КУРС ЛЕКЦИЙ

по дисциплине

«Настройка и сопровождение сетевой инфраструктуры»

Аспирант каф. Э4, инженер отд. 2.1

Мамедов В.М.

2021-2022 гг. Москва

# Содержание курса

[Содержание курса 2](#_Toc89520116)

[Модуль I. Основы сетей передачи данных. Технологии физического уровня 6](#_Toc89520117)

[Лекция I.1. Эволюция компьютерных сетей 6](#_Toc89520118)

[Введение 6](#_Toc89520119)

[Возникновение глобальных сетей 8](#_Toc89520120)

[Возникновение локальных сетей 9](#_Toc89520121)

[Лекция I.2. Общие принципы построения сетей 11](#_Toc89520122)

[Классическая схема построения сети 14](#_Toc89520123)

[Физическая среда передачи данных в локальных сетях 18](#_Toc89520124)

[Принципиально важные параметры кабелей 19](#_Toc89520125)

[Используемые стандарты на кабелей 19](#_Toc89520126)

[Кабели на основе витых пар 20](#_Toc89520127)

[Коаксиальные кабели 22](#_Toc89520128)

[Оптоволоконные кабели 23](#_Toc89520129)

[Бескабельные каналы связи 26](#_Toc89520130)

[Лекция I.3. Коммутация каналов и пакетов 28](#_Toc89520131)

[Коммутация каналов 28](#_Toc89520132)

[Коммутация пакетов 30](#_Toc89520133)

[Постоянная и динамическая коммутация 36](#_Toc89520134)

[Пропускная способность сетей с коммутацией пакетов 37](#_Toc89520135)

[Числовой пример скорости работы коммутаций 39](#_Toc89520136)

[Ethernet как технология коммутации пакетов 41](#_Toc89520137)

[Лекция I.4. Стандартизация и классификация сетей 48](#_Toc89520138)

[Классификация сетей 48](#_Toc89520139)

[Стандартизация сетей 50](#_Toc89520140)

[Протокол и стек протоколов 52](#_Toc89520141)

[Общая характеристика модели OSI 53](#_Toc89520142)

[Вспомогательные протоколы транспортной системы 60](#_Toc89520143)

[Лекция I.5. Сетевые характеристики и качество обслуживания 61](#_Toc89520144)

[Производительность 62](#_Toc89520145)

[Надежность и безопасность 66](#_Toc89520146)

[Расширяемость и масштабируемость 68](#_Toc89520147)

[Прозрачность 68](#_Toc89520148)

[Поддержка разных видов трафика 70](#_Toc89520149)

[Управляемость 71](#_Toc89520150)

[Совместимость 73](#_Toc89520151)

[Выводы 73](#_Toc89520152)

[Семинар I.1. Линии связи 74](#_Toc89520153)

[Семинар I.2. Кодирование и мультиплексирование данных 75](#_Toc89520154)

[Аналогово-цифровое преобразование 75](#_Toc89520155)

[Дискретизация по времени и квантование по уровню 75](#_Toc89520156)

[Мультиплексирование данных 75](#_Toc89520157)

[Кадр. Межкадровая задержка 75](#_Toc89520158)

[Мультиплексирование и демультиплексирование 75](#_Toc89520159)

[Временная и амплитудная модуляция. Несущая волна 75](#_Toc89520160)

[Семинар I.3. Принципы организации первичных сетей 75](#_Toc89520161)

[Организация локальной сети 75](#_Toc89520162)

[Установка и настройка локального сервера 75](#_Toc89520163)

[Передача файлов по протоколам html/ftp 75](#_Toc89520164)

[Семинар I.4. Ethernet в локальных сетях 75](#_Toc89520165)

[Семинар I.5. Ethernet операторского класса 79](#_Toc89520166)

[Предпосылки создания Ethernet операторского класса (CGE) 79](#_Toc89520167)

[Ограничения операторов 80](#_Toc89520168)

[Исходная позиция: Metro-Ethernet 81](#_Toc89520169)

[Расширение до Ethernet операторского класса 81](#_Toc89520170)

[«Сервисы Ethernet» операторского класса 82](#_Toc89520171)

[Транспорт сервисов Ethernet 82](#_Toc89520172)

[Альтернативные признаки, или Чем ЛС отличается от ГлС 83](#_Toc89520173)

[Как преодолеть различия ЛС и ГлС на пути создания CGE 84](#_Toc89520174)

[Синхронные сети Ethernet 85](#_Toc89520175)

[Модуль II. Сети TCP/IP. Сетевые информационные службы 87](#_Toc89520176)

[Лекция II.1. Адресация в стеке протоколов TCP/IP. Протокол межсетевого взаимодействия IP. IPv6 как развитие стека TCP/IP 87](#_Toc89520177)

[Основы TCP/IP 87](#_Toc89520178)

[Уровневая модель TCP/IP 88](#_Toc89520179)

[Канальный уровень 88](#_Toc89520180)

[Межсетевой уровень 89](#_Toc89520181)

[Транспортный уровень 89](#_Toc89520182)

[Прикладной уровень 92](#_Toc89520183)

[Маска подсети и IP-адреса 92](#_Toc89520184)

[ICMP и IGMP 94](#_Toc89520185)

[Порты, сокеты и DNS 94](#_Toc89520186)

[Стек протоколов TCP/IP 96](#_Toc89520187)

[Point-to-Point протоколы 97](#_Toc89520188)

[Лекция II.2. Информационные службы IP-сетей. Основы web-технологии 97](#_Toc89520189)

[HTML/XHTML и CSS 97](#_Toc89520190)

[Использование JavaScript 99](#_Toc89520191)

[Семинар II.1. Протоколы транспортного уровня TCP и UDP 103](#_Toc89520192)

[Семинар II.2. Служба управления сетью. DHCP, DNS, DDNS 103](#_Toc89520193)

[Модуль III. Безопасность компьютерных сетей 104](#_Toc89520194)

[Лекция III.1. Основные понятия и принципы ИБ 104](#_Toc89520195)

[ГОСТ «Защита информации» 104](#_Toc89520196)

[Классификация угроз и атак 105](#_Toc89520197)

[ФЗ «Об информации, ИТ и о защите информации» 106](#_Toc89520198)

[Персональные данные 109](#_Toc89520199)

[Семинар III.1. Технологии безопасности на основе анализа трафика 112](#_Toc89520200)

[Система анализа сетевого трафика нового поколения (NDR) 112](#_Toc89520201)

[Системы учета и обработки компьютерных угроз (Threat Intelligence) 112](#_Toc89520202)

[Поиск угроз (Threat hunting) 113](#_Toc89520203)

[Средства поведенческого анализа («песочницы») 115](#_Toc89520204)

[Приманки для хакеров («Honeypot») 115](#_Toc89520205)

[Развитие технологий обнаружения компьютерных атак в России 116](#_Toc89520206)

[Лабораторные работы 119](#_Toc89520207)

[ЛР1. Создание модели локальной сети 119](#_Toc89520208)

[ЛР2. Исследование кабеля «Витая пара» 119](#_Toc89520209)

[ЛР3. Структуризация локальных вычислительных сетей с помощью коммутаторов 119](#_Toc89520210)

[ЛР4. Тестирование работы сети 119](#_Toc89520211)

# Модуль I. Основы сетей передачи данных. Технологии физического уровня

## Лекция I.1. Эволюция компьютерных сетей

### Введение

Компьютерные сети являются частным случаем распределенной вычислительной системы, в которой несколько компьютеров согласованно выполняет набор взаимосвязанных задач, осуществляя обмен данными в автоматическом режиме.

|  |  |
| --- | --- |
| **Опр. 1** | **Распределенными** **вычислительными системами** называют системы, имеющие более одного центра обработки данных. |

*Ограниченная доступность ЭВМ*

Первые компьютеры 50-х годов (большие и дорогостоящие) использовались очень небольшим числом профессиональных пользователей-ученых. Они функционировали в режиме пакетной обработки и не были предназначены для интерактивной работы пользователя.

*Эпоха перфокарт*

Системы пакетной обработки создавались на базе **мэйнфрейма** - мощного универсального компьютера. Пользователи подготавливали перфокарты, содержащие данные и команды программ, и передавали их в вычислительный центр. Операторы вводили эти карты в компьютер, а готовые результаты пользователи получали на следующий день. Интерактивный режим работы, при котором можно с терминала оперативно руководить процессом обработки своих данных, для пользователей был бы удобней, но их интересами на первых этапах развития вычислительных систем в значительной степени пренебрегали. В ущерб эффективности работы использующих его специалистов основной считалась эффективность работы самого дорогого устройства вычислительной машины - процессора.

*Терминал – первый пользовательский интерфейс*

По мере развития и удешевления элементной базы процессоров в начале 60-х годов прошлого века появились новые способы организации вычислительного процесса, которые позволили учесть интересы пользователей. Начали развиваться интерактивные многотерминальные системы разделения времени.

|  |  |
| --- | --- |
| **Опр. 2** | **Терминал** - устройство, соединенное с компьютером посредством линий связи и выполняющее определенные ограниченные действия, связанные с вводом выводом информации. |

В таких системах каждый пользователь получал собственный терминал, с помощью которого он мог вести диалог с центральным компьютером. Количество одновременно работающих с компьютером пользователей зависело от его мощности так, чтобы ему была не слишком заметна параллельная работа с компьютером других участников процесса.

Терминалы стали размещать на территории всего предприятия, организации, научного центра. При таком способе взаимодействия информационный процесс оставался полностью централизованным, однако некоторые функции, такие как ввод и вывод данных, стали распределенными. Подобные многотерминальные системы имели внешнее сходство с локальными вычислительными сетями. Каждый пользователь получал доступ к периферийным устройствам и общим файлам, при этом у него создавалась иллюзия единоличного использования компьютера, так как он мог запускать нужную ему программу в любой момент и практически сразу получать результат. Многотерминальные системы, работающие в режиме разделения времени, стали первым этапом создания локальных вычислительных сетей. Однако эти системы, имевшие внешнее сходство с распределенными системами, поддерживали только централизованную обработку данных.

*Соотношение ЦЕНА-ПРОИЗВОДИТЕЛЬНОСТЬ*

Кроме того, потребность предприятий и организаций в создании локальных сетей в этот период еще не проявилась - в одном здании нечего было объединять в сеть, так как из-за высокой стоимости вычислительной техники они не могли себе позволить приобретения нескольких компьютеров. Действовал эмпирический закон, который отражал уровень развития технологии производства электронных компонентов того времени.

|  |  |
| --- | --- |
| **Закон 1** | **Закон Гроша.** В соответствии с ним производительность компьютера была пропорциональна квадрату его стоимости, т.е. за одну и ту же сумму было рациональнее приобрести один высокопроизводительный компьютер, чем несколько менее мощных. |

### Возникновение глобальных сетей

*Удаленный терминал*

Потребность в соединении компьютеров, находящихся на большом расстоянии друг от друга, к началу 60-х годов вполне проявилась. Первоначально была решена простая задача - доступа к компьютеру с терминалов, удаленных от него на сотни и тысячи километров. Терминалы соединялись с компьютерами через телефонные сети с помощью модемов. Такие сети делали доступными для пользователей ресурсы мощных удаленных компьютеров класса супер-эвм.

Позднее появились системы, в которых наряду с удаленными соединениями типа терминал-компьютер были реализованы удаленные связи типа компьютер-компьютер. Компьютеры получили возможность обмениваться данными в автоматическом режиме, что является одним из базовых признаков вычислительной сети. На основе подобного механизма в первых сетях были реализованы службы обмена файлами, синхронизации баз данных, электронной почты и другие, ставшие теперь традиционными.

*Глобальные сети*

Хронологически первыми появились глобальные сети (Wide Area Networks - **WAN**), объединяющие территориально рассредоточенные компьютеры, находящиеся в различных городах и странах.

В 1961 году агентство перспективных исследований в области обороны (DARPA) по заданию министерства обороны США, начало создание экспериментальной сети передачи данных. Эта сеть получила название ARPANET и первоначально имела только военное назначение.

Ее основной задачей было изучение взаимосвязи различных компьютерных систем, и разработка способов их взаимодействия в условиях нарушения работоспособности части инфраструктуры. Первого сентября 1969 года в Калифорнийском университете в Лос-Анджелесе был введен в эксплуатацию первый сервер информационной сети **ARPANET**. Идея создания общей сети передачи данных давала большие возможности и была настолько удачной, что организации не имеющие отношения к министерству обороны начали присоединиться к ARPANET. Многие методы передачи информации, которые применяются сейчас, были разработаны именно для этой сети.

Новый этап в развитии глобальной сети начался в 1984 году, когда национальный научный фонд США основал большую информационную сеть - **NSFNet**. Она строилась на тех же принципах что и ARPANET, но была гораздо производительнее, имела научное назначение и объединяла большое количество мелких сетей. Сеть создавалась для объединения научной базы крупнейших университетов США в их исследовательской деятельности и обеспечения взаимодействия учёных этих университетов. В этом же году Национальный научный фонд приступил к созданию пяти информационных центров с мощными суперкомпьютерами. NSFNet должна была связать эти центры с университетами. За короткое время эта сеть завоевала большую популярность, только за первый год существования к ней присоединилось десятки тысяч пользователей.

В 1990 году NSFNet поглотила ARPANET и стала практически национальной информационной сетью. Этот год можно считать началом развития интернета в современном виде. В последующее десятилетие динамичное развитие информационных технологий способствовало тому, что эта сеть стала действительно всемирной. Сегодня число пользователей всемирной паутины достигло двух миллиардов человек, это четвёртая часть всего населения нашей планеты.

### Возникновение локальных сетей

*Причина отставания локальных сетей*

Важное событие, повлиявшее на эволюцию компьютерных сетей, произошло в начале 70-х годов ХХ века. В результате технологических наработок в области элементной базы производства компьютерных компонентов появились большие интегральные схемы (**БИС**). Их широкие функциональные возможности и низкая стоимость привели к созданию мини-компьютеров, которые стали конкурентами мэйнфреймов. Эмпирический закон о соотношении производительности и стоимости перестал соответствовать действительности, так как несколько мини-компьютеров, имея ту же стоимость, что и мэйнфрейм, решали некоторые задачи значительно быстрее.

Небольшие подразделения и отделы предприятий, организаций и научных центров получили возможность иметь собственные компьютеры. Мини-компьютеры решали задачи управления технологическим оборудованием, складом и другие задачи уровня отдела предприятия или научного центра. Появилась концепция распределения компьютерных ресурсов по всему предприятию, однако при этом все компьютеры одной организации по-прежнему продолжали работать независимо друг от друга.

Со временем потребности пользователей вычислительной техники выросли. Их не удовлетворяла автономная работа на компьютере, возникла необходимость в автоматическом режиме обмениваться компьютерными данными с пользователями других подразделений. Ответом на эту потребность стало появление первых локальных вычислительных сетей (**ЛВС-LAN**).

*Особенности организации локальных сетей*

Первоначально для соединения компьютеров использовались нестандартные сетевые технологии. Разнообразные устройства сопряжения, которые использовали собственные способы представления данных, свои типы кабелей и разъемов, могли объединять в сеть только определенные модели компьютеров, для которых они были разработаны (мини-компьютеры PDP-11 с мэйнфреймом IBM 360).

В середине 80-х годов положение дел в локальных сетях существенно изменилось. Утвердились стандартные сетевые технологии для объединения компьютеров в сеть - Ethernet, ArcNet, Token Ring.

Мощным стимулом для их появления послужили персональные компьютеры. ПК стали идеальными элементами для построения сетей – содной стороны, они были достаточно мощными, чтобы обеспечивать работу сетевых операционных систем, а с другой - нуждались в объединении вычислительной мощности для решения сложных задач и разделения периферийных устройств. ПК стали использовать в локальных сетях, не только в качестве клиентских компьютеров, но и в качестве сетевых серверов.

Последствием и движущей силой прогресса локальных сетей стало появление большого числа непрофессиональных пользователей, освобожденных от необходимости изучать специальные команды для работы в сети.

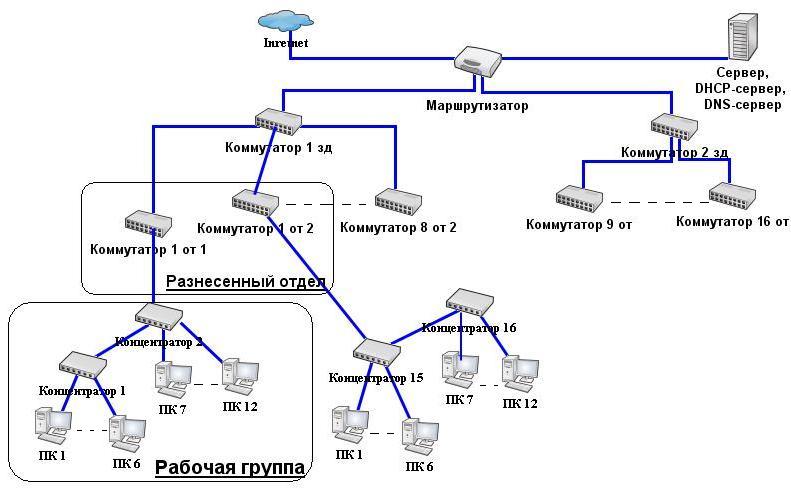
*Становление Ethernet*

Конец 90-х выявил лидера технологий локальных сетей – семейство Ethernet, в которое вошли классическая технология Ethernet 10Мбит/с, а также Fast Ethernet 100Мбит/с и Gigabit Ethernet 1000 Мбит/с.

Простые алгоритмы работы предопределили низкую стоимость оборудования Ethernet. Широкий диапазон иерархии скоростей позволяет строить локальную сеть, выбирая ту технологию семейства, которая в наибольшей степени отвечает задачам предприятия и потребностям пользователей.

## Лекция I.2. Общие принципы построения сетей

Для того чтобы пользователь сети получил возможность использовать ресурсы «чужих» компьютеров, таких как диски, принтеры, плоттеры, необходимо дополнить все компьютеры сети специальными средствами. В каждом компьютере функции передачи данных в линию связи выполняют совместно аппаратный модуль, называемый сетевым адаптером, или сетевой интерфейсной картой, и управляющая программа — драйвер. Задачи более высокого уровня — формирование запросов к ресурсам и их выполнение — решают соответственно клиентские и серверные модули ОС.



Даже в простейшей сети, состоящей из двух компьютеров, возникают проблемы физической передачи сигналов по линиям связи: кодирование и модуляция, синхронизация передающего и принимающего устройств, контроль корректности переданных данных.

|  |  |
| --- | --- |
| **Опр. 1** | **Кодирование** – преобразование сообщения в последовательность некоторых символов (взаимооднозначное соответствие между сообщениями и символами – код, который известен как передающей, так и принимающей стороне. |
| **Опр. 2** | **Модуляция** – преобразование сообщения (первичного сигнала) в сигнал, пригодный для передачи по какой-либо линии связи. |
| **Опр. 3** | **Линия связи** – среда, используемая для передачи сигналов от передатчика к приемнику. Электрическая связь – кабель, радиосвязь – область пространства, в котором распространяются электромагнитные волны от передатчика к приемнику. |
| **Опр. 4** | **Система связи** – совокупность технических средств, служащих для передачи сообщений от источника к потребителю. К таким устройствам относят: линии связи, приемное устройство, передающее устройство и др. |
| **Опр. 5** | **Канал связи** – совокупность технических средств, обеспечивающих передачу сигнала от некоторой точки А системы до другой точки В. |

Важными **характеристиками**, связанными с передачей трафика через физические каналы, являются: предложенная нагрузка, скорость передачи данных, пропускная способность, емкость канала связи, полоса пропускания.

При связывании в сеть более двух компьютеров возникают проблемы выбора:

**Топологии**:

|  |  |  |
| --- | --- | --- |
|  |  |  |
| полносвязной | звезды | кольца |
| Схема компьютерной сети с топологией «шина». |  |  |
| общей шины | иерархического дерева | произвольной |

**Способа адресации:**

|  |  |
| --- | --- |
| 4. Адресация узлов сети | 4. Адресация узлов сети |
| плоский | иерархический |

Способа **разделения линий связи и механизма коммутации**.

В неполносвязных сетях соединение пользователей осуществляется путем коммутации через сеть транзитных узлов. При этом должны быть решены следующие задачи: определение потоков данных и маршрутов для них, продвижение данных в каждом транзитном узле, мультиплексирование и демультиплексирование потоков.

|  |  |
| --- | --- |
| **Опр. 6** | **Мультиплексирование –** уплотнение канала связи, то есть передача нескольких потоков данных с меньшей скоростью по одному каналу связи. Или иначе: создание в исходном канале связи нескольких подканалов связи с меньшей пропускной способностью. |
| **Опр. 7** | **Демультиплексирование** **–** разделение суммарного агрегированного потока на несколько составляющих его потоков. Как правило, операцию коммутации сопровождает также обратная операция мультиплексирования. |
| **Опр. 8** | **Коммутатор** – устройство, предназначенное для соединения нескольких узлов компьютерной сети в пределах одного или нескольких сегментов сети. В памяти у коммутатора находится таблица коммутации, в которой указано соответствие узла порту. В первый момент времени таблица пуста и коммутатор находится в режиме обучения, соотнося активные MAC-адреса с портами. |
| **Опр. 9** | **МАС-адрес** (Media Access Control — надзор за доступом к среде, также Hardware Address, также физический адрес) – уникальный шестибайтный идентификатор, присваиваемый каждой единице активного оборудования или некоторым их интерфейсам в компьютерных сетях Ethernet. Уникальность MAC-адресов достигается за счет того, что каждый производитель сетевых устройств получает конкретный диапазон адресов у регистрирующего комитета IEEE Registration Authority, содержащий адресов. Всего возможных комбинаций MAC-адресов , по прогнозам этого значения будет достаточно для всех потребителей вплоть до 2100 года. |

### Классическая схема построения сети

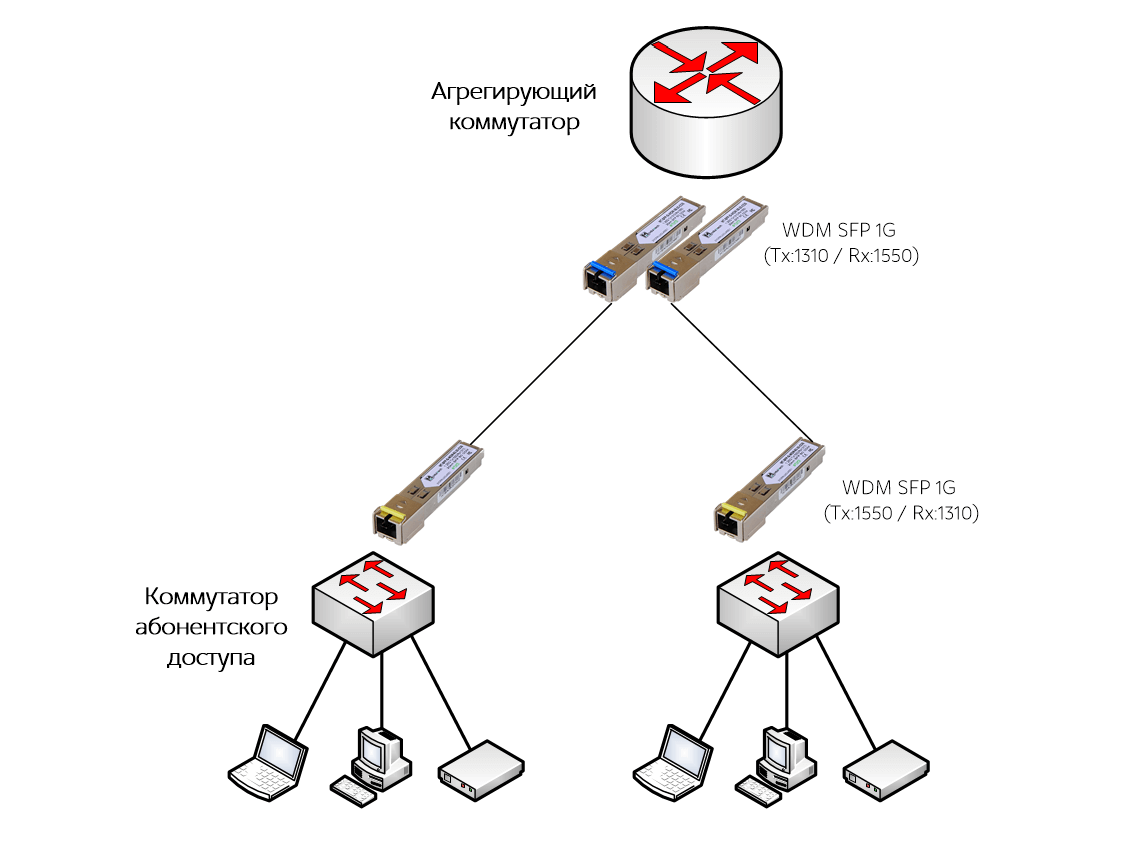
*Уровни сети*

1. **Уровень доступа** – ближайший к конечным абонентам сегмент сети. В качестве активного сетевого оборудования используется бюджетный коммутатор L2, которые имеют 24 или 48 10/100Base-T (100/1000100Base-T) портов для подключения абонентов, и двумя или четырьмя 1,25 Гбит/с SFP-портов для подключения к соседним коммутаторам доступа и к уровню агрегации.

**Интерфейсы уровня доступа**

Для организации соединений 1,25 Гбит/с зачастую используются оптические модули WDM SFP или одноволоконные трансиверы SFP. Для этого типа подключения выбираются именно одноволоконные модули в связи с удобством их инсталляции и обслуживания. Для образования соединения нужно только одно волокно, в качестве оптического коннектора используются простые и надежные коннекторы типа SC/UPC (Subscriber Connector). Реже используются трансиверы с разъемом LC/UPC (Lucent Connector), меньшая распространённость LC разъемов объясняется их недостаточной надежностью по сравнению с SC.

В связи с небольшой удаленностью коммутаторов доступа друг от друга и от уровня агрегации, используются SFP модули с дальностью передачи 3 км или 20 км. Также некоторыми провайдерами используется модификация WDM SFP трансивера на 10 км, которая представляет собой универсальное решение для организации каналов уровня доступа. Стандартные одноволоконные трансиверы ведут передачу на длинах волн 1310 нм и 1550 нм и работают парно, то есть один трансивер передает на длине волны 1310 нм, принимает на 1550 нм, а второй передает на 1550 нм и принимает на 1310 нм. Но иногда сети операторов связи, построены по принципу PON-сетей в рамках, когда по одному волокну передается интернет трафик и КТВ-сигнал. В таком случае используются нестандартные WDM SFP модули с длинами волн передачи 1310 нм и 1490 нм, это позволяет освободить длину волны 1550 нм, которая необходима для передачи КТВ (кабельного телевидения).

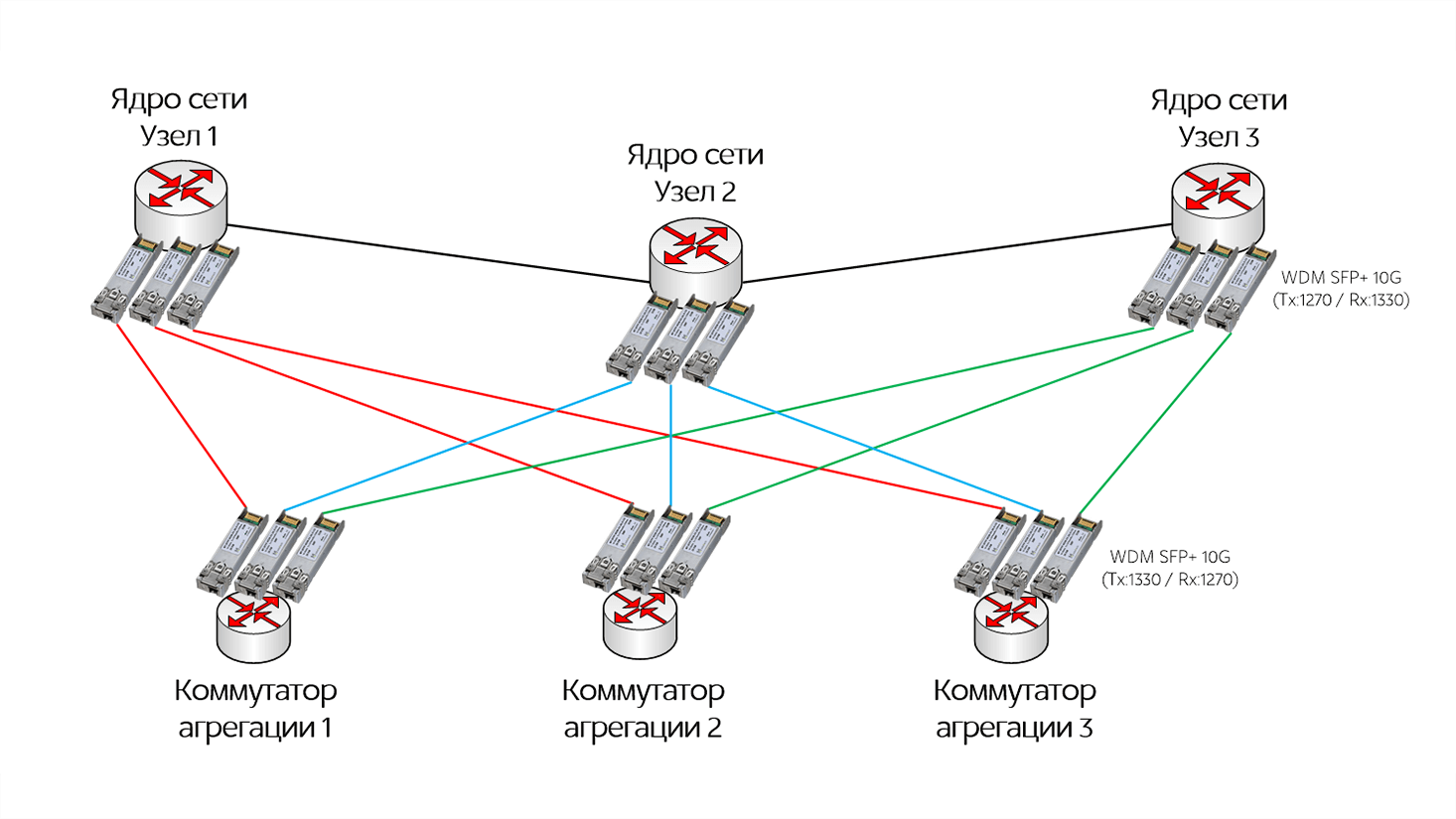


Tx – transmitter (передатчик, частота передачи);

Rx – receiver (приемник, частота приема)

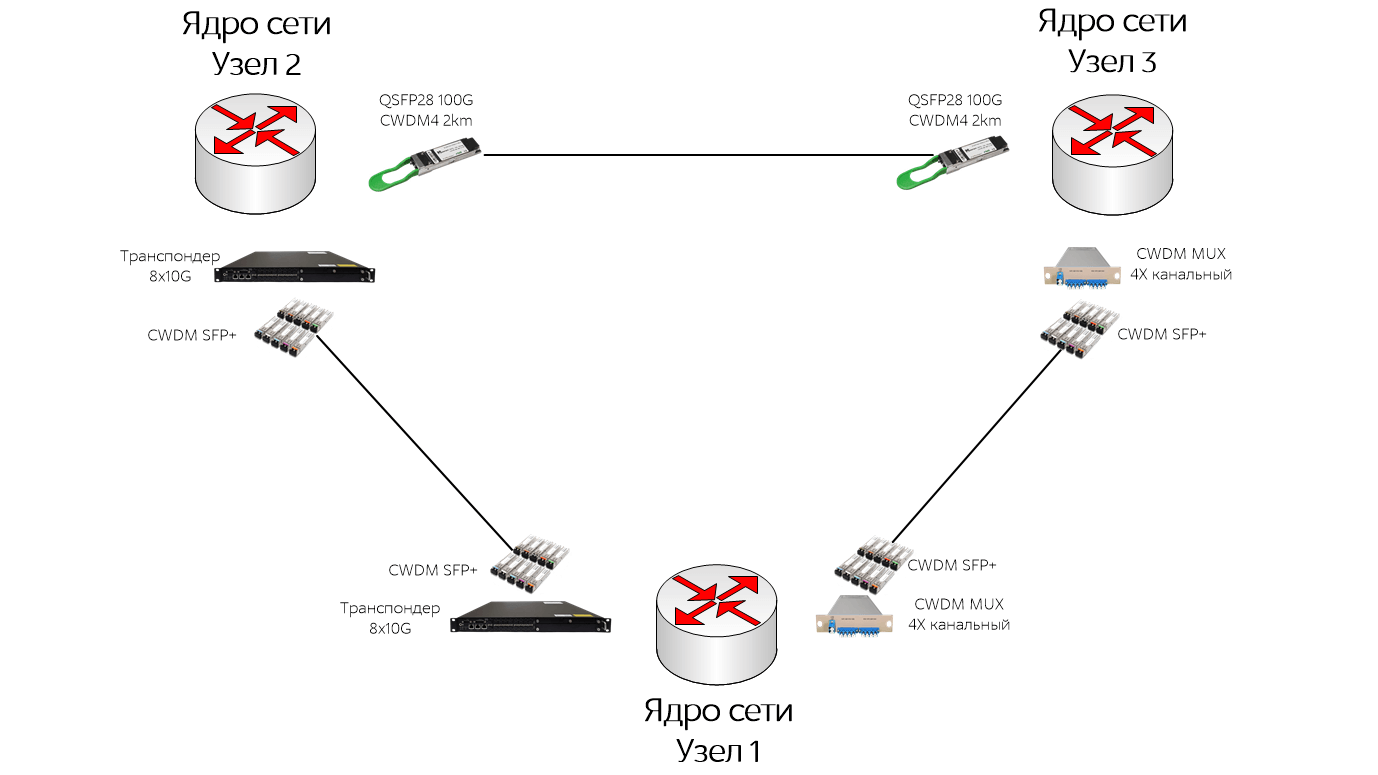
1. **Уровень агрегации** – коммутаторы уровня агрегации подключаются к ядру сети по топологии «Звезда», реже применяется топология «Шина». Объем и скорость передаваемой информации на этом уровне сети заметно выше, чем на уровне доступа. Для организации каналов связи «агрегация – ядро сети» зачастую используются трансиверы со скоростью передачи 10 Гбит/с. В зависимости от схемы прокладки оптических кабелей и их волоконной емкости на уровне агрегации, могут применяться технологии спектрального уплотнения WDM и CWDM, в основном это вызвано дефицитом волокон и необходимостью их экономить. В случае, если уровень агрегации подключается к ядру сети по топологии «Звезда» с организацией одного канала 10 Гбит/с, с каждой точки агрегации логично использовать WDM трансиверы форм-фактора SFP+ или XFP (форм-фактор зависит от используемых коммутаторов агрегации).

В том же случае, если топология подключения уровня агрегации сложнее, чем классическая «Звезда» или же до каждой точки агрегации необходимо доставить больше одного канала 10 Гбит/с, то экономически оправданным является построение CWDM системы, которая позволяет организовать 9 дуплексных каналов связи в рамках одного оптического волокна. Необходимо отметить, что CWDM системы позволяют строить как простые трассы типа «точка-точка», так и трассы со сложной топологией «точка-многоточие» или «кольцо».



Вне зависимости от топологии сети, удаленность узлов агрегации от ядра сети может составлять от нескольких километров до нескольких десятков километров, редко расстояние превышает 20 км.

1. **Уровень ядра сети** – самый ответственный уровень, на нем важна и высокая производительность, и максимальная отказоустойчивость. Резервирование оборудования ядра сети производится с использованием топологии «каждый-с-каждым» и физическим резервированием каналов связи и сервисов. Расстояние между активным сетевым оборудованием на данном уровне может составлять как десятки метров и находиться в рамках одного здания, так и десятков километров с разнесением ядра сети на несколько площадок. Передаваемые скорости внутри ядра сети могут составлять 40 – 100 Гбит/с, все зависит от величины провайдера и объема его абонентской базы.



Соответственно, для организации соединений между коммутаторами ядра сети могут использоваться, как 10 Гбит/с трансиверы, так и высокоскоростные 40 и 100 Гбит/с трансиверы. В зависимости от удаленности сетевого оборудования соответственно применяются, как многомодовые трансиверы типа SR, так и высокопроизводительные системы уплотнения CWDM или DWDM с использованием транспондеров или мукспондеров для передачи высокоскоростных каналов связи.

1. **Серверный уровень** – неотъемлемая часть ядра сети, зачастую располагается недалеко, в пределах одного здания. Его подключение также требует резервирования для обеспечения бесперебойности работы сервисов. В связи с небольшими расстояниями между оборудованием, в пределах машинного зала или здания, на этом уровне сети распространены трансиверы для «коротких» соединений, такие как, DAC-кабели, AOC-кабели, всевозможные вариации Break-out кабелей и трансиверы типа SR и LRM. В основном все соединения имеют скорость передачи 10 Гбит/с и 40 Гбит/с, но с растущим объемом потребляемого трафика все чаще начинает использоваться связка 25 Гбит/с и 100 Гбит/с.

### Физическая среда передачи данных в локальных сетях

Средой передачи информации называются линии (каналы) связи, по которым производится информационный обмен между компьютерами. В большинстве компьютерных сетей (особенно локальных) используются проводные или кабельные каналы связи, хотя сейчас применяются и беспроводные сети находят все более широкое применение.

Информация в локальных сетях, как правило, передается с помощью **последовательного кода**, то есть бит за битом. Такой способ передачи медленнее и сложнее, чем при использовании параллельного кода. Однако при более быстрой **параллельной передаче** (по нескольким кабелям одновременно) значительно увеличивается количество соединительных кабелей (в 8 раз при 8-разрядном коде). При значительных расстояниях между абонентами сети стоимость соединительного кабеля сравнима или превосходит стоимость остальных компонентов сети. Кроме того, передача на большие расстояния при любом типе кабеля требует сложной и дорогой аппаратуры приемника и передатчика, так как при этом необходимо генерировать мощный сигнал на передающем конце и детектировать слабый сигнал со стороны приемника. В случае последовательной передачи для этого требуется только один передатчик и приемник, при параллельной количество требуемых передатчиков и приемников увеличивается. Кроме того, при параллельной передаче очень важно, чтобы длины отдельных кабелей были одинаковы. Иначе в результате прохождения по кабелям разной длины между сигналами на приемном конце образуется временное смещение, которое может привести к сбоям в работе сети или к ее полной неработоспособности.

Кабели делятся на три вида:

1. Электрические (медные) кабели на основе витых пар проводов (twisted pair), которые делятся на экранированные (shielded twisted pair, STP) и неэкранированные (unshielded twisted pair, UTP);
2. Электрические (медные) коаксиальные кабели (coaxial cable);
3. Оптоволоконные кабели (fiber optic).

Каждый тип кабеля имеет свои достоинства и недостатки, поэтому при выборе необходимо учитывать особенности решаемой задачи и отличии конкретной сети, в том числе и используемую топологию.

### Принципиально важные параметры кабелей

1. **Полоса пропускания кабеля** (частотный диапазон сигналов, пропускаемых кабелем) и затухание сигнала в кабеле. Эти параметры тесно связаны между собой, так как с увеличением частоты сигнала растет его затухание.
2. **Помехозащищенность кабеля** и обеспечиваемая им секретность передачи информации. Эти две взаимосвязанные характеристики показывают, как кабель взаимодействует с окружающей средой – как он реагирует на внешние помехи, и насколько просто прослушать передаваемую информацию.
3. **Скорость распространения сигнала** по кабелю или, обратный параметр – задержка сигнала на единицу длины кабеля. Этот параметр имеет существенное значение при выборе длины сети. Типичные величины скорости распространения сигнала – 0,6…0,8 от скорости распространения света в вакууме, типичные величины задержек – 4…5 нс/м.
4. **Величина волнового сопротивления** кабеля (импеданс). Сопротивление учитывают при согласовании кабеля для предотвращения отражения сигнала от его концов. Волновое сопротивление зависит от формы и взаиморасположения проводников, от технологии изготовления и материала диэлектрика кабеля. Типичные значения волнового сопротивления – от 50 до 150 Ом.

### Используемые стандарты на кабелей

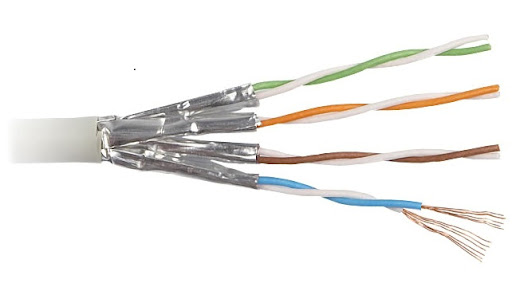
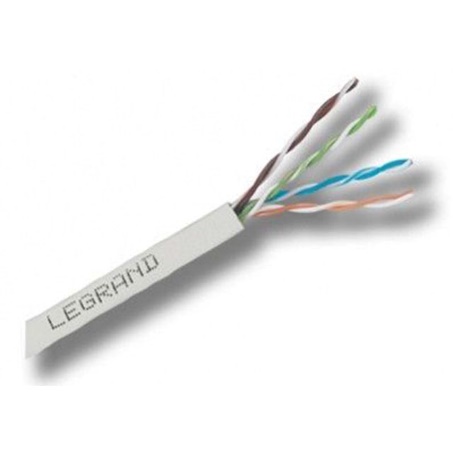
* EIA/TIA 568 (Commercial Building Telecommunications Cabling Standard) – американский;
* ISO/IEC IS 11801 (Generic cabling for customer premises) – международный;
* CENELEC EN 50173 (Generic cabling systems) – европейский.

Эти стандарты описывают практически идентичные кабельные системы, которые отличаются терминологией и нормами на основные регламентируемые параметры.

### Кабели на основе витых пар

Витые пары проводов используются в относительно недорогих и самых популярных кабелях. Они состоят из нескольких пар скрученных попарно изолированных медных проводов в единой диэлектрической (пластиковой) оболочке.

Такие кабели отличаются высокой гибкостью и удобством при прокладке и монтаже. Скручивание проводов позволяет уменьшить индуктивные наводки проводов в кабеле друг на друга и снизить влияние переходных процессов. В кабели разных категорий входят две или четыре витые пары (4 или 8 проводников).



Неэкранированные витые пары характеризуются слабой защищенностью от внешних электромагнитных помех и от подслушивания. Для улучшения этих характеристик применяется экранирование кабелей.

В случае экранированной витой пары STP каждая из витых пар помещается в металлический экран-оплетку для уменьшения собственных излучений кабеля, его защиты от внешних электромагнитных помех и снижения взаимного влияния пар проводов друг на друга. Чтобы экран защищал от помех его необходимо заземлять. Экранированная витая пара существенно дороже, чем ее неэкранированный аналог.

Основным достоинством неэкранированных витых пар являются – простота монтажа разъемов на концах кабеля, а также ремонта любых повреждений по сравнению с другими типами кабеля. В настоящее время витая пара используется для передачи информации на скоростях до 1000 Мбит/с. В соответствии со стандартом EIA/TIA 568, существуют пять основных и две дополнительные категории кабелей неэкранированных витых пар (UTP):

* кабель категории 1 – это телефонный кабель (пары проводов не витые), по которому можно передавать только **речевые данные**;
* кабель категории 2 – это кабель из витых пар для передачи данных в полосе частот до 1 МГц (в настоящее время он используется достаточно редко, а стандарт EIA/TIA 568 не различает кабели категорий 1 и 2);
* кабель категории 3 – это кабель для передачи данных в полосе частот до 16 МГц, состоящий из витых пар с девятью витками проводов на метр длины, имеет волновое сопротивление 100 Ом (самый простой и недорогой тип кабелей, рекомендованный стандартом для локальных сетей, недавно он был самым распространенным, но сегодня вытесняется кабелем 5 категории);
* кабель категории 4 – это кабель, передающий данные в полосе частот до 20 МГц (используется редко, т.к. практически не отличается по своим характеристикам от категории 3);
* кабель категории 5 – на текущий момент самый совершенный кабель, рассчитанный на передачу данных в полосе частот до 100 МГц (состоит из витых пар, которые имеют 27 витков на метр длины (8 витков на фут). Волновое сопротивление кабеля - 100 Ом. Кабель категории 5 ориентировочно на 30…50% дороже, чем кабель категории 3;
* кабель категории 6 перспективный тип витой пары для передачи данных в полосе частот до 250 МГц;
* кабель категории 7 перспективный тип витой пары для передачи данных в полосе частот до 600 МГц.

Кабели выпускаются с двумя типами **внешних оболочек**:

* кабель в поливинилхлоридной (ПВХ, PVC) оболочке дешевле и предназначен для работы в относительно мягких условиях эксплуатации.
* кабель в тефлоновой оболочке дороже, предназначен для менее комфортных условий эксплуатации.

Кабель в ПВХ оболочке называется non-plenum, в тефлоновой оболочке – plenum. Еще один важный параметр любого кабеля – это скорость распространения сигнала в кабеле или задержка распространения сигнала в кабеле в пересчете на единицу его длины. Типичная величина задержки большинства используемых кабелей составляет около 4…5 нс/м. Каждый из проводов, входящих в кабель на основе витых пар имеет свой цвет изоляции, что значительно упрощает монтаж разъемов.

### Коаксиальные кабели

Коаксиальный кабель – это электрический кабель, который состоит из центрального медного провода и металлической оплетки (экрана из фольги), разделенных между собой слоем диэлектрика (внутренней изоляции) и помещенных в общую внешнюю оболочку.

Этот тип кабеля до недавнего времени был очень распространен, что связано с его высокой помехозащищенностью (за счет металлической оплетке), более широкими, чем в случае витой пары, частотными полосами пропускания (свыше 1ГГц), и значительными допустимыми расстояниями передачи (до километра). К нему сложнее механически подключиться для несанкционированного прослушивания сети, он дает также значительно меньше электромагнитных излучений. Однако ему свойственны следующие недостатки: монтаж и ремонт коаксиального кабеля существенно сложнее, чем витой пары, а его стоимость значительно выше (дороже в 1,5 – 3 раза). Сейчас его применяют гораздо реже, чем витую пару.



Чаще всего коаксиальный кабель используется в сетях с топологией типа шина. В этом случае на концах кабеля обязательно должны устанавливаться терминаторы для предотвращения внутренних отражений сигнала, один из которых необходимо заземлить.

Волновое сопротивление кабеля указывается в сопроводительной документации. Чаще всего в локальных сетях применяются 50-омные (RG-58, RG-11, RG-8) и 93-омные кабели (RG-62). Марок коаксиального кабеля немного, он считается морально устаревшим и не перспективным.

Существует два основных типа коаксиального кабеля:

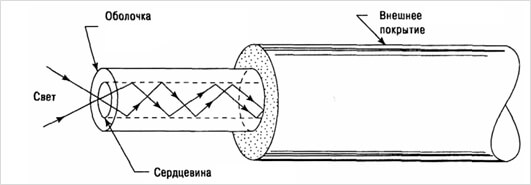
* тонкий (thin) кабель, более гибкий, имеющий диаметр около 5 мм;
* толстый (thick) кабель, значительно более жесткий диаметром 10 мм.

Современные стандарты на кабельные системы не включают коаксиальный кабель в перечень используемых типов кабелей.

### Оптоволоконные кабели

Волоконно-оптический (оптоволоконный) кабель – это кабель с принципиально новым принципом передачи данных. Информация по нему передается не электрическим сигналом, а световым. Главный его элемент – прозрачное стекловолокно, по которому свет проходит на очень большие расстояния (до десятков километров) практически без ослабления. Внутренняя структура оптоволоконного кабеля практически идентична структуре коаксиального электрического кабеля.

Внешний вид оптоволоконного кабеля



Вместо центрального медного провода используется тонкое (диаметром 1 – 10 мкм) стекловолокно, а вместо внутренней изоляции – стеклянная или пластиковая оболочка с иным коэффициентом преломления, не позволяющая свету выходить за пределы стекловолокна. Речь идет о режиме полного внутреннего отражения света от границы двух веществ с разными коэффициентами преломления (у центрального и волокна, и стеклянной оболочки эти коэффициенты различны). Металлическая оплетка кабеля обычно отсутствует, так как экранирование от внешних электромагнитных помех в случае применения такого кабеля не требуется, но иногда ее применяют для механической защиты от окружающей среды.

Оптоволоконный кабель обладает очень хорошими характеристиками по помехозащищенности и секретности передаваемых данных. Никакие внешние электромагнитные помехи не способны в принципе исказить световой сигнал, а сам сигнал не создает электромагнитного излучения. Подключиться к этому типу кабеля для несанкционированного прослушивания сети достаточно сложно, так как при этом нарушается целостность кабеля. Теоретически возможная полоса пропускания волоконно-оптического кабеля достигает величины 1000 ГГц, что гораздо выше, чем у электрических кабелей. Стоимость оптоволоконного кабеля, первоначально довольно значительная, постоянно снижается и сейчас примерно равна стоимости тонкого коаксиального кабеля.

Величина затухания сигнала в оптоволоконных кабелях на частотах, используемых в локальных сетях, составляет от 5 до 20 дБ/км, что примерно соответствует показателям электрических кабелей на низких частотах, на больших частотах (свыше 200 МГц) их преимущества существенны.

Однако оптоволоконный кабель имеет и некоторые недостатки. Основной – относительно высокая сложность монтажа (при установке разъемов необходима высокая точность, от точности скола стекловолокна и качества его полировки зависит затухание в разъеме). Для установки разъемов применяют сварку или склеивание с помощью специального геля, имеющего аналогичный коэффициент преломления света, что и стекловолокно кабеля. Для этого нужны специальные инструменты и высокая квалификация персонала. Использование оптоволоконного кабеля требует применения специальных оптических передатчиков и приемников, преобразующих световые сигналы в электрические и обратно, что существенно увеличивает стоимость сети.

Оптоволоконный кабель менее гибок и прочен по сравнению с электрическим. Стандартная величина допустимого радиуса изгиба составляет около 5 – 10 см, при меньших радиусах изгиба в центральном волокне могут появиться трещины, плохо переносит такой кабель и механическое растяжение. Оптоволоконный кабель чувствителен к ионизирующим излучениям, из-за которых снижается прозрачность стекловолокна, что приводит к увеличению затухания сигнала. Перепады температуры сказываются также отрицательно, стекловолокно может треснуть.

Используют оптоволоконный кабель в сетях с топологией кольцо и звезда. Проблем с заземлением и согласованием при его использовании не существует, кабель обеспечивает идеальную гальваническую развязку сетевых компьютеров. В перспективе этот тип кабеля, вероятно, заменит все виды электрических кабелей.

Используют два различных типа волоконно-оптического кабеля:

* многомодовый (мультимодовый) кабель, более дешевый, но менее качественный;
* одномодовый кабель, с более высокой стоимостью, но имеющий лучшие характеристики в сравнении с предыдущим.

Различия между этими двумя типами в разных режимах прохождения световых лучей в кабеле при передаче данных. В одномодовом кабеле практически все лучи проходят один и тот же путь, форма сигнала почти не искажается, и результате они достигают приемника одновременно. Одномодовый кабель имеет диаметр центрального волокна около 1,3 мкм и передает свет с длиной волны 1,3 мкм. Потери сигнала и дисперсия при этом не велики, что позволяет передавать сигналы на значительно большее расстояние, чем при использовании многомодового кабеля. Для одномодового кабеля применяют лазерные приемопередатчики, которые используют свет с необходимой длиной волны. Кроме того, лазеры имеют большее быстродействие, чем обычные светодиоды. Затухание сигнала в одномодовом кабеле составляет 0,5-5 дБ/км. В перспективе одномодовый кабель, вероятно, станет основным типом из-за своих высоких характеристик.

В многомодовом кабеле траектории световых лучей имеют существенный разброс, в следствии чего форма сигнала при приеме значительно искажается. Центральное волокно кабеля имеет диаметр 62,5 мкм, а диаметр внешней его оболочки 125 мкм. Для передачи данных используется светодиод, что увеличивает срок службы приемопередатчиков и снижает их стоимость. Длина волны света в многомодовом кабеле 0,85 мкм, при этом существует разброс их длин около 30 - 50 нм. Допустимая длина такого типа кабеля составляет около 5 км. Затухание в многомодовом кабеле больше, чем в одномодовом и составляет 5 – 20 дБ/км. Многомодовый кабель – это основной тип волоконно-оптического кабеля в настоящее время, так как он значительно дешевле и доступнее.

Средняя величина задержки сигнала для наиболее распространенных кабелей составляет около 4…5 нс/м, что примерно соответствует величине задержки в электрических кабелях. Оптоволоконные кабели, как и электрические, выпускаются в разных видах оболочек - plenum и non-plenum.

### Бескабельные каналы связи

Кроме кабельных каналов в компьютерных сетях используются также бескабельные (беспроводные) их аналоги. Их главное преимущество состоит в том, что они позволяют реализовать мобильный вариант взаимодействия абонентов. Кроме того, не требуется прокладка проводов и компьютеры сети можно легко перемещать в пределах здания или комнаты. Для реализации беспроводных сетей используют радио и инфракрасные каналы.

**Радиоканал** использует передачу информации с помощью радиоволн, поэтому теоретически он может обеспечить связь на многие тысячи и более километров. Скорость передачи достигает сотен мегабит в секунду (зависит от выбранной длины волны и способа кодирования). В радиоканале используется передача в узком диапазоне частот и модуляция информационным сигналом сигнала несущей частоты.

Недостатками радиоканала являются его плохая защита от прослушивания и очень низкая помехозащищенность. Особенность радиоканала состоит в том, что сигнал свободно излучается в эфир, он не замкнут в кабель, из-за чего возникают проблемы совместимости с другими источниками радиоволн (радио- и телевещательными станциями, радарами, радиолюбительскими и профессиональными передатчиками и др.). Существуют и некоторые сложности с лицензированием радиочастотного диапазона для таких сетей.

Для локальных беспроводных сетей (WLAN – Wireless LAN) в настоящее время применяются подключения по радиоканалу на небольших расстояниях (до 100 метров) и в пределах прямой видимости. Используются частотные диапазоны – 2,4 ГГц и 5 ГГц. Скорость передачи – до 300 Мбит/с.

Сети WLAN позволяют устанавливать беспроводные сетевые соединения на ограниченной территории (в квартире, внутри офисного или университетского здания, на производстве или в общественных местах). Они могут использоваться во временных офисах или в других местах, где прокладка кабелей затруднена или неосуществима совсем, а также в качестве дополнения к существующей проводной локальной сети для обеспечения пользователям мобильного варианта работы.

Популярная технология беспроводных сетей Wi-Fi (Wireless Fidelity) позволяет организовать связь между несколькими (2…16) компьютерами с помощью концентратора (называемого точкой доступа, Access Point, AP), или нескольких концентраторов, если компьютеров от 10…50. Кроме того, данная технология позволяет связать две локальные сети на расстоянии до 25 километров при помощи мощных беспроводных мостов.

Радиоканал используется в глобальных сетях, как для наземной, так и для спутниковой связи. В этом применении у него отсутствуют конкуренты, так как радиоволны теоретически не имеют пределов распространения.

Использование **инфракрасного** канала также предполагает отсутствие соединительных проводов, так как использует для взаимодействия инфракрасное излучение (как у пульта дистанционного управления телевизором). Основным его преимуществом по сравнению с радиоканалом является нечувствительность к электромагнитным помехам, что позволяет применять его в производственных условиях, где всегда много помех от силового оборудования. В этом случае используют высокую мощность передачи для исключения взаимного влияния других источников теплового (инфракрасного) излучения. Применяют такие сети и в областях, где наличие электромагнитных полей является недопустимым (медицина, научные исследования). Скорости передачи данных по инфракрасному каналу не велики, обычно не превышают 5…10 Мбит/с, но при использовании инфракрасных лазеров может быть достигнута скорость более 100 Мбит/с. Секретность передаваемой информации, как и в случае применения радиоканала, не достигается, также требуются сравнительно дорогие приемники и передатчики. Недостаточно надежно функционирует инфракрасная связь в условиях высокой запыленности воздуха.

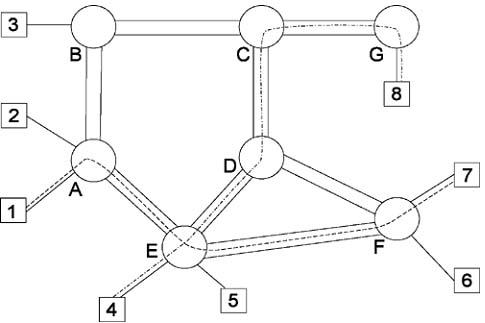
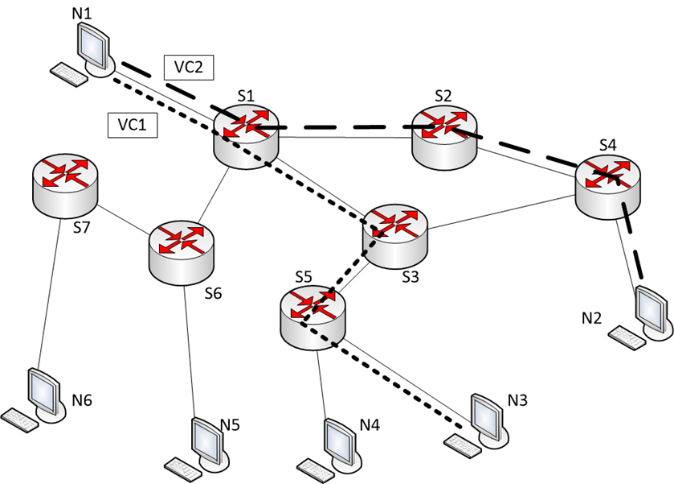
Перечисленные особенности приводит к тому, что применяют инфракрасные каналы в локальных сетях достаточно редко. В основном они используются для связи компьютеров с периферийным оборудованием (интерфейс IrDA). Инфракрасные каналы делятся на две группы:

* каналы прямой видимости, где связь осуществляется с использованием лучей, идущих непосредственно от передатчика к приемнику. В этом случае связь возможна только при отсутствии непрозрачных препятствий между компьютерами сети. Протяженность такого канала прямой видимости достигает нескольких километров.
* каналы на рассеянном излучении. Они работают на сигналах, отраженных от стен, потолка, пола и других препятствий. Связь может осуществляться на гораздо меньших расстояниях, только в пределах одного помещения.

## Лекция I.3. Коммутация каналов и пакетов

Среди множества возможных подходов к решению задачи коммутации абонентов в сетях выделяют два основополагающих:

* коммутация каналов (circuit switching);
* коммутация пакетов (packet switching).

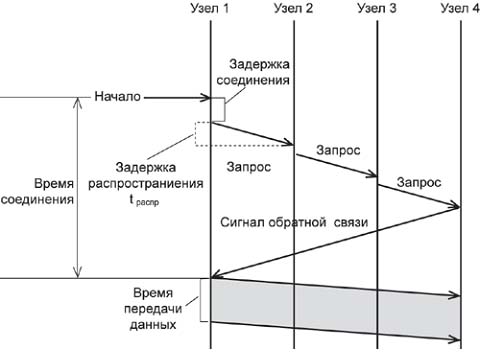
*Общая структура сети с коммутацией абонентов*

### Коммутация каналов

При коммутации каналов коммутационная сеть образует между конечными узлами непрерывный составной физический канал из последовательно соединенных коммутаторами промежуточных канальных участков. Условием того, что несколько физических каналов при последовательном соединении образуют единый физический канал, является равенство скоростей передачи данных в каждом из составляющих физических каналов. Равенство скоростей означает, что коммутаторы такой сети не должны буферизовать передаваемые данные.

В сети с коммутацией каналов перед передачей данных всегда необходимо выполнить процедуру установления соединения, в процессе которой и создается составной канал. И только после этого можно начинать передавать данные.

**Пример:** если сеть, изображенная на рисунке выше, работает по технологии коммутации каналов, то узел 1, чтобы передать данные узлу 7, сначала должен передать специальный запрос на установление соединения коммутатору A, указав адрес назначения 7. Коммутатор А должен выбрать маршрут образования составного канала, а затем передать запрос следующему коммутатору, в данном случае E. Затем коммутатор E передает запрос коммутатору F, а тот, в свою очередь, передает запрос узлу 7. Если узел 7 принимает запрос на установление соединения, он направляет по уже установленному каналу ответ исходному узлу, после чего составной канал считается скоммутированным, и узлы 1 и 7 могут обмениваться по нему данными.



*Установление составного канала*

Техника коммутации каналов имеет свои достоинства и недостатки:

**Достоинства коммутации каналов**

*Постоянная и известная скорость передачи данных по установленному между конечными узлами каналу.* Это дает пользователю сети возможности на основе заранее произведенной оценки необходимой для качественной передачи данных пропускной способности установить в сети канал нужной скорости.

*Низкий и постоянный уровень задержки передачи данных через сеть.* Это позволяет качественно передавать данные, чувствительные к задержкам (называемые также трафиком реального времени) — голос, видео, различную технологическую информацию.

**Недостатки коммутации каналов**

*Отказ сети в обслуживании запроса на установление соединения.* Такая ситуация может сложиться из-за того, что на некотором участке сети соединение нужно установить вдоль канала, через который уже проходит максимально возможное количество информационных потоков. Отказ может случиться и на конечном участке составного канала — например, если абонент способен поддерживать только одно соединение, что характерно для многих телефонных сетей. При поступлении второго вызова к уже разговаривающему абоненту сеть передает вызывающему абоненту короткие гудки — сигнал «занято».

*Нерациональное использование пропускной способности физических каналов.* Та часть пропускной способности, которая отводится составному каналу после установления соединения, предоставляется ему на все время, т.е. до тех пор, пока соединение не будет разорвано. Однако абонентам не всегда нужна пропускная способность канала во время соединения, например в телефонном разговоре могут быть паузы, еще более неравномерным во времени является взаимодействие компьютеров. Невозможность динамического перераспределения пропускной способности представляет собой принципиальное ограничение сети с коммутацией каналов, так как единицей коммутации здесь является информационный поток в целом.

*Обязательная задержка перед передачей данных из-за фазы установления соединения.*

Достоинства и недостатки любой сетевой технологии относительны. В определенных ситуациях на первый план выходят достоинства, а недостатки становятся несущественными. Так, техника коммутации каналов хорошо работает в тех случаях, когда нужно передавать только трафик телефонных разговоров. Здесь с невозможностью «вырезать» паузы из разговора и более рационально использовать магистральные физические каналы между коммутаторами можно мириться. А вот при передаче очень неравномерного компьютерного трафика эта нерациональность уже выходит на первый план.

### Коммутация пакетов

Эта техника коммутации была специально разработана для эффективной передачи компьютерного трафика. Первые шаги на пути создания компьютерных сетей на основе техники коммутации каналов показали, что этот вид коммутации не позволяет достичь высокой общей пропускной способности сети. Типичные сетевые приложения генерируют трафик очень неравномерно, с высоким уровнем пульсации скорости передачи данных. Например, при обращении к удаленному файловому серверу пользователь сначала просматривает содержимое каталога этого сервера, что порождает передачу небольшого объема данных. Затем он открывает требуемый файл в текстовом редакторе, и эта операция может создать достаточно интенсивный обмен данными, особенно если файл содержит объемные графические включения. После отображения нескольких страниц файла пользователь некоторое время работает с ними локально, что вообще не требует передачи данных по сети, а затем возвращает модифицированные копии страниц на сервер — и это снова порождает интенсивную передачу данных по сети.

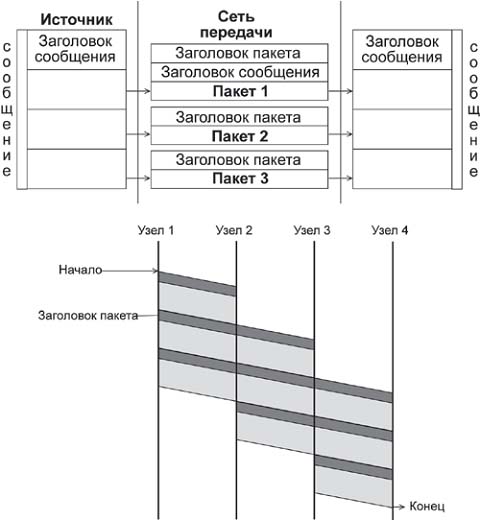
|  |  |
| --- | --- |
| **Опр. 1** | **Коэффициент пульсаций трафика** — это отношение максимальной скорости на каком-либо небольшом периоде времени к средней скорости трафика, измеренной на длительном периоде времени. Неопределенность временных периодов делает коэффициент пульсации качественной характеристикой трафика, речь о которых пойдет в следующих лекциях. |

Коэффициент пульсации трафика отдельного пользователя сети при может достигать 1:50 или даже 1:100. Если для описанной сессии организовать коммутацию канала между компьютером пользователя и сервером, то большую часть времени канал будет простаивать. В то же время коммутационные возможности сети будут закреплены за данной парой абонентов и будут недоступны другим пользователям сети.

При коммутации пакетов все передаваемые пользователем сообщения разбиваются в исходном узле на сравнительно небольшие части, называемые пакетами.

|  |  |
| --- | --- |
| **Опр. 2** | **Информационное сообщение** — логически завершенная порция данных — запрос на передачу файла, ответ на этот запрос, содержащий весь файл и т.д. |

Сообщения могут иметь произвольную длину, от нескольких байт до многих мегабайт. Напротив, пакеты обычно тоже могут иметь переменную длину, но в узких пределах, например от 46 до 1500 байт. Каждый пакет снабжается заголовком, в котором указывается адресная информация, необходимая для доставки пакета на узел назначения, а также номер пакета, который будет использоваться узлом назначения для сборки сообщения (рисунок ниже). Пакеты транспортируются по сети как независимые информационные блоки. Коммутаторы сети принимают пакеты от конечных узлов и на основании адресной информации передают их друг другу, а в конечном итоге — узлу назначения.



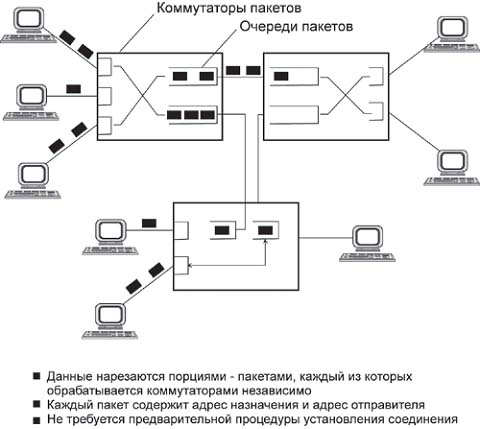
*Разбиение сообщения на пакеты*

Коммутаторы пакетной сети отличаются от коммутаторов каналов тем, что они имеют внутреннюю буферную память для временного хранения пакетов, если выходной порт коммутатора в момент принятия пакета занят передачей другого пакета. В этом случае пакет находится некоторое время в очереди пакетов в буферной памяти выходного порта, а когда до него дойдет очередь, он передается следующему коммутатору. Такая схема передачи данных позволяет сглаживать пульсацию трафика на магистральных связях между коммутаторами и тем самым наиболее эффективно использовать их для повышения пропускной способности сети в целом.

Действительно, для пары абонентов наиболее эффективным было бы предоставление им в единоличное пользование скоммутированный канала связи, как это делается в сетях с коммутацией каналов. В таком случае время взаимодействия этой пары абонентов было бы минимальным, так как данные без задержек передавались бы от одного абонента другому. Простои канала во время пауз передачи абонентов не интересуют, для них важно быстрее решить свою задачу. Сеть с коммутацией пакетов замедляет процесс взаимодействия конкретной пары абонентов, так как их пакеты могут ожидать в коммутаторах, пока по магистральным связям передаются другие пакеты, пришедшие в коммутатор ранее.

Тем не менее, общий объем передаваемых сетью компьютерных данных в единицу времени при технике коммутации пакетов будет выше, чем при технике коммутации каналов. Это происходит потому, что пульсации отдельных абонентов в соответствии с законом больших чисел распределяются во времени так, что их пики не совпадают. Поэтому коммутаторы постоянно и достаточно равномерно загружены работой, если число обслуживаемых ими абонентов действительно велико.

На рисунке ниже показано, что трафик, поступающий от конечных узлов на коммутаторы, распределен во времени очень неравномерно. Однако коммутаторы более высокого уровня иерархии, которые обслуживают соединения между коммутаторами нижнего уровня, загружены более равномерно, и поток пакетов в магистральных каналах, соединяющих коммутаторы верхнего уровня, имеет почти максимальный коэффициент использования. Буферизация сглаживает пульсации, поэтому коэффициент пульсации на магистральных каналах гораздо ниже, чем на каналах абонентского доступа — он может быть равным 1:10 или даже 1:2.



*Сглаживание пульсаций трафика в сети с коммутацией*

*пакетов*

*Пояснение к рисунку.* Данные при коммутации пакетов передаются порциями (пакетами), каждая из которых обрабатывается коммутатором независимо. Каждый пакет содержит адрес назначения и адрес отправителя. Для передачи пакетов не требуется предварительной процедуры установления соединения.

Более высокая эффективность сетей с коммутацией пакетов по сравнению с сетями с коммутацией каналов (при равной пропускной способности каналов связи) была доказана в 60-е годы как экспериментально, так и с помощью имитационного моделирования. Здесь уместна аналогия с мультипрограммными операционными системами. Каждая отдельная программа в такой системе выполняется дольше, чем в однопрограммной системе, когда программе выделяется все процессорное время, пока ее выполнение не завершится. Однако общее число программ, выполняемых за единицу времени, в мультипрограммной системе больше, чем в однопрограммной.

Сеть с коммутацией пакетов замедляет процесс взаимодействия конкретной пары абонентов, но повышает пропускную способность сети в целом.

**Задержки в источнике передачи:**

* время на передачу заголовков;
* задержки, вызванные интервалами между передачей каждого следующего пакета.

**Задержки в каждом коммутаторе:**

* время буферизации пакета;
* время коммутации, которое складывается из:
  + времени ожидания пакета в очереди (переменная величина);
  + времени перемещения пакета в выходной порт.

**Достоинства коммутации пакетов:**

* Высокая общая пропускная способность сети при передаче пульсирующего трафика.
* Возможность динамически перераспределять пропускную способность физических каналов связи между абонентами в соответствии с реальными потребностями их трафика.

**Недостатки коммутации пакетов:**

* Неопределенность скорости передачи данных между абонентами сети, обусловленная тем, что задержки в очередях буферов коммутаторов сети зависят от общей загрузки сети.
* Переменная величина задержки пакетов данных, которая может быть достаточно продолжительной в моменты мгновенных перегрузок сети.
* Возможные потери данных из-за переполнения буферов.

В настоящее время активно разрабатываются и внедряются методы, позволяющие преодолеть указанные недостатки, которые особенно остро проявляются для чувствительного к задержкам трафика, требующего при этом постоянной скорости передачи. Такие методы называются методами обеспечения качества обслуживания (Quality of Service, QoS).

**Выводы по способам коммутации.** Сети с коммутацией пакетов, в которых реализованы методы обеспечения качества обслуживания, позволяют одновременно передавать различные виды трафика, в том числе такие важные как телефонный и компьютерный. Поэтому методы коммутации пакетов сегодня считаются наиболее перспективными для построения конвергентной сети, которая обеспечит комплексные качественные услуги для абонентов любого типа. Тем не менее, нельзя сбрасывать со счетов и методы коммутации каналов. Сегодня они не только с успехом работают в традиционных телефонных сетях, но и широко применяются для образования высокоскоростных постоянных соединений в так называемых первичных (опорных) сетях технологий SDH и DWDM, которые используются для создания магистральных физических каналов между коммутаторами телефонных или компьютерных сетей.

|  |  |
| --- | --- |
| Коммутация каналов | Коммутация пакетов |
| Необходимо предварительно устанавливать соединение | Отсутствует этап установления соединения (дейтаграммный способ) |
| Адрес требуется только на этапе установления соединения | Адрес и другая служебная информация передаются с каждым пакетом |
| Сеть может отказать абоненту в установлении соединения | Сеть всегда готова принять данные от абонента |
| Гарантированная пропускная способность (полоса пропускания) для взаимодействующих абонентов | Пропускная способность сети для абонентов неизвестна, задержки передачи носят случайный характер |
| Трафик реального времени передается без задержек | Ресурсы сети используются эффективно при передаче пульсирующего трафика |
| Высокая надежность передачи | Возможные потери данных из-за переполнения буферов |
| Нерациональное использование пропускной способности каналов, снижающее общую эффективность сети | Автоматическое динамическое распределение пропускной способности физического канала между абонентами |

### Постоянная и динамическая коммутация

Как сети с коммутацией пакетов, так и сети с коммутацией каналов можно разделить на два класса:

* сети с динамической коммутацией;
* сети с постоянной коммутацией.

В сетях с **динамической** коммутацией:

* разрешается устанавливать соединение по инициативе пользователя сети;
* коммутация выполняется только на время сеанса связи, а затем (по инициативе одного из пользователей) разрывается;
* в общем случае пользователь сети может соединиться с любым другим пользователем сети;
* время соединения между парой пользователей при динамической коммутации составляет от нескольких секунд до нескольких часов и завершается после выполнения определенной работы — передачи файла, просмотра страницы текста или изображения и т.п.

Примерами сетей, поддерживающих режим динамической коммутации, являются телефонные сети общего пользования, локальные сети, сети TCP/IP.

Сеть, работающая в режиме **постоянной** коммутации:

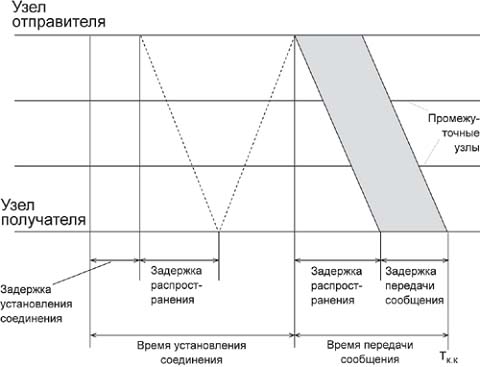
* разрешает паре пользователей заказать соединение на длительный период времени;
* соединение устанавливается не пользователями, а персоналом, обслуживающим сеть;
* период, на который устанавливается постоянная коммутация, составляет обычно несколько месяцев;
* режим постоянной (permanent) коммутации в сетях с коммутацией каналов часто называется сервисом выделенных (dedicated) или арендуемых (leased) каналов;
* в том случае, когда постоянное соединение через сеть коммутаторов устанавливается с помощью автоматических процедур, инициированных обслуживающим персоналом, его часто называют полупостоянным (semi-permanent) соединением, в отличие от режима ручного конфигурирования каждого коммутатора.

Наиболее популярными сетями, работающими в режиме постоянной коммутации, сегодня являются сети технологии SDH, на основе которых строятся выделенные каналы связи с пропускной способностью в несколько гигабит в секунду.

Некоторые типы сетей поддерживают оба режима работы. Например, сети X.25 и ATM могут предоставлять пользователю возможность динамически связаться с любым другим пользователем сети и в то же время отправлять данные по постоянному соединению определенному абоненту.

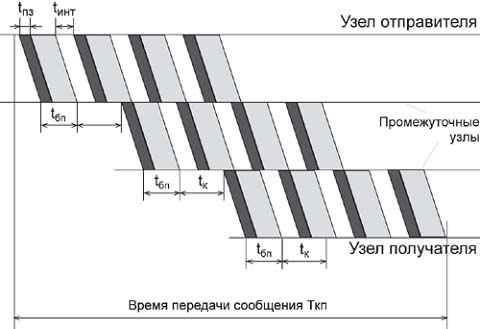
### Пропускная способность сетей с коммутацией пакетов

Одним из отличий метода коммутации пакетов от метода коммутации каналов является неопределенность пропускной способности соединения между двумя абонентами. В случае коммутации каналов после образования составного канала пропускная способность сети при передаче данных между конечными узлами известна — это пропускная способность канала. Данные после задержки, связанной с установлением канала, начинают передаваться на максимальной для канала скорости (рисунок ниже). Время передачи сообщения в сети с коммутацией каналов равно сумме задержки распространения сигнала по линии связи и задержки передачи сообщения. Задержка распространения сигнала зависит от скорости распространения электромагнитных волн в конкретной физической среде, которая колеблется в пределах 0.6…0.9 скорости света в вакууме. Время передачи сообщения равно , где — объем сообщения в битах, а — пропускная способность канала в битах в секунду.



*Задержки передачи данных в сетях с коммутацией каналов*

В сети с коммутацией пакетов картина совсем иная. Процедура установления соединения в этих сетях, если она используется, занимает примерно такое же время, как и в сетях с коммутацией каналов, поэтому будем сравнивать только время передачи данных.



*Задержки при передаче данных в сетях с коммутацией пакетов*

На рисунке выше показан пример передачи данных в сети с коммутацией пакетов. Предполагается, что по сети передается сообщение того же объема, что и сообщение, передаваемое в случае коммутации каналов, однако оно разделено на пакеты, каждый из которых снабжен заголовком. Время передачи сообщения в сети с коммутацией пакетов обозначено на рисунке . При передаче этого разбитого на пакеты сообщения по сети с коммутацией пакетов возникают дополнительные задержки.

Во-первых, это **задержки в источнике передачи**, который, помимо передачи собственно сообщения, тратит дополнительное время на передачу заголовков , к тому же добавляются задержки , вызванные интервалами между передачей каждого следующего пакета (это время уходит на формирование очередного пакета стеком протоколов).

Во-вторых, дополнительное время тратится в каждом коммутаторе. Здесь задержки складываются из времени буферизации пакета (коммутатор не может начать передачу пакета, не приняв его полностью в свой буфер) и времени коммутации . Время буферизации равно времени приема пакета с битовой скоростью протокола. Время коммутации складывается из времени ожидания пакета в очереди и времени перемещения пакета в выходной порт. Если время перемещения пакета фиксировано и, как правило, невелико (от нескольких микросекунд до нескольких десятков микросекунд), то время ожидания пакета в очереди колеблется в очень широких пределах и заранее неизвестно, так как зависит от текущей загрузки сети.

### Числовой пример скорости работы коммутаций

Проведем грубую оценку задержки при передаче данных в сетях с коммутацией пакетов по сравнению с сетями с коммутацией каналов на простейшем примере. Пусть тестовое сообщение, которое нужно передать в обоих видах сетей, имеет объем 200 Кбайт. Отправитель находится от получателя на расстоянии 5000 км. Пропускная способность линий связи составляет 2 Мбит/c.

Время передачи данных по сети с коммутацией каналов складывается из времени распространения сигнала, которое для расстояния 5000 км можно оценить примерно в 25 мс (принимая скорость распространения сигнала равной 2/3 скорости света), и времени передачи сообщения, которое при пропускной способности 2 Мбит/c и длине сообщения 200 Кбайт равно примерно 800 мс. При расчете корректное значение К (210), равное 1024, округлялось до 1000, аналогично значение М (220), равное 1048576, округлялось до 1000000. Таким образом, передача данных оценивается в 825 мс.

Ясно, что при передаче этого сообщения по сети с коммутацией пакетов, обладающей такой же суммарной длиной и пропускной способностью каналов, пролегающих от отправителя к получателю, время распространения сигнала и время передачи данных будут такими же — 825 мс. Однако из-за задержек в промежуточных узлах общее время передачи данных увеличится.

Оценим, на сколько возрастет это время. Будем считать, что путь от отправителя до получателя пролегает через 10 коммутаторов. Пусть исходное сообщение разбивается на пакеты в 1 Кбайт, всего 200 пакетов. Вначале оценим задержку, которая возникает в исходном узле. Предположим, что доля служебной информации, размещенной в заголовках пакетов, по отношению к общему объему сообщения составляет 10%. Следовательно, дополнительная задержка, связанная с передачей заголовков пакетов, составляет 10% от времени передачи целого сообщения, то есть 80 мс. Если принять интервал между отправкой пакетов равным 1 мс, то дополнительные потери за счет интервалов составят 200 мс. Таким образом, в исходном узле из-за пакетирования сообщения при передаче возникла дополнительная задержка в 280 мс.

Каждый из 10 коммутаторов вносит задержку коммутации, которая может составлять от долей до тысяч миллисекунд. В данном примере будем считать, что на коммутацию в среднем тратится 20 мс. Кроме того, при прохождении сообщений через коммутатор возникает задержка буферизации пакета. Эта задержка при величине пакета 1 Кбайт и пропускной способности линии 2 Мбит/c равна 4 мс. Общая задержка, вносимая 10 коммутаторами, составляет примерно 240 мс. В результате дополнительная задержка, созданная сетью с коммутацией пакетов, составила 520 мс. Учитывая, что вся передача данных в сети с коммутацией каналов заняла 825 мс, эту дополнительную задержку можно считать существенной.

Хотя приведенный расчет носит очень приблизительный характер, он объясняет, почему процесс передачи для определенной пары абонентов в сети с коммутацией пакетов является более медленным, чем в сети с коммутацией каналов.

Неопределенная пропускная способность сети с коммутацией пакетов — это плата за ее общую эффективность при некотором ущемлении интересов отдельных абонентов. Аналогично, в мультипрограммной операционной системе время выполнения приложения предсказать невозможно, так как оно зависит от количества других приложений, с которыми данное приложение делит процессор.

На эффективность работы сети влияют размеры пакетов, которые передает сеть. Слишком большие размеры пакетов приближают сеть с коммутацией пакетов к сети с коммутацией каналов, поэтому эффективность сети падает. Кроме того, при большом размере пакетов увеличивается время буферизации на каждом коммутаторе. Слишком маленькие пакеты заметно увеличивают долю служебной информации, так как каждый пакет содержит заголовок фиксированной длины, а количество пакетов, на которые разбиваются сообщения, при уменьшении размера пакета будет резко расти. Существует некоторая «золотая середина», когда обеспечивается максимальная эффективность работы сети, однако это соотношение трудно определить точно, так как оно зависит от многих факторов, в том числе изменяющихся в процессе работы сети. Поэтому разработчики протоколов для сетей с коммутацией пакетов выбирают пределы, в которых может находиться размер пакета, а точнее его поле данных, так как заголовок, как правило, имеет фиксированную длину. Обычно нижний предел поля данных выбирается равным нулю, что дает возможность передавать служебные пакеты без пользовательских данных, а верхний предел не превышает 4 Кбайт. Приложения при передаче данных пытаются занять максимальный размер поля данных, чтобы быстрее выполнить обмен, а небольшие пакеты обычно используются для коротких служебных сообщений, содержащих, к примеру, подтверждение доставки пакета.

### Ethernet как технология коммутации пакетов

Ethernet — пример стандартной технологии коммутации пакетов. Рассмотрим, каким образом описанные выше общие подходы к решению проблем построения сетей воплощены в наиболее популярной сетевой технологии — Ethernet.

|  |  |
| --- | --- |
| **Опр. 3** | **Сетевая технология** — это согласованный набор стандартных протоколов и программно-аппаратных средств (например, сетевых адаптеров, драйверов, кабелей и разъемов), достаточный для построения вычислительной сети. |

Эпитет «достаточный» подчеркивает то обстоятельство, что речь идет о минимальном наборе средств, с помощью которых можно построить работоспособную сеть. Эту сеть можно усовершенствовать, например, за счет выделения в ней подсетей, что сразу потребует кроме протоколов стандарта Ethernet применения протокола IP, а также специальных коммуникационных устройств — маршрутизаторов. Усовершенствованная сеть будет, скорее всего, более надежной и быстродействующей, но за счет надстроек над средствами технологии Ethernet, которая составила базис сети.

Для сетевой технологии Ethernet характерны:

* коммутация пакетов;
* типовая топология «общая шина»;
* плоская числовая адресация;
* разделяемая передающая среда.

Основной принцип, положенный в основу Ethernet, — случайный метод доступа к разделяемой среде передачи данных. В качестве такой среды может использоваться толстый или тонкий коаксиальный кабель, витая пара, оптоволокно или радиоволны.

В стандарте Ethernet строго зафиксирована топология электрических связей. Компьютеры подключаются к разделяемой среде в соответствии с типовой структурой «общая шина» (рисунок ниже). С помощью, разделяемой во времени шины любые два компьютера, могут обмениваться данными. Управление доступом к линии связи осуществляется специальными контроллерами — сетевыми адаптерами Ethernet. Каждый компьютер, а точнее, каждый сетевой адаптер, имеет уникальный MAC-адрес. Передача данных происходит со скоростью 10 Мбит/с. Эта величина является пропускной способностью сети Ethernet.



*Сеть Ethernet*

Суть случайного метода доступа состоит в следующем. Компьютер в сети Ethernet может передавать данные по сети, только если сеть свободна, то есть если никакой другой компьютер в данный момент не занимается обменом. Поэтому важной частью технологии Ethernet является процедура определения доступности среды.

После того как компьютер убедился, что сеть свободна, он начинает передачу и при этом «захватывает» среду. Время монопольного использования разделяемой среды одним узлом ограничивается временем передачи одного кадра.

|  |  |
| --- | --- |
| **Опр. 4** | **Кадр** — это единица данных, которыми обмениваются компьютеры в сети Ethernet. Кадр имеет фиксированный формат и наряду с полем данных содержит различную служебную информацию, например адрес получателя и адрес отправителя. |

Сеть Ethernet устроена так, что при попадании кадра в разделяемую среду передачи данных все сетевые адаптеры начинают одновременно принимать этот кадр. Все они анализируют адрес назначения, располагающийся в одном из начальных полей кадра, и, если этот адрес совпадает с их собственным, кадр помещается во внутренний буфер сетевого адаптера. Таким образом компьютер-адресат получает предназначенные ему данные.

Может возникнуть ситуация, когда несколько компьютеров одновременно решают, что сеть свободна, и начинают передавать информацию. Такая ситуация, называемая коллизией, препятствует правильной передаче данных по сети. В стандарте Ethernet предусмотрен алгоритм обнаружения и корректной обработки коллизий. Вероятность возникновения коллизии зависит от интенсивности сетевого трафика.

После обнаружения коллизии сетевые адаптеры, которые пытались передать свои кадры, прекращают передачу и после паузы случайной длительности пытаются снова получить доступ к среде и передать тот кадр, который вызвал коллизию.

**Основные достоинства технологии Ethernet**

1. Главным достоинством сетей Ethernet, благодаря которому они стали такими популярными, является их экономичность. Для построения сети достаточно иметь по одному сетевому адаптеру для каждого компьютера плюс один физический сегмент коаксиального кабеля нужной длины.

2. Кроме того, в сетях Ethernet реализованы достаточно простые алгоритмы доступа к среде, адресации и передачи данных. Простота логики работы сети ведет к упрощению и, соответственно, снижению стоимости сетевых адаптеров и их драйверов. По той же причине адаптеры сети Ethernet обладают высокой надежностью.

3. И, наконец, еще одним замечательным свойством сетей Ethernet является их хорошая расширяемость, то есть возможность подключения новых узлов.

В сетях с коммутацией пакетов сегодня применяется два класса механизмов передачи пакетов:

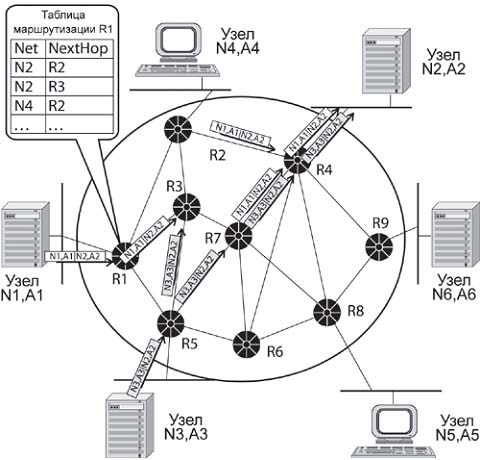
* дейтаграммная передача;
* виртуальные каналы.

Примерами сетей, реализующих дейтаграммный механизм передачи, являются сети Ethernet, IP и IPX. С помощью виртуальных каналов передают данные сети X.25, frame relay и ATM. Сначала мы рассмотрим базовые принципы дейтаграммного подхода.

Дейтаграммный способ передачи данных основан на том, что все передаваемые пакеты обрабатываются независимо друг от друга, пакет за пакетом. Принадлежность пакета к определенному потоку между двумя конечными узлами и двумя приложениями, работающими на этих узлах, никак не учитывается.

Выбор следующего узла — например, коммутатора Ethernet или маршрутизатора IP/IPX — происходит только на основании адреса узла назначения, содержащегося в заголовке пакета. Решение о том, какому узлу передать пришедший пакет, принимается на основе таблицы, содержащей набор адресов назначения и адресную информацию, однозначно определяющую следующий (транзитный или конечный) узел. Такие таблицы имеют разные названия — например, для сетей Ethernet они обычно называются **таблицей продвижения** (forwarding table), а для сетевых протоколов, таких как IP и IPX, — **таблицами маршрутизации** (routing table). Далее для простоты будем пользоваться термином «таблица маршрутизации» в качестве обобщенного названия такого рода таблиц, используемых для дейтаграммной передачи на основании только адреса назначения конечного узла.

В таблице маршрутизации для одного и того же адреса назначения может содержаться несколько записей, указывающих, соответственно, на различные адреса следующего маршрутизатора. Такой подход используется для повышения производительности и надежности сети. В примере на рисунке ниже пакеты, поступающие в маршрутизатор R1 для узла назначения с адресом N2, А2, в целях баланса нагрузки распределяются между двумя следующими маршрутизаторами — R2 и R3, что снижает нагрузку на каждый из них, а значит, уменьшает очереди и ускоряет доставку. Некоторая «размытость» путей следования пакетов с одним и тем же адресом назначения через сеть является прямым следствием принципа независимой обработки каждого пакета, присущего дейтаграммным протоколам. Пакеты, следующие по одному и тому же адресу назначения, могут добираться до него разными путями и вследствие изменения состояния сети, например отказа промежуточных маршрутизаторов.



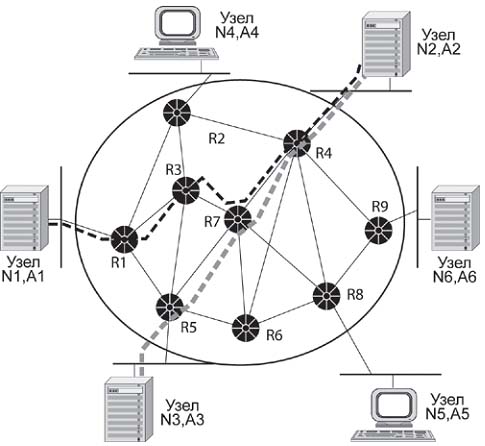
*Дейтаграммный принцип передачи пакетов*

Такая особенность дейтаграммного механизма как размытость путей следования трафика через сеть также в некоторых случаях является недостатком. Например, если пакетам определенной сессии между двумя конечными узлами сети необходимо обеспечить заданное качество обслуживания. Современные методы поддержки QoS работают эффективней, когда трафик, которому нужно обеспечить гарантии обслуживания, всегда проходит через одни и те же промежуточные узлы.

**Виртуальные каналы в сетях с коммутацией пакетов**

Механизм виртуальных каналов (virtual circuit или virtual channel) создает в сети устойчивые пути следования трафика через сеть с коммутацией пакетов. Этот механизм учитывает существование в сети потоков данных.

Если целью является прокладка для всех пакетов потока единого пути через сеть, то необходимым (но не всегда единственным) признаком такого потока должно быть наличие для всех его пакетов общих точек входа и выхода из сети. Именно для передачи таких потоков в сети создаются виртуальные каналы. На рисунке ниже показан фрагмент сети, в которой проложены два виртуальных канала. Первый проходит от конечного узла с адресом N1, A1 до конечного узла с адресом N2, A2 через промежуточные коммутаторы сети R1, R3, R7 и R4. Второй обеспечивает продвижение данных по пути N3, A3 — R5 — R7 — R4 — N2, A2. Между двумя конечными узлами может быть проложено несколько виртуальных каналов, как полностью совпадающих в отношении пути следования через транзитные узлы, так и отличающихся.



*Принцип работы виртуального канала*

Сеть только обеспечивает возможность передачи трафика вдоль виртуального канала, а какие именно потоки будут передаваться по этим каналам, решают сами конечные узлы. Узел может использовать один и тот же виртуальный канал для передачи всех потоков, которые имеют общие с данным виртуальным каналом конечные точки, или же только части из них. Например, для потока реального времени можно использовать один виртуальный канал, а для трафика электронной почты — другой. В последнем случае разные виртуальные каналы будут предъявлять разные требования к качеству обслуживания, и удовлетворить их будет проще, чем в том случае, когда по одному виртуальному каналу передается трафик с разными требованиями к параметрам QoS.

Важной особенностью сетей с виртуальными каналами является использование локальных адресов пакетов при принятии решения о передаче. Вместо достаточно длинного адреса узла назначения (его длина должна позволять уникально идентифицировать все узлы и подсети в сети, например технология АТМ оперирует адресами длиной в 20 байт) применяется локальная, то есть меняющаяся от узла к узлу, метка, которой помечаются все пакеты, перемещаемые по определенному виртуальному каналу. Эта метка в различных технологиях называется по-разному: в технологии X.25 — номер логического канала (Logical Channel number, LCN), в технологии frame relay — идентификатор соединения уровня канала данных (Data Link Connection Identifier, DLCI), в технологии АТМ — идентификатор виртуального канала (Virual Channel Identifier, VCI). Однако назначение ее везде одинаково — промежуточный узел, называемый в этих технологиях коммутатором, читает значение метки из заголовка пришедшего пакета и просматривает свою таблицу коммутации, в которой указывается, на какой выходной порт нужно передать пакет. Таблица коммутации содержит записи только о проходящих через данный коммутатор виртуальных каналах, а не обо всех имеющихся в сети узлах (или подсетях, если применяется иерархический способ адресации). Обычно в крупной сети количество проложенных через узел виртуальных каналов существенно меньше количества узлов и подсетей, поэтому по размерам таблица коммутации намного меньше таблицы маршрутизации, а, следовательно, просмотр занимает гораздо меньше времени и не требует от коммутатора большой вычислительной мощности.

Идентификатор виртуального канала (именно такое название метки будет использоваться далее) также намного короче адреса конечного узла (по той же причине), поэтому и избыточность заголовка пакета, который теперь не содержит длинного адреса, а переносит по сети только идентификатор, существенно меньше.

## Лекция I.4. Стандартизация и классификация сетей

### Классификация сетей

Компьютерные сети классифицируются по двум признакам: общие (пользовательские) и специальные (профессиональные).

**Общие** (пользовательские) признаки:

* по архитектуре;
* по масштабу администрирования;
* по уровню однородности;
* по территориальному признаку;
* по скорости передачи;
* по способу подключения;
* по предоставляемому сервису (службам).

Классификация сетей **по архитектуре**:

* LAN – Local Area Network (ЛВС) – Локальные вычислительные сети: Ethernet, FastEthernet, ARCnet, TokenRing , LokalTalk (Apple) , WLAN, FDDI\*;
* WAN – Wide Area Network (РВС) – Региональные и глобальные вычислительные сети: FDDI\*, ATM, FrameRelay;
* MAN – Metropolian Area Network (TВС) – Городские (территориальные) вычислительные сети.. Это понятие в настоящее вpемя уже не используется. Оно вытеснено понятием WAN;
* GAN – Global Area Network (ГВС) – Глобальные вычислительные сети.Это понятие в настоящее вpемя уже не используется. Оно вытеснено понятием WAN.

Классификация **по масштабу администрирования**:

* Офисные сети (сети отделов);
* Учрежденческие сети (сети кампусов);
* Корпоративные сети;
* Сети общего доступа (Internet).

Классификация **по уровню однородности**:

* Одноранговые (одна машина одновременно клиент и сервер);
* «Клиент-сервер»
  + Клиент – объект (компьютер или программа), запрашивающий некоторые услуги.
  + Сервер – объект (компьютер или программа), предоставляющий некоторые услуги.
* Гибридные;
* Гетерогенные, гомогенные.

Классификация **по скорости передачи данных** (единицы измерения скорости передачи (боды, бит/c, bps, cps, Мб/с, МБ/с):

* коммуникационные модемные каналы: 1200, 2400, 4800, 9600, 14400, 19200, 33600, 56000 bps;
* физическая скорость на коммутируемых телефонных каналах = ( 1200-3000 bod);
* цифровые модемы 64Кб/с, 128 Кб/с, 256Кб/с, 1,0Мб/с, 5Мб/.с, 10Мб/с;
* среднескоростные сети 1, 2, 8, 10, 16, 20 Мб/с;
* скоростные сети 100 Мб/с, 1.5 Гб/с.

Классификация **по типу передающей cреды**:

* проводная (коаксиал, витая паpа, оптоволокно);
* беспроводная (радиоканал, ИК каналы, микроволновые каналы).

Специальные (профессиональные) признаки:

* по топологии сети;
* по способу управления;
* по типу передающей среды;
* по назначению.

Классификация **по топологии сети**:

* сети с топологией «Общая шина»;
* сети с топологией «Звезда»;
* сети с топологией «Кольцо»;
* сети с древовидной топологией;
* сети со смешанной топологией.

### Стандартизация сетей

|  |  |
| --- | --- |
| **Опр. 1** | **Сетевой стандарт** – это набор правил и соглашений, используемых при создании локальной сети и организации передачи данных с применением определенной топологии, оборудования, протоколов и т. д. |

Важнейшим аспектом развития современных телекоммуникационных систем является их стандартизация. Стандартизация необходима всем, кто связан с миром телекоммуникаций, включая производителей электронных компонентов, изготовителей аппаратуры, разработчиков сетей и конечных пользователей. Прежде всего, стандартизация означает массовость производства, что ведет к низким ценам и широкому распространению технологии.

Выбор и утверждение стандарта — это процесс не только технический, но и политический. Как правило, различные фирмы прорабатывают альтернативные варианты будущей технологии. От того, какой из них будет утвержден в качестве стандарта, зависят и объемы будущих прибылей. Поэтому, чтобы стандарт действительно стал общепризнанным, стандартизирующая организация должна быть чрезвычайно авторитетной, а сама процедура утверждения максимально открытой и беспристрастной.

Разработкой стандартов объединенных сетей занимаются самые разные организации путем проведения форумов, превращения неформальных обсуждений в формальные спецификации и распространения их после стандартизации. Большинство организаций, занимающихся стандартизацией, создают формальные стандарты путем проведения специальных мероприятий: формулирования организационных идей, обсуждения подходов, разработки черновых стандартов, голосования по всем или некоторым аспектам. После этого официально издается законченный стандарт.

В зависимости от статуса организаций различают следующие **виды стандартов**:

* стандарты отдельных фирм;
* стандарты специальных комитетов и объединений, создаваемые несколькими фирмами;
* национальные стандарты (например, стандарт FDDI, один из стандартов, разработанных Американским национальным институтом стандартов (ANSI));
* международные стандарты (например, модель и стек OSI Международной организации по стандартизации (ISO)).

Наиболее известные организации, занимающиеся стандартизацией объединенных сетей:

* **Международная организация по стандартизации** (International Organization for Standardization – ISO). ISO является международной организацией, отвечающей за самые различные стандарты, включая многие из тех, которые относятся к сетям. Ее самым известным вкладом в стандартизацию сетей является разработка модели OSI и набора протоколов OSI.
* **Американский национальный институт стандартов** (American National Standards Institute – ANSI). Институт ANSI входит в состав ISO и является координатором групп по стандартизации, формируемых в США на общественных началах. В ANSI был разработан интерфейс распределенной передачи данных по оптоволоконным каналам (Fiber Distributed Data Interface – FDDI) и другие коммуникационные стандарты.
* **Ассоциация электронной промышленности** (Electronic Industries Association – EIA). Ассоциация EIA разрабатывает стандарты передачи данных по электрическим сетям, в том числе и по компьютерным сетям. В EIA разработан широко используемый стандарт EIA/TIA-232 (ранее известный как RS-232).
* **Институт инженеров по электротехнике и радиоэлектронике** (Institute of Electrical and Electronic Engineers -- IEEE). IEEE является профессиональной организацией, разрабатывающей сетевые и другие стандарты. В IEEE разработаны широко используемые стандарты локальных сетей IEEE 802.3 и IEEE 802.5.
* **Международный союз по телекоммуникациям, сектор стандартизации** (International Telecommunication Union Telecommunication Standardization Sector -ITU-T). Ранее он назывался Комитетом по международной телеграфии и телефонии (Comite for International Telegraph and Telephone - CCITT). В настоящее время ITU-T является международной организацией, разрабатывающей стандарты по телекоммуникациям. В частности, в ITU-T был разработан стандарт Х.25.
* **Комитет по вопросам деятельности в Internet** (Internet Activities Board -- IAB). Комитет IAB представляет собой группу исследователей объединенных сетей, обсуждающих вопросы, касающиеся сети Internet, и определяющих общую политику в Internet, принимая решения и формируя для этого рабочие группы. Комитет IAB выпустил некоторые документы Request For Comments (RFC), принятые в качестве стандартов сети Internet, включая протоколы TCP/IP (Transmission Control Protocol/Internet Protocol) и SNMP (Simple Network Management Protocol). Олифер В.Г., Олифер Н.А. - Компьютерные сети. Принципы, технологии, протоколы. переработанное изд.2012год. 943с

В России вопросами стандартизации в качестве головного национального института занимался и продолжает заниматься Госстандарт (в сотрудничестве с отраслевыми институтами ЦНИИС, ЛОНИИС и др.).

### Протокол и стек протоколов

В процессе обмена сообщениями участвуют, по меньшей мере, две стороны, то есть в данном случае необходимо организовать согласованную работу двух иерархий аппаратных и программных средств на разных компьютерах. Оба участника сетевого обмена должны принять множество соглашений.

|  |  |
| --- | --- |
| **Опр. 2** | Стек протоколов – иерархически организованный набор протоколов, достаточный для организации взаимодействия узлов в сети |
| **Опр. 3** | **Открытая система** – любая система (компьютер, вычислительная сеть, ОС и т.д.), построенная в соответствии с открытыми спецификациями. |
| **Опр. 4** | **Спецификация** – формализованное описание аппаратных или программных компонентов, способов их функционирования, взаимодействия с другими компонентами, условий эксплуатации, ограничений и особых характеристик. |
| **Опр. 5** | **Открытые спецификации** – опубликованные, общедоступные спецификации, соответствующие стандартам и принятые в результате достижения согласия после всестороннего обсуждения всеми заинтересованными сторонами. |

Под открытой системой в контексте сетей ЭВМ будем понимать сетевое устройство, готовое взаимодействовать с другими сетевыми устройствами с использованием стандартных правил, определяющих формат, содержание и значение принимаемых и отправляемых сообщений.

Преимущества при соблюдении принципов открытости:

* возможность построения сети из аппаратных и программных средств различных производителей, придерживающихся одного и того же стандарта;
* возможность замены одних компонентов сети другими, что позволяет сети развиваться с минимумом затрат;
* возможность легкого сопряжения одной сети с другой;
* простота освоения и обслуживания сети.

### Общая характеристика модели OSI

Для единого представления данных в сетях с неоднородными устройствами и программным обеспечением международная организация по стандартам ISO (International Standardization Organization) в 1984 году разработала базовую (эталонную) модель обмена информацией в открытых системах OSI (Open System Interconnection). Отдельные уровни модели OSI рассматриваются как группы программ, предназначенных для выполнения определенных функций. Как и любая универсальная модель, OSI довольно громоздка и избыточна. Реальное сетевое оборудование, производимое различными фирмами, не обязательно поддерживает принятое разделение функций.

Все сетевые функции в модели Open System Interconnection разделены на 7 уровней:

1. **Физический уровень** (Physical layer) реализуется аппаратно и обеспечивает передачу битов по физическим каналам, формирование электрических сигналов, кодирование информации, синхронизацию и модуляцию.
2. **Канальный уровень** (Data Link layer) реализуются программно-аппаратно и обеспечивает надежную доставку пакетов между двумя соседними узлами в сети с произвольной топологией и любыми узлами в сети с типовой топологией, а также проверку доступности разделяемой среды, выделение кадров из потока данных и их формирование, подсчет и проверку контрольной суммы.
3. **Сетевой уровень** (Network layer) служит для образования единой транспортной системы, объединяющей несколько сетей, причем эти сети могут использовать различные принципы передачи сообщений между конечными узлами и обладать произвольной структурой связей.
4. **Транспортный уровень** (Transport layer) обеспечивает приложениям или верхним уровням стека передачу данных с той степенью надежности, которая им требуется.
5. **Сеансовый уровень** (Session layer) обеспечивает управление диалогом: фиксирует, какая из сторон является активной в настоящий момент, предоставляет средства синхронизации.
6. **Представительный уровень** (Presentation layer) согласовывает представление (синтаксис) данных при взаимодействии двух прикладных процессов: преобразование данных из внешнего формата во внутренний; шифрование и расшифровка данных.
7. **Прикладной уровень** (Application layer) — это набор разнообразных протоколов, с помощью которых пользователи сети получают доступ к разделяемым ресурсам. Единица данных, которой оперирует прикладной уровень, обычно называется сообщением (message). При этом вышестоящие уровни реализуют более сложные, глобальные процессы, для чего используют в своих целях нижестоящие уровни, а также управляют ими. Задача нижестоящего уровня – предоставление услуг вышестоящему уровню, причем вышестоящему уровню не важны детали реализации этих услуг. Нижестоящие уровни выполняют более простые и конкретные функции. Каждый уровень взаимодействует только с соседними уровнями (выше и ниже него). Верхний уровень соответствует прикладной задаче (работающему в данный момент приложению), нижний – непосредственной передаче сигналов по каналу связи.

Модель OSI относится не только к локальным сетям, но и к любым сетям связи между компьютерами или другими абонентами. В частности, взаимодействие в сети Интернет также можно поделить на уровни в соответствии с моделью OSI. Принципиальные отличия локальных сетей от глобальных, с точки зрения этой модели, наблюдаются только на нижних ее уровнях.

Функции, входящие в уровни модели OSI, реализуются всеми участниками сетевого взаимодействия. При этом каждый уровень одного абонента работает так, как будто у него есть прямая связь с соответствующим уровнем другого абонента. Между одноименными уровнями абонентов сети существует виртуальная (логическая) связь, например, между прикладными уровнями взаимодействующих по сети абонентов. Реальную физическую связь (кабель, радиоканал) абоненты одной сети имеют только на нижнем, первом, физическом уровне. В передающем абоненте информация проходит все уровни модели OSI, начиная с верхнего и заканчивая нижним, в принимающем абоненте полученная информация совершает обратный путь: от нижнего уровня к верхнему.

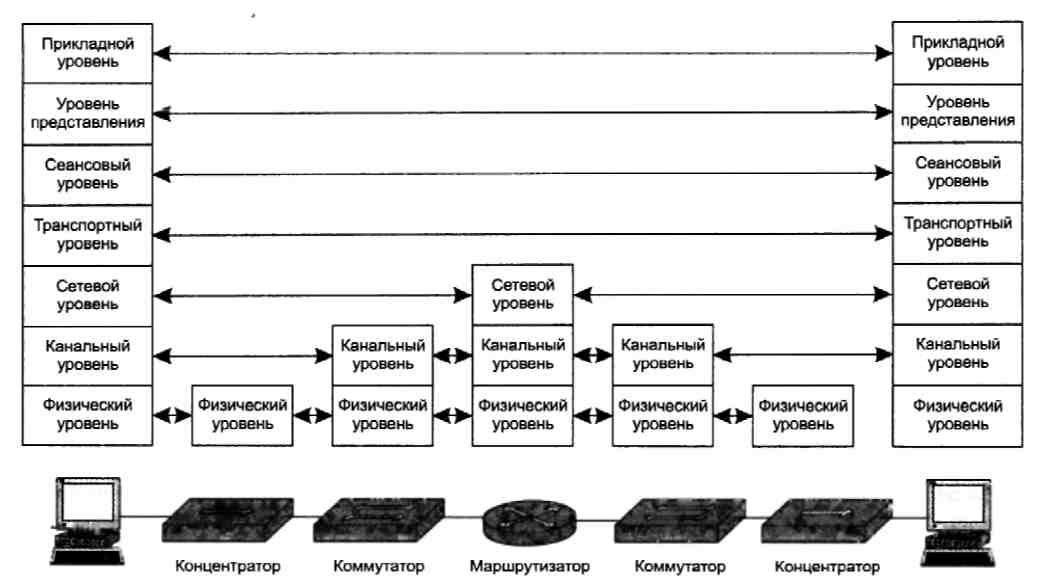
Данные, предназначенные для передачи по сети, на пути от верхнего (седьмого) уровня до нижнего (первого) проходят процесс упаковки – инкапсуляции. Каждый нижеследующий уровень не только производит обработку данных, приходящих с более высокого уровня, но и снабжает их своим заголовком, а также служебной информацией. Такой процесс обрастания служебной информацией продолжается до последнего (физического) уровня. На физическом уровне эта многооболочечная конструкция передается по кабелю приемнику. Там она проходит обратную процедуру декапсуляции, то есть при передаче на вышестоящий уровень убирается одна из оболочек. Верхнего седьмого уровня достигают данные, освобожденные от всех оболочек, то есть от всей служебной информации нижестоящих уровней. При этом каждый уровень абонента приемника производит обработку данных, полученных с нижеследующего уровня по правилам, указанным в убираемой им служебной информации пакета.

Если на пути между абонентами в сети включаются промежуточные устройства, например, трансиверы, репитеры, концентраторы, коммутаторы, маршрутизаторы, то и они тоже могут выполнять функции, входящие в нижние уровни модели OSI. Чем больше сложность этого промежуточного устройства, тем выше уровень функции, которого оно реализует. Но любое промежуточное устройство должно принимать и возвращать информацию на нижнем, физическом уровне, поэтому все внутренние преобразования данных должны производиться дважды и в противоположных направлениях. Промежуточные сетевые устройства в отличие от полноценных абонентов (например, компьютеров) работают только на нижних уровнях модели OSI.

**Функции уровней:**

* Прикладной (7) уровень (Application Layer) или уровень приложений обеспечивает услуги, непосредственно поддерживающие приложения пользователя. Такие как, программные средства передачи файлов, доступа к базам данных, средства электронной почты, службу регистрации на сервере. Этот уровень управляет всеми нижележащими шестью уровнями. Например, если пользователь работает с электронными таблицами Excel и решает сохранить рабочий файл в своей папке на сетевом файл-сервере, то прикладной уровень обеспечивает перемещение файла с локального компьютера на сетевой диск прозрачно для пользователя. К распространенным протоколам верхних трех уровней (7-6-5) относятся:
* FTP (File Transfer Protocol) протокол передачи файлов;
* TFTP (Trivial File Transfer Protocol) протокол пересылки файлов;
* X.400 электронная почта;
* Telnet работа с удаленным терминалом;
* SMTP (Simple Mail Transfer Protocol) протокол почтового обмена;
* CMIP (Common Management Information Protocol) общий протокол управления информацией;
* SLIP (Serial Line IP) IP для последовательных линий. Протокол посимвольной последовательной передачи данных;
* SNMP (Simple Network Management) протокол сетевого управления;
* FTAM (File Transfer, Access, and Management) протокол передачи, доступа и управления файлами.
* Представительский (6) уровень (Presentation Layer) (уровень представления данных) определяет и преобразует форматы данных и их синтаксис в форму, приемлемую для передачи по сети, то есть выполняет функцию переводчика. На этом уровне производится шифрование, дешифрирование данных и их сжатие. Стандартные форматы существуют для текстовых файлов (ASCII, EBCDIC, HTML), звуковых файлов (MIDI, MPEG, WAV), видео (AVI), рисунков (JPEG, GIF, TIFF). Все преобразования форматов представления данных выполняются на представительском уровне.
* Сеансовый (5) уровень (Session Layer) осуществляет управление проведением сеансов связи (устанавливает, поддерживает, прекращает связь). Этот уровень предусматривает три режима проведения сеансов: симплексный (передача данных в одном направлении), полудуплексный (передача данных поочередно в обоих направлениях) и полнодуплексный (передача данных в двух направлениях одновременно). Сеансовый уровень может устанавливать в поток данных специальные контрольные точки, которые позволяют восстанавливать процесс передачи при разрыве связи, после его возобновления. Уровень распознает логические имена абонентов, контролирует их права доступа. Протоколы сетевого уровня реализуются программными модулями операционной системы, а также аппаратными и программными средствами маршрутизаторов.
* Транспортный (4) уровень (Transport Layer) обеспечивает доставку пакетов в нужной последовательности без потерь и ошибок. Здесь же производится разбивка передаваемых данных на блоки, помещаемые в пакеты, и восстановление принимаемых данных из пакетов. Транспортный уровень является промежуточным и связующим между верхними тремя, зависящими от приложений, и тремя нижними уровнями, взаимодействующими с конкретной сетью. Наиболее распространенные протоколы транспортного уровня:
  + TCP (Transmission Control Protocol) протокол управления передачей стека TCP/IP;
  + NCP (NetWare Core Protocol) NetWare - базовый протокол сетей;
  + SPX (Sequenced Packet eXchange) Novell - обмен пакетами.
* Сетевой (3) уровень (Network Layer) отвечает за адресацию пакетов и преобразование логических имен (логических адресов, например, IP-адресов или IPX-адресов) в физические сетевые MAC-адреса (и наоборот). На этом же уровне решается задача выбора пути (маршрута), по которому пакет доставляется к нужному абоненту (если в сети имеется несколько маршрутов). На сетевом уровне действуют такие сложные промежуточные сетевые устройства, как маршрутизаторы. Чаще других на сетевом уровне используются протоколы:
* IP (Internet Protocol) протокол Internet, сетевой протокол стека TCP/IP - предоставляет адресную и маршрутную информацию;
* IPX (Internetwork Packet Exchange) протокол межсетевого обмена пакетами, предназначенный для адресации и маршрутизации пакетов в сетях Novell;
* X.25 международный стандарт для глобальных коммуникаций с коммутацией пакетов (частично этот протокол реализован на уровне 2).
* Канальный (2) уровень (Data link Layer) отвечает за формирование пакетов (кадров) стандартного для данной сети (Ethernet, Token-Ring, FDDI) вида. Он же производит управление доступом к сети, обнаруживает ошибки передачи путем подсчета контрольных сумм, и производит повторную пересылку приемнику ошибочных пакетов. Канальный уровень делится на два подуровня: верхний LLC и нижний MAC. На канальном уровне работают промежуточные сетевые – коммутаторы. Наиболее часто используемые протоколы на канальном уровне включают:
* HDLC (High Level Data Link Control) протокол управления каналом передачи данных высокого уровня;
* IEEE 802.2 LLC обеспечивают MAC для физических сред 802.x;
* X.25 международный стандарт для глобальных коммуникаций с коммутацией пакетов;
* Frame relay сеть, организованная из технологий Х25 и ISDN.
* Физический (1) уровень (Physical Layer) – это самый нижний уровень модели OSI, который отвечает за кодирование передаваемой информации в уровни сигналов, принятые в данной среде передачи, и обратное декодирование. Здесь же определяются требования к соединителям, защите от помех, разъемам, заземлению, электрическому согласованию и т.д. На физическом уровне модели OSI работают такие сетевые устройства, как трансиверы, репитеры и репитеры-концентраторы.

Полный стек протоколов реализован только на конечных узлах, а промежуточные узлы поддерживают протоколы всего трех нижних уровней. Для продвижения пакетов достаточно функциональности нижних трех уровней.



*Соответствие функций различных устройств сети уровням модели OSI*

Сетевые повторители, работающие на физическом уровне, называются концентраторами, или хабами. Они повторяют электрические сигналы, поступающие на одни их интерфейсы, на других своих интерфейсах, улучшая их характеристики — мощность и форму сигналов, синхронность их следования.

Коммутаторы локальных сетей поддерживают протоколы двух нижних уровней, физического и канального, что дает им возможность работать в пределах стандартных топологий.

Маршрутизаторы должны поддерживать протоколы всех трех уровней, так как сетевой уровень нужен им для объединения сетей различных технологий, а протоколы нижних уровней для взаимодействия с конкретными сетями, образующими составную сеть.

В компьютерах коммуникационные протоколы всех уровней (кроме физического и части функций канального уровня) реализуются программно операционной системой или системными приложениями.

Конечные узлы сети (компьютеры и компьютеризованные устройства, например мобильные телефоны) всегда предоставляют как информационные, так и транспортные услуги, а промежуточные узлы сети — только транспортные.

### Вспомогательные протоколы транспортной системы

В реальных сетях некоторые из коммуникационных устройств поддерживают не только протоколы трех нижних уровней, но и протоколы верхних уровней. Так, маршрутизаторы реализуют протоколы маршрутизации, позволяющие автоматически строить таблицы маршрутизации, а концентраторы и коммутаторы часто поддерживают протоколы SNMP и telnet, которые не нужны для выполнения основных функций этих устройств, но позволяют конфигурировать их и управлять ими удаленно. Все эти протоколы являются протоколами прикладного уровня и выполняют некоторые вспомогательные (служебные) функции транспортной системы. Очевидно, что для работы прикладных протоколов сетевые устройства должны также поддерживать протоколы промежуточных уровней, таких как IP и TCP/UDP.

Вспомогательные протоколы можно разделить на группы в соответствии с их функциями:

* Первую группу вспомогательных протоколов представляют протоколы маршрутизации, такие как RIP, OSPF, BGP. Без этих протоколов маршрутизаторы не смогут продвигать пакеты, так как таблица маршрутизации будет пустой (если только администратор не заполнит ее вручную, но это не очень хорошее решение для крупной сети).
* Другая группа вспомогательных протоколов выполняет преобразование адресов. Здесь работает протокол DNS, который преобразует символьные имена узлов в IP-адреса. Протокол DHCP позволяет назначать IP-адреса узлам динамически, а не статически, что облегчает работу администратора сети.
* Третью группу образуют протоколы, которые используются для управления сетью. В стеке TCP/IP здесь находится протокол SNMP (Simple Network Management Protocol — простой протокол управления сетью), который позволяет автоматически собирать информацию об ошибках и отказах устройств, а также протокол Telnet, с помощью которого администратор может удаленно конфигурировать коммутатор или маршрутизатор.

Помимо модели OSI существует также модель IEEE Project 802, принятая в феврале 1980 года (поэтому 802 в названии), которую можно рассматривать как модификацию, развитие, дополнение модели OSI. Стандарты, определяемые этой моделью (спецификации - 802) относятся к двум нижним уровням модели OSI и делятся на двенадцать категорий, каждой из которых присвоен свой номер, например:

* 802.3 – локальная сеть с шинной топологией и методом доступа CSMA/CD;
* 802.5 – локальная сеть с маркерным доступом и топологией кольцо (Token-Ring);
* 802.6 – городская сеть (Metropolitan Area Network, MAN) с расстояниями между сетевыми узлами более 5 км;
* 802.8 – волоконно-оптическая технология;
* 802.11 – беспроводная сеть по радиоканалу (WLAN – Wireless LAN).

## Лекция I.5. Сетевые характеристики и качество обслуживания

Главным требованием, предъявляемым к сетям, является выполнение сетью ее основной функции – обеспечение пользователям потенциальной возможности доступа к разделяемым ресурсам всех компьютеров, объединенных в сеть. Все остальные требования – ***производительность, надежность, совместимость, управляемость, защищенность, расширяемость и масштабируемость*** – связаны с качеством выполнения этой основной задачи.

Хотя все эти требования весьма важны, часто понятие «качество обслуживания» (Quality of Service, QpS) компьютерной сети трактуется более узко – в него включаются только две самые важные характеристики сети – **производительность** и **надежность**.

Независимо от выбранного показателя качества обслуживания сети существуют два подхода к его обеспечению. Первый подход, очевидно, покажется наиболее естественным с точки зрения пользователя сети. Он состоит в том, что сеть (точнее, обслуживающий ее персонал) гарантирует пользователю соблюдение некоторой числовой величины показателя качества обслуживания. Например, сеть может гарантировать пользователю А, что любой из его пакетов, посланных пользователю В, будет задержан сетью не более, чем на 150 мс. Или, что средняя пропускная способность канала между пользователями А и В не будет ниже 5 Мбит/с, при этом канал будет разрешать пульсации трафика в 10 Мбит на интервалах времени не более 2 секунд.

Второй подход состоит в том, что сеть обслуживает пользователей в соответствии с их приоритетами. То есть качество обслуживания зависит от степени привилегированности пользователя или группы пользователей, к которой он принадлежит. Качество обслуживания в этом случае не гарантируется, а гарантируется только уровень привилегий пользователя. Такое обслуживание называется обслуживанием **best effort** – с наибольшим старанием. Сеть старается по возможности более качественно обслужить пользователя, но ничего при этом не гарантирует. По такому принципу работают, например, локальные сети, построенные на коммутаторах с приоритезацией кадров.

### Производительность

Потенциально высокая производительность – это одно из основных свойств распределенных систем, к которым относятся компьютерные сети. Это свойство обеспечивается возможностью распараллеливания работ между несколькими компьютерами сети. К сожалению, эту возможность не всегда удается реализовать.

Существует несколько основных характеристик производительности сети:

* время реакции;
* пропускная способность;
* задержка передачи и вариация задержки передачи.

**Время реакции** сети является интегральной характеристикой производительности сети с точки зрения пользователя. Именно эту характеристику имеет в виду пользователь, когда говорит: «Сегодня сеть работает медленно».

В общем случае время реакции определяется как интервал времени между возникновением запроса пользователя к какой-либо сетевой службе и получением ответа на этот запрос.

Очевидно, что значение этого показателя зависит от типа службы, к которой обращается пользователь, от того, какой пользователь и к какому серверу обращается, а также от текущего состояния элементов сети – загруженности сегментов, коммутаторов и маршрутизаторов, через которые проходит запрос, загруженности сервера и т. п. Поэтому имеет смысл использовать также и средневзвешенную оценку времени реакции сети, усредняя этот показатель по пользователям, серверам и времени дня (от которого в значительной степени зависит загрузка сети).

Время реакции сети обычно складывается из нескольких составляющих. В общем случае в него входит (1) время подготовки запросов на клиентском компьютере, (2) время передачи запросов между клиентом и сервером через сегменты сети и (3) промежуточное коммуникационное оборудование, (4) время обработки запросов на сервере, (5) время передачи ответов от сервера клиенту и время обработки получаемых от сервера ответов на клиентском компьютере.

Ясно, что пользователя разложение времени реакции на составляющие не интересует – ему важен конечный результат, однако для сетевого специалиста очень важно выделить из общего времени реакции составляющие, соответствующие этапам собственно сетевой обработки данных, передачу данных от клиента к серверу через сегменты сети и коммуникационное оборудование.

Знание сетевых составляющих времени реакции дает возможность оценить производительность отдельных элементов сети, выявить узкие места и в случае необходимости выполнить модернизацию сети для повышения ее общей производительности.

**Пропускная способность** отражает объем данных, переданных сетью или ее частью в единицу времени. Пропускная способность уже не является пользовательской характеристикой, так как она говорит о скорости выполнения внутренних операций сети – передачи пакетов данных между узлами сети через различные коммуникационные устройства. Зато она непосредственно характеризует качество выполнения основной функции сети – транспортировки сообщений, и поэтому чаще используется при анализе производительности сети, чем время реакции. Пропускная способность измеряется либо в битах в секунду, либо в пакетах в секунду. Пропускная способность может быть мгновенной, максимальной и средней.

**Средняя пропускная способность** вычисляется путем деления общего объема переданных данных на время их передачи, причем выбирается достаточно длительный промежуток времени – час, день или неделя.

**Мгновенная пропускная способность** отличается от средней тем, что для усреднения выбирается очень маленький промежуток времени - например, 10 мс или 1 с.

**Максимальная пропускная способность** – это наибольшая мгновенная пропускная способность, зафиксированная в течение периода наблюдения.

Чаще всего при проектировании, настройке и оптимизации сети используются такие показатели, как средняя и максимальная пропускные способности. Средняя пропускная способность отдельного элемента или всей сети позволяет оценить работу сети на большом промежутке времени, в течение которого в силу закона больших чисел пики и спады интенсивности трафика компенсируют друг друга. Максимальная пропускная способность позволяет оценить возможности сети справляться с пиковыми нагрузками, характерными для особых периодов работы сети, например утренних часов, когда сотрудники предприятия почти одновременно регистрируются в сети и обращаются к разделяемым файлам и базам данных.

Пропускную способность можно измерять между любыми двумя узлами или точками сети, например между клиентским компьютером и сервером, между входным и выходным портами маршрутизатора. Для анализа и настройки сети очень полезно знать данные о пропускной способности отдельных элементов сети.

Важно отметить, что из-за последовательного характера передачи пакетов различными элементами сети общая пропускная способность сети любого составного пути в сети будет равна минимальной из пропускных способностей составляющих элементов маршрута. Для повышения пропускной способности составного пути необходимо в первую очередь обратить внимание на самые медленные элементы – в данном случае таким элементом, скорее всего, будет маршрутизатор. Следует подчеркнуть, что если передаваемый по составному пути трафик будет иметь среднюю интенсивность, превосходящую среднюю пропускную способность самого медленного элемента пути, то очередь пакетов к этому элементу будет расти теоретически до бесконечности, а практически – до тех пор, пока не заполниться его буферная память, а затем пакеты просто начнут отбрасываться и теряться.

Иногда полезно оперировать с общей пропускной способностью сети, которая определяется как среднее количество информации, переданной между всеми узлами сети в единицу времени. Этот показатель характеризует качество сети в целом, не дифференцируя его по отдельным сегментам или устройствам.

Обычно при определении пропускной способности сегмента или устройства в передаваемых данных не выделяются пакеты какого-то определенного пользователя, приложения или компьютера – подсчитывается общий объем передаваемой информации. Тем не менее для более точной оценки качества обслуживания такая детализации желательна, и в последнее время системы управления сетями все чаще позволяют ее выполнять.

**Задержка передачи** определяется как задержка между моментом поступления пакета на вход какого-либо сетевого устройства или части сети и моментом появления его на выходе этого устройства. Этот параметр производительности по смыслу близок ко времени реакции сети, но отличается тем, что всегда характеризует только сетевые этапы обработки данных, без задержек обработки компьютерами сети. Обычно качество сети характеризуют величинами максимальной задержки передачи и вариацией задержки. Не все типы трафика чувствительны к задержкам передачи, во всяком случае, к тем величинам задержек, которые характерны для компьютерных сетей, обычно задержки не превышают сотен миллисекунд, реже – нескольких секунд. Такого порядка задержки пакетов, порождаемых файловой службой, службой электронной почты или службой печати, мало влияют на качество этих служб с точки зрения пользователя сети. С другой стороны, такие же задержки пакетов, переносящих голосовые данные или видеоизображение, могут приводить к значительному снижению качества предоставляемой пользователю информации – возникновению эффекта «эха», невозможности разобрать некоторые слова, дрожание изображения и т. п.

Пропускная способность и задержки передачи являются независимыми параметрами, так что сеть может обладать, например, высокой пропускной способностью, но вносить значительные задержки при передаче каждого пакета. Пример такой ситуации дает канал связи, образованный геостационарным спутником. Пропускная способность этого канала может быть весьма высокой, например 2 Мбит/с, в то время как задержка передачи всегда составляет не менее 0,24 с, что определяется скоростью распространения сигнала (около 300 000 км/с) и длиной канала (72 000 км).

### Надежность и безопасность

Одной из первоначальных целей создания распределенных систем, к которым относятся и вычислительные сети, являлось достижение большей надежности по сравнению с отдельными вычислительными машинами.

Важно различать несколько аспектов надежности. Для технических устройств используются такие показатели надежности, как (1) среднее время наработки на отказ, (2) вероятность отказа, (3) интенсивность отказов. Однако эти показатели пригодны для оценки надежности простых элементов и устройств, которые могут находиться только в двух состояниях – работоспособном или неработоспособном. Сложные системы, состоящие из многих элементов, кроме состояний работоспособности и неработоспособности, могут иметь и другие промежуточные состояния, которые эти характеристики не учитывают. В связи с этим для оценки надежности сложных систем применяется другой набор характеристик.

**Готовность или коэффициент готовности (availability)** означает долю времени, в течение которого система может быть использована. Готовность может быть улучшена путем введения избыточности в структуру системы: ключевые элементы системы должны существовать в нескольких экземплярах, чтобы при отказе одного из них функционирование системы обеспечивали другие.

Чтобы систему можно было отнести к высоконадежным, она должна как минимум обладать высокой готовностью, но этого недостаточно. Необходимо обеспечить **сохранность данных и защиту их от искажений**. Кроме этого, должна поддерживаться **согласованность (непротиворечивость) данных**, например, если для повышения надежности на нескольких файловых серверах хранится несколько копий данных, то нужно постоянно обеспечивать их идентичность.

Так как сеть работает на основе механизма передачи пакетов между конечными узлами, то одной из характерных характеристик надежности является вероятность доставки пакета узлу назначения без искажений. Наряду с этой характеристикой могут использоваться и другие показатели: (1) вероятность потери пакета (по любой из причин – из-за переполнения буфера маршрутизатора, из-за несовпадения контрольной суммы, из-за отсутствия работоспособного пути к узлу назначения и т. д.), (2) вероятность искажения отдельного бита передаваемых данных, (3) отношение потерянных пакетов к доставленным.

Другим аспектом общей надежности является **безопасность (security)**, то есть способность системы защитить данные от несанкционированного доступа. В распределенной системе это сделать гораздо сложнее, чем в централизованной. В сетях сообщения передаются по линиям связи, часто проходящим через общедоступные помещения, в которых могут быть установлены средства прослушивания линий. Другим уязвимым местом могут быть оставленные без присмотра персональные компьютеры. Кроме того, всегда имеется потенциальная угроза взлома защиты сети от неавторизованных пользователей, если сеть имеет выходы в глобальные сети общего пользования.

Еще одной характеристикой надежности является **отказоустойчивость (fault tolerance)**. В сетях под отказоустойчивостью понимается способность системы скрыть от пользователя отказ отдельных ее элементов. Например, если копии таблицы базы данных хранятся одновременно на нескольких файловых серверах, то пользователи могут просто не заметить отказ одного из них. В отказоустойчивой системе отказ одного из ее элементов приводит к некоторому снижению качества ее работы (деградации), а не к полному останову. Так, при отказе одного из файловых серверов в предыдущем примере увеличивается только время доступа к базе данных из-за уменьшения степени распараллеливания запросов, но в целом система будет продолжать выполнять свои функции.

### Расширяемость и масштабируемость

Термины расширяемость и масштабируемость иногда используют как синонимы, но это неверно – каждый из них имеет четко определенное самостоятельное значение.

**Расширяемость (extensibility)** означает возможность сравнительно легкого добавления отдельных элементов сети (пользователей, компьютеров, приложений, служб), наращивания длины сегментов сети и замены существующей аппаратуры более мощной. При этом принципиально важно, что легкость расширения системы иногда может обеспечиваться в некоторых весьма ограниченных пределах. Например, локальная сеть Ethernet, построенная на основе одного сегмента толстого коаксиального кабеля, обладает хорошей расширяемостью, в том смысле, что позволяет легко подключать новые станции. Однако такая сеть имеет ограничение на число станций – их число не должно превышать 30-40. Хотя сеть допускает физическое подключение к сегменту и большего числа станций (до 100), но при этом чаще всего резко снижается производительность сети. Наличие такого ограничения и является признаком плохой масштабируемости системы при хорошей расширяемости.

**Масштабируемость (scalability)** означает, что сеть позволяет наращивать количество узлов и протяженность связей в очень широких пределах, при этом производительность сети не ухудшается. Для обеспечения масштабируемости сети приходится применять дополнительное коммуникационное оборудование и специальным образом структурировать сеть. Например, хорошей масштабируемостью обладает многосегментная сеть, построенная с использованием коммутаторов и маршрутизаторов и имеющая иерархическую структуру связей. Такая сеть может включать несколько тысяч компьютеров и при этом обеспечивать каждому пользователю сети нужное качество обслуживания.

### Прозрачность

**Прозрачность (transparency)** сети достигается в том случае, когда сеть представляется пользователям не как множество отдельных компьютеров, связанных между собой сложной системой кабелей, а как единая традиционная вычислительная машина с системой разделения времени. Известный лозунг компании Sun Microsystems: «Сеть – это компьютер» говорит именно о такой прозрачной сети.

Прозрачность может быть достигнута на двух различных уровнях – на уровне пользователя и на уровне программиста. На уровне пользователя прозрачность означает, что для работы с удаленными ресурсами он использует те же команды и привычные ему процедуры, что и для работы с локальными ресурсами. На программном уровне прозрачность заключается в том, что приложению для доступа к удаленным ресурсам требуются те же вызовы, что и для доступа к локальным ресурсам. Прозрачность на уровне пользователя достигается проще, так как все особенности процедур, связанные с распределенным характером системы, маскируются от пользователя программистом, который создает приложение. Прозрачность на уровне приложения требует сокрытия всех деталей распределенности средствами сетевой операционной системы.

Сеть должна скрывать все особенности операционных систем и различия в типах компьютеров. Пользователь компьютера Macintosh должен иметь возможность обращаться к ресурсам, поддерживаемым UNIX-системой, а пользователь UNIX должен иметь возможность разделять информацию с пользователями Windows 95. Подавляющее число пользователей ничего не хочет знать о внутренних форматах файлов или о синтаксисе команд UNIX. Пользователь терминала IBM 3270 должен иметь возможность обмениваться сообщениями с пользователями сети персональных компьютеров без необходимости вникать в секреты трудно запоминаемых адресов.

Концепция прозрачности может быть применена к различным аспектам сети. Например, прозрачность расположения означает, что от пользователя не требуется знаний о месте расположения программных и аппаратных ресурсов, таких как процессоры, принтеры, файлы и базы данных. Имя ресурса не должно включать информацию о месте его расположения, поэтому имена типа mashinel : prog.c или \\ftp\_serv\pub прозрачными не являются. Аналогично, прозрачность перемещения означает, что ресурсы должны свободно перемещаться из одного компьютера в другой без изменения своих имен. Еще одним из возможных аспектов прозрачности является прозрачность параллелизма, заключающаяся в том, что процесс распараллеливания вычислений происходит автоматически, без участия программиста, при этом система сама распределяет параллельные ветви приложения по процессорам и компьютерам сети. В настоящее время нельзя сказать, что свойство прозрачности в полной мере присуще многим вычислительным сетям, это скорее цель, к которой стремятся разработчики современных сетей.

### Поддержка разных видов трафика

Компьютерные сети изначально предназначены для совместного доступа пользователя к ресурсам компьютеров: файлам, принтерам и т. п. Трафик, создаваемый этими традиционными службами компьютерных сетей, имеет свои особенности и существенно отличается от трафика сообщений в телефонных сетях или, например, в сетях кабельного телевидения. Однако 90-е годы стали годами проникновения в компьютерные сети трафика мультимедийных данных, представляющих в цифровой форме речь и видеоизображение. Компьютерные сети стали использоваться для организации видеоконференций, обучения и развлечения на основе видеофильмов и т. п. Естественно, что для динамической передачи мультимедийного трафика требуются иные алгоритмы и протоколы и, соответственно, другое оборудование. Хотя доля мультимедийного трафика пока невелика, он уже начал свое проникновение как в глобальные, так и локальные сети, и этот процесс, очевидно, будет продолжаться с возрастающей скоростью.

Главной особенностью трафика, образующегося при динамической передаче голоса или изображения, является наличие жестких требований к синхронности передаваемых сообщений. Для качественного воспроизведения непрерывных процессов, которыми являются звуковые колебания или изменения интенсивности света в видеоизображении, необходимо получение измеренных и закодированных амплитуд сигналов с той же частотой, с которой они были измерены на передающей стороне. При запаздывании сообщений будут наблюдаться искажения.

В то же время трафик компьютерных данных характеризуется крайне неравномерной интенсивностью поступления сообщений в сеть при отсутствии жестких требований к синхронности доставки этих сообщений. Например, доступ пользователя, работающего с текстом на удаленном диске, порождает случайный поток сообщений между удаленным и локальным компьютерами, зависящий от действий пользователя по редактированию текста, причем задержки при доставке в определенных (и достаточно широких с компьютерной точки зрения) пределах мало влияют на качество обслуживания пользователя сети. Все алгоритмы компьютерной связи, соответствующие протоколы и коммуникационное оборудование были рассчитаны именно на такой «пульсирующий» характер трафика, поэтому необходимость передавать мультимедийный трафик требует внесения принципиальных изменений как в протоколы, так и оборудование. Сегодня практически все новые протоколы в той или иной степени предоставляют поддержку мультимедийного трафика.

Особую сложность представляет совмещение в одной сети традиционного компьютерного и мультимедийного трафика. Передача исключительно мультимедийного трафика компьютерной сетью хотя и связана с определенными сложностями, но вызывает меньшие трудности. А вот случай сосуществования двух типов трафика с противоположными требованиями к качеству обслуживания является намного более сложной задачей. Обычно протоколы и оборудование компьютерных сетей относят мультимедийный трафик к факультативному, поэтому качество его обслуживания оставляет желать лучшего. Сегодня затрачиваются большие усилия по созданию сетей, которые не ущемляют интересы одного из типов трафика. Наиболее близки к этой цели сети на основе технологии АТМ, разработчики которой изначально учитывали случай сосуществования разных типов трафика в одной сети.

### Управляемость

Управляемость сети подразумевает возможность централизованно контролировать состояние основных элементов сети, выявлять и разрешать проблемы, возникающие при работе сети, выполнять анализ производительности и планировать развитие сети. В идеале средства управления сетями представляют собой систему, осуществляющую наблюдение, контроль и управление каждым элементом сети - от простейших до самых сложных устройств, при этом такая система рассматривает сеть как единое целое, а не как разрозненный набор отдельных устройств.

Хорошая система управления наблюдает за сетью и, (1) *обнаружив проблему*, активизирует определенное действие, (2) *исправляет ситуацию* и (3) *уведомляет администратора* о том, что произошло и какие шаги предприняты. Одновременно с этим система управления должна (4) *накапливать данные*, на основании которых можно планировать развитие сети. Наконец, система управления должна быть независима от производителя и обладать удобным интерфейсом, позволяющим выполнять все действия с одной консоли.

Решая тактические задачи, администраторы и технический персонал сталкиваются с ежедневными проблемами обеспечения работоспособности сети. Эти задачи требуют быстрого решения, обслуживающий сеть персонал должен оперативно реагировать на сообщения о неисправностях, поступающих от пользователей или автоматических средств управления сетью. Постепенно становятся заметны более общие проблемы производительности, конфигурирования сети, обработки сбоев и безопасности данных, требующие стратегического подхода, то есть планирования сети. Планирование, кроме этого, включает прогноз изменений требований пользователей к сети, вопросы применения новых приложений, новых сетевых технологий и т. п.

Полезность системы управления особенно ярко проявляется в больших сетях: корпоративных или публичных глобальных. Без системы управления в таких сетях нужно присутствие квалифицированных специалистов по эксплуатации в каждом здании каждого города, где установлено оборудование сети, что в итоге приводит к необходимости содержания огромного штата обслуживающего персонала.

В настоящее время в области систем управления сетями много нерешенных проблем. Явно недостаточно действительно удобных, компактных и многопротокольных средств управления сетью. Большинство существующих средств вовсе не управляют сетью, а всего лишь осуществляют наблюдение за ее работой. Они следят за сетью, но не выполняют активных действий, если с сетью что-то произошло или может произойти. Мало масштабируемых систем, способных обслуживать как сети масштаба отдела, так и сети масштаба предприятия, очень многие системы управляют только отдельными элементами сети и не анализируют способность сети выполнять качественную передачу данных между конечными пользователями сети.

### Совместимость

Совместимость или интегрируемость означает, что сеть способна включать в себя самое разнообразное программное и аппаратное обеспечение, то есть в ней могут сосуществовать различные операционные системы, поддерживающие разные стеки коммуникационных протоколов, и работать аппаратные средства и приложения от разных производителей. Сеть, состоящая из разнотипных элементов, называется неоднородной или гетерогенной, а если гетерогенная сеть работает без проблем, то она является интегрированной. Основной путь построения интегрированных сетей - использование модулей, выполненных в соответствии с открытыми стандартами и спецификациями.

### Выводы

Качество работы сети характеризуют следующие свойства: производительность, надежность, совместимость, управляемость, защищенность, расширяемость и масштабируемость.

Существуют два основных подхода к обеспечению качества работы сети. Первый состоит в том, что сеть гарантирует пользователю соблюдение некоторой числовой величины показателя качества обслуживания. Например, сети frame relay и АТМ могут гарантировать пользователю заданный уровень пропускной способности. При втором подходе (best effort) сеть старается по возможности более качественно обслужить пользователя, но ничего при этом не гарантирует.

К основным характеристикам производительности сети относятся: время реакции, которое определяется как время между возникновением запроса к какому-либо сетевому сервису и получением ответа на него; пропускная способность, которая отражает объем данных, переданных сетью в единицу времени, и задержка передачи, которая равна интервалу между моментом поступления пакета на вход какого-либо сетевого устройства и моментом его появления на выходе этого устройства.

Для оценки надежности сетей используются различные характеристики, в том числе: коэффициент готовности, означающий долю времени, в течение которого система может быть использована; безопасность, то есть способность системы защитить данные от несанкционированного доступа; отказоустойчивость - способность системы работать в условиях отказа некоторых ее элементов.

Расширяемость означает возможность сравнительно легкого добавления отдельных элементов сети (пользователей, компьютеров, приложений, сервисов), наращивания длины сегментов сети и замены существующей аппаратуры более мощной.

Масштабируемость означает, что сеть позволяет наращивать количество узлов и протяженность связей в очень широких пределах, при этом производительность сети не ухудшается.

Прозрачность – свойство сети скрывать от пользователя детали своего внутреннего устройства, упрощая тем самым его работу в сети.

Управляемость сети подразумевает возможность централизованно контролировать состояние основных элементов сети, выявлять и разрешать проблемы, возникающие при работе сети, выполнять анализ производительности и планировать развитие сети.

Совместимость означает, что сеть способна включать в себя самое разнообразное программное и аппаратное обеспечение.

## Семинар I.1. Линии связи

В рамках основной программы рассматриваются практические примеры с рассмотрением особенностей и свойств линий связи, изложенных в рамках лекционной части.

Вне основной программы:

* GIT (GITHUB);
* Open Server

## Семинар I.2. Кодирование и мультиплексирование данных

### Аналогово-цифровое преобразование

### Дискретизация по времени и квантование по уровню

### Мультиплексирование данных

### Кадр. Межкадровая задержка

### Мультиплексирование и демультиплексирование

### Временная и амплитудная модуляция. Несущая волна

## Семинар I.3. Принципы организации первичных сетей

### Организация локальной сети

### Установка и настройка локального сервера

### Передача файлов по протоколам html/ftp

## Семинар I.4. Ethernet в локальных сетях

Ethernet — пример стандартной технологии коммутации пакетов. Рассмотрим, каким образом описанные выше общие подходы к решению проблем построения сетей воплощены в наиболее популярной сетевой технологии — Ethernet.

Эпитет «достаточный» подчеркивает то обстоятельство, что речь идет о минимальном наборе средств, с помощью которых можно построить работоспособную сеть. Эту сеть можно усовершенствовать, например, за счет выделения в ней подсетей, что сразу потребует кроме протоколов стандарта Ethernet применения протокола IP, а также специальных коммуникационных устройств — маршрутизаторов. Усовершенствованная сеть будет, скорее всего, более надежной и быстродействующей, но за счет надстроек над средствами технологии Ethernet, которая составила базис сети.

Для сетевой технологии Ethernet характерны:

* коммутация пакетов;
* типовая топология «общая шина»;
* плоская числовая адресация;
* разделяемая передающая среда.

Основной принцип, положенный в основу Ethernet, — случайный метод доступа к разделяемой среде передачи данных. В качестве такой среды может использоваться толстый или тонкий коаксиальный кабель, витая пара, оптоволокно или радиоволны.

В стандарте Ethernet строго зафиксирована топология электрических связей. Компьютеры подключаются к разделяемой среде в соответствии с типовой структурой «общая шина» (рисунок ниже). С помощью, разделяемой во времени шины любые два компьютера, могут обмениваться данными. Управление доступом к линии связи осуществляется специальными контроллерами — сетевыми адаптерами Ethernet. Каждый компьютер, а точнее, каждый сетевой адаптер, имеет уникальный MAC-адрес. Передача данных происходит со скоростью 10 Мбит/с. Эта величина является пропускной способностью сети Ethernet.



*Сеть Ethernet*

Суть случайного метода доступа состоит в следующем. Компьютер в сети Ethernet может передавать данные по сети, только если сеть свободна, то есть если никакой другой компьютер в данный момент не занимается обменом. Поэтому важной частью технологии Ethernet является процедура определения доступности среды.

После того как компьютер убедился, что сеть свободна, он начинает передачу и при этом «захватывает» среду. Время монопольного использования разделяемой среды одним узлом ограничивается временем передачи одного кадра.

Сеть Ethernet устроена так, что при попадании кадра в разделяемую среду передачи данных все сетевые адаптеры начинают одновременно принимать этот кадр. Все они анализируют адрес назначения, располагающийся в одном из начальных полей кадра, и, если этот адрес совпадает с их собственным, кадр помещается во внутренний буфер сетевого адаптера. Таким образом компьютер-адресат получает предназначенные ему данные.

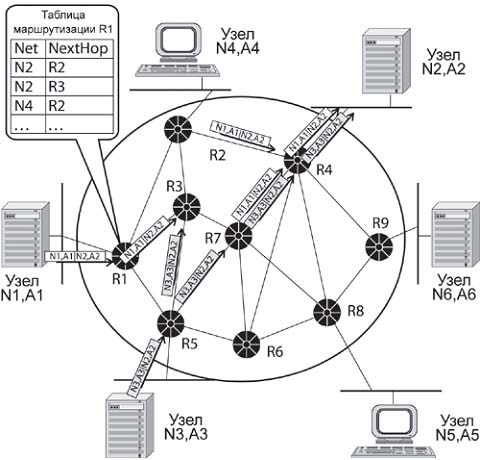
Может возникнуть ситуация, когда несколько компьютеров одновременно решают, что сеть свободна, и начинают передавать информацию. Такая ситуация, называемая коллизией, препятствует правильной передаче данных по сети. В стандарте Ethernet предусмотрен алгоритм обнаружения и корректной обработки коллизий. Вероятность возникновения коллизии зависит от интенсивности сетевого трафика.

После обнаружения коллизии сетевые адаптеры, которые пытались передать свои кадры, прекращают передачу и после паузы случайной длительности пытаются снова получить доступ к среде и передать тот кадр, который вызвал коллизию.

Дейтаграммный способ передачи данных основан на том, что все передаваемые пакеты обрабатываются независимо друг от друга, пакет за пакетом. Принадлежность пакета к определенному потоку между двумя конечными узлами и двумя приложениями, работающими на этих узлах, никак не учитывается.

Выбор следующего узла — например, коммутатора Ethernet или маршрутизатора IP/IPX — происходит только на основании адреса узла назначения, содержащегося в заголовке пакета. Решение о том, какому узлу передать пришедший пакет, принимается на основе таблицы, содержащей набор адресов назначения и адресную информацию, однозначно определяющую следующий (транзитный или конечный) узел. Такие таблицы имеют разные названия — например, для сетей Ethernet они обычно называются **таблицей продвижения** (forwarding table), а для сетевых протоколов, таких как IP и IPX, — **таблицами маршрутизации** (routing table). Далее для простоты будем пользоваться термином «таблица маршрутизации» в качестве обобщенного названия такого рода таблиц, используемых для дейтаграммной передачи на основании только адреса назначения конечного узла.

В таблице маршрутизации для одного и того же адреса назначения может содержаться несколько записей, указывающих, соответственно, на различные адреса следующего маршрутизатора. Такой подход используется для повышения производительности и надежности сети. В примере на рисунке ниже пакеты, поступающие в маршрутизатор R1 для узла назначения с адресом N2, А2, в целях баланса нагрузки распределяются между двумя следующими маршрутизаторами — R2 и R3, что снижает нагрузку на каждый из них, а значит, уменьшает очереди и ускоряет доставку. Некоторая «размытость» путей следования пакетов с одним и тем же адресом назначения через сеть является прямым следствием принципа независимой обработки каждого пакета, присущего дейтаграммным протоколам. Пакеты, следующие по одному и тому же адресу назначения, могут добираться до него разными путями и вследствие изменения состояния сети, например отказа промежуточных маршрутизаторов.



*Дейтаграммный принцип передачи пакетов*

Такая особенность дейтаграммного механизма как размытость путей следования трафика через сеть также в некоторых случаях является недостатком. Например, если пакетам определенной сессии между двумя конечными узлами сети необходимо обеспечить заданное качество обслуживания. Современные методы поддержки QoS работают эффективней, когда трафик, которому нужно обеспечить гарантии обслуживания, всегда проходит через одни и те же промежуточные узлы.

## Семинар I.5. Ethernet операторского класса

Ethernet – известное всем коммерческое название локальной сети Ethernet, которая дает возможность сетевым операторам обеспечить своим пользователям сервисы Ethernet в этих сетях. Сеть Ethernet с момента своего изобретения Робертом Меткалфом (Robert Metcalfe) в 1972 в Исследовательском центре Xerox Palo Alto (XPARC), рис. 1, и последующего предложения использовать ее в 1973 в качестве технологии ЛС прошла долгий путь развития от полудуплексной сети, работавшей на частоте 10 МГц, до полностью дуплексной сети, работающей сегодня уже на частоте 100 ГГц [1, 2].

За эти 40 лет технология Ethernet стала доминирующей не только среди технологий локальных сетей (ЛС), но и в сетях масштаба предприятия. Этот факт привел не только к росту масштаба сетей (а он продолжился от корпоративных до городских метро-сетей), но и к разработке огромного количества сетевых компонентов, которые, в свою очередь, резко снизили себестоимость передаваемых данных. За время своего развития сеть Ethernet расширила список доступной ей среды передачи: медные кабели, витые медные пары, оптоволокно и беспроводная среда. Ее скорости сейчас зашкаливают, выходя на уровень 100–400 Гбит/с [2, 3]. Интерфейсы гигабитного и 10-гигабитного Ethernet сейчас широко используются в рабочих станциях, серверах и мультиплексорах SONET/SDH. А передача потоков на скоростях n×100 Гбит/с осуществляется мультиплексорами SDH, WDM и мультисервисными транспортными платформами, используя не только иерархии SONET/SDH, но и оптическую иерархию OTH [4] на скоростях, стандартизованных в иерархиях и стандартами 40/100-гигабитного Ethernet [1–4].

### Предпосылки создания Ethernet операторского класса (CGE)

Описывая сети Ethernet операторского класса, нужно прежде всего указать на предпосылки, которые привели к созданию CGE (ниже будем использовать сокращение CGE – Carrier Grade Ethernet, а не CE – Carrier Ethernet, чтобы не путать с сокращениями CE для терминов типа Customer Edge, Customer Equipment, см. [5]).

Исторически конкурирующие протоколы и различные кабельные среды, используемые Ethernet, были созданы, прежде всего, для того, чтобы иметь доступ к высокоскоростным, а не к современным устройствам, подключенным к сети Ethernet и обслуживаемым за приемлемую цену. Одна из причин создания конкурирующих протоколов была как раз в том, чтобы снизить цену устройств, работающих с сетью Ethernet на приемлемой скорости.

Протокол Ethernet был достаточно прост и легко масштабировался для работы на скоростях в сотни и десятки тысячи раз выше исходной (достаточно вспомнить ряд рабочих скоростей Ethernet за последние 40 лет: 0,01–0,1–1–10–100 Гбит/с) и был одинаково хорошо адаптирован к этим новым скоростям. Например, новые возможности во временной области, добавленные к стандарту IEEE 802.3 Ethernet для поддержки передачи потоков аудио-видео (AV) данных по ЛС (см. IEEE 802.1 Audio Video Bridging [6]), оказались удобными для приложений, чувствительным к временным задержкам, таким, например, как протокол точного времени IEEE 1588.

Кроме постоянного роста скорости, все больше ЛС-пользователей присоединялись к различным глобальным сетям связи (ГлС), используя интерфейсы Ethernet, или к устройствам, которые имели мостовые переходы в эти сети (например, к цифровой абонентской линии – DSL), или реализовали беспроводную связь между ними. Более того, пользователи, знакомые с такими возможностями сетей Ethernet, могли расширить их для сложных сетей со многими узлами. Необходимость в использовании таких сетей росла, так как они включали много таких сервисов, которые обрабатывались раньше только в ЛС или при наличии специальных соединений, к ним относились, прежде всего, видеосервисы и резервное копирование.

### Ограничения операторов

Из сказанного следует, что операторы глобальных (ГлС/WAN) и региональных/городских (MAN) сетей сталкивались с необходимостью обеспечить три потребности:

* Получение для своих пользователей сервисов Ethernet.
* Использование преимуществ технологии Ethernet по стоимости и объему предоставляемых услуг.
* Замену не-Ethernet-технологий на конкурентные Ethernet-технологии, которые имели бы достаточную емкость сети для хранения контента, резервного копирования и реализации видео высокой четкости, а также гарантировали особенности (надежность передачи и малую задержку), необходимые для поддержки этих сервисов.

Операторы, однако, были ограничены тем, что ряд локальных сервисов не мог мигрировать в глобальные сервисы так быстро, чтобы не превысить возможности ресурсов, обеспеченных сетью, и не получить в результате неприемлемое качество услуг. Сервисы, которые старались расширить слишком быстро, приводили к потере денег, а те, которые требовали слишком долгого ожидания, приводили к потере пользователей. Следовательно, операторы должны были расширять свои сервисы достаточно консервативно, обращая особое внимание на обеспечение качества сервиса (QoS).

### Исходная позиция: Metro-Ethernet

В этой ситуации (в 2001) был организован Форум Metro-Ethernet (MEF). Его цель состояла в том, чтобы разрабатывать общие бизнес-сервисы для сотрудников предприятий, которые имеют доступ в Интернет через оптоволоконные городские сети, соединяя ЛС их предприятий. Принципиальным моментом этой концепции было сформировать простую стоимостную модель Ethernet для глобальной сети [7].

### Расширение до Ethernet операторского класса

Успех сервисов Metro-Ethernet привлек внимание мировой общественности, когда эта концепция была расширена, чтобы включить мировые сервисы, попадающие в национальные и глобальные сети [7], или оптимизировать существующие сети/сервисы:

* включить сервисы сетей доступа, чтобы обеспечить возможности сервисов для более широкого класса пользователей, используя волокно, медный провод, кабель, пассивные оптические сети (PON) и беспроводной доступ;
* оптимизировать (уменьшить) масштабы сетей в результате конвергенции бизнесов, совместного использования районных и беспроводных сетей, охватывающих ту же инфраструктуру и сервисы;
* сделать упор на быстрое развертывание и масштабируемость бизнес-приложений;
* развернуть программы сертификации;
* реализовать все в целом, сохраняя стоимостную модель и простоту сети Ethernet.

### «Сервисы Ethernet» операторского класса

Чтобы создать рынок сервисов Ethernet, необходимо было выяснить и стандартизировать предлагаемые сервисы. Этим (в первую очередь) занялся Форум MEF. Он сыграл ключевую роль в определении трех базовых сервисов:

* E-Line – линия Ethernet – сервис, соединяющий два порта пользователей Ethernet с помощью WAN;
* E-LAN – ЛС Ethernet – многоточечный сервис, соединяющий набор конечных точек пользователей и дающий пользователю видимость того, что эти точки соединены мостами с ЛС Ethernet;
* E-Tree – частное дерево Ethernet – многоточечный сервис, соединяющий один или несколько корневых точек с набором листьев, но предохраняющего их от взаимной связи.

Все эти сервисы стали атрибутами CE/CGE-1 и обеспечили стандартные определения таких характеристик, как ширина полосы, устойчивость к отказам и мультиплексирование сервисов. Они позволяли пользователям сравнивать предложения сервисов и облегчать заключение соглашений об уровне обслуживания (SLA). Аналогичные определения для беспроводных сетей были приведены в стандартах IEEE 802.21 и IEEE 802.11u и нацелены на сервисы, пригодные для мобильных пользователей.

### Транспорт сервисов Ethernet

Форум MEF не указывает, как сервисы Ethernet должны быть обеспечены в сети оператора. Несмотря на преимущества Ethernet, описанные выше, он имеет ряд ограничений при реализации приложений глобальных сетей (WAN). Концепции типа "мост" и "покрывающее дерево" (spanning tree), характерные для ЛС Ethernet, не могут масштабироваться до уровня международных сетей. Более того, у Ethernet отсутствуют механизмы, связанные с функциональной надежностью, необходимой для реализации этих приложений (в частности, механизмы, способные изолировать трафик одного пользователя от другого, чтобы, например, измерить производительность конкретного сервиса пользователя или же оперативно определить характер отказа и восстановить его работу в больших сетях).

Ввиду этих ограничений сервисы Ethernet могли быть переданы по ГлС только с помощью других технологий. Если копнуть глубже, то ограничения сети Ethernet вызваны тем, что Ethernet – это ЛС, а взаимодействовать ей нужно с ГлС. Как же дотянуть ЛС Ethernet до уровня ГлС, чтобы без проблем осуществить транспорт любых сервисов? Решить этот вопрос не так просто даже для таких организаций, как ITU-T и MEF, но можно. Ниже показаны шаги, которые нужно предпринять, чтобы найти приемлемое решение. Эти шаги привели к созданию нового класса технологий – Ethernet операторского класса (CE/CGE-1,2).

### Альтернативные признаки, или Чем ЛС отличается от ГлС

Сначала попытаемся разобраться в том, чем ЛС отличается от ГлС, для этого вспомним традиционную классификацию сетей. Она была разная у разных сетевых специалистов. Специалисты ЛС использовали известный стереотип: LAN, MAN, WAN. Специалисты ГлС говорили о сетях доступа, распределительных и транспортных сетях или приводили другие традиционные классификации [8].

Оказалось, что для оценки различия удобнее перенести центр тяжести первой классификации с сетей на технологии, также разбив их на два класса: локальные и глобальные. Это позволило уйти от указанного стереотипа и конкретизировать набор альтернативных признаков, которые можно сравнивать. Такой набор был предложен и обоснован в работе [8] и представлен в табл. 1. Оценив различие технологий, можно будет понять, как преодолеть их и добиться их нужного взаимодействия (табл. 1).

**Первый** признак – условия работы. В ГлС для передачи сообщения между узлами А и Б требуется предварительное установление соединения: при коммутации цепей нужно соединить звенья сети, формируя непрерывную физическую цепь; при коммутации пакетов нужно установить виртуальное соединение (VC) между узлами, исключающее необходимость маршрутизации.

Для ЛС все узлы внутри сети заранее соединены кабелем (Ethernet), а между собой ЛС соединены мостами, коммутаторами или маршрутизаторами. Предварительное соединение узлов не требуется, нужно установить лишь маршрут следования пакетов. Образ такой сети – "облако/море", по которому "плывут" пакеты (дейтаграммы), отсюда и сети называются дейтаграммными.

**Второй** признак – тип передачи: синхронная или асинхронная. Все цифровые ГлС используют синхронную передачу, т.е. требуют использовать тактовую синхронизацию. Все ЛС не требуют синхронизации, так как передают только асинхронные потоки данных. Это могут делать и ГлС, после того, как преобразуют их в синхронные потоки с помощью специальных устройств (PAD/FRAD) [9].

**Третий** признак – адресация. Поддержка адресаций E.164 и X.121, характерных для ТфОП, – черта всех ГлС. В ЛС существуют другие адресации: физическая (MAC) и логическая (IP), не поддерживаемые ГлС. Поэтому при взаимодействии ЛС и ГлС (например, в IP-телефонии) используют шлюзы, преобразующие эти адреса.

**Четвертый** признак – тип модели. Модели ГлС (одноуровневые или многоуровневые) должны иметь выход на физический уровень ТфОП. Известно [9], что в любом случае физический уровень модели должен быть совместим с физическим уровнем ТфОП (или иметь выход на него).

Модели ЛС тоже имеют физический уровень, но он функционально не соответствует физическому уровню ТфОП (табл. 2).

Для технологий ЛС, чтобы выйти на ТфОП, нужны глобальные технологии-переносчики, такие как PDH, SONET/SDH, IP/MPLS (ограниченно) и WDM. Они инкапсулируют пакеты ЛС в полезную нагрузку или модулируют сигналом ЛС несущую WDM.

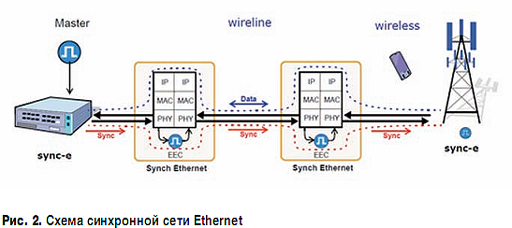
### Как преодолеть различия ЛС и ГлС на пути создания CGE

Из тех различий, которые нужно было преодолеть Ethernet, чтобы стать сетью CGE, первые два преодолевались легко. Действительно, оставаясь в рамках пакетной передачи, характерной для ЛС, легко перейти на формирование виртуального пути (как это делается в ATM и FR [9]), преодолев первое различие: предварительно будет устанавливаться не физическое, а виртуальное соединение.

Второе различие было преодолено путем создания синхронных сетей Ethernet – SyncE.

### Синхронные сети Ethernet

Синхронный Ethernet, SyncE (рис. ниже), – ITU-T-стандарт, разработанный для облегчения передачи синхросигналов через физический уровень Ethernet.



Master – ведущий таймер; wireline, wireless – проводные и беспроводные технологии;

Data, Sync – данные, синхронизация; EEC – ведомый таймер оборудования сетей Ethernet).

Цель разработки – обеспечить сигнал синхронизации для тех сетевых ресурсов, которым он требуется. Этот сигнал может быть отслежен внешними источниками синхронизации, в идеале ведущим таймером сети (рис. 2). Приложения Synch Ethernet (SE) включают сети сотовой связи, проводные технологии доступа, такие как Ethernet PON (EPON) и приложения IPTV или VoIP. Семейство сетей Ethernet, однако, не передает информацию об источниках синхронизации, как, например, сети SDH [9], хотя что-то похожее используется в разработках IETF: Network Time Protocol (NTP) и Precision Time Protocol (РТР).

SyncE был стандартизован ITU-T в кооперации c IEEE и описан в трех основных рекомендациях: G.8261, G.8262 и G.8264. Архитектура SyncE минимально требует замены внутреннего таймера карты Ethernet на таймер с фазовой автоподстройкой частоты, чтобы питать физический уровень Ethernet (PHY).

Преодолеть различие других альтернативных признаков – различия адресации ЛС и ТфОП и несовместимость физических уровней ЛС и ГлС – оказалось значительно труднее. Однако различие в адресации можно преодолеть, используя конвертацию адресов, разработанную для IP-телефонии, а несовместимость физических уровней – только инкапсуляцией пакетов Ethernet в полезную нагрузку одной из технологий ГлС.

Три из них (SONET/SDH, IP/MPLS и WDM) широко используются для этих целей, тогда как четвертая – CET (Carrier Ethernet Transport – транспорт Ethernet операторского класса) – быстро развивается как жизнеспособный логичный вариант передачи сервисов Ethernet.

# Модуль II. Сети TCP/IP. Сетевые информационные службы

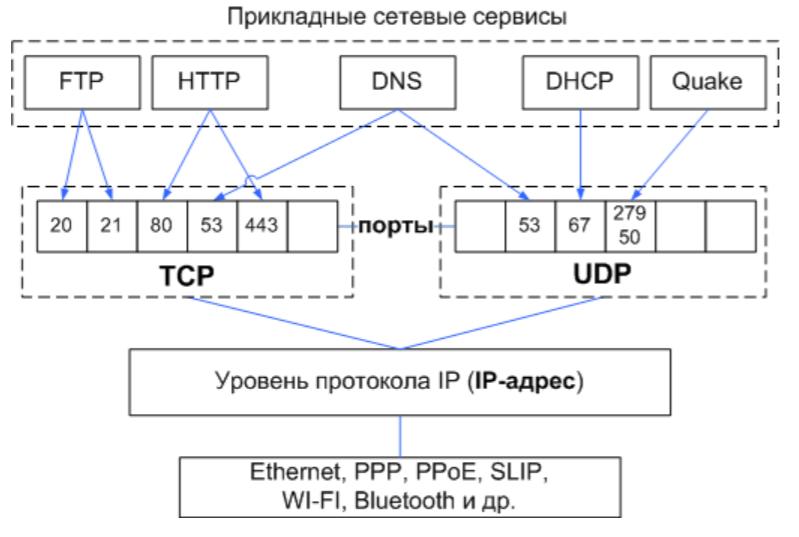
## Лекция II.1. Адресация в стеке протоколов TCP/IP. Протокол межсетевого взаимодействия IP. IPv6 как развитие стека TCP/IP

### Основы TCP/IP

Стек протоколов TCP/IP (Transmission Control Protocol/Internet Protocol, протокол управления передачей/протокол интернета) — сетевая модель, описывающая процесс передачи цифровых данных. Она названа по двум главным протоколам, по этой модели построена глобальная сеть — интернет. Сейчас это кажется невероятным, но в 1970-х информация не могла быть передана из одной сети в другую, с целью обеспечить такую возможность был разработан стек интернет-протоколов также известный как TCP/IP.

Разработкой этих протоколов занималось Министерство обороны США, поэтому иногда модель TCP/IP называют DoD (Department of Defence) модель. Если вы знакомы с моделью OSI (Open System Interconnection), то вам будет проще понять построение модели TCP/IP, потому что обе модели имеют деление на уровни, внутри которых действуют определенные протоколы и выполняются собственные функции. Мы разделили статью на смысловые части, чтобы было проще понять, как устроена модель TCP/IP:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Модель OSI | | Модель TCP/IP | | Пример протокола |
| Прикладной уровень | 7 | 4 | Прикладной уровень | HTTP (80), HTTPS (443)  FTP(20), SSH (22),  DNS (53) и др. |
| Уровень представления | 6 |
| Сеансовый уровень | 5 |
| Транспортный уровень | 4 | 3 | Транспортный уровень | TCP, UDP |
| Сетевой уровень | 3 | 2 | Межсетевой уровень | IGMP, ICMP, ICMPv6 |
| Канальный уровень | 2 | 1 | Канальный уровень | Ethernet, WLAN, Token Ring и др. |
| Физический уровень | 1 |



### Уровневая модель TCP/IP

Выше мы уже упоминали, что модель TCP/IP разделена на уровни, как и OSI, но отличие двух моделей в количестве уровней. Документом, регламентирующим уровневую архитектуру модели и описывающий все протоколы, входящие в TCP/IP, является RFC 1122. Стандарт включает четыре уровня модели TCP/IP, хотя, например, согласно Таненбауму (Таненбаум Э., Уэзеролл Д. Т18 Компьютерные сети), в модели может быть пять уровней.

Три верхних уровня — прикладной, транспортный и сетевой — присутствуют как в RFC, так и у Таненбаума и других авторов. А вот стоит ли говорить только о канальном или о канальном и физическом уровнях — нет единого мнения. В RFC они объединены, поскольку выполняют одну функцию. В статье мы придерживаемся официального интернет-стандарта RFC и не выделяем физический уровень в отдельный. Далее мы рассмотрим четыре уровня модели.

### Канальный уровень

Предназначение канального уровня — дать описание тому, как происходит обмен информацией на уровне сетевых устройств, определить, как информация будет передаваться от одного устройства к другому. Информация здесь кодируется, делится на пакеты и отправляется по нужному каналу, т.е. среде передачи.

Этот уровень также вычисляет максимальное расстояние, на которое пакеты возможно передать, частоту сигнала, задержку ответа и т.д. Все это — физические свойства среды передачи информации. На канальном уровне самым распространенным протоколом является Ethernet, но мы рассмотрим его на примере в конце статьи.

### Межсетевой уровень

Каждая индивидуальная сеть называется локальной, глобальная сеть интернет позволяет объединить все локальные сети. За объединение локальных сетей в глобальную отвечает сетевой уровень. Он регламентирует передачу информации по множеству локальных сетей, благодаря чему открывается возможность взаимодействия разных сетей.

Межсетевое взаимодействие — это основной принцип построения интернета. Локальные сети по всему миру объединены в глобальную, а передачу данных между этими сетями осуществляют магистральные и пограничные маршрутизаторы.

### Транспортный уровень

Постоянные резиденты транспортного уровня — протоколы TCP и UDP, они занимаются доставкой информации.

|  |  |
| --- | --- |
| **Опр. 1** | **TCP** (Transmission Control Protocol – протокол управления передачей) — надежный, он обеспечивает передачу информации, проверяя дошла ли она, насколько полным является объем полученной информации и т.д. TCP дает возможность двум хостам производить обмен пакетами через установку соединения. Он предоставляет услугу для приложений, повторно запрашивает потерянную информацию, устраняет дублирующие пакеты, регулируя загруженность сети. TCP гарантирует получение и сборку информации у адресата в правильном порядке.    Формат заголовка сегмента TCP    Структура пакета TCP    Структура псевдозаголовка пакета TCP |
| **Опр. 2** | **UDP** (User Datagram Protocol – протокол пользовательских датаграмм) — ненадежный, он занимается передачей автономных датаграмм. UDP не гарантирует, что всех датаграммы дойдут до получателя. Датаграммы уже содержат всю необходимую информацию, чтобы дойти до получателя, но они все равно могут быть потеряны или доставлены в порядке отличном от порядка при отправлении.    Формат заголовка пакета UDP    Структура пакета UDP    Структура псевдозаголовка пакета UDP |
| **Опр. 3** | **Датаграмма** (англ. datagram, дейтаграмма) — блок информации, передаваемый протоколом через сеть связи без предварительного установления соединения и создания виртуального канала. Любой протокол, не устанавливающий предварительное соединение (а также обычно не контролирующий порядок приёмо-передачи и дублирование пакетов), называется датаграммным протоколом. Таковы, например, протоколы Ethernet, IP, UDP и др. Название «датаграмма» было выбрано по аналогии со словом телеграмма. Каждая датаграмма содержит в своём заголовке полный адрес места назначения и поэтому является полностью независимой от других датаграмм и в общем случае датаграммы, даже являясь частями одного и того же сообщения, могут быть доставлены получателю различными маршрутами. |

UDP обычно не используется, если требуется надежная передача информации. Использовать UDP имеет смысл там, где потеря части информации не будет критичной для приложения, например, в видеоиграх или потоковой передаче видео. UDP необходим, когда делать повторный запрос сложно или неоправданно по каким-то причинам.

Протоколы L3 не интерпретируют информацию, полученную с верхнего или нижних уровней, они служат только как канал передачи, но есть исключения. RSVP (Resource Reservation Protocol, протокол резервирования сетевых ресурсов) может использоваться, например, роутерами или сетевыми экранами в целях анализа трафика и принятия решений о его передаче или отклонении в зависимости от содержимого.

### Прикладной уровень

В модели TCP/IP отсутствуют дополнительные промежуточные уровни (представления и сеансовый) в отличие от OSI. Функции форматирования и представления данных делегированы библиотекам и программным интерфейсам приложений (API) — своего рода базам знаний. Когда службы или приложения обращаются к библиотеке или API, те в ответ предоставляют набор действий, необходимых для выполнения задачи и полную инструкцию, каким образом эти действия нужно выполнять.

Протоколы прикладного уровня действуют для большинства приложений, они предоставляют услуги пользователю или обмениваются данными с «коллегами» с нижних уровней по уже установленным соединениям. Здесь для большинства приложений созданы свои протоколы, например HTTP для передачи гипертекста по сети, SMTP для передачи почты, FTP для передачи файлов, протокол назначения IP-адресов DHCP и прочие.

### Маска подсети и IP-адреса

Маска подсети помогает маршрутизатору понять, как и куда передавать пакет. Подсетью может являться любая сеть со своими протоколами. Маршрутизатор передает пакет напрямую, если получатель находится в той же подсети, что и отправитель. Если же подсети получателя и отправителя различаются, пакет передается на второй маршрутизатор, со второго на третий и далее по цепочке, пока не достигнет получателя.

**Протокол интернета — IP** (Internet Protocol) используется маршрутизатором, чтобы определить, к какой подсети принадлежит получатель. Свой уникальный IP-адрес есть у каждого сетевого устройства, при этом в глобальной сети не может существовать два устройства с одинаковым IP. Он имеет два подвида, первым был принят IPv4 (IP version 4, версии 4) в 1983 году.

IPv4 предусматривает назначение каждому устройству 32-битного IP-адреса, что ограничивало максимально возможное число уникальных адресов 4 миллиардами (2^32). В более привычном для человека десятичном виде IPv4 выглядит как четыре блока (октета) чисел от 0 до 255, разделенных тремя точками. Первый октет IP-адреса означает его класс, классов всего 4: A, B, C, D.

**Пример.** Рассмотрим IPv4 адрес класса С 223.135.100.7. Первые два октета 223.135 определяют класс, третий — .100 — это номер подсети, а последний означает номер сетевого оборудования. Например, если необходимо отправить информацию с компьютера номер 7 с IPv4 адресом 223.135.100.7 на компьютер номер 10 в той же подсети, то адрес компьютера получателя будет следующий: 223.135.100.10.

В связи с быстрым ростом сети интернет остро вставала необходимость увеличения числа возможных IP-адресов. В 1998 впервые был описан IPv6 (IP version 6, версии 6), который использует 128-битные адреса, и позволяет назначить уникальные адреса для 2^128 устройств. Такого количества IPv6 адресов будет достаточно, чтобы назначить уникальный адрес для каждого атома на планете.

IPv6 имеет вид восьми блоков по четыре шестнадцатеричных значения, а каждый блок разделяется двоеточием. IPv6 выглядит следующим образом:

**2DAB:FFFF:0000:0000:01AA:00FF:DD72:2C4A**

Так как IPv6 адреса длинные, их разрешается сокращать по следующим правилам: ведущие нули допускается опускать, например в адресе выше :00FF: позволяется записывать как :FF:, группы нулей, идущие подряд тоже допустимо сокращать и заменять на двойное двоеточие, наприме:

**2DAB:FFFF::01AA:00FF:DD72:2C4A**

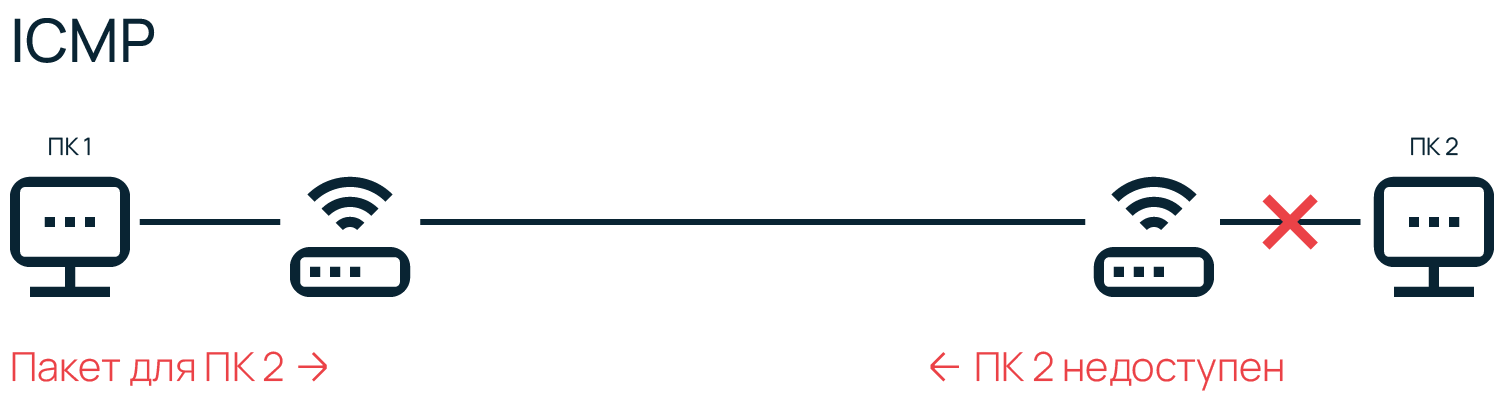
Допускается делать не больше одного подобного сокращения в адресе IPv6.

IP предназначен для определения адресата и доставки ему информации, он предоставляет услугу для вышестоящих уровней, но не гарантирует целостность доставляемой информации.

IP способен инкапсулировать другие протоколы, предоставлять место, куда они могут быть встроены. Как было сказано выше, IP — это 32 бита информации, первые 8 бит в заголовке IP — поля для указания номера инкапсулируемого протокола. Для IPv4 первые 8 бит — поле «протокол», для IPv6 — поле «следующий заголовок». Например, ICMP (межсетевой протокол управляющих сообщений) будет обозначен числом 1, а IGMP (межсетевой протокол группового управления) будет обозначен числом 2.

### ICMP и IGMP

ICMP используется в качестве поддержки маршрутизаторами и другими сетевыми устройствами. Внутри сети он служит для доставки сообщений об ошибках и операционной информации, сообщающей об успехе или ошибке при связи с другим IP. Например, в ситуациях, когда необходимый сервис не может быть запрошен, или когда не был получен ответ от маршрутизатора или хоста.



ICMP никогда не вызывается сетевыми приложениями пользователя, кроме случаев диагностики сети, к примеру, пинг (ping) или traceroute (tracert). ICMP не передает данные, это отличает его от транспортных TCP и UDP, расположенных на L3, которые переносят любые данные. ICMP работает только с IP четвертой версии, с IPv6 взаимодействует ICMPv6.

Сетевые устройства объединяются в группы при помощи IGMP, используемый хостами и роутерами в IPv4 сетях. IGMP организует multicast-передачу информации, что позволяет сетям направлять информацию только хостам, запросившим ее. Это удобно для онлайн-игр или потоковой передаче мультимедиа. IGMP используется только в IPv4 сетях, в сетях IPv6 используется MLD (Multicast Listener Discovery, протокол поиска групповых слушателей), инкапсулированный в ICMPv6.

### Порты, сокеты и DNS

Приложения прикладного уровня, общаются также с предыдущим, транспортным, но они видят его протоколы как «черные ящики». Для приема-передачи информации они могут работать с TCP или UDP, но понимают только конечный адрес в виде IP и порта, а не принцип их работы.

IP присваивается каждому компьютеру межсетевым уровнем, но обмен данными происходит не между компьютерами, а между приложениями, установленными на них. Чтобы получить доступ к тому или иному сетевому приложению недостаточно только IP, для идентификации приложений применяют порты. Комбинация IP-адреса и порта называется **сокетом** или гнездом (**socket**). Поэтому обмен информацией происходит между сокетами. Нередко слово сокет употребляют как синоним для хоста или пользователя, также сокетом называют гнездо подключения процессора.

Из привилегий у приложений на прикладном уровне можно выделить наличие собственных протоколов для обмена данными, а также фиксированный номер порта для обращения к сети. Администрация адресного пространства интернет (IANA), занимающаяся выделением диапазонов IP-адресов, отвечает еще за назначение сетевым приложениям портов.

Так почтовые приложения, которые общаются по SMTP-протоколу, прослушивают порт 25, почта через POP3 приходит на 110-й, по HTTP принимают сообщения веб-сервера — это порт 80, 21-й зарезервирован за FTP. Порт всегда записывается после IP и отделяется от него двоеточием, выглядит это, например, так:

**192.168.1.1:80**

Чтобы не запоминать числовые адреса интернет-серверов была создана DNS — служба доменных имен. DNS всегда слушает на 53 порту и преобразует буквенные имена сетевых доменов в числовые IP-адреса и наоборот. Служба DNS позволяет не запоминать IP — компьютер самостоятельно посылает запрос «какой IP у bmstu.ru?» на 53 порт DNS-сервера, полученного от поставщика услуг интернет.

DNS-сервер дает компьютеру ответ «IP для selectel.ru — XXX.XXX.XXX.XXX». Затем, компьютер устанавливает соединение с веб-сервером полученного IP, который слушает на порту 80 для HTTP-протокола и на порту 443 для HTTPS. В браузере порт не отображается в адресной строке, а используется по умолчанию, но, по сути, полный адрес сайта bmstu выглядит вот так: https://bmstu.ru:443.

Процесс, кодирования данных на прикладном уровне, передача их на транспортном, а затем на межсетевом и, наконец, на канальном уровне называется инкапсуляцией данных. Обратная передача битов информации по иерархии, с канального на прикладной уровни, называют декапсуляцией. Оба процесса осуществляются на компьютерах получателя и отправителя данных попеременно, это позволяет долго не удерживать одну сторону канала занятой, оставляя время на передачу информации другому компьютеру.

### Стек протоколов TCP/IP

О канальном уровне модели TCP/IP мы рассказали меньше всего, давайте вернемся еще раз к началу, чтобы рассмотреть инкапсуляцию протоколов и, что значит «стек».

Большинству пользователей знаком протокол Ethernet. В сети, по стандарту Ethernet, устройства отправителя и адресата имеют определенный MAC-адрес — идентификатор «железа». MAC-адрес инкапсулируется в Ethernet вместе с типом передаваемых данных и самими данными. Фрагмент данных, составленных в соответствии с Ethernet называется фреймом или кадром (frame).

MAC-адрес каждого устройства уникален и двух «железок» с одинаковым адресом не должно существовать, хотя порой такое случается, что приводит к сетевым проблемам. Таким образом, при получении сетевой адаптер занимается извлечением полученной информации из кадра и ее дальнейшей обработкой.

После ознакомления с уровневой структурой модели становится понятно, что информация не может передаваться между двумя компьютерами напрямую. Сначала кадры передаются на межсетевой уровень, где компьютеру отправителя и компьютеру получателя назначается уникальный IP. После чего, на транспортном уровне, информация передается в виде TCP-фреймов либо UDP-датаграмм.

На каждом этапе, подобно снежному кому, к уже имеющейся информации добавляется служебная информация, например, порт на прикладном уровне, необходимый для идентификации сетевого приложения. Добавление служебной информации к основной обеспечивают разные протоколы — сначала Ethernet, поверх него IP, еще выше TCP, над ним порт, означающий приложение с делегированным ему протоколом. Такая вложенность называется стеком, названным TCP/IP по двум главным протоколам модели.

### Point-to-Point протоколы

Point-to-Point (от точки к точке, двухточечный) протокол также известен как PPP. PPP уникален по своим функциям, он применяется для коммуникации между двумя маршрутизаторами без участия хоста или какой-либо сетевой структуры в промежутке. При необходимости, PPP обеспечивает аутентификацию, шифрование, а также сжатие данных. Он широко используется при построении физических сетей, например, кабельных телефонных, сотовых телефонных, сетей по кабелю последовательной передачи и транк-линий (когда один маршрутизатор подключают к другому для увеличения размера сети).

У PPP есть два подвида — PPPoE (PPP по Ethernet) и PPPoA (PPP через асинхронный способ передачи данных — ATM), интернет-провайдеры часто их используют для DSL соединений.

PPP и его старший аналог SLIP (протокол последовательной межсетевой связи) формально относятся к межсетевому уровню TCP/IP, но в силу особого принципа работы, иногда выделяются в отдельную категорию. Преимущество PPP в том, что для установки соединения не требуется сетевая инфраструктура, а необходимость маршрутизаторов отпадает. Эти факторы обуславливают специфику использования PPP протоколов.

## Лекция II.2. Информационные службы IP-сетей. Основы web-технологии

### HTML/XHTML и CSS

Web-страницы – это файлы в формате «неформатированный текст» (plain text, текст в ASCII-кодах), распознаваемые любой операционной системой. Поэтому такой файл может быть отравлен практически на любой компьютер, подключенный к Интернет. Кроме того, для создания web-страницы достаточно иметь самый простой текстовый редактор, например, стандартное приложение Windows Блокнот (Notepad).

Файлы web-страниц имеют расширения htm, html или другие, если при их создании были использованы специальные серверные технологии (например, shtml, asp, php). Тип HTML-файлов происходит от названия языка создания web-страниц HTML (HyperText Markup Language – язык разметки гипертекста). Поэтому web-страницы часто называют HTMLдокументами.

HTML-документ содержит текст и команды языка HTML, которые называют дескрипторами разметки или тегами (tag). Теги языка HTML определяют:

• внешний вид документа (формат шрифта, цвет фона и т. д.);

• структуру документа: взаимное расположение текстовой, графической и другой мультимедийной информации;

• ссылки на другие интернет-ресурсы.

HTML позволяет формировать на странице сайта текстовые блоки, включать в них изображения, организовывать таблицы, управлять отображением цвета документа и задавать форматирование текста, добавлять звуковое сопровождение, организовывать гиперссылки для перехода в другие разделы сайта к иным Интернет-ресурсам, а также задавать взаимное расположение текстовых блоков и других компонент страницы.

Встраиваемые в web-страницу с помощью тегов медийные объекты (графика, видео и т. д.) хранятся в отдельных файлах соответствующих типов.

Любой web-браузер содержит интерпретатор языка HTML, что позволяет ему корректно отображать web-страницу вместе со всем ее содержимым на экране. Все сказанное относится и к XHTML – более поздней модификации языка HTML.

С развитием web-технологий разработчики web-страниц стали придерживаться принципа разделения описания логической структуры web-страницы (которое производится с помощью языков разметки HTML/XHTML) и описания внешнего вида этой web-страницы. Для некоторых вариантов HTML/XHTML соблюдение данного принципа является обязательным. Такой подход позволяет отделить содержимое HTML документа от дизайна и верстки.

Для описания внешнего вида элементов web-страницы на экране браузера стали использовать технологию стилевого оформления webстраниц – таблицы каскадных стилей CSS (Cascading Style Sheets).

Таблицы каскадных стилей CSS – это простая технология определения и присоединения стилей оформления к документам HTML. Стиль оформления – это все то, что определяет внешний вид документа: цвета, шрифты, рамки и границы, отступы, другое оформление и выравнивание текста, расположения отдельных блоков, обтекание и т.д.

Стиль определяется набором правил отображения тегов, задаваемых таблицей стилей. Таблица стилей – это шаблон, который управляет форматированием тегов HTML в web-документе.

Возможности оформления, предоставляемые технологией CSS, гораздо богаче стандартных средств форматирования языка HTML/XHTML.

Важно, что стиль можно определить сразу для группы элементов web-страницы; стиль можно сохранить отдельно от страницы и применить сразу к нескольким страницам, задав, таким образом, для них единое оформление. Кроме того, не представляет труда сменить внешний стиль web-страницы или применить к одной и той же странице несколько стилей. Все это значительно повышает гибкость определения и модификации дизайна страницы.

### Использование JavaScript

Язык сценариев JavaScript предназначен для создания интерактивных web-страниц и web-приложений, позволяющих полностью управлять как самими web-страницами, так и браузерами, в которых эти страницы открыты. Это объектно-ориентированный язык программирования, имеющий схожий с языком Си синтаксис.

Языком JavaScript не владеет какая-либо компания или организация, что отличает его от ряда языков программирования, используемых в web-программировании. Первоначально язык предназначался как для программирования на стороне клиента, так и для программирования на стороне сервера.

Приложения, написанные на JavaScript, могут исполняться на серверах, использующих Java 6 и более поздних версий. Это используется для построения серверных приложений, позволяющих обрабатывать сценарии JavaScript на стороне сервера. Помимо Java 6, существует ряд платформ, использующих существующие движки (интерпретаторы) JavaScript для исполнения серверных приложений. Однако чаще сценарии JavaScript предназначены для исполнения в среде браузера на стороне клиента.

Поскольку в начале развития скриптового языка для браузеров существовали несколько аналогов от разных компаний-разработчиков, ассоциацией ECMA была проведена стандартизация языка JavaScript. Стандартизированная версия имеет название ECMAScript и описывается стандартом ECMA-262 [28].

ECMAScript не является браузерным языком и в нём не определяются методы ввода и вывода информации. Это скорее основа для построения скриптовых языков. Спецификация ECMAScript описывает типы данных, инструкции, ключевые и зарезервированные слова, операторы, объекты, регулярные выражения, не ограничивая авторов производных языков в расширении их новыми составляющими.

Структурно JavaScript можно представить в виде объединения трёх частей:

• ядро (ECMAScript);

• объектная модель браузера (Browser Object Model или BOM);

• объектная модель документа (Document Object Model или DOM).

Если рассматривать JavaScript в отличных от браузера окружениях, то объектная модель браузера и объектная модель документа могут не поддерживаться. Язык JavaScript применятся не только в Интернете, но и в таких программах, как, например, Adobe Acrobat Reader или Adobe Photoshop для расширения их возможностей, аналогично использованию языка VBA (Visual Basic for Applications) в Microsoft Office.

Однако чаще всего JavaScript все же используется как язык, встраиваемый в web-страницы для программного доступа к их элементам. Сценарии JavaScript являются основой клиентской части web-приложений.

Они загружаются с сервера вместе с web-страницами и выполняются браузером на компьютере пользователя. Сценарии JavaScript обрабатываются встроенным в браузер интерпретатором.

JavaScript широко применяется для решения таких задач, как проверка информации, введенной пользователем в форму, перед ее отправкой на сервер и программирование ответных реакций на действия пользователя. Считается, что язык JavaScript занял лидирующую позицию в разработке клиентских web-приложений в связи с развитием AJAX, поскольку браузер стал превалирующей системой доставки приложений.

Следует, однако, помнить об ограничениях языка. Так, в JavaScript отсутствует интерфейс программирования приложений по работе с файловой системой, управлению потоками ввода/вывода, нет базовых типов для бинарных данных, отсутствуют стандартные интерфейсы к web-серверам и базам данных. Кроме того, клиентские скрипты могут быть отключены пользователем в настройках браузера.

Сценарии могут встраиваться в HTML-документ тремя стандартными способами:

• с помощью тега script;

• с помощью обработчика события;

• в виде гиперссылки.

Сценарий JavaScript может быть помещен в любом месте webстраницы внутри контейнера script. Если во время интерпретации HTMLдокумента браузер встретит тег script, он первым делом выполнит код скрипта и лишь затем продолжит интерпретацию страницы дальше. Контейнеров script в одном документе может быть сколько угодно.

Обычно скрипты JavaScript стараются отделить от собственно HTML/XHTML-документа, с этой целью тег script помещают в головную часть head, а в теле страницы по возможности оставляется чистая верстка.

Сценарии могут содержаться как внутри web-страницы, так и храниться в отдельном файле. Файл скриптов – обычный текстовый файл, имеющий расширение js. Подключение внешнего файла скриптов производится с помощью параметра src тега script, значением которого является URL или относительный адрес файла со сценарием.

Использование отдельных файлов для хранения кода сценариев JavaScript очень удобно, так как позволяет создавать, например, собственные библиотеки функций и объектов, используемые многократно и подключаемые при необходимости к разным страницам.

Подключение внешних файлов со сценариями, объявления функций и всех глобальных переменных обычно помещают внутри тега head, то есть в заголовке страниц.

Обычно выполнение сценария привязано к какому-либо событию и служит для его обработки. В качестве событий выступают любые действия пользователя, например, щелчок мыши (сlick), перемещение курсора мыши относительно элемента страницы: наведение указателя на элемент (mouseover), перемещение указателя за пределы элемента (mouseout), изменение значения поля формы (change), нажатие пользователем кнопки отправки данных формы (submit) или внутренние события браузера, например, загрузка страницы (load).

Строго говоря, существуют:

• DOM-события, которые инициируются элементами страницы (click,

mouseover и т.п.);

• События окна браузера (например, resize – изменение размера окна);

• Другие события (например, load, readystatechange – используется в

технологии AJAX).

Любое событие может быть перехвачено и обработано процедурой сценария. Для перехвата события в теги некоторых элементов страницы вводятся параметры обработки события. Имя параметра обработки начинается с приставки on, за которой следует название обрабатываемого события (например, onclick). В качестве значения параметра обработки указывается действие, которое необходимо выполнить.

Определение функции состоит:

• из имени функции, предваренного ключевым словом function. Имена

(идентификаторы) JavaScript должны начинаться с латинской буквы

и могут содержать буквы латинского алфавита, цифры и знак подчеркивания. Идентификаторы чувствительны к регистру символов;

• из списка формальных параметров, заключённых в скобки и разделяемых запятыми. Если функция не имеет параметров, ее имя указываются с пустыми скобками;

• из последовательности операторов JavaScript, составляющих содержание функции, заключённых в фигурные скобки { }. Операторы функции могут содержать вызовы других функций, определённых в текущем приложении.

Вызов функции производится с помощью обработчика событий или в гиперссылке с указанием ее фактических параметров.

Функции отличаются от процедур тем, что в результате выполнения

функции возвращается некоторое значение. В этом случае значение или

содержащее его имя переменной указывается в коде процедуры с ключевым словом return. Функции могут указываться в выражениях и в операции присваивания. Вызов функции в коде web-страницы предваряется словом return. Далее будут приведены примеры использования функций для проверки и управления отправкой данных формы

## Семинар II.1. Протоколы транспортного уровня TCP и UDP

## Семинар II.2. Служба управления сетью. DHCP, DNS, DDNS

# Модуль III. Безопасность компьютерных сетей

## Лекция III.1. Основные понятия и принципы ИБ

Прежде чем говорить об обеспечении безопасности персональных данных, необходимо определить, что же такое информационная безопасность. Термин «информационная безопасность» может иметь различный смысл и трактовку в зависимости от контекста. В данном курсе под информационной безопасностью мы будем понимать защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений, в том числе владельцам и пользователям информации и поддерживающей инфраструктуры.

### ГОСТ «Защита информации»

Основные термины и определения" вводит понятие информационной безопасности как состояние защищенности информации, при котором обеспечены ее конфиденциальность, доступность и целостность.

**Конфиденциальность** – состояние информации, при котором доступ к ней осуществляют только субъекты, имеющие на него право.

**Целостность** – состояние информации, при котором отсутствует любое ее изменение либо изменение осуществляется только преднамеренно субъектами, имеющими на него право;

**Доступность** – состояние информации, при котором субъекты, имеющие право доступа, могут реализовывать его беспрепятственно.

**Угрозы информационной безопасности** – совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации.

**Атакой** называется попытка реализации угрозы, а тот, кто предпринимает такую попытку, - злоумышленником. Потенциальные злоумышленники называются источниками угрозы.

Угроза является следствием наличия уязвимых мест или уязвимостей в информационной системе. Уязвимости могут возникать по разным причинам, например, в результате непреднамеренных ошибок программистов при написании программ.

### Классификация угроз и атак

Угрозы можно классифицировать по нескольким критериям:

* по свойствам информации (доступность, целостность, конфиденциальность), против которых угрозы направлены в первую очередь;
* по компонентам информационных систем, на которые угрозы нацелены (данные, программы, аппаратура, поддерживающая инфраструктура);
* по способу осуществления (случайные/преднамеренные, действия природного/техногенного характера);
* по расположению источника угроз (внутри/вне рассматриваемой ИС).

Обеспечение информационной безопасности является сложной задачей, для решения которой требуется комплексный подход. Выделяют следующие уровни защиты информации:

* законодательный – законы, нормативные акты и прочие документы РФ и международного сообщества;
* административный – комплекс мер, предпринимаемых локально руководством организации;
* процедурный уровень – меры безопасности, реализуемые людьми;
* программно-технический уровень – непосредственно средства защиты информации.

Законодательный уровень является основой для построения системы защиты информации, так как дает базовые понятия предметной области и определяет меру наказания для потенциальных злоумышленников. Этот уровень играет координирующую и направляющую роли и помогает поддерживать в обществе негативное (и карательное) отношение к людям, нарушающим информационную безопасность.

### ФЗ «Об информации, ИТ и о защите информации»

В российском законодательстве базовым законом в области защиты информации является ФЗ "Об информации, информационных технологиях и о защите информации" от 27 июля 2006 года номер 149-ФЗ. Поэтому основные понятия и решения, закрепленные в законе, требуют пристального рассмотрения.

Закон регулирует отношения, возникающие при:

* осуществлении права на поиск, получение, передачу, производство и распространение информации;
* применении информационных технологий;
* обеспечении защиты информации.

Закон дает основные определения в области защиты информации. Приведем некоторые из них:

* информация – сведения (сообщения, данные) независимо от формы их представления;
* информационные технологии – процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов;
* информационная система - совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств;
* обладатель информации - лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам;
* оператор информационной системы - гражданин или юридическое лицо, осуществляющие деятельность по эксплуатации информационной системы, в том числе по обработке информации, содержащейся в ее базах данных.
* конфиденциальность информации - обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя [4].

В статье 3 Закона сформулированы принципы правового регулирования отношений в сфере информации, информационных технологий и защиты информации:

* свобода поиска, получения, передачи, производства и распространения информации любым законным способом;
* установление ограничений доступа к информации только федеральными законами;
* открытость информации о деятельности государственных органов и органов местного самоуправления и свободный доступ к такой информации, кроме случаев, установленных федеральными законами;
* равноправие языков народов Российской Федерации при создании информационных систем и их эксплуатации;
* обеспечение безопасности Российской Федерации при создании информационных систем, их эксплуатации и защите содержащейся в них информации;
* достоверность информации и своевременность ее предоставления;
* неприкосновенность частной жизни, недопустимость сбора, хранения, использования и распространения информации о частной жизни лица без его согласия;
* недопустимость установления нормативными правовыми актами каких-либо преимуществ применения одних информационных технологий перед другими, если только обязательность применения определенных информационных технологий для создания и эксплуатации государственных информационных систем не установлена федеральными законами.

Вся информация делится на общедоступную и ограниченного доступа. К общедоступной информации относятся общеизвестные сведения и иная информация, доступ к которой не ограничен. В законе, определяется информация, к которой нельзя ограничить доступ, например, информация об окружающей среде или деятельности государственных органов. Оговаривается также, что ограничение доступа к информации устанавливается федеральными законами в целях защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства. Обязательным является соблюдение конфиденциальности информации, доступ к которой ограничен федеральными законами.

Запрещается требовать от гражданина (физического лица) предоставления информации о его частной жизни, в том числе информации, составляющей личную или семейную тайну, и получать такую информацию помимо воли гражданина (физического лица), если иное не предусмотрено федеральными законами.

Закон выделяет 4 категории информации в зависимости от порядка ее предоставления или распространения:

* информацию, свободно распространяемую;
* информацию, предоставляемую по соглашению лиц, участвующих в соответствующих отношениях;
* информацию, которая в соответствии с федеральными законами подлежит предоставлению или распространению;
* информацию, распространение которой в Российской Федерации ограничивается или запрещается.

Закон устанавливает равнозначность электронного сообщения, подписанного электронной цифровой подписью или иным аналогом собственноручной подписи, и документа, подписанного собственноручно.

Дается следующее **определение защите информации** – представляет собой принятие правовых, организационных и технических мер, направленных на:

* обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации;
* соблюдение конфиденциальности информации ограниченного доступа;
* реализацию права на доступ к информации.

Обладатель информации, оператор информационной системы в случаях, установленных законодательством Российской Федерации, **обязаны обеспечить**:

* предотвращение несанкционированного доступа к информации и (или) передачи ее лицам, не имеющим права на доступ к информации;
* своевременное обнаружение фактов несанкционированного доступа к информации;
* предупреждение возможности неблагоприятных последствий нарушения порядка доступа к информации;
* недопущение воздействия на технические средства обработки информации, в результате которого нарушается их функционирование;
* возможность незамедлительного восстановления информации, модифицированной или уничтоженной вследствие несанкционированного доступа к ней;
* постоянный контроль за обеспечением уровня защищенности информации.

Таким образом, ФЗ «Об информации, информационных технологиях и о защите информации» создает правовую основу информационного обмена в РФ и определяет права и обязанности его субъектов.

### Персональные данные

Необходимость обеспечения безопасности персональных данных в наше время - объективная реальность. Современный человек не может самостоятельно противодействовать посягательству на его частную жизнь. Возросшие технические возможности по сбору и обработке персональной информации, развитие средств электронной коммерции и социальных сетей делают необходимым принятие мер по защите персональных данных.

Рассмотрим несколько примеров из повседневной жизни, когда нарушаются права человека на конфиденциальность персональных данных. Бывает так, что при оформлении дисконтной карты в магазине покупатель указывает следующие сведения: фамилию, номер телефона, электронный адрес, а затем получает сообщения и письма совершенно из других магазинов, в которых даже никогда не бывал. То есть магазин без согласия покупателя передал его данные третьим лицам. Если газета печатает ФИО и суммы выигрыша победителей лотереи без их ведома, или ТСЖ вывешивает на подъезде списки должников и сумму их долга - это примеры "безобидных " утечек. Кража персональных данных может нанести правообладателю ощутимый материальный ущерб, если речь идет о кредитных картах или информации о сбережениях в банке. Злоумышленники, обладающие достаточными техническими знаниями, похищают реквизиты банковских карт (скиминг) или имитируют сайты финансовых учреждений, чтобы заставить пользователя показать свою личную информацию (фишинг). На самом деле зачастую даже трудно установить источник утечки персональных данных вследствие высокой информатизации современного общества.

Государство на законодательном уровне требует от организаций и физических лиц, обрабатывающих персональные данные, обеспечить их защиту. Законодательство Российской Федерации в области защиты персональных данных основывается на Конституции РФ, международных договорах Российской Федерации, Федеральном законе РФ от 27 июля 2006 г. N 152-ФЗ «О персональных данных», Федеральном законе от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» и других определяющих случаи и особенности обработки персональных данных федеральных законов.

Целью российского законодательства в области защиты персональных данных является обеспечение защиты прав и свобод гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну. Законодательством регулируются отношения, связанные с обработкой персональных данных, осуществляемой государственными органами власти, органами местного самоуправления, юридическими лицами и физическими лицами.

Основополагающим законом в области защиты персональных данных является Федеральный закон "О персональных данных" №152, который был принят Государственной думой 8 июля 2006 года и вступил в силу с 26 января 2007 года. Закон определяет:

* основные понятия, связанные с обработкой персональных данных;
* принципы и условия обработки персональных данных;
* обязанности оператора персональных данных;
* права субъекта персональных данных;
* виды ответственности за нарушение требований ФЗ-№152;
* государственные органы, осуществляющие контроль за соблюдением требований ФЗ-№152.

В соответствии с Законом персональные данные - любая информация, с помощью которой можно однозначно идентифицировать физическое лицо (субъект ПД). К персональным данным, в связи с этим могут относиться фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация, принадлежащая субъекту ПД.

Операторами персональных данных являются государственный орган, муниципальный орган, юридическое или физическое лицо, организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели и содержание обработки персональных данных.

**Обработка персональных данных** – действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных.

**Информационная система персональных данных** (далее ИСПД) – информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств [7].

**Регуляторами** называются органы государственной власти, уполномоченные осуществлять мероприятия по контролю и надзору в отношении соблюдения требований федерального закона. В ФЗ "О персональных данных" установлены три регулятора:

* Роскомнадзор (защита прав субъектов персональных данных)
* ФСБ (требования в области криптографии)
* ФСТЭК России (требования по защите информации от несанкционированного доступа и утечки по техническим каналам).

Так как ФЗ «О персональных данных» является лишь основой правового обеспечения защиты ПД, его требования в дальнейшем были конкретизированы в актах Правительства РФ и Министерства связи, нормативно-методических документах регуляторов.

## Семинар III.1. Технологии безопасности на основе анализа трафика

### Система анализа сетевого трафика нового поколения (NDR)

Класс решений NDR (Network Detection & Response) был сформирован совсем недавно исследовательским центром Gartner. Решения NDR включают в себя следующие технологии:

* анализ сетевого трафика;
* поведенческая аналитика (машинное обучение для оперативного обнаружения, расследования и реагирования на угрозы).

По сути, NDR включает в себя технологии NTA, плюс добавляются исторические метаданные для расследования и поиска угроз, а также автоматического реагирования на угрозы посредством интеграции с различными средствами управления ИТ и ИБ (межсетевые экраны, средства управления доступом к сети и т.п.).

NDR решения обеспечивают полную видимость в сети с обнаружением угроз в режиме реального времени, а интеграция с продуктами EDR и SIEM обеспечивает дополнительную более точную корреляцию данных для выявления инцидентов.

### Системы учета и обработки компьютерных угроз (Threat Intelligence)

Решения класса Threat Intelligence позволяют проводить развернутую аналитику по уязвимостям и угрозам в ИТ-инфраструктуре. Анализ проводится на основе информации об угрозе или по Threat Intelligence Feeds (TIF).

В настоящее время существует достаточное количество открытых источников фидов, на которые можно подписаться. Фиды – это данные, содержащие в себе индикаторы компрометации IoC, то есть признаки, по которым можно распознать потенциальную угрозу. В фидах содержатся хэши вредоносных файлов, IP-адреса и домены, связанные с вредоносной активностью. К примеру, компания может использовать данные фидов для блокировки запросов с подозрительных IP-адресов. Но у фидов есть несомненный минус – отсутствие контекста потока данных, то есть в фидах есть индикаторы, но нет указания по поводу связей этих индикаторов с конкретными атаками, вредоносным файлам и т.д. Для получения данной информации необходимо проводить подробный анализ связей между данными. Процесс требует весомых трудозатрат, так как в большинстве случаев проделывается вручную. В таких ситуациях специалисту на помощь приходят TI-платформы (Threat Intelligence Platform).

**Threat Intelligence Platform** – специализированная платформа, предназначенная для обогащения, обнаружения, распространения и корреляции данных об угрозах. Данный класс решений позволяет в автоматическом режиме связывать фиды, дополнять их контекстной информацией, что позволяет получить максимальную пользу от IoC. Неоспоримым плюсом TI-платформ является возможность подключения и централизованной обработки любых доступных вам источников информации по угрозам, а также интеграция ее с другими инструментами в области кибербезопасности, например, с SIEM системами, платформами реагирования на инциденты или средствами защиты.

На практике такие решения помогают аналитикам находить следы компрометации в сети и системах за счет использования определенных признаков. К примеру, NTA-решение зафиксировало нелегитимный трафик (допустим SYN-flood - одна из разновидностей сетевых атак типа отказ в обслуживании, которая заключается в отправке большого количества запросов на подключение по протоколу TCP в достаточно короткий срок), далее отправило в SIEM отчет о том, что с конкретного IP-адреса зафиксирован SYN-flood. SIEM система проанализировала данные и сформировала инцидент с входным параметром «IP-адрес» и вердикт – SYN-flood. Далее SIEM направляет данную информацию на обогащение в TI-платформу. Платформа начинает проверять свою базу данных на предмет похожих dns-записей. Если в наборе индикаторов компрометации обнаруживаются еще с десяток IP-адресов, то данные адреса проверяются и возвращаются уже аналитику. Аналитик передает информацию администраторам ИТ-инфраструктуры, а они в свою очередь вносят изменения в настройки на маршрутизаторе или межсетевом экране, тем самым заранее заблокировав потенциальные нелегитимные подключения.

### Поиск угроз (Threat hunting)

Процесс Threat hunting или «охота на угрозы» основывается на проактивном поиске следов компрометации или признаков ВПО с целью обнаружения и ликвидации угрозы. То есть поиск угроз происходит не после сработки средства обнаружения или защиты, а в процессе работы аналитика. Аналитик по сути проверяет разные гипотезы, по результатам которых можно обнаружить следы взлома. Основная цель - найти угрозу раньше, чем ею успеют воспользоваться злоумышленники. Для проведения успешной «охоты на угрозы», аналитикам крайне важно получать телеметрию в реальном времени, в этом им помогают описанные выше SIEM/EDR/NDR системы.

Основные составляющие процесса threat hunting:

1. Сбор данных:

* информация от конечных устройств (процессы, запущенные на устройстве; файлы, хранимые на дисках);
* данные сети (сетевые соединения, работа DNS-серверов, маршрутизаторов, коммутаторов и т.д.);
* информация по сработкам из SIEM, NTA/NDR, данные из TI-платформы (это могут быть внешние базы фидов, либо собственная база, накапливаемая по результатам работы центра реагирования), также данные об ИТ-инфраструктуре организации (конфигурации, используемое ПО, уязвимости и т.п.).

1. Аналитика – начиная со сбора статистики, заканчивая поведенческим анализом, на основе машинного обучения (User and Entity Behavioral Analytics, UEBA).
2. Исследование полученных данных.
3. Нейтрализация атаки и разработка сценария реагирования на такого рода атаки.

Проработка гипотез осуществляется за счет опыта специалистов центра реагирования, а также за счет получаемой информации из различных источников, указанных выше.

Важным элементов для поиска угроз является собственная база знаний центра реагирования, которая будет накапливать данные по расследованиям и результатов проверки предыдущих гипотез.

### Средства поведенческого анализа («песочницы»)

Средство поведенческого анализа («песочницы») — изолированная среда для безопасного запуска исполняемых файлов. Доступ к сети, а также считывание информации с устройств ввода обычно либо частично эмулируют, либо ограничивают.

Песочницы используют для анализа файлов на предмет наличия ВПО или, например, для запуска подозрительного кода. Образ песочницы моделирует среду, в которой предполагалось запускать проверяемый объект, это помогает экспертам оперативно проводить поведенческий анализ, что позволяет своевременно выявлять потенциальные угрозы.

Технология поведенческого анализа файлов существует на рынке уже достаточно давно. На данный момент совершенствование применяемых методов осуществляется за счет интеграции с другими классами решений по обнаружению и защите для более комплексного анализа, а также за счет появления более гибкой настраиваемой среды.

На практике данный класс довольно распространен. Основное применение «песочницы» — это поведенческий анализ подозрительных файлов в окружении, максимально точно имитирующем «боевую» ИТ-инфраструктуру.

### Приманки для хакеров («Honeypot»)

Класс решений «Honeypot» предназначен для обнаружения попыток взлома и изучения применяемых методов для прогнозирования атак и принятия мер противодействия. В качестве «приманки» используются изолированные от промышленных систем среды со специально открытыми портами, уязвимостями и другими явными недостатками. В качестве целевых объектов может использоваться веб-сервер, виртуальная машина, сетевое устройство и другие системы и сервисы. Обычно это системы, которые есть в эксплуатации у организации. Внутри среды, предназначенной для выявления атакующих, могут размещаться различные ресурсы, замаскированные под важные файлы, почтовые сообщения, данные учетных записей с целью вызвать интерес у киберпреступников.

Кроме того, для борьбы с фишингом применяются так называемые ханипот-ссылки, встроенные в код веб-сайта, что позволяет выявлять случаи клонирования веб-сайта, заранее предупреждая защищающихся о возможной атаке.

Технология продолжает развиваться и появляются различные инструменты для раскрытия не только применяемых методов, но и действий злоумышленников после их подключения уже к своим системам, например, путем записи в терминальном окне. Это позволяет больше узнать о самих атакующих и проследить к каким еще системам они подключаются.

Для того чтобы поймать более продвинутых злоумышленников, разворачивают ханипоты нового поколения, которые могут виртуализовать целые сети.

### Развитие технологий обнаружения компьютерных атак в России

Технологии выявления компьютерных атак, как правило, перенимались в России от зарубежных производителей, но в последнее время российские разработчики стали активно развивать свои продуктовые направления и инвестировать в новые технологии. На рынок выпускается все больше различных решений, призванных качественно и эффективно решать задачи по безопасности, появляются полностью отечественные стеки решений, от аппаратного обеспечения до приложений. Этому способствует то, что для развития отечественного ИТ-потенциала в России принимаются различные меры на государственном уровне. С целью преодоления зависимости от зарубежных технологий в 2014 году руководством страны был взят курс на усиление политики импортозамещения, в том числе в сфере информационных технологий.

Основным драйвером развития ИТ-отрасли является госрегулирование, например, инициатива правительства по внедрению отечественного ПО в органах государственной власти и госкорпорациях.

Для обеспечения контроля Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации формирует Единый реестр российских программ для электронных вычислительных машин и баз данных. На текущий момент в реестре зарегистрировано более 6000 наименований отечественного программного и аппаратного обеспечения, более 450 из которых относятся к средствам обеспечения ИБ.

Программа по импортозамещению в России дает возможность отечественным производителям наверстать технологических разрыв, который образовался с зарубежными производителями.

Кроме того, вводятся дополнительные меры поддержки ИТ-компаний в виде налоговых послаблений. Это позволит создать более благоприятные условия для работы в России и даст дополнительные возможности для инвестирования в технологии. Так называемый «налоговый маневр» позволит начинающим ИТ-компаниям и стартапам быстрее разрабатывать новые технологии и выводить на рынок, тем самым повышать конкурентный уровень. Конкуренция играет важную роль для обеспечения роста качества выпускаемых программных решений.

Стоит также учитывать непростую обстановку в мире. Так как очень много чувствительной информации находится в «цифре», большой объем государственной деятельности теперь осуществляется в различных ИТ-системах и приложениях, на фоне этого различные государства разворачивают большие кампании друг против друга в киберпространстве. С целью проведения кибершпионажа или нарушения функционирования информационных систем могут быть использованы программные закладки, которые могут поставляться с программными и аппаратными средствами. Именно поэтому для наиболее критических информационных инфраструктур необходимо применять отечественные разработки, которые должны соответствовать не только формальным критериям, но быть эффективными, современными, технологичными и, самое главное, безопасными.

Одним из способов контроля отсутствия программных и аппаратных закладок (недекларированные возможности ПО) является проведение сертификации.

Сертификация – это независимая оценка (экспертиза) программного или аппаратного обеспечения на предмет соответствия установленным критериям. Обязательная сертификация регламентируется законодательством, и существует несколько систем, например, системы сертификации ФСТЭК России, ФСБ России и Министерства обороны Российской Федерации.

В рамках проведения сертификационных испытаний проверяется программное или аппаратное обеспечение на общеизвестные уязвимости, в том числе на предмет аппаратных, программных и алгоритмических закладок.

Аппаратная закладка – это модуль, скрытно внедренный в электронную схему устройства, или же отдельная плата, микросхема, подключенная к атакуемой системе. Программная закладка – это программное обеспечение, скрытно внедренное в защищенную систему, либо намеренно измененный фрагмент кода программы. Это позволяет получить удаленный доступ либо запустить сбор данных. Закладки данного типа потенциально могут быть внедрены путем планового обновления ПО. Алгоритмические закладки – это преднамеренное скрытое искажение части алгоритма программы, в результате которого возможно появление у программного компонента функций, не предусмотренных спецификацией.

Разработчики средств при этом должны представлять исходные коды своих решений для анализа и для некоторых зарубежных компаний это является невыполнимым условием.

Именно из-за наличия рисков, связанных с нарушением функционирования критических для государства информационных инфраструктур, применяется сертифицированные средства мониторинга и защиты.

# Лабораторные работы

## ЛР1. Создание модели локальной сети

## ЛР2. Исследование кабеля «Витая пара»

## ЛР3. Структуризация локальных вычислительных сетей с помощью коммутаторов

## ЛР4. Тестирование работы сети