Badanie bezpieczeństwa IPv6

lp	wykonawca	grupa (*g*)
1.	Grzegorz Pol	3
2.	Artur Mazur	
3.	Michał Grzybowski	
4.		
5.		

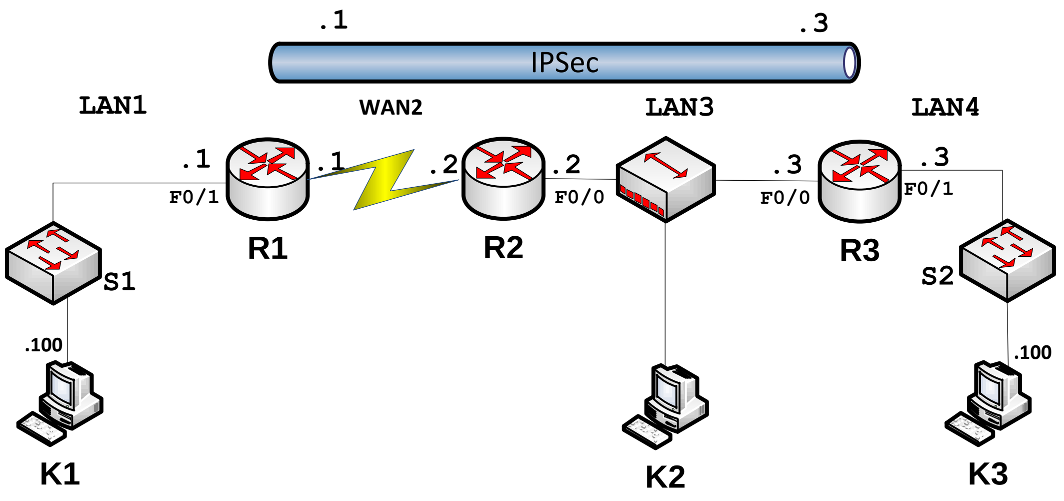
Tabela 1.

zadanie	Funkcja skrótu	Grupa DH	Protokół szyfrowania	Zestaw przekształceń
1.	MD5	2	DES	AH-MD5-HMAC ESP-DES
2.	SHA	5	3DES	AH-SHA-HMAC ESP-3DES
3.	MD5	2	AES	ESP-SHA-HMAC ESP-AES
4.	SHA	5	AES 192	ESP-MD5-HMAC ESP-SEAL
5.	MD5	5	AES 256	AH-MD5-HMAC ESP-AES

Tabela 2. Plan adresacji:

	IPv6
LAN1	2001:g*10+1:1:1::/64
WAN2	2001:g*10+2:2:2::/64
LAN3	2001:g*10+3:3:3::/64
LAN4	2001:g*10+4:4:4::/64
Lo1	1.1.1.1/32
Lo2	2.2.2.2/32
Lo3	3.3.3.3/32
Tunel0	2001:g*10+5:15:15::/64

Topologia:

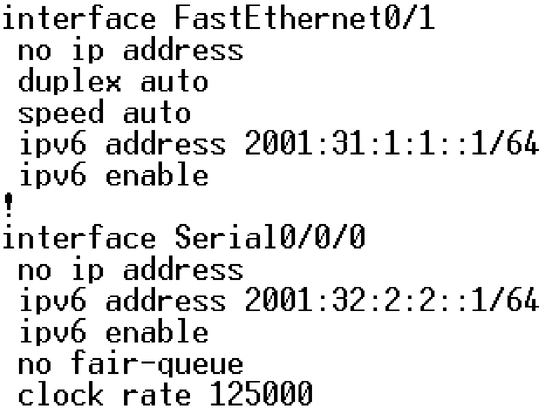


1. **Wyznaczyć adresy dla elementów składowych sieci na podstawie tabeli 1 zależnie od numeru grupy (G) i numeru zadania. Wyniki podać w poniższej tabeli:**

nazwa urządzenia	interfejs	adres/maska
R1	Fa0/1	2001:31:1:1::1
	S0/0/0	2001:32:2:2::1
	Lo1	
	Tunnel0	
R2	Fa0/0	2001:33:3:3::1
	S0/0/0	2001:32:2:2::2
	Lo2	
R3	Fa0/0	2001:33:3:3::2
	Fa0/1	2001:34:4:4::1
	Lo3	
	Tunnel0	
K1	Eth0	2001:31:1:1::100
K3	Eth0	2001:34:4:4::100

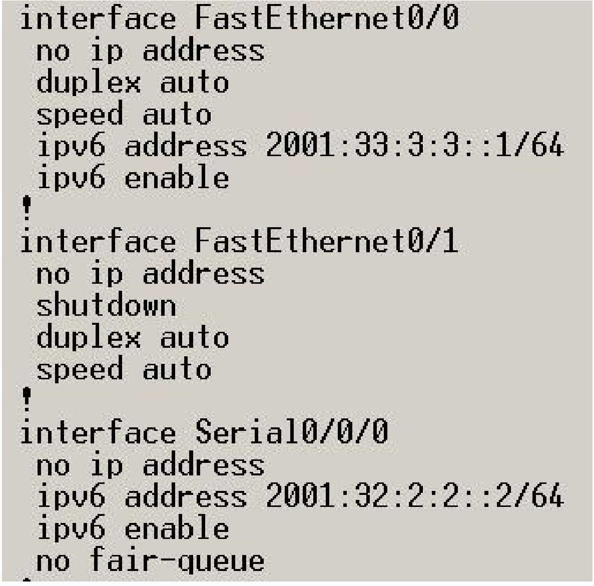
2. **Przygotowanie topologii sieci:**
   A. Zbudować sieć według podanej topologii i wyznaczonego planu adresacji. Poniżej wkleić zrzut ekranu z konfiguracją interfejsów routerów **R1, R2, R3** i komputerów **K1** i **K3**.

zrzut ekranu interfejsów R1



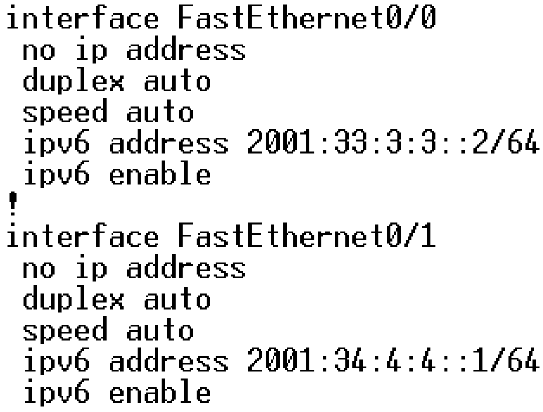
```
interface FastEthernet0/1
 no ip address
 duplex auto
 speed auto
 ipv6 address 2001:31:1:1::1/64
 ipv6 enable
!
interface Serial0/0/0
 no ip address
 ipv6 address 2001:32:2:2::1/64
 ipv6 enable
 no fair-queue
 clock rate 125000
```

zrzut ekranu interfejsów R2



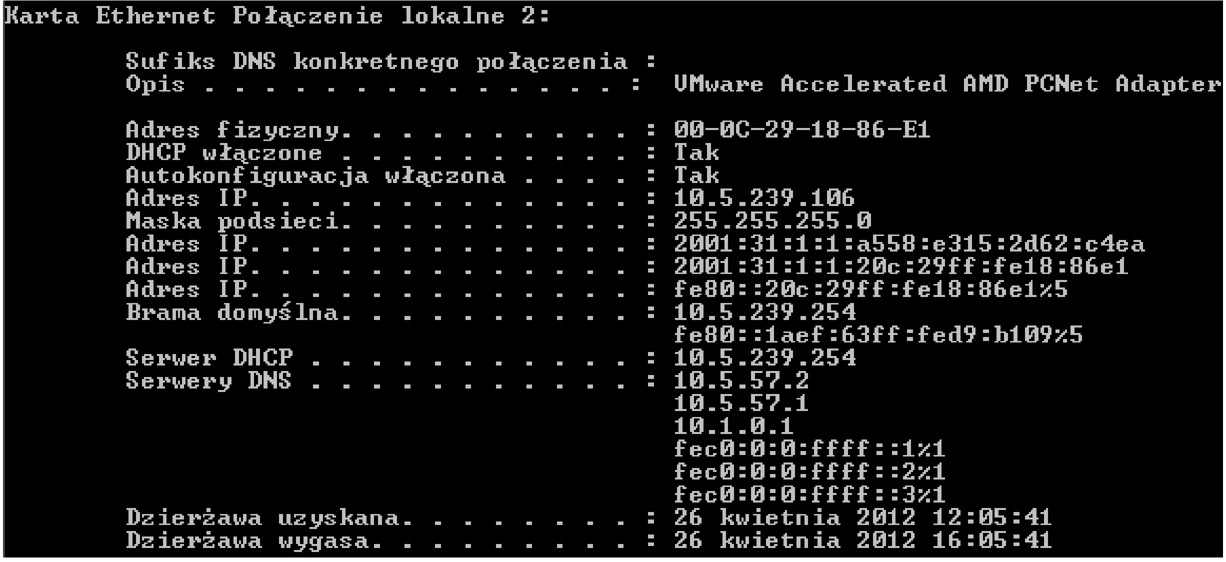
```
interface FastEthernet0/0
 no ip address
 duplex auto
 speed auto
 ipv6 address 2001:33:3:3::1/64
 ipv6 enable
!
interface FastEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface Serial0/0/0
 no ip address
 ipv6 address 2001:32:2:2::2/64
 ipv6 enable
 no fair-queue
```

zrzut ekranu interfejsów R3



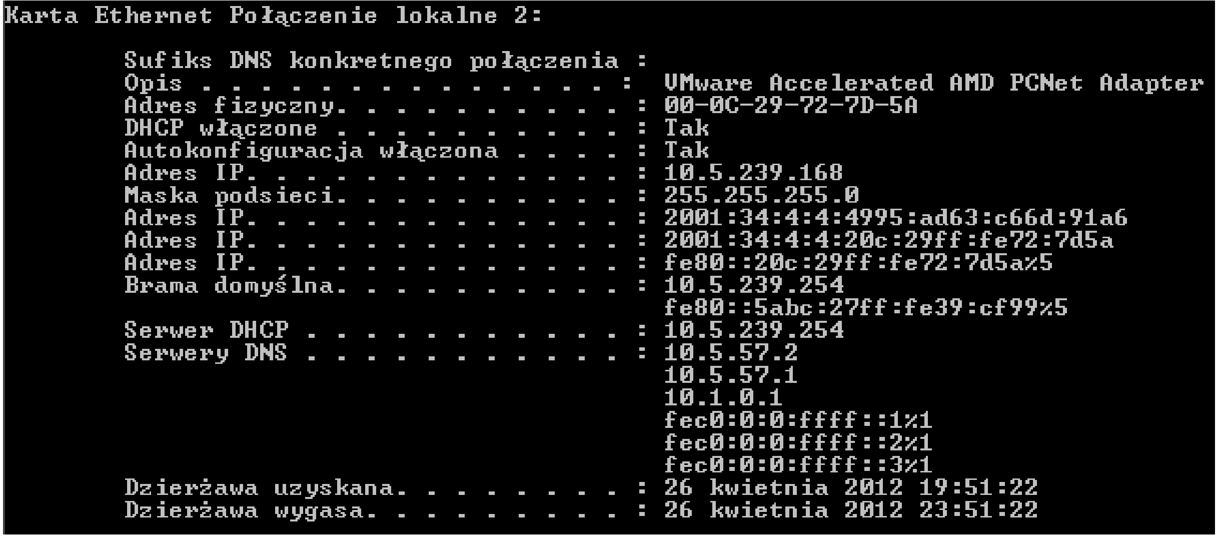
```
interface FastEthernet0/0
 no ip address
 duplex auto
 speed auto
 ipv6 address 2001:33:3:3::2/64
 ipv6 enable
!
interface FastEthernet0/1
 no ip address
 duplex auto
 speed auto
 ipv6 address 2001:34:4:4::1/64
 ipv6 enable
```

zrzut ekranu interfejsów K1



```
Karta Ethernet Połączenie lokalne 2:

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

        Adres fizyczny. . . . . . . . . . : 00-0C-29-18-86-E1
        DHCP włączone . . . . . . . . . . : Tak
        Autokonfiguracja włączona . . . . : Tak
        Adres IP. . . . . . . . . . . . . : 10.5.239.106
        Maska podsieci. . . . . . . . . . : 255.255.255.0
        Adres IP. . . . . . . . . . . . . : 2001:31:1:1:a558:e315:2d62:c4ea
        Adres IP. . . . . . . . . . . . . : 2001:31:1:1:20c:29ff:fe18:86e1
        Adres IP. . . . . . . . . . . . . : fe80::20c:29ff:fe18:86e1%5
        Brama domyślna. . . . . . . . . . : 10.5.239.254
                                            fe80::1aef:63ff:fed9:b109%5
        Serwer DHCP . . . . . . . . . . . : 10.5.239.254
        Serwery DNS . . . . . . . . . . . : 10.5.57.2
                                            10.5.57.1
                                            10.1.0.1
                                            fec0:0:0:ffff::1%1
                                            fec0:0:0:ffff::2%1
                                            fec0:0:0:ffff::3%1
        Dzierżawa uzyskana. . . . . . . . : 26 kwietnia 2012 12:05:41
        Dzierżawa wygasa. . . . . . . . . : 26 kwietnia 2012 16:05:41
```

zrzut ekranu interfejsów K3



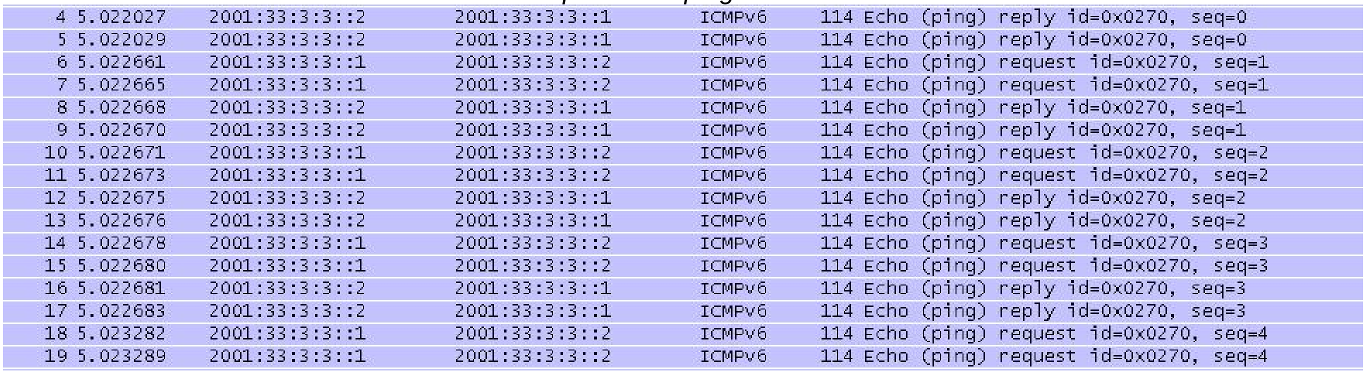
```
Karta Ethernet Połączenie lokalne 2:

        Sufiks DNS konkretnego połączenia :
        Opis . . . . . . . . . . . . . . . :  VMware Accelerated AMD PCNet Adapter
        Adres fizyczny. . . . . . . . . . : 00-0C-29-72-7D-5A
        DHCP włączone . . . . . . . . . . : Tak
        Autokonfiguracja włączona . . . . : Tak
        Adres IP. . . . . . . . . . . . . : 10.5.239.168
        Maska podsieci. . . . . . . . . . : 255.255.255.0
        Adres IP. . . . . . . . . . . . . : 2001:34:4:4:4995:ad63:c66d:91a6
        Adres IP. . . . . . . . . . . . . : 2001:34:4:4:20c:29ff:fe72:7d5a
        Adres IP. . . . . . . . . . . . . : fe80::20c:29ff:fe72:7d5a%5
        Brama domyślna. . . . . . . . . . : 10.5.239.254
                                            fe80::5abc:27ff:fe39:cf99%5
        Serwer DHCP . . . . . . . . . . . : 10.5.239.254
        Serwery DNS . . . . . . . . . . . : 10.5.57.2
                                            10.5.57.1
                                            10.1.0.1
                                            fec0:0:0:ffff::1%1
                                            fec0:0:0:ffff::2%1
                                            fec0:0:0:ffff::3%1
        Dzierżawa uzyskana. . . . . . . . : 26 kwietnia 2012 19:51:22
        Dzierżawa wygasa. . . . . . . . . : 26 kwietnia 2012 23:51:22
```

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

	R1	R2	R3	K1	K3
R1	+	+	-	+	-
R2	+	+	+	-	-
R3	-	+	+	-	+
K1	+	-	-	+	-
K3	-	-	+	-	+

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

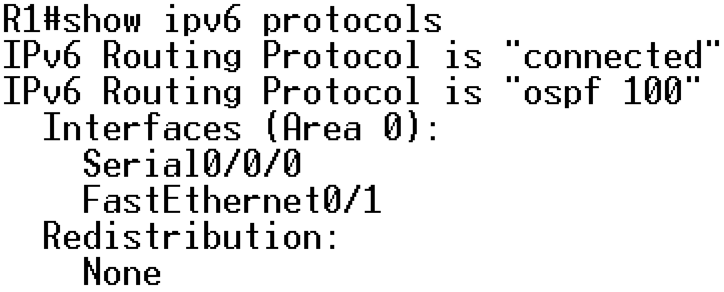
zrzut ekranu polecenia ping dla R2-R3



```
 4 5.022027   2001:33:3:3::2      2001:33:3:3::1      ICMPv6    114 Echo (ping) reply id=0x0270, seq=0
 5 5.022029   2001:33:3:3::2      2001:33:3:3::1      ICMPv6    114 Echo (ping) reply id=0x0270, seq=0
 6 5.022661   2001:33:3:3::1      2001:33:3:3::2      ICMPv6    114 Echo (ping) request id=0x0270, seq=1
 7 5.022665   2001:33:3:3::1      2001:33:3:3::2      ICMPv6    114 Echo (ping) request id=0x0270, seq=1
 8 5.022668   2001:33:3:3::2      2001:33:3:3::1      ICMPv6    114 Echo (ping) reply id=0x0270, seq=1
 9 5.022670   2001:33:3:3::2      2001:33:3:3::1      ICMPv6    114 Echo (ping) reply id=0x0270, seq=1
10 5.022671   2001:33:3:3::1      2001:33:3:3::2      ICMPv6    114 Echo (ping) request id=0x0270, seq=2
11 5.022673   2001:33:3:3::1      2001:33:3:3::2      ICMPv6    114 Echo (ping) request id=0x0270, seq=2
12 5.022675   2001:33:3:3::2      2001:33:3:3::1      ICMPv6    114 Echo (ping) reply id=0x0270, seq=2
13 5.022676   2001:33:3:3::2      2001:33:3:3::1      ICMPv6    114 Echo (ping) reply id=0x0270, seq=2
14 5.022678   2001:33:3:3::1      2001:33:3:3::2      ICMPv6    114 Echo (ping) request id=0x0270, seq=3
15 5.022680   2001:33:3:3::1      2001:33:3:3::2      ICMPv6    114 Echo (ping) request id=0x0270, seq=3
16 5.022681   2001:33:3:3::2      2001:33:3:3::1      ICMPv6    114 Echo (ping) reply id=0x0270, seq=3
17 5.022683   2001:33:3:3::2      2001:33:3:3::1      ICMPv6    114 Echo (ping) reply id=0x0270, seq=3
18 5.023282   2001:33:3:3::1      2001:33:3:3::2      ICMPv6    114 Echo (ping) request id=0x0270, seq=4
19 5.023289   2001:33:3:3::1      2001:33:3:3::2      ICMPv6    114 Echo (ping) request id=0x0270, seq=4
```

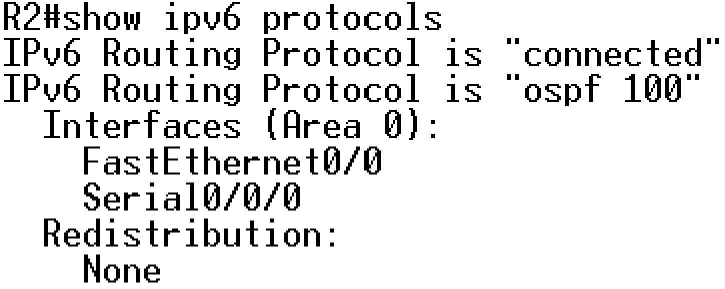
D. Skonfigurować routing dynamiczny w oparciu o protokół OSPFv3 na routerach w sieci. Poniżej wkleić zrzut ekranu z poprawną konfiguracją routera **R1**, **R2** i **R3.**

Zrzut ekranu polecenia show ipv6 protocols dla routera R1



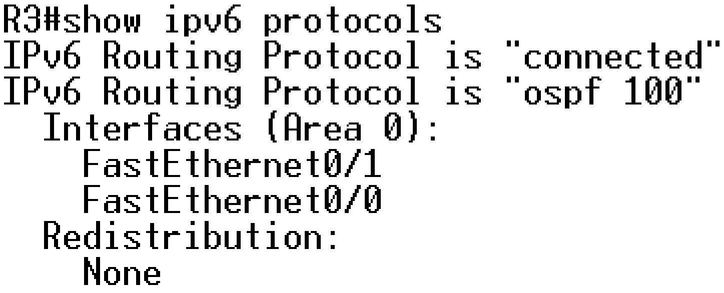
```
R1#show ipv6 protocols
IPv6 Routing Protocol is "connected"
IPv6 Routing Protocol is "ospf 100"
  Interfaces (Area 0):
    Serial0/0/0
    FastEthernet0/1
  Redistribution:
    None
```

Zrzut ekranu polecenia show ipv6 ospf protocols dla routera R2



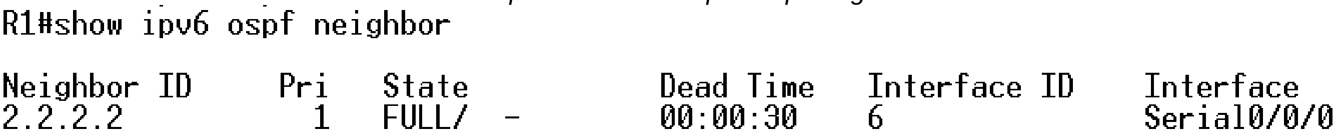
```
R2#show ipv6 protocols
IPv6 Routing Protocol is "connected"
IPv6 Routing Protocol is "ospf 100"
  Interfaces (Area 0):
    FastEthernet0/0
    Serial0/0/0
  Redistribution:
    None
```

Zrzut ekranu polecenia show ipv6 ospf protocols dla routera R3



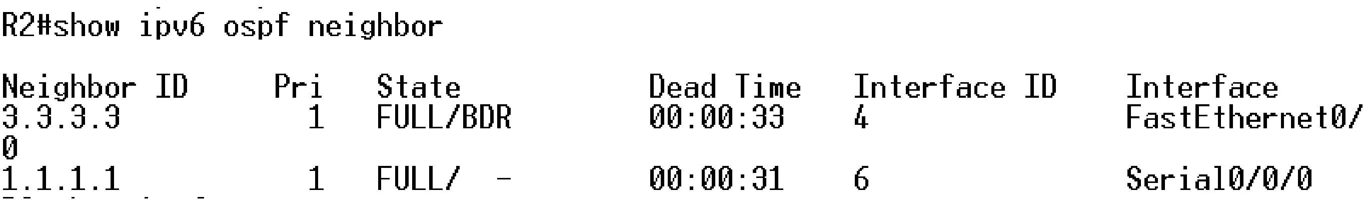
```
R3#show ipv6 protocols
IPv6 Routing Protocol is "connected"
IPv6 Routing Protocol is "ospf 100"
  Interfaces (Area 0):
    FastEthernet0/1
    FastEthernet0/0
  Redistribution:
    None
```

Zrzut ekranu polecenia show ipv6 ospf neighbors dla routera R1



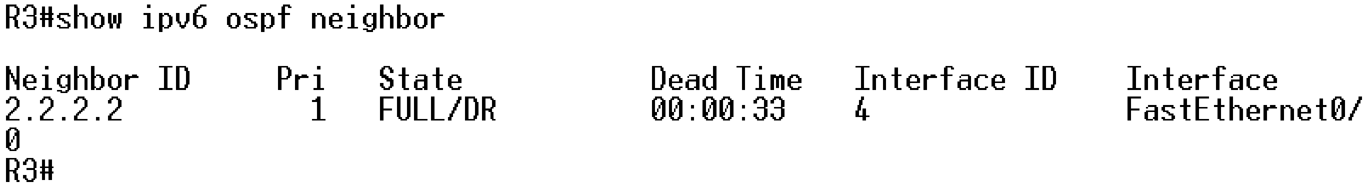
```
R1#show ipv6 ospf neighbor

Neighbor ID     Pri   State           Dead Time   Interface ID    Interface
2.2.2.2           1   FULL/  -        00:00:30    6               Serial0/0/0
```

Zrzut ekranu polecenia show ipv6 ospf neighbors dla routera R2



```
R2#show ipv6 ospf neighbor

Neighbor ID     Pri   State           Dead Time   Interface ID    Interface
3.3.3.3           1   FULL/BDR        00:00:33    4               FastEthernet0/
0
1.1.1.1           1   FULL/  -        00:00:31    6               Serial0/0/0
```

Zrzut ekranu polecenia show ipv6 ospf neighbors dla routera R3



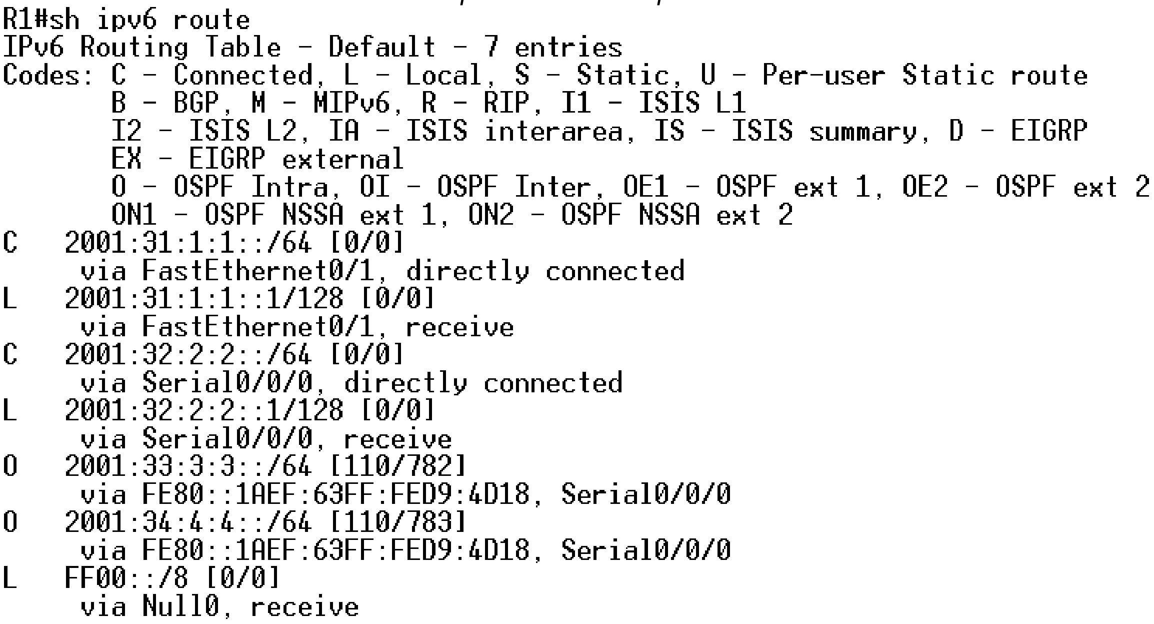
```
R3#show ipv6 ospf neighbor

Neighbor ID     Pri   State           Dead Time   Interface ID    Interface
2.2.2.2           1   FULL/DR         00:00:33    4               FastEthernet0/
0
R3#
```

E. Zweryfikować poprawność działania routingu. Sprawdzić wzajemną osiągalność węzłów w sieci.

	R1	R2	R3	K1	K3
R1	+	+	+	+	+
R2	+	+	+	+	+
R3	+	+	+	+	+
K1	+	+	+	+	+
K3	+	+	+	+	+

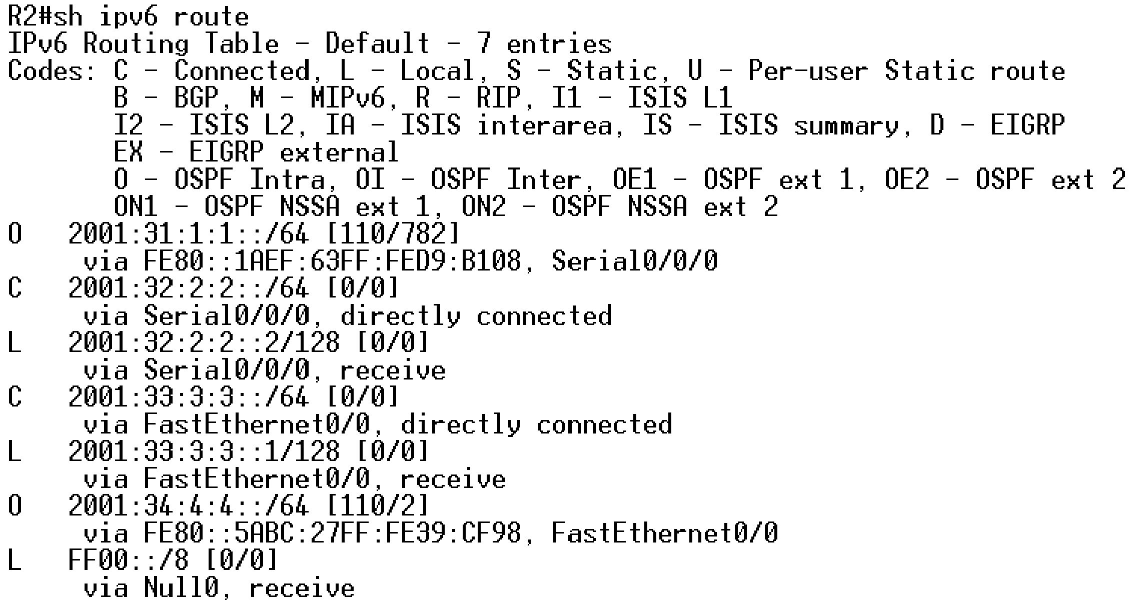
F. Wylistować tablicę routingu routerów **R1**, **R2** i **R3.**

Zrzut ekranu polecenia show ipv6 route dla routera R1



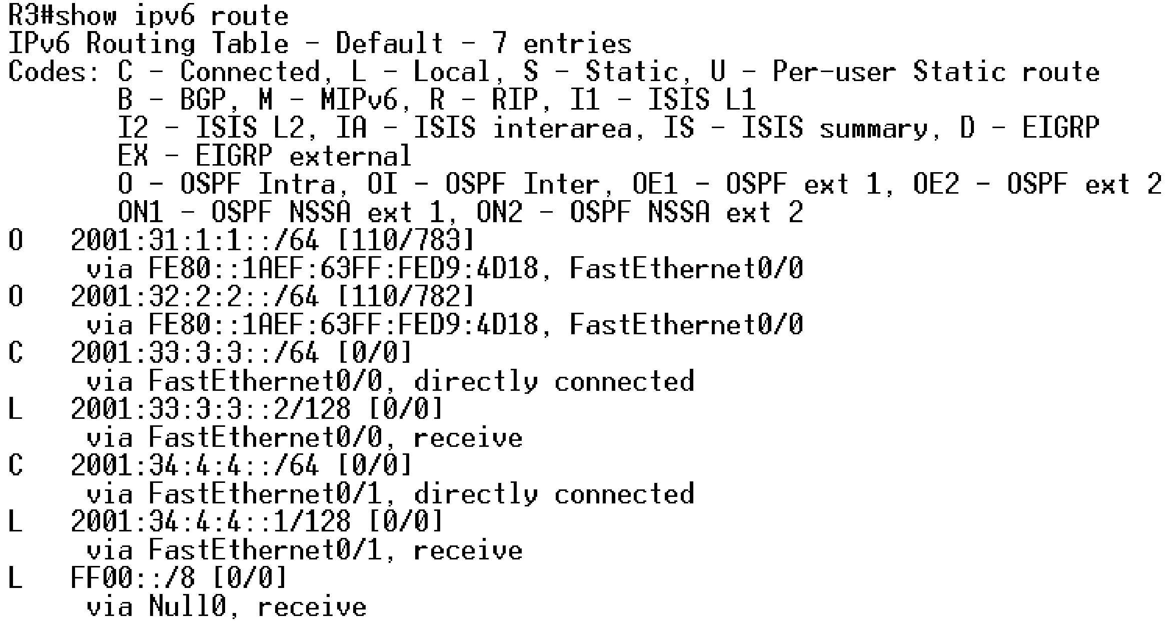
```
R1#sh ipv6 route
IPv6 Routing Table - Default - 7 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
       B - BGP, M - MIPv6, R - RIP, I1 - ISIS L1
       I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary, D - EIGRP
       EX - EIGRP external
       O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
C   2001:31:1:1::/64 [0/0]
     via FastEthernet0/1, directly connected
L   2001:31:1:1::1/128 [0/0]
     via FastEthernet0/1, receive
C   2001:32:2:2::/64 [0/0]
     via Serial0/0/0, directly connected
L   2001:32:2:2::1/128 [0/0]
     via Serial0/0/0, receive
O   2001:33:3:3::/64 [110/782]
     via FE80::1AEF:63FF:FED9:4D18, Serial0/0/0
O   2001:34:4:4::/64 [110/783]
     via FE80::1AEF:63FF:FED9:4D18, Serial0/0/0
L   FF00::/8 [0/0]
     via Null0, receive
```

Zrzut ekranu polecenia show ipv6 route dla routera R2



```
R2#sh ipv6 route
IPv6 Routing Table - Default - 7 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
       B - BGP, M - MIPv6, R - RIP, I1 - ISIS L1
       I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary, D - EIGRP
       EX - EIGRP external
       O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
O   2001:31:1:1::/64 [110/782]
     via FE80::1AEF:63FF:FED9:B108, Serial0/0/0
C   2001:32:2:2::/64 [0/0]
     via Serial0/0/0, directly connected
L   2001:32:2:2::2/128 [0/0]
     via Serial0/0/0, receive
C   2001:33:3:3::/64 [0/0]
     via FastEthernet0/0, directly connected
L   2001:33:3:3::1/128 [0/0]
     via FastEthernet0/0, receive
O   2001:34:4:4::/64 [110/2]
     via FE80::5ABC:27FF:FE39:CF98, FastEthernet0/0
L   FF00::/8 [0/0]
     via Null0, receive
```

Zrzut ekranu polecenia show ipv6 route dla routera R3

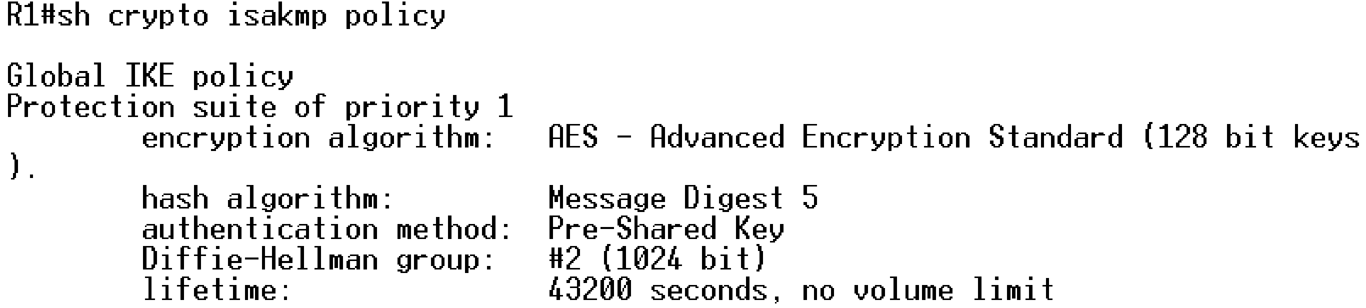


```
R3#show ipv6 route
IPv6 Routing Table - Default - 7 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
       B - BGP, M - MIPv6, R - RIP, I1 - ISIS L1
       I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary, D - EIGRP
       EX - EIGRP external
       O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
O   2001:31:1:1::/64 [110/783]
     via FE80::1AEF:63FF:FED9:4D18, FastEthernet0/0
O   2001:32:2:2::/64 [110/782]
     via FE80::1AEF:63FF:FED9:4D18, FastEthernet0/0
C   2001:33:3:3::/64 [0/0]
     via FastEthernet0/0, directly connected
L   2001:33:3:3::2/128 [0/0]
     via FastEthernet0/0, receive
C   2001:34:4:4::/64 [0/0]
     via FastEthernet0/1, directly connected
L   2001:34:4:4::1/128 [0/0]
     via FastEthernet0/1, receive
L   FF00::/8 [0/0]
     via Null0, receive
```

3. Badanie tunelu IPSec:

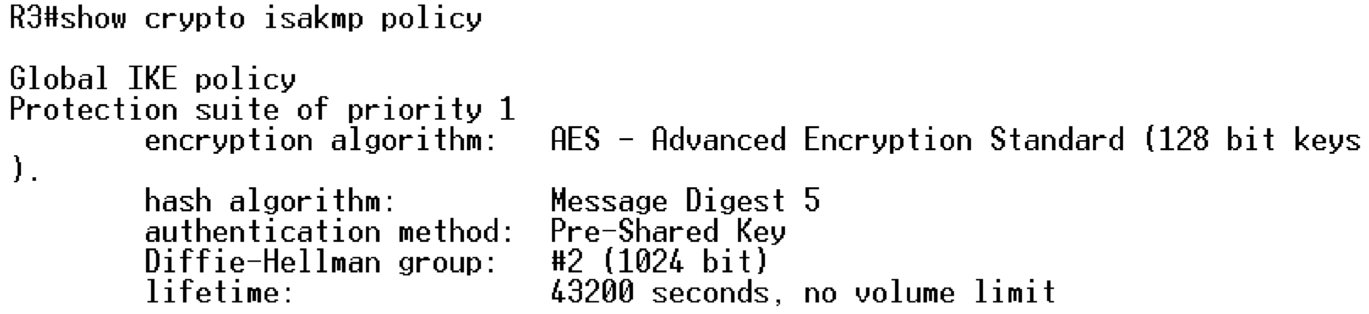
A. Skonfigurować politykę IKE i klucz współdzielony na routerze R1 i R3. Wymagane parametry polityki IKE są podane w tabeli 1, jako klucza współdzielonego użyć „cisco”. Zweryfikować i wkleić poniżej zrzuty ekranu potwierdzające poprawność wprowadzonych ustawień.

Zrzut ekranu polecenia show crypto isakmp policy dla routera R1



```
R1#sh crypto isakmp policy

Global IKE policy
Protection suite of priority 1
        encryption algorithm:   AES - Advanced Encryption Standard (128 bit keys
).
        hash algorithm:         Message Digest 5
        authentication method:  Pre-Shared Key
        Diffie-Hellman group:   #2 (1024 bit)
        lifetime:               43200 seconds, no volume limit
```

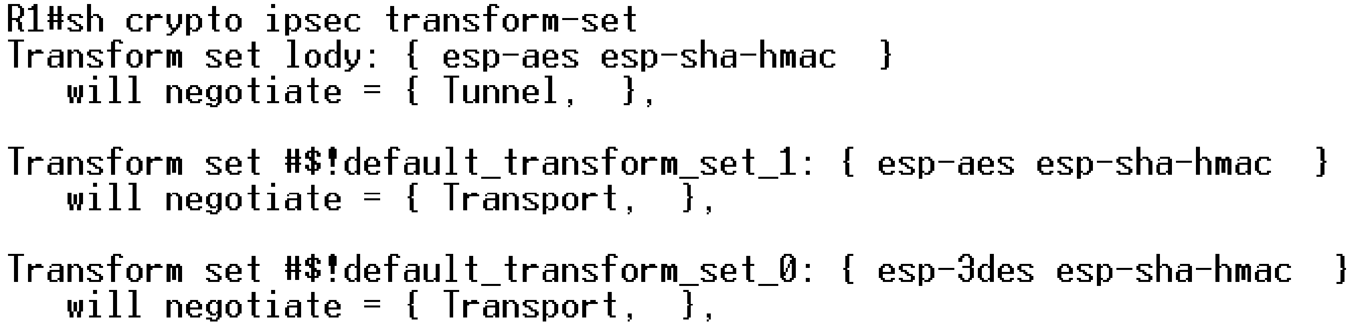
Zrzut ekranu polecenia show crypto isakmp policy dla routera R3



```
R3#show crypto isakmp policy

Global IKE policy
Protection suite of priority 1
        encryption algorithm:   AES - Advanced Encryption Standard (128 bit keys
).
        hash algorithm:         Message Digest 5
        authentication method:  Pre-Shared Key
        Diffie-Hellman group:   #2 (1024 bit)
        lifetime:               43200 seconds, no volume limit
```

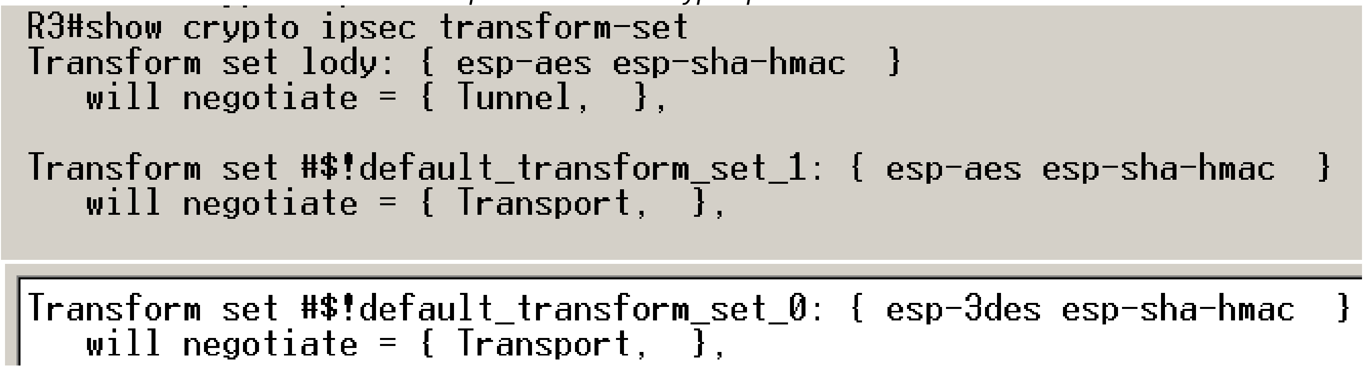
B. Skonfigurować zestaw przekształceń IPSec i profil IPSec na routerze R1 i R3. Wymagane parametry są podane w tabeli 1. Zweryfikować i wkleić poniżej zrzuty ekranu potwierdzające poprawność wprowadzonych ustawień.

Zrzut ekranu polecenia show crypto ipsec transform-set dla routera R1



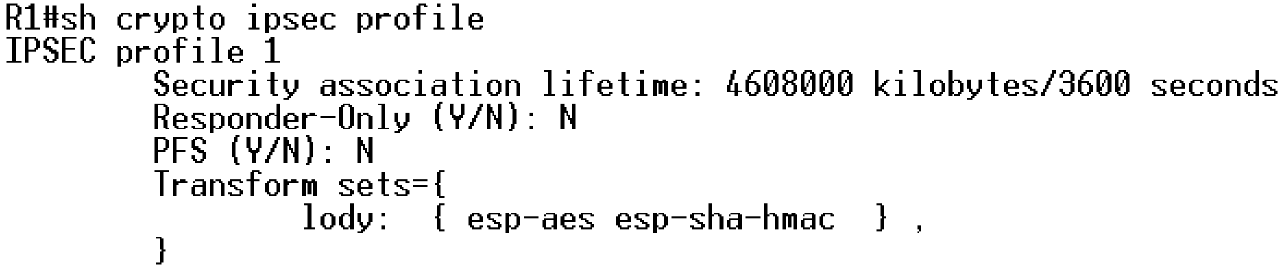
```
R1#sh crypto ipsec transform-set
Transform set lody: { esp-aes esp-sha-hmac  }
   will negotiate = { Tunnel,  },

Transform set #$!default_transform_set_1: { esp-aes esp-sha-hmac  }
   will negotiate = { Transport,  },

Transform set #$!default_transform_set_0: { esp-3des esp-sha-hmac  }
   will negotiate = { Transport,  },
```

Zrzut ekranu polecenia show crypto ipsec transform-set dla routera R3



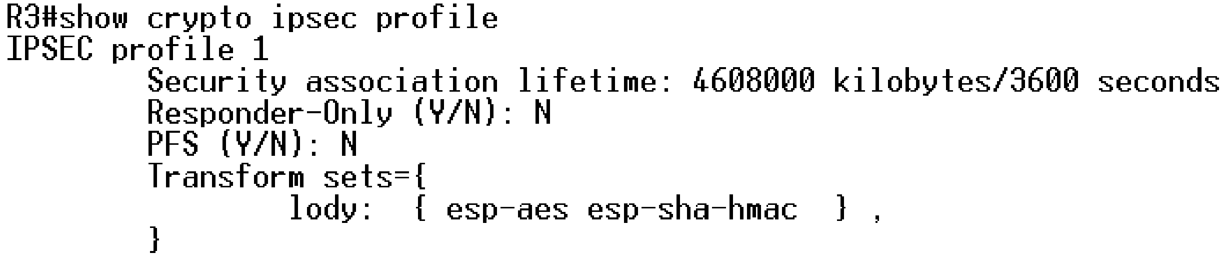
```
R3#show crypto ipsec transform-set
Transform set lody: { esp-aes esp-sha-hmac  }
   will negotiate = { Tunnel,  },

Transform set #$!default_transform_set_1: { esp-aes esp-sha-hmac  }
   will negotiate = { Transport,  },

Transform set #$!default_transform_set_0: { esp-3des esp-sha-hmac  }
   will negotiate = { Transport,  },
```

Zrzut ekranu polecenia show crypto ipsec profile dla routera R1



```
R1#sh crypto ipsec profile
IPSEC profile 1
        Security association lifetime: 4608000 kilobytes/3600 seconds
        Responder-Only (Y/N): N
        PFS (Y/N): N
        Transform sets={
                lody:  { esp-aes esp-sha-hmac  } ,
        }
```

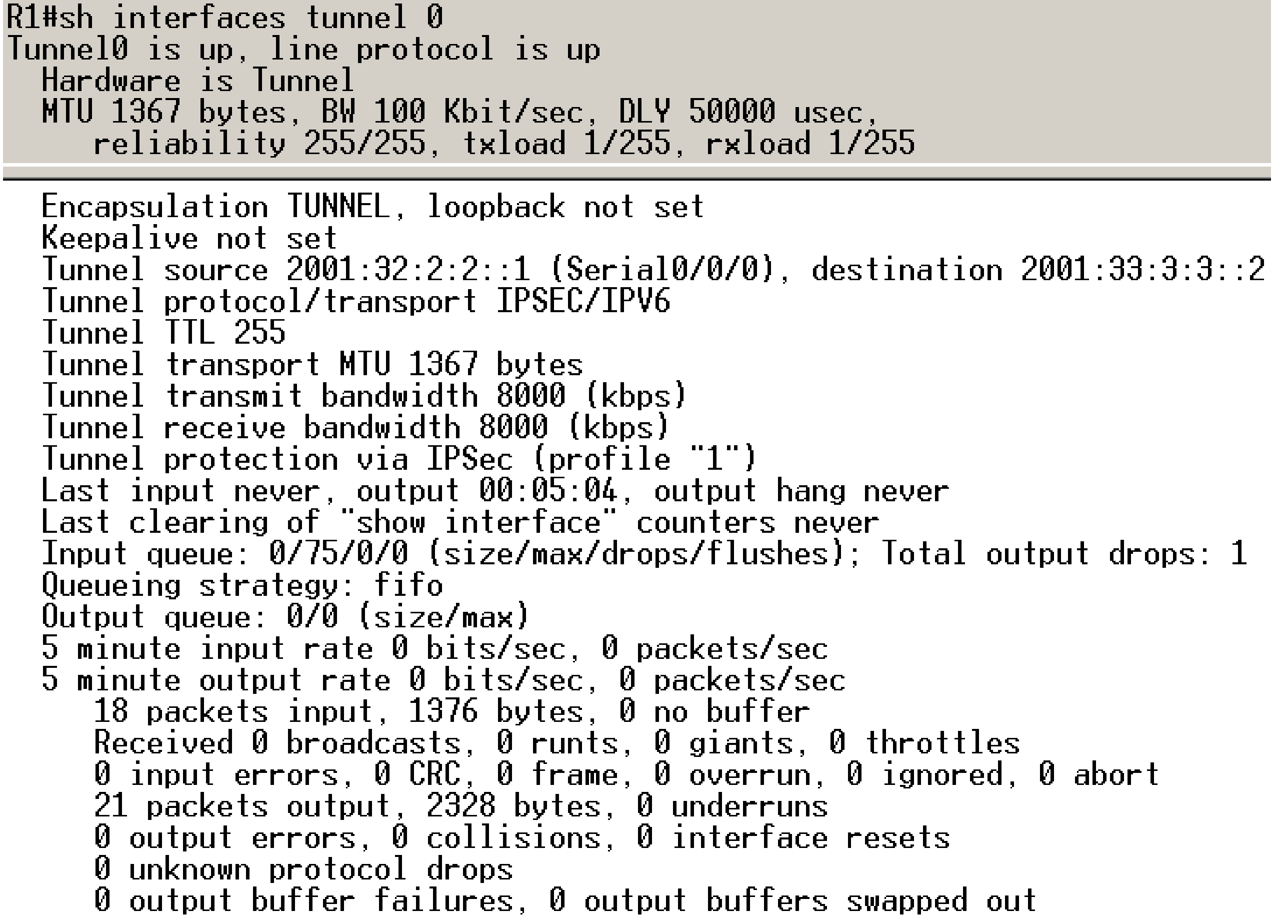
Zrzut ekranu polecenia show crypto ipsec profile dla routera R3



```
R3#show crypto ipsec profile
IPSEC profile 1
        Security association lifetime: 4608000 kilobytes/3600 seconds
        Responder-Only (Y/N): N
        PFS (Y/N): N
        Transform sets={
                lody:  { esp-aes esp-sha-hmac  } ,
        }
```

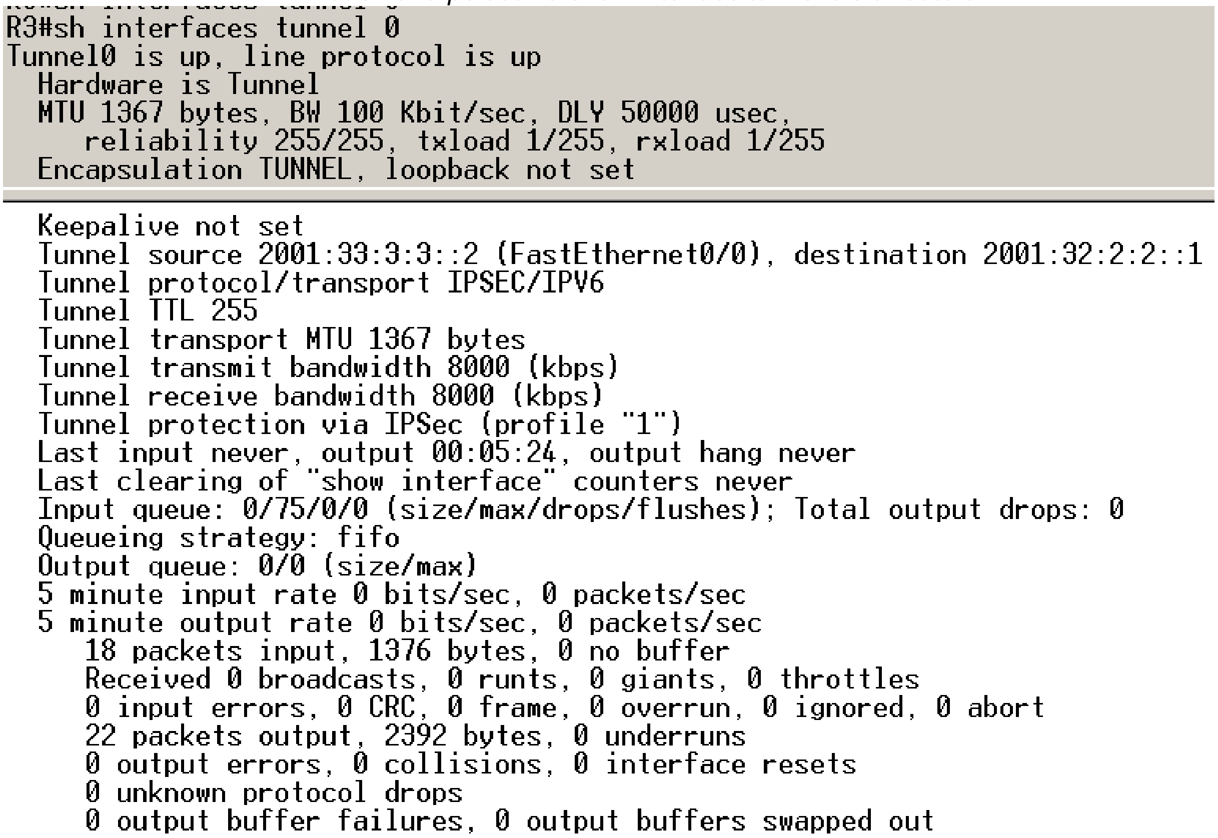
C. Skonfigurować wirtualny interfejs tunelu (VTI), przypisać wcześniej utworzony profil IPSec do tunelu. Zweryfikować i wkleić poniżej zrzuty ekranu potwierdzające poprawność wprowadzonych ustawień.

Zrzut ekranu polecenia show interface tunnel 0 dla routera R1



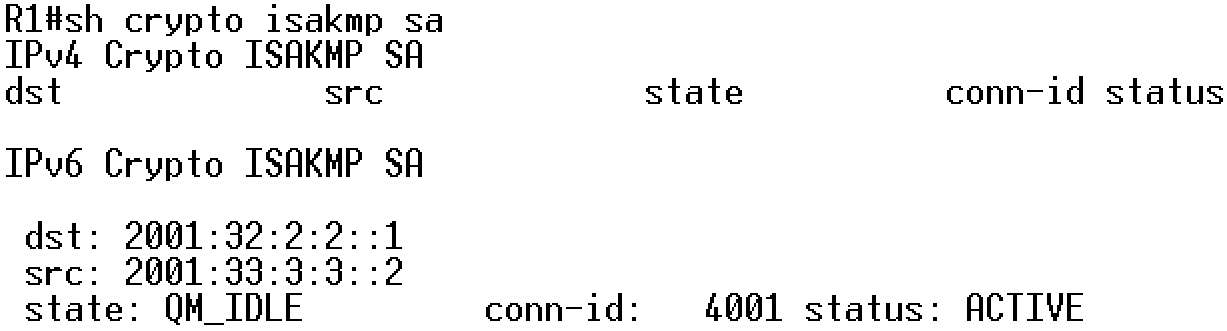
```
R1#sh interfaces tunnel 0
Tunnel0 is up, line protocol is up
  Hardware is Tunnel
  MTU 1367 bytes, BW 100 Kbit/sec, DLY 50000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation TUNNEL, loopback not set
  Keepalive not set
  Tunnel source 2001:32:2:2::1 (Serial0/0/0), destination 2001:33:3:3::2
  Tunnel protocol/transport IPSEC/IPV6
  Tunnel TTL 255
  Tunnel transport MTU 1367 bytes
  Tunnel transmit bandwidth 8000 (kbps)
  Tunnel receive bandwidth 8000 (kbps)
  Tunnel protection via IPSec (profile "1")
  Last input never, output 00:05:04, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 1
  Queueing strategy: fifo
  Output queue: 0/0 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     18 packets input, 1376 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     21 packets output, 2328 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 unknown protocol drops
     0 output buffer failures, 0 output buffers swapped out
```

Zrzut ekranu polecenia show interface tunnel 0 dla routera R1



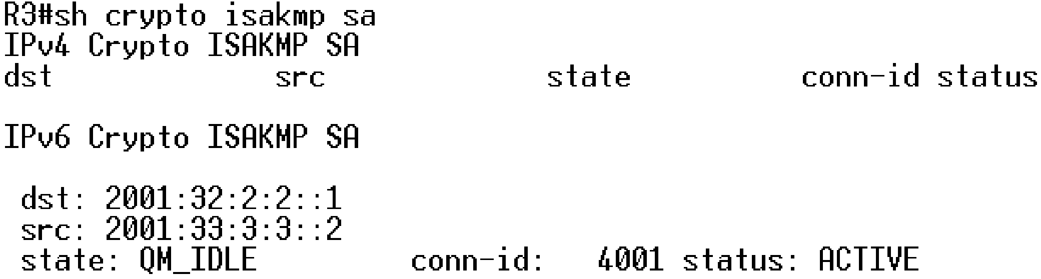
```
R3#sh interfaces tunnel 0
Tunnel0 is up, line protocol is up
  Hardware is Tunnel
  MTU 1367 bytes, BW 100 Kbit/sec, DLY 50000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation TUNNEL, loopback not set
  Keepalive not set
  Tunnel source 2001:33:3:3::2 (FastEthernet0/0), destination 2001:32:2:2::1
  Tunnel protocol/transport IPSEC/IPV6
  Tunnel TTL 255
  Tunnel transport MTU 1367 bytes
  Tunnel transmit bandwidth 8000 (kbps)
  Tunnel receive bandwidth 8000 (kbps)
  Tunnel protection via IPSec (profile "1")
  Last input never, output 00:05:24, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/0 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     18 packets input, 1376 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     22 packets output, 2392 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 unknown protocol drops
     0 output buffer failures, 0 output buffers swapped out
```

Zrzut ekranu polecenia show crypto isakmp sa dla routera R1



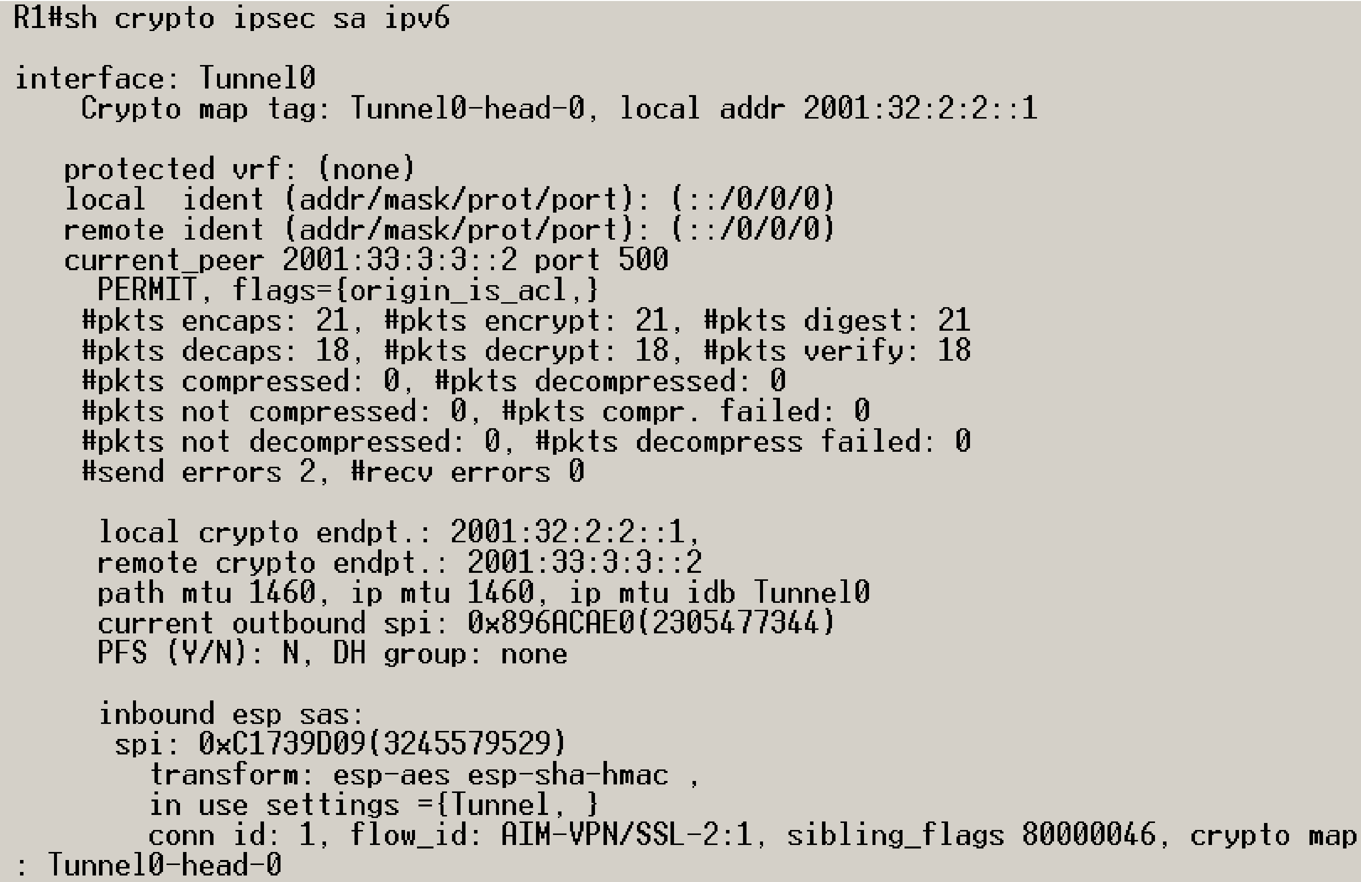
```
R1#sh crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id status

IPv6 Crypto ISAKMP SA

 dst: 2001:32:2:2::1
 src: 2001:33:3:3::2
 state: QM_IDLE        conn-id:   4001 status: ACTIVE
```

Zrzut ekranu polecenia show crypto isakmp sa dla routera R3

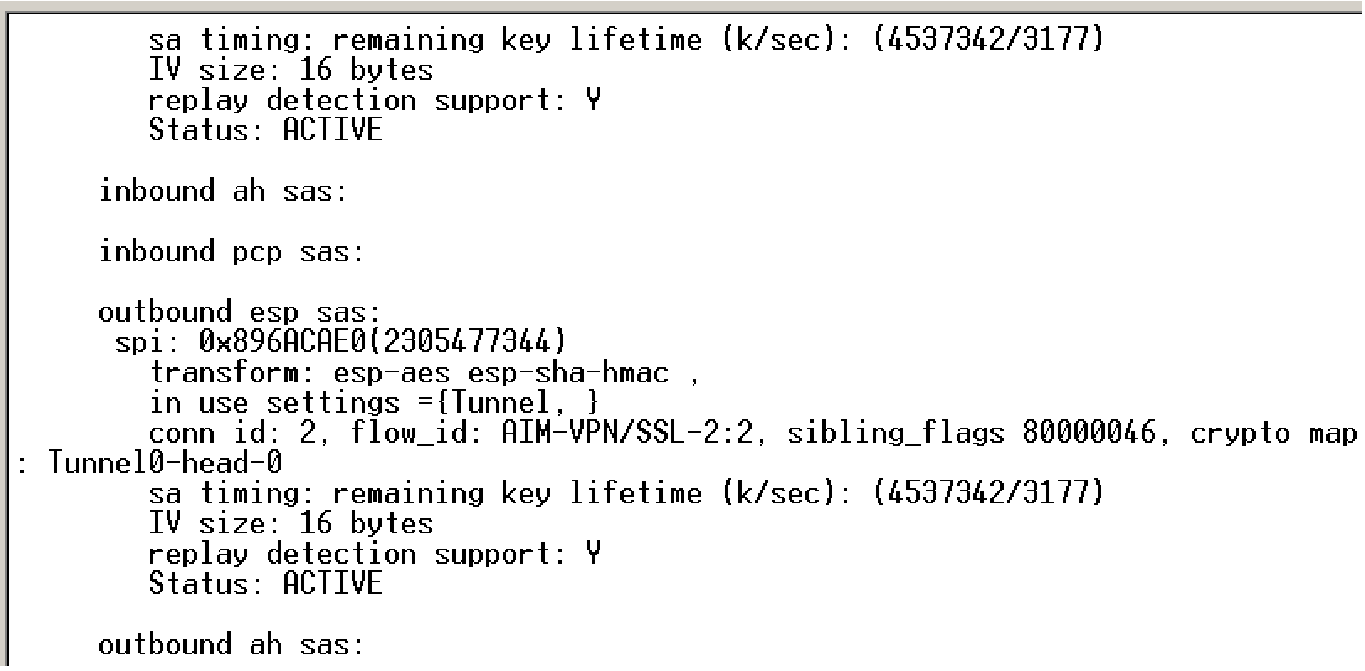


```
R3#sh crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id status

IPv6 Crypto ISAKMP SA

 dst: 2001:32:2:2::1
 src: 2001:33:3:3::2
 state: QM_IDLE        conn-id:   4001 status: ACTIVE
```

Zrzut ekranu polecenia show crypto ipsec sa ipv6 dla routera R1

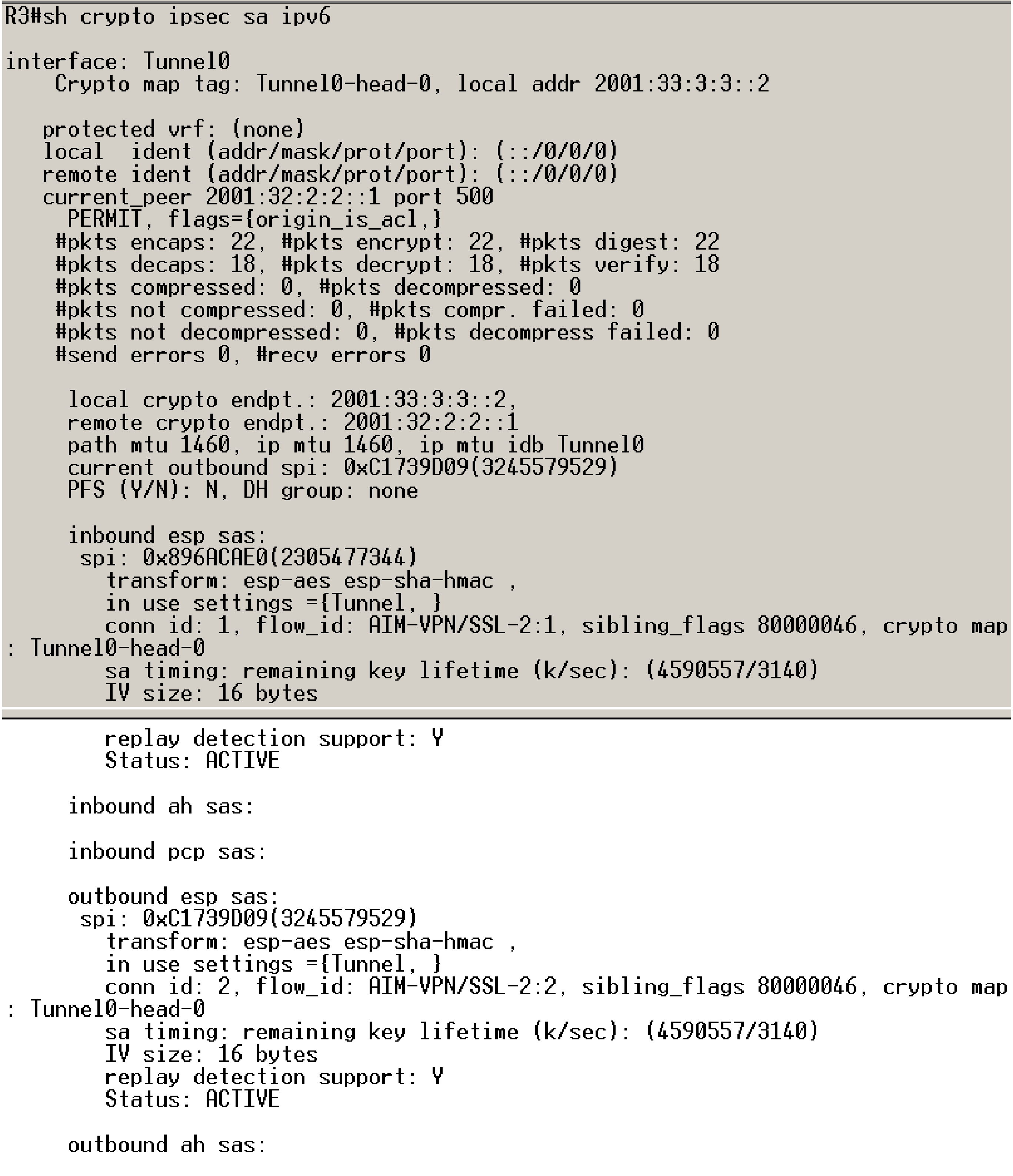


```
R1#sh crypto ipsec sa ipv6

interface: Tunnel0
    Crypto map tag: Tunnel0-head-0, local addr 2001:32:2:2::1

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (::/0/0/0)
   remote ident (addr/mask/prot/port): (::/0/0/0)
   current_peer 2001:33:3:3::2 port 500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 21, #pkts encrypt: 21, #pkts digest: 21
    #pkts decaps: 18, #pkts decrypt: 18, #pkts verify: 18
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 2, #recv errors 0

     local crypto endpt.: 2001:32:2:2::1,
     remote crypto endpt.: 2001:33:3:3::2
     path mtu 1460, ip mtu 1460, ip mtu idb Tunnel0
     current outbound spi: 0x896ACAE0(2305477344)
     PFS (Y/N): N, DH group: none

     inbound esp sas:
      spi: 0xC1739D09(3245579529)
        transform: esp-aes esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 1, flow_id: AIM-VPN/SSL-2:1, sibling_flags 80000046, crypto map
: Tunnel0-head-0
```



```
        sa timing: remaining key lifetime (k/sec): (4537342/3177)
        IV size: 16 bytes
        replay detection support: Y
        Status: ACTIVE

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:
      spi: 0x896ACAE0(2305477344)
        transform: esp-aes esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 2, flow_id: AIM-VPN/SSL-2:2, sibling_flags 80000046, crypto map
: Tunnel0-head-0
        sa timing: remaining key lifetime (k/sec): (4537342/3177)
        IV size: 16 bytes
        replay detection support: Y
        Status: ACTIVE

     outbound ah sas:
```

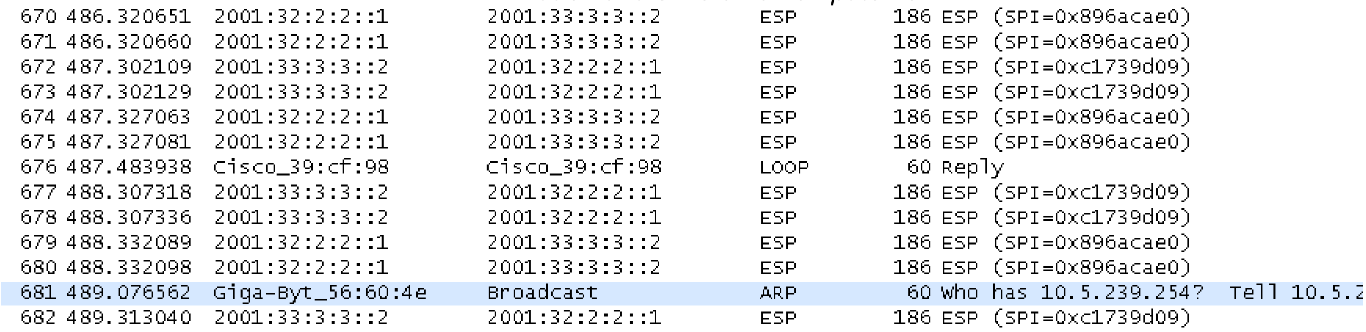
Zrzut ekranu polecenia show crypto ipsec sa ipv6 dla routera R3



```
R3#sh crypto ipsec sa ipv6

interface: Tunnel0
    Crypto map tag: Tunnel0-head-0, local addr 2001:33:3:3::2

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (::/0/0/0)
   remote ident (addr/mask/prot/port): (::/0/0/0)
   current_peer 2001:32:2:2::1 port 500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 22, #pkts encrypt: 22, #pkts digest: 22
    #pkts decaps: 18, #pkts decrypt: 18, #pkts verify: 18
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0

     local crypto endpt.: 2001:33:3:3::2,
     remote crypto endpt.: 2001:32:2:2::1
     path mtu 1460, ip mtu 1460, ip mtu idb Tunnel0
     current outbound spi: 0xC1739D09(3245579529)
     PFS (Y/N): N, DH group: none

     inbound esp sas:
      spi: 0x896ACAE0(2305477344)
        transform: esp-aes esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 1, flow_id: AIM-VPN/SSL-2:1, sibling_flags 80000046, crypto map
: Tunnel0-head-0
        sa timing: remaining key lifetime (k/sec): (4590557/3140)
        IV size: 16 bytes
        replay detection support: Y
        Status: ACTIVE

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:
      spi: 0xC1739D09(3245579529)
        transform: esp-aes esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 2, flow_id: AIM-VPN/SSL-2:2, sibling_flags 80000046, crypto map
: Tunnel0-head-0
        sa timing: remaining key lifetime (k/sec): (4590557/3140)
        IV size: 16 bytes
        replay detection support: Y
        Status: ACTIVE

     outbound ah sas:
```

D. Z komputera K3 poleceniem ping sprawdzić osiągalność interfejsu s0/0/0 routera R2. Wynik ze snifera uruchomionego na komputerze K2 wkleić poniżej.

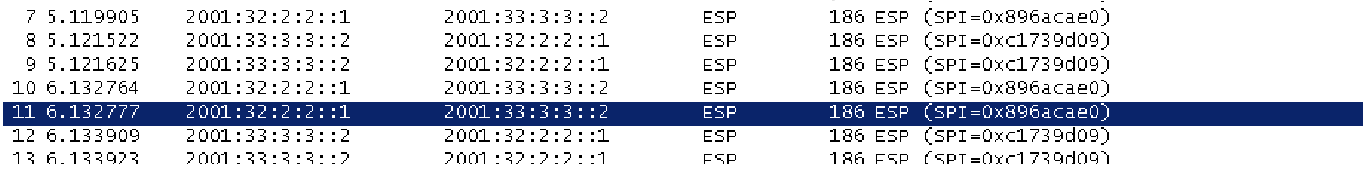
Zrzut ekranu snifera na komputerze K2



```
670 486.320651  2001:32:2:2::1         2001:33:3:3::2        ESP        186 ESP (SPI=0x896acae0)
671 486.320660  2001:32:2:2::1         2001:33:3:3::2        ESP        186 ESP (SPI=0x896acae0)
672 487.302109  2001:33:3:3::2         2001:32:2:2::1        ESP        186 ESP (SPI=0xc1739d09)
673 487.302129  2001:33:3:3::2         2001:32:2:2::1        ESP        186 ESP (SPI=0xc1739d09)
674 487.327063  2001:32:2:2::1         2001:33:3:3::2        ESP        186 ESP (SPI=0x896acae0)
675 487.327081  2001:32:2:2::1         2001:33:3:3::2        ESP        186 ESP (SPI=0x896acae0)
676 487.483938  Cisco_39:cf:98         Cisco_39:cf:98        LOOP        60 Reply
677 488.307318  2001:33:3:3::2         2001:32:2:2::1        ESP        186 ESP (SPI=0xc1739d09)
678 488.307336  2001:33:3:3::2         2001:32:2:2::1        ESP        186 ESP (SPI=0xc1739d09)
679 488.332089  2001:32:2:2::1         2001:33:3:3::2        ESP        186 ESP (SPI=0x896acae0)
680 488.332098  2001:32:2:2::1         2001:33:3:3::2        ESP        186 ESP (SPI=0x896acae0)
681 489.076562  Giga-Byt_56:60:4e      Broadcast             ARP         60 Who has 10.5.239.254?  Tell 10.5.2
682 489.313040  2001:33:3:3::2         2001:32:2:2::1        ESP        186 ESP (SPI=0xc1739d09)
```

E. Z komputera K3 poleceniem ping sprawdzić osiągalność komputera K1. Wynik ze snifera uruchomionego na komputerze K2 wkleić poniżej.

Zrzut ekranu snifera na komputerze K2



```
 7 5.119905    2001:32:2:2::1       2001:33:3:3::2       ESP        186 ESP (SPI=0x896acae0)
 8 5.121522    2001:33:3:3::2       2001:32:2:2::1       ESP        186 ESP (SPI=0xc1739d09)
 9 5.121625    2001:33:3:3::2       2001:32:2:2::1       ESP        186 ESP (SPI=0xc1739d09)
10 6.132764    2001:32:2:2::1       2001:33:3:3::2       ESP        186 ESP (SPI=0x896acae0)
11 6.132777    2001:32:2:2::1       2001:33:3:3::2       ESP        186 ESP (SPI=0x896acae0)
12 6.133909    2001:33:3:3::2       2001:32:2:2::1       ESP        186 ESP (SPI=0xc1739d09)
13 6.133923    2001:33:3:3::2       2001:32:2:2::1       ESP        186 ESP (SPI=0xc1739d09)
```