

Отчёт по лабораторной работе «Локальные сети»

Гребенюк Александр Андреевич

17 декабря 2015 г.

Содержание

1	Получение адреса по DHCP	2
2	Использование VPN	4
3	Правила фильтрации пакетов и трансляции адресов	6
4	Проверка трансляции SNAT	7
5	Проверка правил фильтрации	8
6	Проверка доступа к внутреннему серверу	9

1. Получение адреса по DHCP

Получение “случайного” адреса **ws21** (дамп на **r2**):

```
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 > 255.255.255.255.67: BOOTP/DHCP, Request from
↪ 10:10:10:10:10:ee, length 300, xid 0xe3f347b, 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: 10.20.0.3
        Hostname Option 12, length 4: 'ws21'
        Parameter-Request Option 55, length 13:
            Subnet-Mask, BR, Time-Zone, Default-Gateway
            Domain-Name, Domain-Name-Server, Option 119, Hostname
            Netbios-Name-Server, Netbios-Scope, MTU,
↪ Classless-Static-Route
        NTP
56:70:e1:ed:b9:a2 > 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 > 10.20.0.3.68: BOOTP/DHCP, Reply, length 300, xid
↪ 0xe3f347b, Flags [none]
    Your-IP 10.20.0.3
    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
56:70:e1:ed:b9:a2 > 10:10:10:10:10:ee, ethertype ARP (0x0806), length 42:
↪ Ethernet (len 6), IPv4 (len 4), Request who-has 10.20.0.3 tell 10.20.0.1,
↪ length 28
10:10:10:10:10:ee > 56:70:e1:ed:b9:a2, ethertype ARP (0x0806), length 42:
↪ Ethernet (len 6), IPv4 (len 4), Reply 10.20.0.3 is-at 10:10:10:10:10:ee,
↪ length 28
```

Получение “фиксированного” адреса **ws11** (дамп на **r1**):

```
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 0x809ae340, 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
        Hostname Option 12, length 4: "ws11"
        Parameter-Request Option 55, length 13:
            Subnet-Mask, BR, Time-Zone, Default-Gateway
            Domain-Name, Domain-Name-Server, Option 119, Hostname
            Netbios-Name-Server, Netbios-Scope, MTU,
↪ Classless-Static-Route
    NTP
da:40:3e:6d:e6:8c > 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
↪ 0x809ae340, 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

Маршрутизатор r1:

```
root@r1:~# ip r
default via 172.16.1.2 dev eth1
10.10.0.0/16 dev eth0 proto kernel scope link src 10.10.0.1
10.20.0.0/16 via 10.100.100.2 dev tun0 proto zebra metric 2
10.100.100.2 dev tun0 proto kernel scope link src 10.100.100.1
172.16.0.0/16 dev eth1 proto kernel scope link src 172.16.1.3

root@r1:~# ip -4 a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue state UNKNOWN
    inet 127.0.0.1/8 scope host lo
2: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state
↪ UNKNOWN qlen 1000
    inet 172.16.1.3/16 brd 172.16.255.255 scope global eth1
3: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state
↪ UNKNOWN qlen 1000
    inet 10.10.0.1/16 brd 10.10.255.255 scope global eth0
4: tun0: <POINTOPOINT,MULTICAST,NOARP,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast
↪ state UNKNOWN qlen 100
    inet 10.100.100.1 peer 10.100.100.2/32 scope global tun0

ip: (tos 0xc0, ttl 1, id 18837, 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
ip: (tos 0xc0, ttl 1, id 35177, 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
ip: (tos 0xc0, ttl 1, id 18839, 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
ip: (tos 0xc0, ttl 1, id 35179, 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
```

```
ip: (tos 0xc0, ttl 1, id 18841, 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
```

Проверка работы VPN

```
root@ws21:~# traceroute 10.10.4.10
traceroute to 10.10.4.10 (10.10.4.10), 30 hops max, 60 byte packets
 1  10.20.0.1 (10.20.0.1)  0.185 ms  0.064 ms  0.068 ms
 2  10.100.100.1 (10.100.100.1)  1.835 ms  1.842 ms  1.836 ms
 3  10.10.4.10 (10.10.4.10)  1.814 ms  1.787 ms  1.779 ms
```

3. Правила фильтрации пакетов и трансляции пдресов

Где что дамвим.

сценарий фильтрации

`iptables -L -nv`

`iptables -L -nv -t nat`

4. Проверка трансляции SNAT

Где что дамвим.

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

дамп SNAT (снаружи)

5. Проверка правил фильтрации

Используем telnet.

6. Проверка доступа к внутреннему серверу

Используем telnet / веб-браузер на реальной машине. Должен быть виден DNAT и разрешённый доступ.