

1. История возникновения сетей.	2
2. Классификация сетей. Топологии.	4
3. Понятия «протокол», «интерфейс» и «сервис». Примеры.....	6
4. Понятия «стек протоколов» и «инкапсуляция».....	8
5. Модель взаимодействия открытых систем ISO/OSI.....	9
6. Стек протоколов TCP/IP.	11
7. Стеки сетевых протоколов (обзор).	13
8. Физический уровень.	15
9. Понятие «разделяемая среда». Соединение точка-точка.....	20
10. Канальный уровень.....	22
11. Классический Ethernet. Концентратор. Метод доступа к среде CSMA/CD.	23
12. Коммутируемый Ethernet. Использование коммутаторов. Алгоритм обратного обучения. Алгоритм прозрачного моста.....	28
13. Wi-Fi. Метод доступа к среде CSMA/CA.	31
14. Технологии канального уровня (обзор).	37
15. Сетевой уровень. Понятие «маршрутизация». Согласование различий в сетях.....	47
16. IP-адреса и IP-сети.....	50
17. Разрешение IP-адреса в MAC-адрес.....	53
18. Протокол IPv4.	55
19. Протокол IPv6.	58
20. Протокол ICMP. Назначение и варианты использования.....	63
21. Транспортный уровень. Адресация на транспортном уровне.	65
22. Протокол UDP.	67
23. Протокол TCP. Гарантированная доставка данных. Процесс установки соединения.....	69
24. Протокол TCP. Управление скоростью передачи данных. Скользящее окно, окно управления потокм, окно перегрузки.	72
25. Протокол TCP. Управление скоростью передачи данных. Медленный старт. AIMD.	74
26. Динамическое конфигурирование хостов. Протокол DHCP.....	75
27. Сетевые устройства.	77
28. Преобразование сетевых адресов (NAT).	79

1. История возникновения сетей.

Компьютерная сеть - набор автономных компьютеров, связанных одной технологией (способных обмениваться информацией). Другое название – сеть передачи данных.

Компьютерные сети: логический результат эволюции двух важнейших научно-технических отраслей— компьютерных и телекоммуникационных технологий.

1) Сети представляют собой частный случай распределенных вычислительных систем, в которых группа компьютеров согласованно решает набор взаимосвязанных задач, обмениваясь данными в автоматическом режиме. 2) Компьютерные сети могут рассматриваться как средство передачи информации на большие расстояния, для чего в них применяются методы кодирования и мультиплексирования данных, получившие развитие в различных телекоммуникационных системах.

История развития сетей

50-е – мейнфреймы (мощные и надежные компьютеры универсального назначения)

- 1) громоздкие, дорогие, малое число пользователей, занимали целые здания;
- 2) не были предназначены для интерактивной работы пользователя, применялись в режиме пакетной обработки.
- 3) Системы пакетной обработки, как правило, строились на базе мейнфрейма. Пользователи подготавливали перфокарты, содержащие данные и команды программ, и передавали их в вычислительный центр. Операторы вводили эти карты в компьютер, а распечатанные результаты пользователи получали обычно только на следующий день. Таким образом, одна неверно набитая карта означала как минимум суточную задержку.
- 4) Пренебрежение интересами пользователя (неудобно, долго). Во главу угла ставилась эффективность работы самого дорогого устройства вычислительной машины — процессора, даже в ущерб эффективности работы использующих его специалистов.

Начало 60-х – многотерминальные системы

- 1) Учили интересы пользователей (каждый пользователь получал собственный терминал, с помощью которого он мог вести диалог с компьютером.)
- 2) Терминалы, выйдя за пределы вычислительного центра, рассредоточились по всему предприятию. И хотя вычислительная мощность оставалась полностью централизованной, некоторые функции, такие как ввод и вывод данных, стали распределенными.
- 3) Подобные многотерминальные централизованные системы внешне уже были очень похожи на локальные вычислительные сети. Пользователь мог получить доступ к общим файлам и периферийным устройствам, при этом у него поддерживалась полная иллюзия единоличного владения компьютером, так как он мог запустить нужную ему программу в любой момент и почти сразу же получить результат.
- 4) потребность в создании локальных сетей в это время еще не созрела (производительность компьютера была пропорциональна квадрату его стоимости, отсюда следовало, что за одну и ту же сумму было выгоднее купить одну мощную машину, чем две менее мощных — их суммарная мощность оказывалась намного ниже мощности дорогой машины)

Конец 60-х – первые глобальные сети

- 1) потребность в соединении компьютеров, находящихся на большом расстоянии друг от друга
- 2) реализация механизмов **терминал-компьютер** (терминалы соединялись с компьютерами через телефонные сети с помощью модемов) и **компьютер-**

компьютер (реализованы службы обмена файлами, синхронизации баз данных, электронной почты и другие ставшие теперь традиционными сетевые службы)

3) многое унаследовали от телефонных сетей

Основные идеи:

- отказ от коммутации каналов
- реализация механизма коммутации пакетов

Коммутация каналов – перед передачей данных устанавливается канал связи, по которому передаются все данные

Коммутация пакетов – данные разбиваются на части (пакеты) и передаются по мере готовности

4) 1969 – создание ARPANET (сеть, объединяющая в единую базу суперкомпьютеры оборонных и научных центров)

Идеи:

- Объединяла разные компьютеры с разными ОС
- ОС таких компьютеров – первые сетевые ОС (позволяли рассредоточить пользователей, организовать распределенное хранение и обработку данных между несколькими компьютерами, связанными электрическими связями)

Любая сетевая операционная система, с одной стороны, выполняет все функции локальной операционной системы, а с другой стороны, обладает некоторыми дополнительными средствами, позволяющими ей взаимодействовать через сеть с операционными системами других компьютеров.

Конец 60-х – цифровые телефонные сети

С конца 60-х годов в телефонных сетях все чаще стала применяться передача голоса в цифровой форме. Это привело к появлению высокоскоростных цифровых каналов, соединяющих автоматические телефонные станции (АТС) и позволяющих одновременно передавать десятки и сотни разговоров.

Начало 70-х – первые локальные сети

1) В результате технологического прорыва в области производства компьютерных компонентов появились большие интегральные схемы (БИС). Их сравнительно невысокая стоимость и хорошие функциональные возможности привели к созданию миникомпьютеров, которые стали реальными конкурентами мэйнфреймов.

2) Снабжение компьютерными ресурсами подразделений предприятий, но работа компьютеров автономна

Локальные сети (Local Area Network, LAN) — это объединения компьютеров, сосредоточенных на небольшой территории.

3) На первых порах для соединения компьютеров друг с другом использовались нестандартные сетевые технологии.

Сетевая технология — это согласованный набор программных и аппаратных средств (например, драйверов, сетевых адаптеров, кабелей и разъемов), а также механизмов передачи данных по линиям связи, достаточный для построения вычислительной сети.

Начало 80-х – появление ПК и Интернета

ПК стали идеальными элементами построения сетей — с одной стороны, они были достаточно мощными, чтобы обеспечивать работу сетевого программного обеспечения, а с другой — явно нуждались в объединении своей вычислительной мощности для решения сложных задач, а также разделения дорогих периферийных устройств и дисковых массивов. Поэтому персональные компьютеры стали преобладать в локальных сетях, причем не только

в качестве клиентских компьютеров, но и в качестве центров хранения и обработки данных, то есть сетевых серверов, потеснив с этих привычных ролей миникомпьютеры и мэйнфреймы.

Середина 80-х – Стандартные технологии локальных сетей

Ethernet, Arcnet, Token Ring, Token Bus, несколько позже — FDDL

- 1) Опирались на принцип коммутации пакетов
- 2) Простота построения сети (приобретение кабеля и сетевых адаптеров, установка адаптеров в компьютеры, подсоединение к кабелю, установка сетевых ОС)
- 3) Простой и удобный доступ к сетевым ресурсам

1991 год – изобретение Web

- 1) Гипертекстовая информационная служба World Wide Web, ставшая основным поставщиком информации в Интернете. Ее интерактивные возможности превзошли возможности многих аналогичных служб локальных сетей, так что разработчикам локальных сетей пришлось просто позаимствовать эту службу у глобальных сетей. Процесс переноса технологий из глобальной сети Интернет в локальные приобрел такой массовый характер, что появился даже специальный термин — intranet-технологии (intra — внутренний).
- 2) Объединение и взаимопроникновение сетей - конвергенция

Начало 90-х появление беспроводных сетей

Конец 90-х – развитие технологии Wi-Fi

- был создан в 1991 году
- продукты, предназначавшиеся изначально для систем кассового обслуживания, были выведены на рынок под маркой WaveLAN и обеспечивали скорость передачи данных от 1 до 2 Мбит/с.
- Создатель Wi-Fi — Вик Хейз (*Vic Hayes*)

2. Классификация сетей. Топологии.

Компьютерная сеть - набор автономных компьютеров, связанных одной технологией (способных обмениваться информацией).

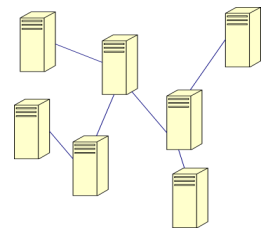
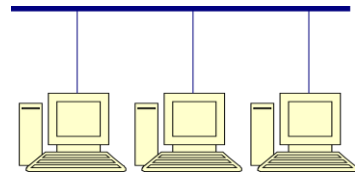
Классификации процесс группирования объектов изучения в соответствии с их общими признаками.

Классификация по территории покрытия:

Тип	Протяженность	Расположение
Персональная	1 м	На столе
Локальная	10 м – 1 км	Комната, здание, кампус
Муниципальная	10 км	Город
Глобальная	100 – 1000 км	Страна, континент
Объединение сетей	10 000 км	Весь мир

Классификация по технологии передачи

- **Широковещательные** сети – единый канал связи, данные получают все компьютеры (Wi-Fi, классический Ethernet)
- Сети **точка-точка** – каналы связи соединяют по 2 компьютера, передача данных через промежуточные компьютеры

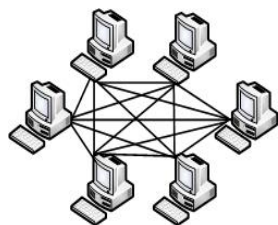


Классификация по типу коммутации

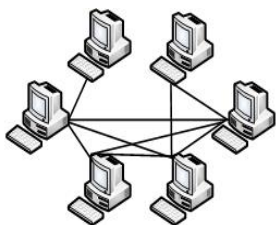
- **Коммутация каналов** – перед передачей данных устанавливается канал связи, по которому передаются все данные
- **Коммутация пакетов** – данные разбиваются на части (пакеты) и передаются по мере готовности

Топология сети – конфигурация графа:

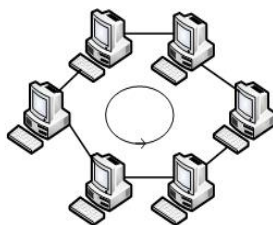
- Вершины – узлы сети (компьютеры и сетевое оборудование)
- Ребра – связи между узлами (физические или информационные)



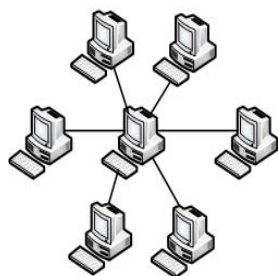
Полносвязная



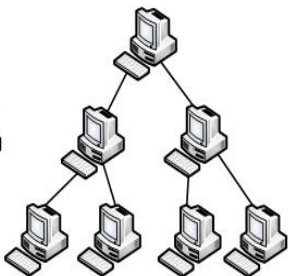
Ячеистая



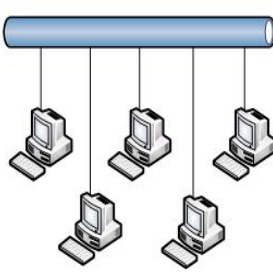
Кольцо



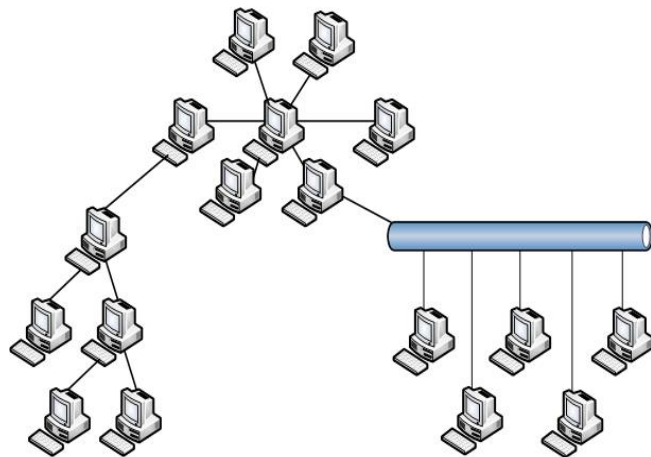
Звезда



Дерево



Общая шина



Смешанная топология

- Полносвязная топология: громоздкий, неэффективный, квадратичная зависимость от числа узлов, используется в многомашинных комплексах или в сетях, объединяющих небольшое количество компьютеров.
- Ячеистая топология получается из полносвязной путем удаления некоторых связей, допускает соединение большого количества компьютеров и характерна, как правило, для крупных сетей.
- Кольцевая топология: обеспечивает резервирование связей (любая пара узлов соединена 2 путями), удобная конфигурация для организации обратной связи (данные, сделав полный оборот, возвращаются к узлу-источнику), необходимы меры по поддержанию канала связи (если один из узлов выйдет из строя).
- Звездообразная топология: каждый компьютер подключен к центральному элементу – концентратору (компьютер или спец. устр-во – коммутатор, маршрутизатор и т.п), роль которого направлять информации одному или всем остальным компьютерам сети, высокая стоимость оборудования, ограниченная возможность добавления узлов.
- Дерево – несколько концентраторов, иерархически соединенные между собой звездообразными связями.

- f) Общая шина: в кач-ве центрального эл-та выступает пассивный кабель, по которому распространяется передаваемая информация (доступна всем компьютерам), дешевизна и простота присоединения узлов, но ненадежность(дефект кабеля) и низкая производительность(только 1 компьютер передает информацию в каждый момент времени).

Физическая и логическая топологии сетей.

Физическая топология описывает реально используемые способы организации физических соединений различного сетевого оборудования (использующиеся кабели, разъемы и способы подключения сетевого оборудования).

Логическая топология определяет реальные пути движения сигналов при передаче данных по используемой физической топологии. Таким образом, логическая топология описывает пути передачи потоков данных между сетевыми устройствами. Она определяет правила передачи данных в существующей среде передачи с гарантированием отсутствия помех влияющих на корректность передачи данных.

- Концентратор (Hub) – устройство для создания сетей Ethernet на основе витой пары
- WiFi:
 - ☐ Физических соединений нет
 - ☐ Логическая топология – общая шина



3. Понятия «протокол», «интерфейс» и «сервис». Примеры.

- Создание сети – сложная задача.
- Проблем при создании сетей очень много
 - Надежность
 - Ошибки при передаче по сети:
 - Искажение передаваемых данных
 - Потеря сообщений
 - Нарушение порядка передачи сообщений
 - Поиск рабочего пути через сеть
 - Несколько путей от источника к адресату
 - Часть оборудования может выходить из строя
 - Развитие сети
 - Масштабируемость
 - Рост числа хостов в сети
 - Объединение сетей
 - Разные механизмы адресации
 - Разные размеры сообщения
 - Нарушение порядка передачи сообщений
 - Распределение ресурсов
 - Распределение пропускной способности сети:
 - Статическое
 - Динамическое
 - Управление потоком
 - Быстрый отправитель перегрузит данными медленного получателя

- Скопление – перегрузка сети большим количеством одновременных отправок
 - Качество обслуживания (все возможные характеристики услуг и сети, желательные для пользователя).
Качество разное для разных типов нагрузки
 - Файлы:
 - Отсутствие искажений данных
 - Задержки допустимы
 - Видео, голос:
 - Минимальная задержка
 - Допустимы небольшие искажения
 - Безопасность
 - Перехват информации, передаваемой по сети
 - Пароль к электронной почте
 - Поддельные узлы сети:
 - Фальшивый сайт банка
 - Изменение сообщений:
 - Было: «Снимите с моего счета \$10»
 - Стало: «Снимите с моего счета \$1000»
- Как организовать сеть так, чтобы все перечисленные проблемы были решены?
 - 1) Декомпозиция - разбиение одной сложной задачи на несколько более простых задач-модулей. Декомпозиция состоит в четком определении функций каждого модуля, а также порядка их взаимодействия.
 - 2) Многоуровневый подход. После представления исходной задачи в виде множества модулей эти модули группируют и упорядочивают по уровням, образуя иерархию. В соответствии с принципом иерархии для каждого промежуточного уровня можно указать непосредственно примыкающие к нему соседние вышележащий и нижележащий уровни.

Сервис определяет, что именно делает уровень

Примеры сервисов:

- a. Надежная передача потока данных
- b. Согласование форматов передаваемых данных
- c. Поиск маршрута между сетями

Сервис не определяет:

- d. Как именно уровень реализует сервис
- e. Как получить доступ к данному уровню

Протокол уровня n – правила и соглашения, используемые для связи уровня n одного хоста с уровнем n другого хоста.

Примеры:

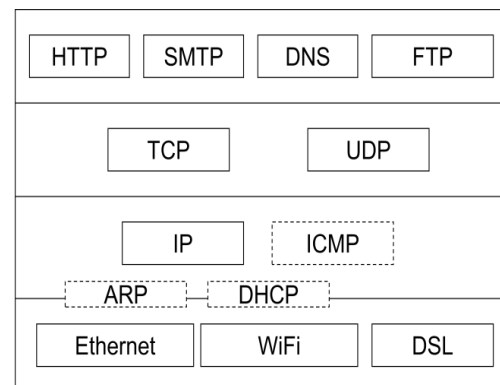
A) Основным протоколом сетевого уровня является межсетевой протокол (Internet Protocol, IP). В его задачу входит продвижение пакета между сетями — от одного маршрутизатора к другому до тех пор, пока пакет не попадет в сеть назначения. Разворачивается на всех шлюзах(не только на хостах), дейтаграммный протокол.

Прикладной

Транспортный

Сетевой

Сетевых
интерфейсов



Каждый отдельный пакет рассматривается сетью как совершенно независимая единица передачи — **дейтаграмма**.

Б) Протоколы прикладного уровня:

FTP - протокол передачи файлов (File Transfer Protocol)

Telnet - протокол эмуляции терминала

SMTP - простой протокол передачи почты (Simple Mail Transfer Protocol)

HTTP - протокол передачи гипертекста (Hypertext Transfer Protocol)

Интерфейс – набор примитивных операций, предоставляемых нижним уровнем верхнему.

Введение интерфейсов дает возможность проводить разработку, тестирование и модификацию отдельного уровня независимо от других уровней.

4. Понятия «стек протоколов» и «инкапсуляция»

Архитектура сети – набор уровней и протоколов сети

❖ Интерфейсы не входят в архитектуру!

Стек протоколов – иерархически организованный набор протоколов, достаточный для организации взаимодействия по сети.

В сети Windows могут использоваться такие стеки протоколов, как NetBIOS/NetBEUI (Microsoft), IPX/SPX (Novell) и TCP/IP.

■ **Инкапсуляция** – включение сообщения вышестоящего уровня в сообщение нижестоящего уровня

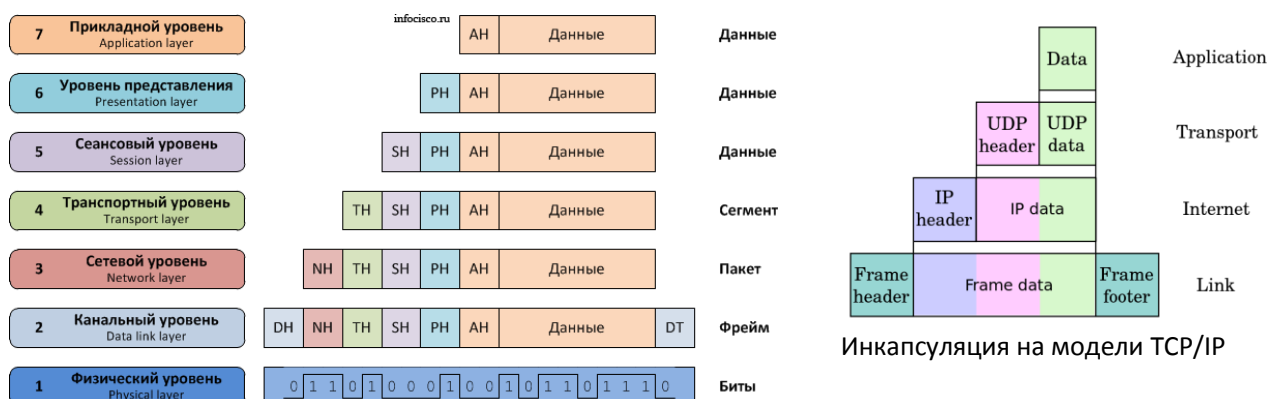
■ **Сообщение:**

☐ **Заголовок**

☐ **Данные**

☐ **Концевик**

Инкапсуляция – это процесс передачи данных с верхнего уровня приложений вниз (по стеку протоколов) к физическому уровню, чтобы быть переданными по сетевой физической среде (витая пара, оптическое волокно, Wi-Fi, и др.). Причём на каждом уровне различные протоколы добавляют к передающимся данным свою информацию.



Инкапсуляция на модели OSI

Процесс преобразования сигналов из провода в данные называется процессом **декапсуляции**.

5. Модель взаимодействия открытых систем ISO/OSI.

- На раннем этапе развития сетей (60-70 годы) стандартизации не было
- Оборудование разных производителей не могло взаимодействовать по сети
 - ☐ Несовместимость сетевого оборудования
 - ☐ Разные протоколы
- Решение – стандарты
Типы стандартов
- De jure (формальные, юридические) – принятые по формальным законам стандартизации
- De facto (фактические) – стандарты, установившиеся сами собой
 - ☐ Новая технология, пользующаяся большой популярностью

Эталонная модель сети описывает сервисы и уровни сети

- Эталонные модели:
 - ☐ Модель взаимодействия открытых систем (ISO OSI) – юридический стандарт
 - ☐ Модель TCP/IP – стандарт де-факто

Сетевая модель OSI (базовая эталонная модель взаимодействия открытых систем) — сетевая модель стека сетевых протоколов OSI/ISO.

- ❖ Принята в качестве стандарта Международной организацией по стандартизации (ISO) в 1983 г.
- ❖ Англоязычное название Open System Interconnection Reference Model (ISO OSI)
- ❖ **Открытая система** – построенная в соответствии с открытыми спецификациями

Открытая спецификация – общедоступная спецификация, соответствующая стандартам.

Преимущества открытых систем:

- Возможность построения сети из оборудования разных производителей
- Безболезненная замена отдельных компонентов на более совершенные
- Легкость объединения нескольких сетей
- ❖ Модель OSI описывает:
 - Семь уровней организации сети
 - Назначение каждого уровня
- ❖ Описание протоколов не включено в модель OSI, они выпущены отдельными стандартами
- ❖ Протоколы на практике не применяются
- ❖ Модель OSI используется в качестве «общего языка» для описания разных сетей (теоретическая модель, показывающая принципы реализации сетевых моделей)

Физический уровень:

- нижний уровень модели, который определяет метод передачи данных, представленных в двоичном виде, от одного устройства (компьютера) к другому.
- Задача: Передача потока битов без искажений в соответствии с заданной частотой
- Не вникает в смысл передаваемой информации

Канальный уровень:

- Предназначен для обеспечения взаимодействия сетей по физическому уровню и контролем над ошибками, которые могут возникнуть.
- Задачи:
 - Установка логического соединения
 - Согласование скоростей передачи и приема информации
 - Обеспечение надежности передачи, обнаружение и коррекция ошибок
- В широкополосной сети:
 - Управление доступом к среде передачи данных

- Физическая адресация
- Канальный уровень может взаимодействовать с одним или несколькими физическими уровнями, контролируя и управляя этим взаимодействием.

Сетевой уровень:

- Предназначен для определения пути передачи данных.
- Отвечает за
 - трансляцию логических адресов и имён в физические,
 - определение кратчайших маршрутов,
 - коммутацию и маршрутизацию,
 - отслеживание неполадок и «заторов» в сети.

Транспортный уровень:

- Предназначен для обеспечения надёжной передачи данных от отправителя к получателю. При этом уровень надёжности может варьироваться в широких пределах.
- Существует множество классов протоколов транспортного уровня, начиная от протоколов, предоставляющих только основные транспортные функции (например, функции передачи данных без подтверждения приема), и заканчивая протоколами, которые гарантируют доставку в пункт назначения нескольких пакетов данных в надлежащей последовательности, мультиплексируют несколько потоков данных, обеспечивают механизм управления потоками данных и гарантируют достоверность принятых данных.

Сеансовый уровень:

- Обеспечивает поддержание сеанса связи, позволяя приложениям взаимодействовать между собой длительное время.
- Уровень управляет
 - созданием/завершением сеанса,
 - обменом информацией,
 - синхронизацией задач,
 - определением права

Модель OSI		
Тип данных	Уровень (layer)	Функции
Данные	7. Прикладной (application)	Доступ к сетевым службам
	6. Представительский (presentation)	Представление и шифрование данных
	5. Сеансовый (session)	Управление сеансом связи
Сегменты (сообщения)	4. Транспортный (transport)	Прямая связь между конечными пунктами и надёжность
Пакеты	3. Сетевой (network)	Определение маршрута и логическая адресация
Кадры (дейтаграммы)	2. Канальный (data link)	Физическая адресация
Биты	1. Физический (physical)	Работа со средой передачи, сигналами и двоичными данными

Сетевое оборудование

Уровень модели OSI	Оборудование
Физический	Концентратор
Канальный	Коммутатор, точка доступа
Сетевой	Маршрутизатор

на передачу данных и поддержанием сеанса в периоды неактивности приложений.

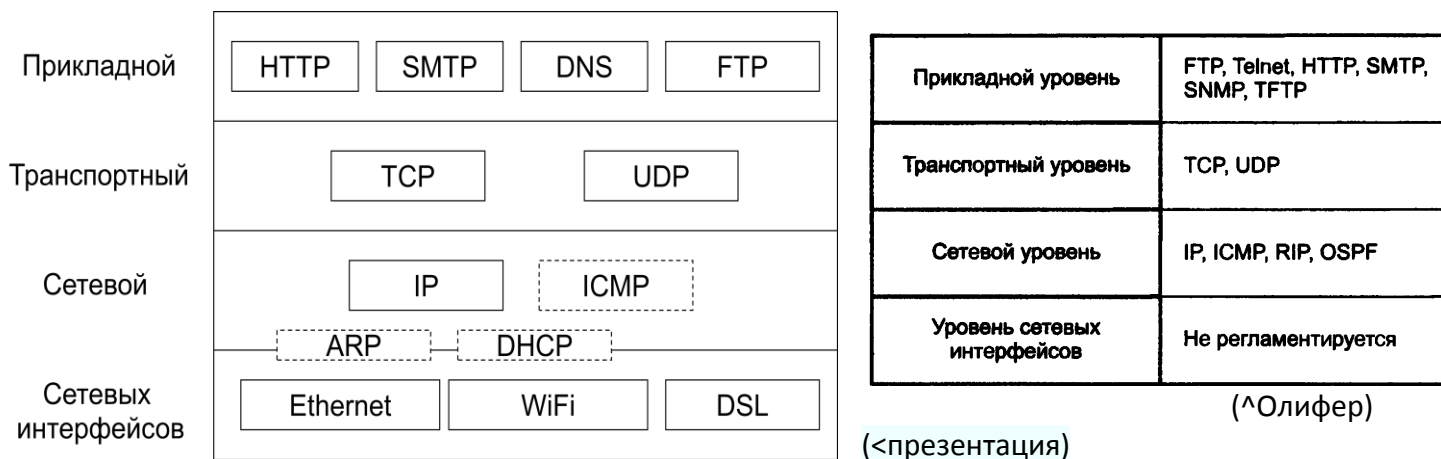
Уровень представления:

- Обеспечивает представление передаваемой по сети информации, не меняя при этом ее содержания, преобразование протоколов и шифрование/дешифрование данных.
- Запросы приложений, полученные с прикладного уровня, на уровне представления преобразуются в формат для передачи по сети, а полученные из сети данные преобразуются в формат приложений.
- На этом уровне может осуществляться сжатие/распаковка или кодирование/декодирование данных, а также перенаправление запросов другому сетевому ресурсу, если они не могут быть обработаны локально.

Прикладной уровень:

- верхний уровень модели, обеспечивающий взаимодействие пользовательских приложений с сетью:
- позволяет приложениям использовать сетевые службы:
 - удалённый доступ к файлам и базам данных,
 - пересылка электронной почты;
- отвечает за передачу служебной информации;
- предоставляет приложениям информацию об ошибках;
- формирует запросы к уровню представления.

6. Стек протоколов TCP/IP.



Эталонная модель TCP/IP

- Стандарт де-факто
- Протоколы TCP/IP стали популярны при создании сети ARPANET
- ARPANET объединяла сети, использующие различные технологии
- Необходимо было разработать модель, которая бы позволила объединять сети на основе стека TCP/IP
- Модель включает:
 - 4 сетевых уровня
 - Протоколы для каждого уровня

Прикладной уровень стека TCP/IP соответствует трем верхним уровням модели OSI: прикладному, представления и сеансовому. Он объединяет сервисы, предоставляемые системой пользовательским приложениям.

Протоколы прикладного уровня:

- **FTP** - протокол передачи файлов (File Transfer Protocol)

- **Telnet** - протокол эмуляции терминала
- **SMTP** - простой протокол передачи почты (Simple Mail Transfer Protocol)
- **HTTP** - протокол передачи гипертекста (Hypertext Transfer Protocol)
- **DNS** (Domain Name System) - протокол обращения к системе доменных имен

Протоколы **транспортного уровня** могут решать проблему негарантированной доставки сообщений («дошло ли сообщение до адресата?»), а также гарантировать правильную последовательность прихода данных. В стеке TCP/IP транспортные протоколы определяют, для какого именно приложения предназначены эти данные.

- **TCP** — «гарантированный» транспортный механизм с предварительным установлением соединения, предоставляющий приложению надёжный поток данных, дающий уверенность в безошибочности получаемых данных, перезапрашивающий данные в случае потери и устраняющий дублирование данных. TCP позволяет регулировать нагрузку на сеть, а также уменьшать время ожидания данных при передаче на большие расстояния. Более того, TCP гарантирует, что полученные данные были отправлены точно в такой же последовательности.
- **UDP** - протокол передачи дейтаграмм без установления соединения. Также его называют протоколом «ненадёжной» передачи, в смысле невозможности удостовериться в доставке сообщения адресату, а также возможного перемешивания пакетов. UDP обычно используется в таких приложениях, как потоковое видео и компьютерные игры, где допускается потеря пакетов, а повторный запрос затруднён или не оправдан, либо в приложениях вида запрос-ответ (например, запросы к DNS), где создание соединения занимает больше ресурсов, чем повторная отправка.

Сетевой уровень, называемый также уровнем Интернета, является стержнем всей архитектуры TCP/IP. Именно этот уровень, функции которого соответствуют сетевому уровню модели OSI, обеспечивает *перемещение пакетов в пределах составной сети*, образованной объединением нескольких подсетей. Протоколы сетевого уровня поддерживают *интерфейс с вышележащим транспортным уровнем*, получая от него запросы на передачу данных по составной сети, а также с нижележащим уровнем сетевых интерфейсов.

- **IP** — (Internet Protocol, межсетевой протокол) основной протокол сетевого уровня. В его задачу входит продвижение пакета между сетями — от одного маршрутизатора к другому до тех пор, пока пакет не попадет в сеть назначения. В отличие от протоколов прикладного и транспортного уровней, протокол IP разворачивается не только на хостах, но и на всех маршрутизаторах (шлюзах). Протокол IP — это дейтаграммный протокол, работающий без установления соединений по принципу доставки с максимальными усилиями. Такой тип сетевого сервиса называют также «ненадежным».
- **ICMP** (*Internet Control Message Protocol* — протокол межсетевых управляющих сообщений) — сетевой протокол, входящий в стек протоколов TCP/IP. В основном ICMP используется для передачи сообщений об ошибках и других исключительных ситуациях, возникших при передаче данных, например, запрашиваемая услуга недоступна, или хост, или маршрутизатор не отвечают. Также на ICMP возлагаются некоторые сервисные функции.
- **DHCP** (*Dynamic Host Configuration Protocol* — протокол динамической настройки узла) — сетевой протокол, позволяющий компьютерам автоматически получать IP-адрес и другие параметры, необходимые для работы в сети TCP/IP.
- **RIP** (протокол маршрутной информации, *Routing Information Protocol*) — один из самых простых протоколов маршрутизации. Применяется в небольших компьютерных сетях, позволяет маршрутизаторам динамически обновлять маршрутную информацию

(направление и дальность в транзитивных участках – участках между двумя узлами, по которым передаются данные), получая ее от соседних маршрутизаторов.

- **ARP** (*Address Resolution Protocol* — протокол определения адреса) — протокол в компьютерных сетях, предназначенный для определения *MAC адреса* по известному IP адресу.

Уровень сетевых интерфейсов описывает, каким образом передаются пакеты данных через физический уровень, включая *кодирование* (то есть специальные последовательности бит, определяющих начало и конец пакета данных). Кроме того, уровень описывает среду передачи данных (будь то коаксиальный кабель, витая пара, оптическое волокно или радиоканал), физические характеристики такой среды и принцип передачи данных (разделение каналов, модуляцию, амплитуду сигналов, частоту сигналов, способ синхронизации передачи, время ожидания ответа и максимальное расстояние).

Так как для каждой вновь появляющейся технологии разрабатываются собственные интерфейсные средства, функции этого уровня нельзя определить раз и навсегда, и именно поэтому нижний уровень стека TCP/IP не регламентируется.

7. Стеки сетевых протоколов (обзор).

Стек протоколов – иерархически организованный набор протоколов, достаточный для организации взаимодействия по сети.

Важнейшим направлением стандартизации в области вычислительных сетей является стандартизация коммуникационных протоколов. Наиболее известными стеками протоколов являются: OSI, TCP/IP, IPX/SPX, NetBIOS/SMB, DECnet, SNA (не все из них применяются сегодня на практике).

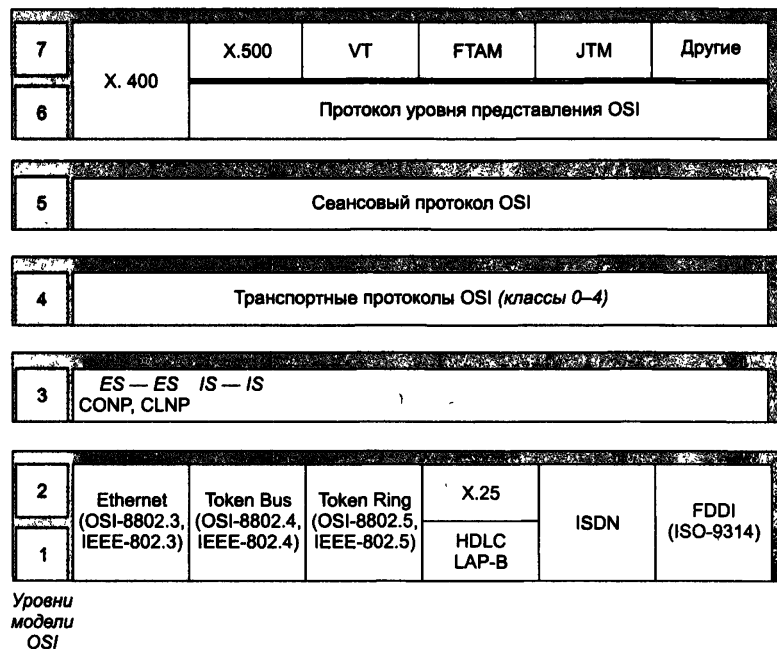
Стек OSI

Важно различать модель OSI и стек протоколов OSI. В то время как модель OSI является концептуальной схемой взаимодействия открытых систем, стек OSI представляет собой набор спецификаций конкретных протоколов. В отличие от других стеков протоколов, стек OSI полностью соответствует модели OSI, включая спецификации протоколов для всех семи уровней взаимодействия, определенных в этой модели.

Протоколы стека OSI отличает сложность и неоднозначность спецификаций. Эти свойства явились результатом общей политики разработчиков стека, стремившихся учесть в своих протоколах все многообразие уже существующих и появляющихся технологий.

На физическом и канальном уровнях стек OSI поддерживает протоколы **Ethernet**, **Token Ring**, **FDDI**, а также протоколы **LLC**, **X.25** и **ISDN**, то есть использует все разработанные вне стека популярные протоколы нижних уровней, как и большинство других стеков.

Сетевой уровень включает протоколы Connection-oriented Network Protocol (**CONP**) и Connectionless Network Protocol (**CLNP**), протоколы маршрутизации стека OSI: **ES-IS** (End System



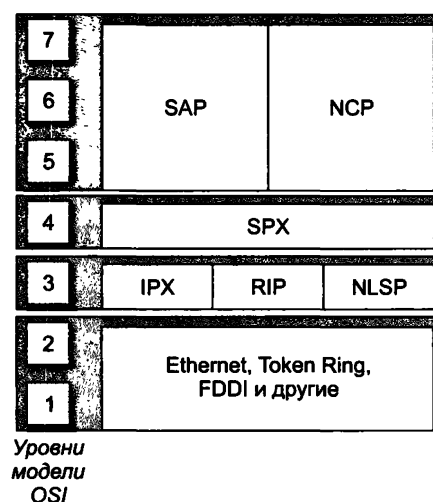
— Intermediate System) между конечной и промежуточной системами и **IS-IS** (Intermediate System — Intermediate System) между промежуточными системами.

Транспортный уровень стека OSI в соответствии с функциями, определенными для него в модели OSI, скрывает различия между сетевыми сервисами с установлением соединения и без установления соединения, так что пользователи получают требуемое качество обслуживания независимо от нижележащего сетевого уровня. Чтобы обеспечить это, транспортный уровень требует, чтобы пользователь задал нужное качество обслуживания.

Службы прикладного уровня обеспечивают передачу файлов, эмуляцию терминала, службу каталогов и почту. Из них наиболее популярными являются служба каталогов (**стандарт X.500**), электронная почта (**X.400**), протокол виртуального терминала (**VTP**), протокол передачи, доступа и управления файлами (**FTAM**), протокол пересылки и управления работами (**JTM**).

Стек IPX/SPX

- является оригинальным стеком протоколов фирмы Novell, разработанным для сетевой операционной системы NetWare еще в начале 80-х годов.
- Протоколы стека разрабатывались с учетом применения в локальных сетях с небольшими сетевыми ресурсами, но с хорошими физическими коммуникационными средствами. Поэтому эти протоколы не очень хорошо работали в составных сетях с глобальными низкоскоростными связями.
- В настоящее время, с одной стороны, возросла пропускная способность глобальных сетей, с другой - усовершенствованы протоколы стека. Все это теперь позволяет стеку IPX/SPX успешно конкурировать с другими стеками при создании корпоративных сетей.

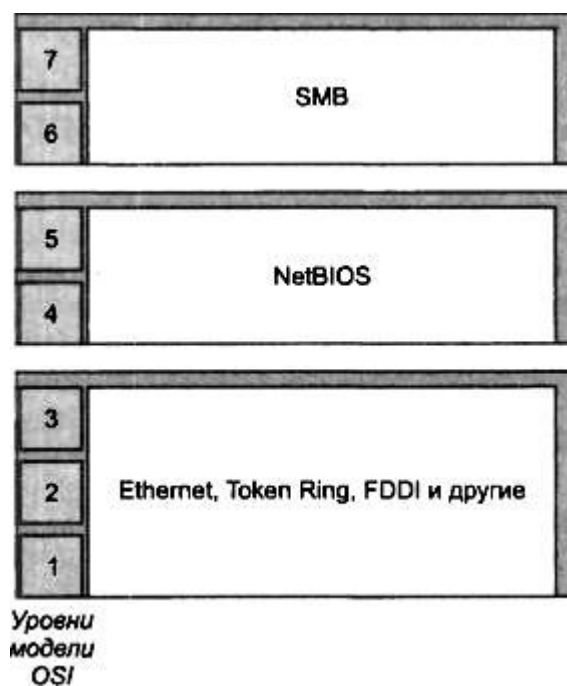


Протоколы:

- **IPX** (Internetwork Packet Exchange) - протокол межсетевого обмена пакетами. Это основной протокол стека, он соотносится с сетевым уровнем модели OSI;
- **SPX** (Sequenced Packet Exchange) - протокол последовательного обмена пакетами; обеспечивает надежность передачи данных;
- **PEP** (Packet Exchange Protocol) - протокол обмена пакетами (считается частью подсистемы NCP и не документирован)
- **NCP** (NetWare Core Protocol) - основной протокол верхнего уровня. Он обеспечивает работу основных служб сетевой ОС Novell NetWare и объединяет функции всех уровней от транспортного до прикладного модели OSI;
- **SAP** (Service Advertising Protocol) - протокол оповещения о сервисах; он используется при широковещательных сообщениях, когда узел передает информацию о сетевых службах, которые он может предоставить; здесь же указывается его сетевой адрес.
- **RIP** (Routing Information Protocol) - протокол маршрутной информации.
- **NLSP** (Network Link Services Protocol) – протокол маршрутизации.

Стек NetBIOS/SMB

- является совместной разработкой компаний IBM и Microsoft



- На физическом и канальном уровнях этого стека задействованы уже получившие распространение протоколы, такие как **Ethernet, Token Ring, FDDI**.
- **NetBIOS** - интерфейс прикладного программирования сетевых приложений.
- **NetBEUI** (NetBIOS Extended User Interface) - расширенный интерфейс протокола NetBIOS
- **NBF** находится на самом нижнем уровне стека. Он выполняет функции протокола транспортного и сетевого уровней и предоставляет базовые услуги связи между устройствами.
- Протокол Server Message Block (**SMB**) поддерживает функции сеансового уровня, уровня представления и прикладного уровня. На основе SMB реализуется файловая служба, а также службы печати и передачи сообщений между приложениями.

Стек протоколов TCP/IP

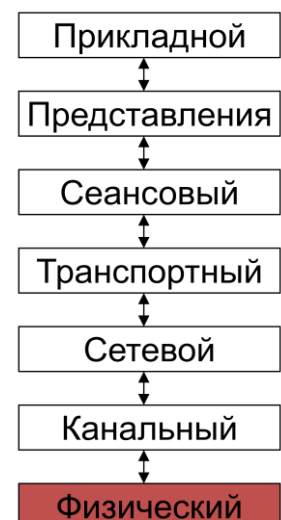
- Стек протоколов TCP/IP представляет собой семейство протоколов, обеспечивающих соединение и совместное использование различных систем. Стек был разработан для работы в разнородных сетях. Протоколы стека отличаются высокой надежностью: они отвечают требованию обеспечения возможности работы узлов сети, уцелевших при ограниченном ядерном нападении. В настоящее время стек протоколов TCP/IP используется как для связи в сети Интернет, так и в локальных сетях.
- В основу архитектуры TCP/IP была целенаправленно заложена одноранговая структура. TCP/IP имеет распределенный характер, в отличие от классической "нисходящей" модели обеспечения надежности. В среде с TCP/IP никакого центрального органа нет. Узлы взаимодействуют непосредственно друг с другом, и каждый из них обладает полной информацией о всех доступных сетевых сервисах. Если какой-либо из хост-компьютеров отказывает, ни одна из остальных машин на это не реагирует (если только ей не нужны данные, которые как раз на отказавшем компьютере и находятся).

Прикладной уровень	FTP, Telnet, HTTP, SMTP, SNMP, TFTP
Транспортный уровень	TCP, UDP
Сетевой уровень	IP, ICMP, RIP, OSPF
Уровень сетевых интерфейсов	Не регламентируется

Протоколы:

- **TCP** (Transmission Control Protocol - протокол управления передачей) - базовый транспортный протокол, давший название всему семейству протоколов TCP/IP;
- **UDP** (User Datagram Protocol) - второй по распространенности транспортный протокол семейства TCP/IP;
- **IP** (Internet Protocol) - межсетевой протокол;
- **ARP** (Address Resolution Protocol - протокол разрешения адресов) - используется для определения соответствия IP-адресов и Ethernet-адресов;
- **SLIP** (Serial Line Internet Protocol) - протокол передачи данных по телефонным линиям;
- **PPP** (Point to Point Protocol) - протокол обмена данными "точка-точка";
- **RPC** (Remote Process Control) - протокол управления удаленными процессами;
- **TFTP** (Trivial File Transfer Protocol) - простой протокол передачи файлов;
- **DNS** (Domain Name System) - протокол обращения к системе доменных имен;
- **RIP** (Routing Information Protocol) - протокол маршрутизации.

8. Физический уровень.



Место в модели OSI

- нижний уровень модели, который определяет метод передачи данных, представленных в двоичном виде, от одного устройства (компьютера) к другому.
- Задача: Передача потока битов без искажений в соответствии с заданной частотой
- Не вникает в смысл передаваемой информации

Среда передачи данных - физическая среда, пригодная для прохождения сигнала

- Служит для физической передачи данных в сети от одного устройства к другому
- Выделяют 3 вида сред:

1) Проводная (воздушная) среда

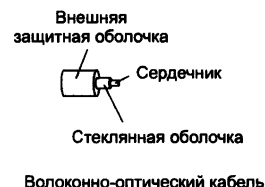
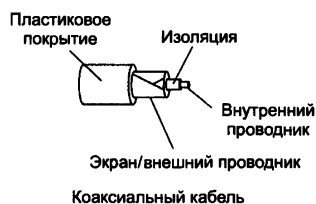
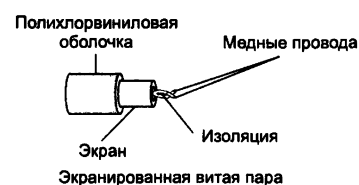
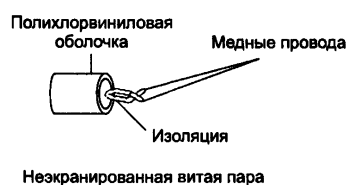
- провода без каких-либо изолирующих или экранирующих оплеток, проложенные между столбами и висящие в воздухе
- Появились самыми первыми
- Использовались для телефонной связи
- Низкая скорость
- Высокие помехи

2) Кабельная среда:

Медные кабели

витая пара:

- ☐ Скрученная пара медных проводов
- ☐ Скручивание снижает помехи
- ☐ В одном кабеле несколько скрученных пар
 - Экранированная витая пара – большая защищенность сигнала от помех
 - Неэкранированная витая пара – больше помех, но дешевле и удобнее при монтаже



коаксиальный кабель:

- ☐ состоит из несимметричных пар проводников.
- ☐ Каждая пара представляет собой внутреннюю медную жилу и соосную с ней внешнюю жилу, которая может быть поллой медной трубой или оплеткой, отделенной от внутренней жилы диэлектрической изоляцией.
- ☐ Внешняя жила играет двойную роль — по ней передаются информационные сигналы и она является экраном, защищающим внутреннюю жилу от внешних электромагнитных полей.
 - «Толстый» коаксиал (Ethernet) - хорошие механические и электрические характеристики, сложность монтажа
 - «Тонкий» коаксиал (Ethernet) (наоборот)
 - Телевизионный кабель (кабельное ТВ)

Оптические кабели

- ☐ состоит из тонких гибких стеклянных волокон, по которым распространяются световые сигналы
- ☐ наиболее качественный тип кабеля
 - Одномодовые кабели:
 - Тонкий сердечник
 - Одна длина волны
 - Дороги в изготовлении
 - Работают на расстоянии до сотен километров

- Многомодовые кабели:
 - Более толстый сердечник
 - Несколько длин волн
 - Дешевы в изготовлении
 - Расстояние до 300 – 500 м
 - При больших расстояниях возникают искажения из-за наложения сигналов с разной длиной волны

3) Беспроводная среда:

- Радиосвязь (образуются с помощью передатчика и приемника радиоволн)
- Спутниковая связь

Передача сигналов

- Задача физического уровня – передать сигнал по среде передачи данных
- Основная проблема: искажение сигналов при передаче по линиям связи:
 - Оптические кабели – низкое искажение
 - Медные кабели – среднее искажение
 - Радиоволны – высокое искажение
- Для того чтобы передатчик и приемник, соединенные некоторой средой, могли обмениваться информацией, им необходимо договориться о том, какие сигналы будут соответствовать двоичным единицам и нулям дискретной информации. Для представления дискретной информации в среде передачи данных применяются сигналы двух типов: **прямоугольные импульсы** и **синусоидальные волны**. В первом случае используют термин **«кодирование»**, во втором — **«модуляция»**.

Основы представления сигналов

- Любой сигнал можно представить суммой гармонических колебаний (с разной частотой и амплитудой)
- **Гармоника** – каждая составляющая разложения сигнала (синусоида)
- **Спектр** (спектральное разложение) – набор всех гармоник
- **Ширина спектра** – разность между максимальной и минимальной частотами гармоник
- **Полоса пропускания** – диапазон частот, при которых гармоники передаются по линии связи без искажения
- Чем больше полоса пропускания кабеля, тем лучше
- Чем меньше спектр сигнала, тем лучше

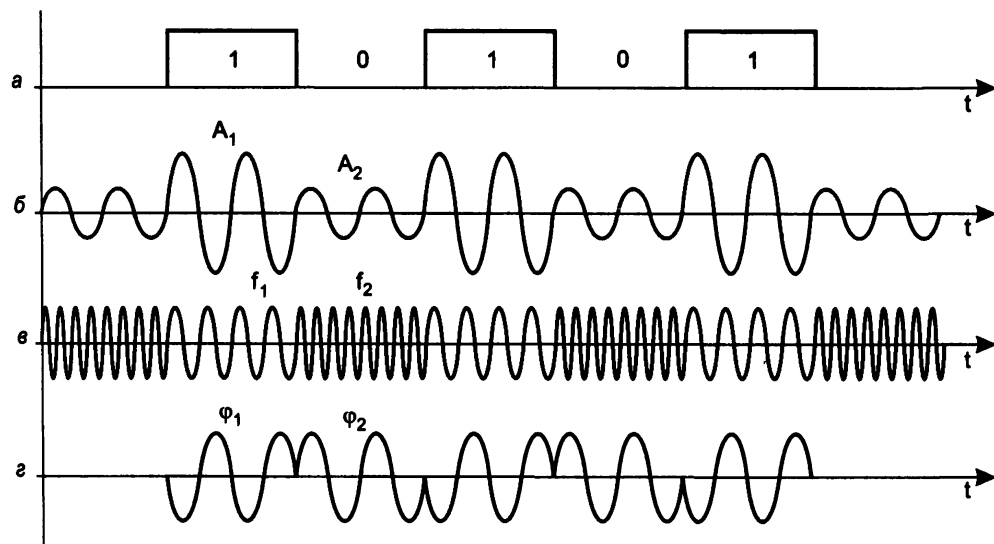
Модуляция

- передача информации с помощью синусоидальных сигналов путем изменения амплитуды, частоты или фазы

Исходная последовательность бит – рисунок а.

Типы модуляции:

При **амплитудной модуляции** для логической единицы выбирается один уровень амплитуды синусоиды несущей частоты, а для логического нуля — другой (рис. б). Этот способ редко используется в чистом



виде на практике из-за низкой помехоустойчивости.

При **частотной модуляции** значения нуля и единицы исходных данных передаются синусоидами с различной частотой — f_1 и f_2 (рис. в). Этот способ модуляции не требует сложных схем и обычно применяется в низкоскоростных модемах, работающих на скоростях 300 и 1200 бит/с.

При **фазовой модуляции** значениям данных 0 и 1 соответствуют сигналы одинаковой частоты, но различной фазы, например 0 и 180° или 0, 90° , 180° и 270° (рис. г).

Для повышения скорости передачи данных прибегают к **комбинированным методам модуляции**. (Например, квадратурная амплитудная модуляция.)

Кодирование, проблема синхронизации приемника и передатчика

- В вычислительной технике для представления данных используется двоичный код. Внутри компьютера единицам и нулям данных соответствуют дискретные электрические сигналы. **Представление данных в виде электрических или оптических сигналов называется кодированием.** Существуют различные способы кодирования двоичных цифр, например **потенциальный** способ, при котором единице соответствует один уровень напряжения, а нулю — другой, или **импульсный** способ, когда для представления цифр используются импульсы различной полярности.
- При выборе способа кодирования нужно одновременно стремиться к достижению нескольких целей:
 - минимизировать ширину спектра сигнала, полученного в результате кодирования;
 - обеспечивать синхронизацию между передатчиком и приемником;
 - обеспечивать устойчивость к шумам;
 - обнаруживать и по возможности исправлять битовые ошибки;
 - минимизировать мощность передатчика.

Синхронизация передатчика и приемника нужна для того, чтобы приемник точно знал, в какой момент времени считывать новую порцию информации с линии связи. При передаче дискретной информации время всегда разбивается на такты одинаковой длительности, и приемник старается считать новый сигнал в середине каждого такта, то есть синхронизировать свои действия с передатчиком.

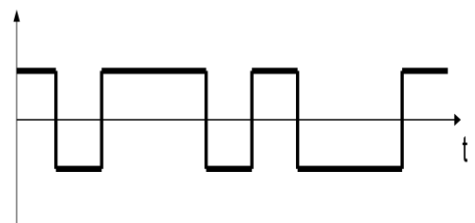
Проблема синхронизации в сетях решается сложнее, чем при обмене данными между близко расположенными устройствами, например, между блоками внутри компьютера или же между компьютером и принтером. На небольших расстояниях хорошо работает схема, основанная на отдельной тактирующей линии связи, так что информация снимается с линии данных только в момент прихода тактового импульса. В сетях использование этой схемы вызывает трудности из-за неоднородности характеристик проводников в кабелях. На больших **расстояниях неравномерность скорости распространения сигнала** может привести к тому, что тактовый импульс придет настолько позже или раньше соответствующего сигнала данных, что бит данных будет пропущен или считан повторно. Другой причиной, по которой в сетях отказываются от использования тактирующих импульсов, является **экономия проводников в дорогостоящих кабелях.**

В сетях для решения проблемы синхронизации применяются так называемые **самосинхронизирующиеся коды**, сигналы которых несут для приемника указания о том, в какой момент времени начать распознавание очередного бита. Любой резкий перепад сигнала — **фронт** — может служить указанием на необходимость синхронизации приемника с передатчиком.

Виды кодирования:

1) Кодирование NRZ

Используется два уровня потенциала:



- a. Положительный – 1
- b. Отрицательный – 0

Преимущества:

- Хорошая распознаваемость сигнала (уровни резко отличаются)
- Простота реализации

Недостатки:

- Низкочастотная составляющая, переходящая в постоянный ток
- Отсутствие синхронизации

2) Избыточное кодирование

- Избыточные коды основываются на добавлении информации, необходимой для синхронизации
- Исходная последовательность битов разбивается на порции – символы
- Каждый исходный символ заменяется на новый с большим количеством битов
- Часть символов в избыточных кодах не используется
- Обнаружение ошибок:
- Получили неиспользуемый символ – значит, произошла ошибка при передаче по сети
- Управляющие символы:
- Начало передачи, конец передачи и т.п.

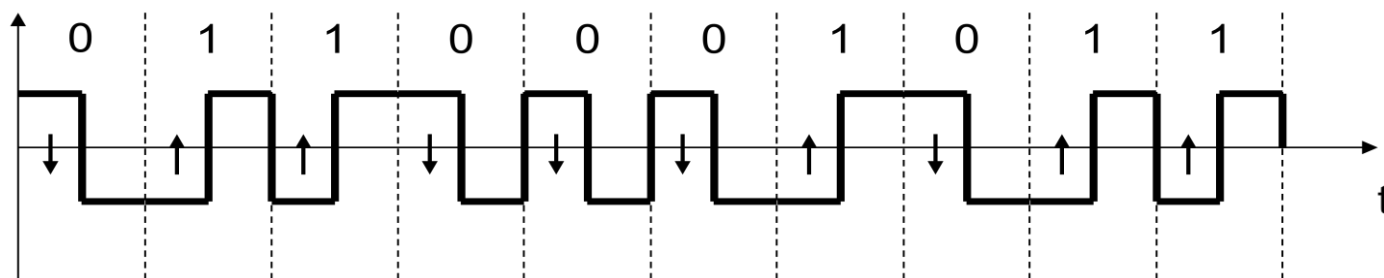
Избыточный код 4В/5В

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

Избыточный код 4В/5В

- ❖ Не содержит длинных последовательностей 0
- ❖ Передается по сети с помощью кодирования, не чувствительного к последовательностям 1 (NRZI)
- ❖ Прост в реализации (таблица перекодировки)

3) Манчестерское кодирование



- Два уровня сигнала
- Кодирование:
 - a. Переход от низкого сигнала к высокому – 1
 - b. Переход от высокого сигнала к низкому – 0
 - c. В начале такта возможен служебный переход сигнала
- XOR данных и тактовых импульсов
- Преимущества:
 - Два уровня сигнала
 - Самосинхронизация
- Недостаток:
 - Частота выше, чем у потенциальных кодов, спектр шире

4) Импульсное кодирование

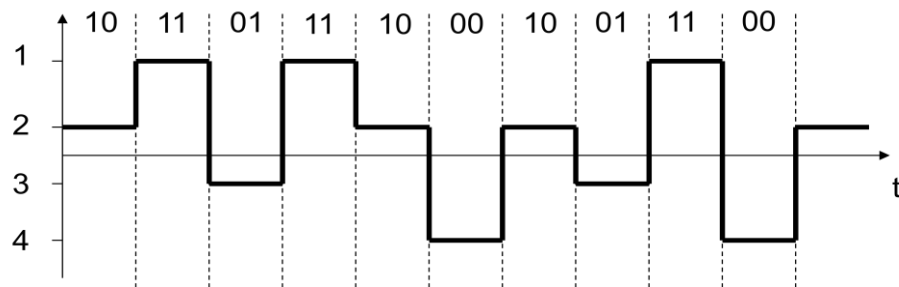
- Информация представляется сменой импульса, происходящей в середине такта
- Хорошая самосинхронизация – сигнал изменяется каждый такт
- Недостаток: широкий спектр по сравнению с потенциальным кодированием из-за высокой частоты

5) Потенциальный код **2B1Q** (каждые два бита (2B) передаются за один такт (1) сигналом, имеющим четыре состояния (Q — Quadra))

- Для передачи данных используется 4 уровня потенциала:

- 1 уровень – 11
- 2 уровень – 10
- 3 уровень – 01
- 4 уровень – 00

- За 1 такт передается 2 бита
- Недостаток: нужен мощный передатчик, чтобы различить 4 уровня сигнала



- 6) Скремблирование – перемешивание информации так, чтобы не оставалось длинных последовательностей 0.

9. Понятие «разделяемая среда». Соединение точка-точка.

Физические каналы связи делятся на несколько типов в зависимости от того, могут они передавать информацию в обоих направлениях или нет.

Направления передачи

Симплексный режим – данные передаются только в одну сторону

Дуплексный режим – данные передаются одновременно в обе стороны

Полудуплексный режим – данные передаются в обе стороны с разделением времени

В том случае, когда линия связи является дуплексным каналом связи, как это показано на рис. 2.20, каждый из интерфейсов монопольно использует канал связи в направлении «от себя». Это объясняется тем, что дуплексный канал состоит из двух независимых сред передачи данных (подканалов), и так как только передатчик интерфейса является активным устройством, а приемник пассивно ожидает поступления сигналов от приемника, то конкуренции подканалов не возникает.

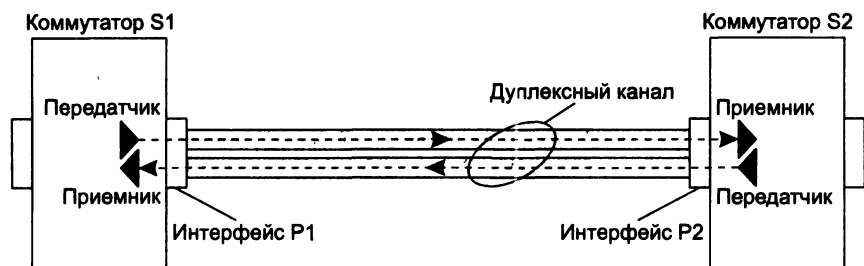


Рис. 2.20. Дуплексный канал — разделяемая среда отсутствует

Такой режим использования среды передачи данных является в настоящее время основным в компьютерных локальных и глобальных сетях.

Однако если в глобальных сетях такой режим использовался всегда, то в локальных сетях до середины 90-х годов преобладал другой режим, основанный на разделяемой среде передачи данных.

Разделяемой средой (shared medium) называется физическая среда передачи данных, к которой непосредственно подключено несколько передатчиков узлов сети. Причем в каждый момент времени только один из передатчиков какого-либо узла сети получает доступ к разделяемой среде и использует ее для передачи данных приемнику другого узла, подключенному к этой же среде.

В наиболее простом случае эффект деления среды возникает при соединении двух интерфейсов с помощью полудуплексного канала связи, то есть такого канала, который может передавать данных в любом направлении, но только попеременно (рис. 2.21). В этом случае к одной и той же среде передачи данных (например, к коаксиальному кабелю или общей радиосреде) подключены два приемника двух независимых узлов сети.

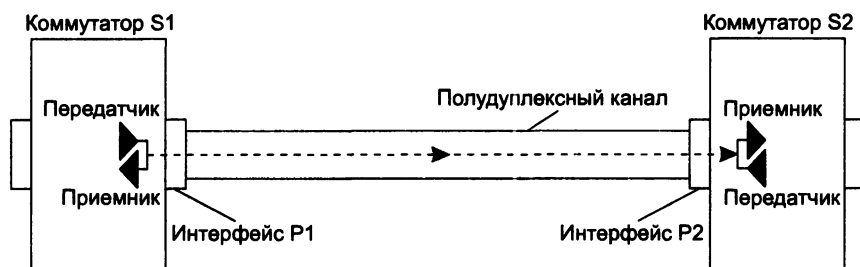


Рис. 2.21. Полудуплексный канал — разделяемая среда

При таком применении среды передачи данных возникает новая задача совместного использования среды независимыми передатчиками таким образом, чтобы в каждый отдельный момент времени по среде передавались данные только одного передатчика. Другими словами, возникает необходимость в механизме синхронизации доступа интерфейсов к разделяемой среде.

Существуют различные способы решения задачи организации совместного доступа к разделяемым линиям связи. Одни из них подразумевают централизованный подход, когда доступом к каналу управляет специальное устройство — арбитр, другие — децентрализованный.

На первый взгляд может показаться, что **механизм деления среды очень похож на механизм мультиплексирования потоков** — в том и другом случаях по линии связи передаются несколько потоков данных. Однако здесь есть принципиальное различие, касающееся того, как контролируется (управляется) линия связи. При мультиплексировании дуплексная линия связи в каждом направлении находится под полным контролем одного коммутатора, который решает, какие потоки разделяют общий канал связи.

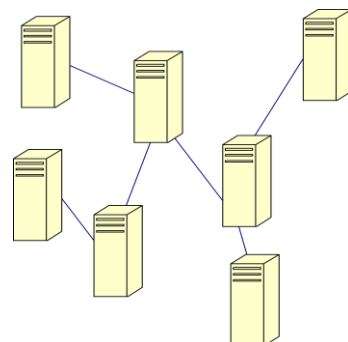
Мультиплексирование — образование из нескольких отдельных потоков общего агрегированного потока, который передается по одному физическому каналу связи. Другими словами, мультиплексирование — это способ деления одного имеющегося физического канала между несколькими одновременно протекающими сеансами связи между абонентами сети.

Сегодня в проворных локальных сетях метод деления среды практически перестал применяться. Основной причиной отказа от разделяемой среды явилась ее низкая и плохо предсказуемая производительность, а также плохая масштабируемость.

Сети **точка-точка** — каналы связи соединяют по 2 компьютера, передача данных через промежуточные компьютеры

Типичным примером сети типа "точка-точка", предоставляющей большие возможности коррекции ошибок и гибкие средства управления, являются открытые сети данных, использующие протокол X.25.

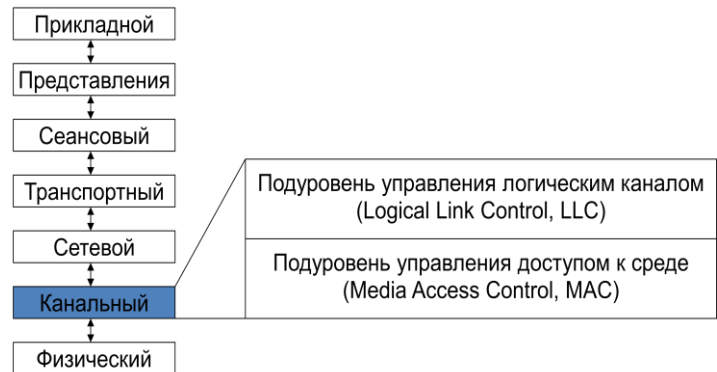
Технология передачи "точка-точка" основана на последовательной передаче данных и обеспечивает:



- высокоскоростную и безошибочную передачу, применяя радиоканал типа "точка-точка";
- проникновение сигнала через стены и перекрытия;
- скорость передачи от 1,2 до 38,4 Кбит/с на расстояние до 60 м внутри здания и 550 м в условиях прямой видимости.

10. Канальный уровень.

- Предназначен для обеспечения взаимодействия сетей по физическому уровню и контролем над ошибками, которые могут возникнуть.
- Задачи:
 - Установка логического соединения
 - Согласование скоростей передачи и приема информации
 - Обеспечение надежности передачи, обнаружение и коррекция ошибок
- В широковещательной сети:
 - Управление доступом к среде передачи данных
 - Физическая адресация
- Канальный уровень может взаимодействовать с одним или несколькими физическими уровнями, контролируя и управляя этим взаимодействием.



Подуровни канального уровня:

- Подуровень управления логическим каналом (LLC)
 - ☐ Отвечает за передачу данных
 - ☐ Обеспечивает проверку и правильность передачи информации по соединению
 - ☐ Общий для разных технологий
 - ☐ выступает в качестве интерфейса между подуровнем MAC и сетевым уровнем

Услуги подуровня LLC

- **LLC1** – передача данных без установления соединения и без подтверждения получения (Ethernet)
- **LLC2** – передача данных с установлением соединения (Token Ring)
- **LLC3** – передача данных без установления соединения, но с подтверждением получения (WiFi)
- **Мультиплексирование**
 - ✓ Передача данных разных протоколов (IP, ARP, ICMP) на уровень MAC
- **Демultipлексирование**
 - ✓ решает, какому из сетевых протоколов передать полученные от MAC данные
- **Управление потоком:**
 - ✓ Предотвращение «затопления» медленного получателя быстрым отправителем
- Подуровень управления доступом к среде (MAC):
 - ☐ Обеспечение доступа к разделяемой среде
 - ☐ Специфичный для разных технологий
 - ☐ Не является обязательным
 - ☐ выступает в качестве интерфейса между подуровнем LLC и физическим (первым) уровнем.

Услуги подуровня MAC

- Адресация (присвоение MAC-адреса каждому устройству)
- Согласование скорости передачи данных

11. Классический Ethernet. Концентратор. Метод доступа к среде CSMA/CD.

История создания и развития

- Первая сеть на разделяемой среде: радиосеть ALOHA, Гавайский университет
- Роберт Меткалф изучал ALOHA в аспирантуре
- Технология Ethernet была разработана вместе со многими первыми проектами корпорации Xerox PARC. Общепринято считать, что Ethernet был изобретён **22 мая 1973 года**, когда **Роберт Меткалф** составил докладную записку для главы PARC о потенциале технологии Ethernet. Но законное право на технологию Меткалф получил через несколько лет.
- **В 1976 году** он и его ассистент Дэвид Боггс (David Boggs) **издали брошюру** под названием «Ethernet: Distributed Packet-Switching For Local Computer Networks».
- **Меткалф ушёл из Xerox в 1979 году и основал компанию 3Com для** продвижения компьютеров и локальных вычислительных сетей (ЛВС). Ему удалось убедить DEC, Intel и Xerox работать совместно и **разработать стандарт Ethernet (DIX)**.
- Впервые этот стандарт был опубликован **30 сентября 1980 года**.
- 1982 г. Создан проект IEEE 802 для стандартизации Ethernet
- Он начал соперничество с двумя крупными запатентованными технологиями: token ring и ARCNET, — которые вскоре были раздавлены под накатывающимися волнами продукции Ethernet. В процессе борьбы 3Com стала основной компанией в этой отрасли.

Типы Ethernet

Название	Скорость	Кабель	Стандарт
Ethernet	10 Мб/с	«Толстый», «тонкий» коаксиал, Витая пара	802.3
Fast Ethernet	100 Мб/с	Витая пара, оптика	802.3u
Gigabit Ethernet	1 Гб/с	Витая пара, оптика	802.3z, 802.3ab
10G Ethernet	10 Гб/с	Витая пара, оптика	802.3ae, 802.3an

Преимущества использования витой пары по сравнению с коаксиальным кабелем:

- возможность работы в дуплексном режиме;
- низкая стоимость кабеля «витой пары»;
- более высокая надёжность сетей при неисправности в кабеле (соединение точка-точка: обрыв кабеля лишает связи два узла. В коаксиале используется топология «шина», обрыв кабеля лишает связи весь сегмент);
- минимально допустимый радиус изгиба меньше;
- большая помехоустойчивость из-за использования дифференциального сигнала;
- возможность питания по кабелю маломощных узлов, например IP-телефонов (стандарт Power over Ethernet, POE);
- гальваническая развязка трансформаторного типа. При использовании коаксиального кабеля в российских условиях, где, как правило, отсутствует заземление компьютеров, применение коаксиального кабеля часто сопровождалось пробоем сетевых карт и иногда даже полным «выгоранием» системного блока.

Причиной перехода на оптический кабель была необходимость увеличить длину сегмента без повторителей.

Типы:

- Классический Ethernet
 - ☐ Разделяемая среда
 - ☐ Ethernet – Gigabit Ethernet
- Коммутируемый Ethernet
 - ☐ Точка-точка
 - ☐ Появился в Fast Ethernet
 - ☐ Единственный вариант в 10G Ethernet

Классический Ethernet

- Исторически появился самый первый
 - Общая шина – коаксиальный кабель
- Проблема общей шины:
- Полный отказ сети в случае:
 - Поломки сетевого адаптера
 - Проблемы с кабелем
 - Неисправности коннекторов или терминаторов
 - Сложность диагностики
 - Сложность монтажа

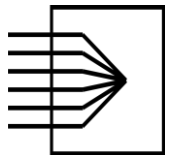
Коннектор - настроенное соединение между почтовыми серверами в различных группах маршрутизации или почтовых системах.

Терминатор — поглотитель энергии (обычно резистор) на конце длинной линии, сопротивление которого равно волновому сопротивлению данной линии.

Коаксиальный кабель => Витая пара => Использование концентраторов

Концентратор (hub) – устройство для создания сетей Ethernet на основе витой пары

- Физическая топология – звезда
- Логическая топология – общая шина
- Работают на физическом уровне
- Соединяют в единую среду кабели, идущие по всем портам
- Данные, поступающие на порт концентратора, передаются на все другие порты, не зависимо от адреса назначения



Характеристики концентраторов:

- **Количество портов** — разъемов для подключения сетевых линий, обычно выпускаются концентраторы с 4, 5, 6, 8, 12, 16, 24 и 48 портами (наиболее популярны с 4, 8 и 16).
- **Скорость передачи данных** — измеряется в Мбит/с, выпускаются концентраторы со скоростью 10 и/или 100 Мбит/с. Скорость может переключаться как автоматически (на наименьшую из используемых), так и с помощью перемычек или переключателей.
- Наличие портов для подключения кабелей Ethernet других типов — коаксиальных или оптических.

Преимущества концентраторов:

- Выше надежность:
 - ☐ Сеть не перестает работать при однократном сбое
- Удобство диагностики:
 - ☐ Сразу можно определить, какой компьютер/кабель вызвал проблемы
- Удобство монтажа
- Возможность использования существующей витой пары (телефонной проводки)
- Дешевизна

Недостатки:

- снижение пропускной способности сети по мере увеличения числа узлов
- поскольку на канальном уровне узлы не изолированы друг от друга, все они будут работать со скоростью передачи данных самого худшего узла
- низкий уровень безопасности (вещание на все порты)

Тест целостности соединения (Link Integrity Test, LIT) – проверка состояния соединения на витой паре

- Каждые 16 мс отправляются импульсы длительностью 100 нс
 - Если порт не используется
- Если получатель принимает импульсы, он считает, что соединение работает
 - Подтверждается светом зеленого светодиода

Типы классического Ethernet

Название	Тип	Максимальная длина сегмента	Узлов на сегмент	Преимущества
10Base5	Толстый коаксиальный	500 м	100	Первый кабель; ныне устарел
10Base2	Тонкий коаксиальный	185 м	30	Не нужны концентраторы
10Base-T	Витая пара	100 м	1024	Низкая цена
10Base-F	Оптоволокно	2000 м	1024	Лучший вариант при прокладке между зданиями

➤ Расшифровка названий:

- 10 – Максимальная скорость 10Мб/с
- Base – технология передачи Baseband, без модуляции (с модуляцией BROAD)
- 5, 2 – округленная максимальная длина сегмента (500 м и 185 м)
- T – тип кабеля витая пара (twisted pair)
- F – тип кабеля оптический (fiber optic)

■ Физический уровень Ethernet :

- ☐ Коаксиальный кабель
- ☐ Витая пара
- ☐ Оптоволокно

■ Канальный уровень Ethernet :

- ☐ Методы доступа и протоколы, одинаковые для любой среды передачи данных
- ☐ В классическом Ethernet смешаны подуровни LLC и MAC

Стандарты:

- Первый вариант – экспериментальная реализация Ethernet в Xerox
- Ethernet II (Ethernet DIX) – фирменный стандарт Ethernet компаний DEC, Intel, Xerox
- IEEE 802.3 – юридический стандарт Ethernet

Стандарты Ethernet II и IEEE 802.3 незначительно отличаются друг от друга.

Формат кадра

6 байт	6 байт	2 байта	46-1500 байт	4 байта
Адрес получателя	Адрес отправителя	Тип	Данные	Контрольная сумма

Заголовок

Концевик

Поле Тип:

- Содержит условный код протокола верхнего уровня:

- ☐ 0800 – IPv4
- ☐ 86DD – IPv6
- ☐ 0806 – ARP

- Используется для реализации мультиплексирования и демultipлексирования

Поле Данные:

- Содержит данные, полученные от протокола верхнего уровня
- Максимальная длина 1500 байт
 - ☐ Выбрана разработчиками Ethernet
 - ☐ Ограничение на размер памяти для буфера
 - ☐ Существует расширение Jumbo Frame
- Минимальная длина 46 байт
 - ☐ Ограничение технологии Ethernet

Контрольная сумма:

- Используется для обнаружения ошибок при передаче кадра по сети
- Вычисляется по алгоритму CRC-32 (Cyclic Redundancy Check)
- При обнаружении ошибки кадр отбрасывается
- Исправления ошибок или перезапросов неправильного кадра нет

Классический Ethernet использует метод доступа к среде

CSMA/CD

- Carrier Sense Multiple Access with Collision Detection
- Множественный доступ с прослушиванием несущей частоты и распознаванием коллизий
- Чтобы избежать коллизий, компьютеры должны передавать данные только тогда, когда среда не используется
- Способ определить, свободна ли среда – прослушивание основной гармонике сигнала (несущей частоты):
 - Несущая частота есть – среда занята
 - Несущей частоты нет – среда свободна
- Классический Ethernet использует манчестерское кодирование, несущая 5-10 МГц

Jumbo Frame - это сверхдлинные (огромные) Ethernet-кадры, которые используются в высокопроизводительных сетях для увеличения

производительности на длинных расстояниях, а также уменьшения нагрузки на центральный процессор. Jumbo-кадры имеют размер, превышающий стандартный размер: от 1500 до 16000 байт.

CRC-32 - алгоритм нахождения контрольной суммы, предназначенный для проверки целостности данных. CRC является практически приложением помехоустойчивого кодирования, основанном на определенных математических свойствах циклического кода.

Коллизия – искажение информации при одновременной передаче данных несколькими компьютерами.

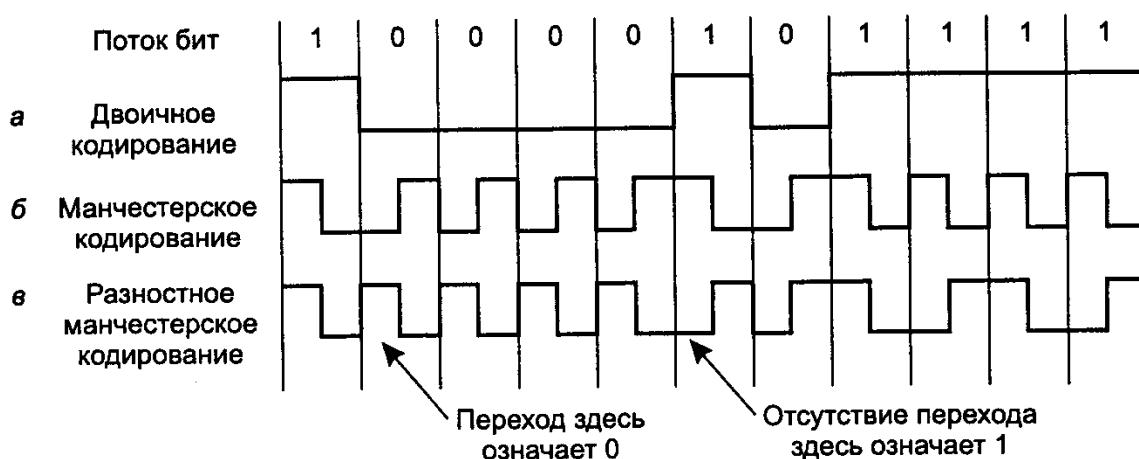
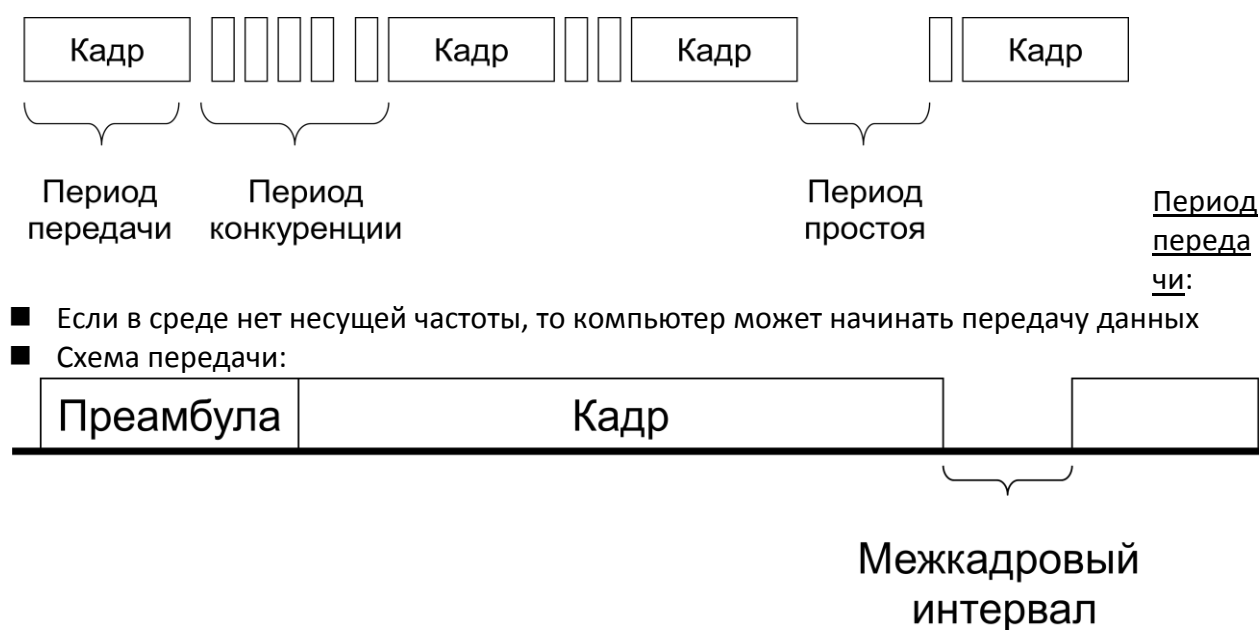


Рис. 4.15. Двоичное кодирование (а); манчестерское кодирование (б); разностное манчестерское кодирование (в)

Модель CSMA/CD



- **Преамбула:**
 - Служит для синхронизации приемника и передатчика
 - Формат преамбулы:
 - ☐ Длина 8 байт
 - ☐ Первые 7 байт: 10101010
 - ☐ Последний байт: 10101011 (ограничитель начала кадра)
- **Передача кадра**
 - После окончания преамбулы компьютер начинает передавать кадр
 - Все остальные компьютеры в сети начинают принимать кадр и записывают его в свой буфер
 - Первые 6 байт кадра содержат адрес получателя:
 - ☐ Компьютер, который узнал свой адрес, продолжает записывать кадр
 - ☐ Остальные удаляют кадр из буфера
- **Межкадровый интервал:**
 - После окончания передачи все компьютеры ждут в течение межкадрового интервала
 - ☐ 9,6 мкс в классическом Ethernet
 - Назначение межкадрового интервала:
 - ☐ Предотвратить монопольный захват канала
 - ☐ Приведение сетевых адаптеров в исходное состояние

Период конкуренции:

- После завершения межкадрового интервала компьютеры могут начать передачу
- Два компьютера начали передачу одновременно – коллизия
- Обнаружение коллизий:
 - ☐ Компьютер передает и принимает сигналы одновременно
 - ☐ Если принятый сигнал отличается от переданного – значит, возникла коллизия
- Jam-последовательность – передается компьютером при обнаружении коллизии для того, чтобы другие компьютеры легче ее распознали
- Если компьютер начал передавать данные и обнаружил коллизия, то он делает паузу
- Длительность паузы: $L * 512$ битовых интервалов

- Битовый интервал – время между появлениями двух последовательных битов данных
 - ☐ 0,1 мкс в классическом Ethernet
- L случайно выбирается из диапазона $[0, 2^N - 1]$
 - ☐ N – номер попытки
- Экспоненциальный двоичный алгоритм отсрочки
- Диапазоны L:
 - ☐ 1 попытка: $[0, 1]$
 - ☐ 2 попытка: $[0, 3]$
 - ☐ 5 попытка: $[0, 31]$
 - ☐ 10 попытка: $[0, 1023]$
- После 10 попыток интервал не увеличивается
- После 16 попыток передача прекращается
- Алгоритм хорошо работает, когда в сети мало компьютеров
- Если компьютеров много, то коллизии возникают чаще:
 - ☐ Растет число попыток передачи
 - ☐ Растет интервал L и длительность пауз
 - ☐ Экспоненциально увеличивается задержка
- Время оборота (round trip time) – время, за которое сигнал коллизии успевает дойти до самого дальнего узла
- Время оборота должно быть меньше, чем время передачи самого короткого кадра
- В противном случае:
 - ☐ Сигнал о коллизии может прийти уже после того, как компьютер завершил передачу кадра
 - ☐ Компьютер будет считать, что кадр передан, а на самом деле произошла коллизия
- Параметры Ethernet подобраны так, чтобы коллизии гарантированно распознавались
- Минимальная длина данных в кадре 46 байт
 - ☐ Если данных меньше, то они дополняются до 46 байт
- Максимальная длина сети 2500 м

Недостатки классического Ethernet

- Плохая масштабируемость:
 - ☐ Сеть становится неработоспособной при загрузке общей среды больше, чем на 30%
 - ☐ Работоспособное количество компьютеров - 30
- При увеличении скорости передачи уменьшается длина сети:
 - ☐ Сокращается время оборота
- Разное время доставки кадра:
 - ☐ Причина – коллизии
 - ☐ Плохо для трафика реального времени
- Низкая безопасность:
 - ☐ Данные в разделяемой среде доступны всем

12. Коммутируемый Ethernet. Использование коммутаторов. Алгоритм обратного обучения. Алгоритм прозрачного моста.

Типы:

- Классический Ethernet
 - ☐ Разделяемая среда
 - ☐ Ethernet – Gigabit Ethernet

- Коммутируемый Ethernet
 - ☐ Точка-точка
 - ☐ Появился в Fast Ethernet
 - ☐ Единственный вариант в 10G Ethernet

Недостатки классического Ethernet

- Плохая масштабируемость:
 - ☐ Сеть становится неработоспособной при загрузке общей среды больше, чем на 30%
 - ☐ Работоспособное количество компьютеров - 30
- При увеличении скорости передачи уменьшается длина сети:
 - ☐ Сокращается время оборота
- Разное время доставки кадра:
 - ☐ Причина – коллизии
 - ☐ Плохо для трафика реального времени
- Низкая безопасность:
 - ☐ Данные в разделяемой среде доступны всем

Пути развития Ethernet

- Сохранение метода CSMA/CD
 - ☐ Увеличение скорости
 - ☐ Добавление коммутируемого Ethernet
 - ☐ Результат: FastEthernet (IEEE 802.3u)
 - Усовершенствование метода доступа к разделяемой среде:
 - ☐ Приоритетный доступ по требованию
 - ☐ Разработчики: HP и AT&T
 - ☐ Результат: 100VG-AnyLAN (IEEE 802.12)
 - ☐ Не используется на практике
- Причина проблем классического Ethernet – разделяемая среда передачи данных
- Чтобы решить проблемы – нужно перейти от разделяемой среды к соединениям точка-точка
- Для этого применяются специальные устройства – **коммутаторы (switch)**

Коммутатор (switch) — устройство, предназначенное для соединения нескольких узлов компьютерной сети в пределах одного или нескольких сегментов сети.

Сравнение концентратора и коммутатора

- | | | |
|---|--|---|
| <ul style="list-style-type: none"> ■ Концентратор работает на физическом уровне <ul style="list-style-type: none"> ○ Выполняет электрическое соединение ○ Не вникает в содержание кадров ■ Коммутатор работает на канальном уровне: <ul style="list-style-type: none"> ○ Анализирует содержимое кадров ○ Извлекает адрес получателя ○ Передает кадр только одному получателю | <ul style="list-style-type: none"> ■ Концентратор (hub)  <ul style="list-style-type: none"> ■ Топология – общая шина ■ Физический уровень | <ul style="list-style-type: none"> ■ Коммутатор (switch)  <ul style="list-style-type: none"> ■ Полносвязная топология ■ Канальный уровень |
|---|--|---|

Алгоритм прозрачного моста

- **Мост** – устройство для объединения нескольких сетей
 - ☐ Предшественник коммутатора
 - ☐ Алгоритм прозрачного моста (объединяют сети с едиными протоколами канального и физического уровней модели OSI)

- Прозрачный мост:
 - ☐ Не заметен для сетевых устройств
 - ☐ Не требует настройки
- Коммутатор:
 - ☐ Мост с большим количеством портов
 - ☐ Алгоритм работы как у моста
- Порты коммутатора не имеют своих MAC-адресов
 - ☐ Коммутатор принимает все пакеты, поступающие на порт
 - ☐ Маршрутизаторы такие адреса имеют
- Коммутатор знает, какие MAC-адреса к какому компьютеру подключены
- **Таблица коммутации** содержит данные о доступности MAC-адресов через порты коммутатора
- Типы записей в таблице коммутации:
 - ☐ Статические – создаются вручную администраторами
 - ☐ Динамические – создаются автоматически
- Коммутатор получает кадр на порт с номером N и читает MAC-адрес получателя
- Коммутатор проверяет, есть ли MAC-адрес в таблице коммутации
- Если адрес есть, то коммутатор пересылает кадр на тот порт, через который доступен данный адрес
- Если адреса нет, то коммутатор передает кадр на все порты, кроме N

Порт коммутатора	MAC-адрес
1	1C-75-08-D2-49-45
2	00-02-B3-A7-49-D1
3	00-04-AC-85-E7-03

Алгоритм обратного обучения (backward learning):

- ❖ применяется для определения наилучшего пути пакетов от источника к приёмнику
- ❖ Коммутатор принимает все кадры, поступающие на порт
- ❖ По адресу отправителя в кадре коммутатор узнает, какие компьютеры подключены к порту
- ❖ Каждый узел берет только нужную информацию из полученных пакетов. Таким образом, каждый узел знает отправителя пакетов и количество хопов(транзитивных участков – участков между двумя узлами, по которым передаются данные), которые этот пакет прошёл. Затем происходит сравнение с данными в таблице маршрутизации, и если у полученного пакета меньшее количество хопов, то происходит обновление таблицы.
- К каждому порту коммутатора подключен только один компьютер/коммутатор
- Режим работы:
 - Полный дуплекс – коллизии не возникают
 - Полудуплекс – коллизия может возникнуть, если компьютер и коммутатор одновременно решат передавать данные
- К порту коммутатора может быть подключен концентратор

- Общая среда передачи, подключенная к порту коммутатора
- Коллизии возникают, как в классическом Ethernet

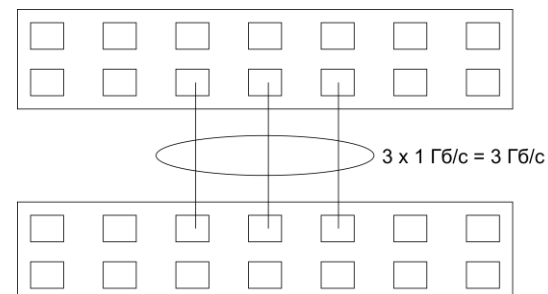
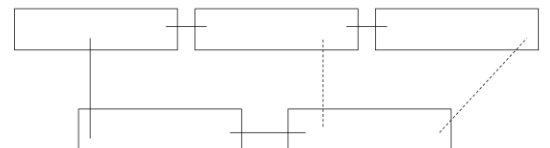
Типы коммутации

- Сквозная (напролет, в реальном времени, on the fly)
 - Коммутатор начинает принимать кадр на одном из портов
 - Приняв первые 6 байт кадра, коммутатор определяет адрес получателя
 - Если порт получателя свободен, коммутатор сразу начинает передавать данные получателю
 - Преимущество: высокая скорость
- С промежуточной буферизацией (с запоминанием, store-and-forward)
 - Если порт получателя занят, коммутатор записывает кадр во внутренний буфер
 - После того, как порт получателя освободится, кадр пересылается из буфера
 - Недостаток: задержка при передаче кадра
 - Преимущество: работает, даже если порт получателя занят
- Параллельная коммутация
 - Коммутатор может передавать данные на разные порты параллельно, предоставляя каждому компьютеру выделенную пропускную способность канала
 - Существенно повышает производительность работы сети

Дополнительные функции коммутаторов:

- Виртуальные локальные сети (VLAN)
 - Виртуальные локальные сети (Virtual local area networks, VLAN) – технология разделения единой сети на несколько логических сетей, изолированных друг от друга
 - Типы VLAN:
 - На основе коммутатора (нетеггированные)
 - Теггированные
- Связующее дерево (Spaning Tree)
 - Надежность:
 - Случайно достали/Сломался кабель
 - Сломался порт
 - Сломался коммутатор
 - Недостатки:
 - Ethernet не допускает нескольких соединений
 - Кадры будут бесконечно переходить из коммутатора в коммутатор
- Агрегация каналов
 - технологии объединения нескольких параллельных каналов передачи данных в один логический.
 - это позволяет увеличить пропускную способность каналов и повысить их надежность.

■ Spaning Tree – технология автоматического отключения дублирующих путей



13. Wi-Fi. Метод доступа к среде CSMA/CA.

- Wi-Fi – технология беспроводных локальных сетей
 - Wi-Fi – торговая марка (принадлежит Wi-Fi Alliance)
 - Стандарт IEEE 802.11
- Никак не расширяется

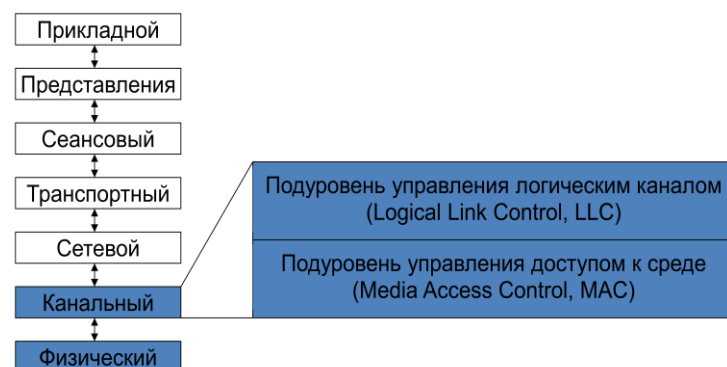
с. Игра слов с Hi-Fi

d. Ранее «Wireless Fidelity»

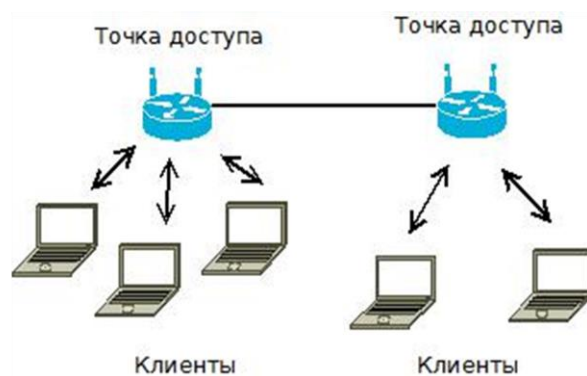
- Обычно схема Wi-Fi сети содержит не менее одной точки доступа и не менее одного клиента.
- Также возможно подключение двух клиентов в режиме точка-точка (Ad-hoc), когда точка доступа не используется, а клиенты соединяются посредством сетевых адаптеров «напрямую».
- Точка доступа передаёт свой идентификатор сети (SSID) с помощью специальных сигнальных пакетов на скорости 0,1 Мбит/с каждые 100 мс. Поэтому 0,1 Мбит/с — наименьшая скорость передачи данных для Wi-Fi.
- Зная SSID сети, клиент может выяснить, возможно ли подключение к данной точке доступа. При попадании в зону действия двух точек доступа с идентичными SSID приёмник может выбирать между ними на основании данных об уровне сигнала.
- Стандарт Wi-Fi даёт клиенту полную свободу при выборе критериев для соединения.

Место Wi-Fi в модели OSI

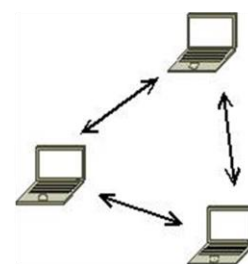
- Физический уровень – способ передачи сигналов
 - ☐ 5 стандартов IEEE серии 802.11
- Уровень MAC – способ доступа к общей среде:
 - ☐ Один общий способ для всех 5 вариантов физического уровня
- Уровень LLC – передача данных
 - ☐ Один общий способ



Архитектура Wi-Fi



Инфраструктурный режим



Произвольный режим
(ad hoc)

Существует два основных способа организации беспроводной сети – это клиент-сервер (Infrastructure Mode) и точка-точка (Ad-hoc).

- В первом случае сеть состоит из одной или нескольких точек доступа и произвольного количества клиентов. Это стандартная модель построения локальной сети, которая принципиально отличается от проводной разве что отсутствием тех самых проводов.

- Во втором случае связь устанавливается непосредственно между несколькими клиентами, минуя точку доступа. Такая модель удобна для соединения между собой нескольких портативных устройств, например, для моментальной печати фотографий с Wi-Fi-камеры на Wi-Fi-принтер или многопользовательской игры на портативных консолях (Sony PSP, Nintendo DS и других).

Wi-Fi и Ethernet

- Wi-Fi похожа на технологию Ethernet
- Адресация – MAC-адреса
- Разделяемая среда:
 - ☐ Ethernet – кабели
 - ☐ Wi-Fi – радиозфир
- Формат кадра уровня LLC

История развития

- Беспроводная сеть ALOHA
 - ☐ Разделяемая среда - радиозфир
- Проводная сеть Ethernet
 - ☐ Разделяемая среда - кабели

Стандарты физического уровня Wi-Fi

Название	Год принятия	Скорость
802.11	1997	1 и 2 Мб/с
802.11a	1999	54 Мб/с
802.11b	1999	11 Мб/с
802.11g	2003	54 Мб/с
802.11n	2009	600 Мб/с

- Коммутируемый Ethernet
 - ☐ Отказ от разделяемой среды
- Беспроводная сеть Wi-Fi
 - ☐ Разделяемая среда – радиозфир

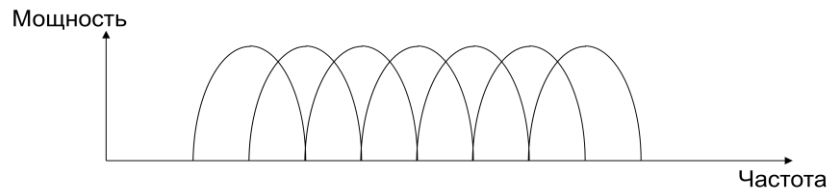
Физический уровень Wi-Fi

- Инфракрасное излучение
 - ☐ 802.11, устаревший метод
- Радиозфир:
 - ☐ 2,4 ГГц – 802.11b, 802.11g, 802.11n

- ☐ 5 ГГц – 802.11a
- Диапазоны 2,4 и 5 ГГц не требуют лицензирования
 - ☐ Можно использовать свободно
 - ☐ Другие устройства также используют этот диапазон и создают помехи

Представление сигнала

- Современные стандарты Wi-Fi используют метод OFMD:
 - ☐ Orthogonal Frequency Division Multiplexing
 - ☐ Мультиплексирование с ортогональным частотным разделением



- Данные передаются параллельно на разных частотах

Адаптация скорости

- Wi-Fi позволяет менять скорость при разном уровне сигнала:
 - ☐ Высокий уровень – скорость увеличивается
 - ☐ Низкий уровень – скорость уменьшается
- Адаптация скорости реализуется за счет изменения числа и ширины гармоник сигнала

Уровень MAC в Wi-Fi

- Wi-Fi использует разделяемую среду передачи данных
 - ☐ Возможны коллизии
- Задача уровня MAC в Wi-Fi:
 - ☐ Обеспечить доступ к разделяемой среде только одного компьютера в каждый момент времени
 - ☐ Безопасность передачи данных

Особенности беспроводной связи

- Вероятность ошибки передачи выше, чем в проводной среде
- Мощность передаваемого сигнала намного выше, чем принимаемого
- Ограниченный диапазон распространения сигнала – не все компьютеры в сети получают данные

Проблема «скрытой станции»

- Станция В находится в зоне досягаемости станций А и С, однако расстояние между станциями А и С настолько велико, что ни одна из них не попадает в зону покрытия другой и не в состоянии определить, производит ли передачу другая.

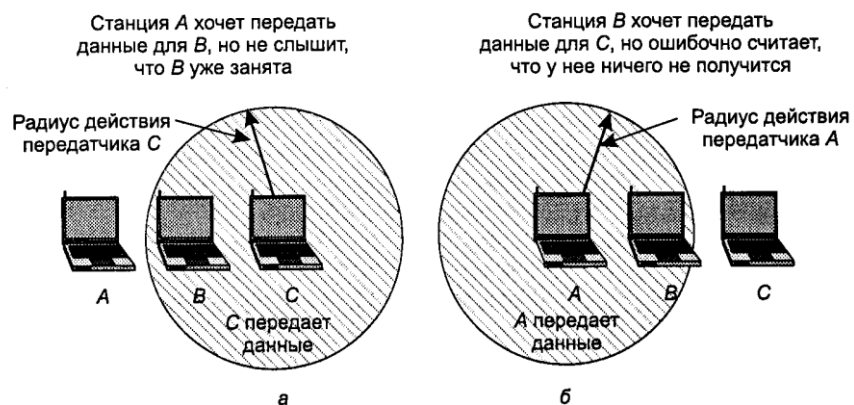


Рис. 4.23. Проблема скрытой станции (а); проблема засвеченной станции (б)

- Станция А выполняет передачу данных станции В.
- Станция С, используя метод многостанционного доступа с контролем несущей и обнаружении коллизий (англ. Carrier Sense Multiple Access with Collision Detection - CSMA/CD), определяет, что эфир свободен, после чего также начинает передавать данные станции В. Таким образом, возникает коллизия.
- Обе станции передают пакеты данных на станцию В до их завершения, не зная, что эти пакеты не могут быть корректно приняты. Фактически, происходит двойная трата ресурсов. Во-первых, возникает конфликт - коллизия данных. Во-вторых, теряется

время передачи всего пакета. В таких случаях говорят, что станция С скрыта для станции А.

Проблема «засвеченной станции»

- В случае, когда передачу ведет узел В, узел С может решить, что начало передачи сообщения узлу D не возможно, так как в зоне С детектируется излучение станции В.

Обнаружение коллизий

- Ethernet
 - ☐ Компьютер передает и одновременно принимает сигнал, если они не совпадают - коллизия
 - ☐ Jam-последовательность для усугубления коллизии
- Wi-Fi
 - ☐ Передаваемый сигнал намного мощнее принимаемого
 - ☐ Проблемы «Скрытой» и «засвеченной» станции
 - ☐ Сигнал о коллизии может не дойти до всех компьютеров

Обнаружение коллизии и ошибок в Wi-Fi

- Wi-Fi использует подтверждение доставки кадра:
 - ☐ Обнаружение коллизий
 - ☐ Обнаружение ошибок
- При отсутствии подтверждения кадр пересылается повторно

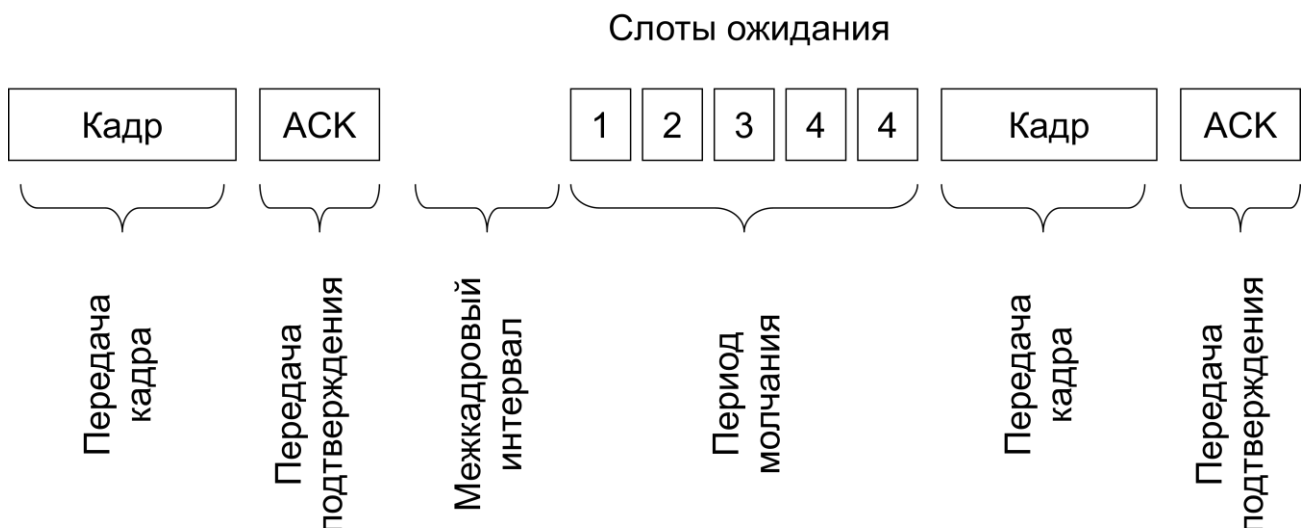
Коллизия в Wi-Fi

- Коллизии в Ethernet дешевы:
 - ☐ Обнаруживаются сразу после возникновения
 - ☐ Все компьютеры в сети информируются о коллизии с помощью Jam-последовательности
- Коллизия в Wi-Fi обходится очень дорого:
 - ☐ Обнаруживается по отсутствию подтверждения
 - ☐ Временные затраты: передача кадра, тайм-аут ожидания подтверждения
- Вывод: коллизий в Wi-Fi следует избегать

Метод доступа к среде

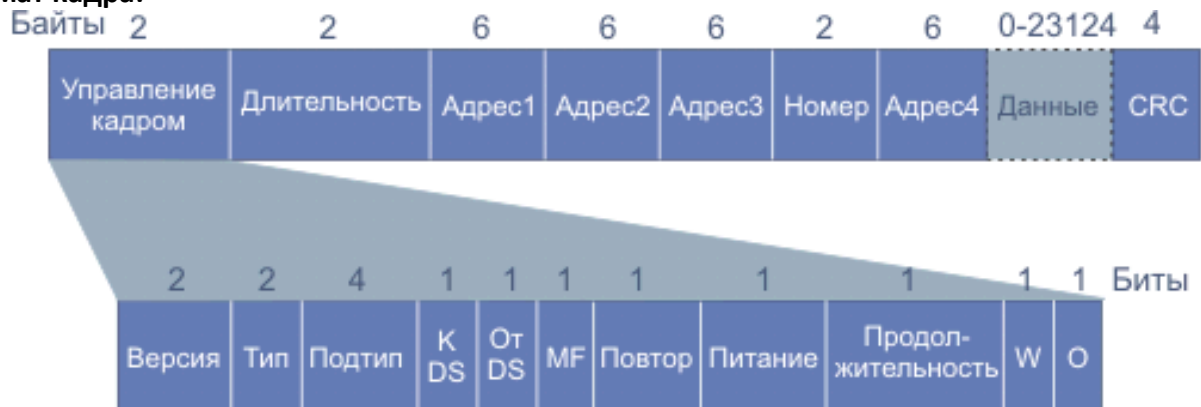
- Метод доступа к среде в Ethernet:
 - ☐ CSMA/CD - Множественный доступ с прослушиванием несущей частоты и распознаванием коллизий
- Метод доступа к среде в Wi-Fi:
 - ☐ **CSMA/CA** - Множественный доступ с прослушиванием несущей частоты с предотвращением коллизий

Модель CSMA/CA



- В Wi-Fi компьютеры прослушивают несущую чтобы определить, свободен ли канал
- Период передачи состоит из двух частей:
 - ☐ Передача кадра
 - ☐ Передача подтверждения
- После завершения передачи и межкадрового интервала компьютеры в Wi-Fi начинают период молчания:
 - ☐ Слот ожидания - промежуток времени фиксированной длины
 - ☐ Количество слотов ожидания компьютеры выбирают случайным образом
- Начинает передачу тот компьютер, который выбрал наименьшее число слотов ожидания
- Компьютер передает кадр и ожидает подтверждения
- Если подтверждение не пришло:
 - ☐ Произошла ошибка
 - ☐ Произошла коллизия
- Производится повторная передача кадра
 - ☐ Время ожидания увеличивается экспоненциально с каждой новой попыткой (как в Ethernet)

Формат кадра:



- **Поле управления кадром** имеет 11 субполей.
 - **Субполе версия протокола** позволяет двум протоколам работать в пределах одной ячейки.
 - Поле **тип** задает разновидность кадра (информационный, служебный или управляющий).
 - **Подтип** (RTS, CTS или ACK).
 - **Биты к DS и от DS** указывают на направление транспортировки кадра: к межсетевой системе (например, Ethernet()) или от нее.
 - Бит **MF** указывает на то, что далее следует еще один фрагмент.
 - Бит **повтор** отмечает повторно посылаемый фрагмент.
 - Бит **управление питанием** используется базовой станцией для переключения в режим пониженного энергопотребления или для выхода из этого режима.
 - Бит **продолжение** говорит о том, что у отправителя имеются еще кадры для пересылки.
 - **Бит W** является указателем использования шифрования в теле кадра согласно алгоритму WEP (Wired Equivalent Protocol).
 - **Однобитовое поле O** сообщает приемнику, что кадры с этим битом (=1) должны обрабатываться строго по порядку.
- Поле **длительность** задает время передачи кадра и его подтверждения.
- **Заголовок содержит четыре адреса.** Это адрес отправителя и получателя, а также адреса ячейки отправителя и места назначения. Поле **номер** служит для нумерации

фрагментов. Из 16 бит номера 12 идентифицируют кадр, а 4 - фрагмент. Управляющие кадры имеют сходный формат, только там отсутствуют поля базовых станций, так как эти кадры не покидают пределов сотовой ячейки. В служебных кадрах отсутствуют поля *данные и номер*, ключевым здесь является содержимое поля *субтип* (RTS, CTS или ACK).

Сервисы Wi-Fi

- Ассоциация
 - ☐ Подключение компьютера к точке доступа
- Аутентификация
 - ☐ Проверка права передачи данных
- Доставка данных
- Служба распределения
 - ☐ Выбор способа доставки: беспроводная или проводная сеть
- Служба конфиденциальности
- Ассоциация
 - ☐ Подключение компьютера к точке доступа
- Аутентификация
 - ☐ Проверка права передачи данных
- Доставка данных
- Служба распределения
 - ☐ Выбор способа доставки: беспроводная или проводная сеть
- Служба конфиденциальности

Безопасность:

- Wired Equivalent Privacy (WEP) – первоначальная схема, высокая уязвимость
Слабые места:
 - ☐ механизмы обмена ключами и проверки целостности данных
 - ☐ малая разрядность ключа и вектора инициализации (*Initialization vector*),
 - ☐ способ аутентификации
 - ☐ алгоритм шифрования
- Wi-Fi Protected Access (WPA) – временная улучшенная схема
 - ☐ усовершенствованная схема шифрования [RC4](#)
 - ☐ обязательная аутентификация с использованием EAP.
 - ☐ система централизованного управления безопасностью, возможность использования в действующих корпоративных политиках безопасности.
- Wi-Fi Protected Access 2 (WPA2):
 - ☐ Используется сейчас
 - ☐ Стандарт 802.11i
 - ☐ Шифрование на основе AES (симметричный алгоритм блочного шифрования)

14. Технологии канального уровня (обзор).

1) Ethernet

История создания и развития

- Первая сеть на разделяемой среде: радиосеть ALOHA, Гавайский университет
- Роберт Меткалф изучал ALOHA в аспирантуре
- Технология Ethernet была разработана вместе со многими первыми проектами корпорации Xerox PARC. Общепринято считать, что Ethernet был изобретён **22 мая 1973 года**, когда **Роберт Меткалф** составил докладную записку для главы PARC о

потенциале технологии Ethernet. Но законное право на технологию Меткалф получил через несколько лет.

- **В 1976 году** он и его ассистент Дэвид Боггс (David Boggs) **издали брошюру** под названием «Ethernet: Distributed Packet-Switching For Local Computer Networks».
- **Меткалф ушёл из Xerox в 1979 году и основал компанию 3Com** для продвижения компьютеров и локальных вычислительных сетей (ЛВС). Ему удалось убедить DEC, Intel и Xerox работать совместно и **разработать стандарт Ethernet (DIX)**.
- Впервые этот стандарт был опубликован **30 сентября 1980 года**.
- 1982 г. Создан проект IEEE 802 для стандартизации Ethernet
- Он начал соперничество с двумя крупными запатентованными технологиями: token ring и ARCNET, —

которые вскоре были раздавлены под накатывающимися волнами продукции Ethernet. В процессе борьбы 3Com стала основной компанией в этой отрасли.

Типы:

- Классический Ethernet
 - ☐ Разделяемая среда
 - ☐ Ethernet – Gigabit Ethernet
- Коммутируемый Ethernet
 - ☐ Точка-точка
 - ☐ Появился в Fast Ethernet
 - ☐ Единственный вариант в 10G Ethernet

Типы Ethernet

Название	Скорость	Кабель	Стандарт
Ethernet	10 Мб/с	«Толстый», «тонкий» коаксиал, Витая пара	802.3
Fast Ethernet	100 Мб/с	Витая пара, оптика	802.3u
Gigabit Ethernet	1 Гб/с	Витая пара, оптика	802.3z, 802.3ab
10G Ethernet	10 Гб/с	Витая пара, оптика	802.3ae, 802.3an

Стандарты:

- Первый вариант – экспериментальная реализация Ethernet в Xerox
- Ethernet II (Ethernet DIX) – фирменный стандарт Ethernet компаний DEC, Intel, Xerox
- IEEE 802.3 – юридический стандарт Ethernet

Стандарты Ethernet II и IEEE 802.3 незначительно отличаются друг от друга.

Формат кадра

6 байт	6 байт	2 байта	46-1500 байт	4 байта
Адрес получателя	Адрес отправителя	Тип	Данные	Контрольная сумма

Заголовок

Концевик

Поле Тип:

- Содержит условный код протокола верхнего уровня:
 - ☐ 0800 – IPv4
 - ☐ 86DD – IPv6
 - ☐ 0806 – ARP
- Используется для реализации мультиплексирования и демultipлексирования

Поле Данные:

- Содержит данные, полученные от протокола верхнего уровня
- Максимальная длина 1500 байт
 - ☐ Выбрана разработчиками Ethernet
 - ☐ Ограничение на размер памяти для буфера
 - ☐ Существует расширение Jumbo Frame
- Минимальная длина 46 байт
 - ☐ Ограничение технологии Ethernet

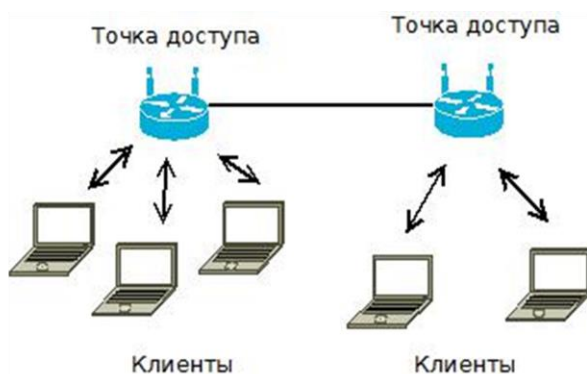
Контрольная сумма:

- Используется для обнаружения ошибок при передаче кадра по сети
- Вычисляется по алгоритму CRC-32 (Cyclic Redundancy Check)
- При обнаружении ошибки кадр отбрасывается
- Исправления ошибок или перезапросов неправильного кадра нет

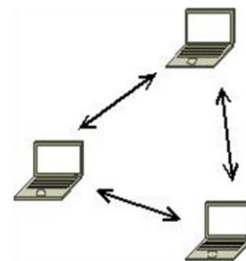
2) Wi-Fi

- Wi-Fi – технология беспроводных локальных сетей
 - e. Wi-Fi – торговая марка (принадлежит Wi-Fi Alliance)
 - f. Стандарт IEEE 802.11
- Никак не расшифровывается
 - g. Игра слов с Hi-Fi
 - h. Ранее «Wireless Fidelity»
- Обычно схема Wi-Fi сети содержит не менее одной точки доступа и не менее одного клиента.
- Также возможно подключение двух клиентов в режиме точка-точка (Ad-hoc), когда точка доступа не используется, а клиенты соединяются посредством сетевых адаптеров «напрямую».
- Точка доступа передаёт свой идентификатор сети (SSID) с помощью специальных сигнальных пакетов на скорости 0,1 Мбит/с каждые 100 мс. Поэтому 0,1 Мбит/с — наименьшая скорость передачи данных для Wi-Fi.
- Зная SSID сети, клиент может выяснить, возможно ли подключение к данной точке доступа. При попадании в зону действия двух точек доступа с идентичными SSID приёмник может выбирать между ними на основании данных об уровне сигнала.
- Стандарт Wi-Fi даёт клиенту полную свободу при выборе критериев для соединения.

Архитектура Wi-Fi



Инфраструктурный режим



Произвольный режим (ad hoc)

Существует два основных способа организации беспроводной сети – это клиент-сервер (Infrastructure Mode) и точка-точка (Ad-hoc).

- В первом случае сеть состоит из одной или нескольких точек доступа и произвольного количества клиентов. Это стандартная модель построения локальной сети, которая принципиально отличается от проводной разве что отсутствием тех самых проводов.
- Во втором случае связь устанавливается непосредственно между несколькими клиентами, минуя точку доступа. Такая модель удобна для соединения между собой нескольких портативных устройств, например, для моментальной печати фотографий с Wi-Fi-камеры на Wi-Fi-принтер или многопользовательской игры на портативных консолях (Sony PSP, Nintendo DS и других).

Формат кадра:



■ Поле **управления кадром** имеет 11 субполей.

- **Субполе версия протокола** позволяет двум протоколам работать в пределах одной ячейки.
- Поле **тип** задает разновидность кадра (информационный, служебный или управляющий).
- **Подтип** (RTS, CTS или ACK).
- **Биты к DS и от DS** указывают на направление транспортировки кадра: к межсетевой системе (например, Ethernet()) или от нее.

- Бит **MF** указывает на то, что далее следует еще один фрагмент.
- Бит **повтор** отмечает повторно посылаемый фрагмент.
- Бит **управление питанием** используется базовой станцией для переключения в режим пониженного энергопотребления или для выхода из этого режима.
- Бит **продолжение** говорит о том, что у отправителя имеются еще кадры для пересылки.
- Бит **W** является указателем использования шифрования в теле кадра согласно алгоритму WEP (Wired Equivalent Protocol).
- **Однобитовое поле O** сообщает приемнику, что кадры с этим битом (=1) должны обрабатываться строго по порядку.
- Поле **длительность** задает время передачи кадра и его подтверждение.
- **Заголовок содержит четыре адреса.** Это адрес отправителя и получателя, а также адреса ячейки отправителя и места назначения. **Поле номер** служит для нумерации фрагментов. Из 16 бит номера 12 идентифицируют кадр, а 4 - фрагмент. Управляющие кадры имеют сходный формат, только там отсутствуют поля базовых станций, так как эти кадры не покидают пределов сотовой ячейки. В служебных кадрах отсутствуют поля *данные и номер*, ключевым здесь является содержимое поля *субтип* (RTS, CTS или ACK).

Сервисы Wi-Fi

- Ассоциация
 - ☐ Подключение компьютера к точке доступа
- Аутентификация
 - ☐ Проверка права передачи данных
- Доставка данных
- Служба распределения
 - ☐ Выбор способа доставки: беспроводная или проводная сеть
- Служба конфиденциальности
- Ассоциация
 - ☐ Подключение компьютера к точке доступа
- Аутентификация
 - ☐ Проверка права передачи данных
- Доставка данных
- Служба распределения
 - ☐ Выбор способа доставки: беспроводная или проводная сеть
- Служба конфиденциальности

Безопасность:

- Wired Equivalent Privacy (WEP) – первоначальная схема, высокая уязвимость
Слабые места:
 - ☐ механизмы обмена ключами и проверки целостности данных
 - ☐ малая разрядность ключа и вектора инициализации (*Initialization vector*),
 - ☐ способ аутентификации
 - ☐ алгоритм шифрования
- Wi-Fi Protected Access (WPA) – временная улучшенная схема
 - ☐ усовершенствованная схема шифрования [RC4](#)
 - ☐ обязательная аутентификация с использованием EAP.
 - ☐ система централизованного управления безопасностью, возможность использования в действующих корпоративных политиках безопасности.
- Wi-Fi Protected Access 2 (WPA2):

- ☐ Используется сейчас
- ☐ Стандарт 802.11i
- ☐ Шифрование на основе AES (симметричный алгоритм блочного шифрования)

3) Token Ring

- Сеть Token-Ring была предложена фирмой IBM в 1985 году (первый вариант появился в 1980 году). Назначением Token-Ring было объединение в сеть всех типов компьютеров, выпускаемых IBM (от персональных до больших).
- Token-Ring является в настоящее время международным стандартом IEEE 802.5.
- Фирма IBM сделала все для максимально широкого распространения своей сети: была выпущена подробная документация вплоть до принципиальных схем адаптеров..
- По сравнению с аппаратурой Ethernet аппаратура Token-Ring оказывается заметно дороже, так как использует более сложные методы управления обменом, поэтому распространена сеть Token-Ring значительно меньше. Однако ее применение становится оправданным, когда требуются большие интенсивности обмена (например, при связи с большими компьютерами) и ограниченное время доступа.

Скорость передачи данных	4,16 Мбит/с
Количество станций в сегменте	260 (экранированная витая пара) 72 (неэкранированная витая пара)
Физическая топология	Звезда
Логическая топология	Кольцо

- В качестве среды передачи в сети IBM Token-Ring сначала применялась витая пара, но затем появились варианты аппаратуры для коаксиального кабеля, а также для оптоволоконного кабеля в стандарте FDDI. Витая пара применяется как неэкранированная (UTP), так и экранированная (STP).
- Основные технические характеристики сети Token-Ring следующие.
 - Максимальное количество концентраторов типа IBM 8228 MAU - 12.
 - Максимальное количество абонентов в сети - 96.
 - Максимальная длина кабеля между абонентом и концентратором — 45 м.
 - Максимальная длина кабеля между концентраторами -45м.
 - Максимальная длина кабеля, соединяющего все концентраторы - 120м.
 - Скорость передачи данных - 4 Мбит/с и 16 Мбит/с.
- В сети Token-Ring используется классический маркерный метод доступа, то есть по кольцу постоянно циркулирует маркер, к которому абоненты могут присоединять свои пакеты данных. Отсюда следует такое важное достоинство данной сети, как отсутствие конфликтов, но отсюда же следуют такие недостатки, как необходимость контроля за целостностью маркера и зависимость функционирования сети от каждого из абонентов (в случае неисправности абонент обязательно должен быть исключен из кольца).
- Для контроля за целостностью маркера используется один из абонентов (так называемый активный монитор). Его аппаратура ничем не отличается от остальных, но его программные средства следят за временными соотношениями в сети и формируют в случае необходимости новый маркер. Активный монитор выбирается при инициализации сети, им может быть любой компьютер сети. Если активный монитор по какой-то причине выходит из строя, то включается специальный механизм, посредством которого другие абоненты (запасные мониторы) принимают решение о назначении нового активного монитора.

- Маркер представляет собой управляющий пакет, содержащий всего три байта: байт начального разделителя (SD - Start Delimiter), байт управления доступом (AC - Access Control) и байт конечного разделителя (ED - End Delimiter).

Начальный разделитель (1 байт)	Управление доступом (1 байт)	Конечный разделитель (1 байт)
--------------------------------------	------------------------------------	-------------------------------------

Формат пакета Token-Ring.



Назначение полей пакета следующее:

- ☐ Начальный разделитель (SD) является признаком начала пакета.
- ☐ Байт управления доступом (AC) имеет то же назначение, что и в маркере.
- ☐ Байт управления пакетом (FC - Frame Control) определяет тип пакета (кадра).
- ☐ Шестибайтовые адреса отправителя и получателя пакета имеют стандартный формат, описанный в разделе 3.2.
- ☐ Поле данных включает в себя передаваемую информацию или информацию управления обменом.
- ☐ Поле контрольной суммы представляет собой 32-разрядную циклическую контрольную сумму пакета (CRC).
- ☐ Конечный разделитель является признаком конца пакета. Кроме того, он определяет, является ли данный пакет промежуточным или заключительным в последовательности передаваемых пакетов, а также содержит признак ошибочности пакета (для этого выделены специальные биты).
- ☐ Байт состояния пакета говорит о том, что происходило с данным пакетом: был ли он принят и скопирован в память приемника. По нему отправитель пакета узнает, дошел ли пакет по назначению и без ошибок или его надо передавать заново.

4) FDDI

- Сеть FDDI (от английского Fiber Distributed Data Interface, оптоволоконный распределенный интерфейс данных) - это одна из новейших разработок стандартов локальных сетей. Стандарт FDDI, предложенный Американским национальным институтом стандартов ANSI (спецификация ANSI X3T9.5), изначально ориентировался на высокую скорость передачи (100 Мбит/с) и на применение перспективного оптоволоконного кабеля (длина волны света - 850 нм).
- Выбор оптоволоконной среды передачи определил такие преимущества новой сети, как **высокая помехозащищенность, максимальная секретность передачи информации и прекрасная гальваническая развязка абонентов**. Высокая скорость передачи, которая в случае оптоволоконного кабеля достигается гораздо проще, позволяет решать многие задачи, недоступные менее скоростным сетям, например, передачу изображений в реальном масштабе времени. Кроме того, оптоволоконный кабель легко решает проблему передачи данных на расстояние нескольких километров без ретрансляции, что позволяет строить гораздо большие по размерам

сети, охватывающие даже целые города и имеющие при этом все преимущества локальных сетей (в частности, низкий уровень ошибок). И хотя к настоящему времени аппаратура FDDI не получила еще широкого распространения, ее перспективы очень неплохие.

- За основу стандарта FDDI был взят метод маркерного доступа, предусмотренный международным стандартом IEEE 802.5 Token-Ring. Небольшие отличия от этого стандарта определяются необходимостью обеспечить высокую скорость передачи информации на большие расстояния. Топология сети FDDI - это кольцо, причем применяется два разнонаправленных оптоволоконных кабеля, что позволяет в принципе использовать полнодуплексную передачу информации с удвоенной эффективной скоростью в 200 Мбит/с (при этом каждый из двух каналов работает на скорости 100 Мбит/с). Применяется и звездно-кольцевая топология с концентраторами, включенными в кольцо.
- Основные технические характеристики сети FDDI следующие.
 - Максимальное количество абонентов сети — 1000.
 - Максимальная протяженность кольца сети - 20 км.
 - Максимальное расстояние между абонентами сети - 2 км.
 - Среда передачи - многомодовый оптоволоконный кабель (возможно применение электрической витой пары).
 - Метод доступа - маркерный.
 - Скорость передачи информации — 100 Мбит/с (200 Мбит/с для дуплексного режима передачи).
- В отличие от метода доступа, предлагаемого стандартом IEEE 802.5, в FDDI применяется так называемая множественная передача маркера. Если в случае сети Token-Ring новый (свободный) маркер передается абонентом только после возвращения к нему его пакета, то в FDDI новый маркер передается абонентом сразу же после окончания передачи им пакета. Последовательность действий здесь следующая.
 - 1) Абонент, желающий передавать, ждет маркера, который идет за каждым пакетом.
 - 2) Когда маркер пришел, абонент удаляет его из сети и передает свой пакет.
 - 3) Сразу после передачи пакета абонент посылает новый маркер.
- Форматы маркера и пакета сети FDDI несколько отличаются от форматов, используемых в сети Token-Ring.
- Назначение полей следующее.
 - Преамбула используется для синхронизации. Первоначально она содержит 64 бита, но абоненты, через которых проходит пакет, могут менять ее размер.
 - Начальный разделитель выполняет функцию признака начала кадра.

Формат маркера FDDI

Преамбула (8 байт)	Начальный разделитель (1 байт)	Управление (1 байт)	Конечный разделитель (1 байт)	Статус пакета (1 байт)
-----------------------	--------------------------------------	------------------------	-------------------------------------	------------------------------

- Адреса приемника и источника могут быть 6-байтовыми

(аналогично Ethernet и Token-Ring) или 2-байтовыми.

- Поле данных может быть переменной длины, но суммарная длина пакета не должна превышать 4500 байт.
- Поле контрольной суммы содержит 32-битную циклическую контрольную сумму пакета.

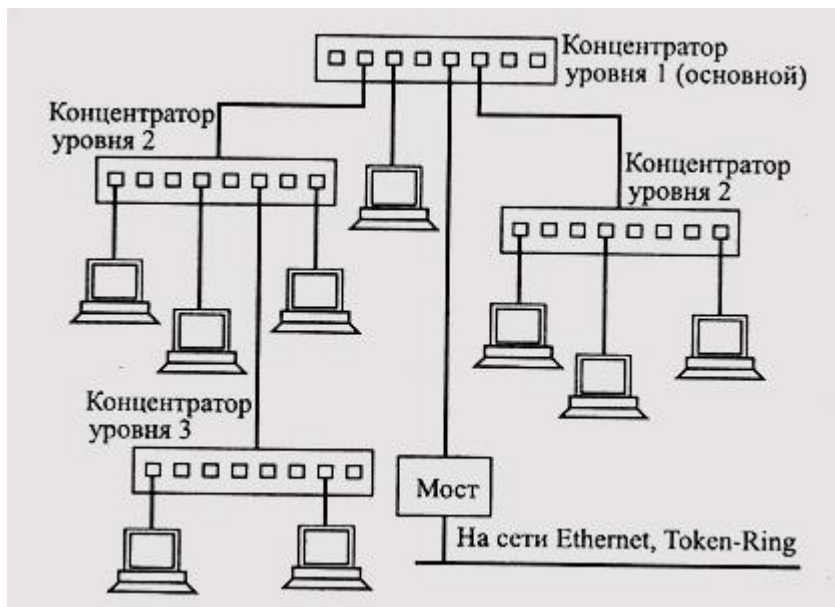
- Конечный разделитель определяет конец кадра.
- Байт состояния пакета включает в себя бит обнаружения ошибки, бит распознавания адреса и бит копирования (все аналогично Token-Ring).

Формат пакета FDDI



5) 100VG-AnyLAN

- Сеть IOOVG-AnyLAN - это одна из последних разработок высокоскоростных локальных сетей, недавно появившаяся на рынке. Она разработана фирмами Hewlett-Packard и IBM и соответствует стандарту IEEE 802.12, так что уровень ее стандартизации достаточно высокий. Главными достоинствами ее являются большая скорость обмена, сравнительно невысокая стоимость аппаратуры (примерно вдвое дороже по сравнению с наиболее популярной сетью Ethernet 10BASE-T), централизованный метод управления обменом без конфликтов и совместимость на уровне пакетов с популярными сетями Ethernet и Token-Ring. В названии сети цифра 100 соответствует скорости 100 Мбит/с, буквы VG обозначают дешевую витую пару категории 3 (Voice Grade), а AnyLAN (любая сеть) обозначает то, что сеть совместима с двумя самыми распространенными сетями.
- Основные технические характеристики сети IOOVG-AnyLAN следующие.
 - Скорость передачи - 100 Мбит/с.
 - Топология - звезда с возможностью наращивания.
 - Метод доступа - централизованный, бесконфликтный (Demand Priority - с запросом приоритета).
 - Среда передачи - счетверенная неэкранированная витая пара (кабели UTP категории 3,4 или 5), сдвоенная витая пара (кабель UTP категории 5), сдвоенная экранированная витая пара (STP), а также оптоволоконный кабель. Сейчас в основном распространена счетверенная витая пара.
 - Максимальная длина кабеля между концентратором и абонентом и между концентраторами - 100 м (для UTP кабеля категории 3), 150 м (для UTP кабеля категории 5 и экранированного кабеля), 2 км (для оптоволоконного кабеля).



концентраторами - 100 м (для UTP кабеля категории 3), 150 м (для UTP кабеля категории 5 и экранированного кабеля), 2 км (для оптоволоконного кабеля).

Структура сети 100VG-AnyLAN

- Сеть IOOVG-AnyLAN состоит из центрального (основного) концентратора уровня 1, к которому

могут подключаться как отдельные абоненты, так и концентраторы уровня 2, к которым в свою очередь подключаются абоненты и концентраторы уровня 3. При этом сеть может иметь не более трех таких уровней. Получается, что максимальный размер сети может составлять 600 метров для неэкранированной витой пары.

- В отличие от неинтеллектуальных концентраторов других сетей (например, Ethernet), концентраторы сети IOOVG-AnyLAN - это интеллектуальные контроллеры, которые управляют всем доступом к сети. Для этого они непрерывно контролируют запросы, поступающие на все порты. Концентраторы принимают все приходящие пакеты и отправляют их только тем абонентам, которым они адресованы. Однако никакой обработки информации они не производят, то есть в данном случае получается все-таки не настоящая (активная) звезда, но и не пассивная звезда.
- Каждый из концентраторов может быть настроен на работу с форматами пакетов Ethernet или пакетов Token-Ring. При этом концентраторы всей сети должны работать с пакетами только какого-нибудь одного формата. Для связи с сетями Ethernet и Token-Ring необходимы мосты, но мосты довольно простые.
- Концентраторы имеют один порт верхнего уровня (для присоединения его к концентратору более высокого уровня) и несколько портов нижнего уровня (для присоединения абонентов). В качестве абонента может выступать компьютер (рабочая станция), сервер, мост, маршрутизатор, коммутатор, а также другой концентратор.
- Каждый порт концентратора может быть установлен в один из двух возможных режимов работы.
 - Нормальный режим предполагает пересылку абоненту, присоединенному к порту, только о пакетов, адресованных лично ему.
 - Мониторный режим предполагает пересылку абоненту, присоединенному к порту, всех пакетов, приходящих на концентратор. Этот режим позволяет одному из абонентов контролировать работу всей сети в целом (выполнять функцию мониторинга).
- Метод доступа к сети IOOVG-AnyLAN довольно типичен для сетей с топологией «звезда» и состоит в следующем. Каждый желающий передавать абонент посылает концентратору свой запрос на передачу. Концентратор циклически прослушивает всех абонентов по очереди и дает право передачи абоненту, следующему по порядку за тем, который закончил передачу. То есть величина времени доступа гарантирована. Но этот простейший алгоритм усложнен в сети IOOVG-AnyLAN, так как запросы могут иметь два уровня приоритета:
 - нормальный уровень приоритета используется для обычных приложений;
 - высокий уровень приоритета используется для приложений, требующих быстрого обслуживания.
- Запросы с высоким уровнем приоритета обслуживаются раньше, чем запросы с нормальным приоритетом. Если приходит запрос высокого приоритета, то нормальный порядок обслуживания прерывается, и после окончания приема текущего пакета обслуживается запрос высокого приоритета. Если таких высокоприоритетных запросов несколько, то возврат к нормальной процедуре обслуживания происходит только после полной обработки всех этих запросов. При этом концентратор следит за тем, чтобы не была превышена установленная величина гарантированного времени доступа. Если высокоприоритетных запросов слишком много, то запросы с нормальным приоритетом автоматически переводятся им в ранг высокоприоритетных. Таким образом, даже низкоприоритетные запросы не будут ждать своей очереди слишком долго.

- Концентраторы более низких уровней также анализируют запросы абонентов, присоединенных к ним, и в случае необходимости пересылают их запросы к концентратору более высокого уровня. За один раз концентратор более низкого уровня может передать концентратору более высокого уровня не один пакет (как обычный абонент), а столько пакетов, сколько абонентов присоединено к нему.
- Интересно решена в сети IOOVG-AnyLAN проблема кодирования передаваемых данных. Вся передаваемая информация проходит следующие этапы обработки.
 - Разделение на квинтеты (группы по 5 бит).
 - Перемешивание, скремблирование (scrambling) полученных квинтетов.
 - Кодирование квинтетов специальным кодом 5B6B (этот код обеспечивает в выходной последовательности не более трех единиц или нулей подряд, что используется для детектирования ошибок).
 - Добавление начального и конечного разделителей кадра.
- В сети 100 VG-AnyLAN предусмотрены два режима обмена: полудуплексный и полнодуплексный.
 - При полудуплексном обмене все четыре витые пары используются для передачи одновременно в одном направлении (от абонента к концентратору или наоборот). Он используется для передачи пакетов.
 - При полнодуплексном обмене две витые пары передают в одном направлении, а две другие - в другом направлении. Он используется для передачи управляющих сигналов.

15.Сетевой уровень. Понятие «маршрутизация».

Согласование различий в сетях.

- Сетевой уровень (network layer) служит для образования единой транспортной системы, объединяющей несколько сетей (построенных на разных технологиях), называемой составной сетью, или интернетом.
- Предназначен для определения пути передачи данных.
- Сервисы сетевого уровня:

- a. Передача без установления соединения
 - Нет гарантии доставки
 - Протокол IP
- b. Передача с установлением соединения
 - Гарантия доставки данных
 - Гарантия нужного порядка получения
 - Использовалась в телефонных сетях

- Отвечает за
 - Объединение сетей
 - трансляцию логических адресов и имён в физические
 - определение кратчайших маршрутов,
 - коммутацию и маршрутизацию,
 - отслеживание неполадок и «заторов» в сети (качество обслуживания)
- Функции сетевого уровня реализуются:
 - группой протоколов;
 - специальными устройствами — **маршрутизаторами**.

Модель OSI

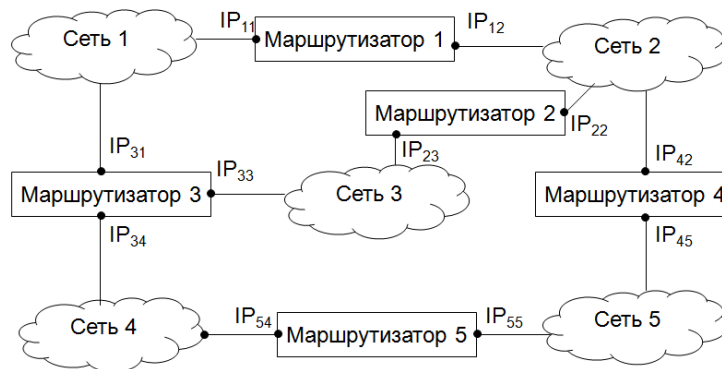
Прикладной
Представления
Сеансовый
Транспортный
Сетевой
Канальный
Физический

Модель TCP/IP

Прикладной
Транспортный
Сетевой
Сетевых интерфейсов

Маршрутизатор – устройство, объединяющее несколько сетей

- Умеет согласовывать различия в сетях
- Имеет несколько сетевых интерфейсов и адрес в каждой сети, к которой подключен



Объединение сетей

Различия сетей

- Сервис
 - ☐ С установлением соединения (WiMAX)
 - ☐ Без установления соединения (Ethernet)
 - ☐ Без установки соединения но с отправкой подтверждений (Wi-Fi)
- Адресация
 - ☐ Разный размер, плоская, иерархическая
 - ☐ MAC адрес в Ethernet, IMEI в 3G
- Широковещание
 - ☐ Поддерживается или нет
- Размер пакета (MTU):
 - ☐ Ethernet - 1500
 - ☐ WiFi - 2304

Согласование сетей

- Соединения
 - ☐ Маршрутизатор принимает пакеты без соединения, а для отправки устанавливает соединение
- Адресация:
 - ☐ Глобальные адреса (у узлов), не зависящие от конкретных технологий
 - ☐ Методы преобразования глобального адреса в локальный (ARP для TCP/IP)
- Широковещание:
 - ☐ Маршрутизатор отправляет пакеты всем хостам в сети по индивидуальным адресам

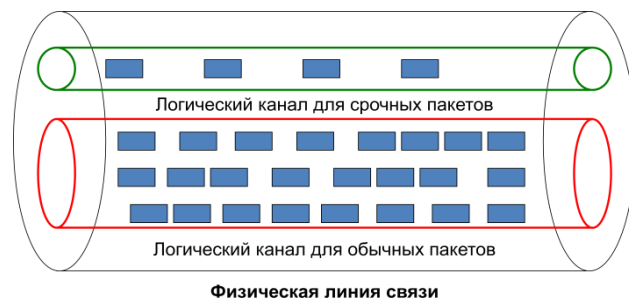
Маршрутизация

- Маршрутизация – поиск маршрута доставки пакета между сетями через транзитные узлы – маршрутизаторы
- Учет изменений в топологии сети
- Учет загрузки каналов связи и маршрутизаторов
- Маршрутизатор собирает информацию о топологии связей между сетями и на основе этой информации строит таблицы коммутации, которые в данном случае носят специальное название таблиц маршрутизации.

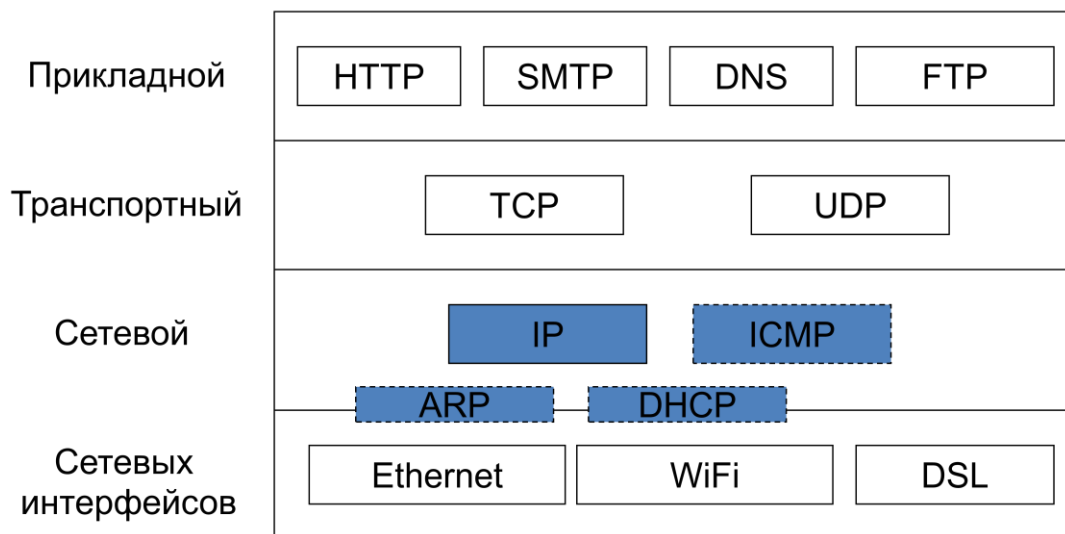
Качество обслуживания

- Параметры качества обслуживания:
 - ☐ Пропускная способность
 - ☐ Задержка

- ☐ Флуктуация (термин, характеризующий любое колебание или любое периодическое изменение)
- ☐ Потери
- Разным приложениям нужны разные параметры качества
- Разные сети могут предоставлять разное качество обслуживания
- Передача файлов:
 - ☐ Нужна высокая пропускная способность
 - ☐ Нельзя терять и искажать данные
 - ☐ Допускается задержка и флуктуация
- Аудио
 - ☐ Низкая пропускная способность
 - ☐ Допускаются потери пакетов
 - ☐ Требуется низкая задержка и флуктуация
- Подходы к обеспечению качества обслуживания
 - Диспетчеризация пакетов
 - Резервирование ресурсов
 - Интегральное обслуживание
 - RFC 2205-2212
 - Резервирование для потоковой передачи
 - Дифференцированное обслуживание (RFC 2474-75, Разбиение данных на классы)
 - Срочная пересылка
 - Два класса обслуживания:
 - Обычный
 - Срочный
 - Классы определяет отправляющий компьютер
 - Стандарт RFC 3246, маршрутизаторы поддерживают классы
- Гарантированная пересылка
 - RFC 2597
 - 12 классов обслуживания:
 - 4 приоритета
 - 3 класса игнорирования пакетов
 - Более совершенная схема, чем в срочной пересылке



Сетевой уровень в TCP/IP



- **IP** (Internet Protocol) – основной протокол сетевого уровня, обеспечивает передачу данных
- **ARP** (Address Resolution Protocol) – протокол определения локального адреса по глобальному
- **DHCP** (Dynamic Host Configuration Protocol) – протокол автоматического назначения IP-адресов компьютерам в сети
- **ICMP** (Internet Control Message Protocol) – управляющий протокол сетевого уровня

16. IP-адреса и IP-сети.

Типы адресов:

- Локальные адреса:
 - ☐ Адреса в технологии сетевого уровня
 - ☐ Пример: MAC адрес в Ethernet, IMEI в 3G
 - ☐ Привязаны к конкретной технологии
 - ☐ Не могут быть использованы в гетерогенных сетях
- Глобальные адреса:
 - ☐ Адреса сетевого уровня
 - ☐ Пример – IP-адреса
 - ☐ Не привязаны к технологии
 - ☐ Применяются при объединении сетей

IP-адреса:

- Глобальные адреса, используемые в стеке протоколов TCP/IP
- Используются для уникальной идентификации компьютеров в составной сети
- Широко используются в Интернет
- Две версии протокола IP:
 - ☐ IPv4: адрес 4 байта
 - ☐ IPv6: адрес 16 байт

Структура IP-адреса (IPv4)

- Длина – 4 байта, 32 бита
- Форма представления:
 - ☐ 4 десятичных числа 0-255, разделенных точками
 - ☐ Пример: 213.180.193.3

- Структура IP-адреса:
 - ☐ Номер сети
 - ☐ Номер компьютера в сети (хоста)
- Пример структуры:
 - ☐ IP-адрес: 213.180.193.3
 - ☐ Номер сети: 213.180.193.0
 - ☐ Номер хоста: 3 (0.0.0.3)

Классы IP-адресов

1. Первоначальный подход – разделение IP-адресов на классы

- В каждом классе жестко определено количество бит для номера сети и хоста
- Определены в стандарте RFC 791
- Использовался до 1993 г.
- Достоинства:
 - По IP-адресу можно точно узнать, где номер сети, а где – хоста
- Недостатки:
 - Фиксированное количество хостов в сети (254 – 65 тыс. – 16 млн.)
 - Неэффективное распределение IP-адресов
- Нехватка IP-адресов
 - Длина IP-адреса 32 бита
 - Максимум **4 294 967 296** IP-адресов
 - Используются не все адреса в сети

Классы IP-адресов

Класс	Пер- вые биты	Номер сети, бит	Диапазон сетей	Максимальное число сетей	Максималь- ное число хостов в сети
A	0	8	1.0.0.0 – 126.0.0.0	126	16 777 214
B	10	16	128.0.0.0 – 191.255.0.0	16 382	65 534
C	110	24	192.0.0.0 – 223.255.255.0	2 097 150	254
D	1110	-	224.0.0.0 – 239.255.255.255	Групповые адреса	
E	11110	-	240.0.0.0- 255.255.255.255	Зарезервировано	

Примечание: адреса класса D по-прежнему групповые, а адреса класса E по-прежнему зарезервированы (несмотря на недостаток IPv4 адресов).

2. Бесклассовая междоменная маршрутизация (Classless Inter Domain Routing, CIDR) – отказ от классов IP-адресов

- Появилась в 1993 г.
- Определена в стандарте RFC 1517-1520
- Используется сейчас
- Для определения номера сети применяются маски переменной длины
- Любое количество хостов в сети

Маска подсети:

- Маска подсети показывает, где в IP-адресе номер сети, а где хоста
- Структура маски:
 - ☐ Единицы в позициях, задающих номер сети
 - ☐ Нули в позициях, задающих номер хоста
- Способ получения номера сети:
 - ☐ Побитовое И маски и IP-адреса
- Пример вычисления адреса сети
 - ☐ IP-адрес: 213.180.193.3
 - ☐ Расчет в двоичном представлении

IP: 11010101.10110100.11000001.00000011
AND
Mask: 11111111.11111111.00000000.00000000
Net: 11010101.10110100.00000000.00000000

☐ Результат: 213.180.0.0

- Представление маски подсети
 - Десятичное представление:
 - IP-адрес: 213.180.193.3
 - Маска подсети: 255.255.255.0
 - Адрес сети: 213.180.193.0
 - В виде префикса:
 - 213.180.193.3 / 24
 - Адрес сети: 213.180.193.0
 - Оба представления эквивалентны

Распределение IP-адресов

- IP – адреса должны быть уникальны во всем мире
- Адреса распределяются специальной организацией – ICANN (Internet Corporation for Assigned Names and Numbers)
- Организации получают блоки IP-адресов и могут использовать по своему усмотрению

Специальные IP-адреса

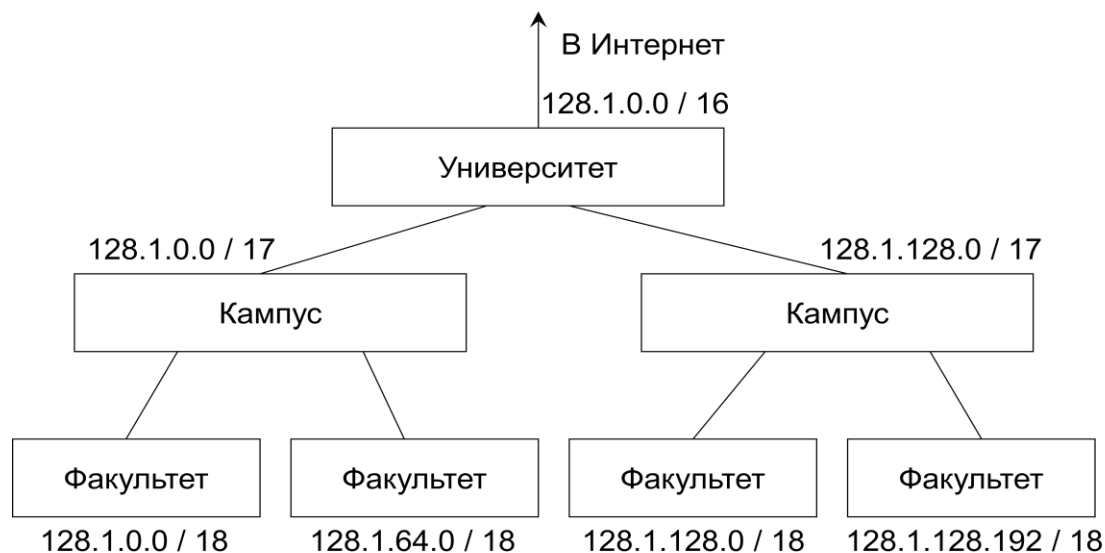
- В номере хоста нельзя использовать только битовые 0 или 1
- Битовые 0 в номере хоста:
 - Адрес сети: 213.180.0.0
- Битовые 1 в номере хоста:
 - Широковещательный адрес: 213.180.255.255
- Договоренность (не обязательная):
 - Хост с номером 1 – маршрутизатор по умолчанию (шлюз): 213.180.0.1
- 0.0.0.0 – текущий хост (сеть)
- 255.255.255.255 – все хосты в текущей сети
- 127.0.0.0 – обратная петля (loopback)
 - Сеть для тестирования
 - Данные не передаются в сеть, а приходят обратно
 - 127.0.0.1 – localhost (текущий компьютер)

Приватные адреса

- Зарезервированные диапазоны адресов:
 - ☐ 10.0.0.0 – 10.255.255.255 / 8
 - ☐ 172.16.0.0 – 172.31.255.255 / 12
 - ☐ 192.168.0.0 – 192.168.255.255 / 16
- Не маршрутизируются в Интернет
- Могут использоваться внутри организации без обращения в ICANN
- Подключение к Internet с использованием технологии NAT (Network Address Translation)

Подсети

- Организация, получив блок адресов в ICANN, может разбить его на части:
 - ☐ Интернет провайдер – выделение сетей для клиентов
 - ☐ Предприятие – сети отделов
- Разбиение осуществляется с использованием масок подсетей
- Пример:



17. Разрешение IP-адреса в MAC-адрес.

MAC-адреса

- Служат для идентификации сетевых интерфейсов узлов сети Ethernet
- Регламентированы стандартом IEEE 802.3
- Длина 6 байт (48 бит)
- Форма записи – шесть шестнадцатеричных чисел:
 - ☐ 1C-75-08-D2-49-45
 - ☐ 1C:75:08:D2:49:45

Типы MAC-адресов

- Индивидуальный (unicast):
 - ☐ 1C-75-08-D2-49-45
- Групповой (multicast, первый бит старшего байта адреса равен 1):
 - ☐ 80-00-A7-F0-00-00
- Широковещательный (broadcast, все 1):
 - ☐ FF-FF-FF-FF-FF-FF

Способы назначения MAC-адресов

- Централизованный (по умолчанию):
 - ☐ Адреса назначаются производителям оборудования
 - ☐ Правила назначения описываются стандартом IEEE 802
 - ☐ При централизованном назначении MAC-адреса должны быть уникальны во всем мире
 - ☐ Структура MAC-адреса:
 - Первые 3 байта – уникальный идентификатор организации (OUI), выдаются IEEE производителям оборудования
 - Последние 3 байта – назначает производитель оборудования, который отвечает за уникальность
 - ☐ Примеры OUI:
 - 00:00:0C – Cisco (еще есть 6C:50:4D, 70:81:05 и др.)
 - 00:02:B3 – Intel
 - 00:04:AC – IBM
- Локальный:
 - ☐ Адреса назначаются администратором сети
 - ☐ Администратор должен обеспечить уникальность
- Индикатор способа назначения - второй бит старшего байта MAC-адреса:
 - ☐ 0 – адрес назначен централизованно

- ☐ 1 – адрес назначен локально

Протокол ARP

- Address Resolution Protocol (ARP) – протокол разрешения адресов
- Задача ARP
 - ☐ По известному глобальному адресу (IP-адресу) найти локальный адрес (в технологии канального уровня)
- Типы ARP:
 - ☐ Для широковещательных сетей
 - ☐ Для глобальных сетей (без широковещания)

ARP в широковещательных сетях

- Схема работы:
 - ☐ Хост-отправитель рассылает широковещательный запрос «У кого адрес IP₁»
 - ☐ Все хосты получают широковещательный запрос
 - ☐ Хост с адресом IP₁ сообщает свой локальный адрес, остальные запрос игнорируют
 - ☐ Хост-отправитель получает ответ и извлекает из него локальный адрес
- Для Ethernet локальный адрес – MAC-адрес

Формат ARP-запроса

Поле	Значение
Тип сети	1
Тип протокола	2048
Длина локального адреса	6
Длина глобального адреса	4
Операция	1
Локальный адрес отправителя	1C:75:08:D2:49:45
Глобальный адрес отправителя	172.16.10.88
Локальный адрес получателя	00:00:00:00:00:00
Глобальный адрес получателя	172.16.10.253

Формат ARP-ответа

Поле	Значение
Тип сети	1
Тип протокола	2048
Длина локального адреса	6
Длина глобального адреса	4
Операция	2
Локальный адрес отправителя	00:1C:C5:34:B3:01
Глобальный адрес отправителя	172.16.10.253
Локальный адрес получателя	1C:75:08:D2:49:45
Глобальный адрес получателя	172.16.10.88

ARP-таблица

- Хост кэширует ответы ARP
 - ☐ Нет необходимости запрашивать MAC-адрес при каждом отправлении
- ARP-таблица хранит данные о соответствии MAC и IP-адресов

IP-адрес	MAC-адрес	Тип
172.16.10.253	00:1C:C5:34:B3:01	Динамический
172.16.10.88	1C:75:08:D2:49:45	Статический

- Типы записи в ARP-таблице
 - ☐ Динамические – создаются в результате рассылки ARP-запросов
 - ☐ Статические – создаются администраторами вручную
- Команды работы с ARP-таблицей:
 - ☐ arp -a – просмотр таблицы
 - ☐ arp -s – добавление статической записи

- ☐ arp -d – удаление записи

Срок жизни записей ARP

- Динамические записи в таблице ARP имеют срок действия
 - ☐ У компьютера может измениться IP-адрес
 - ☐ После истечения срока действия запись удаляется из таблицы ARP
- Добровольное ARP-сообщение (gratuitous ARP)
 - ☐ Отправка ARP-запроса со своим IP-адресом
 - ☐ Используется для сообщения о новом IP-адресе
 - ☐ Предотвращение назначения одинаковых IP

ARP в глобальных сетях

- В сетях, где нет широковещания, нельзя разослать запрос локального адреса всем компьютерам
 - ☐ Сеть IP поверх X.25
- Решение:
 - ☐ Таблицы, формируемые вручную администраторами
 - ☐ ARP-серверы – выделенные маршрутизаторы, ведущие ARP-таблицы

18. Протокол IPv4.

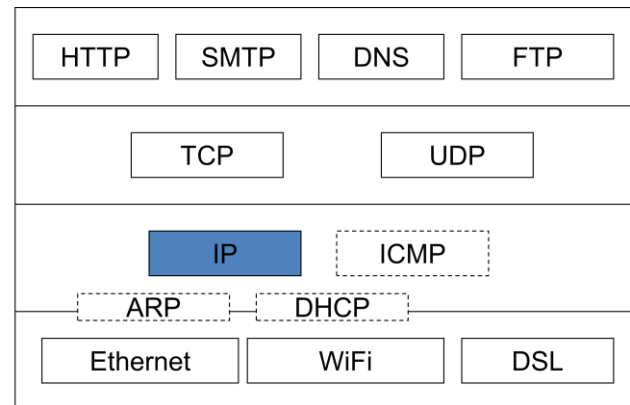
- IP (Internet Protocol) – межсетевой протокол
 - internet – объединенная сеть / subnet - подсеть
 - internetworking – объединение сетей
 - Internet – название самой крупной объединенной сети

Прикладной

Транспортный

Сетевой

Сетевых интерфейсов



- Основа сети Интернет

Сервисы IP

- Передача без установления соединения
 - ☐ Нет гарантии доставки
 - ☐ Произвольный порядок доставки
- Задачи IP
 - ☐ Маршрутизация
 - ☐ Объединение сетей
 - ☐ Качество обслуживания

6 байт	6 байт	2 байта	46-1500 байт	4 байта
Адрес получателя	Адрес отправителя	Тип	Данные	Контрольная сумма
Заголовок				Концевик

- ☐ Доставка на канальном уровне
 - MAC-адреса получателя и отправителя

- ☐ Мультиплексирование
 - Поле «Тип» – протокол вышестоящего уровня
- ☐ Проверка правильности передачи
 - Поле «Контрольная сумма»

Формат заголовка

4 бита Номер версии	4 бита Длина заголовка	8 бит Тип сервиса	16 бит Общая длина	
16 бит Идентификатор пакета			3 бита Флаги	13 бит Смещение фрагмента
8 бит Время жизни		8 бит Тип протокола	16 бит Контрольная сумма	
32 бита IP-адрес отправителя				
32 бита IP-адрес получателя				
Опции и выравнивание (не обязательно)				

- ☐ **Версия**
 - Первым полем пакета является версия протокола размером в четыре бита. Для IPv4 это 4.

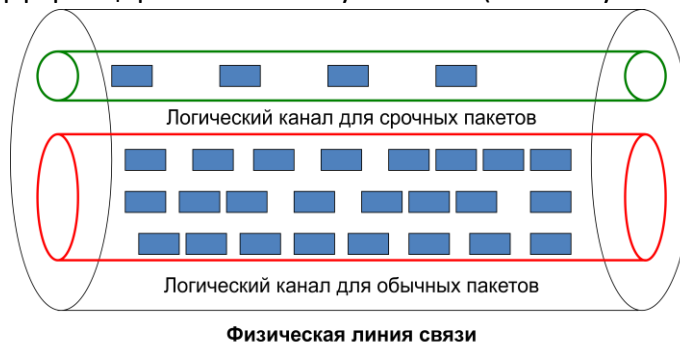
- ☐ В IP **длина заголовка** не фиксирована:
 - Дополнительные опции
 - Служебная информация
 - Заполнитель
 - Поле «Длина заголовка» измеряется в 32-битных словах
 - Длина:
 - Минимальная 20 байт (5 32-битных слов)
 - Максимальная 60 байт (15 32-битных слов)

☐ Тип сервиса

- Назначение – обеспечение качества обслуживания
- Два формата:
 - Тип сервиса (старый)
 - ❖ Используется 6 из 8 бит
 - ❖ PR (3 бита) – приоритет пакета:
 - 0 – самый низкий
 - 7 – самый высокий
 - ❖ Критерий выбора маршрута:
 - D (Delay) – минимизация задержек
 - T (Throughput) – максимизация пропускной способности
 - R (Reliability) – максимизация надежности
 - ❖ Поле «Тип сервиса» было придумано на ранней стадии развития Интернет

PR	D	T	R	
----	---	---	---	--

- ❖ Оказалось, что качество обслуживания на основе поля «Тип сервиса» обеспечить сложно
- ❖ С ростом и увеличением популярности Интернет появились практические подходы:
 - Интегрированное обслуживание
 - Дифференцированное обслуживание
- Дифференцированное обслуживание (используется сейчас)



- ❖ Дифференцированное обслуживание вытеснило традиционное представление поля «Тип сервиса»
- ❖ RFC 2474
- ❖ Простота реализации:
 - Выполняется отдельно на каждом маршрутизаторе (Per-Hop Behavior)
 - Нет необходимости знать топологию сети и требования приложений
- ❖ Используется 6 из 8 бит
- ❖ 3 бита – класс обслуживания
- ❖ 2 бита – варианты обслуживания пакета внутри класса
- ❖ 1 бит – флаг индикатор «выхода» пакета из профиля класса
- ❖ По умолчанию все 0 для совместимости
- **Общая длина** – длина пакета, включая заголовок и данные
 - Измеряется в байтах
 - Максимальное значение – 65535 байт
 - На практике длина выбирается с учетом MTU канального уровня
 - 1500 байт для Ethernet

Фрагментация

- При передаче по сетям с разным MTU IP-пакет может быть разбит на части
- Поля в заголовке IP, отвечающие за фрагментацию:
 - Идентификатор пакета
 - Флаги
 - Смещение фрагмента
- Поле **флаги** состоит из тех бит:
 - Первый бит зарезервирован и не используется
 - DF (Do not Fragment) – не фрагментировать
 - MF (More Fragments) – есть еще фрагменты
- **Идентификатор** пакета:
 - Уникальный номер пакета, разбитого на части (фрагментированного)
 - Все фрагменты пакета должны иметь одинаковый идентификатор
- Получатель может принимать фрагменты разных пакетов

- Задержки в передаче
- Разные маршруты
- Отброшенные пакеты

☐ **Смещение фрагмента:**

- Используется для сборки фрагментированных пакетов
- Фрагменты пакета могут прийти в неправильном порядке
- Содержит смещение поля данных относительно нефраgmentированного пакета

Схема дефрагментации

- Получатель принимает пакет и видит, что установлен флаг MF
- Получатель запоминает идентификатор пакета и записывает в буфер все пакеты с этим идентификатором
- Приходит пакет со сброшенным флагом MF – признак завершения передачи
- Получатель собирает пакет из фрагментов на основе поля «Смещение»

☐ **Время жизни (TTL, Time To Live)** – максимальное время, в течение которого пакет может перемещаться по сети

- Нужно для предотвращения «бесконечного» продвижения пакетов
- Единицы измерения:
 - Секунды
 - Прохождение через маршрутизатор (hop)

☐ **Тип протокола**

- Предназначено для реализации функции мультимплексирования/демультиплексирования
- Код протокола, данные которого передаются (RFC 1700):
 - TCP – 6
 - UDP – 17
 - ICMP – 1

☐ **Контрольная сумма** - рассчитывается по заголовку

- Проверяется и пересчитывается на каждом промежуточном маршрутизаторе
- При ошибке в контрольной сумме пакет отбрасывается
 - Нет оповещения отправителя об ошибке
 - Нет запросов на повторную передачу

☐ Заголовок IP-пакета может включать **дополнительные поля**

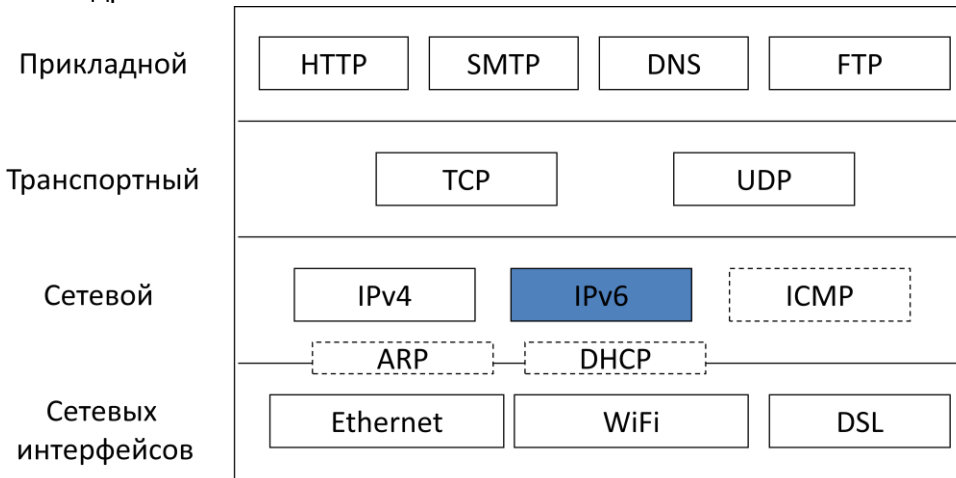
- Примеры опций:
 - Записать маршрут
 - Маршрут отправителя
 - Жесткая маршрутизация
 - Свободная маршрутизация
 - Временные метки

Уже в 1980-е годы стало очевидно, что распределение адресного пространства происходит значительно более быстрыми темпами, чем было заложено в архитектуру IPv4. Это привело сначала к появлению классовой адресации, позднее бесклассовой адресации, и в конечном итоге к разработке нового протокола IPv6.

19. Протокол IPv6.

- IPv6 (Internet Protocol version 6) – протокол сетевого уровня стека TCP/IP
- IPv6 используется для передачи данных на сетевом уровне

- IPv6 – замена IPv4
- IPv6 не совместим с IPv4
- IPv6 совместим с другими протоколами стека TCP/IP: TCP, UDP, ICMP, DHCP, DNS и др.



Цели создания IPv6

- Адресация миллиардов устройств в сети (борьба с нехваткой адресов в IPv4)
- Упрощение протокола для ускорения работы маршрутизаторов
- Обеспечение безопасности
- Качество обслуживания

История создания

- 1990 – проблемная группа проектирования Интернета IETF начала работу над новой версией протокола IP
- 1998 – IPv6 принят в качестве стандарта RFC 2460
- IPv5:
 - ☐ Экспериментальный протокол потоковой передачи данных (Streaming Protocol), предложен в 1979 г.
 - ☐ Не использовался широко
 - ☐ Концепции IPv5 перешли в **ATM** (асинхронный способ передачи данных —

Формат заголовка IPv6

4 бита Номер версии	8 бит Дифференцированное обслуживание	16 бит Метка потока	
16 бит Длина полезной нагрузки		8 бит Следующий заголовок	8 бит Максимальное число транзитных участков
16 байт IPv6-адрес отправителя			
16 байт IPv6-адрес получателя			
Дополнительные заголовки (не обязательно)			

сетевая высокопроизводительная технология коммутации и мультимплексирования, основанная на передаче данных в виде ячеек (cell) фиксированного размера (53 байта), из которых 5 байтов используется под заголовок) и **MPLS** (многопротокольная коммутация по меткам — механизм в высокопроизводительной телекоммуникационной сети, осуществляющий передачу данных от одного узла сети к

другому с помощью меток.)

- **Версия** – номер версии протокола IP: 6
- **Дифференцированное обслуживание** – параметры качества обслуживания (перешло из IPv4)
- **Метка потока** – сообщение об особенных требованиях к обработке
 - Маршрутизаторы смотрят на метку потока и обрабатывают пакеты по разному
 - Аналог виртуальных каналов в MPLS
 - Метки должны быть настроены на всех маршрутизаторах заранее
- **Длина полезной нагрузки** – размер данных в IPv6 пакете (в IPv4 был размер всего пакета)
- **Следующий заголовок** – использование дополнительных заголовков
 - Тип следующего необязательного заголовка
 - Последний тип заголовка – протокол транспортного уровня (TCP или UDP)
- **Максимальное число транзитных участков** – максимальное число маршрутизаторов, после которого пакет отбрасывается (аналог TTL в IPv4)
- **Дополнительные заголовки IPv6**
 - Параметры маршрутизации
 - Параметры получателя
 - Маршрутизация
 - Фрагментация
 - Аутентификация
 - Шифрование

Отличия от IPv4

- В IPv6 отказались от контрольной суммы в заголовке
Аргументация:
 - а) Контрольную сумму необходимо пересчитывать на каждом маршрутизаторе – высокие накладные расходы
 - б) Каналы связи надежные – ошибок мало
 - в) Контрольные суммы рассчитываются на канальном и транспортном уровне: достаточно для обнаружения ошибок
- Маршрутизаторы IPv6 не выполняют фрагментацию
 - Высокие накладные расходы на маршрутизаторе
 - Фрагментацию выполняют хосты, которые отправляют данные

Как хост может узнать MTU(максимальный размер полезного блока данных) в сети?

- ✓ Технология, позволяющая хосту определить MTU
 - RFC 1191 – Path MTU Discovery (1990)
 - RFC 1981 – Path MTU Discovery for IPv6 (1996)
- ✓ Маршрутизатор не фрагментирует IP пакет, а отбрасывает его и отправляет хосту ICMP сообщение:
 - ICMP – Тип 3 (Destination Unreachable), код 4 (fragmentation needed and DF set) + размер MTU
 - ICMPv6 – Тип 2 код 0 (Packet Too Big) + MTU
- ✓ Хост отправляет новый пакет с меньшим размером MTU

Влияние IPv6 на IPv4

- Некоторые возможности IPv6 были внесены в IPv4
- Качество обслуживания:
 - Поле «Тип сервиса» в заголовке IPv4 было заменено на «Дифференцированное обслуживание», как в IPv6
- Безопасность:

- Аутентификация и шифрование были перенесены в IPv4 в виде технологии IPSec (IP Security)

Адресация в IPv6

- Адресация – основное отличие IPv6 от IPv4
 - ☐ IPv4 – размер адреса 4 байта
 - ☐ IPv6 – размер адреса 16 байт
- Рассматриваемые варианты размера адреса
 - ☐ 8 байт – первоначальное предложение разработчиков IPv6
 - ☐ 20 байт – размер адреса в протоколе CLNP (протокол сетевого уровня в стеке OSI)
 - ☐ Адреса переменной длины
- RFC 4291 (IP Version 6 Addressing Architecture)

Форма представления IPv6 адреса

- Размер адреса IPv6 увеличился, старый формат записи неудобен
- Новый формат:
 - 8 групп по четыре шестнадцатеричных цифры
 - 8000:0000:0000:0000:0127:AB68:CD45:EF15

Сокращения IPv6 адреса

- Адреса IPv6 часто содержат много нулей, поэтому разработано несколько форм сокращения
- Ведущие нули в группе можно опустить
 - 8000:0000:0000:0000:0127:AB68:CD45:EF15
 - 8000:0000:0000:0000:**127**:AB68:CD45:EF15
- Несколько подряд идущих групп нулей можно пропустить:
 - 8000::**127**:AB68:CD45:EF15

Специальные IPv6 адреса

- Localhost
 - ::1 (0000:0000:0000:0000:0000:0000:0000:0001)
- Адрес IPv4 в формате IPv6
 - Используется на время переходного периода, когда применяются обе версии протокола
 - Два двоеточия и затем адрес в десятичном виде
 - ::192.168.1.1

Структура

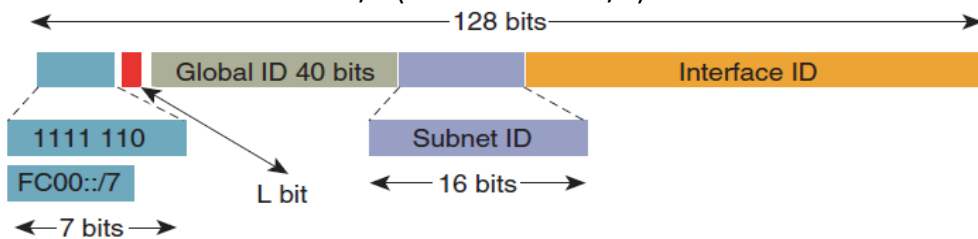


Типы IPv6 адресов

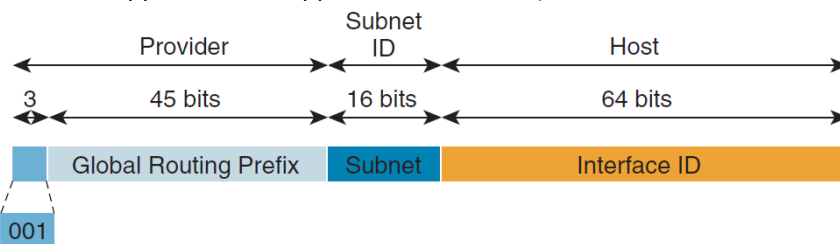
- Unicast
 - Адреса хостов в сети (данные получает только один хост)
- Multicast
 - Групповые адреса (данные получают все хосты в группе)
- Anycast
 - Групповые адреса (данные получает только один хост в группе)
- Нет широковещательных адресов
 - Можно использовать групповой адрес FF02::1

Область действия IPv6 адресов

- Link local – адреса для передачи данных в рамках одного сегмента сети (без маршрутизации)
 - Используются внутри одного сегмента сети
 - Начинаются с FE80::/10
- Site local – адреса для передачи данных внутри организации (аналог Private адресов в IPv4).
 - Маршрутизируются в сети организации, но недоступны их Интернет
 - Используются внутри одной организации
 - Начинаются с FC00::/7 (сейчас с FD00::/8)



- Global ID выбирается для каждой организации по алгоритму из RFC 4193 (с высокой долей вероятности уникальный)
- Global – глобальные адреса для работы в Интернет
 - Используются в Интернет
 - Выделяются регистратором ICANN (не должны дублироваться)
 - Сейчас выделяются из диапазона 2000::/3

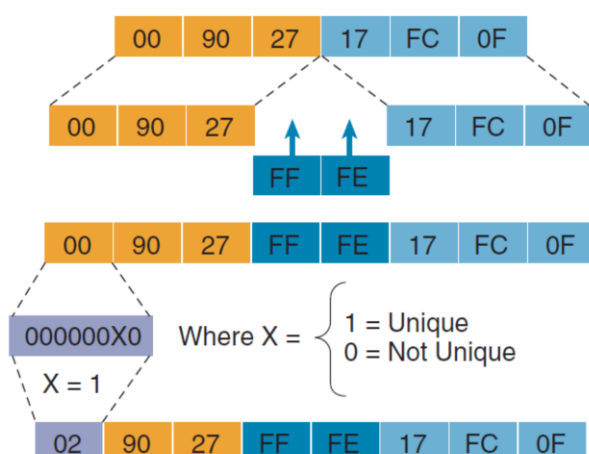


- В IPv6 интерфейс может иметь несколько адресов разных типов

Варианты назначения IPv6 адресов

- Вручную
- DHCPv6
- Автоматическая конфигурация
 - Формирование Interface ID на основе MAC-адреса - процесс EUI-64 (Extended Unique Identifier, 64 бита)

Процесс EUI-64



- В IPv6 хост может получить от маршрутизатора следующие параметры:
 - Subnet ID, адрес шлюза, адрес DNS-сервера и т.д.
- Механизм реализации:
 - Хост отправляет ICMPv6 запрос тип 133 код 0 (Router Solicitation) на групповой адрес FF02::2 (all routers)
 - Маршрутизатор, который получил запрос, отвечает ICMPv6 сообщением тип 134 код 0 (Router Advertisement) с параметрами сети
- Маршрутизаторы периодически рассылают Unsolicited Router Advertisements на групповой адрес FF02::1 (all nodes)

Переход на IPv6

- IPv4 и IPv6 не совместимы, необходим явный переход на IPv6, заметный для пользователей Интернет
- Не предполагается, что переход на IPv6 будет быстрым
 - Долгое время будут сосуществовать два протокола
- Механизмы перехода
 - Dual Stack (параллельное использование с IPv4)
 - Туннелирование (процесс, в ходе которого создается защищенное логическое соединение между двумя конечными точками посредством инкапсуляции различных протоколов)
 - 6to4
 - Teredo
 - Intra-Site Automatic Tunnel Addressing Protocol (ISATAP)

Проблемы внедрения IPv6

- ✓ IPv6 был стандартизован в 1998
- ✓ IPv6 решает насущную проблему – нехватка адресов IPv4
- ✓ IPv6 поддерживается всем современным оборудованием, операционными системами и ПО
- ✓ Протокол IPv6 проще, чем IPv4
- IPv6 не совместим с IPv4
 - Требуется полная замена, заметная для пользователей
- Для многих проблем IPv4 удалось найти решение (хотя бы временное)
 - Нехватка IPv4-адресов – NAT
 - Низкая безопасность – IPSec
 - Качество обслуживания – Дифференцированное обслуживание
- Люди и организации не понимают, зачем переходить на IPv6

20. Протокол ICMP. Назначение и варианты использования.

ICMP (Internet Control Message

Protocol) – протокол межсетевых управляющих сообщений

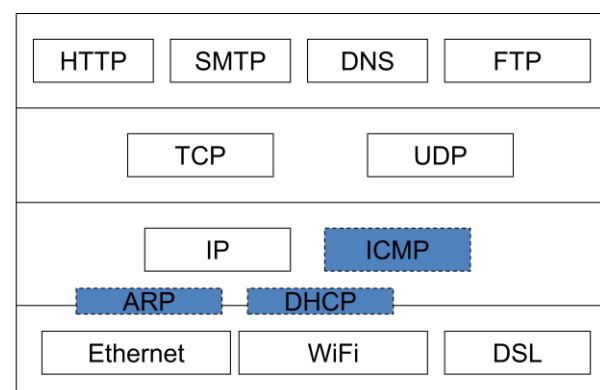
- Определен в RFC 792
- Протокол IP использует передачу без установки соединения
- Нет гарантии доставки пакетов
- ICMP – средство оповещения о проблемах с доставкой пакетов
- Примеры сообщений об ошибках:
 - а. Закончилось время жизни

Прикладной

Транспортный

Сетевой

Сетевых интерфейсов



- пакета (TTL)
 - b. Запрещено фрагментировать пакет (установлен флаг DF), а для передачи нужна дефрагментация
- Сообщения отправляются не всегда:
 - a. Нет сообщений о проблемах с пакетами с ICMP-сообщениями
- IP или ICMP не обязаны обрабатывать сообщения ICMP
 - a. Нет исправления ошибок
 - b. Нет повторной отправки пакетов

Формат пакета ICMP

1 байт	1 байт	2 байта	} Заголовок
Тип сообщения	Код сообщения	Контрольная сумма	
2 байта		2 байта	
Зависит от типа и кода сообщения		Зависит от типа и кода сообщения	
Поле данных			

■ Поля заголовка:

- ☐ Тип – идентификатор типа сообщения

Типы ICMP-сообщений

Тип	Назначение сообщения
0	Эхо-ответ
3	Узел назначения недостижим
4	Подавление источника
5	Перенаправления маршрута
8	Эхо-запрос
11	Истечение времени жизни пакета
12	Проблемы с параметрами
13	Запрос отметки времени
14	Ответ отметки времени
17	Запрос маски
18	Ответ маски

- ☐ Код – идентификатор кода сообщения об ошибке

Пример для типа 3:

Код	Причина
0	Сеть недостижима
1	Узел недостижим
2	Протокол недостижим
3	Порт недостижим
4	Ошибка фрагментации
5	Ошибка в маршруте источника
6	Сеть назначения неизвестна
7	Узел назначения неизвестен
8	Узел-источник изолирован
9	Административный запрет

- ☐ Контрольная сумма
- **Данные:**
 - ☐ Заголовок и первые 8 байт данных IP-пакета
- **Сообщения ICMP:**
 - ☐ Сообщения об ошибках (host unreachable)
 - ☐ Сообщения запрос-ответ (ping)

Применение ICMP

- Диагностика сети
- Утилиты
 - ☐ Ping

Формат ICMP-сообщения ping

Тип = 8/0	Код = 0	Контрольная сумма	Заголовок
Идентификатор запроса		Порядковый номер	
Поле данных Данные Эхо-запроса или Эхо-ответа			

- Простое средство проверки работоспособности сети
- Эхо-протокол:
 - ✓ Эхо-запрос ICMP (Тип = 8)
 - ✓ Эхо-ответ ICMP (Тип = 0)
- Проверка доступности по сети конкретного хоста
- ☐ traceroute (tracert в Windows)
 - Утилита, позволяющая проследить маршрут от отправителя к получателю
 - Находит адреса всех маршрутизаторов, через которые проходит пакет
 - traceroute использует сообщение «Время жизни истекло» (тип 11) для поиска маршрутизаторов
 - Сначала traceroute отправляет IP-пакет с TTL=1
 - Первый маршрутизатор принимает его, уменьшает TTL до 0 и понимает, что пакет нужно отбросить
 - Первый маршрутизатор отправляет ICMP-сообщение «Время жизни истекло», Тип=11
 - traceroute запоминает адрес маршрутизатора
 - traceroute отправляет IP-пакет с TTL=2
 - Так продолжается до тех пор, пока IP-пакет не достигнет получателя

Правила генерации ICMP пакетов

1. При потере ICMP-пакета никогда не генерируется новый.
2. ICMP-пакеты никогда не генерируются в ответ на IP-пакеты с широковещательным или групповым адресом, чтобы не вызывать перегрузку в сети (так называемый «широковещательный шторм»).
3. При повреждении фрагментированного IP-пакета ICMP-сообщение отправляется только после получения первого повреждённого фрагмента, поскольку отправитель всё равно повторит передачу всего IP-пакета целиком.

21. Транспортный уровень. Адресация на транспортном уровне.

Задачи транспортного уровня:

- Передача данных между процессами на хостах
- Предоставление нужного уровня надежности передачи данных, не зависящего от надежности сети
- Адресация

Транспортный и сетевой уровень:

Модель OSI	Модель TCP/IP
Прикладной	Прикладной
Представления	
Сеансовый	Транспортный
Транспортный	
Сетевой	Сетевой
Канальный	Сетевых интерфейсов
Физический	

- Сетевой уровень обеспечивает передачу данных между хостами в объединенной сети
- На одном хосте могут работать несколько приложений с разными требованиями к сети
- Сетевой уровень – передача между хостами
- Транспортный уровень – передача между процессами на хостах

Особенности:

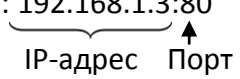
- Транспортный уровень есть только на хостах
 - ☐ Сетевое оборудование – канальный или сетевой уровень
- Сквозное соединение – от процесса отправителя к процессу получателю
 - ☐ Не видит промежуточного сетевого оборудования

Надежность передачи данных

- Транспортный уровень может обеспечить надежность передачи данных выше, чем у лежащей в его основе сети
 - ☐ Эффективно на практике
- Гарантия доставки данных:
 - ☐ Подтверждение получения
 - ☐ Повторная отправка не подтвержденных данных
- Гарантия порядка следования сообщений:
 - ☐ Нумерация сообщений

Адресация

- У хоста в сети есть IP-адрес
- На хосте могут работать несколько приложений
 - ☐ Открыто два окна браузера
 - ☐ Браузер и клиент электронной почты
 - ☐ Сервер Web, DNS и почты
- ***В какое приложение отправить данные из поступившего IP-пакета?***
- Адрес на транспортном уровне: число от 1 до 65535
- Адрес называется портом
- Каждое сетевое приложение на хосте имеет свой порт
- Номера портов у приложений не повторяются
- Форма записи: 192.168.1.3:80


- Полный адрес в Интернет (кортеж из 5 значений, 5tuple):
 - ☐ Транспортный протокол (TCP/UDP)
 - ☐ IP-адрес получателя
 - ☐ Порт получателя
 - ☐ IP-адрес отправителя
 - ☐ Порт отправителя

Типы портов

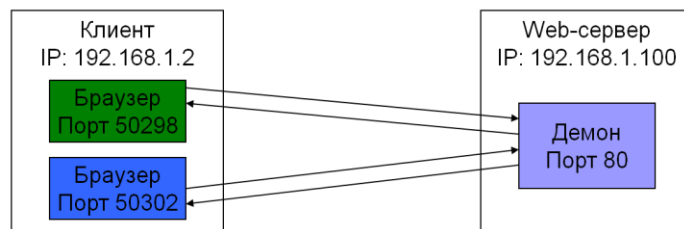
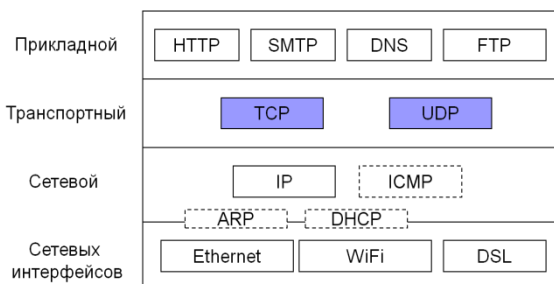
- 1-1024 – Хорошо известные порты
 - ☐ Well-known ports – порты популярных сервисов
 - 80 – HTTP (Web)
 - 22 – SSH
 - 25 – SMTP (Электронная почта)
 - 53 – DNS
 - ☐ Файл /etc/services в UNIX
 - ☐ Ограничение: использовать может только root/Администратор
 - 1025-49151 – Зарегистрированные порты
- Регистрация портов:

- Выполняется Internet Assigned Numbers Authority (IANA - Администрация адресного пространства Интернет)
 - ☐ Хорошо известные порты
 - ☐ Зарегистрированные порты
- Популярные сервисы также могут работать на любых портах
 - ☐ Требуется специальная настройка сервиса
 - ☐ Клиент должен явно указать порт
http://192.168.1.3:8080
- 49151-65535 – Динамические порты
 - ☐ Хорошо известные и зарегистрированные порты используются серверами
 - Клиенты должны знать, к какому порту подключаться
 - ☐ Клиентам также нужны порты для адресации на транспортном уровне
 - ☐ Для клиента номер порта принципиального значения не имеет
 - Значения выбираются случайно из диапазона динамических портов

Порты и IP-адреса

Утилита netstat - отображение статистики протокола и текущих сетевых подключений TCP/IP.

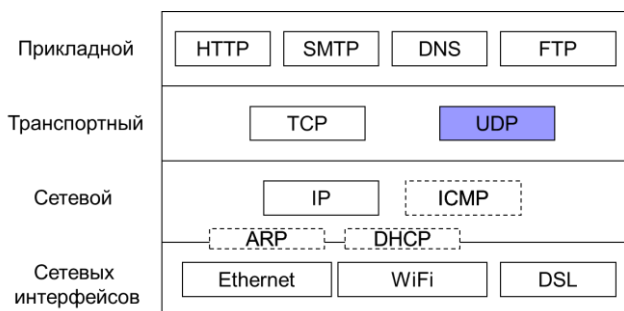
Протоколы транспортного уровня:



➤ **TCP** — «гарантированный» транспортный механизм с предварительным установлением соединения, предоставляющий приложению надёжный поток данных, дающий уверенность в безошибочности получаемых данных, перезапрашивающий данные в случае потери и устраняющий дублирование данных. TCP позволяет

регулировать нагрузку на сеть, а также уменьшать время ожидания данных при передаче на большие расстояния. Более того, TCP гарантирует, что полученные данные были отправлены точно в такой же последовательности.

➤ **UDP** - протокол передачи дейтаграмм без установления соединения. Также его называют протоколом «ненадёжной» передачи, в смысле невозможности удостовериться в доставке сообщения адресату, а также возможного перемешивания пакетов. UDP обычно используется в таких приложениях, как потоковое видео и компьютерные игры, где допускается потеря пакетов, а повторный запрос затруднён или не оправдан, либо в приложениях вида запрос-ответ (например, запросы к DNS), где создание соединения занимает больше ресурсов, чем повторная отправка.



22. Протокол UDP.

UDP - протокол транспортного уровня, который служит для передачи дейтаграмм без установления соединения. Также его называют протоколом «ненадёжной» передачи, в смысле невозможности

удостовериться в доставке сообщения адресату, а также возможного перемешивания пакетов. UDP обычно используется в таких приложениях, как потоковое видео и компьютерные игры, где допускается потеря пакетов, а повторный запрос затруднён или не оправдан, либо в приложениях вида запрос-ответ (например, запросы к DNS), где создание соединения занимает больше ресурсов, чем повторная отправка.

Дейтаграмма — блок информации, посланный как пакет сетевого уровня через передающую среду без предварительного установления соединения и создания виртуального канала. Датаграмма представляет собой единицу информации в протоколе (protocol data unit, PDU) для обмена информацией на сетевом в случае протокола IP, IP-датаграммы) и транспортном (в случае протокола UDP, UDP-датаграммы) уровнях эталонной модели OSI. Название «датаграмма» было выбрано по аналогии со словом телеграмма.

Назначение:

- Основная задача UDP – адресация транспортного уровня
 - ☐ Указать порты отправителя и получателя
- Надежность доставки по сравнению с IP не повышается

Формат заголовка UDP

16 бит Порт отправителя	16 бит Порт получателя
16 бит Длина UDP	16 бит Контрольная сумма UDP

Порт отправителя

- В этом поле указывается номер порта отправителя.
- Предполагается, что это значение задаёт порт, на который при необходимости будет посылаться ответ. В противном же случае, значение должно быть равным 0.
- Если хостом-источником является клиент, то номер порта будет, скорее всего, эфемерным.
- Если источником является сервер, то его порт будет одним из «хорошо известных».

Порт получателя

- Это поле обязательно и содержит порт получателя.
- Аналогично порту отправителя, если клиент — хост-получатель, то номер порта эфемерный, иначе (сервер — получатель) это «хорошо известный порт».

Длина UDP:

- Минимум 8 байт (только заголовок)
- Максимум 65 515 байт (максимальная длина данных IP-пакета)

Контрольная сумма

- Поле контрольной суммы используется для проверки заголовка и данных на ошибки.
- Если сумма не сгенерирована передатчиком, то поле заполняется нулями.
- Поле не является обязательным для IPv4.

Применение UDP

- Преимущество UDP – скорость работы
 - ☐ Нет накладных расходов на установку соединения
- Надежность
 - ☐ В современных сетях ошибки происходят редко
 - ☐ Ошибку может обработать приложение

- Область применения
 - Клиент-сервер, короткие запросы

Применение UDP: DNS

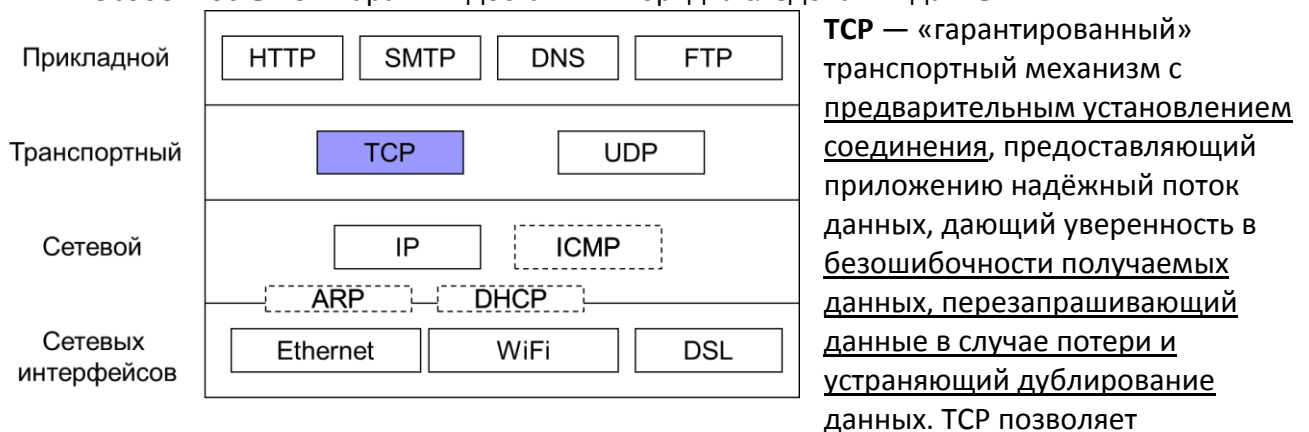
- DNS использует UDP, порт 53
 - Клиент DNS отправляет UDP-запрос серверу DNS
 - Сервер DNS отправляет UDP-ответ клиента
- При использовании TCP сначала нужно было бы установить соединение (три пакета)
- Клиент DNS запускает таймер после отправления запроса
 - Если через определенный промежуток времени ответ не пришел – запрос отправляется еще раз

Протокол UDP не сложен. Действительно, его функции сводятся к простой передаче данных между прикладным и сетевым уровнями, а также примитивному контролю искажений в передаваемых данных. При контроле искажений протокол UDP только диагностирует, но не исправляет ошибку. Если контрольная сумма показывает, что в поле данных UDP-дейтаграммы произошла ошибка, протокол UDP просто отбрасывает поврежденную дейтаграмму.

23. Протокол TCP. Гарантированная доставка данных. Процесс установки соединения.

Transmission Control Protocol (TCP) - протокол управления передачей

- TCP передает поток байт от одного процесса другому
- Сообщение TCP называется **сегментом**
- Особенность TCP: гарантия доставки и порядка следования данных



регулировать нагрузку на сеть, а также уменьшать время ожидания данных при передаче на большие расстояния. Более того, TCP гарантирует, что полученные данные были отправлены точно в такой же последовательности.

Формат заголовка TCP



- Порт источника идентифицирует приложение клиента, с которого отправлены пакеты. По возвращении данные передаются клиенту на основании номера порта источника.
- Порт назначения идентифицирует порт, на который отправлен пакет.
- Порядковый номер – номер пересылаемого байта в сегменте
- Номер подтверждения – номер следующего ожидаемого байта
- Кумулятивное подтверждение (подтверждение приема указанного байта данных и всех предыдущих), что все предыдущие байты получены
- Длина заголовка TCP – длина в 32-х разрядных словах (4 бита)
 - ☐ Заголовок может включать параметры, поэтому длина может быть разной
- 4 бита не используется
- Флаги – 6 шт. по 1 биту
 - ☐ URG – флаг наличия в сегменте срочных данных
 - Используется совместно с полем «Указатель на срочные данные»
 - Позволяет передавать сигналы от отправителя к получателю (прерывания)
 - ☐ ACK – флаг подтверждения
 - Если флаг ACK установлен, значит поле «Номер подтверждения» содержит осмысленные данные
 - ☐ PSH – флаг выталкивания (PUSH)
 - Просит получателя сразу отправлять данные приложению, без буферизации
 - ☐ Флаги RST, SYN и FIN используются для управления соединением
 - SYN – установка соединения
 - FIN, RST – разрыв соединения
- Размер окна – количество байт, которое может быть принято получателем
- Контрольная сумма – контрольная сумма заголовка и данных TCP
 - ☐ Служит для повышения надежности
 - ☐ Не обязательна
- Указатель на срочные данные – смещение от текущего порядкового номера байта до срочных данных в сегменте
- Параметры в заголовке TCP являются необязательными, но некоторые используются широко
- Примеры параметров:
 - ☐ Максимальный размер сегмента (Maximum Segment Size, MSS)
 - ☐ Масштаб окна - позволяет увеличить размер окна до 1 ГБ, что эффективно для быстрых каналов
 - ☐ Метки времени
 - ☐ Выборочное подтверждение (Selective Acknowledgment, SACK) – подтверждение диапазонов принятых байт

Поток байт

Поток байт от приложения

Сегмент	Сегмент	Сегмент	Сегмент
Байт 0	Байт 1024	Байт 2048	Байт 3072

- Транспортная подсистема получает от приложения данные в виде потока байт
- Поток разбивается на отдельные части – сегменты

- Протокол TCP нумерует байты в потоке
 - Сегменты не нумеруются

Гарантия доставки

- Возможные проблемы при доставке:
 - Потеря сегментов
 - Изменение порядка доставки сегментов
 - Повторная доставка сегментов
- Механизмы реализации:
 - Нумерация сообщений
 - Подтверждение получения сообщения
 - Повторная отправка при отсутствии подтверждения

Нумерация сообщений

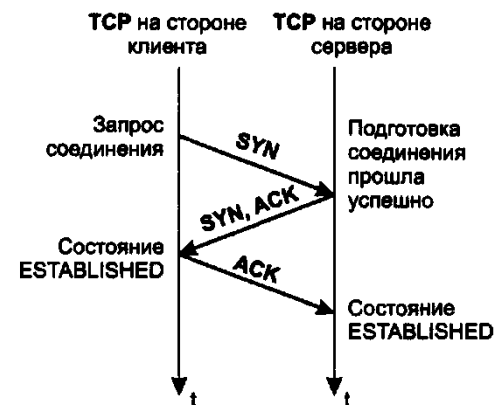
- Как выбрать номер для первого сообщения?
- Возможные проблемы:
 - Пришел задержавшийся сегмент
 - Первый сегмент потерян, сразу пришел второй
 - Первый сегмент выслан повторно
- Начальные номера сегментов не повторяются
- Начальный номер выбирается случайным образом, затем номера увеличиваются

Соединение

- Соединение – договоренность между отправителем и получателем
- Соединение задает:
 - Начальные номера для нумерации данных отправителя и получателя
 - Объем данных, которые готов принять получатель
- Соединение в TCP дуплексное
 - Данные могут передаваться в обе стороны
 - Подтверждение получения и данные в одном сегменте

Установка соединения

- Простейшая схема:
 - Запрос на установку соединения
 - Ответ об установке соединения (или отказ)
- Проблемы:
 - Потеря или повторная доставка сегментов
- Применяемая схема:
 - Трехкратное рукопожатие
- Флаг SYN – признак установки соединения
 - SYN = 1, ACK = 0 – запрос установки соединения (CONNECTION REQUEST)
 - SYN = 1, ACK = 1 – подтверждение установки соединения (CONNECTION ACCEPT)
 - SYN = 0, ACK = 1 – завершение установки соединения



Разрыв соединения

- Соединение в TCP дуплексное
 - Данные могут передаваться в обе стороны
- Схема разрыва соединения
 - Одновременное (обе стороны разорвали соединение)
 - Одностороннее (сторона прекращает передавать данные, но может принимать)
- Флаг FIN – одностороннее закрытие соединения

- ☐ Соединение закрывается, когда обе стороны отправят сегмент с установленным флагом FIN
- Флаг RST – разрыв соединения из-за критической ситуации
 - ☐ Одновременный разрыв соединения обеими сторонами

24. Протокол TCP. Управление скоростью передачи данных. Скользящее окно, окно управления потоком, окно перегрузки.

(Определение и особенности из 23)

Управление потоком в TCP

- Управление потоком позволяет регулировать скорость передачи данных
 - ☐ Предотвращение «затопления» быстрым отправителем медленного получателя
 - ☐ Сеть может быть свободна, но приложение не готово получить данные
- Транспортная подсистема работает с приложениями:
 - ☐ Приложение не обязано забирать данные, как только они появились
 - ☐ Транспортная подсистема не обязана передавать данные приложению или в сеть, как только она их получила
- Для управления потоком TCP использует механизм скользящего окна
- Получатель записывает в поле заголовка TCP «Размер окна» объем данных, которые он готов принять
- Размер окна может меняться динамически
 - ☐ Приложение читает данные из буфера быстро – окно растет
 - ☐ Приложение читает медленно, буфер заполнен – окно уменьшается
- Получатель может установить окно нулевого размера
 - ☐ Передача данных прекращается не зависимо от нагрузки на сеть
- Продолжение передачи:
 - ☐ Получатель повторно отправляет подтверждение с ненулевым размером окна
 - ☐ Отправитель направляет запрос «window probe» - просьба повторить подтверждение и размер окна

Скользящее окно

- Ожидание подтверждения приводит к снижению производительности
- Пример сети:
 - ☐ Пропускная способность 1 Гб/с
 - ☐ Время доставки сегмента – 100 мс
 - ☐ Количество сегментов в секунду – 5 шт.
- Разные варианты подтверждений:
 - ☐ Остановка и ожидание – передача данных после получения подтверждения каждого сообщения (Wi-Fi, канальный уровень)
 - ☐ Скользящее окно – передача заданного количества сообщений без ожидания подтверждения (TCP, транспортный уровень)
- Размер окна – количество байтов данных, которые могут быть переданы без получения подтверждения
- Кумулятивное подтверждение – подтверждение приема указанного байта данных и всех предыдущих

Производительность TCP

- Некоторые приложения читают и пишут данные маленькими порциями
- Эмуляторы терминала telnet или ssh
 - ☐ При нажатии каждой клавиши данные передаются на сервер – 1 байт данных
 - ☐ Для передачи 1 байта данных требуется передать IP-пакет длиной 41 байт (20 байт заголовок IP, 20 байт заголовок TCP, 1 байт данных)

- ☐ Высокие накладные расходы
- Отложенные подтверждения
 - ☐ Задержка отправки подтверждения до 500 мс в надежде получить данные
 - ☐ Терминал за 500 мс выдает эхо, данные отправляются вместе с подтверждением
- Алгоритм Нагеля (Nagle's algorithm)
 - ☐ Получателю отправляется только первая порция маленьких данных
 - ☐ Остальные данные буферизируются, пока не придет подтверждение
 - ☐ Данные из буфера отправляются в одном сегменте
 - ☐ Продолжается накопление данные в буфере, пока не придет новое подтверждение
- Синдром «глупого окна»
 - ☐ Приложение читает данные из буфера по символам
 - ☐ Буфер заполнен, размер окна 0
 - ☐ Приложение прочитало один байт – размер окна увеличился до 1
 - ☐ Отправитель передал 1 байт данных (IP-пакет 41 байт)
 - ☐ Буфер заполнен, размер окна 0

Таймеры TCP

- Таймер повторной передачи
 - ☐ Время ожидания подтверждения получения сегмента
 - ☐ Если подтверждения нет, сегмент отправляется вновь
- Таймер настойчивости
 - ☐ Время, через которое отправляется запрос «window probe»
- Таймер проверки активности
 - ☐ Используется при длительном простое соединения
 - ☐ Задаёт время, через которое должна выполняться проверка работоспособности соединения
- Таймер закрытия соединения
 - ☐ Задаёт ожидание равное двойному времени жизни сегмента
 - ☐ За это время все сегменты соединения должны уйти из сети

Контроль перегрузки в TCP

- Скорость передачи данных по сети определяется не только возможностями получателя, но и нагрузкой на сеть
- Механизмы регулирования скорости:
 - ☐ Окно управления потоком
 - Задаётся получателем (поле «Размер окна» в заголовке TCP)
 - Размер определяется возможностями приложения читать данные из буфера
 - ☐ Окно перегрузки
 - Задаётся отправителем
 - Размер определяется загрузкой сети
 - ☐ Размер скользящего окна определяется меньшим из окон перегрузки или управления потоком
 - Приложение просит много данных, но сеть перегружена:
 - Окно управления потоком: 40Кбайт
 - Окно перегрузки: 20 Кбайт
 - Скользящее окно: 20 Кбайт
 - Сеть свободна, но приложение ограничивает скорость:
 - Окно управления потоком: 20Кбайт

- Окно перегрузки: 40 Кбайт
- Скользящее окно: 20 Кбайт

Окно перегрузки

- Размер окна перегрузки определяется нагрузкой на сеть
- Сигнал о перегрузке – потеря пакетов
 - ☐ Считается, что пакеты редко теряются из-за ошибок передачи
 - ☐ Если ошибки в среде встречаются часто, то это решается на канальном уровне (например, Wi-Fi)
 - ☐ Пакеты отбрасываются маршрутизаторами при перегрузках

25. Протокол TCP. Управление скоростью передачи данных. Медленный старт. AIMD.

(Определение протокола TCP, особенности из 23. Управление потоком из 24)

Контроль перегрузки в TCP

- Скорость передачи данных по сети определяется не только возможностями получателя, но и нагрузкой на сеть
- Механизмы регулирования скорости:
 - ☐ Окно управления потоком
 - Задается получателем (поле «Размер окна» в заголовке TCP)
 - Размер определяется возможностями приложения читать данные из буфера
 - ☐ Окно перегрузки
 - Задается отправителем
 - Размер определяется загрузкой сети
 - ☐ Размер скользящего окна определяется меньшим из окон перегрузки или управления потоком

Окно перегрузки

- Размер окна перегрузки определяется нагрузкой на сеть
- Сигнал о перегрузке – потеря пакетов
 - ☐ Считается, что пакеты редко теряются из-за ошибок передачи
 - ☐ Если ошибки в среде встречаются часто, то это решается на канальном уровне (например, Wi-Fi)
 - ☐ Пакеты отбрасываются маршрутизаторами при перегрузках

Управление размером окна перегрузки

- Транспортная система отправителя не знает, какие сетевые соединения встретятся по пути к получателю
- Как выбрать размер окна перегрузки?
 - ☐ Слишком маленький размер приведет к низкой скорости передачи данных из-за постоянного ожидания подтверждений
 - ☐ Слишком большой размер окна приведет к низкой скорости передачи данных из-за перегрузки сети
- TCP использует следующие механизмы определения размера окна перегрузки:
 - ☐ Аддитивное увеличение мультипликативное уменьшение (AIMD)
 - ☐ Медленный старт
- TCP начинает работу с медленного старта, затем переходит на AIMD

Медленный старт

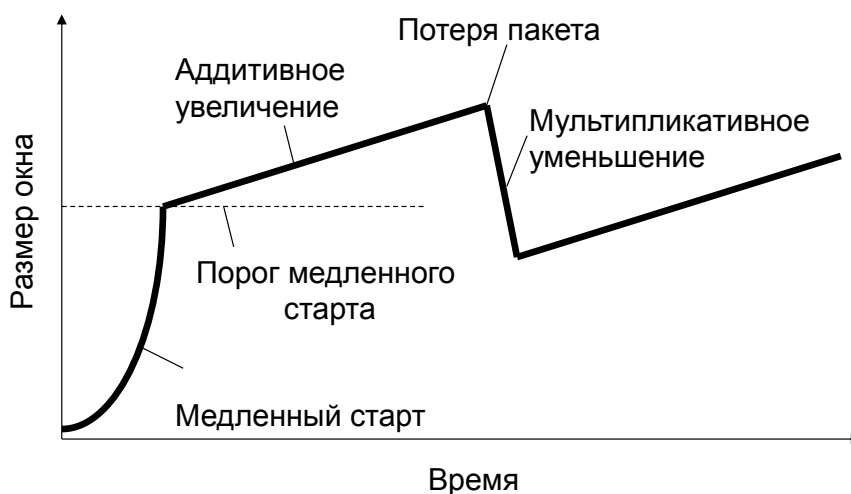
- Особенности медленного старта:

- ☐ Первоначально размер окна перегрузки устанавливается маленьким (1 или 4 сегмента)
- ☐ При каждом получении подтверждения отправляется 2 сегмента
- Экспоненциальный рост размера окна (1 сегмент, 2, 4, 8 и т.д.)
- При потере сегмента медленный старт начинается заново

Метод AIMD

- Особенности метода AIMD
 - ☐ При получении подтверждения размер окна перегрузки увеличивается на 1 (аддитивное увеличение)
 - ☐ При потере сегмента размер окна перегрузки уменьшается в 2 раза (мультипликативное уменьшение)
- Отличия от медленного старта:
 - ☐ Размер окна растет медленнее
 - ☐ При потере сегмента не нужно начинать все с начала

Размер окна перегрузки TCP



26.Динамическое конфигурирование хостов. Протокол DHCP.

DHCP (*Dynamic Host Configuration Protocol* — протокол динамической настройки узла) — сетевой протокол, позволяющий компьютерам автоматически получать IP-адрес и другие параметры, необходимые для работы в сети TCP/IP.

Методы назначения IP-адресов

- Вручную администратором
 - ☐ IP-адрес назначается вручную на каждом компьютере в сети
 - ☐ В крупной сети высокие трудозатраты
 - ☐ Постоянный IP-адрес
- Автоматически
 - ☐ Используется протокол DHCP
 - ☐ Требуется создание DHCP-сервера
 - ☐ Не нужна ручная настройка компьютеров
 - ☐ IP-адрес может меняться

Клиент DHCP - компьютер, который получает IP-адрес автоматически

Сервер DHCP - компьютер, который обеспечивает назначение IP-адресов, ведет таблицу выделенных IP-адресов, чтобы избежать дублирования.

Опции протокола:

Помимо IP-адреса, DHCP также может сообщать клиенту дополнительные параметры, необходимые для нормальной работы в сети. Эти параметры называются опциями DHCP. Список стандартных опций можно найти в RFC 2132.

Некоторыми из наиболее часто используемых опций являются:

- IP-адрес маршрутизатора по умолчанию;
- маска подсети;
- адреса серверов DNS;
- имя домена DNS.

DNS - доменная система имен.

- DNS обеспечивает отображение доменных имен в IP-адреса и наоборот
- DNS-сервер
 - ☐ Сервер, который хранит таблицу соответствия доменных имен и IP-адресов
- Утилиты для DNS:
 - ☐ nslookup
 - ☐ dig (UNIX)
- С точки зрения компьютеров в сети IP-адрес и DNS-имя равнозначны
- DNS-имя может отображаться на несколько IP-адресов

Сообщения протокола:

- DHCP DISCOVER – широковещательный запрос на поиск DHCP-сервера в сети
- DHCP OFFER – предложение IP-адреса DHCP-сервером клиенту
- DHCP REQUEST – запрос IP-адреса DHCP-клиентом
- DHCP ACK – подтверждение назначения IP-адреса DHCP-клиенту
- DHCP RELEASE – освобождение IP-адреса DHCP-клиентом
- Зачем три сообщения с одинаковым IP-адресом?
 - ☐ DHCP OFFER
 - ☐ DHCP REQUEST
 - ☐ DHCP ACK
- В сети может быть несколько DHCP-серверов
 - ☐ Все серверы присылают клиенту IP-адреса (DHCP OFFER)
 - ☐ Клиент запрашивает IP-адрес только у одного DHCP-сервера (DHCP REQUEST)
- DHCP-сервер должен находиться в той же сети, что и клиент
- Поиск DHCP-серверов выполняется с помощью широковещательного запроса
 - Широковещательный запрос не выходит за границы сети (маршрутизатор)
- **DHCP Relay** – устройство, которое принимает широковещательные запросы и пересылает их DHCP-серверу (коммутатор, маршрутизатор и др.)

Схема обмена сообщениями между клиентскими и серверными частями DHCP.

1. Когда компьютер включают, установленный на нем DHCP-клиент посылает ограниченное широковещательное сообщение DHCP-поиска (IP-пакет с адресом назначения, состоящим из одних единиц, который должен быть доставлен всем узлам данной IP-сети).
2. Находящиеся в сети DHCP-серверы получают это сообщение. Если в сети DHCP-серверы отсутствуют, то сообщение DHCP-поиска получает связной DHCP-агент. Он пересылает это сообщение в другую, возможно, значительно отстоящую от него сеть DHCP-серверу, IP-адрес которого ему заранее известен.
3. Все DHCP-серверы, получившие сообщение DHCP-поиска, посылают DHCP-клиенту, обратившемуся с запросом, свои DHCP-предложения. Каждое предложение содержит IP-адрес и другую конфигурационную информацию. (DHCP-сервер, находящийся в другой сети, посылает ответ через агента.)
4. DHCP-клиент собирает конфигурационные DHCP-предложения от всех DHCP-серверов. Как правило, он выбирает первое из поступивших предложений и отправляет в сеть

широковещательный DHCP-запрос. В этом запросе содержатся идентификационная информация о DHCP-сервере, предложение которого принято, а также значения принятых конфигурационных параметров.

5. Все DHCP-серверы получают DHCP-запрос, и только один выбранный DHCP-сервер посылает положительную DHCP-квитанцию (подтверждение IP-адреса и параметров аренды), а остальные серверы аннулируют свои предложения, в частности возвращают в свои пулы предложенные адреса.

6. DHCP-клиент получает положительную DHCP-квитанцию и переходит в рабочее состояние.

Способы назначения IP-адресов

- Пул адресов – список (диапазон) IP-адресов, которые назначает DHCP-сервер
- Способы назначения IP-адресов:
 - ☐ Постоянный – выделенный IP-адрес для каждого MAC-адреса
 - ☐ Динамический – выделение компьютеру любого IP-адреса из пула
- Сколько IP-адресов нужно для пула DHCP-сервера?
- Компьютеры могут появляться и исчезать (ноутбуки, планшеты и т.п.)
- IP-адреса назначаются не навсегда, а на фиксированный срок
 - ☐ Lease time (Срок аренды)
 - После завершения срока аренды IP-адрес должен быть возвращен в пул DHCP-сервера
 - Что делать, если компьютер хочет продолжить работу в сети
 - Повторный запрос IP-адреса
 - Что делать, если компьютер отключился до истечения срока аренды
 - IP-адрес будет считаться занятым, пока не закончится срок аренды

Освобождение IP-адреса

- После того, как компьютер закончил работу в сети, он может вернуть IP-адрес в пул DHCP-сервера
 - ☐ Сообщение DHCP RELEASE
- Команда
 - ☐ ipconfig /release
- Получение нового IP-адреса
 - ☐ ipconfig /renew

27. Сетевые устройства.

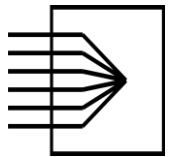
Сетевые устройства - устройства позволяют осуществлять связь с другими сетевыми устройствами или устройствами конечного пользователя.

- Устройства, которые связывают конечного пользователя с сетью, называются также **оконечными узлами или станциями (host)**. Примером таких устройств является обычный персональный компьютер или **рабочая станция**.
- Для работы в сети каждый **хост** оснащен **платой сетевого интерфейса (Network Interface Card — NIC)**, также называемой **сетевым адаптером**.
- Сетевой адаптер представляет собой печатную плату, которая вставляется в слот на материнской плате компьютера, или внешнее устройство. Каждый адаптер NIC имеет уникальный код, называемый MAC-адресом. Этот адрес используется для организации работы этих устройств в сети. Сетевые устройства обеспечивают транспортировку данных, которые необходимо передавать между устройствами конечного пользователя. Они удлиняют и объединяют кабельные соединения, преобразуют данные из одного формата в другой и



управляют передачей данных. Примерами устройств, выполняющих перечисленные функции, являются **повторители, концентраторы, мосты, коммутаторы и маршрутизаторы**.

- Модем - Специальный вид сетевого адаптера для передачи данных по телефонным каналам связи:
 - Аналоговый модем
 - ISDN модем
 - 3G модем
- **Повторители (repeater)** представляют собой сетевые устройства, функционирующие на первом (физическом) уровне эталонной модели OSI. Целью использования повторителя является регенерация и ресинхронизация сетевых сигналов на битовом уровне, что позволяет передавать их по среде на большее расстояние.
- **Концентратор (hub)** – устройство для создания сетей Ethernet на основе витой пары
 - Физическая топология – звезда
 - Логическая топология – общая шина
 - ☐ Работают на физическом уровне
 - ☐ Соединяют в единую среду кабели, идущие по всем портам
 - ☐ Данные, поступающие на порт концентратора, передаются на все другие порты, не зависимо от адреса назначения
- **Мост (bridge)** представляет собой устройство второго уровня, предназначенное для создания двух или более сегментов локальной сети LAN, каждый из которых является отдельным коллизийным доменом. Иными словами, мосты предназначены для более рационального использования полосы пропускания. Целью моста является фильтрация потоков данных в LAN-сети с тем, чтобы локализовать внутрисегментную передачу данных и вместе с тем сохранить возможность связи с другими частями (сегментами) LAN-сети для перенаправления туда потоков данных. Мост собирает информацию о том, на какой его стороне (порте) находится конкретный MAC-адрес, и принимает решение о пересылке данных на основании соответствующего списка MAC-адресов. Мосты осуществляют фильтрацию потоков данных на основе только MAC-адресов узлов.
- **Коммутатор (switch)** — устройство, предназначенное для соединения нескольких узлов компьютерной сети в пределах одного или нескольких сегментов сети.
 - Коммутатор работает на канальном уровне:
 - Анализирует содержимое кадров
 - Извлекает адрес получателя
 - Передает кадр только одному получателю
- **Маршрутизатор** – устройство, объединяющее несколько сетей
 - Умеет согласовывать различия в сетях
 - Имеет несколько сетевых интерфейсов и адрес в каждой сети, к которой подключен
 - Маршрутизаторы способны выбирать наилучший путь в сети для передаваемых данных.
 - Функционируя на третьем уровне, маршрутизатор может принимать решения на основе сетевых адресов вместо использования индивидуальных MAC-адресов второго уровня.
 - Маршрутизаторы также способны соединять между собой сети с различными технологиями второго уровня.



- **брандмауэр (firewall)** используется либо по отношению к программному обеспечению, работающему на маршрутизаторе или сервере, либо к отдельному аппаратному компоненту сети.
 - Брандмауэр защищает ресурсы частной сети от несанкционированного доступа пользователей из других сетей. Работая в тесной связи с программным обеспечением маршрутизатора, брандмауэр исследует каждый сетевой пакет, чтобы определить, следует ли направлять его получателю.
- **Точка доступа (Access Point — AP)**, называемая также базовой станцией, представляет собой беспроводной приемопередатчик локальной сети LAN, который выполняет функции концентратора, т.е. центральной точки отдельной беспроводной сети, или функции моста — точки соединения проводной и беспроводной сетей. Использование нескольких точек AP позволяет обеспечить выполнение функций роуминга (roaming), что предоставляет пользователям беспроводного доступа свободный доступ в пределах некоторой области, поддерживая при этом непрерывную связь с сетью.

28. Преобразование сетевых адресов (NAT).

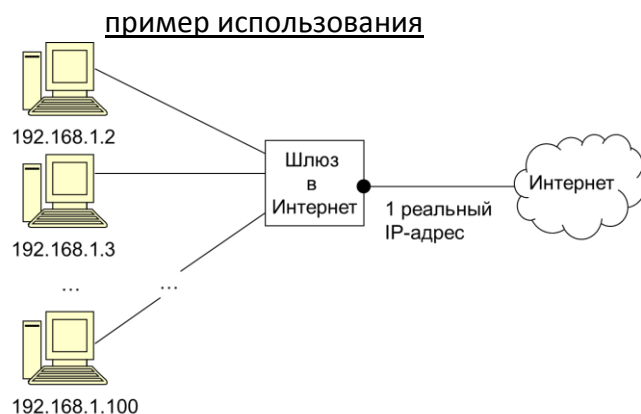
Трансляция сетевых адресов (Network address translation, NAT) – изменение IP-адреса отправителя в пакете

Причины использования:

- I. Нехватка сетевых адресов IPv4
- m. Желание скрыть структуру сети – увеличение безопасности

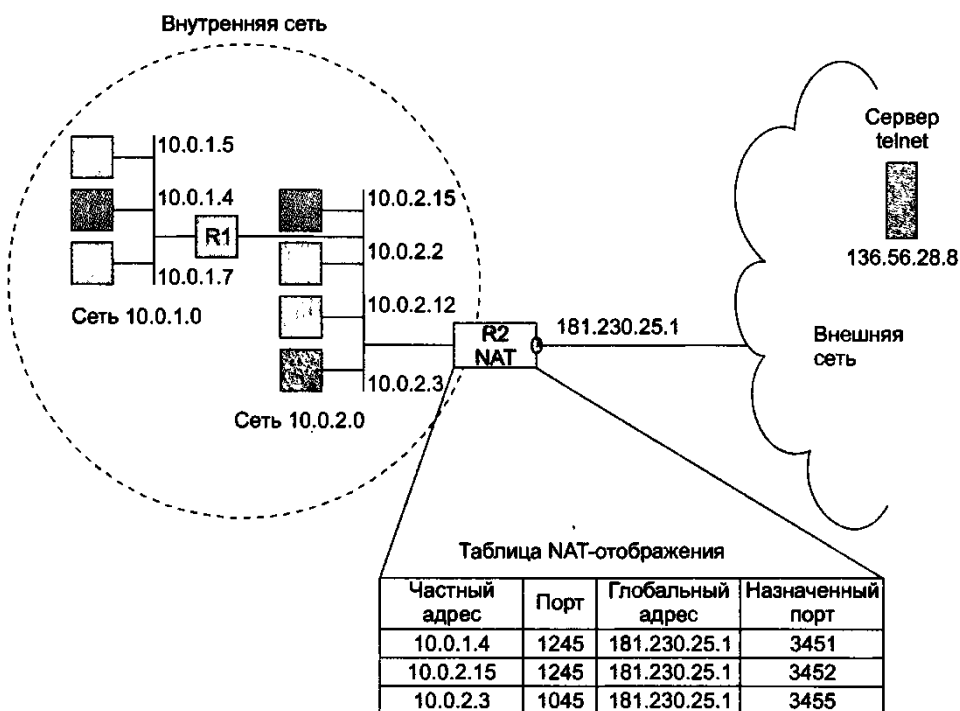
Схема работы NAT

- Преобразованием адресов занимается устройство NAT
 - ☐ Имеет 2 интерфейса и 2 IP-адреса
 - ☐ Один адрес из внутренней сети из диапазона частных адресов
 - ☐ Второй адрес из сети Интернет, реальный адрес
- При поступлении пакета устройство NAT:
 - ☐ Меняет IP-адрес отправителя из внутренней сети на внешний IP-адрес
 - ☐ Меняет Порт отправителя на некоторый уникальный номер порта
 - ☐ Запоминает соответствие Исходные IP-адрес и порт – новый порт в таблице NAT
- При получении ответа на пакет из Интернет устройство NAT:
 - ☐ Ищет номер порта получателя в таблице NAT
 - ☐ Извлекает из таблицы внутренний IP-адрес и порт получателя
 - ☐ Заменяет IP-адрес получателя на внутренний IP-адрес
 - ☐ Заменяет порт получателя на реальный номер порта



- ☐ Отправляет пакет по указанному адресу

Пример



- В тупиковой сети А используются внутренние адреса из блока 10.0.0.0.
- Внешнему интерфейсу маршрутизатора этой сети поставщиком услуг назначен адрес 181.230.25.1.
- Когда хост 10.0.1.4 внутренней сети посылает во внешнюю сеть пакет серверу telnet, то он в качестве адреса назначения использует его глобальный адрес 136.56.28.8.
- Пакет поступает маршрутизатору R1, который знает, что путь к сети 136.56.0.0/16 идет через пограничный маршрутизатор R2.
- Модуль NAPT маршрутизатора R2 транслирует адрес 10.0.1.4 и порт TCP 1245 источника в глобально уникальный адрес 181.230.25.1 и уникально назначенный TCP-порт, в приведенном примере — 3451. В таком виде пакет отправляется во внешнюю сеть и достигает сервера telnet.
- Когда получатель генерирует ответное сообщение, то он в качестве адреса назначения указывает единственный зарегистрированный глобальный адрес внутренней сети, являющийся адресом внешнего интерфейса NAPT-устройства.
- В поле номера порта получателя сервер помещает назначенный номер TCP-порта, взятый из поля порта отправителя пришедшего пакета.
- При поступлении ответного пакета на NAPT-устройство внутренней сети именно по номеру порта в таблице трансляции выбирается нужная строка. По ней определяется внутренний IP-адрес соответствующего узла и действительный номер порта.
- Эта процедура трансляции полностью прозрачна для конечных узлов.

Преимущества:

- Независимость от количества внешних IP-адресов
- Безопасность

Недостатки:

- Нет возможности установить соединение с компьютерами во внутренней сети из внешнего мира

Статическое отображение – трансляция по фиксированным правилам

- Отображать некоторые внутренние IP-адреса на фиксированные внешние IP-адреса
 - Требуется несколько IP-адресов

- Отображать хорошо известные порты одного внешнего IP-адреса на фиксированные внутренние IP-адреса и порты
 - Порт 80 → Внутренний адрес Web-сервера и порт 80
 - Порт 25 → Внутренний адрес почтового сервера и порт 25
 - Порт 21 → Внутренний адрес FTP сервера и порт 21