Вопросы к экзамену

1. Модель OSI. Инкапсуляция в контексте модели OSI.
2. Стек протоколов TCP/IP.
3. Назначение компьютерных сетей. Основные виды компьютерных сетей.
4. Физический уровень в модели OSI. Его роль.
5. Канальный уровень в модели OSI. Его роль.
6. Сетевой уровень в модели OSI. Его роль.
7. Транспортный уровень в модели OSI. Его роль.
8. Среды передачи данных. Виды связи. Duplex, Half-duplex, Simplex.
9. Способы коммутации в сетях электросвязи
10. Топология сетей. Виды топологий.
11. Сетевая технология Ethernet. Адресация в Ethernet. Формат Ethernet фрейма.
12. Коллизии. Домен коллизий. Broadcast домен.
13. Коммутатор. Назначение. Принцип работы.
14. Флуд. Петля коммутации.
15. Формат IPv4-пакета. IPv4-адреса. Частные адреса.
16. Протокол ARP. Принцип работы.
17. Маршрутизатор. Назначение. Принцип работы.
18. Классовая и бесклассовая адресация. Маска подсети.
19. Протокол DHCP. DHCP Relay.
20. Транспортный уровень. Протоколы с гарантированной и негарантированной доставкой данных.
21. Форматы TCP-сегмента и UDPдейтаграммы. Сокеты. 5-tuple
22. Технология NAT. Статический NAT.
23. Технология NAT. Динамический NAT.
24. Технология NAT. Destination NAT. Source NAT.
25. Технология NAT. Перегруженный NAT.
26. Технология Port Forwarding.
27. Технология DNS. Решаемые задачи. Структура доменного имени.
28. Типы записей DNS. Процесс разрешения доменного имени
29. Технология DNS. Обратное разрешение.
30. Асимметричное и симметричное шифрование.
31. Аутентификация и авторизация. Шифрование. Конфиденциальность. Целостность. Доступность.
32. Несанкционированный доступ.
33. Виртуальная частная сеть. Задачи. Протоколы.
34. VLAN. Назначение, примеры использования. VLAN инкапсуляция.
35. Анализаторы трафика. Задачи анализа сетевого трафика.
36. Файрволл. Задачи решаемые файрволлом.
37. Основные компоненты ЛВС. Сетевые устройства. Типы и их функции.
38. Маршрутизация и коммутация. Различия и решаемые задачи.
39. Основные принципы работы VPN.
40. VLAN. Роли интерфейсов коммутаторов. Субинтерфейсы роутера.

Задачи

1. В Cisco Packet Tracer на рабочую область добавьте три ПК и коммутатор. Подключите ПК к коммутатору. Настройте IP-адреса на каждом ПК. Проверьте соединение.
2. В Cisco Packet Tracer на рабочую область добавьте два ПК, сервер и коммутатор. Подключите к коммутатору ПК сервер. Настройте DHCP на сервере. Проверьте соединение между ПК.
3. В Cisco Packet Tracer на рабочую область добавьте два ПК и коммутатор. Настройте IP-адреса на каждом ПК. Проверьте соединение. Посмотрите ARP-таблицы на ПК.
4. В Cisco Packet Tracer на рабочую область добавьте два ПК, маршрутизатор и коммутаторы. Подключите к маршрутизатору коммутаторы и ПК (ПК должны быть в разных сетях).Настройте IP-адреса на интерфейсах маршрутизатора и ПК.Настройте маршрутизацию между разными подсетями. Проверьте соединение между ПК.
5. В Cisco Packet Tracer на рабочую область добавьте два ПК и коммутатор. Подключите ПК к коммутатору. Используйте режим симуляции, чтобы отправить пакеты между устройствами. Проанализируйте трафик, чтобы увидеть, как пакеты перемещаются по сети, какие протоколы используются и какие данные содержатся в пакетах.
6. Вам дана сеть с IP-адресом 192.168.10.0 и маской подсети 255.255.255.224. Рассчитайте количество доступных IP-адресов для хостов в этой сети.
7. В Cisco Packet Tracer на рабочую область добавьте два ПК и коммутатор. Соедините ПК с коммутатором. Настройте IP-адреса на ПК: ПК1: 192.168.1.10/24, ПК2: 192.168.2.20/24. Откройте командную строку на ПК1 и выполните команду ping 192.168.2.20. Объясните, почему нет связи. Как исправить ситуацию?
8. Запустите Wireshark и начните захват трафика на выбранном сетевом интерфейсе. Откройте веб-браузер и посетите несколько сайтов. Остановите захват и проанализируйте полученный трафик. Найдите пакеты, относящиеся к HTTP-протоколу.
9. Запустите Wireshark и начните захват трафика на выбранном сетевом интерфейсе. Откройте несколько приложений, использующих разные протоколы (например, браузер, мессенджер, почтовый клиент).Остановите захват и примените фильтры, чтобы отобразить только трафик определенного протокола (например, HTTP, DNS, TCP).
10. Запустите Wireshark и начните захват трафика на выбранном сетевом интерфейсе. Выполните команду ping на IP-адрес другого устройства в сети. Остановите захват и найдите ARP-запросы и ответы, связанные с этим пингом.
11. Запустите Wireshark и начните захват трафика на выбранном сетевом интерфейсе. Скачайте файл из интернета. Остановите захват и найдите TCP-соединение, связанное с этим скачиванием. Проанализируйте процесс установления соединения (handshake), передачу данных и закрытие соединения.

12 Запустите Wireshark и начните захват трафика на выбранном сетевом интерфейсе. Откройте веб-браузер и введите адрес сайта, который вы раньше не посещали. Остановите захват и найдите DNS-запросы и ответы, связанные с этим сайтом.

13 Запустите Wireshark и начните захват трафика на выбранном сетевом интерфейсе. Откройте несколько приложений, использующих разные протоколы (например, браузер, мессенджер, почтовый клиент). Проанализируйте статистику протоколов, используемых в захваченном трафике. Определите, какой протокол используется чаще всего.

14 На хосте под управлением Linux. Узнайте свой IP-адрес и маску подсети. Проверьте связь с другим устройством и выход в Интернет. Просмотрите таблицу маршрутизации. Узнать, какие сетевые соединения активны в данный момент.

15 На хосте под управлением Linux. Узнайте свой IP-адрес и маску подсети. Проверьте связь с другим устройством и выход в Интернет. Узнайте, через какие узлы проходит пакет до удаленного сервера. Просмотрите правила файрволла.

16 В Cisco Packet Tracer создайте сеть с тремя ПК и маршрутизатором. Подключите ПК к маршрутизатору. Настройте статическую маршрутизацию на маршрутизаторе так, чтобы ПК могли связываться между собой.

17 В Cisco Packet Tracer создайте сеть с тремя ПК и маршрутизатором. Подключите ПК к маршрутизатору. Настройте динамическую маршрутизацию на маршрутизаторе с помощью протокола RIP.

18 Используя iptables или firewalld, настройте правила файрволла, чтобы разрешить входящий трафик на определенный порт (например, порт 80 для веб-сервера), но запретить другие типы входящего трафика.

19 Создайте сеть с двумя ПК и маршрутизатором в Cisco Packet Tracer. Подключите ПК к маршрутизатору. Настройте статический маршрут на маршрутизаторе, чтобы обеспечить связность между двумя подсетями, к которым подключены ПК.

20 Запустите Wireshark и начните захват трафика на выбранном сетевом интерфейсе. Откройте веб-браузер и посетите несколько сайтов. Остановите захват и проанализируйте DNS-запросы и ответы, связанные с этими сайтами.