

Вопросы по курсу «Сетевые технологии»

В каждом варианте теста – 40 вопросов из числа перечисленных ниже.

Требуется выбрать правильный вариант.

Некоторые вопросы требуют выбора нескольких вариантов.

(Это необходимо понять по смыслу вопроса.)

1. Компьютерные сети это сети:
[] – с коммутацией пакетов
[] – с коммутацией каналов
2. В режиме коммутации каналов сохранение очередности передаваемой информации
[] обеспечивается
[] не обеспечивается
3. В режиме коммутации пакетов сохранение очередности передаваемой информации
[] обеспечивается
[] не обеспечивается
4. Какая сеть больше
[] – MAN
[] – WAN
5. Какая сеть больше
[] – MAN
[] – LAN
6. Какая сеть больше
[] – LAN
[] – PAN
7. Какая сеть больше
[] – LAN
[] – WAN
8. Более высокое качество связи достигается
[] – в сети коммутации каналов
[] – в сети коммутации пакетов
9. Более эффективное использование канала достигается
[] – в сети коммутации каналов
[] – в сети коммутации пакетов
10. Инкапсуляция это
[] – объединение данных в пакет при передаче
[] – помещение сообщения протокола одного уровня в сообщение протокола другого уровня
[] – добавление к данным служебного заголовка

11. Интерфейс – это соглашение о взаимодействии
- [] – одинаковых сетевых уровней одной станции
 - [] – разных сетевых уровней одной станции
 - [] – одинаковых сетевых уровней разных станций
 - [] – разных сетевых уровней разных станций
12. Протокол – это соглашение о взаимодействии
- [] – одинаковых сетевых уровней одной станции
 - [] – разных сетевых уровней одной станции
 - [] – одинаковых сетевых уровней разных станций
 - [] – разных сетевых уровней разных станций
13. Стек протоколов это
- [] – множество протоколов эталонной модели OSI
 - [] – упорядоченное по уровням семейство протоколов, предназначенных для совместной работы
 - [] – TCP/IP
 - [] – IPX/SPX
14. В модели OSI выделяется
- [] – 3 уровня
 - [] – 4 уровня
 - [] – 6 уровней
 - [] – 7 уровней
15. В стеке TCP/IP выделяется
- [] – 3 уровня
 - [] – 4 уровня
 - [] – 6 уровней
 - [] – 7 уровней
16. В канале broadband пропускная способность
- [] – используется для передачи одного сигнала
 - [] – делится между несколькими логическими каналами
17. В канале baseband пропускная способность
- [] – используется для передачи одного сигнала
 - [] – делится между несколькими логическими каналами
18. Канал simplex отличается передачей данных
- [] – в одном направлении
 - [] – в двух направлениях одновременно
 - [] – в двух направлениях попеременно
19. Канал duplex отличается передачей данных
- [] – в одном направлении
 - [] – в двух направлениях одновременно
 - [] – в двух направлениях попеременно

20. Канал half-duplex отличается передачей данных
- [] – в одном направлении
 - [] – в двух направлениях одновременно
 - [] – в двух направлениях попаременно
21. Физическое кодирование это
- [] – представление информации состояниями электромагнитного поля или их переходами
 - [] – преобразование последовательности бит в другую последовательность бит
22. Логическое кодирование это
- [] – представление информации состояниями электромагнитного поля или их переходами
 - [] – преобразование последовательности бит в другую последовательность бит
23. Код «Манчестер» использует уровни сигнала:
- [] – 2 уровня
 - [] – 3 уровня
 - [] – 4 уровня
 - [] – 5 уровней
24. Код «MLT-3» использует уровни сигнала:
- [] – 2 уровня
 - [] – 3 уровня
 - [] – 4 уровня
 - [] – 5 уровней
25. Код «РАМ-5» использует уровни сигнала:
- [] – 2 уровня
 - [] – 3 уровня
 - [] – 4 уровня
 - [] – 5 уровней
26. Для логического кодирования используются
- [] – код Хэмминга
 - [] – код 4B/5B
 - [] – код 8B/10B
 - [] – код Рида-Соломона
 - [] – скремблер
27. Модуляция сигнала – это
- [] способ изменения параметров несущего сигнала в соответствии с формой исходного сигнала
 - [] способ изменения параметров исходного сигнала в соответствии с требованиями канала передачи
 - [] способ преобразования аналогового сигнала в цифровой сигнал
28. В сетях передачи данных применяются:
- [] – амплитудная модуляция
 - [] – частотная модуляция
 - [] – широтно-импульсная модуляция
 - [] – квадратурная амплитудно-фазовая манипуляция

29. В сетях передачи данных применяются:

- амплитудная модуляция
- фазовая модуляция
- импульсно-кодовая модуляция
- позиционно-импульсная модуляция

30. Импульсно-кодовая модуляция (PCM)

- определяет способ дискретизации аналогового сигнала
- определяет способ дискретизации и квантования аналогового сигнала
- определяет способ дискретизации, квантования и кодирования аналогового сигнала

31. Минимальная частота дискретизации аналогового сигнала для восстановления сигнала при передаче через цифровые системы связи определяется

- минимальной частотой исходного сигнала
- максимальной частотой исходного сигнала
- минимальной амплитудой исходного сигнала
- максимальной амплитудой исходного сигнала

32. Мультиплексирование – это

- метод передачи данных нескольких каналов в одном канале большей пропускной способности
- метод совместного использования канала несколькими абонентами

33. Существуют методы мультиплексирования (отметить верное):

- с разделением по идентификатору абонента
- со спектральным разделением
- с кодовым разделением
- с разделением по номеру канала

34. Существуют методы мультиплексирования (отметить верное):

- с разделением по времени
- с разделением по частоте
- с разделением по линиям связи
- без разделения

35. Комутация пакетов является частным случаем мультиплексирования

- с разделением по времени
- с разделением по частоте
- с кодовым разделением

36. Сети ATM – сети с коммутацией

- каналов
- пакетов
- ячеек

37. Размер ячейки ATM составляет

- 32 байта
- 48 байт
- 53 байта
- 56 байт
- 64 байта

38. В сети ATM гарантируется сохранение очередности прихода ячеек
[] да
[] нет

39. Сеть ATM
[] ориентирована на предварительное установление соединения
[] не ориентирована на предварительное установление соединения

40. Идентификаторы виртуального канала и виртуального пути ATM
[] задаются пользователем
[] согласуются двумя пользователями
[] выделяются сетевым устройством

41. В протоколе ATM маршрутное поле ячейки:
[] Согласуется между конечными точками, и не меняется на всём пути следования ячейки.
[] Меняется от коммутатора к коммутатору

42. Сколько бит занимает идентификатор VLAN в сети Ethernet (согласно 802.1Q):
[] 11
[] 12
[] 13
[] 14
[] 15
[] 16

43. Сколько разных идентификаторов VLAN в сети Ethernet может быть в одном сегменте (согласно 802.1Q):
[] 1024
[] 2048
[] 4096
[] 8192
[] 16384

44. Сколько разных соединений может одновременно проходить через порт MPLS-коммутатора?
[] – 4096
[] – 16384
[] – 65536
[] – 1048576

45. Метка MPLS
[] Согласуется между конечными точками, и не меняется на всём пути следования пакета.
[] Меняется от коммутатора к коммутатору

46. Протокол MPLS
[] – ориентирован на предварительное установление соединения
[] – не ориентирован на предварительное установление соединения

47. Для управления коммутаторами SDN используется протокол`
[] BGP
[] OpenFlow
[] ICMP
48. Протокол Ethernet относится к
[] – физическому уровню
[] – канальному уровню
[] – сетевому уровню
[] – транспортному уровню
49. Протокол IP относится к
[] – физическому уровню
[] – канальному уровню
[] – сетевому уровню
[] – транспортному уровню
50. Протокол TCP относится к
[] – физическому уровню
[] – канальному уровню
[] – сетевому уровню
[] – транспортному уровню
51. В протоколе Ethernet управление разделяемой средой производится за счет
[] – прослушивания несущей
[] – передачи маркера
52. В протоколе Token Ring управление разделяемой средой производится за счет
[] – прослушивания несущей
[] – передачи маркера
53. Конценратор (HUB) – это устройство сопряжения на
[] – физическом уровне модели OSI
[] – канальном уровне модели OSI
[] – сетевом уровне модели OSI
54. Коммутатор (Switch) – это устройство сопряжения на
[] – физическом уровне модели OSI
[] – канальном уровне модели OSI
[] – сетевом уровне модели OSI
55. Маршрутизатор (Router) – это устройство сопряжения на
[] – физическом уровне модели OSI
[] – канальном уровне модели OSI
[] – сетевом уровне модели OSI
56. Конценратор (HUB) обеспечивает сопряжение
[] – в пределах одной среды передачи данных
[] – между разными средами передачи данных
[] – между разными сетями

57. Коммутатор (Switch) обеспечивает сопряжение

- [] – в пределах одной среды передачи данных
- [] – между разными средами передачи данных
- [] – между разными сетями

58. Маршрутизатор (Router) обеспечивает сопряжение

- [] – в пределах одной среды передачи данных
- [] – между разными средами передачи данных
- [] – между разными сетями

59. Локальной сетью называется

- [] – совокупность компьютеров, сетевых карточек и проводов
- [] – разделяемая среда передачи с несколькими подключенными станциями
- [] – одна разделяемая разделяемая среда передачи с несколькими подключенными станциями, или несколько таких сред, соединенных коммутаторами или мостами

60. Коммутатор (switch) выполняет операции

- [] – коммутации пакетов (switching)
- [] – продвижения пакетов (forwarding)
- [] – построения маршрутов (routing)

61. Маршрутизатор (router) выполняет операции

- [] – коммутации пакетов (switching)
- [] – продвижения пакетов (forwarding)
- [] – построения маршрутов (routing)

62. Маска сети используется для

- [] – группировки станций в локальной сети
- [] – разделению IP-адреса на номер сети и номер хоста
- [] – рассылки широковещательных сообщений
- [] – преобразования IP-адресов в MAC-адреса

63. Сколько станций можно разместить в сети с длиной маски L?

(варианты L = 16, 20, 24, 28)

- [] – 14
- [] – 15
- [] – 16
- [] – 254
- [] – 255
- [] – 256
- [] – 4094
- [] – 4095
- [] – 4096
- [] – 65534
- [] – 65535
- [] – 65536

64. В таблице маршрутизации 2 правила:

Адрес	Маска	Шлюз
10.0.0.0	255.255.255.0	10.0.0.1
10.0.0.0	255.255.255.240	10.0.0.2

Дейтаграмма с адресом получателя 10.0.0.8 будет отправлена на шлюз

- 10.0.0.1
- 10.0.0.2

65. В таблице маршрутизации 2 правила:

Адрес	Маска	Шлюз
192.168.12.0	255.255.255.0	192.168.12.5
192.168.12.0	255.255.255.240	192.168.12.4

Дейтаграмма с адресом получателя 192.168.12.8 будет отправлена на шлюз

- 192.168.12.4
- 192.168.12.5

66. Сообщения канального (DATA LINK) уровня называются

- кадрами
- пакетами
- дейтаграммами
- сегментами

67. Сообщения межсетевого (INTERNETWORK) уровня называются

- кадрами
- пакетами
- дейтаграммами
- сегментами

68. Сообщения транспортного (TRANSPORT) уровня называются

- кадрами
- пакетами
- дейтаграммами
- сегментами

69. Протокол RIP основан на алгоритме маршрутизации

- дистанционно-векторном
- состояния канала
- не основан ни на каком алгоритме

70. Протокол OSPF основан на алгоритме маршрутизации

- дистанционно-векторном
- состояния канала
- не основан ни на каком алгоритме

71. Протокол BGP основан на алгоритме маршрутизации
[] – дистантно-векторном
[] – состояния канала
[] – не основан ни на каком алгоритме
72. Протокол RIP – это протокол
[] – внутренней маршрутизации
[] – внешней маршрутизации
73. Протокол OSPF – это протокол
[] – внутренней маршрутизации
[] – внешней маршрутизации
74. Протокол BGP – это протокол
[] – внутренней маршрутизации
[] – внешней маршрутизации
75. Протокол IP обеспечивает передачу данных между
[] – сетевыми станциями (хостами)
[] – прикладными процессами внутри сетевых станций
76. TCP обеспечивает передачу данных между
[] – сетевыми станциями (хостами)
[] – прикладными процессами внутри сетевых станций
77. UDP обеспечивает передачу данных между
[] – сетевыми станциями (хостами)
[] – прикладными процессами внутри сетевых станций
78. IP – протокол с гарантированной доставкой данных
[] – да
[] – нет
79. TCP – протокол с гарантированной доставкой данных
[] – да
[] – нет
80. UDP – протокол с гарантированной доставкой данных
[] – да
[] – нет
81. IP – протокол с предварительным установлением соединения
[] – да
[] – нет
82. TCP – протокол с предварительным установлением соединения
[] – да
[] – нет
83. UDP – протокол с предварительным установлением соединения
[] – да
[] – нет

84. Гарантированная доставка данных в TCP осуществляется за счет:

- помехоустойчивого кодирования
- повторной передачи недоставленных данных
- переключения на альтернативные каналы доставки данных

85. Подтверждение получения данных в TCP осуществляется за счет:

- специальных пакетов-подтверждений, посылаемых получателем
- информации, передаваемой в обычных пакетах
- информации, передаваемой по дополнительному каналу

86. Пакет с запросом на установление соединения в TCP отличается:

- установленным флагом SYN
- установленным флагом FIN
- установленным флагом ACK
- установленным флагом RST

87. Пакет с запросом на разрыв соединения в TCP отличается:

- установленным флагом SYN
- установленным флагом FIN
- установленным флагом ACK
- установленным флагом RST

88. Номер последовательности (sequence number) в TCP нумерует:

- отправленные пакеты
- принятые пакеты
- отправленные байты
- принятые байты

89. Номер подтверждения (acknoledge number) в TCP нумерует:

- отправленные пакеты
- принятые пакеты
- отправленные байты
- принятые байты

90. Протокол ICMP предназначен для:

- передачи данных между сетевыми станциями (хостами)
- передачи данных между прикладными процессами внутри сетевых станций
- тестирования передачи данных
- управления передачей данных
- оповещения об ошибках передачи данных

91. Протокол маршрутизации – это

- протокол для управления маршрутизаторами
- протокол для обмена маршрутной информацией между маршрутизаторами
- протокол тестирования маршрутов

92. Автономная система – это

- локальная сеть, не связанная с глобальными сетями
- сеть или несколько сетей, использующих один и тот же протокол маршрутизации
- часть Интернет, охватывающая определенное административно-территориальное образование
- локальная сеть с автономными источниками питания

93. Статическая маршрутизация основана на маршрутных правилах

- введенных оператором
- построенным автоматически в процессе взаимодействия с другими маршрутизаторами

94. Динамическая маршрутизация основана на маршрутных правилах

- введенных оператором
- построенным автоматически в процессе взаимодействия с другими маршрутизаторами

95. DNS – это

- средство для назначения имен компьютерам
- средство для преобразования IP-адресов в MAC-адреса
- средство для преобразования символьических имен в MAC-адреса
- средство для преобразования символьических имен в IP-адреса
- средство для преобразования символьических имен в IP-адреса и обратно
- средство для маршрутизации электронной почты
- средство для маршрутизации другого трафика в стеке TCP/IP

96. Домен (в DNS) – это

- часть Интернет, принадлежащая некоторой организации
- поддерево дерева доменных имен, начинающееся с определенной вершины
- произвольное множество доменных имен
- множество доменных имен, оканчивающихся на .com
- одно доменное имя

97. Зона (в DNS) – это

- часть Интернет, принадлежащая некоторой организации
- поддерево дерева доменных имен, начинающееся с определенной вершины
- связная часть дерева доменных имен, размещенная как единое целое на одном из серверов доменных имен
- произвольное множество доменных имен, размещенное на одном из серверов доменных имен

98. Что больше (по числу имен) – зона .ru или домен .ru:

- зона
- домен

99. Каждое имя в DNS может характеризоваться данными, содержащими
- [] – путь к маршрутизатору
 - [] – ip-адрес компьютера
 - [] – почтовый адрес организации
 - [] – телефон организации
 - [] – факс организации
 - [] – имя компьютера
 - [] – фамилию руководителя организации
 - [] – имя сервера электронной почты
 - [] – имя сервера DNS
100. DNS неустойчив к атакам типа:
- [] – раскрытия информации о доменных именах
 - [] – подделки информации о доменных именах
101. Защита информации DNS выполняется при помощи
- [] – шифрования данных
 - [] – добавления Message Authentication Code
 - [] – добавления электронной цифровой подписи
102. Криптографические технологии используются для
- [] – защиты данных от раскрытия
 - [] – защиты данных от изменения
 - [] – гарантии подлинности отправителя данных
 - [] – обеспечения гарантированной доставки данных
 - [] – защиты сетей от несанкционированного доступа
 - [] – аутентификации сторон при соединении
103. Межсетевые экраны (firewall) используются для
- [] – защиты данных от раскрытия
 - [] – защиты данных от изменения
 - [] – гарантии подлинности отправителя данных
 - [] – обеспечения гарантированной доставки данных
 - [] – защиты сетей от несанкционированного доступа
 - [] – аутентификации сторон при соединении
104. Симметричные алгоритмы шифрования используются для
- [] – защиты данных от раскрытия
 - [] – защиты данных от изменения
 - [] – гарантии подлинности отправителя данных
 - [] – обеспечения гарантированной доставки данных
 - [] – защиты сетей от несанкционированного доступа
 - [] – аутентификации сторон при соединении
105. Асимметричные алгоритмы шифрования используются для
- [] – защиты данных от раскрытия
 - [] – защиты данных от изменения
 - [] – гарантии подлинности отправителя данных
 - [] – обеспечения гарантированной доставки данных
 - [] – защиты сетей от несанкционированного доступа
 - [] – аутентификации сторон при соединении

106. Криптографические контрольные суммы и хэш-функции используются для
- [] – защиты данных от раскрытия
 - [] – защиты данных от изменения
 - [] – гарантии подлинности отправителя данных
 - [] – обеспечения гарантированной доставки данных
 - [] – защиты сетей от несанкционированного доступа
 - [] – аутентификации сторон при соединении
107. Электронная цифровая подпись используется для
- [] – защиты данных от раскрытия
 - [] – защиты данных от изменения
 - [] – гарантии подлинности отправителя данных
 - [] – обеспечения гарантированной доставки данных
 - [] – защиты сетей от несанкционированного доступа
 - [] – аутентификации сторон при соединении
108. Симметричный алгоритм шифрования использует для шифрования и расшифровывания
- [] – один и тот же ключ
 - [] – разные ключи
109. Асимметричный алгоритм шифрования использует для шифрования и расшифровывания
- [] – один и тот же ключ
 - [] – разные ключи
110. В алгоритмах электронной подписи используются
- [] – алгоритмы симметричной криптографии
 - [] – алгоритмы асимметричной криптографии
 - [] – криптографические контрольные суммы
 - [] – хэш-функции
111. Алгоритм DES позволяет:
- [] – шифровать данные
 - [] – подписывать данные
 - [] – вырабатывать общий секрет (ключ) для других алгоритмов шифрования
112. Алгоритм Diffie-Hellman позволяет:
- [] – шифровать данные
 - [] – подписывать данные
 - [] – вырабатывать общий секрет (ключ) для других алгоритмов шифрования
113. Алгоритм RSA позволяет:
- [] – шифровать данные
 - [] – подписывать данные
 - [] – вырабатывать общий секрет (ключ) для других алгоритмов шифрования
114. Алгоритм DSS и схема Эль-Гамаля позволяют:
- [] – шифровать данные
 - [] – подписывать данные
 - [] – вырабатывать общий секрет (ключ) для других алгоритмов шифрования

115. Криптографическая контрольная сумма – это
[] – просто контрольная сумма
[] – контрольная сумма с дополнительным параметром – ключем
[] – контрольная сумма с дополнительным параметром – ключем, удовлетворяющая требованиям криптографической устойчивости
116. Для шифрования данных по алгоритму RSA используется
[] – открытый ключ отправителя
[] – открытый ключ получателя
[] – закрытый ключ отправителя
[] – закрытый ключ получателя
117. Для расшифровывания данных по алгоритму RSA используется
[] – открытый ключ отправителя
[] – открытый ключ получателя
[] – закрытый ключ отправителя
[] – закрытый ключ получателя
118. Для создания электронно-цифровой подписи используется
[] – открытый ключ отправителя
[] – открытый ключ получателя
[] – закрытый ключ отправителя
[] – закрытый ключ получателя
119. Для проверки электронно-цифровой подписи используется
[] – открытый ключ отправителя
[] – открытый ключ получателя
[] – закрытый ключ отправителя
[] – закрытый ключ получателя
120. Сертификат открытого ключа – это
[] – формат зашифрованной передачи открытого ключа
[] – электронный документ, удостоверяющий подлинность ключа
[] – документ, удостоверяющий право организации на открытый ключ
121. Сертификат открытого ключа выдается
[] – отправителем
[] – получателем
[] – удостоверяющим центром (Certification Authority)
122. Список отзыва сертификатов – это
[] – список просроченных сертификатов
[] – список отмененных сертификатов
[] – список испорченных сертификатов
123. Удостоверяющи центр (Certification Authority) – это
[] – организация, выпускающая открытые ключи
[] – организация, проверяющая открытые ключи
[] – организация, выпускающая сертификаты открытых ключей

124. Фильтр пакетов (род межсетевого экрана) использует для принятия решений:

- [] – информацию канального уровня
- [] – информацию сетевого уровня
- [] – информацию транспортного уровня
- [] – информацию прикладного уровня
- [] – логин и пароль пользователя

125. Шлюз приложений (род межсетевого экрана) использует для принятия решений:

- [] – информацию канального уровня
- [] – информацию сетевого уровня
- [] – информацию транспортного уровня
- [] – информацию прикладного уровня
- [] – логин и пароль пользователя

126. Демилитаризованная зона – это

- [] – часть сети, по поводу которой заключено соглашение о неприминении сетевых атак
 - [] – часть сети общего пользования, находящаяся под защитой провайдера
 - [] – часть сети общего пользования, находящаяся под защитой интернет-сообщества
 - [] – часть корпоративной сети, правила доступа к которой ослаблены по сравнению с остальной корпоративной сетью
 - [] – часть корпоративной сети, правила доступа к которой ужесточены по сравнению с остальной корпоративной сетью
 - [] – область между двумя межсетевыми экранами

127. MAC-адрес является адресом

- [] – канального уровня
- [] – сетевого уровня
- [] – транспортного уровня
- [] – прикладного уровня

128. IP-адрес является адресом

- [] – канального уровня
- [] – сетевого уровня
- [] – транспортного уровня
- [] – прикладного уровня

129. Номер порта (TCP, UDP) является адресом

- [] – канального уровня
- [] – сетевого уровня
- [] – транспортного уровня
- [] – прикладного уровня

130. Доменное имя является адресом

- [] – канального уровня
- [] – сетевого уровня
- [] – транспортного уровня
- [] – прикладного уровня

131. URL является адресом

- [] – канального уровня
- [] – сетевого уровня
- [] – транспортного уровня
- [] – прикладного уровня

132. Адрес электронной почты является адресом

- [] – канального уровня
- [] – сетевого уровня
- [] – транспортного уровня
- [] – прикладного уровня