Канальный уровень (L2)

Функции и назначение

Канальный уровень отвечает за:

- Адресацию устройств в пределах одной локальной сети (MAC-адреса).
- Контроль ошибок передачи данных.
- Формирование и разбор кадров Ethernet (Data Link Frames).
- Управление доступом к среде передачи данных (CSMA/CD для Ethernet).

Формат Ethernet-кадра

Ethernet II — самый распространенный формат кадров. Он включает:

Следующие поля и количество байт

Преамбула 7

Последовательность 101010… для синхронизации

SFD (Start Frame Delimiter) 1

Указывает начало кадра (10101011)

MAC-адрес назначения 6

MAC-адрес получателя

MAC-адрес отправителя 6

MAC-адрес отправителя

Тип (EtherType) 2

Определяет протокол L3 (0x0800 — IPv4, 0x0806 — ARP)

Данные 46-1500

Полезная нагрузка (IP, ARP и т. Д.)

FCS (Frame Check Sequence) 4

Контрольная сумма (CRC)

Протокол ARP (Address Resolution Protocol)

ARP работает на границе L2 и L3, помогая определить MAC-адреса узлов в локальной сети.

Как работает ARP?

Компьютер отправляет ARP-запрос (broadcast) на MAC-адрес FF:FF:FF:FF:FF:FF, спрашивая:

«Какой MAC-адрес у IP 192.168.1.1?»

Устройство с этим IP отправляет ARP-ответ, сообщая свой MAC-адрес.

Формат ARP-пакета

Следующие поля и количество байт

Тип аппаратуры 2

1 = Ethernet

Тип протокола 2

0x0800 = IPv4

Длина MAC-адреса 1

Обычно 6

Длина IP-адреса 1

Обычно 4

Код операции 2

1 = Запрос, 2 = Ответ

MAC-адрес отправителя 6

MAC-адрес отправителя

IP-адрес отправителя 4

IP-адрес отправителя

MAC-адрес получателя 6

00:00:00:00:00:00 в запросе

IP-адрес получателя 4

IP-адрес искомого устройства

Типичные атаки на ARP

ARP Spoofing (подмена ARP) — злоумышленник отправляет поддельные ARP-ответы, перенаправляя трафик через себя.

ARP Flooding — отправка множества ARP-запросов для заполнения кеша ARP коммутатора**.**

Лабораторная работа N° 5

Сценарий 1

Компьютеры передают данные друг другу через сеть, используя пакеты. Эти пакеты содержат информацию, позволяющую определить отправителя и получателя, а также тип передаваемых данных. Wireshark – это инструмент для анализа сетевого трафика, который позволяет пользователям захватывать, фильтровать и анализировать сетевые пакеты.

Часть 1: Захват и анализ сетевых пакетов

Откройте Wireshark и начните захват данных.

Введите команду ping <IP-адрес> в командной строке.

Остановите захват и проанализируйте пакеты ICMP (Echo Request и Echo Reply).

Анализ:

- Определите MAC-адреса источника и назначения в Ethernet-заголовке.
- Найдите IP-адреса отправителя и получателя в заголовке IP.
- Рассмотрите структуру ICMP-пакета.
- Определите задержку между запросом (Echo Request) и ответом (Echo Reply).
- Проанализируйте пакеты broadcast

Сценарий 2

Когда данные передаются по сети, они инкапсулируются в кадры второго уровня (L2) модели OSI. Wireshark позволяет изучить содержимое этих кадров.

Рассмотрите заголовок Ethernet II:

- Преамбула (8 байт)
- MAC-адрес назначения (6 байт)
- MAC-адрес источника (6 байт)
- Тип кадра (2 байта)
- Данные (46–1500 байт)
- FCS (контрольная сумма кадра) (4 байта)

Определите параметры сети вашего ПК с помощью ipconfig /all.

Часть 2: Анализ Ethernet-кадров в Wireshark

Откройте Wireshark, начните захват пакетов.

Введите фильтр и проанализируйте ARP-запросы и ответы.

Изучите MAC-адреса источника и назначения в ARP-пакетах.

Смените фильтр на icmp, выполните ping и проанализируйте ICMP-пакеты.

Анализ:

- Сравните MAC-адреса в исходящих и входящих пакетах.
- Определите OUI (идентификатор производителя сетевой карты).
- Разберите разницу структуры пакетов ARP и ICMP.