**Лабораторная работа №1**

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

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

С помощью двойного клика по PC1 и PC2 открываем консоль VPCS и настраиваем IP-адреса

ip 192.168.1.1 255.255.255.0

ip 192.168.1.2 255.255.255.0

С помощью show ip проверяем.

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

PC1> ping 192.168.1.2

84 bytes from 192.168.1.2 icmp\_seq=1 ttl=64 time=0.209 ms

84 bytes from 192.168.1.2 icmp\_seq=2 ttl=64 time=0.216 ms

84 bytes from 192.168.1.2 icmp\_seq=3 ttl=64 time=0.215 ms

84 bytes from 192.168.1.2 icmp\_seq=4 ttl=64 time=0.236 ms

84 bytes from 192.168.1.2 icmp\_seq=5 ttl=64 time=0.309 ms

PC1>

PC2> ping 192.168.1.1

84 bytes from 192.168.1.1 icmp\_seq=1 ttl=64 time=0.231 ms

84 bytes from 192.168.1.1 icmp\_seq=2 ttl=64 time=0.285 ms

84 bytes from 192.168.1.1 icmp\_seq=3 ttl=64 time=0.226 ms

84 bytes from 192.168.1.1 icmp\_seq=4 ttl=64 time=0.241 ms

84 bytes from 192.168.1.1 icmp\_seq=5 ttl=64 time=0.206 ms

PC2>

**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**

На соединениях между PC1 — Switch и PC2 — Switch вызываем Wireshark. В каждом окне Wireshark, в поле фильтра вводим arp

ARP Request

Hardware type: Ethernet (1)

Protocol type: IPv4 (0x0800)

Hardware size: 6

Protocol size: 4

Opcode: request (1)

Sender MAC address: Private\_66:68:00 (00:50:79:66:68:00)

Sender IP address: 192.168.1.1

Target MAC address: Broadcast (ff:ff:ff:ff:ff:ff)

Target IP address: 192.168.1.2

ARP Reply:

Hardware type: Ethernet (1)

Protocol type: IPv4 (0x0800)

Hardware size: 6

Protocol size: 4

Opcode: reply (2)

Sender MAC address: Private\_66:68:01 (00:50:79:66:68:01)

Sender IP address: 192.168.1.2

Target MAC address: Private\_66:68:01 (00:50:79:66:68:00)

Target IP address: 192.168.1.1

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

**FastEthernet0/0** → сеть 192.168.1.2 255.255.255.0 192.168.1.1

**FastEthernet1/0** → сеть 192.168.2.2 255.255.255.0 192.168.2.1

enable

configure terminal

interface FastEthernet0/0

ip address 192.168.1.1 255.255.255.0

no shutdown

exit

interface FastEthernet1/0

ip address 192.168.2.1 255.255.255.0

no shutdown

exit

end

write memory

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

PC2> ping 192.168.1.1

84 bytes from 192.168.1.1 icmp\_seq=1 ttl=255 time=9.522 ms

84 bytes from 192.168.1.1 icmp\_seq=2 ttl=255 time=5.671 ms

84 bytes from 192.168.1.1 icmp\_seq=3 ttl=255 time=6.978 ms

84 bytes from 192.168.1.1 icmp\_seq=4 ttl=255 time=6.933 ms

84 bytes from 192.168.1.1 icmp\_seq=5 ttl=255 time=6.080 ms

PC2>

PC1> ping 192.168.2.2

84 bytes from 192.168.2.2 icmp\_seq=1 ttl=63 time=20.131 ms

84 bytes from 192.168.2.2 icmp\_seq=2 ttl=63 time=16.295 ms

84 bytes from 192.168.2.2 icmp\_seq=3 ttl=63 time=15.961 ms

84 bytes from 192.168.2.2 icmp\_seq=4 ttl=63 time=15.106 ms

84 bytes from 192.168.2.2 icmp\_seq=5 ttl=63 time=15.121 ms

PC1>

**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**

В поле фильтра вводим arp

ARP Request

Hardware type: Ethernet (1)

Protocol type: IPv4 (0x0800)

Hardware size: 6

Protocol size: 4

Opcode: request (1)

Sender MAC address: Private\_66:68:00 (00:50:79:66:68:00)

Sender IP address: 192.168.1.2

Target MAC address: Broadcast (ff:ff:ff:ff:ff:ff)

Target IP address: 192.168.1.1

ARP Reply:

Hardware type: Ethernet (1)

Protocol type: IPv4 (0x0800)

Hardware size: 6

Protocol size: 4

Opcode: reply (2)

Sender MAC address: cc:01:7d:5e:00:00 (cc:01:7d:5e:00:00)

Sender IP address: 192.168.1.1

Target MAC address: Private\_66:68:01 (00:50:79:66:68:00)

Target IP address: 192.168.1.2

В поле фильтра вводим icmp

Ping request

Type: 8 (Echo (ping) request)

Code: 0

Checksum: 0x2e87 [correct]

[Checksum Status: Good]

Identifier (BE): 61827 (0xf183)

Identifier (LE): 33777 (0x83f1)

Sequence Number (BE): 1 (0x0001)

Sequence Number (LE): 256 (0x0100)

[Response frame: 14]

Data (56 bytes)

Ping reply

Type: 8 (Echo (ping) reply)

Code: 0

Checksum: 0x3687 [correct]

[Checksum Status: Good]

Identifier (BE): 61827 (0xf183)

Identifier (LE): 33777 (0x83f1)

Sequence Number (BE): 1 (0x0001)

Sequence Number (LE): 256 (0x0100)

[Response frame: 13]

[Response time: 59,949 ms]

Data (56 bytes)