

Рубежный контроль 2.
Вариант 1.

ISU №	345124
ФИО	Хоанг Ван Куан
группа	P3366

1. Дайте краткую характеристику метода доступа CSMA/CD
 - метод доступа к среде передачи, при котором станция, имеющая данные для передачи, прослушивает канал, чтобы определить, не передаёт ли данные в это время другая станция. Если канал свободен — начинается передача. Во время передачи станция продолжает слушать канал: при коллизии передача прекращается и повторяется позже после случайной задержки. Процесс повторяется до успешной передачи
2. Дайте определение классовой IP-адресации. Опишите классы адресов.
 - Классовая IP адресация — это метод IP-адресации, который не позволяет рационально использовать ограниченный ресурс уникальных IP-адресов, т.к. не возможно использование различных масок подсетей
 - Адреса делятся на классы А, В, С, D и Е в зависимости от первых битов и диапазона:
 - + Класс А: для больших сетей
Первый октет (1–126), начинается с бита 0. Остальные октеты — хосты.
Маска: 255.0.0.0
 - + Класс В: для средних сетей
Первые два октета (128–191), начинается с 10. Остальные — хосты
Маска: 255.255.0.0
 - + Класс С: для малых сетей
Первые три октета (192–223), начинается с 110. Последний — хосты.
Маска: 255.255.255.0
 - + Класс D: используется для мультикаст-рассылки, без разделения на сеть и хост.
Диапазон: 224–239
 - + Класс Е: зарезервирован для экспериментов, диапазон: 240–255
Классы D и Е не используются конечными пользователями
3. Что такое клиент-серверное взаимодействие в контексте прикладных протоколов? Приведи пример с POP3.
 - Клиент-серверное взаимодействие - это модель, при которой одна сторона (клиент) отправляет запрос, а другая (сервер) обрабатывает его и возвращает ответ. Такая схема характерна для прикладных сетевых протоколов
 - Пример с POP3: Клиент подключается к серверу электронной почты по протоколу POP3, проходит аутентификацию, получает список писем и загружает их на локальное устройство. После этого письма могут удаляться с сервера.
4. Что такое фаервол, и зачем он нужен?
 - Фаервол — это программа, которая защищает компьютер от атак из Сети. Ее также называют брандмауэром и межсетевым экраном, потому что система как бы экранирует вредоносные действия из интернета. Если она видит подозрительный трафик, то блокирует его
 - Зачем он нужен:
 - + Защита сети от несанкционированного доступа
 - + Блокировки передачи информации неизвестному источнику

+ Предотвращение атак

5. На каком уровне OSI модели работает протокол POP3? Опишите работу этого протокола.
 - Протокол POP3 работает на 7-й уровне OSI (прикладной уровень)
 - POP3 работает через стек TCP/IP и обычно использует порт 110 для незашифрованных соединений или порт 995 для зашифрованных соединений. Когда почтовый клиент настроен на использование POP3, он подключается к почтовому серверу и загружает все сообщения в папку входящих сообщений пользователя
6. Как можно избежать возникновения множественных петель при построении сети на коммутаторах?
 - Чтобы избежать множественных петель в сети на коммутаторах, используется протокол STP. STP - это канальный протокол. Основной задачей STP является устранение петель в топологии произвольной сети Ethernet, в которой есть один или более сетевых мостов, связанных избыточными соединениями.
7. Что такое снифферы, и зачем их используют?
 - сниффер - устройство и/или программное обеспечение, позволяющее считывать, анализировать, а в случае злонамеренности и искажать, сетевой трафик в месте собственного подключения к компьютерной сети
 - Зачем их используют:
 - + Для диагностики сети (поиск неисправностей)
 - + Отладки приложений
 - + Мониторинга безопасности (или взлома, если цель злонамеренная)
8. Как с помощью сниффера можно понять, что на сервер совершается DOS атака? С помощью сниффера можно определить DOS-атаку (Denial of Service) на сервер, анализируя сетевой трафик.
 - 1) Резкий рост числа пакетов, направленных на сервер, превышающий норму
 - 2) Множество одинаковых или похожих запросов с одного или разных IP
 - 3) Трафик от подозрительных IP-адресов или распределённый (DDoS)
 - 4) Высокая частота специфичных пакетов
9. Приведите обобщенную структуру кадра Ethernet? Почему размер блока данных начинается от 46 байт?
 - Обобщённая структура кадра Ethernet
 - 1) Преамбула: 7 байт
 - 2) SFD: 1 байт
 - 3) Конечный MAC-адрес: 6 байт
 - 4) Исходный MAC-адрес: 6 байт
 - 5) Длина/Тип: 2 байт
 - 6) Данные MAC-клиента: 46 -1500 байт
 - 7) Заполняющие байты
 - 8) Контрольная последовательность кадра (FCS): 4 байт
 - Минимальный размер кадра в Ethernet должен составлять 64 байта. При вычитании размера заголовка (14 байт) и FCS (4 байта) остаётся 46 байт для данных
10. Что такое виртуальная локальная сеть?
 - это логическая оверлейная сеть, которая объединяет подмножество устройств, которые совместно используют физическую локальную сеть, изолируя трафик для каждой группы

11. Какую топологию имеет сеть, построенная только на концентраторах?
- Имеет топологию звезда. Так как все устройства подключаются к концентратору. Все данные, поступающие на концентратор, транслируются на все подключённые порты, что характерно для звёздной топологии
12. Что такое прокси-сервер и зачем он используется? Какие основные виды таких серверов Вы знаете?
- Прокси-сервер - это промежуточный канал между оборудованием пользователя и сервером, через который происходит обмен информацией
 - Прокси-серверы применяются для оптимизации работы и усиления безопасности. Они позволяют повысить скорость загрузки страниц сайтов, снизить нагрузку на серверы, скрыть настоящий IP-адрес пользователя, гарантировать защиту от зараженных программ и отражать попытки несанкционированного доступа к интернет-ресурсам
 - Основные виды прокси-серверов:
 - + HTTP-прокси — работает только с веб-трафиком
 - + HTTPS-прокси — поддерживает защищённые соединения
 - + SOCKS-прокси — универсальный, передаёт любые данные (не только HTTP)
 - + Прозрачный прокси — незаметен для пользователя, часто используется для фильтрации
 - + Анонимный прокси — скрывает IP пользователя
13. Поясните особенности маршрутизации в браузере TOR.
- Маршрутизация в TOR использует многослойное шифрование и передачу данных через три случайных узла:
- + Входной узел: Знает отправителя, шифрует данные
 - + Промежуточный узел: Пересылает, снимает слой шифрования
 - + Выходной узел: Отправляет запрос к цели, знает только пункт назначения
- Особенности:
- + Данные шифруются на каждом этапе
 - + IP клиента скрыт, виден только IP выходного узла
 - + Маршрут меняется каждые примерно 10 минут
- Плюс: анонимность. Минус: низкая скорость
14. Опишите принцип действия метода NAT.
- 1) Локальные IP → Публичный IP:
Устройства в локальной сети имеют частные IP
NAT заменяет их на один публичный при выходе в интернет
 - 2) Таблица трансляции: Роутер создаёт таблицу, где сопоставляет локальный IP и порт отправителя с внешним запросом
 - 3) Обратный процесс: Когда ответ приходит на публичный IP, NAT смотрит таблицу и перенаправляет данные на нужный локальный IP и порт
15. У вас есть 300 устройств в локальной сети и только 1 внешний IP-адрес. У каждого устройства открыто по 10 соединений. Сколько портов будет задействовано на NAT-устройстве?
- 3000 портов (10x300)
16. Клиент получил IP-адрес от DHCP-сервера. В какой момент происходит широковещательная передача после получения DHCPOFFER? Поясните ответ.
- Широковещательная передача происходит на этапе DHCPREQUEST — после получения клиентом предложения (DHCPOFFER)

- Пояснение: Клиент выбирает одно из предложений от DHCP-серверов и отправляет DHCPREQUEST в виде широковещательного сообщения (broadcast), так как у него ещё нет окончательно назначенного IP-адреса. Это нужно, чтобы уведомить все серверы о своём выборе.

17. Чем отличается Static NAT от PAT (Port Address Translation)?

NAT осуществляет перевод IPv4-адреса на основе принципа «один к одному» между приватными и общедоступными IPv4-адресами.

С другой стороны, PAT трансформирует и адрес, и номер порта

18. Какие DNS-записи нужно создать для сайта `www.example.com`, если хостинг работает по IP 192.0.2.1?

- A-запись для основного домена
- CNAME-запись если необходимо указать основной домен

19. Сколько одновременных подключений может поддерживать один внешний IP-адрес при использовании PAT, если доступно 64511 TCP-портов?

- 64511 одновременных подключений, так как при использовании PAT каждый уникальный TCP-порт представляет собой отдельное соединение,

20. Устройство подключается к беспроводной сети. На маршрутизаторе установлен фильтр по MAC-адресам. Системный администратор внес MAC-адрес устройства в таблицу, но при следующем соединении устройства с сетью подключения не произошло, как и далее. Что может быть этому причиной?

Возможная причина:

- 1) MAC-адрес изменён. Устройство использует рандомизацию MAC-адреса. Из-за этого фактический передаваемый адрес отличается от того, что внесён в фильтр, и подключение не проходит
- 2) Кэширование или задержка применения настроек. Маршрутизатор мог не применить изменения
- 3) Дублирование MAC-адресов