данных.

TCP-процесс контролирует *буффер* на наполнение и отвечает за передачу и приём данных.

Передающее приложение последовательно, порциями, записывает блоки байтов сообщения, возможно разной длины, в буфер передачи. TCP-процесс формирует из имеющихся в буфере данных соответствующие кол-во сегментов и последовательно отправляет их. Переданные, но неподтвержденные сегменты с данными продолжают оставаться в буфере, так как возможно потребуется их повторная передача.

52. Заголовок TCP



1. Source Port – программный порт источника.
2. Destination Port – программный порт назначения.
3. Sequence Number (SN) – последовательный номер (сегмента).
4. Acknowledgment Number (AN) – подтверждающий номер.
5. Data Offset – смещение данных (в 32-ух битных словах).
6. Reserved – зарезервировано (должно равняться нулю).
7. URG (URGent Pointer field significant) – флаг значимости указателя на экстренные данные.
8. ACK (ACKnowledgment field significant) – флаг значимости подтверждающего номера.
9. NS (Nonce Sum) – флаг – контрольная сумма для проверки правильности кодов явных уведомлений о заторах (связан с QoS, связан с IP заголовком) (RFC 3540).
10. CWR (Congestion Window Reduced) – флаг уменьшения окна затора при явном уведомлении о заторе (RFC 3168).
11. ECE (Explicit Congestion Notification Echo) – флаг подтверждения явного уведомления о заторе (RFC 3168). 9.0.4.11b
12. PSH (PuSH Function) – флаг принудительной доставки данных (без буферизации).
13. RST (ReSeT the connection) – флаг разрыва соединения (например, из-за сбоя на одной из взаимодействующих сторон).
14. SYN (SYNchronize sequence numbers) – флаг синхронизации последовательных номеров.
15. FIN (No more data from sender) – флаг последних данных.
16. Window (W) – предлагаемое окно.

17. Checksum – контрольная сумма.
18. Urgent Pointer – указатель на экстренные данные (RFC 6093).
19. Options – опции (например, MSS).
20. Padding – наполнитель.

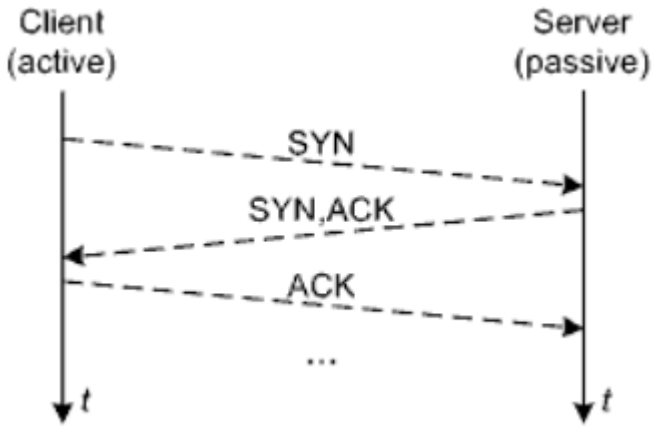
53. Протокол TCP

Протокол TCP – это протокол контроля передачи, который обеспечивает установление надежного соединения между приложениями, а также гарантирует доставку и правильный порядок доставки данных.

Протокол соответствует клиент-серверной модели. Использует *динамическое скользящее окно*.

Функционирование оконного механизма TCP базируется на использовании трех полей в заголовке сегмента: SN , AN, W, и трех флагов (из шести стандартизованных изначально): SYN, ACK, FIN.

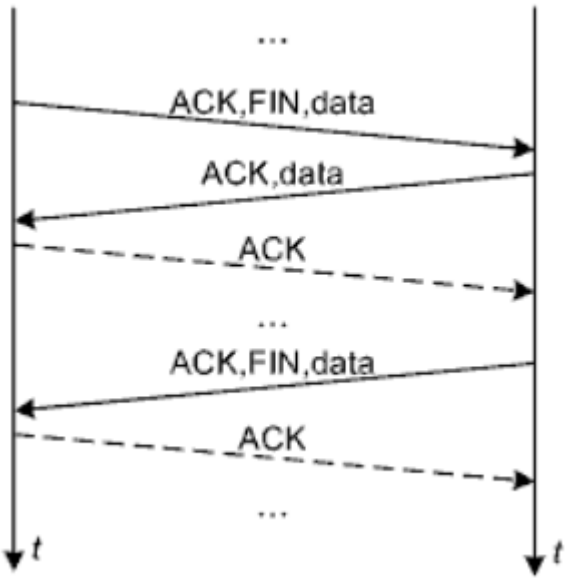
Соединение устанавливается с помощью *тройного рукопожатия (three-way handshake)*:



После установления TCP соединения оно может использоваться в полнодуплексом режиме (передача в обе стороны одновременно).

Поскольку при установлении соединения оно всегда открывается в двух направлениях (по инициативе клиента, но может использоваться в одном любом направлении), для нормального завершения оно и закрыто должно быть в обоих направлениях.

Для закрытия соединения в своем направлении, сторона, в соответствующем сегменте (обычно с последними данными), устанавливает флаг FIN.

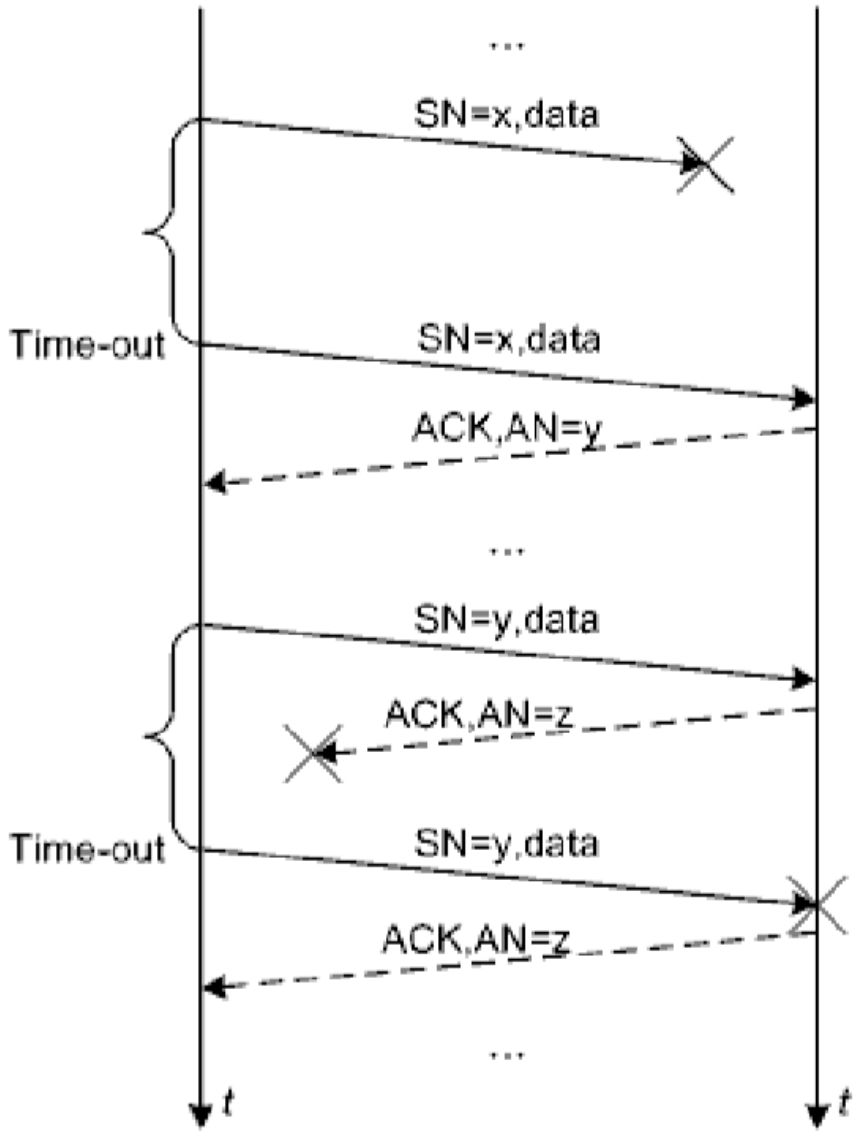


Соединение, нормально закрытое только в одном направлении, или ненормально завершенное на одной из сторон без уведомления другой стороны (в результате сбоя) называют полуоткрытым (half-open).

Размер предлагаемого окна в поле W может изменяться каждый раз для соответствующей коррекции текущего окна передачи, в том числе и при установлении соединения для изменения размера текущего окна передачи по умолчанию.

В случае задания нулевого значения поля W передача данных фактически запрещается. После освобождения места в буфере приема подтверждение обязательно повторяется с уже ненулевым полем W, что разблокирует передающую сторону.

Проблемы возможной потери в СПД некоторых сегментов решается с помощью тайм-аутов:



Передающий TCP-процесс определяет потерю сегмента с данными либо его подтверждения по отсутствию этого подтверждения в течение установленного интервала времени. После наступления тайм-аута сегмент с данными передается повторно.

Протокол TCP обладает несколькими дополнительными возможностями. Возможна пересылка экстренных данных (urgent data) и ускоренная пересылка (push function).

54. Усовершенствования протокола TCP

Причиной разработки дополнений к протоколу TCP стал *синдром "Глупого окна"*. Синдром может возникать по разным причинам и проявляется в том, что текущее окно передачи не соответствует состоянию приемника, тем самым не позволяя его как следует «нагрузить» либо, наоборот, «разгрузить».

1. Решение Нэгла (Nagle) позволяет побороть «синдром глупого окна», когда передающей стороне требуется часто отправлять небольшие сегменты с данными. Объединяются несколько небольших исходящих сообщений и отправляя их все одновременно.

2. Решение Кларка (Clark) позволяет побороть «синдром глупого окна» когда принимающей стороной часто анонсируется небольшое предлагаемое окно. Получатель должен подождать, пока в буфере не накопится значительное количество свободного места и затем анонсировать размер окна максимально большого размера.

3. Дополнения Якобсона (призвано бороться с перегрузками в СПД):

- Медленный старт (slow start). Идея заключается в том, что в начале передачи размер текущего окна передачи нужно увеличивать не «скачком», а плавно, пропорционально скорости получения подтверждений (не превышая размер предлагаемого окна).
- Избегание затора (congestion avoidance). Состоит в сдерживании экспоненциального роста размера текущего окна передачи после преодоления им некоторого порога. Как правило переход к избеганию затора происходит после медленного старта.
- Быстрая повторная передача (fast retransmit). При получении принимающей стороной разупорядоченного сегмента с данными (возможно из-за потери ожидаемого сегмента с данными) незамедлительное повторение подтверждения с AN недостающего сегмента с данными. При получении передающей стороной трех одинаковых подтверждений незамедлительное повторение сегмента с данными согласно AN. Что, в некоторых ситуациях, позволяет успешно передать потерянный сегмент еще до наступления тайм-аута.
- Быстрое восстановление (fast recovery). После обнаружения затора, переход сразу к избеганию коллизий, минуя стадию медленного старта. Как правило в связке с быстрой повторной передачей

55. Протокол UDP и заголовок UDP

Протокол UDP (User Datagram Protocol) – пользовательский дейтаграммным протокол транспортного уровня реализующий способ пересылки данных без гарантии доставки и без гарантии правильного порядка доставки.

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).

56. Классификация и характеристики сред передачи данных

Все исконно используемые в КС СрПД можно разделить на пять типов:

1. Коаксиальные кабели (coaxials) с различным волновым сопротивлением. 185-200 м, 10 Мб/с
2. Экранированные и неэкранированные кабели на основе витых пар (twisted pairs) различных категорий. 30-100 м, 10-100 Мб/с
3. Одно- и многорежимные (одно - и многомодовые) оптоволоконные кабели (fiber равно fibre). 2 км, 10 Мб/с – 2 Гб/с
4. Эфир (ether).
5. Телефонные пары (phone pairs).

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

С точки зрения целевой области применения все кабели делят на:

1. Кабели для внешней прокладки (outdoor cables) – СПД на улице.
2. Кабели для внутренней прокладки (indoor cables) – СПД в помещениях.
3. Оконечные кабели (cords) – для подключения рабочих мест.

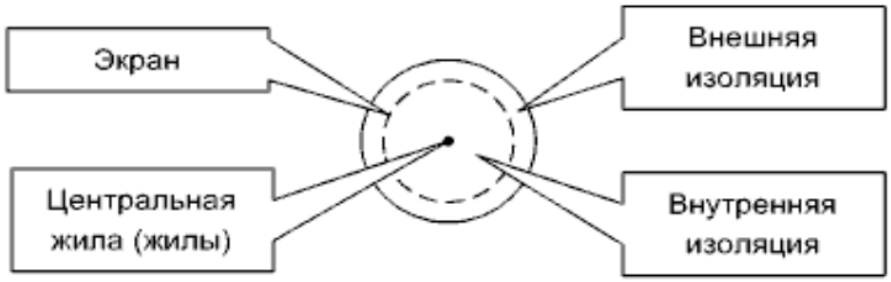
Основные отличительные требования outdoor-кабелей: большее число проводников, высокая прочность, улучшенные электро-магнитные хар-ки, влагостойкость, широкий диапазон рабочих температур.

Indoor-кабелей отличаются меньшими габаритами, большей гибкостью, лучшей пожаростойкостью.

Кабели cords являются сравнительно простыми и низкокачественными.

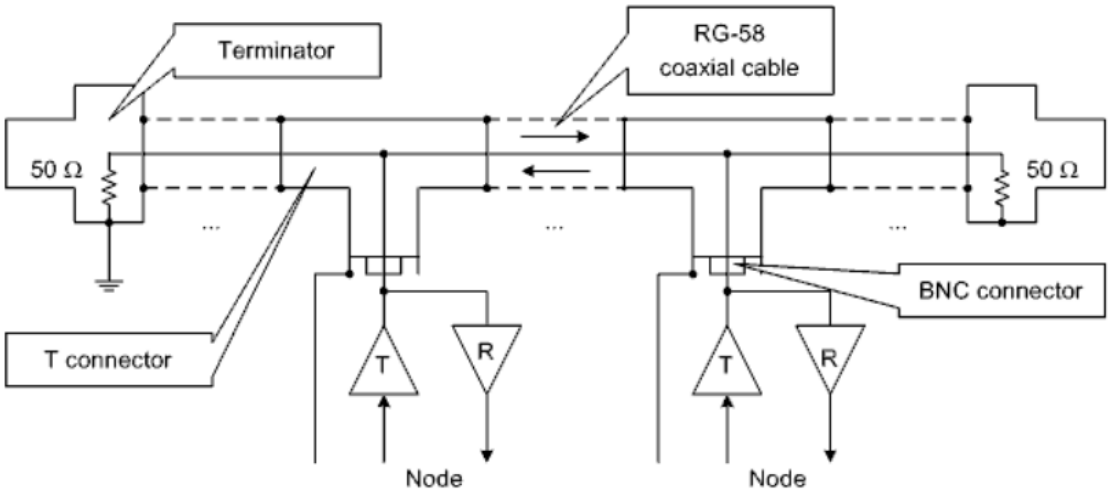
57. Среды передачи данных на основе коаксиальных кабелей

Широко используется в телевидении. Важное достоинство – передавать в один и тот же момент множество сигналов. Коаксиальный кабель, в отличие от витой пары, устойчив к электромагнитным помехам. И способен передавать сигналы на бóльшие расстояния.



Структура коаксиального кабеля

Для формирования сегмента на базе коаксиального кабеля необходимо соответствующее количество BNC-разъемов (Bayonet-Neill-Concelman), Т-соединителей и пара *терминаторов* (terminators), один из которых заземляют.



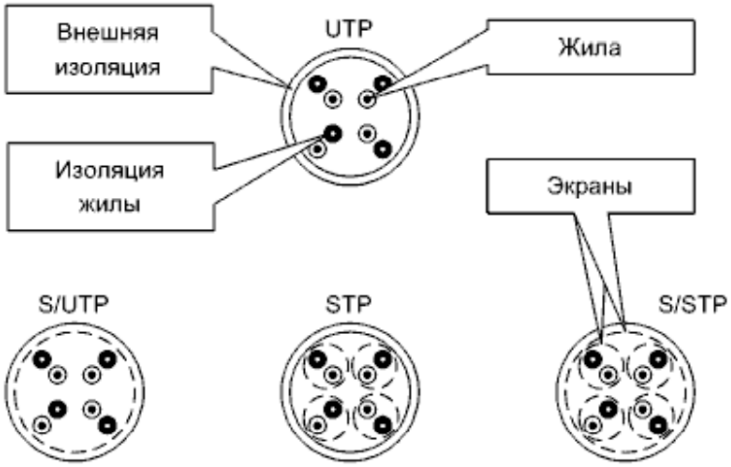
Коаксиальные кабели производители обычно выпускают черными, реже серыми.

58. Среды передачи данных на основе витых пар

В типовых случаях, витыми парами соединяют разноранговое сетевое оборудование. Например, пользовательскую станцию подключают к коммутатору, или коммутатор подключают к маршрутизатору. При этом используют кабели с «прямой» разводкой.

При необходимости, для соединения одноранговое оборудования, например непосредственного связывания двух пользовательских станций, используют кросс-кабели -- пары TD и RD скрещены.

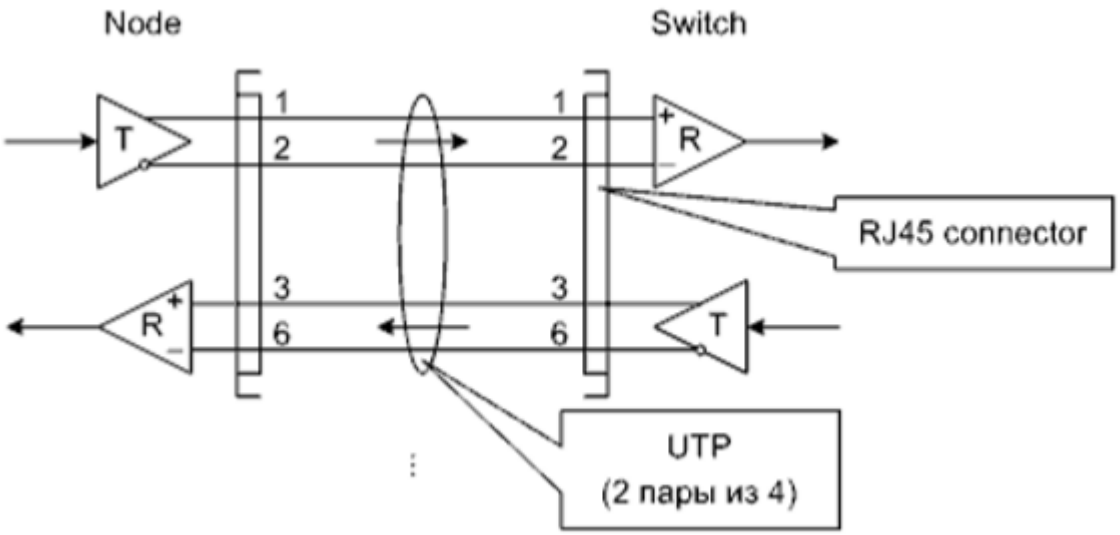
(Полная аналогия с вариантами соединений ООД и АПД.)



Где TP -- Twisted Pair, S -- Shielded, U -- Unshielded, плюс может быть F -- Foiled (если для изготовления экрана применена фольга).

Особо выделяют плоский (flat) кабель (например, для напольной прокладки).

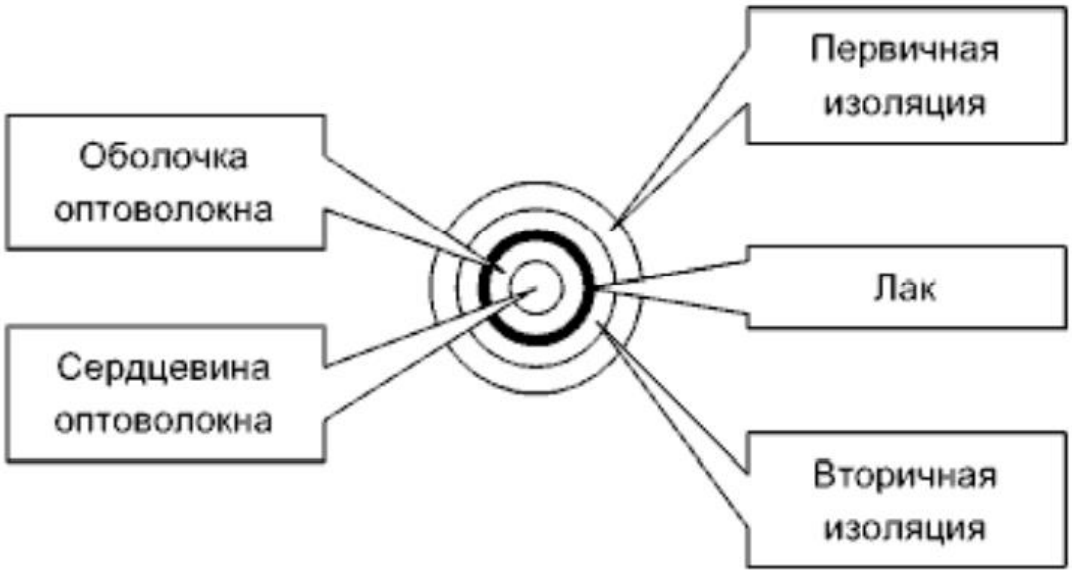
Сама витая пара состоит из 8 кабелей (бело-оранжевый, оранжевый, б-зелёный, синий, б-синий, зелёный, б-коричневый, коричневый), которые разводятся по стандарту 568-B под RJ-45.



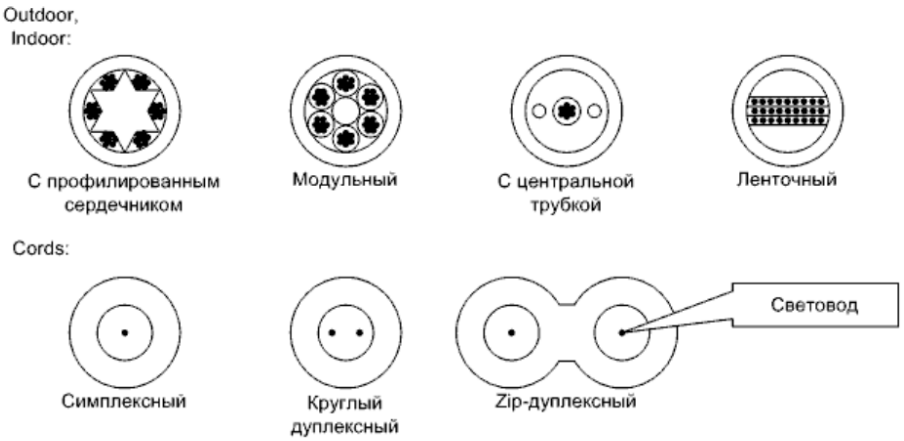
59. Среды передачи данных на основе оптоволоконных кабелей

Рабочими компонентами оптоволоконных кабелей являются *световоды* (primary fiber, waveguide, lightpipe), изготовленные из оптоволокна, то есть особого кварцевого стекла. Поскольку оптоволокно очень хрупкое, его многократно защищают различными способами. Световод -- это оптический волновод.

Рабочими компонентами самого световода являются *оболочка* (cladding) и *сердцевина* (core).

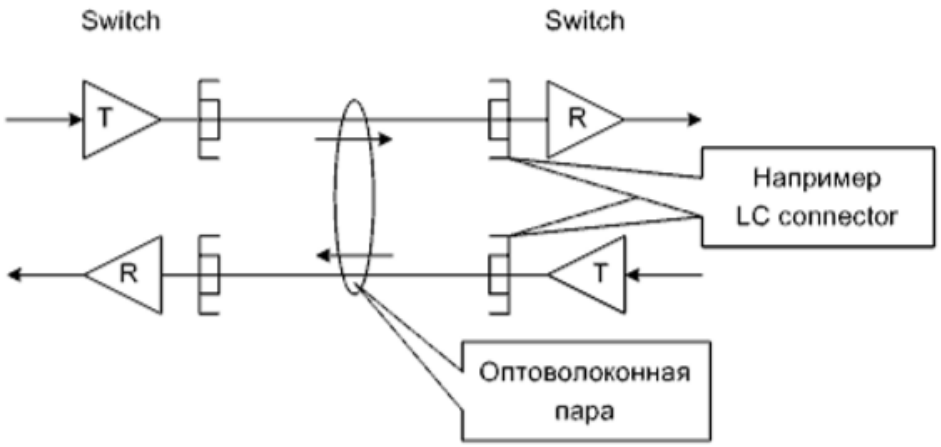


Применяют множество видов оптоволоконных кабелей.



Дополнительно все оптоволоконные кабели делят на два подтипа:

1. Содержащие металлизированные упрочняющие конструкции или проводники.
2. Полностью диэлектрические.



Оптоволоконные соединения выполняют двумя способами:
1. Разъемным, причем может быть:
-- контактным;
-- линзовым.
2. Неразъемным, причем может быть:
-- сплавным;
-- механическим.

Оптоволоконные разъемы так же отличаются больши'м разнообразием. Разработано около 100 типов. Основные стандартные: FC, SC, ST (менее компактные); E-2000 (LSH), LC (более компактные).

60. Физический уровень Ethernet

Основными средами передачи данных по Ethernet являются:

Коаксиальные кабели – используются в основном в телевидении. Возможна передача в один и тот же момент времени множества сигналов. 185-200м, 10 Мб/с, медь

Витые пары – используются в основном в домах. 30-100 м, 10-100 Мб/с, медь

Оптоволоконные кабели – используются для прокладки на больших расстояниях. 2 км, 10 Мб/с – 2 Гб/с, световоды (оптический волновод) из оптоволокна

Телефонные пары

Существуют следующие ключевые стандарты которые использовались или используются:

Коаксиальные:

- 10BASE5
- 10BASE2

Витая пара:

- 100BASE-TX
- 1000BASE-T
- 2.5GBASE-T
- 5GBASE-T
- 10GBASE-T

Оптоволокно:

- 10BASE-FL
- 100BASE-FX
- 1000BASE-SX
- 1000BASE-LX
- 10GBASE-SR
- 10GBASE-LR
- 10GBASE-ER

Не входящее в ключевые стандарты на основе телефонных пар:

- 2BASE-TL

61. Структурированные кабельные системы и их модели

СКС (Structured Cabling System (SCS)) здания либо сооружения - это упорядоченная по тем или иным критериям совокупность телекоммуникационных и силовых кабелей различного сетевого оборудования, а также соответствующих специализированных помещений.

Основой для построения любой СКС является древовидная топология, узлами которой служит сетевое оборудование определенного типа (distributors).

В связи с этим, технические помещения СКС (так же distributors) делят на два типа:

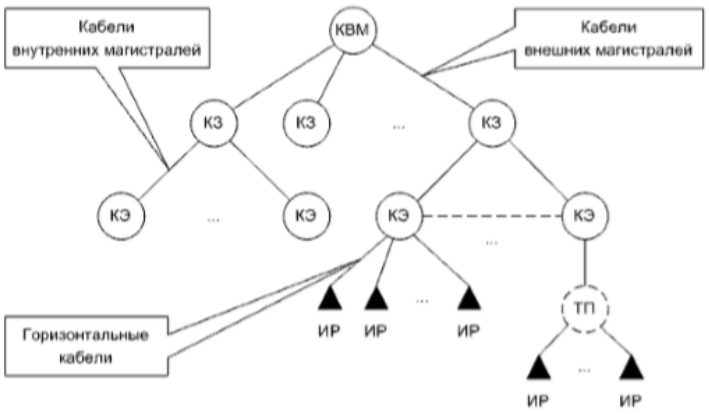
1. Кроссовые (telecommunications rooms)
2. Аппаратные (equipment rooms)

Аппаратные отличаются от кроссовых тем, что в них, наряду с активным, пассивным, монтажным и вспомогательным сетевым оборудование, может быть размещено серверное оборудование.

СКС включает в себя три подсистемы:

1. Подсистемы внешних магистралей (main, campus) - основа для организации связи между компактно расположенными на одной территории зданиями или сооружениями.
2. Подсистема внутренних магистралей или, по-другому, вертикальная (intermediate, building) - связывает между собой этажи одного здания или пространственно разнесенные помещения в одном здании
3. Горизонтальная подсистема (horizontal) - связывает между собой оборудование в пределах этажа или помещения.

Модели СКС



Где:

КВМ -- кроссовая внешних магистралей,

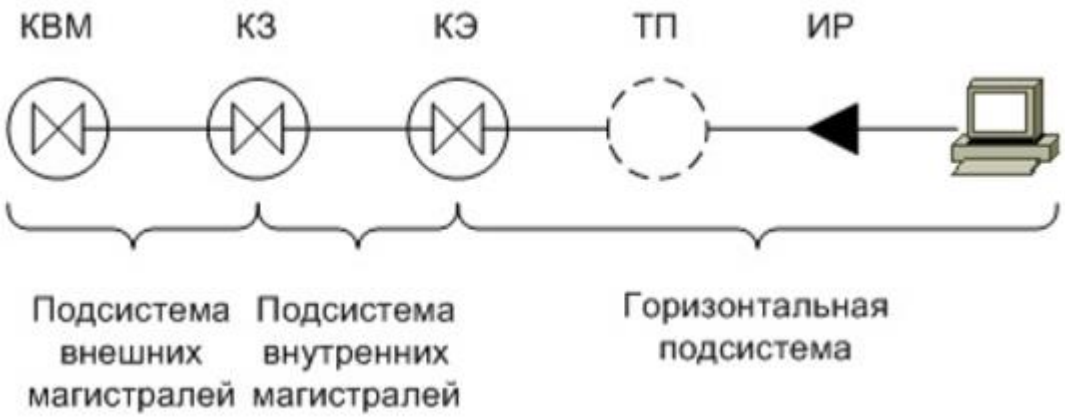
КЗ -- кроссовая здания,

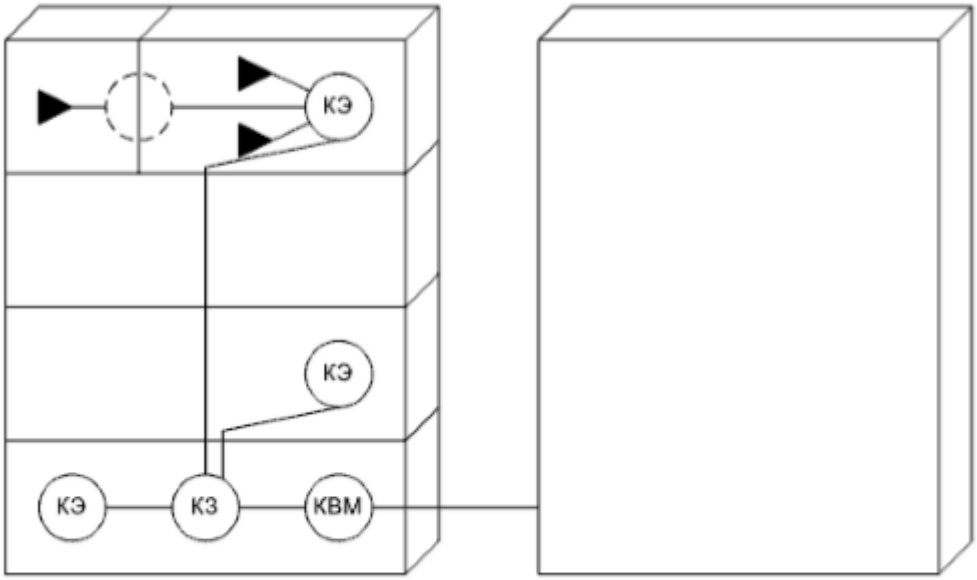
КЭ -- кроссовая этажа,

ТП -- точка перехода,

ИР -- информационная розетка рабочего места.

(Вместо кроссовых могут быть аппаратные. Пунктиром обозначены опциональные компоненты. Аббревиатуры -- нестандартные.)




КЭ
КЭ
КЭ
КЗ
КВМ

62. Питание и заземление в структурированных кабельных системах

При проектировании СКС внимание должно быть уделено подключению к силовым сетям, а также организации защиты посредством заземления, зануления или других способов.

Заземление необходимо для:

1. Предотвращения поражения электрическим током людей.
2. Защиты кабельных трактов и сетевого оборудования как от выхода из строя, так и от помех.
3. Обеспечения возможности прохождения сигналов применительно к некоторым видам сетевого оборудования.

В дополнение к основному контуру заземления (grounding electrode) здания либо сооружения, создают так называемый телекоммуникационный контур заземления или, по-другому, контуру рабочего заземления (telecommunication grounding/bonding)

Рекомендации стандартов по заземлению экранов кабелей (касается и витых пар):

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

Питание

Производится от сети общего потребления.

Относительно недавно производители сетевого оборудования стали разрабатывать технологии, позволяющие запитывать относительно маломощные Ethernet-устройства (например, коммутаторы или точки доступа) через информационные кабели (на основе витых пар). Постепенно были введены два общепромышленных стандарта: 802.3af и 802.3at. Но до сих пор многие производители используют собственные проприетарные технологии.

Примерами могут служить: Cisco Universal Power over Ethernet (UPOE) (до 802.3af была еще технология Inline Power), Microsemi PowerDsine (ряд производителей), Passive PoE (ряд производителей).

63. Пожарная безопасность структурированных кабельных систем

Согласно американским стандартам NEC (National Electrical Code) предусмотрены четыре уровня сертификации пожарной безопасности кабельных систем (первый уровень - высший):

1. Plenum – сюда относят кабели, которые можно без каких -либо ограничений прокладывать в так называемых plenum-полостях (существует приток воздуха, достаточный для постоянного горения).
2. Riser – сюда относят кабели, которые можно прокладывать в кабельных шахтах (например, вертикальных стояках зданий).
3. General purpose – сюда относят кабели, которые можно без дополнительной защиты прокладывать везде, кроме plenum-полостей и кабельных шахт.
4. Residential (limited use) – сюда относят кабели, на прокладку которых наложены специфические ограничения (например, только для жилых помещений).

В стандартах IEC 60332, UL 1685, EN 50266 и некоторых других описаны тесты вертикального и горизонтального распространения огня по кабелям.

64. Технология PoE

PoE (Power over Ethernet) - технологии, позволяющие запитывать относительно маломощные Ethernet-устройства (например, коммутаторы или точки доступа) через информационные кабели (на основе витых пар).

Постепенно были введены два общепринятых стандарта: 802.3af и 802.3at.

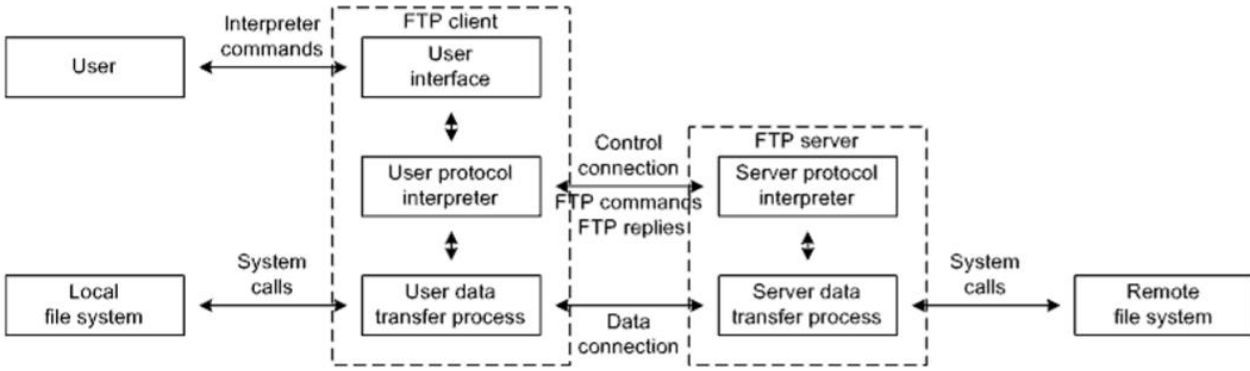
В структуру PoE-системы входит ряд блоков.

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

PSE может располагаться либо на конце (одном из двух) кабеля (endspan), то есть быть интегрированным в соответствующее сетевое устройство (как правило, мощный коммутатор, подключенный к силовой сети напрямую), либо «вклиниваться» в кабель (midspan), то есть быть внешним PoE-инжектором (PoE injector).

Иногда PoE используется и для запитывания «небольших» PD, PoE не поддерживающих, -- со стороны PD в кабель «вклинивается» PoE-DC адаптер.

65. Структура системы FTP



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

FTP-сервер обслуживает запросы *FTP-клиента* и работает на удаленной станции.

FTP-сервер выполняет системные вызовы к удаленной файловой системе.

На рисунке показана взаимосвязь между одним *FTP-клиентом* и одним *FTP-сервером*, но возможна также схема взаимодействия когда по инициативе *FTP-клиента* осуществляется файловый обмен между двумя FTP-серверами.

66. Протокол FTP и режимы обмена по протоколу FTP

Протокол FTP (File transfer protocol) – протокол прикладного уровня для передачи файлов, который базируется на клиент-серверной модели и использует транспорт TCP.

Является универсальным протоколом для пересылки между станциями, работающими под управлением различных ОС, возможно использующий различные файловые системы.

В отличие от многих других протоколов, FTP задействует не одно, а два соединения, значит для него зарезервированы два номера программных портов (на стороне FTP-сервера):

20 – информационное соединение (data connection).

21 – управляющее соединение (control connection).

Режимы обмена по протоколу FTP:

1. Stream – файл пересылается как непрерывный поток байтов (по умолчанию).

Если файл не имеет внутренней структуры, то прием метасимвола означает, что пересылка окончена; для случаев со сложной структурой предусмотрены специальные коды для и <EOR> и <EOF>

2. Block – файл пересылается в виде последовательности блоков, каждый из которых имеет заголовок, в котором записываются счетчик байтов и специальные коды; (поддерживается редко)

3. Compressed – файл пересылается в сжатом простейшими алгоритмами виде (поддерживается редко)

В зависимости от того, кто является инициатором:

1. *Активный режим* является рекомендуемым и наиболее используемым. Соединение инициируется клиентом, а соединение для передачи данных инициируется сервером. И поскольку сервер активно устанавливает соединение для передачи данных с клиентом, этот режим называется активным.

2. *Пассивный режим* обычно устанавливается принудительно. В режиме пассивного FTP-соединения сервер действует полностью пассивно, так как командное соединение и соединение для передачи данных инициируются и устанавливаются клиентом.

67. Структура и особенности системы Telnet

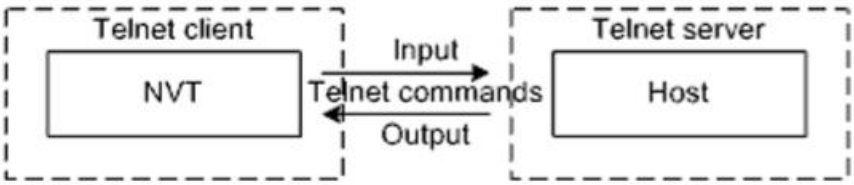
Telnet (Terminal Network) – это протокол, который обеспечивает корректную транспортировку символов потока ввода между NVT и хостом.

Соответствует клиент серверной модели и использует транспорт TCP. Задействует одно соединение. Стандартный номер порта Telnet-сервера - 23. Используется буферизация, в том числе чтобы излишне не загружать СПД.

2 режима работы:

- В режиме по умолчанию «набранные» символы отсылаются незамедлительно.
- В режиме linemode (RFC 1184) символы отсылаются после нажатия Enter.

Структура системы Telnet



Наиболее серьезным из недостатков Telnet является полная незащищенность соединения от несанкционированного доступа. Данные, в том числе и пароли, пересылаются в виде открытого текста (plain text). В современных условиях это не может устраивать любую организацию, даже некоммерческую.

68. Электронные письма и почтовые ящики

Электронные письма (emails) – сообщениями протоколов электронной почты.

Электронные письма имеют текстовую природу. Электронное письмо состоит из *конверта* (envelope) и *содержимого* (content). Содержимое, в свою очередь, состоит из *заголовка* (header) и *основного текста* (body).

Стандарты четко не ограничивают размеры электронного письма и его составных частей. Однако, в реализациях, размер содержимого обычно не должен превышать 64 килобайта, а общий объем (включая приложения) -- несколько мегабайтов.

Очень значимым расширением электронной почты является MIME (Multipurpose Internet Mail Extensions), позволяющее включать в основной текст электронного письма (и «прикреплять » к электронному письму) различные мультимедийные данные.

В настоящее время определены следующие MIME-типы:

1. text -- текст (основное содержимое письма, указывается кодировка, возможна 8-битная кодировка).

2. image -- изображение.

3. audio -- звук.

4. video -- видео.

5. application -- электронные данные, не подпадающие ни под один из других типов.

+6. multipart -- комбинация нескольких типов.

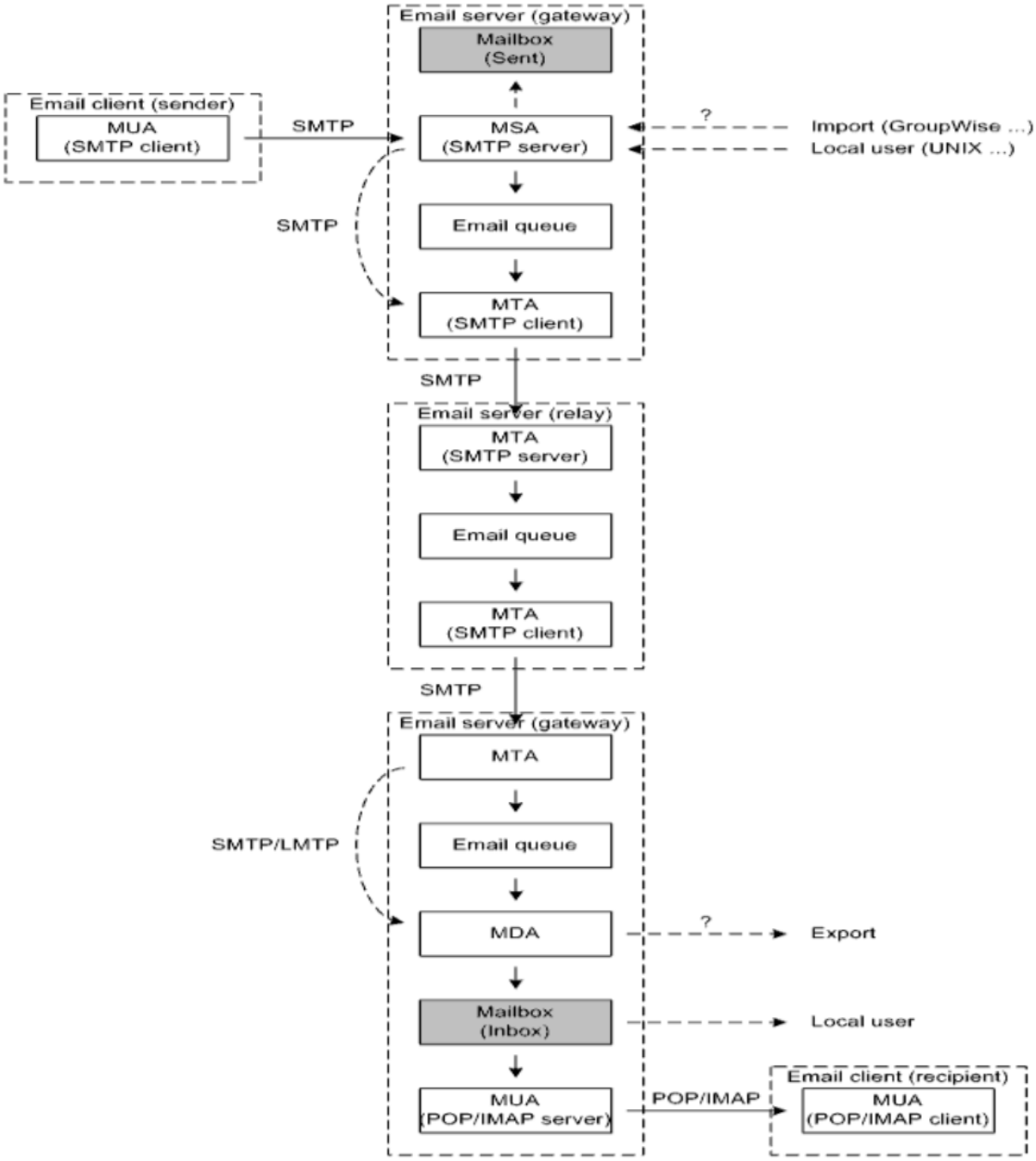
+7. message -- письмо в письме либо внешнее приложение к письму (attachment). Каждый из типов имеет некоторое количество подтипов

Электронные почтовый ящик – файловое хранилище для электронных писем.

Почтовые ящики могут быть расположены как на выделенных для этого почтовых серверах (удаленные), так и на пользовательских станциях (локальные).

Фактически, в системе электронной почты адресуют именно почтовые ящики.

70. Обобщенная структура системы электронной почты


Email server (gateway)
Mailbox
(Sent)
Email client (sender)
MUA
(SMTP client)
SMTP
MSA
(SMTP server)
?
Import (GroupWise ...)
Local user (UNIX ...)
Email queue
SMTP
MTA
(SMTP client)
SMTP
Email server (relay)
MTA
(SMTP server)
Email queue
MTA
(SMTP client)
SMTP
Email server (gateway)
MTA
Email queue
SMTP/LMTP
MDA
?
Export
Mailbox
(Inbox)
Local user
Email client (recipient)
MUA
(POP/IMAP server)
POP/IMAP
MUA
(POP/IMAP client)