

Экзаменационные вопросы

**Курс: «Основы сетей»**

**Тема: Основы сетей**

**Вопросы:**

1. Какие виды сетей бывают и их назначение?
2. Что такое локальные адреса и сетевые IP адреса?
3. Что такое маска сети?
4. Какие виды особых адресов существует?
5. Что такое технология бесклассовой междоменной маршрутизации?
6. Что такое DHCP, какие режимы в нем есть?
7. Опишите алгоритм динамического назначения адресов
8. Опишите процесс маршрутизации из точки A в точку B в интернете
9. Опишите три вида NAT: статическая, динамическая и перегрузка
10. Опишите процесс установки соединения с удаленным сервером (трехэтапный обмен данными)
11. Что такое DNS? Как работает DNS сервер?
12. Что обозначают данные типы записей: А запись, NS запись, CNAME запись, MX запись.
13. **Какие виды сетей бывают и их назначение?**

* Локальная сеть (LAN): Локальная сеть представляет собой сеть, охватывающую небольшую географическую область, обычно в пределах одного здания или небольшого набора зданий.
* Глобальная сеть (WAN): Глобальная сеть охватывает большие географические области, такие как города, страны или даже весь мир. Она предоставляет связь между удаленными локальными сетями и обеспечивает передачу данных на большие расстояния.
* Метрополитенская сеть (MAN): Метрополитенская сеть охватывает город или регион и предоставляет связь между локальными сетями в этой области. Она обычно используется провайдерами интернет-услуг для предоставления доступа к интернету внутри города.
* Беспроводная сеть: использует радиоволны или другие беспроводные технологии для связи между устройствами без необходимости проводного подключения. Примерами беспроводных сетей являются Wi-Fi сети и сотовые сети.
* Виртуальная частная сеть (VPN): VPN обеспечивая безопасное соединение между удаленными пользователями или местоположениями. VPN обычно используется для обеспечения конфиденциальности и безопасности при доступе к ресурсам через ненадежную сеть
* Сеть хранения данных (SAN): — это выделенные сети, которые обеспечивают высокоскоростной доступ к общим устройствам хранения, таким как дисковые массивы или библиотеки лент. Они обеспечивают эффективное хранение, восстановление и резервное копирование данных в корпоративных средах.
* Кампусная сеть (CAN): используется для взаимодействия нескольких LAN в определенной географической зоне, такой как университетский кампус или корпоративный центр.

1. **Что такое локальные адреса и сетевые IP адреса?**

Локальные адреса и сетевые IP-адреса используются в компьютерных сетях для идентификации устройств, подключенных к сети.

1. **Локальные адреса,** также известные как частные адреса, используются в локальной сети для уникальной идентификации устройств. Эти адреса не маршрутизируются в Интернете и предназначены для использования в частной сетевой среде, такой как домашняя или офисная сеть. Локальные адреса определяются в диапазонах частных адресов IPv4
2. **Сетевые IP-адреса**, также называемые общедоступными или глобальными адресами, используются для идентификации устройств в Интернете. Эти адреса являются глобально уникальными и маршрутизируемыми, что обеспечивает связь между устройствами в разных сетях по всему миру. Сетевые IP-адреса назначаются поставщиками услуг Интернета или другими органами по распределению адресов.  
   Сетевые IP-адреса основаны на схеме адресации IPv4 или IPv6. Адреса IPv4 обычно выражаются в виде четырех наборов чисел, разделенных точками, например 192.0.2.123. Однако из-за ограниченной доступности адресов IPv4 произошел переход к IPv6, в котором используется другой формат адресации, позволяющий использовать гораздо больший пул уникальных адресов.  
   Сетевые IP-адреса используются устройствами для связи через Интернет, доступа к веб-сайтам, отправки и получения данных и установления соединений с серверами или другими устройствами в сети.

Таким образом, локальные адреса используются для связи в частной сети, а сетевые IP-адреса используются для связи через Интернет между различными сетями.

1. **Что такое маска сети?**

Cетевая маска — это фундаментальное понятие в компьютерных сетях, которое помогает определить, какая часть IP-адреса представляет сеть, а какая — хост. Он используется вместе с IP-адресами для разделения сети на подсети и обеспечения связи между устройствами.

Сетевая маска, также известная как маска подсети, представляет собой 32-битное значение, сопровождающее IP-адрес. Он служит фильтром, определяющим границу между сетевой и хостовой частями. Сетевая маска выражается в том же формате, что и IP-адрес, и состоит из четырех октетов.

Сетевая маска помогает устройствам определить, находится ли IP-адрес назначения в той же сети или в другой. Если два устройства имеют IP-адреса в одной сети, они могут взаимодействовать напрямую без необходимости маршрутизации через другие сети. Если IP-адрес назначения принадлежит другой сети, устройство отправит данные на маршрутизатор, который перенаправит их в соответствующую сеть на основе своей таблицы маршрутизации.

Cетевая маска — это двоичное значение, связанное с IP-адресом, которое определяет сетевую и узловую части адреса. Это позволяет устройствам определять, находится ли IP-адрес в их локальной сети или в другой сети, облегчая маршрутизацию данных по сетям.

1. **Какие виды особых адресов существует?**

* Широковещательный
* Сетевой адрес
* Адрес обратной связи
* Частные IP-адреса
* Локальный адрес

1. **Что такое технология бесклассовой междоменной маршрутизации?**
2. **Что такое DHCP, какие режимы в нем есть?**

**DHCP или протокол динамической конфигурации хоста** — это сетевой протокол, упрощающий процесс назначения IP-адресов и других параметров конфигурации сети устройствам в сети. Это устраняет необходимость ручной настройки IP-адресов, масок подсети, шлюзов по умолчанию и других сетевых параметров.

DHCP действует как посредник между устройством и сетью, к которой оно подключено. Когда устройство подключается к сети, оно отправляет DHCP-запрос, чтобы найти доступный IP-адрес и другую информацию о конфигурации сети.

**DHCP** может работать в 3 режимах:

* Ручное назначение
* Автоматическое распределение
* Динамическое распределение

1. **Опишите алгоритм динамического назначения адресов?**
2. Обнаружение DHCP: когда устройство подключается к сети, оно передает в сеть сообщение DHCP, запрашивая IP-адрес и другие сведения о конфигурации.
3. Предложение DHCP
4. Запрос DHCP: устройство получает одно или несколько предложений от разных серверов DHCP и выбирает один из них. Затем он отправляет сообщение запроса DHCP на выбранный DHCP-сервер, указывая, что он принимает предложенный IP-адрес и конфигурацию.
5. Подтверждение DHCP: сервер DHCP получает запрос DHCP и отвечает сообщением подтверждения DHCP, подтверждая назначение запрошенного IP-адреса и предоставляя дополнительную информацию о конфигурации сети.
6. Аренда IP-адреса: устройство теперь имеет IP-адрес и другие сетевые настройки. DHCP-сервер также назначает время аренды, которое указывает, как долго устройство может использовать назначенный IP-адрес. Устройство обычно продлевает аренду до истечения срока ее действия, чтобы продолжать использовать тот же IP-адрес.
7. **Опишите процесс маршрутизации из точки A в точку B в интернете**

Маршрутизация — это процесс направления пакетов данных из точки-источника (точка А) в точку назначения (точка Б)

Процесс маршрутизации:

1. Исходное устройство (точка A):
   * Исходное устройство инициирует передачу данных, например отправку запроса на доступ к веб-сайту, разбивает данные на более мелкие пакеты
2. Локальная сеть:
   * Исходное устройство сначала проверяет, находится ли IP-адрес назначения в его локальной сети. Если это так, отправляет пакет непосредственно на целевое устройство в локальной сети.
   * Если IP-адрес назначения находится за пределами локальной сети, исходное устройство ищет шлюз по умолчанию.
3. Таблица маршрутизации:
   * Исходное устройство сверяется со своей таблицей маршрутизации, которая представляет собой список IP-адресов и связанных с ними маршрутизаторов следующего перехода.
   * Таблица маршрутизации помогает определить лучший маршрутизатор следующего перехода для пересылки пакета на основе IP-адреса назначения.
4. Маршрутизатор следующего перехода:
   * Исходное устройство отправляет пакет маршрутизатору следующего перехода, указанному в таблице маршрутизации.
   * Пакет инкапсулируется с новыми заголовками, которые включают исходный и целевой IP-адреса интерфейса маршрутизатора.
   * Затем пакет передается по локальной сети для достижения маршрутизатора следующего перехода.
5. Промежуточные маршрутизаторы:
   * Пакет проходит через ряд промежуточных маршрутизаторов, каждый из которых принимает решение о пересылке на основе своей собственной таблицы маршрутизации.
   * Каждый маршрутизатор проверяет IP-адрес назначения пакета и определяет лучший маршрутизатор следующего перехода, чтобы направить его ближе к месту назначения.
   * Пакет переходит от маршрутизатора к маршрутизатору, пока не достигнет маршрутизатора, который напрямую подключен к сети, в которой находится IP-адрес назначения.
6. Целевая сеть:
   * Пакет достигает маршрутизатора, который напрямую подключен к сети назначения.
   * Маршрутизатор доставляет пакет на целевое устройство в этой сети.
7. Целевое устройство (точка B):
   * Устройство назначения получает пакет и обрабатывает данные.
8. **Опишите три вида NAT: статическая, динамическая и перегрузка**
9. Статический NAT:
   * При использовании статического NAT каждый раз, когда устройство с определенным частным IP-адресом подключается к Интернету, оно всегда использует один и тот же общедоступный IP-адрес.
10. Динамический NAT:
    * Динамический NAT позволяет нескольким устройствам в частной сети использовать пул общедоступных IP-адресов.
    * Когда устройство в частной сети инициирует связь с Интернетом, ему назначается доступный общедоступный IP-адрес из пула.
    * Назначенный общедоступный IP-адрес остается связанным с устройством в течение сеанса или указанного периода ожидания.
    * Динамический NAT полезен, когда доступно ограниченное количество общедоступных IP-адресов, а устройствам в частной сети требуется периодический доступ в Интернет, не требующий фиксированного общедоступного IP-адреса.
11. Перегрузка NAT (PAT):
    * Перегрузка NAT, или преобразование адресов портов (PAT), является расширением динамического NAT.
    * PAT позволяет нескольким устройствам в частной сети использовать один общедоступный IP-адрес.
    * Перегрузка NAT обычно используется в домашних сетях, малых предприятиях и интернет-провайдерах (ISP), где не хватает общедоступных IP-адресов.
12. **Опишите процесс установки соединения с удаленным сервером (трехэтапный обмен данными)**

Процесс установки соединения с удаленным сервером включает трехэтапный обмен данными, который известен как "трехэтапное рукопожатие"

Шаг 1: Клиент отправляет серверу пакет с установленным флагом SYN (синхронизация). Этот пакет содержит случайный номер, который представляет собой начальную позицию данных, которые клиент ожидает получить от сервера.

1. Шаг 2: Подтверждение соединения (SYN+ACK): Сервер получает пакет SYN от клиента и отправляет обратно пакет с установленными флагами SYN и ACK (подтверждение). Пакет SYN содержит случайный номер последовательности, а пакет ACK содержит номер подтверждения (acknowledgment number), который равен номеру последовательности клиента плюс один.
2. Шаг 3: Подтверждение установки соединения (ACK): Клиент получает пакет SYN+ACK от сервера и отправляет последний пакет подтверждения с установленным флагом ACK. Пакет ACK содержит номер подтверждения, равный номеру последовательности сервера плюс один.

После успешного выполнения трехэтапного рукопожатия клиент и сервер могут начать передачу данных в обоих направлениях. Пакеты данных, отправляемые между клиентом и сервером, содержат номера последовательности и подтверждения для обеспечения надежной доставки и контроля целостности данных.

Трехэтапное рукопожатие позволяет клиенту и серверу установить соединение, обменяться необходимой информацией для начала обмена данными и убедиться в готовности обоих участников к передаче данных. Это важный механизм TCP/IP для обеспечения надежности и стабильности соединений в сетях.

1. **Что такое DNS? Как работает DNS сервер?**

**DNS-сервер или сервер системы доменных имен** — это важнейший компонент Интернета, который переводит удобочитаемые доменные имена в числовые IP-адреса, используемые компьютерами для связи друг с другом. Он действует как телефонная книга или каталог для Интернета, помогая устройствам находить правильные IP-адреса, связанные с доменными именами, к которым они хотят получить доступ.

Когда мы вводим доменное имя, такое как «abracatabra.ru», в свой веб-браузер, DNS-сервер отвечает за преобразование этого доменного имени в соответствующий IP-адрес. Это преобразование необходимо, поскольку компьютеры взаимодействуют с использованием IP-адресов, которые представляют собой числовые представления, однозначно идентифицирующие устройства в сети.

Вот как работают DNS-серверы:

1. **DNS-запрос**. Когда мы вводим доменное имя в веб-браузере или выполняете какие-либо действия в сети, связанные с доменными именами, наше устройство отправляет DNS-запрос на DNS-сервер. Запрос DNS содержит доменное имя, которое необходимо разрешить.
2. DNS-сервер, который получает запрос, может не иметь IP-адрес запрошенного в своем кэше. В этом случае он действует как преобразователь. Он начинает с проверки собственного кеша на наличие ранее разрешенного IP-адреса для доменного имени.
3. Если DNS-сервер не имеет запрошенного IP-адреса в своем кеше, ему необходимо найти информацию с других DNS-серверов. Он связывается с другими DNS-серверами в процессе, называемом «итеративным» разрешением. Сервер может начать с запроса одного из корневых DNS-серверов, которые являются DNS-серверами самого высокого уровня, ответственными за всю систему доменных имен.
4. DNS-сервер использует иерархическую структуру для поиска IP-адреса. Он запрашивает корневой DNS-сервер, чтобы получить адрес авторитетного DNS-сервера, ответственного за домен верхнего уровня запрошенного доменного имени (например, .com, .org, .net).
5. DNS-сервер связывается с полномочным DNS-сервером , чтобы получить IP-адрес DNS-сервера, ответственного за конкретное доменное имя. Он запрашивает авторитетный DNS-сервер, на котором хранится конкретный IP-адрес, связанный с запрошенным доменным именем.
6. **Ответ DNS**: как только DNS-сервер получает IP-адрес от авторитетного DNS-сервера, он кэширует результат на определенный период времени и отправляет ответ обратно на устройство, которое инициировало DNS-запрос. Теперь устройство знает IP-адрес, связанный с запрошенным доменным именем.
7. **Что обозначают данные типы записей: А запись, NS запись, CNAME запись, MX запись.**

Данные типы записей относятся к системе доменных имён (DNS) и используются для различных целей при настройке доменных имён. Вот их объяснение:

1. Запись A используется для связывания доменного имени с IP-адресом.
2. Запись NS определяет авторитетные и вспомогательные серверы имен для доменного имени
3. Запись CNAME используется для создания псевдонима для доменного имени.
4. Запись MX определяет серверы, которые принимают и обрабатывают электронную почту для доменного имени.