Отчёт по лабораторной работе «Локальные сети»

Здесь Ф. И. О

30 декабря 2021 г.

Содержание

1. Получение адреса по DHCP

Дампим командой tcpdump -tenv -s 1000 -i eth0 udp на R2, получение случайного адреса

```
10:10:10:10:10:ee > ff:ff:ff:ff:ff:ff, ethertype IPv4 (0x0800), length 342: (tos 0x10, ttl 128,
          Client-Ethernet-Address 10:10:10:10:10:ee
          Vendor-rfc1048 Extensions
            Magic Cookie 0x63825363
            DHCP-Message Option 53, length 1: Discover
            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,
          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,
          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,
          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
```

Дампим командой tcpdump -tenv -s 1000 -i eth0 udp на R1, получение фиксированного адреса

```
10:10:10:10:20:aa > ff:ff:ff:ff:ff:ff, ethertype IPv4 (0x0800), length 342: (tos 0x10, ttl 128,
          Client-Ethernet-Address 10:10:10:10:20:aa
          Vendor-rfc1048 Extensions
            Magic Cookie 0x63825363
            DHCP-Message Option 53, length 1: Discover
            Requested-IP Option 50, length 4: 10.10.4.10
            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 > 10:10:10:10:20:aa, ethertype IPv4 (0x0800), length 342: (tos 0x10, ttl 128,
          Your-IP 10.10.4.10
          Client-Ethernet-Address 10:10:10:10:20:aa
          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
```

```
10:10:10:10:20:aa > ff:ff:ff:ff:ff:ff, ethertype IPv4 (0x0800), length 342: (tos 0x10, ttl 128,
          Client-Ethernet-Address 10:10:10:10:20:aa
          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: 10.10.4.10
            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 > 10:10:10:10:20:aa, ethertype IPv4 (0x0800), length 342: (tos 0x10, ttl 128,
          Your-IP 10.10.4.10
          Client-Ethernet-Address 10:10:10:10:20:aa
          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

ip r на маршрутизаторе R1 после VPN и работы RIP

```
10.100.100.2 dev tun0  proto kernel  scope link  src 10.100.100.1
10.20.0.0/16 via 10.100.100.2 dev tun0  proto zebra  metric 2
10.10.0.0/16 dev eth0  proto kernel  scope link  src 10.10.0.1
172.16.0.0/16 dev eth1  proto kernel  scope link  src 172.16.1.3
default via 172.16.1.2 dev eth1
```

ip -4 a на маршрутизаторе R1

```
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 172.16.1.3/16 brd 172.16.255.255 scope global eth1
4: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000
    inet 10.10.0.1/16 brd 10.10.255.255 scope global eth0
5: tun0: <POINTOPOINT,MULTICAST,NOARP,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 100
    inet 10.100.100.1 peer 10.100.100.2/32 scope global tun0
```

просшулка сообщений RIP на tun0 tcpdump -tvn -i tun0 -s 1518 udp

```
IP (tos 0x0, ttl 1, id 0, offset 0, flags [DF], proto UDP (17), length 52) 10.100.100.2.520 > 2
        RIPv2, Response, length: 24, routes: 1
          AFI: IPv4:       10.20.0.0/16, tag 0x0000, metric: 1, next-hop: self
IP (tos 0x0, ttl 1, id 0, offset 0, flags [DF], proto UDP (17), length 52) 10.100.100.1.520 > 2
        RIPv2, Response, length: 24, routes: 1
          AFI: IPv4:       10.10.0.0/16, tag 0x0000, metric: 1, next-hop: self
```

Проверка работы VPN
Трейс с ws21 до s11

```
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)  7 ms  1 ms  11 ms
 2  10.100.100.1 (10.100.100.1)  3 ms  3 ms  3 ms
 3  10.10.4.10 (10.10.4.10)  14 ms  4 ms  3 ms
```

3. Правила фильтации пакетов и трансляции пдресов

```
#!/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
# По-умолчанию все маршрутизируемые пакеты выбрасываются.
iptables --policy FORWARD DROP
# ICMP разрешим
iptables -A FORWARD -p icmp -j ACCEPT
# Разрешаем любую маршрутизацию для интерфейса VPN
iptables -A FORWARD -i $VPN -j ACCEPT
iptables -A FORWARD -o $VPN -j ACCEPT
# Включение SNAT для маршрутизируемых пакетов, выходящих
# через eth1. Это правило выполняется после самой маршрутизации
# (POSTROUTING) и помещается в таблицу правил "nat".
iptables -t nat -A POSTROUTING -o $INET -j MASQUERADE
# Разрешение пакетов-ответов (они отслеживаются как
# -- state ESTABLISHED)
iptables -A FORWARD -m state --state ESTABLISHED -i $INET -j ACCEPT

iptables -A FORWARD -s 10.10.4.10 -p tcp --dport 80 -j ACCEPT
iptables -A FORWARD -s 10.10.4.20 -j ACCEPT



iptables -t nat -A PREROUTING -p tcp --dport 80 -j DNAT --to 10.10.4.10:80 -i $INET
iptables -A FORWARD -d 10.10.4.10 -p tcp --dport 80 -j ACCEPT
iptables -A FORWARD -s 10.10.4.10 -p tcp --sport 80 -o $INET -j ACCEPT
```

iptables -L -nv

```
Chain INPUT (policy ACCEPT 1708 packets, 134K bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain FORWARD (policy DROP 1 packets, 60 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 ACCEPT     icmp --  *      *       0.0.0.0/0            0.0.0.0/0
    0     0 ACCEPT     all  --  tun0   *       0.0.0.0/0            0.0.0.0/0
```

```
    0     0 ACCEPT     all  --  *      tun0    0.0.0.0/0            0.0.0.0/0
    6   385 ACCEPT     all  --  eth1   *       0.0.0.0/0            0.0.0.0/0           state E
    0     0 ACCEPT     tcp  --  *      *       10.10.4.10           0.0.0.0/0           tcp dpt
    6   337 ACCEPT     all  --  *      *       10.10.4.20           0.0.0.0/0
    0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            10.10.4.10          tcp dpt
    0     0 ACCEPT     tcp  --  *      eth1    10.10.4.10           0.0.0.0/0           tcp spt

Chain OUTPUT (policy ACCEPT 1303 packets, 105K bytes)
 pkts bytes target     prot opt in     out     source               destination
```

iptables -L -nv -t nat

```
Chain PREROUTING (policy ACCEPT 450 packets, 54516 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

Chain POSTROUTING (policy ACCEPT 16 packets, 828 bytes)
 pkts bytes target     prot opt in     out     source               destination
    1    60 MASQUERADE  all  --  *      eth1    0.0.0.0/0            0.0.0.0/0

Chain OUTPUT (policy ACCEPT 72 packets, 4607 bytes)
 pkts bytes target     prot opt in     out     source               destination
```

4. Проверка трансляции SNAT

Пинг yandex.ru с S11 ip - 10.10.4.10
Дамп на R1

```
13:45:51.465234  In 10:10:10:10:20:aa ethertype IPv4 (0x0800), length 100:
10.10.4.10 > 77.88.55.80: ICMP echo request, id 24834, seq 1, length 64
13:45:51.465280 Out fa:de:dc:30:96:57 ethertype IPv4 (0x0800), length 100:
172.16.1.3 > 77.88.55.80: ICMP echo request, id 24834, seq 1, length 64
13:45:51.625769  In a2:91:8c:7e:80:87 ethertype IPv4 (0x0800), length 100:
77.88.55.80 > 172.16.1.3: ICMP echo reply, id 24834, seq 1, length 64
13:45:51.625799 Out 0e:ab:f8:0c:10:4b ethertype IPv4 (0x0800), length 100:
77.88.55.80 > 10.10.4.10: ICMP echo reply, id 24834, seq 1, length 64
```

Дамп на локальном компьютере

```
16:47:49.981967  In fa:de:dc:30:96:57 ethertype IPv4 (0x0800), length 100:
172.16.1.3 > 77.88.55.60: ICMP echo request, id 25346, seq 1, length 64
16:47:49.982024 Out c0:b6:f9:e9:bd:ad ethertype IPv4 (0x0800), length 100:
192.168.184.194 > 77.88.55.60: ICMP echo request, id 25346, seq 1, length 64
16:47:50.072943  In aa:07:27:7b:fd:35 ethertype IPv4 (0x0800), length 100:
77.88.55.60 > 192.168.184.194: ICMP echo reply, id 25346, seq 1, length 64
16:47:50.072994 Out a2:91:8c:7e:80:87 ethertype IPv4 (0x0800), length 100:
77.88.55.60 > 172.16.1.3: ICMP echo reply, id 25346, seq 1, length 64
```

5. Проверка правил фильтрации

Проверка доступа к 80 порту из машины S11
telnet google.com 80

```
Trying 216.58.209.206...
Connected to google.com.
Escape character is '^]'.
hey
HTTP/1.0 400 Bad Request
Content-Type: text/html; charset=UTF-8
Referrer-Policy: no-referrer
Content-Length: 1555
Date: Sun, 26 Dec 2021 14:08:41 GMT

<!DOCTYPE html>
<html lang=en>
  <meta charset=utf-8>
  <meta name=viewport content="initial-scale=1, minimum-scale=1, width=device-width">
  <title>Error 400 (Bad Request)!!1</title>
  <style>
    *margin:0;padding:0html,codefont:15px/22px arial,sans-serifhtmlbackground:#fff;color:#222;p
  </style>
  <a href=//www.google.com/><span id=logo aria-label=Google></span></a>
  <p><b>400.</b> <ins>That's an error.</ins>
  <p>Your client has issued a malformed or illegal request.  <ins>That's all we know.</ins>
Connection closed by foreign host.
```

Проверка доступа ко всем адресам из машины S12
telnet bmstu.ru 22

```
Trying 195.19.50.250...
Connected to bmstu.ru.
Escape character is '^]'.
SSH-2.0-OpenSSH_8.0
dfd
Invalid SSH identification string.
Connection closed by foreign host.
s12:~# telnet bmstu.ru 22
Trying 195.19.50.250...
Connected to bmstu.ru.
Escape character is '^]'.
sds
SSH-2.0-OpenSSH_8.0
Invalid SSH identification string.
Connection closed by foreign host.
```

6. Проверка доступа к внутреннему серверу

telnet 172.16.1.3 80

```
Trying 172.16.1.3...
Connected to 172.16.1.3.
Escape character is '^]'.
hey
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>501 Method Not Implemented</title>
</head><body>
<h1>Method Not Implemented</h1>
<p>hey to /index.html not supported.<br />
</p>
<hr>
<address>Apache/2.2.9 (Debian) Server at 127.0.0.1 Port 80</address>
</body></html>
```