Вопросы к экзамену по учебной дисциплине «Компьютерные сети»
(6 семестр)

1. Отличительные особенности коммутаторов L2 и L3 и маршрутизаторов.
2. Типы интерфейсов коммутаторов L3. Особенности конфигурации коммутаторов L3.
3. Определение и назначение агрегирования каналов. Петля коммутации, причины образования.
4. Назначение протокола STP. Механизм работы STP протокола. Принципы определения корневого коммутатора в автоматическом режиме работы протокола STP.
5. Протокол STP. Типы и содержание информации, которой обмениваются коммутаторы. Формат данных BPDU-кадра.
6. Протокол STP. Состояние и роли портов коммутатора. Принципы конфигурации приоритетов коммутаторов.
7. Отличие протокола STP, PVST, PVST+, RSTP, MSTP. Типы связующих деревьев MSTP.
8. Технологии и методы агрегации каналов, отличительные особенности. Условия настройки агрегации на коммутаторах и основные правила.
9. Отличительные особенности работы LACP и PAgP. Механизм их настройки и принцип работы. Методы балансировки нагрузки, их настройка.
10. Определение и назначение технологии NAT. Типы адресов в NAT. Различия в видах трансляции IP-адресов.
11. Описание принципа работы статического и динамического NAT для преобразования IPv4-адресов. Примеры конфигурации Способы проверки конфигурации NAT.
12. Описание принципа работы PAT для преобразования IPv4-адресов. Последовательность действий и пример конфигурации PAT для диапазона публичных IP-адресов и для одного публичного IP-адреса.
13. Проблемы совместимости IPv6 и IPv4-сетей. Отличие IPv4 и IPv6 заголовков. Расширенные заголовки IPv6.
14. Методы преобразования IPv6-адресов в IPv4. Описание метода двойного стека, его достоинства и недостатки, принципы настройки.
15. Описание механизма туннелирования, его достоинства и недостатки, принципы настройки. Применение IPv6 туннелирования, принципы настройки.
16. Описание принципа работы статического и динамического NAT для преобразования IPv6 в IPv4-адресов. Примеры конфигурации Способы проверки конфигурации NAT.
17. Описание принципа работы PAT NAT-PT. Последовательность действий и пример конфигурации PAT NAT-PT.
18. Назначение и принцип работы IPv4-mapped NAT-PT. Последовательность действий и пример конфигурации IPv4-mapped NAT-PT.
19. Организация доступа к глобальной сети, типы операторов связи. Автономная систем, ее регистрация, типы регистраторов.

20. Принципы функционирования протокола BGP для внутренней и внешней маршрутизации. Список атрибутов BGP, расчет метрики.

21. Процесс отбора маршрутов по протоколу BGP, базы данных BGP.

22. Типы сообщений BGP. Принцип конфигурации BGP и перераспределения маршрутов из других протоколов.

23. Доменное имя и домен. Распределение доменных имен. Компоненты системы доменных имен. Этапы регистрации доменного имени.

24. Функции DNS-резолвера. Способы конфигурации различных DNS-серверов.

25. Назначение аутентификации на маршрутизаторах глобальной сети. Типы аутентификации протокола OSPF. Процесс аутентификации по протоколу OSPF. Способы настройки аутентификации по протоколу OSPF.

26. Способы настройки аутентификации по протоколу OSPF и RIP. Настройка аутентификации в протоколах EIGRP и BGP.

27. Обоснование применения OSPF с несколькими областями. Типы областей Multiarea OSPF. Требования к планированию областей OSPF.

28. Типы маршрутизаторов OSPF. Особенности конфигурации OSPF для нескольких областей. Принципы конфигурации маршрутизаторов для согласования работы по протокола RIP и OSPF.

29. Особенности конфигурации OSPF для нескольких областей. Принципы конфигурации маршрутизаторов для согласования работы по протоколам EIGRP и OSPF.

30. Стандарты последовательной связи и типы соединения DTE–DCE, DTE–DTE.

31. Сравнение протоколов инкапсуляции для передачи данных в глобальную сеть.

32. Описание протокола HDLC и типы поддерживаемых кадров, описание полей.

33. Компоненты протокола PPP и их назначение. Формат кадра PPP, описание полей.

34. Описание этапов установления соединения PPP. Отличия типов аутентификации протокола PPP, особенности их конфигурации.

35. Назначение и принцип работы ACL. Типы ACL и их отличия.

36. Отличительные особенности настройки стандартных и расширенных списков контроля доступа. Примеры конфигурации стандартных и расширенных ACL. Номера портов для разных видов протоколов.

37. Межсетевое экранирование, функции Cisco ASA.

38. Типы систем фильтрации.

39. Принципы базовой конфигурации межсетевого экрана Cisco ASA.

40. Особенности организации сети с межсетевым экраном и демилитаризованной зоной.

41. Назначение и принцип конфигурации демилитаризованной зоны.

42. Назначения технологии VPN, достоинства. Сравнение основных типов сетей VPN. Типы протоколов туннелирования.

43. Описание протокола GRE. Структура пакета, передаваемого через Site-

to-Site VPN. Этапы инкапсулированния пакета при использовании технологии Site-to-Site VPN.

44. Этапы настройки туннеля GRE. Назначение трассировки.

45. Описание IPSec. Типы протоколов IPSec. Этапы настройки туннеля IPsec.

46. Описание процесса создания защищенного соединение по технологии IPSec.

47. Принципы конфигурации Remote access IPSec VPN на маршрутизаторах. Принципы конфигурации Site-to-Site VPN на маршрутизаторах.

48. Способы конфигурации VPN туннелей на межсетевых экранах. Принципы конфигурации Site-to-Site IPSec VPN на межсетевых экранах.

49. Протоколы SSL и TLS. Назначение, отличия, свойства.

50. Способы конфигурации VPN туннелей на межсетевых экранах. Принципы конфигурации туннеля SSL/TLS Clientless Access на межсетевых экранах.

51. Виды spoofing-атак. Цель MAC-spoofing атаки. Последовательность действий при реализации атаки MAC-spoofing.

52. Виды spoofing-атак. Цель ARP-spoofing атаки. Самопроизвольный ARP. Последовательность действий при реализации атаки ARP-spoofing.

53. Виды spoofing-атак. Цель IP-spoofing атаки. Последовательность действий при реализации атаки IP-spoofing.

54. Виды spoofing-атак. Цель DNS-spoofing атаки. Последовательность действий при реализации атаки DNS-spoofing.

55. Виды spoofing-атак. Цель CAM-table overflow атаки. Последовательность действий при реализации атаки CAM-table overflow.

56. Способы защиты от spoofing-атак. Конфигурация функции Port-security. Возможные действия при нарушении функции Port-security.

57. DoS и DDoS атаки и их отличия. Виды DoS и DDoS атак. Классификация и цели DDoS-атак по уровням OSI.

58. Типы DoS и DDoS атак. Атаки Ping и HTTP flood. Последовательность действий при реализации атак Ping и HTTP flood. Способы защиты от атак Ping и HTTP flood.

59. Типы DoS и DDoS атак. Атаки Ping of Death и IP Null. Последовательность действий при реализации атак Ping of Death и IP Null.

60. Типы DoS и DDoS атак. Атаки UDP flood и SYN-flood. Последовательность действий при реализации атаки UDP и SYN-flood. Способы защиты от атаки UDP и SYN-flood.

61. Принцип работы DHCP протокола и его уязвимость. Последовательность действий при реализации атаки DHCP starvation.

62. Принцип работы DHCP протокола и его уязвимость. Последовательность действий при реализации атаки типа MitM.

63. Принцип работы DHCP протокола и его уязвимость. Функция DHCP snooping. Конфигурация функции DHCP snooping.

64. Преимущества VLAN. Процесс передачи кадра в сети с протоколом

802.1Q. Уязвимости процесса передачи кадра в виртуальных локальных сетей.

65. Процесс согласования портов коммутаторов в виртуальных локальных сетях. Уязвимости данного процесса.

66. Протокол VTP, преимущества, недостатки. Роли коммутаторов по протоколу VTP. Настройка протокола VTP на коммутаторе. Типы сообщений протокола VTP.

67. Способы защиты виртуальных локальных сетей.

68. Протоколы для удалённого доступа и настройки сетевого оборудования. Конфигурация разных способов удалённого доступа и настройки сетевого оборудования.

69. Способы перехвата трафика. Назначение снифферов. Протоколы и механизмы зеркалирования трафика. Способы конфигурации зеркалирования портов.

70. Протоколы зеркалирования трафика. Примеры их конфигурации. Проверка настройки зеркалирования на коммутотаторе.

71. Назначение протокола CDP и его уязвимость. Способы конфигурации зашифрованных паролей на сетевых устройствах.

72. Процессы доступа и контроля AAA. Сравнительная характеристика протоколов RADIUS и TACACS+.

73. Описания технологии RADIUS и процесса обмена сообщениями при аутентификации пользователя. Процесс настройки оборудования для использования технологии RADIUS.

74. Описания технологии TACACS+ и процесса обмена сообщениями при аутентификации пользователя. Процесс настройки оборудования для использования технологии TACACS+.

75. Назначение, виды, системы NAC. Политика контроля доступ. Компоненты NAC. Способы NAC.

76. Назначение стандарта 802.1x, основные элементы. Протокол EAPOL. Процесс настройки оборудования для использования стандарта 802.1x.

77. Протокол EAPOL. Этапы работы протокола EAPOL.

78. Процесс настройки аутентификации пользователей для доступа к сети по стандарту 802.1x.

79. Протоколы безопасной передачи данных в беспроводных сетях.

80. Способы аутентификации пользователей при получении доступа к беспроводной сети.

81. Устройство контроля беспроводных сетей. LWAPP, CAPWAP. Принцип конфигурации WLC.

82. Технологии пассивный оптических сетей. Их особенности и отличительные черты.

83. Разновидности xPON сетей. Основные характеристики. Топологии xPON, их сравнительная характеристика. Оборудование, используемое для организации xPON сетей.

84. Схема пассивной оптической сети, описание ее основных участков. Назначение WDM, ODF, OLT, ОРШ, ОРК, ONT. Одноуровневая и многокаскадная схема с размещения сплиттеров.

85. Виды оптических разветвителей. Разъемные соединения. Неразъемные соединения. Резервирование xPON.

86. Структура оптического кабеля. Принципы выбора и прокладки кабеля, расчета оптических волокон в кабеле при проектировании сетей xPON.

87. Расчет оптического бюджета волоконно-оптической линии xPON. Расчеты затухания оптического сигнала.

88. Графический расчет оптического бюджета в сети xPON. Классы затухания для сетей xPON.

89. Варианты построения защищенных локальных сетей на основе межсетевых экранов и дополнительных программно-аппаратных средств фильтрации трафика.