1. Что такое кэш ARP? Какие типы записей могут содержаться в кэше

ARP?

Канальный уровень предназначен для обеспечения взаимодействия сетей

на физическом уровне и контроля за ошибками передачи данных. Связь ме-

жду канальным и сетевым уровнем обеспечивается протоколами преобразо-

вания между сетевыми и физическими адресами – ARP и InARP.

Кэш ARP (Address Resolution Protocol) - это таблица, которая содержит соответствия между IP-адресами и MAC-адресами устройств в локальной сети. Когда устройство отправляет сетевой пакет на другое устройство в сети, оно должно знать MAC-адрес получателя. Для этого оно отправляет запрос ARP на локальную сеть, чтобы узнать MAC-адрес устройства по его IP-адресу.

Записи в кэше ARP могут быть двух типов:

1. Динамические записи - создаются автоматически при запросе ARP и хранятся в кэше некоторое время (обычно несколько минут). Эти записи обновляются, если устройство продолжает общаться в сети.

2. Статические записи - создаются вручную администратором и не удаляются из кэша до тех пор, пока их не удалит администратор. Эти записи используются для сохранения соответствий между IP-адресами и MAC-адресами устройств, которые не меняют своих адресов.

2. Какому классу IP-адресов принадлежат адреса 10.11.0.1, 127.1.1.1?

Адрес 10.11.0.1 принадлежит классу A, так как первый октет находится в диапазоне от 1 до 126, что соответствует классу A. Адрес 127.1.1.1 также принадлежит классу A, но он является адресом петли обратной связи (loopback), который используется для проверки сетевых настроек устройства.

IP-адреса делятся на 5 классов: A, B, C, D и E. Класс IP-адреса определяется первым октетом адреса.

Класс A: адреса с первым октетом в диапазоне от 1 до 126. В таких адресах первый октет используется для идентификации сети, а оставшиеся три октета для идентификации устройства в этой сети. В классе A может быть до 126 различных сетей, каждая из которых может содержать до 16 миллионов устройств.

Класс B: адреса с первым октетом в диапазоне от 128 до 191. В таких адресах первые два октета используются для идентификации сети, а оставшиеся два октета для идентификации устройства в этой сети. В классе B может быть до 16 384 различных сетей, каждая из которых может содержать до 65 536 устройств.

Класс C: адреса с первым октетом в диапазоне от 192 до 223. В таких адресах первые три октета используются для идентификации сети, а оставшийся один октет для идентификации устройства в этой сети. В классе C может быть до 2 097 152 различных сетей, каждая из которых может содержать до 256 устройств.

Класс D: адреса с первым октетом в диапазоне от 224 до 239. Эти адреса используются для многоадресной рассылки.

Класс E: адреса с первым октетом в диапазоне от 240 до 255. Эти адреса зарезервированы для будущих нужд и не используются в настоящее время.

3. Разделите адресное пространство 192.168.1.0 на четыре подсети при

помощи масок.

Для разделения адресного пространства 192.168.1.0 на четыре подсети можно использовать маску подсети /26, которая позволяет использовать 6 битов для идентификации подсети и оставляет 2 бита для идентификации устройств в каждой подсети.

1. Подсеть 1: 192.168.1.0/26 (адрес сети: 192.168.1.0, адрес широковещательной рассылки: 192.168.1.63, диапазон адресов устройств: 192.168.1.1-192.168.1.62)

2. Подсеть 2: 192.168.1.64/26 (адрес сети: 192.168.1.64, адрес широковещательной рассылки: 192.168.1.127, диапазон адресов устройств: 192.168.1.65-192.168.1.126)

3. Подсеть 3: 192.168.1.128/26 (адрес сети: 192.168.1.128, адрес широковещательной рассылки: 192.168.1.191, диапазон адресов устройств: 192.168.1.129-192.168.1.190)

4. Подсеть 4: 192.168.1.192/26 (адрес сети: 192.168.1.192, адрес широковещательной рассылки: 192.168.1.255, диапазон адресов устройств: 192.168.1.193-192.168.1.254)

4. Что такое концентратор? Объясните принцип работы концентратора.

Концентратор (hub). Устройство для объединения нескольких устройств Ethernet в общий физический сегмент.

Концентратор (hub) – это устройство, которое используется для объединения нескольких сетевых устройств в одну сеть. Принцип работы концентратора заключается в том, что он получает сигналы от всех подключенных устройств и повторяет их на все порты, кроме того, на который сигнал был получен. Таким образом, все устройства находятся в одной сети и могут обмениваться данными между собой.

Концентраторы работают на физическом уровне модели OSI и не имеют возможности фильтровать трафик или управлять его потоком. Поэтому, если в сети происходит большой объем передачи данных, то может произойти перегрузка канала связи и уменьшиться скорость передачи данных. Концентраторы часто заменяются на более современные коммутаторы, которые имеют больше возможностей для управления трафиком и повышения производительности сети.

Чем концентратор отличается от повторителя?

Концентратор и повторитель (repeater) имеют схожую функцию – усиление сигнала для передачи на большее расстояние. Однако, концентратор имеет больше портов, чем повторитель, и может объединять несколько устройств в одну сеть. Кроме того, концентратор повторяет сигналы на все порты, кроме того, на который был получен, в то время как повторитель просто усиливает сигнал и передает его дальше без изменений.

5. Что такое шлюз?

Шлюз (gateway) – это устройство или программное обеспечение, которое обеспечивает связь между различными сетями, преобразуя данные из одного протокола в другой. Шлюз может выполнять функции маршрутизации, фильтрации трафика, перевода адресов и т.д. Шлюзы используются для соединения локальных сетей с интернетом или другими удаленными сетями.

Шлюзом будем называть узел внутри подсети, который предоставляет

доступ в другую подсеть. Чаще всего в виде шлюза выступает маршрутизатор.

Схема такой маршрутизации выглядит следующим образом: задан адрес

шлюза по умолчанию. При попытке отправки пакета в сеть, узел проверяет

совпадение подсети назначения пакета с подсетью узла.

Если подсети разные, то пакет отправляется на шлюз. В простейшем

случае шлюз сравнивает сеть IP-адреса назначения с номерами сетей на

своих интерфейсах и в случае их совпадения направляет пакет в узел назначения через этот сетевой интерфейс. В противном случае он отправляет пакет в узел, указанный в качестве шлюза по умолчанию на самом шлюзе. Если такового нет, то пакет теряется.

6. Для чего предназначен протокол ICMP?

Для проверки соединений и корректного функционирования сети

обычно используется протокол ICMP. ICMP (Internet Control MessageProtocol) – протокол управляющих сообщений интернета. ICMP – протокол

сетевого уровня и работает поверх протокола IP.

Он предназначен для обмена информацией об ошибках между маршрутизаторами (шлюзами) сети и узлом-источником пакета. С помощью специальных пакетов этот протокол

сообщает о невозможности доставки пакета, превышении времени жизни, об

аномальных значениях параметров, изменении маршрута пересылки, о состоянии системы и т. п.

В простейшем случае, для проверки работоспособности сети используются два сообщения ICMP: Echo-запрос (Echo request) и Echo-ответ (Echoreply). Когда на узел приходит сообщение ICMP типа «Echo-запрос», он отправляет сообщение «Echo-ответ» на тот узел, с которого пришел запрос.

Пример реализации такого обмена представлен в утилите ping, входящей в состав почти любой сетевой ОС.