Отчёт по лабораторной работе «Локальные сети»

Гребенюк Александр Андреевич

26 декабря 2015 г.

Содержание

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 фильтации пакетов и трансляции пдресов

firewall rules

```
#!/bin/sh
LAN=eth0
INET=eth1
VPN=tun0
# Удаление всех правил в таблице ''filter'' (по-умолчанию).
iptables -F
# Удаление правил в таблице ''nat'' (её надо указать явно).
iptables -F -t nat

iptables -X

iptables --policy FORWARD DROP

iptables -A FORWARD -p icmp -j ACCEPT
iptables -A FORWARD -i $VPN -j ACCEPT
iptables -A FORWARD -o $VPN -j ACCEPT

iptables -A FORWARD -p tcp -i $LAN -o $INET -j ACCEPT
iptables -A FORWARD -p tcp --dport 9 -i $INET -j ACCEPT
iptables -t nat -A PREROUTING -p tcp -m tcp --dport 9 -i $INET -j DNAT --to
↪  10.10.1.1

iptables -t nat -A POSTROUTING -j MASQUERADE

iptables -A FORWARD -m state --state NEW -o $INET -j ACCEPT
iptables -A FORWARD -m state --state ESTABLISHED -i $INET -j ACCEPT
iptables -A FORWARD -p UDP --dport 53 -o $INET -j ACCEPT
```

iptables -L -nv

```
Chain FORWARD (policy DROP 11 packets, 572 bytes)
 pkts bytes target     prot opt in     out     source
↪  destination
   17  1120 ACCEPT     icmp --  *      *       0.0.0.0/0
↪  0.0.0.0/0
   52  2910 ACCEPT     all  --  tun0   *       0.0.0.0/0
↪  0.0.0.0/0
   38  2032 ACCEPT     all  --  *      tun0    0.0.0.0/0
↪  0.0.0.0/0
   16   868 ACCEPT     all  --  *      eth1    0.0.0.0/0
↪  0.0.0.0/0           state NEW
    8   620 ACCEPT     all  --  eth1   *       0.0.0.0/0
↪  0.0.0.0/0           state ESTABLISHED
    0     0 ACCEPT     udp  --  *      eth1    0.0.0.0/0
↪  0.0.0.0/0           udp dpt:53
```

iptables -L -nv -t nat

```
Chain PREROUTING (policy ACCEPT 27 packets, 1524 bytes)
 pkts bytes target     prot opt in     out     source
↪  destination
    0     0 DNAT       tcp  --  eth1   *       0.0.0.0/0
↪  0.0.0.0/0            tcp dpt:9 to:10.10.1.1:9

Chain INPUT (policy ACCEPT 3 packets, 196 bytes)
 pkts bytes target     prot opt in     out     source
↪  destination

Chain OUTPUT (policy ACCEPT 21 packets, 1423 bytes)
 pkts bytes target     prot opt in     out     source
↪  destination

Chain POSTROUTING (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source
↪  destination
   39  2511 MASQUERADE  all  --  *      *       0.0.0.0/0
↪  0.0.0.0/0
```

4. Проверка трансляции SNAT

ws11 - yandex.ru:80

```
IP 10.10.0.1.47455 > 10.10.1.1.discard: Flags [S], seq 2441485168, win
↪ 14600, options [mss 1366,sackOK,TS val 99584 ecr 0,nop,wscale 2], length
↪ 0
IP 10.10.1.1.discard > 10.10.0.1.47455: Flags [S.], seq 1813486520, ack
↪ 2441485169, win 14480, options [mss 1460,sackOK,TS val 126938 ecr
↪ 99584,nop,wscale 2], length 0
IP 10.10.0.1.47455 > 10.10.1.1.discard: Flags [.], ack 1, win 3650, options
↪ [nop,nop,TS val 99586 ecr 126938], length 0
IP 172.16.1.3.60625 > 192.168.1.1.domain: 54778+ PTR?
↪ 3.1.16.172.in-addr.arpa. (41)
IP 10.10.0.1.route > 224.0.0.9.route: RIPv2, Response, length: 44
IP 10.10.0.1.47455 > 10.10.1.1.discard: Flags [P.], seq 1:4, ack 1, win
↪ 3650, options [nop,nop,TS val 99729 ecr 126938], length 3
IP 10.10.1.1.discard > 10.10.0.1.47455: Flags [.], ack 4, win 3620, options
↪ [nop,nop,TS val 127081 ecr 99729], length 0
IP 10.10.0.1.47455 > 10.10.1.1.discard: Flags [P.], seq 4:7, ack 1, win
↪ 3650, options [nop,nop,TS val 99762 ecr 127081], length 3
IP 10.10.1.1.discard > 10.10.0.1.47455: Flags [.], ack 7, win 3620, options
↪ [nop,nop,TS val 127114 ecr 99762], length 0
IP 10.10.0.1.47455 > 10.10.1.1.discard: Flags [P.], seq 7:10, ack 1, win
↪ 3650, options [nop,nop,TS val 99790 ecr 127114], length 3
IP 10.10.1.1.discard > 10.10.0.1.47455: Flags [.], ack 10, win 3620, options
↪ [nop,nop,TS val 127142 ecr 99790], length 0
IP 10.10.0.1.47455 > 10.10.1.1.discard: Flags [F.], seq 10, ack 1, win 3650,
↪ options [nop,nop,TS val 100040 ecr 127142], length 0
IP 10.10.1.1.discard > 10.10.0.1.47455: Flags [F.], seq 1, ack 11, win 3620,
↪ options [nop,nop,TS val 127392 ecr 100040], length 0
```

ws21 - ws11:9

```
IP 10.20.0.3.47456 > 10.10.1.1.discard: Flags [S], seq 3948338987, win
↪ 14600, options [mss 1460,sackOK,TS val 132988 ecr 0,nop,wscale 2], length
↪ 0
IP 10.20.0.3.60211 > 10.20.0.1.domain: 44820+ PTR? 1.1.10.10.in-addr.arpa.
↪ (40)
IP 10.20.0.1.domain > 10.20.0.3.60211: 44820 Refused 0/0/0 (40)
IP 10.20.0.3.36353 > 10.20.0.1.domain: 44820+ PTR? 1.1.10.10.in-addr.arpa.
↪ (40)
IP 10.10.1.1.discard > 10.20.0.3.47456: Flags [S.], seq 643029704, ack
↪ 3948338988, win 14480, options [mss 1366,sackOK,TS val 160341 ecr
↪ 132988,nop,wscale 2], length 0
IP 10.20.0.3.47456 > 10.10.1.1.discard: Flags [.], ack 1, win 3650, options
↪ [nop,nop,TS val 132988 ecr 160341], length 0
IP 10.20.0.1.domain > 10.20.0.3.36353: 44820 Refused 0/0/0 (40)
```

```
IP 10.20.0.3.47456 > 10.10.1.1.discard: Flags [P.], seq 1:11, ack 1, win
↪ 3650, options [nop,nop,TS val 133196 ecr 160341], length 10
IP 10.10.1.1.discard > 10.20.0.3.47456: Flags [.], ack 11, win 3620, options
↪ [nop,nop,TS val 160549 ecr 133196], length 0
IP 10.20.0.1.route > 224.0.0.9.route: RIPv2, Response, length: 44
ARP, Request who-has 10.20.0.3 tell 10.20.0.1, length 28
ARP, Reply 10.20.0.3 is-at 10:10:10:10:10:ee (oui Unknown), length 28
IP 10.20.0.3.47456 > 10.10.1.1.discard: Flags [F.], seq 11, ack 1, win 3650,
↪ options [nop,nop,TS val 133598 ecr 160549], length 0
IP 10.10.1.1.discard > 10.20.0.3.47456: Flags [F.], seq 1, ack 12, win 3620,
↪ options [nop,nop,TS val 160950 ecr 133598], length 0
```

5. Проверка правил фильтрации

```
root@ws11:~# telnet ya.ru 80
Trying 213.180.193.3...
Connected to ya.ru.
Escape character is '^]'.
qwerty
^]
telnet> q
Connection closed.
```

6. Проверка доступа к внутреннему серверу

```
[amadeus@amadea net]$ telnet 172.16.1.3 9
Trying 172.16.1.3...
Connected to 172.16.1.3.
Escape character is '^]'.

lklk;klk
^]
telnet> q
Connection closed.
```