Badanie tunelowania

lp	wykonawca	grupa (*g*)
1.	*Grzegorz Pol*	***3***
2.	*Michał Grzybowski*	
3.	*Artur Mazur*	

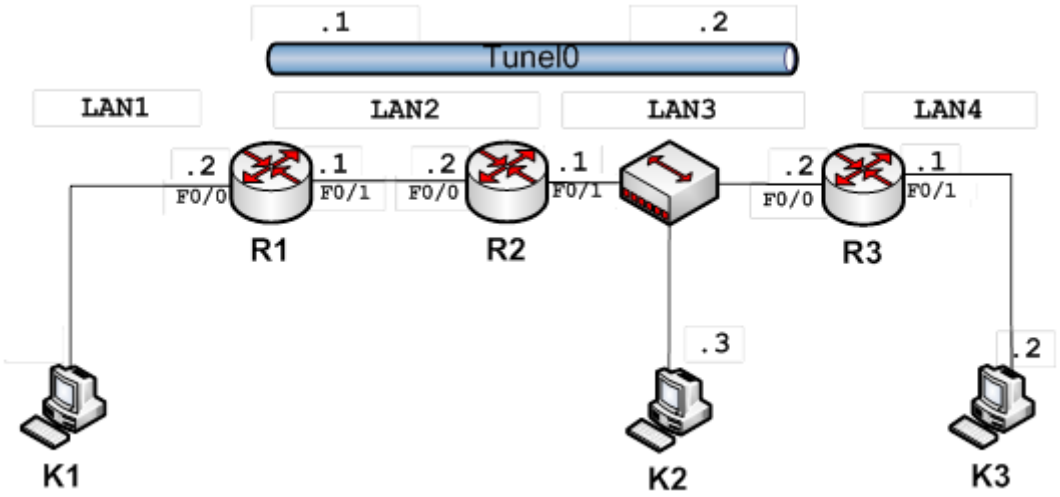
zadanie	rodzaj tunelowania	typ tunelu	wybór
5.	Wyspy IPv4 podłączone przez środowisko IPv6	GRE	x

Tabela 1. Plan adresacji:

	IPv4	IPv6
LAN1	21.31.1.0/24	x
LAN2	x	2001:32:2:2::/64
LAN3	x	2001:33:3:3::/64
LAN4	21.34.4.0/24	x
Tunel0	10.3.0.0/24	x

Topologia:

Ze względu na niewystarczającą ilość switchów oraz znikome ich znaczenie podłączyliśmy komputery K1 i K3 bezpośrednio do routerów zgodnie z poniższą poprawioną już przeze mnie topologią.



1. **Wyznaczyć adresy dla elementów składowych sieci na podstawie tabeli 1 zależnie od numeru grupy (G) i numeru zadania. Wyniki podać w poniższej tabeli:**

nazwa urządzenia	interfejs	adres/maska
R1	**F0/0**	*21.31.1.1 / 24*
	F0/1	*2001:32:2:2::1 / 64*
	Tunnel0	*10.3.0.2 / 24*
R2	**F0/0**	*2001:32:2:2::2 / 64*
	F0/1	*2001:33:3:3::1 / 64*
R3	**F0/0**	*2001:33:3:3::2 / 64*
	F0/1	*21.31.4.1 / 24*
	Tunnel0	*10.3.0.1 / 24*
K1	**Eth0**	*21.31.1.2 / 24*
K2	**Eth0**	*2001:33:3:3:20c:29ff:fefe:10f / 64*
K3	**Eth0**	*21.34.4.2 / 24*

2. **Przygotowanie topologii sieci:**
   A. Zbudować sieć według podanej topologii i wyznaczonego planu adresacji. Poniżej wkleić zrzut ekranu z konfiguracją interfejsów routera **R2** i komputerów **K1**, **K2** i **K3**.

Router R2 *w naszym przypadku ma tylko interfejsy v6. Wklejam wyłącznie najważniejsze dane, o poprawnie skonfigurowanych interfejsach.*

```
R2#show ipv6 interface
FastEthernet0/0 is up, line protocol is up
  IPv6 is enabled, link-local address is FE80::1AEF:63FF:FED9:4D18
  No Virtual link-local address(es):
  Global unicast address(es):
    2001:32:2:2:2::2, subnet is 2001:32:2:2::/64
FastEthernet0/1 is up, line protocol is up
  IPv6 is enabled, link-local address is FE80::1AEF:63FF:FED9:4D19
  No Virtual link-local address(es):
  Global unicast address(es):
    2001:33:3:3:3::1, subnet is 2001:33:3:3::/64
```

Komputer K1 *znajduje się w sieci Lan1 o adresie 21.31.1.0 / 24 i posiada adres 21.31.1.1 / 24.*

```
C:\Documents and Settings\Administrator>ipconfig /all

Konfiguracja IP systemu Windows

        Nazwa hosta . . . . . . . . . . . . : laboratorium
        Sufiks podstawowej domeny DNS . . . . . :
        Typ węzła . . . . . . . . . . . . . : Nieznany
        Routing IP włączony . . . . . . . . : Nie
        Serwer WINS Proxy włączony. . . . . : Nie

Karta Ethernet Połączenie lokalne 2:

        Sufiks DNS konkretnego połączenia :
        Opis . . . . . . . . . . . . . . . :  VMware Accelerated AMD PCNet Adapter

        Adres fizyczny. . . . . . . . . . . : 00-0C-29-94-BE-38
        DHCP włączone . . . . . . . . . . . : Nie
        Adres IP. . . . . . . . . . . . . . : 21.31.1.2
        Maska podsieci. . . . . . . . . . . : 255.255.255.0
        Brama domyślna. . . . . . . . . . . :
```

Komputer K2 *znajduje się w sieci Lan3 o adresie 2001:33:3:3:: / 64 i posiada adres 2001:33:3:3:20c:29ff:fefe:10f / 64*

```
C:\Documents and Settings\Administrator>ipconfig /all

Konfiguracja IP systemu Windows

        Nazwa hosta . . . . . . . . . . . . : laboratorium
        Sufiks podstawowej domeny DNS . . . . . . . :
        Typ węzła . . . . . . . . . . . . . : Nieznany
        Routing IP włączony . . . . . . . . : Nie
        Serwer WINS Proxy włączony. . . . . : Nie

Karta Ethernet Połączenie lokalne 2:

        Sufiks DNS konkretnego połączenia :
        Opis . . . . . . . . . . . . . . . :  VMware Accelerated AMD PCNet Adap

        Adres fizyczny. . . . . . . . . . . : 00-0C-29-FE-01-0F
        DHCP włączone . . . . . . . . . . . : Tak
        Autokonfiguracja włączona . . . . . : Tak
        Adres IP. . . . . . . . . . . . . . : 10.5.239.89
        Maska podsieci. . . . . . . . . . . : 255.255.255.0
        Adres IP. . . . . . . . . . . . . . : 2001:33:3:3:649d:f123:2b28:3ee7
        Adres IP. . . . . . . . . . . . . . : 2001:33:3:3:20c:29ff:fefe:10f
        Adres IP. . . . . . . . . . . . . . : fe80::20c:29ff:fefe:10f%5
        Brama domyślna. . . . . . . . . . . : 10.5.239.254
                                              fe80::5abc:27ff:fe39:cf98%5
                                              fe80::1aef:63ff:fed9:4d19%5
        Serwer DHCP . . . . . . . . . . . . : 10.5.239.254
        Serwery DNS . . . . . . . . . . . . : 10.3.57.1
                                              10.1.0.1
                                              fec0:0:0:ffff::1%1
                                              fec0:0:0:ffff::2%1
                                              fec0:0:0:ffff::3%1
        Dzierżawa uzyskana. . . . . . . . . : 28 marca 2012 16:40:13
        Dzierżawa wygasa. . . . . . . . . . : 28 marca 2012 20:40:13
```

Komputer K3 *znajduje się w sieci Lan4 o adresie 21.34.4.0 / 24 i posiada adres 21.34.4.2 / 24*

```
C:\Documents and Settings\Administrator>ipconfig /all

Konfiguracja IP systemu Windows

        Nazwa hosta . . . . . . . . . . . . : laboratorium
        Sufiks podstawowej domeny DNS . . . . . . . :
        Typ węzła . . . . . . . . . . . . . : Nieznany
        Routing IP włączony . . . . . . . . : Nie
        Serwer WINS Proxy włączony. . . . . : Nie

Karta Ethernet Połączenie lokalne 2:

        Sufiks DNS konkretnego połączenia :
        Opis . . . . . . . . . . . . . . . :  VMware Accelerated AMD PCNet A

        Adres fizyczny. . . . . . . . . . . : 00-0C-29-93-B6-0F
        DHCP włączone . . . . . . . . . . . : Nie
        Adres IP. . . . . . . . . . . . . . : 21.34.4.2
        Maska podsieci. . . . . . . . . . . : 255.255.255.0
        Brama domyślna. . . . . . . . . . . :
```

B. Sprawdzić wzajemną osiągalność sąsiadów przy pomocy komendy **`ping`**.

```
C:\Documents and Settings\Administrator>ping 21.31.1.1

Badanie 21.31.1.1 z użyciem 32 bajtów danych:

Odpowiedź z 21.31.1.1: bajtów=32 czas=1ms TTL=255
Odpowiedź z 21.31.1.1: bajtów=32 czas=1ms TTL=255
Odpowiedź z 21.31.1.1: bajtów=32 czas=1ms TTL=255
Odpowiedź z 21.31.1.1: bajtów=32 czas=1ms TTL=255

Statystyka badania ping dla 21.31.1.1:
    Pakiety: Wysłane = 4, Odebrane = 4, Utracone = 0 (0% straty),
Szacunkowy czas błądzenia pakietów w millisekundach:
    Minimum = 1 ms, Maksimum = 1 ms, Czas średni = 1 ms
```

Komputery K1 i K3 widzą wyłącznie interfejs swojego routera, który tak jak one jest w sieci IPv4. Na screenie obok komputer K1 pinguje interfejs Fa0/0 routera R1.

```
C:\Documents and Settings\Administrator>ping6 -s 2001:33:3:3:20c:29ff:fefe:10f 2
001:33:3:3:3::2

Badanie 2001:33:3:3:3::2
z 2001:33:3:3:20c:29ff:fefe:10f z użyciem 32 bajtów danych:

Odpowiedź z 2001:33:3:3:3::2: bajtów=32 czas=1 ms
Odpowiedź z 2001:33:3:3:3::2: bajtów=32 czas=1 ms
Odpowiedź z 2001:33:3:3:3::2: bajtów=32 czas<1 ms
Odpowiedź z 2001:33:3:3:3::2: bajtów=32 czas<1 ms

Statystyka badania dla 2001:33:3:3:3::2:
    Pakiety: Wysłane = 4, Odebrane = 4, Utracone = 0 (0% utraconych),
Szacunkowy czas błądzenia pakietów w millisekundach:
    Minimum = 0 ms, Maksimum =  1 ms, Średnia =  0 ms

C:\Documents and Settings\Administrator>ping6 -s 2001:33:3:3:20c:29ff:fefe:10f 2
001:33:3:3:3::1

Badanie 2001:33:3:3:3::1
z 2001:33:3:3:20c:29ff:fefe:10f z użyciem 32 bajtów danych:

Odpowiedź z 2001:33:3:3:3::1: bajtów=32 czas=1 ms
Odpowiedź z 2001:33:3:3:3::1: bajtów=32 czas<1 ms
Odpowiedź z 2001:33:3:3:3::1: bajtów=32 czas=1 ms
Odpowiedź z 2001:33:3:3:3::1: bajtów=32 czas=1 ms

Statystyka badania dla 2001:33:3:3:3::1:
    Pakiety: Wysłane = 4, Odebrane = 4, Utracone = 0 (0% utraconych),
Szacunkowy czas błądzenia pakietów w millisekundach:
    Minimum = 0 ms, Maksimum =  1 ms, Średnia =  0 ms

C:\Documents and Settings\Administrator>ping6 -s 2001:33:3:3:20c:29ff:fefe:10f 2
001:32:2:2:2::2

Badanie 2001:32:2:2:2::2
z 2001:33:3:3:20c:29ff:fefe:10f z użyciem 32 bajtów danych:

Odpowiedź z 2001:32:2:2:2::2: bajtów=32 czas<1 ms
Odpowiedź z 2001:32:2:2:2::2: bajtów=32 czas=1 ms
Odpowiedź z 2001:32:2:2:2::2: bajtów=32 czas=2 ms
Odpowiedź z 2001:32:2:2:2::2: bajtów=32 czas=1 ms

Statystyka badania dla 2001:32:2:2:2::2:
    Pakiety: Wysłane = 4, Odebrane = 4, Utracone = 0 (0% utraconych),
Szacunkowy czas błądzenia pakietów w millisekundach:
    Minimum = 0 ms, Maksimum =  2 ms, Średnia =  1 ms

C:\Documents and Settings\Administrator>ping6 -s 2001:33:3:3:20c:29ff:fefe:10f 2
001:32:2:2:2::1

Badanie 2001:32:2:2:2::1
z 2001:33:3:3:20c:29ff:fefe:10f z użyciem 32 bajtów danych:

Odpowiedź z 2001:32:2:2:2::1: bajtów=32 czas=1 ms
Odpowiedź z 2001:32:2:2:2::1: bajtów=32 czas=1 ms
Odpowiedź z 2001:32:2:2:2::1: bajtów=32 czas=1 ms
Odpowiedź z 2001:32:2:2:2::1: bajtów=32 czas=1 ms

Statystyka badania dla 2001:32:2:2:2::1:
    Pakiety: Wysłane = 4, Odebrane = 4, Utracone = 0 (0% utraconych),
Szacunkowy czas błądzenia pakietów w millisekundach:
    Minimum = 1 ms, Maksimum =  1 ms, Średnia =  1 ms
```

Komputer K2 jest osiągalny natomiast w całej dobrze już skonfigurowanej sieci IPv6. Wynik ten był przez nas oczekiwany. Po prawej znajduje się screen, na którym możemy zaobserwować poprawne pingowanie wszystkich interfejsów IPv6 z komputera K2. Komputer K2 oczywiście nie był osiągalny z obu interfejsów IPv4 ani komputerów K1 i K3.

Poniżej też przedstawiam screen, na którym możemy zauważyć, że próba wysłania pakietów ICMP z routera R1 na interfejs Fa0/0 routera R3 zakończyła się sukcesem.

```
R1#ping 2001:33:3:3:3::2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:33:3:3:3::2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/4 ms
```

Podsumowując: urządzenia znajdujące się w sieci o tym samym protokole widzą się nawzajem chyba, że są przedzielone siecią bazującą na innym protokole niż one same.

C. Sprawdzić działanie snifera WireShark na komputerze **K2**.

Niestety podczas wykonywania zadania na zajęciach laboratoryjnych przeoczyliśmy powyższy podpunkt (zauważyliśmy go dopiero w momencie kiedy tunel już powstał). Korzystając z doświadczenia z poprzednich zajęć laboratoryjnych możemy przypuszczać, że powinniśmy zaobserwować:

- *wiadomości MLD (Multicast Listener Report Message) skierowane na adres multicastowy,*
- *wiadomości Router Advertisement na adres multicast*
- *wiadomości na zarezerwowane adresy do automatycznego wykrywania serwerów DNS*
- *wiadomości Neihbor Solicitation i Neighbor Advertisement mających na celu połączenia sąsiadujących węzłów*

3. Badanie tunelu:

A. Skonfigurować tunel pomiędzy routerami **R1** i **R3**. Poniżej wkleić zrzut ekranu z poprawną konfiguracją routera **R1** i **R3**

Po skonfigurowaniu wpisaliśmy polecenie show ip interface w celu pokazania, że Tunel0 został skonfigurowany. Ze screenu zostały wycięte mniej znaczące fragmenty:

```
R1#show ip interface
FastEthernet0/0 is up, line protocol is up
  Internet address is 21.31.1.1/24
  Broadcast address is 255.255.255.255
```

```
FastEthernet0/1 is up, line protocol is up
  Internet protocol processing disabled
Serial0/0/0 is administratively down, line protocol is down
  Internet protocol processing disabled
Serial0/0/1 is administratively down, line protocol is down
  Internet protocol processing disabled
Tunnel0 is up, line protocol is up
  Internet address is 10.3.0.2/24
  Broadcast address is 255.255.255.255
```

Te same polecenie wpisaliśmy w konsoli routera R3 (show ip interface). Niestety fragment, w którym widać, że Tunnel0 jest „up" nie zmieściły się na wykonanym przez nas screenie. W punkcie C jego istnienie i poprawne skonfigurowanie zostanie potwierdzone za pomocą polecenie „show interface tunnel0".

```
FastEthernet0/0 is up, line protocol is up
  Internet protocol processing disabled
FastEthernet0/1 is up, line protocol is up
  Internet address is 21.34.4.1/24
  Broadcast address is 255.255.255.255
```

B. Zweryfikować poprawność działania tunelu. Sprawdzić osiągalność interfejsu komputera **K3** z komputera **K1**. Poniżej wkleić zrzut ekranu potwierdzający działanie tunelu.

```
C:\Documents and Settings\Administrator>ping 21.34.4.1

Badanie 21.34.4.1 z użyciem 32 bajtów danych:

Odpowiedź z 21.34.4.1: bajtów=32 czas=3ms TTL=254
Odpowiedź z 21.34.4.1: bajtów=32 czas=3ms TTL=254
Odpowiedź z 21.34.4.1: bajtów=32 czas=3ms TTL=254
Odpowiedź z 21.34.4.1: bajtów=32 czas=3ms TTL=254

Statystyka badania ping dla 21.34.4.1:
    Pakiety: Wysłane = 4, Odebrane = 4, Utracone = 0 (0% straty),
Szacunkowy czas błądzenia pakietów w millisekundach:
    Minimum = 3 ms, Maksimum = 3 ms, Czas średni = 3 ms
```

Pierwszy od góry screen przedstawia pozytywny wynik pingowania komputera K3 z komputera K1. Sieć Lan1 komunikuje się z siecią Lan4.

Drugi screen przedstawia natomiast próbę pingowania komputera K1 oraz interfejsu Fa0/0 na routerze R1. Obie próby zakończyły się sukcesem.

```
C:\Documents and Settings\Administrator>ping 21.31.1.2

Badanie 21.31.1.2 z użyciem 32 bajtów danych:

Odpowiedź z 21.31.1.2: bajtów=32 czas=5ms TTL=126
Odpowiedź z 21.31.1.2: bajtów=32 czas=4ms TTL=126
Odpowiedź z 21.31.1.2: bajtów=32 czas=4ms TTL=126
Odpowiedź z 21.31.1.2: bajtów=32 czas=3ms TTL=126

Statystyka badania ping dla 21.31.1.2:
    Pakiety: Wysłane = 4, Odebrane = 4, Utracone = 0 (0% straty),
Szacunkowy czas błądzenia pakietów w millisekundach:
    Minimum = 3 ms, Maksimum = 5 ms, Czas średni = 4 ms

C:\Documents and Settings\Administrator>ping 21.31.1.1

Badanie 21.31.1.1 z użyciem 32 bajtów danych:

Odpowiedź z 21.31.1.1: bajtów=32 czas=3ms TTL=254
Odpowiedź z 21.31.1.1: bajtów=32 czas=3ms TTL=254
Odpowiedź z 21.31.1.1: bajtów=32 czas=3ms TTL=254
Odpowiedź z 21.31.1.1: bajtów=32 czas=3ms TTL=254

Statystyka badania ping dla 21.31.1.1:
    Pakiety: Wysłane = 4, Odebrane = 4, Utracone = 0 (0% straty),
Szacunkowy czas błądzenia pakietów w millisekundach:
    Minimum = 3 ms, Maksimum = 3 ms, Czas średni = 3 ms
```

Tunel zestawiony pomiędzy sieciami Lan1 i Lan4 funkcjonuje prawidłowo.

C. Wylistować tablicę routingu routera **R1** (**`show ipv6 route`**) i dane o tunelu (**`show interface tunnel`** ….) - wyniki wkleić poniżej.

Poniżej możemy zauważyć dane tunelu z obu stron (R1 i R3). Jak widać nasz typ tunelu to GRE/IPv6 zgodny z treścią naszego zadania.

```
R1#show interface tunnel 0
Tunnel0 is up, line protocol is up
  Hardware is Tunnel
  Internet address is 10.3.0.2/24
  MTU 1456 bytes, BW 100 Kbit/sec, DLY 50000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation TUNNEL, loopback not set
  Keepalive not set
  Tunnel source 2001:32:2:2:2::1, destination 2001:33:3:3:3::2
  Tunnel protocol/transport GRE/IPv6
  Tunnel TTL 255
```

R1

```
R3>en
R3#show int
R3#show interface tunnel 0
Tunnel0 is up, line protocol is up
  Hardware is Tunnel
  Internet address is 10.3.0.1/24
  MTU 1456 bytes, BW 100 Kbit/sec, DLY 50000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation TUNNEL, loopback not set
  Keepalive not set
  Tunnel source 2001:33:3:3:3::2, destination 2001:32:2:2:2::1
  Tunnel protocol/transport GRE/IPv6
  Tunnel TTL 255
```

R3

Poniżej znajdują się tablice routingu routerów R1 i R3 na którym widoczny jest nasz tunel.

```
R1>en
R1#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

     21.0.0.0/24 is subnetted, 2 subnets
C       21.31.1.0 is directly connected, FastEthernet0/0
S       21.34.4.0 is directly connected, Tunnel0
     10.0.0.0/24 is subnetted, 1 subnets
C       10.3.0.0 is directly connected, Tunnel0
R1#
```

R1

```
R3#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

     21.0.0.0/24 is subnetted, 2 subnets
S       21.31.1.0 is directly connected, Tunnel0
C       21.34.4.0 is directly connected, FastEthernet0/1
     10.0.0.0/24 is subnetted, 1 subnets
C       10.3.0.0 is directly connected, Tunnel0
```

R3

D. Uruchomić snifer Wireshark na komputerze **K2**. Uruchomić komendę **`ping`** na komputerze **K1** w celu sprawdzenia osiągalności komputera **K3**. Przechwycić ramki związane z tą komendą. Jakie rodzaje ramek protokołu ICMPv6 przechwycono?

E. Pokazać zawartość przechwyconej ramki „*Echo request*" i „*Echo Reply*".

Niestety screen został wykonany niewłaściwe (brak filtru na ICMPv6). Pamiętam, że snifer przede wszystkim wychwycił ramki IPv6 Echo request i Echo Reply. Wychwycone pakiety przesyłane przez tunel w adresie miały ostatni adres z sieci IPv6 kończący tunel.

F. Jakich sąsiadów zna komputer **K1** i router **R1**?

Router R1 widzi jako sąsiada dwa adresy IPv6 routera R2 (widać na poniższym screenie).

```
R1>en
R1#show ipv6 neig
R1#show ipv6 neighbors
IPv6 Address                              Age Link-layer Addr State Interface
2001:32:2:2:2::2                            7 18ef.63d9.4d18  STALE Fa0/1
FE80::1AEF:63FF:FED9:4D18                   7 18ef.63d9.4d18  STALE Fa0/1

R1#
```

Niestety nie posiadamy screena z polecenia shop ip neighbors, które w naszym przypadku jest ważniejsze bo oprócz wspomnianego routera R2 sąsiadem R1 powinno być:

- *Węzeł Fa0/0*
- *Źródło tunelu Tunnel0*
- *Komputer K1*

Natomiast komputer K1 powinien mieć za sąsiadów:

- *Adres IPv4 routera R1*
- *Adres broadcast*

PODSUMOWANIE

Zestawienie tuneli choć nietypowe (wg zaleceń sieć IPv6 powinna najpierw pojawiać się w węzłach brzegowych, a dopiero później w szkielecie sieci) funkcjonuje i nie wymaga zbyt wielkiego nakładu sił. Podczas wykonywania zadań nie natrafiliśmy na jakieś większe trudności. Jednak po wykonanych laboratoriach zrobiliśmy niedokładnie niektóre screeny i nie mogliśmy ich przedstawić w sprawozdaniu.