UNIVERZITA PARDUBICE
Fakulta elektrotechniky a informatiky

Analýza principů IGP a EGP routovacích protokolů

Tomáš Kmoníček

Bakalářská práce
2013

Univerzita Pardubice
Fakulta elektrotechniky a informatiky
Akademický rok: **2012/2013**

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Tomáš Kmoníček**
Osobní číslo:	**I10087**
Studijní program:	**B2646 Informační technologie**
Studijní obor:	**Informační technologie**
Název tématu:	**Analýza principů IGP a EGP routovacích protokolů**
Zadávající katedra:	**Katedra informačních technologií**

Zásady pro vypracování:

Cílem bakalářské práce je osvětlení principů EGP protokolů v porovnání s IGP. Autor obecně popíše, principy a uplatnění EGP a IGP protokolů a jejich nejznámějších zástupců. Dále budou shrnuty hlavní rozdíly v chování IGP a EGP protokolů a prakticky ukázány možnosti jejich spolupráce a konfigurace v laboratorních podmínkách. Podrobné konfigurace včetně podrobného popisu budou obsaženy v příloze práce.

Rozsah grafických prací:

Rozsah pracovní zprávy:

Forma zpracování bakalářské práce: **tištěná/elektronická**

Seznam odborné literatury:

ZHANG, Randy a Micah BARTELL. BGP design and implementation. Indianapolis, IN: Cisco Press, c2004, xxv, 638 p. Cisco Press networking technology series. ISBN 15-870-5109-5.
PARKHURST, William R. Cisco OSPF Command and Configuration Handbook (paperback). Indianapolis: Cisco Press, 2008. ISBN 978-158-7055-40

Vedoucí bakalářské práce: **Mgr. Josef Horálek**
Katedra softwarových technologií

Datum zadání bakalářské práce: **21. prosince 2012**
Termín odevzdání bakalářské práce: **10. května 2013**

Univerzita Pardubice Česká republika

L.S.

prof. Ing. Simeon Karamazov, Dr.
děkan

Ing. Lukáš Čegan, Ph.D.
vedoucí katedry

V Pardubicích dne 29. března 2013

Prohlášení autora

Prohlašuji, že jsem tuto práci vypracoval samostatně. Veškeré literární prameny a informace, které jsem v práci využil, jsou uvedeny v seznamu použité literatury.

Byl jsem seznámen s tím, že se na moji práci vztahují práva a povinnosti vyplývající ze zákona č. 121/2000 Sb., autorský zákon, zejména se skutečností, že Univerzita Pardubice má právo na uzavření licenční smlouvy o užití této práce jako školního díla podle § 60 odst. 1 autorského zákona, a s tím, že pokud dojde k užití této práce mnou nebo bude poskytnuta licence o užití jinému subjektu, je Univerzita Pardubice oprávněna ode mne požadovat přiměřený příspěvek na úhradu nákladů, které na vytvoření díla vynaložila, a to podle okolností až do jejich skutečné výše.

Souhlasím s prezenčním zpřístupněním své práce v Univerzitní knihovně.

V Pardubicích dne 18. 4. 2013 Tomáš Kmoníček

Poděkování

Děkuji vedoucímu bakalářské práce Mgr. Josefu Horálkovi za veškeré rady, věcné připomínky a pomoc při zpracování této práce.

Anotace

Cílem bakalářské práce je osvětlení principů EGP protokolů v porovnání s IGP protokoly. V práci jsou obecně popsány principy a uplatnění IGP a EGP protokolů a jejich nejznámějších zástupců. Dále jsou shrnuty hlavní rozdíly v chování IGP a EGP protokolů a prakticky ukázány možnosti jejich spolupráce a konfigurace v laboratorních podmínkách.

Klíčová slova

EGP, IGP, BGP, OSPF, počítačové sítě, směrovač, přepínač

Title

The Analysis of IGP and EGP Routing Protocols Principles.

Annotation

The aim of this work is explanation of EGP principles against IGP principles. There are described the general principles and application of IGP and EGP and their most popular protocols. In this work are summarized major differences in behavior of IGP and EGP protocols and practically shown their cooperation and configuration in laboratory conditions.

Keywords

EGP, IGP, BGP, OSPF, computer network, router, switch

Obsah

Seznam zkratek

ABR	Area Border Router
ACL	Access List
AS	Autonomous System
ASBR	Autonomous System Boundary Router
ASN	Autonomous System Number
BBN	Bolt, Beranek and Newman
BDR	Backup Designated Router
BGP	Border Gateway Protocol
CCNA	Cisco Certified Network Associate
DD	Database Description
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
DR	Designated Router
DUAL	Diffusing Update Algorithm
eBGP	External BGP
EGP	Exterior Gateway Protocol
EGP	Exterior Gateway Protocols
IANA	Internet Assigned Numbers Authority
iBGP	Internal BGP
ICANN	Internet Corporation for Assigned Names and Numbers
IETF	Internet Engineering Task Force
IGP	Interior Gateway Protocol
IOS	Internetwork Operating System
IP	Internet Protocol
ISP	Internet Service Provider
LAN	Local Area Network
LSA	Link-State Advertisement
LSAck	Link-State Acknowledgment
LSDB	Link-State Database
LSID	Link-State Identifier
LSR	Link-State Request
LSU	Link-State Update
MED	Multi Exit Discriminator
MP-BGP	Multiprotocol BGP
MPLS VPN	Multiprotocol Label Switching Virtual Private Networks
MTU	Maximum Transmission Unit
NBMA	Non-broadcast Multiple Access
NSSA	Not so Stubby Area
OSI	Open Systems Interconnection
OSPF	Open Shortest Path First

PA	Path Attributes
PAT	Port Address Translation
RFC	Request for Comments
RID	Router ID
RIR	Regional Internet Registries
TCP	Transmission Control Protocol
TCP/IP	Transmission Control Protocol / Internet Protocol
TTL	Time-To-Live
VLAN	Virtual Local Area Network
WAN	Wide Area Network

Seznam obrázků

Seznam tabulek

Úvod

Internet je decentralizovaný systém počítačových sítí, ve kterém neexistuje jednotná správa. Nejen z tohoto důvodu není směrování dat v Internetu konzistentní. V průběhu dosavadního rozvoje Internetu vznikly různé protokoly, které definují směrování dat na základě různých algoritmů a v průběhu let jsou postupně vylepšovány.

Protokoly se dělí na dvě základní skupiny: vnitřní směrovací protokoly a vnější směrovací protokoly. Z názvů vyplývá základní rozdíl protokolů v účelu směrování dat. Dříve se tyto protokoly lišily ve směrování dat s ohledem na stranu internetové brány, ke které byla síť připojena. V dnešní době se význam přenesl na rozdíl ve směrování vůči autonomním systémům. Vnitřní směrovací protokoly směrují data například uvnitř jedné velké společnosti, která má svůj autonomní systém. Vnější směrovací protokoly data směrují v Internetu mezi různými autonomními systémy a tím zajišťují směrování dat mezi kontinenty, státy a společnostmi.

Cílem bakalářské práce je vysvětlení principů vnějších směrovacích protokolů v porovnání s principy vnitřních směrovacích protokolů a zobrazení jejich spolupráce. Předpokladem pro studium práce je znalost problematiky směrování dat na úrovni kurzů CCNA Exploration 1-4 společnosti Cisco, případně studium zdrojů (PÁV, 2011) a (LAMMLE, 2000). Problematika vnitřních a vnějších směrovacích protokolů je od sebe velmi často oddělována a uvedené zdroje popisují pouze vnitřní směrovací protokoly. Bakalářská práce se zabývá rozšířením znalostí o vnitřních směrovacích protokolech, základy vnějších směrovacích protokolů a hlavně jejich spoluprací, protože pro směrování dat v Internetu je potřebné využití obou typů protokolů a vzájemné předávání informací mezi nimi.

První kapitola práce je věnována struktuře Internetu, autonomním systémům a základnímu rozdělení směrovacích protokolů. Ve druhé kapitole jsou představeny vnitřní směrovací protokoly včetně jejich dalšího rozdělení podle specifických vlastností. Třetí kapitola podrobně popisuje konkrétní vnitřní směrovací protokol OSPF (Open Shortest Path First), který byl pro praktické představení vybrán z důvodů velkého rozšíření ve světě, nezávislosti na výrobci použitého směrovače a velkých možností rozšiřitelnosti protokolu.

V následujících kapitolách jsou uvedeny informace a nastínění konfigurace vnějších směrovacích protokolů, zvláště pak BGP (Border Gateway Protocol), který je dnes jediným používaným zástupcem tohoto typu protokolů. Šestá kapitola práce je věnována výměně cest mezi různými protokoly, především mezi OSPF a BGP. Poslední kapitola práce představuje praktické nasazení protokolů v rámci případové studie velké společnosti, která kromě komunikace mezi jednotlivými pobočkami společnosti vyžaduje i efektivní směrování dat z centrály společnosti do Internetu. Kompletní konfigurace směrovačů použitá v případové studii je přiložena v přílohách.

Veškeré uvedené příkazy a konfigurace uvedené v bakalářské práci jsou použitelné v operačním systému Cisco IOS (Internetwork Operating System).

1 Struktura Internetu

Podle zdrojů (KVÍTEK, 2005) a (ZELENÝ, a další, 2004) je Internet systém mnoha propojených počítačových sítí, které jsou vytvořeny lidmi na celé Zemi. Počítačová síť je systém různých zařízení (např. osobních počítačů, mobilních telefonů, tiskáren) a jejich vzájemných propojení různými komunikačními linkami, které mezi zařízeními umožňují přenos informací. Internet v sobě tedy zahrnuje mnoho velkých, středních i malých počítačových sítí a pomocí linek a zařízení zajišťuje přenos dat mezi všemi koncovými zařízeními v Internetu. Mezi zařízení, která jsou v Internetu používána pro přenos dat mezi koncovými zařízeními, patří brány, směrovače a servery:

- Brány jsou počítače, které umožňují propojení dvou různých počítačových sítí.
- Směrovače jsou specializované počítače, které pro zasílaná data hledají a určují cestu Internetem. Řečeno jinými slovy, posílají informace ze zařízení A do zařízení B cestou, kterou sami zvolí na základě vlastních dat.
- Servery jsou počítače, které ostatním poskytují určité služby a mohou být mezičlánkem mezi počítačovou sítí a Internetem. V rámci jedné počítačové sítě mohou servery poskytovat například zabezpečení proti útokům z jiných počítačových sítí (firewall), přidělování IP (Internet Protocol) adres nebo překlad soukromých IP adres na veřejné.

Internet je decentralizovaný systém, všechna zařízení jsou si mezi sebou rovna a mohou být připojena k velkému počtu jiných zařízení. Při selhání určité linky bývá tedy cíl dostupný i jinými cestami a Internet je díky tomu spolehlivější. Přenos informací mezi zařízeními v Internetu probíhá na základě pravidel definovaných standardními postupy a jazyky, které se nazývají komunikační protokoly. Každá informační služba používá jiný protokol. V Internetu je používáno kolem 100 různých protokolů, které jsou sdruženy v množině protokolů TCP/IP (Transmission Control Protocol / Internet Protocol). (KVÍTEK, 2005)

Zdroj (KOZIEROK, 2005) uvádí, že v historických začátcích Internetu tvořily jeho páteř centrální směrovače (core gateways), které znaly kompletní topologii Internetu a byly centrálně spravovány jednou společností (Bolt, Beranek and Newman – BBN). To se postupem času, díky nárůstu počtu připojených zařízení k Internetu, stalo neudržitelné. V dnešní době není možné, aby směrovače znaly adresy všech sítí v Internetu a přetěžovaly Internet výměnou informací o těchto sítích. Postupem času vznikly autonomní systémy (Autonomous System – AS) a směrování dat v Internetu se značně změnilo.

1.1 Autonomní systém

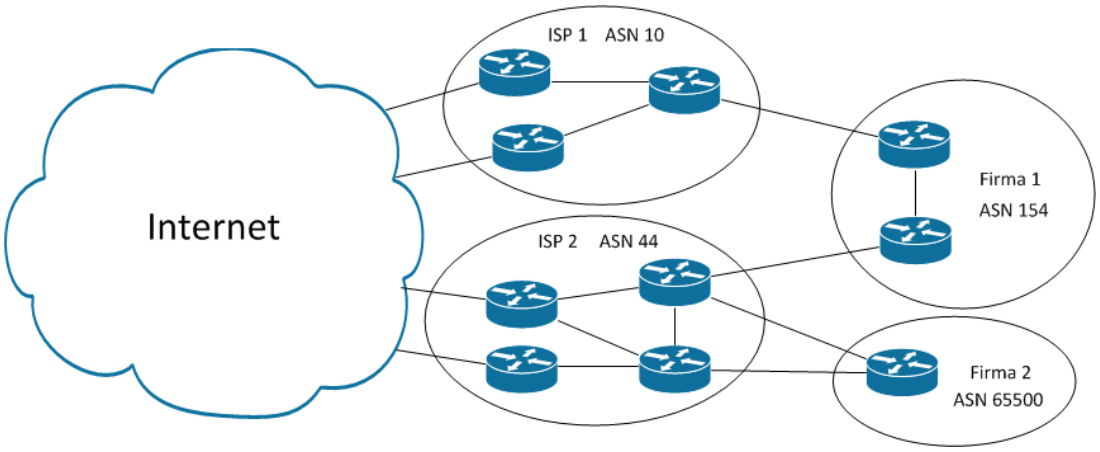
AS je skupina sítí a směrovačů, které jsou společně spravovány. V praxi bývá AS skupina sítí jednoho poskytovatele Internetu (Internet Service Provider – ISP) nebo jedné velké firmy. Každý AS do Internetu posílá pouze svoje základní údaje a adresy, které je možné

dále sumarizovat a tím se počet informací na páteřních směrovačích Internetu značně snižuje.

Z těchto důvodů jsou AS velmi důležité a z pohledu směrování dat v Internetu se dají považovat za základní stavební prvky Internetu.

Zdroj (MAKATI, 2012) vysvětluje, že každý AS má své číslo (Autonomous System Number – ASN). Tato čísla jsou spravována a přidělována organizací IANA (Internet Assigned Numbers Authority (Internet Assigned Numbers Authority, 2013)) pomocí jejich regionálních matrik (Regional Internet Registries – RIR). Původně byla přidělována 16 bitová čísla (rozsah 0-65536), která ale přestávají stačit a dnes se již přidělují 32 bitová čísla. Pokud není potřeba veřejné ASN, je doporučováno použít číslo ze soukromého rozsahu 64512-65534. Organizace IANA je oddělení neziskové organizace ICANN (Internet Corporation for Assigned Names and Numbers (Internet Corporation for Assigned Names and Numbers, 2013)) a kromě přidělování ASN se stará například také o přidělování IP adres, spravuje DNS (Domain Name System) servery nejvyšší úrovně a je zodpovědná za udržování velkého množství Internetových protokolů.

Příklad použití AS je na následujícím obrázku (Obrázek 1), kde je zobrazeno připojení dvou velkých firem přes dva různé ISP. Malé firmy ve většině případů vlastní AS nepotřebují, u velkých firem vlastní AS pomáhá lepšímu výběru cest pro data do Internetu i zpět. Firma 2 je připojena pouze k jednomu ISP, proto je doporučeno použití ASN ze soukromého rozsahu. Každý větší ISP by měl mít do Internetu více různých připojení, proto je u velkých ISP vlastní AS nutností.



Obrázek 1 - Příklad použití AS

1.2 Dělení protokolů na IGP a EGP

Směrovače vybírají cestu pro přeposílání dat na základě informací ze směrovací tabulky, kterou si sami vytvářejí. Data si do směrovací tabulky ukládají podle informací o cestách přijatých od ostatních směrovačů. Komunikace mezi směrovači a výběr cest probíhá pomocí různých směrovacích protokolů. Ty se liší podle obsáhlosti vyměňovaných

informací a podle toho, jaké druhy informací jsou použity k výběru konkrétní cesty. Obecně se protokoly dělí na dvě skupiny podle způsobu využití vypočítaných cest:

- Vnitřní směrovací protokoly (Interior Gateway Protocols – IGP) – jsou používány pro směrování dat uvnitř jednoho AS. IGP se dokáží naučit informace o všech sítích v AS a zasílat data k cílovému zařízení nejlepší cestou. Na směrování dat mezi více AS jsou ale IGP nevhodné. Podrobný popis těchto protokolů je uveden v kapitolách 2 a 3.
- Vnější směrovací protokoly (Exterior Gateway Protocols – EGP) – jsou využity při směrování dat mezi různými AS. Jejich úkolem je směrovat data na okraj AS, ve kterém se nachází cílové zařízení. Přímo k cílovému zařízení data následně směruje vybraný IGP. Podrobný popis EGP se nachází v kapitolách 4 a 5.

2 Představení IGP

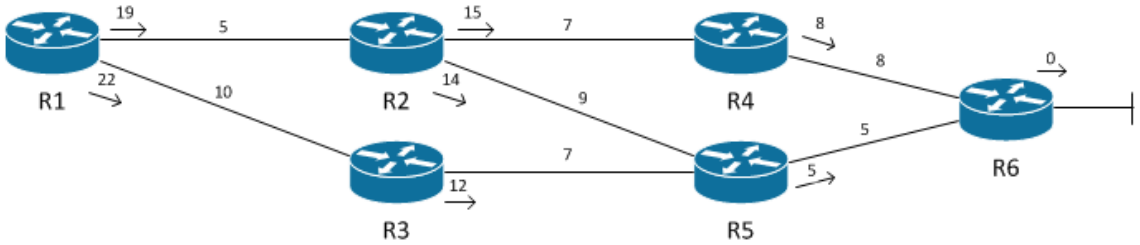
Vnitřní směrovací protokoly jsou určeny ke směrování toku dat mezi různými sítěmi. Vždy ale pouze v rámci jednoho AS. Je možné zároveň používat různé IGP ve stejné části, případně v různých částech AS.

Směrování dat pomocí IGP je založeno na metrice, která představuje vzdálenost do cílové sítě nebo relativní rychlost, během které by se data do cílové sítě měla přenést. Směrovače v závislosti na použitém protokolu vybírají nejlepší cestu do cílové sítě a pakety odesílají nejbližšímu směrovači na této cestě. Směrovače, které si navzájem vyměňují informace o sítích a stávají se tak svými sousedy, musí vždy být ve stejné síti. IGP protokoly se dělí na skupiny podle algoritmu, který používají při výpočtu nejlepších cest.

2.1 Distance-vector protokoly

Jak uvádí zdroj (PÁV, 2011), tyto protokoly si o sítích uchovávají informace nazvané vektor vzdálenosti. Vektor vzdálenosti obsahuje pouze metriku (vzdálenost) do cílové sítě a směr k cílové síti. Při šíření informací mezi směrovači se používá algoritmu Bellman-Ford nebo Ford-Fulkerson. Směrovače si mezi sebou vyměňují metriku, která představuje relativní číselnou dosažitelnost konkrétní sítě z konkrétního směrovače. K přijaté metrice sítě si směrovač uchová směr, který představuje sousední směrovač, od kterého je přijata informace, a k metrice cílové sítě přičte metriku cesty k tomuto sousednímu směrovači. Tímto způsobem se šíří cesta k cílové síti a na každém směrovači je k metrice přičtena metrika poslední části této cesty.

Obrázek 2 znázorňuje šíření metriky cesty do sítě u směrovače R6. Každá linka mezi směrovači má danou metriku a každý ze směrovačů k získané metrice přičítá metriku linky k sousednímu směrovači. Takto vypočtené metriky jsou u směrovačů pro jednotlivé cesty znázorněny se šipkami. Po výběru cesty s nejmenší metrikou bude výsledná cesta ze směrovače R1 do cílové sítě procházet přes R2, R5 a R6. Ostatní cesty mohou sloužit jako záložní.



Obrázek 2 - Algoritmus distance-vector protokolů

Pokud směrovač přijme informaci o cestách do stejné cílové sítě od různých směrovačů, vybere si cestu s nejmenší metrikou. V určitých případech (např. stejné metriky různých cest) může směrovač rozložit zátěž mezi více cest a zasílat data do stejné sítě různými cestami.

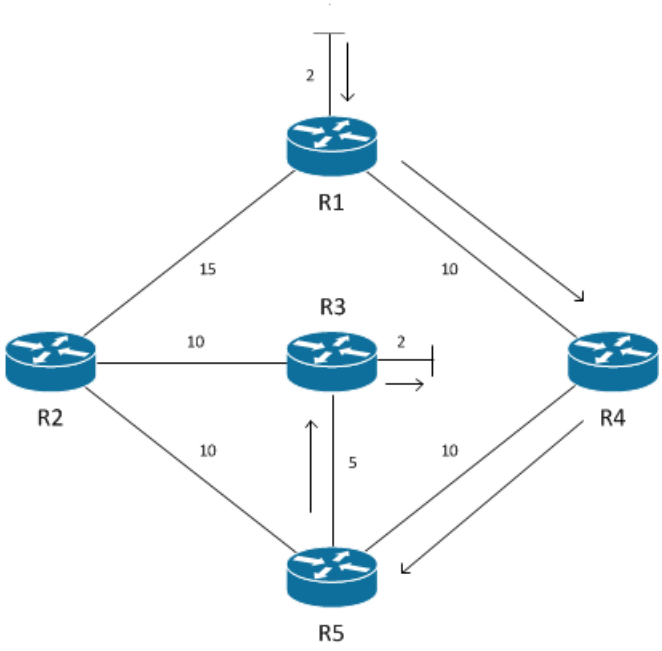
I podle předchozího obrázku (Obrázek 2) je zřejmé, že směrovače využívající distance-vector protokoly neznají celou topologii sítí, to je největší rozdíl proti ostatním typům IGP protokolů. Dalším typickým znakem distance-vector protokolů je periodické zasílání kompletní směrovací tabulky svým sousedům. Tyto protokoly nejsou náročné na výkon a paměť směrovačů a jejich použití bývá nejúčelnější v malých sítích. Mezi nejpoužívanější distance-vector protokoly patří:

- RIP,
- RIP2,
- IGRP.

2.2 Link-state protokoly

Směrovače využívající link-state protokoly si uchovávají informace o kompletní topologii sítí a cesty si každý směrovač počítá nezávisle na ostatních. K výběru cesty protokoly používají Dijkstrův algoritmus pro nalezení nejkratší cesty. Z tohoto principu vyplývá, že na rozdíl od předchozího typu protokolů si směrovače musí všechny informace o sítích předat nezměněné a všechny směrovače musí mít totožné informace. U velmi rozsáhlých sítí by to mohlo způsobit zpomalení sítě, proto link-state protokoly umožňují rozdělit rozsáhlé sítě na oblasti (vysvětleno v následující kapitole) a detailní informace o sítích jsou tak šířeny pouze v rámci jedné oblasti. Informace o sítích z jiných oblastí již nejsou tak obsáhlé.

Obrázek 3 zobrazuje výběr cesty link-state protokolem ze sítě připojené k R1 do sítě připojené ke směrovači R3. Každý ze směrovačů má stejné informace o metrice všech cest, proto R1 vybere cestu přes R4, R5 a R3. R4 po přijetí dat od R1 stejným způsobem zvolí cestu do cílové sítě přes R5 a R3. Další směrovače na cestě pracují obdobným způsobem.



Obrázek 3 - Algoritmus link-state protokolů

Dalším rozdílem proti distance-vector protokolům je frekvence zasílání informací o sítích ostatním směrovačům. Link-state protokoly zasílají aktualizace směrovacích tabulek pouze po zapnutí směrovače a následně se zasílají pouze informace o změnách topologie. Tím, že se informace nezasílají periodicky, se šetří šířka pásma sítě a zároveň dochází k rychlejší konvergenci protokolu. Nevýhodou proti distance-vector protokolům jsou vyšší nároky na operační paměť a výkon směrovače. Zástupci link-state protokolů jsou:

- OSPF,
- IS-IS.

2.3 Hybridní protokoly

Hybridní protokoly obecně používají možnosti obou typů IGP. Hlavním zástupcem této skupiny protokolů je

- EIGRP.

Zdroje se ale neshodují v otázce, zda je EIGRP opravdu hybridní protokol. Zdroj (LAMMLE, 2000) ho jako hybridní označuje a zdroj (ODOM, 2010) uvádí, že EIGRP používá pro výběr cesty balanced hybrid algoritmus, proto nemůže být uváděn v předchozích skupinách protokolů. Naopak zdroj (PÁV, 2011) vysvětluje, že EIGRP není kříženec předchozích skupin a zařazuje ho mezi distance-vector protokoly, i když připouští, že EIGRP může působit jako link-state protokol.

EIGRP byl vyvinut jako náhrada distance-vector protokolu IGRP, při porovnání je ale zřejmá jeho jiná funkčnost. Algoritmus pro šíření aktualizací byl nahrazen algoritmem DUAL (Diffusing Update Algorithm), místo periodického zasílání aktualizací jsou mezi směrovači šířeny pouze změny topologie a směrovače si kromě informací o nejlepší cestě udržují informace o celé topologii.

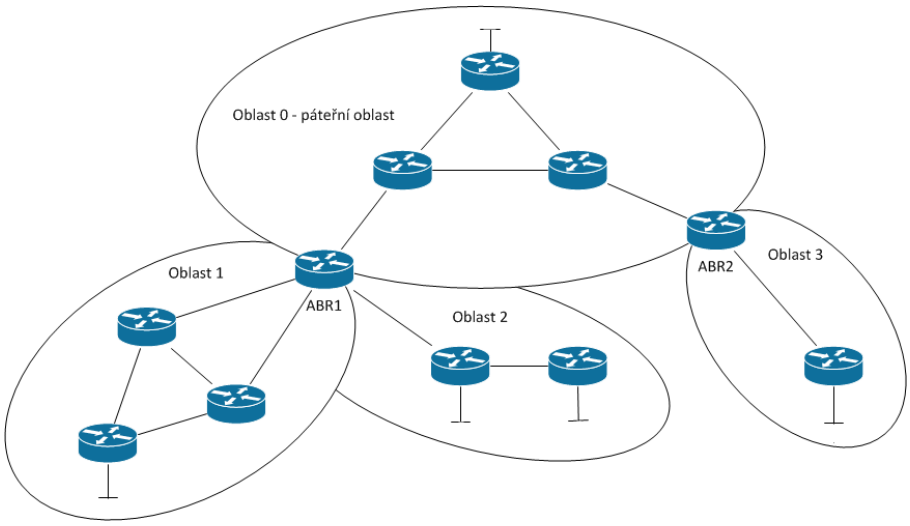
Tyto změny umožňují, že protokol v rychlosti konvergence sítě nezaostává za link-state protokoly. Při výpadku části sítě jsou šířeny zprávy o změně hned (bez čekání na pravidelné aktualizace) a každý směrovač má zároveň uložené informace o celé topologii, takže může rychle využít záložní cesty.

3 Směrovací protokol OSPF

Jak již bylo zmíněno, protokol OSPF používá logiku link-state. Podle ní se proces sestavení databáze cest z pohledu každého směrovače dá rozdělit na 3 základní fáze:

- rozeznání sousedů,
- výměna databáze topologie se sousedy,
- výpočet cest v topologii.

Návrh topologie velké sítě využívající OSPF vyžaduje více plánování než při použití EIGRP. Topologii OSPF je možné rozdělit na oblasti a při tomto rozdělení je potřeba myslet na to, že páteřní oblast musí být přímo spojena se všemi ostatními oblastmi. Každá oblast tedy musí sdílet minimálně jeden hraniční směrovač (Area Border Router – ABR) s páteřní oblastí. Obrázek 4 znázorňuje typickou OSPF topologii.



Obrázek 4 - Typická topologie sítě s OSPF

Hlavním důvodem pro rozdělení topologie na oblasti je úspora výměny informací o topologii mezi směrovači, zmenšení databází ve směrovačích a tím i zmenšení náročnosti na výpočet cest. V rámci jedné oblasti si směrovače vyměňují informace o celé topologii. Každý ABR pak do ostatních oblastí propaguje pouze stručné informace zahrnující adresy sítí bez detailních informací o topologii. Směrovače uvnitř oblasti tedy vnímají sítě z ostatních oblastí podobně, jako kdyby byly připojeny přímo k ABR.

3.1 Základní konfigurace OSPF

Základní konfigurace OSPF je jednoduchá. Každý směrovač má svůj specifický identifikátor ve tvaru IP adresy RID (Router ID), který je možné nastavit příkazem nebo ho směrovač vygeneruje z vlastních IP adres (nejvyšší adresa aktivního loopback rozhraní, případně nejvyšší adresa aktivního rozhraní). Následující konfigurace je tedy kompletní pouze v případě, že směrovač má možnost vygenerovat RID z adres svých rozraní.

```
R1(config)#router ospf 1
R1(config-router)#network 172.16.0.0 0.0.255.255 area 0
R1(config-router)#network 172.16.10.0 0.0.0.255 area 1
```

Prvním příkazem se na směrovači zapne OSPF proces číslo 1. Číslo procesu je interní věc směrovače a nemusí se shodovat se zapnutými procesy na jiných směrovačích. Další 2 příkazy nastavují protokol pro směrování dat v sítích. Příkaz obsahuje adresu sítě, wildcard masku sítě a číslo oblasti, do které je síť zařazena. Číslo oblasti již není pouze interní věc jednoho směrovače a je ho potřeba pro danou síť nastavit na stejnou hodnotu na všech směrovačích, které jsou k síti připojeny. V tomto případě je posledním příkazem zařazena podsíť, která byla zahrnuta již v předchozím příkazu, do jiné oblasti. OSPF zařazuje sítě do oblastí podle nejkonkrétnější wildcard masky. Podsíť 172.16.10.0 tedy bude zahrnuta do oblasti číslo 1. Druhá možnost pro zapnutí směrování je použití OSPF příkazu při konfiguraci rozhraní. V příkazu se analogicky specifikuje číslo procesu a číslo oblasti. Protokol se tím konfiguruje přímo pro rozhraní, směrování bude fungovat i v případě změny IP adresy rozhraní.

```
R2(config-if)#ip ospf 1 area 0
```

3.2 Sousedství v lokálních sítích

Sousedství se vždy vytváří mezi 2 směrovači a je nezávislé na ostatních. Účelem každého sousedství směrovačů je výměna informací o cestách v topologii tak, aby každý směrovač mohl vypočítat svoji nejlepší cestu do každé sítě v topologii. V OSPF je definováno 11 typů záznamů LSA (Link-State Advertisement), pomocí kterých jsou uloženy a vyměňovány informace o topologii (všechny typy nemusí být podporovány). Každý záznam LSA je opatřen LSID (Link-State Identifier). Pro správné směrování v OSPF topologii je potřeba, aby všechny směrovače v dané oblasti měly identickou link-state databázi (Link-State Database – LSDB), do které si směrovače ukládají všechny dostupné informace o topologii. Celková komunikace mezi dvěma směrovači pomocí OSPF probíhá pomocí 5 typů zpráv (ODOM, 2010):

- Hello – pro objevení sousedů a výměnu informací potřebných pro navázání sousedství (v LAN sítích posílané na skupinovou IP adresu 224.0.0.5),
- DD (Database Description) – využívá stručné verze LSA, aby sousedi vzájemně znali podporované typy LSA,
- LSR (Link-State Request) – paket obsahující výčet všech LSID, které směrovač požaduje po svém sousedovi,
- LSU (Link-State Update) – paket obsahující detailní LSA záznamy, typicky posílané jako odpověď na LSR zprávu,
- LSAck (Link-State Acknowledgment) – potvrzení přijetí LSU zprávy.

V lokálních sítích (Local Area Network – LAN) směrovače odesílají Hello zprávy pouze z rozhraní, které jsou zahrnuty v OSPF procesech a zároveň nejsou označeny jako pasivní. Zprávy jsou odesílány na skupinovou adresu 224.0.0.5. Pro navázání sousedství

mezi 2 směrovači ale nestačí, aby byly připojeny do stejné sítě na aktivních rozhraních. Zároveň musí splňovat i další požadavky na konfiguraci:

- každý směrovač musí mít svoje unikátní RID,
- rozhraní musí být ve stejné oblasti,
- mají stejný časovač Hello zpráv a interval Dead,
- musí souhlasit IP MTU (Maximum Transmission Unit – maximální velikost IP paketu),
- pokud je nastavena autentizace, musí být kladně vyhodnocena.

OSPF v rámci výměny informací mezi směrovači rozeznává více stavů, ve kterých se může nacházet sousedství mezi směrovači. Tyto stavy je možné zkontrolovat pomocí následujícího příkazu.

```
R1#show ip ospf neighbor
```

Stav sousedství může z pohledu každého směrovače nabývat těchto hodnot (HALABI, 1996):

- down – od souseda nebyla přijata žádná Hello zpráva před vypršením intervalu Dead,
- attempt – sousedství je nastaveno a byla odeslána Hello zpráva, Hello zpráva od souseda ale ještě nebyla přijata,
- init – Hello zprávy byly vyměněny, ale bez RID nebo nevyhovují další podmínky pro vytvoření sousedství. Pokud nevyhovuje některý z parametrů potřebných pro vytvoření sousedství, tak se tento stav nezmění do té doby, než budou parametry upraveny správcem.
- 2Way – Hello zprávy byly vyměněny včetně RID a všechny parametry pro vytvoření sousedství prošly kontrolou bez problémů,
- exStart – probíhá vyjednávání o sekvenčních číslech a master/slave logice DD paketů,
- exchange – dokončeno vyjednávání podrobností o DD paketech a probíhá výměna DD paketů,
- loading – výměna všech DD paketů je dokončena, směrovače zasílají LSR, LSU a LSAck pakety, aby si vyměnili všechny LSA záznamy,
- full – sousedi mají vyměněné informace a věří, že jejich LSDB pro danou oblast jsou shodné, následuje přepočet směrovací tabulky.

3.3 OSPF autentizace

Pokud je na směrovačích zapnuta autentizace, směrovač následně ověřuje pravost každé OSPF zprávy. Jde o to, aby případný útočník nemohl vytvořit nebo změnit zprávu, ve které by jako zdroj byl označen soused cílového směrovače. Pokud by tato zpráva byla cílovým směrovačem přijata, mohl by být následně ovlivněn tok dat v topologii a útočník by tak mohl převzít kontrolu nad topologií.

Pro autentizaci používají směrovače stejný sdílený klíč (dlouhý maximálně 16 znaků) a generovaný MD5 hash pro každou zprávu, který je přiložen ke zprávě. Pokud směrovač obdrží zprávu, ve které MD5 hash nesouhlasí, směrovač zprávu zahodí. Pokud na směrovačích nesouhlasí sdílený klíč, tak se směrovače nemohou stát sousedy.

OSPF nabízí 3 režimy autentizace:

- 0 – bez autentizace – výchozí nastavení v IOS,
- 1 – čistý text,
- 2 – MD5 – jediné správné řešení při nasazení v produkční síti.

Konfigurace autentizace probíhá ve 2 krocích:

- povolení a zvolení režimu autentizace:
  - možnost konfigurace na rozhraní (příklady pro režimy 0,1,2)
    ```
    R1(config-if)#ip ospf authentication null
    R1(config-if)#ip ospf authentication
    R1(config-if)#ip ospf authentication message-digest
    ```
  - nebo obdobně souhrnně pro OSPF oblast (příklad pro oblast 0, režim 2)
    ```
    R1(config)#router ospf 1
    R1(config-router)#area 0 authentication message-digest
    ```
- konfigurace konkrétního klíče na použitých rozhraních – pro každé použité rozhraní (týká se pouze režimů 1 a 2, viz příklady)
  ```
  R1(config-if)#ip ospf authentication-key key-value
  R1(config-if)#ip ospf message-digest key-number md5 key-value
  ```

Pokud se směrovače v důsledku zamítnutí autentizace nestanou sousedy, nelze stav sousedství zobrazit pomocí příkazu:

```
R1#show ip ospf neighbor
```

Pro zjištění podrobností lze zapnout režim ladění příkazem:

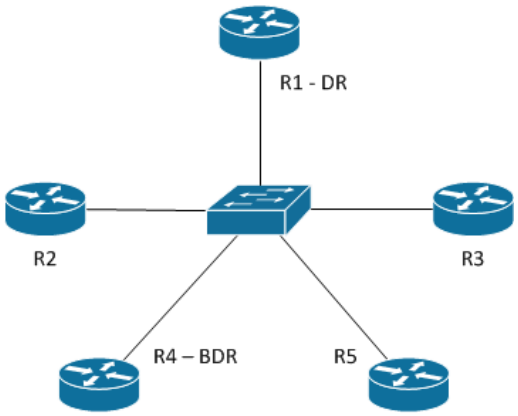
```
R1#debug ip ospf adj
```

Na rozdíl od EIGRP autentizace OSPF nenabízí konfiguraci klíčů závislých na čase. Přesto může být u OSPF při použití režimu MD5 konfigurováno více klíčů na jednom rozhraní, každý klíč pak musí mít vlastní identifikační číslo. Při změně klíčů je tedy potřeba nejdříve na směrovačích v síti vytvořit nové klíče a poté smazat staré. Pokud je současně nastaveno více klíčů, směrovač posílá zprávu vícekrát – podle každého klíče zvlášť.

3.4 DR a BDR

Designated Router (DR) a Backup Designated Router (BDR) jsou směrovače, které si mezi sebou volí směrovače připojené ve stejné síti, pokud v ní existuje možnost připojení 3 nebo více směrovačů a tím existuje i možnost vytvoření více sousedství. DR a BDR se tak obvykle volí i při přímém spojení dvou směrovačů přes Fast Ethernet

a naopak se nevolí při spojení sériovou linkou. Podstata DR a BDR směrovačů je založena na požadavku bezproblémové výměny LSA záznamů v dané síti a na snížení zátěže linky.



Obrázek 5 - Využití DR a BDR

Typické využití DR a BDR je zobrazeno na předchozím obrázku (Obrázek 5). Bez zvolení DR a BDR by každý směrovač navazoval sousedství se všemi ostatními. Tím by v této síti vzniklo celkem 10 sousedství. Po zvolení DR a BDR navazují ostatní směrovače sousedství pouze s těmito vybranými směrovači. Počet sousedství v této síti tak klesne na 7.

DR naváže sousedství se všemi ostatními směrovači a zajišťuje synchronizaci LSDB všech směrovačů v síti. Další sousedství v síti již není nutné, ale BDR má v podstatě záložní roli DR a obvykle všechny směrovače vytvářejí sousedství kromě DR také s BDR. Tím je zajištěno fungování sítě i v případě odpojení DR bez výpadku sítě a bez problémů v přenosech dat, které se DR netýkají. Komunikace mezi směrovači probíhá na základě různých IP adres. Zprávy určené pro DR a BDR směrovače jsou zasílány na skupinovou adresu 224.0.0.6, odpovědi od nich jsou zasílány na obvyklou adresu 224.0.0.5, která znázorňuje skupinu všech OSPF směrovačů.

Pokud nejsou DR a BDR v síti již zvoleny, je DR směrovač zvolen podle informací obsažených v Hello zprávách podle následujícího pořadí kritérií:

- směrovač s nejvyšší prioritou (výchozí nastavení 1, maximálně 255), která lze nastavit v konfiguraci rozhraní příkazem (v příkladu zvolena nejvyšší priorita): `R1(config-if)#ip ospf priority 255`
- pokud je v síti více směrovačů se stejnou nejvyšší prioritou, je zvolen směrovač s nejvyšším RID.

Stejným způsobem je následně zvolen BDR, který ale musí být jiný než DR. Pokud jsou v síti DR a BDR již zvoleny, tak se při připojení nebo odpojení směrovačů proces volby neopakuje a směrovačům zůstávají jejich role, i kdyby se do sítě připojil nový směrovač, který by měl například vyšší prioritu. Celý proces se opakuje pouze v případě, že se ze sítě odpojí DR i BDR. V případě odpojení pouze DR, jeho roli převezme BDR a následně se bude volit nový BDR. V případě odpojení BDR se opět volí pouze BDR. Zjistit, který

směrovač je v dané připojené síti zvolen jako DR, lze snadno pomocí příkazu (pro síť 10.10.34.0):

```
R1#show ip ospf database network 10.10.34.0
```

3.5 Sousedství ve WAN

Zdroj (ODOM, 2010) uvádí, že sousedství ve WAN (Wide Area Network) používá stejné základní principy a vyžaduje stejné požadavky (např. stejná síť, časovače, autentizace) jako sousedství v LAN, ale v různých aspektech se liší v závislosti na použitém typu sítě a použité WAN technologii. Proto je vždy nutné uvědomit si odpovědi na 3 otázky:

- Budou směrovače schopné navázat sousedství pomocí skupinových Hello zpráv?
- Pokusí se směrovače zvolit DR, který směrovač by se jím případně měl stát?
- Se kterými dalšími směrovači by se měl každý směrovač stát sousedem?

3.5.1 Typy sítí OSPF

Typ sítě OSPF je možné nastavit na každém rozhraní použitém v OSPF oblastech a na tomto nastavení záleží 3 důležité vlastnosti:

- možnost objevení sousedů pomocí skupinových Hello zpráv,
- možnost existence více než 2 sousedů v síti připojené na rozhraní,
- pokus o zvolení DR směrovače v síti na daném rozhraní.

V LAN sítích není nutné starat se o nastavení typu sítě. Výchozím type sítě je Broadcast, který povoluje skupinové Hello zprávy, využívá zvolení DR a BDR směrovačů a povoluje více sousedních směrovačů v jedné připojené síti. Při připojení přes některou z WAN technologií je potřeba typ sítě zvolit podle následující tabulky a nastavit na konkrétní rozhraní pomocí příkazu (příklad pro nastavení výchozího typu broadcast):

```
R1(config-if)#ip ospf network broadcast
```

Tabulka 1 - Typy sítí OSPF

Typ rozhraní	Používá DR/BDR	Výchozí časovač Hello	Dynamické vyhledání sousedů	Možnost více než 2 směrovačů v síti
Broadcast	ano	10	ano	ano
Point-to-point[1]	ne	10	ano	ne
Loopback	ne	-	-	ne
Nonbroadcast[2] (NBMA – Non-broadcast Multiple Access)	ano	30	ne	ano
Point-to-multipoint	ne	30	ano	ano
Point-to-multipoint nonbroadcast	ne	30	ne	ano

[1] Výchozí nastavení na subrozhraní využívající Frame Relay.
[2] Výchozí nastavení na fyzickém a multipoint subrozhraní využívající Frame Relay.

3.5.2 Sousedství v síti Point-to-Point

Pokud je vytvořeno spojení na sériovém rozhraní a je zapnut OSPF pro danou síť, směrovač označí typ sítě jako Point-to-Point. V případě úspěšného navázání sousedství není volen DR.

3.5.3 Sousedství v technologii Frame Relay

Většina návrhů Frame Relay využívá přímé spojení pouze dvou směrovačů v jedné síti. V tomto případě se oproti obvyklému typu Point-to-Point sítě nic nemění a není potřeba směrovače více konfigurovat.

V případě připojení více směrovačů do jedné Frame Relay sítě je potřeba více konfigurace podle typu připojení směrovačů. V závislosti na daném typu připojení se musí využít některý z typů sítě broadcast, nonbroadcast, point-to-multipoint nebo point-to-multipoint nonbroadcast.

3.5.4 Sousedstvi v MPLS VPN

MPLS VPN (Multiprotocol Label Switching Virtual Private Networks) je služba, která se podobá Frame Relay, ale v mnoha ohledech se liší. Klient si nemůže pronajmout fyzickou linku mezi svými směrovači jako u Frame Relay. MPLS VPN je služba provozována na třetí vrstvě modelu OSI (Open Systems Interconnection) a proto směrovače zákazníka navazují OSPF sousedství se směrovači poskytovatele služby a sousedství mezi směrovači zákazníka nemůže existovat. Směrovače poskytovatele si pak vyměňují cesty většinou pomocí protokolu Multiprotocol BGP (MP-BGP).

3.5.5 Sousedství v Metro Ethernet

Tato služba je postavena na druhé vrstvě modelu OSI a přenosu dat mezi směrovači pomocí VLAN (Virtual Local Area Network). Díky tomu mohou směrovače klienta navázat sousedství mezi sebou (např. point-to-point nebo point-to-multipoint) a není nutné navazovat OSPF sousedství se směrovači poskytovatele služby.

3.6 Výměna LSDB uvnitř oblasti

Jak již bylo nastíněno, všechny směrovače v oblasti musí mít stejnou databázi adres, kterou si směrovače mezi sebou vyměňují pomocí LSA záznamů. Je tedy nutné, aby každý směrovač dále publikoval databázi, kterou si vytvořil ze svých údajů, ale také z údajů, kterou mu poskytly ostatní směrovače. V LAN sítích je pro distribuci databáze využito konceptu DR a BDR směrovačů.

Aby se předešlo smyčkám při přeposílání informací, má každý LSA záznam svůj identifikátor LSID a sekvenční číslo, které určuje směrovač, který daný LSA vytvořil. Sekvenční číslo je při každé změně navýšeno, a pokud směrovač obdrží dva LSA záznamy se stejným LSID, záznam s menším sekvenčním číslem zničí.

3.6.1 Pravidelné šíření záznamů

Přestože OSPF pravidelně nezasílá aktualizace cest, jako to dělají distance-vector protokoly, tak OSPF zasílá po 30 minutách aktualizace každého LSA záznamu. Směrovač

při vytvoření každé aktualizace nastaví čas danému záznamu na 0 vteřin. Každý směrovač pak čas záznamu po vteřinách přičítá. Pokud se záznam během 30 minut nezmění, zdrojový směrovač záznamu vynuluje čas, nastaví vyšší sekvenční číslo a odesílá záznam znovu ostatním směrovačům v oblasti.

Obvykle mají směrovače také nastavený maximální čas platnosti LSA záznamu MaxAge na 3600 vteřin. Pokud tedy během jedné hodiny nedostane směrovač aktualizovaný záznam s větším sekvenčním číslem, záznam smaže. Této vlastnosti se dá využít i v případě, když směrovač vytvářející konkrétní LSA záznam potřebuje smazat záznam z LSDB v celé oblasti. Směrovač záznamu přiřadí nové sekvenční číslo, čas 3600 vteřin a odešle záznam ostatním směrovačům. Směrovače si po přijmutí takového záznamu vymažou všechny informace, které se záznamu týkají, protože záznam již vypršel. Tento záznam ale pošlou nezměněný dalším směrovačům v oblasti, aby se LSDB v oblasti udržely konzistentní.

3.7 Výběr nejlepší cesty

Směrovač samozřejmě směruje data pouze podle dat ze směrovací tabulky, aby mohl porovnávat i cesty naučené podle různých protokolů. Z LSDB si každý směrovač tedy musí vybrat jen ty cesty, které si do směrovací tabulky uloží. Cesty uložené do směrovací tabulky pomocí protokolu OSPF je možné zobrazit příkazem:

```
R1#show ip route ospf
```

Pokud směrovač má k dispozici všechny informace o topologii a má tedy kompletní LSDB (směrovač nemusí mít kompletní LSDB ve chvíli před výměnnou informací mezi směrovači po zapnutí směrovače nebo změně v topologii), skládá se výběr nejlepší cesty ze třech kroků:

- analýza LSDB a výběr všech možných cest do cílové sítě,
- sečtení ohodnocení (cost) pro všechny výstupní rozhraní směrovačů na konkrétních cestách,
- výběr cesty s nejmenším ohodnocením.

Zjednodušeně se dá říci, že ohodnocení vytváří OSPF pro každé výstupní rozhraní. Tato informace je předávána ostatním směrovačům v LSA záznamech a každý směrovač je schopen sečíst tato ohodnocení pro celou cestu. Ohodnocení rozhraní je možné v konfiguraci změnit a tím je umožněno některé cesty preferovat. Zobrazit ohodnocení jednotlivých rozhraní je možné příkazem:

```
R1#show ip ospf interface
```

Pokud směrovač nalezne více nejlepších cest se shodnou metrikou, může si uložit do směrovací tabulky všechny tyto cesty a využít tak rozložení zátěže na více cest. Počet uložených cest je ale omezen nastavením *maximum-paths* s výchozí hodnotou 4. V případě, že nejlepší cesta je pouze jedna a všechny ostatní cesty mají vypočítanou horší

metriku, do směrovací tabulky je uložena pouze jedna cesta. OSPF tedy podporuje pouze vyvážené rozložení zátěže a nepodporuje zasílání dat cestami s různou metrikou.

3.7.1 Výběr nejlepší cesty do jiné oblasti

Vzhledem k tomu, že podrobné informace o cestách si směrovače vyměňují pouze v rámci jedné oblasti, zdrojový směrovač zná pouze souhrnné ohodnocení cesty v jiné oblasti, které mu poskytuje ABR. Směrovač tedy nezná přesnou cestu a nepočítá ohodnocení všech výstupních rozhraní na cestě. Prakticky se výpočet cesty skládá ze dvou částí:

- výpočet ohodnocení uvnitř vlastní oblasti k ABR,
- přičtení ohodnocení cesty mimo vlastní oblast poskytnutého od ABR.

Opět jsou vypočítána ohodnocení pro všechny možné cesty a stejným způsobem jako u cest uvnitř oblasti je vybrána jedna nebo více cest k cíli, respektive pouze k jednomu nebo více ABR. Směrovač si do směrovací tabulky ukládá cesty do jiných oblastí se značkou O IA (OSPF interarea).

3.7.2 Důležitá pravidla pro výběr cest ABR směrovači

Pokud je mezi dvěma oblastmi zapojeno více ABR směrovačů, mohou ABR směrovače dostat informace o cílové síti z obou oblastí (z jedné oblasti přímou cestu, z druhé oblasti cestu zprostředkovanou přes jiný ABR). Proto v OSPF platí zvláštní pravidla pro výběr cest ABR směrovači:

- přímá cesta do cílové oblasti je vždy lepší než cesta přes jinou oblast, i když nepřímá cesta má lepší metriku,
- ABR použije cesty do nepřímo připojených oblastí, pouze pokud je dostane z páteřní sítě. Ostatní cesty do cizích oblastí směrovač ignoruje.

Z prvního pravidla vyplývá, že pokud je zdroj a cílová síť ve stejné oblasti, data nikdy tuto oblast neopustí, i kdyby měla být cesta přes jinou oblast rychlejší. Druhé pravidlo udává, že všechna data, která jsou směrována do jiné oblasti, vždy budou procházet minimálně přes jeden ABR připojený k páteřní oblasti, případně budou procházet přes páteřní oblast, i kdyby byl ABR směrovač přímo mezi zdrojovou a cílovou oblastí a tato cesta by měla mít nejmenší metriku.

3.7.3 Definice ASBR a jeho rozdíl proti ABR

OSPF kromě ABR definuje další roli směrovače – ASBR (Autonomous System Boundary Router), který stejně jako ABR šíří ostatním směrovačům cesty do sítí, které jsou mimo vlastní OSPF oblast. Tyto cesty ale ASBR zpravidla nezískává z jiných OSPF oblastí, ale vytváří je pomocí šíření defaultní cesty do Internetu, redistribucí cest z jiných protokolů nebo redistribucí statických cest a sumarizací těchto cest. Ostatní směrovače v oblasti rozeznají původ cest od ABR nebo ASBR podle jiných typů šířených LSA záznamů.

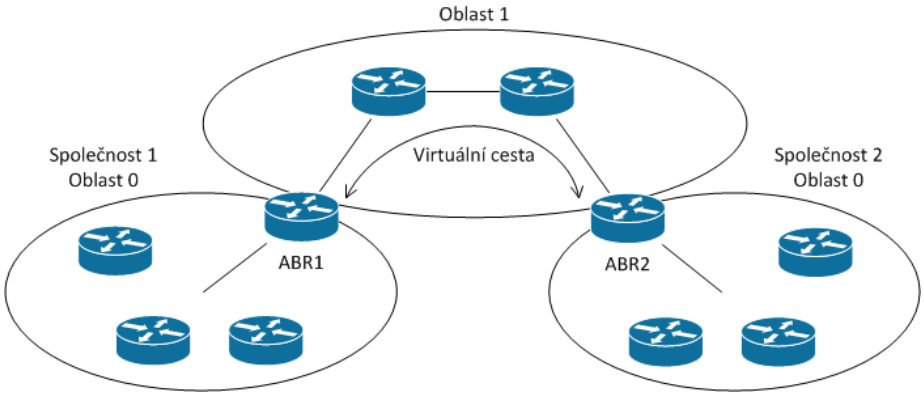
3.8 Virtuální cesty

Základní koncept OSPF obsahuje páteřní oblast, ke které jsou přes ABR připojeny všechny ostatní oblasti. Následkem různých příčin může nastat situace, kdy tento koncept nebude možné splnit, z principu to mohou být například tyto důvody (THOMAS, 2003):

- je potřeba připojit novou oblast ke stávající topologii, ale z finančních důvodů ji nelze přímo spojit s páteřní oblastí,
- z důvodu kombinace selhání různých spojení v páteřní oblasti je páteřní síť rozdělena,
- spojení dvou společností, které v síti používají OSPF, každá společnost má svoji páteřní oblast a není možné obě páteřní oblastí spojit do jedné.

Tyto nebo i jiné důvody by mohly vést k navrhnutí nového rozvržení oblastí. K tomuto postupu OSPF nabízí levnější alternativu virtuálních cest.

Virtuální cesta je založena na vytvoření sousedství mezi dvěma ABR směrovači připojenými ke stejné nepáteřní oblasti a tím vzniká spojení mezi dvěma částmi páteřní oblasti, která se tak stane celistvou. Mezi těmito dvěma ABR může být neomezené množství jiných směrovačů, které jsou součástí nepáteřní oblasti, která se pro tento účel může nazývat tranzitní oblastí.



Obrázek 6 - Spojení dvou páteřních oblastí virtuální cestou

Ke konfiguraci virtuální cesty je potřeba znát RID obou potřebných ABR a číslo oblasti, přes kterou virtuální cesta vede. ABR si mezi sebou následně zasílají obvyklé OSPF zprávy s LSA záznamy zabalené do paketů se standardní cílovou IP adresou (v tomto případě není IP adresa skupinová) a směrovače v tranzitní oblasti tyto zprávy pouze přeposílají. V posílaných LSA záznamech jsou malé rozdíly proti záznamům zasílaným v rámci jednotné páteřní oblasti:

- je nastaven bit DNA (Do Not Age), který zajišťuje, že směrovače tento záznam nesmažou po uplynutí určité doby (ve výchozím nastavení 1 hodina),
- směrovače přes virtuální cestu nezasílají pravidelné aktualizace LSA záznamů (obvykle je zasílají každých 30 minut) z důvodu snížení zátěže cesty,

- ohodnocení virtuální cesty je započítáno pouze jako ohodnocení výstupního rozhraní, je tedy předávána pouze jedna celková informace místo informací o každém směrovači, který tvoří virtuální cestu.

3.8.1 Konfigurace virtuální cesty

Většina konfiguračních příkazů (např. autentizace, Hello časovač, Dead interval) by se v jiných případech konfigurovala pro dané rozhraní. Protože virtuální cesta není závislá na žádném rozhraní, konfiguruje se pomocí příkazu *area virtual-link* v nastavení OSPF procesu. Základní nastavení se provede pomocí následujících příkazů (příklad pro OSPF proces č. 1, tranzitní oblast č. 10 a RID směrovače na druhém konci virtuální cesty 4.4.4.4), analogicky je nutné konfiguraci provést na ABR, které jsou na obou koncích virtuální cesty:

```
R1(config)#router ospf 1
R1(config-router)#area 10 virtual-link 4.4.4.4
```

Přehled a kontrolu virtuálních cest je možné zobrazit příkazy:

```
R1#show ip ospf virtual-links
R1#show ip ospf neighbor
R1#show ip ospf neighbor detail 4.4.4.4
```

Specifická vlastnost RID je to, že pro tuto adresu nemusí být šířena cesta. Z toho vyplývá, že RID nemusí být dosažena příkazem *ping*, ale přesto virtuální cesta bude fungovat.

V produkčním prostředí je opět důležité nastavit autentizaci pro sousedství mezi směrovači. Protože virtuální cesta není závislá na žádném rozhraní, nastavuje se autentizace analogicky jako u obvyklých sousedství OSPF s jediným rozdílem – nastavují se příkazem *area virtual-link*. Příklad uvádí konfiguraci autentizace v režimu MD5 pro OSPF proces č. 1, tranzitní oblast č. 10, RID protějšího ABR 4.4.4.4, číslo klíče 2 a heslo pass, nastavení je opět nutné konfigurovat na obou ABR:

```
R1(config)#router ospf 1
R1(config-router)#area 10 virtual-link 4.4.4.4 authentication
message-digest message-digest-key 2 md5 pass
```

4 Představení EGP

Vnější směrovací protokoly jsou určeny ke směrování toku dat mezi různými autonomními systémy, které samy o sobě mohou být velmi rozsáhlé. EGP nejsou určeny pro směrování uvnitř AS, o to se starají IGP. EGP se tedy zpravidla nevyskytují v malých ani středně velkých sítích, ale v dnešní době mají na starost směrování dat na páteřních linkách Internetu. V některých případech (pokud má AS více směrovačů připojených k jiným AS) může několik směrovačů uvnitř AS pro šíření nejlepších cest používat kromě IGP i EGP. Z podstaty těchto dvou skupin protokolů vyplývá, že pro komunikaci mezi dvěma zařízeními připojenými k Internetu je nutná spolupráce IGP a EGP.

EGP jako základní informaci, kterou propaguje ostatním směrovačům, uvažuje dvojici IP adresy a cestu znázorněnou sekvencí ASN.

4.1 Zástupci EGP

Pro přenos dat v počítačových sítích se v různých verzích používali 2 zástupci vnějších směrovacích protokolů. Prvním zástupcem byl Exterior Gateway Protocol (EGP), který byl poprvé popsán společností BBN v roce 1982[3] a jeho formální specifikace byla vytvořena v roce 1984[4]. Tento protokol měl zásadní omezení pro použití pouze na stromové struktuře AS. Dnes se v Internetu používá topologie mesh, proto tento protokol již není možné v Internetu použít.

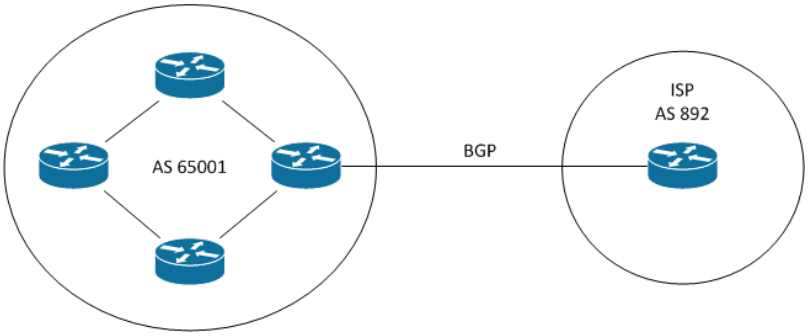
Dalším vnějším směrovacím protokolem je BGP, který byl poprvé popsán v roce 1989[5]. Dnes se používá již čtvrtá verze tohoto protokolu, která byla definována v roce 1995 a je dále aktualizována. Poslední aktualizace byla popsána v květnu 2012[6].

4.2 Typy autonomních systémů

Každý AS, který je připojen do Internetu, má pouze omezený počet směrovačů, které jsou spojeny s dalšími AS a mohou tak data do Internetu směrovat. Tyto směrovače se nazývají hraniční směrovače a zpravidla tedy používají IGP pro směrování uvnitř AS a EGP pro směrování mimo vlastní AS.

[3] RFC 827 Exterior Gateway Protocol (EGP) viz (BOLT BERANEK AND NEWMAN INC., 1982)
[4] RFC 904 Exterior Gateway Protocol Formal Specification viz (NETWORK WORKING GROUP, 1984)
[5] RFC 1265 BGP Protocol Analysis viz (NETWORK WORKING GROUP, 1991)
[6] RFC 6608 Subcodes for BGP Finite State Machine Error (IETF, 2012)

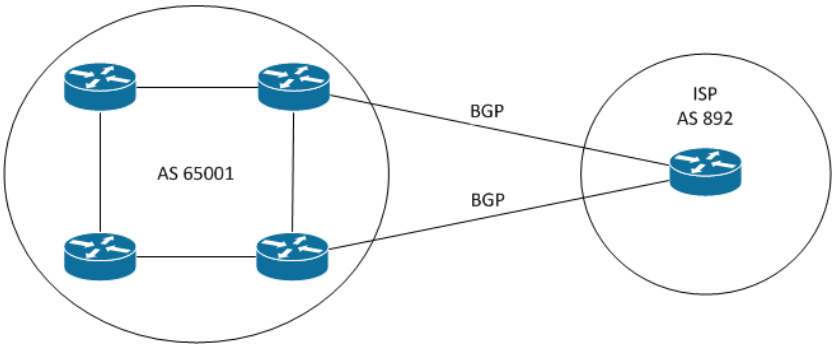
4.2.1 Single homed



Obrázek 7 - Single homed AS

AS má pouze jeden hraniční směrovač, který je k poskytovateli Internetu připojen pouze jednou linkou. Všechna data směrovaná do Internetu nebo z Internetu prochází tímto směrovačem. AS v tomto případě má ASN z rozsahu privátních čísel, protože všechna data prochází přes autonomní systém ISP a ten bude do Internetu propagovat všechny IP adresy ze svého AS i z tohoto privátního AS v rámci svého ASN.

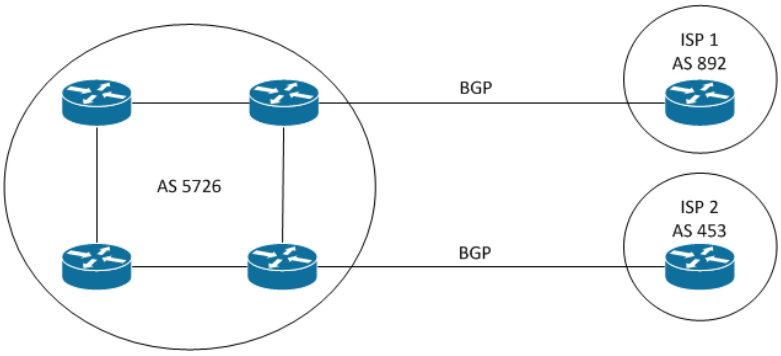
4.2.2 Dual homed



Obrázek 8 - Dual homed AS

AS je připojen redundantně více linkami, ale pouze k jednomu ISP. Linky mohou být mezi stejnými směrovači (jeden směrovač z AS a jeden z ISP) nebo mohou být i mezi více směrovači, jak ukazuje předchozí obrázek (Obrázek 8). Tento typ připojení AS se používá pro rozložení zátěže nebo pouze jako záložní spojení.

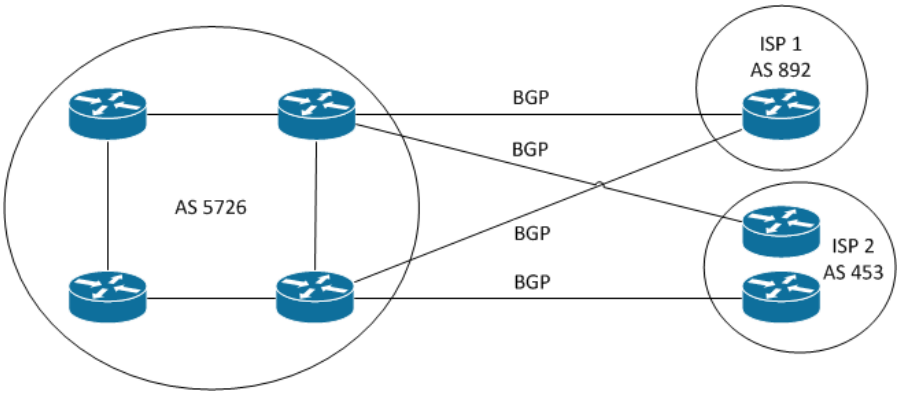
4.2.3 Single multihomed



Obrázek 9 - Single multihomed AS

Připojení k Internetu je provedeno přes více ISP. Ke každému ISP ale vede pouze jedna linka. Hraniční směrovač může být jeden nebo jich může být více. Z důvodu připojení autonomního systému k více ISP již nemůže mít AS privátní ASN. Správce AS tedy musí zažádat matriku IANA o přidělení veřejného ASN.

4.2.4 Dual multihomed

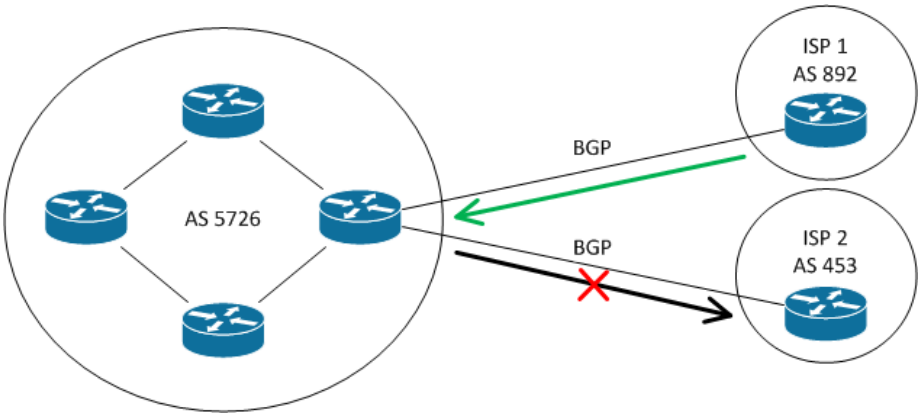


Obrázek 10 - Dual multihomed AS

AS je připojen k více ISP, ke kterým je připojen redundantními linkami.

Dále je potřeba multihomed AS rozlišovat podle toho, zda jimi může nebo nemůže procházet cizí provoz.

4.2.5 Netranzitní multihomed AS



Obrázek 11 - Netranzitní multi homed AS

AS neslouží pro přenos cizích dat. Měl by umožňovat pouze přenos dat se zdrojovou nebo cílovou adresou v daném AS. Mimo svůj AS jsou propagovány pouze vlastní adresy.

4.2.6 Tranzitní multihomed AS

Přes daný AS mohou procházet data, která zde nezačínají ani nekončí. EGP propaguje cesty do svého, sousedních i dalších AS.

4.3 Základní principy EGP

Některé principy mají EGP společné s IGP. Například dva směrovače musí navázat sousedství před výměnou informací o sítích, které si následně vyměňují včetně prefixu. Každý směrovač pak samostatně z těchto informací vybírá nejlepší cesty do konkrétních sítí a ty si ukládá do směrovací tabulky. Naopak sousedi EGP nemusí být ve stejné síti a sousedství musí být nastaveno konkrétní IP adresou, protože nejsou využity skupinové adresy. Sousedství je pak navázáno pomocí spolehlivého TCP (Transmission Control Protocol), který využívá port 179, a mezi sousedy je předáváno více informací o konkrétních cestách. EGP pro výběr cesty používají logiku nazvanou vektor cesty (Path vector logic), která je podobná distance-vector logice, kterou používají např. protokoly IGRP nebo EIGRP.

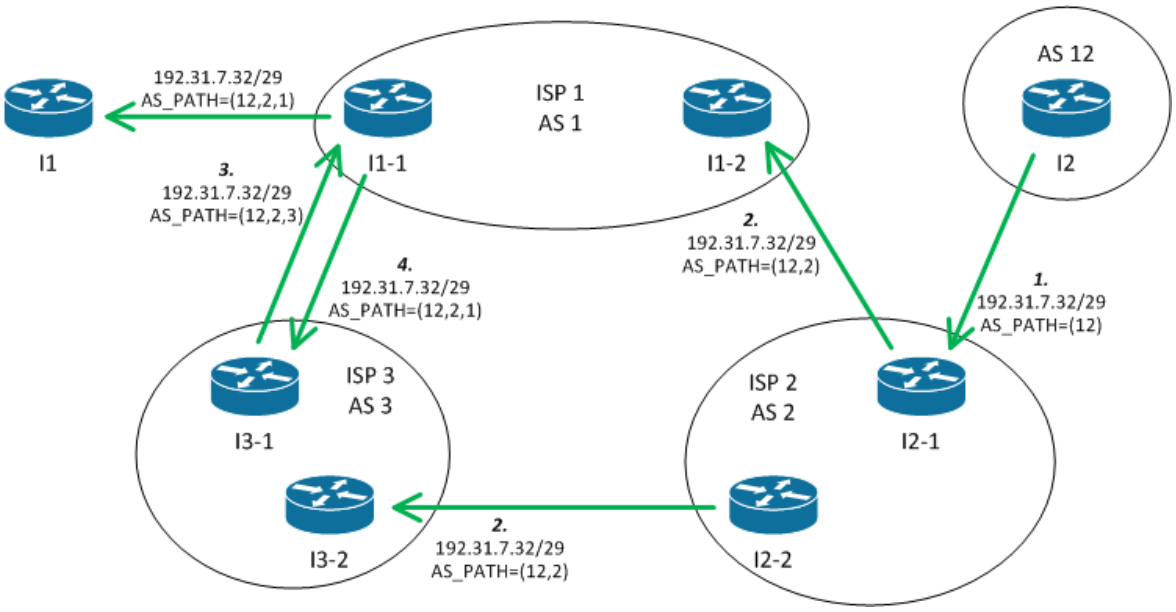
5 Směrovací protokol BGP

EGP protokoly šíří mnoho informací o cestě k síti. BGP pro tento účel používá atributy cesty (Path Attributes – PA). Základní informace o cestách, které BGP šíří, jsou IP adresa sítě a cesta k této síti znázorněna sekvencí ASN. Tato sekvence se nazývá AS_SEQ a je uložena v atributu AS_PATH. Tato informace pro danou cestu znázorňuje, přes které AS vede cesta do cílové sítě. BGP pak AS_PATH používá pro dvě zásadní funkce:

- výběr nejlepší cesty založené na nejmenším počtu AS na cestě k síti (výchozí chování BGP, v praxi ale bývá chování na základě konfigurace složitější),
- prevence smyček při směrování paketů – pokud do AS přichází cesta, která již obsahuje vlastní ASN, je tato cesta ignorována.

Tyto funkce lze využít díky tomu, že ASN jsou unikátní a přidělovaná organizací IANA. V případě duplicitních ASN by AS odmítaly některé cesty v Internetu a doručení dat by nemuselo být funkční. Problém by mohl nastat v případě použití privátních ASN, proto je nutné takové AS začleňovat na konec Internetové sítě, nejlépe pouze s jedním připojením k Internetu. Toto použití se dá srovnat s použitím soukromých IPv4 adres.

Na následujícím obrázku (Obrázek 12) je znázorněno šíření cesty do sítě, která je součástí AS 12. Adresa sítě je 192.31.7.32/29 a hraniční směrovač v AS 12 tuto adresu šíří s AS_PATH = 12. Následně si cestu vymění BGP směrovače uvnitř AS 2 a při šíření cesty mimo svůj AS přidají své ASN do AS_PATH. Cestu tedy šíří s AS_PATH = 12,2. Do AS 1 se dostane cesta ze dvou zdrojů s různými AS_PATH (z jednoho zdroje 12,2 a z druhého 12,2,3) a ve výchozí konfiguraci si BGP směrovače vyberou cestu s menším počtem tranzitních AS, takže cestu s AS_PATH 12,2,3 směrovače ignorují. Při dalším šíření do jiných AS směrovače k cestě opět přidají své ASN a cestu šíří s AS_PATH 12,2,1.



Obrázek 12 - Příklad topologie pro vysvětlení základních principů BGP

5.1 Interní a externí BGP

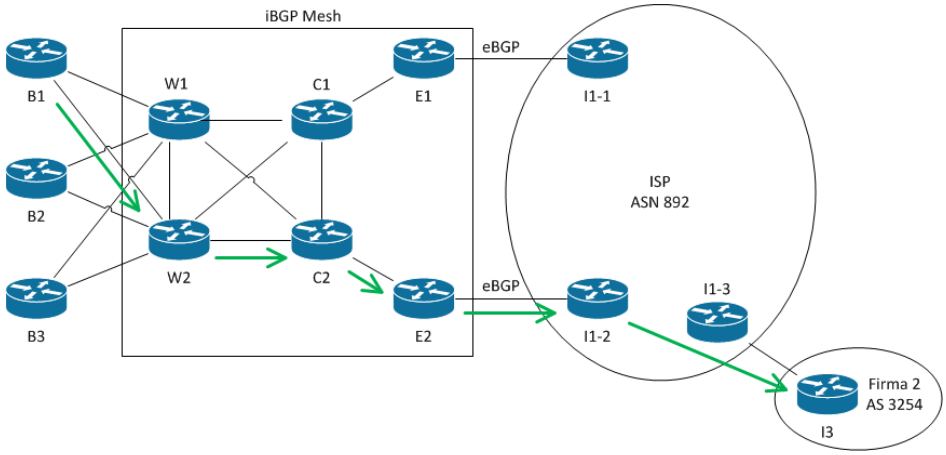
BGP definuje dva druhy sousedství (soused se v případě BGP označuje také jako peer, sousedství se označuje peering). První typ sousedství je iBGP (internal BGP), které je navázáno mezi sousedy ve stejném AS. Druhý typ je eBGP (external BGP) a je navázáno mezi směrovači z různých AS. Směrovače se při výměně dat chovají odlišně podle typu sousedství a to již při jeho navazování. První odlišnost v chování byla již nastíněna – v případě šíření cesty přes eBGP směrovač aktualizuje AS_PATH. To se v iBGP vztahu neděje.

5.2 Směrování dat z podnikové sítě do Internetu

Pro podnikové sítě existují dvě možnosti, jak směrovat svá data do Internetu. První možnost je nastavení statické defaultní cesty, která zajistí, že data směrovaná do všech sítí, do kterých nejsou známy cesty, budou směrovaná jednou konkrétní cestou. Tou bývá jeden směrovač připojený k ISP. V případě více směrovačů připojených k ISP lze tímto způsobem řešit záložní nebo redundantní připojení. Výhody tohoto řešení jsou jednoduchá konfigurace a celkově významně menší náročnost na výkon směrovačů. V případě veřejných adres použitých v podnikové síti je nutné, aby šíření těchto adres do Internetu zajistil ISP.

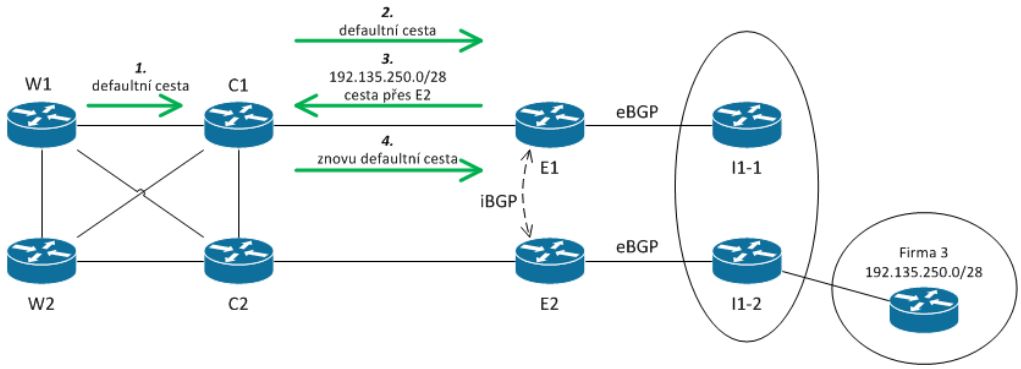
Druhou možností je konfigurace BGP na některých směrovačích v podnikové síti a navázání BGP sousedství se všemi připojenými ISP. Pokud nemá podnik významný důvod ke zvolení této možnosti, je první možnost určitě lepší volba. Důvody k zavedení BGP v podnikové síti mohou být například potřeba směrovat data z podniku do některých částí Internetu jinou cestou než ostatní data, případně potřeba přijímat data z Internetu do některých podnikových sítí přes jiného ISP než u ostatních sítí.

Předtím, než je zvolen způsob směrování dat do Internetu, je nutné si uvědomit, kolik směrovačů musí mít zapnutý a nakonfigurovaný BGP. Pokud podniková síť má více připojení k Internetu a je potřeba některé cesty preferovat před jinými, mohou se při špatné konfiguraci sítě vyskytnout problémy. Na následujícím obrázku (Obrázek 13) je znázorněna situace dualhomed připojení k Internetu, kdy je pro danou cílovou síť pomocí BGP preferována cesta přes směrovač E2 a kdy je potřeba konfigurace BGP na 6 podnikových směrovačích.



Obrázek 13 - Správné dualhomed připojení k Internetu

V tomto případě všechny směrovače, které tvoří síť sousedství iBGP znají nejlepší cestu do cílové sítě přes směrovač E2. Pokud by ale iBGP sousedství vytvořily například pouze směrovače E1 a E2 (Obrázek 14), může nastat smyčka při zasílání dat, protože ostatní směrovače nemohou znát informaci, že nejlepší cesta vede přes E2. Pokud by tedy směrovače zaslali data směrovači E1, ten by data následně přeposlal na E2. Protože ale neexistuje přímé spojení mezi E1 a E2, došlo by ke smyčce mezi směrovači C1 a E1, data by do cílové sítě tedy nikdy nedorazila.



Obrázek 14 - Špatné dualhomed připojení k Internetu

5.3 Rozdíly mezi částečnými a plnými BGP aktualizacemi

Každá podniková síť má několik možností, jak pracovat s BGP cestami, které jim mohou poskytnout ISP:

- vyžádat si od ISP pouze defaultní cestu,
- vyžádat si plné aktualizace BGP cest,
- vyžádat částečné aktualizace doplněné defaultní cestou.

Výběr řešení záleží na typu podnikového AS. Pro typ Single homed, kdy je AS připojen k Internetu pouze jednou fyzickou cestou, je nejvýhodnější použít defaultní cestu. Ostatní možnosti jsou zbytečné, protože data do Internetu nemohou být směrována jinými cestami. U AS typu Dual homed je situace podobná, data budou vždy směrována přes jednoho ISP

a rozdíl v celkové cestě dat k cílovému zařízení v Internetu bude minimální, i když data mohou opustit podnikovou síť přes různé směrovače. Cesta od ISP k cílovému zařízení poté bude volena vždy stejným způsobem.

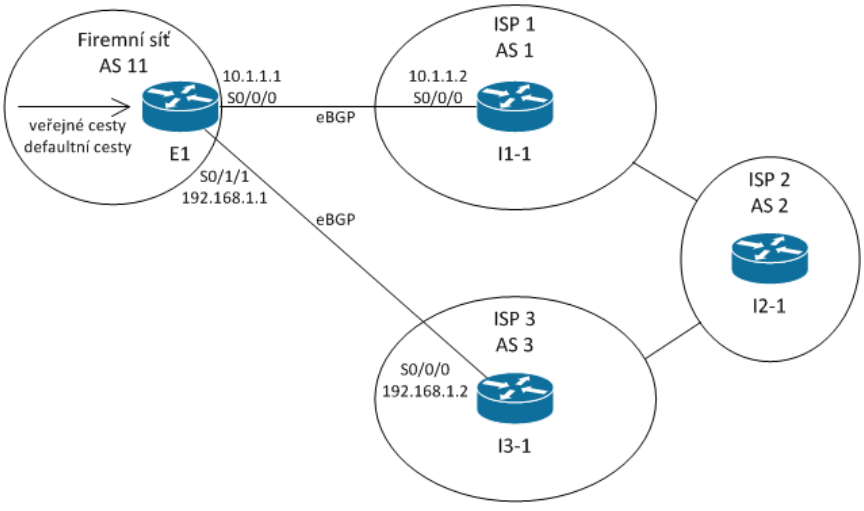
V případě připojení podnikového AS k více ISP může být užitečné volit cestu již v AS a data zasílat různým ISP podle toho, který ISP nabízí lepší cestu k cílové síti v Internetu. Nejjednodušší možnost by tedy mohla být vyžádat si plné aktualizace BGP cest od všech připojených ISP. BGP tabulky ale mohou obsahovat stovky tisíc záznamů, výměna těchto dat mezi směrovači zahlcuje síť a následně může způsobit velké vytížení směrovačů, které se podle těchto dat rozhodují pro nejlepší cestu. V předchozích příkladech je také vysvětleno, že v některých případech je potřeba, aby v rámci AS používalo BGP větší množství směrovačů. V tomto případě pak pro rozhodnutí hrají velkou roli finance, protože ne všechny směrovače jsou schopné efektivně používat takové množství informací.

Kompromisem mezi těmito dvěma možnostmi je využití částečných BGP aktualizací. Při využití této možnosti je potřeba domluvit se s jednotlivými ISP, které cesty budou do podnikové sítě zasílat. K tomu ISP bude zasílat i defaultní cestu, aby se data mohla dostat do všech cílových sítí.

5.4 Externí sousedství v BGP

Základní konfigurace eBGP je poměrně snadná a bude vysvětlena na příkladu. Podniková síť má ASN 11 a přes směrovač E1 je připojena ke dvěma ISP (s ASN 1 a 3). Následující příkazy znázorňují konfiguraci jak na podnikovém směrovači, tak na směrovačích ISP. Poslední číslo v každém příkazu jsou ASN, na kterých závisí navázání eBGP sousedství:

```
E1(config)#router bgp 11
E1(config-router)#neighbor 10.1.1.2 remote-as 1
E1(config-router)#neighbor 192.168.1.2 remote-as 3
I1-1(config)#router bgp 1
I1-1(config-router)#neighbor 10.1.1.1 remote-as 11
I3-1(config)#router bgp 3
I3-1(config-router)#neighbor 192.168.1.1 remote-as 11
```



Obrázek 15 - Příklad eBGP

K navázání eBGP je potřeba splnění několika podmínek:

- ASN zadané na konci příkazu *neighbor remote-as* musí souhlasit s ASN zadaném na druhém směrovači na konci příkazu *router bgp*,
- směrovače musí mít rozdílné RID,
- pokud je nakonfigurována autentizace, musí její kontrola proběhnout bez problému,
- musí být navázáno TCP spojení mezi IP adresou směrovače a IP adresou zadanou v příkazu *neighbor remote-as*.

Možnosti volby RID jsou stejné jako u EIGRP nebo OSPF. RID je vybráno ve stejném pořadí (konfigurované RID, nejvyšší adresa aktivního loopback rozhraní, nejvyšší adresa aktivního rozhraní). Jediný rozdíl je v příkazu, kterým lze RID ručně konfigurovat (příklad pro konfiguraci BGP RID 10.10.10.10 v ASN 15):

```
R1(config)#router bgp 15
R1(config-router)#bgp RID 10.10.10.10
```

Případná autentizace je zajištěna pomocí MD5 hashe po konfuguraci následujícím příkazem (v ASN 15, pro souseda 10.10.10.20, autentizační heslo passw). Konfigurace musí analogicky proběhnout na obou sousedních směrovačích:

```
R1(config)#router bgp 15
R1(config-router)#neighbor 10.10.10.20 password passw
```

Splnění podmínky navázání TCP spojení mezi směrovači je u předcházejícího příkladu splněno díky přímému spojení směrovačů a konfiguraci sousedství na základě IP adres rozhraní, které toto spojení zajišťují. Zajištění úspěšného navázání TCP spojení ale může v některých situacích vyžadovat další konfiguraci.

5.4.1 Redundantní spojení eBGP

Při základní konfiguraci směrovač navazuje TCP spojení podle adresy odchozího rozhraní se zadanou adresou směrovače, který se má stát sousedem. Při použití přímých spojení a konfiguraci IP adres protějších rozhraní tedy nenastane žádný problém. Pokud mezi směrovači existuje více fyzických spojení a jedno z nich selže (následkem bude deaktivace rozhraní), může selhat i TCP spojení, protože jeho provoz je možný pouze na aktivních rozhraních. Pro spolehlivou konfiguraci redundantního spojení eBGP je možné použít dvě možnosti.

První možností je vytvoření více sousedství mezi stejnými směrovači. Pro každé fyzické spojení mezi směrovači je možné vytvořit nové sousedství. Tím bude zajištěna spolehlivost i v případě selhání jednoho spojení. Nevýhoda vychází z podstaty každého sousedství, protože v každém sousedství se vyměňují BGP aktualizace a v tomto případě by se mezi dvěma směrovači vyměňovaly informace vícekrát.

Lepší možností je vytvoření TCP spojení mezi loopback rozhraními směrovačů. Vytvoří se tak jediné sousedství mezi směrovači a TCP spojení v případě selhání fyzické linky

zůstane zachováno. Postup konfigurace na každém směrovači se dá rozdělit na několik kroků:

- konfigurace loopback rozhraní,
- zajištění, aby směrovače znaly cesty k loopback rozhraní souseda, například pomocí statických cest nebo některého z IGP,
- konfigurace sousedství probíhá pomocí IP adres loopback rozhraní a obsahuje další dva příkazy pro nastavení zdrojové adresy TCP spojení a možnosti navazovat eBGP na vzdálenost více zařízení třetí vrstvy modelu OSI. V příkladu jsou použity tyto údaje: vlastní ASN 11, IP adresa vlastního loopback rozhraní 192.168.1.1, ASN souseda 21, IP adresa loopback rozhraní souseda 192.168.2.1.

```
R1(config)#router bgp 11
R1(config-router)#neighbor 192.168.2.1 remote-as 21
R1(config-router)#neighbor 192.168.2.1 update-source 192.168.1.1
! (možno využít například i #neighbor 192.168.2.1 update-source
! loopback 1)
R1(config-router)#neighbor 192.168.2.1 ebgp-multihop 2
```

V základní konfiguraci BGP přiřazuje každému IP paketu hodnotu TTL=1 (Time-To-Live) a paket opouští zdrojový směrovač s touto hodnotou. Cílový směrovač paket přijme na fyzickém rozhraní a po zjištění, že paket není pro toto rozhraní určen, je paket ve směrovači předán logice směrování. Ta zjišťuje výstupní rozhraní směrovače na cestě k cíli a jako výstupní rozhraní označí loopback. Poté je ale paketu snížena hodnota TTL na nulu a paket je zničen. Na loopback rozhraní se tedy paket nedostane. (ODOM, 2010)

Proto je potřeba příkazem *neighbor ebgp-multihop* nastavit základní TTL alespoň na hodnotu 2. V tom případě pak cílový směrovač před předáním paketu na loopback rozhraní pracuje s hodnotou TTL=1 a paket je tomuto rozhraní předán.

5.4.2 Typy BGP zpráv

Pro navázání sousedství, jeho udržení a následnou komunikaci BGP sousedů slouží čtyři druhy BGP zpráv:

- Open – používáno pro navázání spojení mezi sousedy a výměnu základních parametrů jako je ASN nebo autentizace,
- Keepalive – odesílána periodicky pro udržení sousedství,
- Update – slouží pro výměnu síťových cest a jejich PA,
- Notification – signalizuje BGP chybu, po této zprávě většinou následuje nový pokus o navázání sousedství.

5.4.3 Ověření funkčnosti spojení eBGP

BGP sousedství má podobně jako OSPF několik stavů. U BGP je základem sousedství navázání TCP spojení, poté výměna BGP Open zpráv, které mají podobnou funkci jako OSPF Hello zprávy, a poté se kontrolují parametry, aby se směrovače mohly stát svými sousedy. Pokud jsou tyto parametry ověřeny, směrovače by měly dosáhnout stavu

Established. Teprve poté si směrovače vymění BGP aktualizace, které obsahují informace o síťových cestách. BGP rozlišuje těchto 6 stavů sousedství (ODOM, 2010):

- Idle – proces je administrativně vypnut nebo čeká na další pokus o navázání spojení,
- Connect – proces čeká na dokončení TCP spojení,
- Active – TCP spojení bylo navázáno, ale zatím nebyla odeslána žádná BGP zpráva,
- Opensent – byla odeslána BGP Open zpráva sousedovi, ale zatím nebyla přijata tato zpráva od souseda,
- Openconfirm – Open zpráva byla odeslána i přijata, další kroky jsou přijetí Keepalive nebo Notification zprávy pro potvrzení nebo vyvrácení shody parametrů sousedství,
- Established – všechny parametry souhlasí, sousedství je navázáno a následně mohou být vyměněny BGP aktualizace.

Stav, ve kterém se sousedství nachází, je možné zobrazit následujícími příkazy (ve druhém příkazu pouze pro souseda s IP adresou 192.168.2.1):

```
R1#show ip bgp summary
R1#show ip bgp neighbors 192.168.2.1
```

Spojení mezi BGP sousedy lze kromě úplného zrušení také odstavit. To může být užitečné v případě, kdy je potřeba sousedství vypnout pouze na nějaký čas a následně ho opět obnovit. Toho lze docílit následujícími příkazy (vlastní ASN 11, pro souseda 192.168.2.1):

```
R1(config)#router bgp 11
R1(config-router)#neighbor 192.168.2.1 shutdown
R1(config-router)#no neighbor 192.168.2.1 shutdown
```

Pokud je sousedství úspěšně navázáno, je několik možností, jak zobrazit cesty, které směrovač zná díky protokolu BGP (příkazy lze upravit podle vlastních požadavků):

- všechny cesty, které směrovač zná pomocí BGP:
  ```
  R1#show ip bgp
  R1#show ip bgp longer-prefixes
  ```
- všechny defaultní cesty:
  ```
  R1#show ip bgp 0.0.0.0 0.0.0.0
  ```
- všechny cesty přijaté od konkrétního souseda:
  ```
  R1#show ip bgp neighbors 192.168.2.1 received-routes
  ```
- cesty od konkrétního souseda po aplikaci vstupních filtrů:
  ```
  R1#show ip bgp neighbors 192.168.2.1 routes
  ```
- cesty odesílané sousedovi po aplikaci výstupních filtrů:
  ```
  R1#show ip bgp neighbors 192.168.2.1 advertised-routes
  ```
- shrnutí počtu naučených cest:
  ```
  R1#show ip bgp summary
  ```

5.5 Vložení podnikových cest do BGP z důvodu šíření cest pro ISP

Ve chvíli, kdy podniková síť používá BGP při směrování dat do Internetu, je zároveň výhodné šířit přes BGP vlastní cesty, které zajistí tok dat z prostředí Internetu do podnikové sítě. Existují dvě základní možnosti, jak zajistit, aby BGP znal a šířil informace o podnikových sítích: příkaz *network* a redistribuce informací z IGP nebo statických cest. Obě možnosti mají stejný cíl, šířit pouze veřejné adresy a nejlépe šířit pouze jednu adresu, která zahrne všechny veřejné adresy v podniku.

5.5.1 Vložení cest do BGP příkazem network

U IGP po zadání příkazu *network* směrovač kontroluje, které IP adresy vlastních rozhraní vyhovují adrese a masce sítě zadané pomocí tohoto příkazu. Směrovač následně aktivuje daný IGP na všech rozhraních, které zadání vyhovují.

U BGP tento příkaz funguje jiným způsobem. BGP porovnává zadanou adresu a masku se záznamy ve směrovací tabulce směrovače. Všechny záznamy směrovací tabulky, které odpovídají zadaným parametrům, následně směrovač přenese i do BGP tabulky. V základní konfiguraci směrovač přenáší pouze záznamy, ve kterých se adresy a masky přesně shodují. Pokud je potřeba přenést například dvě sítě 190.135.0.0/24 a 190.135.1.0/24, je nutné zadat příkaz *network* pro každou z těchto sítí. Pokud bude zadána adresa 190.135.0.0/23, v základní konfiguraci nebude do BGP tabulky přenesena žádná z požadovaných sítí.

Po přenesení sítí do BGP tabulky je zajištěno šíření cest a možnost směrování do těchto sítí pomocí BGP. Záznamy uložené v BGP tabulce lze zobrazit příkazem:

```
R1#show ip bgp
```

Možností, jak do BGP tabulky zanést cestu zahrnující více sítí, je vytvoření souhrnné statické cesty s výstupním rozhraní null0. V případě předchozího příkladu by bylo možné vytvořit statickou cestu do sítě 190.135.0.0/23 na rozhraní null0. Poté by bylo možné příkazem *network* přenést tuto cestu do BGP tabulky. Cesta by tím byla vytvořena a ve chvíli, kdy by směrovač obdržel data s cílem v jedné z uvedených sítí, by směrovač vybíral nejlépe vyhovující cestu, takže by data přeposlal do konkrétní sítě. Na rozhraní null0 by data směrována nebyla.

Příkaz *network* nabízí ještě jednu možnost jak cesty sumarizovat. Tuto možnost lze použít při vynechání nepovinného parametru, který určuje masku sítě, a při zapnutí automatické sumarizace BGP cest (která je v základní konfiguraci vypnutá). Tato sumarizace následně funguje pouze pro zanesení IP adresy sítě se základní maskou dané třídy sítě do BGP tabulky. Nezávisle na nastavení automatické sumarizace se při vynechání masky v příkazu *network* hledá ve směrovací tabulce záznam, který odpovídá zadané adrese se základní maskou dané třídy sítě. Pouze v případě zapnuté automatické sumarizace se následně hledají i podsítě spadající do zadané sítě se základní maskou třídy. Pokud je odpovídající podsíť nalezena, je do BGP tabulky zanesen záznam odpovídající síti zadané v příkazu *network* se základní maskou třídy sítě. Vždy, pokud je zadána maska sítě (i když se

shoduje se základní maskou třídy), se hledá pouze přesně odpovídající záznam ve směrovací tabulce a sumarizace není uplatněna.

Pokud by ve směrovací tabulce směrovače byly například tyto podsítě: 6.1.0.0/16, 6.2.1.0/24 a 6.226.128.0/17, je možné je do BGP tabulky přenést jako jeden záznam odpovídající hodnotě 6.0.0.0/8 pomocí těchto příkazů (pro směrovač v ASN 11):

```
R1(config)#router bgp 11
R1(config-router)#no auto-summary
R1(config-router)#network 6.0.0.0
```

V příkladu je důležité vynechání masky, protože i v případě zadání základní masky 255.0.0.0 by směrovač ve směrovací tabulce hledal pouze záznamy přesně odpovídající zadání. V příkladu takový záznam není uveden, takže by se do BGP tabulky nepřeneslo nic.

5.5.2 Redistribuce cest

Pomocí redistribuce je možné přenést cesty, které směrovač zná z jiných zdrojů, do BGP, aby byly šířeny dále. Je potřeba vybrat pouze cesty s veřejnými adresami a důležitou roli zde má také sumarizace, protože směrovač obvykle zná velké množství cest a adres sítí, které je ale potřeba do Internetu přenášet jako jednu cestu, případně co nejméně cest. Sumarizaci těchto adres je možné zajistit několika způsoby:

- šíření sumární cesty již v IGP,
- vytvoření statické sumární cesty s výchozím rozhraním null0 a redistribuce pouze této statické cesty (směrování dat následně bude fungovat díky konkrétnějším cestám do jednotlivých sítí),
- sumarizace cest přímo v BGP příkazem *aggregate-address*.

Všechny možnosti redistribuce cest mezi protokoly budou vysvětleny v sedmé kapitole.

5.5.3 Směrovací mapy

Po zanesení cest do BGP je často potřeba, aby dále nebyly šířeny všechny cesty, které má daný směrovač uloženy v BGP tabulce. V případě podnikové sítě s několika směrovači využívajícími BGP se mohou šířit informace o sítích mezi směrovači, případně i o dalších vnitřních sítích, které by neměly být dostupné z Internetu. Cesty do těchto sítí by obecně neměly být šířeny do Internetu, zvláště pokud mají soukromé adresy. Řešením je filtrování cest na místě eBGP spojení podnikové sítě s ISP pomocí směrovacích map.

Dalším důvodem pro filtrování cest může být zamezení toho, aby se podnikový AS stal tranzitním. Pokud je podnikový AS připojen přes různá eBGP do jiných AS a šíří mezi nimi všechny cesty, ostatní směrovače do podnikového AS mohou zasílat data, která mají cíl jinde v Internetu, a podnikový AS by tato data pouze přeposlal do dalšího AS. Přeposílání dat zvyšuje zátěž směrovačů a v podnikové sítí je nežádoucí.

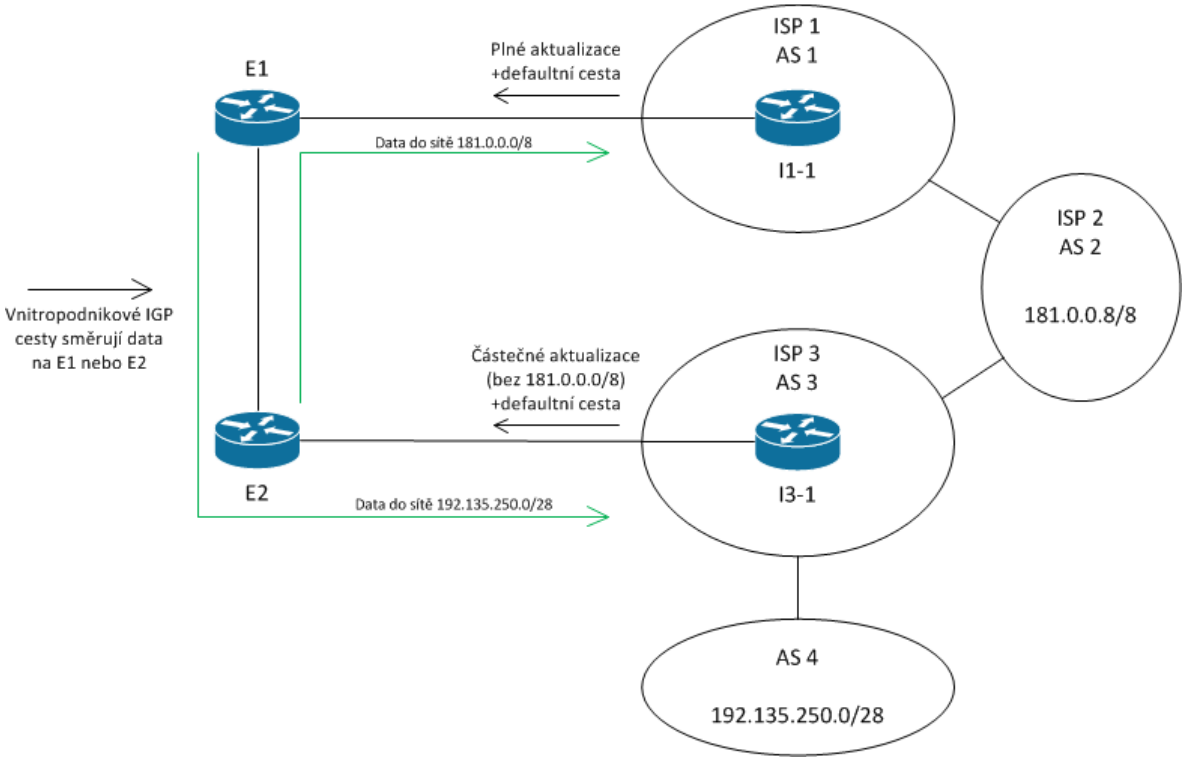
V následujícím příkladu je uvedeno šíření cesty do jediné sítě (81.2.5.0/24) přes eBGP, ostatní cesty jsou filtrovány. Směrovací mapa s názvem *only-5* k tomu využívá *prefix-list*

číslo 5, ve kterém je povolena konkrétní síť a ostatní jsou defaultně zakázány. V případě filtru adres šířených k sousedovi je v konfiguraci důležité uvést směr *out*. Při potřebě filtrovat příchozí aktualizace je možné využít směr *in*. Více informací o směrovacích mapách je uvedeno v podkapitole 7.4.

```
R1(config)#router bgp 10
R1(config-router)#neighbor 52.23.14.15 remote-as 11
R1(config-router)#neighbor 52.23.14.15 route-map only-5 out
R1(config)#route-map only-5 permit
R1(config-route-map)#match ip address prefix 5
R1(config)#ip prefix-list 5 permit 81.2.5.0/24
```

5.6 Interní sousedství v BGP

Pokud je v podnikové síti více směrovačů připojených k ISP, je potřeba, aby se tyto podnikové směrovače staly svými sousedy. Protože směrovače jsou ve stejném AS, jedná se o interní sousedství iBGP. To je potřebné zejména kvůli tomu, aby si směrovače vyměnily informace o svých cestách a věděly, který směrovač by měl být pro konkrétní cílovou adresu směrem z podnikové sítě výstupní z důvodu nejlepší cesty ke konkrétní cílové síti.



Obrázek 16 - Volba nejlepší cesty do konkrétních sítí

Obrázek 16 znázorňuje tok dat z podnikové sítě do různých cílových sítí. Podnikové směrovače díky iBGP ví, který ISP má lepší cesty do cílových sítí, a data jsou podle toho směrována. V obrázku je také naznačeno, které cesty jsou od ISP poskytovány. Od ISP1 jsou poskytovány úplné a od ISP2 částečné BGP aktualizace. V základní konfiguraci je za lepší cestu považována ta, která prochází přes nejméně AS. Proto jsou data do sítě

192.135.25.0/26 zasílána přes E2. Data do sítě 181.0.0.0/8 jsou zasílána přes E1, protože ISP1 nabízí BGP aktualizace s konkrétní cestou do této sítě a ISP3 pro cestu do této sítě nabízí pouze defaultní cestu.

Při porovnání záznamů o síti 181.0.0.0/8 v BGP tabulkách směrovačů E1 a E2 nalezneme pouze jediný rozdíl – směrovač E1 má cestu uloženou jako externí (naučenou přes eBGP), směrovač E2 jako interní (naučenou přes iBGP). Tento rozdíl se následně může projevit v použití různých PA při výběru nejlepších cest. Ostatní informace o cestě jsou v BGP tabulce stejné včetně atributu Next Hop, který označuje nejbližší eBGP směrovač na cestě k cílové síti.

Aby při šíření cest pomocí BGP nevznikaly problémy a smyčky, řídí se směrovače dvěma pravidly:

- směrovače v BGP aktualizacích šíří pouze nejlepší cestu,
- v rámci iBGP se nešíří cesty naučené přes iBGP. To znamená, že směrovač uvnitř jednoho AS nešíří cesty, které se pomocí BGP naučil v rámci svého AS od jiných směrovačů. Toto pravidlo má podobný základ jako Split Horizon, i když se tak v BGP nenazývá.

Konfigurace iBGP je v podstatě stejná jako konfigurace eBGP, jako atribut *remote-as* se uvádí ASN, které je pro oba směrovače stejné:

```
R1(config)#router bgp 11
R1(config-router)#neighbor 10.10.10.20 remote-as 11
R2(config)#router bgp 11
R2(config-router)#neighbor 10.10.10.10 remote-as 11
```

Stavy sousedství a ostatní konfigurace, jako je autentizace nebo spojení mezi loopback rozhraními, jsou stejné jako v případě eBGP.

5.6.1 Podstata Next Hop adresy

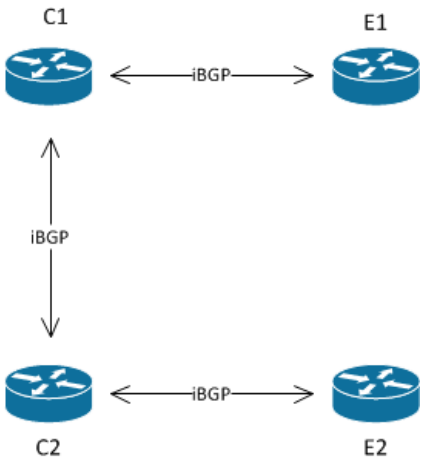
Jak již bylo zmíněno, Next Hop adresa určuje první směrovač mimo vlastní AS, který je na cestě k cílové síti. Koncept je zde tedy jiný než u IGP, kde Next Hop je vždy v přímo připojené síti. U BGP to tak být nemusí a směrovač tedy nemusí znát ani cestu k Next Hop směrovači. Aby bylo zajištěno správné směrování dat, existují dvě možnosti řešení:

- Vytvoření záznamu ve směrovací tabulce směrovače s cestou k Next Hop směrovači. To v praxi většinou znamená vytvoření statické cesty k ISP směrovači nebo použití IGP mezi podnikovými směrovači a směrovači ISP.
- Nastavení iBGP sousedství s parametrem *next-hop-self*, který zajistí šíření cest se změněnou adresou Next Hop na adresu konfigurovaného směrovače. V praxi to znamená, že směrovač, který se naučí cesty z eBGP a bude konfigurován jako *next-hop-self*, bude v rámci iBGP šířit cesty s vlastní adresou v Next Hop. Směrovače, které takovou informaci dostanou, již mají cestu k tomuto směrovači a data mu přepošlou. Konfigurovaný směrovač ale má ve své BGP tabulce původní adresu Next Hop a data na tuto adresu přepošle. Konfigurace je jednoduchá:

```
R1(config)#router bgp 11
R1(config-router)#neighbor 10.10.10.20 remote-as 11
R1(config-router)#neighbor 10.10.10.20 next-hop-self
```

5.6.2 Správné vytvoření iBGP

Jak již bylo na začátku kapitoly popsáno (Obrázek 14), pro předejití vzniku směrovacích smyček v některých případech nestačí vytvořit iBGP pouze mezi směrovači, které jsou přímo připojené k ISP. Při bližším zkoumání předchozího příkladu by se mohlo jako správné zdát řešení, které zobrazuje následující obrázek (Obrázek 17).



Obrázek 17 - Nedostatečné spojení iBGP mezi podnikovými směrovači

Bohužel ani toto řešení není dostatečné z důvodu, který byl již také nastíněn. Směrovače v iBGP nešíří cesty, které se v iBGP naučily. To znamená, že C1 dále nepřepošle cesty naučené od E1, C2 nepřepošle cesty od E2 atd. Jediné správné řešení je vytvoření sousedství mezi všemi směrovači navzájem způsobem mesh. Každý směrovač tedy naváže 3 sousedství a celkem jich mezi 4 směrovači bude 6.

5.7 Proces výběru nejlepší cesty

Volba cesty pomocí BGP závisí na hodnotách PA a některých dalších vlastnostech jednotlivých cest. Pokud existuje více možných cest do cílové sítě, BGP postupně porovnává jednotlivé PA a vlastnosti různých cest, dokud nenarazí na jejich rozdílné hodnoty. Poté směrovač pošle data cestou, která nabízí lepší hodnotu daného atributu. Směrovač tedy nemusí pro každou cílovou síť porovnávat všechny atributy různých cest, pokud v průběhu porovnávání narazí na rozdílnou hodnotu stejného atributu. Pořadí porovnávání atributů je jasně dané (ODOM, 2010):

- NEXT_HOP – porovnává se dostupnost next-hop směrovače. Pokud není známa cesta k adrese next-hop, nelze cestu do cílové sítě použít.
- Weight – atribut, který není definován v RFC, je podporován pouze směrovači Cisco a je uložen pouze na daném směrovači, není šířen ostatním. Větší hodnota tohoto čísla preferuje danou cestu.

- LOCAL_PREF – atribut, který je šířen v rámci jednoho AS, větší hodnota preferuje danou cestu.
- Směrovač preferuje cesty, které do BGP zanesl sám, před cestami naučenými přes iBGP nebo eBGP (tato vlastnost není dána konkrétním PA).
- AS_PATH – menší počet ASN v AS_PATH znamená pro BGP lepší cestu.
- ORIGIN – pořadí pro preferenci cest je I, E, ?. Atribut označuje zdroj, z jakého byla cesta do BGP zanesena. Může to být IGP, EGP nebo neznámý zdroj.
- MED (Multi Exit Discriminator) – atribut, kterým lze ovlivnit směrování do vlastního AS. Menší číslo znamená lepší cestu a toto číslo směrovač šíří do jiných AS, aby směrovače v jiných AS mohly tuto cestu preferovat nebo ji používat pouze jako záložní.
- Typ sousedství – BGP vždy preferuje cestu přes eBGP před cestou iBGP.
- IGP metrika k next-hop směrovači – pokud není rozdíl mezi cestami při předchozím porovnávání, uloží si směrovač do směrovací tabulky cestu, u které eviduje menší metriku cesty k next-hop směrovači.
- V některých případech se může stát, že ani po porovnání všech předchozích vlastností nebude nejlepší cesta vybrána. IGP by podobnou situaci mohly řešit vybráním a použitím více různých cest. BGP ale vždy vybírá pouze jednu jedinou cestu, kterou bude dále šířit svým sousedům (do směrovací tabulky může BGP po konfiguraci uložit i více cest). Proto při shodě předchozích vlastností BGP postupně vybírá cestu podle dalších kritérií, která už s kvalitou cesty nebo s řízeným výběrem nesouvisí:
    - nejdéle známá cesta přes eBGP,
    - nejnižší BGP RID souseda,
    - nejnižší IP adresa souseda.

Je nutno dodat, že hodnoty všech číselných BGP vlastností (Weight, Local_pref, MED) mají pro všechny cesty stejné defaultní hodnoty. Směrovače hodnoty těchto vlastností mohou změnit pouze na základě přímé konfigurace těchto hodnot. Z výčtu možností, které BGP bere v úvahu při výběru nejlepší cesty, tedy vyplývá, že při základní konfiguraci se směrovač většinou rozhoduje na základě dvou vlastností cest: délky AS_PATH a typu sousedství, ze kterého se směrovač cestu naučil. V případě shody těchto vlastností se směrovač rozhoduje na základě IGP metriky k next-hop směrovači.

5.8 Ovlivnění výběru cesty konfigurací

BGP neumožňuje změnu všech informací, které si o cestách uchovává, přesto je možné výběr cest efektivně ovlivnit. Obecně je možné ovlivňovat 3 PA: Local_pref, AS_Path a MED. Cisco směrovače navíc umožňují měnit hodnotu vlastnosti Weight, která není na směrovačích jiných výrobců implementována. Před konfigurací je potřeba si uvědomit pořadí, v jakém dochází k porovnávání vlastností cest a které vlastnosti je potřeba ovlivnit, aby bylo dosaženo požadovaného výsledku. Zároveň je každá vlastnost v BGP použita

odlišně a jejich použití závisí i na požadavku ovlivnění cest z podnikové sítě do Internetu nebo opačně.

5.8.1 Směrovací mapy

Pro využití všech možností pro ovlivnění výběru cesty je potřeba využívat směrovací mapy, které umožňují konfigurovat vlastnosti jednotlivých cest. Směrovací mapa se skládá z příkazů pro povolení nebo zakázání konkrétních cest. Protože cesty, které nevyhovují žádnému příkazu *match* ve směrovací mapě, jsou odmítnuty a filtrovány, je pro správné použití všech dostupných cest potřeba na konec směrovací mapy vložit příkaz, který povolí všechny cesty.

Příkazy ve směrovací mapě mají pořadová čísla, která určují pořadí vykonání těchto příkazů. Pokud cesta vyhovuje určitému příkazu *match*, vykonají se pro cestu příkazy, které jsou zde přiřazeny. Ostatní příkazy *match* se již pro konkrétní cestu nekontrolují. Směrovací mapa tedy využívá posloupnosti příkazů a pro určitou cestu se provede vždy jen první vyhovující skupina příkazů. Cesty, na které se mají konfigurovaná nastavení aplikovat, lze vybrat podle různých kritérií. Nejjednodušší možností pro výběr cest, které se mají ovlivnit, je využití *prefix-list*.

Vytvořenou směrovací mapu je potřeba aplikovat na určité sousedství se zvoleným směrem, kterým se šíří cesty, které se mají ovlivnit. Pro ovlivnění cest, které se směrovač učí od jiného směrovače, je potřeba zvolit směr *in*. Cesty, kterým má být nastaven atribut MED, který ovlivňuje cesty směrující k danému směrovači a které se od směrovače učí ostatní, musí mít zvolen směr *out*. Konkrétní příklady konfigurace jsou uvedeny dále u vysvětlení ovlivnění daných vlastností.

5.8.2 Konfigurace vlastnosti Weight

Vlastnost Weight je interní informace určitého směrovače a její hodnota není šířena ostatním směrovačům. Proto dokáže na jednom směrovači ovlivnit výběr cesty z více různých možností a přitom neovlivní ostatní části sítě. V podnikové síti lze tuto vlastnost použít například pro výběr cesty pro data směřující z podniku do Internetu. Lze takto například preferovat určitého ISP před ostatními. Hodnota vlastnosti Weight může nabývat hodnot 0 – 65 535 a směrovač jako lepší cestu vybírá cestu s vyšší hodnotou Weight. Defaultní hodnota je 0 pro naučené cesty a 32 768 pro cesty, které směrovač do BGP zanesl sám.

Možnosti konfigurace vlastnosti Weight jsou dvě:

- Pro všechny cesty naučené od určitého souseda (příklad pro ASN 11, souseda 10.10.10.20 a novou hodnotu Weight 20 000):
  ```
  R1(config)#router bgp 11
  R1(config-router)#neighbor 10.10.10.20 weight 20000
  ```
- Konfigurace různých hodnot pro různé cesty, které jsou přijaty od jednoho souseda, je možná pomocí směrovací mapy. Konfigurace pro nastavení hodnoty Weight podobně jako v předchozím příkladu, ale pouze pro cesty do sítě 10.0.0.0/8, může

vypadat následovně:

```
R1(config)#ip prefix-list match-10 permit 10.0.0.0/8
R1(config)#route-map set-weight-20k permit 10
R1(config-route-map)#match ip address prefix-list match-10
R1(config-route-map)#set weight 20000
R1(config)#route-map set-weight-20k permit 20
R1(config)#router bgp 11
R1(config-router)#neighbor 10.10.10.20 route-map set-weight-20k in
```

Příkaz *route-map set-weight-20k permit 20* je důležitý právě pro povolení šíření aktualizací o všech cestách. Bez tohoto příkazu by všechny cesty, které předtím nebyly směrovací mapou odchyceny a povoleny, byly filtrovány a směrovač by je nepřijmul a nevložil si je do BGP tabulky.

5.8.3 Konfigurace atributu Local_pref

Local_pref je PA, to znamená, že na rozdíl od vlastnosti Weight je šířen v BGP aktualizacích ostatním směrovačům. Omezení šíření je určeno na jeden AS. Tento atribut se v podnikové síti využívá při připojení více ISP tak, aby všechny BGP směrovače uvnitř AS znaly cestu, která je do dané cílové sítě nejlepší. Lze takto poměrně jednoduše ovlivnit, kterou cestou budou odesílána všechna data z AS směřující do určité sítě. Defaultní hodnota Local_pref je 100 a může nabývat hodnot od 0 do 2^{32}-1. Preferovány jsou cesty s vyšší hodnotou. Hodnotu Local_pref může nastavovat pouze směrovač, který cesty zanáší do AS ze sousedství eBGP.

Konfigurace je možná dvěma způsoby:

- změnou defaultní hodnoty, která bude použita pro všechna eBGP (příklad pro ASN 11 a novou hodnotu Local_pref 500):

  ```
  R1(config)#router bgp 11
  R1(config-router)#bgp default local-preference 500
  ```

- pomocí směrovací mapy. Konfigurace je podobná jako při nastavení Weight, ale sousedství musí být eBGP, směr aktualizací je také *in*. Příkaz *set* může vypadat takto:

  ```
  R1(config-route-map)#set local-preference 500
  ```

5.8.4 Možnosti změny atributu AS_Path

Atribut AS_Path na rozdíl od předchozích sám BGP ovlivňuje a jeho hodnotu mění vždy při šíření cesty přes eBGP. Proto je potřebné při jeho nastavení dávat větší pozor, aby při směrování dat nenastaly problémy. BGP používá AS_Path jako prevenci před vznikem směrovacích smyček, proto by nebylo dobré z tohoto atributu informace mazat. Možnost ovlivnění výběru cesty změnou hodnoty tohoto atributu spočívá v přidání dalších ASN k informacím, které atribut již obsahuje. Tím BGP vyhodnotí danou cestu jako horší, protože cesta obsahuje více AS než ta původní.

Aby tato cesta zůstala zachována a aby v případě jejího použití nebyla data směrována jinou cestou (v nejhorším případě by data nemusela být doručena), je potřeba zvolit přidání ASN, které už cesta obsahuje. Nejlepší možností je vložení vlastního ASN nebo číslo AS,

ze kterého byla cesta přijata. Pokud směrovač patří do AS 11 a cestu se naučil z AS 12, je dobré použít jedno z těchto čísel.

ASN se přidávají na začátek AS_Path a konfigurace je možná pomocí směrovací mapy s příkazem *set* (vložení dvou ASN 12):

```
R1(config-route-map)#set as-path prepend 12 12
```

Díky tomu, že se hodnota tohoto atributu šíří i do jiných AS, je možné změnou AS_Path ovlivnit cesty směřující z AS do Internetu i cesty z Internetu do AS. V obou případech je nejlepší ovlivnit tento atribut na směrovačích u sousedství eBGP. V prvním případě s nastavením směrovací mapy sousedství se směrem in, ve druhém případě se směrem *out*.

5.8.5 Konfigurace atributu MED

Na rozdíl od předchozích možností pro ovlivnění výběru cesty slouží MED pouze pro cesty směřující do vlastního AS. MED tedy do sousedních AS šíří informace o tom, která cesta by měla být vybrána pro směrování dat do vlastního AS. Dobře toho lze využít pouze při využití Dual homed připojení k Internetu, tedy při připojení více linkami k jednomu ISP, případně při využití Multihomed připojení, kdy je AS připojeno přes více ISP, ty ale spolu musí spolupracovat. V případě připojení k více ISP, které spolu nespolupracují, nelze příchozí cestu ovlivnit, protože MED není dalším AS propagován a je šířen pouze v rámci AS, které přímo sousedí s AS, který MED do cesty zanesl.

Směrovače v sousedních AS preferují cestu s menší hodnotou MED. Tato hodnota může být v rozsahu od 0 do 2^{32}-1 a defaultně je nastavena na 0. V konfiguraci směrovačů i ve výpisech příkazu *show* je MED označen jako *metric* a konfiguruje se pomocí směrovací mapy (v příkladu různý MED pro 2 sousedy pro všechny cesty):

```
R1(config)#route-map med-to-20 permit 10
R1(config-route-map)#set metric 10
R1(config)#route-map med-to-30 permit 10
R1(config-route-map)#set metric 20
R1(config)#router bgp 11
R1(config-router)#neighbor 10.10.10.20 route-map med-to-20 out
R1(config-router)#neighbor 10.10.20.30 route-map med-to-30 out
```

5.9 Vymazání BGP sousedství

Specifickou vlastností u BGP sousedství je uchování všech původních cest, které směrovač zná, i po zapnutí filtrů a směrovacích map, které šíření cest omezují nebo ovlivňují. V praxi to například znamená, že pokud si dva směrovače vyměňují kompletní BGP aktualizace a následně jeden ze směrovačů aplikuje směrovací mapu nebo začne šířit pouze defaultní cestu, druhý směrovač si může uchovat původní cesty a používat je. Tato vlastnost může být nežádoucí a dá se omezit vymazáním sousedství. K tomuto vymazání může dojít například restartováním směrovače, administrativním restartováním BGP sousedství nebo pomocí příkazu *clear ip bgp*. Vymazání sousedství se dělí na dva druhy – tvrdé a měkké. Při tvrdém vymazání dochází k odpojení sousedství (včetně TCP spojení) a opětovnému navázání. Při měkkém vymazání k odpojení nedochází a pouze se smažou

některé BGP informace. Příkaz *clear ip bgp* nabízí různé možnosti především měkkého vymazání, v přehledu jsou uvedeny ty základní:

- `R1#clear ip bgp *` - tvrdé vymazání všech BGP sousedství,
- `R1#clear ip bgp 10.10.10.20` – tvrdé vymazání sousedství se sousedem s RID 10.10.10.20
- `R1#clear ip bgp 10.10.10.20 out` – vymazání výstupních cest ke stejnému sousedovi,
- `R1#clear ip bgp * soft` – měkké vymazání všech sousedství.

6 Porovnání IGP a EGP protokolů

Všechny rozdíly mezi IGP a EGP protokoly vycházejí z rozdílnosti účelu jejich použití. Úkolem EGP je směrovat data mezi AS. O topologii AS nemají žádné informace. Důležité tedy je nasměrovat data na některý z hraničních směrovačů, další směrování v rámci jednoho AS je již úkolem IGP. EGP zároveň nemusí využívat nejkratší nebo nejrychlejší cestu k cílovému AS, páteřní linky v Internetu a konektivita mezi nimi je draze placena a tím je ovlivněno i směrování dat. Ty jsou směrovány pouze k těm směrovačům, ke kterým má ISP zaplacenou linku. To v praxi znamená, že data mohou být posílána poměrně nákladnou (z pohledu logiky IGP) cestou. Oproti IGP má EGP zároveň mnohem více možností nastavení pro výběr cest a nerozhoduje se pouze na základě jednoho údaje, kterým je pro IGP nejlepší metrika. Na druhou stranu EGP nesleduje informace o cestách, jako je počet směrovačů na cestě k cíli, šířka pásma daného spoje nebo zpoždění, které na cestě vzniká.

V případě opomenutí účelu EGP a nasazení např. protokolu BGP v podnikové síti bez účasti jiných směrovacích protokolů brzy vyjde najevo, že pro funkčnost sítě je potřeba rozdělit topologii na mnoho AS a je potřeba velké množství konfigurace směrovačů. I v případě bezchybného nastavení protokolu ale mohou data být směrována jiným způsobem, než je očekáváno. Hlavně z důvodu rozsáhlé konfigurace podobné nasazení EGP protokolů ztrácí jakýkoli smysl.

Nasazení IGP protokolů v sítích zahrnujících více AS by se mohlo zdát smysluplnější. IGP se vždy snaží volit nejlepší cestu do cílové sítě a to by mohla být proti EGP výhoda. V tomto případě by problémem u OSPF byla nutnost přímého propojení páteřní oblasti se všemi ostatními, u EIGRP je problém nepoužitelnosti na jiných směrovačích než od společnosti Cisco. Při použití IGP pro směrování ve velkém počtu sítí nastává větší problém kvůli náročnosti na paměť a výkon směrovačů. Tabulky směrovačů v Internetu v dnešní době obsahují kolem 450 000 BGP záznamů o cestách (BGP Reports, 2013). EGP protokoly jsou navržené tak, aby takové množství informací byly schopné zpracovávat s relativně malou náročností na výkon a paměť směrovačů. IGP protokoly toho schopné nejsou a směrování dat v Internetu pomocí IGP je nemožné.

Každý z typů protokolů má svoji určitou úlohu směrování dat uvnitř nebo mezi AS a protokoly nelze zaměňovat. Pro směrování dat mezi dvěma koncovými zařízeními v Internetu nelze použít jeden nebo druhý protokol, ale je potřeba využití obou typů protokolů a jejich spolupráce. Často je potřeba využití výměny naučených cest mezi protokoly. Způsob, jakým protokoly mohou spolupracovat a cesty si vyměňovat, je popsán v následující kapitole.

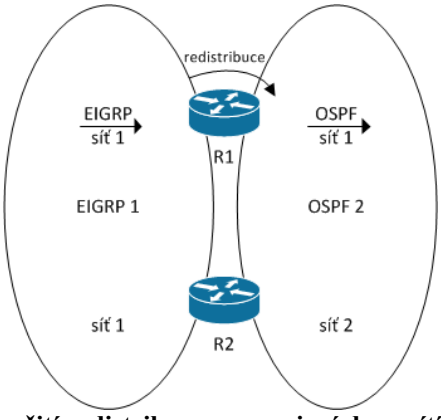
7 Redistribuce cest

Každý protokol má svoji vlastní databázi cest nezávislou na ostatních protokolech, které jsou v síti použity, a žádný protokol nedokáže používat cesty jiných protokolů. Kvůli rozmanitosti Internetu i podnikových sítí je ale nutné, aby si odlišné protokoly mohly cesty mezi sebou vyměňovat. Výměna cest se označuje jako redistribuce a díky ní je zajištěno bezproblémové směrování dat například mezi různými částmi podnikové sítě nebo mezi různými podniky, i když jsou na cestě pro směrování využity různé protokoly.

7.1 Základní využití redistribuce

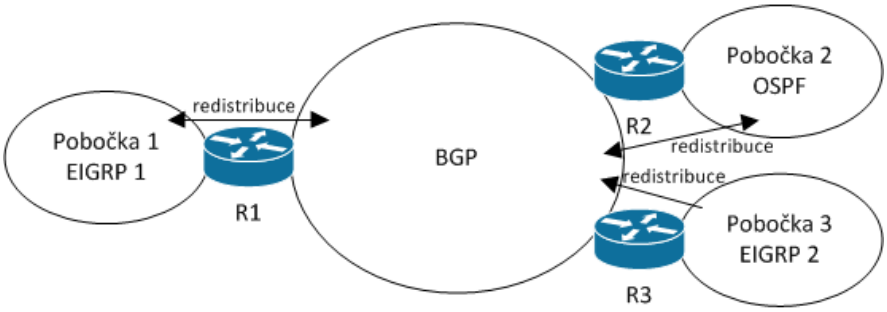
Mimo zmíněného důvodu pro využití redistribuce při použití různých protokolů existují i další. Souhrn nejčastějších důvodů je:

- spojení dvou sítí s různými IGP,



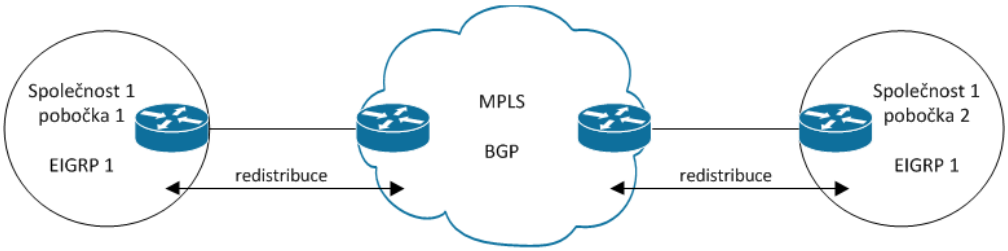
Obrázek 18 - Použití redistribuce pro spojení dvou sítí s různými IGP

- spojení dvou sítí se stejným IGP (redistribuce nemusí probíhat mezi různými protokoly, ale může být využita i při použití jednoho protokolu),
- oddělená správa různých částí podnikové sítě,
- spojení sítí partnerských společností,
- možnost využití směrovačů různých výrobců v jedné síti (například využití EIGRP na Cisco směrovačích a OSPF na směrovačích od jiných výrobců),
- využití redistribuce mezi IGP a EGP u nadnárodních firem s velkými podnikovými sítěmi v různých státech,



Obrázek 19 - Využití redistribuce s BGP v rámci jedné firmy

- použití WAN technologie na 3. vrstvě modelu OSI (například MPLS).



Obrázek 20 - Využití redistribuce s BGP na technologii MPLS

Vzhledem k rozdílnosti protokolů a obecné potřebě používat pro směrování dat pokud možno nejlepší cesty, jsou základní principy redistribuce následující:

- redistribuce cest je určena jako vložení cest do určitého protokolu, vzájemnou redistribuci mezi dvěma protokoly je proto potřeba konfigurovat pro každý protokol zvlášť,
- redistribuce probíhá v rámci jednoho směrovače,
- cesty se redistribuují z údajů uložených ve směrovací tabulce směrovače,
- údaje ze směrovací tabulky se při redistribuci rozlišují podle zdroje, ze kterého byly údaje do tabulky uloženy.

V praxi shrnutí těchto principů znamená konfiguraci, která odpovídá např. požadavku vložit cesty z EIGRP do OSPF protokolu. Konfigurace se provede na jednom směrovači, který vložené cesty může šířit ostatním směrovačům. Cesty, které se do OSPF protokolu vloží, jsou ale závislé na směrovací tabulce. V tabulce s naučenými EIGRP cestami může mít směrovač mnohem více uložených záznamů. Do směrovací tabulky si směrovač ukládá pouze nejlepší cesty a jedině ty se následně mohou přenést do OSPF protokolu. Informace o cestách se také přenášejí pouze ze směrovací tabulky, takže pokud v EIGRP tabulce je o cestě více informací, tak se tyto informace nevyužijí, ale při redistribuci lze další informace explicitně nastavit. Rozlišení cest podle zdroje, ze kterého byly cesty naučeny, mimo jiné znamená také to, že lze redistribuovat informace o statických cestách nebo přímo připojených sítích.

7.2 Možnosti redistribuce mezi IGP a EGP

Motivace pro použití redistribuce s EGP v podnikových sítích při připojení k více ISP byla již zmíněna. Před praktickým využitím této možnosti je ale nutné si uvědomit všechny důsledky tohoto kroku, které vyplývají z vlastností směrovacích protokolů.

Při redistribuci velkého množství adres z EGP do IGP může dojít k zahlcení podnikové sítě a k přetížení podnikových směrovačů. EGP jsou na rozdíl od IGP vyvinuty k efektivní práci s velkým množstvím cest. Žádný IGP neumí efektivně zpracovávat informace o statisících cest, proto je nutné do IGP redistribuovat pouze nejnutnější cesty a co nejvíce využívat defaultní cesty do Internetu.

Pokud je rozhodnuto o použití EGP uvnitř podnikové sítě, je potřeba uvážit počet směrovačů, které budou EGP používat. Jak již bylo vysvětleno, při zvolení malého počtu směrovačů může nastat problém se smyčkami při směrování dat a přístup k Internetu se tak může v části sítě stát nedostupným. Naopak při zapnutí BGP na větším množství směrovačů je obvykle potřeba vytvořit velké množství iBGP spojení a zvláště při příjmu kompletních BGP aktualizacích od ISP si mohou směrovače vyměňovat velké množství informačních dat, které mohou síť zahltit. Je tedy dobré zvolit co nejmenší počet směrovačů s EGP, které ale dokáží eliminovat možné problémy se směrováním dat a dokáží ve spolupráci s IGP vybrat nejlepší cestu při směrování dat z podnikových sítí do Internetu.

7.3 Administrativní vzdálenost

Vzhledem k tomu, že směrovače si ukládají cesty z různých protokolů do směrovací tabulky podle administrativní vzdálenosti protokolů, a zároveň redistribuce mezi protokoly využívá cesty uložené ve směrovací tabulce, je potřeba vědět, které cesty budou s ohledem na svůj zdroj ve směrovací tabulce uloženy. Cesty, které jsou následně redistribuovány a šířeny jiným protokolem, mohou mít administrativní vzdálenosti jiné, než cesty, které si protokol vytvořil sám.

Tabulka 2 - Administrativní vzdálenost protokolů na směrovačích Cisco

Cesta	Administrativní vzdálenost
Přímo připojená	0
Statická	1
Souhrnná cesta EIGRP	5
externí BGP	20
interní EIGRP	90
IGRP	100
OSPF	110
IS-IS	115
RIP	120
EGP	140
ODR	160
externí EIGRP	170
interní BGP	200
Nedosažitelná	255

V případě potřeby je možné administrativní vzdálenost protokolu změnit příkazem *distance* (v příkladu uvedena změna administrativní vzdálenosti BGP v ASN 1 na 112, při výběru cesty tedy bude preferován protokol OSPF před BGP):

```
R1(config)#router bgp 1
R1(config-router)#distance 112
```

Příkaz *distance* nabízí pro různé protokoly různé možnosti a nabízí změnu administrativní vzdálenosti například pouze pro některé adresy sítí.

7.4 Směrovací mapy

Základní redistribuce vždy zahrnuje všechny cesty, které jsou uložené ve směrovací tabulce a mají jeden konkrétní společný zdroj. Pro všechny tyto cesty společně lze upravit některá nastavení jako je metrika nebo je možné označení cest stejnou značkou.

Dalším parametrem při konfiguraci redistribuce může být určení směrovací mapy, která bude při redistribuci na všechny cesty aplikována. Směrovací mapy nabízejí několik možností, jak umožnit konfiguraci redistribuce, která se bude vztahovat ke konkrétním cestám. Nastavením lze ovlivnit například následující možnosti konkrétních cest:

- zakázat redistribuci cesty,
- změnit metriku cesty,
- při redistribuci do OSPF zvolit typ metriky E1 nebo E2,
- přiřadit cestě značku, pomocí které lze následně cestu na jiných směrovačích identifikovat.

Cesty, na které se mají konfigurovaná nastavení aplikovat, lze vybrat podle různých kritérií například těmito příkazy:

- `match interface` – výběr rozhraní, které je pro cestu výstupní,
- `match ip address` – výběr podle cílové adresy cesty, parametrem příkazu je ACL (Access List),
- `match ip address prefix-list` – zahrnuje cesty s cílovými adresami podle pravidel vytvořených v *prefix-list*,
- `match ip next-hop` – určuje cesty podle adresy následujícího směrovače na cestě k cílové síti, parametrem je ACL,
- `match ip route-source` – určuje cesty podle adresy směrovače, který je jejich zdrojem, parametrem příkazu je ACL,
- `match metric` – výběr cesty podle její metriky, atribut lze doplnit znaménky + nebo – pro výběr podle rozsahu metrik,
- `match route-type` – parametrem může být typ cesty internal, external, type-1, type-2, level-1 nebo level-2,
- `match tag` – umožňuje výběr cesty podle vložené značky nebo více značek zapsaných za sebou.

Směrovací mapa se skládá z příkazů pro povolení nebo zakázání konkrétních cest. Při redistribuci jsou zakázané cesty filtrovány a nejsou redistribuovány. Povolená cesta bude vždy redistribuována. Pokud budou této cestě nastaveny některé z možných nastavení, tak budou použity. V případě, že některé nastavení nebude cestě přímo nastaveno, použije se nastavení z příkazu *redistribute*, případně základní nastavení protokolu, do kterého je redistribuce provedena. Pokud cesta nevyhovuje žádnému příkazu *match* ve směrovací mapě, je tato cesta odmítnuta a je filtrována. Pro změnu chování směrovací mapy, aby všechny cesty nevyhovující příkazům *match* byly povoleny,

je možné na konec směrovací mapy vložit příkaz *permit* bez příkazu *match*, který povolí všechny cesty.

Při tvorbě směrovací mapy je potřeba si uvědomit, v jakém pořadí jsou vybírány příkazy, které budou provedeny. Příkazy *match* ve směrovací mapě mají pořadová čísla, která určují pořadí, ve kterém se bude kontrolovat, zda jim daná cesta odpovídá. Pokud cesta příkazu *match* odpovídá, bude pro danou cestu aplikována daná skupina příkazů. Ostatní příkazy *match* se již pro konkrétní cestu nekontrolují. Pro určitou cestu se tedy provede vždy jen první vyhovující skupina příkazů.

7.4.1 Příklad konfigurace směrovací mapy

Při konfiguraci směrovací mapy, která bude sloužit v podnikové síti při redistribuci z jedné pobočky do druhé (obě pobočky využívají OSPF), je potřeba redistribuovat pouze adresy sítě 10.0.0.0/8. Za předpokladu, že pobočky podniku používají různé podsítě rozsahu 10.0.0.0/8, je potřeba zajistit, aby při propojení poboček více směrovači nebyly cesty jedné pobočky vraceny zpět do sítě pobočky přes jiný směrovač, než který cesty redistribuoval do jiné pobočky. To bude zajištěno označkováním cest číslem pobočky a filtrováním těchto cest při redistribuci do sítě stejné pobočky.

```
R1(config)#route-map branch-1-to-2 deny 10
R1(config-route-map)#match tag 2
R1(config)#route-map branch-1-to-2 permit 20
R1(config-route-map)#match ip address only10
R1(config-route-map)#set metric 40
R1(config-route-map)#set tag 1
R1(config)#ip access-list extended only10
R1(config-ext-nacl)#permit ip 10.0.0.0 255.0.0.0 any
```

Stejnou směrovací mapu je možné konfigurovat na obou směrovačích, které provádějí redistribuci, a aplikovat ji na redistribuci z pobočky č. 1 do pobočky č. 2. Tato směrovací mapa má název *branch-1-to-2* a skládá se ze dvou položek s pořadovými čísly 10 a 20. První položka zabraňuje redistribuci cest označených značkou 2. Tak budou v topologii označeny cesty, které se šíří z pobočky 2 do pobočky 1. Proto je potřeba, aby se tyto cesty nešířily opačným směrem zpět do pobočky 2. Druhá položka směrovací mapy povoluje redistribuci cest, jejichž cílová IP adresa vyhovuje ACL s názvem *only10*, který povoluje pouze adresy z rozsahu 10.0.0.0/8. Mapa těmto cestám zároveň definuje metriku 40 a značku 1. Všechny ostatní cesty nebudou redistribuovány, protože směrovací mapa nevyhovující cesty odmítá. Poslední dva řádky konfigurace zajišťují vytvoření ACL *only10*. Směrovací mapu je následně potřebné aplikovat pro redistribuci.

7.5 Redistribuce cest do OSPF

Cesty vložené do OSPF pomocí redistribuce jsou šířeny podobným způsobem jako cesty, které OSPF vytvořil sám. Jediný rozdíl v šíření je typ LSA záznamu, podle kterého zdroj cesty lze určit. Na rozdíl od cest, které se OSPF naučil analýzou sítě a jsou šířeny pomocí LSA typu 2 a 3, cesty vložené do OSPF redistribucí se šíří pomocí LSA 5 a 7. Směrovač, který redistribuuje cesty do OSPF, má roli ASBR.

7.5.1 Možnosti konfigurace

Základní konfigurace redistribuce je možná jedním jednoduchým příkazem (redistribuce do OSPF procesu č.1 z BGP ASN 11):

```
R1(config)#router ospf 1
R1(config)#redistribute bgp 11
```

V tomto případě jsou všechna nepovinná nastavení použita s jejich základními hodnotami, které se řídí pravidly (platné pouze pro redistribuci do OSPF):

- cesty redistribuované z BGP mají metriku 1,
- cesty redistribuované z jiného OSPF procesu přebírají stejnou metriku,
- metrika cest redistribuovaných z ostatních zdrojů je 20,
- pro každou cestu, která není v oblasti NSSA (Not so Stubby Area) je vytvořen záznam LSA 5 a pro každou cestu z NSSA je vytvořen záznam LSA7,
- je použit externí typ metriky č. 2 (E2),
- jsou šířeny pouze cesty se základní maskou tříd, nejsou šířeny cesty do podsítí.

Příkaz *redistribute* pro redistribuci do OSPF (u ostatních protokolů má příkaz určité odlišnosti) nabízí několik nepovinných parametrů, které ovlivňují způsob, jakým budou cesty zpracovány (uvedeno v pořadí pro zadání do příkazu, vždy se uvádí dané klíčové slovo, za kterým případně následuje hodnota parametru):

- *metric* – hodnota (číslo) parametru definuje metriku, se kterou budou cesty vloženy do OSPF tabulky, toto číslo může být následně změněno přes route-map,
- *metric-type* – číselná hodnota parametru (může být 1 = E1 nebo 2 = E2) definuje typ externí metriky cest,
- *match* – parametr, který při redistribuci cest z OSPF umožňuje vybrat typ cest, které budou použity, může nabývat např. hodnot internal nebo external,
- *tag* – parametr umožňuje přidat šířeným cestám značku, pomocí které mohou být cesty identifikovány i na jiných směrovačích,
- *route-map* – aplikuje logiku směrovací mapy na redistribuované cesty,
- *subnets* – jediný parametr bez hodnoty zajišťuje vložení adres cest včetně celých masek a tím umožňuje redistribuci podsítí.

Zobrazit přenesené informace o sítích je možné pomocí příkazu *show*, kde jsou distribuované cesty ve výpisu pod označením Type-5 a Type-7 LSA:

```
R1#show ip ospf database
```

7.5.2 Rozdíl mezi cestami s metrikou E1 a E2

OSPF nabízí dva druhy externích cest – E1 a E2. Jediný rozdíl mezi těmito typy je ve výpočtu ohodnocení cest do cílových sítí. U cest typu E1 směrovače sčítají ohodnocení cesty od směrovače k ASBR a ohodnocení cesty od ASBR do cílové sítě. U cest typu E2 se bere v úvahu pouze ohodnocení cesty od ASBR do cílové sítě. Ohodnocení cesty

od směrovače k ASBR směrovač použije pouze v případě, kdy více různých cest má stejné ohodnocení cesty.

Využití konfigurace typu cesty přichází v úvahu, pokud je k dispozici více ASBR, které mají cestu do cílové sítě. V případě, že bude jedna cesta šířena jako typ E1, bude tato cesta směrovači vždy preferována před cestami typu E2. Druhou možností pro preferování určité cesty je využití cest typu E2 a explicitního nastavení různých metrik na ASBR. Pokud je cílem využití více cest a rozdělení zátěže mezi tyto cesty, je potřeba při redistribuci nastavit cesty jako typ E1.

7.5.3 Nastavení metriky cest

Při základním nastavení se při redistribuci z BGP nastavuje metrika cesty 1, z OSPF se metrika přebírá ze zdrojových informací a při redistribuci z jiných zdrojů se nastavuje metrika 20. Pokud toto nastavení z různých důvodů nevyhovuje, lze upravit třemi způsoby:

- Pro všechny zdroje při redistribuci příkazem (pro OPSF proces č. 1 a nastavení metriky na 50):
```
R1(config)#router ospf 1
R1(config-router)#default-metric 50
```
- Pro všechny cesty z určitého zdroje v příkazu *redistribute* (pro OSPF proces č. 1, redistribuci z BGP AS 1 a nastavení metriky na 50):
```
R1(config)#router ospf 1
R1(config-router)#redistribute bgp 1 metric 50
```
- Různé metriky pro cesty z jednoho zdroje lze nastavit pomocí příkazů *route-map*.

7.6 Redistribuce cest do BGP

V případě redistribuce cest do prostředí Internetu je potřeba vybírat pouze veřejné adresy, které by měly být sumarizované, aby šířených cest bylo co nejméně.

7.6.1 Výběr adres pro redistribuci

Při redistribuci jednotlivých cest je potřeba vybrat konkrétní cesty pomocí směrovací mapy, která případně umožňuje i upravení parametrů konkrétních cest (příklad pro redistribuci cest do sítě 6.0.0.0/8 s podsítěmi a redistribuci z OSPF procesu č. 1):

```
R1(config)#router bgp 11
R1(config-router)#redistribute ospf 1 route-map only-6
R1(config)#route-map only-6 permit
R1(config-route-map)#match ip address prefix 6
R1(config)#ip prefix-list 6 permit 6.0.0.0/8 le 32
```

Pokud je cesta sumarizována již pomocí IGP, stačí redistribuovat pouze tuto jednu cestu nahrazením příkazu *ip prefix-list* v předchozím příkladu následujícím:

```
R1(config)#ip prefix-list 6 permit 6.0.0.0/8
```

7.6.2 Sumarizace pomocí statické cesty

Pokud cesta není v IGP sumarizována, je možné vytvořit statickou sumarizovanou cestu s odchozím rozhraním null0 tak, jak bylo již uvedeno při použití příkazu *network*.

Redistribuce do BGP pak musí být provedena stejně jako v předchozím případě, kdy byla cesta v IGP již sumarizována.

7.6.3 Sumarizace cest v BGP

Sumarizaci cest lze provést také přímo v BGP. Pro využití této možnosti je potřeba provést redistribuci cest do BGP stejným způsobem, jak je uvedeno v prvním příkladu této podkapitoly. Následně je potřeba přidat příkaz *aggregate-address*:

```
R1(config)#router bgp 11
R1(config-router)#aggregate-address 6.0.0.0 255.0.0.0 summary-only
```

V BGP tabulce budou uloženy adresy jednotlivých podsítí a posledním příkazem se vytvoří sumarizovaná adresa sítě. Díky parametru *summary-only* bude sousedům zasílána pouze tato sumarizovaná adresa a adresy podsítí zasílány nebudou.

7.6.4 Vymazání BGP sousedství

Důvody a možnosti k vymazání BGP sousedství byly vysvětleny v podkapitole 5.9. Po provedení předchozích změn je potřebné vymazání sousedství, aby se změny projevily ve směrovací tabulce směrovače.

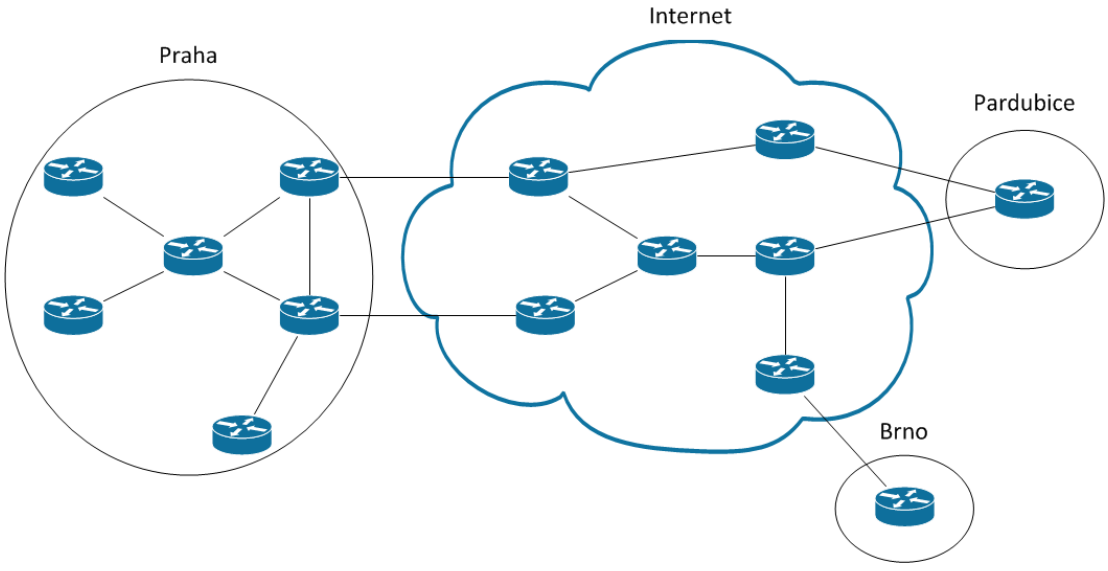
8 Případová studie využití IGP a EGP protokolů

Praktické využití protokolů je v této kapitole popsáno na případu velké fiktivní společnosti působící v České republice. Tato společnost sídlí v Praze, kde zaměstnává přes 2000 lidí. Další pobočky jsou vybudovány v Brně a v Pardubicích, kde dohromady působí dalších 800 lidí. Společnost se mimo jiné zabývá vývojem informačních systémů, a proto potřebuje kvalitní infrastrukturu počítačových sítí.

V pražské centrále jsou servery, které ke své činnosti využívají i pobočky společnosti a musí být zároveň přístupné i z Internetu. Spojení poboček soukromými síťovými linkami by pro společnost bylo velmi nákladné, proto výměna dat probíhá přes Internet. Případová studie je zaměřena na zobrazení komunikace uvnitř centrály a výměny dat s pobočkami, která probíhá přes různé ISP a Internet.

Vzhledem k rozsáhlosti vnitřních sítí centrály společnosti je samozřejmostí využití IGP. Protokoly splňující dnešní požadavky pro směrování dat jsou EIGRP, IS-IS a OSPF. Vývojovým týmem společnosti byl nejdříve zavrhnut EIGRP z důvodu omezení použitelnosti pouze na směrovačích od společnosti Cisco. Při následném výběru mezi IS-IS a OSPF byly oba protokoly shledány jako vyhovující, ale nakonec byl zvolen OSPF z důvodu větší nabídky služeb.

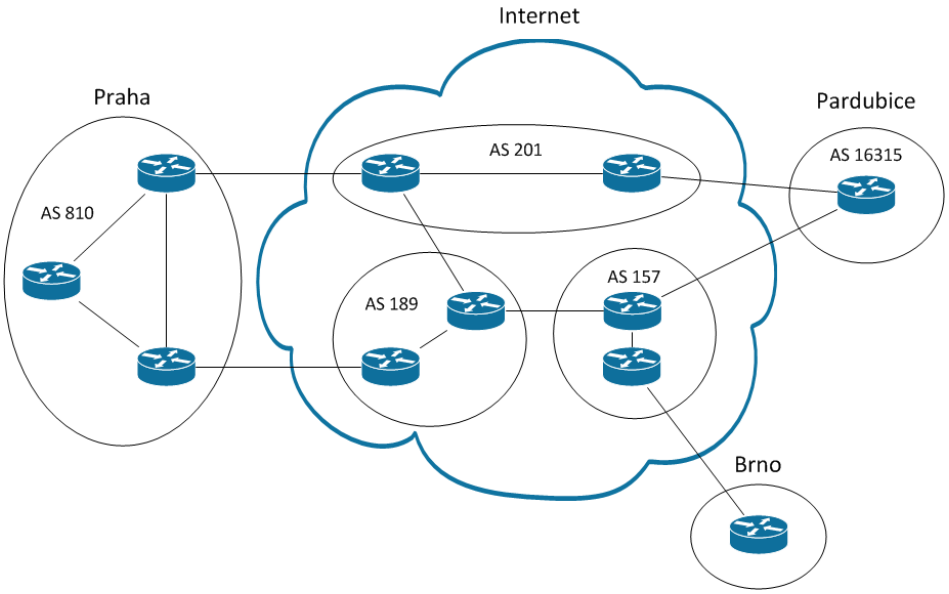
Pro lepší směrování dat ze sítí společnosti do Internetu přes různé ISP byla schválena možnost využití BGP protokolu na směrovačích připojených k ISP. Obrázek 21 zobrazuje propojení směrovačů případové studie, které je dále detailně popsáno. Studie se nezabývá detaily připojení jednotlivých koncových zařízení do sítí, ale pouze nejdůležitějšími prvky pro směrování dat vzhledem k Internetu a mezi pobočkami společnosti. Internetová část studie zahrnuje pouze směrovače, které by byly využity v případě jejich bezproblémové funkčnosti. V případě výpadku některého ze směrovačů nebo linky mezi směrovači by byly využity záložní cesty, které v této studii nejsou zahrnuty.



Obrázek 21 - Propojení centrály a poboček společnosti

Případová studie byla zpracována v simulátoru GNS3 (Graphical Network Simulator (GNS3, 2013)) se směrovači Cisco řad 3700 a 7200 s nainstalovaným IOS verze 12.4. V přílohách této práce je přiložena veškerá konfigurace směrovačů s podrobným popisem všech prováděných kroků ve formě komentářů. Vytvořený projekt v simulátoru GNS3 je přiložen na CD.

8.1 Rozdělení autonomních systémů



Obrázek 22 - Rozdělení AS

Obrázek 22 znázorňuje rozdělení směrovačů, které využívají BGP, do AS. Směrovač brněnské pobočky BGP nevyužívá a na obrázku je uveden pouze pro názorné zobrazení připojení této pobočky k Internetu. Cesty sítí tohoto směrovače budou do Internetu šířeny ze směrovače brněnského ISP, a proto budou zahrnuty do AS 157.

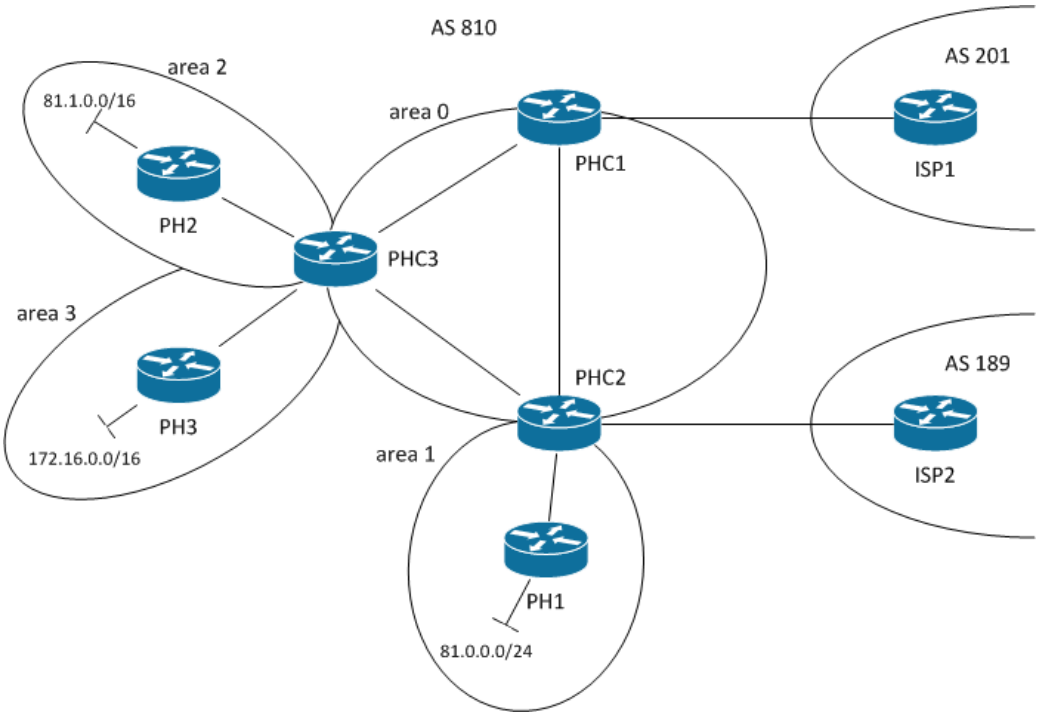
8.2 Centrála společnosti – Praha

K Internetu je centrála připojena přes 2 ISP. Pro lepší možnosti směrování dat do Internetu využívají směrovače v jádru centrály BGP. Protože oba ISP jsou v jiných AS, je potřebné, aby centrála měla vlastní AS. Společnosti bylo pro centrálu přiděleno ASN 810 a rozsah veřejných IP adres 81.0.0.0/14. Struktura připojení centrály je zobrazena na následujícím obrázku (Obrázek 23). BGP by nemělo být využito na velkém počtu směrovačů, proto společnost využije BGP na 3 směrovačích: PHC1, PHC2, PHC3. Pro směrování dat uvnitř AS byl zvolen protokol OSPF a topologie byla rozdělena na 4 oblasti.

Směrovače využívající BGP tvoří páteřní oblast 0. Oblast 1 je vyhrazena serverům, které musí být přístupné z prostředí Internetu, proto pro ně bude využit veřejný rozsah IP adres 81.0.0.0/24. Další dvě oblasti využijí zaměstnanci společnosti. Oblast 2 využije vedení podniku, které pro jednodušší komunikaci s ostatními pobočkami také potřebuje veřejné

IP adresy. Do oblasti 3 jsou zahrnuta zařízení, které veřejné adresy nepotřebují a jsou jim přidělovány adresy ze soukromého rozsahu 172.16.0.0/16.

Směrovače PH2 a PH3 koncovým zařízením poskytují přidělování IP adres pomocí DHCP (Dynamic Host Configuration Protocol) pro usnadnění jejich konfigurace, servery připojené přes směrovač PH1 DHCP nevyužívají a IP adresy jsou nastavené staticky. Směrovač PH3 navíc musí zařídit PAT (Port Address Translation), který zajistí, že IP adresy soukromého rozsahu 172.16.0.0/16 budou přeloženy na veřejnou IP adresu, pomocí které bude umožněna komunikace koncových zařízení v Internetu. Techniky společnosti byl pro všechny rozhraní směrovačů na centrále společnosti vymezen rozsah IP adres 81.2.0.0/24. Tento rozsah je následně rozdělen do podsítí s prefixem 30 a podsítě jsou rozděleny na jednotlivá spojení mezi směrovači. Přestože směrovače mají veřejné IP adresy, není nutné šířit jejich cesty do Internetu s jednou výjimkou – IP adresa směrovače PH3 musí být šířena z důvodu poskytnutí překladu adres PAT. Směrovače PH1, PH2 a PH3 by ve využité topologii být nemusely, v případové studii jsou zahrnuty pro zobrazení fungování rozsáhlejší sítě a v podniku by mohly být využity pro budoucí rozšíření síťové infrastruktury.



Obrázek 23 - Centrála společnosti

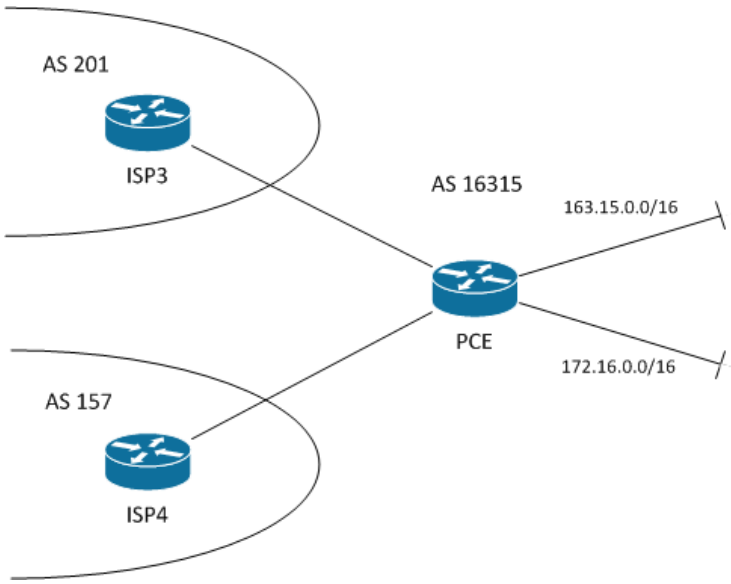
Výsledná konfigurace směrovačů v centrále společnosti se skládá z těchto kroků:

- nastavení všech spojení mezi jednotlivými směrovači,
- konfigurace DHCP na směrovačích PH2 a PH3,
- nastavení PAT na PH3,
- aktivace a konfigurace OSPF na všech směrovačích,

- nastavení defaultní cesty k ISP a nastavení jejího šíření v OSPF na směrovačích PHC1 a PHC2,
- aktivace BGP a vytvoření interního sousedství mezi směrovači PHC1, PHC2 a PHC3,
- u iBGP sousedství na směrovačích PHC1 a PHC2 je potřeba nastavit parametr *next-hop-self*, protože ostatní směrovače neznají cesty ke směrovačům připojeným přes eBGP,
- vytvoření externího sousedství PHC1 s ISP1 a PHC2 s ISP2,
- zanesení sítě 81.0.0.0/24 do BGP na směrovači PHC2,
- zanesení sítě 81.1.0.0/16 a adresy 81.0.1.1 loopback rozhraní směrovače PH3 (z důvodu PAT) do BGP na směrovači PHC3,
- sumarizace některých podnikových cest (81.0.0.0/16) v BGP na směrovačích PHC1 a PHC2,
- zajištění, aby AS 810 nebyl tranzitní – filtrováním šířených cest pomocí směrovacích map na směrovačích PHC1 a PHC2 pro eBGP sousedy.

8.3 Pobočka společnosti v Pardubicích

Proti centrále jsou obě pobočky společnosti znatelně menší, a proto nepotřebují ani rozsáhlejší síťovou topologii. Všechny servery společnosti jsou umístěny v centrále a pobočky se k nim tedy potřebují pouze připojit a nepotřebují řešit zázemí pro vlastní servery. Obrázek 24 zobrazuje připojení pardubické pobočky.



Obrázek 24 - Pobočka v Pardubicích

Protože je pobočka připojena ke dvěma ISP, má vlastní AS a směrovač PCE bude využívat BGP ke směrování dat do Internetu. Dále jsou ke směrovači ze stejných důvodů jako v centrále připojeny pro zaměstnance 2 sítě – jedna s veřejnými a druhá se soukromými IP adresami. Pro obě sítě směrovač poskytuje DHCP, pro soukromé adresy směrovač poskytuje také PAT. Pro komunikaci ve vnitřních sítích pobočky není potřeba žádný

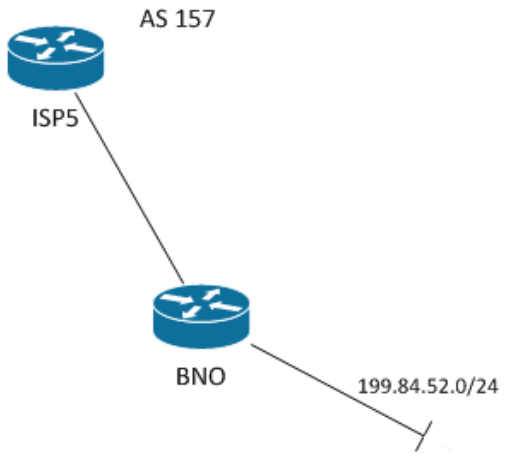
směrovací protokol, protože obě sítě si směrovač uchovává jako přímo připojené a směrování mezi nimi poskytuje automaticky.

Na pobočce je potřebná následující konfigurace směrovače PCE:

- vytvoření sítí pro zaměstnance,
- konfigurace dvou DHCP,
- konfigurace PAT,
- aktivace BGP a vytvoření externích sousedství s ISP3 a ISP4,
- zanesení sítě 163.15.0.0/16 do BGP,
- zanesení adresy 159.243.15.253/32, která byla poskytnuta pro PAT, do BGP (adresa přiřazena na loopback rozhraní),
- zajištění, aby AS pobočky nebyl tranzitní – filtrováním šířených cest k ISP. K redistribuci adres do BGP a k filtrování cest eBGP sousedům může být použita stejná směrovací mapa.

8.4 Pobočka v Brně

V Brně má společnost nejmenší pobočku a zároveň nejmenší síťovou infrastrukturu. Na pobočce je zatím pouze jedna síť s veřejnými IP adresami a jediný směrovač je připojen do Internetu přes jednoho ISP. Z tohoto důvodu nemohou být data do Internetu směrována jinými cestami a použití BGP by zde bylo zcela zbytečné. Proto pobočka nemá vlastní AS a cesty do sítě pobočky jsou do BGP šířeny poskytovatelem s jeho ASN. Pro vnitřní síť pobočky směrovač poskytuje DHCP. Obrázek 25 zobrazuje jednoduché zapojení počítačové sítě na pobočce.



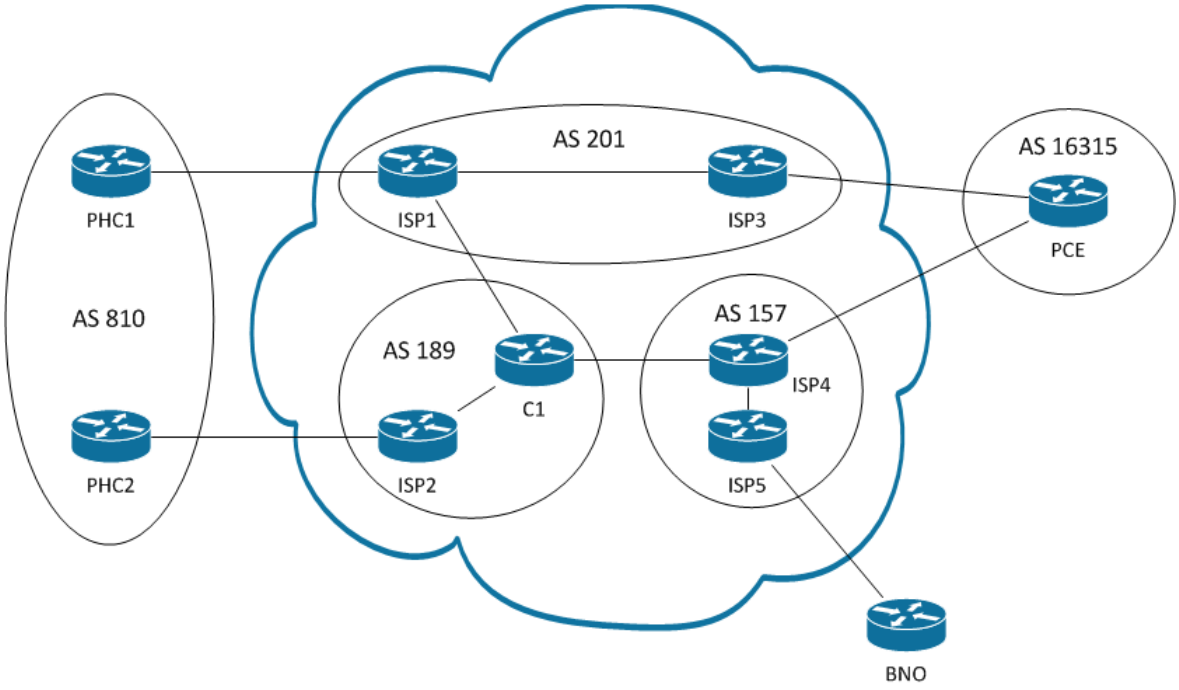
Obrázek 25 - Pobočka v Brně

Konfigurace směrovače BNO je proti ostatním poměrně jednoduchá, k zajištění funkčnosti sítě je potřeba:

- vytvořit vnitřní síť pobočky a nastavit připojení k ISP5,
- na směrovači nastavit DHCP pro síť 199.84.52.0/24,
- konfigurovat defaultní cestu z BNO k ISP5,

- ISP5 by měl vytvořit statickou cestu do sítě 199.84.52.0/24 a zanést ji do BGP.

8.5 Internetová část



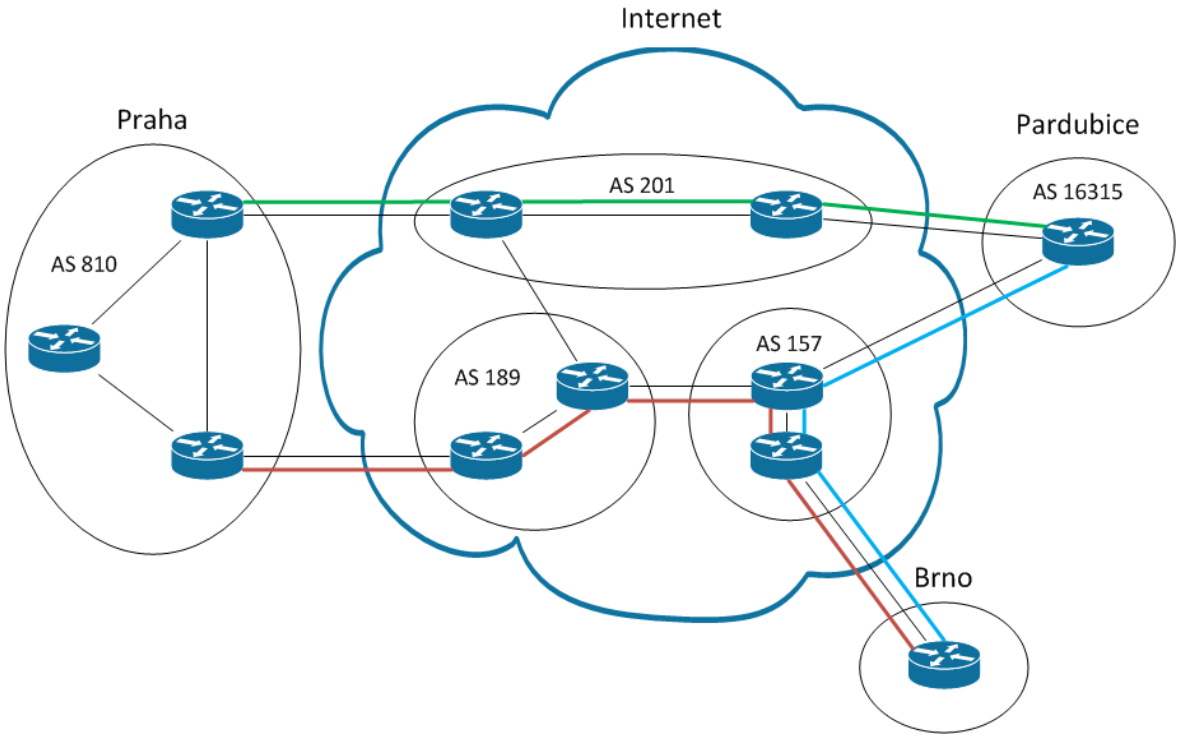
Obrázek 26 - Internetové spojení mezi centrálou a pobočkami

Obrázek 26 zobrazuje rozdělení AS společnosti i části Internetu, který je v ideálním případě využit pro přenos dat mezi centrálou a pobočkami společnosti.

Konfigurace směrovačů v Internetu sestává z kroků:

- vytvoření iBGP: ISP1 s ISP3, ISP2 s C1 a ISP4 s ISP5,
- protože si směrovače v jednotlivých AS nepředávají informace o cestách k ostatním směrovačům, všem iBGP je potřeba konfigurovat parametr *next-hop-self*,
- vytvoření eBGP: ISP1 s PHC1, ISP1 s C1, ISP2 s PHC2, ISP3 s PCE, ISP4 s PCE a C1 s ISP4,
- po dohodě s brněnskou pobočkou společnosti je na ISP5 vytvořena statická cesta do sítě brněnské pobočky a tato cesta je na ISP5 šířena do BGP.

Výsledkem konfigurace všech směrovačů je využití cest Internetem mezi centrálou a pobočkami společnosti označených na následujícím obrázku (Obrázek 27). Protože na směrovačích nejsou upraveny vlastnosti BGP cest, jako nejlepší cestu označuje BGP tu, která vede přes nejmenší počet AS. Proto cesta mezi pražskou centrálou a pardubickou pobočkou vede přes AS 201, cesta mezi pardubickou a brněnskou pobočkou přes AS 157 a cesta mezi pražskou centrálou a brněnskou pobočkou přes AS 189 a AS 157.



Obrázek 27 - Výsledné cesty dat společnosti

Závěr

Cílem bakalářské práce bylo vysvětlení principů EGP v porovnání s IGP a vysvětlení možností jejich spolupráce. Pro názornější zobrazení byl popis kromě obecných vlastností IGP a EGP protokolů zaměřen na konkrétní protokoly OSPF a BGP. Práce byla vytvořena na základě informací získaných během studia kurzu CCNP Route, vlastních zkušeností a informací z uvedené literatury.

Ve většině literatury je problematika IGP a EGP striktně rozdělena. Tato práce byla zaměřena i na opačný přístup vysvětlení obou typů protokolů, protože pro směrování dat v Internetu je nutné používat oba typy protokolů a je potřeba, aby spolu protokoly spolupracovaly.

V teoretické části práce byly nejdříve popsány principy IGP protokolů, poté EGP protokolů a následně možnosti jejich vzájemného propojení tak, aby podnikové sítě mohly využívat přednosti obou typů protokolů s ohledem na komunikaci v Internetu.

Praktická část bakalářské práce se věnuje případové studii velké společnosti. Studie zahrnuje názornou konfiguraci všech směrovačů společnosti, ve které jsou použity protokoly OSPF a BGP. V poslední části případové studie je popsána konfigurace všech směrovačů, které se nacházejí v Internetu na cestě mezi centrálou a pobočkami společnosti. Případová studie tak ukázala hlavně využití předností OSPF spolu s možnostmi BGP v počítačových sítích společnosti, která tak může mít větší kontrolu nad tokem dat do Internetu. Případová studie byla zpracována na směrovačích Cisco s operačním systémem IOS 12.4 ve volně dostupném simulačním programu GNS3. Vytvořený projekt je přiložen na CD a konfigurace všech směrovačů je přiložena v přílohách.

Přestože BGP nabízí mnoho dalších možností, které kvůli rozsáhlosti problematiky nemohly být v rámci této práce zpracovány, je jasné, že ke konfiguraci BGP je potřeba mnohem více znalostí a určitý nadhled nad problematikou, než je potřeba ke konfiguraci IGP. Také je potřeba si uvědomit, že špatná konfigurace IGP vede v nejhorším případě k nefunkčnosti sítě společnosti. Ačkoli je to nezanedbatelný problém, špatná konfigurace BGP může mít následky mnohem větší. Každý směrovač, který s ostatními komunikuje pomocí BGP může špatnou konfigurací ovlivnit směrování dat ve výrazné části Internetu. Při jeho konfiguraci je tedy potřeba si uvědomit velkou míru zodpovědnosti, která je nutná hlavně při filtrování cest zasílaných svým sousedům.

Literatura

BGP Reports. 2013. BGP Analysis Reports. *BGP Reports.* [Online] 17. 3 2013. [Citace: 17. 3 2013.] http://bgp.potaroo.net/index-bgp.html.

BOLT BERANEK AND NEWMAN INC. 1982. RFC 827 - Exterior Gateway Protocol (RGP). *IETF Tools.* [Online] 10 1982. [Citace: 20. 10 2012.] http://tools.ietf.org/html/rfc827.

BOTHA, Deon. 2009. Open Shortest Path First – OSPF Fundamentals – DR and BDR. *Network Ninja and the road to cisco.* [Online] 18. 2 2009. [Citace: 1. 2 2013.] http://networkninja.co.za/cisco-systems/open-shortest-path-first-ospf-fundamentals-dr-and-bdr/.

GNS3. 2013. Graphical Network Simulator. *GNS3.* [Online] 18. 3 2013. [Citace: 20. 3 2013.] http://www.gns3.net/.

GRYGÁREK, Petr. 2009. *VŠB | Katedra informatiky FEI VŠB-TUO.* [Online] 27. 5 2009. [Citace: 20. 10 2012.] http://www.cs.vsb.cz/grygarek/SPS/lect/BGP/BGP.html.

HALABI, Sam. 1996. *OSPF Design Guide.* místo neznámé : NSA group, 1996.

IANA. 2012. Autonomous System (AS) Numbers. *IANA - Internet Assigned Numbers Authority.* [Online] 5. 10 2012. [Citace: 20. 10 2012.] http://www.iana.org/assignments/as-numbers/as-numbers.xml.

IETF. 2012. RFC 6608 - Subcodes for BGP Finite State Machine Error. *IETF Tools.* [Online] 5 2012. [Citace: 20. 10 2012.] http://tools.ietf.org/html/rfc6608.

Internet Assigned Numbers Authority. 2013. *Internet Assigned Numbers Authority.* [Online] ICANN, 4. 1 2013. [Citace: 12. 3 2013.] http://www.iana.org/.

Internet Corporation for Assigned Names and Numbers. 2013. *Internet Corporation for Assigned Names and Numbers.* [Online] ICANN, 12. 3 2013. [Citace: 12. 3 2013.] http://www.icann.org/.

KOZIEROK, Charles M. 2005. TCP/IP Exterior Gateway Protocol (EGP). *The TCP/IP Guide.* [Online] 20. 9 2005. [Citace: 20. 10 2012.] http://www.tcpipguide.com/free/t_TCPIPExteriorGatewayProtocolEGP.htm.

—. 2005. *The TCP/IP Guide.* San Francisco : No Starch Press, Inc., 2005. ISBN 1-59327-047-X.

KVÍTEK, Libor. 2005. *Internet a zdroje.* Olomouc : Přírodovědecká fakulta, Univarzita Palackého, 2005.

LAMMLE, Todd. 2000. *CCNA Cisco Certified Network Associate Study Guide.* Alameda : SYBEX Inc., 2000. ISBN 0-7821-2647-2.

MAKATI, Mufaddal. 2012. The Internet Structure. *Rawbytes.* [Online] 30. 12 2012. [Citace: 12. 3 2013.] http://www.rawbytes.com/the-internet-structure/5/.

MĚŘÍČEK, Tomáš. 2012. *Metodika nasazení protokolu BGP pro směrování mezi autonomními uzly.* Hradec Králové : Univerzita Hradec Králové, 2012.

NETWORK WORKING GROUP. 1991. RFC 1265 - BGP Protocol Analysis. *IETF Tools.* [Online] 10 1991. [Citace: 20. 10 2012.] http://tools.ietf.org/html/rfc1265.

—. 1984. RFC 904 - Exterior Gateway Protocol Formal Specification. *IETF Tools.* [Online] 5 1984. [Citace: 20. 10 2012.] http://tools.ietf.org/html/rfc904.

ODOM, Wendell. 2010. *CCNP ROUTE 642-902 Official Certification Guide.* Indianapolis : Cisco Press, 2010. ISBN 978-1-58720-253-7.

PÁV, Miroslav. 2011. *CCNA Exploration - Směrování, koncepce a protokoly.* Plzeň : VOŠ a SPŠE Plzeň, 2011.

PETERKA, Jiří. 2005. Rodina protokolů TCP/IP. [Online] 2005. [Citace: 20. 10 2012.] http://www.earchiv.cz/down/tcpip22_6.pdf.

THOMAS, M. Thomas II. 2003. *OSPF Network Design Solutions.* Indianapolis : Cisco Press, 2003. ISBN 1-58705-032-3.

ZELENÝ, Tomáš a JAKUBEC, Petr. 2004. Historie a současnost internetu a jeho základní struktura. *Internet a zdroje KFC/INTZ.* [Online] 21. 1 2004. [Citace: 12. 3 2013.] http://fch.upol.cz/skripta/intz/Interw_1.pdf.

Příloha A – Konfigurace směrovačů centrály společnosti

Směrovač PH1

```
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
!nastaveni jmena zarizeni
hostname PH1
!
boot-start-marker
boot-end-marker
no aaa new-model
memory-size iomem 5
ip cef
no ip domain lookup
ip domain name lab.local
ip auth-proxy max-nodata-conns 3
ip admission max-nodata-conns 3
multilink bundle-name authenticated
archive
 log config
  hidekeys
!
!nastaveni ip adres rozhrani
interface FastEthernet0/0
 ip address 81.2.0.22 255.255.255.252
 duplex auto
 speed auto
interface FastEthernet0/1
 ip address 81.0.0.1 255.255.255.0
 duplex auto
 speed auto
!
!nastaveni OSPF procesu cislo 1,zapnuti pro site 81.0.0.0/24,81.2.0.20/30
router ospf 1
 log-adjacency-changes
 network 81.0.0.0 0.0.0.255 area 1
 network 81.2.0.20 0.0.0.3 area 1
!
ip forward-protocol nd
no ip http server
no ip http secure-server
!
!vypnuti zobrazovani informace o rozdilnem nastaveni duplex
no cdp log mismatch duplex
!
control-plane
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line vty 0 4
```

```
 login
end
```

Směrovač PH2

```
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
!nastaveni jmena zarizeni
hostname PH2
!
boot-start-marker
boot-end-marker
no aaa new-model
memory-size iomem 5
ip cef
no ip dhcp use vrf connected
!
!nastaveni adresy,ktera nebude pridelovana pomoci dhcp
!(=adresa smerovace)
ip dhcp excluded-address 81.1.0.1
!
!nastaveni sady pridelovane pomoci dhcp=rozsah adres,brana a dns servery
ip dhcp pool dhcp-pool
   network 81.1.0.0 255.255.0.0
   default-router 81.1.0.1
   dns-server 8.8.8.8 8.8.4.4
!
no ip domain lookup
ip domain name lab.local
ip auth-proxy max-nodata-conns 3
ip admission max-nodata-conns 3
multilink bundle-name authenticated
archive
 log config
  hidekeys
!
!nastaveni ip adres rozhrani
interface FastEthernet0/0
 ip address 81.2.0.2 255.255.255.252
 duplex auto
 speed auto
interface FastEthernet0/1
 ip address 81.1.0.1 255.255.0.0
 duplex auto
 speed auto
!
!nastaveni OSPF procesu cislo 1,zapnuti pro site 81.0.0.0/16,81.2.0.0/30
router ospf 1
 log-adjacency-changes
 network 81.1.0.0 0.0.255.255 area 2
 network 81.2.0.0 0.0.0.3 area 2
!
ip forward-protocol nd
no ip http server
no ip http secure-server
!
!vypnuti zobrazovani informace o rozdilnem nastaveni duplex
```

```
no cdp log mismatch duplex
!
control-plane
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line vty 0 4
 login
end
```

Směrovač PH3

```
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
!nastaveni jmena zarizeni
hostname PH3
!
boot-start-marker
boot-end-marker
no aaa new-model
memory-size iomem 5
ip cef
no ip dhcp use vrf connected
!
!nastaveni adresy,ktera nebude pridelovana pomoci dhcp
!(=adresa smerovace)
ip dhcp excluded-address 172.16.0.1
!
!nastaveni sady pridelovane pomoci dhcp=rozsah adres,brana a dns servery
ip dhcp pool dhcp-pool
   network 172.16.0.0 255.255.0.0
   default-router 172.16.0.1
   dns-server 8.8.8.8 8.8.4.4
!
no ip domain lookup
ip domain name lab.local
ip auth-proxy max-nodata-conns 3
ip admission max-nodata-conns 3
multilink bundle-name authenticated
archive
 log config
  hidekeys
!
!nastaveni loopback rozhrani, kvuli snadnemu sireni IP adresy v OSPF
interface Loopback0
 ip address 81.0.1.1 255.255.255.252
!
!nastaveni ip adres rozhrani a vnitrni/vnejsi strany prekladu adres PAT
interface FastEthernet0/0
 ip address 81.2.0.6 255.255.255.252
 ip nat outside
 ip virtual-reassembly
```

```
 duplex auto
 speed auto
interface FastEthernet0/1
 ip address 172.16.0.1 255.255.0.0
 ip nat inside
 ip virtual-reassembly
 duplex auto
 speed auto
!
!nastaveni OSPF procesu cislo 1,zapnuti pro site 81.0.1.0/30,81.2.0.4/30
router ospf 1
 log-adjacency-changes
 network 81.0.1.0 0.0.0.3 area 3
 network 81.2.0.4 0.0.0.3 area 3
!
ip forward-protocol nd
no ip http server
no ip http secure-server
!
!nastaveni ip adresy pouzite pro preklad adres PAT
ip nat pool nat-pool 81.0.1.1 81.0.1.1 prefix-length 30
!
!prirazeni access-listu cislo 1 jako sady vnitrnich adres pro PAT
!a v predchozim kroku nastavene adresy jako vnejsi sady adres pro PAT
ip nat inside source list 1 pool nat-pool overload
!
!nastaveni access-listu, ktery je pouzit jako vnitrni sada adres pro PAT
access-list 1 permit 172.16.0.0 0.0.255.255
!
!vypnuti zobrazovani informace o rozdilnem nastaveni duplex
no cdp log mismatch duplex
!
control-plane
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line vty 0 4
 login
end
```

Směrovač PHC1

```
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
!nastaveni jmena zarizeni
hostname PHC1
!
boot-start-marker
boot-end-marker
no aaa new-model
memory-size iomem 5
ip cef
```

```
no ip domain lookup
ip domain name lab.local
ip auth-proxy max-nodata-conns 3
ip admission max-nodata-conns 3
multilink bundle-name authenticated
archive
 log config
  hidekeys
!
!nastaveni ip adres rozhrani
interface FastEthernet0/0
 ip address 53.1.10.2 255.255.255.252
 duplex auto
 speed auto
interface FastEthernet0/1
 ip address 81.2.0.9 255.255.255.252
 duplex auto
 speed auto
interface FastEthernet1/0
 ip address 81.2.0.17 255.255.255.252
 duplex auto
 speed auto
!
!nastaveni OSPF procesu cislo 1,zapnuti pro site 81.2.0.8/30,81.2.0.16/30
!nastaveni sireni defaultni cesty
router ospf 1
 log-adjacency-changes
 network 81.2.0.8 0.0.0.3 area 0
 network 81.2.0.16 0.0.0.3 area 0
 default-information originate
!
!nastaveni BGP v AS 810, nastaveni sousedu,sumarizace adres 81.0.0.0/16
!nastaveni smerovaci mapy only-public-bgp pro filtraci cest,
!ktere jsou odesilany sousedovi 53.1.10.1
!pro iBGP sousedy nastaven parametr next-hop-self
router bgp 810
 no synchronization
 bgp log-neighbor-changes
 aggregate-address 81.0.0.0 255.255.0.0 summary-only
 neighbor 53.1.10.1 remote-as 201
 neighbor 53.1.10.1 route-map only-public-bgp out
 neighbor 81.2.0.10 remote-as 810
 neighbor 81.2.0.10 next-hop-self
 neighbor 81.2.0.18 remote-as 810
 neighbor 81.2.0.18 next-hop-self
 no auto-summary
!
ip forward-protocol nd
!
!nastaveni defaultni cesty na vystup rozhrani FastEthernet0/0
ip route 0.0.0.0 0.0.0.0 FastEthernet0/0
!
no ip http server
no ip http secure-server
!
!nastaveni prefix-listu pro povoleni rozsahu adres ve smerovaci mape
ip prefix-list 20 seq 5 permit 81.0.0.0/15 le 32
!
!vypnuti zobrazovani informace o rozdilnem nastaveni duplex
no cdp log mismatch duplex
```

```
!
!konfigurace smerovaci mapy pouzite pri zasilani aktualizaci pres eBGP
route-map only-public-bgp permit 10
 match ip address prefix-list 20
!
control-plane
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line vty 0 4
 login
end
```

Směrovač PHC2

```
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
!nastaveni jmena zarizeni
hostname PHC2
!
boot-start-marker
boot-end-marker
no aaa new-model
memory-size iomem 5
ip cef
no ip domain lookup
ip domain name lab.local
ip auth-proxy max-nodata-conns 3
ip admission max-nodata-conns 3
multilink bundle-name authenticated
archive
 log config
  hidekeys
!
!nastaveni ip adres rozhrani
interface FastEthernet0/0
 ip address 53.5.8.130 255.255.255.252
 duplex auto
 speed auto
interface FastEthernet0/1
 ip address 81.2.0.10 255.255.255.252
 duplex auto
 speed auto
interface FastEthernet1/0
 ip address 81.2.0.13 255.255.255.252
 duplex auto
 speed auto
interface FastEthernet2/0
 ip address 81.2.0.21 255.255.255.252
 duplex auto
 speed auto
!
```

```
!nastaveni OSPF procesu cislo 1,zapnuti pro 3 site
!nastaveni sireni defaultni cesty
router ospf 1
 log-adjacency-changes
 network 81.2.0.8 0.0.0.3 area 0
 network 81.2.0.12 0.0.0.3 area 0
 network 81.2.0.20 0.0.0.3 area 1
 default-information originate
!
!nastaveni BGP v AS 810, sumarizace adres 81.0.0.0/16,
!redistribuce cest z OSPF procesu 1 vyhovujicich smer. mape only-public,
!nastaveni BGP sousedu,
!nastaveni smerovacich map pro filtraci cest zasilanych pres eBGP,
!ktere jsou temto sousedum odesilany,
!pro iBGP sousedy nastaven parametr next-hop-self
router bgp 810
 no synchronization
 bgp log-neighbor-changes
 aggregate-address 81.0.0.0 255.255.0.0 summary-only
 redistribute ospf 1 route-map only-public
 neighbor 53.5.8.129 remote-as 189
 neighbor 53.5.8.129 route-map only-public-bgp out
 neighbor 81.2.0.9 remote-as 810
 neighbor 81.2.0.9 next-hop-self
 neighbor 81.2.0.14 remote-as 810
 neighbor 81.2.0.14 next-hop-self
 no auto-summary
!
ip forward-protocol nd
!
!nastaveni defaultni cesty na vystup rozhrani FastEthernet0/0
ip route 0.0.0.0 0.0.0.0 FastEthernet0/0
!
no ip http server
no ip http secure-server
!
!nastaveni 2 prefix-listu pro povoleni adres ve smerovacich mapach
ip prefix-list 10 seq 5 permit 81.0.0.0/24 le 32
ip prefix-list 20 seq 5 permit 81.0.0.0/15 le 32
!
!vypnuti zobrazovani informace o rozdilnem nastaveni duplex
no cdp log mismatch duplex
!
!konfigurace smerovacich map pouzitych pri redistribuci cest do BGP
!a pri zasilani BGP aktualizaci
route-map only-public permit 10
 match ip address prefix-list 10
route-map only-public-bgp permit 10
 match ip address prefix-list 20
!
control-plane
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line vty 0 4
```

```
 login
end
```

Směrovač PHC3

```
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
!nastaveni jmena zarizeni
hostname PHC3
!
boot-start-marker
boot-end-marker
no aaa new-model
memory-size iomem 5
ip cef
ip auth-proxy max-nodata-conns 3
ip admission max-nodata-conns 3
multilink bundle-name authenticated
archive
 log config
  hidekeys
!
!nastaveni ip adres rozhrani
interface FastEthernet0/0
 ip address 81.2.0.18 255.255.255.252
 duplex auto
 speed auto
interface FastEthernet0/1
 ip address 81.2.0.14 255.255.255.252
 duplex auto
 speed auto
interface FastEthernet1/0
 ip address 81.2.0.5 255.255.255.252
 duplex auto
 speed auto
interface FastEthernet2/0
 ip address 81.2.0.1 255.255.255.252
 duplex auto
 speed auto
!
!nastaveni OSPF procesu cislo 1,zapnuti ruznych oblasti pro 4 site
router ospf 1
 log-adjacency-changes
 network 81.2.0.0 0.0.0.3 area 2
 network 81.2.0.4 0.0.0.3 area 3
 network 81.2.0.12 0.0.0.3 area 0
 network 81.2.0.16 0.0.0.3 area 0
!
!nastaveni BGP redistribuce cest z OSPF procesu 1, ktere vyhovuji
!smerovaci mape only-public, nastaveni BGP sousedu
router bgp 810
 no synchronization
 bgp log-neighbor-changes
 redistribute ospf 1 route-map only-public
 neighbor 81.2.0.13 remote-as 810
 neighbor 81.2.0.17 remote-as 810
 no auto-summary
```

```
!
ip forward-protocol nd
ip http server
no ip http secure-server
!
!nastaveni 2 prefix-listu pro povoleni 2 rozsahu adres ve smerovaci mape
ip prefix-list 10 seq 5 permit 81.1.0.0/16 le 32
ip prefix-list 11 seq 5 permit 81.0.1.0/30 le 32
!
!vypnuti zobrazovani informace o rozdilnem nastaveni duplex
no cdp log mismatch duplex
!
!konfigurace smerovaci mapy pouzite pri zasilani BGP aktualizaci
route-map only-public permit 10
 match ip address prefix-list 10
route-map only-public permit 11
 match ip address prefix-list 11
!
control-plane
line con 0
line aux 0
line vty 0 4
 login
end
```

Příloha B – Konfigurace směrovače pobočky společnosti v Pardubicích

```
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
!nastaveni jmena zarizeni
hostname PCE
!
boot-start-marker
boot-end-marker
no aaa new-model
memory-size iomem 5
ip cef
no ip dhcp use vrf connected
!
!nastaveni adres,ktere nebudou pridelovana pomoci dhcp
! (=adresy smerovace)
ip dhcp excluded-address 172.16.0.1
ip dhcp excluded-address 163.15.0.1
!
!nastaveni sad pridelovanych pomoci dhcp=rozsah adres,brana a dns servery
ip dhcp pool dhcp-163
   network 163.15.0.0 255.255.0.0
   default-router 163.15.0.1
   dns-server 8.8.8.8 8.8.4.4
ip dhcp pool dhcp-172
   network 172.16.0.0 255.255.0.0
   default-router 172.16.0.1
   dns-server 8.8.8.8 8.8.4.4
!
ip auth-proxy max-nodata-conns 3
ip admission max-nodata-conns 3
multilink bundle-name authenticated
archive
 log config
  hidekeys
!
!nastaveni loopback rozhrani, kvuli snadne redistribuci ip adresy do BGP
interface Loopback0
 ip address 159.243.15.253 255.255.255.255
!
!nastaveni ip adres rozhrani a vnitrni/vnejsi strany prekladu adres PAT
interface FastEthernet0/0
 ip address 53.2.5.8 255.255.255.0
 ip nat outside
 ip virtual-reassembly
 duplex auto
 speed auto
interface FastEthernet0/1
 ip address 53.69.221.23 255.255.255.0
 ip nat outside
 ip virtual-reassembly
 duplex auto
 speed auto
interface FastEthernet1/0
 ip address 163.15.0.1 255.255.0.0
```

```
 duplex auto
 speed auto
interface FastEthernet2/0
 ip address 172.16.0.1 255.255.0.0
 ip nat inside
 ip virtual-reassembly
 duplex auto
 speed auto
!
!nastaveni BGP: redistribuce pripojenych siti vyhovujicich smerovaci mape
!nastaveni BGP sousedu a nastaveni smerovacich map pro filtraci cest,
!ktere jsou temto sousedum odesilany
router bgp 16315
 no synchronization
 bgp log-neighbor-changes
 redistribute connected route-map only-public
 neighbor 53.2.5.1 remote-as 201
 neighbor 53.2.5.1 route-map only-public out
 neighbor 53.69.221.1 remote-as 157
 neighbor 53.69.221.1 route-map only-public out
 no auto-summary
!
ip forward-protocol nd
ip http server
no ip http secure-server
!
!nastaveni ip adresy pouzite pro preklad adres PAT
ip nat pool nat-pool 159.243.15.253 159.243.15.253 prefix-length 30
!
!prirazeni access-listu cislo 1 jako sady vnitrnich adres pro PAT
!a v predchozim kroku nastavene adresy jako vnejsi sady adres pro PAT
ip nat inside source list 1 pool nat-pool
!
!nastaveni prefix-listu pro povoleni 2 rozsahu adres ve smerovaci mape
ip prefix-list pl-only-public seq 5 permit 163.15.0.0/16
ip prefix-list pl-only-public seq 10 permit 159.243.15.253/32
!
!nastaveni access-listu, ktery je pouzit jako vnitrni sada adres pro PAT
access-list 1 permit 172.16.0.0 0.0.255.255
!
!vypnuti zobrazovani informace o rozdilnem nastaveni duplex
no cdp log mismatch duplex
!
!konfigurace smerovaci mapy pouzite pri zasilani BGP aktualizaci
route-map only-public permit 10
 match ip address prefix-list pl-only-public
!
control-plane
line con 0
line aux 0
line vty 0 4
end
```

Příloha C – Konfigurace směrovače pobočky společnosti v Brně

```
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
!nastaveni jmena zarizeni
hostname BNO
!
boot-start-marker
boot-end-marker
no aaa new-model
memory-size iomem 5
ip cef
no ip dhcp use vrf connected
!
!nastaveni adresy,ktera nebude pridelovana pomoci dhcp
!(=adresa smerovace)
ip dhcp excluded-address 199.84.52.1
!
!nastaveni sady pridelovane pomoci dhcp=rozsah adres, brana a dns servery
ip dhcp pool dhcp-pool
   network 199.84.52.0 255.255.255.0
   default-router 199.84.52.1
   dns-server 8.8.8.8 8.8.4.4
!
no ip domain lookup
ip domain name lab.local
ip auth-proxy max-nodata-conns 3
ip admission max-nodata-conns 3
multilink bundle-name authenticated
archive
 log config
  hidekeys
!
!nastaveni ip adres rozhrani
interface FastEthernet0/0
 ip address 195.42.31.15 255.255.255.0
 duplex auto
 speed auto
interface FastEthernet0/1
 ip address 199.84.52.1 255.255.255.0
 duplex auto
 speed auto
!
ip forward-protocol nd
!
!nastaveni defaultni cesty smerem k ISP
ip route 0.0.0.0 0.0.0.0 FastEthernet0/0
!
no ip http server
no ip http secure-server
!
!vypnuti zobrazovani informace o rozdilnem nastaveni duplex
no cdp log mismatch duplex
!
control-plane
line con 0
 exec-timeout 0 0
```

```
 privilege level 15
 logging synchronous
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line vty 0 4
 login
end
```

Příloha D – Konfigurace směrovačů v Internetu

Směrovač ISP1

```
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
!nastaveni jmena zarizeni
hostname ISP1
!
boot-start-marker
boot-end-marker
no aaa new-model
ip cef
no ip domain lookup
ip domain name lab.local
!
!nastaveni ip adres rozhrani
interface FastEthernet0/0
 no ip address
 shutdown
 duplex half
interface FastEthernet1/0
 ip address 53.1.10.1 255.255.255.252
 duplex auto
 speed auto
interface FastEthernet1/1
 no ip address
 shutdown
 duplex auto
 speed auto
interface POS2/0
 ip address 53.5.93.193 255.255.255.252
interface POS3/0
 ip address 53.45.52.73 255.255.255.252
!
!nastaveni BGP v AS 201,
!nastaveni sousedu,pro iBGP souseda nastaven parametr next-hop-self
router bgp 201
 no synchronization
 bgp log-neighbor-changes
 neighbor 53.1.10.2 remote-as 810
 neighbor 53.5.93.194 remote-as 189
 neighbor 53.45.52.74 remote-as 201
 neighbor 53.45.52.74 next-hop-self
 no auto-summary
!
no ip http server
no ip http secure-server
!
!vypnuti zobrazovani informace o rozdilnem nastaveni duplex
no cdp log mismatch duplex
!
control-plane
gatekeeper
 shutdown
line con 0
```

```
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 stopbits 1
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 stopbits 1
line vty 0 4
 login
end
```

Směrovač ISP2

```
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
!nastaveni jmena zarizeni
hostname ISP2
!
boot-start-marker
boot-end-marker
no aaa new-model
ip cef
no ip domain lookup
ip domain name lab.local
!
!nastaveni ip adres rozhrani
interface FastEthernet0/0
 no ip address
 shutdown
 duplex half
interface FastEthernet1/0
 ip address 53.5.8.129 255.255.255.252
 duplex auto
 speed auto
interface FastEthernet1/1
 no ip address
 shutdown
 duplex auto
 speed auto
interface POS2/0
 ip address 53.5.8.161 255.255.255.252
!
!nastaveni BGP v AS 189,
!nastaveni sousedu,pro iBGP souseda nastaven parametr next-hop-self
router bgp 189
 no synchronization
 bgp log-neighbor-changes
 neighbor 53.5.8.130 remote-as 810
 neighbor 53.5.8.162 remote-as 189
 neighbor 53.5.8.162 next-hop-self
 no auto-summary
!
no ip http server
no ip http secure-server
!
```

```
!vypnuti zobrazovani informace o rozdilnem nastaveni duplex
no cdp log mismatch duplex
!
control-plane
gatekeeper
 shutdown
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 stopbits 1
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 stopbits 1
line vty 0 4
 login
end
```

Směrovač C1

```
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
!nastaveni jmena zarizeni
hostname C1
!
boot-start-marker
boot-end-marker
no aaa new-model
ip cef
no ip domain lookup
ip domain name lab.local
interface FastEthernet0/0
 no ip address
 shutdown
 duplex half
!
!nastaveni ip adres rozhrani
interface POS1/0
 ip address 53.18.195.17 255.255.255.252
interface POS2/0
 ip address 53.5.93.194 255.255.255.252
interface POS3/0
 ip address 53.5.8.162 255.255.255.252
!
!nastaveni BGP v AS 189,
!nastaveni sousedu,pro iBGP souseda nastaven parametr next-hop-self
router bgp 189
 no synchronization
 bgp log-neighbor-changes
 neighbor 53.5.8.161 remote-as 189
 neighbor 53.5.8.161 next-hop-self
 neighbor 53.5.93.193 remote-as 201
 neighbor 53.18.195.18 remote-as 157
 no auto-summary
!
```

```
no ip http server
no ip http secure-server
control-plane
gatekeeper
 shutdown
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 stopbits 1
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 stopbits 1
line vty 0 4
 login
end
```

Směrovač ISP3

```
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
!nastaveni jmena zarizeni
hostname ISP3
!
boot-start-marker
boot-end-marker
no aaa new-model
ip cef
no ip domain lookup
ip domain name lab.local
!
!nastaveni ip adres rozhrani
interface FastEthernet0/0
 no ip address
 shutdown
 duplex half
interface FastEthernet1/0
 ip address 53.2.5.1 255.255.255.0
 duplex auto
 speed auto
interface FastEthernet1/1
 no ip address
 shutdown
 duplex auto
 speed auto
interface POS2/0
 ip address 53.45.52.74 255.255.255.252
!
!nastaveni BGP v AS 201,
!nastaveni sousedu,pro iBGP souseda nastaven parametr next-hop-self
router bgp 201
 no synchronization
 bgp log-neighbor-changes
 neighbor 53.2.5.8 remote-as 16315
 neighbor 53.45.52.73 remote-as 201
```

```
 neighbor 53.45.52.73 next-hop-self
 no auto-summary
!
no ip http server
no ip http secure-server
!
!vypnuti zobrazovani informace o rozdilnem nastaveni duplex
no cdp log mismatch duplex
!
control-plane
gatekeeper
 shutdown
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 stopbits 1
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 stopbits 1
line vty 0 4
 login
end
```

Směrovač ISP4

```
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
!nastaveni jmena zarizeni
hostname ISP4
!
boot-start-marker
boot-end-marker
no aaa new-model
ip cef
no ip domain lookup
ip domain name lab.local
!
!nastaveni ip adres rozhrani
interface FastEthernet0/0
 no ip address
 shutdown
 duplex half
interface POS1/0
 ip address 53.18.195.18 255.255.255.252
interface FastEthernet2/0
 ip address 53.69.221.1 255.255.255.0
 duplex auto
 speed auto
interface FastEthernet2/1
 no ip address
 shutdown
 duplex auto
 speed auto
interface POS3/0
```

```
 ip address 53.69.222.9 255.255.255.252
!
!nastaveni BGP v AS 157,
!nastaveni sousedu,pro iBGP souseda nastaven parametr next-hop-self
router bgp 157
 no synchronization
 bgp log-neighbor-changes
 neighbor 53.18.195.17 remote-as 189
 neighbor 53.69.221.23 remote-as 16315
 neighbor 53.69.222.10 remote-as 157
 neighbor 53.69.222.10 next-hop-self
 no auto-summary
!
no ip http server
no ip http secure-server
!
!vypnuti zobrazovani informace o rozdilnem nastaveni duplex
no cdp log mismatch duplex
!
control-plane
gatekeeper
 shutdown
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 stopbits 1
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 stopbits 1
line vty 0 4
 login
end
```

Směrovač ISP5

```
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
!nastaveni jmena zarizeni
hostname ISP5
!
boot-start-marker
boot-end-marker
no aaa new-model
ip cef
no ip domain lookup
ip domain name lab.local
!
!nastaveni ip adres rozhrani
interface FastEthernet0/0
 no ip address
 shutdown
 duplex half
interface FastEthernet1/0
 ip address 195.42.31.1 255.255.255.0
```

```
 duplex auto
 speed auto
interface FastEthernet1/1
 no ip address
 shutdown
 duplex auto
 speed auto
interface POS2/0
 ip address 53.69.222.10 255.255.255.252
!
!nastaveni BGP v AS 157, redistribuce statickych cest do BGP
!nastaveni iBGP souseda, nastaven parametr next-hop-self
router bgp 157
 no synchronization
 bgp log-neighbor-changes
 redistribute static
 neighbor 53.69.222.9 remote-as 157
 neighbor 53.69.222.9 next-hop-self
 no auto-summary
!
!nastaveni staticke cesty do brnenske pobocky spolecnosti
ip route 199.84.52.0 255.255.255.0 195.42.31.15
!
no ip http server
no ip http secure-server
!
!vypnuti zobrazovani informace o rozdilnem nastaveni duplex
no cdp log mismatch duplex
!
control-plane
gatekeeper
 shutdown
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 stopbits 1
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 stopbits 1
line vty 0 4
 login
end
```