Семенова С.С, проект sof\_lab1

**Лабораторная работа №1**

**Тема: Освоение инструментария для выполнения работ, построение простой сети**

**Задание:**

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 на всех линках(nb!), задокументировать и проанализировать заголовки пакетов в программе Wireshark, для фильтрации трафика, относящегося к указанному протоколу использовать фильтры Wireshark.

5) Создать простейшую сеть, состоящую из 1 маршрутизатора и 2 компьютеров, назначить им произвольные ip адреса из разных сетей.

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

7) Перехватить трафик протокола arp и icmp на всех линках(nb!), задокументировать и проанализировать заголовки пакетов в программе Wireshark, для фильтрации трафика, относящегося к указанному протоколу использовать фильтры Wireshark.

**Ход работы:**

1. Установили и настроили эмулятор GNS3.

Сложностей не возникло.

2. Создали простейшую сеть, состоящую из 1 коммутатора и 2 компьютеров, назначили им произвольные ip адреса из одной сети:

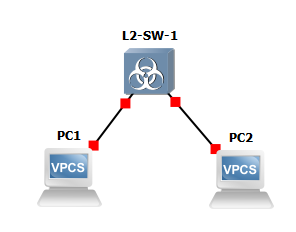


Рис. 1. Топология сети.

Для начала проверили конфигурации на обоих компьютерах:

**PC1>** show

NAME IP/MASK GATEWAY MAC LPORT RHOST:PORT

PC1 0.0.0.0/0 0.0.0.0 00:50:79:66:68:03 20136 127.0.0.1:20137

fe80::250:79ff:fe66:6803/64

**PC2>** show

NAME IP/MASK GATEWAY MAC LPORT RHOST:PORT

PC2 0.0.0.0/0 0.0.0.0 00:50:79:66:68:01 20138 127.0.0.1:20139

fe80::250:79ff:fe66:6801/64

Назначили им произвольные адреса из одной подсети:

**PC1>** ip 172.198.4.2/24

Checking for duplicate address...

PC1 : 172.198.4.2 255.255.255.0

**PC2>** ip 172.198.4.3/24

Checking for duplicate address...

PC2 : 172.198.4.3 255.255.255.0

3. Запустили симуляцию, выполнили команду ping с одного из компьютеров, используя ip адрес второго компьютера:

**PC1>** ping 172.198.4.3

84 bytes from 172.198.4.3 icmp\_seq=1 ttl=64 time=15.806 ms

84 bytes from 172.198.4.3 icmp\_seq=2 ttl=64 time=7.653 ms

84 bytes from 172.198.4.3 icmp\_seq=3 ttl=64 time=0.426 ms

84 bytes from 172.198.4.3 icmp\_seq=4 ttl=64 time=2.654 ms

84 bytes from 172.198.4.3 icmp\_seq=5 ttl=64 time=0.627 ms

То же самое со вторым компьютером:

**PC2>** ping 172.198.4.2

84 bytes from 172.198.4.2 icmp\_seq=1 ttl=64 time=5.927 ms

84 bytes from 172.198.4.2 icmp\_seq=2 ttl=64 time=11.389 ms

84 bytes from 172.198.4.2 icmp\_seq=3 ttl=64 time=3.491 ms

84 bytes from 172.198.4.2 icmp\_seq=4 ttl=64 time=0.590 ms

84 bytes from 172.198.4.2 icmp\_seq=5 ttl=64 time=1.720 ms

4. Перехватили трафик протокола arp на всех линках, задокументировав и проанализировав заголовки пакетов в программе Wireshark, для фильтрации трафика, относящегося к указанному протоколу, использовали фильтры Wireshark.

Файлы с экспортированными пакетами в репозитории: ARP\_PC1.pcapng и ARP\_PC2.pcapng

Фильтр, который был использован: ARP

Протокол ARP используется для того, чтобы узнать неизвестный MAC-адрес по известному IP-адресу.



В файле ARP\_PC1.pcapng можно увидеть, что было перехвачено всего два пакета (запрос и ответ).

В первой строке можно увидеть, что мы делали запрос по краткой информации. Указан свой MAC-адрес, далее назначение на широковещательный MAC-адрес, и характерная информация с запросом есть ли искомый IP-адрес в сети и на какой IP нужно ответить, если он все-таки есть.

Следующий пакет – это ARP ответ. Указана краткая информация о том, что запрашиваемый IP-адрес соответствует такому-то MAC-адресу.

В заголовках пакета можно увидеть то же самое. В начале идет служебная информация о сети, с каким типом сетевого оборудования и протоколом сетевого уровня происходит работа. В поле opcode содержится информация о коде операции. Заначение 1 – это ARP-запрос, а 2 – ответ.

Для PC2 данные аналогичны.

5. Далее создали еще одну простейшую сеть, состоящую из 1 маршрутизатора и 2 компьютеров, назначили им произвольные IP адреса из разных сетей.

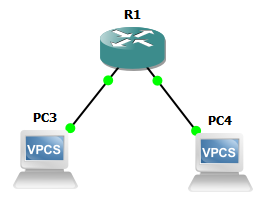


Рис. 2. Топология сети

Для начала проверили конфигурации на обоих компьютерах:

**PC3>** show

NAME IP/MASK GATEWAY MAC LPORT RHOST:PORT

PC3 0.0.0.0/0 0.0.0.0 00:50:79:66:68:02 20144 127.0.0.1:20145

fe80::250:79ff:fe66:6802/64

**PC4>** show

NAME IP/MASK GATEWAY MAC LPORT RHOST:PORT

PC4 0.0.0.0/0 0.0.0.0 00:50:79:66:68:00 20146 127.0.0.1:20147

fe80::250:79ff:fe66:6800/64

Назначили им произвольные адреса из разных сетей:

**PC3>** ip 200.100.200.2/24 200.100.200.1

Checking for duplicate address...

PC3 : 200.100.200.2 255.255.255.0 gateway 200.100.200.1

**PC4>** ip 100.200.100.2/24 100.200.100.1

Checking for duplicate address...

PC4 : 100.200.100.2 255.255.255.0 gateway 100.200.100.1

Настроили маршрутизатор:

**R1#**conf t

Enter configuration commands, one per line. End with CNTL/Z.

**R1(config)#int** fa0/0

**R1(config-if)#**ip address 200.100.200.1 255.255.255.0

**R1(config-if)#**no shutdown

**R1(config-if)#**

\*Mar 1 00:04:51.519: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to up

\*Mar 1 00:04:52.519: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up

**R1(config-if)#**end

**R1#**

\*Mar 1 00:09:45.519: %SYS-5-CONFIG\_I: Configured from console by console

**R1#**conf t

Enter configuration commands, one per line. End with CNTL/Z.

**R1(config)#**int fa 1/0

**R1(config-if)#i**p address 100.200.100.1 255.255.255.0

**R1(config-if)#**no shutdown

**R1(config-if)#**

\*Mar 1 00:10:44.563: %LINK-3-UPDOWN: Interface FastEthernet1/0, changed state to up

\*Mar 1 00:10:45.563: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet1/0, changed state to up

**R1(config-if)#**end

**R1#**

\*Mar 1 00:10:49.563: %SYS-5-CONFIG\_I: Configured from console by console

**R1#**copy running-config startup-config

Destination filename [startup-config]?

Building configuration...

6. Запустили симуляцию, выполнили команду ping с одного из компьютеров, используя ip адрес второго компьютера, предварительно проверив еще ping со шлюзом:

**PC3>** ping 200.100.200.1

84 bytes from 200.100.200.1 icmp\_seq=1 ttl=255 time=0.721 ms

84 bytes from 200.100.200.1 icmp\_seq=2 ttl=255 time=5.328 ms

84 bytes from 200.100.200.1 icmp\_seq=3 ttl=255 time=4.506 ms

84 bytes from 200.100.200.1 icmp\_seq=4 ttl=255 time=4.588 ms

84 bytes from 200.100.200.1 icmp\_seq=5 ttl=255 time=4.719 ms

**PC3>** arp

cc:01:51:23:00:00 200.100.200.1 expires in 39 seconds

**PC3>** ping 100.200.100.2

84 bytes from 100.200.100.2 icmp\_seq=1 ttl=63 time=13.242 ms

84 bytes from 100.200.100.2 icmp\_seq=2 ttl=63 time=15.301 ms

84 bytes from 100.200.100.2 icmp\_seq=3 ttl=63 time=14.917 ms

84 bytes from 100.200.100.2 icmp\_seq=4 ttl=63 time=14.372 ms

84 bytes from 100.200.100.2 icmp\_seq=5 ttl=63 time=15.333 ms

То же самое со вторым компьютером:

**PC4>** ping 100.200.100.1

84 bytes from 100.200.100.1 icmp\_seq=1 ttl=255 time=0.642 ms

84 bytes from 100.200.100.1 icmp\_seq=2 ttl=255 time=4.677 ms

84 bytes from 100.200.100.1 icmp\_seq=3 ttl=255 time=5.043 ms

84 bytes from 100.200.100.1 icmp\_seq=4 ttl=255 time=5.501 ms

84 bytes from 100.200.100.1 icmp\_seq=5 ttl=255 time=4.579 ms

**PC4>** arp

cc:01:51:23:00:10 100.200.100.1 expires in 7 seconds

**PC4>** ping 200.100.200.2

84 bytes from 200.100.200.2 icmp\_seq=1 ttl=63 time=10.868 ms

84 bytes from 200.100.200.2 icmp\_seq=2 ttl=63 time=14.756 ms

84 bytes from 200.100.200.2 icmp\_seq=3 ttl=63 time=14.269 ms

84 bytes from 200.100.200.2 icmp\_seq=4 ttl=63 time=25.249 ms

84 bytes from 200.100.200.2 icmp\_seq=5 ttl=63 time=15.487 ms

7. Перехватили трафик протоколов arp и icmp на всех линках, задокументировав и проанализировав заголовки пакетов в программе Wireshark, для фильтрации трафика, относящегося к указанному протоколу, использовали фильтры Wireshark.

Файлы с экспортированными пакетами в репозитории: ARP\_ICMP\_PC3.pcapng и ARP\_ICMP\_PC4.pcapng.

Фильтр, который был использован: ARP || ICMP

Для протокола ARP все работает аналогично предыдущему примеру, но только для PC3, так как сначала мы делали запрос на шлюз, в трафике он указан. Но до PC4 ARP-запрос не дошел, т.к. компьютеры находятся в разных сетях, и сам протокол ниже сетевого уровня и через маршрутизатор не проходит.

В трассировке мы видим, что утилита ping использует эхо-протокол. Она посылает эхо-запрос. Компьютер, который получил такой запрос, должен отправить эхо-ответ. В нашем случае было отправлено 5 эхо-запросов на каждый из узлов. В файле сначала проверка доступности шлюза по умолчанию, далее ping на соседний хост. И также 5 эхо-ответов получено.

В начале каждого из пакетов идет заголовок канального уровня, далее заголовок протокола сетевого уровня, потом данные протокола ICMP. В заголовке ICMP первые два поля – это тип и код сообщения. Type = 8 – эхо запрос, type = 0 – эхо ответ. Код сообщения 0.