Отчёт по лабораторной работе «Локальные сети»

Зиновьев Денис, ИУ7-32м

14 декабря 2019 г.

Содержание

1. Получение адреса по DHCP

Выполняем tcpdump для просмотра DHCP для **ws21**.

```
r2:~# tcpdump -ntve -s 0 -i eth0 udp
10:10:10:10:10:ee > 3a:40:ee:31:9e:cd, ethertype IPv4 (0x0800), length 342: (tos 0x0, ttl 64,
        id 0, offset 0, flags [DF], proto UDP (17), length 328) 10.20.0.2.68 > 10.20.0.1.67:
        BOOTP/DHCP, Request from 10:10:10:10:10:ee, length 300, xid 0xa0252a50, Flags [none]
          Client-IP 10.20.0.2
          Client-Ethernet-Address 10:10:10:10:10:ee
          Vendor-rfc1048 Extensions
            Magic Cookie 0x63825363
            DHCP-Message Option 53, length 1: Release
            Server-ID Option 54, length 4: 10.20.0.1
10:10:10:10:10:ee > ff:ff:ff:ff:ff:ff, ethertype IPv4 (0x0800), length 342: (tos 0x10, ttl 128,
        id 0, offset 0, flags [none], proto UDP (17), length 328) 0.0.0.0.68 > 255.255.255.255.
        BOOTP/DHCP, Request from 10:10:10:10:10:ee, length 300, xid 0x1ea78936, Flags [none]
          Client-Ethernet-Address 10:10:10:10:10:ee
          Vendor-rfc1048 Extensions
            Magic Cookie 0x63825363
            DHCP-Message Option 53, length 1: Discover
            Requested-IP Option 50, length 4: 10.20.0.2
            Parameter-Request Option 55, length 12:
              Subnet-Mask, BR, Time-Zone, Default-Gateway
```

```
              Domain-Name, Domain-Name-Server, Option 119, Hostname
              Netbios-Name-Server, Netbios-Scope, MTU, Classless-Static-Route
3a:40:ee:31:9e:cd > 10:10:10:10:10:ee, ethertype IPv4 (0x0800), length 342: (tos 0x10, ttl 128,
        id 0, offset 0, flags [none], proto UDP (17), length 328) 10.20.0.1.67 > 10.20.0.2.68:
        BOOTP/DHCP, Reply, length 300, xid 0x1ea78936, Flags [none]
          Your-IP 10.20.0.2
          Client-Ethernet-Address 10:10:10:10:10:ee
          Vendor-rfc1048 Extensions
            Magic Cookie 0x63825363
            DHCP-Message Option 53, length 1: Offer
            Server-ID Option 54, length 4: 10.20.0.1
            Lease-Time Option 51, length 4: 43200
            Subnet-Mask Option 1, length 4: 255.255.0.0
            Default-Gateway Option 3, length 4: 10.20.0.1
            Domain-Name-Server Option 6, length 4: 10.20.0.1
10:10:10:10:10:ee > ff:ff:ff:ff:ff:ff, ethertype IPv4 (0x0800), length 342: (tos 0x10, ttl 128,
        id 0, offset 0, flags [none], proto UDP (17), length 328) 0.0.0.0.68 > 255.255.255.255.
        BOOTP/DHCP, Request from 10:10:10:10:10:ee, length 300, xid 0x1ea78936, Flags [none]
          Client-Ethernet-Address 10:10:10:10:10:ee
          Vendor-rfc1048 Extensions
            Magic Cookie 0x63825363
            DHCP-Message Option 53, length 1: Request
            Server-ID Option 54, length 4: 10.20.0.1
            Requested-IP Option 50, length 4: 10.20.0.2
            Parameter-Request Option 55, length 12:
              Subnet-Mask, BR, Time-Zone, Default-Gateway
              Domain-Name, Domain-Name-Server, Option 119, Hostname
              Netbios-Name-Server, Netbios-Scope, MTU, Classless-Static-Route
3a:40:ee:31:9e:cd > 10:10:10:10:10:ee, ethertype IPv4 (0x0800), length 342: (tos 0x10, ttl 128,
        id 0, offset 0, flags [none], proto UDP (17), length 328) 10.20.0.1.67 > 10.20.0.2.68:
        BOOTP/DHCP, Reply, length 300, xid 0x1ea78936, Flags [none]
          Your-IP 10.20.0.2
          Client-Ethernet-Address 10:10:10:10:10:ee
          Vendor-rfc1048 Extensions
            Magic Cookie 0x63825363
            DHCP-Message Option 53, length 1: ACK
            Server-ID Option 54, length 4: 10.20.0.1
            Lease-Time Option 51, length 4: 43200
            Subnet-Mask Option 1, length 4: 255.255.0.0
            Default-Gateway Option 3, length 4: 10.20.0.1
            Domain-Name-Server Option 6, length 4: 10.20.0.1
10:10:10:10:10:ee > 3a:40:ee:31:9e:cd, ethertype IPv4 (0x0800), length 342: (tos 0x0, ttl 64,
        id 0, offset 0, flags [DF], proto UDP (17), length 328) 10.20.0.2.68 > 10.20.0.1.67:
        BOOTP/DHCP, Request from 10:10:10:10:10:ee, length 300, xid 0xaaf2d20, Flags [none]
          Client-IP 10.20.0.2
          Client-Ethernet-Address 10:10:10:10:10:ee
          Vendor-rfc1048 Extensions
            Magic Cookie 0x63825363
            DHCP-Message Option 53, length 1: Release
            Server-ID Option 54, length 4: 10.20.0.1
```

```
10:10:10:10:10:ee > ff:ff:ff:ff:ff:ff, ethertype IPv4 (0x0800), length 342: (tos 0x10, ttl 128,
        id 0, offset 0, flags [none], proto UDP (17), length 328) 0.0.0.0.68 > 255.255.255.255.
        BOOTP/DHCP, Request from 10:10:10:10:10:ee, length 300, xid 0xf1fc4d3f, Flags [none]
          Client-Ethernet-Address 10:10:10:10:10:ee
          Vendor-rfc1048 Extensions
            Magic Cookie 0x63825363
            DHCP-Message Option 53, length 1: Discover
            Requested-IP Option 50, length 4: 10.20.0.2
            Parameter-Request Option 55, length 12:
              Subnet-Mask, BR, Time-Zone, Default-Gateway
              Domain-Name, Domain-Name-Server, Option 119, Hostname
              Netbios-Name-Server, Netbios-Scope, MTU, Classless-Static-Route
3a:40:ee:31:9e:cd > 10:10:10:10:10:ee, ethertype IPv4 (0x0800), length 342: (tos 0x10, ttl 128,
        id 0, offset 0, flags [none], proto UDP (17), length 328) 10.20.0.1.67 > 10.20.0.2.68:
        BOOTP/DHCP, Reply, length 300, xid 0xf1fc4d3f, Flags [none]
          Your-IP 10.20.0.2
          Client-Ethernet-Address 10:10:10:10:10:ee
          Vendor-rfc1048 Extensions
            Magic Cookie 0x63825363
            DHCP-Message Option 53, length 1: Offer
            Server-ID Option 54, length 4: 10.20.0.1
            Lease-Time Option 51, length 4: 43200
            Subnet-Mask Option 1, length 4: 255.255.0.0
            Default-Gateway Option 3, length 4: 10.20.0.1
            Domain-Name-Server Option 6, length 4: 10.20.0.1
10:10:10:10:10:ee > ff:ff:ff:ff:ff:ff, ethertype IPv4 (0x0800), length 342: (tos 0x10, ttl 128,
        id 0, offset 0, flags [none], proto UDP (17), length 328) 0.0.0.0.68 > 255.255.255.255.
        BOOTP/DHCP, Request from 10:10:10:10:10:ee, length 300, xid 0xf1fc4d3f, Flags [none]
          Client-Ethernet-Address 10:10:10:10:10:ee
          Vendor-rfc1048 Extensions
            Magic Cookie 0x63825363
            DHCP-Message Option 53, length 1: Request
            Server-ID Option 54, length 4: 10.20.0.1
            Requested-IP Option 50, length 4: 10.20.0.2
            Parameter-Request Option 55, length 12:
              Subnet-Mask, BR, Time-Zone, Default-Gateway
              Domain-Name, Domain-Name-Server, Option 119, Hostname
              Netbios-Name-Server, Netbios-Scope, MTU, Classless-Static-Route
3a:40:ee:31:9e:cd > 10:10:10:10:10:ee, ethertype IPv4 (0x0800), length 342: (tos 0x10, ttl 128,
        id 0, offset 0, flags [none], proto UDP (17), length 328) 10.20.0.1.67 > 10.20.0.2.68:
        BOOTP/DHCP, Reply, length 300, xid 0xf1fc4d3f, Flags [none]
          Your-IP 10.20.0.2
          Client-Ethernet-Address 10:10:10:10:10:ee
          Vendor-rfc1048 Extensions
            Magic Cookie 0x63825363
            DHCP-Message Option 53, length 1: ACK
            Server-ID Option 54, length 4: 10.20.0.1
            Lease-Time Option 51, length 4: 43200
            Subnet-Mask Option 1, length 4: 255.255.0.0
            Default-Gateway Option 3, length 4: 10.20.0.1
```

```
            Domain-Name-Server Option 6, length 4: 10.20.0.1
```

Выполняем tcpdump для просмотра DHCP для **ws11**.

```
r1:~# tcpdump -ntve -s 0 -i eth0 udp
10:10:10:10:10:ba > ff:ff:ff:ff:ff:ff, ethertype IPv4 (0x0800), length 342:
        (tos 0x10, ttl 128, id 0, offset 0, flags [none], proto UDP (17), length 328)
        0.0.0.0.68 > 255.255.255.255.67: BOOTP/DHCP, Request from 10:10:10:10:10:ba,
        length 300, xid 0x78f623f, Flags [none]
          Client-Ethernet-Address 10:10:10:10:10:ba
          Vendor-rfc1048 Extensions
            Magic Cookie 0x63825363
            DHCP-Message Option 53, length 1: Discover
            Requested-IP Option 50, length 4: 10.10.1.1
            Parameter-Request Option 55, length 12:
              Subnet-Mask, BR, Time-Zone, Default-Gateway
              Domain-Name, Domain-Name-Server, Option 119, Hostname
              Netbios-Name-Server, Netbios-Scope, MTU, Classless-Static-Route
0e:ab:f8:0c:10:4b > 10:10:10:10:10:ba, ethertype IPv4 (0x0800), length 342:
        (tos 0x10, ttl 128, id 0, offset 0, flags [none], proto UDP (17), length 328)
        10.10.0.1.67 > 10.10.1.1.68: BOOTP/DHCP, Reply,
        length 300, xid 0x78f623f, Flags [none]
          Your-IP 10.10.1.1
          Client-Ethernet-Address 10:10:10:10:10:ba
          Vendor-rfc1048 Extensions
            Magic Cookie 0x63825363
            DHCP-Message Option 53, length 1: Offer
            Server-ID Option 54, length 4: 10.10.0.1
            Lease-Time Option 51, length 4: 43200
            Subnet-Mask Option 1, length 4: 255.255.0.0
            Default-Gateway Option 3, length 4: 10.10.0.1
            Domain-Name-Server Option 6, length 4: 10.10.0.1
10:10:10:10:10:ba > ff:ff:ff:ff:ff:ff, ethertype IPv4 (0x0800), length 342:
        (tos 0x10, ttl 128, id 0, offset 0, flags [none], proto UDP (17), length 328)
        0.0.0.0.68 > 255.255.255.255.67: BOOTP/DHCP, Request from 10:10:10:10:10:ba,
        length 300, xid 0x78f623f, Flags [none]
          Client-Ethernet-Address 10:10:10:10:10:ba
          Vendor-rfc1048 Extensions
            Magic Cookie 0x63825363
            DHCP-Message Option 53, length 1: Request
            Server-ID Option 54, length 4: 10.10.0.1
            Requested-IP Option 50, length 4: 10.10.1.1
            Parameter-Request Option 55, length 12:
              Subnet-Mask, BR, Time-Zone, Default-Gateway
              Domain-Name, Domain-Name-Server, Option 119, Hostname
              Netbios-Name-Server, Netbios-Scope, MTU, Classless-Static-Route
0e:ab:f8:0c:10:4b > 10:10:10:10:10:ba, ethertype IPv4 (0x0800), length 342:
        (tos 0x10, ttl 128, id 0, offset 0, flags [none], proto UDP (17), length 328)
        10.10.0.1.67 > 10.10.1.1.68: BOOTP/DHCP, Reply, length 300, xid 0x78f623f, Flags [none]
          Your-IP 10.10.1.1
```

```
          Client-Ethernet-Address 10:10:10:10:10:ba
          Vendor-rfc1048 Extensions
            Magic Cookie 0x63825363
            DHCP-Message Option 53, length 1: ACK
            Server-ID Option 54, length 4: 10.10.0.1
            Lease-Time Option 51, length 4: 43200
            Subnet-Mask Option 1, length 4: 255.255.0.0
            Default-Gateway Option 3, length 4: 10.10.0.1
            Domain-Name-Server Option 6, length 4: 10.10.0.1
```

2. Использование VPN

```
r2:~# ip r
10.100.100.1 dev tun0  proto kernel  scope link  src 10.100.100.2
10.20.0.0/16 dev eth0  proto kernel  scope link  src 10.20.0.1
10.10.0.0/16 via 10.100.100.1 dev tun0  proto zebra  metric 2
172.16.0.0/16 dev eth1  proto kernel  scope link  src 172.16.1.4
default via 172.16.1.2 dev eth1
```

```
r2:~# ip -4 a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue
    inet 127.0.0.1/8 scope host lo
3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000
    inet 172.16.1.4/16 brd 172.16.255.255 scope global eth1
4: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000
    inet 10.20.0.1/16 brd 10.20.255.255 scope global eth0
5: tun0: <POINTOPOINT,MULTICAST,NOARP,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 100
    inet 10.100.100.2 peer 10.100.100.1/32 scope global tun0
```

```
r2:~# tcpdump -nv -s 0 -i tun0
00:01:37.392336 IP (tos 0x0, ttl 1, id 0, offset 0, flags [DF],
        proto UDP (17), length 52) 10.100.100.2.520 > 224.0.0.9.520:
        RIPv2, Response, length: 24, routes: 1
          AFI: IPv4:       10.20.0.0/16, tag 0x0000, metric: 1, next-hop: self
00:01:39.342992 IP (tos 0x0, ttl 1, id 0, offset 0, flags [DF],
        proto UDP (17), length 52) 10.100.100.1.520 > 224.0.0.9.520:
        RIPv2, Response, length: 24, routes: 1
          AFI: IPv4:       10.10.0.0/16, tag 0x0000, metric: 1, next-hop: self<Paste>
```

```
ws21:~# traceroute 10.10.4.10
traceroute to 10.10.4.10 (10.10.4.10), 64 hops max, 40 byte packets
 1  10.20.0.1 (10.20.0.1)  0 ms  0 ms  0 ms
 2  10.100.100.1 (10.100.100.1)  1 ms  1 ms  1 ms
 3  10.10.4.10 (10.10.4.10)  7 ms  1 ms  1 ms
```

3. Правила фильтрации пакетов и трансляции адресов

```
r1:~# iptables -t nat -A PREROUTING -p tcp --dport 25 -i eth1 -j DNAT --to 10.10.4.10:25
```

```
r1:~# iptables -L -nv
Chain INPUT (policy ACCEPT 727 packets, 55201 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain FORWARD (policy ACCEPT 27 packets, 1744 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain OUTPUT (policy ACCEPT 561 packets, 44581 bytes)
 pkts bytes target     prot opt in     out     source               destination
r1:~# iptables -L -nvt nat
Chain PREROUTING (policy ACCEPT 28 packets, 2635 bytes)
 pkts bytes target     prot opt in     out     source               destination
    3   180 DNAT       tcp  --  eth1   *       0.0.0.0/0            0.0.0.0/0   tcp dpt:25 to:1

Chain POSTROUTING (policy ACCEPT 40 packets, 2514 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain OUTPUT (policy ACCEPT 27 packets, 1638 bytes)
 pkts bytes target     prot opt in     out     source               destination
```

4. Проверка трансляции SNAT

Где что дампим.

```
дамп SNAT в LAN (как вариант -i any tcp)
```

```
дамп SNAT (снаружи)
```

5. Проверка доступа к внутреннему серверу

```
s11:~# nc -lp 25
```

```
r1:~# tcpdump -nv -s 0 -i eth1 tcp
tcpdump: listening on eth1, link-type EN10MB (Ethernet), capture size 65535 bytes
08:20:12.969014 IP (tos 0x10, ttl 64, id 64807, offset 0, flags [DF], proto TCP (6), length 60)
ckOK,timestamp 4079445261 0,nop,wscale 7>
08:20:12.980724 IP (tos 0x0, ttl 63, id 0, offset 0, flags [DF], proto TCP (6), length 60) 172.
s 1460,sackOK,timestamp 166544 4079445261,nop,wscale 1>
08:20:12.980900 IP (tos 0x10, ttl 64, id 64808, offset 0, flags [DF], proto TCP (6), length 52)
544>

r1:~# tcpdump -nv -s 0 -i eth0 tcp
tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 65535 bytes
08:20:12.980453 IP (tos 0x10, ttl 63, id 64807, offset 0, flags [DF], proto TCP (6), length 60)
08:20:12.980707 IP (tos 0x0, ttl 64, id 0, offset 0, flags [DF], proto TCP (6), length 60) 10.1
08:20:12.980909 IP (tos 0x10, ttl 63, id 64808, offset 0, flags [DF], proto TCP (6), length 52)
```