

Экзаменационные вопросы к курсу

"Введение в компьютерные сети" 2023 год.

1. Базовая модель взаимодействия сетевых приложений. Понятия сервиса, интерфейса и протокола.
2. Виды задержек передачи данных при пакетной коммутации и их свойства.
3. Устройство пакетного коммутатора. Методы оценки сквозной задержки при пакетной коммутации. Метод справедливой взвешенной очереди и его свойства, условия его применимости.
4. Методы оценки сквозной задержки при пакетной коммутации.
5. Коммутация пакетов: методы управления задержкой пакета в сети.
6. Устройство пакетного коммутатора. Виды буферизации в пакетных коммутаторах. Различия в работе коммутатора и маршрутизатора
7. Заголовки IP, TCP. Фрагментация PDU и управление ею. Методы управления потоком.
8. Явление перегрузки, причины ее возникновения и основные методы борьбы с ней.
9. Алгоритмы управления перегрузкой: AIMD в случае одного потока и в случае нескольких потоков. Способы обнаружения перегрузки и виды алгоритмов управления перегрузкой.
10. Управление передачей в TCP: алгоритм управления перегрузкой Tahoe и алгоритм управления перегрузкой Reno – основные отличия.
11. Алгоритмы маршрутизации в Интернет: основные подходы, маршрутизация по вектору расстояния.
12. Алгоритмы маршрутизации в Интернет: основные подходы, маршрутизация по состоянию канала.
13. Маршрутизация в Интернет: OSPF протокол для внутренней маршрутизации.
14. Маршрутизация в Интернет: структура Интернета, понятие автономной системы, протокол EBGP внешней маршрутизации.
15. Понятие автономной системы, ее структуры. Протоколы EBGP и IBGP – назначение и основные различия.
16. Маршрутизация в Интернет: взаимосвязь протоколов OSPF и BGP.
17. Понятие групповой маршрутизации, протоколы групповой маршрутизации.

18. Маршрутизация на L2, ее отличие от маршрутизации на L3. Протокол STP, алгоритм построения ST дерева коммутатором. Способ определения designated port и root port
19. Представление о коммутации по меткам – MPLS протокол. Понятие VPN – Virtual Privet Network. Реализация VPN с помощью MPLS.
20. Среды передачи (магнитные носители, витая пара, среднечастотный и широкополосный кабели, оптоволокно, сравнение кабелей и оптоволокон).
21. Передача цифровых данных по цифровым сигналам. Передача аналоговых данных по цифровым сигналам.
22. Передача цифровых данных по аналоговым сигналам. Передача аналоговых данных по аналоговым сигналам.
23. Физические среды передачи данных. Беспроводная связь (электромагнитный спектр, радиопередача, микроволновая передача, видимое излучение). Протоколы MACA.
24. Семейство протоколов IEEE 802.11. Система передачи данных WiFi: принципы организации, структура кадра, алгоритм функционирования.
25. Проблемы передачи данных на канальном уровне. Сервис, предоставляемый сетевому уровню.
26. . Сравнение производительности систем: чистая ALOHA, слотированная ALOHA. Протоколы множественного доступа с обнаружением несущей (настойчивые и не настойчивые CSMA, CSMA с обнаружением коллизий).
27. Протокол IEEE 802.3 и система передачи данных Ethernet (кабели, способ физического кодирования, понятие коллизии, алгоритм вычисления задержки, MAC подуровень, структура кадра, LLC подуровень).
28. Сетевые коммутаторы: организация, основные функции, принципы функционирования. Коммутатор канального уровня с обучением. Виртуальные сети на основе протокола IEEE 802.1Q.
29. Сетевой уровень в Интернет: адресация Ipv4 и IPv6, протокол маршрутизации IP, протоколы ARP, RARP, DHCP.
30. Транспортный уровень: адресация, установление соединения, разрыв соединения, управление потоком и буферизацией, восстановление последовательности сегментов.
31. Ключевые функции системы безопасности компьютерных систем.
32. Безопасность информации в сетях: основные понятия: угрозы, информация, документы, уязвимость, нарушитель, информационная безопасность, целостность, конфиденциальность, доступность, атака.

33. Понятия угрозы и уязвимости в компьютерных сетях, классификация угроз.
34. Понятия идентификации, аутентификации и авторизации. Примеры алгоритмов.
35. Функции монитора безопасности. Объектно-субъектная модель управления доступом.
36. Понятия и виды политик безопасности.
37. Основные виды шифрования. Алгоритмы шифрования с закрытым ключом. Примеры.
38. Основные виды шифрования. Алгоритмы шифрования с открытым ключом. Примеры.
39. Информационная безопасность: основные задачи. Протоколы установления подлинности на основе закрытого ключа, протокол Диффи-Хелмана. Электронная подпись.
40. Объектно-субъектная модель управления доступом.
41. Протокол установления секретного ключа Диффи-Хелмана
42. Протокол RSA с открытым ключом
43. Протокол взаимной аутентификации на основе открытых ключей.
44. Информационная безопасность: контроль доступа и защита от компьютерных атак. Межсетевые экраны и их виды. Системы обнаружения и предотвращения компьютерных атак (метод аномалий и метод злоупотреблений).
45. Служба DNS: основные функции, структуры данных, принципы функционирования. Режим адресации anycast.
46. Организация, функционирование и основные протоколы почтовой службы и прикладной протокол FTP.
47. NAT: основные функции, типы и принципы функционирования, влияние на приложения.
48. Устройство ЦОД. Понятие облачных вычислений. Механизмы виртуализация и масштабирования.
49. Современные проблемы компьютерных сетей: Программно Конфигурируемые Сети (ПКС): структура, принципы функционирования, протокол Open Flow.
50. Протокол Open Flow, организация и принципы работы ПКС коммутатора, маршрутизация в ПКС сетях.