

Части курса:

1. Основная теория
2. Практика по настройке сети
3. Клиент-серверное приложение

**Литература:** Таненбаум «Компьютерные сети»; Олифер, Олифер «Компьютерные сети».  
Будет 2-3 тестирования, без них не будет допуска к экзамену

## 1 История развития компьютерных сетей

Прародитель компьютерных сетей — телефонные сети (MAN). Сети, с которыми привыкли взаимодействовать, называются LAN.

DARPA — оборонная компания USA, создатель сети Internet.

Типы компьютерных сетей:

1. По территориальному признаку;
2. По типу среды передачи данных;
3. По архитектуре сети;

Рассмотрим эти пункты подробнее:

**Территориальный признак:**

1. Глобальные сети (страны, интернет);
2. Локальные сети (несколько городов);

**Тип среды передачи данных:**

1. Проводные сети;
  - (a) Телефон:
    - i. Витая пара (4 проводка);
    - ii. «Лопша» (2 проводка) и это не витая пара.
  - (b) Витая пара:
    - i. 4-8 проводков
    - ii. Экранированная/неэкранированная/дважды экранированная витая пара;
    - iii. Экранированная витая пара представляет собой заключенную в проводящий материал витую пару.
    - iv. Дважды экранированная витая пара имеет дополнительный экран, который покрывает все витые пары.
  - (c) Оптоволокно:
    - i. Трубка из гнувшегося стекла, покрытого отражающим материалом. Свет отражается от стенок.
    - ii. Скорости передачи - гигабайты в секунду.

(d) Коаксиал

(e) pass

## 2. Беспроводные сети;

(a) WiFi (2,4 ГГц, 5 ГГц);

- i. Максимальное расстояние, заявленное в спецификации — 300 метров. В условиях зданий - 10-20 метров.
- ii. Скорость данных (300 Мбит для 5 ГГц).

(b) LiFi;

- i. Световые волны (световая передача данных).
- ii. Скорости до 1 Гбит.

(c) Спутниковая связь;

- i. Примеры технологий: GPS, спутниковый телефон.

(d) Инфракрасный порт;

- i. Передача данных в прямой видимости.
- ii. Скорость достаточно низкая (Килобиты).

(e) Bluetooth;

- i. Средняя скорость.
- ii. Дальность до 30 метров.

(f) Сотовая связь;

- i. Дальность  $\approx 20 - 30$  км.

(g) Радиосвязь;

- i. Требуется приемник и передатчик.
- ii. Влияют длина волны, частота.

(h) Фотоэлемент;

(i) NFC;

- i. Магнитное поле.

## Архитектура сети:

### 1. Топология сети (способ организации узлов);

(a) Полносвязные топологии (каждый-с-каждым).

- i. Полносвязная топология
  - А. Плюсы: нет посредников (высокая скорость), надежность.
  - В. Минусы: себестоимость, сложность настройки.

(b) Ячеистые (неполносвязные).

- i. Топология «Кольцо».
  - А. Плюсы: стоимость, простота;
  - В. Минусы: средняя надежность, средняя сложность.

С. Технологии (Token Ring и FDDI).

ii. Топология «Звезда».

iii. Топология «Дерево».

iv. Топология «Общая шина».

А. Технология Ethernet работает по этой топологии.

(с) Смешанные топологии.

2. Протокол;

**Проблема.** Узнать о скоростях передачи данных через все проводные соединения.

## 2 Адресация в компьютерных сетях

Типы адресов:

1. unicast (192.168.0.1);

2. multicast (192.168.0.255);

3. broadcast (255.255.255.255);

Виды глобальных адресов:

- IP-адрес;
- MAC-адрес (6F.1A.48.21.40.FE) — адрес сетевой карты; первые несколько бит — код производителя.

Адресация:

- Классовая. Вид:

<i>A</i>	0	адрес сети 7 бит	адрес узла 24 бит
<i>B</i>	10	адрес сети 14 бит	адрес узла 16 бит
<i>C</i>	110	адрес сети 21 бит	адрес узла 8 бит
<i>D</i>	1110	многоадресная	рассылка
<i>E</i>	1111	зарезервировано	

- Безклассовая

Для примера возьмем адрес 192.168.131.15;

Чтобы выделить 16 компьютеров нам требуется выделить 4 бита. Введем для этого маску 11...1.11...1.11...1.11110000 (количество нулей равно количеству выделенных байтов). Применив поразрядную конъюнкцию к IP и маске получим адрес сети.

**Виды IP-адресации:**

- IP v4 (4 байта адреса);
- IP v6 (6 байт адреса)

## 3 Коммутация

Коммутация:

- Каналов
- Пакетов

Мультиплексирование/демультиплексирование (Mux/Demux).

Мультиплексирование — «уплотнение» каналов в один. Демультиплексирование - обратная операция. Аналогично с пакетами.

## 4 Маршрутизация

Маршрутизация:

1. Статическая;
2. Динамическая;

Таблица маршрутизации применяется для статической маршрутизации и составляется вручную.

Динамическая маршрутизация автоматически определяет хороший путь для связи.

Маршрутизатор — устройство, осуществляющее маршрутизации.

## 5 Сетевые устройства

1. Сетевая карта/сетевой интерфейс.
2. Коммутатор/switch/hub.
3. Маршрутизатор.
4. Хаб/концентратор.
5. Mux/Demux.
6. Модем.
7. Повторитель.
8. Точка доступа.

## 6 Стандартизация сетей

- ISO;
- IEEE;
- Модель OSI;
- Эталонная модель OSI (7 уровней);

- Стандартная модель OSI (4 уровня).

Рассмотрим эталонную модель. Уровни:

1. Физический (Технологии ADSL, ISDN, ATM, RS-х, FDDI, );
  - (a) Определяет характеристики сигналов;
  - (b) Среду передачи данных;
  - (c) Физическую топологию среды;
  - (d) Спецификацию среды передачи данных;
  - (e) Интерфейсы оборудования;
  - (f) Напряжение, соответствующее нулю и единице;
  - (g) Время длительности бита;
  - (h) Как начинается и заканчивается передача данных;
  - (i) Количество проводов для соединения;
2. Канальный (Технологии Ethernet, протокол PtPP);
  - (a) Взаимодействие со средой передачи данных (MAC);
  - (b) Надежная доставка (с использованием контрольных сумм);
  - (c) Управление потоком (управление буфером данных);
  - (d) Функции исправления ошибок (в режимах Дуплекс (передача в обе стороны одновременно)/Полудуплекс (попеременно в обе стороны));
3. Сетевой (Протокол IP);
  - (a) Управление подсетью;
  - (b) Определяет маршруты;
  - (c) Соединяет разнородные сети (шлюз (чаще всего входит в состав маршрутизатора));
  - (d) Передача дейтаграмм;
  - (e) Адресация узлов в текущей подсети;
  - (f) best effort delivery — доставка с максимальной доступной скоростью;
  - (g) На этом уровне работают протоколы (IP (Internet Protocol), ARP (Address Resolution Protocol), RARP (Reverse ARP), ICMP (), DHCP (Dynamic Host Control Protocol));
4. Транспортный (TCP, UDP);
  - (a) Надежность передачи данных;
    - i. Контроль ошибок:
      - A. Искажение данных
      - B. Потеря данных
      - C. Дублирование
      - D. Изменение порядка следования

- ii. Контроль потока данных;
  - (b) Сегментирование потока данных и его обратная сборка;
  - (c) Обеспечивает совместный доступ к потоку данных;
  - (d) Протоколы: TCP (Transport Control Protocol), UDP (User Datagram Protocol);
5. Сеансовый (POP);
- (a) Организует сеансы связи;
    - i. Устанавливает;
    - ii. Поддерживает;
    - iii. Разрывает;
    - iv. Обеспечивает синхронизацию передачи данных;
6. Представительский (POP/SMTP, SNMP, Telnet, HTTP, FTP, DNS);
- (a) Сопоставление семантики и синтаксиса данных;
  - (b) Преобразование;
  - (c) Кодирование/декодирование данных;
7. Прикладной (WEB, Email).
- (a) Обеспечение взаимодействия между пользователем и сетью.
  - (b) Предоставляет службы:
    - i. Электронная почта
    - ii. FTP
    - iii. Telnet

Имеется связь (интерфейс) между соседними уровнями. Каждый уровень имеет протокол.

Обработка и передача сообщений.

Имеется некоторое сообщение. При переходе на следующий (нижний) уровень перед ним записывают заголовок, который содержит IP-адреса отправителя и получателя, порты, информацию о протоколах, интерфейсах, типе сообщения и тому подобно. После сообщения добавляется концевик, который содержит служебную информацию для проверки правильности доставки сообщения (контрольные суммы). Для каждого уровня заголовки и концевика свои. Таким образом, физический уровень передает уже гораздо больший пакет. После передачи данных пакет проходит обратную «распаковку». Если целостность пакета нарушена, то он будет отброшен.

Порт — идентификатор ID процесса или приложения, для которого предназначается этот пакет.

Можно объединить сеансовый и транспортный уровень, прикладной и представительский, канальный и физический.

## 7 Электронная почта

Основные компоненты электронной почты:

1. Почтовые клиенты:

- (a) Thunderbird;
- (b) Outlook;
- (c) The Bat;

## 2. Почтовые серверы:

- (a) Функции:
  - i. Хранение
  - ii. Отправка
  - iii. Организация очередей
- (b) Состав:
  - i. MDA (агент проверки доставки сообщений)
  - ii. MTA (агент отправки сообщений)
  - iii. MUA (user-agent);
- (c) Примеры:
  - i. SendMail;
  - ii. qmail;
  - iii. MS Exchange Server;
  - iv. Postfix;
  - v. Procmal/MailDrop;
  - vi. Exim.
- (d) Протоколы:
  - i. Отправка: SMTP;
  - ii. Перенаправление: POP3;
  - iii. Копирование: IMAP;

## 3. Протоколы получения почты;

## 4. Протоколы отправки почты;

# 8 Протокол SMTP

В качестве команд этого протокола используется ASCII-text. Для передачи данных используется протокол TCP. Стандартный порт протокола — 25.

Схема послыки почты состоит из 3-х этапов:

- 1) Приветствие;
- 2) Пересылка почты;
- 3) Закрытие сессии;

В процессе выполняются следующие команды:

MAIL FROM — устанавливает обратный адрес.

RCPT TO — устанавливает получателя данного сообщения.

DATA — для отправки сообщений.

Протокол получения почты: POP3 (Post Office Protocol). Работает на 110 порту. Он скачивает все письма с сервера, удаляя их на нём.

Аналог: IMAP. 143 порт. Аналог тонкого клиента, который скачивает с сервера лишь заголовки, и копии писем.

По протоколу HTTP тоже можно получать почту. Сверхтонкий клиент, предоставляющий веб-морду к серверу.

Разберем подробно каждый протокол получения почты.

## 8.1 POP3

Стадии:

- 1) Авторизация на сервере;
- 2) Транзакция (скачивание с сервера);
- 3) Обновление (обмен информацией с сервером).

У него больше команд, чем у SMTP:

USER — идентифицирует пользователя с указанным именем;

PASS — указывает пароль для пары клиент-сервер;

QUIT — закрывает TCP соединение;

STAT — возвращает число писем в на сервере;

LIST — запрашивает список сообщений;

RETR — извлекает сообщение с почтового ящика;

DELE — помечает сообщение на удаление;

NOOP (сам NOOB) — сервер возвращает положительный ответ, но не выполняет действий.

LAST — возвращает наибольший размер сообщения из всех, к которым обращались.

RSET — отменяет DELE.

Дополнительные (не входящие в базовую конфигурацию) команды:

APOP — передача на сервер username and password;

UIDL — перенумеровать все сообщения в рамках текущей сессии;

## 8.2 IMAP

Исходное соединение и подтверждение соединения с сервером. Состояния сервера:

- 1) Без аутентификации. Клиент должен предоставить логин и пароль.
- 2) Аутентификация проведена. Клиент выбирает почтовый ящик. Выбор произведен.
- 3) Отклонено. Указали причину. Закрыли сессию.
- 4) Переход от 1 состояния к 2.
- 5) Переход от аутентификации к выбору ящика.
- 6) Если выбор не произведен вернуться к аутентификации.
- 7) Закрытие сессии.

## 9 Протоколы TCP и UDP

### 9.1 UDP

Чтобы передать сообщение по протоколу UDP, нужно совершить следующие действия. Допустим, мы хотим передать сообщение. Мы передаем сообщение, если клиент принял сообщение, то все закончилось. Если нет - тоже закончилось.

Плюсы UDP:



- Минимум действий;
- Быстрая передача данных (минимум задержек);
- Контроль целостности пакета

Минусы:

- Возможны потери

Структура UDP пакета:

0-15	16-31
Порт отправителя	Порт получателя
Длина пакета	Контрольная сумма
Данные, данные, данные	

## 9.2 TCP

Пример. Отправитель запрашивает готовность получателя. Затем они устанавливают соединение. Затем происходит передача данных, причем если пакет не был принят, отправитель отправит его еще раз (и так до 16 раз). Затем сессия закрывается.

Работа:

1. Установка логического соединения (сеанс связи);
2. Пересылка сообщений;
3. Проверки доставки/целостности, повторы недоставленных пакетов;
4. Разрыв сеанса.

Структура:

Порт отправителя			Порт получателя
Порядковый номер			
Номер подтверждения			
Длина заголовка	////////	Флаги (6 бит)	Окно получателя
Контрольная сумма			Указатель срочных данных
Параметры			
Много данных (1500 Eth, 2272 Wi-Fi, 4500 FDDI)			

Флаги:

- IRG — важность.
- ACK — номер подтверждения.
- PSH — сокращение от Push. Протолкнуть данные, накопившиеся в буфере.
- RST — умышленный обрыв соединения/сброс буфера.
- SYN — синхронизация.
- FIN — завершение соединения.

Плюсы:

- Надежность;
- Порядок пакетов.

Минусы:

- Скорость.
- Задержки.

## 10 Служба DNS.

Все компьютеры в сети имеют IP-адреса. Но запомнить IP трудно, поэтому были придуманы доменные имена типа vk.com. Доменные имена обладают своими иерархиями.

$$\underbrace{apmath}_{\text{адрес сайта}} . \underbrace{spb}_{\text{домен второго уровня}} . \underbrace{ru}_{\text{старш. домен}}$$

DNS — система, занимающаяся сопоставлением доменных имен и IP-адресов. Бывает двух видов:

- Централизованная — единственный сервер, на котором лежит таблица со всем этим добром. Из минусов — нагруженность сервера и ненадежность.
- Распределенная — несколько серверов, которые хранят копии одной таблицы.

## 11 Аспекты сетевой безопасности.

Аспекты:

1. Конфиденциальность;
2. Целостность данных;
3. Аутентификация;
4. Доступность.

Сетевые угрозы:

1. Сниффинг («прослушка» пакетов).
2. Аутентификация:
  - (a) Перехват пароля/ключа;
  - (b) Подбор пароля (brute force).
3. Недостаточная аутентификация.
4. MitM — man-in-the-middle.
5. Лавинные атаки.

- (a) Недостаточное сопротивление автоматизации (атака ботов — DoS). Борьба — Captcha.
  - (b) Распределенная лавинная атака (DDoS).
  - (c) Флуд.
6. Вирусы, сетевые черви, трояны.
7. Сетевая разведка.
- (a) Скан портов
  - (b) Заметание следов
  - (c) Инъекции SQL, PHP
  - (d) Переполнение буфера
  - (e) Атака на функции форматирования строк
8. Выполнение команд операционной системы.

Защита:

1. Сигнатурный (качественный анализ трафика)
2. Статистический
3. Гибридный.

Защита от вирусов:

1. Антивирус.
2. Компьютерная гигиена (мойте компьютер перед выходом в интернет, дети).
3. Виртуальная машина (или любая другая песочница).
4. Не подключаться к сети, залить все порты эпоксидкой и выковырять дисковод
5. He-windows.
6. Admin/user.

## 12 SPAM

Виды спама:

1. Реклама
2. Вирусы
3. Фишинг
4. Антиреклама (черный пиар)
5. Ниггерские (на самом деле — нигерийские) письма

- (a) На жалость
- (b) Богатые больные люди без наследников
- (c) Лотереи

6. Реклама незаконных товаров

7. Реклама спамерских услуг

8. Наука/образование

Борьба со спамом

1. Фильтры

- (a) Статическая фильтрация
- (b) Адаптивная

## 13 Способы защиты сетей. Брандмауэры

Брандмауэр — защита, которая стоит между глобальной и локальной сетью.  
Бывают

1. Аппаратными

2. Программными

Типы:

1. Брандмауэр с фильтрацией пакетов.

Сетевой уровень. Проверяет адрес отправителя и адрес получателя, информацию о приложении или протоколе. Вдобавок следит за портами отправителя и получателя.

(a) Плюсы:

- i. Недорогой или просто поставляется вместе с антивирусом
- ii. Неплохая скорость.

(b) Минусы:

- i. Слабая защита.
- ii. Требуется труд настройка.

2. Шлюз сеансового уровня.

Работает на сеансовом уровне. Следит за квантированием сеанса связи (логикой пакетов).

(a) Канальные посредники: `pipe proxy`.

(b) Аппаратные посредники: `proxy server`.

i. Плюсы:

A. Надежная защита.

ii. Минусы:

- А. Скорость меньше.
- В. Стоит дороже.

### 3. Шлюз прикладного уровня.

Этот парниша работает на прикладном уровне. Он может смотреть в пакет, а значит, его можно настроить на фильтрацию определенных команд, в частности, фильтрацию в том числе и служебной или полезной информации. Существуют так называемые посредники прикладного уровня, которые работают каждый с определенными службами (разные посредники для Telnet и FTP, к примеру). Также этот шлюз занимается проблемами аутентификации.

#### (a) Плюсы:

- i. Надежная защита.

#### (b) Минусы:

- i. Большая стоимость
- ii. Малая скорость работы
- iii. Прозрачность.

### 4. Брандмауэр экспертного уровня.

А этот чувак вообще крутой и объединяет функции предыдущих брандмауэров. Работает напрямую с операционной системой, отслеживает сеансы связи, предоставляет посредников, фильтрует.

#### (a) Плюсы:

- i. Максимальная надежность.

#### (b) Минусы:

- i. Максимальная стоимость.
- ii. Средняя скорость.
- iii. Средняя прозрачность.

Д/З: Найти представителей для всех типов брандмауэров.

Устройства, которые могут выполнять функции брандмауэра (аппаратные):

1. Отдельно выделенный компьютер (бастион). Ему для работы требуется 2 сетевых интерфейса и в этом случае он называется двудомный шлюз.
2. Маршрутизаторы.
3. Шлюз.

## 14 Технология локальных сетей

А именно:

- Ethernet/FE/GE
- Token Ring

- FDDI

Их всех объединяет некоторые свойства:

- Расстояние между узлами 100-2000 метров без повторителя;
- Единый формат адреса (6 байт)
- Раздельная среда передачи данных
- Высокая скорость протоколов
- Простота логики протоколов.

Деление по методу доступа к среде:

1. Случайный доступ (технология Ethernet). Сеть проверяет, можно ли положить кадр, после чего кладет. Но может так произойти, что туда уже положил кадр другой поток. Есть вероятность того, что возникнет коллизия и наш кадр наложится на что-то уже существующее в сети. Поэтому этот доступ также называется CSMA/CC. Преимущества: простой алгоритм, дешевое оборудование, возможность широковещательной передачи данных. Минусы: большие потери данных из-за коллизий (особенно ощутимо при загрузке сети более 50%), ограниченная длина сети.
  - (a) Битовая скорость — 10 Мбит/с
  - (b) Интервал отсрочки — 512 бит.
  - (c) Межкадровый интервал — 9.6 мкс
  - (d) Максимальное число повторов — 16.
  - (e) Максимальное возрастание диапазона паузы — 10
  - (f) Максимальная длина кадра без преамбулы — 1518 байт
  - (g) Минимальная длина кадра — 64 байта
2. Детерминированный доступ (Token Ring, FDDI)
  - (a) Кольцо с маркером
  - (b) Шина с маркером

## 15 Протокол LLC

Относится к уровню управления логическими каналами

Заголовок Ethernet	Кадр LLC
Кадр Ethernet	

Три типа процедур LLC:

- 1) LLC1 — без установления соединения и без подтверждения.
- 2) LLC2 — с установлением соединения и подтверждением.
- 3) LLC3 — без установления соединения, но с подтверждением.

Подробно рассмотрим LLC2.

В нем существуют 3 вида кадров:

- 1) Информационный кадр (полезные данные)

- 2) Управляющий кадр (Команды/ответы)  
 3) Ненумерованный кадр (установление соединения).

Как выглядит кадр:

Флаг	DSAP	SSAP	Управляющее поле	Данные	Флаг
01111110		источник			

Структура поля управления:

Тип кадра	Разряды поля управления															
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Информационный	0	N(S)							P/F	N(R)						
Управляющий	1	0	S		not use				P/F	N(R)						
Ненумерованный	1	1	M		P/F		M		not use							

ДЗ: посмотреть, что за поля скрываются под буковками.

Формат кадра Ethernet

DA	SA	Pr	Data				FCS	что
6	6	2	46-1500				4	размер в байтах
			1	1	1-2	46-1497		отличия LLC
			DSAP	SSAP	Cnt	Data		

Технологии Token Ring и FDDI разберем сами. Я что-то устал :)