СОДЕРЖАНИЕ

1 Понятие компьютерной сети ... 2
2 Классификация компьютерных сетей ... 3
3 Стандарты компьютерных сетей ... 4
4 Наиболее распространенные модели компьютерных сетей ... 5
5 Физический уровень модели OSI ... 7
6 Канальный уровень модели OSI ... 8
7 Сетевой уровень модели OSI ... 9
8 Транспортный и сеансовый уровни модели OSI ... 10
9 Прикладной уровень и уровень представления модели OSI ... 11
10 Семейство протоколов TCP/IP ... 12
11 Эволюция COM-портов и их место в современных ПК ... 13
12 Структура COM-портов ПК ... 15
13 Цепи RS-232 и их использование ... 16
14 Ассинхронный режим работы com-порта ... 18
15 Синхронный режим работы com-порта ... 19
16 Тактирование com-порта ... 20
17 Архитектура COM-портов ПК ... 21
18 Стандарты, близкие к RS-232 ... 22
19 Структура типового пакета компьютерной сети ... 23
20 Инкапсуляция и ее проявления в компьютерных сетях ... 24
21 Бит-стаффинг ... 25
22 Байт-стаффинг ... 26
23 Особенности линейного кодирования и классификация линейных кодов, применяемых в компьютерных сетях ... 27
24 Линейные коды без возврата к нулю и с возвратом к нулю ... 28
25 Манчестерские и многоуровневые линейные коды ... 29
26 Блочные линейные коды ... 31
27 Поля Галуа и их применение в компьютерных сетях ... 32
28 Модель помехоустойчивого канала связи и теорема Шеннона ... 33
29 Линейные помехоустойчивые коды, включая коды Хэмминга и циклические коды ... 34
30 Классификация помехоустойчивых кодов ... 36
31 Классификация каналов в сети передачи данных ... 37
32 Логические и физические топологии LAN ... 38
33 Логические и физические топологии WAN и RAS ... 39
Инфа про то, зачем нам нужны вообще какие-то методы доступа к какому-то моноканалу к 34 вопросу ... 40
34 Особенности случайных методов доступа к моноканалу ... 41
35 CSMA/CD (Ethernet) ... 42
36 Кадр Ethernet ... 44
37 CSMA/CA (Wi-Fi) ... 45
38 Кадры Wi-Fi ... 47
39 Особенности детерминированных методов доступа к моноканалу ... 49

40 Алгоритм Token Ring 50
Про формат кадров Token Ring и назначение основных полей. 52
41 Реализации детерминированных методов доступа к моноканалу 55
42 Адресация в компьютерных сетях и классификация адресов 57
43 MAC-адреса 59
44 Заголовок IPv4 61
45 Заголовок IPv6 62
46 Протокол ARP 63
47 Структура системы DNS 64
48 Сообщения DNS 65
49 Виртуальные соединения в сети передачи данных 68
50 Классификация оконных механизмов, используемых в сети передачи данных 69
51 Структура системы TCP 70
52 Заголовок TCP 71
53 Протокол TCP 72
54 Усовершенствования протокола TCP 74
55 Протокол UDP и заголовок UDP 75
56 Классификация и характеристики сред передачи данных 76
57 Среды передачи данных на основе коаксиальных кабелей 77
58 Среды передачи данных на основе витых пар 78
59 Среды передачи данных на основе оптоволоконных кабелей 79
60 Физический уровень Ethernet 80
61 Структурированные кабельные системы и их модели 81
62 Питание и заземление в структурированных кабельных системах 83
63 Пожарная безопасность структурированных кабельных систем 85
64 Технология PoE 86

1 Понятие компьютерной сети

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

Любую КС можно рассматривать с двух точек зрения:

1. Программной
2. Аппаратной

В основе любой КС лежит так называемая сеть передачи данных (СПД), которая может задействовать различные среды передачи данных (СрПД). Иногда в составе СПД выделяют базовую (опорную) СПД.

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

1.Оконечные - находятся по периметру СПД (ООД – оконечное оборудование данных)

2.Посредники - составляют ядро СПД (АПД – аппаратура передачи данных)

Весь трафик в СПД традиционно разделяют на три базовых типа:

1.Обычные компьютерные данные (data)

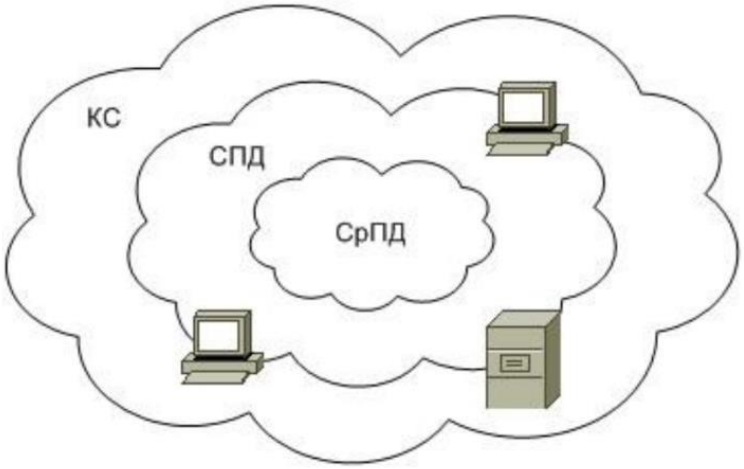
2.Голос (voice)

3.Видео (video)

Каждый тип обладает характерными особенностями. СПД, поддерживающие пересылку разнородного трафика, в нотации Cisco называют конвергированными (converged networks)

Особенности трафика обеспечиваются так называемым качеством обслуживания Quality of Service (QoS).

Традиционные виды компьютерных данных без исключения, по умолчанию, обслуживаются по принципу «Все делается для доставки пакетов, но при этом ничего не гарантируется» (best efforts), что, по сути, является отсутствием QoS. Гарантии «возникают» при работе с голосом и видео.



2 Классификация компьютерных сетей

С одной стороны, выделяют:

1.Local Area Networks (LANs) - локальные КС (ЛКС)

2.Wide Area Networks (WANs) - глобальные КС (ГКС)

3.Metropolitan Area Networks (MANs) - городские КС

4.Personal Area Networks (PANs) - личные КС

5.Remote Access Services (RASes) - КС для подключения удаленных пользователей (teleworkers)

6.Data Center Networks КС - центров обработки данных

7.Home Networks – Домашние КС

8.Industrial Networks - промышленные КС

С другой:

1.Intranets - внутренние КС предприятий и организаций

2.Internets - КС публичного доступа

LAN выделяют прежде всего территориально - в современном понимании, охватывает территорию не более кампуса, но при этом подразумевают определенные технологии.

WAN выделяют прежде всего технологически и, в общем случае, может охватывать произвольную территорию.

MAN представляет собой промежуточный вариант между LAN и WAN.

PAN позволяет подключить к компьютеру периферийные устройства.

RAS существует в контексте WAN.

Home, Industrial и Datacenter Networks являются специализированными вариантами LAN.

Intranet обычно выделяют по ведомственной принадлежности пользователей.

Практически все Internets сейчас интегрированы в одну сборную одноименную сеть.

Intranet почти всегда имеет связь с Internet. Кроме того, сети могут быть:

1.Изолированными (isolated)

2.Открытыми для прослушивания (open)

С точки зрения организации взаимодействия КС могут быть:

1.Сильносвязанными

2.Слабосвязанными

В случае сильносвязанной КС подразумевают наличие так называемой хост-ЭВМ (host) с одной стороны и терминала (terminal) - с другой. Мы имеем дело с хост-терминальной моделью.

В случае слабосвязанной КС подразумевают наличие сервера (server) с одной стороны и клиента (client) - с другой. Мы имеем дело с клиентсерверной моделью.

По типу коммутации:

1.Канальная

2.Пакетная

3 Стандарты компьютерных сетей

Стандарт - это набор правил и соглашений, используемых при создании локальной сети и организации передачи данных с применением определенной топологии, оборудования, протоколов и т. д.

Все стандарты, в том числе в области КС, делят на:

1)Международные (например, ISO/IEC)

2)Европейские (например, EN)

3)Американские (например, ANSI/TIA/EIA)

Стандарты лишь формализуют определенные требования в той или иной предметной области. Стандарты могут носить предварительный или временный характер. Могут включать дополнения и списки обнаруженных ошибок. Могут устаревать или замещаться другими стандартами.

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

Сертификация позволяет определить факт соответствия стандарту. В 1980 г при IEEE был создан специальный комитет по стандартизации КС, результатом работы которого стало множество стандартов 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 включительно

2)Fast Ethernet - 100 Mbit/s

3)Gigabit Ethernet – 1, 10, 100, 40, 25, Gbit/s и Multigigabit

Организации работающие со стандартизацией КС:

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

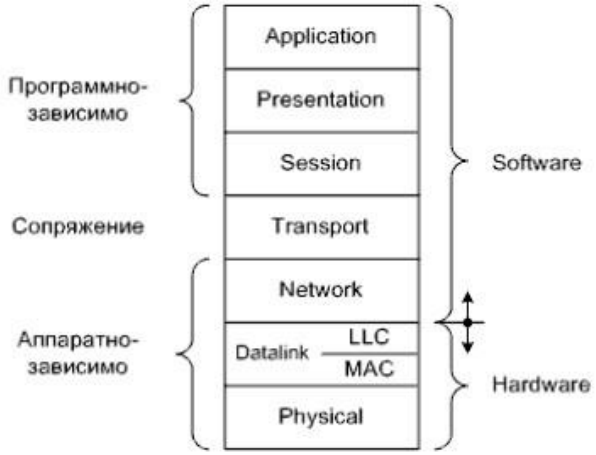
В локальных КС, за разработку сетевых стандартов отвечает комитет 802 под эгидой IEEE.

Наиболее известными подкомитетами являются следующие:

- IEEE 802.1. - Данный подкомитет занимается разработкой стандартов межсетевого взаимодействия и управления сетевыми устройствами.
- IEEE 802.3. - Данный подкомитет занимается разработкой стандартов для проводных сетей стандарта Ethernet, которые для доступа к среде передачи данных используют метод множественного доступа с контролем несущей частоты и обнаружением коллизий CSMA/CD.
- IEEE 802.11. Этот комитет разрабатывает стандарты и правила функционирования устройств в беспроводных локальных сетях, которые работают с частотами 2,4; 3,6 и 5 ГГц. (Wi-Fi)

4 Наиболее распространенные модели компьютерных сетей

Из всех моделей КС наиболее фундаментальной является открытая модель взаимодействия систем - Open System Interconnection (OSI) разработанная ISO. OSI – модель, определяющая разные уровни взаимодействия систем, дает им стандартные имена и указывает, какую работу должен делать каждый уровень. Модель включает 7 уровней.



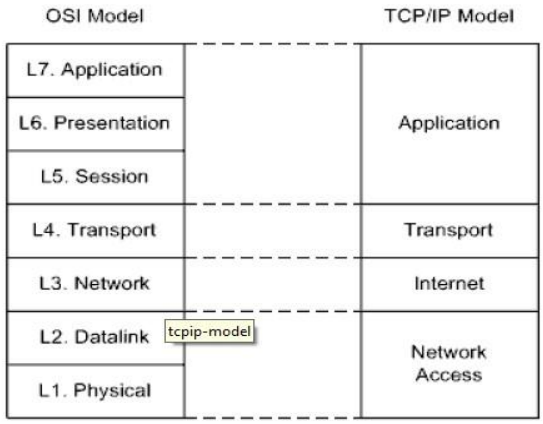
На вершине иерархии находится человек, но абонентами КС являются взаимодействующие программы.

Взаимодействие в рамках модели OSI может быть вертикальным (обеспечивает работу между соседними уровнями на одном устройстве) и горизонтальным (обеспечивает связь программ и процессов на различных устройствах).

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

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

И в том, и в другом случае предполагают определенную абстракцию. Ещё одна модель связана с семейством протоколов TCP/IP Её сопоставление с моделью OSI на след рисунке.



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

1.Access – доступ

2.Distribution (иногда aggregation) – распределение

3.Core – ядро

Уровень доступа предназначен для обеспечения подключений к КС оконечных пользователей. Особое внимание здесь уделяют предоставлению пользователям требующихся им ресурсов.

Уровень распределения предназначен для обеспечения взаимодействия в пределах групп пользователей. Особое внимание здесь уделяют резервированию соединений.

Уровень ядра предназначен для обеспечения высокоскоростной связи между относительно удаленными группами пользователей. Особое внимание здесь уделяют характеристикам трафика.

На всех уровнях значительное место отведено разграничению трафика с целями защиты пользователей друг от друга и защиты КС от пользователей.

При этом всем, технологии могут быть различными. Догм нет. В настоящий момент самая популярная из пропагандируемых Cisco архитектур – Cisco Borderless Network.

5 Физический уровень модели OSI

На физическом (physical) уровне формализуют подключение того либо иного сетевого устройства к СрПД. В пространстве физический уровень охватывает «точку» подключения.

Специфическими понятиями физического уровня являются:

1)Среда

2)Разъём (физический порт)

3)Несущая (частота)

4)Модуляция

5)Сигнал

Фундаментальная задача уровня заключается в передаче сигнала.

Для передачи сигнала используется несущая и её модуляция.

Несущая – частота гармонических электрических (электромагнитных) колебаний, служащих переносчиком информации при ее передаче посредством модуляции этих колебаний сигналами, соответствующими передаваемому сообщению.

Модуляция – процесс изменения одного или нескольких параметров несущего высокочастотного колебания в соответствии с изменением параметров передаваемого сигнала.

Сигнал – материальное воплощение сообщения для использования при передаче обработке и хранении информации.

Функции физического уровня реализуются на всех устройствах, подключенных к сети. Со стороны компьютера функции физического уровня выполняются сетевым адаптером или последовательным портом.

Физический уровень определяет такие виды сред передачи данных как оптоволокно, витая пара и т. д.

Стандартными типами сетевых интерфейсов, относящимися к физическому уровню, являются:

- RS-232
- RS-485
- Функции физического уровня модели OSI:
- Побитовая доставка
- Физическое кодирование (способ представления данных в виде импульсов)
- Адресация на основе уникальных MAC-адресов
- Предоставления протокола множественного доступа

6 Канальный уровень модели OSI

Канальный (datalink) уровень определяет взаимодействие станций в пределах сегмента. Полученные с физического уровня данные в битах он упаковывает в кадры, проверяет их на целостность и, если нужно, исправляет ошибки (либо формирует повторный запрос поврежденного кадра) и отправляет на сетевой уровень.

Сегмент (segment) – множество станций, объединенных посредством одной СрПД, то есть «видящих» друг друга непосредственно.Технологически сегменты могут быть самыми разными. Физически любая КС состоит из некоторого, большего или меньшего, количества сегментов. В традиционном понимании СрПД соответствует физическому соединению (link). Но многие современные технологии предполагают опциональное или обязательное наличие в СрПД «прозрачных» устройств-посредников, таких как преобразователи сред или коммутаторы.

Станция (узел) – любое устройство, способное передавать или принимать сетевой трафик: ПК, сервер, маршрутизатор и так далее.

Специфическими понятия канального уровня являются:

1)Сегмент сети

2)Физическая и логическая топология сегмента

3)Пакет(кадр)

4)Бит- и байт-стаффинг

5)Адресация в пределах сегмента

6)Канальный код

7)Код проверки целостности сегмента (кадра)

8)Алгоритм доступа к моноканалу

Канальный уровень разделяют на два подуровня:

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

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

На подуровне MAC, более низком, выполняется взаимодействие с физическим уровнем, то есть средозависимые операции, такие как формирование и распознавание пакетов, адресация, канальное кодирование и другие.

На подуровне LLC, более высоком, выполняется взаимодействие с сетевым уровнем, то есть средонезависимые операции, такие как разбиение данных на пакеты, сборка данных из пакетов, определение соответствующей подсистемы сетевого уровня и другие.

На этом уровне работают коммутаторы, мосты и другие устройства.

Эти устройства используют адресацию второго уровня (канальный уровень). Протоколы канального уровня:

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

7 Сетевой уровень модели OSI

Сетевой уровень позволяет «выйти» за пределы сегмента.

На *сетевом* (network) уровне формализуют построение полноценной КС произвольного масштаба, охватывающей произвольное количество сегментов.

Специфическими понятиями сетевого уровня являются:

-- пакет (собственно пакет);

-- адресация в пределах всей КС;

-- маршрутизация.

Маршрутизация – поиск маршрута доставки пакета между сетями через транзитные узлы (маршрутизаторы).

Адресация в глобальных КС основана на протоколе IP.

8 Транспортный и сеансовый уровни модели OSI

Транспортный уровень позволяет перейти от оборудования к программам.

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

Специфическими понятиями транспортного уровня является:

1)Пакет (сегмент сообщения)

2)Программный порт

3)Логическое соединение

4)Надёжность доставки

5)Алгоритм борьбы с заторамиСПД

Пример протоколов: TCP, UDP.

Сеансовый или сессионный (session) уровень позволяет предоставить доступ к транспорту всем программам в многозадачном окружении.

Специфическими понятиями транспортного уровня является:

1)Сессия

2)Программный порт

3)Алгоритм мультиплексирования программ

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

9 Прикладной уровень и уровень представления модели OSI

Прикладной (application) уровень призван решать конкретные пользовательские задачи с помощью КС. Предназначен для решения таких задач, как:

1)Пересылка файлов между компьютерами

2)Пересылка электронных писем

3)Поддержка удаленных текстовых и графических терминалов, в том числе для администрирования

4)Пересылка мультимедийных документов

5)Обмен мгновенными сообщениями

6)Совместная разработка чего-либо

Специфических понятий прикладного уровня великое множество, и они зависят от решаемых задач.

К протоколам прикладного уровня относятся: HTTP, FTP, RDP.

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

Основными задачами уровня представления являются:

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

2)Шифрование информации с целью обеспечения её защиты при пересылке по открытым для прослушивания сетям.

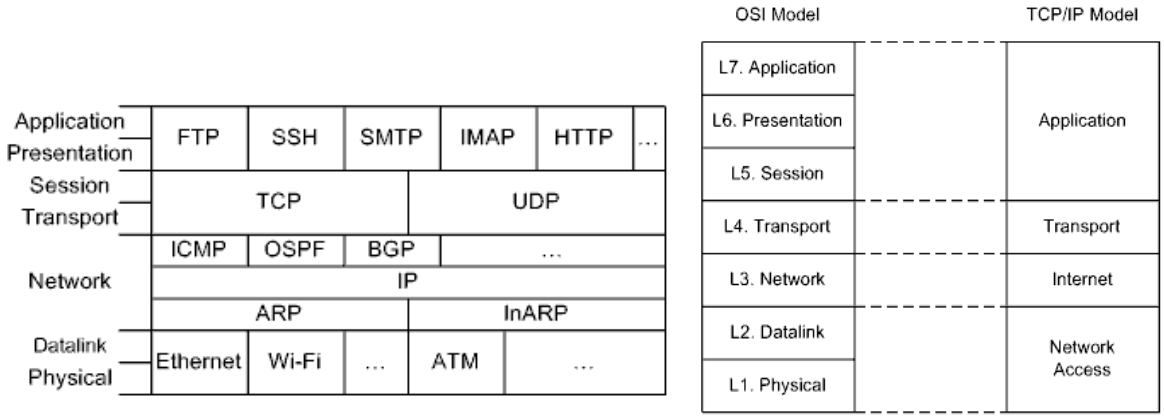
Поскольку обычно уровень представления «привязан» к прикладному уровню, в реализациях эти уровни часто совмещаются.

10 Семейство протоколов TCP/IP

Разделение протоколов по уровням:

- Прикладной уровень и Уровень представления: FTP, SMTP, SSH, HTTP.
- Транспортный и сеансовый: TCP, UDP.
- Сетевой уровень: ICMP, OSPF, IP, ARP, RARP.
- Физический и канальный: Ethernet, Wi-Fi, ATM.

Семейство протоколов TCP/IP описано в стандартах RFC (Request For Comments). С семейством протоколом TCP/IP связана одноименная модель.



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

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

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

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

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

11 Эволюция COM-портов и их место в современных ПК

В развитии COM-порта ПК можно выделить следующие основные этапы:

1)В семидесятые годы XX века, компания Intel разработала два контроллера последовательного порта. Один из них, 8250, получил название UART (Universal Asynchronous Receiver/Transmitter). Второй, 8251, получил название USART (Universal Synchronous/Asynchronous Receiver/Transmitter). Эти контроллеры были рассчитаны на подключение по шине X-Bus (шина ввода-вывода, внутрисхемный восьмибитный предшественник системной шины ISA) и поэтому без труда были перенесены в первые ПК на базе процессора 8086 и его модификаций с тогда наиболее распространенной системной шиной ISA. Микросхема UART либо USART устанавливалась на плату специального адаптера и подключались к материнской плате ПК посредством разъема системной шины. В это же время возникла традиция устанавливать последовательные порты парами (COM1 и COM2).

2)Времена доминирования процессоров 80286. В СССР был создан аналог 8251 под названием КР580ВВ51А. На Западе же, наоборот, развитие получила микросхема 8250. Апофеозом достаточно быстрого усовершенствования 8250 стали несколько UART, среди которых следует выделить 16550 разработки National Semiconductor. Именно эта микросхема стала де факто стандартной на длительное время (архитектурная совместимость сохраняется вплоть до настоящего времени). 16550 имеет два основных преимущества перед 8250:

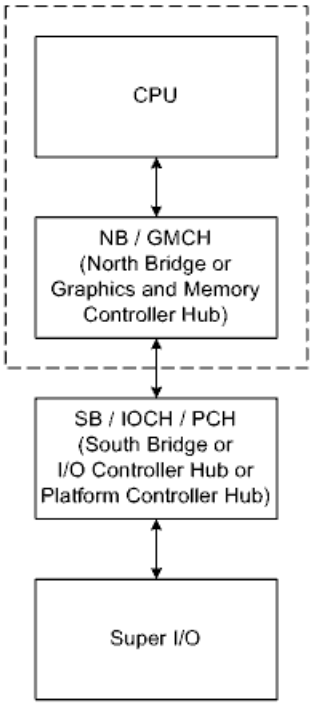
- более высокая пропускная способность последовательного интерфейса (максимальная стандартная пропускная способность увеличена с 9600 baud до 115200 baud);
- возможность буферизации (две очереди FIFO по 16 байт -- на стороне передатчика и на стороне приемника).

3) В дальнейшем интеграционные процессы привели к появлению так называемых мультикарт -- подключаемых посредством разъема системной шины (по-прежнему обычно ISA) плат расширения с интегрированными контроллерами: последовательного порта (2x16550), параллельного порта, игрового порта, НГМД и НЖМД. Причем все эти функции сочетались в одной большой интегральной схеме (БИС) с типичным названием Multi I/O.

4) Для ПК на базе поздних Intel486 уже была характерна интеграция чипа Multi I/O на материнскую плату.

5) Во времена процессоров Pentium сформировалась действительная до сих пор базовая крупноблочная структура материнской платы ПК, состоящая из четырех основных БИС. Контроллеры последовательного порта (по той же схеме 2x16550) в составе интегрированной периферии были перенесены и в эту структуру. Однако, в связи с некоторой заменой функционала интегрированной периферии (например, удаление контроллера НЖМД и добавление контроллера клавиатуры), вместо названия Multi I/O стало

больше использоваться название Super I/O. С этого момента реализации последовательных портов не претерпели никаких изменений.



После перехода от мостовой (bridges) организации ПК к хабовой (hubs) в рамках данной структуры (начиная с восьмисотой серии чипсетов Intel в эпоху Pentium III) для внутрисхемного подключения Super I/O вместо шины X-Bus стала использоваться шина LPC (Low Pin Count) – специализированная разновидность шины PCI с небольшим числом разрядов

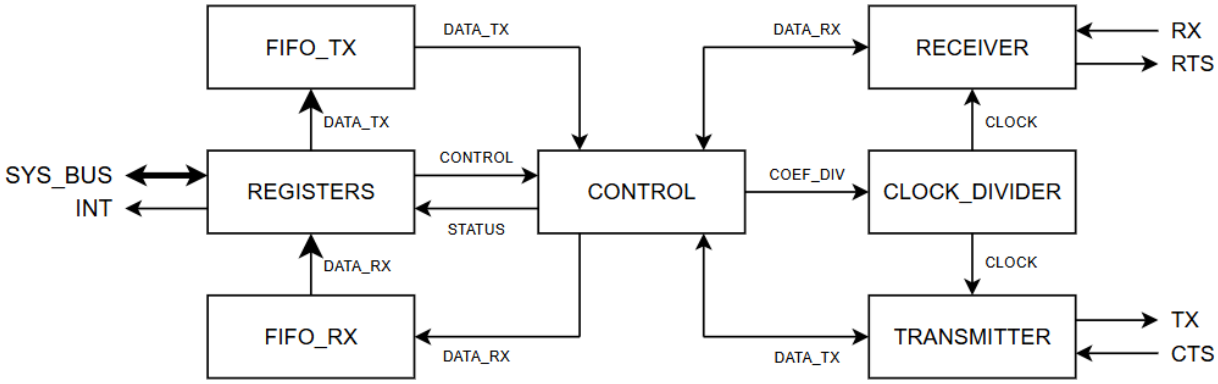
6) В настоящее время (приблизительно с 2005 года) традиционный последовательный интерфейс ПК считают устаревшим (legacy), часто исключают из состава интегрированной периферии. Однако возобновлено производство мультикарт -- новые версии представляют собой платы расширения с интерфейсом PCI. Сейчас в качестве основного последовательного интерфейса ПК рассматривают шину USB (Universal Serial Bus), впервые введенную в состав ПК еще в эпоху процессоров Pentium.

12 Структура COM-портов ПК

Сам факт передачи информации подразумевает наличие передатчика, приемника и канала, по которому они связаны. Как и следует из названия, UART 16550 сочетает в себе функции как приемника, так и передатчика. Предоставлена возможность подключения к двунаправленному физическому каналу связи (или, по-другому, линии) в соответствии со стандартом RS-232.

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.

В Структуру com-порта входит сама шина данных, приёмный и передающий буффер, программируемые бод-генератор для тактирования, множество регистров (информационные, служебные, управляющие).



13 Цепи RS-232 и их использование

Традиционное назначение цифровых цепей RS-232:

1)SOUT (Serial Output) - выход передатчика;

2)SIN (Serial Input) - вход приемника;

3)RTS (Request to Send) - сигнал-запрос от UART к модему о передаче байта;

4)CTS (Clear to Send) - сигнал-подтверждение от модема к UART о готовности принять байт для передачи;

5)DSR (Data Set Ready) - сигнал от модема к UART о готовности к взаимодействию;

6)DTR (Data Terminal Ready) - сигнал от UART к модему о готовности к взаимодействию;

7)DCD (Data Carrier Detect) - сигнал от модема к UART об обнаружении данных;

8)RI (Ring Indicator) - сигнал от модема к UART об обнаружении входящего телефонного звонка.

9)GND

Служебные цепи RS-232 позволяют организовать контроль информационного потока (flow control). Например, это позволяет избегать переполнения приемника, приостанавливая «быстрый» передатчик. Следует отметить, что практически все служебные цепи напрямую связаны с соответствующими регистрами управления и состояния UART 16550, то есть «открыты» для программирования. Следовательно, алгоритмы контроля реализуют программно и закладывают, например, в драйверы операционных систем.

Контроль может быть как полуаппаратным (с задействованием сигналов RS-232), так и сугубо программным.

Очевидно, что традиционное использование пары RTS/CTS позволяет контролировать передачу только в одном направлении -- от UART к модему. Для контроля передачи в обратном направлении использовалась пара DSR/DTR. В большинстве современных реализаций контроль по прежнему предполагает наличие обратной связи, но осуществляется только приемником. Два основных метода:

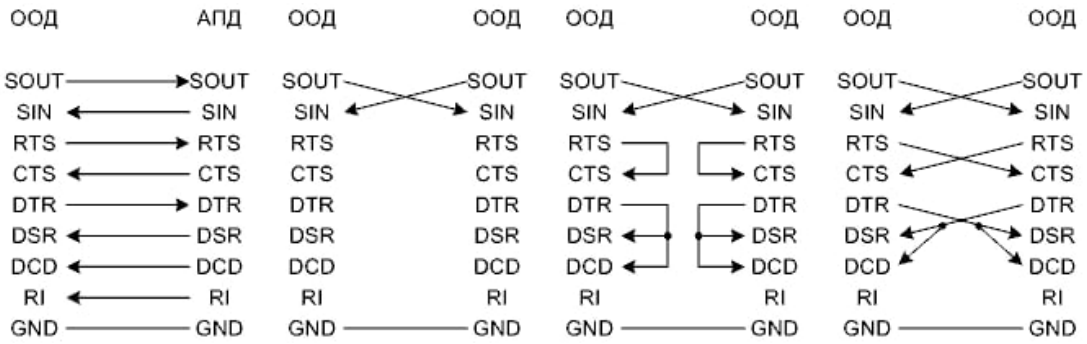
1. RTS/CTS -- полуаппаратный.

2. XON/XOFF -- программный.

UART контролирует передачу данных «к себе» управляя активностью цепи RTS, модем -- CTS.

Значительно реже применяют метод DTR/DSR -- полностью аналогичен методу RTS/CTS, но значения сигналов сохраняются на протяжении всего информационного обмена, а не каждой посылки.

При полностью программном контроле, приемник передает в обратном направлении специальный байт XON (стандартное значение 11h) для инициирования передачи и специальный байт XOFF (стандартное значение 13h) для остановки передачи.

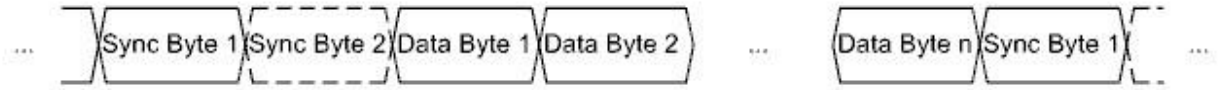

ООД
АПД
SOUT
SIN
RTS
CTS
DTR
DSR
DCD
RI
GND
ООД
ООД
ООД
ООД
ООД
ООД

14 Ассинхронный режим работы com-порта

Атомарной, то есть минимальной неделимой единицей, с которой работает как UART, так и USART, является байт, причем один байт не обязательно равен восьми битам и может содержать от 5 до 8 битов. По умолчанию линия находится в состоянии логической единицы. При наличии байта для передачи передатчик переводит линию в состояние логического нуля, то есть передает старт-бит, что говорит приемнику о том, что на следующем такте нужно «ловить» первый информационный бит. 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. 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. Ошибки отслеживаются приемником.

15 Синхронный режим работы com-порта

При «простое» передатчик «заполняет» линию специальными байтами синхронизации, тем самым настраивая приемник. Все поступающие байты передаются без «обрамления». Как и в асинхронном режиме, ошибки отслеживаются приемником. При обнаружении ошибок, а при длительной непрерывной передаче из-за накапливающихся фазовых сдвигов они неизбежно возникают, приемник должен каким-либо дополнительным способом (так как текущую цепь задействовать невозможно) приостановить передатчик, чтобы тот вновь «заполнил» линию байтами синхронизации.



16 Тактирование com-порта

Тактирование сдвиговых регистров UART 16550 осуществляется с помощью встроенного программируемого бод-генератора (baud generator) (тактирование некоторых первых реализаций UART осуществлялось таймером). Бод-генератор представляет собой программируемый делитель частоты. Выходная частота бод-генератора Fout определяется по формуле: Fout = Fin / (16 DL), где Fin -- входная частота, DL -- шестнадцатибитная константа, старшая и младшая части которой хранятся в двух регистрах UART (DLL и DLM).

На вход бод-генератора поступает меандр, получаемый от внешнего кварцевого резонатора, который тактирует и сам автомат UART. Частота тактирования автомата UART по крайней мере в 16 раз больше Fout. Следует учитывать, что, для того чтобы правильно рассчитать DL, необходимо точно знать Fin. Вполне естественно, что на разных материнских платах используют разные микросхемы и разные кварцевые резонаторы. Применительно к современным Super I/O, эта частота может достигать 48 MHz, то есть совпадать с частотой синхронизации Super I/O. Но, за счет еще одного деления частоты (при загрузке ПК BIOS конфигурирует UART инициализируя соответствующие регистры конфигурационного пространства Super I/O), как правило, Fin приводится к классическому значению 1,843 MHz. При этом, если DL = 1 (нулевое значение DL использовать крайне не рекомендуется), то Fout = 115200 Hz.

Пропускную способность последовательных каналов связи принято оценивать в бодах. Один бод (baud) равен одному сигналу в секунду.

В случае с UART 16550 производительность, измеренная в бодах, совпадает с производительностью, измеренной в битах в секунду (bit/s равно bps).

17 Архитектура COM-портов ПК

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

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

Отображение частично зависит от значения Divisor Latch Access Bit (DLAB) -- самого старшего (седьмого) бита регистра LCR.

Назначение регистров:

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

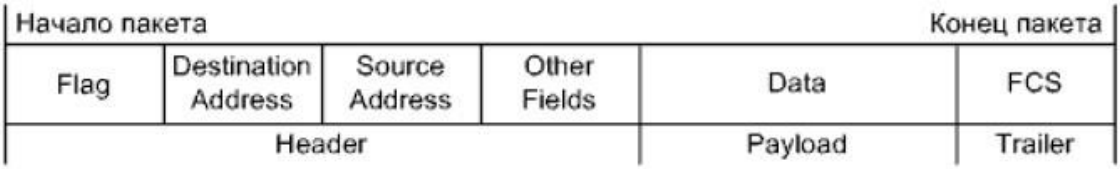
В результате, закономерным продолжением стандарта RS-232 стали два стандарта: RS-422 и RS-485. При этом RS-422 можно рассматривать как промежуточный на пути к RS-485 стандарт. Сравнение основных характеристик упомянутых стандартов приведено в таблице.

Основные сравнительные характеристики RS-232, RS-422 и RS-485

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

Для передачи данных посредством интерфейса RS-485 требуются специальные трансиверы с гальванической развязкой, позволяющие реализовать дифференциальный способ передачи сигнала. Гальваническая развязка может быть либо трансформаторной, либо оптронной. О СрПД в стандарте не сказано, но, как правило, используют витую пару (twisted pair) и разъемы типа RJ.

19 Структура типового пакета компьютерной сети



Назначение полей:

Flag - флаг начала пакета

Destination Address - адрес назначения

Source Address - адрес источника

Other Fields - прочие поля - специфические поля (в том числе и специфические флаги) определенной реализации.

Data – данные - «полезное» наполнение пакета

FCS (Frame Check Sequence) - контрольная сумма – позволяет проверить целостность пакета.

Часть пакета, включающую поля, расположенные до начала данных, принято называть заголовком (header) пакета, после данных – хвостовиком (trailer).

Обычно в байт ориентированных реализациях длина пакета кратна восьми битам, то есть пакет состоит из так называемых октетов.

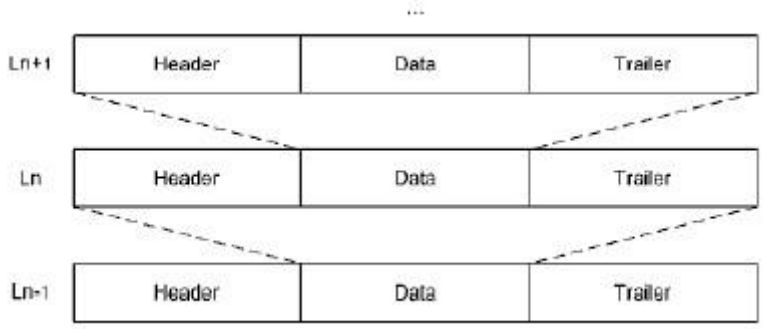
Все поля в составе любого пакета можно условно разделить на полезные и служебные. Полезная нагрузка заключается в собственно данных. Но следует понимать, что вкладываемая в качестве данных информация может носить служебный характер. В некоторых пакетах поле данных не предусмотрено вообще.

Сколько дополнительного трафика порождается в связи с наличием служебных полей оценивают, как overhead.

20 Инкапсуляция и ее проявления в компьютерных сетях

В соответствии с концепцией модели OSI, соседние уровни абстрагированы друг от друга. Поэтому вполне закономерно, что на каждом уровне работают со своими структурами данных. При продвижении информации между уровнями возникает необходимость в преобразованиях структур данных. Преобразования выражаются в инкапсуляции и декапсуляции.

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



Функционал любого из вышестоящих уровней «знает», какие нижестоящие ресурсы ему необходимы и чем он «располагает». Поэтому процесс инкапсуляции не доставляет трудностей. А вот функционал нижестоящего уровня при разборе полученных пакетов заранее не знает, какой из вышестоящих подсистем передавать эти пакеты.

Проблему решают введением в структуру пакета служебного поля, в котором записывается код протокола вышестоящего уровня.

Важной особенностью инкапсуляции является то, что в большинство реализаций заложена возможность передавать пакеты, относящиеся к некоторому протоколу некоторого уровня, вкладывая их в пакеты другого протокола того же уровня, то есть организовывать туннелирование (применяется для защищенных каналов и передачи стороннего трафика).

Если при выполнении инкапсуляции данные некоторого уровня не помещаются в поле отведенной длины, то можно прибегнуть к фрагментации - разбить данные на фрагменты и передать цепочку пакетов. Принимающая сторона будет вынуждена выполнить дефрагментацию.

Перемежение позволяет «распараллелить» пересылку пакетов или их фрагментов и заключается в одновременном задействовании нескольких каналов. Особенно это применимо в низкоскоростных СрПД.

Фрагментация (при наличии альтернативных путей в СПД) и перемежение могут привести к «перемешиванию» пакетов и, как следствие, разрушению сообщения. Контроль за порядком фрагментов может быть возложен как на протокол подверженного фрагментации уровня, так и на протокол вышестоящего уровня.

21 Бит-стаффинг

При бит-стаффинге совпадающая с флагом последовательность разбивается с помощью вставки дополнительно бита с соответствующим значением.

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

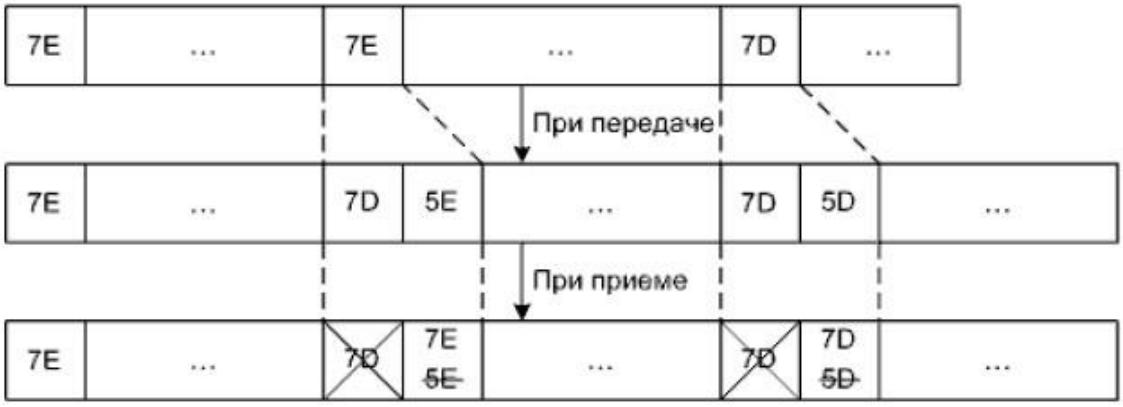
На передающей стороне после нуля и шести единиц всегда вставляется седьмая единица, а на принимающей стороне единица после нуля и шести единиц всегда удаляется.

Бит-стаффинг используется при задействовании **синхронных** СрПД.

Битстаффинг, в отличие от байт-стаффинга, обычно реализуют аппаратно.

22 Байт-стаффинг

В сравнении с алгоритмами бит стаффинга, алгоритмы байт стаффинга манипулируют байтами, являются более сложными и более «затратными», но при программировании они позволяют избежать битовых операций (битстаффинг, в отличие от байт-стаффинга, обычно реализуют аппаратно).



Единственным способом обеспечения уникальности флагового байта является замена совпадающего с ним байта на некий выбранный другой. Но возникает вопрос, как принимающая сторона отличит замененный байт от такого же не заменённого. Решением является применение так называемого ESC символа. Наличие ESC символа говорит станции приемнику о факте замены, а следующий за ESC символом символ код замены позволяет определить какая замена была осуществлена. Байт-стаффингу можно подвергать целые группы символов.

Байт-стаффинг применяют при задействовании асинхронных СрПД.

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

Одной из основных предпосылок для разработки линейных кодов, является проблема, проявляющаяся во многих системах передачи цифровой (не только) информации, известная как **девиацией несущей** (carrier deviation).

Очевидно, передатчик и приемник должны работать на одной частоте. В большинстве случаев, передатчик и приемник имеют разные источники синхронизации. При этом тактовые генераторы далеко не идентичны.

Если состояние линии очень долго не изменяется, что происходит при передаче очень длинных нулевых либо единичных последовательностей с использованием классической амплитудной модуляции цифровых цепей (логический ноль соответствует земле, а логическая единица некоторому положительному потенциалу относительно земли), то приемнику «цепляться не за что». В результате накапливаются фазовые сдвиги, что в конце концов приводит к возникновению ошибок.

Современная схемотехническая база для борьбы с девиацией несущей, имеет в распоряжении блок **ФАПЧ** (фазовой автоподстройки частоты), позволяющий автоматически подстраивать тактовый генератор приемника к тактовому генератору передатчика.

Все линейные коды, в той или иной степени, направлены на преобразование битовых последовательностей, чтобы в линии постоянно происходили изменения. В том числе, за счет равномерного распределения нулей и единиц.

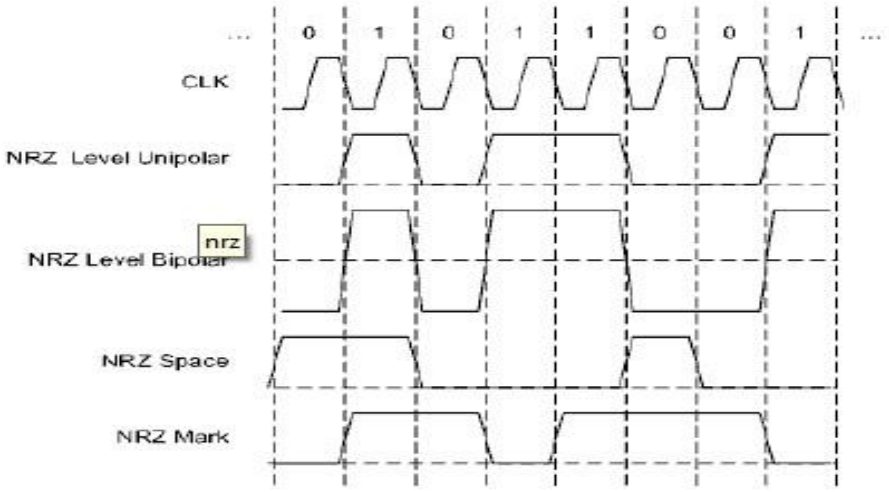
Шесть факторов, влияющих на классификацию линейных кодов:

1) Кодирование уровнями либо переходами
2) Наличие инвертирования
3) Однополярность либо многополярность
4) Наличие так называемого “возврата к нулю”
5) Наличие самосинхронизации
6) Наличие перестановки или подмены битов

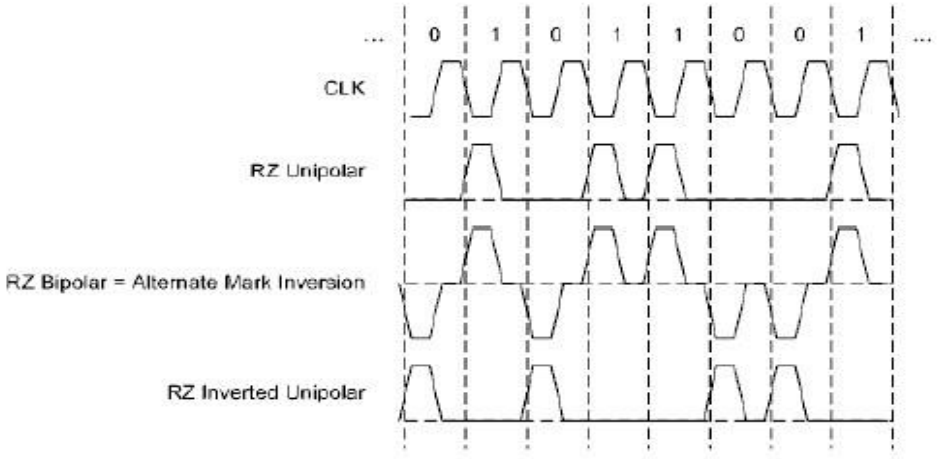
24 Линейные коды без возврата к нулю и с возвратом к нулю

NRZ коды выражаются в изменении уровней между тактами. В простейших случаях, логические уровни в исходной последовательности не преобразуются совсем либо инвертируются. Более сложными случаями являются space и mark. При space-варианте ноль во входной последовательности кодируется сменой текущего уровня в выходной, а единица сохранением текущего уровня. При mark варианте, наоборот, единицы в исходной последовательности приводят к переключению уровней. Начальное состояние значения не имеет.

Space и mark инверсны друг относительно друга. NRZ коды могут быть однополярными и двухполярными. Требуется наличие дополнительной цепи для тактирования. Примеры технологий с применением NRZ: RS-232, USB, HDLC.



RZ коды 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.



Примеры технологий с применением RZ: IrDA.

25 Манчестерские и многоуровневые линейные коды

Манчестерские коды выражаются в переходах между уровнями во время тактов, поэтому их иногда называют фазовыми кодами. Есть два «равноправных» варианта собственно манчестерского кода. 1) Ноль во входной последовательности заменяется на переход от единицы к нулю, а единица заменяется на переход от нуля к единице. 2) Либо наоборот.

Манчестерские коды обладают свойством самосинхронизации.

Существуют несколько кодов близких к Манчестерским:

1.Код Миллера

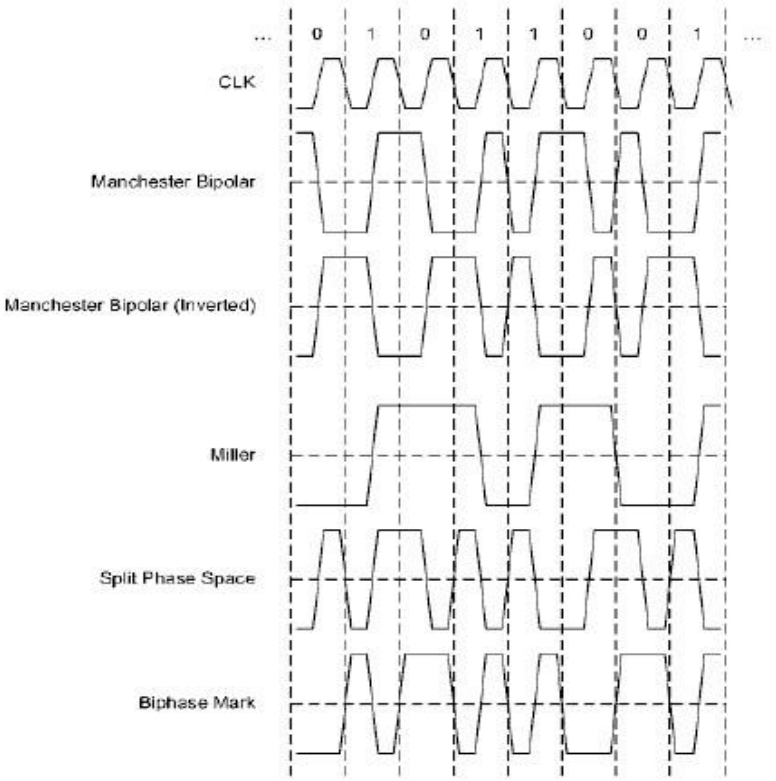
2.Split Phase код

3.Biphase код

Согласно коду Миллера (Miller), ноль соответствует отсутствию перехода во время такта, единица соответствует переходу во время такта, плюс между двумя нулями всегда выполняется смена уровня.

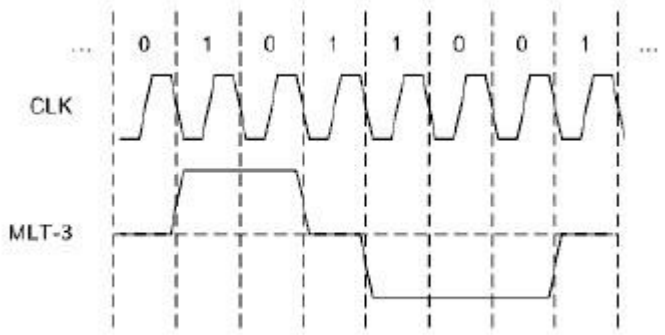
Согласно коду Split Phase учитывается направление предыдущего перехода. При space-варианте ноль соответствует переходу во время такта в направлении, противоположном направлению предыдущего перехода, единица соответствуют переходу во время такта в направлении, совпадающем с направлением предыдущего перехода. При mark-варианте «роли» нулей и единиц из входной последовательности инвертируются.

Согласно коду Biphase, кроме возможных переходов во время тактов, всегда выполняется смена уровня между тактами. При space-варианте ноль соответствуют переходу во время такта, единица соответствуют отсутствию перехода во время такта. При mark-варианте «роли» нулей и единиц из входной последовательности инвертируются.



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

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



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

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 вышеперечисленными кодами. В связи с избыточностью блочных кодов, во многих из них предусмотрены контрольные последовательности, которые, по сути, являются управляющими символами.

Первым примером может служить код 4b/5b, применяемый в Fast Ethernet и CDDI.

Более сложным примером может служить код 8b/10b, применяемый в оптических вариантах Gigabit Ethernet. Биты входного блока обозначают как ABCDEFGH от младшего к старшему, выходного abcdefghij 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 собственно блоков данных D, имеются контрольные блоки K, которые кодируют альтернативно. Таким образом, входной блок обозначают как Dx.y либо Kx.y. Наконец, в код 8b/10b заложена гибкая система уравнивания количества нулей и количества единиц, заключающаяся в динамическом выборе блока для замены (одного из двух) исходя из текущего значения так называемого RD (Running Disparity). Предусмотрено два значение RD -1 и +1. При выборе текущего значения RD учитывается предыдущее значение RD и соотношение нулей и единиц во входном блоке (плюс есть исключения).

Пример таблиц для 8b/10b

3b	4b	
HGF	*fghj*	
D	RD = -1	RD = +1
000	1011	0100
001	1001	
010	0101	
011	1100	0011
100	1101	0010
101	1010	
110	0110	
111	1110	0001
111	0111	1000

5b	6b		5b	6b	
EDCBA	*abcdei*		*EDCBA*	*abcdei*	
D	RD = -1	RD = +1	*D*	RD = -1	RD = +1
00000	100111	011000	10000	011011	100100
00001	011101	100010	10001	100011	
00010	101101	010010	10010	010011	
00011	110001		10011	110010	
00100	110101	001010	10100	001011	
00101	101001		10101	101010	
00110	011001		10110	011010	
00111	111000	000111	10111	111010	000101
01000	111001	000110	11000	110011	001100
01001	100101		11001	100110	
01010	010101		11010	010110	
01011	110100		11011	110110	001001
01100	001101		11100	001110	
01101	101100		11101	101110	010001
01110	011100		11110	011110	100001
01111	010111	101000	11111	101011	010100

27 Поля Галуа и их применение в компьютерных сетях

Поле *GF(p)* из целых чисел 0, 1 ... *p - 1*, порожденное в результате отображения f: *Z/p -> GF(p)*, где *Z/p* -- факторкольцо множества целых чисел, в котором роль идеала играет простое число *p*, 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.

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 $GF(p^n)$.

Сложение бинарных векторов (совпадает с вычитанием) проблему не представляет и соответствует поразрядной операции **xor**. А вот с умножением и делением дела обстоят значительно сложнее. Скалярное произведение не подходит, так как его результат может «выйти» за пределы поля. Векторное произведение определено только для трехразрядных векторов. Полиномиальное представление так же с ходу не решает проблему, так как произведение полиномов опять же «выводит» за пределы поля.

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)*.

Деление векторов в математике не известно. После перехода на язык полиномов, опять же для обеспечения конечности поля Галуа, деление всегда должно быть безостаточным.

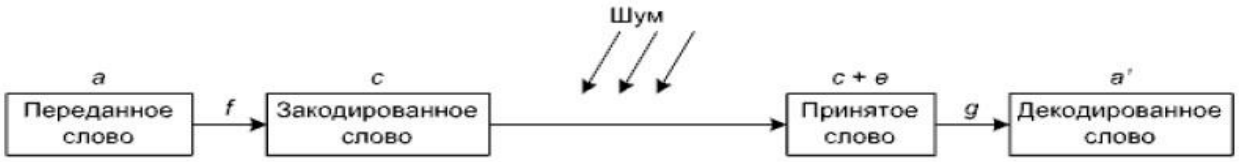
Деление можно представить как умножение полинома-делимого на полином, обратный делителю. При этом для достижения цели на основании математических выкладок, необходимо ввести еще одно ограничение: порождающий полином должен быть неприводимым по модулю *p* (например, если *p* = 2 и *n* = 4, то полином $x^4 + 1$ (число 17) не подходит, так как

$x^4 + 1 \equiv (x^2 + 1)^2 \pmod 2$).

Возведение в степень обладает цикличностью.

28 Модель помехоустойчивого канала связи и теорема Шеннона

Считается, что начало помехоустойчивому кодированию положила теорема Шеннона, утверждающая что любой дискретный канал связи, имеет конечную пропускную способность и этот канал может быть задействован для передачи информации со сколь угодно большой степенью достоверности, не смотря на наличие помех.



Передаваемое сообщение разбивается на блоки фиксированного размера a из k битов $a_1, a_2, \ldots a_k$. Кодер выполняет функцию f называемую схемой кодирования и тем самым преобразует вектор a в вектор c из $n > k$ битов $c_1, c_2, \ldots c_n$ называемый кодовым словом. В процессе пересылки кодового слова по каналу связи на него накладывается вектор ошибок e в котором единичные биты соответствуют искажениям. После применения декодером схемы декодирования g получается вектор a' в идеале совпадающий с исходным вектором a.

Подобная схема кодирования является избыточной. На практике всегда ищут компромисс между степенью обеспечения достоверности при передаче и вычислительной сложностью кодов (что в первую очередь отражается на скорости декодирования). В КС множество кодовых слов получается из множества исходных слов как отображение из конечного поля $GF(2^k)$ в конечное поле $GF(2^n)$.

При более простых схемах кодирования, в кодовом слове сначала располагаются биты входного сообщения, называемые информационными, а за ними дополнительные биты, называемые проверочными $a_1, a_2, \ldots a_k, c_{k+1}, c_{k+2}, \ldots c_n$. В более сложных случаях проверочные биты чередуются с информационными.

29 Линейные помехоустойчивые коды, включая коды Хэмминга и циклические коды

Если H -- матрица размером $(n - k) \times$ n ранга $n - k$ и $H * c^T = 0$, то множество всех n-разрядных векторов, входящих в поле $GF(2^n)$ (в общем случае $GF(p^n)$), называют ***линейным (n,k)-кодом*** (в математическом смысле) длины n и размерности k. А матрицу H называют проверочной. (*с – кодовое слово, вроде как)*.

Самыми примитивными из линейных кодов являются подсчет контрольной суммы и дублирование информационных символов.

Перед выбором того либо иного помехоустойчивого кода всегда нужно определиться, что требуется от кода. Если перефразировать, то нужно ответить на два вопроса:

1.Сколько бинарных ошибок код должен обнаруживать.

2.Сколько бинарных ошибок код должен исправлять.

Число координат (позиций), которыми два вектора x и y различаются называют расстоянием Хэмминга – $d(x,y)$. Число ненулевых позиций вектора x называют весом Хэмминга $w(x)$. Видно, что расстояние Хэмминга показывает количество возникших ошибок.

Для увеличения корректирующей способности кода следует стремиться увеличивать расстояния между кодовыми словами. При этом минимальное расстояние $d_{\min}$ называют кодовым и оно является очень важной характеристикой помехоустойчивого кода. Согласно теореме, для того чтобы линейный код исправлял t ошибок должно выполняться условие: $d_{\min} >= 2t + 1$.

Для того, чтобы линейный код обнаруживал t ошибок должно выполняться условие $d_{\min} >= t + 1$.

Для того чтобы линейный код имел $d_{\min} >= s + 1$, необходимо и достаточно, чтобы любые s столбцов его проверочной матрицы были линейно независимы.

Способность того или иного кода сохранять свои характеристики зависит и от количественного соотношения информационных и проверочных символов. В теории помехоустойчивого кодирования определяют так называемые верхние и нижние границы кодов.

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

Циклические коды являются особо выделяемой подгруппой линейных кодов. Циклическим кодом называют линейный код, удовлетворяющий дополнительному условию: если вектор $a_0, a_1 \ldots a_{n-1}$ является кодовым словом, то и его циклический сдвиг $a_{n-1}, a_0 \ldots a_{n-2}$ 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 сравниваются остатки. 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 в процессе кодирования не используется и поэтому «отбрасывается». Для того чтобы максимально разнообразить остатки в качестве порождающего полинома должен выбираться неприводимый полином.

Существуют два подхода к реализации циклического кода на стороне приемника:

1) Согласно базовой идее, описанной выше
2) На порождающий полином делится всё принятое кодовое слово.

Если ошибок не прошло, то остаток будет нулевым. Оба подхода равноценны.

30 Классификация помехоустойчивых кодов

Основные группы помехоустойчивых кодов:

1)Линейные коды, в том числе: коды Хэмминга, циклические коды, БЧХ-коды (коды Боуза-Чоудхури-Хоквингема), РМ коды (коды РидаМаллера), итеративные коды, коды на основе матриц Адамара, симплексные коды и некоторые другие.

2)Коды для контроля модульных и пакетных ошибок, в том числе РСкоды (коды Рида-Соломона), низкоплотные модульные коды, векторные модульные коды, итеративные модульные коды и некоторые другие.

3)Свёрточные коды

4)Арифметические коды

5)Низкоскоростные коды, в том числе: коды максимальной длины, нелинейные коды, D-коды и некоторые другие.

31 Классификация каналов в сети передачи данных

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

1)Симплексном – передача данных по каналу возможна только в одном направлении.

2)Полудуплексном – данные могут передаваться в обоих направлениях, но в один момент времени возможна передача только в одном направлении.

3)Полнодуплексном – данные могут передаваться в обоих направлениях одновременно.

Сейчас в КС доминируют полнодуплексные каналы.

Последовательный канал может быть:

1)Выделенным – зарезервирован за определённой парой станций абонентов.

2)Разделяемым – может использоваться несколькими станциями абонентами.

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

С точки зрения общей организации процесса пересылки данных все СПД можно разделить на 2 фундаментальных типа:

1) СПД с коммутацией пакетов (packet-switched)
2) СПД с коммутацией каналов (circuit-switched)

32 Логические и физические топологии LAN

Топология «возникает» на канальном уровне, когда речь идет об организации сегмента.

Прежде всего, топологии делят на два типа:

1)Point-to-point - топология «точка к точке» связывает только две станции.

2)Multi-access (multipoint to multipoint) - топология со множественным доступом - связывает более двух станций.

Эти два типа позволяют организовывать двунаправленные каналы между любым требующимся количеством абонентов поэтому их реализуют наиболее часто.

Применительно к однонаправленным каналам можно добавить еще два пункта:

1)Point-to-multipoint – иногда.

2)Multipoint-to-point – очень редко.

Менее двух станций в сегменте быть не может.

Если топологически классифицировать аппаратные технологии, то есть еще два ракурса:

1)Физическая топология – отражает физические связи между устройствами.

2)Логическая топология – отражает логические связи между устройствами.

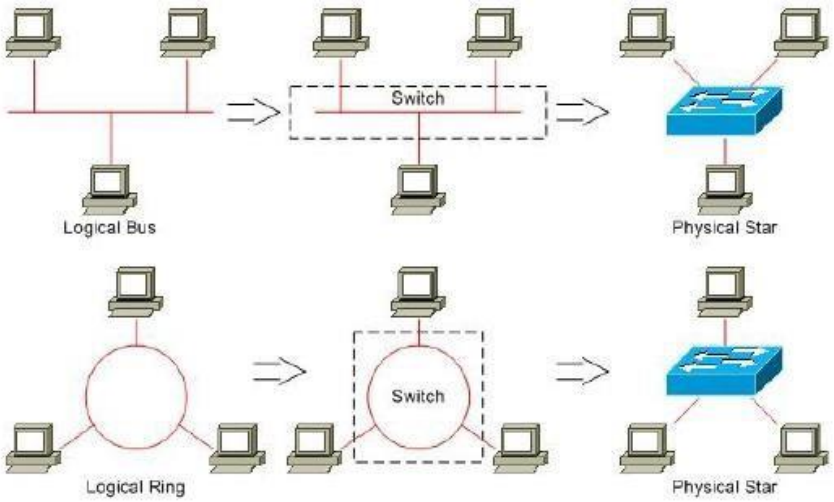
Характерными топологиями ЛКС (LAN) являются:

1) Шина.

2) Кольцо.

3) Звезда.

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



33 Логические и физические топологии WAN и RAS

Топология «возникает» на канальном уровне, когда речь идет об организации сегмента.

Прежде всего, топологии делят на два типа:

1)Point-to-point - топология «точка к точке» связывает только две станции.

2)Multi-access (multipoint to multipoint) - топология смножественным доступом - связывает более двух станций.

Эти два типа позволяют организовывать двунаправленные каналы между любым требующимся количеством абонентов поэтому их реализуют наиболее часто.

Применительно к однонаправленным каналам можно добавить еще два пункта:

1)Point-to-multipoint – иногда.

2)Multipoint-to-point – очень редко.

Менее двух станций в сегменте быть не может.

Если топологически классифицировать аппаратные технологии, то есть еще два ракурса:

1)Физическая топология – отражает физические связи между устройствами.

2)Логическая топология – отражает логические связи между устройствами.

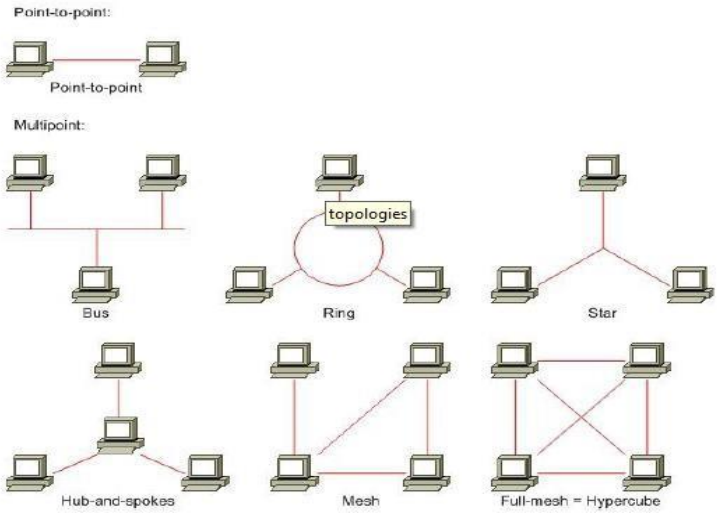
Характерными топологиями ГКС (WAN) являются:

1)Сеть (произвольно связанная) (mesh)

2)Ступица со спицами (hub-and-spokes)

3)Полносвязная сеть (full-mesh)

Характерной RAS(Remote access server) топологией является point-to-point. Можно сказать, что для ГКС-технологий существует только одна типичная топология (произвольно связанная сеть), остальные можно рассматривать как ее частные случаи.



Топологии КС с детализацией до станций и СрПД

Инфа про то, зачем нам нужны вообще какие-то методы доступа к какому-то моноканалу к 34 вопросу

Проблема заключается в «столкновениях» конкурирующих передатчиков. Если находящиеся в равных условиях два либо более передатчиков одновременно выдают сигналы в СрПД (уустанавливают соответствующие уровни напряжения), то возникает противоречие. Таковое единовременно неразрешимое противоречие принято называть коллизией.

Коллизия может быть как логической (информационный конфликт) так и физической (несовместимые физические процессы).

Классическим способом защиты оборудования от коллизий является гальваническая развязка (трансформаторная либо оптронная). При попытках установить разные уровни, как правило, наблюдаются эффекты «зануления» и «заединичивания» в зависимости от особенностей элементной базы.

Ситуация с коллизией может затрагивать только станции, подключенные к одной СрПД, то есть сегмент компьютерной сети. Сегмент, в котором возможно возникновение коллизий называется **доменом коллизий**. Понятие коллизии относится не только к сигналу, а и к пакету.

Физические свойства СрПД не позволяют мгновенно передавать сигналы. Следовательно и возникшая коллизия распространяется по сегменту с конечной скоростью. Под **окном коллизий** (collision window) понимается временной интервал, в течение которого любая из станций гарантированно обнаруживает коллизию, равный удвоенному времени прохождения сигнала между двумя максимально удаленными станциями. Без учета окна коллизий, влияющего на время постудержания сигнала, невозможно спроектировать работоспособный сегмент.

Существуют два основных подхода к проблеме коллизий:

1)Не допускать коллизии вообще, то есть пользоваться детерминированными методами доступа к моноканалу.

2)Допускать коллизии и каким-то образом выходить из них, что достижимо только использованием случайных методов доступа к моноканалу Во втором случае так же можно выделить два подхода:

1)Не обращать внимание на причины возникновения коллизий, а упор делать на способ выхода из них.

2)Пытаться предотвращать коллизии тем самым максимально снижая их количество, ну а если коллизии все-таки возникают, то «тяжело» выходить из них.

Таким образом, все методы доступа к моноканалу делят на:

1)Случайные.

2)Детерминированные.

34 Особенности случайных методов доступа к моноканалу

Все **случайные** методы основаны на использовании генератора случайных чисел (поэтому их так и называют), который позволяет делать случайные задержки при доступе к моноканалу, а значит и с определенной степенью вероятности избегать коллизии.

На эффективность случайных методов наиболее существенное влияние оказывают следующие факторы:

1)Кол-во взаимодействующих станций.

2)Инертность среды передачи данных.

3)Длина кадра.

4)Частота синхронизации.

Случайные методы **допускают** коллизии и каким-то образом выходят из них.

//НЕ ИЗ ГЛЕЦА

Преимущества:

1) Реализуются достаточно просто.
2) Обеспечивают быстрый доступ к каналу при малой нагрузке.
3) Позволяет легко подключать или отключать станции.
4) Обладает высокой «живучестью» - способностью выполнять свои функции при наличии сбоев и отказов. а) Большинство ошибочных и не благоприятных условий приводит к молчанию или конфликту, и обе эти ситуации поддаются обработке, б) нет необходимости в центральном управляющем устройстве. В сетях стремятся уйти от централизованного управления.

Недостатки:

1) При больших нагрузках время ожидания доступа к шине становится большим и меняется не предсказуемо.
2) Все абоненты имеют равные права, нет приоритетности кадров и станций.

35 CSMA/CD (Ethernet)

С точки зрения изучения случайных методов доступа к моноканалу наиболее наглядным примером является классический алгоритм CSMA/CD (Carrier Sense Multiple Access with Collision Detection) множественный доступ с прослушиванием несущей и обнаружением коллизий, описанный в стандарте Ethernet (IEEE 802.3).

Задержка перед началом очередной попытки передачи после коллизии измеряется в так называемых **слот таймах**, количество которых является случайным целым числом r

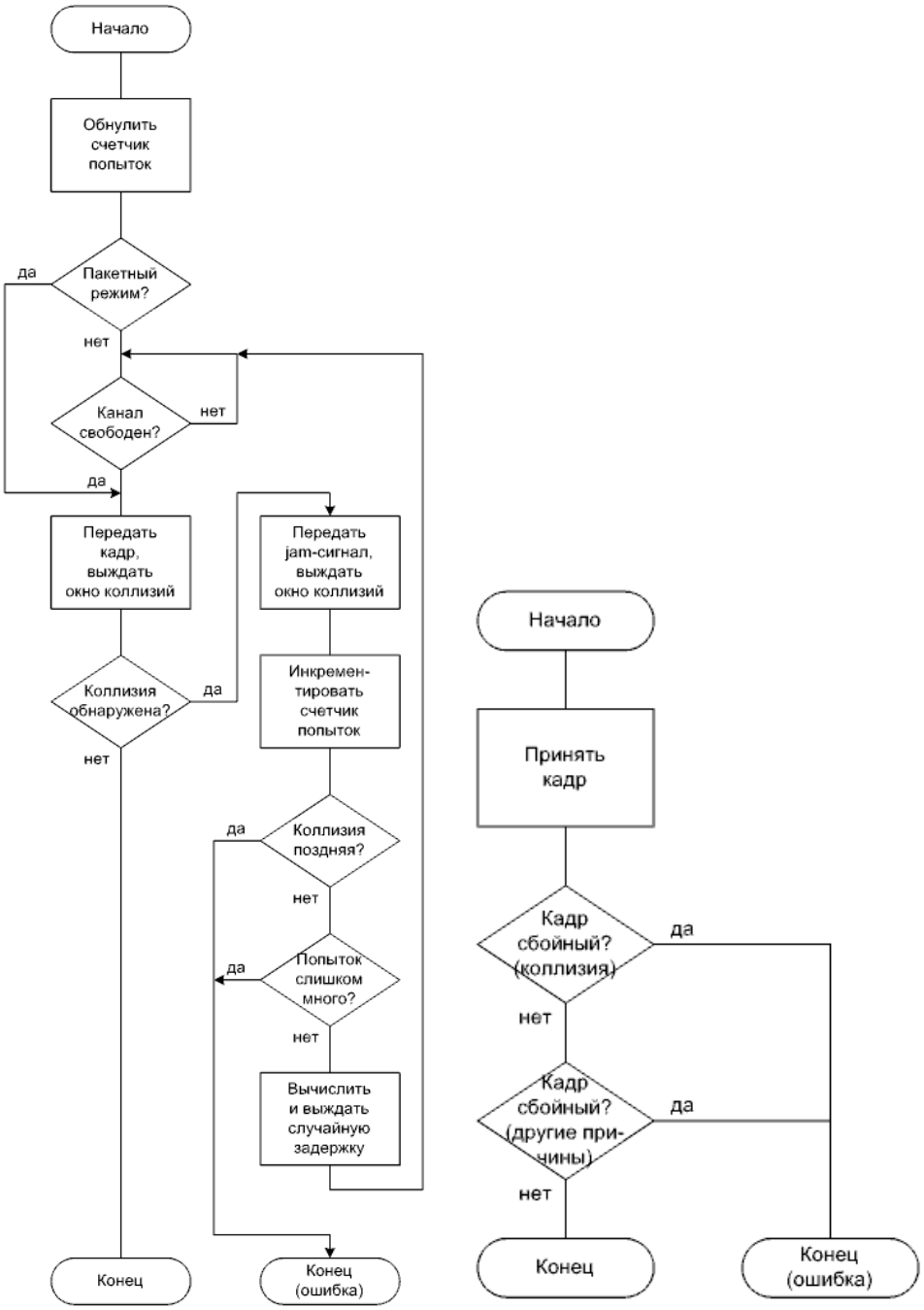
$0 <= r <= 2^k$, где k = min (n, 10), где n номер попытки.

После превышения счетчиком попыток некоторого порогового значения дальнейшие попытки считаются бесперспективными. Значение k не может быть больше 10. Значение n не может быть больше 16.

Качество диспетчеризации при обработке коллизий по большому счету зависит от одного базового параметра. **Слот-тайм** (slot time) является минимальной неделимой единицей 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 передачи jam-сигнала.

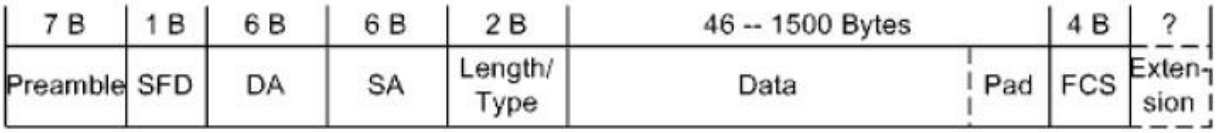
В стандарт заложен механизм ускорения распределенного обнаружения коллизий, заключающийся в их «усилении». Каждая обнаружившая коллизию станция передает специальный **jam-сигнал** некоторой длительности (значение стандартом не регламентируется). Jam-сигнал выполняет две важные функции. Во-первых, является 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.

Под **окном коллизий** (collision window) понимают временной интервал, в течение которого любая из станций гарантированно обнаруживает коллизию, равный удвоенному времени прохождения сигнала между двумя максимально удаленными станциями.



Алгоритм CSMA/CD.
Передача очередного кадра на 1 картинке и прием на 2

36 Кадр Ethernet



Поля:

1)Preamble – преамбула

2)SFD (Start Frame Delimiter) – разграничитель начала кадра

3)DA (Destination Address) – адрес назначения

4)SA (Source Address) – адрес источника

5)Length/Type – длина либо тип

6)Data – данные

7)Pad – наполнитель

8)FCS (Frame Check Sequence) – контрольная сумма

9)Extension – расширитель

Предусмотрены полудуплексный и полнодуплексный режимы, «поведение» в которых несколько различается.

В качестве преамбулы выступают семь байтов со значением 10101010b, а в качестве SFD байт со значением 10101011b.

При сборке кадра учитываются ограничения на его длину. Ограничивается не только максимальная длина, а и минимальная.

При недостаче в поле данных вслед за ним в кадр вставляются дополнительные октеты наполнители (значения стандартом не регламентируются).

Если значение поля Length/Type меньше 1536 (600h) (по стандарту, фактически: 1500), то указывает длину инкапсулируемых данных, если больше либо равно -- тип.

При необходимости, октеты-расширители дополняет кадр до тайм-слота (только в полудуплексном режиме).

В качестве контрольного кода используется код CRC.

37 CSMA/CA (Wi-Fi)

Еще одним примером случайных методов доступа к моноканалу является гораздо более сложный алгоритм 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).

Для понимания алгоритма необходимо ввести термины из стандарта.

Применительно к Wi-Fi, MAC-подуровень канального уровня поделен еще на два слоя. На нижнем слое расположен только один блок под названием **DCF** (Distributed Coordination Function) -- функционал распределенного координируемого взаимодействия. DCF и составляет ядро алгоритма CSMA/CA. Все станции сегмента должны поддерживать DCF.

Стандартом предусмотрены целых шесть вариантов отслеживаемых межкадровых интервалов -- IFSes (InterFrame Spaces): 1. RIFS (Reduced IFS) -- сокращенный. 2. SIFS (Short IFS) -- короткий. 3. PIFS (PCF IFS) -- для PCF. 4. **DIFS** (DCF IFS) -- для DCF. 5. AIFS (Arbitration IFS) -- для QoS-арбитража. 6. EIFS (Extended IFS) -- расширенный.

Случайную задержку измеряют в слот-таймах, как и в Ethernet, но алгоритм другой. Количество слот таймов является случайным целым числом Random:

0 <= Random <= CW, где CW(contention window) – так называемое окно состязаний, CW_{min} <= CW <= CW_{max}, и берётся из ряда 7, 15, 31 (2^n – 1). Типичные значения: CWmin =15, CWmax=1023.

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

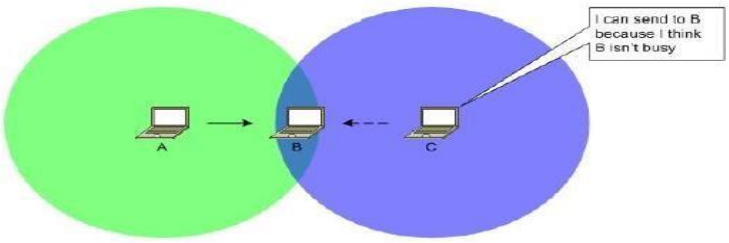
Для беспроводных каналов свойственны две проблемы, которые получили следующие названия:

1)Hidden node problem - проблема скрытой станции

2)Exposed node problem - проблема доступной станции

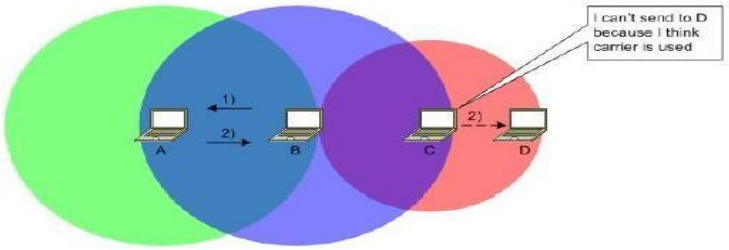
Предполагается, что все станции взаимодействуют в рамках одного канала. (Эти проблемы возникнут и в проводных каналах, если не учесть окно коллизий)

Проблему скрытой станции можно сформулировать так: станция C может ошибочно начать передачу станции B, так как не может «услышать» что станция A уже передает станции B (станция A «скрыта» от станции C)

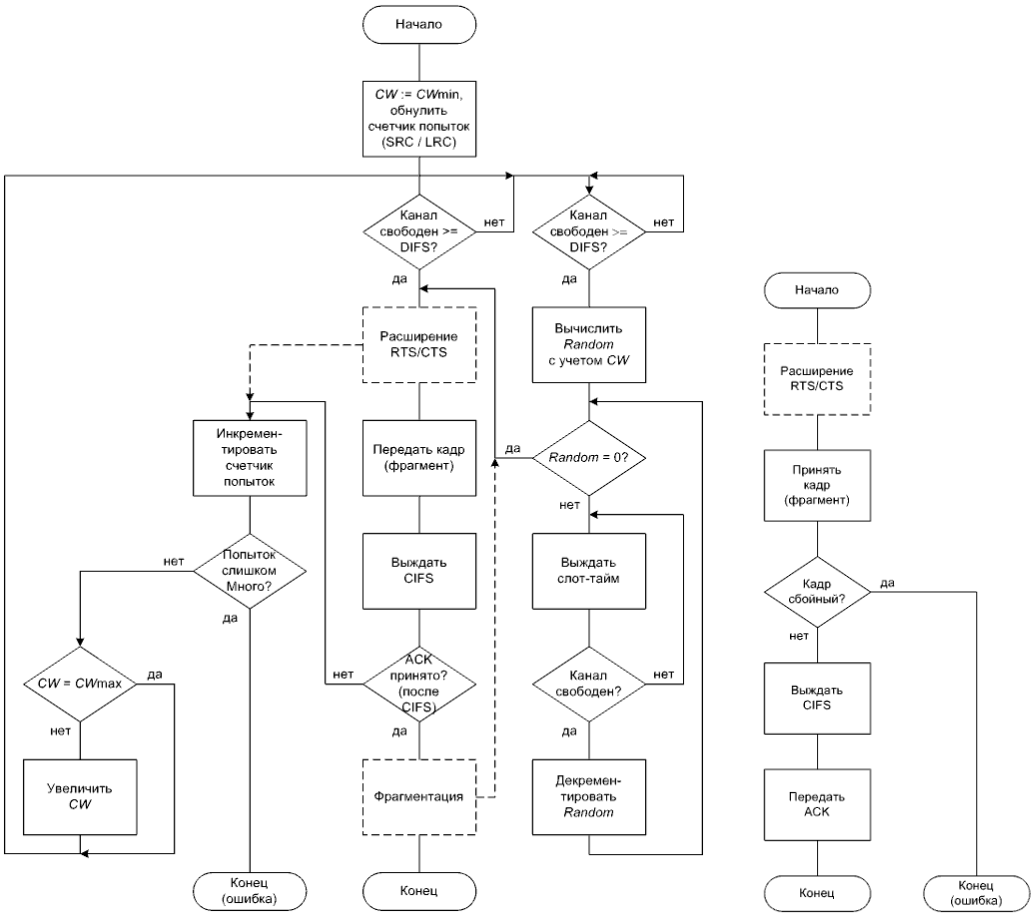


Проблему доступной станции можно сформулировать так: станция C, зная о взаимодействии станций A и B, не может передать станции D во время

пассивности станции B, а могла бы, поскольку считает канал занятым ошибочно (станция C «доступна» для станции D)

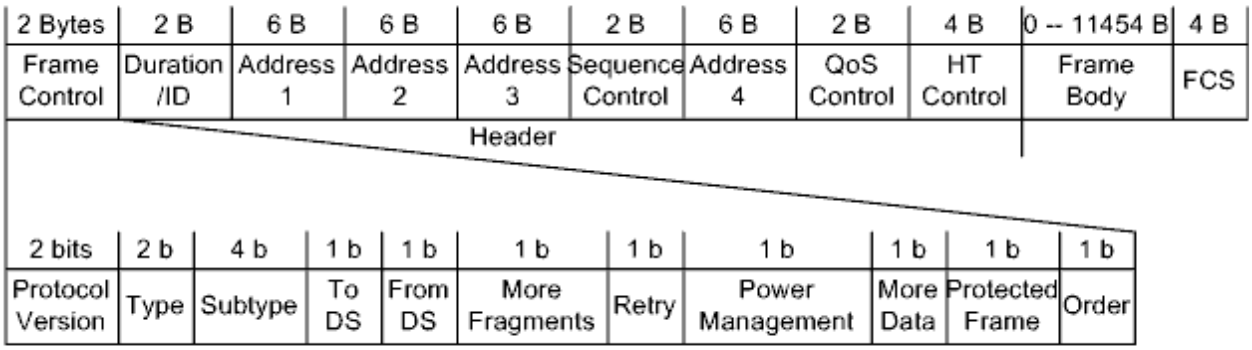


Частично решить проблемы помогает опциональное расширение RTS/CTS.



CSMA/CA: отправка и принятие кадров

38 Кадры 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 пересылки (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: 00b -- Management -- управление, 01b -- Control -- контроль 10b -- Data -- данные, 11b -- Reserved -- зарезервировано.

3.Subtype -- подтип (в настоящее время определено около сорока подтипов).

4.To DS -- флаг направления в распределительную систему (проводную систему, связывающую беспроводные сегменты).

5.From DS -- флаг направления из распределительной системы.

6.More Fragments -- флаг наличия фрагментации.

7.Retry -- флаг повторной попытки передачи.

8.Power Management -- флаг режима энергосбережения.

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

10.Protected Frame -- флаг защищенности кадра (шифрования).

11.Order -- флаг упорядоченности (при QoS). Таким образом, существуют три типа кадров.

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

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

2)SA (Source Address) – адрес источника,

3)DA (Destination Address) – адрес назначения,

4)TA (Transmitting station Address) – адрес станции передатчика (непосредственного)

5)RA (Receiving station Address) – адрес станции приемника (непосредственного)

39 Особенности детерминированных методов доступа к моноканалу

Если случайные методы уместно использовать при шинной топологии, применительно к которой четко выражена возможность возникновения коллизий, то детерминированные методы хорошо «ложатся» на кольцевую топологию. Концептуальная разница между случайными и детерминированными методами заключается в том, возникает ли случайность при «обращении» станции к моноканалу.

Если при некотором такте кольца какая-либо из станций имеет собственный кадр для передачи и при этом получила из кольца еще один кадр, который необходимо «продвигать» дальше, то появляется вопрос о том, какой из этих кадров передавать.

Единственным способом преодоления логических коллизий является введение приоритетов. В то время как все случайные методы «завязаны» на генератор случайных задержек, все детерминированные методы «завязаны» на систему приоритетов в том или ином виде. Возникает задача распределенного либо централизованного назначения приоритетов, причем ни одна из станций кольца заранее ничего «не знает» о других станциях.

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:

1)Централизованное либо распределённое управление

2)Алгоритм назначения приоритетов

3)Топологические особенности

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

1)Количество взаимодействующих станций

2)Частота синхронизации

3)Длина кадра

Если сравнивать детерминированные методы со случайными, то сложно сказать какие из них «лучше» При применении случайных методов основные потери производительности возникают из-за вносимых задержек, а при применении детерминированных методов потери обусловлены ретрансляцией кадров. Если оценивать реализации, которые уже имеются на рынке, то все же детерминированные алгоритмы в среднем демонстрируют бОльшую производительность. Однако оборудование в среднем более дорогостоящее.

40 Алгоритм Token Ring

С точки зрения детерминированных методов доступа к моноканалу наиболее наглядным примером является классический алгоритм, описанный в стандарте Token Ring (IEEE 802.5).

В Token Ring применяется централизованное управление. Закономерным следствием является необходимость включения в кольцо по крайней мере одной управляющей станции, наделенной особыми полномочиями и призванной инициализировать кольцо и следить за его работоспособностью. В терминологии Token Ring такую управляющую станцию обобщенно называют **станцией-монитором** (monitor station).

Кроме единственной основной станции монитора (active monitor) в состав кольца может входить некоторое количество резервных (standby monitors). Функции станции монитора:

1)Инициализировать подключившиеся к кольцу станции.

2)Тактировать (на физическом уровне) работу кольца.

3)Контролировать наличие и валидность маркера.

4)Предотвращать зацикливания.

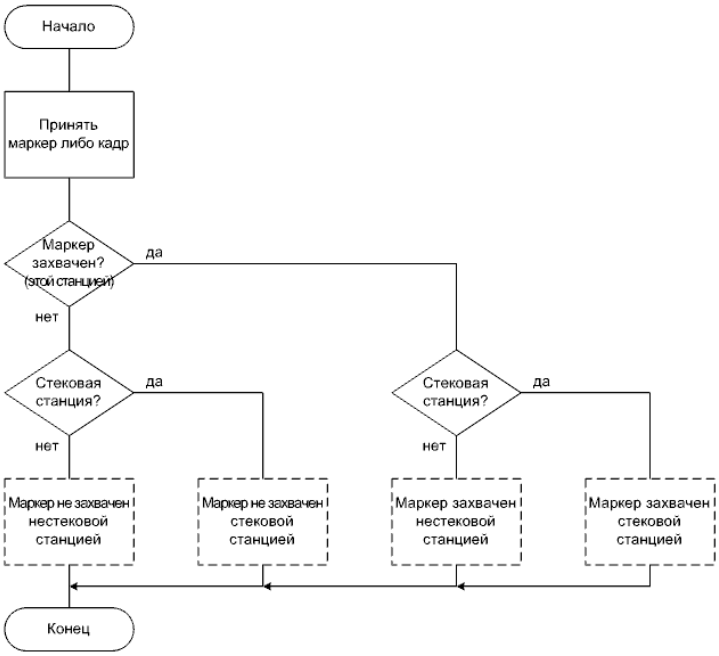
Несмотря на то, что теоретически кольцо предполагает некоторую возможность «распараллеливания» (то есть, одновременно по разным частям кольца могут циркулировать несколько кадров), очень обобщенно алгоритм Token Ring можно представить как «бесконечно» циркулирующий под управлением станции-монитора маркер, который анализируется всеми пользовательскими станциями и к которому при необходимости «цепляются» данные.

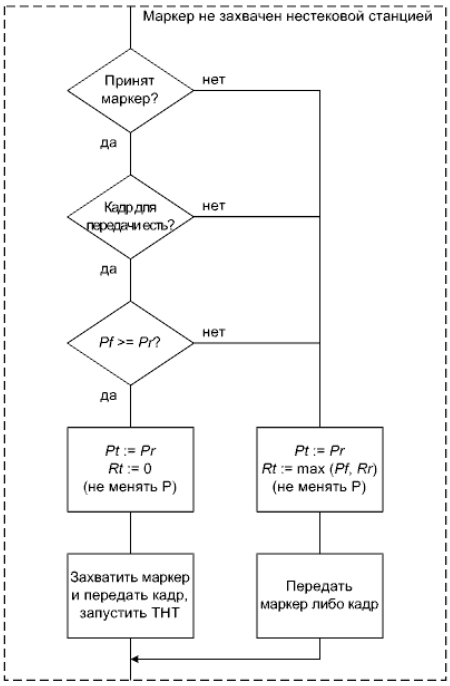
В стандарт заложена комплексная система приоритетов, однако некоторые «тонкости» оставлены на откуп реализациям. Механизм приоритетов Token Ring основан на связке двух полей -- P и R. Поле P отображает текущий уровень приоритета, а поле R -- запрашиваемый. Каждое из этих полей может иметь значение от 000b до 111b, то есть доступно восемь уровней приоритета.

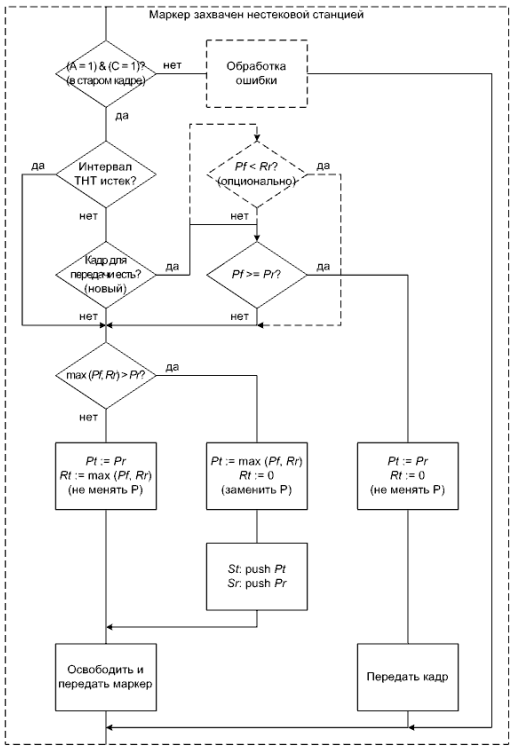
С помощью маркера, который передается по цепочке от станции к станции, предоставляется право на передачу. Если у станции нет своего кадра для передачи, то она передает маркер дальше. Если у станции есть кадр для передачи, то она захватывает маркер, заменой значения поля T с нуля на единицу преобразует маркер в кадр, добавляет все соответствующие поля и передает. Приоритет автоматически «достается» станции, до которой маркер дошел раньше. Внесенный таким образом в кольцо кадр ретранслируется всеми промежуточными станциями до тех пор, пока не достигнет адресованной станции-абонента.

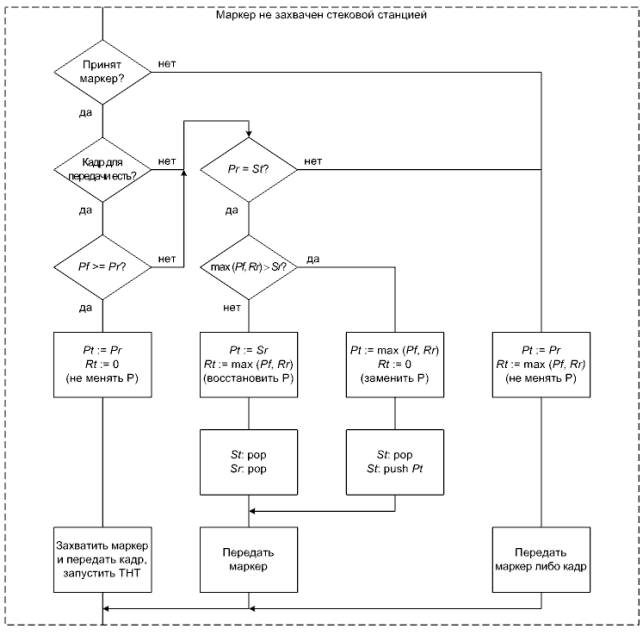
За удаление кадра из кольца ответственна станция, создавшая его. Поэтому станция-абонент, распознавшая свой адрес в принятом кадре, вместо удаления кадра отмечает факт распознавания присваиванием единичных значений обоим битам A и передает кадр дальше. Если станция-абонент «забирает» данные из кадра, то она присваивает единичные значения

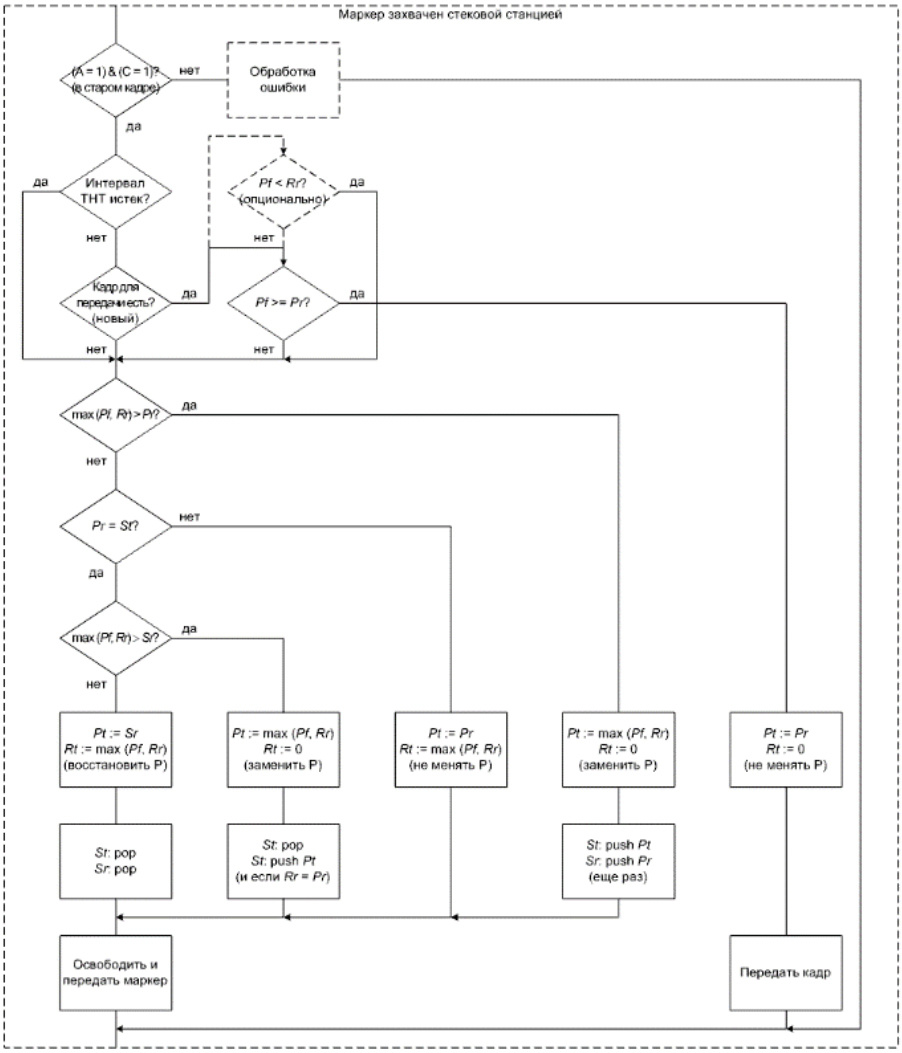
и обоим битам C. Значения битов A и C проверяются при возвращении кадра к создавшей его станции. На основании результатов проверки делаются соответствующие выводы. Но нужно освободить маркер. В нормальном случае станция освобождает маркер сразу после того, как дождется возвращения кадра.











Про формат кадров Token Ring и назначение основных полей.

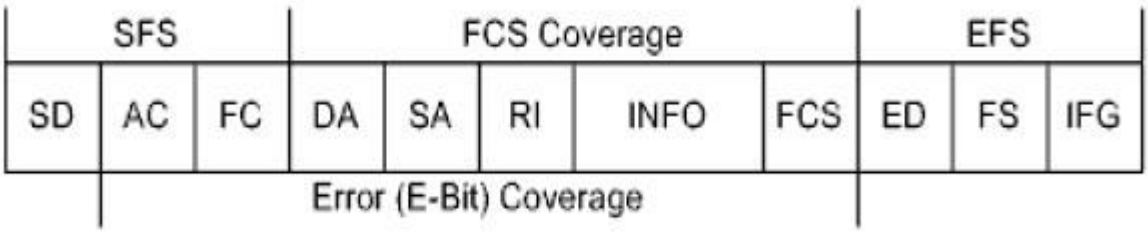
В стандарте предусмотрены четыре вида передаваемых последовательностей:

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 специальные последовательности. Формат кадров Token Ring и назначение основных полей.



Поля:

1)SD (Starting Delimiter) - начальный разделитель

2)AC (Access Control) - контроль доступа

3)FC (Frame Control) - контроль кадра

4)DA (Destination Address) - адрес назначения

5)SA (Source Address) - адрес источника

6)RI (Routing Information) - информация о маршрутизации (может отсутствовать)

7)INFO (information) - данные (могут отсутствовать)

8)FCS (Frame Check Sequence) - контрольная сумма

9)ED (Ending Delimiter) - конечный разделитель

10)FS (Frame Status) - состояние кадра

11)IFG (InterFrame Gap) - межкадровый интервал

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

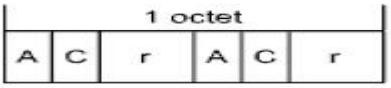
Где:

1)P (Priority bits) - текущий уровень приоритета

2)T (Token bit) - идентификатор маркера 0 маркер, 1 кадр

3)M (Monitor bit) - бит монитора

4)R (Reservation bits) - запрашиваемый уровень приоритета Формат поля состояния кадра:



Где:

1)A (Address-recognized bit) - флаг распознания адреса (дублируется)

2)C (frame-Copied bit) - флаг копирования кадра (дублируется)

3)r (reserved) – зарезервировано

Механизм приоритетов Token Ring основан на связке двух полей P и R. Поле P отображает текущий уровень приоритета, а поле R запрашиваемый. Каждое из этих полей может иметь значение от 000b до 111b, то есть доступно восемь уровней приоритета.

Условно можно выделить два режима взаимодействия:

1)Все станции имеют одинаковые приоритеты («отсутствие» приоритетов)

2)Станции могут иметь разные приоритеты («наличие» приоритетов, совместимое расширение первого режима, некоторые станции могут пользоваться кольцом более интенсивно связь с QoS)

При «отсутствии» приоритетов станция монитор создает и «запускает» в кольцо маркер с нулевыми полями P и R (назначение этих полей не проявляется)

С точки зрения отдельно взятой станции порядок доступа к кольцу можно свести к трем шагам:

1)Захват маркера и передача кадра.

2)Освобождение маркера и при необходимости коррекция текущего уровня приоритета.

3)Восстановление текущего уровня приоритета если он был скорректирован.

Соблюдение перечисленных выше правил гарантирует, что любая станция рано или поздно дождется возможности передать любой кадр.

Кроме всего прочего, в Token Ring заложено несколько механизмов обеспечения надежности, включая авто переконфигурирование и сигнализацию об ошибках.

В качестве контрольного кода используется код CRC. Скорость Token Ring равна 4 либо 16 Mbit/s (100 Mbit/s самые поздние реализации).

41 Реализации детерминированных методов доступа к моноканалу

0)Token Ring. В Token Ring используется система приоритетов на основе двух полей: P (текущий уровень приоритета) и R (запрашиваемый). Оба поля могут принимать значения от 0 до 7 (000b–111b). Маркер, передаваемый от станции к станции, предоставляет право на передачу данных. Если у станции нет кадра для отправки, она передаёт маркер дальше. При наличии кадра станция захватывает маркер, заменяя T(тип) на 1, и передаёт кадр, который ретранслируется всеми станциями до адресата. Станция-абонент подтверждает получение, выставляя биты A и C (флаг распознавания адреса и флаг копирования кадра) в 1, после чего кадр продолжает движение. Станция-отправитель освобождает маркер после возврата кадра.

Логическая топология: однонаправленное кольцо.

Физическая топология: звезда.

Скорость: 4, 16 Mbit/s, в более поздних 100.

Кроме Token Ring следует упомянуть еще ряд существующих технологий реализаций детерминированных методов:

1)Технология ARCNET (Attached Resource Computer NETwork) Скорость: 2,5 Mbit/s. Алгоритм являлся аналогом упрощенного варианта алгоритма Token Ring (без системы приоритетов).

Логическая топология: однонаправленное кольцо.

Физическая топология: шина или звезда.

Первая широко используемая в ЛКС технология. На данный момент сильно устарела из-за Ethernet.

2)Технология Token Bus (IEEE 802.4).

Скорость: 1, 5, 10, 20 Mbit/s

Логическая топология: однонаправленное кольцо

Физическая топология: шина

Алгоритм представлял собой адаптацию алгоритма Token Ring к шинной топологии. Почти не применяли, сильно устарела.

3)Технология FDDI (Fiber Distributed Data Interface), CDDI (Copper Distributed Data Interface).

FDDI использовался для оптических СрПД, а CDDI – для электрических. Скорость: 100 Mbit/s, 200 Mbit/s

Логическая топология: однонаправленное кольцо с резервированием 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 включают в двойное кольцо).

Алгоритм представляет собой расширение алгоритма Token Bus. CDDI почти не использовали, FDDI был быстро вытеснен с рынка сетевых технологий после появления более дешевого Fast Ethernet, но ограниченно применяем до сих пор.

4) Технология 100VG-AnyLAN.

Скорость: 100 Mbit/s

Логическая топология: дерево

Физическая топология: дерево (с опциональным резервированием).

Алгоритм представляет собой альтернативу Fast Ethernet (гибрид Ethernet и Token Ring). На технологию возлагали большие надежды, но она была быстро отвергнута рынком и в скорости практически исчезла.

42 Адресация в компьютерных сетях и классификация адресов

логический и физический адрес и про юни бро мульти эни каст адреса

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

В форматах большинства пакетов присутствуют два адреса:

1)Адрес назначения (destination address)

2)Адрес источника (source address)

В процессе пересылки пакета между абонентами адресация играет ключевое значение. Производительность СПД напрямую зависит от расположения адресов в пакете. Поэтому адреса «выносят» в самое начало пакета. Более того, поскольку с точки зрения доставки пакета адрес назначения является более важным (в СПД анализируется именно этот адрес), он как правило располагается раньше.

Следует учитывать, что важное влияние на адресацию оказывает инкапсуляция. Адресация всегда «привязана» к некоторому протоколу, а протокол, в свою очередь, «привязан» к уровню модели OSI. Поэтому закономерно, что на каждом из уровней присутствует своя независимая система адресации.

Для того, чтобы взаимодействующие сетевые процессы могли найти друг друга, во всех реальных системах используется три уровня адресации:

1. Необходимо адресовать подсеть -- используется *адрес подсети* (subnet address).

2. Необходимо адресовать станцию в подсети -- используется *адрес станции* (node address).

3. Необходимо адресовать процесс в станции -- используется так называемый *адрес программного порта* (software port).

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 уровнях.

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 такую адресацию называют физической. Адреса сетевого и прикладного уровней назначают пользователи. Часто такую адресацию называют логической.

При назначении программных портов учитываются диапазоны, к которым они относятся.

Диапазоны программных портов применительно к семейству TCP/IP

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

Так называемые хорошо известные порты предназначены для адресации основных сервисов в Internet. Порты для дополнительных публичных сервисов нужно регистрировать. Порты для приватных (и редких) сервисов регистрировать не нужно.

Специально для компьютерных сетей были разработаны четыре основных способа адресации, которые заключаются в применении адресов четырех базовых типов:

1)Юникаст - пакет с таковым адресом назначения должен быть обработан одной соответствующей станцией.

2)Бродкаст - или, по-другому, широковещательных - пакет с таковым адресом назначения должен быть обработан всеми станциями.

3) Мультикаст - пакет с таковым адресом назначения должен быть обработан несколькими станциями из множества.

4) Эникаст - пакет с таковым адресом назначения должен быть обработан одной станцией из множества.

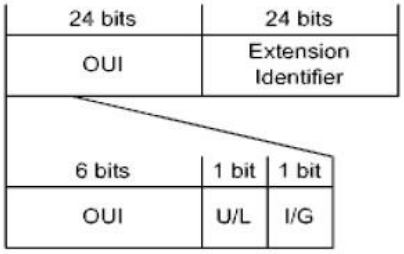
По сути, мультикаст и эникаст адреса являются групповыми идентификаторами (Group IDs).

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

Наиболее сложной формой адресации является эникаст адресация. Очевидно, что каждый раз при приеме эникаст пакета должен осуществляться выбор на основе какого-либо критерия. При этом адресуемые станции должны осуществлять выбор в пределах группы сами. Отправившая пакет станция не может принимать участие в алгоритме выбора, она уже сделала свой «выбор» записав в пакет в качестве адреса назначения эникаст адрес. Выбор должен быть сделан заблаговременно, чтобы принимающая станция была готова к поступлению в группу пакета. Примером критерия выбора может служить время задержки. Выбор может осуществляться однократно либо периодически.

43 MAC-адреса

Уникальность MAC адресов контролирует IEEE RA (IEEE 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. Формат EUI-48:



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

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

OUIs выдают централизовано, уникальность оставшейся части должны обеспечивать 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:

1)MA-L (MAC Address - Large) - 24 бита (данная схема использовалась IEEE RA до 1 января 2014 г

2)MA-M (MAC Address Medium) - 28 битов (схема доступна после 1 января 2014 г)

3) MA-S (MAC Address Small) 36 битов (схема доступна после 1 января 2014 г)

Иногда поле OUI рассматривают как CID (Company ID), что, по большому счету, то же самое зависит от комбинации значений битов U/L и I/G (рассматривают уже как биты X и M соответственно).

По правилам IEEE MAC-адреса записывают в следующей нотации:

XX-XX-XX-XX-XX-XX

Где X-шестнадцатеричная цифра (верхний регистр)

Но очень часто используют альтернативные нотации. Примеры:

```
00-16-41-57-7D-48 -- IEEE
00-16-41-57-7d-48
00:16:41:57:7D:48
00:16:41:57:7d:48
0016.4157.7d48 -- Cisco
```

Все юникаст-MAC-адреса должны иметь нулевое значение бита I/G. Групповые MAC-адреса формируются по особым правилам. В качестве бродкаст-MAC-адреса принято использовать значение:

FF-FF-FF-FF-FF-FF

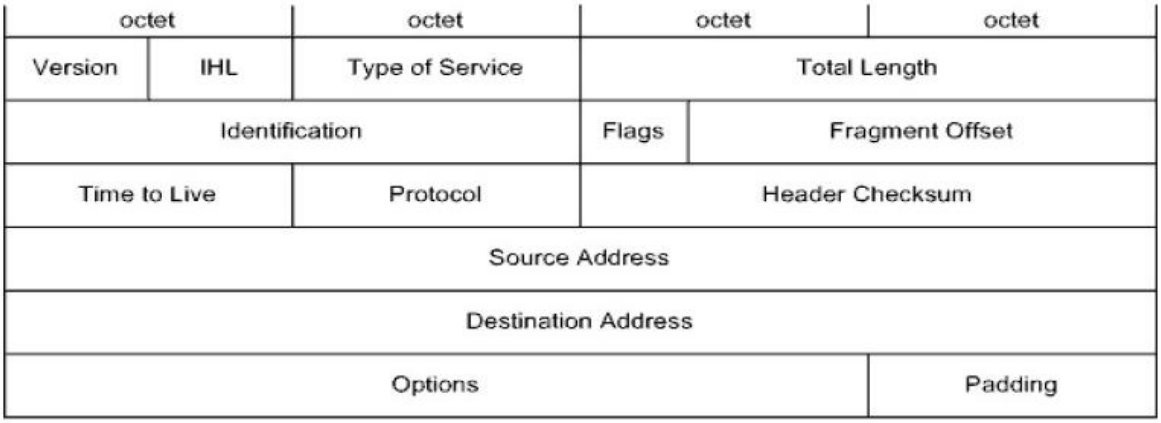
Следует отметить, что EUI-64 может использоваться не только для адресации, а и для просто идентификации устройств.

Примеры технологий с применением EUI-48: Ethernet, Wi-Fi, Token Ring

Примеры технологий с применением EUI-64: IPv6, FireWire

44 Заголовок IPv4

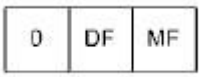
В семействе TCP/IP за адресацию на сетевом уровне отвечает протокол IP. Заголовок протокола IPv 4 (версии 4) имеет фиксированную структуру.



Поля:

1) Version -- версия (значение равно 4). (4 бита)
2) IHL (Internet Header Length) -- длина заголовка (в тридцатидвухбитных словах, минимальное значение равно 5). (4 бита)
3) Type of Service -- тип сервиса (связано с QoS). (8 бит)
4) Total Length -- общая длина заголовка и данных (в байтах, не может превышать 65535 байтов). (16 бит)
5) Identification -- уникальный идентификатор пакета (при фрагментации позволяет определить к какому пакету относится фрагмент). (16 бит)
6) Flags -- флаги. (3 бита)
7) Fragment Offset -- смещение текущего фрагмента (в шестидесятичетырехбитных словах, смещение первого фрагмента равно нулю). (13 бит)
8) Time to Live -- «время жизни» (при каждой ретрансляции уменьшается, когда становится равным нулю пакет уничтожается, в действительности уже давно измеряется как «расстояние»). (8 бит)
9) Protocol -- протокол (инкапсулируемый в поле данных). (8 бит)
10) Header Checksum -- контрольная сумма заголовка. (16 бит)
11) Source Address -- адрес источника. (32 бита)
12) Destination Address -- адрес назначения. (32 бита)
13) Options -- опции (например, связанные с безопасностью, размер вариативен). (произвольно)
14) Padding (произвольно)

Поле flags:

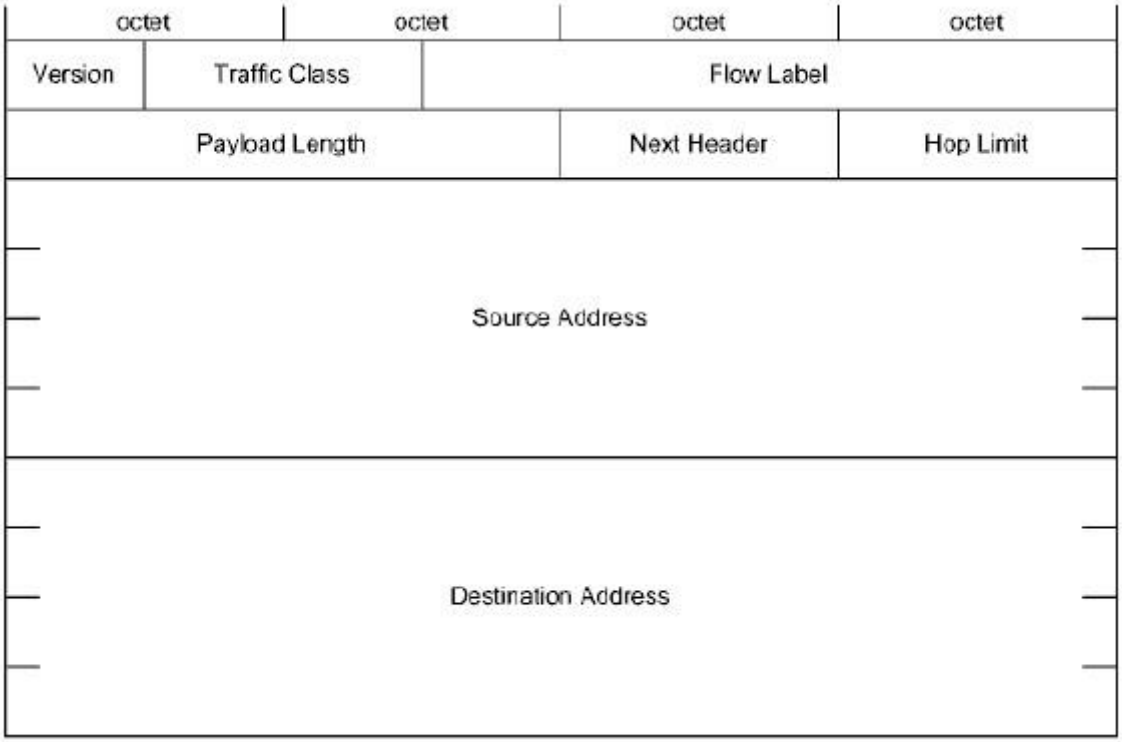


DF (Don’t Fragment): 0 - пакет фрагментирован, 1 пакет нефрагментирован

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

45 Заголовок IPv6

Заголовок протокола IPv6 имеет «гибкую» структуру. Заголовки «каскадируются» сколько заголовков нужно, столько и вставляется



Поля:

1)Version - версия (значение равно 6). (4 бита)

2)Traffic Class - класс трафика (связано с QoS). (8 бит)

3)Flow Label - метка потока (связано с QoS). (20 бит)

4)Payload Length - длина полезной нагрузки без заголовка (в байтах, аналог поля Total Length). (16 бит)

5)Next Header - селектор следующего заголовка (в том числе, аналог поля Protocol). (8 бит)

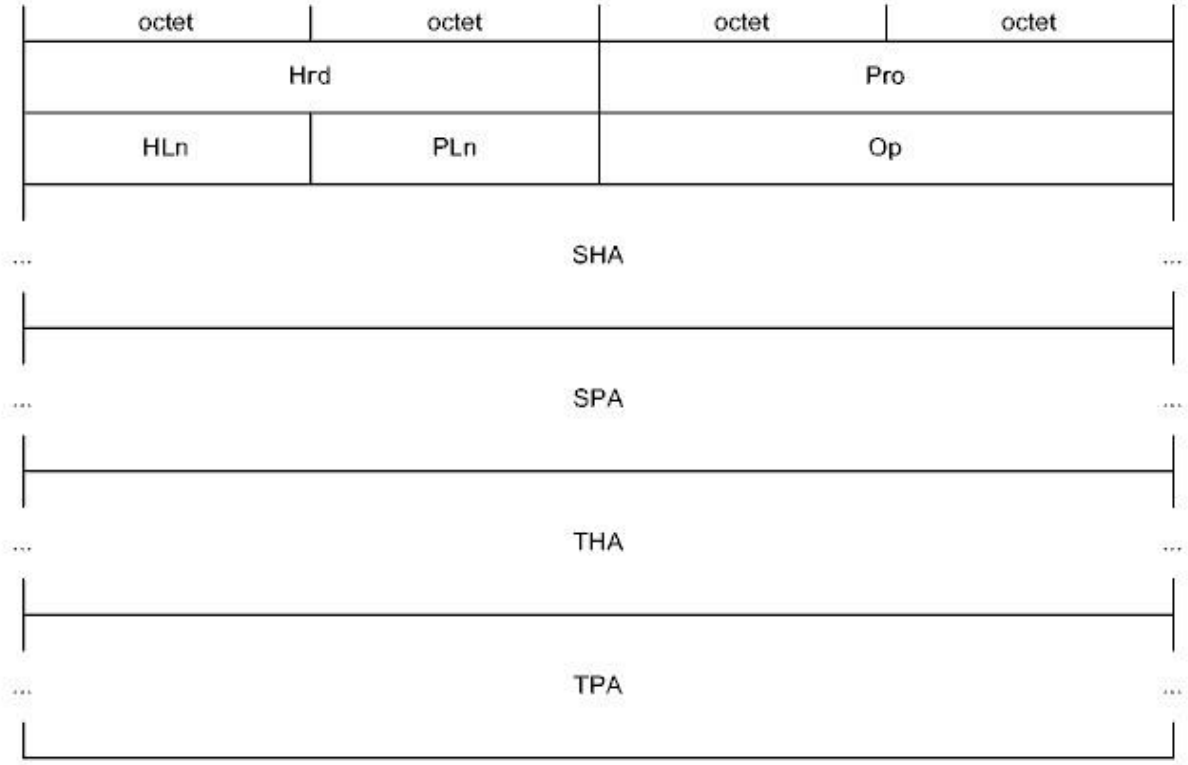
6)Hop Limit - ограничитель числа «прыжков» (аналог поля Time to Live). (8 бит)

7)Source Address - адрес источника (16 октетов)

8)Destination Address - адрес назначения (16 октетов)

46 Протокол ARP

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



Поля

1)Hrd - тип оборудования (1 - Ethernet)

2)Pro - протокол (800h - IP)

3)HLn (Hardware address Length) - длина аппаратного (физического) адреса (в байтах, 6 - Ethernet)

4)PLn (Protocol address Length) - длина протокольного (логического) адреса (в байтах, 4 - IP)

5)Op (Opcode) - код операции: 1 – Request – запрос, 2 – Reply – ответ (и некоторые другие)

6)SHA (Sender Hardware Address) - аппаратный адрес запрашивающей станции

7)SPA (Sender Protocol Address) - протокольный адрес запрашивающей станции

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

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

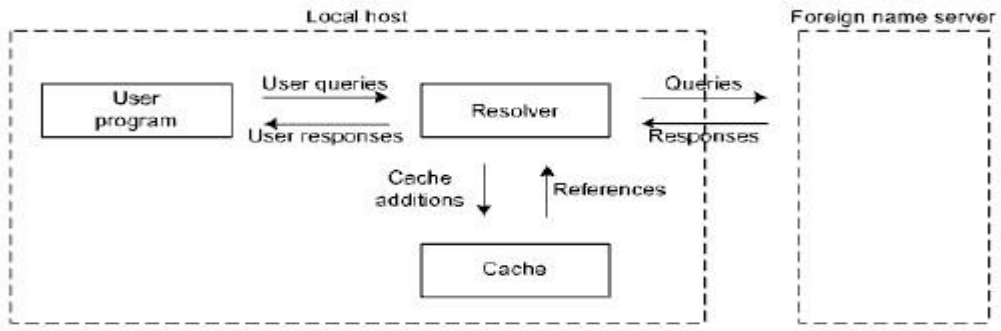
47 Структура системы DNS

Протокол системы DNS (Domain Name System) (два основных RFCs, RFC 1034 -- больше теория, RFC 1035 -- больше практика) предназначен для восстановления соответствий между IP-адресами и адресами прикладного уровня.

Следует отметить, что под **доменом** (иногда cloud) в СПД обобщенно понимают совокупность устройств, работающих в рамках некоторых единых правил.

Некоторые служебные протоколы, в том числе DNS, нельзя однозначно сопоставить с моделью OSI. Исходя из инкапсуляции, протокол DNS следует условно отнести к прикладным.

Структура системы DNS:



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

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

2)Серверы названий (name servers).

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

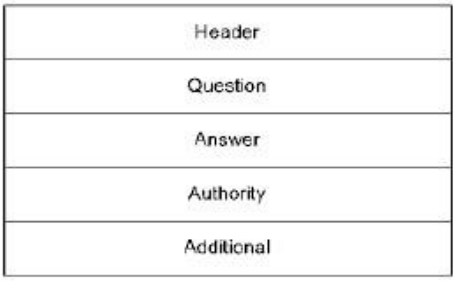
Адресное пространство доменных названий имеет иерархическую древовидную структуру. Каждый узел дерева на некотором уровне иерархии обозначают DNS меткой (DNS label) длиной от 0 до 63 байтов (должна начинаться с буквы и состоять из комбинации букв любого регистра, цифр и символа -). Метка нулевой длины зарезервирована и является корнем дерева. При присоединении станции к определенному домену ей так же присваивают метку. Доменное название строится из меток в соответствии с путем к корневой метке. Полная длина не может превышать 255 байтов. Доменное название может относиться как к отдельно взятой станции, так и к некоторой ветви дерева, то есть к DNS домену (DNS domain). Доменное название может быть, как абсолютным, то есть содержащим всю цепочку меток от станции до корневой метки, так и относительным, то есть содержащим только часть меток. Внутреннее представление метки: один байт, в котором указана длина метки, за которым следуют собственно байты метки. При интерпретации меток регистр букв не учитывается.

Согласно принятой нотации записи доменных названий метки разделяют точками, и корневая метка является крайней справа.

48 Сообщения DNS

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

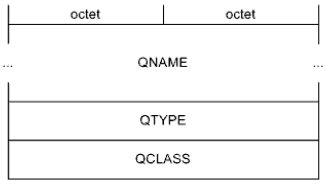
Формат сообщения DNS:



Поля:

1)Header - заголовок

2)Question - вопрос



1)QNAME (Query NAME) -- доменное название в запросе.

2)QTYPE -- (Query TYPE) -- тип запроса.

3)QCLASS (Query CLASS) -- класс запроса.

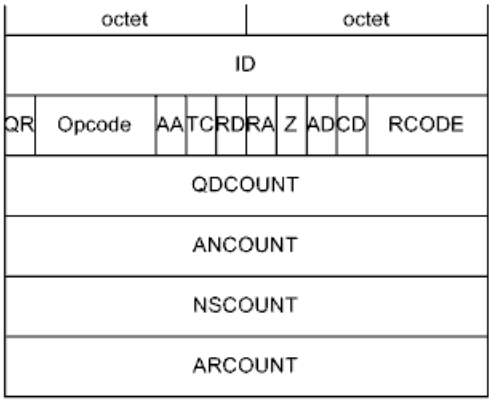
3)Answer - ответ

4)Authority - авторитетный ответ

5)Additional - дополнение

Заголовок присутствует всегда, остальные поля вариативны

Формат заголовка сообщения DNS:



Поля:

1)ID (IDentifier) – идентификатор (2 октета)

2)QR (Query/Responce) -- флаг запроса-ответа: 0 -- Query -- запрос, 1 -- Responce -- ответ. (1 бит)

3)OPCODE (OPeration CODE) -- код операции (запроса) (4 бита)

4) AA TC RD RA Z AD CD – флаги (7 бит)

5) RCODE (Response CODE) -- код ответа (4 бита)

6) QDCOUNT (Query DNS COUNT) -- количество элементов (RRs) в поле Question (обычно один). (2 октета)

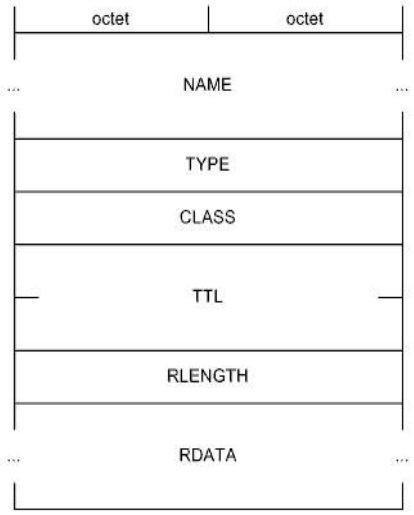
7) ANCOUNT (ANswer COUNT) -- количество элементов (RRs) в поле Answer. (2 октета)

8) NSCOUNT (Name Server COUNT) -- количество элементов (RRs) в поле Authority. (2 октета)

9) ARCOUNT (Additional Records COUNT) -- количество элементов (RRs) в поле Additional. (2 октета)

Каждой входящей в систему DNS станции (как и каждому домену) соответствует некоторое количество RRs(Resource Records) запись о ресурсах.

Формат DNS RR:



Поля:
1)NAME - доменное название (к которому относится RR, целевое при поиске)
2)TYPE - тип
3)CLASS - класс (семейство протоколов)
4)TTL (Time To Live) - «время жизни» (то есть время валидности RR, в секундах)
5)RLENGTH (Resource LENGTH) - длина данных ресурса
6)RDATA (Resource DATA) - данные ресурса (зависят от типа и класса)

Основные **типы RRs**:

1)A (A host address) - IP адрес хоста

2)NS (Name Server) - авторитетный сервер названий домена

5)CNAME (Canonical NAME) - каноническое доменное название (станции либо домена, для псевдонима)

6)SOA (Start of a zone of Authority) - оригинальные параметры зоны (сервер с изначальным описанием зоны, контактное лицо, время валидности и другие)

10) NULL - нулевая запись (произвольная информация)

12)PTR - указатель доменное название станции (при обратных преобразованиях)

13)HINFO (Host INFO) - информация о станции (процессор и ОС)

15)MX (Mail eXchange) доменное название почтового сервера в домене (включая приоритет, этот тип используется и вместо нескольких отмененных типов)

16)TXT (TeXT strings) - текстовые строки (либо строка)

28) AAAA (-) IPv6 адрес хоста

33) SRV (SeRVer selection) - описание сервиса (любого дополнительного сетевого сервиса на станции, например, файлового)

Классы RRs:
1)IN - Internet
2)CS - CSNET (устарел и аннулирован)
3)CH - Chaosnet (устарел)
4)HS - Hesiod (для БД, очень редкий)
Остальные значения классов зарезервированы

Примеры значений RRs класса IN:
A: 192.168.11.1.
CNAME: 5-508-fileserv.bsuir.by.
MX: 10 mail.bsuir.by.
NS: proxy1.bsuir.by.
PTR: 5-508-fileserv.bsuir.by.

Полное описание полей заголовка сообщения DNS:

1. ID (IDentifier) -- идентификатор (программы, сгенерировавшей запрос).
2. QR (Query/Responce) -- флаг запроса-ответа: 0 -- Query -- запрос, 1 -- Responce -- ответ.
3. OPCODE (OPeration CODE) -- код операции (запроса): 0 – QUERY (standard QUERY) -- стандартный запрос (о прямом преобразовании), 1 -- IQUERY (Inverse QUERY) -- запрос об обратном преобразовании (RFC 3425 отменен, альтернатива -- использование PTR RR), 2 -- STATUS (server STATUS request) -- запрос состояния сервера, 4 -- NOTIFY -- уведомление (об изменениях в БД о зоне) (RFC 1996), 5 -- UPDATE – обновление (динамическое обновление БД о зоне) (RFC 2136), 6 -- DSO (DNS Stateful Operations) -- стабильные DNS-операции (альтернативный унифицированный синтаксис) (RFC 8490), остальные значения зарезервированы.
4. AA (Authoritative Answer) -- флаг авторитетного ответа.
5. TC (TrunCation) -- флаг «усеченности» сообщения (при слишком длинном сообщении).
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 верифицированности ответа (RFC 4035).
10. CD (Checking Disabled) -- флаг отсутствия необходимости в криптографической верификации ответа (при запросе) (RFC 4035).
11. RCODE (Response CODE) -- код ответа: 0 -- NoError (No Error) -- ошибок нет, 1 -- FormErr (Format Error) -- ошибка в формате, 2 – ServFail (Server Failure) -- сбой сервера, 3 -- NXDomain (Non-eXistent Domain Name) -- доменное название не существует, 4 -- NotImp (Not Implemented) -- запрос не поддерживается, 5 -- Refused (Query Refused) -- запрос отклонен, остальные значения относятся к расширениям DNS (RFC 2136, RFC 2845, RFC 2930, RFC 4635, RFC 6672, RFC 6891, RFC 7873, RFC 8490) и зарезервированы.
12. QDCOUNT (Query DNS COUNT) -- количество элементов (RRs) в поле Question (обычно один).
13. ANCOUNT (ANswer COUNT) -- количество элементов (RRs) в поле Answer.
14. NSCOUNT (Name Server COUNT) -- количество элементов (RRs) в поле Authority.
15. ARCOUNT (Additional Records COUNT) -- количество элементов (RRs) в поле Additional.

49 Виртуальные соединения в сети передачи данных

Одним из ключевых терминов транспортного уровня является термин **соединение**. По сути дела, понятие соединения связано с понятием готовности. Если абоненты находятся в состоянии «нормальной готовности» передавать или принимать данные, то считают что между ними установлено соединение. С учетом абстрагирования от более низких уровней модели OSI и инкапсуляции, соединение может быть выражено неявно.

Нужно отличать виртуальные соединения (virtual connections) от физических соединений (physical connections). Абоненты программы физически соединены быть не могут. Следовательно, применительно к ним, соединения являются сугубо виртуальными.

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

1)Организация взаимодействия абонентов программ

2)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:

1)PVCs (Permanent Virtual Circuits) выделенные виртуальные цепи

2)SVCs (Switched Virtual Circuits) коммутируемые виртуальные цепи

Термин виртуальный канал (virtual channel) может в равной степени подходить как к виртуальным соединениям, так и к виртуальным цепям. При разговоре о соединениях невозможно обойти стороной вопрос о надежности. Существуют два способа организации взаимодействия:

1. Без гарантированной доставки -- в СПД предпринимаются определенные усилия по доставке пакетов, но при этом ничего не гарантируется (при необходимости, соответствующий контроль возлагается на программы-абоненты).

2. С гарантированной доставкой -- алгоритм работы транспортной службы гарантирует доставку пакетов (программы-абоненты могут не контролировать наличие и очередность пакетов).

Однако, соединение без гарантированной доставки практического смысла не имеет. Поэтому наличие соединения как правило говорит о надежности.

50 Классификация оконных механизмов, используемых в сети передачи данных

Простейшим подходом к обеспечению контроля доставки информационных пакетов является применение метода, который обобщенно можно назвать **методом запросов подтверждений** (requests/acknowledges). Оптимизировать обмен данными позволяет применение **оконного метода**, суть которого состоит в том, что до перехода к ожиданию квитанций передается не один, а несколько пакетов.

Выделяют два основных критерия классификации оконных методов.

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

1)Статическим - неизменяемый размер окна заложен в протокол или устанавливается на весь сеанс обмена

2)Динамическим размер окна может изменяться (увеличиваться или уменьшаться) в процессе передачи сообщения

Исходя из способа обработки очереди пакетов, окно может быть:

1)Фиксированным - перед формированием следующего окна текущее должно быть полностью «закрыто», то есть должны быть приняты все необходимые квитанции.

2)Скользящим - существует возможность сдвигать окно относительно последовательности пакетов.

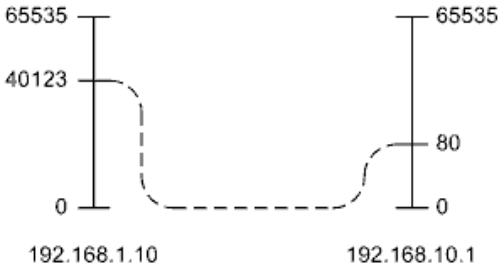
С точки зрения реализации, наиболее простым является статическое окно фиксированного размера. Основной его недостаток состоит в отсутствии возможности адаптации к изменениям в СПД.

Динамическое окно позволяет успешно адаптироваться к изменениям в СПД. При увеличении загруженности окно целесообразно сужать, а при снижении – расширять.

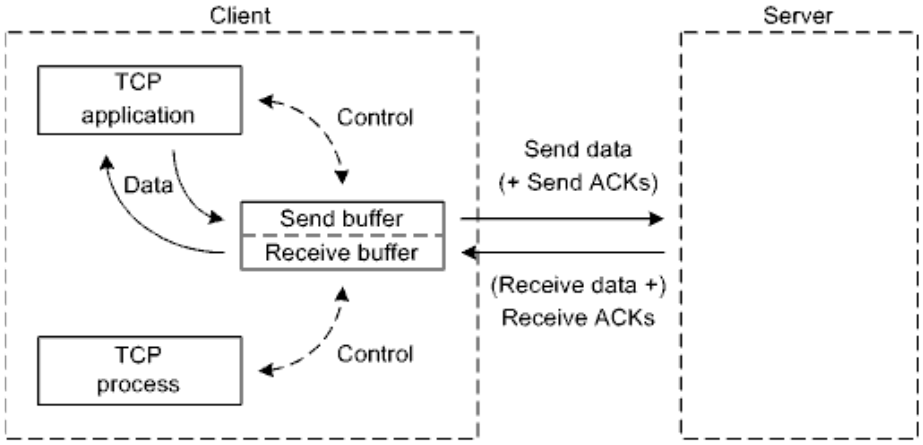
Скользящее окно, особенно в сочетании с динамическим, позволяет ускорить адаптацию к топологическим и другим изменениям в СПД.

51 Структура системы TCP

TCP соответствует клиент-серверной модели. **Сокет** (socket) -- это «привязка» к виртуальному каналу, соединяющему между собой два взаимодействующих сетевых процесса, с точки зрения одного (любого) из этих процессов, причем с учетом всех трех уровней адресации.



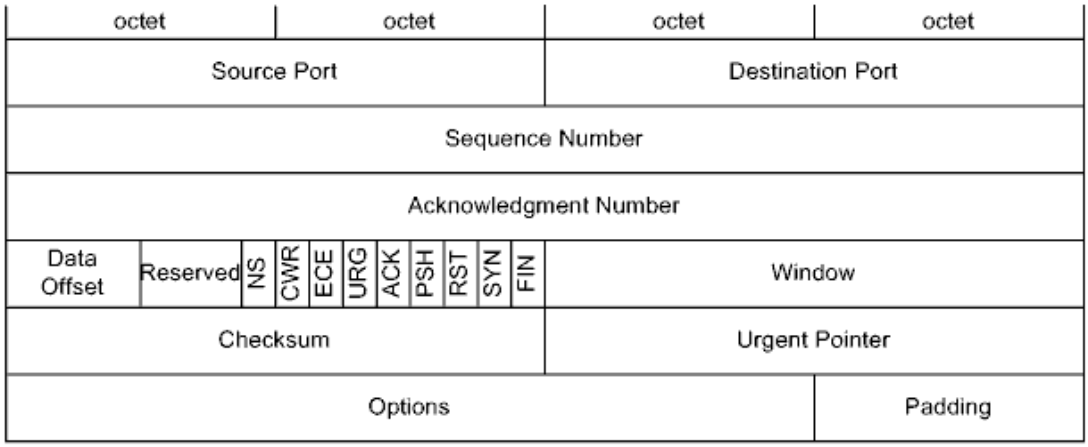
Структура соединения TCP:



Применительно к каждому TCP соединению нужно выделять приложение, производящее или потребляющее сетевые данные, и TCP процесс, предоставляющий коммуникационные услуги (например, специальный драйвер ОС). Синхронизировать работу приложения и TCP процесса можно только с помощью буферизации. TCP интерфейс, которым пользуется приложение, состоит из примитивов для работы с буфером, позволяющих контролируя записывать или считывать данные. Доступ к буферу имеет и TCP процесс, который отслеживает наполнение буфера и, используя ресурсы более низких уровней, организует прием или передачу данных.

//мы считаем что на этом структура все, детали реализации не входят

52 Заголовок TCP



Поля:

1)Source Port - программный порт источника (2 октета)

2)Destination Port - программный порт назначения (2 октета)

3)Sequence Number (SN) - последовательный номер (сегмента)(4октета)

4)Acknowledgment Number (AN) - подтверждающий номер (4 октета)

5)Data Offset - смещение данных (в 32 ухбитных словах) (4 бита)

6)Reserved - зарезервировано (должно равняться нулю) (3 бита)

7)NS (Nonce Sum) – флаг - контрольная сумма для проверки правильности кодов явных уведомлений о заторах (связан с QoS, связан с IP заголовком) (1 бит)

8)CWR (Congestion Window Reduced) - флаг уменьшения окна затора при явном уведомлении о заторе (1 бит)

9)ECE (Explicit Congestion Notification Echo) - флаг подтверждения явного уведомления о заторе (1 бит)

10)URG (URGent Pointer field significant) - флаг значимости указателя на экстренные данные (1 бит)

11)ACK (ACKnowledgment field significant) - флаг значимости подтверждающего номера (1 бит)

12)PSH (PuSH Function) - флаг принудительной доставки данных (без буферизации) (1 бит)

13)RST (ReSeT the connection) - флаг разрыва соединения (из-за сбоя на одной из взаимодействующих сторон) (1 бит)

14)SYN (SYNchronize sequence numbers) - флаг синхронизации последовательных номеров (1 бит)

15)FIN (No more data from sender) - флаг последних данных (1 бит)

16)Window (W) - предлагаемое окно (2 октета)

17)Checksum - контрольная сумма (2 октета)

18)Urgent Pointer - указатель на экстренные данные (2 октета)

19)Options - опции (MSS) (3 октета)

20)Padding – наполнитель (1 октета)

53 Протокол TCP

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

Установление TCP соединения, известное как «тройное рукопожатие» (three way handshake), основывается на использовании флагов SYN и ACK

Несмотря на то, что процесс установления соединения несимметричен, в дальнейшем, в общем случае, оно используется в полнодуплексном режиме.

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

По правилу протокола, поле SN пересылаемого сегмента отражает собственный SN этого сегмента. По другому правилу, в поле AN указывается SN ожидаемого сегмента, коим является следующий по порядку сегмент. При установлении соединения данные не пересылаются. Поэтому, для того чтобы не нарушать указанные правила, в качестве SNs используют невключенные в нумерацию байтов сообщения ISNs, а в качестве ANs просто инкрементированные SNs. Обойтись без передачи SNs при установлении соединения невозможно, так как стороны должны однозначно идентифицировать это соединение. После синхронизации SNs соединение считается установленным.

Не смотря на предоставляемые возможности, данные вполне могут пересылаться только в одном направлении, то есть в симплексном режиме. При этом в направлении, попутном направлению пересылки данных, в качестве AN используется SN следующего по порядку несуществующего (вообще, либо уже, либо пока) сегмента, что никоим образом не противоречит уже приведенным правилам. Если сегментов с данными пересылается несколько, то ANs дублируются столько раз, сколько нужно. Это приводит к дублированию SNs в ответных сегментах без данных. Аналогичные дублирования возникают и при приостановке пересылки данных в определенном направлении.

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.

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.

Проблема 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. Отрицательные подтверждения не предусмотрены вообще. Принимающий TCP процесс подтверждает все принятые сегменты с данными, причем подтверждает всегда. При этом если принята копия (что говорит о потере подтверждения), то она удаляется. Получение сегмента с SN больше ожидаемого говорит о возможной потере сегментов с данными или о разупорядочивании.

54 Усовершенствования протокола TCP

Хорошо известна проблема, вошедшая в историю под обобщенным названием «синдром глупого окна» («silly window syndrome»), в свое время «стопорившая» значительную часть пространства Internet. 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».

Решение Нэгла позволяет побороть «синдром глупого окна» когда передающей стороне требуется часто отправлять небольшие сегменты с данными.

Решение Кларка позволяет побороть «синдром глупого окна» когда принимающей стороной часто анонсируется небольшое предлагаемое окно.

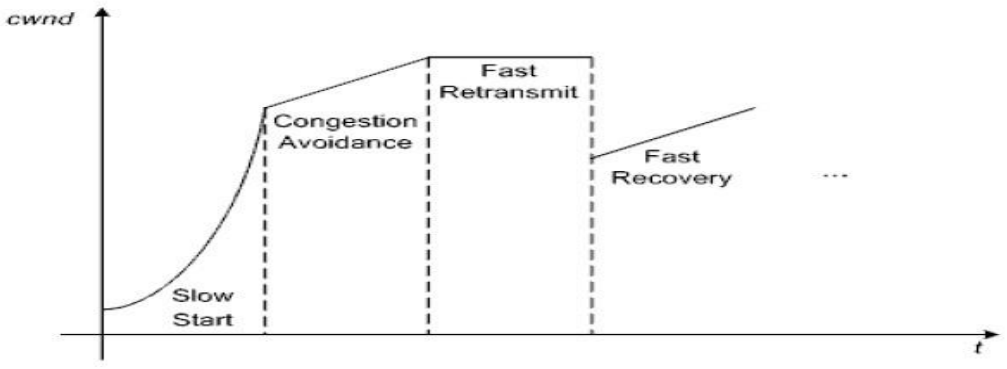
Также стандартизированы четыре дополнения Ван Якобсона, призванные бороться с перегрузками в СПД:

1)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)

2)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.

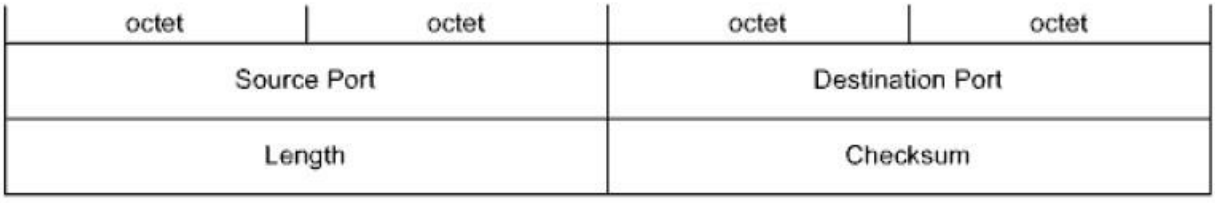
3)Быстрая повторная передача (fast retransmit). При получении принимающей стороной разупорядоченного сегмента с данными (возможно из-за потери ожидаемого сегмента с данными) незамедлительный повтор подтверждения с AN недостающего сегмента с данными. При получении передающей стороной трех одинаковых подтверждений незамедлительный повтор сегмента с данными согласно AN. Что, в некоторых ситуациях, позволяет успешно переслать потерянный сегмент еще до наступления тайм аута.

4)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 транспортного уровня UDP (User Datagram Protocol) реализует способ пересылки данных без гарантии доставки, часто называемый дейтаграммным (datagram)(хотя user datagram это пакет с контролируемыми пользователем данными, а datagram это любой пакет с данными)



Поля:

1)Source Port - программный порт источника (2 октета)

2)Destination Port - программный порт назначения (2 октета)

3)Length - длина дейтаграммы включая заголовок (в байтах) (2 октета)

4)Checksum - контрольная сумма (подзаголовок, плюс заголовка, плюс данных) (2 октета)

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

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

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

Физически проводные СрПД выражаются в виде:

1.Отдельных проводов (wires).
2.Кабелей (cables).
3.Шлейфов (ribbon cables).

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 характеристики, влагостойкость, широкий диапазон рабочих температур, наличие дополнительных упрочняющих или гальванически развязывающих вставок.

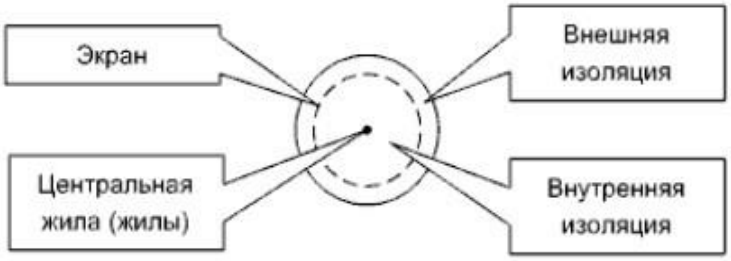
Indoor-кабели отличаются от outdoor-кабелей меньшими габаритами и массой, большей гибкостью, лучшей пожаростойкостью, при сохранении тех же ключевых достоинств.

Кабели cords являются сравнительно простыми и низкокачественными.

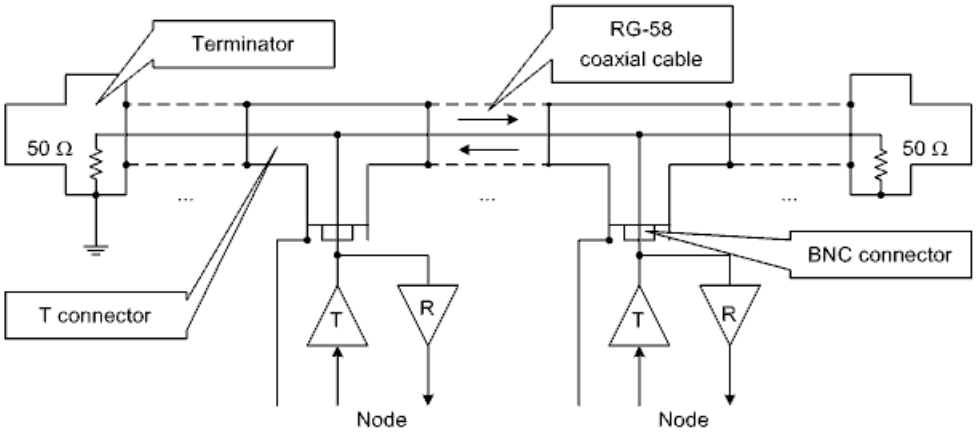
57 Среды передачи данных на основе коаксиальных кабелей

В сегментах КС широко использовали три базовых вида коаксиальных кабелей: с волновым сопротивлением 50 Ω -- RG-8, RG-58, и с волновым сопротивлением 75 Ω -- RG-59.

Коаксиальные outdoor- и indoor-кабели отличаются от cord-кабелей в основном внешней изоляцией.



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



Коаксиальные кабели производители обычно выпускают черными, реже серыми.

// непонятно откуда

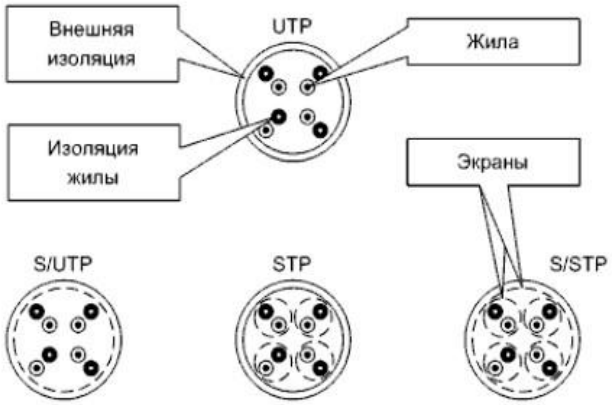
Широко используется в телевидении. Важное достоинство – передавать в один и тот же момент множество сигналов.

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

Коаксиальные кабели производители обычно выпускают черными, реже серыми.

58 Среды передачи данных на основе витых пар

В сегментах КС широко используются четыре вида витых пар:



Где:

•TP – twisted pair

•S – shielded

•U – unshielded

•может быть F – Foiled (если для изготовления экрана применена фольга).

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

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 однорангового оборудования, например непосредственного связывания двух пользовательских станций, используют кросс-кабели -- пары TD и RD скрещены. (Полная аналогия с вариантами соединений ООД и АПД.)

Сама витая пара состоит из 8 кабелей (бело-оранжевый, оранжевый, зелёный, синий, бело-синий, зелёный, бело-коричневый, коричневый). Для подключения кабелей на основе витых пар применяют разъемы RJ45. У нас традиционно выбирают стандарт 568-B.

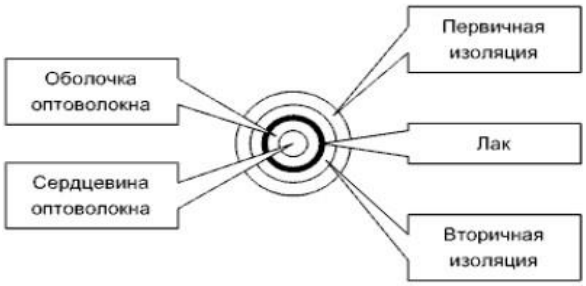
Цвета самих кабелей (и колпаков разъемов) в стандартах не оговорены.

От производителей более-менее доступны кабели 12 стандартных цветов (привязаны к палитре RAL).

Обычные кабели имеют серый цвет (различные оттенки). Другие цвета (например, оранжевый или, даже, белый) «говорят» о более высоком качестве (например, лучшей пожарной безопасности). И востребованы для маркировки кабельных систем.

59 Среды передачи данных на основе оптоволоконных кабелей

Рабочими компонентами оптоволоконных кабелей являются световоды изготовленные из оптоволокна, т.е. особого кварцевого стекла. Световод – это оптический волновод. Рабочим компонентом является оболочка и сердцевина.



Большое количество изоляции обусловлено хрупкостью кабеля.

В стандартах также предусмотрены 8 видов световодов: OM1, OM2, OM3, OM4, OM5 – многорежимные, OS1, OS2, OS1a – однорежимные. Также 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).

Еще одно отличие заключается в том, что в стандартах оговорена цветовая маркировка оптоволоконных световодов, кабелей, разъемов, а также модулей (со световодами разных видов) в составе кабелей.

Если цветовая маркировка по тем или иным причинам не подходит, то, как альтернатива, предусмотрена маркировка штриховкой.

60 Физический уровень Ethernet

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

Ключевые использовавшиеся либо используемые стандарты:

10BASE5 (1983) -- «толстый» (thick) коаксиальный кабель 50 Ω (до 500 m) плюс внешние приемопередатчики;

10BASE2 (802.3a, 1985) -- «тонкий» (thin) коаксиальный кабель 50 Ω (до 185 m) плюс интегрированные приемопередатчики;

10BASE-T (802.3i, 1990) -- две телефонные витые пары (до 100 m);

10BASE-FL (802.3j, 1993) -- два многорежимных световода (до 500 m) плюс нечетко регламентированные источники излучения (обычно LEDs);

100BASE-TX (802.3u, 1995) -- две неэкранированные либо экранированные витые пары категории 5 (до 100 m);

100BASE-FX (802.3u, 1995) -- два многорежимных световода (до 2 km) (реализации поддерживают и однорежимные световоды длиной десятки километров) плюс нечетко регламентированные источники излучения (реализации поддерживают LEDs и лазеры);

1000BASE-SX (802.3z, 1998) -- два многорежимных световода (до 275 m -- 62,5 um, до 550 m -- 50 um) плюс коротковолновые (short wavelength) лазеры (770 -- 860 nm);

1000BASE-LX (802.3z, 1998) -- два однорежимных (до 5 km) либо многорежимных световода (до 550 m) плюс длинноволновые (long wavelength) лазеры (1270 -- 1355 nm);

1000BASE-T (802.3ab, 1999) -- четыре неэкранированные либо экранированные витые пары категории 5 (до 100 m);

2.5GBASE-T (802.3bz, 2016) -- четыре неэкранированные либо экранированные витые пары категории 5e (расстояние до 100 m);

5GBASE-T (802.3bz, 2016) -- четыре неэкранированные либо экранированные витые пары категории 5e (расстояние до 100 m);

10GBASE-SR (802.3ae, 2002) -- два многорежимных световода (до 33 m -- 62,5 um, до 400 m -- 50 um) плюс коротковолновые лазеры (840 -- 860 nm);

10GBASE-LR (802.3ae, 2002) -- два однорежимных световода (до 10 km) плюс длинноволновые лазеры (1310 nm);

10GBASE-ER (802.3ae, 2002) -- два однорежимных световода (до 30 km) плюс экстрадлинноволновые (extra long wavelength) лазеры (1550 nm);

10GBASE-T (802.3an, 2006) -- четыре неэкранированные (до 55 m) либо экранированные (до 100 m) витые пары категории 6, либо четыре неэкранированные, либо экранированные витые пары категории 6A (до 100 m).

61 Структурированные кабельные системы и их модели

Структурированная кабельная система (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).

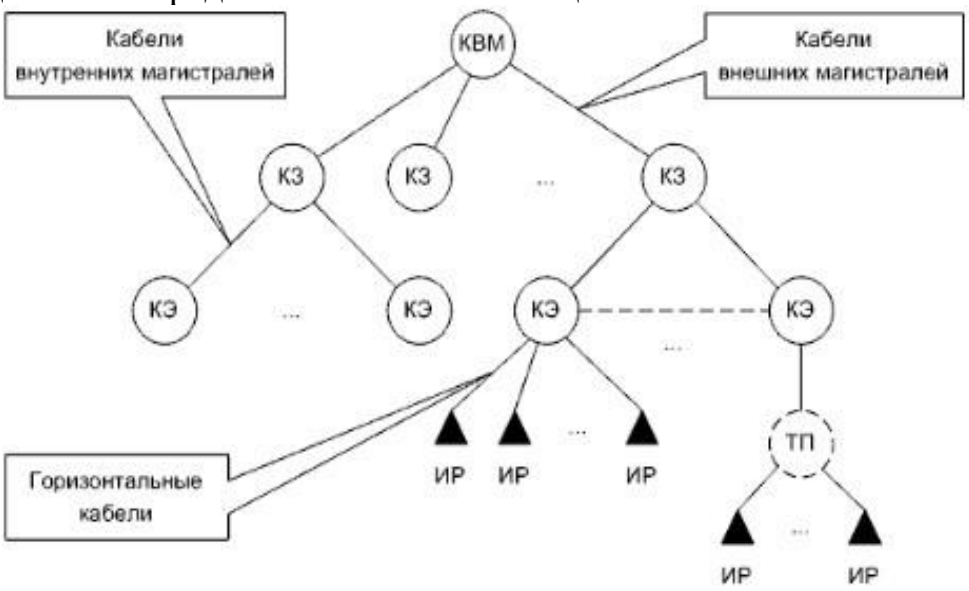
Аппаратные отличаются от кроссовых тем, что в них, наряду с активным, пассивным, монтажным и вспомогательным сетевым оборудованием, может быть размещено серверное оборудование.

В общем случае, согласно стандартам ISO/IEC 11801, ANSI/TIA/EIA-568 и EN 50173, СКС включает в себя три подсистемы:

1. Подсистема 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.



Основная модель СКС

КВМ -- кроссовая внешних магистралей,

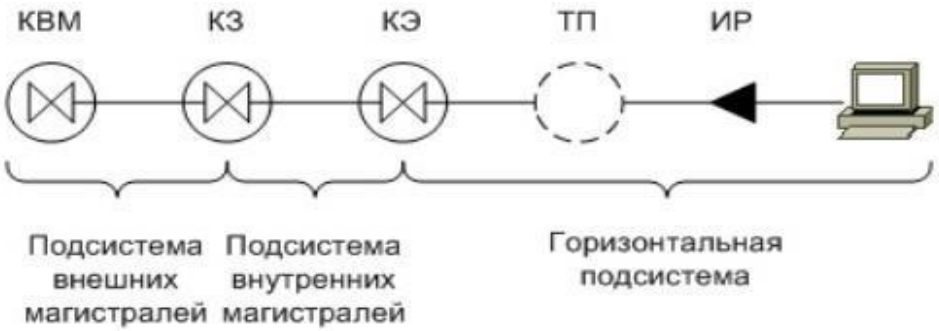
КЗ -- кроссовая здания,

КЭ -- кроссовая этажа,

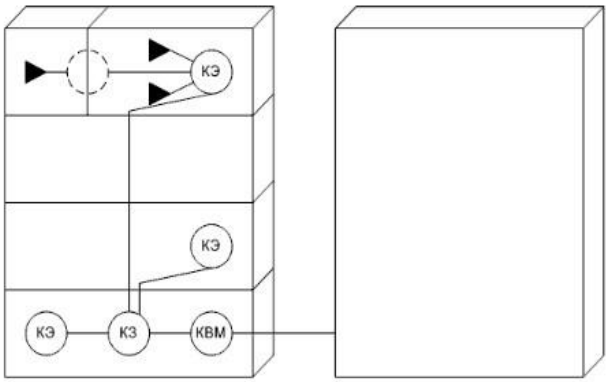
ТП -- точка перехода,

ИР -- информационная розетка рабочего места.

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



Горизонтальная модель СКС



Функциональная модель СКС здания

Таким образом, суммарно СКС содержит: кабели и сетевое оборудование всех трех подсистем, плюс точки перехода (consolidation points), плюс информационные розетки.

Иерархическая сетевая модель Cisco хорошо «ложится» на модели СКС.

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.

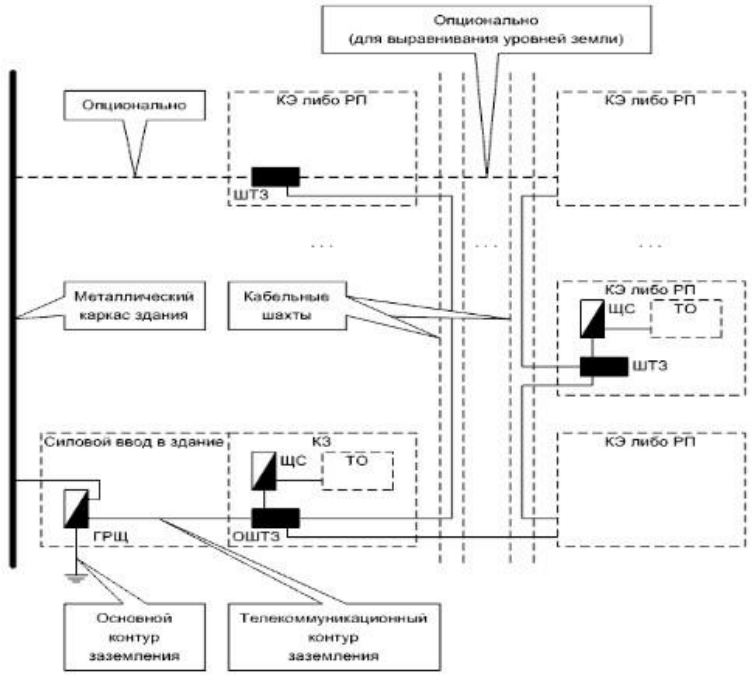
Заземление необходимо для:

1)Предотвращение поражения людей электрическим током

2)Защита кабельных трактов и сетевого оборудования от выхода из строя/помех

3)Обеспечения возможности прохождения сигналов применительно некоторым видам сетевого оборудования.

Согласно стандарту TIA-607, в дополнение к основному контуру заземления (grounding electrode) здания либо сооружения, создают так называемый телекоммуникационный контур заземления или, по-другому, контур рабочего заземления (telecommunications grounding/bonding).



Модель заземления

•ГРЩ – главный распределительный щит здания

•ШТЗ – шина телекоммуникационного заземления

•ОШТЗ – основная ШТЗ

•ЩС – щит силовой

•РП – рабочее место

•ТО – телекоммуникационное оборудования

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.

Для защиты от электрических разрядов в атмосфере (особенно вертикальной подсистемы) применяют специальные устройства -- грозоразрядники (lightning gaps).

63 Пожарная безопасность структурированных кабельных систем

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

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

1)Plenum – сюда относят кабели, которые можно располагать как угодно (при притоке воздуха, достаточного для поддержания горения, так называемая plenum-область)

2)Riser – кабели, которые можно прокладывать в кабельных шахтах

3)General purpose – кабели, которые можно прокладывать везде, кроме plenum-областей.

4)Residential – кабели, на прокладку которых нанесены определённые ограничения (например, только для жилых помещений)

В состав маркировки кабелей обычно вводят дополнительные обозначения материала оболочек:

1. PVC (PolyVinyl Chloride) -- ПВХ (поливинил хлорид).
2. PE (PolyEthylene) -- полиэтилен.
3. PA (PolyAmide) -- полиамид (нейлон).
4. FR (Flame Retardant) -- огнестойкий.
5. LS (Low Smoke) -- низкое выделение дыма при горении.
6. NC (Non Corrosive) -- не подвержен коррозии.
7. UVR (Ultra Violet Resistant) -- не подвержен влиянию ультрафиолетового излучения.
8. HF (Halogen Free) = NH (No Halogen) = ZH (Zero Halogen) -- не содержит галогенов.
9. CST (Corrugated Steel Tape armor равно armour) – бронирован гофрированной стальной лентой.

64 Технология PoE

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), -- технологии под общим названием **PoE (Power over Ethernet)**.

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).

В структуру PoE входят ряд блоков:

1)PSE (Power Sourcing Equipment) – вводит питающее напряжение в кабель.

2)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.

Исходя из потребляемой мощности, PDs делят на пять стандартных классов:

Class 0. 0,44 -- 12,95 W -- по умолчанию.

Class 1. 0,44 -- 3,84 W -- очень малой мощности.

Class 2. 3,84 -- 6,49 W -- малой мощности.

Class 3. 6,49 -- 12,95 W -- средней мощности.

Class 4. 12,95 -- 25,5 W -- большой мощности.