

# **PRECHOD Z IPV4 NA IPV6 A TUNELOVANIE, P2P MCT/GRE STATICKÉ TUNELY, MULTIPOINT AUTOMAT 6TO4 A ISATAP**

Bc. Lukáš Urbančok



## 1 PRECHOD Z IPV4 NA IPV6 A TUNELOVANIE

V tejto úlohe preskúmame techniky podporované **Cisco** zariadeniami pre **prechod** (migráciu) **z IPv4 na IPv6**. Stručne sú zhrnuté základy a jednoduchá **konfigurácia** **duálnej sady IPv4/IPv6**, **tunelovania** a **prekladu adries**. V prípade potreby **detailného štúdia** sa laboratórna úloha odvoláva na **téoriu DP** kap. 1.3. Jednotliví zákazníci majú **unikátne potreby** podľa existujúcej infraštruktúry. Buď majú **len 2 pobočky** alebo infraštruktúra pokrýva **sieť spoločností**. Práca bola rozdelená do niekoľkých bodov, ktoré pokrývajú základné **praktické znalosti** so zameraním **prechodu** na protokolovú sadu **IPv6**. [1]

### 1.1 Teória:

Predpokladá sa, že je **známe**, čo je **IPv4** alebo **IPv6 adresa** a ako vypadá či už v **DEC** alebo **BIN** podobe. Rozdelenie adries do *tried A, B, C* **výpočet sieťovej** alebo **broadcastovej adresy** nie je náplňou tejto úlohy. V prípade potreby zopakovať si IP protokol, verím, že **odkazy na literatúru** v diplomovej práci budú dostatočným zdrojom. Čo sa týka **migrácie z IPv4 na IPv6**, predpokladá sa **zabezpečenie kompatibility** hardwaru a softwaru (aplikácií) **podporu IPv6**. Laboratórna úloha sa zaoberá technológiami migrácie prípadne **tunelovania** sieťových prvkov. [6]

Využívajú sa nasledujúce **migračné mechanizmy** pre hladkú integráciu IPv6:

- **Duálna sada** (*nezávislá* implementácia IPv4 a IPv6 súbežne)
- **Tunelovanie** (Tunneling – *zapuzdrenie* IPv6 paketu do IPv4 paketu)
  - IPv6 nad IPv4 statické tunely MCT (*RFC 4213*), GRE tunely
  - Tunely protokolu ISATAP (*RFC 5214*), Tunel 6to4 (*RFC 3056*)
- **Preklady** (translations)
  - NAT-PT (Protocol Translation – preklad medzi IPv4 a IPv6) [1]

**Duálna sada (Dual-stack)** je nastavovanie IPv4 a IPv6 pod rozhranie, čo nám aktivuje súbežný chod obchodu sád IP. Nakoľko konfigurácia IPv4 a IPv6 bola testovaná v predchádzajúcich laboratórnych úlohách, začneme **tunelovaním**. Prvým typom tunelov sú **statické P2P tunely** ako je na *Obr. 1*:

## 1.2 Zadanie:

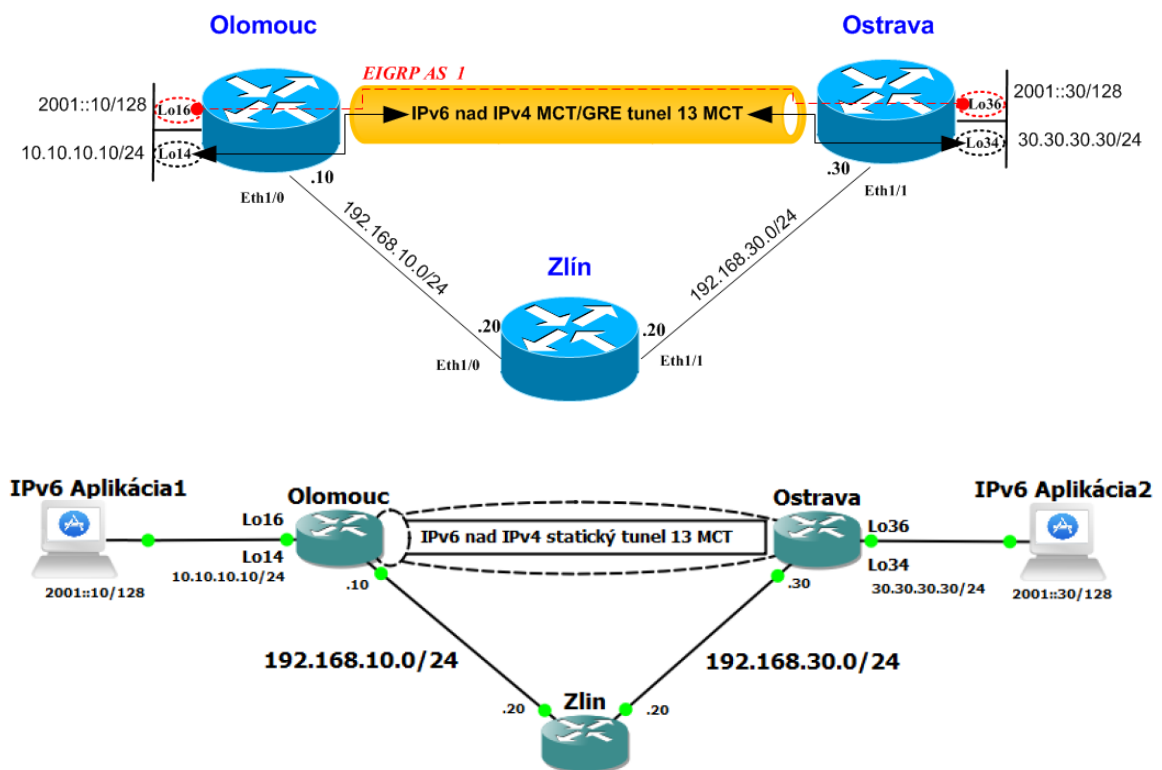
Najväčší poskytovateľ Internetu v Európe sa rozhodol, že zabezpečí konektivitu IPv6 pre svojich zákazníkov. V topológii sú 3 smerovače *Zlín*, *Ostrava* a *Olomouc*. Na hraničných smerovačoch Ostrava a Olomouc bežia **zákaznícke siete na IPv6**. Bohužiaľ smerovač v Zlíne ešte **nepodporuje sadu IPv6** a konektivita, je zabezpečená **pomocou IPv4** sady. Nakoľko **zákazníci Lo10 a Lo30** používajú **aplikáciu**, ktoré pracuje s IPv6 potrebujú zabezpečiť **konektivitu IPv6 infraštruktúry**, preto správca siete navrhol implementovať **statické P2P IPv6 tunely**. [1][2]

## 2.1 Migrácia z IPv4 na IPv6 pomocou statických a GRE tunelov

Nasledujúce ciele boli navrhnuté správcom siete pri vytváraní **statického tunela**. [4]

## 2.2 Topológia IPv6 nad IPv4 MCT/GRE tunela:

Topológia z laboratórnej úlohy pre konfiguráciu statického **IPv6 nad IPv4 MCT/GRE tunela**:



Obr. 1: Topológia z laboratórnej úlohy pre konfiguráciu statického IPv6 tunela [autor]

## 2.3 Riešenie

V tejto časti pomocou jednoduchej **topológie** sa ukázu ako fungujú *statické a GRE tunely*. Oba typy tunelov sú veľmi podobné. Podporujú **IGP** cez tunely prepúšťajú **všesmerovú premávku**. Manuálne tunely sa **odkazujú** na *RFC 4213*, ktoré definuje ako *zapuzdriť IPv6 pakety do IPv4*. Toto môže podporovať rôzne protokoly a ak sa konfigurovalo **IPSEC** (odborový štandard sady protokolov a algoritmov) **VPN** (Virtual Private Network) s IGP, ktoré prechádza cez a musia **použiť GRE**. [3]

### 2.3.1 Nastavte IPv4 a IPv6 adresy na rozhraniach

**Nastavenie IPv4 a IPv6 adries** na rozhraniach podľa *Obr. 1. Spätnoväzbové slučky* predstavujú **zákaznícku aplikáciu**, ktorej chcú zabezpečiť **konektivitu IPv6 adries**.

*Tab. 1: Nastavenie IPv4 a IPv6 adries na rozhraniach [autor]*

```
!Ostrava:
!
conf term
IPv6 unicast-routing
IPv6 cef
interface Loopback 36
ipv6 address 2001::30/128
interface Ethernet1/1
ip address 192.168.30.30 255.255.255.0
full-duplex
no shutdown
!Olomouc:
!
conf term
IPv6 unicast-routing
IPv6 cef
interface Loopback 16
ipv6 address 2001::10/128
interface Ethernet1/0
ip address 192.168.10.10 255.255.255.0
full-duplex
no shutdown
!Zlín:
!
conf term
IPv6 unicast-routing
IPv6 cef
interface Ethernet1/1
ip address 192.168.30.20 255.255.255.0
full-duplex
no shutdown
interface Ethernet1/0
ip address 192.168.10.20 255.255.255.0
full-duplex
no shutdown
```

### 2.3.2 Nastavte manuálne tunelovanie pomocou spätnoväzbových slučiek a pridajte inzerovanie do smerovacieho protokolu OSPF

Dobrym zvykom pri vytváraní tunela je používať spätnoväzbovú slučku, pretože v prípade pádu, sa smerovací protokol pokúsi nájsť inú cestu k spätnoväzbovej slučke suseda, na rozdiel od aplikácií na fyzické rozhranie. Nasledujúca konfigurácia pridáva i manuálny mód tunelovanie podľa RFC 4213. [1]

Tab. 2: Konfigurácia IPv4 a IPv6 spätnoväzbových slučiek pre všetky rozhrania [autor]

```
!Ostrava:
!
show interface tunnel 13
conf terminal
interface tunnel 13
tunnel source Loopback 34
tunnel destination 10.10.10.10
tunnel mode ipv6ip
!Olomouc:
!
show interface tunnel 13
conf terminal
interface tunnel 13
tunnel source Loopback 14
tunnel destination 30.30.30.30
tunnel mode ipv6ip
```

Pomocou vyššie zmienenej konfigurácie si jednoducho vytvorí manuálny tunel. V prípade neupresnenia módu tunela, automaticky sa používa GRE tunelovanie (RFC 2784). Ide o bezstavový protokol TCP/IP (47) k zapuzdereniu paketov jedného protokolu (IPv6) do iného (IPv4). Použitím `show interface tunnel 13` sa jednoducho overí stav tunelu 13.[3]

```
Olomouc#show interface tunnel 13
Tunnel13 is up, line protocol is up
Hardware is Tunnel
MTU 17920 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 10.10.10.10 (Loopback14), destination 30.30.30.30
Tunnel Subblocks:
  src-track:
    Tunnel13 source tracking subblock associated with Loopback14
    Set of tunnels with source Loopback14, 1 member (includes iterators), on interface <OK>
Tunnel protocol/transport IPv6/IPv4
Tunnel TTL 255
Tunnel transport MTU 1480 bytes
Tunnel transmit bandwidth 8000 (kbps)
Tunnel receive bandwidth 8000 (kbps)
Last input 00:00:17, output 00:00:16, output hang never
Last clearing of "show interface" counters 00:01:11
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
11 packets input, 1240 bytes, 0 no buffer
Received 0 broadcasts (0 IP multicasts)
0 runts, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
10 packets output, 928 bytes, 0 underruns
0 output errors, 0 collisions, 0 interface resets
0 unknown protocol drops
0 output buffer failures, 0 output buffers swapped out

Ostrava#show interface tunnel 13
Tunnel13 is up, line protocol is up
Hardware is Tunnel
MTU 17920 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 30.30.30.30 (Loopback34), destination 10.10.10.10
Tunnel Subblocks:
  src-track:
    Tunnel13 source tracking subblock associated with Loopback34
    Set of tunnels with source Loopback34, 1 member (includes iterators), on interface <OK>
Tunnel protocol/transport IPv6/IPv4
Tunnel TTL 255
Tunnel transport MTU 1480 bytes
Tunnel transmit bandwidth 8000 (kbps)
Tunnel receive bandwidth 8000 (kbps)
Last input 00:00:23, output 00:01:24, output hang never
Last clearing of "show interface" counters 00:01:31
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
10 packets input, 1128 bytes, 0 no buffer
Received 0 broadcasts (0 IP multicasts)
0 runts, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
11 packets output, 1020 bytes, 0 underruns
0 output errors, 0 collisions, 0 interface resets
0 unknown protocol drops
0 output buffer failures, 0 output buffers swapped out
```

Obr. 2: Overenie stavu tunelu 13 z hraničných smerovačov Ostrava a Olomouc [autor]

### 2.3.3 Nastav tunel medzi ZURICHOM a GENEVOU, pokiaľ nie sú povolené špecifikácie cieľa tunelovania

Poslednou časťou pre **dostupnosť IPv6** aplikácie cez *IPv4 sieť* je potrebné **inzerovať** a **načúvať** adresy *spätnoväzbových slučiek a tunela*. Môže sa použiť ľubovoľný **smerovací protokol** popísaný v DP v kapitole 1.5.1, ale použije sa **najjednoduchší RIPng pre IPv6**. [2]

Tab. 3: Konfigurácia RIPng pre IPv6 na smerovačoch Ostrava a Olomouc [autor]

```

!Ostrava:
!
show ipv6 route rip
conf terminal
ipv6 router rip RIPng
exit
interface Loopback 36
ipv6 rip RIPng enable
exit
interface tunnel 13
ipv6 enable
ipv6 rip RIPng enable
!Olomouc:
!
show ipv6 route rip
conf terminal
ipv6 router rip RIPng
exit
interface Loopback 16
ipv6 rip RIPng enable
exit
interface tunnel 13
ipv6 enable
ipv6 rip RIPng enable

```

Nasledujúca konfigurácia **aktivovala** smerovací protokol **RIPng** na spätnoväzbovej slučke a **tunelu13** a pridala **IPv6 adresu** pre *tunnel13*, na ktorom nie sú **potrebné žiadne IPv4 adresy**. Následne si môže **skontrolovať** zo smerovacej tabuľky, že oba smerovače **vedia** o sebe:

```

Ostrava#show ipv6 route rip
IPv6 Routing Table - default - 3 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
B - BGP, R - RIP, H - NHRP, I1 - ISIS L1
I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary, D - EIGRP
EX - EIGRP external, ND - ND Default, NDP - ND Prefix, DCE - Destination
NDR - Redirect, O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1
OE2 - OSPF ext 2, ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2, 1 - LISP
R 2001::10/128 [120/2]
  via FE80::A0A:A0A, Tunnel13

Olomouc#show ipv6 route rip
IPv6 Routing Table - default - 3 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
B - BGP, R - RIP, H - NHRP, I1 - ISIS L1
I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary, D - EIGRP
EX - EIGRP external, ND - ND Default, NDP - ND Prefix, DCE - Destination
NDR - Redirect, O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1
OE2 - OSPF ext 2, ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2, 1 - LISP
R 2001::30/128 [120/2]
  via FE80::1E1E:1E1E, Tunnel13

```

Obr. 3: Overenie smerovania RIPng pre IPv6 na smerovačoch Ostrava a Olomouc [autor]

### 2.3.4 V tomto bode, by mali byť dostupné spätnoväzbové slučky, ktoré predstavujú IPv6 aplikácie. Testuj dostupnosť spojení so špecifikáciou zdrojovej aplikácie

Jednoduchá úloha, ktorá len overí konektivitu, siete *IPv6 aplikácií*, čo bola hlavná žiadosť zákazníka pomocou **pingu** medzi smerovačmi *Ostrava* a *Olomouc*. [3]

Tab. 4: Kontrola dostupnosti spätnoväzbových slučiek na smerovačoch pre IPv4 a IPv6 [autor]

```
!Ostrava:
!
ping 2001::30 source Loopback 36
!Olomouc:
!
ping 2001::10 source Loopback 16
```

### 2.3.5 Pomocou ladenia over prichádzajúce ICMPv6 pakety z predchádzajúcej úlohy a pred samotným testom, aktivuj odchytyvanie pomocou Wiresharku.

#### Odpovedá výstup zachytených paketov žiadanému stavu?

Nasledujúce zadanie sa týka **testovania paketov** a prieskumu **zapuzdrenia IPv6** paketu do *IPv4* pri manuálnom tunelovaní. [3]

```
Olomouc#ping 2001::30 source Loopback 16
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001::30, timeout is 2 seconds:
Packet sent with a source address of 2001::10
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 12/13/16 ms
Olomouc#
*Mar  8 09:14:53.771: ICMPv6: Sent echo request, Src=2001::10, Dst=2001::30
*Mar  8 09:14:53.791: ICMPv6: Received echo reply, Src=2001::30, Dst=2001::10
*Mar  8 09:14:53.799: ICMPv6: Sent echo request, Src=2001::10, Dst=2001::30
*Mar  8 09:14:53.815: ICMPv6: Received echo reply, Src=2001::30, Dst=2001::10
*Mar  8 09:14:53.823: ICMPv6: Sent echo request, Src=2001::10, Dst=2001::30
*Mar  8 09:14:53.843: ICMPv6: Received echo reply, Src=2001::30, Dst=2001::10
*Mar  8 09:14:53.851: ICMPv6: Sent echo request, Src=2001::10, Dst=2001::30
*Mar  8 09:14:53.863: ICMPv6: Received echo reply, Src=2001::30, Dst=2001::10
Olomouc#
*Mar  8 09:14:53.867: ICMPv6: Sent echo request, Src=2001::10, Dst=2001::30
*Mar  8 09:14:53.883: ICMPv6: Received echo reply, Src=2001::30, Dst=2001::10
Olomouc#
*Mar  8 09:14:57.675: ICMPv6: Received echo request, Src=2001::30, Dst=2001::10
*Mar  8 09:14:57.679: ICMPv6: Sent echo reply, Src=2001::10, Dst=2001::30
*Mar  8 09:14:57.699: ICMPv6: Received echo request, Src=2001::30, Dst=2001::10
*Mar  8 09:14:57.703: ICMPv6: Sent echo reply, Src=2001::10, Dst=2001::30
*Mar  8 09:14:57.731: ICMPv6: Received echo request, Src=2001::30, Dst=2001::10
*Mar  8 09:14:57.735: ICMPv6: Sent echo reply, Src=2001::10, Dst=2001::30
*Mar  8 09:14:57.751: ICMPv6: Received echo request, Src=2001::30, Dst=2001::10
*Mar  8 09:14:57.755: ICMPv6: Sent echo reply, Src=2001::10, Dst=2001::30
Olomouc#
*Mar  8 09:14:57.771: ICMPv6: Received echo request, Src=2001::30, Dst=2001::10
*Mar  8 09:14:57.775: ICMPv6: Sent echo reply, Src=2001::10, Dst=2001::30

Ostrava#ping 2001::10 source Loopback 36
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001::10, timeout is 2 seconds:
Packet sent with a source address of 2001::30
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 12/25/36 ms
Ostrava#
*Mar  8 08:37:49.291: ICMPv6: Sent echo request, Src=2001::30, Dst=2001::10
*Mar  8 08:37:49.303: ICMPv6: Received echo reply, Src=2001::10, Dst=2001::30
*Mar  8 08:37:49.311: ICMPv6: Sent echo request, Src=2001::30, Dst=2001::10
*Mar  8 08:37:49.343: ICMPv6: Received echo reply, Src=2001::10, Dst=2001::30
*Mar  8 08:37:49.351: ICMPv6: Sent echo request, Src=2001::30, Dst=2001::10
*Mar  8 08:37:49.371: ICMPv6: Received echo reply, Src=2001::10, Dst=2001::30
*Mar  8 08:37:49.379: ICMPv6: Sent echo request, Src=2001::30, Dst=2001::10
*Mar  8 08:37:49.411: ICMPv6: Received echo reply, Src=2001::10, Dst=2001::30
Ostrava#
*Mar  8 08:37:49.419: ICMPv6: Sent echo request, Src=2001::30, Dst=2001::10
*Mar  8 08:37:49.455: ICMPv6: Received echo reply, Src=2001::10, Dst=2001::30
Ostrava#
*Mar  8 09:14:53.495: ICMPv6: Received echo request, Src=2001::10, Dst=2001::30
*Mar  8 09:14:53.499: ICMPv6: Sent echo reply, Src=2001::30, Dst=2001::10
*Mar  8 09:14:53.507: ICMPv6: Received echo request, Src=2001::10, Dst=2001::30
*Mar  8 09:14:53.511: ICMPv6: Sent echo reply, Src=2001::30, Dst=2001::10
*Mar  8 09:14:53.539: ICMPv6: Received echo request, Src=2001::10, Dst=2001::30
*Mar  8 09:14:53.539: ICMPv6: Sent echo reply, Src=2001::30, Dst=2001::10
*Mar  8 09:14:53.559: ICMPv6: Received echo request, Src=2001::10, Dst=2001::30
*Mar  8 09:14:53.559: ICMPv6: Sent echo reply, Src=2001::30, Dst=2001::10
Ostrava#ping 2001::10 source Loopback 36
*Mar  8 09:14:53.575: ICMPv6: Received echo request, Src=2001::10, Dst=2001::30
*Mar  8 09:14:53.579: ICMPv6: Sent echo reply, Src=2001::30, Dst=2001::10
```

Obr. 4: Ladenie ICMPv6 paketov pri pingu pre IPv4 a IPv6 [autor]

Pomocou *debug ipv6 icmp* sa aktivuje ladenie ICMPv6 paketov pri pingu. **Vypínanie Ladenia** je možné urobiť pomocou **negovania príkazu** alebo všeobecné vypnutie ladenia *undebg all*. [4]

### 2.3.6 Zmeň mód tunelovania na GRE, over nastavenie a porovnaj výstup zachytených paketov vo Wiresharku s prechádzajúcou úlohou.

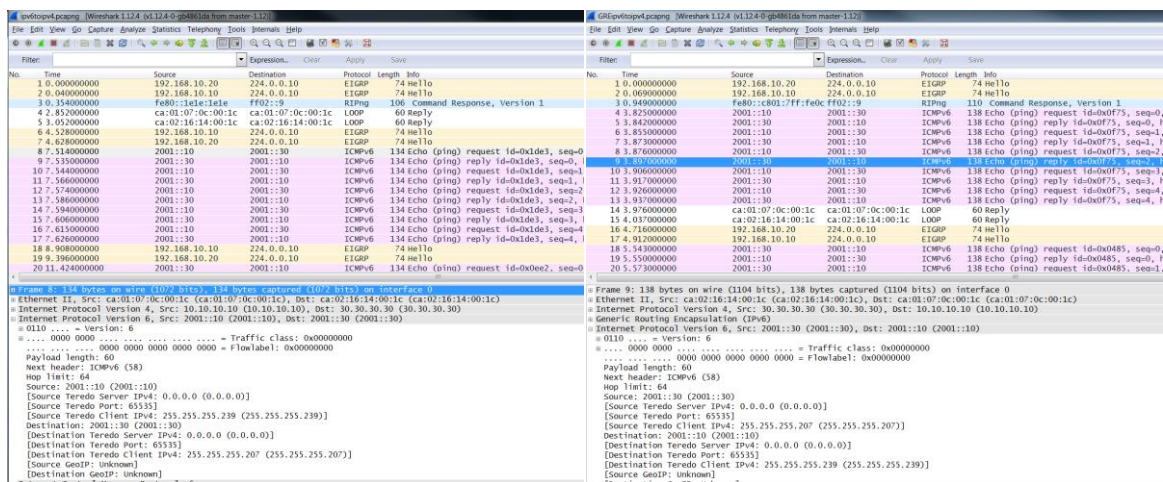
Nasledujúce **otázka** sa týka pochopenia **rozdielu** medzi manuálnym *ipv6ip tunelom* a prednastaveným *GRE tunelom*. Nastavenie *GRE tunela*, sa môže urobiť v tomto prípade **dvomi spôsobmi**; zrušením *ipv6ip* a nastavenie **prednastavených hodnôt**, alebo novou konfiguráciou *GRE*:

Tab. 5: Konfigurácia typu tunela na prednastavený GRE medzi Ostrava a Olomouc [autor]

```

!Ostrava:
!
interface tunnel 13
no tunnel mode ipv6ip ! zrušením ipv6ip a nastavenie prednastaveného GRE módu
tunnel mode gre ip
!Olomouc:
!
interface tunnel 13
no tunnel mode ipv6ip zrušením ipv6ip a nastavenie prednastaveného GRE módu
tunnel mode gre ip
    
```

Použitím pingu z predchádzajúcej úlohy sa generujú pakety, ktoré sú zachytené:[9]



Obr. 5: Zachytenie paketov ICMPv6 v MCT a GRE tunela medzi Ostrava a Olomouc [autor]

Pri detailnom skúmaní **odchytených paketov** vo Wiresharku sa zistí, že sa **líši veľkosť MTU a IPv6 linková-lokálna adresa** na rozhraní tunela.

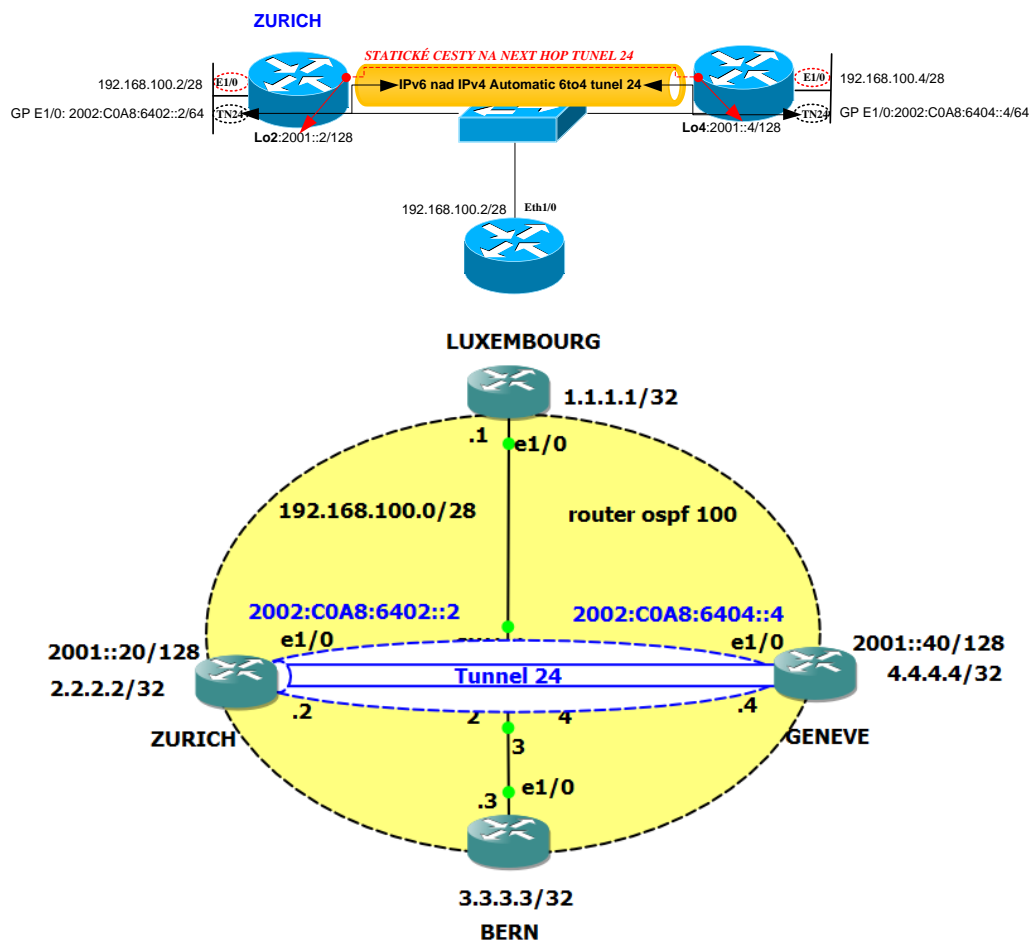
- IPv6 linková-lokálna na rozhraní **GRE tunela** je tvorená pomocou **EUI-64** a použije **najnižšie číslo rozhrania** z MAC adresy,
- IPv6 linková-lokálna na rozhraní **manuálneho tunela** je **FE80::/96+ 32 bitov** zo zdrojovej **IPv4 adresy tunela**. [10]

### 3.1 Migrácia z IPv4 na IPv6 pomocou dynamických automatických 6to4 a ISATAP tunelov

Nasledujúce ciele boli **navrhnuté** správcom siete pri vytváraní **dynamických multipoint automatických 6to4 a ISATAP tunelov**. Tieto metódy sú použité pri **migrácii** viac bodových **spojení**, kde má zákazník veľa **pobočiek**. Jednotlivé typy sa líšia podľa **zapuzdrenia do tunela**. Tunely sú dynamické, pretože sa **nešpecifikujú** koncové **IPv4** adresy (**cieľový uzol**), ale sú **automaticky** určené. **Nevýhodou** multipoint **IPv6** tunelov je, že **nepodporujú IPv6 IGP** (interior gateway protocol). **Musia byť** použité **statické cesty** alebo **BGP** (Border Gateway Protocol), ktorým sa nebude zaoberať úloha, pretože **presahuje rozsah zadania**. [10]

### 3.2 Topológia 6to4 a ISATAP tunela:

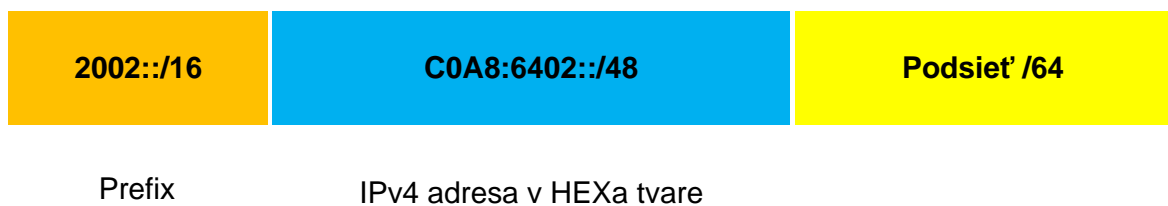
Topológia z úlohy pre konfiguráciu **automatických 6to4 a ISATAP tunela**:



Obr. 6: Topológia z laboratórnej úlohy pre konfigurácie 6to4 a ISATAP tunela [autor]

### 3.3 Riešenie

Tieto typy sú využívané ako **multipoint tunely**. V úlohe na **koncových častiach siete**, ktoré predstavujú zakončené **zákaznícke siete**, používajúce **IPv6 adresu**, ktoré musia byť **obalené IPv4 adresami**. Pre účely tunelovania je použitý **rozsah adries 2002::/16**, ktorý je **rezervovaný pre tieto účely**. Tento rozsah nemôže byť nikdy použitý ako **globálne unicastové adresy**. Pre koncové body je **použitý prefix /48**. Čo je potrebné urobiť, je **premeniť IPv4 adresu do HEXa tvaru ako 17 bitov do 48 bitového prefixu**. Nasledujúci krok je **doplnenie podsiete do /64** pre všetky podsiete medzi **koncovými stanicami**. Ako je zrejmé z nasledujúceho *Obr. 7*, je **2002::/16** použiteľný rozsah pre **tunely**. Ďalšia časť je **IPv4 adresa koncového bodu tunela konvertovaná do HEXa tvaru**. Až **/64** rozsah je možné **použiť** pre vytvorenie **podsietí**. **C0A8:6402** je možné **konvertovať späť** do **IPv4 adresy 192.168.100.2** [10]



*Obr. 7: Ilustrácia použitej IPv6 adresy pre tunely [autor]*

V Cisco smerovačoch sa môže **pomôcť s príkazom** `ipv6 general-prefix prefix-name {ipv6-prefix/prefix-length | 6to4 interface-type interface-number}`, ktorý k prefixu **pripojí konvertovanú adresu** definovaného rozhrania: [3]

*Tab. 6: Výpočet IPv4 HEX adresy pomocou Cisco smerovača [autor]*

```

!ZURICH:
!
ZURICH(config)#ipv6 general-prefix TEST 6to4 Ethernet1/0
ZURICH(config)#end
ZURICH#
ZURICH#show ipv6 general-prefix
IPv6 Prefix TEST, acquired via 6to4
2002:C0A8:6402::/48 Valid lifetime infinite, preferred lifetime infinite
!
!GENEVE:
GENEVE(config)#ipv6 general-prefix TEST 6to4 Ethernet1/0
GENEVE(config)#exi
GENEVE#show ipv6 general-prefix
IPv6 Prefix TEST, acquired via 6to4
2002:C0A8:6404::/48 Valid lifetime infinite, preferred lifetime infinite

```

V prípade, že si chcete **overiť** svoje výpočtové **znanosti** pre prevod medzi *hexadecimálne* a *binárne/dekadické*. Jednoducho sa **nastaví IPv4** pod rozhranie a použije sa vyššie **zmienený IPv6 prefix**. Výhodou automatického tunela je, že nie je **potrebné konfigurovať** cieľ tunela na smerovačoch *ZURICH* alebo *GENEVA*. [6]

### 3.3.1 Nastavte IPv4 a IPv6 adresy na rozhraniach

Nastavenie **IPv4 a IPv6** adries na rozhraniach podľa *Obr. 6. spätnoväzbové slučky* predstavujú **zákaznícku aplikáciu**, ktorej si chce **zabezpečiť** konektivitu cez IPv6 adries.

Tab. 7: Nastavenie IPv4 a IPv6 adries na rozhraniach [autor]

```
!VŠETKY SMEROVAČE:
!
IPv6 unicast-routing
IPv6 cef
!
interface Ethernet1/0
IPv6 enable
!LUXEMBOURG:
conf term
hostname LUXEMBOURG
interface Ethernet1/0
ip address 192.168.100.1 255.255.255.240
full-duplex
no shutdown
!
!ZURICH:
conf term
hostname ZURICH
!
interface Ethernet1/0
ip address 192.168.100.2 255.255.255.240
full-duplex
no shutdown
!
!BERN:
conf term
hostname BERN
!
interface Ethernet1/0
ip address 192.168.100.3 255.255.255.240
full-duplex
no shutdown
!
!GENEVE:
conf term
hostname GENEVE
interface Ethernet1/0
ip address 192.168.100.4 255.255.255.240
full-duplex
no shutdown
```

### 3.3.2 Nastavte IPv4 konektivity medzi smerovačmi pomocou OSPF protokolu.

Ďalšie zadanie sa týka nastavenia *dynamického protokola OSPF*, ktorý zabezpečí **konektivitu** cez celú sieť a inzerovanie všetkých spätnoväzbových slučiek a **dostupných** sietí v **budúcnosti**. Pre ďalšiu úlohu vytvorenia **tunela** sú vytvorené *IPv6 prefixy* podľa *Tab. 6*, za účelom **naviazania** rozhrania tunela medzi **smerovačmi**. [6]

*Tab. 8: Nastavte IPv4 konektivity medzi smerovačmi pomocou EIGRP protokolu [autor]*

```
! LUXEMBOURG:
conf term
router ospf 100
network 0.0.0.0 255.255.255.255 area 1
!
! ZURICH:
conf term
interface Loopback2
ip address 2.2.2.2 255.255.255.255
!
interface Loopback20
ipv6 address 2001::20/128
ipv6 enable
!
!BERN:
conf term
interface Loopback3
ip address 3.3.3.3 255.255.255.255
!
router ospf 100
network 0.0.0.0 255.255.255.255 area 1
!
!GENEVE:
conf term
!
router ospf 100
network 0.0.0.0 255.255.255.255 area 1
interface Loopback4
ip address 4.4.4.4 255.255.255.255
!
interface Loopback40
ipv6 address 2001::40/128
```

### 3.3.3 Nastavte automatické 6to4 tunelovanie pomocou fyzického rozhrania

Pri **vytváraní tunela** je dobrým zvykom používať (*spätnoväzbovú slučku*), pretože v prípade pádu *fyzického rozhrania* nespôsobí *pád tunelu* a pokúsi nájsť inú cestu k spätnoväzbovej slučke **suseda**. Nakoľko bolo v predchádzajúcom príklade **použité rozhranie** *spätnoväzbovej slučky*, **nasledujúca úloha** používa rozhranie *Ethernet1/0*. Cieľové rozhranie **tunela** nie je potrebné definovať, pretože je **nastavený** mód **IPv6IP 6to4**. Ten povie smerovaču, že **IPv4 adresa je získaná z IPv6 adresy**. [10]

*Tab. 9: Konfigurácia IPv4 a IPv6 spätnoväzbových slučiek pre všetky rozhrania [autor]*

```

! ZURICH:
conf term
!
interface Tunnel24
ipv6 address 2002:C0A8:6402::2/64
tunnel source a/0
tunnel mode ipv6ip 6to4
!
!GENEVE:
conf term
interface Tunnel24
ipv6 address 2002:C0A8:6404::4
ipv6 enable
tunnel source Ethernet1/0
tunnel mode ipv6ip 6to4

```

Pomocou vyššie zmienenej konfigurácie sa jednoducho vytvorí **ipv6ip tunel**. V prípade **upresnenia** módu tunela sa používa **6to4 tunelovanie (RFC 3056, 6434)**. Ideo **bezstavový protokol TCP/IP (47)** k **zapuzdereniu paketov** jedného protokolu (**IPv6**) do iného (**IPv4**). Použitím sa jednoducho **overí stav tunelu 24**:

```

GENEVE#show interface tunnel 24
Tunnel24 is up, line protocol is up
Hardware is Tunnel
MTU 17920 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 192.168.100.4 (Ethernet1/0)
Tunnel Subblocks:
  src-track:
    Tunnel24 source tracking subblock associated with Ethernet1/0
    Set of tunnels with source 192.168.100.4, 1 member (includes iterators), on interface <CR>
  tunnel protocol/transport ipv6 6to4
Tunnel TTL 255
Tunnel transport MTU 1480 bytes
Tunnel transmit bandwidth 8000 (kbps)
Tunnel receive bandwidth 8000 (kbps)
Last input never, output never, output hang never
Last clearing of "show interface" counters 00:56:48
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
  0 packets input, 0 bytes, 0 no buffer
  Received 0 broadcasts (0 IP multicasts)
  0 runs, 0 giants, 0 throttles
  0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
  0 packets output, 0 bytes, 0 underruns
  0 output errors, 0 collisions, 0 interface resets
  0 unknown protocol drops
  0 output buffer failures, 0 output buffers swapped out

ZURICH#show interface tunnel 24
Tunnel24 is up, line protocol is up
Hardware is Tunnel
MTU 17920 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 192.168.100.2 (Ethernet1/0)
Tunnel Subblocks:
  src-track:
    Tunnel24 source tracking subblock associated with Ethernet1/0
    Set of tunnels with source 192.168.100.2, 1 member (includes iterators), on interface <CR>
  tunnel protocol/transport ipv6 6to4
Tunnel TTL 255
Tunnel transport MTU 1480 bytes
Tunnel transmit bandwidth 8000 (kbps)
Tunnel receive bandwidth 8000 (kbps)
Last input never, output never, output hang never
Last clearing of "show interface" counters 00:58:44
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
  0 packets input, 0 bytes, 0 no buffer
  Received 0 broadcasts (0 IP multicasts)
  0 runs, 0 giants, 0 throttles
  0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
  0 packets output, 0 bytes, 0 underruns
  0 output errors, 0 collisions, 0 interface resets
  0 unknown protocol drops
  0 output buffer failures, 0 output buffers swapped out

```

Obr. 8: Overenie stavu tunela 24 z hraničných smerovačov GENEVE a ZURICH [autor]

### 3.3.4 Nastav statické smerovanie na rozhraniach spätnoväzbových slučiek a tunela

Poslednou časťou pre **dostupnosť IPv6 aplikácie cez IPv4 sieť** je potrebné **inzerovať a načúvať** adresy spätnoväzbových slučiek a tunela. Môžu sa **použiť statické cesty** alebo **BGP (Border Gateway Protocol)**, ktorým sa **nebude zaoberať úloha**, pretože presahuje **rozsah zadania**, preto sú aplikované statické cesty. [10]

Tab. 10: Konfigurácia statického IPv6 smerovania na smerovačoch ZURICH a GENEVE [autor]

```

! ZURICH:
conf term
ipv6 route 2001::40/128 2002:C0A8:6404::4
ipv6 route 2002::/16 Tunnel24

```

```
!GENEVE:
conf term
ipv6 route 2001::20/128 2002:C0A8:6402::2
ipv6 route 2002::/16 Tunnel24
```

Nasledujúca konfigurácia **aktivovala statické smerovanie** na *spätnoväzbovú slučku 40* (zo smerovača *ZURICH*) a *20* (zo smerovača *GENEVA*) na druhej strane. Ukazuje sa na **IPv6 adresy**, ktoré majú *HEX tvar* z pôvodnej *IPv4* podľa *Tab. 6*. **Smerovače** musia mať **rekurzívne smerovanie**, aby sa **vracala** odpoveď a bol záznam v **smerovacej tabuľke** pre *2002::*. Preto potrebuje druhé **statické smerovanie**, ktoré smeruje **premávku** priamo do rozhrania *Tunel 24*. Následne si môže **skontrolovať** zo smerovacej tabuľky, že oba **smerovače** vedia o sebe a že **zákaznícka sieť** je smerovaná **do Tunel 24**:

```
GENEVE#show ipv6 route
IPv6 Routing Table - default - 6 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
B - BGP, R - RIP, H - NHRP, I1 - ISIS L1
I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary, D - EIGRP
EX - EIGRP external, ND - ND Default, NDP - ND Prefix, DCE - Destination
NDR - Redirect, O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1
OE2 - OSPF ext 2, ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2, L - LISP
S 2001::20/128 [1/0]
   via 2002:C0A8:6402::2
LC 2001::40/128 [0/0]
   via Loopback40, receive
S 2002::/16 [1/0]
   via Tunnel24, directly connected
C 2002:C0A8:6404::/64 [0/0]
   via Tunnel24, directly connected
L 2002:C0A8:6404::4/128 [0/0]
   via Tunnel24, receive
L FF00::/8 [0/0]
   via Null0, receive

ZURICH#show ipv6 route
IPv6 Routing Table - default - 6 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
B - BGP, R - RIP, H - NHRP, I1 - ISIS L1
I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary, D - EIGRP
EX - EIGRP external, ND - ND Default, NDP - ND Prefix, DCE - Destination
NDR - Redirect, O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1
OE2 - OSPF ext 2, ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2, L - LISP
LC 2001::20/128 [0/0]
   via Loopback20, receive
S 2001::40/128 [1/0]
   via 2002:C0A8:6602:4
S 2002::/16 [1/0]
   via Tunnel24, directly connected
C 2002:C0A8:6402::/64 [0/0]
   via Tunnel24, directly connected
L 2002:C0A8:6402::2/128 [0/0]
   via Tunnel24, receive
L FF00::/8 [0/0]
   via Null0, receive
```

Obr. 9: Overenie statického IPv6 smerovania na smerovačoch *ZURICH* a *GENEVE* [autor]

### 3.3.5 V tomto bode, by mali byť dostupné spätnoväzbové slučky, ktoré predstavujú IPv6 aplikácie. Testuj dostupnosť spojení so špecifikáciou zdrojovej aplikácie

Jednoduchá úloha, ktorá len **overí konektivitu** siete *IPv6 aplikácií*, čo bola **hlavná žiadosť** zákazníka pomocou **pingu** medzi smerovačmi *ZURICH* a *GENEVE*. [3]

Tab. 11: Kontrola dostupnosti spätnoväzbových slučiek na smerovačoch pre *IPv4* a *IPv6* [autor]

```
! ZURICH:
ping 2001::40 source Lo20
traceroute 2001::40
!GENEVE:
ping 2001::20 source Lo20
```

```
traceroute 2001::20
```

### 3.3.6 Pomocou ladenia over prichodzie ICMPv6 pakety z predchadzajúcej úlohy a pred samotným testom, aktivuj odchyťovanie pomocou Wiresharku.

**Odpovedá výstup zachytených paketov žiadanému stavu?**

Nasledujúce zadanie sa týka testovania paketov a **prieskumu zapuzdrenia IPv6** paketu do IPv4 pri **6to4** tunelovaní.

```
GENEVE#ping 2001::20 source Lo40
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001::20, timeout is 2 seconds:
Packet sent with a source address of 2001::40
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 12/33/64 ms
GENEVE#
*Apr 14 14:01:47.207: ICMPv6: Sent echo request, Src=2001::40, Dst=2001::20
*Apr 14 14:01:47.267: ICMPv6: Received echo reply, Src=2001::20, Dst=2001::40
*Apr 14 14:01:47.275: ICMPv6: Sent echo request, Src=2001::40, Dst=2001::20
*Apr 14 14:01:47.343: ICMPv6: Received echo reply, Src=2001::20, Dst=2001::40
*Apr 14 14:01:47.347: ICMPv6: Sent echo request, Src=2001::40, Dst=2001::20
*Apr 14 14:01:47.359: ICMPv6: Received echo reply, Src=2001::20, Dst=2001::40
*Apr 14 14:01:47.363: ICMPv6: Sent echo request, Src=2001::40, Dst=2001::20
*Apr 14 14:01:47.379: ICMPv6: Received echo reply, Src=2001::20, Dst=2001::40
GENEVE#
*Apr 14 14:01:47.379: ICMPv6: Sent echo request, Src=2001::40, Dst=2001::20
*Apr 14 14:01:47.399: ICMPv6: Received echo reply, Src=2001::20, Dst=2001::40
GENEVE#
*Apr 14 14:01:49.535: ICMPv6: Received echo request, Src=2001::20, Dst=2001::40
*Apr 14 14:01:49.535: ICMPv6: Sent echo reply, Src=2001::40, Dst=2001::20
*Apr 14 14:01:49.615: ICMPv6: Received echo request, Src=2001::20, Dst=2001::40
*Apr 14 14:01:49.615: ICMPv6: Sent echo reply, Src=2001::40, Dst=2001::20
*Apr 14 14:01:49.623: ICMPv6: Received echo request, Src=2001::20, Dst=2001::40
*Apr 14 14:01:49.623: ICMPv6: Sent echo reply, Src=2001::40, Dst=2001::20
*Apr 14 14:01:49.631: ICMPv6: Received echo request, Src=2001::20, Dst=2001::40
*Apr 14 14:01:49.635: ICMPv6: Sent echo reply, Src=2001::40, Dst=2001::20

ZURICH#
*Apr 14 14:01:47.419: ICMPv6: Received echo request, Src=2001::40, Dst=2001::20
*Apr 14 14:01:47.423: ICMPv6: Sent echo reply, Src=2001::20, Dst=2001::40
*Apr 14 14:01:47.487: ICMPv6: Received echo request, Src=2001::40, Dst=2001::20
*Apr 14 14:01:47.487: ICMPv6: Sent echo reply, Src=2001::20, Dst=2001::40
*Apr 14 14:01:47.523: ICMPv6: Received echo request, Src=2001::40, Dst=2001::20
*Apr 14 14:01:47.527: ICMPv6: Sent echo reply, Src=2001::20, Dst=2001::40
*Apr 14 14:01:47.555: ICMPv6: Received echo request, Src=2001::40, Dst=2001::20
*Apr 14 14:01:47.555: ICMPv6: Sent echo reply, Src=2001::20, Dst=2001::40
ZURICH#debug ip icmp debug ipv6 icmp
*Apr 14 14:01:47.567: ICMPv6: Received echo request, Src=2001::40, Dst=2001::20
*Apr 14 14:01:47.571: ICMPv6: Sent echo reply, Src=2001::20, Dst=2001::40
ZURICH#ping 2001::40 source Lo20
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001::40, timeout is 2 seconds:
Packet sent with a source address of 2001::20
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/27/84 ms
ZURICH#
*Apr 14 14:01:49.711: ICMPv6: Sent echo request, Src=2001::20, Dst=2001::40
*Apr 14 14:01:49.795: ICMPv6: Received echo reply, Src=2001::40, Dst=2001::20
*Apr 14 14:01:49.795: ICMPv6: Sent echo request, Src=2001::20, Dst=2001::40
*Apr 14 14:01:49.803: ICMPv6: Received echo reply, Src=2001::40, Dst=2001::20
*Apr 14 14:01:49.803: ICMPv6: Sent echo request, Src=2001::20, Dst=2001::40
*Apr 14 14:01:49.831: ICMPv6: Received echo reply, Src=2001::40, Dst=2001::20
*Apr 14 14:01:49.835: ICMPv6: Sent echo request, Src=2001::20, Dst=2001::40
*Apr 14 14:01:49.847: ICMPv6: Received echo reply, Src=2001::40, Dst=2001::20
```

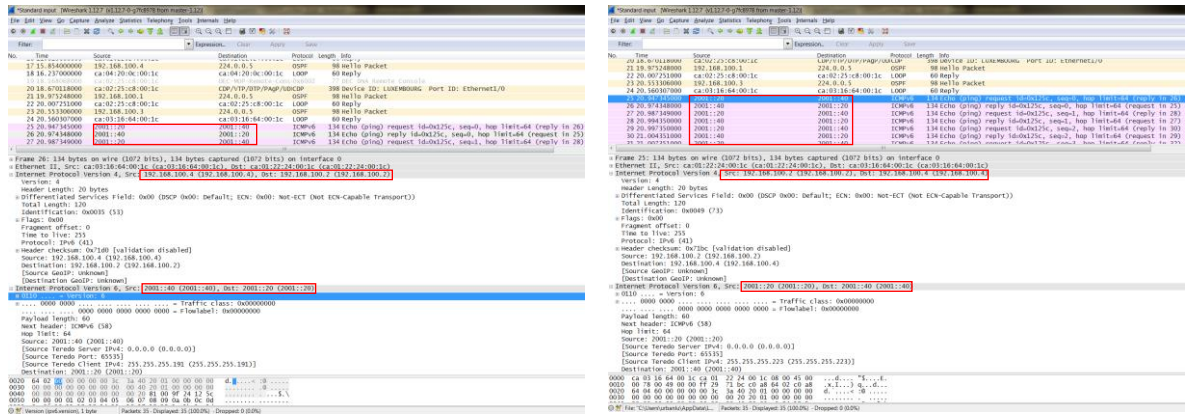
*Obr. 10: Ladenie ICMPv6 paketov pri pingu medzi zákazníkymi pobočkami cez Tunel 24*

*[autor]*

Pomocou *debug ipv6 icmp* sa aktivuje ladenie *ICMPv6* paketov pri pingu. **Vypínanie ladenia**, ktoré je možné urobiť pomocou **negovania** príkazu alebo všeobecné **vypnutie ladenia** *undebug all*. [4]

### 3.3.7 Nastav a porovnaj výstup zachytených paketov vo Wiresharku a počas testovania dostupnosti preskúmaj zabalenie paketov

Použitím pingu z predchádzajúcej úlohy sa generujú pakety, ktoré sú zachytené: [9]



Obr. 11: Zachytenie paketov ICMPv6 v 6to4 Tunelu24 medzi ZURICH a GENEVE [autor]

### 3.3.8 Nastav mód tunelovania na ISATAP, over nastavenie a porovnaj výstup zachytených paketov vo Wiresharku s prechádzajúcou úlohou

Nasledujúce otázka sa týka **pochopenia rozdielu** medzi **ISATAP tunelom** a prednastaveným **6to4 tunelom**. Nastavenie **ISATAP** tunela, je potrebné urobiť medzi smerovačmi **BERN** a **LUXEMBOURG**; nastavenie **novej konfigurácie ISATAP** tunela:

Tab. 12: Konfigurácia ISATAP tunela medzi smerovačmi BERN a LUXEMBOURG [autor]

```

! BERN:
!
BERN (config-if)# exit
BERN (config)# interface tunnel 35
BERN (config-if)# ipv6 address 2001::/64 eui-64
BERN (config-if)# no ipv6 nd suppress-ra
BERN (config-if)# tunnel source Lo3
BERN (config-if)# tunnel mode ipv6ip isatap
!
! LUXEMBOURG:
!
LUXEMBOURG:
LUXEMBOURG (config)# interface tunnel 35
LUXEMBOURG (config-if)# ipv6 enable
LUXEMBOURG (config-if)# ipv6 address autoconfig
LUXEMBOURG (config-if)# tunnel source Eth1/0
LUXEMBOURG (config-if)# tunnel destination 3.3.3.3
LUXEMBOURG (config-if)# tunnel mode ipv6ip
    
```

Konfiguruje sa **smerovač BERN** do **ISATAP módu tunelovania** a je použitý prefix **2001::/64** s **EUI-64**. Je potrebné použiť i **no ipv6 nd suppress-ra** (no ipv6 nd ra suppress)

za účelom **nepovolenia** inzerovania **RA** na **rozhraní tunelu**. Smerovač **LUXEMBOURG** môže použiť **RA** pre autokonfiguráciu. Cieľ sa nastaví **Lo3**, čím sa získa spojenie. [10]

**Použitím pingu** na vzdialenú unicast adresu sa **generujú pakety**, ktoré sú zachytené:

No.	Time	Source	Destination	Protocol	Length	Info
360	470.407036000	192.168.201.1	224.0.0.10	EIGRP	74	Hello
361	474.583453000	192.168.201.2	224.0.0.10	EIGRP	74	Hello
362	474.749470000	2001::c0a8:c902	2001::5efe:606:606	ICMPv6	134	Echo (ping) request id=0x10db, seq=0, hop limit=64 (reply in 363)
363	474.778473000	2001::5efe:606:606	2001::c0a8:c902	ICMPv6	134	Echo (ping) reply id=0x10db, seq=0, hop limit=64 (request in 362)
364	474.829478000	2001::c0a8:c902	2001::5efe:606:606	ICMPv6	134	Echo (ping) request id=0x10db, seq=1, hop limit=64 (reply in 365)
365	474.848480000	2001::5efe:606:606	2001::c0a8:c902	ICMPv6	134	Echo (ping) reply id=0x10db, seq=1, hop limit=64 (request in 364)
366	474.869482000	2001::c0a8:c902	2001::5efe:606:606	ICMPv6	134	Echo (ping) request id=0x10db, seq=2, hop limit=64 (reply in 367)
367	474.888484000	2001::5efe:606:606	2001::c0a8:c902	ICMPv6	134	Echo (ping) reply id=0x10db, seq=2, hop limit=64 (request in 366)
368	474.890484000	2001::c0a8:c902	2001::5efe:606:606	ICMPv6	134	Echo (ping) request id=0x10db, seq=3, hop limit=64 (reply in 369)
369	474.908486000	2001::5efe:606:606	2001::c0a8:c902	ICMPv6	134	Echo (ping) reply id=0x10db, seq=3, hop limit=64 (request in 368)
370	474.910486000	2001::c0a8:c902	2001::5efe:606:606	ICMPv6	134	Echo (ping) request id=0x10db, seq=4, hop limit=64 (reply in 371)
371	474.938489000	2001::5efe:606:606	2001::c0a8:c902	ICMPv6	134	Echo (ping) reply id=0x10db, seq=4, hop limit=64 (request in 370)
372	475.291534000	192.168.201.1	224.0.0.10	EIGRP	74	Hello

Frame 362: 134 bytes on wire (1072 bits), 134 bytes captured (1072 bits) on interface 0  
 Ethernet II, Src: ca:0a:31:e4:00:1c (ca:0a:31:e4:00:1c), Dst: ca:08:10:04:00:1d (ca:08:10:04:00:1d)  
 Internet Protocol Version 4, Src: 192.168.201.2 (192.168.201.2), Dst: 6.6.6.6 (6.6.6.6)  
 Internet Protocol Version 6, Src: 2001::c0a8:c902 (2001::c0a8:c902), Dst: 2001::5efe:606:606 (2001::5efe:606:606)  
 0110 .... = Version: 6  
 .... 0000 0000 .... = Traffic class: 0x00000000  
 .... 0000 0000 0000 0000 0000 = Flowlabel: 0x00000000  
 Payload length: 60  
 Next header: ICMPv6 (58)  
 Hop limit: 64  
 Source: 2001::c0a8:c902 (2001::c0a8:c902)  
 [Source Teredo Server IPv4: 0.0.0.0 (0.0.0.0)]  
 [Source Teredo Port: 65535]  
 [Source Teredo Client IPv4: 63.87.54.253 (63.87.54.253)]  
 Destination: 2001::5efe:606:606 (2001::5efe:606:606)  
 [Destination Teredo Server IPv4: 0.0.0.0 (0.0.0.0)]  
 [Destination Teredo Port: 41217]  
 [Destination Teredo Client IPv4: 249.249.249.249 (249.249.249.249)]  
 [Destination ISATAP IPv4: 3.3.3.3 (3.3.3.3)]  
 [Source GeoIP: Unknown]  
 [Destination GeoIP: Unknown]  
 Internet Control Message Protocol v6

```

0000  ca 08 10 04 00 1d ca 0a 31 e4 00 1c 08 00 45 00  ....1....E.
0010  00 78 00 10 00 00 ff 29 25 96 c0 a8 c9 02 06 06  .X.....)%....
0020  06 06 60 00 00 00 00 3c 3a 40 20 01 00 00 00 00  ..<:@.....
0030  00 00 00 00 00 00 c0 a8 c9 02 20 01 00 00 00 00  .....:.....
0040  00 00 00 00 5e fe 06 06 06 06 80 00 ad 4f 10 db  ....A.....0..
0050  00 00 00 00 01 03 03 04 05 06 07 08 09 0a 0b 0c  .....

```

Obr. 12: Zachytenie paketov ICMPv6 v 6to4 tunela24 medzi BERN a LUXEMBOURG  
 [autor]







Pri **detailnom skúmaní** odchytených paketov vo Wireshark sa zistí, že sa líši **ISATAP** od **6to4** tunela a že nepoužíva rezervovaný rozsah **2002::/16**, ale globálne unikastové adresy. **ISATAP** má zabudované **IPv4** adresy v posledných **dvoch kvartáloch**. Ďalej používa **jednotný prefix** na základe, ktorého sa vytvoria tunely s použitím **EUI-64**. Jedná sa o **HUB & SPOKE** topológiu. **EUI-64** pracuje trochu inak pre účely tunelovania:

- Smerovače používajú **0000:5EFE** pre **5. a 6. kvartál**
- Smerovače budú používať zdrojovú tunelovú adresu, ktorá sa preloží pre **7. a 8. kvartál**[10]

Čo bola **posledná úloha** tejto laboratórnej úlohy. Existuje nepreberné množstvo úloh, ktoré je možné vytvoriť pre **účely testovania**.

Výsledné **nastavenie** smerovačov pre konfiguráciu tunelov pre IPv4 a IPv6:

Tab. 13: Konfigurácia OSPF pre IPv4 a IPv6 smerovačov v Cisco IOS 15.2(4) S3 [autor]

LUXEMBOURG	GENEVE	BERN	ZURICH	Wireshark	GNS3
 LUXEMB.txt	 GENEVE.txt	 BERN.txt	 ZURICH.txt	 isatap.pcapng	 test6to4.gns3

Laboratórna úloha **slúži** k **riešeniu** často sa vyskytujúcich **problémov** v danej **technológii** **sietí** tunelov. V tejto laboratórnej úlohe ste sa **naučili techniky prechodu z IPv4 na IPv6 a tunelovanie, MCT/GRE statické tunely, multipoint automatické 6TO4 a ISATAP.** [2, 3]

Pre konfiguráciu tunelov a zobrazenie súčasného stavu sa použijú nasledujúce príkazy:

Tab. 14: Syntax aplikovaných príkazov a vysvetlenie významu OSPF IPv4 a IPv6 [autor]

	Syntax + Príkaz	Význam/Účel
Syntax príkazu:	<b>router#show interfaces</b> router#show interface tunnel 13	Zobrazenie štatistík pre rozhrania na smerovači.
Syntax príkazu:	<b>router (config)#ipv6 unicast-routing</b> <b>router (config)#ipv6 unicast-routing</b>	Zasielanie IPv6 prenos z CEF na smerovači.
Syntax príkazu:	<b>router (config-if)#ipv6 address IPv6 Address</b> router (config-if)#ipv6 address 2001::30/128	Nastavenie IPv6 adresy pre dané rozhranie s prefixom.
Syntax príkazu:	<b>router (config-if)#ip address IP Address</b> router (config-if)# ip address 192.168.30.30 255.255.255.0	Nastavenie IPv4 adresy pre dané rozhranie.
Syntax príkazu:	<b>router (config)#ipv6 enable</b> router (config)#ipv6 enable	Povolenie spracovávanía IPv6 na danom rozhraní .
Syntax príkazu:	<b>router (config)#interface [brief] [ type number ] [prefix]</b> router (config)#interface tunnel 13	Vstup do konfiguračného rozhrania tunel 13
Syntax príkazu:	<b>router (config-router)#router-id RID</b> router (config-rtr)#router-id RID	RID špecifikované v konfigurácii OSPF procesu
Syntax príkazu:	<b>r(config)#router ospf 1; network 1.1.1.1 0.0.0.0 area 1;</b> <b>r(config)#interface Ethernet1/0; ipv6 ospf 1 area 1;</b>	Nastavenie inzerovania siete v OSPFv2 a OSPFv3.
Syntax príkazu:	<b>#show ip ospf neighbor [[detail]   [summary]]</b> <b>#show ipv6 ospf neighbor [[detail]   [summary]]</b>	Zobrazí susedov, ktorých OSPF IPv4 a IPv6 pozná.
Syntax príkazu:	<b>router#show ip route</b> router#show ipv6 route	Zobrazenie smerovacej tabuľky pre IPv4 a IPv6.
Syntax príkazu:	<b>router#show ip protocols</b> router#show ipv6 protocols	Zobrazenie detaily pre IPv4 a IPv6 protokoly.
Syntax príkazu:	<b>r#ipv6 general-prefix prefix-name</b> r(config)#ipv6 general-prefix TEST 6to4 Ethernet1/0	Konvertovanie adresy na definovanom rozhraní

Syntax příkazu:	<b>r(config-if)# tunnel destination IP Address</b> r(config-if)# tunnel destination 3.3.3.3	Nastavenie cieľovej IPv4 adresy tunela.
Syntax příkazu:	<b>r(config-if)# tunnel mode ipv6ip</b> r(config-if)# tunnel source Eth1/0	Nastavenie módu tunelovania.
Syntax příkazu:	<b>r(config-if)# no ipv6 nd suppress-ra</b> r(config-if)# no ipv6 nd suppress-ra	Nepovolenie inzerovania RA na rozhraní tunela.
Syntax příkazu:	<b>r(config-if)# tunnel mode ipv6ip</b> r(config-if)# tunnel mode ipv6ip	Nastavenie módu tunelovania IPv6IP.
Syntax příkazu:	<b>r(config-if)# tunnel mode ipv6ip isatap</b> r(config-if)# tunnel mode ipv6ip isatap	Nastavenie módu tunelovania isatap.
Syntax příkazu:	<b>r(config-if)# tunnel mode gre ip</b> r(config-if)# tunnel mode gre ip	Nastavenie módu tunelovania GRE.
Syntax příkazu:	<b>router#clear ip ospf [process-id] process</b> router#clear ipv6 ospf [process-id] process	Reset celého OSPFv2 a OSPFv3 procesu PID.
Syntax příkazu:	<b>show ipv6 interface [brief] [ type number ] [prefix]</b> router# show ipv6 interface Loopback 36	Zobrazenie stavu rozhrania Loopback 36 a ipv6 adres
Syntax příkazu:	<b>router#clear ip route</b> router#clear ipv6 route	Vymazanie OSPF smerovacej tabuľky
Syntax příkazu:	<b>router#show ip ospf</b> router#show ipv6 ospf	Overenie OSPFv2 info Overenie OSPFv3 info
Syntax příkazu:	<b>router#debug ip ospf packet</b> router#debug ipv6 ospf packet	Diagnostika OSPFv2 Diagnostika OSPFv3
Syntax příkazu:	<b>router#undebug all</b>	Vypnutie všetkých debug oznámení na termináli.
Syntax příkazu:	<b>router#ping [-t] [-a] [-n count] [-l size] [-f] [-r count] [-R]</b> R2# ping 10.1.1.2	Overenie odozvy protistrany (icmp)
Syntax příkazu:	<b>router#traceroute IP Address</b> router#traceroute 2A00:CB20:F:2::6	Zistenie cesty k cieľu pre IPv4 a IPv6 adresu
Syntax příkazu:	<b>#copy running-config startup-config /write memory</b> <b>r(config-if)#copy running-config startup-config</b>	Uloženie aktuálneho nastavenia do NVRAM.

**ZOZNAM POUŽITÉJ LITERTÚRY**

- [1] MCFARLAND, Shannon. *IPv6: kompletní průvodce nasazením v podnikových sítích*. Vyd. 1. Brno: Computer Press, 2011, 368 s. ISBN 978-80-251-3684-3.
- [2] LAMMLE, Todd. *CCNA: výukový průvodce*. 1. vydání. Překlad Jakub Goner. Brno: Computer Press, 2015. ISBN 978-80-251-4602-6.
- [3] Cisco Networking Academy Course Catalog, [Online]. [cit. 2015-10-28].  
Dostupné z :  
[www.cisco.com/web/learning/netacad/course\\_catalog/CCNAexploration.html](http://www.cisco.com/web/learning/netacad/course_catalog/CCNAexploration.html).
- [4] *GNS3 | Graphical Network Simulator*. [Online]. [cit. 2015-10-28]. Dostupné z:  
[www.gns3.net](http://www.gns3.net).
- [5] ODOM, Wendell. *Cisco CCENT/CCNA ICND1 100-101 official cert guide, academic edition*. Academic edition. Indianapolis, IN: Cisco Press, 2013. ISBN 1587144859.
- [6] ODOM, Wendell. *Cisco CCNA routing and switching ICND2 200-101 official cert guide*. Indianapolis, Indiana: Cisco Press, 2013. ISBN 1587143739.
- [7] HUCABY, Dave. *CCNP routing and switching SWITCH 300-115 official cert guide*. Indianapolis, IN: Cisco press, 2015. ISBN 978-1-58720-560-6.
- [8] URBANČOK, Lukáš. *Technologie IPv6, její bezpečnost a simulace sítí s využitím GNS3*. Zlín, 2016. Diplomová práce. Fakulta aplikované informatiky - Univerzita Tomáše Bati ve Zlíně. Katedra počítačových a komunikačních systémů. Vedoucí kvalifikační práce Ing. Jiří Korbel, Ph.D.
- [9] SANDERS, Chris. *Analýza sítí a řešení problémů v programu Wireshark*. Brno: Computer Press, 2012. ISBN 978-80-251-3718-5.
- [10] ODOM, Wendell. *CCNP ROUTE 642-902 official certification guide*. Indianapolis, Ind.: Cisco Press, c2010. Official certification guide series. ISBN 978-1-58720-253-7.

**ZOZNAM POUŽITÝCH SYMBOLOV A SKRATIEK**

6to4	technológia tunelovanie
BDR	Záložný Určený Smerovač (Backup Designated Router)
BGP	Border Gateway Protocol
BIN	Binárna
CCNA	Cisco Certified Network Associate
DEC	Dekadická
DP	Diplomová práca
DR	Určený Smerovač (Designated Router)
E1/0	Ethernet 1/0
EIGRP	Enhanced Interior Gateway Routing Protocol
EUI-64	automatický výpočet adresy rozhrania v podsieti z MAC adresy
GRE	Generic Routing Encapsulation
H&S	Hub&Spoke
HEX	Hexadecimálna
ICMPv6	Internet Control Message Protocol v6 – poskytovateľ služieb správ
IF	Rozhranie (Interface)
IGP	Interior Gateway Protocol
IPSEC	Oborový štandard sady protokolov a algoritmov
IPV4	Internet Protocol Version 4
IPV6	Internet Protocol Version 6
ISATAP	Intra-Site Automatic Tunnel Addressing Protokol
LO1	Spätnoväzbová slučka (Loopback1)
MAC	L2 adresa, ktorá jednoznačne identifikuje fyzické pripojenie hostiteľa
MCT	Manually Configured Tunnel
MD5	Message Digest 5
NAT-PT	Prechod medzi IPv4 a IPv6
NVRAM	Non Volatile Random Access Memory
OSPF	Open Shortest Path First
P2P	Point-to-Point
PID	ID procesu (Process-ID)
RA	Router advertisement
RFC	Request For Change
RID	ID smerovača (Router-ID)
RIPng	Routing Information Protokol
RTR	Smerovač (Router)
SHA	Secure Hash Algorithm
SIA	Stuck In Active
TCP/IP	Transmission Control Protocol/Internet Protokol
VPN	Virtual Private Network

**ZOZNAM OBRÁZKOV**

<i>Obr. 1: Topológia z laboratórnej úlohy pre konfiguráciu statického IPv6 tunela</i> <i>[autor] .....</i>	<i>3</i>
<i>Obr. 2: Overenie stavu tunelu 13 z hraničných smerovačov Ostrava a Olomouc</i> <i>[autor] .....</i>	<i>5</i>
<i>Obr. 3: Overenie smerovania RIPng pre IPv6 na smerovačoch Ostrava a Olomouc</i> <i>[autor] .....</i>	<i>6</i>
<i>Obr. 4: Ladení ICMPv6 paketov pri pingu pre IPv4 a IPv6 [autor].....</i>	<i>7</i>
<i>Obr. 5: Zachytenie paketov ICMPv6 v MCT a GRE tunela medzi Ostrava a Olomouc</i> <i>[autor] .....</i>	<i>8</i>
<i>Obr. 6: Topológia z laboratórnej úlohy pre konfigurácie 6to4 a ISATAP tunela</i> <i>[autor] .....</i>	<i>9</i>
<i>Obr. 7: Ilustrácia použitej IPv6 adresy pre tunely [autor] .....</i>	<i>10</i>
<i>Obr. 8: Overenie stavu tunela 24 z hraničných smerovačov GENEVE a ZURICH</i> <i>[autor] .....</i>	<i>13</i>
<i>Obr. 9: Overenie statického IPv6 smerovania na smerovačoch ZURICH a GENEVE</i> <i>[autor] .....</i>	<i>14</i>
<i>Obr. 10: Ladenie ICMPv6 paketov pri pingu medzi zákazníkymi pobočkami cez</i> <i>Tunel 24 [autor] .....</i>	<i>15</i>
<i>Obr. 11: Zachytenie paketov ICMPv6 v 6to4 Tunelu24 medzi ZURICH a GENEVE</i> <i>[autor] .....</i>	<i>16</i>
<i>Obr. 12: Zachytenie paketov ICMPv6 v 6to4 tunela24 medzi BERN</i> <i>a LUXEMBOURG [autor] .....</i>	<i>17</i>

**ZOZNAM TABULIEK**

<i>Tab. 1: Nastavenie IPv4 a IPv6 adres na rozhraniach [autor].....</i>	<i>4</i>
<i>Tab. 2: Konfigurácia IPv4 a IPv6 spätnoväzbových slučiek pre všetky rozhrania [autor] .....</i>	<i>5</i>
<i>Tab. 3: Konfigurácia RIPng pre IPv6 na smerovačoch Ostrava a Olomouc [autor] .....</i>	<i>6</i>
<i>Tab. 4: Kontrola dostupnosti spätnoväzbových slučiek na smerovačoch pre IPv4 a IPv6 [autor].....</i>	<i>7</i>
<i>Tab. 5: Konfigurácia typu tunela na prednastavený GRE medzi Ostrava a Olomouc [autor] .....</i>	<i>8</i>
<i>Tab. 6: Výpočet IPv4 HEX adresy pomocou Cisco smerovača [autor] .....</i>	<i>10</i>
<i>Tab. 7: Nastavenie IPv4 a IPv6 adres na rozhraniach [autor].....</i>	<i>11</i>
<i>Tab. 8: Nastavte IPv4 konektivity medzi smerovačmi pomocou EIGRP protokolu [autor] .....</i>	<i>12</i>
<i>Tab. 9: Konfigurácia IPv4 a IPv6 spätnoväzbových slučiek pre všetky rozhrania [autor] .....</i>	<i>12</i>
<i>Tab. 10: Konfigurácia statického IPv6 smerovania na smerovačoch ZURICH a GENEVE [autor].....</i>	<i>13</i>
<i>Tab. 11: Kontrola dostupnosti spätnoväzbových slučiek na smerovačoch pre IPv4 a IPv6 [autor].....</i>	<i>14</i>
<i>Tab. 12: Konfigurácia ISATAP tunela medzi smerovačmi BERN a LUXEMBOURG [autor] .....</i>	<i>16</i>
<i>Tab. 13: Konfigurácia OSPF pre IPv4 a IPv6 smerovačov v Cisco IOS 15.2(4) S3 [autor] .....</i>	<i>18</i>
<i>Tab. 14: Syntax aplikovaných príkazov a vysvetlenie významu OSPF IPv4 a IPv6 [autor] .....</i>	<i>18</i>