Элтекс. Модуль 4

Лабораторная работа №1

Выполнил: Плотников Михаил Юрьевич

Проект в GNS3: L1\_PlotnikovMY

Тема

Освоение инструментария для выполнения работ, построение простой сети.

Задания

1) Установить и настроить эмулятор GNS3;

2) Создать простейшую сеть, состоящую из 1 коммутатора и 2 компьютеров, назначить им произвольные ip адреса из одной сети;

3) Запустить симуляцию, выполнить команду ping с одного из компьютеров, используя ip адрес второго компьютера;

4) Перехватить трафик протокола arp и проанализировать заголовки пакетов в программе Wireshark, для фильтрации трафика, относящегося к указанному протоколу использовать фильтры Wireshark.

Ход работы

После установки эмулятора GNS3 в окне “Preferences” во вкладке “Qemu VMs” добавим L2 коммутатор, загрузив его образ. Зададим изображение устройству и категорию “Switches”. Загруженный коммутатор в окне “Qemu VMs” представлен на рисунке 1.

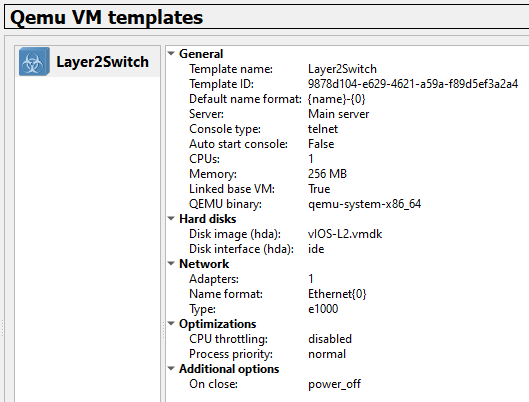


Рисунок 1 — загруженный L2 коммутатор в окне “Qemu VMs”

Создадим сеть из одного коммутатора и двух компьютеров согласно заданию (рисунок 2).

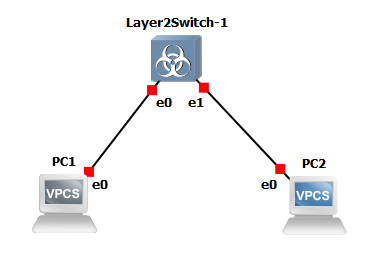


Рисунок 2— Сеть в окне программы

Запустим симуляцию и в консоли компьютеров зададим следующие IP‑адреса: PC1 — 192.168.0.2 (рисунок 3), PC2 — 192.168.0.3 (рисунок 4) при маске 255.255.255.0 и шлюзе 192.168.0.1.



Рисунок 3 — Настройка IP-адреса для PC1



Рисунок 4 — Настройка IP‑адреса для PC2

Проверим доступность соединения, запустив команду ping с компьютера PC2, указав ip PC1 (рисунок 5).

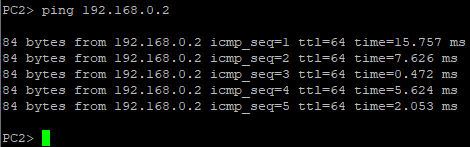


Рисунок 5 — Выполнение команды ping

Запустим захват пакетов между коммутатором и PC2 (рисунок 6).

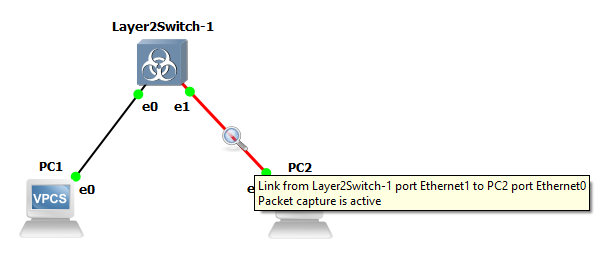


Рисунок 6 — Отображение процесса захвата пакетов в окне GNS3

В появившемся окне программы Wireshark применим фильтр arp, с которым будет производиться отображение захваченных только пакетов протокола ARP. При первом выполнении команды ping с компьютера PC2 на PC1 заметим два пакета протокола (рисунок 7). Первый пакет является запросом MAC-адреса компьютера PC1, второй — ответом.

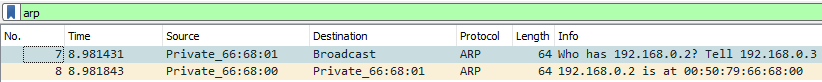


Рисунок 7 — Захваченные пакеты протокола ARP

В Warkshark проанализировать содержимое пакета можно в следующих окнах (рисунок 8). Справа представлено содержимое в двоичном виде с помощью шестнадцатеричных цифр, слева — в расшифрованном виде. Так, например, во втором пакете можно найти информацию об IP‑адресе отправителя (см. рисунок) — 192.168.0.2 или c0 a8 00 02, а также отправленный им свой MAC‑адрес 00:50:79:66:68:00.

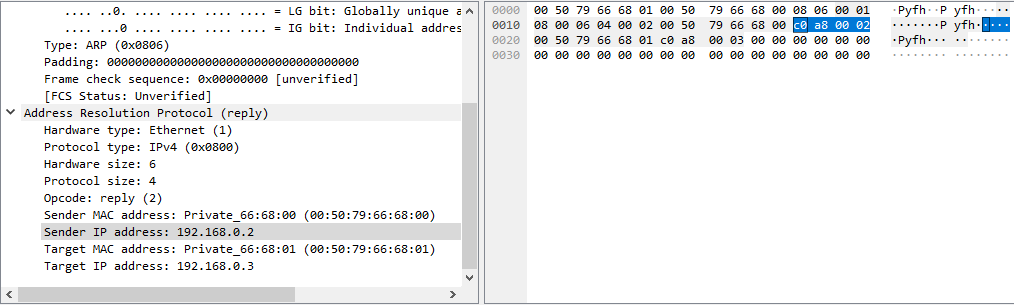


Рисунок 8 — Содержимое второго пакета (ответа)

Заключение

Wireshark является встроенным инструментом в GNS3 и не нуждается в отдельной установке. Для упрощения процесса установки и настройки коммутатора L2 можно воспользоваться инструкцией, доступной по ссылке: https://www.sysnettechsolutions.com/en/add-layer-2-switch-in-gns3/