Лабораторная работа 5

**Разрешение адресов по протоколу ARP. APR-спуфинг**

**Цель работы**

Ознакомиться с механизмом работы протокола ARP. Научиться формировать и отправлять пользовательские пакеты. Ознакомиться с журналом работы сетевого устройства в эмуляторе. Научиться проводить сетевую атаку вида ARP-спуфинг.

**Теоретический материал**

**Протокол ARP**

ARP (Address Resolution Protocol — протокол определения адреса) —

протокол в компьютерных сетях, предназначенный для определения MAC- адреса сетевого устройства по известному IP-адресу. Наибольшее распространение ARP получил благодаря повсеместности сетей IP, построенных поверх Ethernet, поскольку в подавляющем большинстве случаев при таком сочетании используется ARP.

Описание протокола было опубликовано в ноябре 1982 г. в RFC 826. ARP был спроектирован для случая передачи IP-пакетов через сегмент Ethernet. При этом общий принцип, предложенный для ARP, 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 протокола: узел (хост А), которому нужно выполнить отображение IP-адреса на MAC-адрес, формирует ARP-запрос, вкладывает его в кадр протокола канального уровня, указывая в нем известный IP- адрес (хост В), и рассылает запрос широковещательно (в поле MAC-адрес назначения заголовка Ethernet указывается широковещательный MAC-адрес FF:FF:FF:FF:FF:FF). Все узлы локальной сети получают ARP-запрос и сравнивают указанный там IP-адрес с собственным. В случае их совпадения узел (хост В) формирует ARP-ответ, в котором указывает свой IP-адрес и свой локальный адрес и отправляет его уже направленно, так как в ARP запросе отправитель (хост А) указывает свой локальный адрес.

При получении ARP-ответа хост А записывает в кэш ARP запись с соответствием IP-адреса хоста В и MAC-адреса хоста В, полученного из ARP- ответа. Время хранения такой записи ограничено. По истечении времени хранения хост А посылает повторный запрос, теперь уже адресно, на известный MAC-адрес хоста В. В случае, если ответ не получен, снова посылается широковещательный запрос.

Самопроизвольный ARP (gratuitous 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.

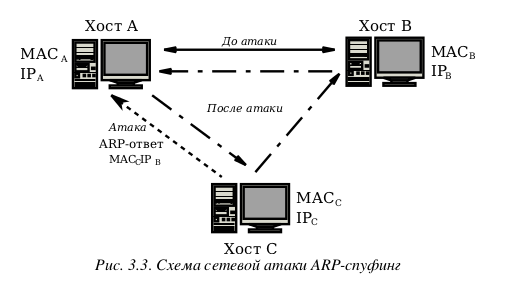
Несмотря на эффективность самопроизвольного ARP, он является особенно небезопасным, поскольку с его помощью можно уверить удаленный узел в том, что MAC-адрес какой-либо системы, находящейся с ней в одной сети, изменился, и указать, какой адрес используется теперь.

**Сетевая атака ARP-спуфинг**

Сетевая атака ARP-спуфинг (ARP-spoofing) основана на использовании самопроизвольного ARP.

Чтобы перехватить сетевые пакеты, которые атакуемый хост (А) отправляет на хост В, атакующий хост (С) формирует ARP-ответ, в котором ставит в соответствие IP-адресу хоста В свой MAC-адрес. Далее этот пакет отправляется на хост А. В том случае, если хост А 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 А на хост В, будут передаваться хосту С.



**Порядок выполнения лабораторной работы**

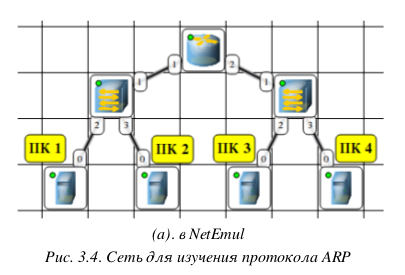
**Часть 1. Построение модели сети**

1. Выбрать исходные данные для выполнения работы согласно своему варианту. Полученную согласно варианту сеть с маской /27 разбить на две подсети с маской /28 каждая.

2. Используя соответствующие инструменты на панели эмулятора, построить сеть в соответствии с рис. 3.4. В свойствах маршрутизатора необходимо указать количество интерфейсов, равное 2.



3. Настроить интерфейсы компьютеров и маршрутизаторов, задав каждому IP-адрес и маску подсети (слева — первая подсеть в заданной сети, справа — вторая подсеть). Добавить возле каждого компьютера и интерфейса роутера надписи с их IP-адресом и маской подсети.



4. Настроить на компьютерах маршруты "по-умолчанию"(IP сети = 0.0.0.0; маска подсети = 0.0.0.0). Можно воспользоваться «Таблицей маршрутизации» либо вызвать свойства компьютера двойным щелчком, указать шлюз по умолчанию и включить маршрутизацию.

5. Включить маршрутизацию на маршрутизаторе.

6. Проверить работоспособность построенной модели ЛВС, передав пакеты (TCP, 5 KB) от компьютера в левой подсети до компьютера в правой подсети.

7. Задать каждому компьютеру имя-описание, воспользовавшись пунктом контекстного меню «Задать описание».

**Часть 2. Определение MAC-адреса с помощью ARP-запроса**

1. Запустить для компьютеров 1 и 2 журналы пакетов (пункт меню «Показать журнал»).

2. Очистить ARP-таблицу компьютера 1.

3. Выделить компьютер 1 и с помощью инструмента «Конструктор пакетов» сформировать пакет ARP-запроса для определения MAC-адреса компьютера 2. Помните, что ARP-запрос рассылается широковещательно (MAC-адрес получателя в заголовке Ethernet — FF:FF:FF:FF:FF:FF), а MAC-адресискомого узла в заголовке ARP приравнивается к нулевому 00:00:00:00:00:00. MAC-адрес компьютера 1 указан в окне «Интерфейсы» для компьютера 1.

4. Запустить ARP-запрос, проследить за ним и за сгенерированным для него ARP-ответом по схеме сети и журналам компьютеров 1 и 2.

5. Открыть ARP-таблицу компьютера 1 и убедиться, что запись добавилась в таблицу.

6. Сохранить скриншот экрана (с открытыми журналами) для отчета.

**Часть 3. Реализация атаки ARP-спуфинг**

1. Запустить для компьютеров 1 и 2 журналы пакетов (пункт меню «Показать журнал»). При необходимости очистить их.

2. Очистить ARP-таблицу компьютера 1.

3. Выделить компьютер 2 и с помощью инструмента «Конструктор пакетов» сформировать пакет ARP-ответа, в котором будут указаны

* MAC отправителя — MAC компьютера 2;
* IP отправителя — IP интерфейса роутера в левой подсети;
* MAC получателя — MAC компьютера 1;
* IP получателя — IP компьютера 1.

4. Запустить ARP-ответ, проследить за ним. Может возникнуть окно одублировании IP-адресов в сети — это происходит в том случае, если из-за действий коммутатора пакет-атаку получает и роутер. Окно быстро закрыть.

5. Сразу же запустить передачу пакетов (UDP, 5 KB) от компьютера 1 на компьютер 3. Убедиться, что пакеты вначале приходят на компьютер 2 и лишь потом (если на компьютере 2 включена маршрутизация) отправляются на компьютер 3 (через маршрутизатор).

6. Сохранить скриншот экрана (с открытыми журналами) для отчета.

Проект сохранить для отчета.

**Содержание отчета**

1. Файл проекта лабораторной работы и собственно файл отчета в котором -

2. Разбиение заданной сети /27 на две подсети /28.

3. Скриншоты с результатами разрешения адреса (часть 2) и сетевой атаки (часть 3).

6. По каждой части лабораторной должны быть приведены выводы

по работе.