

# Router IP

Patryk Kaniewski

2020-10-22

## Spis Treści

<b>1</b>	<b>Grupa wykonująca zadanie</b>	<b>2</b>
<b>2</b>	<b>Wstęp</b>	<b>2</b>
2.1	Cel ćwiczenia . . . . .	2
2.2	Schemat ćwiczenia . . . . .	2
2.3	Wymagany sprzęt . . . . .	2
2.4	Plan ćwiczenia . . . . .	2
<b>3</b>	<b>Ćwiczenie</b>	<b>3</b>
3.1	Wstępna konfiguracja . . . . .	3
3.2	Badanie zachowania NAT . . . . .	4
3.3	Wyłączenie NAT . . . . .	5
3.4	Badanie zachowania Routera bez NAT . . . . .	6
<b>4</b>	<b>Wnioski</b>	<b>7</b>
4.1	Działanie NAT . . . . .	7
4.2	Napotkane problemy . . . . .	7

## 1 Grupa wykonująca zadanie

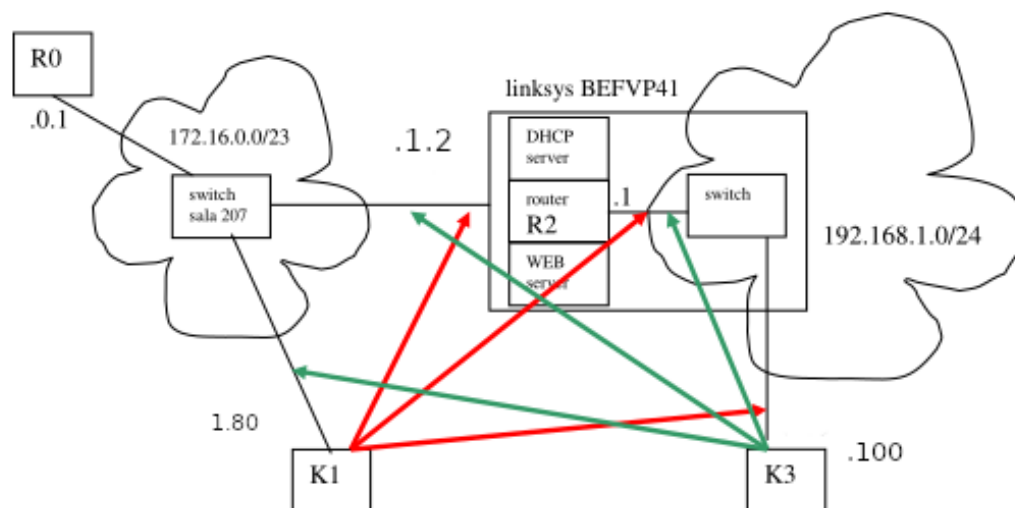
- Patryk Kaniewski
- Jakub Caban
- Dominik Gandziarek

## 2 Wstęp

### 2.1 Cel ćwiczenia

Celem ćwiczenia jest pokazanie w jaki sposób NAT (Network Address Translation) ukrywa strukturę sieci wewnętrznej

### 2.2 Schemat ćwiczenia



### 2.3 Wymagany sprzęt

- Router z możliwością wyłączenia NAT (np Linksys BEFVP41)
- 2 Komputery osobiste
- skrzętka komputerowa UTP zakończona 8PC8 (np. cat5e)

### 2.4 Plan ćwiczenia

1. Podłączenie routera i komputerów wg. schematu
2. Włączenie i zalogowanie się na router i komputery (może być potrzebne konto administratora)

3. Badanie zachowania się sieci NAT (np. ping K1<->R1<->K3)
4. Wyłączenie sieci NAT na routerze (w BEFVP41 NAT Setup->Advanced Routing->Dynamic Routing->NAT->Disabled)
5. Ustawienie ręcznej konfiguracji R1 (zmiana domyślnej bramy na WAN routera)

## 3 Ćwiczenie

### 3.1 Wstępna konfiguracja

#### 3.1.1 K1

Ethernet adapter Ethernet:

```
Connection-specific DNS Suffix . : pwsz.pk
Link-local IPv6 Address . . . . . : fe80::1cb5:9d48:9e1b:f847%11
IPv4 Address. . . . . : 172.16.1.80
Subnet Mask . . . . . : 255.255.254.0
Default Gateway . . . . . : 172.16.0.1~
```

#### 3.1.2 K3

Windows IP Configuration

Ethernet adapter Ethernet:

```
Connection-specific DNS Suffix . : pwsz.pk
Link-local IPv6 Address . . . . . : fe80::dc70:7154:4ecd:c188%4
IPv4 Address. . . . . : 192.168.1.100
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.1.1
```

### 3.1.3 R1

The screenshot shows the Linksys Status page. At the top, there is a navigation bar with tabs: Setup, VPN, Password, Status (selected), DHCP, Log, Help, and Advanced. Below the navigation bar, a message states: "This screen displays the router's current status and settings. This information is read-only." The main content area is titled "STATUS" and contains the following information:

- Host Name:** (empty)
- Firmware Version:** 1.41e, Aug 05 2003
- Current Time:** Oct. 22 2020 Thu. 0:15:25
- Login:** Disable
- LAN:** (MAC Address: 00-0C-41-AD-90-6C)
  - IP Address:** 192.168.1.1
  - Subnet Mask:** 255.255.255.0
  - DHCP server:** Enabled
- WAN:** (MAC Address: 00-0C-41-AD-90-6D)
  - IP Address:** 172.16.1.2
  - Subnet Mask:** 255.255.254.0
  - Default Gateway:** 172.16.0.1
  - DNS:** 172.16.0.10, 172.16.0.12, 0.0.0.0
  - DHCP Remaining Time:** 23:10:44

At the bottom, there are buttons for "DHCP Release", "DHCP Renew", "DHCP Clients Table", and "Help".

## 3.2 Badanie zachowania NAT

### 3.2.1 K3 -> K1

Pingowanie z sieci NAT do sieci zewnętrznej jest normalnym zachowaniem które można zaobserwować podczas poprawnego działania większości połączeń internetowych

Pinging 172.16.1.80 with 32 bytes of data:

Reply from 172.16.1.80: bytes=32 time=2ms TTL=128

Reply from 172.16.1.80: bytes=32 time=2ms TTL=128

Reply from 172.16.1.80: bytes=32 time=3ms TTL=128

Reply from 172.16.1.80: bytes=32 time=2ms TTL=128

Ping statistics for 172.16.1.80:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

Approximate round trip times in milli-seconds:

Minimum = 2ms, Maximum = 3ms, Average = 2ms

Jak widać adresem źródłowym jest adres zewnętrzny routera IP a nie K3

No.	Time	Source	Destination	Protocol	Length	Info
20	2.946457	172.16.1.2	172.16.1.80	ICMP	74	Echo (ping) request id=0x0001, seq=28/7168, ttl=128 (reply in 21)
21	2.947332	172.16.1.80	172.16.1.2	ICMP	74	Echo (ping) reply id=0x0001, seq=28/7168, ttl=128 (request in 20)
26	3.950748	172.16.1.2	172.16.1.80	ICMP	74	Echo (ping) request id=0x0001, seq=29/7424, ttl=128 (reply in 27)
27	3.951628	172.16.1.80	172.16.1.2	ICMP	74	Echo (ping) reply id=0x0001, seq=29/7424, ttl=128 (request in 26)
30	4.958826	172.16.1.2	172.16.1.80	ICMP	74	Echo (ping) request id=0x0001, seq=30/7680, ttl=128 (reply in 31)
31	4.959176	172.16.1.80	172.16.1.2	ICMP	74	Echo (ping) reply id=0x0001, seq=30/7680, ttl=128 (request in 30)
33	5.968666	172.16.1.2	172.16.1.80	ICMP	74	Echo (ping) request id=0x0001, seq=31/7936, ttl=128 (reply in 34)
34	5.969564	172.16.1.80	172.16.1.2	ICMP	74	Echo (ping) reply id=0x0001, seq=31/7936, ttl=128 (request in 33)

### 3.2.2 K1 -> K3

NAT nie pozwala pingować wewnętrznych zasobów sieciowych

Pinging 192.168.1.100 with 32 bytes of data:

Request timed out.

Request timed out.

Request timed out.

Request timed out.

Ping statistics for 192.168.1.100:

Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

### 3.2.3 K1-> R2(LAN)

Jak iż nie widzimy wewnętrznej sieci, pingi na adres wewnętrzny również są odrzucane

Pinging 192.168.1.1 with 32 bytes of data:

Request timed out.

Request timed out.

Request timed out.

Request timed out.

Ping statistics for 192.168.1.1:

Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

## 3.3 Wyłączenie NAT

Należy wyłączyć router NAT na routerze. Dla Linksys NAT Setup->Advanced Routing->Dynamic Routing->NAT->Disabled.

### 3.3.1 K1

Aby umożliwić dwustronna komunikacje musimy ręcznie ustawić interfejs sieciowy na K1.

Należy ustawić bramę domyślną na adres WAN R2 (w naszym przypadku 172.16.1.2).

Windows IP Configuration

Ethernet adapter Ethernet:

```
Connection-specific DNS Suffix . :
Link-local IPv6 Address . . . . . : fe80::1cb5:9d48:9e1b:f847%11
IPv4 Address. . . . . : 172.16.1.80
Subnet Mask . . . . . : 255.255.254.0
Default Gateway . . . . . : 172.16.1.2
```

### 3.4 Badanie zachowania Routera bez NAT

#### 3.4.1 K3->K1

Połączenie z sieci wewnętrznej na zewnątrz nadal jest utrzymane.

```
Pinging 172.16.1.80 with 32 bytes of data:
Reply from 172.16.1.80: bytes=32 time=2ms TTL=127
Reply from 172.16.1.80: bytes=32 time=2ms TTL=127
Reply from 172.16.1.80: bytes=32 time=2ms TTL=127
Reply from 172.16.1.80: bytes=32 time=2ms TTL=127
```

```
Ping statistics for 172.16.1.80:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 2ms, Average = 2ms
```

#### 3.4.2 K1->K3

Po wyłączeniu translacji adresów, mamy pełen dostęp do sieci wewnętrznej 192.168.1.0/24.

```
Pinging 192.168.1.100 with 32 bytes of data:
Reply from 192.168.1.100: bytes=32 time=2ms TTL=127
Reply from 192.168.1.100: bytes=32 time=2ms TTL=127
Reply from 192.168.1.100: bytes=32 time=3ms TTL=127
Reply from 192.168.1.100: bytes=32 time=3ms TTL=127
```

```
Ping statistics for 192.168.1.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 3ms, Average = 2ms
```

Możemy zaobserwować jawność adresów obydwu maszyn.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.00000000	172.16.1.80	192.168.1.100	ICMP	74	Echo (ping) request id=0x0001, seq=119/30464, ttl=127 (reply in 2)
2	0.00092000	192.168.1.100	172.16.1.80	ICMP	74	Echo (ping) reply id=0x0001, seq=119/30464, ttl=128 (request in 1)
3	0.11071700	192.168.1.100	213.241.62.154	TCP	66	63733->8001 [SYN] Seq=0 win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
4	1.00406300	172.16.1.80	192.168.1.100	ICMP	74	Echo (ping) request id=0x0001, seq=120/30720, ttl=127 (reply in 5)
5	1.00493900	192.168.1.100	172.16.1.80	ICMP	74	Echo (ping) reply id=0x0001, seq=120/30720, ttl=128 (request in 4)
6	2.01404200	172.16.1.80	192.168.1.100	ICMP	74	Echo (ping) request id=0x0001, seq=121/30976, ttl=127 (reply in 7)
7	2.01454800	192.168.1.100	172.16.1.80	ICMP	74	Echo (ping) reply id=0x0001, seq=121/30976, ttl=128 (request in 6)
8	3.16802400	172.16.1.80	192.168.1.100	ICMP	74	Echo (ping) request id=0x0001, seq=122/31232, ttl=127 (no response found!)
9	3.16837800	192.168.1.100	172.16.1.80	ICMP	74	Echo (ping) reply id=0x0001, seq=122/31232, ttl=128 (request in 8)
10	3.19056200	192.168.1.100	91.228.166.16	TCP	66	63726->80 [SYN] Seq=0 win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1

#### 3.4.3 K1->R2

Po usunięciu blokady na pingi na routerze (patrz 4.2). Możemy pingować wszystkie interfejsy routera z sieci wewnętrznej.

```
Pinging 192.168.1.1 with 32 bytes of data:
Reply from 192.168.1.1: bytes=32 time=1ms TTL=150
Reply from 192.168.1.1: bytes=32 time=1ms TTL=150
Reply from 192.168.1.1: bytes=32 time=1ms TTL=150
Reply from 192.168.1.1: bytes=32 time=1ms TTL=150
```

```
Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 1ms, Average = 1ms
```

```
Pinging 172.16.1.2 with 32 bytes of data:
Reply from 172.16.1.2: bytes=32 time=1ms TTL=150
Reply from 172.16.1.2: bytes=32 time=1ms TTL=150
Reply from 172.16.1.2: bytes=32 time=1ms TTL=150
Reply from 172.16.1.2: bytes=32 time=1ms TTL=150
```

```
Ping statistics for 172.16.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 1ms, Average = 1ms
```

## 4 Wnioski

### 4.1 Działanie NAT

NAT maskuje wszystkie urządzenia które się za nim znajdują. Utrudnia on zewnętrzny dostęp do wewnętrznych zasobów sieciowych. Wewnętrzne urządzenia wychodząc na sieci zewnętrzne są ukrywane (router NAT nadpisuje w pakiecie IP pole source adress).

### 4.2 Napotkane problemy

Domyślnie router Linksys blokuje zewnętrzne pingi.

Tą opcję można wyłączyć w Filters-> Block WAN Request



[Filters](#)
[Forwarding](#)
[Dynamic Routing](#)
[Static Routing](#)
[DMZ Host](#)
[MAC Clone](#)
[DDNS](#)
[Setup](#)

## FILTERS

Filters enable you to prevent certain PCs on your network from accessing your Internet connection.

Filtered Private IP Range:

(0 to 254)

1: 192.168.1.0 ~ 0

2: 192.168.1.0 ~ 0

3: 192.168.1.0 ~ 0

4: 192.168.1.0 ~ 0

5: 192.168.1.0 ~ 0

Filtered Private Port Range:

(0 to 65535)

1: Both 0 ~ 0

2: Both 0 ~ 0

3: Both 0 ~ 0

4: Both 0 ~ 0

5: Both 0 ~ 0

Private MAC Filter

[Edit MAC Filter Setting](#)

Block WAN Request: ☐ Enable ☒ Disable

Multicast Pass Through: ☒ Enable ☐ Disable

IPSec Pass Through: ☒ Enable ☐ Disable

PPTP Pass Through: ☒ Enable ☐ Disable

Remote Management: ☐ Enable ☒ Disable Port: 8080

Remote Upgrade: ☐ Enable ☒ Disable

MTU: ☐ Enable ☒ Disable Size: 0

[Apply](#)
[Cancel](#)
[Help](#)