Протоколы, сервисы и услуги
в Интернет и IP-сетях

Тема № 5
Протоколы ARP, InARP, RARP

доц. каф. СС и ПД, к.т.н. С. С. Владимиров

2017 г.

Протоколы ARP и Inverse ARP

ARP (Address Resolution Protocol) — Протокол определения (разрешения) адреса

Протокол в компьютерных сетях, предназначенный для определения канального адреса (MAC) по известному сетевому адресу (IPv4). Как правило используется совместно с протоколом IPv4 в сетях, на основе технологии Ethernet. Описание протокола было опубликовано в ноябре 1982 года в RFC 826 (с обновлениями в RFC 5227/2008 и RFC 5494/2009). 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.

По модели OSI протокол ARP относят или к канальному, или к сетевому уровням. Также часто указывают, что он находится между этими уровнями модели OSI. С точки зрения взаимодействия с другими протоколами пакет ARP инкапсулируется напрямую в кадр Ethernet, т. е. протокол ARP работает поверх Ethernet. В поле «Ethertype» заголовка кадра Ethernet протоколу ARP соответствует $ID = \texttt{0x0806}$.

Типы ARP-пакетов

1. ARP запрос (ARP request)
2. ARP ответ (ARP reply)

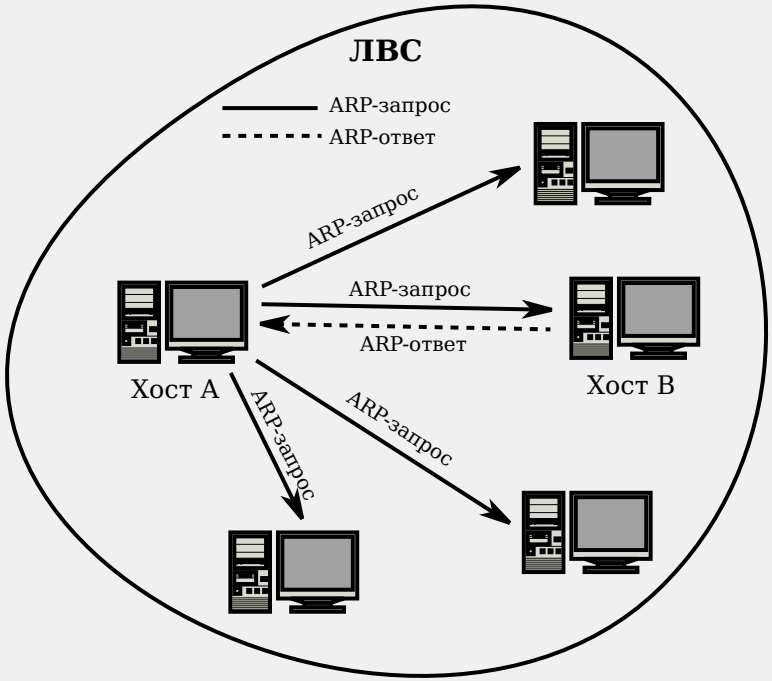
Inverse ARP (Inverse Address Resolution Protocol, InARP)

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. Описание протокола опубликовано в RFC 2390.
InARP реализовано как расширение ARP. Форматы пакетов этих протоколов одни и те же, различаются лишь коды операций и заполняемые поля.

Принцип работы ARP

Порядок разрешения адреса

1. В начале передачи данных от узла *A* на узел *B*, узел *A* должен определить его MAC-адрес, т. е. он должен выполнить процедуру отображения IP-адреса на локальный MAC-адрес. Для этого узел *A* формирует ARP запрос, указывая в нем известный IP-адрес *B*, и рассылает запрос широковещательно по протоколу канального уровня.
2. Все узлы локальной сети получают ARP запрос и сравнивают указанный в нем IP-адрес с собственным.
3. Определив, что MAC-адрес в запросе совпадает с его MAC-адресом, узел *B* формирует ARP-ответ, в котором указывает свой IP-адрес и свой локальный адрес и отправляет его уже направленно, так как в ARP запросе отправитель *A* указывает свой MAC-адрес.



4. Получив ARP-ответ, передающий узел *A* записывает соответствие MAC-адреса *B* его IP-адресу в специальную ARP-таблицу. Теперь, пока запись хранится в ARP-таблице (т. н. время жизни записи), данные могут передаваться от *A* к *B*. Необходимо отметить, что для передачи данных от *B* к *A* требуется провести обратную процедуру.
5. В случае когда данные от *A* к *B* всё ещё передаются, но время жизни записи в ARP-таблице истекает, узел *A* должен обновить запись. Для этого он посылает *повторный ARP-запрос*, который отправляется на известный MAC-адрес узла *B*. В том случае, если ответ на повторный запрос не приходит, процедура разрешения адреса повторяется с самого начала (посредством широковещательного ARP-запроса).

ARP-таблица. Самопроизвольный ARP

Пример ARP-таблицы

```
user@pc:/$ sudo arp -a
HostPC1.lan (192.168.1.111) at 24:08:34:2a:ef:34 [ether] on eth0
Server2.lan (192.168.1.3) at 1c:2b:d4:f9:78:35 [ether] on eth0
OpenWrt.lan (192.168.1.203) at e8:14:f6:43:3b:12 [ether] on eth0
Gateway.lan (192.168.1.1) at e8:d3:27:2e:0f:75 [ether] on eth0
```

Самопроизвольный ARP (gratuitous ARP)

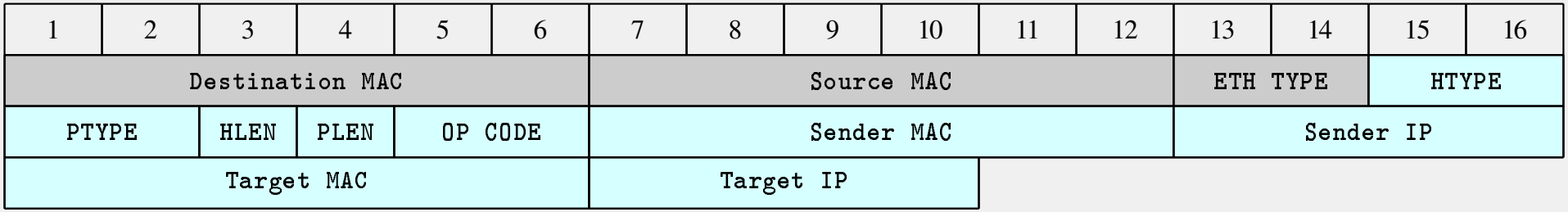
Это такое поведение ARP, когда ARP-ответ присылается, когда в этом (с точки зрения получателя) нет особой необходимости. Самопроизвольный ARP-ответ это пакет-ответ ARP, присланный без запроса. Он применяется для определения конфликтов IP-адресов в сети: как только станция получает адрес по DHCP или адрес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

ARP-пакет

Структура ARP-пакета



Hardware type (HTYPE)

Номер протокола передачи канального уровня (`0x0001` для протокола Ethernet).

Protocol type (PTYPE)

Код протокола сетевого уровня (`0x0800` для протокола IPv4).

Hardware length (HLEN)

Длина физического адреса в байтах. Адреса Ethernet имеют длину 6 байт.

Protocol length (PLEN)

Длина логического адреса в байтах. IPv4 адреса имеют длину 4 байта.

ARP-пакет

Operation code (OP CODE)

Код операции: `0x01` в случае ARP-запроса и `0x02` в случае ARP-ответа

Sender MAC. Sender hardware address (SHA)

Физический адрес отправителя.

Sender IP. Sender protocol address (SPA)

Сетевой адрес отправителя.

Target MAC. Target hardware address (THA)

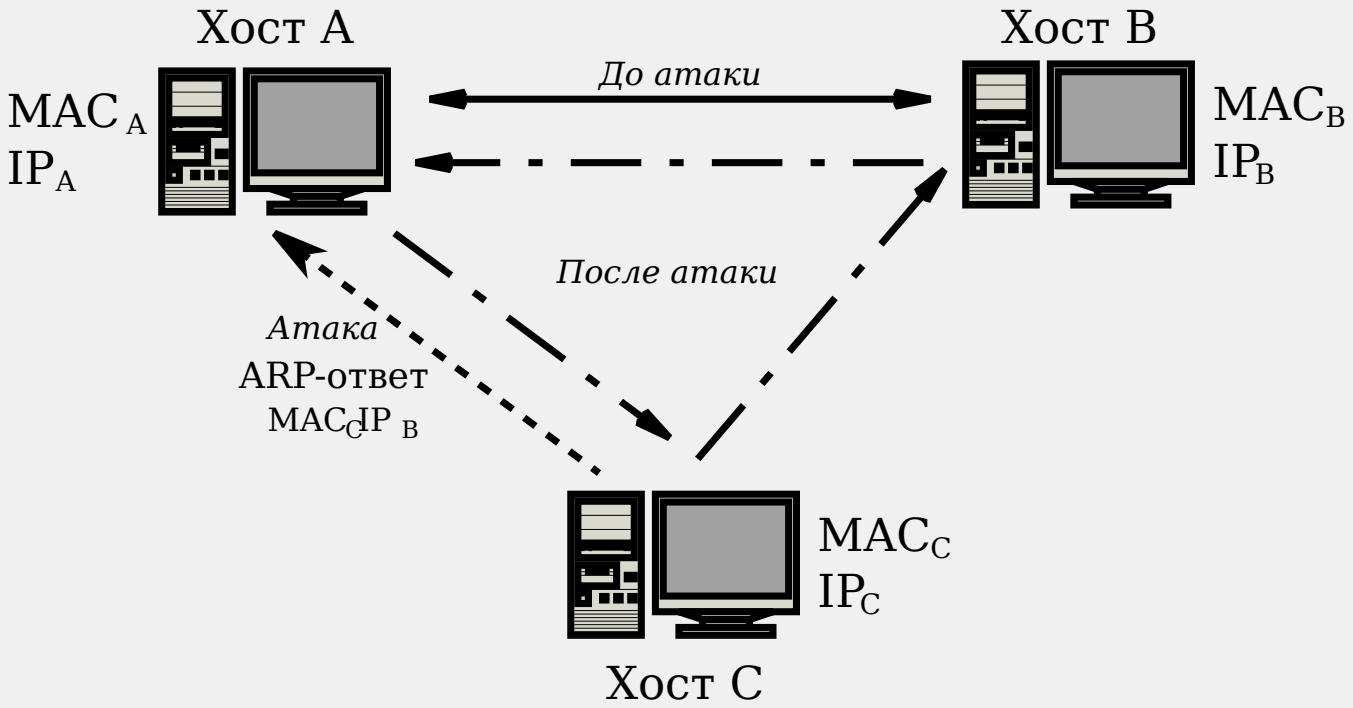
Физический адрес получателя. При запросе поле заполняется нулями.

Target IP. Target protocol address (TPA)

Сетевой адрес получателя.

ARP-spoofing (ARP-poisoning)

Схема сетевой атаки ARP-спуфинг

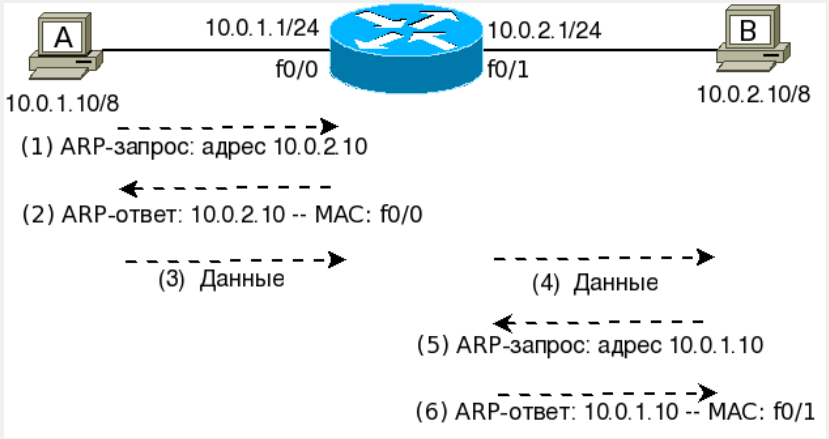


Сетевая атака ARP-спуфинг (ARP-spoofing) основана на использовании самопроизвольного ARP.
Чтобы перехватить сетевые пакеты, которые атакуемый хост (*A*) отправляет на хост *B*, атакующий хост (*C*) формирует ARP-ответ, в котором ставит в соответствие IP-адресу хоста *B* свой MAC-адрес. Далее этот пакет отправляется на хост *A*. В том случае, если хост *A* поддерживает самопроизвольный ARP, он модифицирует собственную ARP-таблицу и помещает туда запись, где вместо настоящего MAC-адреса хоста *B* стоит MAC-адрес атакующего хоста *C*.
Теперь пакеты, отправляемые хостом *A* на хост *B*, будут передаваться хосту *C*.

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).

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



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. RARP является дополнением к ARP, и описан в RFC 903. Формат пакета RARP практически идентичен пакету ARP. С точки зрения выполняемых функций, RARP является скорее аналогом DHCP/BOOTP.

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

Несколько RARP серверов в сети

Оособенность протокола 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.
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.

Источники

- Материалы с сайта `https://wikipedia.org/`
- Материалы с сайта `https://www.rfc-editor.org/`
- Telecommunication technologies — телекоммуникационные технологии / Ю. А. Семенов. URL: `http://book.itep.ru/`
- Proxy ARP. URL: `http://xgu.ru/wiki/Proxy_ARP`