Вот ответы на все вопросы по предмету «Компьютерные сети» в соответствии с курсом лекций:

1. Названия уровней модели OSI по порядку (сверху вниз):

1. Прикладной (Application)
2. Представления (Presentation)
3. Сеансовый (Session)
4. Транспортный (Transport)
5. Сетевой (Network)
6. Канальный (Data Link)
7. Физический (Physical)

2. Прикладной уровень (Application Layer):

Функции: Обеспечивает интерфейс между сетевыми службами и приложениями пользователя. Определяет протоколы для обмена данными между приложениями. Управляет доступом к сети.

Примеры протоколов: HTTP, HTTPS, FTP, SMTP, POP3, IMAP, DNS, Telnet, SSH, DHCP, SNMP.

3. Уровень представления данных (Presentation Layer):

Функции: Преобразование данных в форму, понятную прикладному уровню. Кодирование/декодирование, шифрование/дешифрование, сжатие/распаковка данных. Гарантирует, что данные одного приложения будут поняты другим приложением.

Примеры протоколов/стандартов: SSL/TLS (шифрование), MIME (кодирование данных для почты), JPEG, GIF, MPEG (форматы представления данных).

4. Сеансовый уровень (Session Layer):

Функции: Установление, управление, поддержание и завершение сеансов связи между приложениями на разных хостах. Синхронизация диалога (контрольные точки), управление диалогом (дуплекс/полудуплекс).

Примеры протоколов: NetBIOS, PPTP (частично), RPC (Remote Procedure Call), SIP (установление сеансов VoIP).

5. Транспортный уровень (Transport Layer):

Функции: Обеспечение сквозной (end-to-end) доставки данных между процессами на хостах-источнике и назначения. Сегментация данных приложения, контроль ошибок, управление потоком (flow control), мультиплекксирование/демультиплекксирование соединений. Гарантирует надежность доставки (или указывает на ее отсутствие).

Примеры протоколов: TCP (Transmission Control Protocol - надежный, с установлением соединения), UDP (User Datagram Protocol - ненадежный, без установления соединения).

6. Сетевой уровень (Network Layer):

Функции: Определение пути (маршрутизация) пакетов через сеть от источника к получателю. Логическая адресация (IP-адреса), фрагментация/дефрагментация пакетов. Обеспечивает связь между различными сетями.

Примеры протоколов: IP (Internet Protocol), ICMP (Internet Control Message Protocol), IGMP (Internet Group Management Protocol), OSPF, RIP, BGP (протоколы маршрутизации).

7. Канальный уровень (Data Link Layer):

Функции: Обеспечение надежной передачи кадров (frames) между непосредственно соединенными узлами (в пределах одной локальной сети). Физическая адресация (MAC-адреса), обнаружение и (иногда) исправление ошибок передачи, управление доступом к среде (MAC - Media Access Control).

Примеры протоколов: Ethernet (IEEE 802.3), Wi-Fi (IEEE 802.11), PPP (Point-to-Point Protocol), HDLC (High-Level Data Link Control), MAC Sublayer Protocols (CSMA/CD, CSMA/CA).

8. Физический уровень (Physical Layer):

Функции: Передача неструктурированного потока битов по физической среде. Определение электрических, оптических, механических и функциональных характеристик интерфейса со средой передачи. Кодирование сигналов (представление битов в виде электрических/оптических импульсов), синхронизация битов.

Примеры протоколов/технологий: RS-232, V.35, Ethernet (10BASE-T, 100BASE-TX, 1000BASE-SX и т.д.), USB Physical Layer, Bluetooth Physical Layer, спецификации физических сред (витая пара, коаксиальный кабель, оптоволокно).

9. Инкапсуляция и Деинкапсуляция в модели OSI:

Инкапсуляция: Процесс добавления заголовка (а иногда и трейлера) к данным при движении вниз по уровням модели OSI на передающей стороне. Каждый уровень добавляет свою управляющую информацию (протокольный блок данных - PDU) к данным, полученным от уровня выше.

Данные приложения -> Сегмент/Дейтаграмма (Транспорт) -> Пакет (Сеть) -> Кадр (Канальный) -> Биты (Физический).

Деинкапсуляция: Процесс удаления заголовков (и трейлеров) при движении данных вверх по уровням модели OSI на принимающей стороне. Каждый уровень считывает и обрабатывает информацию в заголовке своего уровня, а затем передает оставшиеся данные уровню выше.

Биты -> Кадр (удаляется заголовок/трейлер Канального) -> Пакет (удаляется заголовок Сетевого) -> Сегмент/Дейтаграмма (удаляется заголовок Транспортного) -> Данные приложения.

10. Формулы скорости передачи данных на Физическом уровне:

1. Теоретическая максимальная скорость (Пропускная способность канала):

`$C = 2 B \log_2(M)$` [бит/с]

`C` - Пропускная способность канала (бит/с)

`B` - Ширина полосы пропускания канала (Гц)

`M` - Количество уровней сигнала (количество различных состояний сигнала, используемых для кодирования битов). Для базовых схем: M=2 (0 и 1) -> $\log_2(2)=1$.

Описание: Формула Найквиста. Определяет теоретический предел скорости передачи данных по каналу с заданной полосой пропускания `B` без шума при использовании `M` уровней сигнала. Удвоение связано с теоремой отсчетов (частота Найквиста = 2B).

2. Максимальная скорость с учетом шума (Предел Шеннона):

`$C = B \log_2(1 + S/N)$` [бит/с]

`C` - Пропускная способность канала (бит/с)

`B` - Ширина полосы пропускания канала (Гц)

`S/N` - Отношение сигнал/шум (Signal-to-Noise Ratio). Часто выражается в децибелах (dB): `SNR_db = 10 $\log_{10}$(S/N)`. Тогда `S/N = 10^(SNR_db / 10)`.

Описание: Формула Шеннона-Хартли. Определяет теоретическую максимальную скорость безошибочной передачи данных по каналу с заданной полосой пропускания `B` и отношением сигнал/шум `S/N`, при наличии шума Гауссова типа. Учитывает влияние шума.

11. Физическое кодирование “Код NRZ” (Non-Return to Zero):

Принцип работы: Самый простой метод. Уровень сигнала остается постоянным в течение всего битового интервала.

`0` - представлен одним напряжением (обычно низким, например, 0V).

`1` - представлен другим напряжением (обычно высоким, например, +5V).

Особенности: Нет возврата к нулевому уровню между битами. Нет встроенной синхронизации (проблема при длинных последовательностях нулей или единиц - приемник теряет синхронизацию битов). Требует отдельной линии тактового сигнала или сложных методов восстановления тактовой частоты. Уязвим к постоянной составляющей (DC bias).

12. Физическое кодирование “Манчестер-II”:

Принцип работы: Каждый битовый интервал разделен на две половины. Переход уровня сигнала происходит в середине каждого битового интервала. Этот переход используется для синхронизации.

`0` - представлен переходом от высокого уровня к низкому в середине интервала.

`1` - представлен переходом от низкого уровня к высокому в середине интервала.

Особенности: Синхронизация встроена в сигнал (нет проблемы длинных последовательностей одинаковых битов). Нет постоянной составляющей (DC balance). Требует вдвое большей полосы пропускания, чем NRZ для той же скорости передачи данных (частота перехода вдвое выше битовой скорости). Широко использовался в классическом Ethernet (10 Мбит/с).

13. Физическое кодирование “PAM-5” (5-Level Pulse Amplitude Modulation):

Принцип работы: Использует 5 различных уровней напряжения амплитуды импульса для кодирования информации. Позволяет передавать несколько бит на

одном символе (символе линии). В Gigabit Ethernet (1000BASE-T) используется 4D-PAM5: каждые 2 бита данных кодируются в один из 5 уровней напряжения на одной из 4 витых пар в кабеле одновременно (двунаправленная передача по всем парам).

Особенности: Позволяет достигать высоких скоростей (1 Гбит/с и выше) по медной витой паре категории 5e. Более сложная схема модуляции по сравнению с бинарными (двухуровневыми). Требует сложных методов коррекции ошибок и выравнивания канала из-за межсимвольной интерференции.

14. Логическое кодирование (код 4B/5B):

Принцип работы: Каждой группе из 4 бит данных ставится в соответствие 5-битный код. Эти 5-битные коды выбираются из таблицы так, чтобы гарантировать достаточное количество переходов сигнала (для синхронизации) и отсутствие длинных последовательностей нулей. Затем 5-битный код передается с использованием физического кодирования (например, NRZI).

Преимущества:

Синхронизация: Обеспечивает достаточное количество переходов сигнала в потоке данных, устраняя проблему длинных последовательностей нулей, присущую базовым NRZ/NRZI.

Контроль ошибок: Некоторые недопустимые 5-битные коды могут использоваться для индикации ошибок.

Эффективность: Избыточность 20% (5 бит для передачи 4 бит данных) лучше, чем у Манчестера (100% избыточность). Пропускная способность канала используется эффективнее.

Применение: Использовался в Fast Ethernet (100BASE-TX) поверх физического кодирования MLT-3.

15. Структура СКС (Структурированная Кабельная Система):

Структура: Иерархическая система кабелей и коммутационных элементов (кроссов, патч-панелей), удовлетворяющая стандартам (TIA/EIA-568). Состоит из подсистем:

1. Горизонтальная подсистема: От телекоммуникационной розетки на рабочем месте до горизонтального кросса (HC) в телекоммуникационном шкафу/комнате этажа. Используется витая пара Cat 5e/6/6a/7 или оптоволокно.

2. Магистральная подсистема: Соединяет телекоммуникационные комнаты этажей (HC) с главным кроссом (MC) здания и кроссами комплекса зданий (IC). Используется многопарный кабель UTP/STP или (чаще) многожильное оптоволокно.

3. Подсистема рабочего места: Кабель от розетки до оконечного оборудования (ПК, телефон).

4. Аппаратная/Телекоммуникационная комната: Размещение кроссового оборудования (патч-панели, коммутаторы, маршрутизаторы) для горизонтальной подсистемы и подключения к магистрали.

Пример типовой проводки по зданию:

Этаж: В телекоммуникационных шкафах (TR) на каждом этаже установлены патч-панели для горизонтальной разводки и активное оборудование (коммутаторы).

Горизонтальная разводка: Кабели витой пары Cat 6 идут от патч-панелей в TR к розеткам на рабочих местах в офисах этого этажа.

Магистраль: Оптоволоконные кабели (многомодовые или одномодовые) идут от патч-панелей в TR каждого этажа вертикально вниз/вверх в Главную аппаратную (MDF/ER) в подвале/цоколе здания.

Главная аппаратная (MDF/ER): Содержит главные патч-панели, магистральные коммутаторы/маршрутизаторы, оборудование связи с внешним миром (телефония, интернет).

16. CSMA/CD (Carrier Sense Multiple Access with Collision Detection):

Суть: Протокол доступа к разделяемой среде передачи (например, классический Ethernet на коаксиале или хабах).

Принципы работы:

1. Прослушивание несущей (Carrier Sense): Узел, желающий передать, сначала прослушивает среду. Если среда свободна (нет несущей), он начинает передачу.

2. Множественный доступ (Multiple Access): Несколько узлов имеют равный доступ к одной и той же среде.

3. Обнаружение коллизий (Collision Detection): Во время передачи узел продолжает прослушивать среду. Если он обнаруживает, что сигнал в среде отличается от передаваемого им (из-за наложения сигналов от другого узла), это означает коллизию.

4. Прекращение передачи: При обнаружении коллизии узел немедленно прекращает передачу.

5. Отправка Jam-сигнала: Узел посылает короткий сигнал "затора" (jam), чтобы все узлы в сегменте узнали о коллизии.

6. Ожидание и повтор: Каждый участвовавший в коллизии узел ожидает случайный промежуток времени (определяемый алгоритмом отката - backoff

algorithm, обычно бинарная экспоненциальная задержка), а затем повторяет попытку передачи с шага 1.

17. Простейший концентратор (Hub, Повторитель):

Принцип работы:

1. Работает на Физическом уровне (L1) модели OSI.
2. Принимает электрический (или оптический) сигнал на один из своих портов.
3. Усиливает (регенерирует) этот сигнал.
4. Ретранслирует (дублирует) усиленный сигнал на все свои остальные порты (кроме порта, с которого сигнал пришел).

Последствия: Создает единый домен коллизий - все устройства, подключенные к хабу (и к другим хабам, соединенным с ним), конкурируют за одну и ту же среду передачи с помощью CSMA/CD. Пропускная способность сети делится между всеми устройствами. Не фильтрует трафик по MAC-адресам. Не знает топологию сети.

18. Широковещательный шторм (Broadcast Storm):

Что это: Состояние сети, при котором она перегружается огромным количеством широковещательных (или иногда многоадресных) пакетов, лавинообразно генерируемых и ретранслируемых устройствами.

Причины появления:

1. Петли в топологии (L2 loops): Физические или логические петли в сети на канальном уровне (L2), особенно при отсутствии STP (Spanning Tree Protocol) или его сбое. Широковещательный пакет, попав в петлю, бесконечно циркулирует по сети, копируясь коммутаторами на каждом обороте.
2. Неисправное оборудование/софт: Сетевые карты или драйверы, генерирующие бесконечные широковещательные пакеты (например, при сбое).
3. Злонамеренные атаки: Намеренная генерация широковещательного трафика для отказа в обслуживании (DoS).
4. Протоколы, генерирующие широковещания: Неконтролируемое использование протоколов типа ARP, DHCP, NetBIOS в очень больших плоских сетях (без VLAN).

Последствия: Полная или почти полная потеря полезной пропускной способности сети, так как вся доступная полоса заполняется штормовым трафиком. Зависание устройств. Трудности с диагностикой и управлением сетью.

19. Коммутатор 2 уровня (L2 Switch):

Принцип работы:

1. Работает на Канальном уровне (L2) модели OSI. Оперирует MAC-адресами.

2. Таблица MAC-адресов (CAM-таблица): Строит таблицу соответствия MAC-адресов устройств номерам портов, на которых они "живут". Делает это, изучая исходный MAC-адрес (Source MAC) входящих кадров.

3. Прием кадра: Получает кадр Ethernet на один из своих портов.

4. Фильтрация и Переадресация:

Смотрит на MAC-адрес назначения (Destination MAC) в кадре.

Ищет этот MAC в своей таблице:

Если MAC найден в таблице и он связан с другим портом (не тем, откуда пришел кадр) -> Коммутатор пересылает кадр только на этот конкретный порт (точка-точка).

Если MAC найден в таблице и он связан с тем же портом, откуда пришел кадр -> Коммутатор отбрасывает кадр (фильтрация в пределах одного сегмента).

Если MAC не найден в таблице -> Коммутатор затопляет (flood) кадр на все свои порты, кроме того, откуда он пришел (как хаб, но только для неизвестных адресов).

Если MAC назначения - Широковещательный (FF:FF:FF:FF:FF:FF) или Многоадресный (Multicast) -> Коммутатор по умолчанию затопляет кадр на все порты, кроме исходного (если не настроено IGMP Snooping для многоадресности).

5. Создание доменов коллизий: Каждый порт коммутатора представляет собой отдельный домен коллизий (в отличие от хаба). Полнодуплексная связь устраняет коллизии на портах.

6. Логическая сегментация: Разбивает один широковещательный домен (домен L2) на множество доменов коллизий, но сам по себе не сегментирует широковещательные домены (все порты в одном VLAN по умолчанию - один широковещательный домен).

20. Коммутатор 3 уровня (L3 Switch):

Принцип работы: Сочетает функциональность коммутатора L2 и маршрутизатора.

1. Коммутация L2: На канальном уровне работает как обычный L2 коммутатор (фильтрация/пересылка по MAC, создание доменов коллизий).

2. Маршрутизация L3: На сетевом уровне (L3) способен маршрутизировать трафик между разными IP-подсетями/VLAN. Для этого он:

Имеет IP-адреса, назначенные на свои виртуальные интерфейсы (SVI - Switched Virtual Interface), каждый из которых представляет собой шлюз по умолчанию для своей VLAN.

Строит таблицу маршрутизации (RIB - Routing Information Base), используя статические маршруты или динамические протоколы маршрутизации (RIP, OSPF, EIGRP).

Принимает решение о пересылке пакетов на основе IP-адреса назначения и таблицы маршрутизации.

3. Аппаратная маршрутизация (ASIC): Ключевое отличие от "программных" маршрутизаторов - коммутаторы L3 выполняют маршрутизацию на аппаратном уровне с помощью специализированных микросхем (ASIC). Это обеспечивает очень высокую скорость маршрутизации (часто на скорости коммутации проводов - wire speed), сравнимую со скоростью коммутации L2.

4. Коммутация на основе потока (Flow-Based): Первый пакет в новом потоке (между парой IP-адресов) обрабатывается процессором маршрутизации (CPU), который определяет путь (интерфейс и следующий хоп) и создает запись в кеше коммутации (FIB - Forwarding Information Base). Последующие пакеты этого потока пересылаются на аппаратном уровне (ASIC) по информации из FIB, что и обеспечивает высокую скорость.

21. Маршрутизатор (Router):

Принцип работы:

1. Работает на Сетевом уровне (L3) модели OSI. Оперирует IP-адресами.

2. Интерфейсы: Имеет несколько сетевых интерфейсов (портов), каждый подключен к разной IP-сети/подсети.

3. Таблица маршрутизации (Routing Table): Содержит информацию о том, как достичь других сетей. Включает:

Сеть назначения / Маска: Целевая IP-сеть.

Next-Hop (Следующий прыжок): IP-адрес следующего маршрутизатора на пути к сети назначения.

Выходной интерфейс: Локальный интерфейс, через который нужно отправить пакет к next-hop.

Метрика: "Стоимость" маршрута (используется протоколами для выбора лучшего пути).

Источник: Как получен маршрут (прямо подключенная сеть, статический маршрут, динамический протокол - RIP, OSPF и т.д.).

4. Принятие решения о маршрутизации:

Получает пакет на одном из своих интерфейсов.

Смотрит на IP-адрес назначения в пакете.

Ищет в таблице маршрутизации наиболее специфичный (с самой длинной маской) маршрут, который соответствует адресу назначения.

Если маршрут найден:

Уменьшает TTL (Time To Live) в IP-заголовке на 1 (если TTL=0, пакет отбрасывается, отсылается ICMP Time Exceeded).

Пересчитывает контрольную сумму IP-заголовка.

Инкапсулирует IP-пакет в новый кадр канального уровня (L2) для интерфейса, указанного в маршруте (с новыми MAC-адресами источника и назначения для следующего сегмента).

Передает кадр через указанный выходной интерфейс.

Если маршрут не найден -> пакет отбрасывается, отсылается ICMP Destination Unreachable.

5. Соединение сетей: Основная задача - соединять разные IP-сети/подсети, изолируя широковещательные домены (каждый интерфейс маршрутизатора - граница широковещательного домена).

6. Выполнение протоколов маршрутизации: Обменивается информацией о сетях с другими маршрутизаторами для автоматического построения и обновления таблиц маршрутизации (RIP, OSPF, BGP и т.д.).

22. Виртуальные локальные сети (VLAN - Virtual Local Area Network):

Что это: Технология, позволяющая логически сегментировать один физический коммутируемый домен L2 на несколько изолированных широковещательных доменов.

Суть: Приписывание портов коммутатора к определенному VLAN. Порты, принадлежащие разным VLAN, не могут обмениваться данными на канальном уровне (L2), даже если они подключены к одному и тому же физическому коммутатору. Обмен между VLAN возможен только через маршрутизацию (L3) - либо на маршрутизаторе, либо на коммутаторе L3.

Преимущества:

Логическая группировка: Группировка устройств по функциям (бухгалтерия, отдел продаж), а не по физическому расположению.

Сокращение широковещательных доменов: Уменьшает область распространения широковещательного трафика, повышая производительность и безопасность.

Повышение безопасности: Изоляция трафика между VLAN (без маршрутизации устройства из разных VLAN не видят друг друга).

Гибкость управления: Упрощение перемещений устройств между группами (достаточно изменить настройку VLAN на порту коммутатора).

Теггирование (802.1Q): Для передачи трафика нескольких VLAN по одному физическому каналу (транк - trunk) между коммутаторами используется стандарт IEEE 802.1Q. В кадр Ethernet добавляется VLAN Tag (4 байта) между полями Source MAC и EtherType/Length, содержащий идентификатор VLAN (VID - 12 бит, диапазон 1-4094).

23. Названия уровней модели стека TCP/IP по порядку (сверху вниз):

1. Прикладной (Application)
2. Транспортный (Transport)
3. Сетевой (Internet)
4. Канальный (Network Access / Link)

24. Различия TCP и UDP:

Характеристика	TCP (Transmission Control Protocol)	UDP (User Datagram Protocol)
Надежность	Надежный (гарантированная доставка)	Ненадежный (доставка не гарантирована)
Установление соединения	С установлением соединения (3-way handshake)	Без установления соединения (connectionless)
Порядок доставки	Гарантирует порядок доставки сегментов	Не гарантирует порядок доставки дейтаграмм
Контроль потока	Есть (механизм скользящего окна)	Нет

| Контроль перегрузки | Есть (механизмы предотвращения перегрузки) | Нет |

| Заголовок | Большой (20 байт минимум + опции), сложный | Маленький (8 байт), простой |

| Накладные расходы | Высокие | Низкие |

| Использование | HTTP, HTTPS, FTP, SMTP, Telnet, SSH | DNS, DHCP, SNMP, VoIP (RTP), видеостриминг, TFTP |

| Структура PDU | Сегмент (Segment) | Дейтаграмма (Datagram) |

25. Пример адресации на разных уровнях TCP/IP:

Прикладной уровень (Application): Имена доменов (например, `www.example.com` - преобразуются DNS в IP), Имена служб/Порты (например, `http://` указывает на порт 80).

Транспортный уровень (Transport): Номера портов (Port Numbers). Например:

IP-пакет от `192.168.1.100:54321` (исходный IP:порт) к `93.184.216.34:80` (IP назначения:порт).

Порт назначения указывает на приложение (веб-сервер на порту 80).

Исходный порт идентифицирует сеанс на клиенте.

Сетевой уровень (Internet): IP-адреса (например, `192.168.1.100` - источник, `93.184.216.34` - назначение). Уникально идентифицируют хост в сети.

Канальный уровень (Network Access): MAC-адреса (например, `00:1A:2B:3C:4D:5E` - источник, `00:0C:29:XX:XX:XX` - назначение (MAC шлюза или соседа)). Уникально идентифицируют сетевой интерфейс в локальном сегменте сети.

26. Типы рассылок в TCP/IP:

1. Юникаст (Unicast): От одного отправителя одному конкретному получателю (определенному по уникальному IP-адресу). Стандартный тип связи (веб-серфинг, почта, FTP).

2. Широковещательная рассылка (Broadcast): От одного отправителя всем устройствам в локальной сети (L2 широковещательный домен).

L2 Broadcast: MAC-адрес назначения = `FF:FF:FF:FF:FF:FF`.

L3 Broadcast: IP-адрес назначения = `255.255.255.255` (ограниченный широковещательный - local broadcast) или `[сеть].255` (напр., `192.168.1.255` -

направленный широковещательный - directed broadcast, если разрешено). Маршрутизаторы обычно не пересылают широковещательные пакеты между сетями.

Примеры: ARP (запрос), DHCP (DISCOVER/REQUEST).

3. Многоадресная рассылка (Multicast): От одного отправителя группе устройств, которые выразили желание получать трафик для этой группы.

L3 Multicast: IP-адреса назначения из диапазона `224.0.0.0` - `239.255.255.255` (например, `224.0.0.1` - все хосты в локальной сети, `224.0.0.5` - OSPF маршрутизаторы).

L2 Multicast: Соответствующий MAC-адрес из диапазона `01:00:5E:00:00:00` - `01:00:5E:7F:FF:FF`, вычисляемый из IP multicast группы.

Примеры: Видеоконференции, IPTV, обновление ПО группе устройств, протоколы маршрутизации (OSPF, EIGRP).

4. Эникаст (Anycast): От одного отправителя ближайшему (в терминах метрики маршрутизации) устройству в группе, использующей один и тот же IP-адрес. Не является отдельным типом пакета на L3, реализуется протоколами маршрутизации (BGP). Примеры: Корневые DNS-серверы, CDN (Content Delivery Network) узлы.

27. Классы IP-адресов в TCP/IP (Историческая классовая адресация - устарела, заменена CIDR):

Класс A:

Первый бит = `0`.

Диапазон: `1.0.0.0` - `126.255.255.255`.

Маска по умолчанию: `255.0.0.0` (/8).

Сетей: 126 (по 16.7 млн. хостов).

Класс B:

Первые два бита = `10`.

Диапазон: `128.0.0.0` - `191.255.255.255`.

Маска по умолчанию: `255.255.0.0` (/16).

Сетей: ~16,384 (по 65,534 хоста).

Класс C:

Первые три бита = `110`.

Диапазон: `192.0.0.0` - `223.255.255.255`.

Маска по умолчанию: `255.255.255.0` (/24).

Сетей: ~2 млн. (по 254 хоста).

Класс D (Multicast):

Первые четыре бита = `1110`.

Диапазон: `224.0.0.0` - `239.255.255.255`.

Нет масок/хостов - только группы.

Класс E (Зарезервирован):

Первые четыре бита = `1111`.

Диапазон: `240.0.0.0` - `255.255.255.255`.

Важно: Современные сети используют бесклассовую адресацию (CIDR - Classless Inter-Domain Routing), где маска подсети указывается явно (`/24`, `/27` и т.д.) и может быть любой длины, не ограничиваясь границами классов A/B/C.

28. Таблица маршрутизации (Routing Table):

Что это: База данных, хранящаяся в памяти маршрутизатора (или L3 коммутатора, или даже хоста), которая содержит информацию о том, как достичь удаленных IP-сетей.

Содержимое: Каждая запись (маршрут) обычно содержит:

Сеть назначения (Destination Network): IP-адрес целевой сети.

Маска подсети (Subnet Mask): Маска, определяющая размер сети назначения.

Next Hop (Следующий прыжок): IP-адрес следующего маршрутизатора на пути к сети назначения, которому нужно передать пакет.

Выходной интерфейс (Outgoing Interface): Локальный физический или логический интерфейс маршрутизатора, через который нужно отправить пакет, чтобы он достиг next hop.

Метрика (Metric): Числовое значение, представляющее "стоимость" или "предпочтительность" маршрута (чем меньше, тем лучше). Используется для выбора лучшего пути при наличии нескольких маршрутов к одной сети.

Административное расстояние (AD - Administrative Distance): Приоритет источника маршрута (прямое подключение - 0, статический - 1, OSPF - 110, RIP - 120 и т.д.). Чем меньше AD, тем более надежным считается источник. Используется для выбора между маршрутами из разных источников к одной сети.

Источники записей:

Прямо подключенные сети (Connected): Автоматически добавляются при назначении IP-адреса интерфейсу и включении интерфейса (AD=0).

Статические маршруты (Static): Вручную введенные администратором маршруты (AD=1).

Динамические протоколы маршрутизации (Dynamic): Маршруты, полученные от других маршрутизаторов через протоколы (RIP, OSPF, EIGRP, BGP). AD зависит от протокола.

Функция: Используется процессом маршрутизации для определения выходного интерфейса и IP-адреса следующего прыжка для каждого входящего IP-пакета на основе его IP-адреса назначения.

29. Пример работы RIP2 (Routing Information Protocol version 2):

Принцип: Дистанционно-векторный протокол (Distance Vector). Каждый маршрутизатор периодически (каждые 30 сек) рассылает всю свою таблицу маршрутизации всем соседям по широковещанию (RIP v1) или многоадресно на `224.0.0.9` (RIP v2).

Как наполняются таблицы:

1. Инициализация: Маршрутизатор добавляет свои прямо подключенные сети в таблицу с метрикой 1 (хоп=1) и помечает их как источник `C` (Connected).

2. Обновление от соседа: Маршрутизатор R1 получает от соседа R2 обновление RIP. В обновлении содержится список сетей, известных R2, и метрика, с которой R2 знает эти сети (Hop Count).

3. Обработка обновления: Для каждой сети `X` в обновлении от R2:

R1 увеличивает метрику, полученную от R2, на 1 (так как до `X` через R2 будет на 1 хоп больше, чем до R2).

Если сети `X` нет в таблице R1 -> R1 добавляет запись: Сеть=X, NextHop=R2, Метрика = (Метрика_R2 + 1).

Если сеть `X` есть в таблице R1 с NextHop=R2 -> R1 обновляет запись новой метрикой (Метрика_R2 + 1), даже если она хуже.

Если сеть `X` есть в таблице R1 с NextHop=другой_маршрутизатор -> R1 сравнивает новую метрику (Метрика_R2 + 1) с текущей метрикой для `X`:

Если новая метрика лучше (меньше) -> Заменяет запись (NextHop=R2, Метрика=новая).

Если новая метрика хуже или равна -> Игнорирует.

4. Таймеры:

Invalid Timer (180 сек): Если обновление для маршрута не получено за 180 сек, маршрут помечается как возможно недоступный (метрика=16 - бесконечность), но остается в таблице.

Flush Timer (240 сек): Если за 240 сек от соседа не пришло подтверждение маршрута, он удаляется из таблицы.

Holddown Timer (180 сек): После получения обновления с худшей метрикой (но не 16) для существующего маршрута, маршрутизатор игнорирует все последующие обновления с лучшей метрикой для этой сети в течение Holddown времени (чтобы избежать распространения ложной информации).

5. Распространение: R1 теперь включает информацию о сети `X` (с NextHop=R2 и увеличенной метрикой) в свои собственные периодические обновления, рассылаемые соседям.

Особенности RIP2: Поддержка VLSM/CIDR (маски в обновлениях), аутентификация, многоадресные обновления (`224.0.0.9`). Максимальная метрика (макс. хопов) = 15. Метрика 16 = бесконечность (сеть недостижима).

30. NAT (Network Address Translation - Преобразование Сетевых Адресов):

Суть: Технология, позволяющая множеству устройств в частной (локальной) сети использовать один или несколько публичных (глобальных) IP-адресов для выхода в Интернет (или другую внешнюю сеть).

Как работает (основной тип - SNAT: Source NAT):

1. Устройство в локальной сети (с частным IP, напр. `192.168.1.100`) отправляет пакет во внешнюю сеть (Интернет).

2. Пакет достигает маршрутизатора/шлюза с настроенным NAT.

3. Преобразование исходящего адреса (Source):

Маршрутизатор заменяет частный исходный IP-адрес (`192.168.1.100`) в IP-заголовке на свой публичный IP-адрес (напр., `93.184.216.34`).

Маршрутизатор часто заменяет и исходный порт TCP/UDP на уникальный порт из своего пула (чтобы отличать сессии разных внутренних хостов). Например: `192.168.1.100:54321` -> `93.184.216.34:45000`.

4. Маршрутизатор сохраняет запись о этом преобразовании (маппинге) в своей NAT-таблице (Private IP:Port <-> Public IP:Port).

5. Пакет с публичным исходным адресом и портом отправляется дальше в Интернет.

6. Ответ из Интернета: Приходит ответ, адресованный на `93.184.216.34:45000`.

7. Обратное преобразование (Destination):

Маршрутизатор ищет в своей NAT-таблице запись для публичного IP:порта назначения (`93.184.216.34:45000`).

Находит соответствие частному IP:порту (`192.168.1.100:54321`).

Заменяет IP-адрес назначения в IP-заголовке на `192.168.1.100`.

Заменяет порт назначения в TCP/UDP заголовке на `54321`.

8. Пакет пересылается на внутренний хост `192.168.1.100`.

Типы NAT:

Статический NAT (Static NAT): Постоянное сопоставление одного частного IP с одним публичным IP (1:1). Используется для серверов внутри сети, доступных извне.

Динамический NAT (Dynamic NAT): Сопоставление частного IP с публичным IP из пула доступных публичных адресов на время сессии. Адрес берется из пула динамически.

PAT / NAPT (Port Address Translation / Network Address Port Translation): Самый распространенный тип. Множество частных IP преобразуются в один публичный IP, но с разными портами источника (Many:1). Именно он описан в примере выше.

Причины использования:

Экономия публичных IPv4-адресов.

Безопасность (ограниченная): Скрывает структуру внутренней сети от внешнего мира.

Гибкость: Упрощает смену ISP (меняется только публичный IP на шлюзе).

31. “Порт” в протоколах UDP и TCP:

Что это: 16-битное число (0-65535), используемое на Транспортном уровне (L4) для идентификации конечной точки сетевого соединения на конкретном хосте.

Функции:

1. Мультиплекксирование/Демультиплекксирование: Позволяет одному IP-хосту (с одним IP-адресом) одновременно поддерживать множество сетевых приложений/сервисов. Каждое приложение/сервис "слушает" на определенном порту. Транспортный уровень использует порты, чтобы определить, какому приложению передать входящие данные.

2. Идентификация службы: Номера портов используются для согласования клиентом и сервером, к какому конкретному сервису нужно подключиться.

Стандартные (well-known) порты (0-1023) зарезервированы за распространенными службами (HTTP - 80, HTTPS - 443, SSH - 22, DNS - 53 и т.д.).

Структура в сегменте/дейтаграмме:

В заголовках TCP и UDP есть поля:

Source Port (Исходный порт): Порт на хосте-отправителе. Обычно выбирается случайным образом клиентским приложением (эфемерный порт > 1023).

Destination Port (Порт назначения): Порт на хосте-получателе. Указывает на конкретный сервис (напр., 80 для веб-сервера).

Пример: Веб-браузер (клиент) на хосте `192.168.1.100` использует исходный порт `49152` и порт назначения `80` для подключения к веб-серверу на `93.184.216.34`. Веб-сервер отвечает, используя исходный порт `80` и порт назначения `49152`.

32. Проблемы передачи цифрового сигнала по радиоканалу:

1. Затухание (Attenuation): Ослабление мощности сигнала с увеличением расстояния. Зависит от частоты и среды.

2. Многолучевое распространение (Multipath Propagation): Сигнал от передатчика достигает приемника несколькими путями (прямой + отражения от объектов). Приводит к:

Интерференции: Конструктивной (усиление) или деструктивной (ослабление, замирания - fading) в точке приема.

Межсимвольной интерференции (ISI): "Размазывание" символов во времени из-за разной длины путей, что затрудняет их распознавание.

3. Замирания (Fading): Быстрые (быстрые замирания - fast fading) или медленные (медленные замирания - slow fading) изменения уровня сигнала из-за многолучевости, движения приемника/передатчика или изменения среды.

4. Шум: Тепловой шум, атмосферные помехи, индустриальные помехи.

5. Интерференция (Co-Channel & Adjacent-Channel Interference):

Co-Channel (CCI): Помехи от другого передатчика, работающего на той же частоте.

Adjacent-Channel (ACI): Помехи от передатчика, работающего на соседней частоте (из-за неидеальности фильтров).

6. Доплеровский сдвиг (Doppler Shift): Изменение частоты принимаемого сигнала из-за относительного движения передатчика и приемника. Особенно критично на высоких скоростях и высоких частотах.

7. Ограниченный спектр: Радиочастотный спектр - ограниченный ресурс. Необходимость эффективного использования полосы пропускания.

8. Безопасность: Легкость перехвата сигнала по сравнению с проводной средой.

33. OFDM и OFDMA:

OFDM (Orthogonal Frequency Division Multiplexing - Мультиплексирование с ортогональным частотным разделением каналов):

Принцип: Высокоскоростной поток данных разделяется на множество медленных параллельных потоков. Каждый медленный поток модулирует свою собственную ортогональную поднесущую частоту. Поднесущие расположены так близко, что их спектры перекрываются, но ортогональность (интеграл за период произведения любых двух разных поднесущих = 0) позволяет их разделить на приеме без взаимных помех.

Преимущества:

Высокая устойчивость к межсимвольной интерференции (ISI) благодаря длинному символьному интервалу (при той же общей скорости).

Эффективное использование спектра за счет перекрытия поднесущих.

Устойчивость к узкополосным помехам (повреждает только несколько поднесущих).

Относительно простая реализация с помощью БПФ (FFT/IFFT).

Применение: Wi-Fi (802.11a/g/n/ac/ax), WiMAX, DSL, DVB-T, 4G LTE (в нисходящем канале).

OFDMA (Orthogonal Frequency Division Multiple Access - Множественный доступ с ортогональным частотным разделением каналов):

Принцип: Расширение OFDM для поддержки множественного доступа. В OFDMA поднесущие группируются в небольшие блоки (ресурсные блоки - Resource Units, RU в Wi-Fi 6). Эти блоки динамически распределяются между разными пользователями (устройствами) для одновременной передачи/приема данных.

Преимущества (по сравнению с OFDM + TDMA/CSMA):

Повышение эффективности: Одновременная связь с несколькими пользователями в одном временном интервале.

Снижение задержек (Latency): Не нужно ждать своей очереди во временной области для коротких пакетов.

Более эффективное использование спектра: Тонкое распределение ресурсов под нужды пользователей (назначается нужное количество поднесущих).

Масштабируемость: Лучше поддерживает большое количество устройств (IoT).

Применение: Wi-Fi 6 (802.11ax) - в нисходящем (DL) и восходящем (UL) каналах, 5G NR.

34. Модуляция в Wi-Fi:

Суть: Процесс изменения параметров несущего высокочастотного сигнала (амплитуды, частоты, фазы) в соответствии с передаваемыми цифровыми данными.

Основные типы модуляции, используемые в Wi-Fi (802.11):

1. DSSS/FHSS (Прямая последовательность / Скачкообразная перестройка частоты): Использовались в ранних стандартах (802.11, 802.11b).

2. OFDM (Orthogonal Frequency Division Multiplexing): Основа для высокоскоростных стандартов (802.11a/g/n/ac/ax). В рамках OFDM используется:

BPSK (Binary Phase Shift Keying): 1 бит на символ. Самая устойчивая, самая низкая скорость. (Напр., 6 Мбит/с в 802.11a/g).

QPSK (Quadrature Phase Shift Keying): 2 бита на символ. (Напр., 12 Мбит/с).

QAM (Quadrature Amplitude Modulation): Комбинирует амплитудную и фазовую модуляцию. Чем выше порядок, тем выше скорость, но требуется лучшее отношение сигнал/шум (SNR).

16-QAM: 4 бита на символ. (Напр., 24 Мбит/с).

64-QAM: 6 бит на символ. (802.11n: до 65 Мбит/с на поток; 802.11ac: базовая).

256-QAM: 8 бит на символ. (802.11ac: до 86.7 Мбит/с на поток; 802.11ax: базовая).

1024-QAM: 10 бит на символ. (802.11ax: до 120 Мбит/с на поток).

3. MIMO (Multiple Input Multiple Output): Не модуляция, а технология использования множества антенн для передачи нескольких пространственных потоков данных одновременно на одной частоте. Работает совместно с OFDM и QAM, умножая пропускную способность (кол-во потоков x скорость модуляции). (802.11n: до 4x4; 802.11ac: до 8x8; 802.11ax: до 8x8).

Адаптивность: Точки доступа и клиенты Wi-Fi постоянно оценивают качество канала (SNR, затухание). В зависимости от условий они автоматически выбирают наиболее подходящую схему модуляции и кодирования (MCS - Modulation and Coding Scheme), чтобы обеспечить максимально возможную скорость при допустимом уровне ошибок.

35. Типовые топологии в беспроводной связи:

1. "Точка-Точка" (Point-to-Point - P2P):

Описание: Прямое беспроводное соединение между двумя узлами (антеннами). Обычно узлы направлены друг на друга.

Применение: Соединение двух зданий (мост), магистральные каналы связи, спутниковая связь "земная станция - спутник".

2. "Точка-Многоточка" (Point-to-Multipoint - P2MP):

Описание: Один центральный узел (базовая станция, точка доступа) обменивается данными с множеством удаленных узлов (клиентов, абонентских станций). Удаленные узлы обычно не взаимодействуют друг с другом напрямую через центральный узел.

Применение: Сотовые сети (BS -> MS), Wi-Fi (AP -> клиенты), фиксированный беспроводной доступ (WISP), спутниковое ТВ (спутник -> приемники).

3. Инфраструктурный режим (Infrastructure Mode / Star Topology):

Описание: Частный случай P2MP. Все клиентские устройства (STA) соединяются с центральной Точкой Доступа (AP). AP действует как мост между беспроводной и проводной сетью (или как маршрутизатор). Клиенты не общаются напрямую друг с другом; весь трафик идет через AP.

Применение: Классические сети Wi-Fi в офисах, домах, общественных местах.

4. Режим AD-HOC (Ad-Hoc Mode / Peer-to-Peer / IBSS - Independent Basic Service Set):

Описание: Устройства соединяются напрямую друг с другом без использования центральной точки доступа. Формируют временную сеть "на лету". Каждое устройство может быть и клиентом, и маршрутизатором (в более сложных mesh-сетях).

Применение: Прямая передача файлов между устройствами (Wi-Fi Direct), временные сети (конференции, игры), сенсорные сети, mesh-сети (частично).

5. Ячеистая сеть (Mesh Topology):

Описание: Устройства (mesh-ноды) соединяются друг с другом множеством связей, образуя сетку. Трафик от клиента может достигать точки выхода в интернет (шлюза) через несколько промежуточных прыжков (нодов). Пути могут быть избыточными и динамически перестраиваться при изменении условий или отказе нодов.

Применение: Домашние mesh-системы Wi-Fi для покрытия больших площадей, городские беспроводные сети, промышленные IoT сети, военные сети. Стандарты: Wi-Fi Mesh (802.11s), Zigbee, Thread.