# Вопросы к части I

### **1. Почему сети WAN появились раньше, чем сети LAN?**

Сети WAN (Wide Area Network) появились раньше, потому что они использовались для подключения удаленных вычислительных центров, офисов и пользователей, находящихся на больших расстояниях друг от друга. В 1960-х и 1970-х годах существовала необходимость связывать компьютеры через большие географические расстояния, что привело к созданию таких сетей. В то время как локальные сети (LAN) стали более актуальными позже, когда развитие вычислительной техники и технологий позволило объединять устройства в пределах одного здания или небольшого региона.

### **2. Интернет в соответствии с критериями классификации компьютерных сетей**

Интернет можно классифицировать как:

* **Тип**: Глобальная сеть (WAN), охватывающая весь мир.
* **Схема соединений**: Сеть с коммутацией пакетов.
* **Топология**: Многослойная с различными структурами (дерево, кольцо, шина и т.д.).
* **Типы передачи**: Пакетная передача данных.
* **Цель**: Обслуживание разнообразных приложений (интернет-сервисы, обмен данными, коммуникации и т.д.).

### **3. Главное отличие многотерминальной системы от компьютерной сети**

Многотерминальная система — это система, где несколько терминалов подключены к центральному устройству (например, компьютеру), но не могут обмениваться данными друг с другом. В компьютерной сети терминалы (или узлы) могут обмениваться данными между собой, не имея необходимости в центральном узле.

### **4. Определения:**

* **Клиент** — это устройство или программа, которая запрашивает и получает услуги или ресурсы от сервера.
* **Сервер** — это устройство или программа, которая предоставляет услуги или ресурсы клиенту.
* **Сетевая служба** — это набор функций, которые предоставляются пользователям в компьютерной сети, например, электронная почта или файловое хранилище.
* **Сетевой сервис** — это конкретный сервис, предоставляемый в рамках сетевой службы, например, доступ к веб-страницам через HTTP.
* **Сетевая услуга** — это процесс или операция, предоставляемая пользователям в рамках сети, как часть сетевого сервиса.

### **5. Наиболее распространенный тип топологии в локальных сетях**

На данный момент наиболее распространенной топологией в локальных сетях является **звезда**. В такой сети все устройства подключены к центральному узлу (например, к свитчу), который управляет передачей данных.

### **6. Параметры данных как признак информационного потока:**

* a) **Адрес назначения** — позволяет понять, куда направляются данные.
* б) **Адрес источника** — указывает на исходное устройство, которое отправило данные.
* в) **Тип приложения** — помогает определить, для какого приложения или сервиса предназначены данные.
* г) **Номер интерфейса, на который поступил пакет** — может быть использован для идентификации интерфейса или порта, через который данные поступили в систему.

### **7. Утверждения о скорости передачи данных и пропускной способности:**

* **a) Скорость передачи данных может быть выше предложенной нагрузки (речь об одних и тех же данных)** — Это неверно, поскольку предложенная нагрузка — это нагрузка, которую система может обрабатывать в данный момент.
* **б) Скорость передачи данных всегда ниже пропускной способности** — Это верно, поскольку пропускная способность — это максимальная скорость передачи данных, а реальная скорость передачи данных может быть меньше.
* **в) Пропускная способность никак не связана с предложенной нагрузкой** — Это неверно, пропускная способность и нагрузка напрямую связаны, поскольку нагрузка определяет, как эффективно используется канал.
* **г) Скорость передачи данных может быть ниже предложенной нагрузки** — Это верно, так как реальная передача данных может не использовать всю доступную пропускную способность.

### **8. Можно ли организовать надежную передачу данных без установления логического соединения?**

Да, можно. Например, в сетях с коммутацией пакетов (например, в Интернете) данные могут передаваться по принципу "отправить и забыть", где каждый пакет передается независимо, а надежность обеспечивается за счет повторной передачи потерянных пакетов.

### **9. Логическое соединение, которое можно назвать виртуальным каналом**

Виртуальный канал — это логическое соединение, которое эмулирует физическое соединение между двумя узлами, но при этом данные могут передаваться через разные маршруты. Такой канал может быть организован в сетях с коммутацией пакетов или в виртуальных частных сетях (VPN).

### **10. Утверждения о коммутации каналов:**

* **а) В сетях с коммутацией каналов необходимо предварительно устанавливать соединение** — Верно. Передача данных возможна только после установления соединения.
* **б) В сетях с коммутацией каналов не требуется указывать адрес назначения данных** — Неверно. Адрес назначения указывается при установке соединения.
* **в) Сеть с коммутацией пакетов более эффективна, чем сеть с коммутацией каналов** — Верно. Сети с коммутацией пакетов более гибкие и эффективные в использовании ресурсов.
* **г) Сеть с коммутацией каналов предоставляет гарантированную пропускную способность** — Верно. В сети с коммутацией каналов канал выделяется на определенное время, обеспечивая стабильную пропускную способность.
* **д) Данные, поступившие в составной канал, доставляются вызываемому абоненту без задержек и потерь** — Неверно. В реальных условиях могут быть задержки и потери.
* **е) Составной канал постоянно закрепляется за двумя абонентами** — Верно.
* **ж) Составной канал имеет постоянную и фиксированную пропускную способность на всем своем протяжении** — Верно.

### **11. Недостатки сетей с коммутацией каналов**

* Неэффективное использование ресурсов, так как канал заблокирован на протяжении всего соединения, даже если данные не передаются.
* Сложности с масштабированием и высокой стоимостью за счет необходимости выделения ресурсов для каждого соединения.

### **12. Негативные свойства сетей с коммутацией пакетов для мультимедийной информации**

* Задержки в передаче, из-за того что данные разбиваются на пакеты, которые могут передаваться разными маршрутами.
* Потери пакетов, что может нарушить качество мультимедийного контента, особенно в видео и аудио передаче.

### **13. Характеристики, полностью определяемые пропускной способностью канала:**

* **г) время сериализации** — Это время, необходимое для передачи всего пакета данных в канал, и оно напрямую зависит от пропускной способности канала. Сила сигнала или другие факторы на этом уровне не влияют. Другие характеристики, такие как время коммутации пакета, время распространения сигнала и время ожидания в очереди, не зависят напрямую от пропускной способности канала.

### **14. Элементарный канал цифровых фонных сетей 64 Кбит/с:**

Элементарный канал с пропускной способностью 64 Кбит/с в цифровых сетях обычно используется для передачи одного голосового канала в телефонной сети. Это стандарт для каналов в телефонных системах (например, в ISDN). Время, необходимое для передачи одного бита данных, составляет *164000\frac{1}{64000}* секунды, что равно примерно 15.625 микросекунд на бит.

Если это канал для передачи одного голосового канала, то 64 Кбит/с — это именно требуемая пропускная способность для передачи звуковых сигналов, оцифрованных с использованием кодирования с битовой скоростью 64 Кбит/с (например, G.711).

### **15. Почему линия связи, соединяющая коммутаторы, не может иметь пропускную способность 30,710 Кбит/с?**

Пропускная способность канала, соединяющего коммутаторы, не может быть 30,710 Кбит/с из-за несовпадения с установленными стандартами и ограничениями оборудования. Линии между коммутаторами обычно имеют ограничение, и часто используются с пропускной способностью, соответствующей числу каналов, которые могут передаваться одновременно. Например, каналы ISDN имеют стандартную пропускную способность 64 Кбит/с, и если коммутатор работает с таким стандартом, то сумма пропускных способностей будет ограничена. Кроме того, технические и экономические факторы могут ограничивать использование такого канала.

### **16. Аналогия между методами передачи:**

Описанный метод обмена письмами (где каждая глава отправляется и подтверждается) близок к **методу с установлением логического соединения**. Это связано с тем, что каждая глава (или пакет) передается по определенному маршруту, и гарантируется, что она будет получена (как подтверждение получения). Это аналогично установлению соединения и подтверждению доставки пакетов в сетях с коммутацией соединений.

### **17. Почему скорость передачи данных в сетях с коммутацией пакетов всегда ниже пропускной способности?**

**Правильный ответ:**

* **б) из-за разделения линий связи с другими пользователями** — В сетях с коммутацией пакетов каналы могут делиться между разными пользователями, что приводит к снижению скорости передачи данных для каждого отдельного потока.
* **г) из-за задержек на коммутаторах** — В процессе передачи данных пакеты могут испытывать задержки из-за обработки на маршрутизаторах и коммутаторах.

### **18. Почему пакетный коммутатор имеет буферную память?**

* **а) для принятия решения о коммутации пакета требуется выполнить анализ заголовка пакета** — Буферная память позволяет коммутатору временно хранить пакеты для анализа их заголовков.
* **б) коммутатор иногда не успевает обработать пакет до прихода следующего** — В случае, если коммутатор не успевает обработать все поступающие пакеты вовремя, они могут быть помещены в буфер.
* **г) скорость передачи данных в одной линии связи коммутатора выше, чем в другой** — Если входная линия быстрее, чем выходная, пакеты будут помещены в буфер.

### **19. Сходство и различие составного и виртуального каналов:**

* **Сходство**: Оба типа каналов предоставляют логическое соединение для передачи данных между двумя узлами, создавая видимость прямого канала.
* **Различие**: Составной канал выделяет физическую полосу пропускания, которая полностью резервируется для конкретного соединения, а виртуальный канал использует общую физическую инфраструктуру, разделяя пропускную способность между несколькими соединениями с логической изоляцией.

### **20. Аналогия с методами продвижения в компьютерных сетях:**

* **Дейтаграммная пакетная коммутация** — **Доставка товаров по почте**. Каждый товар отправляется независимо, и если один товар не дошел, его нужно отправить повторно.
* **Коммутация каналов** — **Движение автотранспорта**. Для доставки товара необходим выделенный путь.
* **Пакетная коммутация на основе виртуальных каналов** — **Лесосплав**. Поток объектов (пакетов) движется по заранее определенному маршруту, но с возможностью динамического изменения.
* **Пакетная коммутация на основе логических соединений** — **Движение городских автобусов**. Есть заранее установленные маршруты, и пассажиры (пакеты) следуют по ним.

### **21. Какой метод передачи данных более защищен от атак — коммутация каналов или коммутация пакетов?**

**Коммутация каналов** обычно более защищена от атак, поскольку выделяется постоянный путь для передачи данных, что делает ее менее уязвимой к вмешательствам. В коммутации пакетов данные передаются через общие каналы, и могут быть перехвачены или изменены на пути.

### **22. На каком уровне модели OSI работают сетевые службы и приложения?**

* **Сетевые службы** работают на **сетевом уровне (Layer 3)**, предоставляя функции маршрутизации и передачи данных между различными узлами.
* **Приложения** работают на **прикладном уровне (Layer 7)**, где находятся сервисы, обеспечивающие взаимодействие пользователя с сетью (например, HTTP, FTP).

### **23. Можно ли представить модель взаимодействия сетевых средств с шести уровнями?**

Да, можно. Модели взаимодействия могут быть различными, и она может включать шесть уровней, если для конкретного контекста это будет более удобно. Например, можно объединить несколько уровней модели OSI, например, транспортный и сеансовый, в один уровень, если это будет разумно для конкретной архитектуры.

### **24. Всегда ли справедливо утверждение: «Протокол - это стандарт, формализованно описывающий правила взаимодействия двух систем»?**

**Да**, это утверждение в целом верно. Протокол — это набор правил, который описывает, как данные должны быть переданы между двумя или более системами, включая формат сообщений, порядок обмена и условия для успешной передачи.

### **25. Взаимодействие двух компьютеров с разными драйверами сетевых адаптеров Ethernet:**

Если оба компьютера имеют одинаковое программное и аппаратное обеспечение, но их драйверы сетевых адаптеров Ethernet поддерживают разные интерфейсы с протоколом сетевого уровня (IP), то **они не смогут нормально взаимодействовать**. Это связано с тем, что сетевые интерфейсы и драйверы должны быть совместимы на уровне передачи данных и маршрутизации. Различия в реализации протоколов сетевого уровня (например, IPv4 и IPv6) или интерфейсов на уровне драйверов могут привести к несовместимости, мешая правильной работе сети.

### **26. Инкапсуляция PDU и уровень протокола:**

Если протокольная единица данных (PDU) некоторого протокола инкапсулирована в PDU другого протокола, это **не всегда** означает, что первый протокол относится к уровню **k+1** модели OSI. Это может быть верно для некоторых типов протоколов, но не является универсальным правилом. Инкапсуляция означает, что один протокол "оборачивает" данные другого, но это не обязательно определяет их уровень в модели OSI. Важно учитывать, какие функции выполняет каждый из этих протоколов.

### **27. Преимущества открытых спецификаций:**

Открытые спецификации дают несколько ключевых преимуществ:

* **Совместимость и интеграция**: Устройства и программное обеспечение, поддерживающие открытые стандарты, могут легко взаимодействовать, что упрощает интеграцию различных систем.
* **Гибкость и инновации**: Открытые спецификации позволяют разработчикам создавать инновационные решения, не ограниченные патентами или закрытыми стандартами.
* **Снижение затрат**: Открытые стандарты помогают уменьшить затраты, так как они часто являются бесплатными и не требуют лицензионных сборов.
* **Портативность**: Программы и оборудование, использующие открытые стандарты, могут работать в разных средах.

### **28. Вычисление стандартного отклонения и коэффициента вариации по гистограмме:**

Для вычисления стандартного отклонения и коэффициента вариации нужно знать данные на гистограмме. Без изображения гистограммы невозможно точно вычислить эти параметры. Стандартное отклонение определяется как квадратный корень из дисперсии, а коэффициент вариации — как отношение стандартного отклонения к среднему значению, выраженное в процентах.

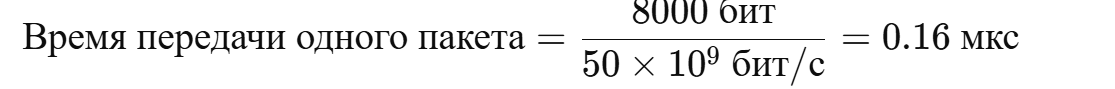
### **29. Как уменьшить скорость потока пакетов:**

Скорость потока пакетов можно уменьшить следующими способами:

* **Использование алгоритмов управления перегрузкой** (например, TCP Congestion Control).
* **Уменьшение размера пакетов** (это может уменьшить частоту передачи).
* **Использование сжатия данных**, что также снижает количество передаваемых битов.
* **Модификация уровня приоритета пакетов** в случае работы с QoS (Quality of Service).

### **30. Скорость передачи отдельного пакета в потоке 50 Гбит/с на канале 100 Гбит/с:**

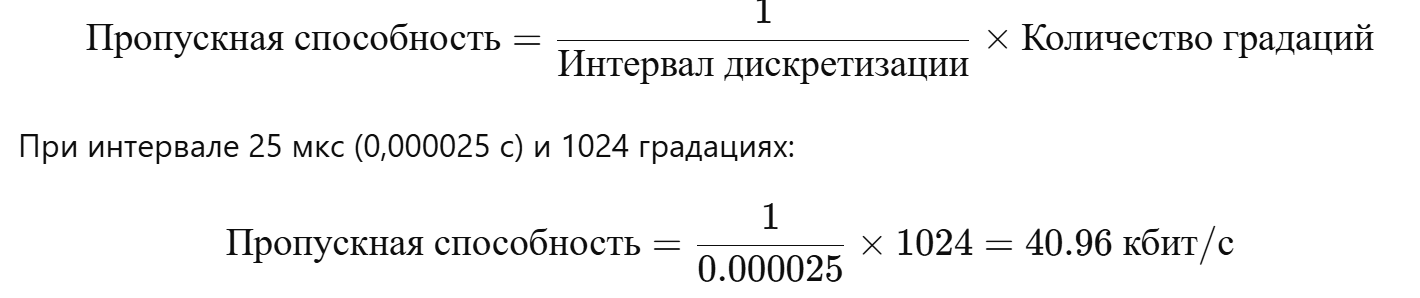
Скорость передачи отдельного пакета в потоке зависит от размера пакета. Если размер пакета *PP* равен 1000 байт (8 000 бит), то:



Таким образом, скорость передачи одного пакета — это 0.16 микросекунд на пакет, если скорость потока 50 Гбит/с.

### **31. Пропускная способность для голосового трафика (дискретизация 25 мкс и 1024 градации):**

Пропускная способность для передачи голосового трафика может быть вычислена по формуле:



Таким образом, для передачи голосового трафика потребуется пропускная способность около 41 кбит/с.

### **32. Тип обслуживания для трех классов трафика с минимальной гарантированной способностью:**

Для обеспечения различных минимальных гарантированных способностей для трех классов трафика целесообразно применить **систему с приоритетным обслуживанием** или **сервис с гарантированной пропускной способностью**, например, **DiffServ (Differentiated Services)**. Эти системы позволяют выделить гарантированные ресурсы для каждого класса трафика, что помогает избежать проблем с задержками и потерями для важных данных.

### **33. Причины возникновения очередей при невысокой средней загрузке:**

Очереди могут возникать даже при невысокой средней загрузке, если:

* **Трафик является бурным** (временные пики), что вызывает периодические перегрузки.
* **Распределение пакетов** может быть неравномерным, например, передача больших пакетов или потоков может заполнять буфер быстрее.
* **Наличие задержек обработки** на маршрутизаторах или коммутаторах.

### **34. Приложения, чувствительные к потерям пакетов, задержкам и вариациям задержек:**

Приложения, которые наиболее чувствительны к потерям пакетов, задержкам и их вариациям:

* **Мультимедийные сервисы** (видео и аудио, особенно в реальном времени).
* **Программа управления роботом** — для точных и своевременных действий.
* **Широковещательная рассылка аудиоинформации** — потеря пакетов и задержки ухудшают качество.

Менее чувствительные:

* **Файловый сервис** — может использовать повторную передачу.
* **Электронная почта** — нет строгих требований по времени доставки.
* **Текстовый редактор** — не зависит от времени.

### **35. Может ли трафик передаваться с большими задержками, но без джиттера?**

Да, это возможно. Трафик может передаваться с высокими задержками, но без джиттера (вариаций задержек), если задержка постоянна для каждого пакета, что обеспечивается стабильной сетью и отсутствием переполнений.

### **36. Нежелательные последствия приоритетного обслуживания:**

Приоритетное обслуживание может привести к следующим нежелательным последствиям:

* **Задержки для низкоприоритетного трафика** (проблемы с задержкой или даже потеря пакетов).
* **Дискриминация трафика** — важные пакеты могут получать все ресурсы, оставляя другие потоки без обслуживания.
* **Недоиспользование ресурсов** — если приоритетный трафик низкий, может не использоваться вся пропускная способность канала.

### **37. Причины погрешности при измерении времени оборота пакетов:**

* **Активные схемы измерений**: Погрешности могут возникнуть из-за искусственного влияния на поток данных, например, дополнительных задержек при генерации измерений или нестабильности измерительной системы.
* **Пассивные схемы измерений**: Погрешности могут быть связаны с неточностью оборудования, из-за ошибок во временных метках или потерянных данных.

### **38. Параметр трафика, изменяющийся при инжиниринге:**

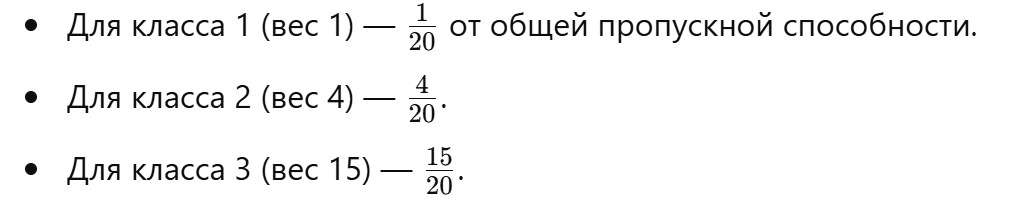
При инжиниринге трафика изменяется, как правило, **интервал между пакетами** или **плотность потока данных**. Это делается для уменьшения перегрузки сети или для обеспечения QoS.

### **39. Нужно ли буферизировать поток данных в коммустаторе?**

Если скорость обработки пакетов на коммутационном блоке равна 1 мкс, а скорость поступления пакетов 10,000 пакетов в секунду, то в среднем между двумя пакетами будет задержка 100 мкс, что значительно превышает время обработки. Таким образом, для предотвращения потерь пакетов необходим **буфер** для очереди.

### **40. Разделение пропускной способности между тремя классами трафика:**

Для реализации взвешенного обслуживания с пропорциями 1:4:15 для классов трафика, в каждый цикл просмотра по 100 мкс должно передаваться:



Примерное распределение объемов данных будет следующим:

* Класс 1 — 1/20 от 100 мкс.
* Класс 2 — 4/20 от 100 мкс.
* Класс 3 —15/20 от 100 мкс.

### **41. Коэффициент пульсации трафика как количественная характеристика**

**Да, коэффициент пульсации трафика** является количественной характеристикой. Он измеряет степень вариативности трафика во времени, характеризуя колебания интенсивности потока данных. Коэффициент пульсации трафика позволяет количественно оценить, насколько нагрузка на сеть может изменяться от одного момента времени к другому. Этот коэффициент может быть полезен для анализа поведения трафика, его стабильности и предсказуемости, что важно для планирования пропускной способности и эффективного управления сетью.

### **42. Влияние профилирования и сглаживания на пиковую и среднюю скорость кондиционируемых потоков**

**Профилирование** и **сглаживание** — это методы, применяемые для управления трафиком в сети, особенно для обеспечения качества обслуживания (QoS). Их влияние на пиковую и среднюю скорость кондиционируемых потоков следующее:

* **Профилирование**: этот процесс включает в себя ограничение скорости передачи данных (например, путем настройки максимальных и минимальных значений трафика в сети). Профилирование может привести к **уменьшению пиковой скорости трафика**, потому что оно ограничивает его в пиковые моменты. Однако **средняя скорость** может оставаться неизменной, так как профилирование регулирует только экстремальные колебания трафика, обеспечивая более стабильную и предсказуемую нагрузку на сеть.
* **Сглаживание**: сглаживание используется для уменьшения резких изменений в интенсивности трафика. Оно **снижает пики трафика**, уменьшая возможные переполнения и задержки в сети. Средняя скорость трафика может изменяться в зависимости от того, насколько сильно сглаживание "разглаживает" пиковые значения, но **пиковая скорость значительно снижается**. В результате трафик становится более стабильным и предсказуемым.

Таким образом, **профилирование и сглаживание** помогают уменьшить **пиковые значения** трафика, делая нагрузку на сеть более управляемой, но не всегда изменяют среднюю скорость значительно.

### **43. Профилирование и потеря пакетов: объяснение противоречия**

Профилирование трафика — это механизм, который используется для обеспечения качества обслуживания (QoS) в сети. В процессе профилирования трафик, который выходит за пределы установленных лимитов (например, максимальной скорости передачи), может быть **отфильтрован или отброшен**.

**Как это связано с потерей пакетов?** Потеря пакетов действительно ухудшает качество обслуживания, так как данные могут быть потеряны, и будет необходимо их повторно передавать, что увеличивает задержки и снижает надежность. Однако в контексте **профилирования** потеря пакетов может рассматриваться как компромисс для улучшения общей производительности сети, особенно в случае, когда трафик перегружает сеть.

**Объяснение противоречия**:

* **Преднамеренная потеря пакетов** в процессе профилирования используется для предотвращения **перегрузки сети**. Если трафик слишком высок, это может привести к большим задержкам и ухудшению качества обслуживания. Профилирование помогает **управлять потоком трафика**, ограничивая или отклоняя избыточные пакеты, чтобы избежать перегрузки сети, которая может вызвать более серьезные проблемы, чем потеря небольшого числа пакетов.
* Например, в случае **трафика с ограниченной пропускной способностью**, если трафик слишком интенсивен и не может быть обработан сетью, **потери пакетов** могут быть неизбежными, но это будет способствовать тому, чтобы сеть оставалась в рабочем состоянии, поддерживая приемлемую производительность для оставшихся пакетов.

Таким образом, потеря пакетов в процессе профилирования может **увеличить эффективность сети** в условиях перегрузки, что в конечном итоге **улучшает общее качество обслуживания**, несмотря на потери.

# **Вопросы к части II**

1. **Может ли линия связи быть составным каналом?**

Да, линия связи может быть составным каналом. Составной канал — это канал, который может передавать несколько потоков данных одновременно через разные подканалы. Например, линия связи с несколькими каналами может передавать данные через разные частотные диапазоны или с использованием различных методов мультиплексирования (например, частотного или временного). Таким образом, линия связи может быть частью составного канала, если она поддерживает такую передачу.

1. **Укажите, к какому типу линий связи относятся волоконно-оптические кабели:**
   1. **б) направленные проводные.**

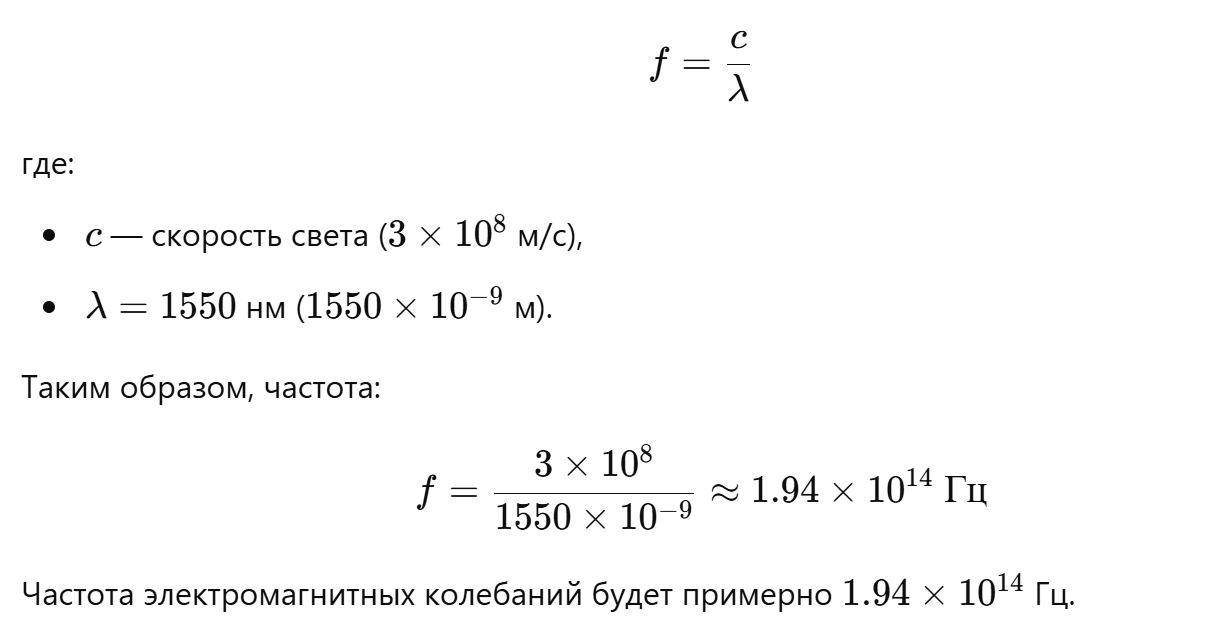
Волоконно-оптические кабели являются направленными проводными линиями связи, поскольку они передают световые сигналы в одном направлении через оптоволоконные нити, обеспечивая высокоскоростную и высококачественную передачу данных на большие расстояния.

1. **Сетевой адаптер является устройством:**

Сетевой адаптер является устройством **DTE (Data Terminal Equipment)**. Это устройство, которое подключается к сети и предоставляет интерфейс для подключения с конечными устройствами, такими как компьютеры, серверы, маршрутизаторы и т. д.

1. **Чем отличаются усилители и регенераторы телекоммуникационных сетей?**
   1. **Усилители** увеличивают амплитуду сигнала, но не восстанавливают его исходную форму, что может приводить к накоплению искажений и шумов. Усилители применяются для увеличения дальности передачи.
   2. **Регенераторы** восстанавливают сигнал в его первоначальном виде (включая устранение шума), преобразуя его в цифровую форму или усиливая, чтобы устранить потери качества из-за затухания и искажений. Это позволяет поддерживать качественную передачу на дальние расстояния.
2. **Какова частота электромагнитных колебаний волны длиной 1550 нм?**

Для вычисления частоты можно использовать формулу связи между длиной волны *λ*, скоростью света *c* и частотой *f*:



1. **Можно ли выполнить преобразование Фурье для непериодической функции?**

Да, можно выполнить преобразование Фурье для непериодической функции. В случае непериодической функции используется **преобразование Фурье с непрерывным спектром**, что дает представление о функции в виде интеграла по частотам, а не суммы дискретных частот.

1. **Какие меры можно предпринять для увеличения информационной скорости звена?**
   1. **б) выбрать кабель с более широкой полосой пропускания.**

Выбор кабеля с более широкой полосой пропускания позволит передавать данные с большей скоростью, так как больше частотных диапазонов будет доступно для передачи информации.

1. **Поясните, почему полезно знать амплитудно-частотную характеристику линии:**
   1. **а) она позволяет узнать затухание сигнала определенной амплитуды и любой частоты.**

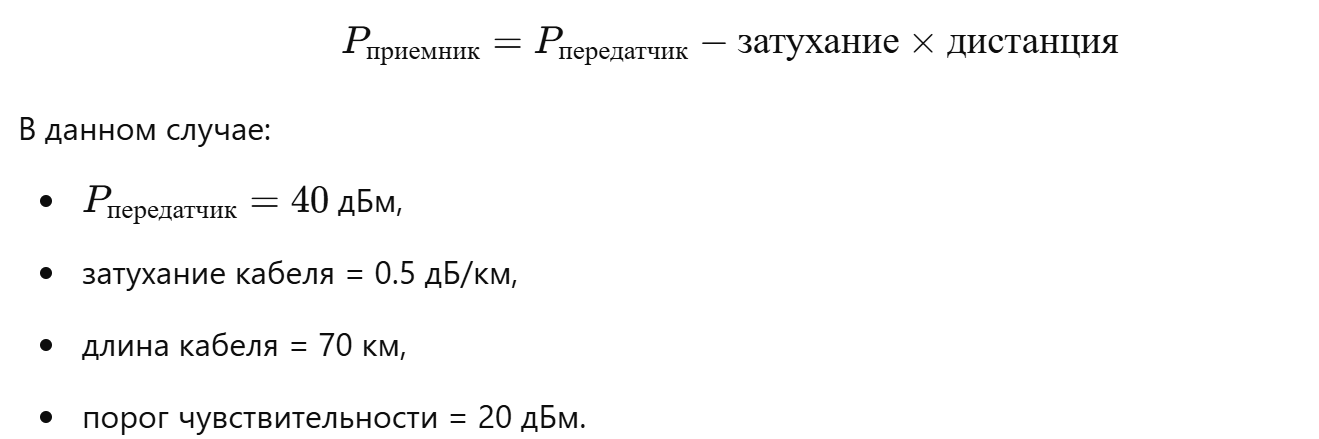
Амплитудно-частотная характеристика показывает, как амплитуда сигнала изменяется в зависимости от частоты, что важно для оценки того, как линия передает различные частоты и какие искажения могут возникать.

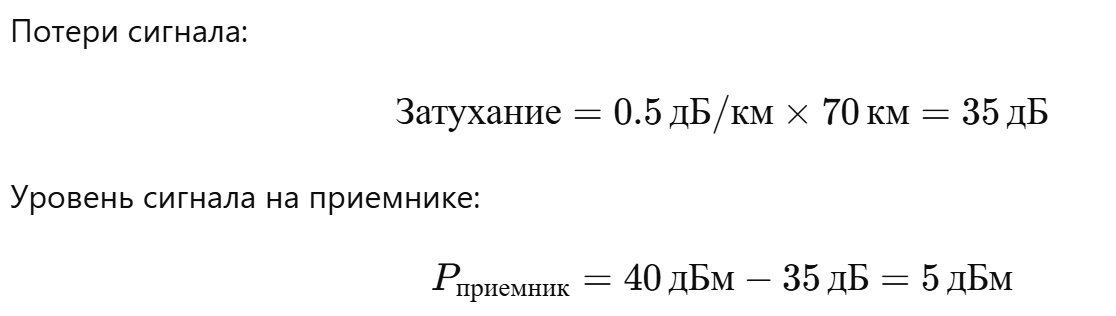
1. **Дайте определение порога чувствительности приемника.**

Порог чувствительности приемника — это минимальный уровень сигнала, который приемник может правильно обработать, чтобы извлечь полезную информацию. Если сигнал ниже этого порога, приемник не сможет надежно распознать передаваемую информацию.

1. **Проверьте, достаточна ли мощность передатчика для устойчивой передачи данных.**

Чтобы проверить, достаточно ли мощности передатчика для устойчивой передачи данных, нужно рассчитать потери сигнала по пути. Формула для расчета затухания:





Поскольку 5 дБм больше порога чувствительности 20 дБм, мощность передатчика недостаточна для устойчивой передачи данных, потому что сигнал на приемнике оказался ниже порога чувствительности.

1. **Что является причиной перекрестных наводок на ближнем конце кабеля?**

Перекрестные наводки (crosstalk) могут быть вызваны **электромагнитными помехами** от соседних проводников в кабеле, когда сигнал на одном проводнике индуцирует нежелательные сигналы на другом проводнике.

1. **Какой кабель более качественно передает сигналы - с большим значением параметра NEXT или с меньшим?**

Кабель с **меньшим значением NEXT (Near-End Crosstalk)** передает сигналы более качественно. Это связано с тем, что меньший NEXT означает меньшее количество электромагнитных помех между проводниками, что улучшает качество сигнала.

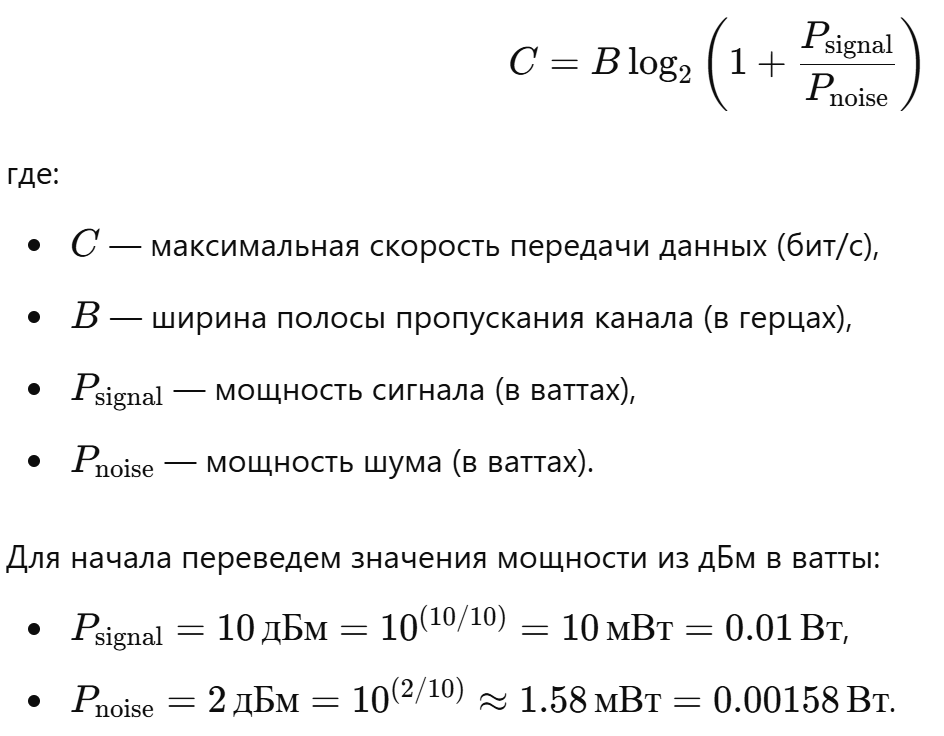
1. **Какой тип кабеля предназначен для передачи данных на большие расстояния?**

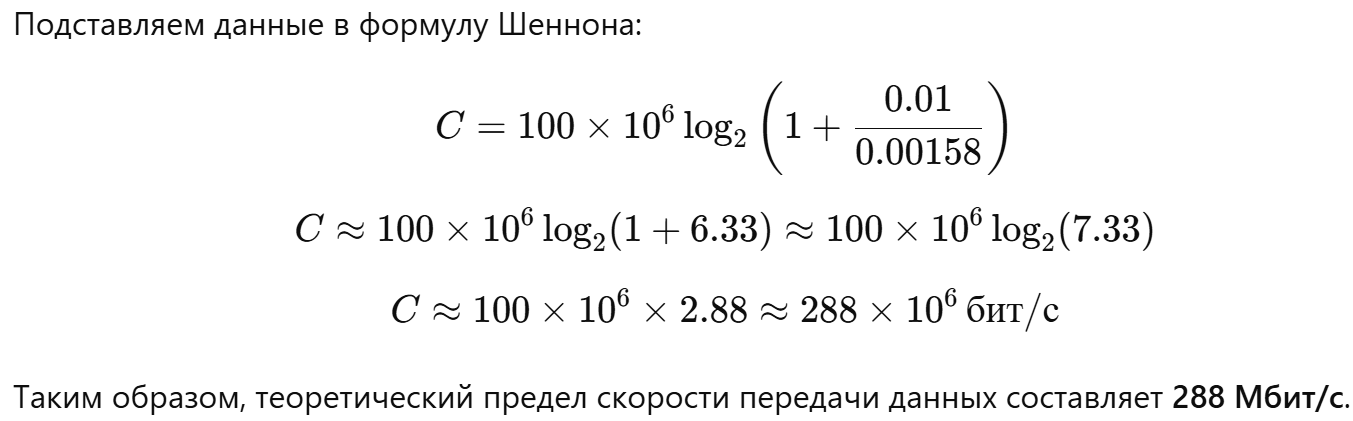
* **б) одномодовый.**

Одномодовый оптоволоконный кабель предназначен для передачи данных на большие расстояния, так как он использует один модовый путь для света, что снижает искажения и затухания на длинных дистанциях по сравнению с многомодовыми кабелями.

1. **Каким будет теоретический предел скорости передачи данных в битах в секунду по линии связи с шириной полосы пропускания 100 мГц, если мощность передатчика составляет 10 дБм, а мощность шума в линии связи равна 2 дБм?**

Для расчета теоретического предела скорости передачи данных можно использовать **формулу Шеннона** для канала с добавлением шума:



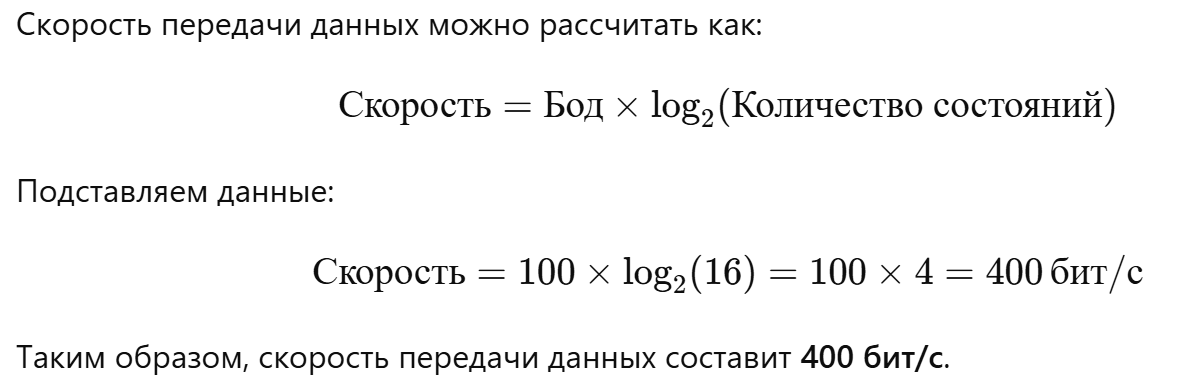


Таким образом, теоретический предел скорости передачи данных составляет **288 Мбит/с**.

1. **Можно ли кодировать дискретную информацию аналоговыми сигналами?**

Да, можно. Дискретную информацию можно кодировать с помощью аналоговых сигналов, используя различные методы, такие как амплитудная модуляция (AM), частотная модуляция (FM) или фазовая модуляция (PM). В этих методах дискретные данные (например, двоичные данные) кодируются путем изменения параметров аналогового сигнала.

1. **Какой будет скорость передачи данных на линии, если частота изменения сигнала равна 100 бод, а сигнал имеет 16 состояний?**



1. **Несут ли информацию импульсы на тактовой шине компьютера?**

Да, импульсы на тактовой шине компьютера несут информацию, особенно в контексте синхронизации и передачи сигналов управления между различными компонентами системы.

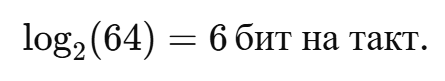
1. **Регенерацией оптического сигнала называется:**

* **b) восстановление формы сигнала за счет преобразования в электрическую форму и обратно.**

Регенерация оптического сигнала включает в себя преобразование оптического сигнала в электрический, его восстановление (фильтрация и усиление) и затем преобразование обратно в оптический сигнал для дальнейшей передачи.

1. **Сколько бит за один такт передается при кодировании 64-QAM?**

В 64-QAM (квадратная амплитудная модуляция) используется 64 различных состояния, что позволяет передавать:



Таким образом, при кодировании 64-QAM передается **6 бит за один такт**.

1. **Поясните, из каких соображений выбрана частота дискретизации 8 кГц в методе квантования РСМ.**

Частота дискретизации 8 кГц была выбрана в методе квантования РСМ (реконструкции с кодированием в реальном времени) для обеспечения адекватного представления звукового сигнала. Она в два раза превышает максимальную частоту, составляющую 4 кГц, что соответствует теореме Найквиста, гарантируя полное восстановление звука без искажений.

1. **Спектр какого сигнала уже при одной и той же тактовой частоте передатчика?**

* **б) амплитудной модуляции.**

Амплитудная модуляция (AM) имеет более широкий спектр при одной и той же тактовой частоте по сравнению с потенциальным кодом, так как для AM используется переменная амплитуда сигнала для кодирования данных.

1. **Чем логическое кодирование отличается от физического?**

Логическое кодирование определяет способ представления данных в цифровой форме, например, как двоичные данные преобразуются в последовательности символов (0 и 1). Физическое кодирование связано с конкретным способом передачи этих данных через физический канал (например, изменение напряжения или частоты для передачи логических единиц и нулей).

1. **Как можно повысить скорость передачи данных по кабельной линии связи:**

* **б) увеличить число символов кода и сохранить ту же тактовую частоту сигнала.**

Увеличение числа символов кода позволяет передавать больше информации за один такт, что увеличивает общую скорость передачи данных, не изменяя тактовую частоту.

1. **Какими способами можно улучшить свойство самосинхронизации кода NRZI:**

* **а) использовать логическое кодирование, исключающее появление длинных последовательностей единиц.**

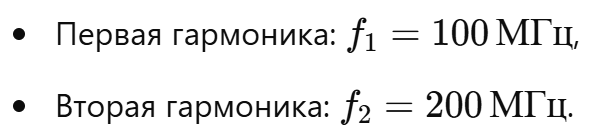
Логическое кодирование, исключающее длинные последовательности единиц, помогает улучшить самосинхронизацию, так как позволяет избегать потери синхронизации в процессе передачи.

1. **Какой режим временного мультиплексирования используется в сетях с коммутацией пакетов?**

В сетях с коммутацией пакетов используется **асинхронное мультиплексирование**. В этом режиме каждый пакет передается независимо, и для каждого пакета может быть использован разный интервал времени.

1. **Найдите первые две гармоники спектра NRZ-сигнала при передаче последовательности 110011001100… если тактовая частота передатчика равна 100 МГц.**

Для NRZ-сигнала с тактовой частотой 100 МГц спектр сигнала будет содержать гармоники, соответствующие частотам:



1. **Во сколько раз увеличится ширина спектра кода NRZ при увеличении тактовой частоты передатчика в 3 раза?**

Ширина спектра кода NRZ пропорциональна тактовой частоте передатчика. Если тактовая частота увеличится в 3 раза, ширина спектра также увеличится в 3 раза.

1. **Какими из следующих характеристик обладают первичные сети:**

* **a) поддерживают технику коммутации каналов,**
* **b) мультиплексируют данные на основании техники асинхронного TDM,**
* **b) предоставляют услуги канала «точка - точка».**

Первичные сети обычно поддерживают коммутацию каналов, используют технику мультиплексирования для эффективного использования канала и предоставляют каналы для связи между конкретными точками.

1. **Цифровой кросс-коннектор первичной сети отличается от мультиплексора ввода-вывода тем, что он:**

* **б) коммутирует данные в цифровом формате.**

Цифровой кросс-коннектор (DCC) используется для маршрутизации и коммутирования цифровых данных между различными потоками и каналами без изменения их содержания, тогда как мультиплексор ввода-вывода (MUX) обычно используется для объединения нескольких низкоскоростных каналов в один более высокоскоростной канал.

1. **Если при планировании первичной сети количество пользователей и интенсивности генерируемых ими потоков данных были оценены неверно, то:**

* **б) это приведет к невозможности обслуживания некоторого количества пользователей.**

Неправильная оценка потребностей в пропускной способности может привести к перегрузке сети и невозможности обслуживания всех пользователей, особенно если сеть недостаточно масштабируется для обработки таких потоков данных.

1. **Кадрирование информации в первичной сети преследует цель:**

* **б) мониторинга качества работы сети.**

Кадрирование позволяет организовать и структурировать данные для правильной передачи и мониторинга. Оно помогает не только передавать данные, но и контролировать их состояние и качество в сети.

1. **Мультикадры в первичных сетях используются для:**

* **б) распределения длинных полей заголовка кадра между несколькими кадрами.**

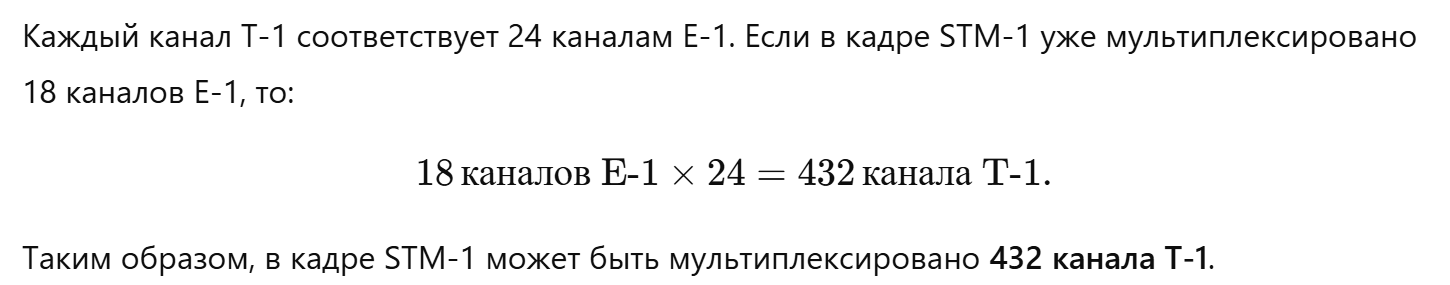
Мультикадры используются для оптимизации передачи информации, особенно когда длина заголовков слишком велика для одного кадра, что помогает уменьшить нагрузку на сеть и повысить ее эффективность.

1. **Укажите, какие варианты организации услуг первичной сети являются реализуемыми:**

* **б) OTN/DWDM.**

Одна из реализуемых технологий для первичных сетей — это использование оптической транспортной сети (OTN) в сочетании с Dense Wavelength Division Multiplexing (DWDM), что позволяет эффективно управлять и мультиплексировать большое количество каналов через оптическое волокно.

1. **Сколько каналов T-1 может мультиплексировать кадр STM-1, если в нем уже мультиплексировано 18 каналов E-1?**



1. **Регенераторная SDH выполняет следующие функции:**

* **б) выполняет ввод-вывод пользовательских данных.**

Регенераторная SDH занимается восстановлением и усилением сигнала для передачи данных между пользователями, а также выполняет преобразование формата данных для их корректной передачи.

1. **Почему кольцо является одной из самых популярных топологий сети SDH?**

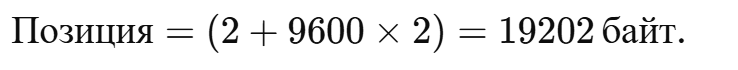
Кольцевая топология в SDH используется, потому что она предоставляет высокую степень отказоустойчивости. В случае выхода одного из каналов из строя, данные могут быть перенаправлены по кольцу, что обеспечивает непрерывность связи.

1. **Согласуются ли иерархии скоростей Ethernet и SDH?**

Нет, иерархии скоростей Ethernet и SDH не полностью согласуются. SDH имеет свою иерархию скорости (например, STM-1, STM-4), в то время как Ethernet имеет свою (например, 1 Gbps, 10 Gbps). Взаимодействие между ними часто требует адаптеров или преобразователей.

1. **Каким будет порядковый номер второго байта третьего кадра STM-1 при мультиплексировании его в кадр STM-4?**

Кадр STM-1 состоит из 9 600 байт. В кадре STM-4 четыре кадра STM-1, и каждый из них будет располагаться последовательно в структуре. Второй байт третьего кадра STM-1 будет находиться на позиции:



Таким образом, это будет **19 202-й байт** в кадре STM-4.

1. **По какой причине в кадре STM-1 используется три указателя?**

Три указателя в кадре STM-1 используются для обеспечения синхронизации и правильного указания местоположения данных в кадре. Эти указатели необходимы для управления и корректной маршрутизации данных, особенно при использовании мультиплексирования и обработки потоков.

1. **С какой целью в технологиях PDH и SDH используется чередование байтов?**

Чередование байтов в PDH и SDH используется для уменьшения эффекта "перекрестных наводок" и улучшения синхронизации, а также для увеличения эффективности передачи данных. Это помогает избежать потерь данных и улучшить качество связи.

1. **В чем отличие схем защиты 1+1 и 1:1?**

В схеме **1+1** защита означает, что имеется два канала: основной и резервный. Резервный канал используется только при отказе основного канала. В схеме **1:1** защита означает, что существует только один резервный канал, который может одновременно обслуживать несколько основных каналов (к примеру, один резервный канал для двух или более основных каналов).

**42. Поясните, чем тонкое выравнивание скоростей SDH отличается от грубого выравни- вания: a) точностью; б) тонкое выравнивание согласует фактические скорости, а грубое - номинальные; b) тонкое выравнивание согласует номинальные скорости, а грубое - фактические.**

**Тонкое выравнивание** и **грубое выравнивание** в контексте SDH (системы синхронной цифровой иерархии) относятся к методам согласования скоростей передачи данных в разных частях сети, и их различия связаны с точностью выравнивания и с тем, какие именно скорости согласуются (фактические или номинальные).

Ответ:

* **b) Тонкое выравнивание согласует фактические скорости, а грубое — номинальные.**

**Пояснение**:

* **Тонкое выравнивание** (fine synchronization) связано с более точной настройкой фактической скорости потока данных. Это позволяет точно синхронизировать передачу данных, чтобы минимизировать ошибки и потерю синхронизации в канале. Такой процесс учитывает небольшие отклонения от идеальных значений, корректируя фактическую скорость потока для обеспечения синхронности.
* **Грубое выравнивание** (coarse synchronization), наоборот, согласует скорости, ориентируясь на номинальные значения, которые указаны в стандартах и спецификациях. Оно позволяет на более общем уровне согласовать скорость потока данных между оборудованием, но не учитывает небольшие, часто несущественные отклонения от этих номинальных значений.

Таким образом, тонкое выравнивание обеспечивает более высокую точность синхронизации, что критично для корректной работы высокоскоростных каналов связи, таких как в SDH, в то время как грубое выравнивание достаточно для простых систем или с меньшими требованиями к точности синхронизации.

**43. Адреса какого типа используются в таблицах коммутации SDH?**

Ответ:

**б) Составные: номер порта и номера виртуальных контейнеров в каждом уровне иерархии.**

**Пояснение:** В системе SDH (синхронная цифровая иерархия) используются составные адреса, которые включают номер порта и идентификаторы виртуальных контейнеров (VC). Это позволяет эффективно маршрутизировать данные в сети, гарантируя, что данные будут перенаправлены к правильным узлам и контейнерам в сети.

**44. Технология DWDM повысила скорости магистралей первичных сетей за счет:**

Ответ:

**b) Параллельной передачи данных по нескольким волнам.**

**Пояснение:** DWDM (Dense Wavelength Division Multiplexing) — это технология мультиплексирования, которая позволяет передавать несколько потоков данных по одной оптоволоконной линии, используя разные длины волн света (оптические каналы). Это увеличивает пропускную способность линии без необходимости в дополнительных физических кабелях.

**45. Для выделения отдельной волны из неокрашенного сигнала можно использовать следующие световые эффекты:**

Ответ:

**a) Дифракцию.**

**Пояснение:** Для выделения отдельных длин волн в системе DWDM можно использовать эффект дифракции. Это позволяет разделить многоканальный сигнал, передаваемый через оптоволокно, на отдельные потоки данных, что делает возможным выделение нужной длины волны для дальнейшей передачи.

**46. Назовите преимущества гибкого частотного плана DWDM.**

**Ответ:**

Преимущества гибкого частотного плана DWDM включают:

* **Гибкость в использовании спектра:** позволяет оптимизировать использование доступного спектра, назначая каналы на более узкие или более широкие частоты в зависимости от пропускной способности.
* **Увеличение плотности каналов:** возможность размещать больше каналов на той же оптоволоконной линии.
* **Снижение затрат:** позволяет использовать более эффективные методы распределения и управления спектром, что может уменьшить затраты на инфраструктуру.
* **Гибкость в масштабировании:** позволяет адаптировать систему для более высоких скоростей передачи, что критически важно для магистральных сетей.

**47. Транспондер преобразует длину волны, используя:**

Ответ:

**b) Преобразование О-Е-О (Оптика-Электричество-Оптика).**

**Пояснение:** Транспондер в сетях DWDM преобразует оптические сигналы в электрические и обратно в оптические сигналы с новой длиной волны. Это позволяет использовать разные длины волн в разных частях сети, что увеличивает пропускную способность сети.

**48. Почему волноводы дифракционной решетки имеют разную длину?**

**Ответ:**

Волноводы дифракционной решетки имеют разную длину, потому что они используются для разделения оптических сигналов по разным длинам волн. Длина волновода и его характеристики зависят от длины волны, на которую настроена решетка. Это важно для эффективного управления различными длинами волн в многоканальных оптических системах.

**49. Может ли мультиплексор ввода-вывода ввести в магистраль волну длины 11, если ее вывел?**

**Ответ:**

Да, мультиплексор ввода-вывода может ввести в магистраль волну той же длины, что была выведена, при условии, что система поддерживает соответствующие механизмы для управления длинами волн и может перенаправить эту волну в нужное место в сети.

**50. Главной особенностью устройств ROADM является:**

Ответ:

**б) Поддержка удаленной программной реконфигурации.**

**Пояснение:** ROADM (Reconfigurable Optical Add-Drop Multiplexer) — это устройства в оптических сетях, которые позволяют программно изменять маршрут оптических волн в сети без необходимости физического вмешательства. Это позволяет динамично управлять потоком данных в сети.

**51. Технология OTN унаследовала от технологии SDH:**

Ответ:

**a) Иерархию скоростей с коэффициентом 4.**

**Пояснение:** OTN (Optical Transport Network) унаследовала от SDH структуру иерархий скоростей, где каналы мультиплексируются с коэффициентом 4, что помогает эффективно передавать данные в оптических сетях.

**52. Приведите аргументы за и против двух подходов к перевозке пассажиров в примере-аналогии.**

**Ответ:**

* **За:**
  + Преимущества для каждого подхода: более высокоскоростной транспорт может быть быстрее и удобнее для пассажиров.
  + Разные подходы могут быть более эффективными для разных типов пассажиров и маршрутов.
* **Против:**
  + Высокоскоростной транспорт может требовать больших затрат на инфраструктуру.
  + Медленный транспорт может быть менее комфортным и более долгим.

**53. Каким образом кадры OTN размером в 15 232 байта переносят кадры STM-16 размером в 38 880 байт?**

**Ответ:**

Кадры OTN используют технологию **побайтового мультиплексирования** для инкапсуляции данных, таких как кадры STM-16. Это означает, что кадры STM-16 могут быть разделены и включены в кадры OTN в виде виртуальных контейнеров, что позволяет передавать их по сети с повышенной гибкостью и пропускной способностью.

**54. Трибутарный слот OTN имеет:**

Ответ:

**b) фиксированный объем.**

**Пояснение:** В OTN (Optical Transport Network) трибутарный слот представляет собой логическую единицу, которая используется для транспортировки данных, таких как каналы с разными уровнями. Этот слот имеет фиксированный объем, что позволяет выделить четко определенный размер для передачи данных в рамках сети OTN.

**55. Макспондер OTN выполняет функции:**

Ответ:

**b) транспондера.**

**Пояснение:** Макспондер OTN (Optical Transport Network) выполняет функции транспондера, который преобразует оптические сигналы с одной длиной волны в сигналы с другой длиной волны, обеспечивая тем самым совместимость между различными частями сети и повышая гибкость и эффективность передачи данных.

**56. Укажите, какие из приведенных ниже утверждений верны при любых условиях: a) в сетях с коммутацией каналов необходимо предварительно устанавливать соеди- нение; б) в сетях с коммутацией каналов не требуется указывать адрес назначения данных; b) сеть с коммутацией пакетов более эффективна, чем сеть с коммутацией каналов; г) сеть с коммутацией каналов предоставляет взаимодействующим абонентам гарант- тированную пропускную способность; д) данные, поступившие в составной канал, доставляются вызываемому абоненту без задержек и потерь; e) составной канал постоянно закрепляется за двумя абонентами; ж) составной канал имеет постоянную и фиксированную пропускную способность на всем своем протяжении.**

Из приведённых утверждений верными при любых условиях являются следующие:

**a) в сетях с коммутацией каналов необходимо предварительно устанавливать соединение.**

**Пояснение:** В сетях с коммутацией каналов перед передачей данных необходимо установить соединение между отправителем и получателем, чтобы выделить ресурсы канала, необходимые для передачи данных.

**г) сеть с коммутацией каналов предоставляет взаимодействующим абонентам гарантированную пропускную способность.**

**Пояснение:** Сети с коммутацией каналов выделяют ресурсы (например, полосу пропускания) на время сеанса связи, что обеспечивает гарантированную пропускную способность для передачи данных.

**е) составной канал постоянно закрепляется за двумя абонентами.**

**Пояснение:** В сетях с коммутацией каналов составной канал используется исключительно двумя абонентами в процессе их взаимодействия и остаётся закреплённым за ними на время сеанса связи.

**ж) составной канал имеет постоянную и фиксированную пропускную способность на всём своём протяжении.**

**Пояснение:** Составной канал (например, в коммутации каналов) имеет фиксированную пропускную способность, которая не изменяется в процессе передачи, так как ресурсы канала заранее зарезервированы для связи между абонентами.

Остальные утверждения **не всегда верны** при любых условиях:

**б) в сетях с коммутацией каналов не требуется указывать адрес назначения данных.**

Не верно. В сетях с коммутацией каналов необходимо указывать адрес назначения, чтобы установить физическое соединение между абонентами.

**с) сеть с коммутацией пакетов более эффективна, чем сеть с коммутацией каналов.**

Не всегда верно. Эффективность зависит от конкретных условий: в случае больших и постоянных потоков данных сеть с коммутацией каналов может быть более эффективной, в то время как для переменных или коротких сообщений предпочтительнее может быть сеть с коммутацией пакетов.

**д) данные, поступившие в составной канал, доставляются вызываемому абоненту без задержек и потерь.**

Не верно. Хотя в сети с коммутацией каналов гарантирована пропускная способность, всё равно могут возникать задержки и потери из-за проблем с физическими линиями или других факторов.

# **Вопросы к части III**

1. **Преимущества и недостатки разделяемой среды:**

**Преимущества:**

* 1. **Экономия ресурсов:** Разделяемая среда позволяет нескольким устройствам использовать один и тот же канал передачи данных, что экономит ресурсы.
  2. **Гибкость:** Легкость подключения и расширения сети, поскольку новые устройства могут быть подключены к общей сети без значительных изменений в инфраструктуре.
  3. **Простота в управлении:** Отсутствие необходимости в выделении отдельных каналов для каждого устройства или группы устройств.

**Недостатки:**

* 1. **Коллизии:** В разделяемой среде могут происходить коллизии, когда два устройства пытаются одновременно передать данные, что приводит к потерям данных и необходимости повторной передачи.
  2. **Снижение производительности:** В условиях высокой нагрузки на сеть производительность может значительно снизиться из-за коллизий и конкурентного доступа к среде.
  3. **Ограниченная пропускная способность:** Пропускная способность канала ограничена, и она делится между всеми устройствами, что может привести к перегрузкам.

1. **Верно ли утверждение: «Маркерный доступ обеспечивает более эффективное использование пропускной способности разделяемой среды?»**

Да, **верно.**

Маркерный доступ (например, в сетях с методом доступа Token Passing, как в протоколах Token Ring и FDDI) позволяет избежать коллизий, так как только одно устройство в сети может передавать данные в любой момент времени, а другие устройства ждут своей очереди. Это повышает эффективность использования канала, уменьшая количество потерь данных, которые часто возникают при коллизиях в других методах доступа, таких как CSMA/CD (Carrier Sense Multiple Access with Collision Detection).

1. **К какому типу относится МАС-адрес 02:25:86:64:ca:e4?**

Это **универсальный (или глобальный) MAC-адрес.**

Он начинается с префикса "02", который указывает на то, что это адрес, присвоенный производителем и уникальный для каждого устройства в мире. Уникальность адреса обеспечивается регистрацией у организации IEEE.

1. **Преамбула в кадре Ethernet нужна для (выберите вариант ответа):**
   1. **a) вхождения приемника в синхронизм.**

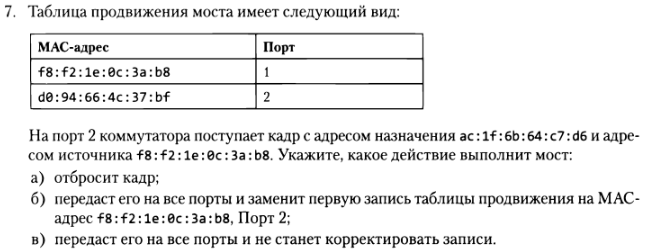
**Пояснение:** Преамбула в Ethernet-кадре используется для синхронизации приемника с передатчиком, чтобы приемник мог правильно интерпретировать данные, особенно в случае высокоскоростных соединений. Она помогает подготовить устройства для правильного восприятия данных в кадре.

1. **При повышении скорости передачи данных максимальный диаметр сети Ethernet на разделяемой среде (выберите вариант ответа):**
   1. **b) уменьшается.**

**Пояснение:** При повышении скорости передачи данных для того, чтобы предотвратить потери данных из-за задержек, максимальный диаметр сети Ethernet на разделяемой среде должен быть уменьшен. Чем выше скорость передачи, тем меньшее расстояние может быть покрыто из-за увеличения времени распространения сигнала.

1. **Для повышения производительности сети Ethernet количество ее сегментов (при сохранении числа станций в сети) нужно (выберите вариант ответа):**
   1. **a) увеличить.**

**Пояснение:** Увеличение количества сегментов в сети Ethernet позволяет уменьшить количество устройств на каждом сегменте и, как следствие, снизить нагрузку и вероятность коллизий, что повышает общую производительность сети.



## **Анализ задачи и ответ**

**Постановка задачи:** Дан коммутатор (мост) с таблицей переадресации MAC-адресов. Необходимо определить, какое действие совершит коммутатор при поступлении кадра с определенным MAC-адресом назначения.

**Таблица переадресации:**

|  |  |
| --- | --- |
| MAC-адрес | Порт |
| f8:f2:1e:0c:3a:b8 | 1 |
| d0:94:66:4c:37:bf | 2 |

**Входящий кадр:**

* MAC-адрес назначения: ac:1f:6b:64:c7:d6
* MAC-адрес источника: f8:f2:1e:0c:3a:b8

**Анализ:**

1. **Проверка таблицы:** В таблице переадресации нет записи для MAC-адреса назначения ac:1f:6b:64:c7:d6.
2. **Определение действия:** Поскольку коммутатор не нашел соответствующей записи в таблице, он не знает, на какой порт следует направить кадр.

**Ответ:**

**а) отбросит кадр.**

**Пояснение:**

* **Принцип работы коммутатора:** Коммутатор работает на основе таблицы MAC-адресов, которая сопоставляет MAC-адрес с портом. Когда на коммутатор приходит кадр, он ищет в таблице MAC-адрес назначения. Если запись найдена, кадр направляется на соответствующий порт. Если запись не найдена, кадр обычно отбрасывается.
* **Цель отбрасывания кадра:** Отбрасывание кадра, для которого нет записи в таблице, предотвращает зацикливание кадров в сети и позволяет избежать перегрузки сети.

**Вывод:** В данном случае коммутатор не может определить, на какой порт следует направить кадр, поэтому он отбрасывает его.

**Дополнительные замечания:**

* **Обучение коммутатора:** Со временем коммутатор обучается, запоминая MAC-адреса устройств, подключенных к его портам. Когда на коммутатор приходит кадр, он добавляет информацию о MAC-адресе источника и порте, через который он пришел, в свою таблицу.
* **Динамическая таблица:** Таблица переадресации коммутатора является динамической. Записи в ней могут добавляться, удаляться или обновляться по мере изменения топологии сети.

Таким образом, коммутатор выполняет свою основную функцию - переадресацию кадров на основе таблицы MAC-адресов.

1. **Поясните, для чего в стандарте Gigabit Ethernet введено поле расширения:**

* **б) для обеспечения диаметра сети 200 м при работе на разделяемой среде.**

**Пояснение:** Поле расширения в стандарте Gigabit Ethernet используется для увеличения диапазона передачи на разделяемой среде. Это особенно важно для обеспечения работы на более длинных расстояниях (например, до 200 метров на витой паре), где требуется больше данных для синхронизации и корректной передачи.

1. **Существует ли вариант стандарта 10G Ethernet на витой паре?**

Да, существует стандарт **10GBASE-T**, который позволяет работать с Ethernet на скорости 10 Гбит/с по витой паре. Этот стандарт поддерживает работу на расстоянии до 100 метров с использованием четырех пар медных проводников.

1. **Поясните, за счет чего повышена скорость в стандарте 100GBase-SR4 по сравнению со стандартом 10GBase-SR:**

* **г) применения четырех параллельных потоков.**

**Пояснение:** Стандарт 100GBase-SR4 использует четыре параллельных оптических потока (4 канала по 25 Гбит/с каждый) для достижения скорости 100 Гбит/с. Это существенно увеличивает пропускную способность по сравнению с 10GBase-SR, который использует один поток.

1. **Поясните, какие механизмы позволили достичь требуемой скорости в стандарте 400G Ethernet:**

* **г) применение кодов FEC.**

**Пояснение:** Стандарт 400G Ethernet использует коды исправления ошибок FEC (Forward Error Correction), которые обеспечивают надежность передачи данных на таких высоких скоростях. Это позволяет компенсировать потери данных из-за ошибок, возникающих при передаче на больших расстояниях и высоких скоростях.

1. **Каким образом можно назначить некоторый коммутатор корневым?**

Чтобы назначить коммутатор корневым, необходимо настроить его **приоритет** в протоколе Spanning Tree Protocol (STP). Коммутатор с наименьшим значением приоритета и наименьшим MAC-адресом будет выбран корневым. Корневой коммутатор - это центральный узел, через который проходят все маршруты в сети STP.

1. **Верно ли утверждение: «порт, имеющий минимальное расстояние до корневого коммутатора среди всех портов данного коммутатора, является назначенным?»**

Нет, **не верно.**

Порт, который имеет минимальное расстояние до корневого коммутатора, является **корневым портом** на данном коммутаторе. **Назначенным портом** является порт, через который осуществляется передача данных к другим коммутаторам или узлам, а его выбор зависит от других факторов, таких как стоимость пути и конфигурация сети.

1. **Протокол RSTP находит покрывающее дерево быстрее протокола STP, так как он (выберите вариант ответа):**

* **г) сокращает период фиксации отказа в сети.**

**Пояснение:** Rapid Spanning Tree Protocol (RSTP) значительно быстрее восстанавливает сеть после отказа, сокращая время обнаружения и восстановления состояния сети. Это достигается за счет более быстрого перехода портов в состояние передачи, а также более эффективной обработки изменений в сети.

1. **Составьте список доступа, запрещающий узлу с МАС-адресом f8:f2:1e:0c:3а:b8 обращаться к узлу с МАС-адресом ас:1f:6b:64:c7:d6, при этом все остальные взаимодействия в сети должны быть разрешены.**

Для этого необходимо использовать список контроля доступа (ACL) на уровне MAC-адресов. Пример ACL:

deny mac-address f8:f2:1e:0c:3a:b8 to mac-address ac:1f:6b:64:c7:d6 permit any

Это запрещает обмен между двумя конкретными узлами, но разрешает все остальные соединения.

1. **Сервер и клиентский компьютер подключены к портам одного и того же коммутатора: сервер — к порту Ethernet 10G, а клиент — Ethernet 1G. На клиенте работает только одно приложение, которое обращается к серверу. Повысится ли скорость обмена клиента с сервером, если клиенту добавить еще один порт Ethernet 1G, соединяющий его с коммутатором, и образовать группу LAG из двух его портов Ethernet 1G?**

Нет, **скорость обмена не повысится.**

Для клиента с двумя портами Ethernet 1G, объединенными в LAG, скорость передачи будет ограничена 2 Гбит/с, если приложение может эффективно использовать оба порта одновременно. Однако в случае с сервером на порту Ethernet 10G, реальная скорость будет ограничена 1 Гбит/с, так как у клиента порты 1G, и он не может использовать всю пропускную способность порта 10G.

1. **Каким образом можно предотвратить включение некоторого порта в группу LAG протоколом LACP?**

Для этого можно **деактивировать LACP** на соответствующем порту или использовать настройки **приоритетов портов**, чтобы указать, что порт не должен быть частью группы. Это можно сделать с помощью команды **"lacp max-bundle"** или конфигурацией режима на порту как "on" или "passive" для нежелательного порта.

1. **Поясните, каким образом можно объединить несколько VLAN (выберите вариант ответа):**

* **б) приписать их к одному транку.**

**Пояснение:** Для объединения нескольких VLAN между двумя коммутаторами используется технология транкинга (обычно с использованием стандарта IEEE 802.1Q). Все VLAN передаются по одному физическому каналу с метками, чтобы различать их.

1. **Какое действие выполняет порт доступа, передавая помеченный кадр клиентскому узлу (кадр получен от порта-транка по внутренней шине коммутатора)?**

Порт доступа удаляет метку VLAN из кадра и передает его клиенту без метки, так как порт доступа обычно предназначен для работы с кадрами одного VLAN.

1. **Для превращения Ethernet в технологию операторского класса были произведены изменения в нескольких областях, среди них (выберите вариант ответа):**

* **b) добавлены функции ОАМ.**

**Пояснение:** Для того чтобы Ethernet мог быть использован в сетях операторского уровня, были добавлены функции OAM (Operations, Administration, and Maintenance), которые обеспечивают мониторинг, диагностику и управление сетями. Эти функции необходимы для обеспечения надежности и высококачественного обслуживания в операторских сетях.

1. **Каждая точка МЕР выполняет следующие функции (выберите вариант ответа):**

* **c) принимает сообщения ССМ.**

**Пояснение:** МЕР (Maintenance Entity Relay) в контексте Ethernet OAM (Operations, Administration, and Maintenance) выполняет функции передачи и обработки сообщений, таких как сообщения ССМ (Continuity Check Messages), которые используются для проверки непрерывности соединения между узлами сети.

1. **Корректно ли при конфигурировании протокола CFM назначить домену оператора уровень 6, а домену пользователя - уровень 3?**

Нет, **это некорректно.**

**Пояснение:** В протоколе CFM (Connectivity Fault Management) уровни для доменов оператора и пользователя обычно должны быть назначены так, чтобы уровень домена оператора был выше уровня домена пользователя. Это необходимо для правильной иерархии в сети, где домен оператора имеет более высокий приоритет и контроль. Уровень 6 — это уровень, который обычно используется для оператора, а уровень 3 — для пользователя, поэтому такая настройка может вызвать проблемы.

1. **Пограничные коммутаторы провайдера, работающие по стандарту РВВ, должны изучать часть МАС-адреса узлов клиента (выберите вариант ответа):**

* **b) при оказании услуги E-LAN.**

**Пояснение:** В случае использования услуги Ethernet-Private LAN (E-LAN), пограничные коммутаторы провайдера могут изучать часть МАС-адреса, чтобы правильно маршрутизировать и обрабатывать трафик между различными узлами клиента. Это необходимо для создания виртуальных LAN-сетей и обеспечения взаимодействия между клиентами.

# **Вопросы к части IV**

### **1. Какие из приведенных адресов могут быть использованы в качестве IP-адресов сетевого интерфейса для узлов Интернета? Для синтаксически правильных адресов определите их класс: A, B, C, D или E.**

* **a) 123.1.223.5**
* **Синтаксически правильный.** Это адрес из **класса C**. Адреса класса C имеют первый октет в диапазоне 192–223.
* **б) 225.0.0.1**

**Синтаксически правильный.** Это адрес из **класса D** (адреса для мультикастинга). Класс D имеет первый октет в диапазоне 224–239.

* **в) 194.87.45.255**

**Синтаксически правильный.** Это адрес из **класса C**. Адреса класса C имеют первый октет в диапазоне 192–223.

* **г) 10.124.251.252**

**Синтаксически правильный.** Это **частный IP-адрес** из **класса A**. Адреса класса A имеют первый октет в диапазоне 1–126, и 10.x.x.x — это частная сеть.

* **д) 125.24.255.255**

**Синтаксически правильный.** Это адрес из **класса A**. Адреса класса A имеют первый октет в диапазоне 1–126.

* **е) 17.213.355.205**

**Синтаксически неверный.** Адрес 355 в третьем октете выходит за пределы допустимых значений (максимальное значение для октета — 255).

* **ж) 179.12.255.255**

**Синтаксически правильный.** Это адрес из **класса B**. Адреса класса B имеют первый октет в диапазоне 128–191.

* **з) 127.0.23.55**

**Синтаксически правильный.** Это адрес из **класса A**, но это **loopback-адрес** (для тестирования на локальном устройстве).

* **и) 1.0.0.13**

**Синтаксически правильный.** Это адрес из **класса A**. Адреса класса A имеют первый октет в диапазоне 1–126.

* **к) 124.1.1.1**

**Синтаксически правильный.** Это адрес из **класса A**. Адреса класса A имеют первый октет в диапазоне 1–126.

* **л) 192.134.216.255**

**Синтаксически правильный.** Это адрес из **класса C**. Адреса класса C имеют первый октет в диапазоне 192–223.

* **м) 293.236.254.11**

**Синтаксически неверный.** Адрес 293 в первом октете выходит за пределы допустимых значений (максимум 255).

* **н) 13.13.13.13**

**Синтаксически правильный.** Это адрес из **класса A**. Адреса класса A имеют первый октет в диапазоне 1–126.

### **2. Пусть IP-адрес некоторого узла подсети равен 108.5.18.167, а значение маски для этой подсети — 255.255.255.240. Определите номер подсети. Какое максимальное число сетевых интерфейсов может быть в этой подсети?**

* Маска **255.255.255.240** соответствует **/28**. Это означает, что у нас есть 28 бит, выделенных под сеть, и 4 бита под узлы.
* Адрес **108.5.18.167** в двоичной форме: 01101100.00000101.00010010.10100111.
* Маска сети **255.255.255.240** в двоичной форме: 11111111.11111111.11111111.11110000.

Чтобы найти номер подсети, нужно выполнить побитовую операцию AND между адресом и маской:

Адрес: 01101100.00000101.00010010.10100111  
Маска: 11111111.11111111.11111111.11110000  
Результат: 01101100.00000101.00010010.10100000

Результат — **108.5.18.160**. Это номер подсети.

Для подсети с маской **/28** (или 255.255.255.240) мы имеем 16 адресов (2^4), но два адреса не могут быть использованы: один для адреса сети, а другой для широковещательного адреса. Таким образом, максимальное количество интерфейсов, которые можно подключить, — **14**.

### **3. Какое максимальное количество подсетей теоретически можно организовать, если в вашем распоряжении имеется сеть класса C? Какое значение должна при этом иметь маска? При ответе не принимайте во внимание двухточечные соединения.**

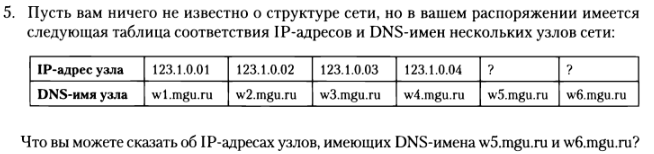
Сеть класса C имеет **24 бита** для адреса сети (например, маска 255.255.255.0 или /24), что оставляет **8 бит** для адреса узла.

* Чтобы разделить сеть на подсети, нужно занять часть этих 8 бит для сети. Теоретически, можно использовать все 8 бит для подсетей.
* Максимальное количество подсетей, которые можно создать, будет равно **2^8 = 256**.
* При этом маска подсети будет **/32**, что дает по одному адресу на каждую подсеть, но это теоретическое максимальное значение. Реально, не все подсети будут использованы для узлов, так как учитываются адреса сети и широковещательные.

### **4. Пусть вам ничего не известно об узлах, кроме их DNS-имен: w1.piter.ru,** [**www.msk.ru**](http://www.msk.ru/)**,** [**www.piter.ru**](http://www.piter.ru/)**, echo.msk.ru. Что вы можете сказать о том, насколько близко территориально находятся они относительно друг друга?**

**Ответ: г) ничего определенного.**

Пояснение: DNS-имена не дают точной информации о географическом расположении узлов. Домены могут быть распределены по разным регионам или использовать различные дата-центры, так что без дополнительной информации (например, о конкретных IP-адресах и их геолокации) нельзя точно определить, насколько близки узлы территориально.



## **Анализ таблицы соответствия IP-адресов и DNS-имен**

**Постановка задачи:** Нам дана таблица, сопоставляющая IP-адреса с DNS-именами нескольких узлов сети. Требуется сделать вывод о возможных IP-адресах узлов с DNS-именами w5.mgu.ru и w6.mgu.ru, основываясь на имеющейся информации.

**Анализ имеющихся данных:**

* **IP-адреса:** Все представленные IP-адреса принадлежат к одной и той же подсети 123.1.0.0/24. Это означает, что первые три октета (123.1.0) у всех узлов в этой сети будут одинаковыми. Различаться будет только последний октет.
* **DNS-имена:** Все DNS-имена имеют общий суффикс ".mgu.ru", что указывает на принадлежность к одной и той же доменной зоне.
* **Последовательность IP-адресов:** Первые четыре записи в таблице демонстрируют последовательное увеличение последнего октета IP-адреса.

**Выводы и предположения:**

1. **Логическое продолжение последовательности:** Исходя из логики последовательного увеличения последнего октета IP-адреса в первых четырех записях, можно предположить, что IP-адреса для w5.mgu.ru и w6.mgu.ru будут следующими в этой последовательности: 123.1.0.05 и 123.1.0.06 соответственно.
2. **Отсутствие строгой зависимости:** Однако важно отметить, что это лишь предположение. В реальных сетях адреса могут присваиваться по различным схемам, и не всегда соблюдается строгая последовательность. Например, адреса могут распределяться случайным образом или по функциональному признаку.
3. **Необходимость дополнительной информации:** Для более точного определения IP-адресов узлов w5.mgu.ru и w6.mgu.ru требуется дополнительная информация о схеме адресации в данной сети. Это может быть:
   1. **Документация сети:** В документации сети может быть описана схема присвоения IP-адресов.
   2. **Конфигурация DHCP-сервера:** Если в сети используется DHCP-сервер, то в его конфигурации можно найти информацию о диапазонах IP-адресов и правилах их распределения.
   3. **Результаты сканирования сети:** С помощью специальных инструментов можно провести сканирование сети и определить активные устройства и их IP-адреса.

**Ответ:**

На основании имеющейся информации можно предположить, что IP-адреса узлов с DNS-именами w5.mgu.ru и w6.mgu.ru будут соответственно 123.1.0.05 и 123.1.0.06. Однако это предположение может быть неверным, если в сети используется другая схема адресации. Для получения точного ответа необходимо обратиться к дополнительным источникам информации.

**Важно понимать, что:**

* **IP-адресация** - это сложная тема, и существует множество различных схем адресации.
* **Предположения, основанные на ограниченных данных, могут быть неточными.**
* **Для получения точной информации необходимо обратиться к документации сети или использовать специальные инструменты для анализа сети.**

### **6. Какая запись из следующих эквивалентна значению маски /29?**

Маска /29 означает, что первые 29 бит в маске — это единицы, а оставшиеся 3 бита — нули. Это эквивалентно маске **255.255.255.248**.

Ответ: **б) 255.255.255.248**

### **7. Могут ли для двухточечной связи быть назначены адреса 197.220.12.9/31 и 197.220.12.10/31?**

Да, это возможно. В IPv4 для **точечных соединений** (например, соединений между двумя маршрутизаторами) могут использоваться сети с маской /31. Маска /31 позволяет иметь только два возможных адреса — один для каждого из узлов, что идеально подходит для двухточечных соединений. В этом случае адреса **197.220.12.9/31** и **197.220.12.10/31** могут быть использованы.

Ответ: **Да**

### **8. Содержимое ARP-таблицы изменяется в результате следующих событий:**

* **a) при получении ARP-ответов на запрос:** Да, при получении ARP-ответа (в котором содержится MAC-адрес узла, соответствующий IP-адресу), ARP-таблица обновляется.
* **б) при получении широковещательных ARP-запросов:** Нет, сам ARP-запрос не изменяет ARP-таблицу. Таблица обновляется только при получении ARP-ответа.
* **в) по истечении времени жизни записи в ARP-таблице:** Да, записи в ARP-таблице имеют ограниченный срок жизни и удаляются по истечении этого времени.

Ответ: **a) при получении ARP-ответов на запрос; и b) по истечении времени жизни записи в ARP-таблице.**

### **9. Протокол ARP функционально можно разделить на клиентскую и серверную части. Опишите, какие функции вы отнесли бы к клиентской части, а какие — к серверной?**

* **Клиентская часть ARP:** Эта часть инициирует ARP-запрос для того, чтобы узнать MAC-адрес устройства, соответствующий его IP-адресу. Например, когда устройство хочет передать пакет, но не знает MAC-адрес назначения.
* **Серверная часть ARP:** Эта часть отвечает на ARP-запросы, предоставляя свой MAC-адрес для заданного IP-адреса. Если устройство получает ARP-запрос с запросом на MAC-адрес для своего IP-адреса, оно отправляет ARP-ответ.

### **10. В чем состоят функции нижнего уровня стека TCP/IP?**

Нижний уровень стека TCP/IP включает в себя несколько функций:

* **a) кодирование и мультиплексирование электрических сигналов:** Эта функция относится к физическому уровню (например, передачи данных по проводам).
* **б) инкапсуляция и декапсуляция данных сетевого уровня в кадры нижележащей технологии:** Это относится к канальному уровню, где пакеты данных инкапсулируются в кадры перед передачей по физическому каналу.
* **в) формирование кадров и синхронизация:** Эта функция также относится к канальному уровню, где осуществляется преобразование данных в кадры.
* **г) доступ к среде передачи:** Это тоже относится к канальному уровню, который управляет доступом к физической среде передачи.
* **д) преобразование сетевых адресов в адреса нижележащей технологии:** Это также относится к канальному уровню, где сетевые адреса (IP-адреса) преобразуются в MAC-адреса для передачи по локальной сети.

Ответ: **б) инкапсуляция и декапсуляция данных сетевого уровня в кадры нижележащей технологии;** и **г) доступ к среде передачи;**

### **11. Поясните, что понимается под термином «линия связи» (Link) в технологии TCP/IP.**

**Ответ:**

* **a) любая коммуникационная среда, которая позволяет IP-узлам взаимодействовать друг с другом без промежуточных маршрутизаторов.** Это наилучшее определение, так как термин "линия связи" в контексте TCP/IP обычно относится к любой физической или логической связи, которая соединяет два узла, позволяя им обмениваться данными без необходимости проходить через промежуточные маршрутизаторы. Например, это может быть Ethernet-соединение или прямое соединение между двумя устройствами.

### **12. Передается ли в IP-пакете маска в тех случаях, когда маршрутизация реализуется с использованием масок?**

Нет, маска не передается в IP-пакете. Маска сети используется для определения сети, к которой принадлежит адрес назначения, но она не передается вместе с самими данными. Вместо этого маршрутизаторы используют таблицы маршрутизации и маски для вычисления правильных маршрутов.

Ответ: **Нет.**

### **13. Какие элементы сети могут выполнять фрагментацию?**

Фрагментация пакетов может выполняться на уровнях **IP** и **сетевого оборудования**.

* **a) только компьютеры;** — нет, фрагментация обычно выполняется маршрутизаторами.
* **б) только маршрутизаторы;** — да, маршрутизаторы выполняют фрагментацию, если размер пакета превышает максимальный размер передачи (MTU) на следующем сегменте сети.
* **в) компьютеры, маршрутизаторы, мосты, коммутаторы;** — нет, мосты и коммутаторы не фрагментируют пакеты. Только маршрутизаторы могут это делать.
* **г) компьютеры и маршрутизаторы;** — да, компьютеры могут фрагментировать пакеты, если они непосредственно передают их в сети, и маршрутизаторы могут это делать при необходимости.

Ответ: **г) компьютеры и маршрутизаторы.**

### **14. Что произойдет, если при передаче пакета он был фрагментирован, причем один из фрагментов не дошел до узла назначения по истечении тайм-аута?**

* **a)** IP-модуль узла-получателя отбросит все полученные фрагменты пакета, в котором потерялся один фрагмент, а IP-модуль узла-отправителя не будет предпринимать никаких действий по повторной передаче данного пакета.
* **b)** IP-модуль получателя сообщит о неполучении одного фрагмента, а IP-модуль узла-отправителя повторит передачу всего пакета, в состав которого входил недошедший фрагмент.

**Ответ: b)** Если один из фрагментов теряется, IP-модуль получателя не может собрать исходный пакет, так как фрагменты пакета должны быть получены полностью. Получатель будет ожидать все фрагменты в течение определенного времени, и если один из фрагментов не будет получен (по истечении тайм-аута), то он отправит запрос на повторную передачу всего пакета.

### **15. Кому адресовано ICMP-сообщение?**

**Ответ: a)** ICMP-сообщение адресовано протоколу IP узла-отправителя пакета, вызвавшего ошибку. ICMP используется для диагностики и передачи ошибок между узлами, а также для отправки сообщений об ошибках маршрутизации и доставки.

### **16. Сколько ARP-таблиц имеет компьютер? маршрутизатор? коммутатор?**

* **Компьютер:** Обычно у компьютера одна ARP-таблица, которая содержит соответствие между IP-адресами и MAC-адресами на его сетевых интерфейсах.
* **Маршализатор:** Маршрутизатор имеет одну ARP-таблицу на каждый интерфейс. Это означает, что для каждого интерфейса маршрутизатор будет хранить свою ARP-таблицу, соответствующую каждому сетевому сегменту.
* **Коммутатор:** Коммутатор не имеет ARP-таблицы в традиционном смысле, как маршрутизатор. Он имеет таблицу MAC-адресов, которая используется для определения, на какой порт передать кадр в зависимости от MAC-адреса назначения.

### **17. В студенческом общежитии живет 350 студентов, и каждый из них имеет собственный ноутбук. В общежитии оборудована специальная комната, в которой развернута компьютерная сеть, имеющая 20 коннекторов для подключения компьютеров. Время от времени студенты работают в этом компьютерном классе, подключая свои ноутбуки к сети. Каким количеством IP-адресов должен располагать администратор этой компьютерной сети, чтобы все студенты могли подключаться к сети, не выполняя процедуру конфигурирования своих ноутбуков при каждом посещении компьютерного класса?**

Администратор должен предоставить как минимум 350 IP-адресов для студентов, так как каждый студент имеет свой ноутбук и может подключаться к сети в любое время. Однако для компьютерного класса, где имеется 20 коннекторов, необходимо будет обеспечить 20 IP-адресов, чтобы ноутбуки студентов могли быть подключены и работать.

Таким образом, администратор должен располагать как минимум **350 IP-адресами** для студентов и **20 дополнительными IP-адресами** для обеспечения коннекторов в классе.

**Ответ:** **350 IP-адресов для студентов** и **20 IP-адресов для коннекторов**.

### **18. Какие из следующих утверждений верны?**

* **a) broadcast является частным случаем multicast:** Это неверно, так как broadcast — это рассылка данных всем узлам в сети, а multicast — рассылка данным группе узлов. Это разные методы рассылки.
* **б) broadcast является частным случаем anycast:** Это неверно, так как broadcast — это рассылка всем узлам, а anycast — это рассылка данным ближайшему узлу из группы, что отличается от broadcast.
* **в) multicast является частным случаем anycast:** Это неверно, потому что multicast — это рассылка нескольким узлам, в то время как anycast предназначен для отправки данных только одному из узлов, который находится ближе.
* **г) ни один из этих способов рассылки не является частным случаем другого:** Это верно, поскольку broadcast, multicast и anycast — это разные методы рассылки, каждый из которых имеет свои особенности.

**Ответ:** **г) ни один из этих способов рассылки не является частным случаем другого.**

### **19. Почему провайдеры при выделении адресов своим клиентам стремятся к тому, чтобы адресные пространства сетей, располагающихся территориально по соседству, имели совпающие префиксы?**

Ответ заключается в оптимизации маршрутизации. Когда адресные пространства соседних сетей имеют одинаковые префиксы, маршрутизаторы могут использовать агрегацию маршрутов, что уменьшает количество записей в таблицах маршрутизации и ускоряет процесс маршрутизации. Это также помогает в упрощении сетевой инфраструктуры и улучшении производительности.

**Ответ:** Провайдеры стремятся к совпадению префиксов, чтобы уменьшить количество записей в таблицах маршрутизации и повысить эффективность маршрутизации.

### **20. Какие из следующих утверждений правильны?**

* **a) клиентом DNS-сервера является резольвер:** Верно. Резольвер — это клиент DNS-сервера, который отправляет запросы на разрешение имен.
* **б) DNS-клиентом является практически каждый узел Интернета:** Верно. Каждый узел Интернета, который использует доменные имена, является DNS-клиентом, отправляющим запросы к DNS-серверам.
* **в) запись типа АААА файла зоны отображает DNS-имя в IPv4-адрес:** Это неверно. Запись типа AAAA используется для отображения доменного имени в **IPv6-адрес**, а не в IPv4.
* **г) для каждой зоны существует один первичный и несколько вторичных серверов DNS:** Верно. Каждая зона DNS обычно имеет один первичный сервер и несколько вторичных, которые получают копию данных с первичного сервера.

**Ответ:** **a) клиентом DNS-сервера является резольвер;** и **б) DNS-клиентом является практически каждый узел Интернета;** и **г) для каждой зоны существует один первичный и несколько вторичных серверов DNS.**

### **21. Сравните таблицу моста или коммутатора с таблицей маршрутизатора. Каким образом формируются эти таблицы? Какую информацию содержат? От чего зависит их объем?**

* **Таблица моста или коммутатора:** Эта таблица содержит информацию о **MAC-адресах** устройств, которые подключены к каждому порту. Коммутатор использует таблицу для того, чтобы узнать, на какой порт нужно отправить данные. Таблица формируется динамически, когда коммутатор наблюдает за кадрами, проходящими через его порты, и ассоциирует MAC-адреса с портами.
* **Таблица маршрутизатора:** Таблица маршрутизатора содержит **IP-адреса** и информацию о том, через какой интерфейс или маршрутизатор отправлять пакеты для каждой подсети. Таблица маршрутизации может быть как статической, так и динамической, в зависимости от протокола маршрутизации (например, RIP, OSPF). Маршрутизаторы используют эту таблицу для принятия решений о том, куда направить пакеты.

**От чего зависит объем таблиц:**

* Объем таблицы моста зависит от количества **MAC-адресов** в сети.
* Объем таблицы маршрутизатора зависит от количества **подсетей** и **маршрутов**, которые маршрутизатор должен поддерживать.

**Ответ:** Таблицы моста или коммутатора содержат MAC-адреса и информацию о портах, в то время как таблицы маршрутизатора содержат информацию о маршрутах и IP-адресах. Объем этих таблиц зависит от количества устройств в сети и маршрутов в маршрутизаторе.

### **22. Рассмотрим маршрутизатор на магистрали Интернета. Какие записи содержатся в поле адреса назначения его таблицы маршрутизации?**

* **a) номера всех сетей Интернета:** Это неверно, потому что маршрутизатор обычно не хранит записи для каждой сети в Интернете.
* **б) номера некоторых сетей Интернета:** Верно. Маршрутизатор хранит записи для сетей, с которыми он может маршрутизировать трафик.
* **в) номера некоторых сетей и адреса некоторых конечных узлов Интернета:** Это неверно, поскольку таблицы маршрутизации обычно содержат только информацию о сетях, а не об отдельных конечных узлах.
* **г) номера сетей, подсоединенных к интерфейсам данного маршрутизатора:** Это неверно, поскольку таблица маршрутизации включает не только локальные сети, но и маршруты к удаленным сетям.

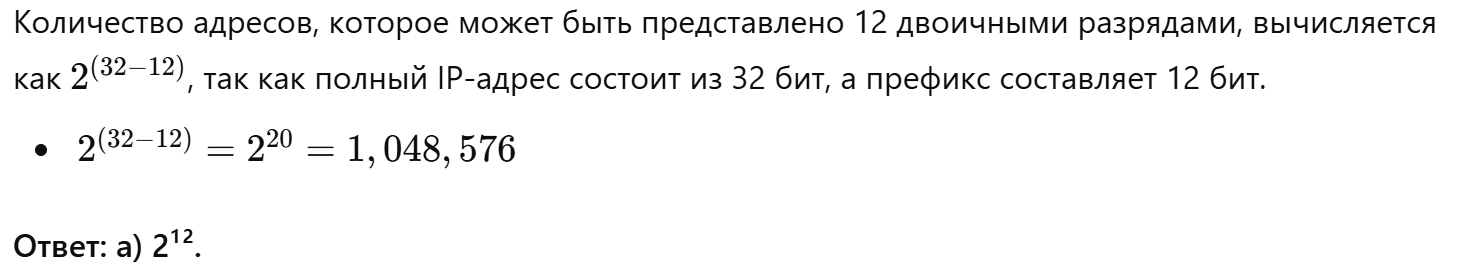
**Ответ:** **б) номера некоторых сетей Интернета.**

### **23. Сколько записей о маршрутах по умолчанию может включать таблица маршрутизации?**

Таблица маршрутизации может содержать **одну запись о маршруте по умолчанию**, которая используется, если маршрутизатор не находит более специфичного маршрута для адреса назначения.

**Ответ:** **1 запись.**

### **24. Пусть префикс непрерывного пула IP-адресов составляет 12 двоичных разрядов. Сколько адресов входит в этот пул?**



### **25. Передается ли в IP-пакете маска в тех случаях, когда маршрутизация реализуется с использованием масок?**

IP-пакет сам по себе не передает маску маршрутизации. Маски маршрутизации обычно используются для определения сетевых адресов в таблицах маршрутизации, но не включаются непосредственно в данные IP-пакетов.

**Ответ:** **Нет, маска не передается в IP-пакете.**

### **26. Приведите примеры, когда может возникнуть необходимость в использовании специфических маршрутов.**

Специфические маршруты могут быть использованы в следующих случаях:

* **Маршрут к локальной сети:** Например, в случае маршрутизатора, который должен обрабатывать трафик для сети, подключенной непосредственно к его интерфейсу.
* **Маршрут к определенному узлу:** В случае, если требуется отправить трафик в конкретную точку (например, сервер с уникальным IP-адресом).
* **Маршрут для подключения к VPN:** Когда трафик должен быть направлен через туннель или через специфический сервер.
* **Маршруты с использованием политики:** Например, когда маршрутизатор принимает решения на основе типа трафика (например, для определенных приложений).

### **27. Какие преимущества дает технология CIDR? Что мешает ее широкому внедрению?**

**Преимущества CIDR:**

* **Эффективное использование адресного пространства:** CIDR позволяет использовать адреса с переменной длиной префикса, что уменьшает количество пустых IP-адресов.
* **Агрегация маршрутов:** CIDR помогает агрегировать маршруты, что уменьшает количество записей в таблицах маршрутизации.
* **Более гибкая маршрутизация:** CIDR позволяет более гибко управлять размером сети и упрощает администрирование.

**Что мешает широкому внедрению:**

* **Совместимость с устаревшими системами:** Системы и устройства, которые не поддерживают CIDR, могут требовать дополнительной настройки.
* **Меньше административного контроля:** Некоторые администраторы могут предпочитать старые способы маршрутизации с фиксированными масками.

### **28. Почему в записи о маршруте по умолчанию в качестве адреса сети назначения часто указывается 0.0.0.0 с маской 0.0.0.0?**

Запись маршрута с адресом 0.0.0.0 и маской 0.0.0.0 используется как **маршрут по умолчанию**, который применяется, когда маршрутизатор не может найти более специфичный маршрут для адреса назначения. Это своего рода "catch-all" маршрут, который направляет трафик в случае, если для адреса назначения нет более детализированной записи.

**Ответ:** Это маршрут по умолчанию для трафика, для которого нет других маршрутов.

### **29. В каких случаях система DNS использует протокол UDP, а в каких — TCP?**

* **UDP:** DNS обычно использует UDP для запросов, так как это более быстрый протокол, который подходит для малых пакетов, которые часто бывают при запросах DNS.
* **TCP:** DNS использует TCP, когда размер ответа слишком велик для передачи через UDP (например, когда ответ содержит множество записей, и его размер превышает 512 байт). Также TCP используется для установления устойчивого соединения при передаче зоновых данных.

**Ответ:** DNS использует UDP для обычных запросов, а TCP — для передачи больших данных (например, зоновых файлов).

### **30. Если при обмене данными по методу с возвращением на N пакетов отправитель получил квитанцию на (п + 1)-й пакет, а квитанция на предыдущий п-й пакет не пришла, то (выберите вариант ответа):**

* **a) отправитель считает п-й пакет успешно принятым и продолжает передачу:** Это неверно. Отправитель должен дождаться квитанции на п-й пакет, прежде чем продолжить передачу.
* **б) по истечении тайм-аута отправитель повторно отсылает п-й пакет:** Верно. Если квитанция на п-й пакет не пришла в течение тайм-аута, отправитель повторно отправит п-й пакет.
* **в) по истечении тайм-аута получатель повторно отсылает квитанцию на п-й пакет:** Это неверно. Получатель обычно не повторяет квитанции, это обязанность отправителя.

**Ответ:** **б) по истечении тайм-аута отправитель повторно отсылает п-й пакет.**

### **31. Как соотносятся размеры окна приема и окна передачи в методе с выборочным повторением?**

В методе **выборочного повторения**:

* Окно передачи обычно **больше**, чем окно приема, так как отправитель может передавать несколько пакетов одновременно, но получатель может подтвердить пакеты только по одному.

**Ответ:** **a) окно передачи больше, чем окно приема.**

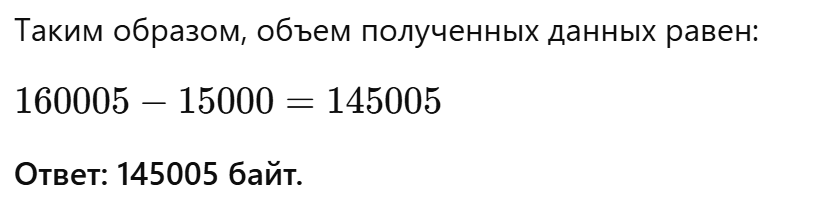
### **32. Может ли приложение, используя протокол UDP, обеспечить надежную связь?**

Протокол UDP сам по себе не предоставляет надежности. Однако приложение может использовать дополнительные механизмы (например, контроль целостности, тайм-ауты, повторные попытки), чтобы обеспечить надежность связи.

**Ответ:** **Да, приложение может реализовать надежную связь поверх UDP, но сам UDP не предоставляет этой надежности.**

### **33. Какой объем данных получен в течение ТСР-сеанса отправителем ТСР-сегмента, в заголовке которого в поле квитанции помещено значение 160005, если известно, что первый полученный байт имел номер 15000?**

Номер байта в квитанции указывает на следующий ожидаемый байт. В данном случае, квитанция указывает, что следующий байт будет 160005, что означает, что отправитель успешно получил байты с 15000 по 160004.



### **34. Укажите, в каком виде передаются квитанции на получение сегментов в протоколе ТСР:**

* **a) квитанция передается в поле данных ТСР-сегмента с установленным в заголовке флагом АСК:** Это неверно. Квитанция не передается в поле данных сегмента, а в поле заголовка.
* **б) квитанция - это флаг АСК:** Это тоже неверно. Флаг ACK (Acknowledge) используется для указания, что сегмент является подтверждением, но квитанция — это не просто флаг.
* **b) квитанция - это значение поля последовательного номера в заголовке ТСР-сегмента с установленным флагом АСК:** Это неверно. Значение поля последовательного номера не является квитанцией. Этот номер указывает на следующий ожидаемый байт, но не является квитанцией сам по себе.
* **г) квитанция - это значение поля подтвержденного номера в заголовке ТСР-сегмента с установленным флагом АСК:** Это верно. Квитанция в протоколе ТСР — это значение поля "подтвержденный номер" в заголовке сегмента, который указывает номер последнего успешно полученного байта. Также при этом устанавливается флаг ACK.

**Ответ:** **г) квитанция - это значение поля подтвержденного номера в заголовке ТСР-сегмента с установленным флагом АСК.**

### **35. Проведите с партнером сеанс моделирования работы протокола ТСР.**

Это задание направлено на практическое освоение работы протокола TCP. Оно предполагает моделирование с помощью карточек с ключевыми полями (номер первого байта, размер сегмента, номер квитанции и т. д.) для симуляции передачи данных и обработки квитанций.

**Рекомендация:** Во время моделирования:

* Обратите внимание на потери пакетов (карточек), что моделирует потерю сегментов в реальной сети.
* Имплементируйте тайм-ауты для повторной передачи утраченных сегментов.
* Отслеживайте изменения окна передачи и порядок последовательных номеров.

Это упражнение поможет понять, как работает управление потоками и надежная передача данных в протоколе TCP.

### **36. Как влияет на эффективность передачи протокола ТСР размер окна? Величина тайм-аута?**

* **Размер окна** влияет на количество данных, которые могут быть отправлены до получения подтверждения от получателя. Чем больше размер окна, тем больше данных можно отправить без ожидания подтверждения, что увеличивает эффективность передачи. Однако слишком большое окно может привести к перегрузке сети или буферов, если каналы связи не справляются с высокой нагрузкой.
* **Величина тайм-аута** влияет на скорость повторной передачи сегментов, если они были потеряны. Если тайм-аут слишком мал, это может привести к избыточной повторной передаче, что замедлит обмен. Если тайм-аут слишком велик, это может замедлить восстановление после потери данных.

**Влияние:**

* **Большое окно** — улучшает пропускную способность, но требует более точного контроля за состоянием сети.
* **Короткий тайм-аут** — ускоряет обнаружение потерь, но может привести к излишним повторным передачам.
* **Длинный тайм-аут** — увеличивает время восстановления после потерь, но снижает количество повторных передач.

### **37. Может ли работать маршрутизатор, не имея таблицы маршрутизации?**

* **a) может, если выполняется маршрутизация от источника:** Это неверно, поскольку маршрутизатор без таблицы маршрутизации не может направлять трафик, даже если используется маршрутизация от источника.
* **б) нет, это невозможно:** Это неверно. Теоретически, маршрутизатор может работать без таблицы маршрутизации, если все маршруты прописаны вручную.
* **b) может, если выполняется лавинная маршрутизация:** Это тоже неверно. Лавинная маршрутизация (или динамическая маршрутизация) требует таблицы маршрутизации.
* **г) может, если в маршрутизаторе задан маршрут по умолчанию:** Это верно. Если маршрутизатор настроен с маршрутом по умолчанию, то он может работать, направляя трафик на этот маршрут в случае отсутствия других записей.

**Ответ:** **г) может, если в маршрутизаторе задан маршрут по умолчанию.**

### **38. К какому типу относится протокол OSPF?**

* **a) протокол маршрутизации:** Верно, OSPF — это протокол маршрутизации.
* **б) протокол, основанный на алгоритме состояния связей:** Это тоже верно. OSPF использует алгоритм состояния связей (Link State).
* **c) адаптивный протокол:** Верно. OSPF адаптируется к изменениям в сети.
* **г) централизованный:** Это неверно. OSPF — это дистрибутивный протокол.
* **д) дистанционно-векторный:** Это неверно. OSPF — это протокол состояния связей, а не дистанционно-векторный.
* **е) внутренний шлюзовый протокол:** Верно. OSPF используется для маршрутизации внутри автономной системы, т.е. это внутренний шлюзовый протокол (IGP).

**Ответ:** **б) протокол, основанный на алгоритме состояния связей.**

### **39. Какие параметры сети учитывают метрики, поддерживаемые протоколом OSPF?**

Метрики, поддерживаемые протоколом OSPF, включают:

* **a) пропускная способность:** Это верно. OSPF использует пропускную способность канала в качестве метрики для выбора наилучшего маршрута.
* **б) время передачи:** Это неверно. OSPF не использует время передачи как метрику.
* **c) надежность каналов связи:** Это также неверно. OSPF не учитывает надежность канала напрямую.
* **г) количество хопов:** Это неверно. OSPF использует стоимость маршрута, основанную на пропускной способности, а не количество хопов.

**Ответ:** **a) пропускная способность.**

### **40. Поясните, какие недостатки традиционной маршрутизации привели к созданию SDN?**

SDN (Software-Defined Networking) была создана для решения ряда проблем традиционной маршрутизации, таких как:

* **a) негибкая процедура продвижения трафика на основе единственного поля - адреса назначения:** Это относится к традиционным методам маршрутизации, где маршруты часто устанавливаются только на основе IP-адреса назначения. SDN решает эту проблему, позволяя более гибко управлять маршрутизацией с использованием программных методов, в том числе на основе различных факторов (например, трафика, состояния сети, приложений).
* **б) децентрализованные протоколы построения таблиц маршрутизации медленно реагируют на изменения топологии сети:** Это также одна из проблем традиционной маршрутизации. В традиционных протоколах (например, RIP или OSPF) обновления маршрутов могут занимать время, а топология сети изменяется динамически. SDN решает эту проблему с помощью централизованного контроля, где изменения в сети можно быстро учесть.
* **b) децентрализованные протоколы построения таблиц маршрутизации позволяют находить только квази-оптимальные маршруты:** Это также верно для традиционных маршрутизаторов, использующих децентрализованные алгоритмы маршрутизации. SDN позволяет оптимизировать маршруты с более точной настройкой, подходящей для специфических приложений.
* **г) для агрегированных потоков на интернет-магистралях необходима гибкая и адаптивная обработка на основе логического разделения трафика на отдельные потоки:** Это связано с необходимостью для SDN эффективно обрабатывать сложные маршруты и управлять потоками трафика, например, в условиях перегрузки сети или при необходимости передачи больших объемов данных.
* **д) нестандартный командный язык конфигурирования сетевых устройств препятствует унификации управления этими устройствами:** Традиционные устройства имеют разнообразие интерфейсов конфигурации, что затрудняет их централизованное управление. В SDN управление централизовано, и сеть управляется с помощью одного стандартизированного интерфейса, что упрощает администрирование.

**Ответ:** **все эти недостатки способствовали созданию SDN.**

### **41. Система, в которой функции сетевых устройств (маршрутизаторов, коммутаторов, файерволов и др.) реализуются не на основе аппаратной специализированной платформы, а программным путем в серверах общего назначения, называется:**

* **a) виртуальной частной сетью VPN:** Это неверно, VPN — это технология для создания защищенной связи между узлами через общедоступную сеть.
* **б) виртуальной локальной сетью VLAN:** Это также неверно, VLAN — это логическое разделение сетей на основе их функций, но не виртуализация всего сетевого оборудования.
* **b) виртуальной сетью NFV:** Это верно. NFV (Network Functions Virtualization) представляет собой концепцию виртуализации сетевых функций, таких как маршрутизаторы, коммутаторы и файерволы, на серверном оборудовании общего назначения.

**Ответ:** **b) виртуальной сетью NFV.**

### **42. Какой МАС-адрес имеет сетевой интерфейс, если известно, что его глобальный уникальный адрес 2001:718::280:48FF:FEEB:7960 был получен в результате автоконфигурирования?**

Для адреса IPv6, полученного с использованием автоконфигурирования, МАС-адрес генерируется на основе интерфейсного идентификатора. В данном случае интерфейсный идентификатор (последняя часть адреса) — 280:48FF:FEEB:7960. На основании этого можно вычислить соответствующий МАС-адрес. Однако для расчета самого МАС-адреса нужно использовать определенные правила преобразования. В частности, нужно инвертировать 7-й бит (универсальность) и использовать стандартные префиксы для MАC-адресов.

Для данного вопроса конкретный МАС-адрес может быть рассчитан из адреса, однако для примера можно привести его как часть глобального уникального адреса, начинающегося с: 02:00:00:48:FF:FE.

### **43. Какие из записей IPv6-адреса FEDC:0000:0000:0006:0030:0000:0000:7654 синтаксически ошибочными?**

* **a) FEDC::6:30:0:0:7654;** Это верно. Эта запись использует ::, что сокращает несколько нулевых блоков. Однако использование сокращения должно быть корректным, и здесь оно допускается, так как :: используется только один раз.
* **б) FEDC::0006:30:0:0:7654;** Это также верно, так как :: используется для сокращения 0-ов. Такая запись синтаксически правильная.
* **b) FEDC::6:30::7654;** Это неверно. Два символа :: не могут быть использованы в одной записи. Это нарушает правила записи адреса.
* **г) FEDC:0:0:6:3::7654.** Это неверно, так как в записи снова используется дважды ::. Это синтаксическая ошибка.

**Ответ:** **b) FEDC::6:30::7654.**

### **44. Какие типы адресов определены в IPv6?**

* **a) anycast:** Это верно. Тип адреса anycast используется для отправки пакета ближайшему (по маршруту) узлу из группы узлов с одним и тем же адресом.
* **б) multicast:** Это верно. Мультикаст-адреса позволяют отправлять пакеты группе узлов.
* **в) broadcast:** Это неверно. В IPv6 нет отдельного типа broadcast, так как для этого используется multicast.
* **r) unicast:** Это верно. Уникаст-адреса используются для отправки пакета одному конкретному получателю.
* **д) loopback:** Это верно. Адрес loopback (например, ::1) используется для связи с самим собой.

**Ответ:** **a) anycast, б) multicast, r) unicast, д) loopback.**

### **45. Объясните назначение группового адреса запрашиваемого узла (Solicited-Node Multicast Address). Почему в группу, описываемую этим адресом, скорее всего, входит только один узел?**

Групповой адрес запрашиваемого узла (Solicited-Node Multicast Address) в IPv6 используется для разрешения адресов при ARP-подобных запросах. Когда узел хочет узнать МАС-адрес другого узла в сети, он отправляет сообщение на адрес группы запрашиваемого узла. Это адрес с уникальным идентификатором для каждого узла, обычно получаемым из его адреса.

Поскольку каждый запрос ссылается на конкретный узел, адрес обычно используется только одним узлом, и в группу входит только один узел.

### **46. Поле «Класс трафика» в IPv6 аналогично полю «Тип сервиса» в IPv4 и используется для организации обслуживания с различным уровнем QoS. Зачем в IPv6 введено еще одно поле — «Метка потока», также направленное на поддержание QoS? Какие дополнительные возможности оно предоставляет?**

Поле **«Метка потока»** в IPv6 используется для обработки трафика, который принадлежит одному потоку. Это позволяет сетям (и маршрутизаторам) маркировать пакеты, которые принадлежат определенному потоку данных, например, для мультимедийных приложений, видеоконференций и других сервисов, требующих гарантированной пропускной способности и задержки. Это позволяет сетям с QoS более эффективно управлять такими потоками.

### **47. Чем отличается информация в основном заголовке IPv6 от информации заголовка IPv4?**

* **a) в IPv6 отсутствует поле «Контрольная сумма»:** Это верно. В IPv6 контрольная сумма убрана, так как её выполнение возложено на другие уровни стека протоколов.
* **б) в IPv6 появилось новое поле «Метка потока»:** Это верно. В IPv6 добавлено поле для маркировки потока, которое отсутствует в IPv4.
* **b) поле «Длина поля данных» имеет большую разрядность, достаточную для задания длины джамбограммы:** Это верно. В IPv6 поле длины данных (Payload Length) имеет большую разрядность.
* **г) поля «Адрес источника» и «Адрес назначения» имеют большую разрядность:** Это верно, так как в IPv6 они занимают по 128 бит.
* **д) основной заголовок IPv6 короче заголовка IPv4:** Это неверно. Заголовок IPv6 немного больше по размеру, чем в IPv4, из-за расширенного формата и нового поля.

**Ответ:** **a) в IPv6 отсутствует поле «Контрольная сумма».**

### **48. Какие из перечисленных технологий наиболее подходят, когда узлы двух сетей IPv6 необходимо соединить через транзитную сеть IPv4?**

Из предложенных вариантов технология, которая позволяет соединить два узла, использующие IPv6, через транзитную сеть IPv4, это **туннелирование**:

* **a) транслирование стеков:** Это обычно относится к технологии, когда один стек протоколов преобразуется в другой. Это не подходит для соединения через транзитную сеть IPv4, так как это подразумевает использование разных протоколов.
* **б) инкапсуляция IPv4 in IPv6:** Это относится к инкапсуляции IPv4-пакетов в IPv6, что не является правильным для вашей задачи.
* **b) туннелирование IPv6 over IPv4:** Это верно. В этом случае IPv6-данные инкапсулируются в IPv4-пакеты для передачи по сети, поддерживающей только IPv4. Это называется туннелированием IPv6 через IPv4 (6to4, Teredo и другие).
* **г) мультиплексирование стеков:** Это неверно, так как мультиплексирование стеков в контексте сетевых протоколов не используется для того, чтобы объединить два стека через транзитную сеть.
* **д) двойной стек:** Это также верно, но двойной стек подразумевает использование одновременно IPv4 и IPv6 на одном узле, а не соединение через транзитную сеть IPv4 для IPv6.

**Ответ:** **b) туннелирование IPv6 over IPv4.**

### **49. Предложите несколько возможных стратегий поведения владельцев сетей в условиях существования двух разных стеков — IPv6 и IPv4.**

Когда две сети используют разные протоколы — IPv6 и IPv4, владельцы сетей могут выбрать одну или несколько стратегий для интеграции этих стеков:

1. **Двойной стек (Dual Stack):** Использование как IPv4, так и IPv6 на одном устройстве или в одной сети. Это позволяет сетям поддерживать взаимодействие с обоими протоколами. Владелец сети должен настроить оба стека, что может потребовать больше ресурсов для управления.
2. **Туннелирование:** Использование туннелей для передачи IPv6-данных по сети IPv4 (например, 6to4, ISATAP). Это полезно, если сеть полностью поддерживает IPv4, а IPv6 требует переходного механизма.
3. **Транслирование:** Применение NAT64 или DNS64 для преобразования IPv6 в IPv4 (и наоборот). Это полезно в случаях, когда необходимо обеспечить совместимость между двумя протоколами на уровне приложений.
4. **Прямое использование IPv6:** Если сеть полностью поддерживает IPv6, можно настроить сети с использованием только этого протокола и постепенно переходить от IPv4. Это обеспечит более современное и масштабируемое подключение.
5. **Решения с применением шлюзов или прокси-серверов:** В случае, когда необходимо интегрировать IPv4 и IPv6 сети, можно использовать шлюзы, которые выполняют преобразование между этими протоколами.

**Ответ:** Стратегии могут включать **двойной стек**, **туннелирование**, **транслирование**, **прямое использование IPv6** или **решения с прокси/шлюзами**.

### **50. На веб-сервере и на вашем клиентском компьютере установлен двойной стек: IPv4 и IPv6. Каким образом браузер на вашем компьютере может выбрать, по какому протоколу он будет взаимодействовать с этим веб-сервером?**

Когда браузер на клиентском компьютере пытается подключиться к веб-серверу, использующему двойной стек (IPv4 и IPv6), он сначала проверяет DNS-запись для домена и получает два возможных адреса:

1. **AAAA-запись (IPv6):** Браузер проверяет наличие записи AAAA (для IPv6) в DNS. Если такая запись существует, и сервер поддерживает IPv6, браузер обычно сначала использует этот адрес.
2. **A-запись (IPv4):** Если нет IPv6-записи или браузер не может установить соединение по IPv6, он обращается к A-записи, которая указывает на IPv4-адрес.
3. **Алгоритм предпочтения:** Некоторые браузеры могут иметь предпочтение для использования IPv6, если оно доступно, так как это более современный протокол, но в случае проблем с IPv6 автоматически будет использован IPv4.
4. **Параметры настроек:** В некоторых случаях в операционных системах или браузерах могут быть установлены настройки, предпочтительные для одного из протоколов (например, предпочитать IPv4).

**Ответ:** Браузер использует **DNS-запись AAAA** для IPv6, а если она недоступна или есть проблемы с IPv6, использует **DNS-запись A** для IPv4.

### **51. Опишите процедуру проверки наличия дубликата адреса с помощью протокола ND (Neighbor Discovery) для случая, когда интерфейс узла А имеет МАС-адрес ОС-1С-09-48-ЕВ-5С-65 и неподтвержденный индивидуальный адрес 2001:620:1234:F8:41.**

Процесс проверки наличия дубликата адреса в IPv6 происходит с использованием протокола Neighbor Discovery (ND). Основной механизм — это **Neighbor Solicitation (NS)** и **Neighbor Advertisement (NA)**.

1. **Шаг 1: Узел А генерирует Neighbor Solicitation (NS):**
   1. Узел А (с MAC-адресом ОС-1С-09-48-ЕВ-5С-65 и IPv6-адресом 2001:620:1234:F8:41) отправляет **Neighbor Solicitation (NS)** для проверки, не используется ли этот адрес кем-то еще в сети. В сообщении NS содержится его предполагаемый адрес (в данном случае 2001:620:1234:F8:41).
2. **Шаг 2: Проверка на дубликаты:**
   1. Узел А отправляет этот запрос на **Multicast-адрес**, соответствующий конкретному адресу. Все устройства в сети с этим адресом должны ответить, если они используют его.
3. **Шаг 3: Узлы, которые используют этот адрес, отправляют Neighbor Advertisement (NA):**
   1. Если другой узел в сети использует данный адрес 2001:620:1234:F8:41, он должен ответить на запрос с помощью **Neighbor Advertisement (NA)**, подтверждая, что этот адрес уже занят.
4. **Шаг 4: Узел А получает NA (если адрес занят):**
   1. Если на запрос NS приходит ответ NA, это означает, что адрес уже используется, и узел А не может использовать его. В противном случае адрес считается уникальным, и узел А может его присвоить своему интерфейсу.

**Ответ:** Узел А отправляет **Neighbor Solicitation (NS)** для проверки дубликатов. Если адрес уже используется, ответ от другого узла будет содержать **Neighbor Advertisement (NA)**.

# **Вопросы к части V**

### **1. Какие из перечисленных услуг относятся к информационным?**

**Ответ:**

* **б) интернет-телефония**
* **b) веб-хостинг**

Обе эти услуги относятся к информационным, так как обеспечивают обработку и передачу информации через интернет.

### **2. К какому типу сети оператора связи должен быть подключен центр данных, управляющий роботами в реальном масштабе времени?**

**Ответ:**

* **a) к магистрали**

Центр данных, управляющий роботами в реальном времени, должен быть подключен к сети оператора связи, которая имеет высокую пропускную способность и низкую задержку, что характерно для магистральных сетей.

### **3. В чем разница между технологиями «IP поверх OTN» и «IP поверх DWDM»?**

* **IP поверх OTN (Optical Transport Network):** Это интеграция IP-трафика в структуру оптической транспортной сети. OTN предоставляет прозрачную передачу для данных через оптические сети, оптимизируя их маршрутизацию и управление трафиком.
* **IP поверх DWDM (Dense Wavelength Division Multiplexing):** Это метод мультиплексирования, который позволяет передавать несколько каналов данных через один оптоволоконный канал, используя разные длины волн света. В этой технологии IP-трафик передается поверх DWDM-сети.

**Основная разница:** OTN предоставляет абстракцию для транспортировки данных, тогда как DWDM занимается мультиплексированием оптических сигналов для увеличения пропускной способности.

### **4. Назовите преимущества и недостатки техники виртуальных каналов.**

**Преимущества:**

* Экономия на инфраструктуре, так как виртуальные каналы позволяют передавать несколько логических каналов по одному физическому.
* Гибкость в создании каналов и их изменении в зависимости от нагрузки.

**Недостатки:**

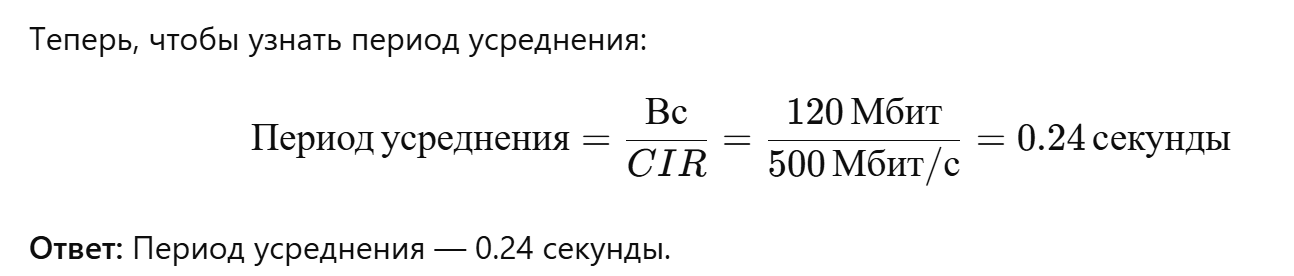
* Сложность в управлении и мониторинге, особенно в больших сетях.
* Возможно снижение качества обслуживания из-за совместного использования физического канала несколькими логическими.

### **5. Какой период усреднения скорости оговорен в SLA, если CIR = 500 Мбит/с и Вс = 15 Мбайт?**

Согласно SLA (Service Level Agreement), **CIR** — это гарантированная скорость, а **Вс** — это объем данных. Чтобы рассчитать период усреднения:

* CIR = 500 Мбит/с = 500 000 Кбит/с
* Вс = 15 Мбайт = 15 \* 8 Мбит = 120 Мбит

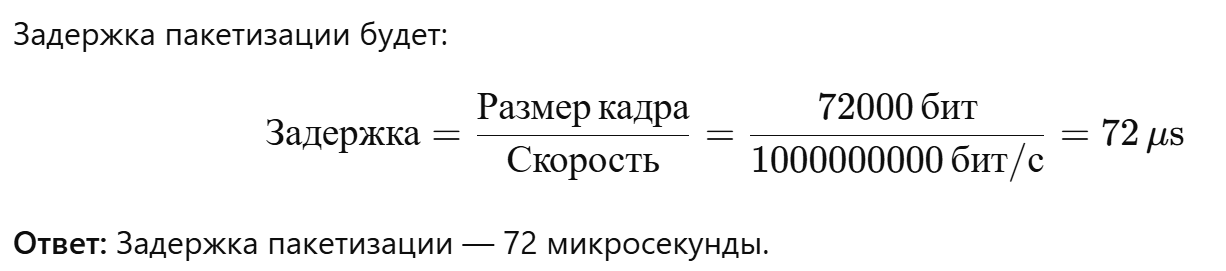
Теперь, чтобы узнать период усреднения:



**6. Чему равна задержка пакетизации для кадров Ethernet с размером поля данных 9000 байт (Jumbo frames)?**

Задержка пакетизации зависит от скорости передачи и размера данных.

* Размер кадра = 9000 байт = 72 000 бит.
* Пусть скорость передачи равна 1 Гбит/с (1000 Мбит/с).



### **7. Почему нисходящая скорость технологии ADSL всегда выше восходящей?**

Технология **ADSL (Asymmetric Digital Subscriber Line)** использует асимметричную архитектуру, где более широкая полоса пропускания выделяется для нисходящего трафика (от интернета к пользователю) и уже для восходящего (от пользователя к интернету). Это обусловлено тем, что большинство пользователей чаще скачивают данные, чем отправляют их.

### **8. Поясните, каким образом можно повысить скорость технологии ADSL.**

**Ответ:**

* **b) за счет замены части абонентского медного окончания оптическим волокном.**

Медное соединение имеет ограниченную пропускную способность, и использование оптики на определенных участках может значительно увеличить скорость.

### **9. Почему сети PON дешевле активных оптических сетей?**

Сети **PON (Passive Optical Network)** дешевле активных оптических сетей, потому что в PON используются пассивные компоненты (например, оптические сплиттеры), которые не требуют питания и активного управления, в отличие от активных сетей, где каждый узел требует сложного оборудования и энергии.

### **10. Какой метод мультиплексирования применяется в технологии PON?**

В **технологии PON** применяется метод **WDM (Wavelength Division Multiplexing)** или **TDM (Time Division Multiplexing)**. Наиболее часто используется TDM, где несколько пользователей делят одну волокно по времени.

### **11. Какой алгоритм доступа применяется в технологии PON?**

В **PON** применяется метод доступа **TDMA (Time Division Multiple Access)**, при котором каждому пользователю выделяется временной слот для передачи данных.

### **12. Перечислите функциональные модули IP-маршрутизатора, которые используются в LSR.**

**Функциональные модули IP-маршрутизатора, используемые в LSR (Label Switch Router):**

* **Маршрутизатор пакетов** — для обработки IP-адресов.
* **Модуль меток** — для обработки меток MPLS.
* **Модуль таблицы маршрутов** — для определения маршрута в сети.
* **Модуль очередей** — для управления трафиком.

### **13. Предположим, что LSR использует формат кадров Ethernet. Означает ли это, что LSR продвигает кадры на основе таблицы продвижения, полученной в соответствии со стандартом IEEE 802.1D?**

Нет, **LSR** (Label Switch Router) использует **метки MPLS**, а не таблицы, основанные на стандартном Ethernet (IEEE 802.1D). LSR работает с метками и таблицами меток, а не с адресами MAC.

### **14. Протокол LDP является частью технологии:**

**Ответ:**

* **b) MPLS TE** (Traffic Engineering).

Протокол **LDP (Label Distribution Protocol)** используется для распространения меток в сети MPLS, в том числе в рамках **Traffic Engineering**.

### **15. Можно ли в сети, поддерживающей MPLS, передавать часть трафика с помощью обычного IP-продвижения?**

**Ответ:** Да, в сети MPLS можно передавать часть трафика с использованием **обычного IP-продвижения**. MPLS работает параллельно с IP, и трафик может направляться как через MPLS-соединения, так и по обычному IP-маршруту.

### **16. Технология MPLS является гибридом технологий:**

**Ответ:**

* **b) IP и технологии виртуальных каналов.**

MPLS (Multiprotocol Label Switching) объединяет возможности маршрутизации на основе IP и технологии виртуальных каналов (например, виртуальные каналы в сети MPLS используются для быстрого маршрутизирования трафика с помощью меток).

### **17. Какие функциональные модули IP-маршрутизатора используются в LSR?**

**Ответ:**

* **a) блок продвижения.**

**LSR (Label Switch Router)** использует блок продвижения для обработки и передачи пакетов на основе меток MPLS. Этот блок отвечает за коммутирование пакетов в зависимости от метки, а не IP-адреса.

### **18. Класс эквивалентности продвижения - это:**

**Ответ:**

* **c) группа IP-пакетов, имеющих одни и те же требования к условиям транспортировки.**

Класс эквивалентности продвижения (Forwarding Equivalence Class, FEC) включает в себя набор пакетов, которые обрабатываются одинаково в сети и передаются по одному и тому же пути.

### **19. Какой из вариантов управления распределением меток протоколом LDP называется упорядоченным?**

**Ответ:**

* **a) метка назначается по запросу от вышележащего устройства LSR.**

В упорядоченном распределении меток в протоколе LDP, метка назначается устройством только по запросу от соседнего устройства (вышележащего устройства в сети).

### **20. Поясните, зачем в сообщении Echo Request протокола LSP Ping в качестве назначения применяется адрес 127.0.0.1.**

**Ответ:**

* **b) этот адрес выбран произвольно, как не имеющий значения, потому что сообщение передается на основе меток MPLS.**

Адрес 127.0.0.1 (loopback) используется в сообщении Echo Request для тестирования сети MPLS. Он не имеет значения в контексте маршрутизации IP, так как сам пакет ориентирован на тестирование пути меток в сети MPLS.

### **21. Протокол BFD отличается от протокола LSP Ping следующими свойствами:**

**Ответ:**

* **b) он проще в реализации.**

**BFD (Bidirectional Forwarding Detection)** проще в реализации, так как он используется для быстрой проверки состояния маршрутов и обнаружения неисправностей в сетевых соединениях. LSP Ping более специализирован для проверки меток в MPLS-сетях.

### **22. Какой механизм отказоустойчивости MPLS является более универсальным?**

**Ответ:**

* **b) защита пути.**

**Защита пути** в MPLS более универсальна, поскольку она обеспечивает отказоустойчивость на уровне пути, который используется для передачи трафика. В случае сбоя пути трафик может быть перенаправлен по резервному пути.

# **Вопросы к части VI**

### **1. Может ли проводная связь быть мобильной?**

**Ответ:**

Проводная связь традиционно предполагает фиксированные соединения, однако с помощью технологий, таких как адаптивные кабели, порты и системы мобильной связи (например, мобильные сети с использованием проводных линий), можно создать гибридные системы, которые позволяют проводным соединениям быть мобильными в определенном контексте.

### **2. Частоты какого диапазона выше: видимого света или микроволнового?**

**Ответ:**

Частоты видимого света выше, чем частоты микроволнового диапазона. Видимый свет имеет частоты от 430 до 770 ТГц, в то время как микроволновые частоты обычно находятся в диапазоне от 300 МГц до 300 ГГц.

### **3. Вследствие какого эффекта электромагнитные волны следуют поверхности Земли?**

**Ответ:**

Электромагнитные волны следуют поверхности Земли вследствие **эффекта проводимости** или **рефракции**. Это явление связано с тем, что в атмосфере существует градиент плотности, который влияет на распространение волн, заставляя их следовать по кривизне Земли.

### **4. За счет чего технологии широкополосного сигнала уменьшают влияние помех на полезный сигнал?**

**Ответ:**

Технологии широкополосного сигнала, такие как **модуляция с частотным и временным кодированием**, уменьшают влияние помех на полезный сигнал, потому что широкий спектр позволяет распределить сигнал по большему числу частот. Это делает систему менее уязвимой к помехам, поскольку помехи воздействуют только на часть спектра.

### **5. Как определяется коэффициент усиления антенны?**

**Ответ:**

Коэффициент усиления антенны определяется как отношение интенсивности излучения антенны в заданном направлении к интенсивности излучения идеальной (изотропной) антенны, которая излучает одинаково во всех направлениях. Этот параметр выражается в децибелах (дБ).

### **6. Какой размер должен быть у антенны-диполя?**

**Ответ:**

Длина антенны-диполя должна быть около **половины длины волны** сигнала, для которого она настроена. Например, для сигнала с частотой 300 МГц длина волны составит 1 м, а длина диполя — около 0,5 м.

### **7. В чем отличие назначений пространственного мультиплексирования и пространственного разнесения?**

**Ответ:**

* **Пространственное мультиплексирование** используется для увеличения пропускной способности канала путем отправки нескольких потоков данных одновременно через разные антенны, используя тот же спектр.
* **Пространственное разнесение** используется для повышения надежности передачи путем отправки одного потока данных через разные пути, что позволяет минимизировать потерю пакетов при помехах.

### **8. Какой вариант FHSS эффективнее уменьшает влияние помех — быстрый или медленный расширение частоты?**

**Ответ:**

**Медленное расширение частоты** более эффективно уменьшает влияние помех, так как оно позволяет более равномерно распределять спектр, избегая насыщения на определенных частотах и уменьшая вероятность попадания помех на частоту.

### **9. За счет чего возможно выделить сигнал отдельного канала из общего сигнала в типлексировании CDMA?**

**Ответ:**

В типлексировании **CDMA** (Code Division Multiple Access) выделение сигнала отдельного канала происходит за счет **различных кодов**, назначаемых каждому пользователю. Эти коды позволяют отделить сигналы друг от друга, даже если они используют одну и ту же частотную полосу.

### **10. Какой должна быть частота модуляции сигнала в подканалах OFDM, если известно, что эти подканалы сдвинуты относительно друг друга на 20 кГц?**

**Ответ:**

Частота модуляции каждого подканала в **OFDM** должна быть **20 кГц**, чтобы избежать перекрытия спектров подканалов и обеспечить эффективное использование полосы частот без интерференции.

### **11. В чем состоит негативный эффект засвеченного терминала?**

**Ответ:**

Засвеченный терминал — это терминал, который получает сигнал с очень высоким уровнем шума или помех. Это может привести к тому, что терминал не сможет правильно распознать или декодировать сигнал, снижая качество связи или даже приводя к потере данных.

### **12. Каким образом обнаруживает коллизии уровень МАС в сетях 802.11?**

**Ответ:**

В сетях **802.11** уровень **MAC** (Media Access Control) обнаруживает коллизии путем использования алгоритма **CSMA/CA** (Carrier Sense Multiple Access with Collision Avoidance). Он слушает канал на предмет его занятости, и если канал свободен, то отправляется данные. Если коллизия все же происходит, станции повторно пытаются передать данные через случайный интервал времени.

### **13. Может ли станция сети 802.11 передать кадр другой станции, входящей в ту же BSS, не непосредственно, а через точку доступа?**

**Ответ:**

Да, станция в сети **802.11** может передать кадр другой станции, входящей в ту же **BSS (Basic Service Set)**, через точку доступа, если они находятся в одной сети и точка доступа выполняет функцию ретранслятора.

### **14. Какое значение имеет поле «Длительность» кадра Wi-Fi с широковещательным адресом назначения?**

**Ответ:**

Поле **«Длительность»** в кадре Wi-Fi с широковещательным адресом назначения указывает время, в течение которого канал будет занят передачей данных, чтобы другие устройства знали, когда можно будет передавать свои данные.

### **15. Каким образом синхронизируются станции в распределенном режиме доступа?**

**Ответ:**

Станции в **распределенном режиме доступа** сети **802.11** синхронизируются с использованием **тайм-метки**. Все станции отслеживают время через временные метки, синхронизированные с точкой доступа, и ожидают своей очереди для передачи данных.

### **16. За счет чего режим PCF всегда имеет приоритет перед режимом DCF?**

**Ответ:**

В режиме **PCF** (Point Coordination Function) точка доступа (или координирующая станция) управляет доступом к каналу и разрешает передачу данных в контролируемой последовательности, что дает ему приоритет перед режимом **DCF** (Distributed Coordination Function), где станции конкурируют за доступ к каналу без централизованного управления.

### **17. За счет чего достигается увеличение расстояния взаимодействия устройств Bluetooth Long Distance?**

**Ответ:**

Для увеличения расстояния взаимодействия в **Bluetooth Long Distance** используется **усиление сигнала**, а также **улучшенные антенны** и повышенная мощность передачи, что позволяет устройствам взаимодействовать на больших расстояниях.

### **18. Какого класса должны быть устройства Bluetooth, чтобы взаимодействовать на расстоянии 30 м?**

**Ответ:**

Для взаимодействия на расстоянии 30 м устройства **Bluetooth** должны быть **класса 1**, так как они поддерживают радиус действия до 100 метров.

### **19. Предложите вариант организации сот GSM с повторным использованием четырех частот.**

**Ответ:**

Для организации сот в **GSM** с повторным использованием частот можно использовать схему, в которой частотные каналы повторяются через каждые 4 клетки, обеспечивая эффективное использование частот в сети. Например, можно разбить территорию на 4 группы, каждая из которых будет использовать свои частоты.

### **20. Как можно увеличить количество одновременно обслуживаемых абонентов в некоторой области покрытия мобильной сети GSM?**

**Ответ:**

Для увеличения количества обслуживаемых абонентов можно **уменьшить размер сот**, **повысить плотность базовых станций** или применить **технологии частотного повторного использования**.

### **21. Почему пейджинг выполняется в нескольких сотах?**

**Ответ:**

Пейджинг выполняется в нескольких сотах, чтобы гарантировать, что абонент получит сигнал о входящем вызове, независимо от того, в какой части своей области покрытия он находится.

### **22. Назовите недостаток метода эстафетной передачи при первом превышении мощности сигнала новой соты мощности сигнала текущей соты?**

**Ответ:**

Недостаток метода эстафетной передачи заключается в том, что **при первом превышении мощности сигнала новой соты** может произойти **перенос соединения** до того, как текущая сота завершит передачу данных, что может привести к потере пакетов или ухудшению качества связи.

### **23. Почему нельзя узнать номер своего мобильного телефона, просматривая данные его установок?**

**Ответ:**

Номер мобильного телефона обычно не отображается напрямую в настройках устройства по соображениям безопасности и конфиденциальности. Устройства и операторы мобильной связи предпочитают скрывать такие данные от пользователей, чтобы избежать утечек личной информации. Чтобы узнать свой номер, нужно обратиться к оператору связи или воспользоваться специальными командными кодами (например, \*#100# или \*#101# в некоторых сетях).

### **24. Какова максимально возможная скорость передачи пользовательских данных в сети GPRS (при выделении всех тайм-слотов одному пользователю)?**

**Ответ:**

Максимальная теоретическая скорость передачи данных в сети **GPRS** при использовании всех тайм-слотов и с учётом наилучшего сценария составляется примерно **171,2 кбит/с**. Это достигается при использовании всех 8 тайм-слотов (в одном тайм-слоте может быть передано до 21,4 кбит/с). Однако на практике скорость может быть ниже из-за различных факторов, таких как помехи, загруженность сети и другие.

### **25. Сколько ресурсных блоков сети LTE нужно выделить логическому каналу, чтобы его скорость передачи данных была равна 2,016 Мбит/с при методе кодирования 64-QM?**

**Ответ:**

В сети **LTE** один **ресурсный блок** (RB) занимает 180 кГц и может передавать различные объемы данных в зависимости от выбранной схемы модуляции и кодирования. Для кодирования 64-QM (64-QAM), при оптимальных условиях, один ресурсный блок может обеспечивать скорость около 1,5–2 Мбит/с (в зависимости от текущего спектра и условий связи).

Чтобы получить скорость **2,016 Мбит/с**, нужно рассчитать количество требуемых ресурсных блоков:

* При 64-QAM, один RB может передавать около 2 Мбит/с.
* Для 2,016 Мбит/с потребуется **1 ресурсный блок**.

### **26. С какой целью устанавливается GRE-туннель между шлюзами GW и PDN-GW сети LTE?**

**Ответ:**

**GRE-туннель** (Generic Routing Encapsulation) между **GW** (Gateway) и **PDN-GW** (Packet Data Network Gateway) используется в сети LTE для **инкапсуляции IP-пакетов** в другие пакеты для передачи через публичную сеть или другие сегменты сети. Это позволяет:

* **Изолировать трафик** и скрыть его от общего потока.
* Обеспечить **надежную передачу данных** между сетями.
* Позволить безопасную и эффективную передачу данных между **операторами связи** и **пользовательскими сетями**.

Туннель также помогает обеспечивать передачу данных между различными регионами и уровнями сети LTE.

### **27. Какие технологии используются для виртуализации сети 5G?**

**Ответ:**

Для виртуализации в сети **5G** используются несколько технологий, включая:

* **Network Functions Virtualization (NFV)** — технология виртуализации функций сети, позволяющая программно управлять и развертывать сетевые функции (например, маршрутизаторы, брандмауэры, контроллеры) без необходимости использования специализированного оборудования.
* **Software-Defined Networking (SDN)** — технология, которая позволяет централизованно управлять сетью, разделяя план управления и план передачи данных, что позволяет более гибко адаптировать сеть к различным требованиям.
* **Cloud-native архитектура** — использование облачных технологий и контейнеров (например, Kubernetes) для управления инфраструктурой и приложениями в 5G сети.
* **Edge Computing** — виртуализация обработки данных на периферии сети, что позволяет снизить задержки и повысить производительность.

### **28. В чем преимущества и недостатки нового диапазона частот 26 Гц в сетях 5G?**

**Ответ:**

**Преимущества диапазона частот 26 Гц в сетях 5G:**

* **Высокая пропускная способность**: Диапазон 26 ГГц позволяет достигать очень высоких скоростей передачи данных, что критично для поддержания требуемых характеристик 5G, таких как высокая скорость и низкие задержки.
* **Меньше помех**: Меньшее использование этого диапазона в настоящее время снижает помехи и перегрузки от других систем, что может улучшить качество связи.

**Недостатки диапазона частот 26 ГГц:**

* **Ограниченный радиус покрытия**: Из-за высокой частоты сигнал не распространяется далеко и плохо проникает через стены и другие препятствия, что ограничивает его использование в местах с плотной застройкой.
* **Высокая уязвимость к атмосферным воздействиям**: Атмосферные явления, такие как дождь или туман, могут сильно ослабить сигнал в этих диапазонах частот.
* **Необходимость в плотной сети базовых станций**: Для обеспечения стабильной связи в диапазоне 26 ГГц потребуется большое количество базовых станций, что увеличивает затраты на развертывание и эксплуатацию сети.

# **Вопросы к части VII**

### **1. Как письмо находит путь к почтовому серверу получателя?**

**Ключевая роль DNS**

Когда вы отправляете электронное письмо на адрес вида [name@domain.com](mailto:name@domain.com), почтовый сервер отправителя начинает процесс доставки. Для этого он должен определить IP-адрес почтового сервера, обслуживающего домен domain.com. Этот процесс осуществляется с помощью **DNS (Domain Name System)**.

**Механизм работы:**

1. **Запрос к DNS-серверу:** Почтовый сервер отправителя отправляет запрос к DNS-серверу, чтобы узнать IP-адрес, соответствующий доменному имени domain.com.
2. **Получение IP-адреса:** DNS-сервер, имеющий информацию о доменных именах и их соответствующих IP-адресах, возвращает IP-адрес почтового сервера получателя.
3. **Отправка письма:** Зная IP-адрес, почтовый сервер отправителя направляет письмо непосредственно на этот сервер.

**Дополнительные факторы:**

* **MX-записи:** В DNS хранятся специальные записи (MX-записи), которые указывают на почтовые серверы для определенных доменов. Они помогают выбрать наиболее подходящий почтовый сервер для доставки письма.
* **SMTP:** Протокол SMTP (Simple Mail Transfer Protocol) используется для передачи электронных писем между почтовыми серверами.

**Визуализация процесса:** [Изображение, иллюстрирующее процесс отправки электронного письма и роль DNS]

### **2. Сравнение почтовых протоколов IMAP, POP3 и SMTP**

|  |  |
| --- | --- |
| Свойство протокола | Протоколы |
| Используется почтовым клиентом для передачи письма на сервер | SMTP |
| Используется почтовым клиентом для получения письма с сервера | IMAP, POP3 |
| При получении почты письмо перемещается с сервера на клиент | POP3 |
| При получении почты письмо копируется с сервера на клиент | IMAP |

**Пояснения:**

* **SMTP (Simple Mail Transfer Protocol):** Используется только для отправки писем с почтового клиента на почтовый сервер.
* **POP3 (Post Office Protocol version 3):** При использовании POP3 письма загружаются с почтового сервера на устройство пользователя и удаляются с сервера. Это означает, что письма, загруженные на одно устройство, не будут доступны на других устройствах.
* **IMAP (Internet Message Access Protocol):** IMAP позволяет оставлять копии писем на почтовом сервере, обеспечивая доступ к ним с различных устройств. Пользователь может выбирать, какие письма загрузить на свое устройство, а какие оставить на сервере.

**Выбор протокола:**

Выбор протокола зависит от того, как пользователь хочет работать с электронной почтой:

* **POP3:** Подходит для пользователей, которые хотят загружать свои письма на одно устройство и не нуждаются в постоянном доступе к ним с разных устройств.
* **IMAP:** Более гибкий протокол, позволяющий работать с почтой с различных устройств и оставлять копии писем на сервере.

**Дополнительная информация:**

* **Другие протоколы:** Существуют и другие протоколы для работы с электронной почтой, такие как Exchange ActiveSync, но IMAP и POP3 являются наиболее распространенными.
* **Безопасность:** Рекомендуется использовать защищенные соединения (например, через SSL/TLS) для предотвращения перехвата почты при передаче.

**Вывод:** DNS играет ключевую роль в определении маршрута электронного письма, а протоколы SMTP, IMAP и POP3 определяют, как почтовые клиенты взаимодействуют с почтовыми серверами. Выбор протокола зависит от потребностей пользователя.

### **3. Браузер находит информацию по адресам специального формата, например, такому:**

[**http://www.bbc.co.uk/mobile/web/versions.shtml**](http://www.bbc.co.uk/mobile/web/versions.shtml). Поясните, какая часть данной записи представляет собой:

**Ответ:**

* **a) путь к объекту** – это **/mobile/web/versions.shtml**. Этот компонент URL указывает путь к конкретному ресурсу на веб-сервере.
* **b) DNS-имя сервера** – это [**www.bbc.co.uk**](http://www.bbc.co.uk/). Это имя домена, которое браузер использует для поиска IP-адреса сервера через систему доменных имен (DNS).
* **c) URL-имя** – это целый адрес: [**http://www.bbc.co.uk/mobile/web/versions.shtml**](http://www.bbc.co.uk/mobile/web/versions.shtml). Это полное имя ресурса, включая протокол и путь.
* **d) тип протокола доступа** – это **http**. Это указывает на протокол, который используется для доступа к ресурсу (в данном случае HTTP).

### **4. Что вы можете сказать о HTTP-сообщении вида HTTP/1.1 200 OK?**

**Ответ:**

* **a) это HTTP-запрос** – это неверно. Это не запрос, а **HTTP-ответ** от сервера.
* **b) это HTTP-ответ** – правильно. **HTTP/1.1 200 OK** является частью HTTP-ответа сервера, который сообщает, что запрос был успешно обработан.
* **c) 200 - это код состояния** – правильно. **200** в ответе — это код состояния, который означает, что запрос был успешно выполнен.
* **d) 200 - это объем переданной информации** – неверно. **200** — это код состояния, а не объем данных.
* **e) OK означает, что информация зашифрована открытым ключом** – неверно. **OK** означает, что запрос был успешно выполнен, но не связано с шифрованием.
* **f) OK означает, что «все в порядке!»** – правильно. **OK** в ответе подтверждает успешное выполнение запроса.

### **5. Укажите, какие из следующих утверждений правильны:**

**Ответ:**

* **a) веб-сервер находится постоянно в активном состоянии, прослушивая ТСР-порт 80** – **неправильно**. Веб-сервер обычно активен и прослушивает порт 80 только после того, как сервер был запущен, но не всегда работает в состоянии постоянного ожидания, пока не получит запрос.
* **b) веб-сервер переходит в активное состояние, получив запрос от клиента на ТСР-порт 80** – **правильно**. Сервер начинает работать и обрабатывать запросы, когда на его порт 80 поступает запрос от клиента.
* **c) после отправки всех объектов клиенту сервер разрывает с ним ТСР-соединение** – **неправильно**. Веб-сервер может использовать механизмы постоянного соединения (например, HTTP/1.1 с Keep-Alive), чтобы оставить соединение открытым для последующих запросов.
* **d) веб-сервер не хранит информацию о том, какие страницы пользователь уже посетил** – **правильно**. Веб-сервер не хранит такую информацию по умолчанию, но может использовать куки или сессии для хранения данных о посещенных страницах.
* **e) получив запрос от клиента, веб-сервер отображает все объекты на экране** – **неправильно**. Веб-сервер не отображает объекты на экране, это задача **браузера**. Сервер только отправляет данные (HTML, изображения и т. д.), а браузер их интерпретирует и отображает.

### **6. За счет чего в версии HTTP/2 достигается ускорение процесса построения веб-страницы браузером по сравнению с HTTP 1.0 и 1.1?**

**Ответ:**

HTTP/2 ускоряет процесс построения веб-страницы за счет нескольких ключевых технологий:

* **Мультиплексирование**: В HTTP/2 несколько запросов и ответов могут передаваться по одному соединению, что исключает проблему "head-of-line blocking" (задержка из-за ожидания завершения одного запроса, прежде чем начнется обработка следующего).
* **Сжатие заголовков**: HTTP/2 использует механизм сжатия заголовков данных, что уменьшает объем передаваемой информации и ускоряет обработку запросов.
* **Приоритетизация**: HTTP/2 позволяет задавать приоритет для различных запросов, позволяя браузеру загрузить наиболее важные элементы страницы (например, изображения) быстрее.
* **Серийная передача**: Сервер может отправлять ответы на несколько запросов сразу, даже если они относятся к разным ресурсам.

### **7. В чем состоят недостатки организации почтовой службы, при которой почтовый клиент и сервер установлены на компьютере у каждого абонента?**

**Ответ:**

* **Отсутствие централизованного управления**: Каждый компьютер должен быть настроен индивидуально, что усложняет администрирование и обновления.
* **Риск утраты данных**: В случае сбоя компьютера данные (почта) могут быть утрачены, так как нет централизованного хранения.
* **Проблемы с синхронизацией**: Отсутствие единой почтовой базы затрудняет синхронизацию сообщений между различными устройствами, что может привести к несогласованности данных.
* **Низкая безопасность**: При использовании локальных почтовых серверов безопасность может быть ослаблена, особенно если нет должной защиты.

### **8. Агент системы управления сетью - это (выберите вариант ответа):**

**Ответ:**

* **a) программа, устанавливаемая на управляемое устройство** – правильно. Агент системы управления сетью — это программа, которая устанавливается на управляемое устройство (например, маршрутизатор или сервер) и взаимодействует с менеджером сети, отправляя ему данные о состоянии устройства.

### **9. Что такое MIB в системе управления сетью? Варианты ответов:**

**Ответ:**

* **b) база данных управляющей информации** – правильно. MIB (Management Information Base) — это база данных, которая содержит информацию о конфигурации и состоянии управляемых устройств. Она используется агентами системы управления сетью для предоставления данных менеджеру.

### **10. Какую роль играет агент в двухзвенной схеме управления устройством? Варианты ответов:**

**Ответ:**

* **b) роль сервера** – правильно. Агент в схеме управления устройством выполняет роль "сервера", предоставляя информацию о состоянии устройства, отвечая на запросы от менеджера и выполняя команды по его указанию.

### **11. Какой протокол может быть использован для взаимодействия менеджера и агента системы управления сетью? Варианты ответов:**

**Ответ:**

* **a) SNMP** – правильно. SNMP (Simple Network Management Protocol) — это основной протокол, который используется для взаимодействия между менеджером сети и агентом.

# **Вопросы к части VIII**

## **Анализ и заполнение таблицы: Субъекты и объекты системы контроля доступа**

### **Понятие субъекта и объекта в системе контроля доступа**

* **Субъект** - это активная сущность системы, которая может инициировать действия и взаимодействовать с другими компонентами системы. Субъекты обладают определенными правами доступа и могут выполнять различные операции над объектами.
* **Объект** - это пассивная сущность системы, к которой могут применяться различные действия. Объекты хранят данные или предоставляют услуги.

### **Заполнение таблицы**

|  |  |  |
| --- | --- | --- |
| Элемент системы | Объекты | Субъекты |
| Пользователи |  | X |
| Устройства | X |  |
| Прикладные процессы |  | X |
| Файлы | X |  |
| Пропускная способность каналов связи | X |  |
| Сетевые сервисы | X |  |

### **2. Используя приведенный далее список терминов, вставьте пропущенные слова в следующее предложение:**



### **3. Вставьте пропущенные слова из списка:**



### **4. Приведите примеры ситуаций, при которых обеспечивается конфиденциальность, но не гарантируется целостность данных.**

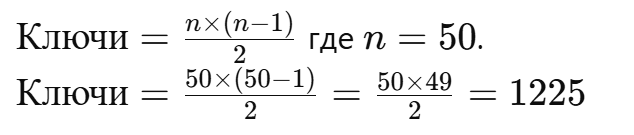


### **5. Как называется свойство, которое характеризует систему, в которой документ имеет достоверную информацию о его источнике (авторе)?**

**Ответ:** Это свойство называется **аутентичность**.

### **6. Сколько секретных ключей требуется для переписки 50 человек «каждый с каждым», использующих алгоритм DES?**

**Ответ:** Для переписки 50 человек «каждый с каждым» необходимо 1225 секретных ключей. Это можно вычислить по формуле:



### **7. Что определяет криптостойкость алгоритма шифрования:**

* a) секретность алгоритма;
* **б) секретность ключа**;
* b) сложность алгоритма.

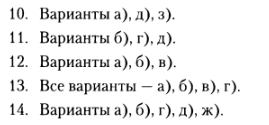
**Ответ:** Криптостойкость алгоритма шифрования в первую очередь зависит от **секретности ключа**. Секретность алгоритма может быть нарушена, если его структура становится известна, но надежность шифрования сохраняется благодаря секретности ключа. Сложность алгоритма также влияет, но ключ имеет основное значение.

### **8. Можно ли передать секретный ключ по открытому каналу, не используя шифрование?**



### **9. В главе 28 рассмотрен пример архитектуры сети с защитой периметра и разделением внутренних зон. Предложите альтернативный вариант.**





### **10. Какие из перечисленных ниже свойств образуют триаду безопасности CIA:**

* **a) конфиденциальность**;
* **б) неотказуемость**;
* **b) аутентичность**;
* **г) владение**;
* **д) целостность**;
* **e) полезность**;
* **ж) захват привилегий**;
* **3) доступность.**

**Ответ:** Триада безопасности CIA включает следующие компоненты:

* **a) конфиденциальность** (Confidentiality),
* **д) целостность** (Integrity),
* **3) доступность** (Availability).

Неотказуемость, аутентичность, владение и другие перечисленные элементы могут быть важны для безопасности, но они не входят в стандартную триаду безопасности.

### **11. Укажите, какие из перечисленных атак являются активными (выберите вариант ответа):**

* **a) прослушивание сетевого трафика**;
* **б) спуфинг**;
* **b) социальный инжиниринг**;
* **г) атака «отказ в обслуживании»**;
* **д) внедрение вируса**.

**Ответ:** Активными атаками являются:

* **б) спуфинг** — подделка подлинных данных с целью обмануть систему или пользователя.
* **г) атака «отказ в обслуживании»** (DoS) — воздействие на систему с целью её недоступности.
* **д) внедрение вируса** — заражение системы с целью ее разрушения или контроля.

### **12. Укажите, какие из следующих утверждений являются ошибочными:**

* **a) Нет смысла предусматривать подсистему аутентификации приложения, основанную на использовании многоразовых паролей, если многоразовые пароли уже используются и при логическом входе в систему.**
* **б) Надежная система авторизации может компенсировать недостаточную стойкость паролей пользователей, которые они использовали при входе.**
* **b) Стойкость системы защиты считается достаточной, если затраты на нее превысили запланированный уровень.**
* **г) Затраты на обеспечение безопасности информации, по крайней мере, не должны превышать величину потенциального ущерба от ее утраты.**
* **д) Иногда стойкость системы обеспечения безопасности считают достаточной, если стоимость ее преодоления злоумышленниками превосходит стоимость полученной ими выгоды.**
* **Ответ: a)** — Неправильно. Подсистема аутентификации для приложения может понадобиться, даже если используется логический вход, так как она может быть специфичной для особенностей данного приложения.
* **б)** — Это ошибочное утверждение. Надежная система авторизации не может полностью компенсировать слабость паролей пользователей, но может уменьшить риски с помощью дополнительных мер.
* **b)** — Затраты на защиту не должны превышать уровень потенциального ущерба, иначе система безопасности станет экономически нецелесообразной.

### **13. Что из перечисленного может быть секретным ключом криптосистемы (выберите вариант ответа):**

* **a) геометрическая фигура**;
* **б) сборник детских сказок**;
* **b) картина**;
* **г) число 5.**

**Ответ: tất cả**

**14. В каких из перечисленных ниже средств обеспечения безопасности используется шифрование (выберите вариант ответа):**

* **a) аутентификация** — да, в аутентификации может использоваться шифрование, например, для проверки подлинности через протоколы вроде TLS.
* **б) авторизация** — обычно шифрование не используется непосредственно для авторизации, однако оно может быть частью процесса в контексте защищенного канала.
* **b) протокол NAT** — нет, NAT (Network Address Translation) не использует шифрование.
* **г) защищенный канал** — да, защищенные каналы, такие как HTTPS, используют шифрование для защиты передаваемых данных.
* **д) сетевой экран прикладного уровня** — нет, сетевой экран (или фаервол) не занимается шифрованием, он фильтрует трафик.
* **e) фильтрующий маршрутизатор** — нет, фильтрующий маршрутизатор не использует шифрование, он управляет маршрутизацией и фильтрацией трафика.
* **ж) цифровая подпись** — да, цифровые подписи используют криптографию и шифрование для обеспечения целостности данных и подлинности отправителя.

**Ответ: a, б, г, д, ж**

### **15. Какую роль в обеспечении безопасности компьютерной сети играет протокол NAT?**

**Ответ:** Протокол **NAT** (Network Address Translation) Скрывает внутреннюю структуру сети.

### **16. Вставьте пропущенные слова («открытый» или «закрытый») в следующее предложение:**

«Сертификат может быть представлен в форме, состоящей из трех частей: во-первых, **открытой** части; во-вторых, той же информации, зашифрованной **закрытым** ключом сертифицирующей организации; в-третьих, части, представляющей собой первые две части, зашифрованные **закрытым** ключом владельца».

### **17. Установите соответствие следующих терминов на русском языке (ущерб; уязвимость; вредоносное ПО; доступность; целостность; подмена содержимого пакета; распределенная атака, «отказ в обслуживании») и английском языке (Denial of Service; availability; integrity; vulnerability; malware; impact; spoofing; DDoS).**

* **ущерб** — **impact**
* **уязвимость** — **vulnerability**
* **вредоносное ПО** — **malware**
* **доступность** — **availability**
* **целостность** — **integrity**
* **подмена содержимого пакета** — **spoofing**
* **распределенная атака, «отказ в обслуживании»** — **DDoS** (Distributed Denial of Service)
* **отказ в обслуживании** — **Denial of Service (DoS)**

### **18. Укажите, какие из нижеперечисленных свойств определяют одностороннюю функцию Y(x) (выберите вариант ответа):**

* **a) Y(x) чрезвычайно сложно вычислить для любого входного значения х;**
* **б) Y(x) просто вычисляется для любого входного значения х;**
* **b) аргумент х легко вычислить по известному Y;**
* **г) вычисление х по известному Y чрезвычайно затруднено;**
* **д) вычисление х по известному Y абсолютно невозможно;**
* **e) значения функции от близких значений аргументов не должны значительно различаться.**

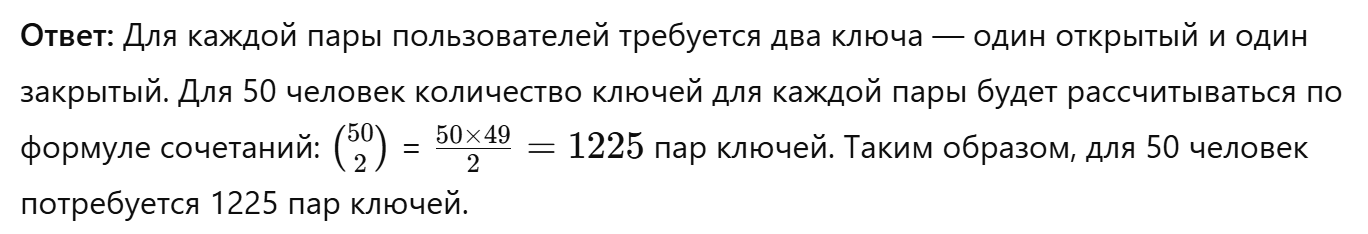
**Ответ:** **б, г**

### **19. Поясните назначение алгоритма Диффи-Хеллмана (выберите вариант ответа):**

* **a) решает проблему передачи секретного ключа по открытому каналу;**
* **б) это то же самое, что и алгоритм RSA;**
* **в) смягчает проблему масштабируемости распределения ключей.**

**Ответ:** **a) в**

### **20. Сколько ключей требуется для секретной переписки 50 человек «каждый с каждым», использующих алгоритм RSA?**



### **21. Какие из следующих утверждений правильные (выберите вариант ответа):**

* **a) открытый ключ нужно защищать от подглядывания;**
* **б) открытый ключ нужно защищать от подмены;**
* **b) теоретически возможно зашифровать текст одним ключом, а расшифровать другим, который абсолютно никак не связан с первым;**
* **г) алгоритм RSA основан на использовании функции разложения произведения большого числа на сомножители.**

**Ответ:**

* **б)** — Открытый ключ нужно защищать от подмены, чтобы предотвратить атаки типа "человек посередине" (man-in-the-middle).
* **г)** — Это правильное утверждение. RSA основывается на трудности разложения больших чисел на простые множители, что делает его безопасным при правильном использовании.

### **22. В чем состоит ручная синхронизация паролей? Варианты ответов:**

* **a) администратор синхронизирует значения БД паролей на разных серверах сети;**
* **б) ручная процедура приведения всех паролей пользователя к единому значению;**
* **b) использование одного и того же пароля для доступа к разным по степени защищенности сервисам.**

**Ответ:** b

### **23. Поясните, что представляют собой аутентификаторы из разряда «что-то знаю» (выберите вариант ответа):**

* **a) многоразовый пароль;**
* **б) одноразовый пароль, сгенерированный устройством;**
* **b) преобразование пользователем в соответствии с некоторым правилом символов, выводимых системой на экран, и использование их в качестве пароля;**
* **г) информация о месте и времени встречи.**

**Ответ:** **a) в, г**

**24. Отметьте недостатки аутентификации с использованием многоразовых паролей (выберите вариант ответа):**

* **a) возможность разгадывания пароля, если он слишком короткий** — да, короткие пароли легче взломать.
* **б) необходимость передачи пароля по сети в открытом виде** — да, если не используется шифрование, пароль может быть перехвачен.
* **b) возможность подслушивания, подглядывания, «выманивания» пароля** — да, пароли могут быть украдены при подслушивании или фишинговых атаках.
* **г) ручная синхронизация** — да, синхронизация паролей между системами может быть неудобной и рискованной.
* **д) трудность запоминания надежных паролей** — да, сложные пароли трудно запомнить.
* **e) сложность реализации** — нет, реализация аутентификации с использованием паролей довольно простая.

**Ответ:** (a, b, г, д)

### **25. Укажите, что из перечисленного содержится в сертификате (выберите вариант ответа):**

* **a) информация о владельце сертификата** — да, сертификат содержит информацию о владельце, например, имя и адрес.
* **б) открытый ключ владельца сертификата** — да, сертификат содержит открытый ключ.
* **b) закрытый ключ владельца сертификата** — нет, закрытый ключ не содержится в сертификате, он хранится у владельца в безопасном месте.
* **г) открытый ключ сертифицирующей организации** — нет, сертификат не содержит открытый ключ сертифицирующей организации.
* **д) закрытый ключ сертифицирующей организации** — нет, сертифицирующая организация использует свой закрытый ключ для подписания сертификатов, но сам ключ не содержится в сертификате.
* **e) информация о сертифицирующем центре, выпустившем данный сертификат** — да, сертификат содержит информацию о центре сертификации.

**Ответ:** В сертификате содержится **a)** информация о владельце сертификата, **б)** открытый ключ владельца сертификата, и **e)** информация о сертифицирующем центре.

**26**

### **Поясните, как убедиться в подлинности сертификата (выберите вариант ответа):**

* **a) его надо расшифровать с помощью открытого ключа владельца сертификата и сравнить с открытой информацией сообщения;** — неверно, открытый ключ владельца не используется для проверки подлинности сертификата.
* **б) его надо расшифровать с помощью закрытого ключа владельца сертификата и сравнить с открытой информацией сообщения;** — неверно, закрытый ключ владельца используется для подписания сообщений, но не для проверки сертификата.
* **b) его надо расшифровать с помощью открытого ключа сертифицирующей организации;** — да, подлинность сертификата проверяется с использованием открытого ключа сертифицирующей организации, которая подписала сертификат.
* **г) его надо послать для проверки в сертифицирующий центр.** — неверно, проверка подлинности сертификата выполняется с использованием открытого ключа сертифицирующей организации, а не отправкой в центр.

**Ответ:** Сначала а затем в

### **27. Основная идея процедуры единого логического входа состоит в том, что (выберите вариант ответа):**

* **a) пользователь выполняет логический вход в сеть только один раз при поступлении на работу, все остальное время система выполняет только его авторизацию;** — неверно, единого входа не достаточно для авторизации на всех сервисах.
* **б) все пользователи выполняют процедуру логического входа с одного и того же компьютера;** — неверно, процесс единого входа работает на уровне системы, а не на конкретном устройстве.
* **b) пользователь выполняет логический вход в сеть только один раз, затем результат этой аутентификации используется другими серверами или приложениями.** — да, основная цель процедуры единого логического входа заключается в том, чтобы один вход был достаточен для доступа ко всем нужным ресурсам.

**Ответ:** Основная идея заключается в **b)**, когда пользователь выполняет единую аутентификацию и использует результат для доступа к разным сервисам.

### **28. Укажите цели использования электронной подписи (выберите вариант ответа):**

* **a) доказательство целостности сообщения;** — да, электронная подпись подтверждает, что сообщение не было изменено.
* **б) обеспечение конфиденциальности сообщения;** — нет, конфиденциальность обеспечивается с помощью шифрования, а не электронной подписи.
* **b) доказательство авторства сообщения.** — да, электронная подпись служит доказательством того, что сообщение подписано конкретным человеком.

**Ответ:** а,с

### **29. Пояснение, что из перечисленного характеризует дискреционный метод управления доступом (DAC) и мандатный метод (MAC):**

* **a) описание прав доступа дается в виде списков ACL** — это характерно для **дискреционного метода** управления доступом. В этом методе владельцы объектов могут определять, кто имеет доступ к объектам через списки контроля доступа (ACL).
* **б) право назначать права на доступ к объектам делегируются отдельным пользователям — владельцам объектов** — это также относится к **дискреционному методу**. В данном случае владельцы объектов могут делегировать права доступа другим пользователям.
* **b) данная система управления доступом страдает от невозможности гарантированно проводить общую политику** — это также относится к **дискреционному методу**, поскольку в этом методе отсутствуют централизованные политические механизмы, и доступ может быть ограничен только владельцем объекта.
* **г) права доступа отдельного пользователя описываются АСЕ** — это относится к **дискреционному методу**. В этом случае доступ описывается через записи в списке контроля доступа (ACE), где для каждого объекта или ресурса определены права доступа для пользователей.
* **д) решение о предоставлении права доступа принимается операционной системой на основе правила** — это характерно для **мандатного метода** (MAC), где операционная система или администратор принимает решения, исходя из политики безопасности, и пользователи не могут самостоятельно назначать права доступа.
* **e) субъект может по своему усмотрению передать часть своих полномочий другим субъектам** — это свойственно **дискреционному методу** управления доступом, где владельцы ресурсов могут делегировать доступ другим пользователям.
* **ж) данная система управления доступом позволяет гарантированно проводить общую политику** — это свойственно **мандатному методу** (MAC), так как доступ регулируется центральной политикой безопасности и не зависит от воли владельцев объектов.

**Ответ:**

* **Дискреционный метод** (DAC): a, б, b, г, e
* **Мандатный метод** (MAC): д, ж

### **30. Основные функции файервола:**

* **a) аутентификация** — нет, файервол не выполняет аутентификацию.
* **б) авторизация** — нет, файервол не осуществляет авторизацию пользователей.
* **b) аудит** — нет, файервол не предназначен для аудита (хотя может записывать логи трафика).
* **г) фильтрация трафика** — да, это основная функция файервола — фильтрация трафика, разрешение или блокирование пакетов на основе установленных правил.

**Ответ:** в, **г)**

### **31. Как может выглядеть запись в расширенном списке доступа, запрещающая передачу сообщений ICMP «Перенаправление маршрута» от любого хоста к хостам подсети 145.8.146.0/24?**

Для того чтобы запретить передачу сообщений ICMP типа «Перенаправление маршрута» (Type 5) от любого хоста к подсети 145.8.146.0/24, запись в расширенном списке доступа может выглядеть так:

access-list 100 deny icmp any 145.8.146.0 0.0.0.255 redirect  
access-list 100 permit ip any any

Здесь:

* deny icmp any 145.8.146.0 0.0.0.255 redirect — запрещает ICMP сообщения типа «Перенаправление маршрута» (Type 5) от любого хоста к подсети 145.8.146.0/24.
* permit ip any any — разрешает весь другой трафик.

Ответ: access-list 120 deny ICMP any 145.8.146.0 0.0.0.255 eq 5.

### **32. Что означает данный список доступа:**

access-list 2 permit 93.8.25.2 0.0.0.0  
access-list 2 deny 93.8.25.0 0.0.0.255

* Первая запись разрешает доступ от хоста с IP-адресом **93.8.25.2** (маска 0.0.0.0 означает точное совпадение IP-адреса).
* Вторая запись запрещает доступ к подсети **93.8.25.0/24** (маска 0.0.0.255 означает, что блокируются все IP-адреса с 93.8.25.x).

Таким образом, Разрешить прохождение через маршрутизатор пакетов хоста 93.8.25.2, запрещая передачу пакетов, отправляемых любым другим хостом подсети 93.8.25.0/24.

### **33. Какие из следующих утверждений о технологии NAT справедливы?**

* **a) устройство, поддерживающее NAT, заменяет внешние IP-адреса пакетов, которые использовались при маршрутизации пакета через Интернет, внутренними** — да, это основная функция NAT, замена внутренних IP-адресов на внешний публичный адрес при выходе в Интернет.
* **б) устройство, поддерживающее NAT, фильтрует входящий трафик, отбрасывая пакеты с частными IP-адресами назначения** — да, NAT фильтрует пакеты с частными IP-адресами, поскольку эти адреса не могут быть использованы в Интернете.
* **в) причина обращения к технологии NAT — дефицит адресов IPv4** — да, NAT помогает решить проблему дефицита публичных IPv4-адресов, позволяя нескольким устройствам использовать один публичный IP-адрес.
* **г) причина обращения к технологии NAT — скрытие адресов хостов для повышения безопасности сети** — да, NAT скрывает внутренние IP-адреса хостов от внешнего мира, что повышает безопасность сети.

**Ответ:** **a, в, г** верны.

### **34. Какова должна быть защита общедоступного сервера (компьютера-бастиона)?**

* **a) поскольку доступ к этому компьютеру открыт, его помещают в демилитаризованную зону, поэтому он не требует защиты** — нет, компьютер-бастион должен быть защищен, даже если он расположен в демилитаризованной зоне.
* **б) уровень защиты компьютера-бастиона такой же, как у серверов внутренней сети** — нет, компьютер-бастион должен быть защищен гораздо более строго.
* **поль) компьютер-бастион должен быть особенно тщательно защищен от внешних злоумышленников** — да, он должен иметь строгую защиту, так как является уязвимой точкой для атак.
* **г) правила, определенные для компьютера-бастиона по доступу к ресурсам внутренней сети, должны быть более строгими, чем правила, регламентирующие доступ к нему внешних пользователей** — да, так как компьютер-бастион является уязвимым и требует более строгого контроля для доступа к внутренним ресурсам.

**Ответ:** в**)** и **г)** верны.

### **35. В чем состоят главные отличия системы обнаружения вторжений (IDS) от файерволов с запоминанием состояния сеанса?**

* **a) IDS не блокирует подозрительный трафик** — да, IDS не блокирует трафик, а лишь обнаруживает и сообщает о подозрительных событиях.
* **б) IDS анализирует не только события, связанные с прохождением трафика, но и другие подозрительные события в сети** — да, IDS может анализировать и другие события, такие как аномалии в поведении пользователей или системы.
* **b) IDS не выполняет журнализацию событий** — неверно, IDS обычно выполняет журналирование событий для анализа и расследования.
* **г) в отличие от файерволов, системы IDS всегда являются исключительно программными** — неверно, IDS могут быть как программными, так и аппаратными.

**Ответ:** **a)** и **б)** верны.

### **36. Справедливо ли следующее утверждение: «Прокси-сервер всегда работает в режиме запоминания состояния сеанса»?**

**Ответ:** Да

### **37. Какие функции системы безопасности из перечисленных направлены на обеспечение подотчетности (выберите вариант ответа):**

* **a) авторизация** — не совсем, авторизация направлена на проверку прав доступа, а не на обеспечение подотчетности.
* **б) аудит** — да, аудит помогает отслеживать действия пользователей и системы, что способствует подотчетности.
* **b) протоколирование событий** — да, это важный аспект обеспечения подотчетности, так как позволяет фиксировать все важные события.
* **г) мониторинг** — да, мониторинг помогает отслеживать текущие события и действия, что также способствует подотчетности.
* **д) журнализация событий** — да, журнализация событий фиксирует важные действия и события, что важно для подотчетности.

**Ответ:** **б) аудит, b) протоколирование событий, г) мониторинг, д) журнализация событий**

### **38. В IDS для обнаружения вторжений применяются несколько типов правил:**

* **a) правила, основанные на сигнатуре атаки** — да, это основной тип правил, основанных на известных сигнатурах атак.
* **б) правила доступа на основе меток безопасности объекта и субъекта** — это скорее относится к методам контроля доступа, а не IDS.
* **b) правила, основанные на анализе протоколов** — да, анализ протоколов также используется для выявления аномалий и вторжений.
* **г) правила, основанные на статистических аномалиях трафика** — да, это относится к методам обнаружения на основе анализа статистики трафика, например, выявление аномального трафика.

**Ответ:** **a) правила, основанные на сигнатуре атаки, b) правила, основанные на анализе протоколов, г) правила, основанные на статистических аномалиях трафика**

### **39. В чем состоит главная уязвимость протокола IP?**

* **a) заголовок IP-пакета переносит адреса источника и назначения в незашифрованном виде** — да, это основная уязвимость, так как IP-адреса передаются открыто и могут быть подменены злоумышленниками.
* **б) он использует широковещательные адреса назначения** — это не уязвимость протокола, а особенность.
* **b) он позволяет каждому узлу Интернета взаимодействовать с каждым без предварительного установления соединения** — это тоже не уязвимость, а нормальная работа протокола.
* **г) он поддерживает фрагментацию пакетов** — это не уязвимость, хотя фрагментация может быть использована в некоторых атаках.

**Ответ:** в, г

### **40. С помощью протокола ICMP злоумышленник может (выберите вариант ответа):**

* **a) определить, что некоторый хост находится в работоспособном состоянии** — да, это возможно с помощью запросов **ping** (ICMP Echo Request), которые могут использоваться для проверки доступности хоста.
* **б) организовать DoS-атаку** — да, это возможно с помощью ICMP, например, в атаке **Ping of Death** или **Smurf Attack**.
* **b) перенаправить маршрут** — да, злоумышленник может использовать ICMP для атаки на маршруты с помощью сообщения ICMP **Redirect**.
* **г) узнать, через какие промежуточные маршрутизаторы проходит маршрут до некоторого конечного узла** — да, это возможно с помощью команды **traceroute**, которая использует ICMP для выявления маршрута.

**Ответ:** **a) определить, что некоторый хост находится в работоспособном состоянии, б) организовать DoS-атаку, b) перенаправить маршрут, г) узнать, через какие промежуточные маршрутизаторы проходит маршрут до некоторого конечного узла**

### **41. С какой целью злоумышленник должен подавить отправку АСК-сегментов на атакуемый сервер в ходе атаки SYN Flood?**

* **a) чтобы скрыть свой IP-адрес** — это не является основной целью атаки SYN Flood.
* **б) чтобы открытые соединения оставались незавершенными** — да, это основная цель SYN Flood атаки. Злоумышленник отправляет SYN-запросы и не завершает соединение, что приводит к исчерпанию ресурсов сервера.
* **b) чтобы закрыть открытые соединения** — нет, цель атаки SYN Flood заключается в сохранении незавершенных соединений.

**Ответ:** **б) чтобы открытые соединения оставались незавершенными**

### **42. Чем атака DNS-спуфинга отличается от атаки отравления DNS-кэша?**

* **a) ничем, это разные названия одной и той же атаки** — нет, это не так.
* **б) в результате атаки отравления DNS-кэша DNS-сервер терпит крах, в то время как атака DNS-спуфинга к краху сервера не приводит** — это не совсем так, отравление кэша может не всегда приводить к сбою сервера.
* **b) в атаке DNS-спуфинга ложный ответ передается клиенту, а в атаке отравления DNS-кэша - DNS-серверу** — да, это правильное объяснение. В атаке DNS-спуфинга злоумышленник подменяет информацию для клиента, а в атаке отравления DNS-кэша — для DNS-сервера.
* **г) в атаке DNS-спуфинга ложный ответ передается DNS-серверу, а в атаке отравления DNS-кэша - клиенту** — это неверно, так как в DNS-спуфинге ложный ответ идет на клиент, а не на сервер.

**Ответ:** **b) в атаке DNS-спуфинга ложный ответ передается клиенту, а в атаке отравления DNS-кэша - DNS-серверу**

### **43. Каким образом можно «подделать» маршрутное объявление BGP, которое вы передаете вашему соседу, если ваша автономная система является транзитной для этого маршрута, а вы хотите, чтобы сосед не использовал этот маршрут для передачи трафика?**

**Ответ: а, в**

**44. С какой целью в семействе протоколов IPSec функции обеспечения целостности включены в два протокола - AH и ESP?**

**Ответ:**

* б

### **45. Какую цель обычно преследует злоумышленник, используя эффект переполнения стека?**

**Ответ:**

* **б) поместить в стек вредоносный код и передать ему управление** — переполнение стека происходит, когда программа записывает больше данных, чем выделено для стека, что может быть использовано для внедрения вредоносного кода и перенаправления управления на его выполнение.

### **46. Антивирусная программа, работающая по методу сигнатур, может (выберите вариант ответа):**

**Ответ:**

* **a) выявлять только известные вредоносные коды** — антивирусы, работающие по методу сигнатур, анализируют файлы на наличие известных паттернов, которые идентифицируют вирусы, червей, троянов и другие вредоносные программы, но не могут эффективно обнаруживать новые или модифицированные угрозы.

### **47. Могут ли куки, переданные веб-сервером вашему веб-браузеру, заразить ваш компьютер вирусом?**

**Ответ:**

* **Ответ: нет.** Куки сами по себе не могут заразить компьютер вирусом. Это текстовые файлы, которые сохраняются в браузере для хранения данных о пользователе (например, предпочтения или состояние сеанса). Однако если веб-сайт содержит вредоносный код или использует куки в качестве части атаки (например, XSS или CSRF), это может привести к небезопасному поведению.

### **48. С какой целью веб-сервер передает куки веб-браузеру клиента?**

**Ответ:**

* **б) для сохранения состояния сеанса пользователя** — куки часто используются для хранения информации о сеансе пользователя, чтобы сервер мог идентифицировать его на протяжении всего взаимодействия. Это позволяет поддерживать продолжение сеанса, например, в интернет-магазинах или на сайтах с авторизацией.

### **49. Какое утверждение относительно протокола HTTPS является правильным?**

**Ответ:**

* **a) протокол HTTPS использует защищенный канал SSL для предотвращения атак на сеанс между веб-браузером и веб-сервером** — HTTPS использует SSL/TLS (Transport Layer Security) для шифрования канала и защиты данных от атак, таких как прослушивание и подделка.

### **50. Что делает облачные вычисления более безопасными, чем традиционные?**

**Ответ:**

* **г) централизация вычислительных ресурсов** — централизация вычислительных ресурсов в облаке позволяет лучше управлять безопасностью, поскольку специалисты могут использовать более строгие меры защиты и протоколы в одной централизованной инфраструктуре, чем на отдельных физических устройствах в традиционных системах. Это также облегчает управление обновлениями и мониторингом безопасности.

**ОТВЕТЫ:**

