VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ
ÚSTAV TELEKOMUNIKACÍ

FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION
DEPARTMENT OF TELECOMMUNICATIONS

NÁVRH NOVÝCH LABORATORNÍCH ÚLOH PRO SIMULAČNÍ PROSTŘEDÍ GNS3

BAKALÁŘSKÁ PRÁCE
BACHELOR'S THESIS

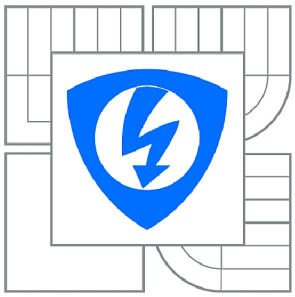
AUTOR PRÁCE
AUTHOR

FRANTIŠEK BUREŠ

BRNO 2015

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

BRNO UNIVERSITY OF TECHNOLOGY



FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ

ÚSTAV TELEKOMUNIKACÍ

FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION

DEPARTMENT OF TELECOMMUNICATIONS

NÁVRH NOVÝCH LABORATORNÍCH ÚLOH PRO SIMULAČNÍ PROSTŘEDÍ GNS3

DESIGN OF NEW LABORATORY EXERCISES FOR GNS3 NETWORK SIMULATOR

BAKALÁŘSKÁ PRÁCE

BACHELOR'S THESIS

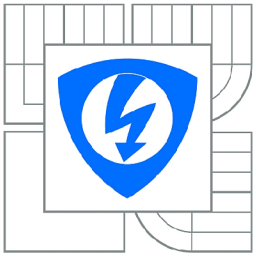
AUTOR PRÁCE — FRANTIŠEK BUREŠ

AUTHOR

VEDOUCÍ PRÁCE — Ing. JAN JEŘÁBEK, Ph.D.

SUPERVISOR

BRNO 2015



VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

Fakulta elektrotechniky a komunikačních technologií

Ústav telekomunikací

Bakalářská práce

bakalářský studijní obor
Teleinformatika

Student: František Bureš ***ID:*** 154241
Ročník: 3 ***Akademický rok:*** 2014/2015

NÁZEV TÉMATU:

Návrh nových laboratorních úloh pro simulační prostředí GNS3

POKYNY PRO VYPRACOVÁNÍ:

Prostudujte možnosti simulačního prostředí GNS3/Dynamips, problematiku operačních systémů pro Cisco zařízení a obsahy kurzů XCA3 až XCA5. V rámci této bakalářské práce se zaměřte na návrh tří nových laboratorních úloh určených pro virtualizované prostředí. Hlavní témata úloh volte zejména z těchto okruhů: porovnání protokolů IPv4 a IPv6 při různých operacích, směrovací protokoly s IPv4 a IPv6, problematika síťové bezpečnosti s IPv4 a IPv6, technika MPLS a tunelovací protokoly. Ke každé úloze vytvořte i český návod vhodný pro studenty, včetně kontrolních otázek a doplňujících úkolů. Kde to bude vhodné, připravte do úlohy výchozí topologii a konfiguraci. Délka každé úlohy musí být přibližně dvě hodiny.

DOPORUČENÁ LITERATURA:

[1] TEARE, Diane. Implementing Cisco IP routing (ROUTE): foundation learning guide : foundation learning for the ROUTE 642-902 exam. Indianapolis: Cisco Press, 2010, xxix, 945 s. ISBN 978-1-58705-882-0.
[2] FROOM, Richard, Balaji SIVASUBRAMANIAN a Erum FRAHIM. Implementing Cisco IP switched networks (SWITCH): foundation learning guide. 1st ed. Indianapolis: Cisco Press, 2010, xxiv, 526 s. ISBN 978-1-58705-884-4.
[3] RANJBAR, Amir. Troubleshooting and mainting cisco IP networks (TSHOOT) foundation learning guide: foundation learning for the CCNP TSHOOT 642-832. 1st ed. Indianapolis: Cisco Press, 2010, xviii, 531 s. ISBN 978-1-58705-876-9.

Termín zadání: 9.2.2015 ***Termín odevzdání:*** 2.6.2015

Vedoucí práce: Ing. Jan Jeřábek, Ph.D.
Konzultanti bakalářské práce:

doc. Ing. Jiří Mišurec, CSc.
Předseda oborové rady

ABSTRAKT

Cílem bylo vytvořit tři úlohy s postupem a nápovědou v prostředí GNS3. Všechny úlohy mají sloužit jako rozšíření praktických zkušeností z Cisco kurzu CCNP a ukázka funkčnosti GNS3. Celá práce se zaměřuje na použití IPv6 a koexistenci s IPv4. Teoretické části jsou věnovány přípravě na úlohy a jejich hlavní cíl je vysvětlení a použití příkazů v dané problematice. U Prostředí GNS3 je popsána instalace a základní nastavení. Jednotlivé úlohy na téma MP-BGP, IPv6 tunely a IPsec VPN s využitím VTI jsou rozděleny do určitých částí. Obsažen je postupný návod s topologií, podrobnější nápověda a v příloze celá konfigurace.

KLÍČOVÁ SLOVA

GNS3, IPv6, BGP, MP-BGP, EIGRP, IPsec VPN, VTI, ZBF, Tunelování, GRE tunel, 6to4 tunel, ISATAP tunel, Cisco, Směrovač

ABSTRACT

The goal was to create three laboratory tasks with process and help in GNS3 environment. All laboratory tasks should be used for extending practise experiences from Cisco course CCNP and illustration of GNS3 function. Whole thesis is focused on using IPv6 and coexistence with IPv4. Teoretical parts are dedicated for preparation on laboratory tasks and their main goal is explaining and use of commands in specific problematics. In GNS3 environment, there is explained instalation and basic settings. Laboratory tasks on theme MP-BGP, IPv6 tunnels and IPsec VPN with use of VTI are divided into specific parts. The parts consist of the described procedures with topology, detailed instructions and the entire configuration in Annex.

KEYWORDS

GNS3, IPv6, BGP, MP-BGP, EIGRP, IPsec VPN, VTI, ZBF, Tunneling, GRE tunnel, 6to4 tunnel, ISATAP tunnel, Cisco, Router

BUREŠ, František *Návrh nových laboratorních úloh pro simulační prostředí GNS3*: bakalářská práce. Brno: Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, Ústav telekomunikací, 2015. 91 s. Vedoucí práce byl Ing. Jan Jeřábek, Ph.D.

PROHLÁŠENÍ

Prohlašuji, že svou bakalářskou práci na téma „Návrh nových laboratorních úloh pro simulační prostředí GNS3“ jsem vypracoval samostatně pod vedením vedoucího bakalářské práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou všechny citovány v práci a uvedeny v seznamu literatury na konci práce.

Jako autor uvedené bakalářské práce dále prohlašuji, že v souvislosti s vytvořením této bakalářské práce jsem neporušil autorská práva třetích osob, zejména jsem nezasáhl nedovoleným způsobem do cizích autorských práv osobnostních a/nebo majetkových a jsem si plně vědom následků porušení ustanovení § 11 a následujících autorského zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů, včetně možných trestněprávních důsledků vyplývajících z ustanovení části druhé, hlavy VI. díl 4 Trestního zákoníku č. 40/2009 Sb.

Brno ....

(podpis autora)

PODĚKOVÁNÍ

Rád bych poděkoval vedoucímu bakalářské práce panu Ing. Janu Jeřábkovi, Ph.D za odborné vedení, konzultace, trpělivost a podnětné návrhy k práci.

Brno ....

(podpis autora)

Faculty of Electrical Engineering
and Communication
Brno University of Technology
Purkynova 118, CZ-61200 Brno
Czech Republic

http://www.six.feec.vutbr.cz

PODĚKOVÁNÍ

Výzkum popsaný v této bakalářské práci byl realizován v laboratořích podpořených z projektu SIX; registrační číslo CZ.1.05/2.1.00/03.0072, operační program Výzkum a vývoj pro inovace.

Brno . . . . . .

. . . . . .

(podpis autora)

EVROPSKÁ UNIE
EVROPSKÝ FOND PRO REGIONÁLNÍ ROZVOJ
INVESTICE DO VAŠÍ BUDOUCNOSTI

OP Výzkum a vývoj
pro inovace

OBSAH

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

ÚVOD

Simulační nástroje jsou v dnešní době důležitým pomocníkem nejen na poli informatiky. Pomocí simulačního softwaru lze testovat skutečné situace bez nutnosti nákupu reálných zařízení, což ocení nejenom studenti, ale i odborníci v praxi. Sítě lze simulovat např. pomocí Cisco Packet Traceru nebo GNS3.

S protokolem IPv6 (Internet Protocol version 6) se v dnešní době setkal snad každý trochu informatikou obeznámený člověk. Jedná se o protokol 3. vrstvy ISO/OSI (International Standards Organization / Open Systen Interconnection) modelu. Byl vytvořen jako „nástupce“ protokolu IPv4 (Internet Protocol version 4). Hlavním důvodem pro vytvoření byl nedostatečný adresní prostor. V dnešní době, kdy prakticky IPv4 adresy došly a zapracovává se IPv6, je pro síťové specialisty nutnost znát rozdíly, které mohou být v konfiguraci značné.

Minimálně několik následujících let je nutné, aby byla možná koexistence IPv4 a IPv6. Stále se totiž používá mnoho zařízení podporující pouze IPv4 a je nutnost postupného vybudování a otestování IPv6 infrastruktury. Existuje několik řešení pro komunikaci mezi IPv4 a IPv6 sítěmi, které jsou určeny pro různé situace. Základní techniky pro kategorizaci jsou dual-stack, překladové techniky a tunelování.

Pro alespoň částečné pochopení fungování Internetu je dobré znát protokol BGP (Border Gateway Protocol), který propojuje navzájem více AS (Autonomous System), což jsou zpravidla sítě pod zprávou jedné organizace.

VPN (Virtual Private Network) se používá k vzdálenému připojení do lokální sítě, obvykle jde o připojení zaměstnanců přes Internet do pobočky společnosti. Pro zabezpečení se používá skupina protokolů IPsec (Internet Protocol security). Každá větší síť by měla mít nějaké zabezpečení na hranici s venkovní sítí, často se využívá firewall.

Cílem této práce je návrh 3 úloh pro simulační prostředí GNS3. Teoretické části obsahují základní informace potřebné pro vypracování praktických úloh a jejich porozumění. Zaměření je především na praktické použití příkazů. Samotné úlohy jsou rozděleny na úvod, kde je obsažena topologie a pozadí úlohy. Dále je uveden postup řešení a nakonec nápověda. Celá konfigurace, krok po kroku, je obsažena v příloze.

1 GNS3

GNS3 je open-source grafický simulátor sítí. Stejně jako VMware nebo VirtualBox umožňují emulovat operační systémy, tak GNS3 pomocí Dynamips a Qemu emuluje síťové prvky. VirtualBox ve spojení s GNS3 lze použít pro propojení virtualizovaných systémů s ostatními prvky.

Dynamips je program, který umožňuje emulaci Cisco IOS, v současné době pouze pro směrovače. Problém s Cisco přepínači je v tom, že určité operace dělají hardwarově. Qemu emuluje zažízení Cisco ASA, Cisco IDS, Cisco PIX, Juniper směrovače a další.

Je to velice používaný nástroj pro přípravu na Cisco certifikace CCNA, CCNP a CCIE. Není to pouze nástroj pro učení, určitě najde využití i ve firemní sféře jako testovací prostředí. Tento program má obrovskou komunitu lidí, kteří tvoří podporu na oficiálním fóru a dělí se o své zkušenosti ve formě článků nebo videí. Podporované operační systémy jsou Windows, Linux a Mac OS [1].

V roce 2014 se stalo mnoho revolučních věcí, které posunuly celý projekt na vyšší úroveň. Byly vybudovány zcela nové webové stránky a fórum, kde je možnost přidat se do určitých skupin a společně řešit problémy v určité oblasti. Nové verze se dočkal také samotný software GNS3. Vyšla verze 1.0 (později i dodatečné balíčky), kde není sice moc nových možností, ale spíše se sází na lepší propracování a stabilitu. Za zmínku stojí možnost nakonfigurovat si rovnou svůj směrovač s moduly a nastavením, který můžeme opakovaně používat a nemusíme nastavovat každý zvlášť, jak tomu bylo dříve.

1.1 Instalace GNS3 a základní nastavení

V této části popíši základní informace o instalaci a nastavení GNS3. Budu popisovat postupy pro GNS3 verzi 1.0 na platformě Windows, ale principy jsou na všech platformách a verzích stejné. Rozeberu tyto části:

- instalaci
- nastavení směrovače
- vytváření základní topologie

Instalace

Pro stažení je třeba přejít na oficiální stránky www.GNS3.com, kde je nutno se prvně registrovat. Na stránkách také lze nalézt podrobný návod instalace na všechny podporované platformy. Kromě příručky pro instalaci lze stáhnout i návody na nastavení

zařízení a vytváření topologie, vše v anglickém jazyce. Instalace je ve formě „all-in-one“, což znamená, že si lze v průběhu instalace vybrat přesně komponenty, které chceme. Hlavní možnosti jsou GNS3, Dynamips a Qemu.

Nastavení směrovače

1. spustit program GNS3
2. v hlavním menu kliknout na edit - preference
3. nyní se nacházíte v nastavení jednotlivých modulů, zde kliknout na Dynamips - IOS routers - new
4. vložit cestu uloženého IOS
5. GNS3 by měla sama detekovat platformu a doplnit název
6. nastavení velikosti RAM, pokud máte prostředky, doporučuji velikost zvětšit
7. můžete předdefinovat moduly - jak Ethernet, tak WIC
8. nastavení Idle-PC, toto je velice důležité a sníží to značně vytížení procesoru, lze popřípadě změnit v nastavení zařízení (s hvězdičkou je doporučované)

Vytváření základní topologie

1. V levé části programu lze zvolit typ zařízení a jednoduše přetáhnout na plochu.
2. Propojení zařízení se dělá pomocí kliknutí na poslední prvek v levé části (ikona pro propojení) a následným kliknutím na zařízení.
3. Zařízení lze zapnout po jednom (pravým tlačítkem myši klikneme na zařízení - start) nebo vše naráz tlačítkem start v hlavní nabídce.
4. Konfigurace se provádí kliknutím pravého tlačítka myši na zařízení - console.
5. Dále jsou možnosti vytváření popisků a jiné grafické úpravy viz příloha Obrázky.

2 INTERNET PROTOKOL VERZE 6

IPv6 (Internet Protocol version 6) [5] je protokol 3. vrstvy ISO/OSI (International Standards Organization / Open Systen Interconnection) modelu. Hlavní důvod pro vytvoření IPv6 byl nedostatek adresního prostoru IPv4 (Internet Protocol version 4). S vytvořením nového protokolu přišla i možnost úprav, např. povinná podpora IPsec (Internet Protocol security) a výhody plynoucí z mnohem většího adresního prostoru jako možná end-to-end konektivita a přehlednější směrování.

2.1 Porovnání IPv6 hlavičky s IPv4

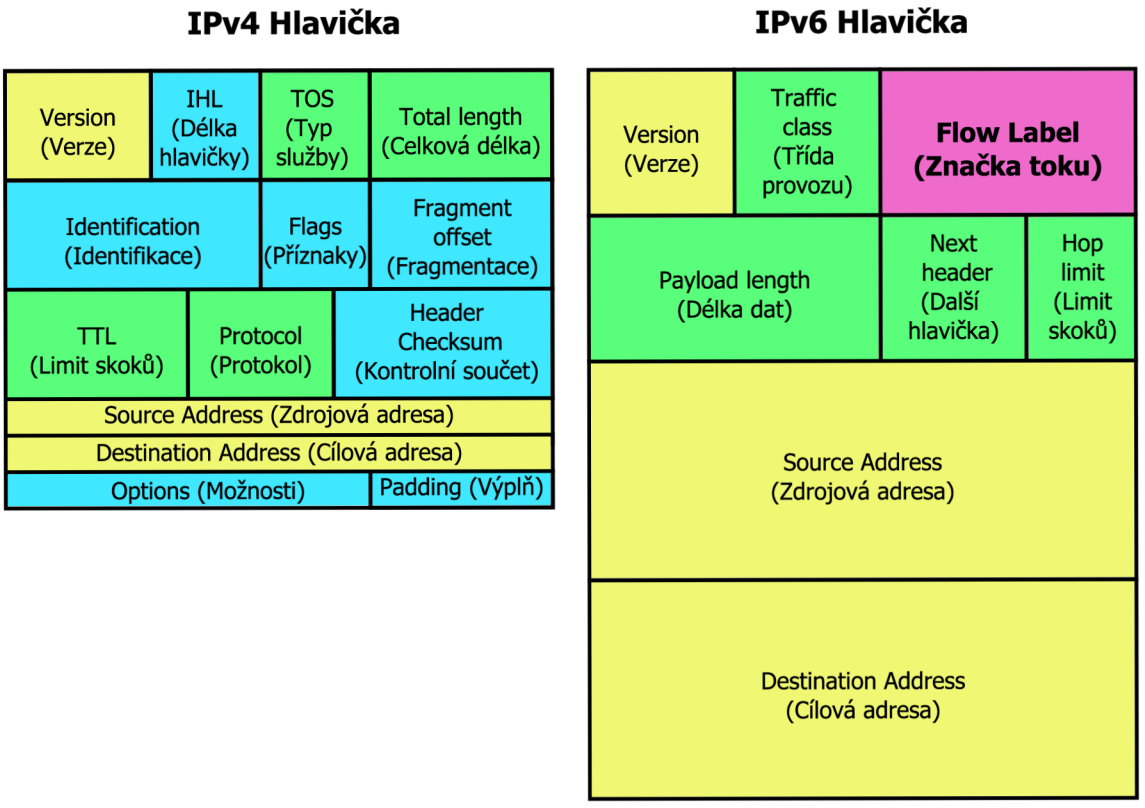
Hlavička IPv6 protokolu [3] je velmi zjednodušena oproti IPv4, jediné pole Flow label (QoS - kvalita služeb) je přidáno, přesto je celková délka hlavičky přibližně dvojnásobná ve srovnání s IPv4. Je zde i možnost rozšíření hlaviček výhodná pro směrování a fragmentaci, velikost paketu poté může sahat do výše 4 GB, jedná se o tzv. jumbo pakety (nastavení pole Payload length na 0).

Detailnější porovnání hlaviček je zobrazeno na obr. 2.1. Je vidět, že prakticky polovina políček se při vytváření IPv6 vynechala (modře zvýrazněné). Tři políčka si zachovala stejné názvy i význam (žlutě zvýrazněné), čtyři políčka mají stejný význam, ale změnily název (zeleně zvýrazněné). Pouze jediné již zmiňované pole Flow label (fialově zvýrazněné) bylo přidáno do hlavičky IPv6 [2].

2.2 IPv6 adresy

U IPv6 adres ubývá možnost broadcastu (všesměrových adres). Používá se buď unicast (směrová adresa), multicast (vícesměrová adresa) nebo anycast (výberová adresa). U anycastu se jedná o výběrové adresy označující skupinu rozhraní, kde by měl být paket doručen nejbližšímu členovi. Jde o loadbalancing (vyvažování zátěže), kde směrovač rozhoduje o výběru cesty [3]. Používá se např. u kořenových DNS (Domain Name System) serverů.

IPv6 adresy se liší oproti IPv4 také zápisem. IPv6 adresy jsou 128 bitové a využívá se hexadecimální zápis. Adresa je rozdělena do 8 částí po 16 bitech, každá část je oddělena dvojtečkou. Na rozdíl od IPv4 rozhraní obsahuje zpravidla více adres, musí mít adresu typu Link-local a poté 1 či více unicastových adres. Link-local adresy se používají pro komunikaci sousedních zařízení, využívají se i ve směrování jako next-hop. Je možná i konfigurace IPv6 adresy pomocí modified EUI-64 (adresa vytvořená z MAC adresy). Adresní prostor IPv4 je 2^{32}, IPv6 obsahuje celkem 2^{128} adres, což odpovídá pro představu 5.10^{28} adres na každého člověka na světě [3].



Obr. 2.1: Porovnání IPv4 a IPv6 hlaviček

Speciální IPv6 adresy:

- ::/0 (defaultní směr, odpovídá 0.0.0.0/0 u IPv4)
- ::1/128 (loopback adresa, odpovídá 127.0.0.1 u IPv4)
- ::/128 (nespecifikovaná adresa)
- FE80::/10 (Link-local unicastové adresy, odpovídá 169.254.x.x u IPv4)
- FF00::/8 (multicastové adresy)
- všechny ostatní adresy jsou globální unicastové

IPv6 multicastové adresy [7]:

- FF02::1 - adresa všech uzlů
- FF02::2 - adresa všech směrovačů
- FF02::9 - RIP (Routing Information Protocol) směrovače
- FF02::A - EIGRP (Enhanced Interior Gateway Routing Protocol) směrovače
- FF02::5 - OSPF (Open Shortest Path First) IGP (Internal Gateway Protocol)
- FF02::6 - OSPF IGP designated směrovače
- FF05::101 - NTP (Network Time Protocol) servery

2.3 Konfigurace IPv6 na Cisco směrovači

Konfigurace je velmi podobná IPv4, u většiny příkazů se zamění pouze `ipv6` za `ip`. Při konfiguraci směrovacího protokolu se již setkáváme s odlišnostmi, ale princip samozřejmě zůstává stejný jako při konfiguraci směrování s IPv4. Sítě u IPv6 směrovacích protokolů se přidávají oproti IPv4 přímo aktivací směrovacího protokolu na rozhraní, kromě MP-BGP (Multiprotocol Border Gateway Protocol). Také je třeba nastavit router-id (identifikace směrovače) ve formátu IPv4 adresy, pokud směrovač nemá na žádném rozhraní žádnou IPv4 adresu.

Podporované směrovací protokoly:

- RIPng
- OSPFv3
- EIGRPv6
- IS-IS (Intermediate System to Intermediate System)
- MP-BGP

Příklad nastavení IPv6 adresy na rozhraní:

- `ipv6 enable`
  aktivuje IPv6 na rozhraní, které dostane link-local adresu
- `ipv6 address 2001:1:2:3::1/64`
  pouze rozdíl `ipv6` oproti `ip`
- `ipv6 address 2001:1:2:3::/64 eui-64`
  vytvoření ipv6 adresy pomocí EUI-64
- `ipv6 address autoconfig`
  bezestavová konfigurace

Povolení IPv6 směrování:

- `ipv6 unicast-routing`
  povolí směrování IPv6 paketů

3 MOŽNOSTI PROPOJENÍ IPV4 A IPV6 SÍTÍ

Je těžké říci, kdy se zcela přejde na nový standart IPv6 (Internet Protocol version 6) a zda vůbec. Minimálně několik dalších let je nutné, aby IPv4 (Internet Protocol version 4) a IPv6 sítě byly schopny spolu komunikovat. Důvodů je hned několik, od nepodporování IPv6 na starších zařízeních, po postupnou možnost vybudování IPv6 infrastruktury, aby byl přechod co nejjednodušší. V současné době existuje mnoho řešení, základní 3 techniky [2], podle kterých se dá kategorizovat jsou:

- Dual-stack
- Překladové techniky
- Tunelování

3.1 Dual-stack

Síťové prvky mají nakonfigurované jak IPv4, tak IPv6 adresy. Používá se pouze jako dočasné řešení, protože využívá hodně výpočetního výkonu. V síťových prvcích jsou najednou vytvořeny 2 různé směrovací tabulky, popřípadě další instance směrovacích protokolů, atd. Nejen, že to vyžaduje více výpočetního výkonu, ale složitěji se odhalují chyby [3]. Příklad konfigurace:

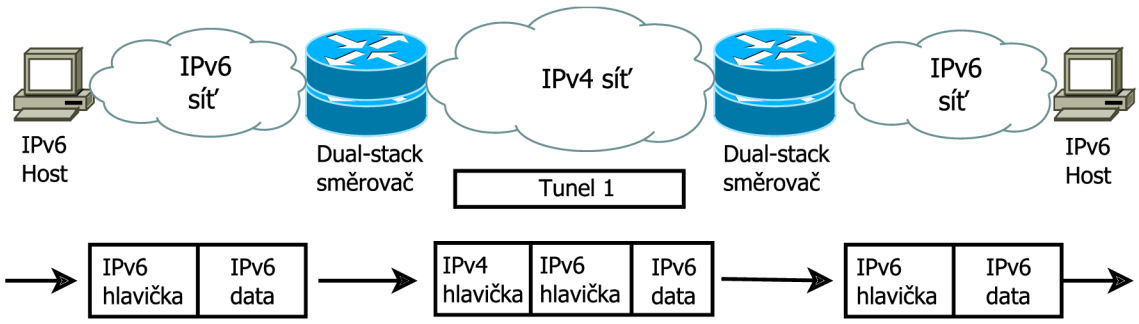
```
R1(config)# interface fa0/0
R1(config-if)# ip address 192.168.1.1 255.255.255.0
R1(config-if)# ipv6 address 2001:1:1:1::1/64
R1# show ip interface fa0/0
R1# show ipv6 interface fa0/0
```

3.2 Překladové techniky

Jedním z těchto mechanizmů je NAT64 [12], který je nástupce NAT-PT. NAT64 umožňuje komunikaci zařízení, která podporují jiné verze protokolů. NAT64 se implementuje mezi IPv6 a IPv4 sítí a je nutné správné nastavení mapování adres v závislosti na směru překladu. IPv4 adresy vzhledem k většímu adresnímu prostoru IPv6 jsou mapovány staticky bezstavově. Pro opačné mapování se používá dynamický stavový přístup, NAT (Network Address Translation) obsahuje dynamickou mapovací tabulku, jako IPv4 adresa je většinou použita adresa NAT zařízení a datové toky jsou odlišeny číslem portu. Často je použit také s DNS64 mechanizmem, který plní funkci mapování adres při provádění DNS (Domain Name System) služeb.

3.3 Tunelování

Izolované IPv6 sítě mohou být propojeny přes IPv4 infrastrukturu. Pouze hraniční zařízení musejí být dual-stack. Princip je takový, že IPv6 paket se zapouzdří do jiného protokolu, např. IPv4. Zapouzdření může provést nejen směrovač, ale i koncová stanice, pokud je určitý způsob tunelování podporovaný. Poté se paket přenese přes IPv4 síť a na hraničním zařízení se provede rozbalení IPv4 paketu na IPv6 a následuje doručení [2], viz obr. 3.1.



Obr. 3.1: Princip tunelování - zapouzdření IPv6 paketu do IPv4 a rozbalení

Techniky používané k sestavení tunelů:

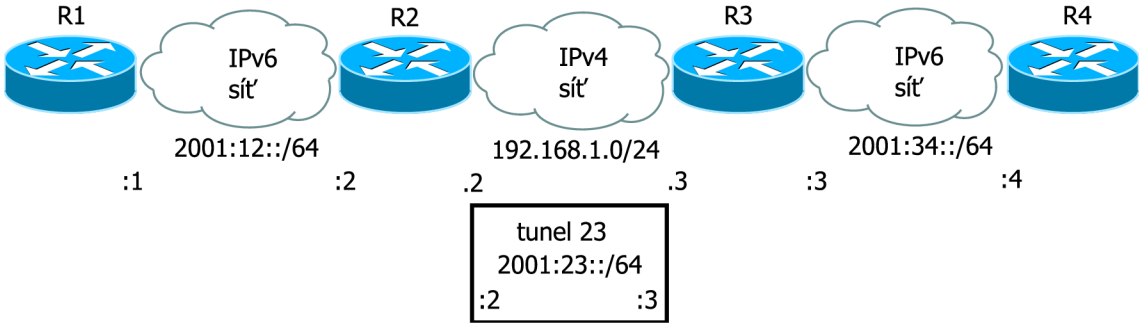
- Manuálně konfigurovatelné (Manuální tunel, GRE (Generic Routing Encapsulation) tunel)
- Polo-automatické (Tunnel broker)
- Automatické (6to4, 6rd)

3.3.1 Manuální tunel

Manuální tunel představuje permanentní linku mezi dvěmi IPv6 sítěmi, mezi kterými leží IPv4 síť. Využití je jako jednoduchý point-to-point (bod-bod) tunel, který může být použit jak v rámci lokality, tak mezi pobočkami. Hraniční směrovač nebo koncový bod na každé straně tunelu musí být dual-stack. Manuálně se nastavuje jak IPv6 adresa na rozhraní tunelu, tak IPv4 adresy zdroje tunelu a cíle tunelu. Může přenášet pouze IPv6 pakety. Můžeme použít i dynamické směrování přes tunel [3]. Příklad manuálního tunelu viz obr. 3.2 a konfigurace (bez směrování):

```
R2(config)# interface tunnel 23
R2(config-if)# ipv6 address 2001:23::2/64
R2(config-if)# tunnel source 192.168.1.2
R2(config-if)# tunnel destination 192.168.1.3
R2(config-if)# tunnel mode ipv6ip
```

```
R3(config)# interface tunnel 23
R3(config-if)# ipv6 address 2001:23::3/64
R3(config-if)# tunnel source 192.168.1.3
R3(config-if)# tunnel destination 192.168.1.2
R3(config-if)# tunnel mode ipv6ip
```



Obr. 3.2: Topologie s adresami použitými v příkladu konfigurace GRE a Manuálního tunelu

3.3.2 GRE tunel

GRE (Generic Routing Encapsulation) tunely byly vytvořeny firmou Cisco. GRE tunely jsou konfigurací velice podobné manuálním tunelům. Jejich využití je také velmi podobné manuálním, ale na rozdíl od manuálních podporují přenos více protokolů (obsahují v hlavičce pole Protocol Type). GRE je pouze zapouzdřovací protokol, ale často se používá ve spojení s IPsec (Internet Protocol security) protokolem, který zajišťuje bezpečnost přenosu [3]. Příklad GRE tunelu viz obr. 3.2 a konfigurace (bez směrování):

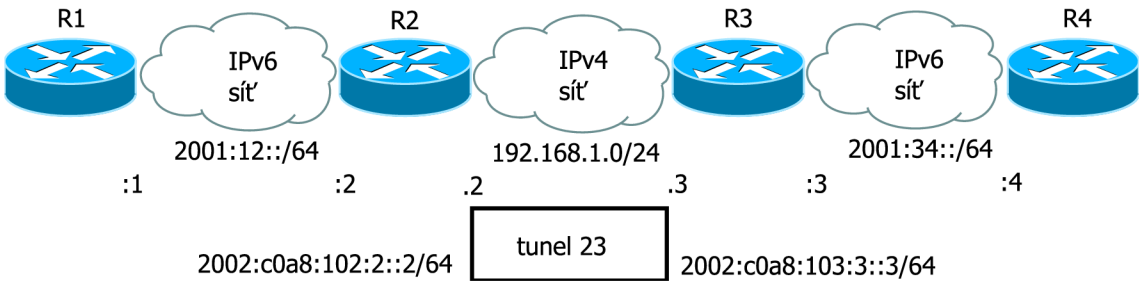
```
R2(config)# interface tunnel 23
R2(config-if)# ipv6 address 2001:23::2/64
R2(config-if)# tunnel source 192.168.1.2
R2(config-if)# tunnel destination 192.168.1.3
R2(config-if)# tunnel mode gre (ip, ipv6, multipoint)

R3(config)# interface tunnel 23
R3(config-if)# ipv6 address 2001:23::3/64
R3(config-if)# tunnel source 192.168.1.3
R3(config-if)# tunnel destination 192.168.1.2
R3(config-if)# tunnel mode gre (ip, ipv6, multipoint)
```

3.3.3 6to4 tunel

6to4 tunely jsou automatická tunelovací metoda, která se používá jako point-to-multipoint (bod-více bodů, v konfiguraci se nezadává koncový bod) oproti point-to-point (bod-bod) využití Manuálních a GRE tunelů. 6to4 tunel používá prefix 2002::/16, 32 bitů po prefixu /16 je reprezentováno IPv4 adresou hraničního směrovače, která je převedena do hexadecimálního tvaru. Tento prefix /48 je určený pro celý IPv6 ostrov. Dalších 16 bitů je k dispozici pro podsítě a dalších 64 bitů pro interface ID [2].

6to4 tunely se využívají k propojení více IPv6 sítí, kde každá z nich musí mít připojení do sdílené IPv4 sítě (třeba Internet). Hlavní požadavek je mít veřejnou IPv4 adresu, z které se vytvoří již zmíněný /48 prefix. Princip tunelu je takový, že když směrovač obdrží adresu z rozsahu 2002::/16, tak využije tunel. Z IPv6 adresy převede z prefixu /16 - /48 IPv4 adresu, kterou použije jako next-hop. Poté, co se přenese paket po IPv4 síti se opět sestaví do IPv6 a odešle se do cíle [3]. Příklad 6to4 tunelu viz obr. 3.3 a konfigurace (bez směrování):

```
(192.168.1.2 hexadecimálně = c0a8:102)
(192.168.1.3 hexadecimálně = c0a8:103)

R2(config)# interface tunnel 23
R2(config-if)# ipv6 address 2002:c0a8:102:2::2/64
R2(config-if)# tunnel source 192.168.1.2
R2(config-if)# tunnel mode ipv6ip 6to4

R3(config)# interface tunnel 23
R3(config-if)# ipv6 address 2002:c0a8:103:3::3/64
R3(config-if)# tunnel source 192.168.1.3
R3(config-if)# tunnel mode ipv6ip 6to4
```

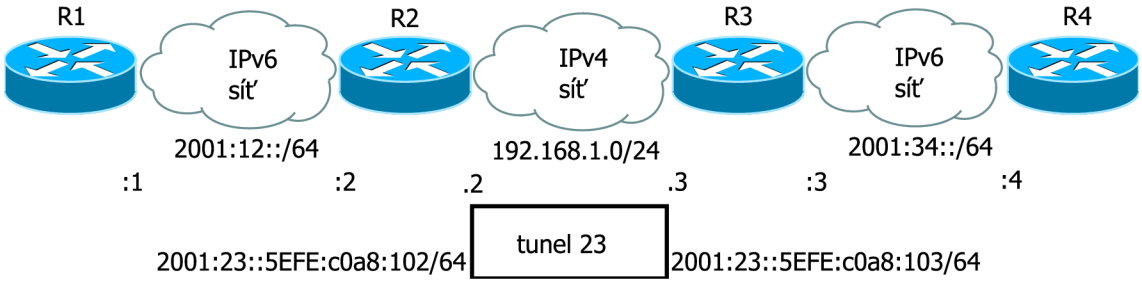


Obr. 3.3: 6to4 tunel - topologie s adresami použitými v příkladu konfigurace

3.3.4 ISATAP tunel

ISATAP (Intra-Site Automatic Tunnel Addressing Protocol) tunel je podobný 6to4 tunelu. Používá se opět k propojení IPv6 sítí přes IPv4 síť a IPv6 adresa je tvořená z IPv4 adresy. Oproti 6to4 tunelu, který je využíván typicky pro propojení poboček, je ISATAP tunel využíván k propojení IPv6 sítí v rámci lokality (v názvu má také Intra-Site). ISATAP tunely používají IPv6 adresu skládající se z jakéhokoli prefixu /64 následovaným interface ID vytvořeným EUI-64 mechanizmem. Interface ID se skládá z 32 bitů (0000:5EFE) a 32 bitů, které jsou vytvořeny převodem IPv4 adresy (zdroj tunelu) do hexadecimálního tvaru [8]. Příklad ISATAP tunelu viz obr. 3.4 a konfigurace (bez směrování):

```
(192.168.1.2 hexadecimálně = c0a8:102)
(192.168.1.3 hexadecimálně = c0a8:103)

R2(config)# interface tunnel 23
R2(config-if)# ipv6 address 2001:23::/64 eui-64
R2(config-if)# tunnel source 192.168.1.2
R2(config-if)# tunnel mode ipv6ip isatap

R3(config)# interface tunnel 23
R3(config-if)# ipv6 address 2001:23::/64 eui-64
R3(config-if)# tunnel source 192.168.1.3
R3(config-if)# tunnel mode ipv6ip isatap
```



Obr. 3.4: ISATAP tunel - topologie s adresami použitými v příkladu konfigurace

4 BORDER GATEWAY PROTOCOL

BGP (Border Gateway Protocol) se používá pro směrování mezi AS (Autonomous System), v současné době jako jediný EGP (External Gateway Protocol). Jako jediný směrovací protokol také používá TCP (Transmission Control Protocol). EIGRP (Enhanced Interior Gateway Routing Protocol) a OSPF (Open Shortest Path First) používají přímo IP (Internet Protocol), RIP (Routing Information Protocol) používá UDP (User Datagram Protocol). Garantuje loop-free (bez smyček) výměnu směrovacích informací [9]. MP-BGP (Multiprotocol Border Gateway Protocol) dovoluje přenášet informace o jiných protokolech než IPv4, např. IPv6 nebo MPLS (Multiprotocol Label Switching).

4.1 Porovnání EGP s IGP

BGP je EGP (External Gateway Protocol) oproti ostatním směrovacím IGP (Internal Gateway Protocol) a také pracuje na jiném principu. BGP je path vector směrovací protokol, což znamená, že si nevybírá cestu jen na základě „nejlepší“ cesty, ale je policy-based, směrovací rozhodnutí dělá na základě použití BGP atributů. BGP sousedé si posílají „všechny“ BGP atributy u každého záznamu [8]. Podrobnější porovnání IGP s EGP viz tab. 4.1 .

Tab. 4.1: Porovnání IGP s EGP protokoly podle typu a metriky

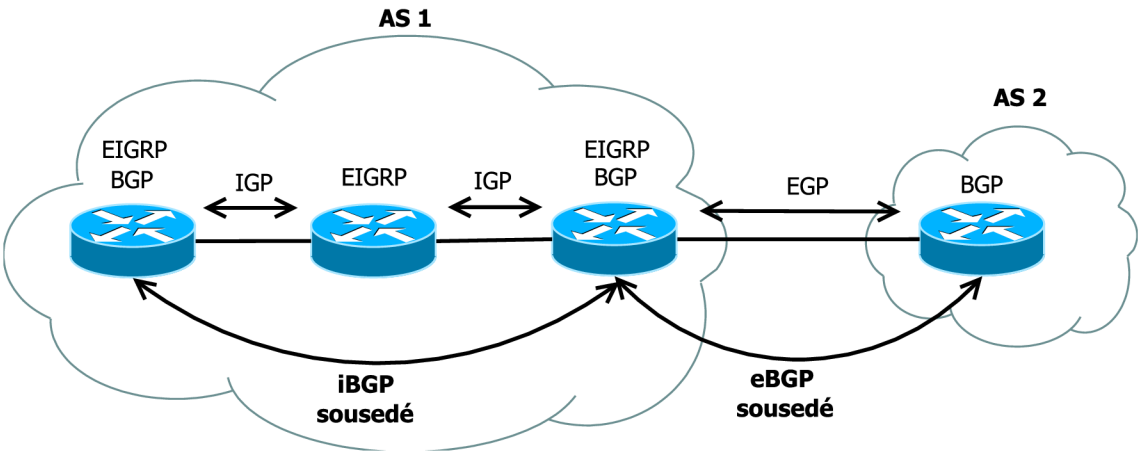
Protokol	**IGP/EGP**	**Typ**	**Metrika**
RIP	IGP	Distance vector	Hop count
OSPF	IGP	Link state	Cost
EIGRP	IGP	Advanced distance vector	Composite
IS-IS	IGP	Link state	Metric
BGP	EGP	Path vector	Attributes

4.2 Porovnání iBGP s eBGP

Každý směrovač, který používá BGP je označován jako BGP speaker, pokud 2 směrovače podporující BGP ustanoví TCP spojení, jsou BGP neighbors (sousedé). Jestli jsou 2 sousedé v rámci jednoho AS, jejich spojení nazýváme iBGP (internal Border Gateway Protocol), pokud ne, jde o eBGP (external Border Gateway Protocol) viz obr. 4.1. Rozdíl je v tom, že pokud obdrží směrovač cestu od iBGP souseda naučenou v rámci jeho AS, nepošle o tom informace dalšímu sousedovi a next-hop (další skok) se implicitně nemění. Tímto se docílí loop-free (bez smyček) topologie [2].

Stavy mezi BGP sousedy:

- Idle - jakmile je příkaz `neighbor` nakonfigurovaný
- Connect - směrovač zná směr k sousedovi a dokončil three-way handshake
- Open sent - zpráva Open byla poslána spolu s parametry BGP session (spojení)
- Open confirm - směrovač obdržel souhlas s parametry spojení
- Established - sousedství navázáno, může začít výměna směrovacích informací
- Ověření stavu - `Router#show ip bgp neighbors`



Obr. 4.1: Porovnání BGP sousedství iBGP s eBGP

4.3 Autonomní systém

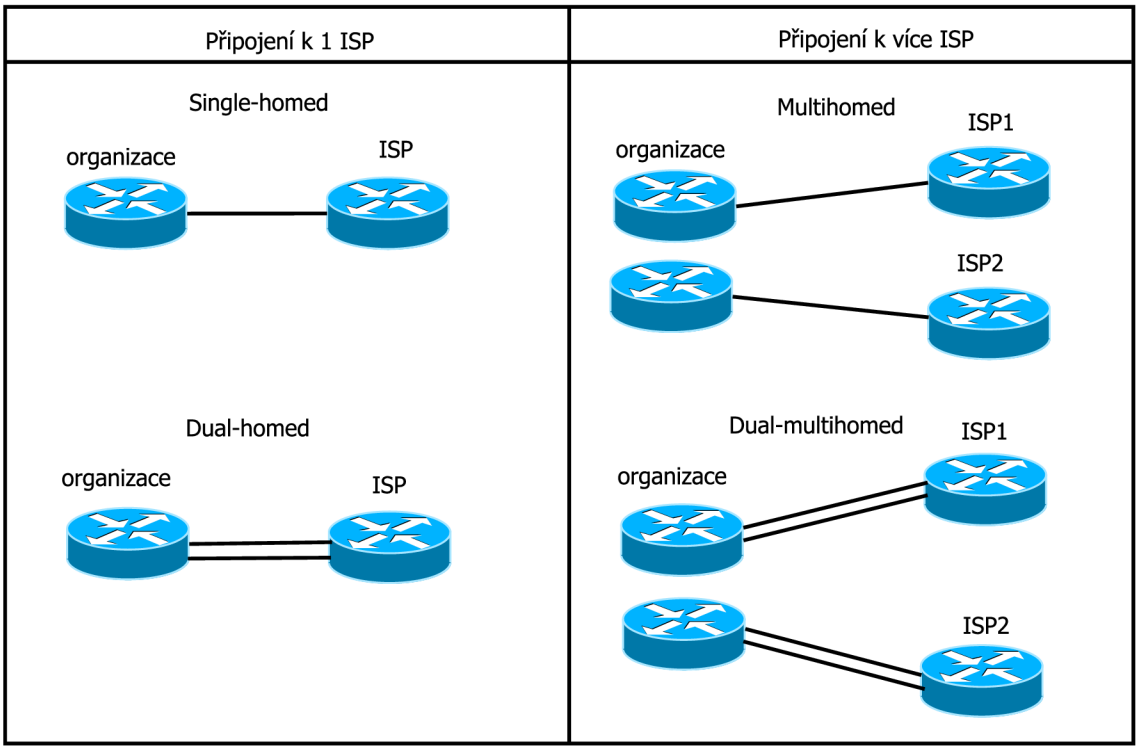
AS (Autonomous System) je skupina směrovačů, která sdílí směrovací politiky a patří pod jednu administrativní doménu. Většinou patří jedné organizaci. V AS může být použito více IGP, ale vnějšímu světu bude celý AS vnímán jako jedna entita. Pokud je AS připojen do Internetu, musí mít svoje unikátní číslo. Pokud má AS jenom jednoho poskytovatele Internetu, je vyžadováno použít privátní rozsah AS (podobné privátnímu rozsahu v IPv4) [10]. Organizace IANA (Internet Assigned Numbers Authority) je zodpovědná za rozdělování AS v rámci celého světa skrz 5 neziskových organizací rozdělených geograficky [11].

Číslování AS:

- 2B čísla (0-65535), rozsah 64512 - 65535 je určen pro privátní AS
- 4B čísla (65536-4294967296), zavedena kvůli nedostatku 2B čísel, zápis možný ve tvaru 2B.2B

Při návrhu připojení AS k ISP (Internet Service Provider) je potřeba brát v potaz možné výpadky a problémy, jak na naší straně, tak na straně ISP. Proto je důležité

promyslet redundanci v závislosti na důležitosti konektivity a financích viz obr. 4.2. Je také důležité promyslet, zda je nutné mít svůj vlastní AS nebo postačí výchozí směr k ISP.



Obr. 4.2: Možnosti připojení k poskytovateli Internetu (ISP)

4.4 Atributy cesty

Atributy cesty nesou informace o daném směru, podle kterých se vybírá nejlepší cesta. Nějaké atributy jsou povinné a automaticky posílány, jiné jsou nepovinné s možností konfigurace viz tab. 4.2. Pomocí atributů lze měnit chování BGP. Atributy [9] jsou přenášeny pomocí BGP update zprávy.

Základní dělení atributů:

- Well-known Mandatory - povinně podporovaný atribut, povinně posílaný
- Well-known Discretionary - povinně podporovaný atribut, nepovinně posílaný
- Optional Transitive - nepovinně podporovaný atribut, povinnost i bez podpory přeposlat
- Optional Nontransitive - nepovinně podporovaný atribut, nesmí se bez podpory přeposlat

Tab. 4.2: Rozdělení atributů do základních skupin

Atribut	Skupina v eBGP	Skupina v iBGP
AS_PATH	Well-known Mandatory	Well-known Mandatory
NEXT_HOP	Well-known Mandatory	Well-known Mandatory
ORIGIN	Well-known Mandatory	Well-known Mandatory
LOCAL_PREF	zakázáno	Well-known Discretionary
ATOMIC_AGGREGATE	Well-known Discretionary	Well-known Discretionary
AGGREGATOR	Optional Transitive	Optional Transitive
COMMUNITY	Optional Transitive	Optional Transitive
MULTI_EXIT_DISC	Optional Nontransitive	Optional Nontransitive

AS_PATH
Obsahuje list AS, přes které je třeba projít pro dosáhnutí dané cesty. Kdykoli prochází update cesty přes další AS, přidá číslo AS na začátek listu s atributy.

NEXT_HOP
Udává IP adresu, která je dalším „hopem“ k dané cestě. IP adresa nevyjadřuje běžný next hop, ale IP adresu hraničního směrovače v dalším AS, takže v rámci jednoho AS se nebude měnit. Pokud směrovač nezná cestu k next hopu, nelze vložit směr do směrovací tabulky.

ORIGIN
Označuje původ cesty. Nabízí 3 možnosti původu cesty. IGP (v BGP tabulce uvedeno „i“) - původ v současném AS. EGP (v BGP tabulce uvedeno „e“) - směr naučen od EGP (historický protokol). Incomplete (v BGP tabulce uvedeno „?“) - směr naučen z redistribuce.

LOCAL_PREF
Označuje preferenci cesty k danému směru. Přenáší se pouze v rámci iBGP, větší hodnota je preferována (implicitně 100).

ATOMIC_AGGREGATE, AGGREGATOR a COMMUNITY
ATOMIC_AGGREGATE je nastaven buď na true nebo false, true značí informaci o agregaci více směrů do 1. AGGREGATOR udává kdo je zdrojem informace o agregaci. COMMUNITY atribut může být použit pro filtraci směrů. BGP směrovače označkují směr a umožní dělat rozhodnutí v závislosti na značce.

MED (MULTI_EXIT_DISC)
Udává hodnotu, která patří pro sousední AS a označuje preferovanou cestu do našeho AS. Menší číslo je preferované.

4.5 Základní konfigurace BGP

`Router(config)#router bgp` *`autonomous_system`*
Konfigurace v jakém AS se směrovač nachází. Maximálně 1 instance.

`Router(config-router)#neighbor` *`ip-address | peer-group-name`* `remote-as` *`autonomous_system`*
Konfigurace souseda. Nutnost sousedovy IP adresy, aby byla ve směrovací tabulce (nestačí výchozí směr). `Remote-as` určuje v jakém AS se soused nachází.

`Router(config-router)#neighbor` *`ip-address | peer-group-name`*
`update-source` *`interface-type interface-number`*
`Update-source` se používá, pokud chceme nastavit jako zdrojovou IP adresu adresu určitého rozhraní (nejčastěji loopback). Používá se při redundantním propojení, když chceme, aby výpadek jedné linky nezpůsobil rozpad sousedství.

`Router(config-router)#network` *`network-number[mask netmask]`*
BGP přidá síť do seznamu, který je posílán sousedům.

`Router#clear ip bgp` *`{* | AS | neighbor address | peer-group-nape}`*
`[out | soft | in]`
Resetování sousedství. Existují možnosti resetovat pouze jednoho souseda, soft reset (šetrnější) a směr (in, out), ve kterém chceme reset provést.

Odlišnosti v MP-BGP:
`Router(config-router)#bgp router-id` *`ip-address`*
Nutnost zadání router id, pokud nemá směrovač nikde IPv4 adresu.

`Router(config-router)#address-family ipv6 [unicast | multicast | vpnv6]`
Specifikace IPv6 adresní rodiny a vložení konfiguračního módu.

`Router(config-router-af)#neighbor` *`ipv6-address`* `activate`
Aktivování sousedství pro výměnu prefixů pro IPv6 adresní rodinu s lokálním směrovačem.

5 ENHANCED INTERIOR GATEWAY ROUTING PROTOCOL

EIGRP (Enhanced Interior Gateway Routing Protocol) [2] je Distance-Vector směrovací protokol. Využívá DUAL (Diffusing Update ALgorithm) algoritmus pro výpočet nejlepší cesty. Je to classless (beztřídní) protokol podporující VLSM (Variable Length Subnet Mask). Podporuje IPv4, IPv6, IPX (Internetwork Packet Exchang) a AppleTalk. Používá transportní protokol RTP (Reliable Transport Protocol), který zajišťuje spolehlivý přenos dat. Administrativní vzdálenost je pro interní EIGRP cesty 90, pro externí 170.

5.1 Principy a funkčnost EIGRP

Základní termíny

- Successor - nejlepší cesta (next-hop) k cíli, může jich být více
- Feasible successor - záložní cesta (next-hop) k cíli, může jich být více, nalezneme v tabulce topologie
- Reported distance - aktuální vzdálenost od souseda k cíli, kterou nám posílá
- Feasible distance - hodnota Reported distance, kterou nám zašle soused + cesta k sousedovi
- Feasibility condition - ověření, že nikde nemůže nastat smyčka, použití při volbě S a FS (pokud je RD menší než FD, nikde nemůže být smyčka)

Metrika

Jedná se o kompozitní metriku skládající se ze 4 částí, implicitně jsou aktivovány jen Bandwidth (šířka pásma) a Delay (zpoždění). Pokud jsou stejné hodnoty metriky, je preferována cesta s největším MTU (Maximum Transmission Unit) [8]. Parametry metriky:

- Bandwidth (šířka pásma) - statický parametr
- Delay (zpoždění) - statický parametr
- Reliability (spolehlivost) - dynamický parametr
- Load (zatížení) - dynamický parametr

Zprávy v EIGRP

- Hello - Objevování EIGRP sousedů, posílá se každých 5 sekund na rychlých rozhraních a 60 sekund na pomalejších jak 1544 kbps.

- Acknowledgement (ACK) - Potvrzování komunikace na zprávy Update, Query a Reply. Unicastově posílané a principielně stejné jak Hello pakety, ale s prázdným tělem (pouze číslo potvrzení).
- Query - Multicastově posílané, potvrzovaná komunikace. Hledání nejlepší cesty do cíle (spouští se nebo šíří difúzní výpočet).
- Reply - Unicastově posílané, potvrzovaná komunikace. Odpověď na Query.
- Update - Multicastově nebo unicastově posílané, potvrzovaná komunikace. Přenášejí směrovací informace a mohou spustit difúzní výpočet.

Tabulky

- Route (směrovací tabulka) - nejlepší záznam ke každé cestě
- Neighbor (tabulka sousedsví) - informace o sousedních směrovačích
- Topology (topologická tabulka) - všechny cesty do všech cest (stav, FD a RD)

5.2 Základní konfigurace

- vytvoří EIGRP IPv6 směrovací proces
  `R1(config)#router eigrp` *`autonomous-system-number`*
- vypne automatické nastavení classful (třídní) masky
  `R1(config-router)#no auto-summary`
- přidání sítě do EIGRP
  `R1(config-router)#network` *`network-number`* `[wildcard-mask]`

Odlišnosti EIGRP pro IPv6 a IPv4

Je třeba zadat router-id ve tvaru IPv4 adresy, pokud směrovač nemá žádnou IPv4 adresu. Doporučuje se příkaz `no shutdown` v instanci EIGRP. EIGRP sítě se přidávají tak, že se EIGRP instance aktivuje přímo na rozhraní. Je také nutno povolit IPv6 směrování [3]. Příklad konfigurace:

```
R1(config)#ipv6 unicast-routing
R1(config)#ipv6 router eigrp 100
R1(config-router)#router-id 1.1.1.1
R1(config-router)#no shutdown
R1(config)#interface loopback0
R1(config-if)#ipv6 eigrp 100
```

6 IPSEC VPN

VPN (Virtual Private Network) [2] se používá k vzdálenému připojení do LAN (Local Area Network). Většinou se jedná o připojení přes Internet do LAN pobočky společnosti a jelikož Internet není bezpečná síť a je možné naše zprávy odchytit nebo změnit, je třeba implementovat zabezpečení. IPsec (Internet Protocol security) je skupina protokolů pro zabezpečení IP komunikace. VPN se rozlišuje na 2 základní typy :

1. **Site-to-site VPN**
   - Většinou propojení dvou poboček společnosti. VPN řeší pouze hraniční zařízení (směrovač, firewall) a uživatelé nepotřebují žádného klienta.
2. **Remote Access VPN**
   - Připojení jednotlivých uživatelů do vzdálené LAN sítě. Každý uživatel musí mít softwarového VPN klienta (např. Cisco AnyConnect VPN client) nebo se využívá i webový prohlížeč a SSL (Secure Sockets Layer) VPN.

6.1 Internet Protocol security

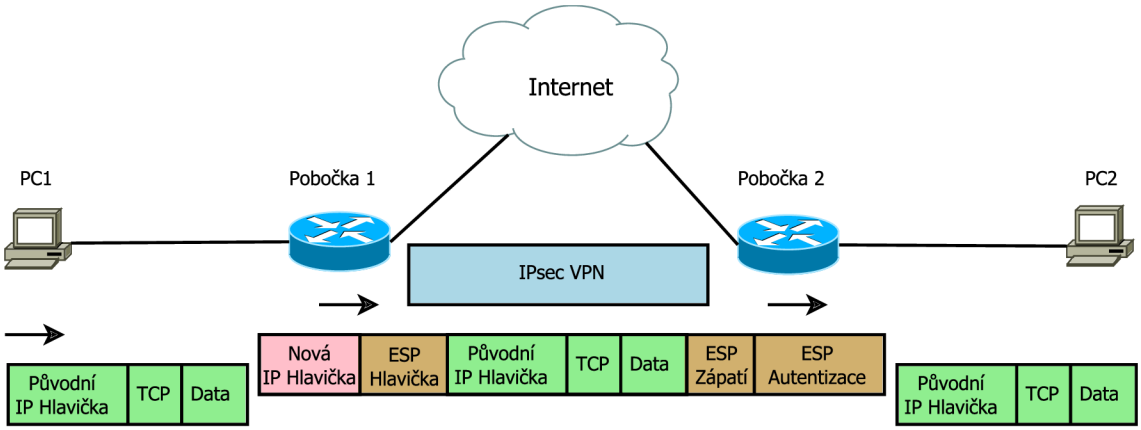
IPsec (Internet Protocol security) je skupina protokolů sloužící pro autentizaci, důvěrnost a integritu komunikace pracující na 3. vrstvě ISO/OSI modelu [3].

IPsec podporuje dva způsoby šifrování:

- Transportní mód - V transportním módu jsou pouze data zašifrována. Hlavička zůstává původní a nešifrovaná.
- Tunelovací mód - V tunelovacím módu je celý paket zašifrován a zabalen do nového paketu s novou IP hlavičkou. Není možné zjistit IP adresu koncového zařízení, tunelovací mód je použit mezi hraničními zařízeními. Příklad zapouzdření a rozbalení IP paketu viz obr. 6.1.

Základní protokoly IPsec:

- Authentication Header (AH) - AH zajišťuje integritu a autentizaci. Neposkytuje šifrování.
- Encapsulating Security Payload (ESP) - ESP zajišťuje integritu, autentizaci a oproti AH i důvěrnost díky šifrování. Lze využít také pouze šifrování nebo pouze autentizaci.



Obr. 6.1: Zapouzdření a rozbalení IP paketu při použití IPsec tunelovacího módu s protokolem ESP (site-to-site VPN)

- Security Association (SA) - SA využívá více protokolů dohromady k zajištění bezpečné komunikace. Bezpečná asociace je sestavena pomocí ISAKMP (Internet Security Association and Key Management Protocol) společně s IKE (Internet Key Exchange), kde je dohodnuto šifrování a autentizace.

6.2 IPsec VPN konfigurace

Při konfiguraci IPsec VPN je třeba postupně aplikovat [8]:

1. **ISAKMP (Internet Security Association and Key Management Protocol) politiky**
   - Obsahuje autentizaci (např. pre-share key) a šifrování (např. aes, 3des) jako inicializaci prvních bezpečnostních detailů.
2. **IPsec detaily**
   - Obsahuje detaily šifrování pomocí IPsec (definujeme ipsec transform-set).
3. **Crypto ACL**
   - Je to ACL (Access list) definující provoz, na který budou aplikovány bezpečnostní prvky. `Deny` parametr znamená poslání provozu ve formě čistého textu.
4. **VPN tunel informace**
   - Spojí všechny informace o tunelu dohromady. Nastavení transform-setu, peera a crypto ACL.
5. **Aplikování Crypto mapy**
   - Aplikuje se Crypto mapa vytvořená v minulém kroku přímo na rozhraní.

6.3 Příklad konfigurace IPsec VPN

1. **ISAKMP politiky**
   - `R1(config)# crypto isakmp policy 1`
   - `R1(config-isakmp)# encryption aes`
   - `R1(config-isakmp)# authentication pre-share`
   - `R1(config-isakmp)# group 1`
   - `R1(config)# crypto isakmp key key123 address 213.111.222.121`
2. **IPsec detaily**
   - `R1(config)# crypto ipsec transform-set set1 esp-aes esp-sha-hmac`
3. **Crypto ACL**
   - `R1(config)# access-list 120 permit ip 192.168.1.0 0.0.0.255 10.0.0.0 0.255.255.255`
4. **VPN tunel informace**
   - `R1(config)# crypto map map1 20 ipsec-isakmp`
   - `R1(config-crypto-map)# set transform-set set1`
   - `R1(config-crypto-map)# set peer 213.111.222.121`
   - `R1(config-crypto-map)# match address 120`
5. **Aplikování Crypto mapy**
   - `R1(config)# interface f0/1`
   - `R1(config-if)# crypto map map1`

Ověření:

1. **Detaily crypto mapy**
   - `R1# show crypto map`
2. **Zobrazení crypto spojení**
   - `R1# show crypto session`
3. **Nastavení SA (Security Association)**
   - `R1# show crypto ipsec sa`
4. **Zobrazení IPsec událostí**
   - `R1# debug crypto ipsec`

6.4 Virtual Tunnel Interface

IPsec VTI (Virtual Tunnel Interface) [13] poskytuje směrovatelné rozhraní pro IPsec tunel. To zjednoduší aplikaci NAT (Network Address Translation), ACL (Access Control List) a QoS (Quality of Service), což můžeme aplikovat podle rozhraní buď ve formě otevřeného textu, šifrovaného textu nebo obojí.

Konfigurace IPsec VPN s využitím VTI přináší určité výhody jako možnost přenášet dynamické směrování a multicast. Směrujeme šifrované zprávy přes VTI, nešifrované přes fyzické rozhraní a na každý provoz na každém rozhraní lze aplikovat vlastní politiky (QoS, ACL).

Existují 2 typy VTI rozhraní:

- Statické VTI - Slouží pro site-to-site připojení. Výhoda je v možnosti využití dynamického směrovacího protokolu bez nutnosti použití GRE (navíc 4 bytes pro GRE hlavičku). Navíc mohou být určité nastavení aplikovatelná přímo na rozhraní, což zlepšuje kontrolu a přehlednost.
- Dynamické VTI - Využívané pro remote-access VPN. Tunely zajišťují oddělené virtuální přístupové rozhraní pro každé VPN spojení na vyžádání. Lze využít opět ACL a QoS.

6.4.1 VTI pro Site-to-Site IPsec VPN

Při konfiguraci IPv6 IPsec VPN s využitím VTI je třeba postupně aplikovat [13]:

1. **IKE (Internet Key Exchange) politiky a předsdílený klíč v IPv6**
   - Obsahuje autentizaci a šifrování jako inicializaci prvních bezpečnostních detailů.
2. **IPsec transform set a IPsec profil**
   - Transform set je kombinace bezpečnostních protokolů a algoritmů přijatelných pro IPsec směrovače.
3. **ISAKMP profil v IPv6 (nepovinné)**
   - ISAKMP profil umožňuje modularitu ISAKMP konfigurace pro první fázi vyjednávání, např. mapování různých ISAKMP parametrů na různé IPsec tunely.
4. **IPv6 IPsec VTI**
   - Konfigurace IPv6 IPsec VTI, což zahrnuje adresu tunelu a povolení IPv6 na rozhraní. Dále je třeba nastavit zdroj, cíl tunelu, mód tunelu a IPsec profil.

6.4.2 Příklad konfigurace

Příklad konfigurace VTI pro Site-to-Site IPv6 IPsec VPN:

1. **IKE politiky a předsdílený klíč v IPv6**
   - `R1(config)# crypto isakmp policy 1`
   - `R1(config-isakmp)# encryption aes`
   - `R1(config-isakmp)# authentication pre-share`
   - `R1(config-isakmp)# group 1`
   - `R1(config)# crypto isakmp key 0 key123 address ipv6 2001:1:1:1::1/64`
2. **IPsec transform set a IPsec profil**
   - `R1(config)# crypto ipsec transform-set mipsec_transf esp-aes esp-sha-hmac`
   - `R1(config)# crypto ipsec profile ipsec_prof`
   - `R1(config-crypto-transform)# set-transform-set ipsec_transf`
3. **ISAKMP profil v IPv6 (nepovinné)**
   - `R1(config)# crypto isakmp profile isakmp_prof`
   - `R1(config-isakmp-profile)# self-identity address ipv6`
   - `R1(config-isakmp-profile)# match identity address ipv6 2001:13:13:13::3/64`
4. **IPv6 IPsec VTI**
   - `Router(config)# ipv6 unicast-routing`
   - `Router(config)# interface tunnel 13`
   - `Router(config-if)# ipv6 address 13:13:13:13::1/64`
   - `Router(config-if)# ipv6 enable`
   - `Router(config-if)# tunnel source 2001:13:13:13::1`
   - `Router(config-if)# tunnel destination 2001:13:13:13::3`
   - `Router(config-if)# tunnel mode ipsec ipv6`
   - `Router(config-if)# tunnel protection ipsec profile ipsec_prof`

7 ZONE-BASED POLICY FIREWALL

Existuje více možností firewallu, jedním z nich je CBAC (Context-Based Access Control), který je Cisco IOS firewall stateful inspection (inspekční stavový). Je to model, kde jsou inspekční politiky aplikovány na rozhraní. Na všechen provoz, který projde rozhraním, jsou aplikovány stejné politiky. Tento model se stává díky tomuto principu velmi omezený, zvláště pokud na zařízení je více rozhraní, na které chceme aplikovat různá pravidla.

ZBF (Zone-Based Policy Firewall) [14] mění zastaralejší model u CBAC na mnohem více flexibilní a lépe pochopitelný. Jeho hlavním principem jsou zóny, které jsou aplikovány na rozhraní. Inspekční politiky jsou aplikovány na provoz mezi zónami.

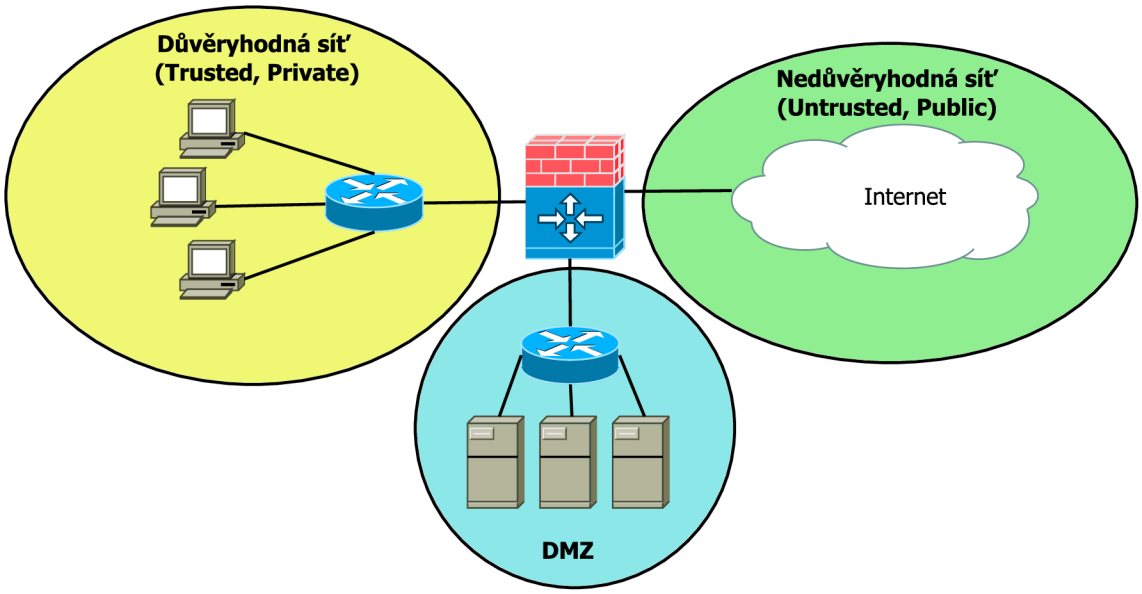
7.1 Pravidla pro aplikaci ZBF

- Zóna musí být nakonfigurována předtím, než je přiřazena na rozhraní.
- Na rozhraní může být přiřazena pouze jedna bezpečnostní zóna.
- Když je na rozhraní přiřazena zóna, tak je implicitně veškerý provoz z a na rozhraní blokován kromě provozu z a na rozhraní se stejnou zónou.
- Self zone (vlastní zóna) je jediná výjimka výchozí politiky zakazovat veškerý provoz. Všechen provoz je povolen, pokud není dodatečně zakázán.
- Mezi dvěma zónami může být nakonfigurováno pass (projít), inspect (prohlédnout) a drop (zahodit).
- Pokud provoz prochází přes více rozhraní na směrovači, všechny rozhraní musí být členem nějaké zóny.

7.2 Návrh zabezpečení sítě pomocí ZBF

Je důležité si rozmyslet, jak navrhnout zóny podle potřebného zabezpečení, aby na každé rozhraní byla aplikována zóna s odpovídající úrovní ochrany. Klasický případ aplikování zón na rozhraní podle potřeby ochrany viz obr. 7.1 a cíle ochrany [2] podle účelu:

- **Rozhraní připojené k veřejné nedůvěryhodné síti (untrusted)** - Klasicky připojení do Internetu. Většinou je třeba přistupovat pouze k DMZ (Demilitarized Zone) zařízením (zařízení v demilitarizované zóně). Také je obvykle zbytečné, aby zařízení připojené přes toto rozhraní měli konektivitu k privátní zóně a mohli ji teoreticky ohrozit.



Obr. 7.1: Návrh rozdělení sítě na části podle požadavků ochrany pro vytvoření a aplikaci zón v ZBF

- **Rozhraní připojené k privátní důvěryhodné síti (trusted)** - Zařízení, která jsou připojena přes toto rozhraní jsou např. počítače v lokální síti jedné pobočky. Pokud se jedná o větší množství zařízení (velká společnost), tak se používá ještě dělení zón na základě oddělení nebo práv zaměstnanců. V této situaci je přístup většinou povolen jak do DMZ zóny, tak do nedůvěryhodné zóny.
- **Rozhraní připojené k zařízením v demilitarizované zóně (DMZ)** - DMZ se využívá kvůli bezpečnosti a je oddělena od všech ostatních zařízení, protože jsou v ní umístěné služby (e-mail, web, DNS) pro dostupnost i z Internetu. Obvyklé nastavení pro DMZ bývá takové, že přístup k jejím zdrojům jak už bylo řečeno je možný ze všech zón, ale veškerá konektivita původem z DMZ je blokována. Je to blokované z toho důvodu, že do DMZ je přístup i z nedůvěryhodné sítě a pokud by došlo k nějaké kompromitaci, tak zařízení z DMZ nebudou využitelné k žádnému útoku na privátní ani veřejnou zónu.

7.3 ZBF - postup konfigurace

Tento postup konfigurace může být použit při konfiguraci ZBF. Aplikace přesně podle pořadí není nutná, ale některé kroky musejí být učiněny dříve než ostatní (např. dříve je nutno vytvořit zónu, než ji aplikujeme na rozhraní). Konfigurace ZBF se skládá z několika částí [14]:

1. **Vytvoření zón**
   - Vytvoření zón a možný popis (description) zón.
2. **Konfigurace class-map (mapa třídy)**
   - Klasifikace provozu, který chceme podrobovat inspekci, lze použít podmínky OR (nebo), AND (a zároveň) nebo NOT (kromě toho) mezi určitými typy provozu.
3. **Konfigurace policy-map (mapa politik)**
   - Vytvoření map politik pro aplikace nějaké akce pro provoz definovaný v mapě třídy, lze použít pass (projít), drop (zahodit), inspect (prohlédnout), log (zaznamenat), reset.
4. **Definování párů zón**
   - Konfigurace páru zón ve směru inside (dovnitř) a outside (ven).
5. **Aplikace map politik na páry zón**
   - Dříve nadefinované mapy politik jsou aplikovány na páry zón.
6. **Aplikace zón na rozhraní**
   - Aplikujeme vytvořené zóny na rozhraní.

7.4 Příklad konfigurace

1. **Vytvoření zón**
   - `R1(config)#zone security INSIDE`
   - `R1(config)#zone security OUTSIDE`
2. **Konfigurace class-map (mapa třídy)**
   - `R1(config)#class-map type inspect match-any IN-TO-OUT-CLASS`
   - `R1(config-cmap)#match protocol icmp`
3. **Konfigurace policy-map (mapa politik)**
   - `R1(config)#Policy-map type inspect IN-TO-OUT-POLICY`
   - `R1(config-pmap)#Class type inspect IN-TO-OUT-CLASS`
   - `R1(config-pmap-c)#Inspect`
4. **Definování párů zón**
   - `R1(config)#Zone-pair security IN-TO-OUT source INSIDE destination OUTSIDE`
5. **Aplikace map politik na páry zón**
   - `R1(config)#Zone-pair security IN-TO-OUT source INSIDE destination OUTSIDE`
   - `R1(config-sec-zone-pair)#service-policy type inspect IN-TO-OUT-POLICY`

6. **Aplikace zón na rozhraní**
    - `R1(config)#interface fastethernet 0/0`
    - `R1(config-if)#zone-member security OUTSIDE`
    - `R1(config)#interface fastethernet 1/0`
    - `R1(config-if)#zone-member security INSIDE`

Ověření:

- Ověření zón - jejich popis a rozhraní, na jaké jsou aplikované

  `R1#show zone security`

- Ověření párů zón - zdrojová zóna a cílová zóna, politiky aplikované na páry zón

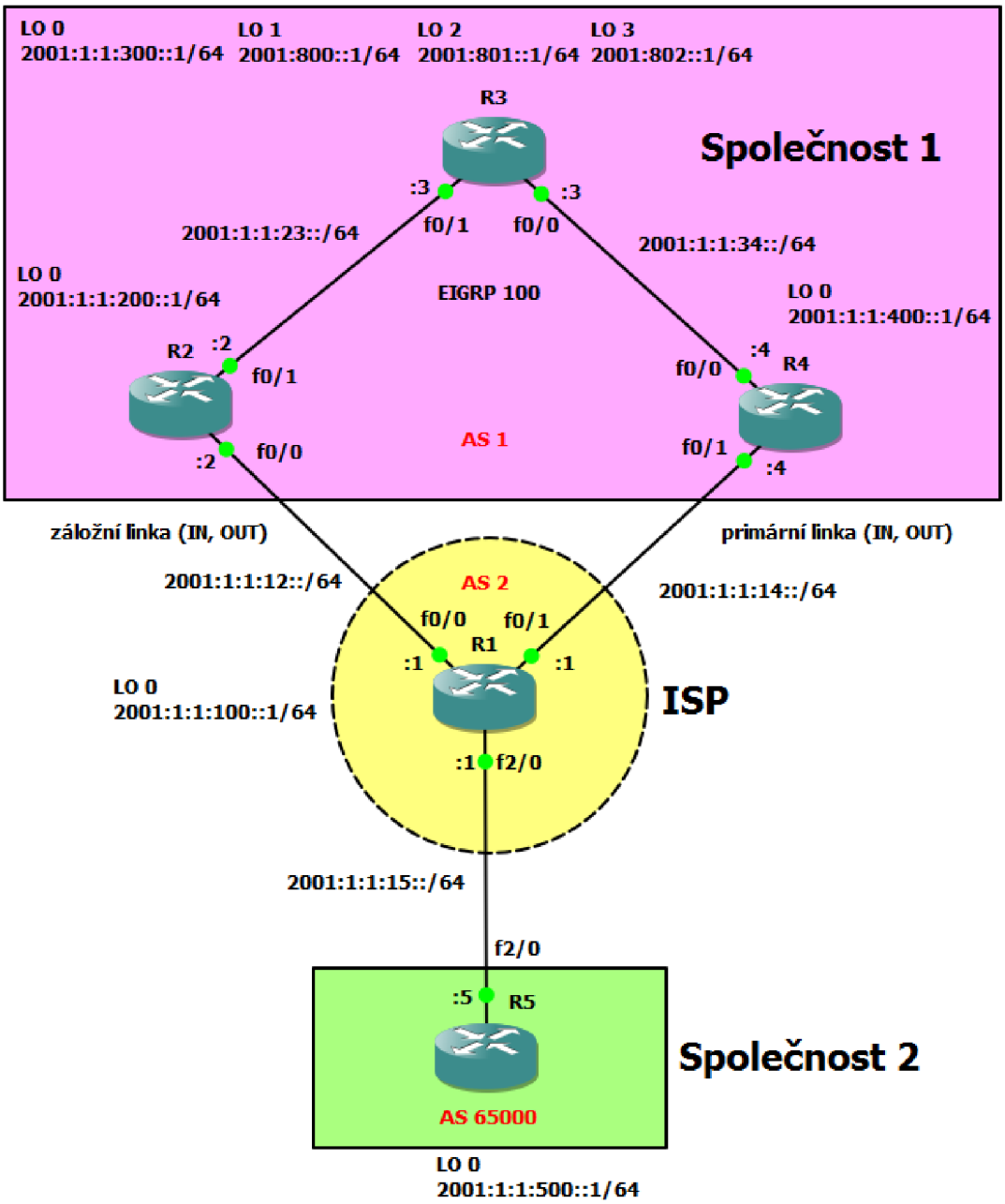
  `R1#show zone-pair security`

- Ověření inspekce spojení vytvořené kvůli mapě politik aplikované na pár zón - je vidět, kolik paketů bylo shodných s typem provozu, který je definovaný v class-map, popřípadě kolik bylo zahozeno paketů viz obr. 7.2

```
R1#show policy-map type inspect zone-pair session

policy exists on zp IN-TO-OUT
 Zone-pair: IN-TO-OUT

  Service-policy inspect : IN-TO-OUT-POLICY

    Class-map: IN-TO-OUT-CLASS (match-any)
      Match: protocol icmp
        4 packets, 240 bytes
        30 second rate 0 bps

    Inspect

      Class-map: class-default (match-any)
      Match: any
      Drop
        2 packets, 48 bytes
```

Obr. 7.2: Výstup ověření inspekce spojení vytvořené kvůli mapě politik aplikované na pár zón

8 ÚLOHA - MULTIPROTOCOL BORDER GATEWAY PROTOCOL



Obr. 8.1: Topologie úloha MP-BGP

8.1 Obsah konfigurace

- IPv6 adresy
- EIGRPv6
- MP-BGP, pokročilé nastavení sousedů
- Statické IPv6 směry
- Sumarizace v MP-BGP
- Změny BGP atributů (NEXT_HOP, LOCAL_PREF, MED)
- Filtrování privátních AS

8.2 Pozadí a cíle úlohy

V topologii viz obr. 8.1 jsou 2 společnosti a jeden ISP (Internet Service Provider). V celé úloze jsou výhradně použity IPv6 adresy. Do BGP jsou zahrnuty všechny loopback sítě v celé topologii. Všechna BGP sousedství jsou navázána pomocí Lo0 kromě sousedství mezi R5 a R1.

Společnost 1 má Dual-homed připojení k jednomu ISP a veřejné číslo Autonomního systému 1. Ve skutečnosti by se tedy jednalo o malou nebo středně velkou společnost, která snese výpadky svého poskytovatele. V rámci Společnosti 1 spolu komunikují směrovače pomocí EIGRPv6. Všechny směrovače také mají všechny BGP cesty a správné next-hopy. R3 v BGP posílá pouze sumarizovanou cestu Lo 1 – 3.

ISP je reprezentován jedním směrovačem v AS 2. Při komunikaci s R3 je v obou směrech primární linka mezi R4 a R1, linka mezi R2 a R1 je záložní. Na R1 se filtruje posílání informací o původu cesty z privátních AS.

Společnost 2 je ukázkou malé firmy bez žádné redundance konektivity. Obsahuje číslo privátního AS 65000. Pokud máte omezený výpočetní výkon, lze vynechat R5, který zde figuruje pouze pro ukázku odfiltrování privátních AS na ISP.

Konfiguraci provádějte co nejefektivněji, např. využitím peer-group u BGP. **Aby se změny v BGP projevily co nejdříve, je nutné používat příkaz:**
`clear ip bgp *` | *`as-number`* | *`ip-address`* `[soft] [in | out]`

Výhradně používejte co nejšetrnější formu, kterou byste museli použít v reálné situaci. Soft reset umožní změnu ve směrovacích tabulkách bez resetování BGP spojení.

8.3 Postup řešení

V této části bude postupný návod k řešení, v další sekci je doplňující nápověda a odpovědi na kontrolní otázky. Celá konfigurace je případně uvedena v příloze Konfigurace úloh.

1. **Zapojení topologie a nastavení IPv6 adres na rozhraní**
   - Adresy pro ušetření času můžete zkopírovat z přílohy Konfigurace úloh, proto je vhodné zvolit si i stejné rozhraní jako v topologii.
   - Vyzkoušejte si alespoň jeden směrovač nakonfigurovat sami.
2. **Povolení EIGRPv6 100 v rámci AS 1**
   - Do EIGRP vložte všechna rozhraní (u všech IPv6 směrovacích protokolů kromě MP-BGP je třeba nastavit směrovací protokol na rozhraní) v AS kromě rozhraní přímo vedoucích k R1.
   - Ověřte funkčnost EIGRP.
3. **Konfigurace iBGP v AS 1**
   - Navažte iBGP sousedství mezi R3 a R2, R3 a R4. Co lze na R3 využít jako optimalizaci pro stejnou konfiguraci souseda R2 a R4?
   - Jak ověříte stav sousedství a sítě v rámci BGP (posílané, obdržené)?
   - Proč neobdržel R2 BGP sítě R4 a opačně?
   - Nakonfigurujte R3 jako route reflector pro R2, R4 a ověřte předchozí bod.
4. **Konfigurace eBGP**
   - Nakonfigurujte všude a efektivně sousedství s využitím adres loopbacku 0 kromě sousedství mezi R1 a R5 (tam použijte adresu společné linky).
   - Pokud jste ještě dodatečně nic nenakonfigurovali, nefunguje eBGP sousedství mezi R1 a R2, R4. Co je ještě třeba nakonfigurovat?
   - Ověřte sousedství.
5. **Ověřte funkčnost pomocí PING v celé topologii**
   - Ověřte ping z R5 na R3. Proč nefunguje?
6. **Změna Next_hopu**
   - R2 a R4 při posílání cesty k R3 nemění BGP atribut NEXT_HOP a R3 nemá cestu k loopbacku 0 na R1. Je tedy třeba tento atribut změnit, aby R3 měl správný next hop. Lze použít route-mapu, aplikujte ji na správných zařízeních ve správném směru (aplikují se v address-family na souseda).
   - Ověřte znovu ping, který by nyní měl být funkční mezi všemi loopbacky v topologii.
7. **Sumarizace loopbacku 1 - 3 na R3 a posílání pouze sumární cesty v BGP**
   - Sumarizujte co nejefektivněji.
   - Nezapomeňte posílat POUZE sumární cestu.
   - Jak ověříte, že už se posílá pouze sumární cesta?
8. **Privátní AS**
   - Všimněte si, že i směrovače v AS 1 mají u cesty k R5 uvedeno AS 65000, což ale spadá do privátního rozsahu a ISP by to měl filtrovat.

- Proveďte filtrovaní posílání privátního čísla AS.
- Ověřte, že už směrovače v AS 1 nemají informaci o privátním AS, ale v něm přítomná síť zůstala dostupná.

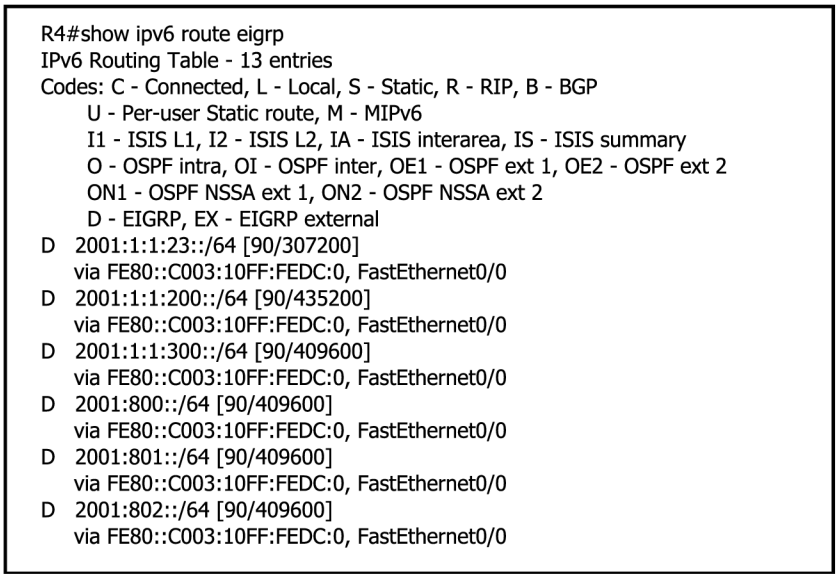
9. **Nastavení preferované cesty z R3 mimo AS 1 a opačně**
   - Kterou cestou nyní prochází R3 do sítě mimo svůj AS (např. jakou cestou prochází ping na R5)? Přes R2 nebo R4 a proč?
   - Nastavte, aby byla preferovaná cesta přes R4 a záložní přes R2.
   - Kterou cestou nyní jde R5 a R1 do sítě R3? Přes R2 nebo R4 a proč?
   - Nastavte, aby byla preferovaná cesta přes R4 a záložní přes R2.
   - Nyní zkuste `traceroute` mezi R3 a R5 (oboje loopback 0) a zkontrolujte, že v obou směrech se jde přes R4.
10. **Je vždy preferovaná cesta mezi R1 a R4?**
    - Zamyslete se, zda je vždy preferovaná cesta mezi R1 a R4, nebo se někdy jde i přes R2 a popřípadě za jaké situace.

8.4 Nápověda a odpovědi

1. **Zapojení topologie a nastavení IPv6 adres na rozhraní**
   - IPv6 adresy lze zkontrolovat pomocí příkazu:

     ```
     R#show ipv6 interface brief
     ```

2. **Povolení EIGRPv6 100 v rámci AS 1**
   - Jelikož směrovače nemají žádnou IPv4 adresu, je třeba zadat v nastavení EIGRP router-id ve formátu IPv4 adresy. Zadejte router-id analogicky k názvu směrovače (R1 = 1.1.1.1).
   - Nezapomeňte povolit IPv6 směrování.
   - Příklad ověření u R4 viz obr. 8.2.
3. **Konfigurace iBGP v AS 1**
   - Použijte peer-group pro R2 a R4 na R3.
   - iBGP sousedi by měli být propojeni každý s každým, protože cesty naučené v rámci iBGP soused neposílá dalšímu iBGP sousedovi kvůli zajištění topologie bez smyček. Pokud chceme ale ušetřit propoj a zprávy, které chodí mezi všemi iBGP sousedy, můžeme použít R3 jako route reflector, který bude svým 2 klientům posílat navzájem naučené cesty.
   - U route reflectoru se používá stejný příkaz jako pro IPv4 BGP, ale je ho nutno zadat až do adresní rodiny (address-family). Dle výpisů by sice bylo sousedství funkční (UP), ale nepřenášely by se IPv6 adresy.



Obr. 8.2: Výstup ověření konfigurace EIGRPv6 na R4

- Ověření BGP sousedství:
  `R#show ip bgp ipv6 unicast neighbors`
- Příklad ověření posílaných a přijímaných sítí v rámci iBGP na R2:
  `R2#show ip bgp ipv6 unicast neighbors 2001:1:1:300::1 routes`
  `R2#show ip bgp ipv6 unicast neighbors 2001:1:1:300::1 advertised-routes`
- Po konfiguraci route-reflector by se mělo zobrazit toto:

```
*Mar  BGP-5-ADJCHANGE: ... Down RR client config change
*Mar  BGP-5-ADJCHANGE: ... Down RR client config change
*Mar  BGP-5-ADJCHANGE: neighbor 2001:1:1:400::1 Up
*Mar  BGP-5-ADJCHANGE: neighbor 2001:1:1:200::1 Up
```

- Nyní znovu ověřte přijímané sítě na R2 a R4 a už je vidět, že mají BGP směry na vzájemné loopbacky viz obr. 8.3.

4. **Konfigurace eBGP**
   - Opět použijte peer-group při konfiguraci sousedů R2 a R4 na R1.
   - R2 a R4 nemají cestu k loopbacku 0 na R1 a opačně, proto nelze navázat sousedství, přidejte statické cesty.
   - Pokud se jedná o eBGP a konfigurujeme update-source, je nutné zadat `ebgp-multihop` a počet hopů, protože implicitně by to mělo být přímé spojení a pouze to je povoleno. Opět nezapomeňte na router-id.
   - Ověření BGP sousedství:
     `R#show ip bgp ipv6 unicast neighbors`

```
R2#show ip bgp ipv6 unicast neighbors 2001:1:1:300::1 routes
BGP table version is 15, local router ID is 2.2.2.2
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*>i2001:1:1:300::/64
                    2001:1:1:300::1          0    100      0 i
*>i2001:1:1:400::/64
                    2001:1:1:400::1          0    100      0 i
*>i2001:800::/64    2001:1:1:300::1          0    100      0 i
*>i2001:801::/64    2001:1:1:300::1          0    100      0 i
*>i2001:802::/64    2001:1:1:300::1          0    100      0 i

Total number of prefixes 5
```

Obr. 8.3: Výstup ověření funkce route-reflector na R2 - přibyla BGP sít Loopbacku z R4

5. **Ověřte funkčnost pomocí PING v celé topologii**
   - Zkuste se podívat na směrovací tabulky R3 a R5, tam lze nalézt vše.
   - První problém mohl nastat, pokud jste jako zdrojovou či cílovou IPv6 adresu neuvedli loopback 0 (jinak se použije zdrojová adresa ethernetového rozhraní, která se neposílá v rámci BGP).
   - Další problém je, že v rámci iBGP se nezmění atribut NEXT_HOP a R3 nezná cestu k loopbacku 0 na R1, který je uveden jako další hop k síti loopbacku 0 na R5. V Dalším kroku ho tedy změníme.
6. **Změna Next_hopu**
   - Route-mapu vytvoříme na R2 a R4, uvnitř využijeme příkaz `set ipv6 next-hop` + adresa dalšího hopu a aplikujeme v adresní rodině (address-family) na souseda R3 ve směru out.
7. **Sumarizace loopbacku 1 - 3 na R3 a posílání pouze sumární cesty v BGP**
   - Nejefektivnější sumarizace (příkaz) s vynucením posílání pouze sumární cesty je:

     ```
     R3(config-router-af)#aggregate-address 2001:800::/30
     summary-only
     ```

   - Příklad obdržených BGP sítí na R2 již se sumarizovanou cestou viz obr. 8.4.

```
R2#Show ip bgp ipv6 unicast neighbors 2001:1:1:300::1 routes
BGP table version is 21, local router ID is 2.2.2.2
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*>i2001:1:1:300::/64
                    2001:1:1:300::1          0    100      0 i
*>i2001:1:1:400::/64
                    2001:1:1:400::1          0    100      0 i
*>i2001:800::/30    2001:1:1:300::1          0    100      0 i

Total number of prefixes 3
```

Obr. 8.4: Výstup ověření obdržených BGP sítí na R2 již se sumarizovanou cestou

8. **Privátní AS**
   - Příklad posílání čísla privátního AS na R2 viz obr. 8.5.

```
R2#show ip bgp ipv6 unicast
BGP table version is 21, local router ID is 2.2.2.2
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*> 2001:1:1:100::/64
                    2001:1:1:100::1          0             0 2 i
*> 2001:1:1:200::/64
                    ::                       0         32768 i
*>i2001:1:1:300::/64
                    2001:1:1:300::1          0    100      0 i
*>i2001:1:1:400::/64
                    2001:1:1:400::1          0    100      0 i
*> 2001:1:1:500::/64
                    2001:1:1:100::1                       0 2 65000 i
*>i2001:800::/30    2001:1:1:300::1          0    100      0 i
```

Obr. 8.5: Výstup ověření posílání čísla privátního AS na R2

   - Jedná se o intuitivní příkaz, který je třeba zadat opět v adresní rodině. Zadává se ale u sousedů, pro které to budeme filtrovat, ne u toho, který leží v privátním AS. Po správné konfiguraci by mělo číslo privátního AS zmizet ze směrovačů v AS 1.
9. **Nastavení preferované cesty z R3 mimo AS 1 a opačně**
   - V této situaci záleží na router-id, pokud jste podle návodu nastavili router-id analogicky k názvu směrovače (např. R2 = 2.2.2.2), tak budete mít současnou preferovanou cestu přes R2 a záložní přes R4 (z R3 na R1 nebo R5, opačně to je opět něco jiného). Přednost má směrovač s nižším router-id. Lze ověřit pomocí `traceroute`.

- Pro manipulaci s výběrem cesty použijeme atribut LOCAL_PREF, čím vyšší, tím lepší (implicitně 100). Využijeme route-mapu jako u agregace směrů na R3 a podobným způsobem také aplikujeme (stačí na R4 zvětšit). Ověřte `traceroute` z R3 na R5 a podívejte se do tabulky BGP cest viz obr. 8.6. Použijte šetrný způsob vynucení poslání BGP zpráv sousedovi R3 z R4, aby se změna projevila rovnou (`clear ip bgp ipv6 unicast 1 soft out`).

```
R3#show ip bgp ipv6 unicast
BGP table version is 23, local router ID is 3.3.3.3
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*>i2001:1:1:100::/64
                    2001:1:1:400::1          0    150      0 2 i
*>i2001:1:1:200::/64
                    2001:1:1:200::1          0    100      0 i
*> 2001:1:1:300::/64
                    ::                       0         32768 i
*>i2001:1:1:400::/64
                    2001:1:1:400::1          0    100      0 i
*>i2001:1:1:500::/64
                    2001:1:1:400::1          0    150      0 2 65000 i
s> 2001:800::/64    ::                       0         32768 i
*> 2001:800::/30    ::                                 32768 i
s> 2001:801::/64    ::                       0         32768 i
s> 2001:802::/64    ::                       0         32768 i
```

Obr. 8.6: Výstup ověření zvětšení LOCAL_PREF R4 na R3

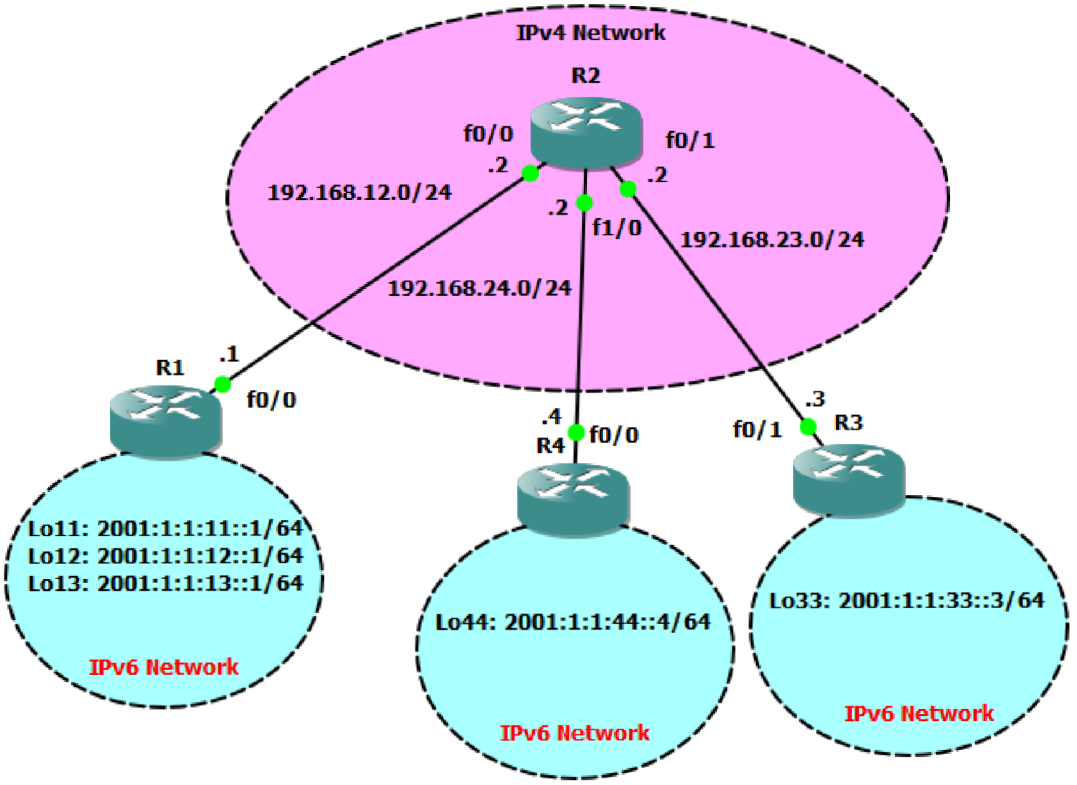
- Z R5 a R1 na R3 záleží, kterou cestu se naučil směrovač dříve. Můžete zkusit `traceroute` a zjistit, kterou cestou to jde nyní, poté resetovat BGP spojení s preferovaným směrovačem a zkusit znovu `traceroute` a cesta se změní na cestu, která tam je déle, takže opačnou, než před tím.
- Pro manipulaci s výběrem cesty (pro permanentní výběr cesty přes R4) použijeme atribut MED, čím nižší, tím lepší (implicitně 0). Využijeme route-mapu jako u LOCAL_PREF a podobným způsobem také aplikujeme. Je důležité si uvědomit, zda OUT nebo IN směr. Ověřte `traceroute` z R5 na R3 a podívejte se do tabulky BGP cest viz obr. 8.7 (změna atributu u R2 i R4 - stačilo by zvýšit pouze hodnotu R2). Použijte šetrný způsob vynucení poslání BGP zpráv sousedovi R1, aby se změna projevila rovnou (`clear ip bgp ipv6 unicast 2 out`).

```
R1#show ip bgp ipv6 unicast
BGP table version is 38, local router ID is 1.1.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*> 2001:1:1:100::/64
                    ::                       0         32768 i
*> 2001:1:1:200::/64
                    2001:1:1:400::1         50           0 1 i
*                   2001:1:1:200::1         75           0 1 i
*  2001:1:1:300::/64
                    2001:1:1:200::1         75           0 1 i
*>                  2001:1:1:400::1         50           0 1 i
*  2001:1:1:400::/64
                    2001:1:1:200::1         75           0 1 i
*>                  2001:1:1:400::1         50           0 1 i
*> 2001:1:1:500::/64
                    2001:1:1:15::5           0           0 65000 i
*  2001:800::/30    2001:1:1:200::1         75           0 1 i
*>                  2001:1:1:400::1         50           0 1 i
```

Obr. 8.7: Výstup ověření upravení MED R4 a R2 na R1

10. **Je vždy preferovaná cesta mezi R1 a R4?**
    - Pokud jdeme z R2 na R1 a opačně, tak to jde přímo a ne přes R4. Máme tam vytvořenou statickou cestu k loopbacku 0 s nižší administrativní vzdáleností (šlo by jednoduše zvětšit, za příkaz stačí dát vyšší číslo). Stále by se ale nic nezměnilo, protože R2 má cestu od eBGP souseda R1 s AD menší, než od iBGP souseda R3. Opět bychom museli zvětšit pomocí route-mapy i tuto Administrativní vzdálenost.

9 ÚLOHA - IPV6 TUNELY



Obr. 9.1: Topologie úloha IPv6 tunely

9.1 Obsah konfigurace

- Manuální tunel
- GRE (Generic Routing Encapsulation) tunel
- ISATAP (Intra-Site Automatic Tunnel Addressing Protocol) tunel
- 6to4 tunel
- EIGRPv6
- Statické směrování
- Sumarizace IPv6 adres
- Převod IPv4 adres na IPv6 pro 6to4 tunel

9.2 Pozadí a cíle úlohy

Směrovače R1, R3 a R4 vyjadřují zařízení, která podporují jak IPv4, tak IPv6. Postupně v další sekci bude vždy uvedena přesná situace, kde bude rozebráno, jaký tunel se hodí a proč. Budou použity 4 tunely, pokud bude situace s využitím point-to-point (bod-bod) tunelu, R4 bude vynechán. R2 představuje zařízení, které podporuje pouze IPv4 a prochází přes něho veškerá komunikace mezi ostatními směrovači.

V prvních dvou situacích bude topologie viz obr. 9.1 představovat jednu lokalitu, kde spolu chtějí prvně dva, poté tři směrovače komunikovat přes společnou IPv4 síť, aby poskytly i konektivitu mezi IPv6 sítěmi, které jsou připojeny k jednotlivým směrovačům.

V posledních dvou situacích bude topologie představovat prvně dvě, poté tři lokality (např. pobočky společnosti), které spolu chtějí komunikovat přes společnou IPv4 síť, aby poskytly i konektivitu mezi IPv6 sítěmi, které jsou připojeny k jednotlivým směrovačům.

9.3 Postup řešení

V této části bude postupný návod k řešení, pokaždé bude vytvořena nějaká situace, kde by se dal použít tunel a cílem bude vybrat vhodný a nakonfigurovat ho. V další sekci je doplňující nápověda a odpovědi na kontrolní otázky. Celá konfigurace je případně uvedena v příloze Konfigurace úloh.

1. **Zapojení topologie a nastavení IPv4 a IPv6 adres na rozhraní**
   - Adresy pro ušetření času můžete zkopírovat z přílohy Konfigurace úloh, proto je vhodné zvolit si i stejné rozhraní jako v topologii.
   - Vyzkoušejte si alespoň jeden směrovač nakonfigurovat sami.
2. **Situace 1**
   - Představme si síť v rámci jedné lokality. R4 je vynechán. R1 a R3 jsou zařízení, ke kterým jsou už připojené IPv6 sítě z důvodu postupného přechodu na IPv6. R1 a R3 spolu chtějí komunikovat přes IPv4 síť, kde se nachází zařízení R2, které nepodporuje IPv6. V této situaci se jeví možnost použít techniku tunelování.
   - Jaký tunel se hodí pro tuto situaci a proč?
3. **Manuální tunel 13 mezi R1 a R3**
   - Tato technika je využívána pro point-to-point (bod-bod) spojení přes tunel, takže je třeba zadat zdrojovou a cílovou adresu tunelu (IPv4). Také je třeba zadat IPv6 adresu tunelu, zadejte 2001:13:13:13::1/64 pro R1 a 2001:13:13:13::3/64 pro R3.
   - Jako mód tunelu u tohoto způsobu je použit `ipv6ip`.

- Pokud jste dodatečně již nenakonfigurovali nic dalšího, nebude tunel fungovat, co je třeba dodělat?
- Jak ověříte nastavení tunelu?

4. **Směrování: EIGRP 1**
   - Abychom zajistili konektivitu všech IPv6 sítí, je třeba nakonfigurovat směrování. R1 obsahuje více sítí, abychom nemuseli všechny směry zadávat ručně, využijeme EIGRPv6 směrovaní.
   - Co je třeba navíc nakonfigurovat v EIGRPv6 oproti EIGRP a jak ověříme funkčnost?
   - Ověřte konektivitu všech IPv6 sítí a funkčnost tunelu.
5. **Situace 2**
   - Přidáme do sítě další zařízení R4, ke kterému je připojená IPv6 síť z důvodu rozšíření sítě v jedné lokalitě. Je třeba, aby R1 i R4 komunikoval s R3, který představuje směrovač vyšší vrstvy. Hodí se stále používat Manuální tunely a proč/proč ne?
   - Jaký tunel se hodí pro tuto situaci a proč?
6. **ISATAP tunel 3 mezi R1, R4 a R3**
   - Pokud jste tak již neučinili, zapněte R4 a nakonfigurujte na něm IPv4 a IPv6 adresu.
   - Zrušte manuální tunel na R1 a R3 z minulé situace. Ověřte, že komunikace mezi lokalitami už nefunguje.
   - Tato technika je využívána pro point-to-multipoint (bod - více bodů) tunely, takže je třeba zadat pouze zdrojovou adresu tunelu (IPv4). Také je třeba zadat IPv6 adresu tunelu vytvořenou pomocí eui-64 mechanizmu, zadejte adresy z rozsahu 2001:33:33:33::/64.
   - Jako tunnel mode je použito `ipv6ip isatap` u tohoto způsobu.
   - Pokud jste dodatečně již nenakonfigurovali nic dalšího, nebude tunel fungovat, co je třeba dodělat?
   - Ověřte nastavení tunelu.
7. **Směrování**
   - Bude možné opět použít dynamické směrování?
   - Nakonfigurujte směrování, aby byla možná konektivita všech IPv6 sítí (u loopback sítí na R1 použijte nejefektivnější sumarizaci).
   - Ověřte konektivitu všech IPv6 sítí a funkčnost tunelu.
8. **Situace 3**
   - Představte si, že R2 je ISP. R1, R3 a R4 představují hraniční směrovače lokalit (poboček). R4 prozatím vynechme. Co musíme řešit v této situaci kromě pouhého přenesení paketů?
   - Jaký tunel se hodí pro tuto situaci a proč?

9. **GRE tunel 13 mezi R1 a R3**
    - Vypněte R4.
    - Zrušte ISATAP tunel z minulé situace.
    - Konfigurace je hodně podobná manuálnímu tunelu, použijte stejné adresy.
    - Jako tunnel mode nemusíte zadávat nic, GRE tunel je implicitní volba na Cisco zařízeních.
    - Ověřte funkčnost tunelu.
10. **Směrování**
    - Bude možné použít dynamické směrování?
    - Nakonfigurujte směrování, aby byla možná konektivita všech IPv6 sítí mezi R1 a R3.
    - Ověřte konektivitu všech IPv6 sítí.
11. **Situace 4**
    - Přidáme do sítě další zařízení R4, ke kterému je připojená IPv6 síť z důvodu rozšíření společnosti (přidání 1 pobočky). Je třeba, aby spolu všechny pobočky komunikovaly. Hodí se stále používat GRE tunely a proč/proč ne?
    - Jaký tunel se hodí pro tuto situaci a proč?
12. **6to4 tunel 3 mezi R1, R4 a R3**
    - Pokud jste tak již neučinili, zapněte R4.
    - Zrušte GRE tunel z minulé situace.
    - Tato technika je využívána pro point-to-multipoint tunely, takže je třeba zadat pouze zdrojovou adresu tunelu (IPv4). Také je třeba zadat IPv6 adresu tunelu ve speciálním formátu, kde adresa je složená z prefixu 2002::/16 následovaným IPv4 adresou hraničního směrovače převedenou do hexa-decimálního tvaru. Jak musí adresa vypadat (např. na R1)?
    - Jako tunnel mode je použito `ipv6ip 6to4` u tohoto způsobu.
    - Ověřte funkčnost tunelu.
13. **Směrování**
    - Statické směrování bude nakonfigurované podobně jako u situace 2.
    - Ověřte konektivitu všech IPv6 sítí a funkčnost tunelu.

9.4 Nápověda a odpovědi

1. **Zapojení topologie a nastavení IPv4 a IPv6 adres na rozhraní**
   - IPv6 adresy lze zkontrolovat pomocí příkazu:

     ```
     R#show ipv6 interface brief
     ```

   - IPv4 adresy lze zkontrolovat pomocí příkazu:

     ```
     R#show ip interface brief
     ```

2. **Situace 1**
   - Pro spojení point-to-point (R1 s R3) se hodí např. GRE tunel nebo Manuální tunel. Konfigurace těchto tunelů je jednoduchá a dostačující pro tuto situaci.
3. **Manuální tunel mezi R1 a R3**
   - Cílová IPv4 adresa, kterou jste zadali do konfigurace tunelu, není ve směrovací tabulce, je tedy třeba dodělat toto směrování na R1 a R3.
   - Ověření nastavení tunelu (pokud máte již nakonfigurované směrování mezi R1 a R3, bude UP, jinak DOWN):

     ```
     R#show interface tunnel 13
     ```

4. **Směrování: EIGRP 1**
   - Je třeba prvně povolit IPv6 směrování. Sítě se přidávají tak, že povolíme směrování EIGRP přímo na rozhraní (pokud by směrovač neměl IPv4 adresu, tak bychom také museli zadat router-id ve tvaru IPv4 adresy). Nezapomeňte EIGRP povolit na rozhraní tunelu i ethernetovém rozhraní.
   - Nyní by měl fungovat ping mezi všemi loopbacky na R1 a R3. Příklad kontroly tunelu na R1 viz obr. 9.2. Ověření směrování:

     ```
     R#show ipv6 route
     R#show ip route
     ```

5. **Situace 2**
   - Nyní bychom při zachování manuálního tunelování museli vytvořit další tunel mezi R4 a R3, toto řešení už není optimální vzhledem k možnému dalšímu růstu sítě, což by znamenalo pokaždé konfiguraci i na straně R3 a vzrůstající počet tunelů. Pokud bychom chtěli komunikaci i mezi R4 a R1, opět bychom konfigurovali tunel na obou směrovačích.
   - V této situaci je vhodné použít point-to-multipoint tunel, což bude znamenat jedinou konfiguraci tunelu na R3. Pokud síť opět rozšíříme, stačila by konfigurace na straně nového zařízení a ne na všech směrovačích. Hodí se použít ISATAP tunel, který je point-to-multipoint a je určen k tunelování v rámci jedné lokality.

```
R1#show interface tunnel 13
Tunnel13 is up, line protocol is up
  Hardware is Tunnel
  MTU 1514 bytes, BW 9 Kbit, DLY 500000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation TUNNEL, loopback not set
  Keepalive not set
  Tunnel source 192.168.12.1 (FastEthernet0/0), destination 192.168.23.3
  Tunnel protocol/transport IPv6/IP
  Tunnel TTL 255
  Fast tunneling enabled
  Tunnel transmit bandwidth 8000 (kbps)
  Tunnel receive bandwidth 8000 (kbps)
  Last input 00:00:03, output 00:00:00, 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
     117 packets input, 13998 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
     119 packets output, 12088 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 output buffer failures, 0 output buffers swapped out
```

Obr. 9.2: Výstup ověření Manuálního tunelu mezi R1 a R3 na R1

6. **ISATAP tunel 3 mezi R1, R4 a R3**
   - Zdrojová IPv4 adresa, kterou jste zadali do konfigurace tunelu (u R4), není ve směrovací tabulce R3 (u R4 zase adresa R3), je tedy třeba dodělat toto směrování na R3 a R4 (pokud bychom chtěli, aby i R1 mohl komunikovat s R4, tak i na R1).
   - Ověření nastavení tunelu:

     `R#show interface tunnel 3`

7. **Směrování**
   - Není možno přenášet multicasty (problém s dynamickým směrováním), u OSPF je způsob pomocí příkazu `ipv6 ospf neighbor` *`ipv6 neighbor address`* v nastavení rozhraní tunelu. Nakonfigurujte statické směrování.
   - Sumární adresa loopbacků na R1 je 2001:1:1:10::/62. Pokud má být konektivita všech IPv6 sítí, tak je třeba nakonfigurovat i IPv4 směrování mezi R1 a R4.
   - Příklad kontroly tunelu na R1 viz obr. 9.3. Ověření směrování:

     `R#show ipv6 route`

```
R1#show interface tunnel 3
Tunnel3 is up, line protocol is up
  Hardware is Tunnel
  MTU 1514 bytes, BW 9 Kbit, DLY 500000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation TUNNEL, loopback not set
  Keepalive not set
  Tunnel source 192.168.12.1 (FastEthernet0/0), destination UNKNOWN
  Tunnel protocol/transport IPv6 ISATAP
  Tunnel TTL 255
  Fast tunneling enabled
  Tunnel transmit bandwidth 8000 (kbps)
  Tunnel receive bandwidth 8000 (kbps)
  Last input never, output 00:01:17, 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
     0 packets input, 0 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
     4 packets output, 384 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 output buffer failures, 0 output buffers swapped out
```

Obr. 9.3: Výstup ověření ISATAP tunelu 3 na R1

8. **Situace 3**
   - Pokud cesta vede přes nebezpečnou síť jako je Internet, je třeba i zabezpečení, tunely dělají pouze zapouzdření, pro toto řešení se používá například IPsec VPN často i ve spojení s GRE tunelem (ten je schopen přenášet i jiné protokoly než IPv6). Konfigurace IPsec VPN je kvůli časové náročnosti vynechána.
   - Hodí se opět point-to-point tunel z již známých důvodů. Nakonfigurujeme GRE tunel mezi R1 a R3, protože manuální již byl použit.
9. **GRE tunel 13 mezi R1 a R3**
   - Ověření nastavení tunelu:

     ```
     R#show interface tunnel 13
     ```

10. **Směrování**
    - Ano, bude to možné, jedná se o point-to-point tunel, kde je zadáván jak zdroj, tak cíl tunelu. Použijte třeba EIGRPv6 (nezapomeňte EIGRP povolit na rozhraní tunelu i ethernetu).
    - Příklad kontroly tunelu na R1 viz obr. 9.4. Ověření směrování:

      `R#show ipv6 route`

```
R1#show interface tunnel 13
Tunnel13 is up, line protocol is up
  Hardware is Tunnel
  MTU 1514 bytes, BW 9 Kbit, DLY 500000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation TUNNEL, loopback not set
  Keepalive not set
  Tunnel source 192.168.12.1 (FastEthernet0/0), destination 192.168.23.3
  Tunnel protocol/transport GRE/IP
    Key disabled, sequencing disabled
    Checksumming of packets disabled
  Tunnel TTL 255
  Fast tunneling enabled
  Tunnel transmit bandwidth 8000 (kbps)
  Tunnel receive bandwidth 8000 (kbps)
  Last input 00:01:04, output 00:01:12, 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
     10 packets input, 952 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
     10 packets output, 952 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 output buffer failures, 0 output buffers swapped out
```

Obr. 9.4: Výstup ověření GRE tunelu 13 na R1

11. **Situace 4**
    - Nyní nastává stejný problém jako po přidání R4 v situaci 2. Opět je třeba použít point-to-multipoint tunel.
    - Pro situaci propojení více lokalit je vhodné použít 6to4 tunel. 6to4 tunel používá prefix 2002::/16, 32 bitů po prefixu /16 je reprezentováno IPv4 adresou hraničního směrovače, která je převedena do hexa-decimálního tvaru. Tento prefix /48 je určený pro celý IPv6 ostrov. V Internetu je tedy nutností IPv4 veřejná adresa hraničního směrovače a poté mají všechny adresy v IPv6 ostrově v sobě ukrytou IPv4 adresu hraničního směrovače, která je použita jako next-hop při použití tunelu.

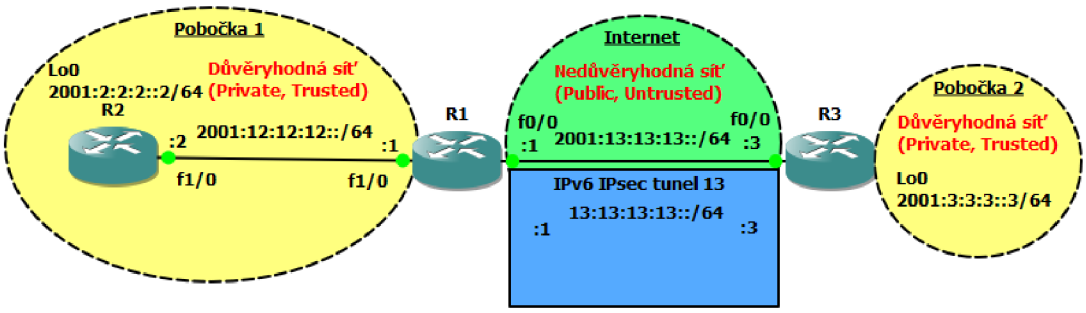
12. **6to4 tunel 3 mezi R1, R4 a R3**
    - Prefix, jak bylo zmíněno je 2002::/16. Poté převedeme IPv4 adresy do hexa-decimálního formátu (R1=c0a8:0c01, R3=c0a8:1703, R4=c0a8:1804). Adresa tedy vypadá např. 2002:c0a8:0c01:1::1/64 na R1 (po převedené IPv4 adrese zbývá 16 bitů na ID podsítě (v tomto případě zvoleno jako "1") a ::1 vyjadřuje interface id.
13. **Směrování**
    - Příklad kontroly tunelu na R1 viz obr. 9.5. Ověření směrování:

      `R#show ipv6 route`

```
R1#show  interface tunnel3
Tunnel3 is up, line protocol is up
  Hardware is Tunnel
  MTU 1514 bytes, BW 9 Kbit, DLY 500000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation TUNNEL, loopback not set
  Keepalive not set
  Tunnel source 192.168.12.1 (FastEthernet0/0), destination UNKNOWN
  Tunnel protocol/transport IPv6 6to4
  Tunnel TTL 255
  Fast tunneling enabled
  Tunnel transmit bandwidth 8000 (kbps)
  Tunnel receive bandwidth 8000 (kbps)
  Last input 00:00:01, output 00:00:01, 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
     5 packets input, 700 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
     11 packets output, 1176 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 output buffer failures, 0 output buffers swapped out
```

Obr. 9.5: Výstup ověření 6to4 tunelu 3 na R1

10 ÚLOHA - IPSEC VPN A ZONE BASED FIREWALL



Obr. 10.1: Topologie úloha IPsec VPN a Zone Based Firewall

10.1 Obsah konfigurace

- IPv6 adresy
- Statické IPv6 směry
- Nastavení IPv6 IPsec VPN s využitím VTI
- Zone Based Firewall

10.2 Funkčnost v GNS3

V první řadě je třeba použít IOS s podporou konfigurace bezpečnostních prvků. V této úloze může nastat problém ještě při konfiguraci Zone Based Firewallu za použití IPv6. Při použití IPv4 není žádný problém, ale při použití IPv6 se může objevit situace, kdy jde vše nakonfigurovat, ale nemusí být funkční.

Funkčnost s IPv6 v GNS3 verzi 1.2.3 jsem dosáhl pouze s IOSem 15.1(4)M pro řadu 7200, což značně vytěžuje procesor, proto jsem v topologii volil pouze 3 směrovače.

10.3 Pozadí a cíle úlohy

R1 a R3 představují hraniční směrovače dvou poboček (Pobočka 1 a Pobočka 2). R2 je vnitřní směrovač v Pobočce 1. V celé topologii viz obr. 10.1 jsou použity výhradně

IPv6 adresy. Jelikož mezi R1 a R3 je veřejná, tím pádem nedůvěryhodná síť (Internet), chceme komunikaci mezi těmito hraničními zařízeními poboček zabezpečit. Pro zabezpečení využijeme IPv6 IPsec VPN s využitím Virtual Tunnel Interface.

Nakonfigurujeme Zone Based Firewall na R1, kde budeme předpokládat, že rozhraní vedoucí k R2 je v důvěryhodné síti, kdežto rozhraní vedoucí k R3 je v nedůvěryhodné síti. ICMP zprávy budou moci projít z důvěryhodné sítě do nedůvěryhodné a zpět, ale z nedůvěryhodné sítě budou ICMP zprávy filtrovány na R1.

10.4 Postup řešení

V této části bude postupný návod k řešení, v další sekci je doplňující nápověda a odpovědi na kontrolní otázky. Celá konfigurace je případně uvedena v příloze Konfigurace úloh.

1. **Zapojení topologie a nastavení IPv6 adres na rozhraní**
   - Adresy pro ušetření času můžete zkopírovat z přílohy Konfigurace úloh, proto je vhodné zvolit si i stejná rozhraní jako v topologii.
   - Vyzkoušejte si alespoň jeden směrovač nakonfigurovat sami.
2. **IKE politiky a předsdílený klíč**
   - Nyní provedeme konfiguraci IPv6 IPsec VPN s využitím VTI mezi R1 a R3, IKE politiky a předsdílený klíč je první krok konfigurace.
   - V tomto kroku nastavte ISAKMP politiky s prioritou 5. Šifrování bude AES. Dále nastavte skupinu zabezpečení na hodnotu 2 a autentizaci pomocí předsdíleného klíče. Toto nastavení bude stejné u R1 i R3.
   - Nastavte jednotlivě na R1 a R3 ISAKMP předsdílený klíč s parametrem, aby následovalo heslo v nešifrované formě, které bude *key123* a zadejte IPv6 adresu rozhraní protějšího konce VPN (adresu ethernetu, ne tunelu) pro spárování s klíčem.
   - Jak ověříme nastavení IKE politik a klíče?
3. **IPsec transform set a IPsec profil**
   - V tomto kroku bude stejná konfigurace jak na R1, tak na R3. Transform set je kombinace bezpečnostních protokolů a algoritmů, které jsou přijatelné pro IPsec směrovače.
   - Nastavte IPsec transform set s názvem *ipsec_transf*, ESP transformaci používající AES šifrování a ESP používající HMAC-SHA autentizaci.
   - Nastavte tunelovací mód VPN.
   - Vytvořte IPsec profil jménem *ipsec_prof* a uvnitř nastavte IPsec transform set vytvořený v minulém kroku.

4. **IPsec IPv6 VTI**
    - Nyní je třeba nakonfigurovat virtuální tunelovací rozhraní (VTI) - vytvořte tunel 13.
    - Povolte IPv6 na tomto rozhraní.
    - Nastavte IPv6 adresu tunelu podle obr. **??**.
    - Nakonfigurujte zdrojovou a cílovou adresu tunelu. Zdrojová a cílová adresa tunelu je IPv6 adresa ethernetových rozhraní mezi R1 a R3.
    - Jako tunelovací mód nastavte IPsec IPv6.
    - Nezapomeňte aplikovat ochranu v podobě IPsec profilu.
    - Nyní je tunel hotov, proč ale stále není možná komunikace přes tunel?
5. **Směrování a ověření**
    - Požadujeme, aby veškerá komunikace probíhala přes právě nakonfigurovaný tunel.
    - Nakonfigurujte statické směrování na všech směrovačích, aby byla možná konektivita z jakéhokoliv směrovače na loopback 0 u směrovače R2 i R3.
    - Ověřte, že funguje konektivita na oba loopbacky ze všech směrovačů a komunikace prochází přes tunel.
    - Ověřte konfiguraci tunelu a přesvědčte se, že komunikace je posílaná šifrovaně.
    - Jaké jsou výhody využití VTI? Jak byste řešili, aby provoz mezi pobočkami šel přes tunel, ale ostatní provoz do Internetu ne (nebyl by šifrovaný)?
    - Jako samostatný úkol zkuste vymyslet, popřípadě nakonfigurovat a ověřit, jak by se dala v současné topologii nakonfigurovat situace, kdy by některý provoz procházel přes tunel (reprezentace šifrované výměny dat mezi pobočkami) a některý by nešel přes tunel (stále by provoz fyzicky šel po lince mezi ethernetovými rozhraními R1 a R3, ale ne šifrovaný - reprezentace nešifrovaného provozu do Internetu).
6. **Vytvoření zón**
    - V této části nastává konfigurace Zone Based firewallu. Prakticky celá konfigurace bude probíhat na R1.
    - Vytvoříme dvě zóny, jednu INSIDE pro vnitřní důvěryhodnou síť a jednu nazvanou OUTSIDE pro vnější nedůvěryhodnou síť.
7. **Konfigurace class map (mapa třídy)**
    - Nakonfigurujte mapu třídy, která bude provádět inspekci pro protokol ICMP a bude se jmenovat IN-TO-OUT-CLASS.
8. **Konfigurace policy map (mapa politik)**
    - Vytvořte mapu politik typu inspect s názvem IN-TO-OUT-POLICY a nastavte třídu typu inspect s již vytvořenou mapou třídy (a v ní proveďte

příkaz `inspect`).
    - Vytvořte pro pozdější přehlednost ve statistikách ještě jednu třídu class-default s akcí drop (ukáže počet zahozených paketů).
9. **Vytvoření párů zón a aplikace politik na ně**
    - Vytvořte jeden pár zón IN-TO-OUT, kde vložíte jako zdrojovou zónu dříve vytvořenou zónu pro důvěryhodnou síť a jako cílovou zónu vložte zónu pro nedůvěryhodnou síť.
    - Na nový pár zón aplikujte již vytvořené servisní politiky typu inspect (mapy politik).
10. **Aplikace zón na rozhraní**
    - Nyní byste měli být schopni sami rozhodnout, na které rozhraní aplikovat jakou zónu (jaké zóny je členem).
    - Nezapomeňte, že máme vytvořené virtuální tunelovací rozhraní mezi R1 a R3.
11. **Ověření funkčnosti firewallu**
    - Proveďte ping z R2 na R3 a opačně, jakým způsobem by to mělo fungovat?
    - Jak to, že funguje ping z R2 na R3, když opačně nefunguje, ale odpověď R3 na ping R2 jde cestou zpět na R2?
    - Zkuste z R2 na R3 poslat zprávu jiného typu než ICMP a ověřte, zda bude blokována na firewallu.
    - Ověřte statistiky firewallu, aby byla vidět jeho funkčnost.
    - Zkuste přidat protokol využitý v minulém bodě do povolených stejně jako ICMP a ověřte, zda tyto zprávy firewall už nezahazuje (pokud stále zahazuje, je třeba ještě upravit další část mapy třídy).

10.5 Nápověda a odpovědi

1. **Zapojení topologie a nastavení IPv6 adres na rozhraní**
   - IPv6 adresy lze zkontrolovat pomocí příkazu:

     ```
     R#show ipv6 interface brief
     ```

2. **IKE politiky a předsdílený klíč**
   - Parametr pro zadání hesla v nešifrované formě je `key 0` a poté následuje samotné heslo.
   - IPv6 adresa zadaná na R1 by měla být 2001:13:13:13::3/64, na R3 2001:13:13:13::1/64. Před samotnými adresami je třeba zadat parametr `ipv6`.
   - Ověření nastavení IKE politik viz obr. 10.2.

```
R1#show crypto isakmp policy

Global IKE policy
Protection suite of priority 5
        encryption algorithm:   AES - Advanced Encryption Standard (128 bit keys).
        hash algorithm:         Secure Hash Standard
        authentication method:  Pre-Shared Key
        Diffie-Hellman group:   #2 (1024 bit)
        lifetime:               86400 seconds, no volume limit
```

Obr. 10.2: Výstup ověření nastavení IKE politik na R1

3. **IPsec transform set a IPsec profil**
   - ESP transformace bude mít šifrování nastaveno pomocí parametru `esp-aes` a autentizaci pomocí `esp-sha-hmac`.
   - Ověření IPsec profilu:

     ```
     R#show crypto ipsec profile
     ```

4. **IPsec IPv6 VTI**
   - Povolení IPv6 na rozhraní tunelu se provádí pomocí příkazu `ipv6 enable`.
   - IPv6 adresa pro zdroj tunelu na R3 je 2001:13:13:13::3, cíl je 2001:13:13:13::1 (na R1 je to opačně).
   - Není nakonfigurované směrování, proto stále není možná konektivita, toto bude konfigurováno v dalším kroku, stejně jako ověření tunelu.
5. **Směrování a ověření**
   - Na R2 je nejjednodušší použít výchozí směr přes R1, jelikož má připojení pouze přes jedno rozhraní do ostatních sítí.

- Obdobně je to také u R3, ale tam chceme, aby veškerá komunikace šla přes tunel, takže vytvoříme výchozí směr a jako další hop nastavíme IPv6 adresu tunelu na straně R1 (13:13:13:13::1).
- Na R1 chceme nakonfigurovat cestu do loopback sítí na směrovačích R2 a R3, cesta do sítě vedoucí přes R3 by opět měla vést přes tunel, jako v minulém případě na R3.
- Nyní by měla být zajištěna celková konektivita, abychom ověřili, že zároveň komunikace jde přes tunel, můžeme pomocí traceroute zkontrolovat např. cestu z R2 na loopback R3 a z R3 na loopback R2. Měli byste vidět, že místo sítě 2001:13:13:13::/64 se jde přes tunel (síť 13:13:13:13::/64).
- Ověření šifrování a dešifrování (počet paketů, algoritmus) lze provést pomocí:

  ```
  R#show crypto engine connection active
  ```

- Ověření ISAKMP SA (zdrojová, cílová adresa tunelu, stav):

  ```
  R#show crypto isakmp sa
  ```

- Ověření detailů spojení přes tunel (stav spojení, doba spojení, počet šifrovaných/dešifrovaných paketů) viz obr. 10.3.

```
R1#show crypto session detail
Crypto session current status

Code: C - IKE Configuration mode, D - Dead Peer Detection
K - Keepalives, N - NAT-traversal, T - cTCP encapsulation
X - IKE Extended Authentication, F - IKE Fragmentation

Interface: Tunnel13
Uptime: 00:37:46
Session status: UP-ACTIVE
Peer: 2001:13:13:13::3 port 500 fvrf: (none) ivrf: (none)
      Phase1_id: 2001:13:13:13::3
      Desc: (none)
  IKEv1 SA: local 2001:13:13:13::1/500
          remote 2001:13:13:13::3/500 Active
          Capabilities:(none) connid:1001 lifetime:23:22:12
  IPSEC FLOW: permit ipv6 ::/0 ::/0
        Active SAs: 2, origin: crypto map
        Inbound:  #pkts dec'ed 8 drop 0 life (KB/Sec) 4534747/1333
        Outbound: #pkts enc'ed 20 drop 2 life (KB/Sec) 4534746/1333
```

Obr. 10.3: Výstup ověření detailu spojení přes tunel 13 a zobrazení šifrování/dešifrování paketů na R1

- VTI je směrovatelné rozhraní, takže provoz, který bychom chtěli šifrovaný, bychom směrovali přes VTI a ostatní přes ethernetové rozhraní.
- Možné řešení by mohlo vypadat tak, že bychom vytvořili na R2 i R3 nové loopbacky. Směrování na R1 a R3 bychom museli uzpůsobit, aby provoz

mezi novými loopbacky neprocházel přes tunel (další hop by místo adresy tunelu byla adresa ethernetového rozhraní mezi R1 a R3). V této situaci bychom si podle počtu šifrovaných paketů na R1 a R3 mohli ověřit, že když provedeme ping mezi loopbacky 0 u R2 a R3, tak provoz bude šifrovaný, což značí provoz mezi pobočkami. Dále bychom si mohli ověřit, že když provedeme ping mezi novými loopbacky na R2 a R3, tak provoz nebude šifrovaný (počet šifrovaných paketů se na R3 a R1 nezvýší), což reprezentuje průchod z pobočky ke zdrojům v Internetu.

6. **Vytvoření zón**
   - Ověření vytvoření zón:

     ```
     R1#show zone security
     ```

7. **Konfigurace class map (mapa třídy)**
   - Ověření mapy třídy (mělo by být vidět, že chceme inspekci protokolu ICMP):

     ```
     R1#show class-map type inspect
     ```

8. **Konfigurace policy map (mapa politik)**
   - Ověření mapy politik viz obr. 10.4.

```
R1#sh policy-map type inspect
  Policy Map type inspect IN-TO-OUT-POLICY
    Class IN-TO-OUT-CLASS
      Inspect
```

Obr. 10.4: Výstup ověření konfigurace mapy politik na R1

9. **Vytvoření párů zón a aplikace politik na ně**
   - Ověření párů zón a politik aplikovaných na nich:

     ```
     R1#show zone-pair security
     ```

10. **Aplikace zón na rozhraní**
    - Je třeba dát VTI do zóny OUTSIDE, jelikož komunikace prochází přes již dříve vytvořený tunel.
    - Ověření zón párů a politik aplikovaných na nich:

      ```
      R1#show zone security
      ```

11. **Ověření funkčnosti firewallu**
    - Podle konfigurace by ping měl fungovat z R2 na R3, ale ne opačně.
    - Činnost firewallu lze ověřit pomocí příkazu:

      ```
      R1#show policy-map type inspect zone-pair session
      ```

- Ping z R2 na R3 funguje právě z principu firewallu s funkcí inspect, což označí zprávu, která jde ven a poté když přijde odpověď na tu zprávu, tak to firewall pozná a povolí průchod.
- Zkuste telnet z R2 na R3, který využívá TCP protokol, nyní by měl být provoz na firewallu zahozen viz obr. 10.5.

```
R1#show policy-map type insp zone-pair sessions

policy exists on zp IN-TO-OUT
 Zone-pair: IN-TO-OUT

  Service-policy inspect : IN-TO-OUT-POLICY

    Class-map: IN-TO-OUT-CLASS (match-all)
      Match: protocol icmp

    Inspect

    Class-map: class-default (match-any)
      Match: any
      Drop
        2 packets, 48 bytes
```

Obr. 10.5: Výstup ověření zahození zprávy telnet firewallem na R1

- Povolte protokol TCP stejně jako ICMP a ověřte, zda je zpráva stále zahazována. Problém nastává ještě s výchozím nastavením map třídy, což je match-all (shoda všech protokolů). My budeme chtít toho chování změnit na match-any (shoda jakéhokoli protokolu), aby stačila jedna shoda protokolu. Nyní už by zprávy neměly být zahazovány, znovu ověřte.

11 ZÁVĚR

V bakalářské práci byl využit nástroj GNS3, který umožňuje simulovat komplexní síťové topologie s využitím mnoha zařízení. V celé práci jsou využity pouze Cisco směrovače, nicméně GNS3 podporuje také např. Cisco ASA, Cisco PIX a Juniper směrovače.

Všechny úlohy jsou navrhnuty s požadavkem na vysokou míru samostatnosti při vypracování, ale nechybí i patřičná nápověda. U každé úlohy je uvedena topologie, pozadí a cíle. Další části už jsou praktického charakteru, část Postup řešení poskytuje důležité informace o konfiguraci krok po kroku, ale dává prostor pro samostatné zamyšlení nad daným problémem. Část Nápověda a odpovědi poskytuje podrobnější nápovědu a ověření správnosti pomocí výstupů ověření ze směrovačů, nechybí i odpovědi na kontrolní otázky.

První úloha zaměřená na MP-BGP (Multiprotocol Border Gateway Protocol) má komplexní charakter v této problematice a pomocí pokročilého řízení směrování na základě BGP atributů poskytuje určitý pohled na fungování Internetu. Další úloha byla navrhnuta kvůli rozlišení druhů tunelů a jejich použití, pokaždé byla nastíněna jedna reálná situace, kde by se mohl použít tunel a probíhalo vybírání správného. Poté proběhla změna v síti, buď kvůli rozšíření sítě nebo změně pohledu na síť (uvnitř jedné lokality a propojení více lokalit). Poslední úloha na téma IPv6 (Internet Protocol version 6) IPsec (Internet Protocol security) VPN (Virtual Private Network) a ZBF (Zone-Based Policy Firewall) ukazovala moderní řešení bezpečnosti a propojení do vzdálené lokální sítě.

Při návrhu poslední úlohy nastalo několik problémů, jak v první části IPsec VPN, tak ve druhé ohledně ZBF. V první části bylo možné nakonfigurovat IPsec VPN s využitím IPv6 pouze pomocí VTI (Virtual Tunnel Interface), což ale nakonec nabídlo nové moderní řešení s několika výhodami. V druhé části musel být vybrán IOS obsahující bezpečnostní prvky, ale opět při použití IPv6 nastal problém. Řešením bylo použití obsáhlého nového IOSu 15.1(4)M na verzi směrovačů 7200, což ale vytěžuje výrazně procesor.

Nasazení IPv6 ukázalo stále ještě problémy v implementaci a odladění chyb, nicméně pro budoucnost Internetu je to nevyhnutelné řešení. V rámci praktické části byly obsaženy postupy právě pro nasazování a přechod na IPv6. Úlohy slouží z těchto důvodů jako doplnění znalostí z Cisco kurzu CCNP a ukázka implementace IPv6. Jednotlivé praktické části budou zveřejněny v anglické verzi na fóru GNS3, popřípadě budou použity v rámci školní výuky.

LITERATURA

[1] *Documentation. GNS3* [online]. © 2007-2015 [cit. 2015-03-28]. Dostupné z URL: <https://community.gns3.com/community/software/documentation>.

[2] TEARE, Diane. *Implementing Cisco IP routing (ROUTE): foundation learning guide : foundation learning for the ROUTE 642-902 exam. Indianapolis: Cisco Press,* c2010, xxix, 945 s. ISBN 978-1-58705-882-0.

[3] SATRAPA, Pavel. *IPv6: internetový protokol verze 6. 3., aktualiz. a dopl. vyd. Praha: CZ.NIC,* c2011, 407 s. CZ.NIC. ISBN 978-80-904248-4-5.

[4] *Co je IPv6. Internet Protokol verze 6* [online]. 2.7.2012 [cit. 2014-12-15]. Dostupné z URL: <https://www.ipv6.cz/Co_je_IPv6>.

[5] *Vlastnosti protokolu. IPv6* [online]. 2.7.2012 [cit. 2015-03-28]. Dostupné z URL: <https://www.ipv6.cz/Vlastnosti_protokolu>.

[6] *BGP Next Hop Propagation. Cisco* [online]. © 2005 [cit. 2014-12-15]. Dostupné z URL: <http://www.cisco.com/c/en/us/td/docs/ios/12_2s/feature/guide/fs_bgpnh.html>.

[7] *IPv6 Multicast Address Space Registry. Internet Assigned Numbers Authority* [online]. 23.2.2015 [cit. 2015-03-28]. Dostupné z URL: <http://www.iana.org/assignments/ipv6-multicast-addresses/ipv6-multicast-addresses.xhtml>.

[8] CONLAN, Patrick J. *Cisco network professional´s advanced internetworking guide. Hoboken: Wiley Publishing,* 2009, xxvii, 854 s. ISBN 978-0-470-38360-5.

[9] *Border Gateway Protocol. Cisco DocWiki* [online]. © 1992-2015 [cit. 2015-03-29]. Dostupné z URL: <http://docwiki.cisco.com/wiki/Border_Gateway_Protocol>.

[10] *Exploring Autonomous System Numbers. Cisco* [online]. © 2005 [cit. 2015-03-29]. Dostupné z URL: <http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_9-1/autonomous_system_numbers.html>.

[11] *Autonomous System (AS) Numbers. Internet Assigned Numbers Authority* [online]. 5.9.2014 [cit. 2015-03-28]. Dostupné z URL: <http://www.iana.org/assignments/as-numbers/as-numbers.xhtml>.

[12] *NAT64 Technology: Connecting IPv6 and IPv4 Networks. Cisco* [online]. 1.4.2012 [cit. 2015-04-09]. Dostupné z URL: <http://www.cisco.com/c/en/us/products/collateral/ios-nx-os-software/enterprise-ipv6-solution/white_paper_c11-676278.html>.

[13] *IPsec Virtual Tunnel Interface. Cisco* [online]. 1.1.2011 [cit. 2015-04-24]. Dostupné z URL: <http://www.cisco.com/c/en/us/td/docs/ios/sec_secure_connectivity/configuration/guide/15_0/sec_secure_connectivity_15_0_book/sec_ipsec_virt_tunnl.html>.

[14] *Zone-Based Policy Firewall Design and Application Guide. Cisco* [online]. 27.12.2010 [cit. 2015-04-24]. Dostupné z URL: <http://www.cisco.com/c/en/us/support/docs/security/ios-firewall/98628-zone-design-guide.html>.

SEZNAM SYMBOLŮ, VELIČIN A ZKRATEK

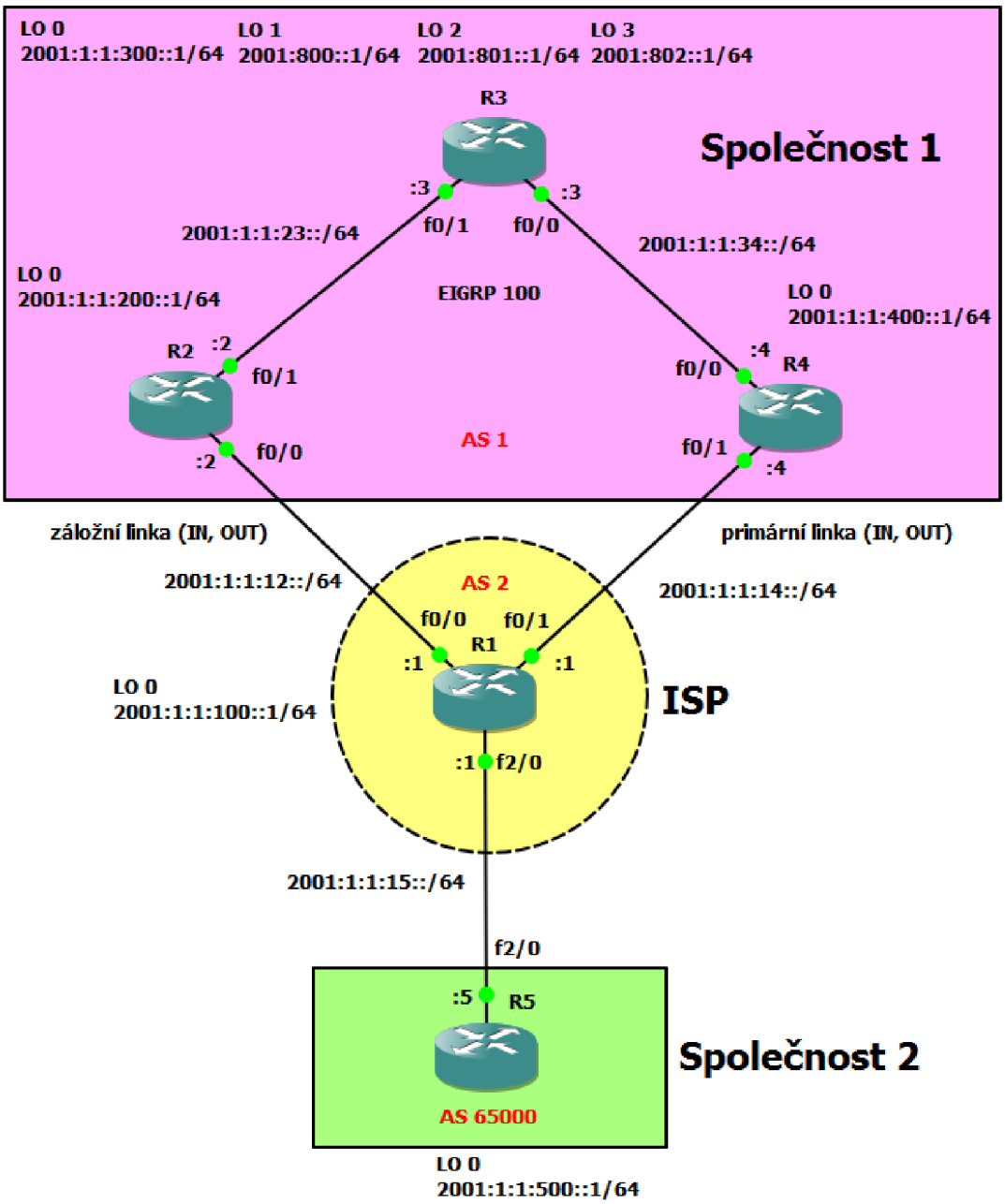
AS	Autonomous System
BGP	Border Gateway Protocol
CBAC	Context-Based Access Control
CLNS	Connectionless Network Service
DMZ	De-Militarized Zone
DNS	Domain Name System
DUAL	Diffusing Update ALgorithm
eBGP	external Border Gateway Protocol
EGP	External Gateway Protocol
EIGRP	Enhanced Interior Gateway Routing Protocol
GRE	Generic Routing Encapsulation
IANA	Internet Assigned Numbers Authority
iBGP	internal Border Gateway Protocol
IGP	Internal Gateway Protocol
IKE	Internet Key Exchange
IP	Internet Protocol
IPsec	Internet Protocol security
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
IPX	Internetwork Packet Exchang
ISAKMP	Internet Security Association and Key Management Protocol
ISATAP	Intra-Site Automatic Tunnel Addressing Protocol
IS-IS	Intermediate System to Intermediate System
ISO/OSI	International Standards Organization / Open Systen Interconnection

ISP	Internet Service Provider
LAN	Local Area Network
MP-BGP	Multiprotocol Border Gateway Protocol
MPLS	Multiprotocol Label Switching
MTU	Maximum Transmission Unit
NAT	Network Address Translation
NTP	Network Time Protocol
OSPF	Open Shortest Path First
RIP	Routing Information Protocol
RTP	Reliable Transport Protocol
SSL	Secure Sockets Layer
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
VLSM	Variable Length Subnet Mask
VPN	Virtual Private Network
VTI	Virtual Tunnel Interface
ZBF	Zone-Based Policy Firewall

SEZNAM PŘÍLOH

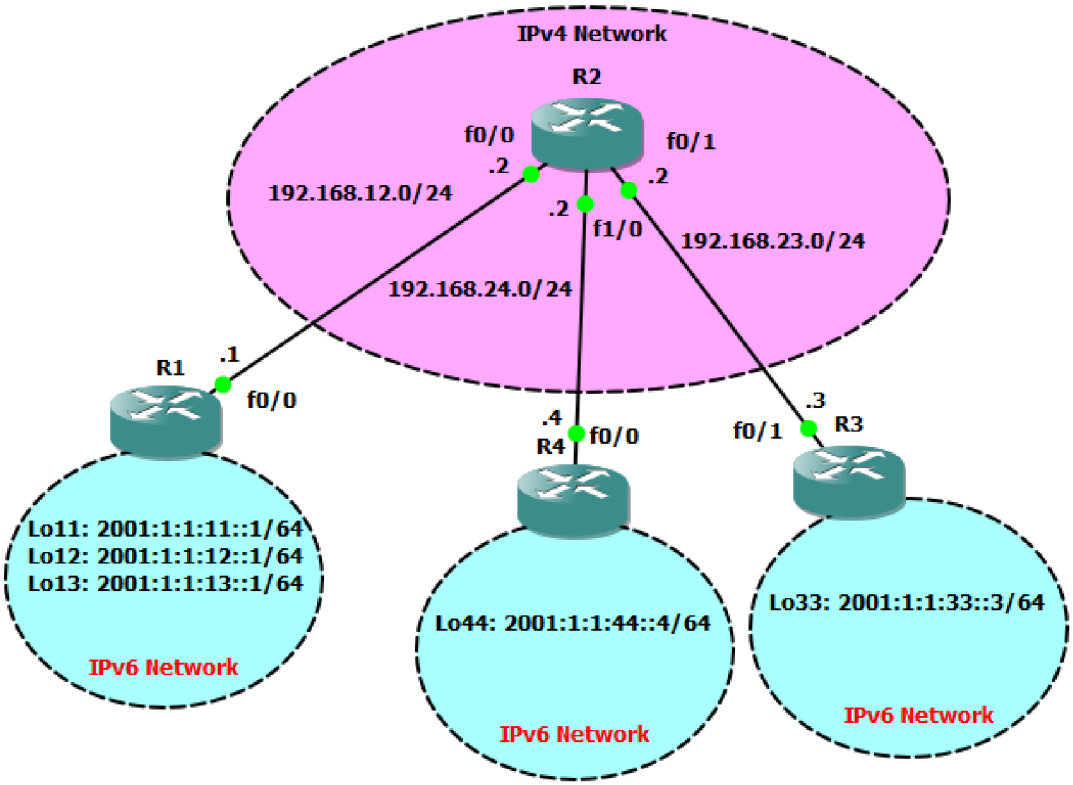
A OBRÁZKY

A.1 Topologie úloha MP-BGP



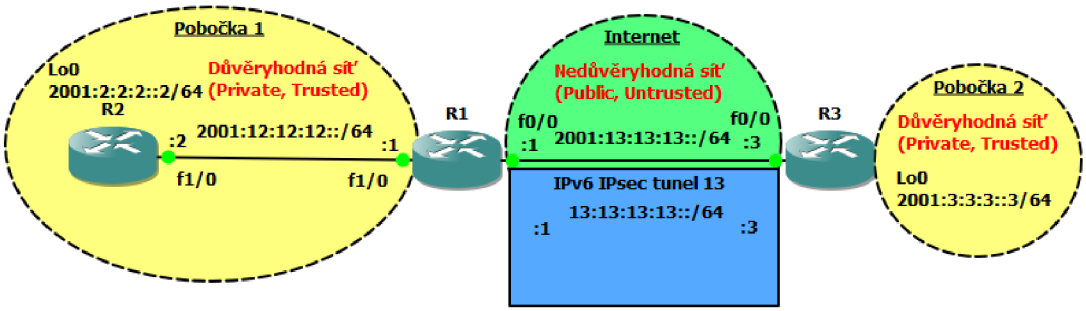
Obr. A.1: Topologie úloha MP-BGP

A.2 Topologie úloha IPv6 tunely



Obr. A.2: Topologie úloha IPv6 tunely

A.3 Topologie úloha IPsec VPN a Zone Based Firewall



Obr. A.3: Topologie úloha IPsec VPN a Zone Based Firewall

B KONFIGURACE ÚLOH

Zde jsou uvedeny použité příkazy v každé úloze ve tvaru, který umožňuje přímo zkopírovat text a vložit jako konfiguraci. Postupně je přiložena konfigurace potřebná pro každý krok úlohy.

B.1 Úloha MP-BGP

1. **Zapojení topologie a nastavení IPv6 adres na rozhraní**

```
R1:
int f 0/1
ipv6 address 2001:1:1:14::1/64
no shut
int f 0/0
ipv6 address 2001:1:1:12::1/64
no shut
int f 2/0
ipv6 address 2001:1:1:15::1/64
no shut
int lo0
ipv6 address 2001:1:1:100::1/64

R2:
int f 0/1
ipv6 address 2001:1:1:23::2/64
no shut
int f 0/0
ipv6 address 2001:1:1:12::2/64
no shut
int lo0
ipv6 address 2001:1:1:200::1/64

R3:
int f 0/1
ipv6 address 2001:1:1:23::3/64
no shut
int f 0/0
ipv6 address 2001:1:1:34::3/64
```

```
no shut
int lo0
ipv6 address 2001:1:1:300::1/64
int lo1
ipv6 address 2001:800::1/64
int lo2
ipv6 address 2001:801::1/64
int lo3
ipv6 address 2001:802::1/64

R4:
int f 0/1
ipv6 address 2001:1:1:14::4/64
no shut
int f 0/0
ipv6 address 2001:1:1:34::4/64
no shut
int lo0
ipv6 address 2001:1:1:400::1/64

R5:
int f 2/0
ipv6 address 2001:1:1:15::5/64
no shut
int lo0
ipv6 address 2001:1:1:500::1/64
```

2. **Povolení EIGRPv6 100 v rámci AS 1**

```
R2:
ipv6 unicast-routing
ipv6 router eigrp 100
router-id 2.2.2.2
no shutdown
exit
int lo0
ipv6 eigrp 100
int f 0/1
ipv6 eigrp 100
```

```
R3:
ipv6 unicast-routing
ipv6 router eigrp 100
router-id 3.3.3.3
no shutdown
exit
int lo0
ipv6 eigrp 100
int lo1
ipv6 eigrp 100
int lo2
ipv6 eigrp 100
int lo3
ipv6 eigrp 100
int f 0/1
ipv6 eigrp 100
int f 0/0
ipv6 eigrp 100

R4:
ipv6 unicast-routing
ipv6 router eigrp 100
router-id 4.4.4.4
no shutdown
exit
int lo0
ipv6 eigrp 100
int f 0/0
ipv6 eigrp 100
```

3. **Konfigurace iBGP v AS 1**

```
R2:
router bgp 1
bgp router-id 2.2.2.2
address-family ipv6 unicast
neighbor 2001:1:1:300::1 remote-as 1
neighbor 2001:1:1:300::1 update-source lo0
neighbor 2001:1:1:300::1 activate
network 2001:1:1:200::/64
```

```
R3:
router bgp 1
bgp router-id 3.3.3.3
neighbor comp1 peer-group
neighbor comp1 remote-as 1
neighbor comp1 update-source Loopback0
neighbor 2001:1:1:200::1 peer-group comp1
neighbor 2001:1:1:400::1 peer-group comp1
address-family ipv6 unicast
neighbor 2001:1:1:200::1 activate
neighbor 2001:1:1:400::1 activate
network 2001:1:1:300::/64
network 2001:800::/64
network 2001:801::/64
network 2001:802::/64

R4:
router bgp 1
bgp router-id 4.4.4.4
address-family ipv6 unicast
neighbor 2001:1:1:300::1 remote-as 1
neighbor 2001:1:1:300::1 update-source lo0
neighbor 2001:1:1:300::1 activate
network 2001:1:1:400::/64
```

Route-reflector

```
R3:
Router bgp 1
Address-family ipv6 unicast
neighbor comp1 route-reflector-client
```

4. **Konfigurace eBGP**

```
R1:
ipv6 unicast-routing
router bgp 2
bgp router-id 1.1.1.1
neighbor comp1 peer-group
```

```
neighbor comp1 remote-as 1
neighbor comp1 ebgp-multihop 2
neighbor comp1 update-source Loopback0
neighbor 2001:1:1:400::1 peer-group comp1
neighbor 2001:1:1:200::1 peer-group comp1
neighbor 2001:1:1:15::5 remote-as 65000
address-family ipv6 unicast
neighbor 2001:1:1:15::5 activate
neighbor 2001:1:1:400::1 activate
neighbor 2001:1:1:200::1 activate
network 2001:1:1:100::/64

R2:
router bgp 1
neighbor 2001:1:1:100::1 remote-as 2
neighbor 2001:1:1:100::1 update-source Loopback0
neighbor 2001:1:1:100::1 ebgp-multihop 2
address-family ipv6 unicast
neighbor 2001:1:1:100::1 activate
network 2001:1:1:200::/64

R4:
router bgp 1
neighbor 2001:1:1:100::1 remote-as 2
neighbor 2001:1:1:100::1 update-source Loopback0
neighbor 2001:1:1:100::1 ebgp-multihop 2
address-family ipv6 unicast
neighbor 2001:1:1:100::1 activate
network 2001:1:1:400::/64

R5:
ipv6 unicast-routing
router bgp 65000
bgp router-id 5.5.5.5
neighbor 2001:1:1:15::1 remote-as 2
address-family ipv6 unicast
neighbor 2001:1:1:15::1 activate
network 2001:1:1:500::/64
```

Statické cesty

```
R1:
ipv6 route 2001:1:1:200::1/128 2001:1:1:12::2
ipv6 route 2001:1:1:400::1/128 2001:1:1:14::4

R4:
ipv6 route 2001:1:1:100::1/128 2001:1:1:14::1

R2:
ipv6 route 2001:1:1:100::1/128 2001:1:1:12::1
```

5. **Ověřte funkčnost pomocí PING v celé topologii**

```
R3:
ping 2001:1:1:500::1 source lo0
```

6. **Změna Next_hopu**

```
R2:
route-map NEXTHOP
set ipv6 next-hop 2001:1:1:200::1
exit
router bgp 1
address-family ipv6 uni
neighbor 2001:1:1:300::1 route-map NEXTHOP out

R4:
route-map NEXTHOP
set ipv6 next-hop 2001:1:1:400::1
exit
router bgp 1
address-family ipv6 uni
neighbor 2001:1:1:300::1 route-map NEXTHOP out
```

7. **Sumarizace loopbacku 1 - 3 na R3 a posílání pouze sumární cesty v BGP**

```
R3:
Router bgp 1
Address-family ipv6 unicast
aggregate-address 2001:800::/30 summary-only
```

8. **Privátní AS**

```
R1:
router bgp 2
address-family ipv6 unicast
neighbor comp1 remove-private-as
```

9. **Nastavení preferované cesty z R3 mimo AS 1 a opačně**

LOCAL_PREF

```
R2:
route-map secondary_loc permit 10
set local-preference 125
exit
router bgp 1
address-family ipv6 unicast
neighbor 2001:1:1:100::1 route-map secondary_loc in

R4:
route-map primary_loc permit 10
set local-preference 150
exit
router bgp 1
address-family ipv6 unicast
neighbor 2001:1:1:100::1 route-map primary_loc in
```

MED

```
R2:
route-map secondary_med permit 10
set metric 75
exit
router bgp 1
address-family ipv6 unicast
neighbor 2001:1:1:100::1 route-map secondary_med out

R4:
route-map primary_med permit 10
set metric 50
exit
```

```
router bgp 1
address-family ipv6 unicast
neighbor 2001:1:1:100::1 route-map primary_med out
```

B.2 Úloha IPv6 tunely

1. **Zapojení topologie a nastavení IPv4 a IPv6 adres na rozhraní**

   IPv4 adresy

```
R1:
int f 0/0
ip add 192.168.12.1 255.255.255.0
no shut

R2:
int f 0/0
ip add 192.168.12.2 255.255.255.0
no shut
int f 0/1
ip add 192.168.23.2 255.255.255.0
no shut
int f1/0
ip add 192.168.24.2 255.255.255.0
no shut

R3:
int f 0/1
ip add 192.168.23.3 255.255.255.0
no shut

R4:
int f0/0
ip add 192.168.24.4 255.255.255.0
no shut
```

   IPv6 adresy

```
R1:
int lo11
ipv add 2001:1:1:11::1/64
int lo12
ipv add 2001:1:1:12::1/64
```

```
int lo13
ipv add 2001:1:1:13::1/64

R3:
int lo33
ipv add 2001:1:1:33::3/64

R4:
int lo44
ipv add 2001:1:1:44::4/64
```

2. **Situace 1**
3. **Manuální tunel 13 mezi R1 a R3**

```
R1:
interface tunnel 13
ipv6 address 2001:13:13:13::1/64
tunnel source f0/0
tunnel destination 192.168.23.3
tunnel mode ipv6ip

R3:
interface tunnel 13
ipv6 address 2001:13:13:13::3/64
tunnel source f0/1
tunnel destination 192.168.12.1
tunnel mode ipv6ip
```

Směrování mezi R1 a R3

```
R1:
ip route 192.168.23.0 255.255.255.0 f0/0

R3:
ip route 192.168.12.0 255.255.255.0 f0/1
```

4. **Směrování: EIGRP 1**

```
R1:
ipv6 unicast-routing
ipv6 router eigrp 1
```

```
router-id 1.1.1.1
no shut
int tunnel 13
ipv6 eigrp 1
int lo11
ipv6 eigrp 1
int lo12
ipv6 eigrp 1
int lo13
ipv6 eigrp 1

R3:
ipv6 unicast-routing
ipv6 router eigrp 1
router-id 3.3.3.3
no shut
int tunnel 13
ipv6 eigrp 1
int lo33
ipv6 eigrp 1
```

5. **Situace 2**
6. **ISATAP tunel 3 mezi R1, R4 a R3**

```
R1:
interface tunnel 3
ipv add 2001:33:33:33::/64 eui-64
tunnel source f0/0
tunnel mode ipv6ip isatap

R3:
interface tunnel 3
ipv add 2001:33:33:33::/64 eui-64
tunnel source f0/1
tunnel mode ipv6ip isatap
```

```
R4:
interface tunnel 3
ipv add 2001:33:33:33::/64 eui-64
tunnel source f0/0
tunnel mode ipv6ip isatap
```

Směrování mezi R3 a R4

```
R4:
ip route 192.168.23.0 255.255.255.0 f0/0

R3:
ip route 192.168.24.0 255.255.255.0 f0/1
```

Zrušení Manuálního tunelu

```
R1:
no interface tunnel13

R3:
no interface tunnel13
```

7. **Směrování**

```
R1:
ipv6 route 2001:1:1:44::/64 tunnel3 2001:33:33:33:0:5EFE:C0A8:1804
ipv6 route 2001:1:1:33::/64 tunnel3 2001:33:33:33:0:5EFE:C0A8:1703
ip route 192.168.24.0 255.255.255.0 192.168.12.2

R4:
ipv6 route 2001:1:1:33::/64 tunnel3 2001:33:33:33:0:5EFE:C0A8:1703
ip route 192.168.12.0 255.255.255.0 192.168.24.2
sumarizovaná:
ipv6 route 2001:1:1:10::/62 tunnel3 2001:33:33:33:0:5EFE:C0A8:C01

R3:
ipv6 route 2001:1:1:44::/64 tunnel3 2001:33:33:33:0:5EFE:C0A8:1804
sumarizovaná:
ipv6 route 2001:1:1:10::/62 tunnel3 2001:33:33:33:0:5EFE:C0A8:C01
```

8. **Situace 3**
9. **GRE tunel 13 mezi R1 a R3**

```
R1:
int tunnel 13
ipv6 add 2001:13:13:13::1/64
tunnel source f0/0
tunnel dest 192.168.23.3

R3:
int tunnel 13
ipv6 add 2001:13:13:13::3/64
tunnel source f0/1
tunnel dest 192.168.12.1
```

Odstranění ISATAP tunelu

```
R1:
no Int tun 3

R3:
no Int tun 3

R4:
no Int tun 3
```

10. **Směrování**

```
R1:
int tunnel 13
ipv eigrp 1

R3:
int tunnel 13
ipv eigrp 1
```

11. **Situace 4**
12. **6to4 tunel 3 mezi R1, R4 a R3**

```
R1:
interface tunnel 3
ipv add 2002:c0a8:0c01:1::1/64
```

```
tunnel source f0/0
tunnel mode ipv6ip 6to4

R3:
interface tunnel 3
ipv add 2002:c0a8:1703:3::3/64
tunnel source f0/1
tunnel mode ipv6ip 6to4

R4:
interface tunnel 3
ipv add 2002:c0a8:1804:4::4/64
tunnel source f0/0
tunnel mode ipv6ip 6to4
```

Odstranění GRE tunelu

```
R1:
no interface tunnel13

R3:
no interface tunnel13
```

13. **Směrování**

```
R1:
ipv6 route 2002::/16 tunnel 3
ipv6 route 2001:1:1:44::/64 2002:c0a8:1804:4::4
ipv6 route 2001:1:1:33::/64 2002:c0a8:1703:3::3
exit

R3:
ipv6 route 2002::/16 tunnel 3
ipv6 route 2001:1:1:44::/64 2002:c0a8:1804:4::4
ipv6 route 2001:1:1:10::/62 2002:c0a8:0c01:1::1

R4:
ipv6 route 2002::/16 tunnel 3
ipv6 route 2001:1:1:10::/62 2002:c0a8:0c01:1::1
ipv6 route 2001:1:1:33::/64 2002:c0a8:1703:3::3
```

B.3 Úloha IPsec VPN a ZBF

1. **Zapojení topologie a nastavení IPv6 adres na rozhraní**

```
R1:
interface f 1/0
ipv6 address 2001:12:12:12::1/64
no shut
interface f 0/0
ipv6 address 2001:13:13:13::1/64
no shut

R2:
interface f 1/0
ipv6 address 2001:12:12:12::2/64
no shut
interface lo0
ipv6 address 2001:2:2:2::2/64

R3:
interface f 0/0
ipv6 address 2001:13:13:13::3/64
no shut
interface lo0
ipv6 address 2001:3:3:3::3/64
```

2. **IKE politiky a předsdílený klíč**

```
R1 a R3:
crypto isakmp policy 5
encryption aes
group 2
authentication pre-share

R1:
crypto isakmp key 0 key123 address ipv6 2001:13:13:13::3/64

R3:
crypto isakmp key 0 key123 address ipv6 2001:13:13:13::1/64
```

3. **IPsec transform set a IPsec profil**

```
R1 a R3:
crypto ipsec transform-set ipsec_transf esp-aes esp-sha-hmac
mode tunnel
exit
crypto ipsec profile ipsec_prof
set transform-set ipsec_transf
```

4. **IPsec IPv6 VTI**

```
R1:
interface tunnel 13
ipv6 enable
ipv6 address 13:13:13:13::1/64
tunnel source 2001:13:13:13::1
tunnel destination 2001:13:13:13::3
tunnel mode ipsec ipv6
tunnel protection ipsec profile ipsec_prof

R3:
interface tunnel 13
ipv6 enable
ipv6 address 13:13:13:13::3/64
tunnel source 2001:13:13:13::3
tunnel destination 2001:13:13:13::1
tunnel mode ipsec ipv6
tunnel protection ipsec profile ipsec_prof
```

5. **Směrování a ověření**

```
R1:
ipv6 unicast-routing
ipv6 route 2001:3:3:3::/64 13:13:13:13::3
ipv6 route 2001:2:2:2::/64 2001:12:12:12::2

R2:
ipv6 unicast-routing
ipv6 route 0::/0 2001:12:12:12::1
```

```
R3:
ipv6 unicast-routing
ipv6 route 0::/0 13:13:13:13::1
```

6. **Vytvoření zón**

```
R1:
zone security INSIDE
zone security OUTSIDE
```

7. **Konfigurace class map (mapa třídy)**

```
R1:
class-map type inspect match-any IN-TO-OUT-CLASS
match protocol icmp
```

8. **Konfigurace policy map (mapa politik)**

```
R1:
policy-map type inspect IN-TO-OUT-POLICY
class type inspect IN-TO-OUT-CLASS
inspect
exit
class class-default
drop
```

9. **Vytvoření párů zón a aplikace politik na ně**

```
R1:
zone-pair security IN-TO-OUT source INSIDE destination OUTSIDE
service-policy type inspect IN-TO-OUT-POLICY
```

10. **Aplikace zón na rozhraní**

```
R1:
interface tunnel 13
zone-member security OUTSIDE
interface f1/0
zone-member security INSIDE
```