Лекция 04

Протоколы ICMP, IGMP, ARP/InARP, RARP.

Протокол ICMP

ICMP (**Internet Control Message Protocol — протокол межсетевых управляющих сообщений**) — сетевой протокол, входящий в стек протоколов TCP/IP. В основном ICMP используется для передачи сообщений об ошибках и других исключительных ситуациях, возникших при передаче данных, например, запрашиваемая услуга недоступна, или хост, или маршрутизатор не отвечают. Также на ICMP возлагаются некоторые сервисные функции.

Протокол ICMP описан в **RFC 792** (с дополнениями в **RFC 950**) и является стандартом Интернета (входит в стандарт STD 5 вместе с IP). Хотя формально ICMP использует IP (ICMP-пакеты инкапсулируются в IP пакеты), он является неотъемлемой частью IP и обязателен при реализации стека TCP/IP. Текущая версия ICMP для IPv4 называется ICMPv4. В IPv6 существует аналогичный протокол ICMPv6.

Каждое ICMP-сообщение инкапсулируется непосредственно в пределах одного IP-пакета, и, таким образом ICMP является т.н. "ненадежным" (не контролирующим доставку и её правильность). В отличие от UDP, где реализация надёжности возложена на ПО прикладного уровня, ICMP (в силу специфики применения) обычно не нуждается в реализации надёжной доставки. Тот же Ping, например, служит как раз для проверки потерь IP-пакетов на маршруте.

Примеры использования ICMP-сообщений

- **ICMP-сообщения (тип 12)** генерируются при нахождении ошибок в заголовке IP-пакета (за исключением самих ICMP-пакетов, дабы не привести к бесконечно растущему потоку ICMP-сообщений об ICMP-сообщениях).
- **ICMP-сообщения (тип 3)** генерируются маршрутизатором при отсутствии маршрута к адресату.
- Утилита Ping, служащая для проверки возможности доставки IP-пакетов, использует **ICMP-сообщения** с типом **8 (эхо-запрос)** и **0 (эхо-ответ)**.
- Утилита Traceroute, отображающая путь следования IP-пакетов, использует **ICMP-сообщения с типом 11**.
- **ICMP-сообщения с типом 5** используются маршрутизаторами для обновления записей в таблице маршрутизации отправителя.
- **ICMP-сообщения с типом 4** используются получателем (или маршрутизатором) для управления скоростью отправки сообщений отправителем.

Правила генерации ICMP-пакетов

- При потере ICMP-пакета никогда не генерируется новый.
- ICMP-пакеты никогда не генерируются в ответ на IP-пакеты с широковещательным или групповым адресом, чтобы не вызывать перегрузку в сети (так называемый «широковещательный шторм»).
- При повреждении фрагментированного IP-пакета ICMP-сообщение отправляется только после получения первого повреждённого фрагмента, поскольку отправитель всё равно повторит передачу всего IP-пакета целиком.

ICMP туннель

Скрытый канал для передачи данных, организованный между двумя узлами, использующий IP-пакеты с типом протокола ICMP (обычно echo request, echo reply).

Узлы обмениваются сообщениями echo request/echo reply, напоминающими работу утилиты ping, однако содержимое сообщений является информацией, передаваемой внутри канала. В случае, если оба узла имеют возможность принимать/отправлять запросы, передача может осуществляться любым узлом, в случае, если один из узлов находится за NAT'ом, он может только отправлять запросы (и получать ответы).

Протокол IGMP

IGMP (**Internet Group Management Protocol — протокол управления группами Интернета**) — протокол управления групповой (multicast) передачей данных в сетях, основанных на протоколе IP. IGMP используется маршрутизаторами и IP-узлами для организации сетевых устройств в группы.

IGMP используется только в сетях IPv4, так как в IPv6 групповая передача пакетов реализована через протокол Multicast Listener Discovery.

IGMP используется клиентским компьютером и соседними коммутаторами для соединения клиента и локального маршрутизатора, осуществляющего групповую передачу. Далее между локальным и удаленным маршрутизаторами используется протокол Protocol Independent Multicast (PIM), с его помощью групповой трафик направляется от видеосервера к многочисленным клиентам групповой передачи.

Согласно RFC существует три версии IGMP.

- IGMPv1 определен в RFC 1112,
- IGMPv2 — в RFC 2236
- IGMPv3 — в RFC 3376.

Основным улучшением в IGMPv3 относительно IGMPv2 является поддержка фильтрации IP-адресов. С помощью этого механизма узел может сообщить, с каких адресов он хочет получать пакеты, а с каких нет.

IGMP snooping — процесс отслеживания сетевого трафика IGMP, который позволяет сетевым устройствам канального уровня (свитчам) отслеживать IGMP-обмен между потребителями и поставщиками (маршрутизаторами) многоадресного (multicast) IP-трафика, формально происходящий на более высоком (сетевом) уровне. Эта функциональность доступна во многих управляемых коммутаторах для сети Ethernet (по крайней мере среднего и верхнего ценовых уровней), но всегда требует отдельного включения и настройки.

После включения IGMP snooping коммутатор начинает анализировать все IGMP-пакеты между подключенными к нему компьютерами-потребителями и маршрутизаторами-поставщиками multicast трафика. Обнаружив IGMP-запрос потребителя на подключение к multicast группе, коммутатор включает порт, к которому тот подключён, в список её членов (для ретрансляции группового трафика). И наоборот: услышав запрос 'IGMP Leave' (покинуть), удаляет соответствующий порт из списка группы.

Протокол ARP

ARP (**Address Resolution Protocol — протокол определения адреса**) — протокол в компьютерных сетях, предназначенный для определения MAC адреса по известному IP адресу.

Наибольшее распространение ARP получил благодаря повсеместности сетей IP, построенных поверх Ethernet, поскольку практически в 100 % случаев при таком сочетании используется ARP. В семействе протоколов IPv6 ARP не существует, его функции возложены на ICMPv6.

Описание протокола было опубликовано в ноябре 1982 года в RFC 826. ARP был спроектирован для случая передачи IP-пакетов через сегмент Ethernet. При этом общий принцип, предложенный для ARP, может, и был использован и для сетей других типов.

Существуют следующие типы сообщений ARP: запрос ARP (ARP request) и ответ ARP (ARP reply). Система-отправитель при помощи запроса ARP запрашивает физический адрес системы-получателя. Ответ (физический адрес узла-получателя) приходит в виде ответа ARP.

Принцип работы

- Узел, которому нужно выполнить отображение IP-адреса на локальный адрес, формирует ARP запрос, вкладывает его в кадр протокола канального уровня, указывая в нем известный IP-адрес, и рассылает запрос широковещательно.
- Все узлы локальной сети получают ARP запрос и сравнивают указанный там IP-адрес с собственным.
- В случае их совпадения узел формирует ARP-ответ, в котором указывает свой IP-адрес и свой локальный адрес и отправляет его уже направленно, так как в ARP запросе отправитель указывает свой локальный адрес.

Самопроизвольный ARP — такое поведение ARP, когда ARP-ответ присылается, когда в этом (с точки зрения получателя) нет особой необходимости. Самопроизвольный ARP-ответ это пакет-ответ ARP, присланный без запроса. Он применяется для определения конфликтов IP-адресов в сети: как только станция получает адрес по DHCP или адрес присваивается вручную, рассылается ARP-ответ gratuitous ARP.

Самопроизвольный ARP может быть полезен в следующих случаях:

- Обновление ARP-таблиц, в частности, в кластерных системах;
- Информирование коммутаторов;
- Извещение о включении сетевого интерфейса.

Несмотря на эффективность самопроизвольного ARP, он является особенно небезопасным, поскольку с его помощью можно уверить удалённый узел в том, что MAC-адрес какой-либо системы, находящейся с ней в одной сети, изменился и указать, какой адрес используется теперь.

Inverse ARP

Inverse Address Resolution Protocol, Inverse ARP или InARP — протокол для получения адресов сетевого уровня (например IP адресов) других рабочих станций по их адресам

канального уровня (например, DLCI в Frame Relay сетях). В основном используется во Frame Relay и ATM сетях.

ARP переводит адреса сетевого уровня в адреса канального уровня, в то же время InARP можно рассматривать как его инверсию. InARP реализовано как расширение ARP. Форматы пакетов этих протоколов одни и те же, различаются лишь коды операций и заполняемые поля.

ARP-spoofing (ARP-poisoning) — техника сетевой атаки, применяемая преимущественно в Ethernet, но возможная и в других, использующих протокол ARP сетях, основанная на использовании недостатков протокола ARP и позволяющая перехватывать трафик между узлами, которые расположены в пределах одного широковещательного домена. Относится к числу spoofing-атак.

Proxy ARP — техника использования ARP-протокола, позволяющая объединить две не связанные на канальном уровне сети в одну. Хосты, находящиеся в этих сетях, могут использовать адреса из одной IP-подсети и обмениваться трафиком между собой без использования маршрутизатора (как им кажется).

Например, на рисунке изображены два хоста A и B, которые находятся на канальном уровне в разных сегментах. На хостах не настроен шлюз по умолчанию. И маски подсетей на маршрутизаторе и на хостах отличаются.

Если на маршрутизаторе включен Proxy ARP на обоих интерфейсах, то происходит следующее:

1. Хост A хочет отправить какие-то данные хосту B. Так как, на хосте A IP-адрес 10.0.1.10 с маской /8, то он считает, что хост B с IP-адресом 10.0.2.10/8, также находится с ним в одной сети (хосты считают, что они в сети 10.0.0.0/8). Хосту A необходимо узнать MAC-адрес хоста B. Он отправляет ARP-запрос в сеть.
2. Маршрутизатор получает ARP-запрос, но не перенаправляет его, так как получатель в другой сети. Если на маршрутизаторе включен Proxy ARP, то маршрутизатор отправляет хосту A ARP-ответ, в котором подставляет свой MAC-адрес. То есть, для хоста A, создается соответствие 10.0.2.10 - MAC f0/0.
3. Теперь хост A может отправить данные.
4. Маршрутизатор получается пакет, смотрит на IP-адрес получателя и перенаправляет пакет на него (при условии, что в ARP кеше маршрутизатора уже есть запись для хоста B).
5. Хост B аналогичным образом считает, что хост A с ним в одной сети. Хосту B необходимо узнать MAC-адрес хоста A. Он отправляет ARP-запрос в сеть.
6. Маршрутизатор получает ARP-запрос, но не перенаправляет его, так как получатель в другой сети. Если на маршрутизаторе включен Proxy ARP, то маршрутизатор отправляет хосту B ARP-ответ, в котором подставляет свой MAC-адрес. То есть, для хоста B, создается соответствие 10.0.1.10 - MAC f0/1.

Протокол RARP

RARP (**Reverse Address Resolution Protocol — Обратный протокол преобразования адресов**) — протокол сетевого уровня модели OSI, выполняет обратное отображение адресов, то есть преобразует физический адрес в IP-адрес. Используется для систем, не имеющих диска, таких как X терминалы или бездисковые рабочие станции для определения собственного IP адреса.

Протокол применяется во время загрузки узла (например компьютера), когда он посылает групповое сообщение-запрос со своим физическим адресом. Сервер принимает это сообщение и просматривает свои таблицы (либо перенаправляет запрос куда-либо ещё) в поисках IP-адреса, соответствующего физическому. После обнаружения найденный адрес отсылается обратно на запросивший его узел. Другие станции также могут «слышать» этот диалог и локально сохранить эту информацию в своих ARP-таблицах.

RARP позволяет разделять IP-адреса между не часто используемыми хост-узлами. После использования каким-либо узлом IP-адреса он может быть освобождён и выдан другому узлу.

RARP является дополнением к ARP, и описан в RFC 903.

RARP отличается от «обратного» ARP (Inverse Address Resolution Protocol, или InARP), описанного в RFC 2390, который предназначен для получения IP-адреса, соответствующего MAC-адресу другого узла. InARP является дополнением к протоколу разрешения адресов и используется для обратного поиска. RARP является скорее аналогом DHCP/BOOTP.

При работе с бездисковыми PC RARP служит также для передачи ссылки на образ системы в сети.

Несколько RARP серверов в сети

Еще одна особенность заключается в том, что RARP запросы посылаются в виде широковещательных запросов аппаратного уровня. Это означает, что они не перенаправляются маршрутизаторами. Чтобы позволить бездисковым системам загружаться, даже если RARP сервер выключен, в сети обычно существуют несколько RARP серверов (на одном и том же кабеле).

По мере того как количество серверов растет (чтобы повысить надежность), увеличивается сетевой траффик, так как каждый сервер посылает RARP отклик на каждый RARP запрос. Бездисковые системы, которые посылают RARP запросы, обычно используют первый полученный ими RARP отклик. Более того, существует вероятность, что несколько RARP серверов отправят отклики одновременно, увеличивая тем самым количество коллизий в Ethernet.

Краткие выводы

RARP используется большинством бездисковых систем при загрузке, для получения свох IP адресов. Формат пакета RARP практически идентичен пакету ARP. Запрос RARP широковещательный, в нем содержится аппаратный адрес отправителя, при этом он спрашивает кого-либо послать ему его IP адрес. Отклик обычно персональный.

Проблемы с RARP заключаются в том, что он использует широковещательные запросы на

канальном уровне, поэтому большинство маршрутизаторов не могут перенаправлять RARP запросы; а также в том, что передается минимум необходимой информации: только IP адрес системы.

Несмотря на то что концепция RARP довольно проста, реализация RARP сервера зависит от системы. Также надо отметить, что не все TCP/IP реализации предоставляют RARP сервер.