Univerzita Pardubice

Fakulta elektrotechniky a informatiky

Problematika protokolu BGP

Jakub Snášel

Bakalářská práce

2013

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

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Jakub Snášel**
Osobní číslo:	**I09260**
Studijní program:	**B2646 Informační technologie**
Studijní obor:	**Informační technologie**
Název tématu:	**Problematika protokolu BGP**
Zadávající katedra:	**Katedra informačních technologií**

Zásady pro vypracování:

Představení problematiky EGP protokolů a jejich zástupce BGP (Border Gateway Protocol). Představení principů směrování s využitím BGP páteřního směrovacího protokolu určeného především k výměně směrovacích informací mezi autonomními systémy a provedení konfigurace simulované WAN sítě s protokolem BGP v laboratorních podmínkách. Důraz bude kladen na jednotlivé kroky konfigurace a jejich vztah k principům fungování BGP a jeho směrovacím algoritmům. Bakalářská práce bude obsahovat představení teorie a schematických návrhů. Součástí budou výpisy konfigurace routerů.

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.**
***WHITE, Russ, Danny MCPHERSON a Sangli SRIHARI. Practical BGP. Boston: Addison-Wesley, 2005, xii, 434 p. ISBN 03-211-2700-5.**

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:

Tuto práci jsem 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 19. 4. 2013

Jakub Snášel

Poděkování:
Tímto děkuji vedoucímu bakalářské práce Mgr. Josefu Horálkovi za podporu a přátelské vedení při zpracování bakalářské práce.

ANOTACE

Záměrem této bakalářské práce je představit problematiku protokolu BGP. Úvodní kapitoly nejprve popisují základní strukturu Internetu a podrobné vysvětlení protokolu BGP s jeho vlastnostmi a možnostmi základního nastavení. Následné kapitoly jsou zaměřeny na politiku samotného směrování, redistribuci a filtraci cest.

KLÍČOVÁ SLOVA

autonomní systémy, Internet, směrování, směrovací protokoly, sítě, WAN, ISP

TITLE

Problems of BGP protocol

ANNOTATION

The intent of this bachelor thesis is to propose problems of BGP protocol. Introductory chapters describe the basic structure of the Internet and a detailed explanation of BGP protocol with its abilities and options of its basic configuration. The following chapters are focused on the actual routing policy, redistribution and routes filtering.

KEYWORDS

autonomous systems, the Internet, routing, routing protocols, networks, WAN, ISP

OBSAH

SEZNAM ILUSTRACÍ

SEZNAM TABULEK

SEZNAM PŘÍLOH

SEZNAM ZKRATEK A ZNAČEK

AS	Autonomous System	Autonomní Systém
BGP	Border Gateway Protocol	
CCNA	Cisco Certified Network Associate	
CEF	Cisco Express Forwarding	
eBGP	External BGP / Exterior BGP	Externí BGP
EGP	Exterior Gateway Protocol	
EIGRP	Enhanced Interior Gateway Routing Protocol	
IANA	Internet Assigned Numbers Authority	
iBGP	Internal BGP / Interior BGP	Interní BGP
ID	Identifier	Identifikátor
IGP	Interior Gateway Protocol	
IOS	Internetwork Operating System	
IP	Internet Protocol	
IS-IS	Intermediate System to Intermediate System	
ISP	Internet Service Provider	Poskytovatel Internetového připojení
MED	Multi-Exit Discriminator	
MPLS	MultiProtocol Label Switching	
NAT	Network Address Translation	Překlad Síťových Adres
NLRI	Network Layer Reachability Information	
OSPF	Open Shortest Path First	
RIP	Routing Information Protocol	
RIR	Regional Internet Registries	
RR	Route Reflector	Reflektor Cest
TCP	Transmission Control Protocol	
TTL	Time To Live	
UDP	User Datagram Protocol	
VPN	Virtual Private Network	Virtuální Privátní Síť
VRF	Virtual Routing and Forwarding	
WAN	Wide Area Network	

ÚVOD

Od svého počátku do současnosti prošel Internet značným vývojem a postupně se rozšířil natolik, že už není reálné udržovat ve směrovačích úplnou informaci o jeho topologii. Tuto informaci by totiž bylo nutné aktualizovat s výpadkem nebo připojením linky kdekoli na světě, to by vedlo ke značným prodlevám a dalším komplikacím. Proto se v současnosti směrování v Internetu řeší hierarchickým způsobem. K tomu nám slouží tzv. autonomní systémy, které umožňují rozdělení celého Internetu na jeho jednotlivé podčásti. Autonomním systémem rozumíme souvislou skupinu sítí a směrovačů spadajících pod společnou správu a řídících se jednotnou směrovací politikou. Pod společnou směrovací politikou si představme dohodnutý interní směrovací protokol. Směrovací informace mezi jednotlivými autonomními systémy se potom předávají pomocí hraničních směrovačů používajících Border Gateway Protocol (BGP).

Cílem bakalářské práce je představit čtenáři současnou strukturu Internetu, BGP a jeho funkčnost. Praktická část potom popíše průběh zapojení a nastavení základní sítě využívající BGP.

Práce předpokládá pokročilé znalosti počítačových sítí alespoň na úrovni kurzu CCNA 4 od společnosti Cisco.

1 ZÁKLADNÍ POJMY

1.1 Autonomní systém

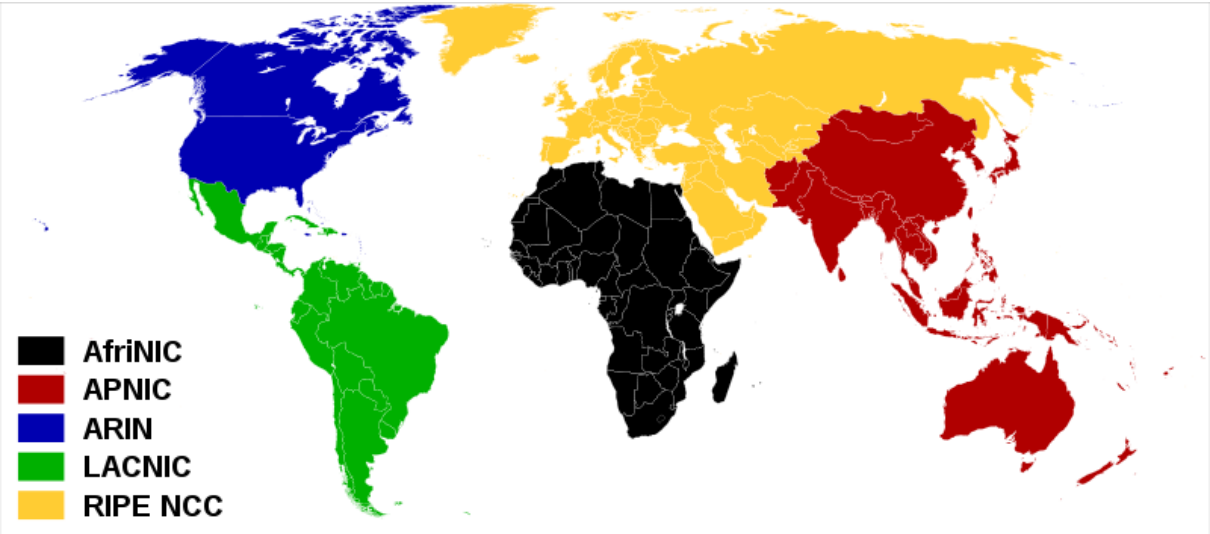
Podle [1], [2], [3] a [4]. Autonomním systémem rozumíme souvislou skupinu sítí a směrovačů spadajících pod společnou správu a řídících se jednotnou směrovací politikou. Pod společnou směrovací politikou si představme dohodnutý interní směrovací protokol. Příkladem autonomního systému tak může být autonomní systém jednoho poskytovatele Internetu nebo velké firmy.

Pro směrování v rámci jednotlivých autonomních systémů se používají tzv. interní směrovací protokoly (Interior Gateway Protocol – IGP). Pro směrování mezi jednotlivými autonomními systémy se potom používají tzv. externí směrovací protokoly (Exterior Gateway Protocol – EGP).

Z pohledu externích směrovacích protokolů jsou autonomní systémy chápány jako základní jednotky, jejichž struktura není mimo hranice autonomního systému známa. Autonomní systémy je možné na základě několika hledisek rozdělit na:

- Politické – rozděleny na základě politiky jednotlivých poskytovatelů internetového připojení (Internet Service Provider – ISP).
- Geografické – rozděleny na základě polohy (např. světadíly, státy, kraje).
- Technické – BGP je, na výkonnost a paměť směrovače, náročným směrovacím protokolem, protože směrovač může zpracovávat celou směrovací tabulku Internetu.

V případě, že chceme námi vytvořený autonomní systém připojit k veřejné síti Internet pomocí externího směrovacího protokolu (např. BGP), musí mít tento systém přiděleno jedinečné číslo autonomního systému. O správu a přidělování těchto čísel se stará organizace IANA (Internet Assigned Numbers Authority). Při tomto procesu spolupracuje s regionálními internetovými matrikami (Regional Internet Registries – RIR). RIR byly založeny za účelem správy a registrace IP adres a čísel autonomních systémů v hlavních zeměpisných lokalitách.



Obrázek 1 Regionální internetové matriky (RIR)[1]

Každý autonomní systém připojený k Internetu je označen 16bitovým číslem zapsaným v dekadickém tvaru v rozsahu hodnot 0 až 65535. Čísla 0, 23456, 65535 jsou rezervována pro speciální účely, 64512 až 64534 jsou určena pro privátní autonomní systémy a zbytek (1 až 64511 bez 23456) je určen pro autonomní systémy na Internetu.

V souvislosti s rostoucím počtem autonomních systémů (rozšiřování Internetu) začíná zásoba volných čísel autonomních systémů docházet. Proto se připravuje přechod na 32bitové číslování. Nová 32bitová čísla se budou skládat z vyšší a nižší 16bitové části a budou se zapisovat jako dekadická čísla odpovídající těmto částem oddělená tečkou.

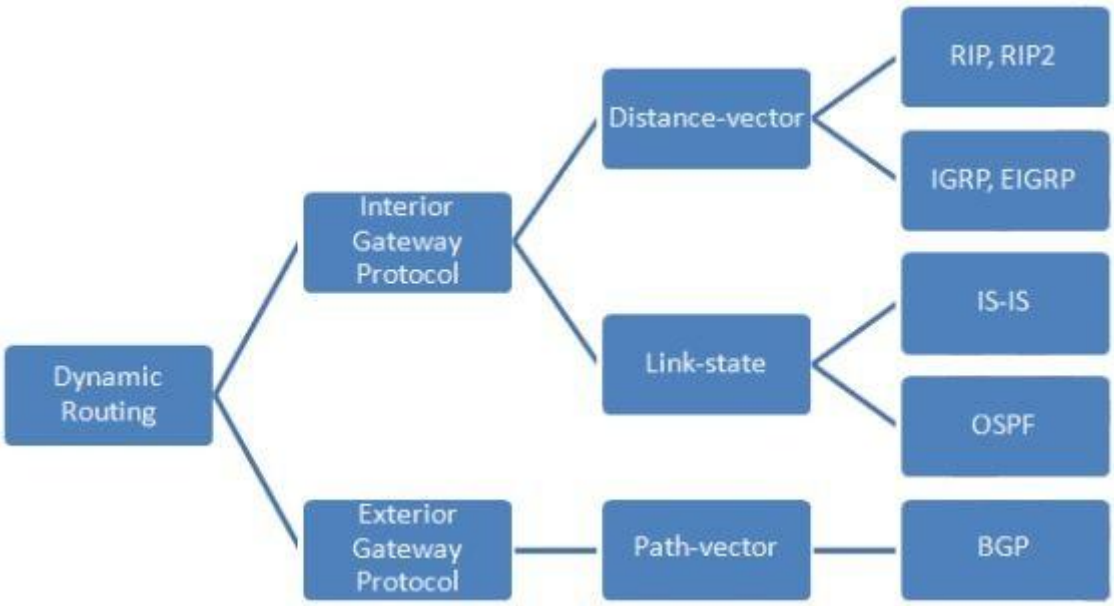
Zavedení nového číslování je závislé na zavedení nové verze protokolu BGP, která ho bude podporovat.

1.2 Interní a externí směrovací protokoly

Podle [1], [5] a [6]. Směrovací protokoly obecně udržují směrovací tabulku a stanovují přesná pravidla komunikace a formáty zpráv nesoucích směrovací informace. Směrovací protokoly dělíme:

- Statické – směrovací tabulka je dána konfigurací počítače, změny je třeba provést ručně. Využívá ho většina zařízení v Internetu.
- Dynamické – průběžně reaguje na změny v topologii sítě a přizpůsobuje jim směrovací tabulky. Podle způsobu výměny informací o stavu sítě, lze dynamické směrování rozdělit do několika základních skupin.

[1] Regional Internet registry. In: *Wikipedia: the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation, 2001-, 2 April 2013 [cit. 2013-03-11]. Dostupné z: http://en.wikipedia.org/wiki/Regional_Internet_registry



Obrázek 2 Základní rozdělení dynamických směrovacích protokolů[2]

1.2.1 Interní směrovací protokoly (IGP)

Slouží k výměně směrovacích informací v rámci jednotlivých autonomních systémů.

Distance-vector směrovací protokoly

Směrovače udržují ve směrovací tabulce informaci o vzdálenosti (vektoru) do dané sítě. Tuto tabulku periodicky zasílají sousedům, kteří si svoji tabulku upraví a odesílají dál. Podle vzdálenosti se potom určuje nejlepší cesta.

- RIP
  - nejběžnější IGP v Internetu
  - směrovací tabulky aktualizuje každých 30 sekund
  - směruje pouze do vzdálenosti 15 skoků – omezená velikost sítě
  - pro malé a střední sítě
- EIGRP
  - pouze pro Cisco zařízení, pro velké heterogenní sítě
  - maximum 255 skoků
  - využívá metriku, kterou určuje z pásma a zpoždění (případně i zátěže a spolehlivosti)

Link-state směrovací protokoly

Směrovače udržují komplexní databázi síťové topologie. Do svého okolí periodicky zasílají

[2] Směrování a směrovací protokoly. *Neoo72* [online]. [21-Jun-2009] [cit. 2013-03-11]. Dostupné z: http://www.neoo72.ic.cz/doc/pos/10_protokoly.pdf

Hello pakety nesoucí informace o stavu směrovače. Rychle reaguje na změnu topologie.

- OSPF
  - směrovače zasílají informace všem sousedním směrovačům v oblasti a vytvářejí databázi topologie (model celé oblasti)
  - pomocí Dijkstrova algoritmu se vypočítává nejkratší cesta a zapisuje se do směrovací tabulky, k výpočtu používá cenu cesty (ohodnocené hrany)
  - neomezený počet skoků
  - pro rozsáhlé heterogenní sítě
- IS-IS
  - podobný OSPF, stejný princip, ale místo ceny cesty vypočítává ohodnocení pomocí metriky

1.2.2 Externí směrovací protokoly (EGP)

Slouží pro komunikaci mezi jednotlivými autonomními systémy. Prioritou je stabilita. Prakticky jediným představitelem je v současnosti BGP.

1.3 Porovnání BGP a IGP

Interní směrovací protokoly byly navrženy k výměně informací v rámci jednotlivých autonomních systémů. Přestože každý z interních protokolů pracuje jinak, všechny byly navrženy se společným cílem – najít v rámci autonomního systému optimální cestu k cíli.

Pro IGP platí některé nebo všechny z následujících charakteristik:

- odhaluje topologii sítě,
- snaží se dosáhnout rychle konvergence,
- vyžaduje pravidelné aktualizace k zajištění přesnosti směrovacích informací,
- spadá pod totožnou administrativní kontrolu,
- předpokládá společnou směrovací politiku,
- poskytuje omezené řízení směrovací politiky.

Kvůli těmto charakteristickým znakům nejsou IGP vhodné k zajištění komunikace mezi autonomními systémy. K zajištění komunikace mezi autonomními systémy je důležité, aby byl protokol schopný zajistit rozsáhlou kontrolu směrovací politiky, protože různé systémy často vyžadují různé směrování a administrativu.

Další nevýhodou IGP je nutnost periodického obnovování směrovacích tabulek, to není možné v tak rozsáhlé síti, jako je Internet, zajistit.

Naproti tomu BGP byl od začátku navrhován k zajištění komunikace mezi autonomními systémy. Dva z nejdůležitějších cílů byly zajištění řízení směrovací politiky a škálovatelnosti.

BGP obvykle není vhodný jako náhrada IGP kvůli jeho pomalejším reakcím na změny v topologii. Při použití uvnitř autonomního systému slouží ke snížení konvergenčního času. Oba typy protokolů mají při navrhování sítí své místo a je důležité je použít vhodným způsobem.

Tabulka 1 Porovnání směrovacích protokolů[3]

Protokol	Interní / Externí	Typ	Hierarchie	Metrika
RIP	Interní	Vektor vzdálenosti	Ne	Počet přeskoků
OSPF	Interní	Stav linky	Ano	Cena
IS-IS	Interní	Stav linky	Ano	Metrika
EIGRP	Interní	Pokročilý vektor vzdálenosti	Ne	Kombinovaný
BGP	Externí	Vektor cesty	Ne	Atributy

[3] MĚŘIČEK, Tomáš. *Metodika nasazení protokolu BGP pro směrování mezi autonomními uzly*. Hradec Králové, 2012. Diplomová práce. Univerzita Hradec Králové, Fakulta informatiky a managementu, Katedra informačních technologií. str. 4

2 PROTOKOL BGP

2.1 BGP obecně

BGP je dynamický směrovací protokol používaný pro směrování mezi autonomními systémy. Je základem propojení sítí různých ISP v peeringových uzlech.

Směrování mezi autonomními systémy má charakteristické požadavky, které se nevyskytují v interním směrování. Směrovací tabulky obsahují stovky tisíc záznamů, nejdůležitějším kritériem nebývá vzdálenost, ale posuzují se nastavitelné parametry zohledňující například cenu a dodatečná pravidla aplikovaná v závislosti na zdroji, cíli, seznamu tranzitních autonomních systémů a dalších atributech.

Vzhledem k velkému počtu záznamů se v případě změn v topologii vyměňují pouze informace o změnách, nikoliv celé směrovací tabulky.

2.2 Vlastnosti BGP

Podle [7].

2.2.1 Stabilita

Stabilita je klíčovým atributem rozsáhlých sítí, a proto je na ni kladen zvláštní důraz. Internet je v dnešní době tak rozsáhlou sítí, že pokud by docházelo k flapování velkého množství cest, znamenalo by to velké problémy pro celou počítačovou síť.

Flapování může být způsobeno špatnou konfigurací, která způsobí časté změny stavů cest (up a down). To potom způsobí nadměrnou činnost všech ostatních směrovačů, protože musí při každé takové změně aktualizovat směrovací tabulku. BGP je navrženo tak, že v průběhu těchto aktualizací nemusí fungovat provoz běžné komunikace. Na Internetu mohou aktualizace BGP tabulek způsobit výpadek i na několik minut.

Vliv na stabilitu má také konvergence sítě, tím se rozumí stav, kdy mají všechny směrovače kompletní směrovací tabulku a nedochází tedy k žádné aktualizaci. V nezkonvergovaných sítích může docházet ke ztrátě packetů nebo výskytu směrovacích smyček. Při procesu konvergování sítě je snížena její stabilita. Poměr mezi konvergencí a stabilitou může záviset i na samotném poskytovateli internetového připojení. Např. když BGP používá VPN (privátní veřejnou síť) pomocí MPLS (protokol pro přepínání podle návěští), je kladen větší důraz na konvergenci sítě, než na její stabilitu.

2.2.2 Spolehlivost

Na rozdíl od většiny ostatních protokolů používajících UDP (User Datagram Protocol) používá BGP k zaručení spolehlivosti TCP (Transmission Control Protocol). Díky tomu se

BGP nemusí starat o fragmentování, přeposílání, potvrzování a doručování ve správném pořadí. O to se stará právě TCP. Navíc se ještě může ověřování použité v TCP využít i v BGP. Po navázání spojení začne BGP v určitém časovém intervalu posílat svým sousedům dotazovací zprávy, aby zjistil, jestli jsou stále na příjmu. K tomu používá BGP keepalive zprávy a časovač Hold down.

Pro spolehlivé přeposílání jsou důležité přesné směrovací informace. Ke zvýšení spolehlivosti používá BGP několik technik. Po přijmutí aktualizace zkontroluje BGP atribut AS_PATH (BGP atribut obsahující seznam všech autonomních systémů na trase), slouží k prevenci výskytu směrovacích smyček. Aktualizace pocházející ze stejného autonomního systému nebo jím procházející jsou automaticky zahozeny. Na příchozí aktualizace lze také použít příchozí filtry, které potom pustí pouze aktualizace splňující místní síťovou politiku. Přeskok k síti (next-hop) je předtím, než BGP prohlásí cestu za platnou, pravidelně kontrolován.

Ze směrovací tabulky je nezbytné co nejdříve odstraňovat nedosažitelné cesty. Protokol je odstraní, jakmile dojde k výpadku s jeho sousedem. Tím je v BGP zachována spolehlivost tras.

2.2.3 Škálovatelnost

Velikost škálovatelnosti protokolu lze změřit ve dvou oblastech, a to podle počtu spojení, nebo podle počtu tras. BGP je navržen tak aby zvládl stovky spojení a udržoval více než 100 000 linek. Konkrétní hodnoty závisí na použitém hardwaru a verzi operačního systému směrovače.

Možnosti ke zvýšení škálovatelnosti protokolu buď redukují počet udržovaných cest (linek), nebo snižují počet generovaných aktualizací.

V BGP propaguje směrovač nejlepší cesty pouze svým přímým sousedním směrovačům. Jakmile dojde ke změně u jakékoliv z těchto cest, automaticky se vybere jiná cesta a ta je automaticky inzerována okolním směrovačům. Stará cesta je potom zapomenuta.

Pokud dochází k výměně směrovacích informací v rámci jednoho autonomního systému, musí být směrovače ve stavu full-mesh (kompletní vzájemná relace mezi směrovači). Směrovače ve stavu full-mesh snižují škálovatelnost BGP na základě počtu udržovaných vazeb na každém směrovači. Řešení potom spočívá v zavedení reflektorů, konfederací a agregací cest.

2.2.4 Flexibilita

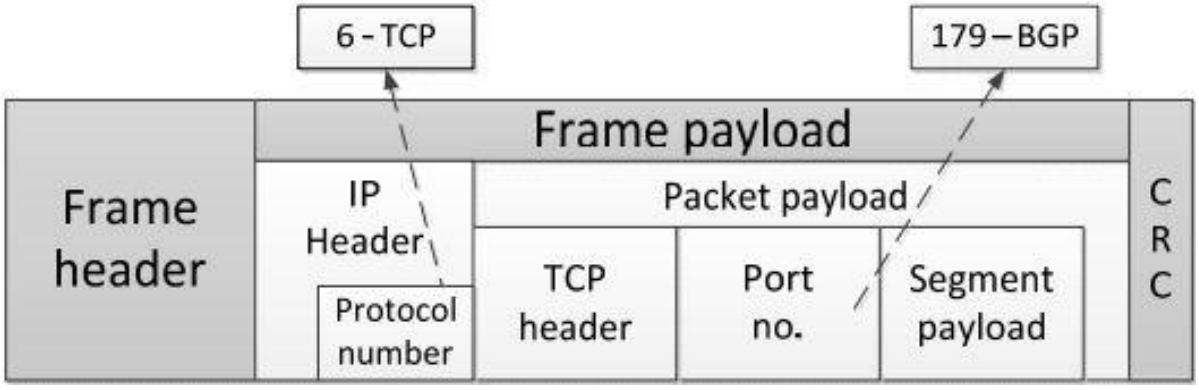
BGP je flexibilním protokolem využívajícím několik upravitelných atributů použitelných pro nastavení politiky sítě. Tyto parametry popisují vlastnosti BGP prefixů.

Existují dvě základní politiky protokolu BGP:

- Směrovací (Routing) – Ovlivňuje výběr příchozích a odchozích cest. Příkladem je nastavení filtrování příchozích cest, kde jsou povoleny pouze cesty od poskytovatele internetového připojení a jeho zákazníků. Případně lze nastavením určitých parametrů preferovat jednu cestu nad ostatními.
- Administrativní (Administrative) – Kontroluje příchozí a odchozí cesty autonomního systému. Příkladem je ochrana hraničního směrovače v podobě omezení maximálního počtu přijímacích prefixů nebo nastavení hraničního směrovače k propagování pouze zvolených odchozích cest.

2.3 Charakteristika protokolu BGP

Podle [3], [8]. BGP je path-vector protokolem využívajícím transportního protokolu TCP k zajištění spolehlivého spojení a komunikace. BGP tedy předpokládá, že je samotné spojení spolehlivé, a proto nemá implementováno žádné opakování přenosu a mechanismus pro obnovení z chyb (jako má např. protokol EIGRP). BGP informace je nesena v TCP segmentu na portu 179 uvnitř IP paketu.



Obrázek 3 Rámec s rozebraným IP paketem[4]

Mezi jednotlivými BGP směrovači je pomocí TCP vytvořeno spojení, kterým jsou BGP zprávy odesílány. Směrovače na jednom BGP spoji nazýváme BGP sousedé. Po navázání TCP spojení probíhá mezi směrovači výměna kompletní BGP směrovací tabulky.

Vlastní komunikace potom začíná zprávou *Open*. Po výměně této zprávy se tyto sousední směrovače dostávají do stavu *Established* a mohou si začít vyměňovat BGP aktualizace. Protože se jedná o spolehlivé spojení, dochází v průběhu provozu sítě pouze k částečným aktualizacím BGP směrovací tabulky a to jen v případech změn v síti.

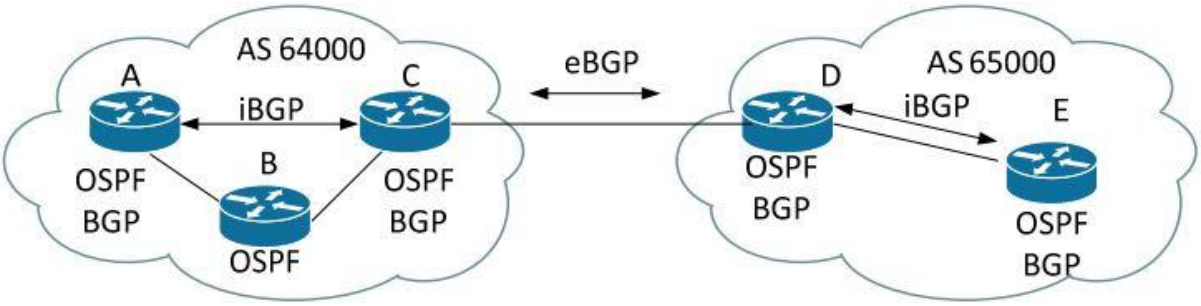
Standardně dochází k pravidelným výměnám *Keepalive* zpráv každých 60 sekund

[4] TEARE, Diane. *Implementing Cisco IP routing (ROUTE): foundation learning guide : foundation learning for the ROUTE 642-902 exam*. Indianapolis: Cisco Press, c2010, xxix, 945 s. ISBN 978-1-58705-882-0. str. 495

a k odpočítávání *Dead* intervallu (standardně 180 sekund). Podobně jako u *Hello* a *Dead* zpráv u EIGRP a OSPF.BGP v Internetu propaguje přes 300 000 sítí, tento počet stále roste. TCP používá dynamickou velikost rámce povolující posílání až 65 576 B dat bez nutnosti zastavení přenosu s následnou kontrolovat. Např. pokud je velikost paketu 500 B a je nastavena maximální velikost rámce, tak BGP zastaví přenos dat a počká na ověření až po odeslání 130 paketů.

2.4 Typy vazeb mezi směrovači

Podle [2], [3], [7]. Mezi dvojicemi hraničních směrovačů sousedních autonomních systémů se pomocí UPDATE zpráv šíří směrovací informace. V případě, že je v jednom autonomním systému hraničních směrovačů více, je potřeba zajistit šíření směrovacích informací nejen mezi BGP peery různých autonomních systémů, ale i mezi směrovači stejného autonomního systému (tzn. přes síť směrovačů s nějakým IGP směrovacím protokolem). Vazbu mezi BGP směrovači různých autonomních systémů nazýváme externí BGP (eBGP). Vazbě mezi BGP směrovači totožného autonomního systému potom označujeme jako interní BGP (iBGP). V případě iBGP je vazba mezi BGP směrovači pouze logická, nemusejí být přímými sousedy. Rozdíly mezi vztahy iBGP a eBGP jsou pouze minimální, liší se pouze v přidávání cest do směrovacích tabulek a procesem aktualizace BGP.



Obrázek 4 Vazby mezi BGP směrovači (iBGP, eBGP)[5]

2.4.1 Externí BGP (eBGP)

Nejčastější fyzické spojení mezi dvěma směrovači je tvořeno pouze jednou linkou vedoucí mezi různými autonomními systémy s nastaveným eBGP vztahem. Mezi sousedními směrovači neprobíhá žádná komunikace na úrovních interních směrovacích protokolů. K navázání samotného BGP spojení mezi dvěma směrovači musí nejprve proběhnout třícestné navázání komunikace (three-way handshake) TCP na obou stranách linky. Proto musí být IP

[5] MĚŘIČEK, Tomáš. *Metodika nasazení protokolu BGP pro směrování mezi autonomními uzly*. Hradec Králové, 2012. Diplomová práce. Univerzita Hradec Králové, Fakulta informatiky a managementu, Katedra informačních technologií. str. 12

adresa v network příkazu v BGP dosažitelná bez použití interního směrovacího protokolu. Toho lze dosáhnout použitím IP adresy dosažitelné pomocí přímo připojené sítě, nebo použitím statické cesty směřující k této IP adrese.

Podmínky pro použití eBGP:

- Odlišné číslo autonomního systému – sousední směrovače se musí nacházet v různých autonomních systémech.
- Stanovení sousedů – před samotnou výměnou BGP směrovacích aktualizací musí být navázáno TCP spojení.
- Dosažitelnost – IP adresa použitá v BGP network příkazu musí být dosažitelná (eBGP sousedé jsou mezi sebou zpravidla přímo propojeni).

2.4.2 Interní BGP (iBGP)

Interní BGP spojení probíhá mezi směrovači stejného autonomního systému. Významem iBGP je mít totožné směrovací informace o vnějších autonomních systémech a poskytovat tyto informace dále ostatním směrovačům nacházejícím se v jiných autonomních systémech. Sousední iBGP směrovače nemusejí být propojeny přímo, dokud jsou dosažitelné tak, že mezi nimi TCP naváže sousední BGP vztah. Sousední směrovače jsou mezi sebou dosažitelné, pokud jsou připojeny napřímo, je použita statická cesta nebo pomocí interního směrovacího protokolu. Většinou se v BGP network příkazu používá loopback IP adresa směrovače, protože mezi směrovači stejného autonomního systému často existuje několik možných cest.

Podmínky pro použití iBGP:

- Totožné číslo autonomního systému – sousední směrovače se musí nacházet ve stejném autonomním systému.
- Stanovení sousedů – před samotnou výměnou BGP směrovacích aktualizací musí být navázáno TCP spojení.
- Dosažitelnost – iBGP sousedé musí být navzájem dosažitelní (zpravidla jsou ve stejném autonomním systému).

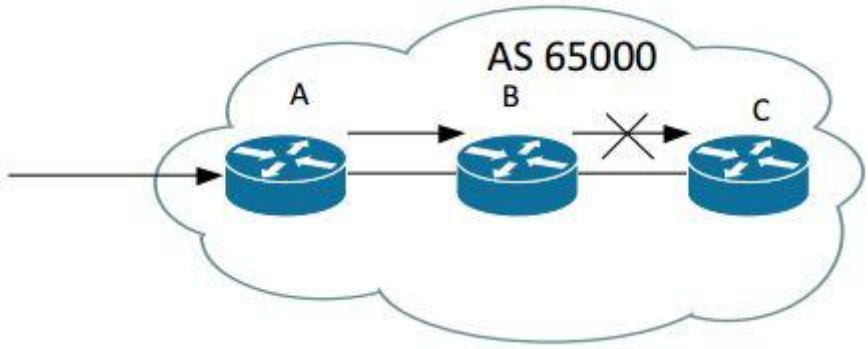
2.5 Split-Horizon a Full-Mesh v iBGP

Podle [3], [7]. Při navrhování BGP se předpokládalo, že se bude využívat pouze mezi různými autonomními systémy a uvnitř autonomních systémů se nevyskytne. Transitní autonomní systém (většinou se jedná o poskytovatele internetového připojení) je takový autonomní systém, který leží mezi dvěma vzájemně komunikujícími autonomními systémy. Všechny směrovače transitního autonomního systému musí znát všechny externí cesty. Kvůli velikosti

Internetu již není možné využít redistribuce BGP cest do IGP protokolů na hraničním směrovači. Proto se přešlo k používání full-mesh iBGP.

U eBGP zamezujeme vytváření smyček tak, že do autonomního systému nepřijímáme cesty, jejichž path vector už obsahuje číslo tohoto autonomního systému. Tato metoda ale nejde uplatnit v případě předávání informace mezi více směrovači v tomtéž autonomním systému (iBGP). Proto je důležité dodržovat k předávání informace v rámci autonomního systému dodatečné podmínky:

- Split-Horizon - informace přijatá z iBGP se šíří na eBGP peery, ale nešíří se na další iBGP peery.
- Informace přijatá z eBGP se šíří na ostatní eBGP peery i na všechny iBGP peery.



Obrázek 5 Pravidlo Split-horizon[6]

Pravidlo split-horizon zabrání ve spojení (viz Obrázek 5) směrovači B v propagaci cest naučených od směrovače A. Zabraňuje tak výskytu směrovacích smyček uvnitř autonomního systému. K naučení všech BGP cest uvnitř autonomního systému je proto potřeba použít full-mesh iBGP spojení.

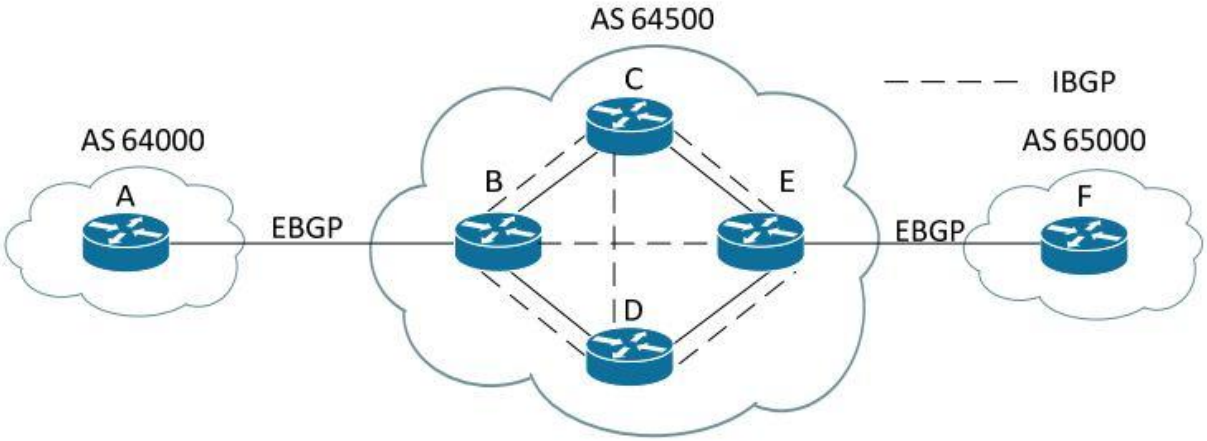
Interní směrovací protokoly si vyměňují směrovací informace pouze se svými přímými sousedy. K šíření topologických změn uvnitř autonomního systému používají broadcast nebo multicast. Pro zpracování směrovací aktualizace a zachování totožných topologických informací musí všechny směrovače uvnitř autonomního systému pracovat se stejným směrovacím protokolem.

Použitím zapojení full-mesh jsou všichni iBGP sousedé po přijetí aktualizace z vnějšího autonomního systému pomocí eBGP směrovače, který aktualizaci přijal, informováni o změnách v síti. iBGP směrovač už potom svým sousedům informaci o aktualizaci neposílá,

[6] MĚŘIČEK, Tomáš. *Metodika nasazení protokolu BGP pro směrování mezi autonomními uzly*. Hradec Králové, 2012. Diplomová práce. Univerzita Hradec Králové, Fakulta informatiky a managementu, Katedra informačních technologií. str. 14

protože předpokládá, že je o těchto změnách hraniční eBGP směrovač informoval také.

Důvodem použití full-mesh je pravidlo split-horizon, které zabraňuje výskytu směrovacích smyček. Kvůli nutnosti zajištění spolehlivého doručování nemůže být TCP spojení broadcastové ani multicastové. Proto nemůže vysílat BGP broadcastově ani multicastově. Existence full-mesh spojení v autonomním systému je proto předpokladem pro stejný výběr nejlepších cest z autonomního systému.



Obrázek 6 Full-Mesh iBGP[7]

Full-Mesh spojení (viz Obrázek 6) zajišťuje, že jakmile směrovač B přijme aktualizaci od směrovače A, rozešle ji všem směrovačům uvnitř autonomního systému. Aktualizace je poslána pouze jednou a není nikde duplikována.

Pokud by neexistovalo iBGP spojení mezi směrovači B a E, nejednalo by se o full-mesh spojení (pouze partial-mesh). Směrovač B by pak odeslal aktualizační zprávu směrovačům C a D. Ty už by kvůli split-horizon pravidlu aktualizační zprávu směrovači E neposlaly (stejný autonomní systém). Směrovač E by potom neměl žádné informace o AS 64000, ani o případných dalších následujících autonomních systémech.

2.6 Typy redundantních spojení

Podle [2], [3], [7]. Redundantní spojení slouží k zajištění konektivity sítě při případném výpadku na jedné z linek. V případě připojení sítě k Internetu ho lze také použít jako záložní (redundantní) připojení k poskytovateli internetového připojení. Může ho být dosaženo nasazením rezervních linek nebo zařízení, jako jsou například směrovače.

[7] MĚŘIČEK, Tomáš. *Metodika nasazení protokolu BGP pro směrování mezi autonomními uzly*. Hradec Králové, 2012. Diplomová práce. Univerzita Hradec Králové, Fakulta informatiky a managementu, Katedra informačních technologií. str. 15

Typy připojení autonomního systému k poskytovateli internetového připojení jsou:

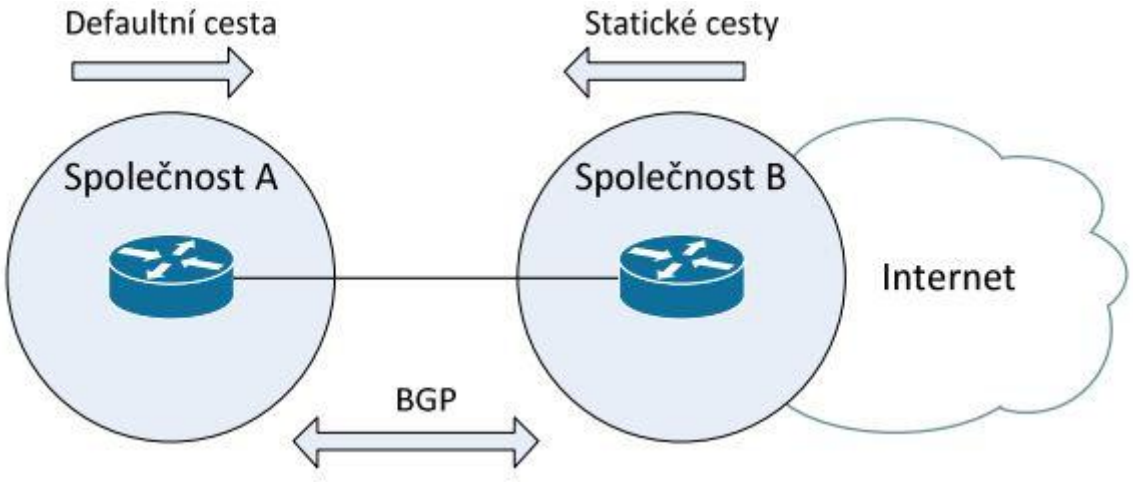
- Single-Homed
- Dual-Homed
- Dual-Homed Single-Multihomed
- Dual-Multihomed

2.6.1 Single-Homed

Spojení *Single-Homed* spočívá v připojení k jednomu poskytovateli pomocí jedné linky. Pro všechny směrovače v podnikové síti potom existuje jeden krajní směrovač, pomocí kterého je síť k poskytovateli připojena. Tím jsou potlačeny výhody použití BGP.

Používá se u sítí, které nevyžadují trvalé bezvýpadkové připojení k veřejné síti.

Single-Homed spojení nevyžaduje použití BGP, většinou se používají statické cesty. Nastavení připojení k poskytovateli je jednoduché, pokud ale nastane jakákoliv změna v topologii, dojde, narozdíl od použití BGP, k určitému časovému výpadku. Výchozí cesta je nastavena na straně zákazníka a statická cesta na straně poskytovatele. Druhou možností je použití protokolu BGP, to je ale náročnější na znalosti správce sítě. Na straně zákazníka potom dochází k propagaci sítě poskytovateli a poskytovatel ve stejném okamžiku oznámí pouze výchozí cestu k nově připojené síti (to je k navázání konektivity dostatečné).



Obrázek 7 Single-Homed spojení[8]

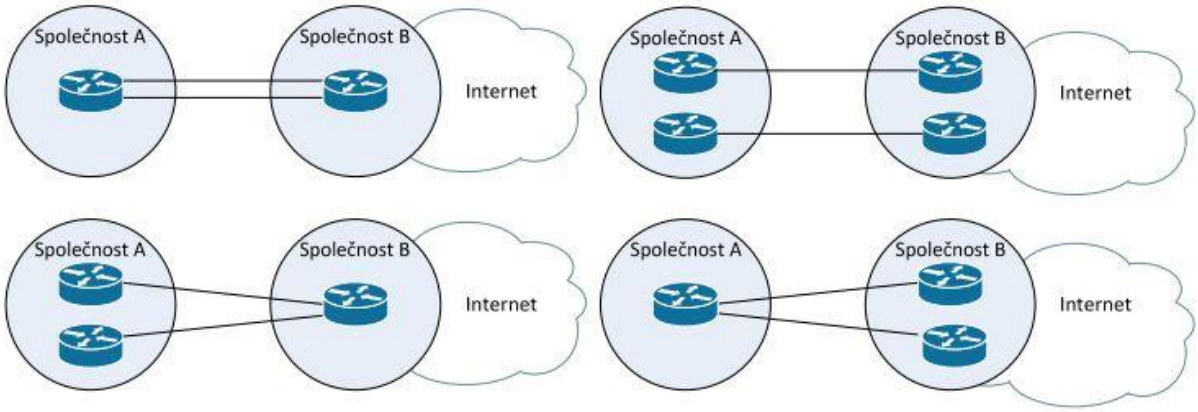
2.6.2 Dual-Homed

Spojení *Dual-Homed* spočívá v připojení k jednomu poskytovateli za použití záložních (redundantních) linek. Existují čtyři možnosti realizace tohoto spojení:

[8] MĚŘIČEK, Tomáš. *Metodika nasazení protokolu BGP pro směrování mezi autonomními uzly*. Hradec Králové, 2012. Diplomová práce. Univerzita Hradec Králové, Fakulta informatiky a managementu, Katedra informačních technologií. str. 8

- Dvojité propojení jednoho směrovače zákazníka s jedním směrovačem poskytovatele.
- Propojení jednoho směrovače na straně zákazníka se dvěma směrovači poskytovatele.
- Propojení dvou krajních směrovačů zákazníka s jedním směrovačem poskytovatele.
- Propojení linek na dvou samostatných směrovačích zákazníka se dvěma samostatnými směrovači poskytovatele.

Ve všech případech lze potom použít buď jedno primární a jedno záložní spojení, kdy k přijímání a odesílání dat slouží primární linka a záložní cesta je použita pouze v případě výpadku primární nebo rozdělení zátěže mezi obě linky pomocí Cisco expresního zasílání (Cisco Express Forwarding (CEF) switching). V obou případech probíhá směrování staticky nebo dynamicky (většinou za použití BGP).



Obrázek 8 Dual-Homed spojení[9]

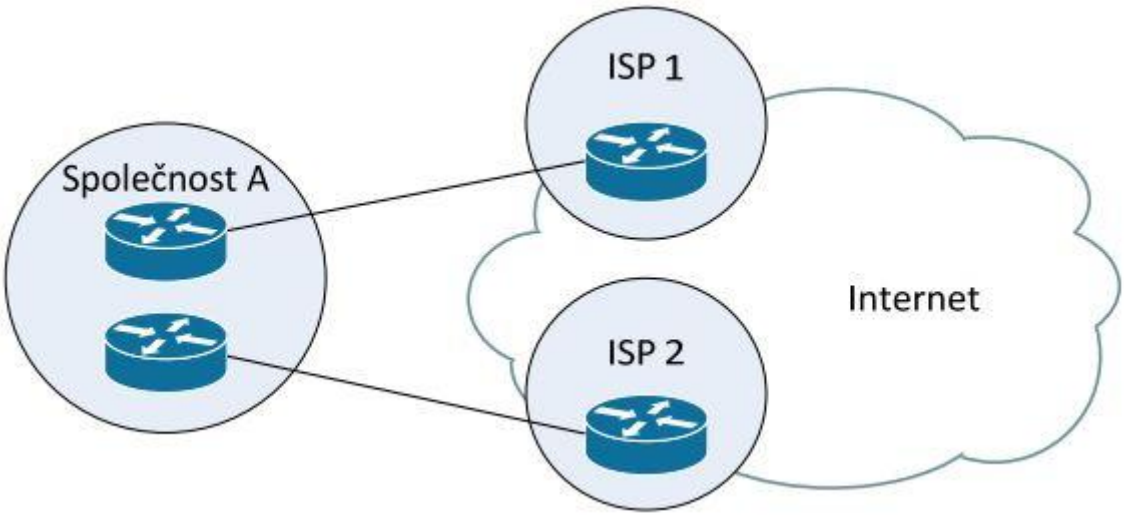
2.6.3 Single-Multihomed

Spojení *Single-Multihomed* spočívá v připojení k několika odlišným poskytovatelům internetového připojení. Výhody tohoto spojení jsou:

- Pro různé cílové sítě je použit poskytovatel, který je cíli blíže.
- Škálovatelnost řešení mezi poskytovateli.
- Dosažení nezávislosti na jednom poskytovateli (např. při výpadku linky nebo změně politiky).

K dosažení funkčnosti tohoto typu spojení je nutné zajistit dynamické směrování např. použitím BGP.

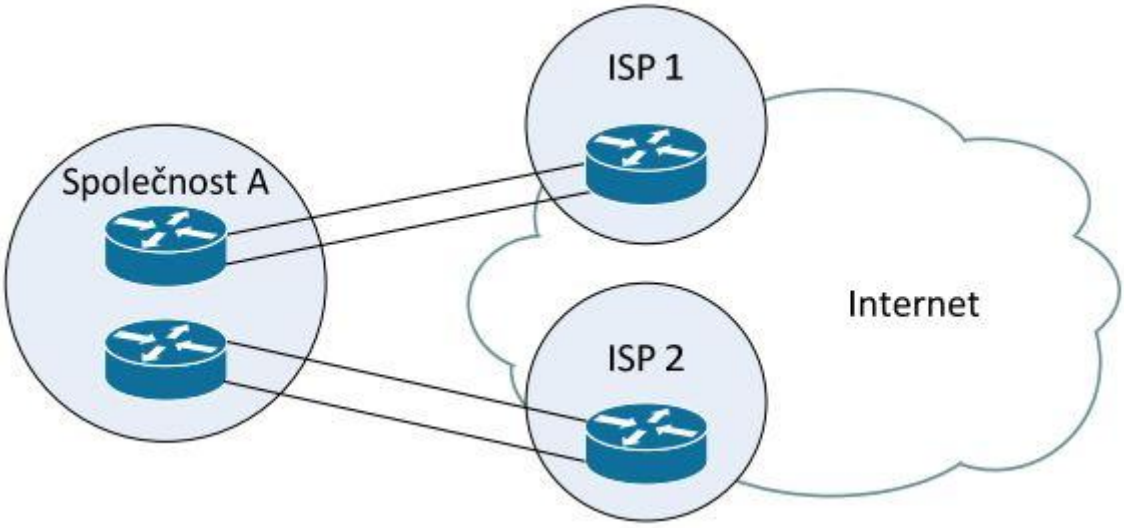
[9] MĚŘIČEK, Tomáš. *Metodika nasazení protokolu BGP pro směrování mezi autonomními uzly*. Hradec Králové, 2012. Diplomová práce. Univerzita Hradec Králové, Fakulta informatiky a managementu, Katedra informačních technologií. str. 9



Obrázek 9 Single-Multihomed spojení[10]

2.6.4 Dual-Multihomed

Spojení *Dual-Multihomed* spočívá v redundantním připojení k několika odlišným poskytovatelům internetového připojení. Používá se výhradně BGP. Většinou je použito několik krajních směrovačů zákazníka pro každé spojení s poskytovatelem. Propojení je redundantní a využívá všech výhod spojení *Single-Homed*.



Obrázek 10 Dual-Multihomed spojení[11]

[10] MĚŘIČEK, Tomáš. *Metodika nasazení protokolu BGP pro směrování mezi autonomními uzly*. Hradec Králové, 2012. Diplomová práce. Univerzita Hradec Králové, Fakulta informatiky a managementu, Katedra informačních technologií. str. 9

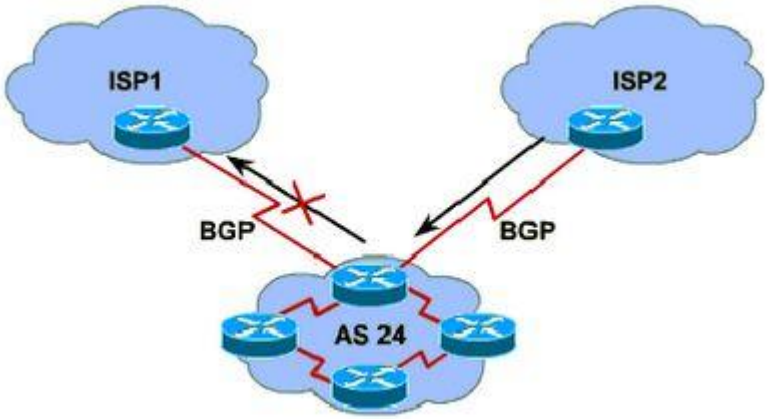
[11] MĚŘIČEK, Tomáš. *Metodika nasazení protokolu BGP pro směrování mezi autonomními uzly*. Hradec Králové, 2012. Diplomová práce. Univerzita Hradec Králové, Fakulta informatiky a managementu, Katedra informačních technologií. str. 10

2.7 Netranzitní a tranzitní multihomed spojení autonomních systémů

Podle [2], [3], [7].

2.7.1 Netranzitní multihomed spojení

Používá se v případě připojení sítě, z důvodu odolnosti proti výpadku, k více různým poskytovatelům. Autonomní systém potom nepřipouští přenos (tranzit) cizího provozu.



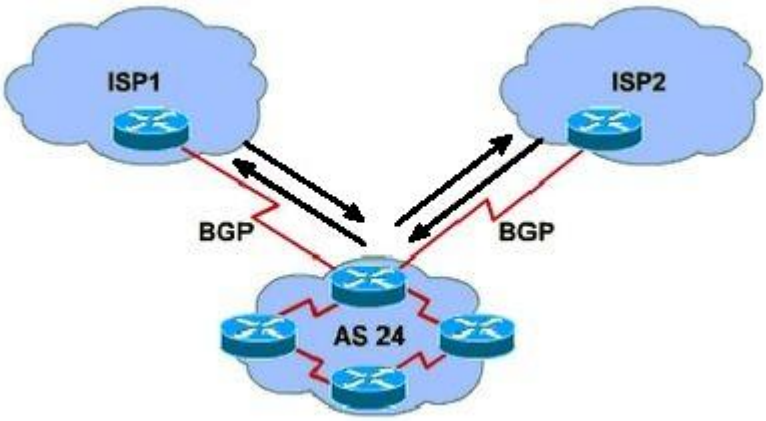
Obrázek 11 Netranzitní multihomed spojení[12]

AS 24 na Obrázek 11 nepropaguje cesty k sítím ISP2 do ISP1. Provoz ISP1 pro ISP2 se ale může autonomnímu systému AS 24 vnutit explicitně (např. statickým směrováním). Proto se u netranzitních multihomed autonomních systémů instalují na vstupní linky filtry, které nepropouštějí pakety určené pro sítě vně tohoto netranzitního autonomního systému.

[12] GRYGÁREK, Petr. Směrovací protokol BGP. *Katedra informatiky: Fakulta elektrotechniky a informatiky, VŠB-TUO* [online]. Dostupné z: http://www.cs.vsb.cz/grygarek/SPS/lect/BGP/BGP.html

2.7.2 Tranzitní multihomed spojení

Tranzitní multihomed spojení umožňuje přenos cizího provozu přes vlastní autonomní systém.



Obrázek 12 Tranzitní multihomed spojení[13]

Na Obrázek 12 je znázorněno, že si AS24 vyměňuje směrovací informace s autonomními systémy ISP1 a ISP2.

Typickým příkladem tranzitního autonomního systému je autonomní systém poskytovatele internetového připojení.

2.8 Synchronizace BGP

Podle [3], [7], [9]. Pravidlo pro použití BGP synchronizace – BGP směrovač nemůže použít ani zveřejnit cestu získanou z iBGP spojení, pokud není lokální nebo nepochází z interního směrovacího protokolu.

Synchronizace BGP může být vypnuta v případě existence vzájemné relace mezi všemi směrovači uvnitř jednoho autonomního systému.

V dnešní době se již synchronizace běžně nepoužívá z důvodu *full-mesh* relace mezi směrovači uvnitř autonomního systému.

2.9 Použití/nepoužití BGP

Podle [3], [10].

2.9.1 Použití BGP

BGP je vhodné použít v případě celkového porozumění jeho principu, když je zaručený přínos k chodu sítě a je splněn alespoň jeden z následujících bodů:

---

[13] Vlastní modifikace obrázku: GRYGÁREK, Petr. Směrovací protokol BGP. *Katedra informatiky: Fakulta elektrotechniky a informatiky, VŠB-TUO* [online]. Dostupné z: http://www.cs.vsb.cz/grygarek/SPS/lect/BGP/BGP.html

- Autonomní systém je propojen s několika autonomními systémy.
- Je nutné zajistit komunikaci autonomního systému s jiným autonomním systémem.
- Je potřeba měnit směrovací politiku provozu z a do autonomního systému.
- Společnost chce svůj provoz na Internetu odlišit od provozu poskytovatele internetového připojení (když je podnik propojený s poskytovatelem statickou cestou, je jeho provoz na Internetu k nerozeznání od provozu poskytovatele).

BGP umožňuje komunikaci a výměnu paketů mezi jednotlivými poskytovateli internetového připojení. Poskytovatelé jsou mezi sebou propojeni několika linkami a při výměně informací dodržují stanovená pravidla. K nastavení těchto pravidel slouží právě BGP. Pokud není protokol nakonfigurovaný správně, může to mít výrazný dopad na plynulý provoz podnikové sítě. Příkladem může být podnik připojený k Internetu přes dva poskytovatele. V takovém případě je potřeba nastavit směrovací politiku tak, aby zabránila posílání paketů od jednoho poskytovatele ke druhému přes podnikovou síť. Zároveň je potřeba přijímat pakety určené do podnikové sítě od obou poskytovatelů s minimálními nároky na šířku pásma.

2.9.2 Nepoužití BGP

BGP se nedoporučuje používat v případech, kdy:

- existuje pouze jediné připojení k Internetu nebo k jinému autonomnímu systému;
- krajní směrovače nemají pro potřeby BGP aktualizací dostatečnou paměť nebo výkon;
- si administrátor není jistý v porozumění filtrování a manipulaci cest.

2.10 BGP tabulky

Podle [3], [9], [10]. BGP využívá nezávisle na směrovači dvě směrovací tabulky. Jednu odpovídající IP směrovací tabulce existující na všech směrovačích a druhou, zcela oddělenou, sloužící pouze pro účely BGP.

- BGP tabulka
  - obsahuje seznam všech sítí získaných od každého ze sousedů,
  - k jednomu cíli může obsahovat několik různých záznamů,
  - ke každé cestě eviduje její BGP atributy.
- IP směrovací tabulka
  - obsahuje seznam nejlepších cest do cílových sítí,
  - z BGP tabulky jsou vybrány pouze nejlepší cesty.

Nejlepší cesty z BGP tabulky jsou na směrovači nabídnuty IP směrovací tabulce. Informace o cestách mohou být sdíleny na základě, na příslušném směrovači nastavené, redistribuce.

BGP dále uchovává informace o sousedních směrovačích propojených pomocí BGP (tabulka sousedů). K navázání BGP sousednosti je potřeba příslušné sousední směrovače nastavit. BGP potom vytvoří TCP spojení ke všem nastaveným směrovačům a uchová informace o jejich stavech pomocí zasílání pravidelných BGP/TCP Keepalive zpráv.

Po navázání sousednosti proběhne mezi sousedními směrovači výměna nejlepších BGP cest, které se uloží do tzv. BGP forwarding databáze. Na základě výběru nejlepších cest k jednotlivým sítím se tyto cesty u každého směrovače zadají do IP směrovací tabulky. Směrovače poté porovnají nabídnuté BGP cesty s již uvedenými cestami ke konkrétním sítím a pomocí administrativní vzdálenosti vyberou ty nejlepší.

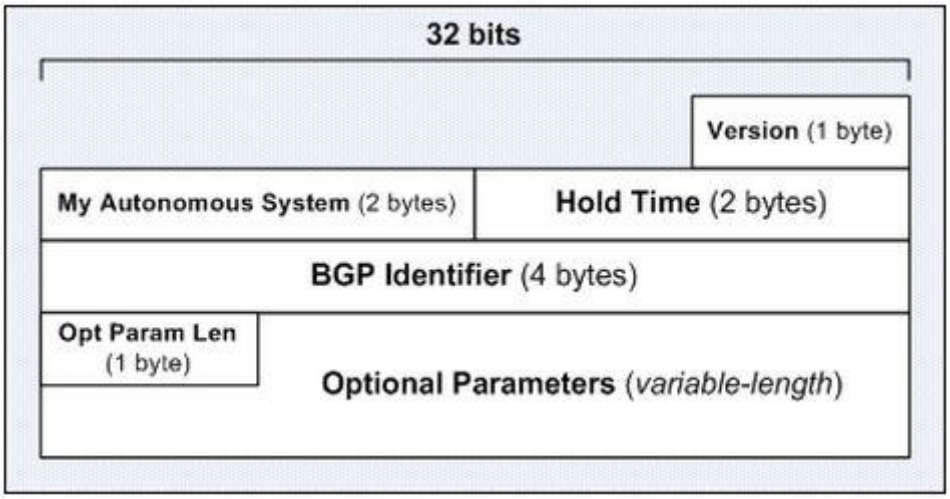
2.11 BGP zprávy

Podle [2], [3], [7], [11], [12]. BGP rozlišuje čtyři typy zpráv:

- Open
- Keepalive
- Update
- Notification

2.11.1 Open zprávy

Open zpráva je první zprávou, kterou BGP směrovač po navázání TCP spojení rozešle všem sousedním BGP směrovačům. Po jejím potvrzení je BGP spojení navázáno a dále se posílají pouze *Update, Keepalive* a *Notification* zprávy. Po navázání spojení si sousední BGP směrovače přepošlou své kompletní BGP směrovací tabulky. Po této výměně už jsou úpravy v tabulkách posílány pouze pomocí *Update* zpráv.



Obrázek 13 Formát BGP Open zprávy[14]

[14] BGP Message Types. *A New Beginning* [online]. Dostupné z: http://choudharysanjeev.blogspot.cz/

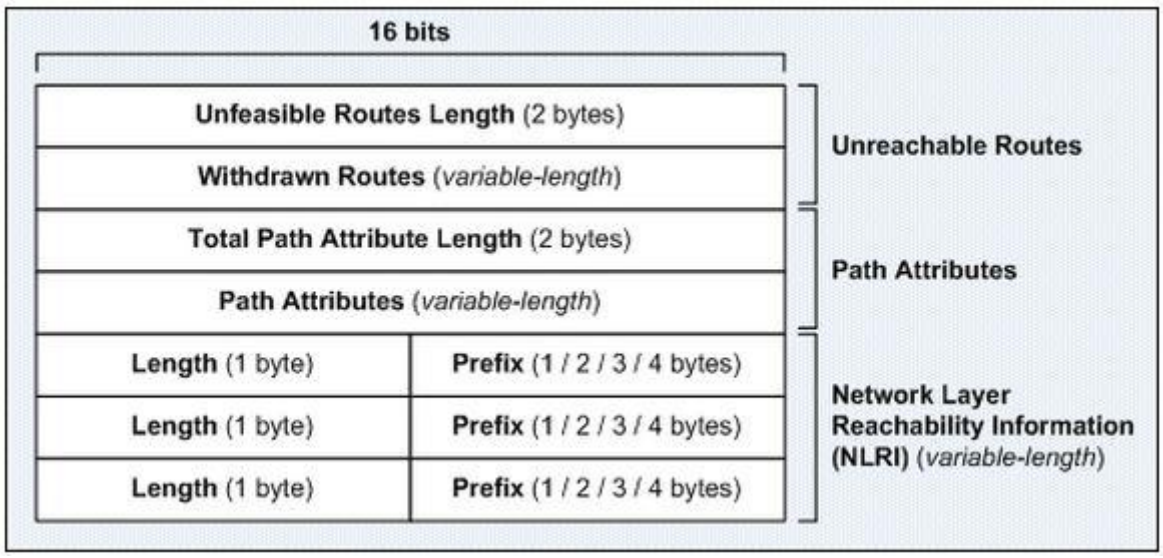
- Version – aktuálně mezi sousedními směrovači používaná verze BGP (v současnosti většinou verze 4)
- My AS Number – číslo odesílajícího autonomního systému, které určuje:
  - jedná se o iBGP spojení
  - jedná se o eBGP spojení
  - číslo AS neodpovídá, spojení se ukončí
- Hold Time – maximální počet sekund, které mohou uplynout, než směrovač obdrží *Keepalive* nebo *Update* zprávu od směrovače, který zprávu poslal
- BGP ID – identifikační číslo odesílajícího směrovače
- Opt Param Len – volitelné pole obsahující délku všech volitelných parametrů. Zpráva neobsahující volitelné parametry má v tomto poli hodnotu 0.
- Optional Parameters – pole proměnné délky obsahující volitelné parametry

2.11.2 Keepalive zprávy

Keepalive zpráva se skládá pouze z 19bytové hlavičky a slouží k ověření funkčnosti linky mezi sousedy. Posílá se periodicky (standardně s intervalem 60 sekund). Spojení se považuje za nefunkční, pokud od souseda nepřišla zpráva *Keepalive* po dobu *Hold Time* určenou předtím ve zprávě *Open*. V takovém případě směrovač dojde k názoru, že je soused nedostupný a spojení ukončí.

2.11.3 Update zprávy

Update zpráva nese samotnou směrovací informaci. Jedna zpráva se vždy použije pouze pro jednu cestu. Všechny parametry ve zprávě se potom týkají konkrétní cesty a všech na této cestě dostupných sítí. Zpráva také obsahuje sekci *Withdrawn Routes* obsahující cesty, které přestaly být funkční a mají být ze směrovací tabulky odstraněny.



Obrázek 14 Formát BGP Update zprávy[15]

- Unfeasible Routes Length – 2 byty dlouhé pole určující celkovou velikost následujících odstraněných cest. Hodnota 0 značí, že nebyly odstraněny žádné cesty a pole Withdrawn Routes bude prázdné.
- Withdrawn Routes – pole s proměnnou délkou obsahující seznam odstraněných cest
- Total Path Attribute Length – 2 byty dlouhé pole určující celkovou velikost atributů následujících tras. Hodnota 0 značí, že v Update zprávě není uvedena hodnota NLRI.
- Path Attributes – pole s proměnnou délkou obsahující seznam atributů tras.
- Network Layer Reachability Information (NLRI) – pole s proměnnou délkou obsahující seznam IP prefixů dostupných pomocí této cesty. Nulová délka pole značí prefix shodující se se všemi IP prefixy.

2.11.4 Notification zprávy

Notification zpráva značí chybu v činnosti BGP. Vysílá se také při absenci zprávy *Keepalive*. Po vyslání *Notification* zprávy dojde k ukončení vazby mezi sousedy rozpojením TCP spojení. Zpráva obsahuje číslo chyby, číslo konkrétní chyby a její údaje.

[15] BGP Message Types. *A New Beginning* [online]. Dostupné z: http://choudharysanjeev.blogspot.cz/

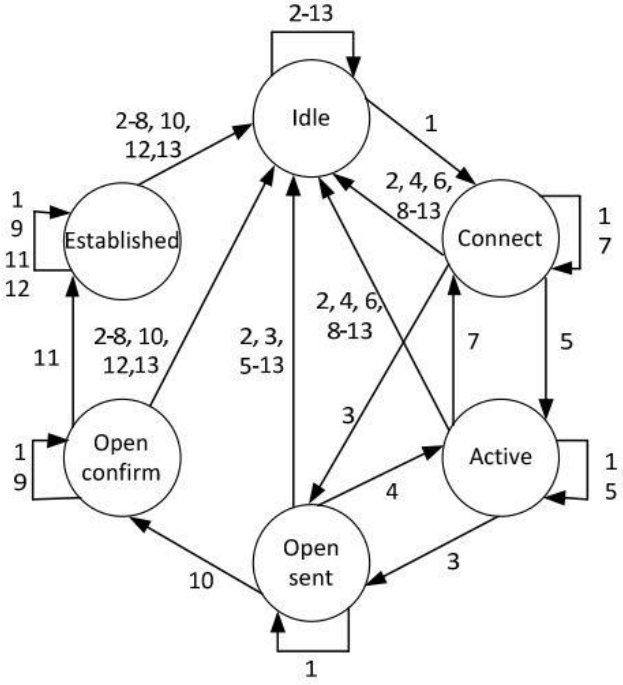
Tabulka 2 Druhy chyb Notification zpráv[16]

Číslo chyby		Podčíslo chyby	Podčíslo chyby – česky
1	**Message Header Error**	1 Connection Not Synchronized 2 Bad Message Length 3 Bad Message Type	1 Nesynchronizované spojení 2 Špatná délka zprávy 3 Špatný typ zprávy
2	**OPEN message error**	1 Unsupported Version 2 Bad Peer AS 3 Bad BGP Identifier 4 Unsupported Optional Parameter 5 Authentication Failure 6 Unacceptable Hold Time	1 Nepodporovaná verze 2 Špatný Peer AS 3 Špatný BGP identifikátor 4 Nepodporovaný volitelný parametr 5 Chybné ověření identity 6 Neakceptovatelný Hold Time
3	**UPDATE message error**	1 Malformed Attribute List 2 Unrecognized Well-known Attribute 3 Missing Well-known Attribute 4 Attribute Flags Error 5 Attribute Length Error 6 Invalid Origin Attribute 7 AS Routing Loop 8 Invalid NEXT-HOP Attribute 9 Optional Attribute Error 10 Invalid Network Field	1 Poškozený seznam atributů 2 Nerozpoznaný Well-known atribut 3 Chybějící Well-know atribut 4 Chyba vlajek atributu 5 Chyba délky atributu 6 Nesprávný původ atributu 7 Směrovací smyčka AS 8 Nesprávný NEXT-HOP atribut 9 Chyba volitelného atributu 10 Chyba pole Network
4	**Hold Timer Expired**	Žádný podkód – Vypršel Hold Timer	
5	**Finite State Error**	Žádný podkód – Chyba konečného stavu (neukončitelnost)	
6	**Cease**	Žádný podkód – Umlčení spojení	

[16] Vlastní modifikace tabulky: INETDAEMON. BGP Notification Message. INETDAEMON ENTERPRISES. *InetDaemon.Com: Free Online IT Tutorials and Internet Training* [online]. Dostupné z: http://www.inetdaemon.com/tutorials/internet/ip/routing/bgp/operation/messages/notification.shtml

2.12 BGP konečný automat (Finite State Machine)

Podle [10]. Jednotlivé fáze BGP spojení mezi sousedními směrovači lze popsat pomocí konečného automatu.



Vstupní událost	Popis
1	BGP start
2	BGP stop
3	BGP transport connection open
4	BGP transport connection closed
5	BGP transport connection open failed
6	BGP transport fatal error
7	ConnectRetly timer expired
8	Hold timer expired
9	Keepalive timer expired
10	Receive Open message
11	Receive Keepalive message
12	Receive Update message
13	Receive Notification message

Obrázek 15 BGP konečný automat[17]

Obrázek 15 znázorňuje kompletní BGP konečný automat a vstupní události způsobující jednotlivé přechody mezi stavy.

- ***Idle*** – Stav, kdy BGP začíná a odmítá všechna příchozí spojení. Spouští se časovač ConnectRetly a inicializuje se TCP spojení se sousedním směrovačem, přechází do stavu *Connect*.
- ***Connect*** – Proces BGP čeká na navázání TCP spojení. Po úspěšném navázání spojení se obnoví časovač ConnectRetly, dokončí se inicializace, sousednímu směrovači se pošle *Open* zpráva a přejde se do stavu *Open sent*. Pokud je spojení neúspěšné, čeká se na příchozí TCP spojení od sousedního směrovače, obnoví se časovač ConnectRetly a přejde se do stavu *Active*.
- ***Active*** – BGP se snaží se sousedním směrovačem navázat TCP spojení. Pokud je spojení navázáno úspěšně, provede BGP stejnou akci jako ve stavu *Connect*. V opačném případě vyprší časovač ConnectRetly, BGP proces jej obnoví a přejde do stavu *Connect*.

[17] HOONG, Yap Chin. *CCNP ROUTE Complete Guide*. 1st Edition. United States of America: CreateSpace Independent Publishing Platform, 2010. ISBN 1453807667. str. 203

- ***Open sent*** – Směrovač čeká na *Open* zprávu od svého souseda. Po přijetí ji zkontroluje. V případě zjištění jakékoliv chyby je zaslána *Notification* zpráva a přejde se do stavu *Idle*. V opačném případě se pošle *Keepalive* zpráva a nastaví se Keepalive časovač. Na obou koncích spojení se zjistí hodnota *Hold* a vybere se ta nižší. Pokud je hodnota 0, časovače Keepalive a Hold se nespustí. Dále se podle čísla autonomního systému zjistí, zda se jedná o interní nebo externí spojení a přejde se do stavu *Open confirm*.
- ***Open confirm*** – Od sousedního směrovače byla úspěšně přijata zpráva *Open* a čeká se na *Notification* nebo *Keepalive* zprávu. Po přijmutí *Keepalive* zprávy se přejde do stavu *Established*. Při přijmutí *Notification* zprávy nebo přerušení TCP spojení se proces vrátí do počátečního stavu *Idle*.
- ***Established*** – Stav, ve kterém je BGP spojení úspěšně navázáno a směrovače si mezi sebou posílají *Keepalive*, *Update* a *Notification* zprávy. Při přijmutí *Keepalive* nebo *Update* zprávy se časovač Hold obnovuje (v případě, že dohodnutý čas Hold není nulový). Při přijmutí *Notification* zprávy se přechází do počátečního stavu *Idle*.

Časovač ConnectRetly je vždy nastaven na 120 sekund a nemůže být změněn. Zprávy *Keepalive* a *Update* jsou mezi směrovači zasílány pouze ve stavu *Established*.

2.13 BGP atributy cest

Podle [2], [3], [7], [9]. BGP směrovače posílají ostatním BGP směrovačům aktualizační zprávy o cílových sítích. Tyto zprávy obsahují informace o dostupnosti jednotlivých sítí a atributy cest k těmto sítím. Atributy jsou seznamem BGP metrik popisujících jednotlivé cesty. Slouží tedy k vnějšímu ovlivnění směrovací politiky. Pomocí atributů vyjadřujeme preferenci, resp. zákaz některých cest podle nejrůznějších kriterií. Rozdělují se do čtyř skupin:

- Dobře známé povinné (Well-known mandatory) – atributy, které se musí objevit ve všech aktualizačních zprávách BGP a musí být rozpoznatelné BGP procesem.
- Dobře známé volitelné (Well-known discretionary) – atributy, které se nemusí objevit ve všech aktualizačních zprávách, ale jsou BGP procesem rozpoznatelné.
- Volitelné tranzitivní (Optional transitive) – pokud je BGP směrovač nerozpozná, rozešle je beze změny spolu s ostatními atributy dalším směrovačům.
- Volitelné netranzitivní (Optional nontransitive) – pokud je BGP směrovač nerozpozná, tak je odstraní a dalším směrovačům pošle pouze zbylé atributy.

Tabulka 3 Atributy BGP cest[18]

Atribut	eBGP	iBGP
Origin	Dobře známý povinný	Dobře známý povinný
AS-path	Dobře známý povinný	Dobře známý povinný
Next-hop	Dobře známý povinný	Dobře známý povinný
MED	Volitelný netrantzitivní	Volitelný netrantzitivní
Local-preference	Nepovolený	Dobře známý volitelný
Atomic-aggregate	Dobře známý povinný	Dobře známý volitelný
Aggregator	Volitelný tranzitivní	Volitelný tranzitivní
Community	Volitelný tranzitivní	Volitelný tranzitivní
Originator ID	Volitelný netranzitivní	Volitelný netranzitivní
Cluster list	Volitelný netranzitivní	Volitelný netranzitivní
Weight	Pouze Cisco	Pouze Cisco

2.13.1 Origin

Atribut *Origin* patří do skupiny dobře známých povinných atributů. Určuje, odkud se informace o BGP cestě vzala (původ cesty). Je automaticky vygenerovaný v době vnoření cesty do BGP procesu. Může nabývat tří hodnot:

- IGP (ORIGIN 1) – Cesta prochází z interního směrovacího protokolu. Zpravidla se jedná o cestu zařazenou do BGP použitím příkazu **network**. V BGP směrovací tabulce je označena znakem *i*.
- EGP (ORIGIN 2) – Cesta získaná redistribucí z dnes již nepoužívaného protokolu EGP. V BGP směrovací tabulce je označena znakem *e*.
- INCOMPLETE (ORIGIN 3) – Původ cesty není známý. Většinou se jedná o cestu redistribuovanou z jiného směrovacího protokolu. V BGP směrovací tabulce je označena znakem *?*.

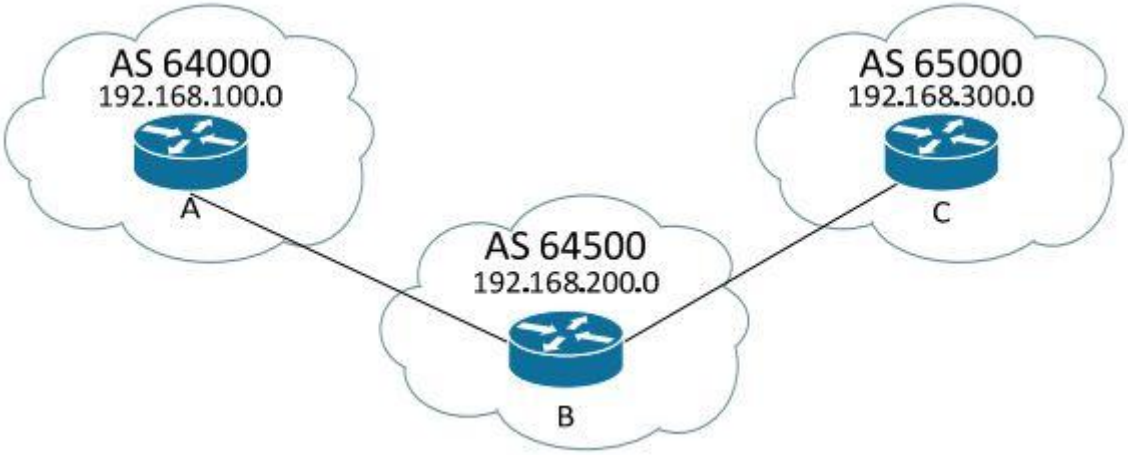
Při výběru cest je upřednostňován prefix s nižší hodnotou atributu *Origin*.

Hodnotu atributu lze změnit použitím route mapy.

2.13.2 AS-Path

Atribut *AS-Path* patří do skupiny dobře známých povinných atributů. Je základem funkce path-vector algoritmu. Obsahuje řetězec čísel autonomních systémů, přes které postupně vede cesta k cílové síti. Pokud se cesta dostane do autonomního systému, jehož číslo už AS-PATH obsahuje, cesta se ignoruje. Tímto způsobem se odstraňují cesty obsahující smyčku.

[18] MĚŘIČEK, Tomáš. *Metodika nasazení protokolu BGP pro směrování mezi autonomními uzly*. Hradec Králové, 2012. Diplomová práce. Univerzita Hradec Králové, Fakulta informatiky a managementu, Katedra informačních technologií. str. 21



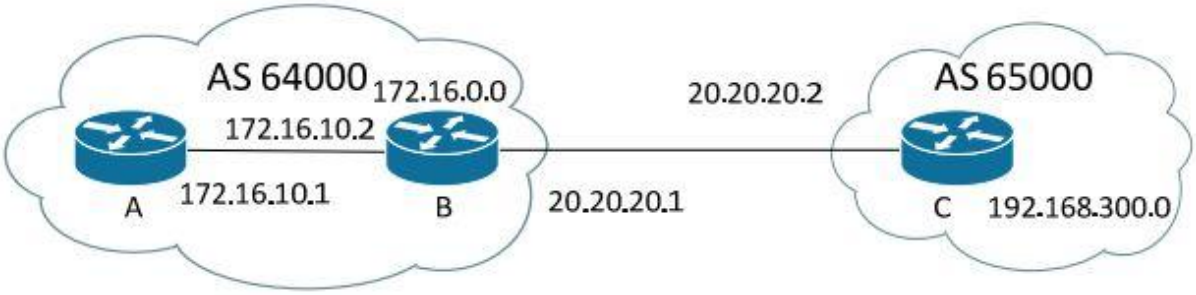
Obrázek 16 Atribut AS-PATH[19]

Směrovač A nacházející se v autonomním systému 64000 inzeruje síť 192.168.100.0 spolu s číslem AS. Jakmile síť dojde do autonomního systému 64500, směrovač B okamžitě zapíše své číslo AS k propagované síti od směrovače A a danou síť přepošle do AS 65000. Na směrovači C bude mít cesta do sítě 192.168.100.0 stanovenou trasu přes AS (64500, 64000). Pro zbylé sítě platí stejné schéma. Na směrovači A bude tedy mít síť 192.168.300.0 cestu přes AS (64500, 65000).

2.13.3 Next-hop

Atribut *Next-hop* patří do skupiny dobře známých povinných atributů. U interních směrovacích protokolů (IGP) se předpokládá, že adresa nejbližšího souseda na cestě k cílové síti (next hop) je adresa některého bezprostředně sousedícího směrovače. Např. u distance-vector protokolů adresa směrovače, který cestu poskytl. Naopak u BGP se jako atribut *Next-hop* zachovává adresa hraničního směrovače, který do autonomního systému informaci o cestě zaslal, tedy adresu směrovače z cizího autonomního systému. Proto je nutné, aby interní směrovací protokol cestu k tomuto směrovači znal. Často se tedy do interního směrovacího protokolu propagují i adresy spojovacích linek mezi autonomními systémy.

[19] MĚŘIČEK, Tomáš. *Metodika nasazení protokolu BGP pro směrování mezi autonomními uzly*. Hradec Králové, 2012. Diplomová práce. Univerzita Hradec Králové, Fakulta informatiky a managementu, Katedra informačních technologií. str. 23



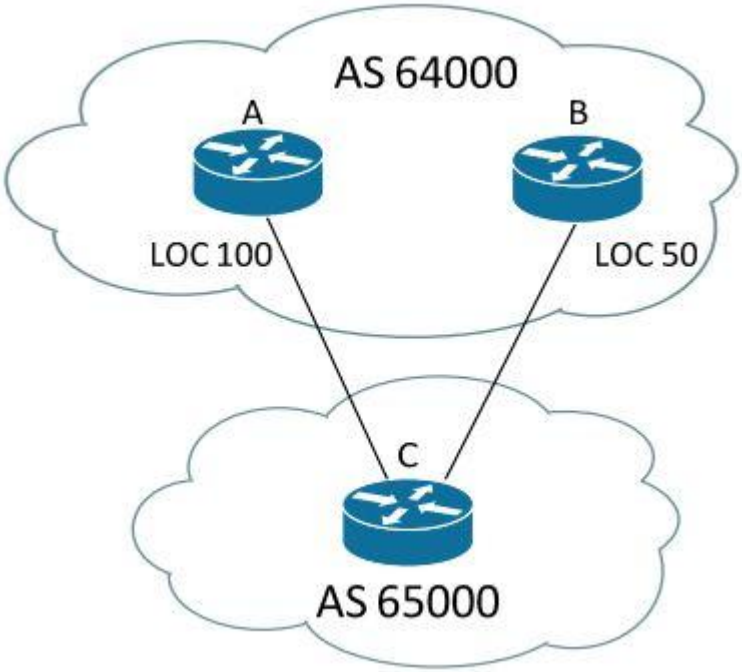
Obrázek 17 Atribut NEXT-HOP[20]

Směrovač C propaguje síť 192.168.300.0 směrovači B s přeskokem 20.20.20.1 a směrovač B propaguje směrovači C s přeskokem 20.20.20.2 síť 172.16.0.0. Samotný přeskok z eBGP je inzerován do iBGP. To znamená, že směrovač B propaguje síť 192.168.300.0 dále směrovači A s přeskokem 20.20.20.2. Síť 192.168.300.0 je tedy od směrovače A dosažitelná pomocí přeskoku 20.20.20.2 a ne 172.16.10.2. Směrovač A proto musí vědět, jak se dostat k síti 20.20.20.0, ať už pomocí interního směrovacího protokolu nebo statické cesty.

2.13.4 Local-preference

Atribut *Local-preference* patří do skupiny dobře známých volitelných atributů. Pomocí tohoto atributu se mohou směrovače multihomed autonomního systému dohodnout na společné volbě cesty k síti dostupné přes více alternativních linek. Atribut *Local-preference* může nabývat hodnot 0 až 4 294 967 295. Směrovače potom vybírají cestu s vyšší hodnotou atributu *Local-preference*. Atribut *Local-preference* ovlivňuje pouze směrovače uvnitř stejného autonomního systému a nemá žádný vliv na eBGP spojení.

[20] MĚŘIČEK, Tomáš. *Metodika nasazení protokolu BGP pro směrování mezi autonomními uzly*. Hradec Králové, 2012. Diplomová práce. Univerzita Hradec Králové, Fakulta informatiky a managementu, Katedra informačních technologií. str. 23



Obrázek 18 Atribut LOCAL-PREFERENCE[21]

Cesta ke směrovači C od směrovače A má nastavený atribut *Local-preference* na hodnotu 100, cesta od směrovače B potom na hodnotu 50. Veškerá komunikace z AS 64000 do AS 65000 bude díky vyšší hodnotě atributu *Local-preference* probíhat přes směrovač A.

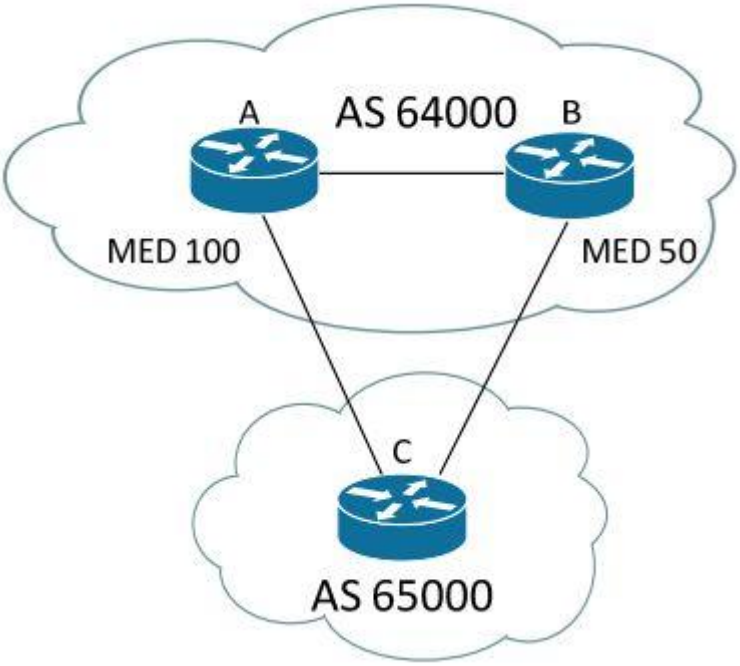
Tento atribut využijeme hlavně v případě, kdy je autonomní systém k jinému autonomnímu systému připojen více linkami podporujícími různé rychlosti přenosu (např. T3 a T1). Cílem je potom nastavit na směrovačích atribut *Local-preference* tak, aby odchozí komunikace probíhala přes rychlejší spojení (T3), pomalejší linka potom slouží jako záložní a je použita při případném výpadku rychlejší linky.

2.13.5 MED

Atribut *MED* (Multi-Exit Discriminator) patří do skupiny volitelných netranzitivních atributů. Na rozdíl od atributu *Local-preference* ovlivňujícího odchozí cestu, lze atributem *MED* ovlivnit volbu cesty používané sousedním autonomním systémem k dosažení jednotlivých sítí uvnitř, resp. za naším autonomním systémem. Atribut *MED* může nabývat hodnot 0 až 4 294 967 295. Upřednostňována je potom cesta s nižší hodnotou atributu *MED*. Atribut je poslán sousednímu autonomnímu systému a do dalšího autonomního systému již propagován není (netranzitivní). Hodnoty atributu *MED* mohou být k cestám přiřazeny manuálně nebo se

[21] MĚŘIČEK, Tomáš. *Metodika nasazení protokolu BGP pro směrování mezi autonomními uzly*. Hradec Králové, 2012. Diplomová práce. Univerzita Hradec Králové, Fakulta informatiky a managementu, Katedra informačních technologií. str. 25

může převzít hodnota metriky používaného interního směrovacího protokolu. Tím se optimalizuje rozhodnutí sousedního autonomního systému o volbě nejvhodnější vstupní linky, která je cílové síti nejblíže.



Obrázek 19 Atribut MED[22]

Směrovač A má nastavený atribut *MED* na hodnotu 100, směrovač B na hodnotu 50. Když směrovač C přijme aktualizaci (obsahující *MED* atribut) od směrovače A i B, začne upřednostňovat cestu do AS 64000 přes směrovač B, protože směrovač B má nižší hodnotu atributu *MED*.

2.13.6 Atomic-aggregate

Atribut *Atomic-aggregate* patří do skupiny dobře známých volitelných atributů. Může nabývat hodnot TRUE a FALSE. Směrovač tento atribut použije v případě, že provedl sumarizaci cest a chce tuto informaci propagovat do okolních autonomních systémů.

2.13.7 Aggregator

Atribut *Aggregator* patří do skupiny volitelných tranzitivních atributů, které mohou být zahrnuty v souhrnných aktualizacích. Směrovač provádějící agregaci se v cestě identifikuje v atributu *Aggregator* připojením svého ROUTER_ID (jeho vlastní IP adresy a čísla autonomního systému).

---

[22] MĚŘIČEK, Tomáš. *Metodika nasazení protokolu BGP pro směrování mezi autonomními uzly*. Hradec Králové, 2012. Diplomová práce. Univerzita Hradec Králové, Fakulta informatiky a managementu, Katedra informačních technologií. str. 24

2.13.8 Community

Atribut *Community* patří do skupiny volitelných tranzitivních atributů. Slouží k filtrování příchozích a odchozích cest použitím označení cest pomocí tagu určujícího konkrétní komunitu. Směrovače se potom na základě tohoto tagu rozhodují, jak budou na komunikaci reagovat. Jakýkoliv směrovač má možnost jakoukoliv příchozí nebo odchozí cestu sám označit, případně po přečtení tagu u cesty odfiltrovat nebo přesměrovat.

Cisco IOS podporuje následující komunity:

- NO_EXPORT – Komunity s tímto tagem by neměly být posílány přes eBGP spojení, ale mohou být posílány sub-autonomním systémům uvnitř stejné konfederace.
- LOCAL_AS – Komunity jsou propagovány pouze uvnitř jednoho autonomního systému. Při použití konfederací je umožněn příjem komunit pouze u sub-autonomních systémů. Pokud není použita konfederace, chová se jako NO_EXPORT.
- NO_ADVERTISE – Komunity nejsou propagovány na žádné vnitřní nebo vnější spojení.
- INTERNET – Komunity nemají žádná omezení.

2.13.9 Originator-ID

Atribut *Originator-ID* patří do skupiny volitelných netranzitivních atributů. Používá se, při použití reflektorů cest, k zabránění výskytů směrovacích smyček. Atribut je vytvořen prvním RR směrovačem (reflektorem) a později není nijak měněn. *Originator-ID* je 32bitové číslo, pocházející většinou z iBGP spojení. Když obdrží RR směrovač aktualizaci obsahující jeho vlastní *Originator-ID*, tuto cestu zahodí, a zabrání tak vzniku směrovací smyčky.

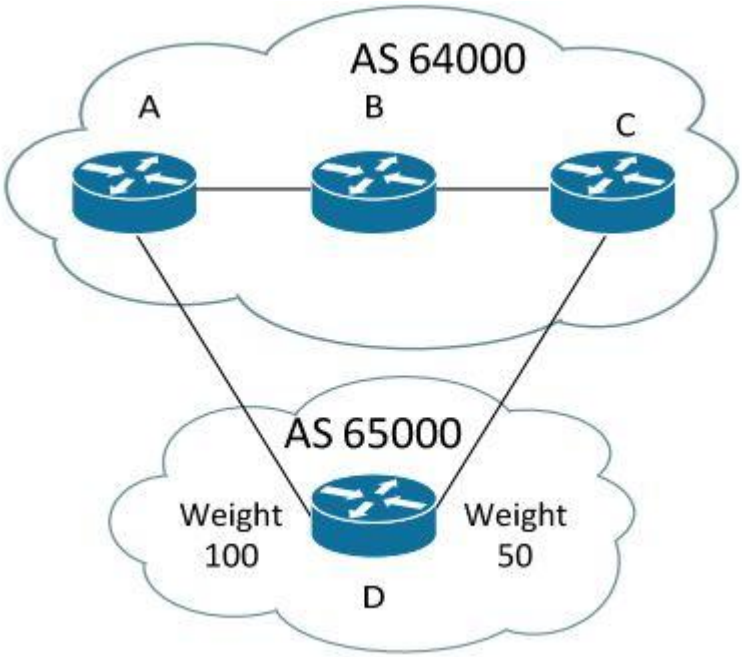
2.13.10 Cluster list

Atribut *Cluster list* patří do skupiny volitelných netranzitivních atributů. Slouží u reflektorů cest jako prevence výskytu směrovacích smyček uvnitř autonomního systému. K identifikaci konkrétních směrovačů zapojených do reflektorů cest slouží ID clusteru. *Cluster list* je seznam ID clusterů označujících clustery, které prošly aktualizací (cesta reflektorů cest). Pokud reflektor najde u předchozí cesty v *Cluster list*u svoje ID, dozví se tak, že vznikla směrovací smyčka, a takovou cestu ignoruje.

2.13.11 Weight

Atribut *Weight* je definován společností Cisco. Podobně jako umožňuje atribut *Local-preference* preferovat nějakou cestu v rámci všech směrovačů uvnitř autonomního systému, umožňuje atribut *Weight* nastavit preferenci cesty v rámci jednoho směrovače. Rozsah hodnot

atributu *Weight* je 0 až 65535. Při výběru cesty je preferována cesta s vyšší hodnotou atributu *Weight*.



Obrázek 20 Atribut WEIGHT[23]

Od směrovače D vedou ke směrovači B dvě cesty. Směrovač se na základě vyšší hodnoty atributu *Weight* u cesty vedoucí přes směrovač A rozhodne tuto cestu k přenosu použít.

2.14 Rozhodovací proces při výběru cest

Pokud má směrovač k dispozici více různých cest k nějaké síti, musí z nich do směrovací tabulky vybrat jednu. K rozhodnutí potom slouží atributy BGP cest popsané výše. Rozhodování probíhá podle jednotlivých kriterií v následujícím pořadí:

1. vyšší hodnota atributu WEIGHT
2. vyšší hodnota atributu LOCAL_PREFERENCE
3. preference cesty generované samotným routerem (pocházející z jeho autonomního systému) získaná např. redistribucí z interního směrovacího protokolu
4. kratší AS_PATH (menší počet čísel autonomních systémů v AS_PATH)
5. preferovanější hodnota atributu ORIGIN (nejpreferovanější IGP, následuje EGP a INCOMPLETE)
6. nižší hodnota atributu MED

[23] MĚŘIČEK, Tomáš. *Metodika nasazení protokolu BGP pro směrování mezi autonomními uzly*. Hradec Králové, 2012. Diplomová práce. Univerzita Hradec Králové, Fakulta informatiky a managementu, Katedra informačních technologií. str. 27

7. cesty získané z eBGP jsou preferovány před cestami z iBGP
8. next-hop dostupný přes kratší cestu vnitřkem autonomního systému
9. nižší ROUTER_ID

Kriterium s vyšším číslem se uplatní pouze v případě, kdy se podle kriteria s nižším číslem nedalo rozhodnout.

3 ZÁKLADNÍ KONFIGURACE BGP SÍTĚ

Podle [3], [7], [9], [13], [14].

3.1 Základní příkazy pro nastavení BGP

1 ***(global)*** **router bgp** *číslo-AS*

Slouží ke spuštění BGP na směrovači. Číslo-AS odpovídá číslu autonomního systému, do kterého směrovač patří. Po nastavení sousedních směrovačů určí BGP proces, zda se jedná o iBGP nebo eBGP spojení. Na jednom směrovači může běžet pouze jeden BGP proces. Ke spuštění BGP procesu je nutné tento příkaz použít v kombinaci s jedním z následujících příkazů.

2 ***(router)*** **neighbor** [*ip-adresa* | *jméno-skupiny-partnerů*] **remote-as** *číslo-AS*

(router) **neighbor** [*ip-adresa* | *jméno-skupiny-partnerů*] **description** *text*

Slouží k určení BGP sousedů a spuštění BGP procesu. Je možné definovat IP adresu BGP partnera nebo celou skupinu. Skupina se skládá z několika partnerů se stejnými atributy nebo společnou směrovací politikou. iBGP partneři se mohou nacházet v různých sítích, v takovém případě musí být dosažitelní pomocí interního směrovacího protokolu. Jednotlivé partnery je možné popsat nepovinným příkazem **description**.

3 ***(router)*** **neighbor** [*ip-adresa* | *skupina-partnerů*] **update-source** *rozhraní*

Tento příkaz není povinný. Lze jím upravit výchozí zdrojovou adresu uvedením konkrétního *rozhraní*. Při komunikaci s iBGP partnery se používá rozhraní loopbak, protože je vždy dostupné. V takovém případě je nutné dosažitelnost tohoto rozhraní ostatním iBGP partnerům zabezpečit.

4 ***(router)*** **network** *číslo-sítě* [**mask** *maska*]

Slouží k přidání sítě do seznamu sítí, které budou následně propagovány ostatním BGP směrovačům. Zadávané sítě musí být ve směrovací tabulce uvedené jako přímo připojené, statické nebo zjištěné z jiného dynamického směrovacího protokolu. Nepovinný parametr masky slouží ke sdružování do větších nebo menších celků, než jsou třídní sítě.

Alternativou je redistribuce cest z interního směrovacího protokolu.

(router) **redistribute** *protokol* [*id-procesu*] … [**route-map** *mapa*]

V případě potřeby je možné sítě do BGP redistribuovat z používaného interního směrovacího protokolu. K zajištění filtrace těchto cest se doporučuje použít směrovací mapu.

5 ***(router)*** **aggregate-address** *adresa maska* [**as-set**] [**summary-only**] [**suppress-map** *mapa*] [**advertise-map** *mapa*] [**atribute-map** *mapa*]

Tento příkaz není povinný. Slouží k agregaci cest. Pokud se ve směrovací tabulce vyskytuje nejméně jedna specifičtější cesta, generuje se zadaná agregovaná cesta. **Summary-only** zamezí výskytu specifičtějších cest. V případě, že se agregovaná cesta skládá ze specifičtějších cest z různých autonomních systémů, lze pomocí doprovodného příkazu **as-set** nastavit propagování čísla autonomních systémů, ze kterých tyto cesty pocházejí. Pomocí směrovacích map lze propagovat pouze agregované cesty (**advertise-map**), potlačit některé specifičtější cesty (**suppress-map**) nebo měnit BGP parametry (**atribute-map**).

6 ***(router)*** [**no**] **synchronisation**

Tento příkaz není povinný. Slouží k zapnutí nebo vypnutí BGP synchronizace. Dnes už se BGP synchronizace nepoužívá. Podrobněji v kapitole 2.8 na straně 29.

7 Tyto příkazy jsou nepovinné. Slouží k nastavení atributů (podrobněji v kapitole 2.13 na straně 36).

A. Váha sítě

(router) **neighbor** [*ip-adresa* | *skupina-partnerů*] **weight** *váha*

Slouží k nastavení váhy ke konkrétnímu partnerovi nebo skupině partnerů. Alternativou je

(route-map) **set weight** *váha*

sloužící k nastavení váhy pomocí směrovací mapy.

B. Místní preference

(router) **bgp default local-preference** *hodnota*

Slouží k nastavení výchozí místní preference v rámci autonomního systému. Alternativou je

(route-map) **set local-preference** *hodnota*

sloužící k nastavení místní preference pomocí směrovací mapy.

C. MED (metrika)

(router) **default-metric** *metrika*

Slouží k nastavení výchozí metriky.

Alternativou je

(route-map) **set metric** *metrika*

sloužící k nastavení metriky pomocí směrovací mapy.

8 Tyto příkazy jsou nepovinné a slouží k nastavení komunit.

A. ***(route-map)*** **set community** *komunita* [**additive**]

Slouží k nastavení komunity pomocí směrovací mapy. Vytvořením komunity dojde ke sdružení cest vybraných na základě požadavků nastavených uvnitř směrovací mapy. Hodnotu *komunita* lze zvolit v rozsahu 0 až 4 294 967 200. Jedna cesta může být ve více komunitách. Volitelný příkaz **additive** slouží k přidání nové hodnoty k již existujícímu seznamu hodnot. Možné hodnoty jsou **no-advertise** (cesta nebude propagována), **no-export** (cesta nebude propagována eBGP partnerům) a **internet** (cesta bude propagována všem partnerům.

B. ***(router)*** **neighbor** [*ip-adresa* | *skupina-partnerů*] **send-community**

Slouží k poslání a povolení předávání atributů komunit BGP partnerům.

9 Tyto příkazy jsou nepovinné a slouží k filtrování propagovaných příchozích cest pomocí komunit.

A. ***(global)*** **ip community-list** *číslo-seznamu* [**permit | deny**] *komunita*

Slouží k nastavení seznamu komunit. Počet hodnot *komunita* není omezen, oddělují se mezerou a mohou nabývat hodnoty 0 až 4 294 967 200 spolu s volně doprovodnými příkazy **no-advertise**, **no-export** a **internet**. Každý seznam komunit končí příkazem **deny all**.

B. ***(route-map)*** **match community-list** *číslo-seznamu* [**exact**]

Slouží k nastavení směrovací mapy. Číslo seznamu slouží k určení seznamu komunit a může nabývat hodnot 1 až 99. Nepovinný příkaz **exact** nařizuje přesnou shodnost se seznamem.

10 Tyto příkazy jsou nepovinné a slouží k filtraci sítí.

A. ***(router)*** **neighbor** [*ip-adresa* | *skupina-partnerů*] **prefix-list** *název-seznamu* [**in | out**]

Slouží k vytvoření seznamu prefixů, který umožňuje povolit nebo zakázat jednotlivé sítě v závislosti na délce jejich prefixu.

B. ***(global)*** **access-list** *číslo-seznamu* [**permit | deny**] [**ip**] *síť* [*filtr* | *filtr-sítě maska filtr-masky*]

Slouží k vytvoření standardního očíslovaného přístupového seznamu. *Číslo-seznamu* může nabývat hodnot 1 až 99, zvolená čísla sítí potom buď povolí, nebo zakáže. U filtrací tzv. supersítí je nutné zadat rozšířený přístupový seznam s příkazem **ip** a filtrovat síť i její masku.

C. ***(global)*** **access-list standard** *název*

(access-list) [**permit | deny**] *síť* [*filtr*]

Kombinace těchto příkazů slouží k vytvoření standardního pojmenovaného přístupového seznamu.

D. ***(router)*** **neighbor** [*ip-adresa* | *seznam-partnerů*] **distribute-list** *acl* [**in | out**]

Slouží k vytvoření distribučního seznamu. Vytvořený seznam *acl* (standardní nebo rozšířený) umožní filtraci síťových adres od nebo k zadanému partnerovi. Klíčová slova **in** a **out** určují směr filtru.

11 Tyto příkazy jsou nepovinné a slouží k filtraci příchozích a odchozích cest BGP aktualizací autonomních systémů.

A. ***(global)*** **ip as-path access-list** *číslo-seznamu-AS* [**permit | deny**] *výraz*

Slouží k vytvoření seznamu cest autonomních systémů. Pro povolení nebo zakázání BGP aktualizací podle cest pomocí regulárního výrazu lze využít několik seznamů (1 až 199).

B. ***(router)*** **neighbor** [*ip-adresa* | *seznam-partnerů*] **filter-list** *číslo-seznamu-AS* [**in | out**]

Slouží k vytvoření filtračního seznamu. Seznam pro filtrování cest autonomních systémů pomocí jejich tras slouží k filtraci aktualizací od nebo k zadanému sousednímu směrovači. Pomocí příkazu **in** nebo **out** lze zvolit v každém směru pouze jediný filtr.

12 Tyto příkazy jsou nepovinné a slouží k nastavení správy příchozích a odchozích aktualizací pomocí směrovacích map.

A. ***(global)*** **route-map** *název-mapy* [**permit | deny**] [*sekvenční-číslo*]

Slouží k vytvoření směrovací mapy skládající se z jednoho nebo více příkazů, které se vyhodnocují podle sekvenčního čísla (pokud je zadané) nebo podle pořadí. Příkaz **permit** (výchozí nastavení) slouží k použití mapy. V jedné směrovací mapě může existovat několik nepovinných příkazů **match** a **set.** V případě použití více **match** příkazů musí být, k přejití na příkazy **set,** splněny všechny jejich podmínky. Pokud se po provedení všech příkazů nenalezne žádná shoda, daná aktualizace se neodešle.

1. Nastavení **match** (podmínka shody)

   (route-map) **match as-path** *číslo-seznamu-AS*

   Slouží k porovnání jednotlivých autonomních systémů získaných ze seznamu cest autonomních systémů (11A) na cestě s číslem 1 až 199.

   (route-map) **match ip-address** *acl* [*... acl*]

Slouží k porovnání čísel sítí získaných ze seznamu prefixů (10A) nebo ze standardního očíslovaného přístupového seznamu (10B).

(route-map) **match community-list** *komunitní-seznam* [**exact**]

Slouží k porovnání čísel komunit získaných ze seznamu komunit (9).

2. Nastavení příkazu **set**

(route-map) **set as-path prepended** *cesta*

Slouží ke změně cesty pomocí autonomního systému. Pomocí příkazu *cesta* uvedením čísla AS lze ovlivnit výběr cesty.

(route-map) **set origin** [**igp | egp** *as* **| incomplete**]

Slouží ke změně původu cesty.

(route-map) **set local-preference** *hodnota*

Slouží ke změně místní preference.

(route-map) **set weight** *váha*

Slouží ke změně váhy u příchozích cest.

(route-map) **set metric** [+ | -] *metrika*

Slouží ke změně atributu MED.

B. ***(router)*** **neighbor** [*ip-adresa* | *skupina-partnerů*] **route-map** *název-mapy* [**in | out**]

Slouží k aplikaci směrovací mapy na příchozí nebo odchozí aktualizace. Směrovací mapa upraví jednotlivé aktualizace od nebo k zadanému partneru.

13 Tyto příkazy jsou nepovinné a slouží k nastavení BGP konfederace.

A. ***(router)*** **bgp confederation identifier** *autonomní-systém*

Slouží k vytvoření konfederace. Vytvořená konfederace se okolí jeví jako samostatný autonomní systém.

B. ***(router)*** **bgp confederation peers** *autonomní-systém* [*autonomní-systém*]

Slouží k přiřazení autonomního systému ke konfederaci. Sousedé v eBGP vztahu si aktualizace vyměňují podle daných pravidel.

14 Tyto příkazy jsou nepovinné a slouží k nastavení BGP reflektorů cest.

A. ***(router)*** **neighbor** *ip-adresa* **route-reflector-client**

Slouží k vytvoření reflektoru cest. Místní směrovač je nastaven jako reflektor cest přeposílající jednotlivé BGP aktualizace všem iBGP klientům. Partner směrovače se zadanou *ip-adresou* se stane klientem.

B. ***(router)*** **bgp cluster-id** [*id-klastru* | *ip-adresa*]

Slouží k přiřazení identifikátoru klastru. Na zvoleném reflektoru se nastaví 4B identifikátor klastru, který se s aktualizacemi sloužícími k detekci smyček předá ostatním reflektorům.

15 Tyto příkazy jsou nepovinné a slouží k nastavení mechanizmu dampening.

A. ***(global)*** **bgp dampening**

Slouží k vytvoření dampeningu, který se používá k omezení nestability sítě. Při výskytu destabilizace cesty do autonomního systému přiřadí směrovač cestě kumulativní penalizace. Cesta je dále propagována, ale je označena jako problémová. Při opětovné destabilizaci se proces opakuje. Překročí-li cesta *limit potlačení*, přestává se dále propagovat. Pokud dojde v době nastaveného *poločasu* ke stabilizaci, sníží se její penalizace na polovinu. Pokud klesne cena penalizace pod hodnotu *limitu použitelnosti*, dojde k opětovné propagaci cesty. Cesty s nastavenou hodnotou *limitu potlačení* jsou testovány každých 10 sekund. Potlačení propagování cest je omezeno na *maximální dobu potlačení*.

B. ***(global)*** **bgp dampening** *poločas limit-použitelnosti limit-potlačení maximum-potlačení* [**route-map** *mapa*]

Slouží k nastavení dampeningu. Jednotlivé hodnoty lze nastavit:

poločas – 1 až 45 minut (výchozí 15 minut)

limit-použitelnosti – 1 až 20 000 (výchozí 750)

limit-potlačení – 1 až 20 000 (výchozí 2 000)

maximum-potlačení – 1 až 20 000 minut (výchozí 60 minut)

3.2 Skupiny partnerů (Peer Groups)

Skupiny partnerů slouží k usnadnění BGP konfigurace. Mnoho sousedních směrovačů se řídí stejnou směrovací politikou. Nastavení stejné směrovací politiky na jednotlivých směrovačích lze usnadnit nastavením jedné směrovací politiky. Pomocí skupiny partnerů potom můžeme tuto politiku přiřadit celé skupině směrovačů. Členové skupiny partnerů tuto politiku dědí. Směrovač může být nastaven tak, aby toto nastavení pro některé skupiny partnerů přepsal. Tuto možnost lze použít pouze v případě, že nijak neovlivní odchozí aktualizace. Směrování se potom stává efektivnějším, protože nedochází ke generování jednotlivých aktualizací pro jednotlivé sousední směrovače, ale pouze ke generování jedné aktualizace, která se po obdržení směrovačem zdědí v celé jeho skupině partnerů.

(router) **neighbor** *jméno-skupiny-partnerů* **peer-group**

Slouží k vytvoření skupiny partnerů. Jméno skupiny je pouze na lokálním směrovači.

(router) **neighbor** *ip-adresa* **peer-group** *jméno-skupiny-partnerů*

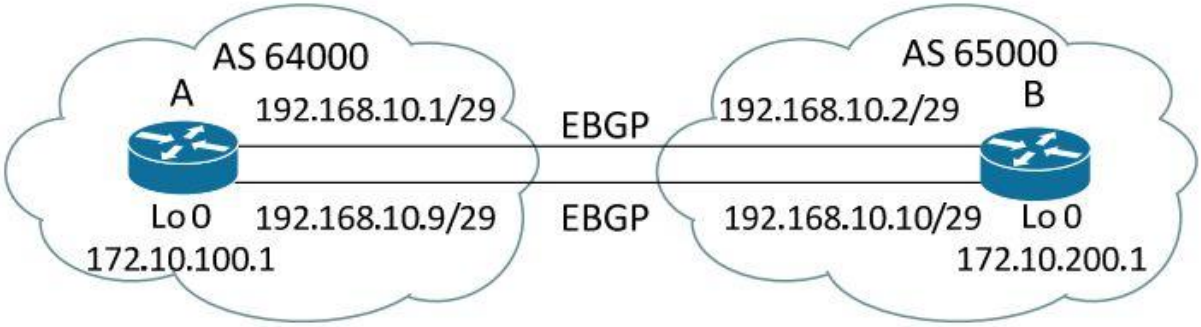
Slouží k připojení jednotlivých sousedních směrovačů k dané skupině partnerů. Směrovač může být připojený pouze k jedné skupině partnerů.

3.3 Multihop

Ve výchozím nastavení je **ebgp-multihop** vypnutý. Používá se v případě redundantních cest mezi eBGP sousedními směrovači.

(router) **neighbor** [*ip-adresa* | *skupina-partnerů*] **ebgp-multihop 2**

Při partnerství s externím sousedním směrovačem existuje pouze jedna adresa dostupná bez nutnosti provedení dalšího nastavení. Tou je adresa přímo připojeného rozhraní. Směrovací informace z interního směrovacího protokolu nejsou mezi externími partnery vyměňovány, proto musí být směrovač s jeho externím sousedem připojeni přímo. Rozhraní loopbacku není nikdy připojeno přímo. V případě použití loopbacku je proto nutné aplikovat statickou adresu směřující na fyzickou adresu přímo připojené sítě. Dále je nutné aplikovat příkaz **ebgp-multihop**, který směrovači umožní BGP spojení s externími partnery sídlícími na nepřímo připojené síti. Příkaz navýší hodnotu TTL (Time To Live) o 1, tím zvýší výchozí počet skoků pro eBGP partnery a povolí tak směrování na eBGP loopback.



Obrázek 21 eBGP-multihop[24]

RA(config)# router bgp 64000

RA(config-router)# neighbor 172.10.200.1 remote-as 65000

RA(config-router)# neighbor 172.10.200.1 update-source loopback0

RA(config-router)# neighbor 172.10.200.1 ebgp-multihop 2

RA(config)# ip route 172.10.200.1 255.255.255.255 192.168.10.2

RA(config)# ip router 172.10.200.1 255.255.255 192.168.10.10

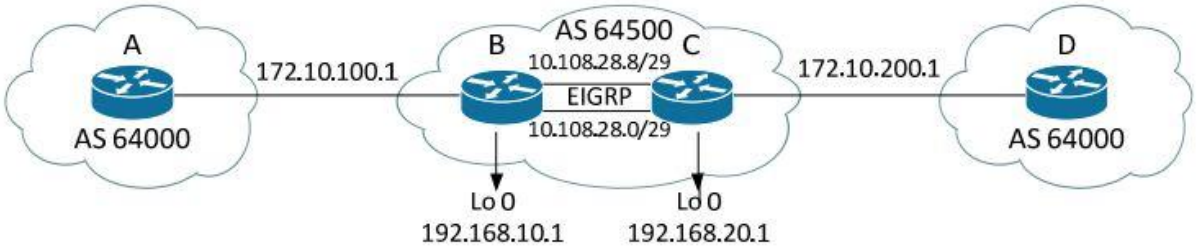
[24] MĚŘIČEK, Tomáš. *Metodika nasazení protokolu BGP pro směrování mezi autonomními uzly*. Hradec Králové, 2012. Diplomová práce. Univerzita Hradec Králové, Fakulta informatiky a managementu, Katedra informačních technologií. str. 37

Směrovač A v autonomním systému 64000 je redundantně spojen se směrovačem B v autonomním systému 65000. Směrovač A se přes loopback ukazuje směrovači B a používá jeho loopback adresu jako IP adresu pro BGP aktualizace. K navázání spojení s loopbackem je nutné použití statických cest. Příkaz **ebgp-multihop** změní chování BGP a informuje BGP o tom, že se sousední IP adresa nachází dále. V tomto případě je loopback vzdálen dva přeskoky. Jeden ke směrovači B a druhý přes směrovač B na rozhraní loopbacku.

3.4 Next-hop

(router) **neighbor** [*ip-adresa* | *skupina-partnerů*] **next-hop-self**

Pomocí tohoto příkazu můžeme, v případě redundantního spojení, směrovač donutit používat zdrojovou IP adresu aktualizace jako přeskok pro každou síť propagovanou ke zvolenému sousedovi. Výběr adresy přeskoku se potom nepřenechává protokolu BGP.



Obrázek 22 Next-hop[25]

RB(config)# router bgp 64500

RB(config-router)# neighbor 172.10.100.1 remote-as 64000

RB(config-router)# neighbor 192.168.20.1 remote-as 64500

RB(config-router)# neighbor 192.168.20.1 update-source loopback0

RB(config-router)# neighbor 192.168.20.1 next-hop-self

RB(config)# router eigrp 1

RB(config-router)# network 10.108.28.0

RB(config-router)# network 192.168.10.0

Směrovače B a C jsou redundantně spojeny. Směrovač B si tedy může vybrat, po které lince bude komunikovat. Zdrojová IP adresa proto závisí na odchozím rozhraní. Příkaz **update-source loopback** přinutí směrovač použít jako zdrojovou IP adresu pro veškeré iBGP zprávy IP adresu rozhraní loopbacku. Příkaz **neighbor next-hop-self** potom změní původní BGP přeskok. Směrovač B tedy sousednímu směrovači C propaguje jako přeskok adresu 192.168.10.1.

[25] MĚŘIČEK, Tomáš. *Metodika nasazení protokolu BGP pro směrování mezi autonomními uzly*. Hradec Králové, 2012. Diplomová práce. Univerzita Hradec Králové, Fakulta informatiky a managementu, Katedra informačních technologií. str. 38

4 REDISTRIBUCE

Podle [3], [7], [8], [10], [14], [15]. Přestože je někdy vhodné používat v celé podnikové síti stejný směrovací protokol, můžeme se v mnoha firmách setkat s kombinací několika různých směrovacích protokolů. Díky redistribuci cest může jeden nebo více směrovačů převzít cesty zjištěné z jednoho směrovacího protokolu a oznamovat je v jiném směrovacím protokolu.

Důvody použití redistribuce:

- Spojení firem s rozdílnými interními směrovacími protokoly.
- Společnost používá delší dobu několik směrovacích protokolů.
- Propojení mezi obchodními partnery.
- Propojení např. Cisco (EIGRP) směrovačů s ostatními (OSPF) směrovači.
- U mezinárodních společností používajících BGP pro interní směrování.

Problémy redistribuce:

- Možnost vzniku směrovacích smyček. – Při nesprávném nastavení redistribuce cest u více směrovačů v síti může směrovač poslat informaci o síti do autonomního systému, ze kterého tuto informaci získal jiný směrovací protokol.
- Různá metrika směrovacích protokolů. – Různé směrovací protokoly používají různou metriku pro určení nejlepší cesty. Tato informace nemůže být při redistribuci přenesena do jiného směrovacího protokolu. Výběr cest pro tyto cesty potom nemusí být optimální, a mohou tak vznikat neúplné směrovací informace o sítích.
- Různá doba konvergence směrovacích protokolů. – Různé směrovací protokoly mají odlišnou dobu nutnou pro dosažení konvergence. Jeden směrovací protokol potom může vědět o nedostupnosti sítě dříve než jiný.

Některé problémy lze vyřešit pomocí změny administrativní vzdálenosti, metriky, případně použitím filtrovacích technik.

4.1 Výběr cest

U redistribuce lze výběr nejlepší cesty do cílové sítě ovlivnit změnou administrativní vzdálenosti a metriky.

4.1.1 Administrativní vzdálenost

Administrativní vzdálenost slouží k ohodnocení důvěryhodnosti cesty pocházející z různých směrovacích protokolů. V případě existence více cest do stejného cíle se na základě

administrativní vzdálenosti směrovač rozhodne, kterému směrovacímu protokolu dá přednost. Cesta s nižší administrativní vzdáleností je důvěryhodnější.

Tabulka 4 Výchozí administrativní vzdálenosti směrovacích protokolů[26]

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

(router) **distance** *administrativní-vzdálenost* [*adresa převrácená-maska* [*standardní-přístupový-seznam*] [*rozšířený-přístupový-seznam*]]

Tento příkaz slouží ke změně administrativní vzdálenosti směrovacího protokolu. Směrovač potom na základě změněné administrativní vzdálenosti vybere cesty z jiného směrovacího protokolu.

V případě použití protokolu EIGRP se použije příkaz:

(router) **distance** *interní-vzdálenost externí-vzdálenost*

4.1.2 Metrika

Metrika slouží k určení nejlepší cesty od daného směrovacího protokolu k cílové síti. Hodnota 0 značí nekonečnou vzdálenost, taková cesta je potom nedosažitelná a není redistribuována.

[26] MĚŘIČEK, Tomáš. *Metodika nasazení protokolu BGP pro směrování mezi autonomními uzly*. Hradec Králové, 2012. Diplomová práce. Univerzita Hradec Králové, Fakulta informatiky a managementu, Katedra informačních technologií. str. 40

Tabulka 5 Výchozí metriky redistribuovaných cest[27]

Protokol	Metrika
RIP	0 (nekonečno)
IGRP /EIGRP	0 (nekonečno)
OSPF	1 pro BGP cesty 20 pro ostatní cesty
IS-IS	0 (nekonečno)
BGP	nastavena podle IGP metriky

(router) **default-metric** *hodnota*

Tento příkaz slouží k nastavení výchozí metriky pro všechny směrovací protokoly, které budou redistribuovány do protokolu, kde je tento příkaz zadán. K ovlivnění pouze jednoho směrovacího protokolu slouží parametr **metric** v příkazu **redistribute.** Metrika nastavená příkazem **redistribute** přepíše výchozí hodnotu nastavenou pomocí příkazu **default-metric.**

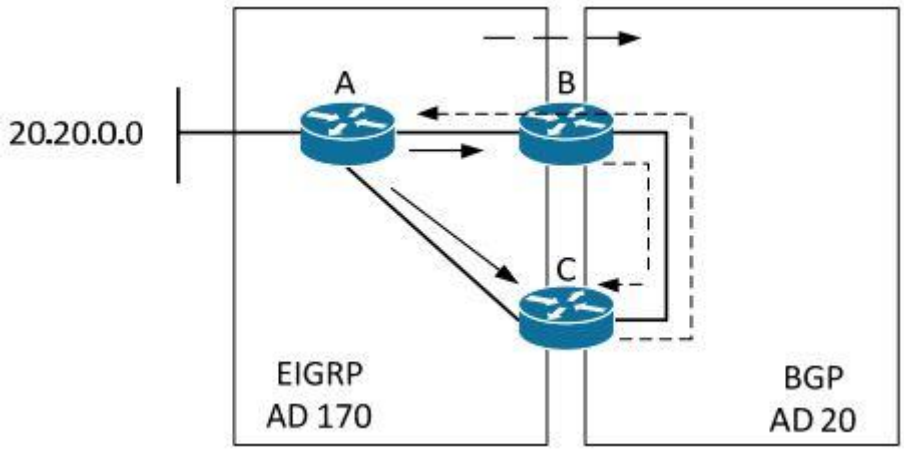
4.2 Možnosti redistribuce

Redistribuce mezi směrovacími protokoly může probíhat na jednom nebo více směrovačích a jedním nebo oběma směry.

4.2.1 Jednocestná redistribuce

Redistribuce cest je nastavena pouze na jednom směrovači (hraničním), ten redistribuuje cesty z jednoho protokolu do druhého. U jednocestné redistribuce se pro vzájemnou dostupnost zařízení v síti nastaví v opačném směru výchozí nebo statická cesta. Síť bude vždy funkční a z důvodu pouze jedné cesty mezi protokoly se v ní nevyskytnou směrovací smyčky. Může dojít k neefektivnímu výběru trasy cesty mezi směrovači.

[27] Vlastní modifikace tabulky: MĚŘIČEK, Tomáš. *Metodika nasazení protokolu BGP pro směrování mezi autonomními uzly*. Hradec Králové, 2012. Diplomová práce. Univerzita Hradec Králové, Fakulta informatiky a managementu, Katedra informačních technologií. str. 41



Obrázek 23 Jednocestná redistribuce[28]

Směrovač A propaguje směrovačům B a C externí cestu 20.2.0.0 v protokolu EIGRP s administrativní vzdáleností 170. Redistribuce cest je nastavena pouze na směrovači B. Směrovač B redistribuuje externí cestu do protokolu BGP a tu propaguje směrovači C. Směrovač C má tedy dvě cesty vedoucí ke směrovači A. Jednu s administrativní vzdáleností 170 a druhou přes směrovač B s administrativní vzdáleností 20. Místo posílaní paketů po přímo připojené lince bude směrovač C posílat pakety delší cestou.

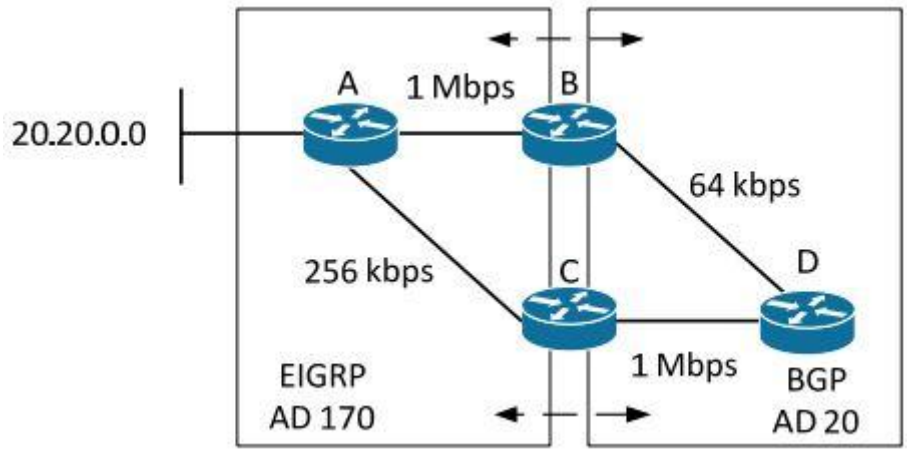
4.2.2 Vícecestná redistribuce

Redistribuce cest je nastavena na více hraničních směrovačích. V případě vícecestné redistribuce hrozí, převážně kvůli rozdílnosti metrik a administrativních vzdáleností jednotlivých směrovacích protokolů, výskyt směrovacích smyček.

Zabránění výskytu směrovacích smyček u redistribuce cest:

- Pokud je to možné, vyvarovat se vícecestné redistribuce použitím výchozích a statických cest.
- Redistribuované cesty označit a nevhodné cesty filtrovat.
- Propagovat mezi protokoly korektní hodnoty metriky.
- Změnit administrativní vzdálenost redistribuovaných cest.

[28] MĚŘIČEK, Tomáš. *Metodika nasazení protokolu BGP pro směrování mezi autonomními uzly*. Hradec Králové, 2012. Diplomová práce. Univerzita Hradec Králové, Fakulta informatiky a managementu, Katedra informačních technologií. str. 42



Obrázek 24 Vícecestná redistribuce[29]

Cena linky v protokolu EIGRP a OSPF je rozdílná a na první pohled je zřejmé, že výhodnější cesta od směrovače A ke směrovači D vede přes směrovač C. Během redistribuce je bohužel částečně ztracena velikost metriky a směrovač D posílá pakety přes směrovač B. Hrozí také výskyt směrovacích smyček.

4.3 Nastavení redistribuce

(router) **redistribuce** *protokol* [*id-procesu* | *id-oblasti*] {**level-1 | level-1-2 | level-2**}
[**match** {**internal | external** [**1 | 2**] | **nssa-external** [**1 | 2**]}]
[**metric** {*hodnota-metriky* | **transparent**}] [**metric-type** *hodnota-typu*]
[**tag** *značka-cesty*] [**route-map** *značka-mapy*] [**subnets**]

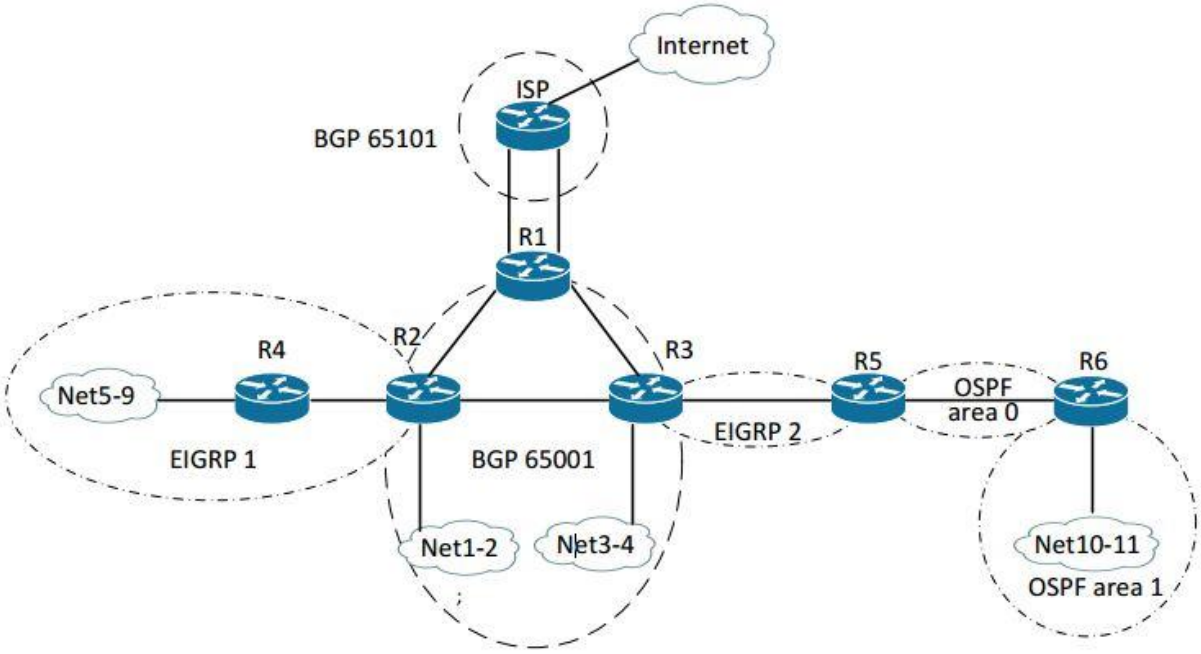
Příkaz **redistribuce** se aplikuje uvnitř zvoleného směrovacího protokolu a identifikuje směrovací *protokol*, ze kterého se redistribuce cest provede. Povinný parametr *protokol* může nabývat hodnot **bgp**, **connected**, **eigrp**, **isis**, **iso-igrp**, **mobile**, **odr**, **ospf**, **rip** a **static [***ip-adresa*]. Hodnota *id-procesu* určuje číslo autonomního systému a vyplní se pouze při redistribuci z protokolů BGP a EIGRP. Hodnota *id-oblasti* určuje oblast protokolu OSPF. Příkazem **level** se upřesňují cesty pocházející z protokolu IS-IS. Příkazy **internal**, **external** a **nssa-external** slouží k určení typu cest protokolu OSPF. Příkaz **metric** přiřadí redistribuovaným cestám velikost metriky. V případě nezadání je hodnota nastavena na hodnotu výchozí. U protokolu RIP (**transparent**) se použije metrika pro redistribuované cesty uložená ve směrovací tabulce. Parametr *hodnota-typu* označuje u protokolu OSPF typ cesty (E1 nebo E2). Příkaz **tag** se použije při redistribuci externích OSPF cest. Samotný protokol

[29] MĚŘIČEK, Tomáš. *Metodika nasazení protokolu BGP pro směrování mezi autonomními uzly*. Hradec Králové, 2012. Diplomová práce. Univerzita Hradec Králové, Fakulta informatiky a managementu, Katedra informačních technologií. str. 42

tento údaj nepoužije, ale může být použit u předávání informací mezi ASBR směrovači. Pokud není zadaná *značka-cesty*, použije se pro cesty redistribuované z BGP a EIGRP číslo autonomního systému, do kterého příslušný směrovač patří. Příkaz **route-map** umožňuje filtraci redistribuovaných cest pomocí směrovacích map. Při redistribuci do protokolu OSPF jsou zpravidla redistribuovány pouze třídní sítě. Použitím příkazu **subnets** budou do protokolu OSPF redistribuovány i cesty podsítí.

4.4 Způsoby zapojení

4.4.1 Připojení k jednomu ISP



Obrázek 25 Redistribuce – připojení k jednomu ISP[30]

Nastavení redistribuce na směrovači R2:

R2#sh run

router eigrp 1

redistribute bgp 65001 metric 64 1000 255 1 1500

network 100.100.100.20 0.0.0.3

no auto-summary

!

router bgp 65001

bgp redistribute-internal

[30] MĚŘIČEK, Tomáš. *Metodika nasazení protokolu BGP pro směrování mezi autonomními uzly*. Hradec Králové, 2012. Diplomová práce. Univerzita Hradec Králové, Fakulta informatiky a managementu, Katedra informačních technologií. str. 46

network 140.140.0.0 mask 255.255.255.128
network 140.140.0.128 mask 255.255.255.128
aggregate-address 140.140.0.0 255.255.255.0 summary-only
redistribute eigrp 1
neighbor 100.100.100.9 remote-as 65001
neighbor 100.100.100.14 remote-as 65001
no auto-summary

Nastavení redistribuce na směrovači R3:
R3#sh run
router eigrp 2
redistribute bgp 65001 metric 64 100 255 1 1500
network 100.100.100.24 0.0.0.3
no auto-summary
!
router bgp 65001
bgp redistribute-internal
network 160.160.0.0 mask 255.255.255.192
network 160.160.0.64 mask 255.255.255.192
aggregate-address 160.160.0.0 255.255.255.128 summary-only
redistribute eigrp 2
neighbor 100.100.100.13 remote-as 65001
neighbor 100.100.100.17 remote-as 65001
no auto-summary

Nastavení redistribuce na směrovači R5:
R5#sh run
router eigrp 2
redistribute ospf 1 metric 64 100 255 1 1500
network 100.100.100.24 0.0.0.3
no auto-summary
!
router ospf 1
redistribute eigrp 2 subnets

network 100.100.100.28 0.0.0.3 area 0

default-information originate

Výpis směrovací tabulky směrovače R5:

R5#sh ip route

Gateway of last resort is 100.100.100.25 to network 0.0.0.0

100.0.0.0/30 is subnetted, 3 subnets

D EX 100.100.100.20 [170/40537600] via 100.100.100.25, 00:03:26, Serial0/0

C 100.100.100.28 is directly connected, Serial0/1

C 100.100.100.24 is directly connected, Serial0/0

140.140.0.0/24 is subnetted, 1 subnets

D EX 140.140.0.0 [170/40537600] via 100.100.100.25, 00:03:26, Serial0/0

160.160.0.0/16 is variably subnetted, 3 subnets, 2 masks

D EX 160.160.0.0/26 [170/40537600] via 100.100.100.25, 00:03:34, Serial0/0

D EX 160.160.0.0/25 [170/40537600] via 100.100.100.25, 00:03:41, Serial0/0

D EX 160.160.0.64/26 [170/40537600] via 100.100.100.25, 00:03:41, Serial0/0

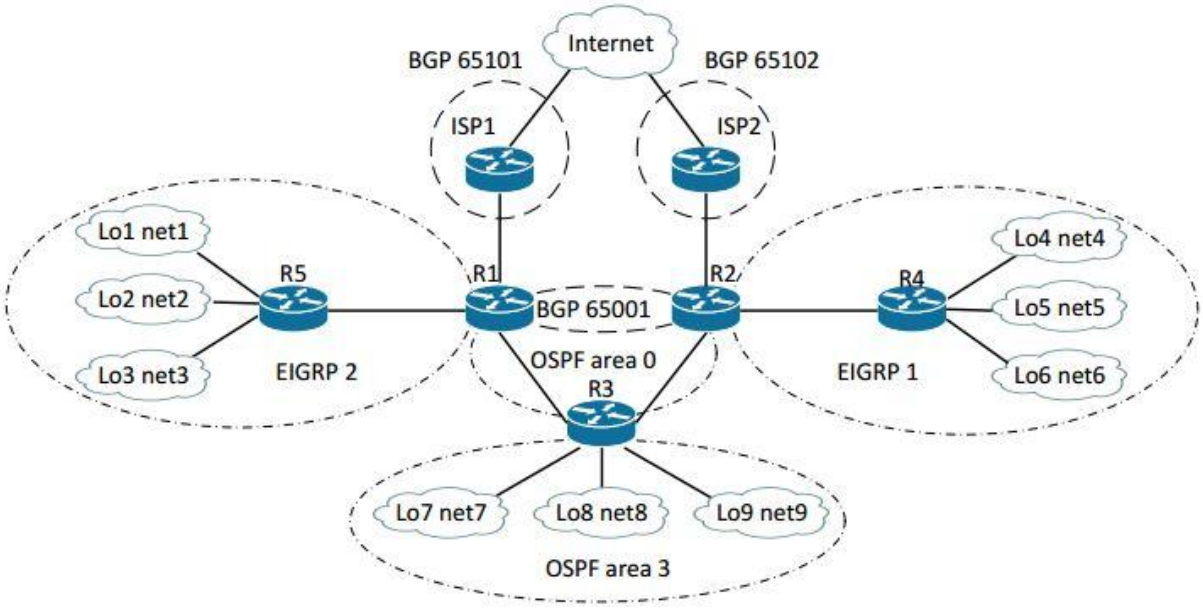
180.180.0.0/23 is subnetted, 1 subnets

O IA 180.180.0.0 [110/65] via 100.100.100.30, 00:05:43, Serial0/1

D*EX 0.0.0.0/0 [170/40537600] via 100.100.100.25, 00:02:12, Serial0/0

D EX 200.200.0.0/23 [170/40537600] via 100.100.100.25, 00:03:45, Serial0/0

4.4.2 Připojení ke dvěma ISP



Obrázek 26 Redistribuce – připojení ke dvěma ISP[31]

Nastavení redistribuce na směrovači R1:

R1#sh run

router eigrp 2

redistribute ospf 1 metric 64 100 255 1 1500

network 100.100.100.16 0.0.0.3

no auto-summary

!

router ospf 1

redistribute eigrp 2 subnets

redistribute bgp 65001 subnets

network 100.100.100.8 0.0.0.3 area 0

default-information originate

!

router bgp 65001

network 100.100.100.0 mask 255.255.255.252

redistribute eigrp 2

redistribute ospf 1

---

[31] MĚŘIČEK, Tomáš. *Metodika nasazení protokolu BGP pro směrování mezi autonomními uzly*. Hradec Králové, 2012. Diplomová práce. Univerzita Hradec Králové, Fakulta informatiky a managementu, Katedra informačních technologií. str. 44

neighbor 100.100.100.1 remote-as 65101
neighbor 100.100.100.1 route-map PRI-ISP-IN in
neighbor 100.100.100.1 route-map PRI-ISP-MED-OUT out
neighbor 100.100.100.13 remote-as 65001
neighbor 100.100.100.13 next-hop-self
no auto-summary

Nastavení redistribuce na směrovači R2:
R2#sh run
router eigrp 1
redistribute ospf 1 metric 64 100 255 1 1500
network 100.100.100.20 0.0.0.3
no auto-summary
!
router ospf 1
redistribute eigrp 1 subnets
redistribute bgp 65001 subnets
network 100.100.100.12 0.0.0.3 area 0
default-information originate
!
router bgp 65001
network 100.100.100.4 mask 255.255.255.252
redistribute eigrp 1
redistribute ospf 1
neighbor 100.100.100.5 remote-as 65102
neighbor 100.100.100.5 route-map SEC-ISP-IN in
neighbor 100.100.100.5 route-map SEC-ISP-MED-OUT out
neighbor 100.100.100.9 remote-as 65001
neighbor 100.100.100.9 next-hop-self
no auto-summary

Výpis směrovací tabulky směrovače R3:
R3#sh ip route
Gateway of last resort is 100.100.100.9 to network 0.0.0.0

100.0.0.0/30 is subnetted, 6 subnets

O E2 100.100.100.4 [110/1] via 100.100.100.13, 00:01:34, Serial0/1

O E2 100.100.100.0 [110/1] via 100.100.100.9, 00:01:34, Serial0/0

C 100.100.100.12 is directly connected, Serial0/1

C 100.100.100.8 is directly connected, Serial0/0

O E2 100.100.100.20 [110/20] via 100.100.100.13, 00:01:39, Serial0/1

O E2 100.100.100.16 [110/20] via 100.100.100.9, 00:01:39, Serial0/0

192.40.0.0/24 is variably subnetted, 4 subnets, 3 masks

C 192.40.0.64/28 is directly connected, Loopback1

C 192.40.0.32/27 is directly connected, Loopback3

C 192.40.0.0/27 is directly connected, Loopback2

O 192.40.0.0/25 is a summary, 00:01:50, Null0

O E2 192.50.0.0/24 [110/20] via 100.100.100.9, 00:01:40, Serial0/0

O E2 192.60.0.0/24 [110/20] via 100.100.100.13, 00:01:42, Serial0/1

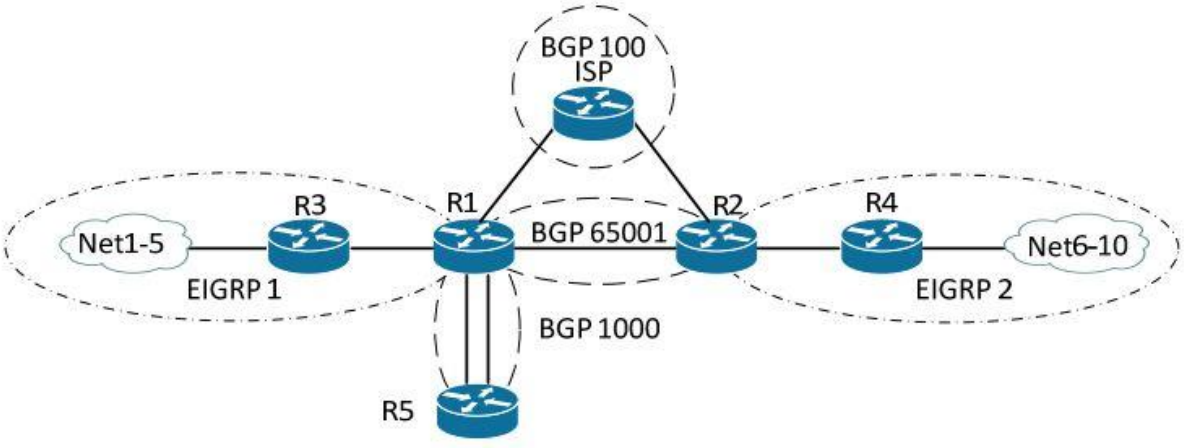
O*E2 0.0.0.0/0 [110/1] via 100.100.100.9, 00:01:42, Serial0/0

5 VÝBĚR CEST

Podle [2], [3], [7], [10], [13], [14]. Výběr příchozích a odchozích cest z protokolu BGP v autonomním systému lze ovlivnit několika různými způsoby:

- změnou velikosti cesty
- místním upřednostněním cest
- změnou parametru MED (metriky)
- cestou v autonomním systému (AS-path)

Zatímco interní směrovací protokoly upřednostňují nejrychlejší možnou cestu, BGP upřednostňuje cestu stálejší.



Obrázek 27 Výběr cest – místní preference, metrika, váha cesty[32]

Nastavení směrovače R1:

R1#sh run

router bgp 65001

redistribute eigrp 1

neighbor 100.100.100.1 remote-as 100

neighbor 100.100.100.1 route-map PRIMARY-ISP-IN in

neighbor 100.100.100.1 route-map PRIMARY-ISP-MED-OUT out

neighbor 100.100.100.10 remote-as 65001

neighbor 100.100.100.22 remote-as 1000

neighbor 100.100.100.22 route-map WEIGHT-FA0/0 in

neighbor 100.100.100.26 remote-as 1000

[32] MĚŘIČEK, Tomáš. *Metodika nasazení protokolu BGP pro směrování mezi autonomními uzly*. Hradec Králové, 2012. Diplomová práce. Univerzita Hradec Králové, Fakulta informatiky a managementu, Katedra informačních technologií. str. 48

neighbor 100.100.100.26 route-map WEIGHT-FA0/1 in
no auto-summary
!
route-map PRIMARY-ISP-IN permit 10
set local-preference 150
!
route-map PRIMARY-ISP-MED-OUT permit 10
set metric 50
!
route-map WEIGHT-FA0/1 permit 10
set weight 75
!
route-map WEIGHT-FA0/0 permit 10
set weight 150

Nastavení směrovače R2:
R2#sh run
router bgp 65001
redistribute eigrp 2
neighbor 100.100.100.5 remote-as 100
neighbor 100.100.100.5 route-map SECONDARY-ISP-IN in
neighbor 100.100.100.5 route-map SECONDARY-ISP-MED-OUT out
neighbor 100.100.100.9 remote-as 65001
no auto-summary
!
route-map SECONDARY-ISP-IN permit 10
set local-preference 100
!
route-map SECONDARY-ISP-MED-OUT permit 10
set metric 75

5.1 Změna místní preference

Hodnotu atributu *local-preference* si iBGP směrovače v rámci jednoho autonomního systému mezi sebou vyměňují a určí podle ní preferovanou výstupní cestu z autonomního systému.

Pokud se BGP směrovač nachází v jiném autonomním systému, tento atribut od svého souseda nepřijme. Výchozí hodnota atributu je 100. V případě existence více výchozích cest z autonomního systému se upřednostňuje cesta s vyšší hodnotou *local-preference*. Změna místní preference může zásadně ovlivnit výběr cesty z jednoho autonomního systému do druhého. V případě chybného nastavení může dojít k přetížení linkového spojení, zatímco zbylé cesty zůstanou nevyužité.

5.1.1 Nastavení místní preference

K nastavení místní preference se doporučuje použít směrovací mapy, ve kterých se upřednostní jedna cesta nad druhou.

(router) **neighbor** [*ip-adresa*] **route-map** *název-mapy* **in**

Klíčové slovo **in** je povinné pro aktualizace pocházející z eBGP spojení

Uvnitř směrovací mapy se použije příkaz **set local-preference** *hodnota*. Parametr *hodnota* je v rozsahu 1 až 4 294 967 295.

(router) **default local-preference** *hodnota*

Příkaz nastaví výchozí hodnotu *local-preference*, a tím preferenci všech nových cest v autonomním systému.

Výpis BGP tabulky směrovače R1:

R1#sh ip bgp

	Network	*Next Hop*	*Metric*	*LocPrf*	*Weight*	*Path*
*	*i 0.0.0.0*	*100.100.100.5*	*0*	*100*	*0*	*100 i*
***>**		***100.100.100.1***	***0***	***150***	***0***	***100 i***
*	*i 100.100.100.0/30*	*100.100.100.5*	*0*	*100*	*0*	*100 i*
***>**		***100.100.100.1***	***0***	***150***	***0***	***100 i***
*	*i 100.100.100.4/30*	*100.100.100.5*	*0*	*100*	*0*	*100 i*
***>**		***100.100.100.1***	***0***	***150***	***0***	***100 i***
*>	*100.100.100.12/30*	*0.0.0.0 0*			*32768*	*?*
*>	*i 100.100.100.16/30*	*100.100.100.10*	*0*	*100*	*0*	*?*
*>	*140.140.0.0/22*	*100.100.100.14*	*2297856*		*32768*	*?*
*	*150.150.0.0/24*	*100.100.100.26*	*0*		*75*	*1000 i*
*>		*100.100.100.22*	*0*		*150*	*1000 i*
*>	*i 180.180.0.0/23*	*100.100.100.18*	*2297856*	*100*	*0*	*?*

5.2 Změna metriky cesty

Změna atributu *MED* (metriky) umožňuje směrovači jednoho autonomního systému ovlivnit výběr cesty směrovače v jiném autonomním systému. Atribut je vhodné použít v případě několika přímo připojených cest mezi různými autonomními systémy. Nevýhodou metriky je, že se nemusí projevit na provozu sítě, protože se při výběru cest vyhodnocuje až po atributech váhy, místní preference, AS cesty a původu cesty. V případě chybného nastavení metriky může dojít, stejně jako u atributu *local-preference*, k přetížení spojení, zatímco zbylé cesty zůstanou nevyužité.

5.2.1 Nastavení metriky cesty

Metrika cesty se nastavuje pomocí směrovací mapy.

(router) **neighbor** [*ip-adresa*] **route-map** *název-mapy* **out**

V případě metriky se u směrovací mapy používá klíčové slovo **out.**

Uvnitř směrovací mapy se použije příkaz **set metric** *hodnota*. Parametr *hodnota* je v rozsahu 1 až 4 294 967 295.

(router) **default-metric** *hodnota*

Příkaz nastaví výchozí hodnotu metriky cesty. V případě již nastavené metriky konkrétní cesty je tato hodnota přepsána. Hodnota metriky se využije pouze u přímo připojených spojení s rozdílnými autonomními systémy.

V případě nezadání atributu *MED* je cesta ohodnocena metrikou 0, a je tak nejvýhodnější. Toto výchozí chování lze změnit pomocí příkazu **bgp bestpath med missing-as-worst** uvnitř BGP procesu. Cesta s nenastavenou hodnotou je potom ohodnocena metrikou 4 294 967 295 a je nejméně výhodná.

Výpis BGP tabulky směrovače ISP:

ISP#sh ip bgp

	Network	*Next Hop*	*Metric*	*LocPrf*	*Weight*	*Path*
*>	*0.0.0.0*	*0.0.0.0*	*0*		*32768*	*i*
*>	*100.100.100.0/30*	*0.0.0.0*	*0*		*32768*	*i*
*>	*100.100.100.4/30*	*0.0.0.0*	*0*		*32768*	*i*
*	*100.100.100.12/30*	*100.100.100.6*	*75*		*0*	*65001 ?*
***>**		***100.100.100.2***	***50***		***0***	***65001 ?***
***>**	***100.100.100.16/30***	***100.100.100.2***	***50***		***0***	***65001 ?***
*		*100.100.100.6*	*75*		*0*	*65001 ?*
*	*140.140.0.0/22*	*100.100.100.6*	*75*		*0*	*65001 ?*

***>**		***100.100.100.2***	***50***		***0***	***65001 ?***
***>**	***150.150.0.0/24***	***100.100.100.2***	***50***		***0***	***0 65001 1000 i***
***>**	***180.180.0.0/23***	***100.100.100.2***	***50***		***0***	***65001 ?***
*		*100.100.100.6*	*75*		*0*	*65001 ?*

5.3 Změna váhy cesty

Atribut *Weight* lze využít pouze u směrovačů od společnosti Cisco. Atribut ovlivňuje váhu konkrétní odchozí cesty. Atribut lze na konkrétní cestu na Cisco směrovači nastavit při přijetí BGP aktualizace, nebo na všechny cesty od jednoho sousedního směrovače pomocí směrovací mapy. Algoritmus pro určení nejlepší cesty potom upřednostní cestu s vyšší hodnotou váhy. Atribut ovlivňuje pouze směrovač, na kterém byl nastaven, na sousední směrovače nemá žádný vliv. Před použitím atributu *Weight* musí směrovač zkontrolovat příchozí aktualizace. Atribut nemůže být předáván aktualizacemi mezi směrovači, protože zprávy protokolu BGP neosahují pole pro uložení této hodnoty.

5.3.1 Nastavení váhy cesty

(router) **neighbor** [*ip-adresa*] **route-map** *název-mapy* **in**

Příkaz pro nastavení váhy cesty pomocí směrovací mapy. Po zadání příkazu směrovač aplikuje směrovací mapu na všechny aktualizační BGP zprávy od zvoleného sousedního směrovače. Použije se klíčové slovo **in**, protože se jedná o atribut ovlivňující odchozí cesty. Uvnitř směrovací mapy se potom použije příkaz **set weight** *váha*.

(router)**neighbor** [*ip-adresa* | *skupina-partnerů*] **weight** [*váha*]

Příkaz ovlivní všechny cesty pocházející od zvoleného sousedního směrovače. Není použito klíčové slovo **in** ani **out**, protože váha cesty může být nastavena pouze na vstupu.

Výpis BGP tabulky směrovače R5:

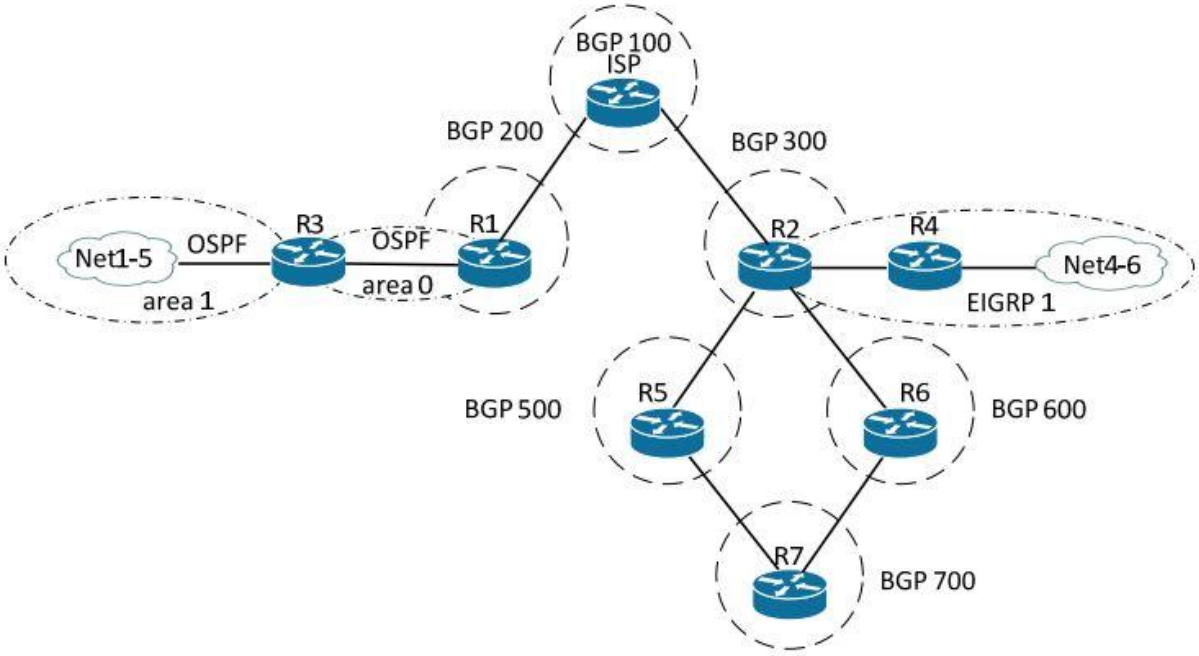
R5#sh ip bgp

	Network	*Next Hop*	*Metric*	*LocPrf*	*Weight*	*Path*
*	*0.0.0.0*	*100.100.100.25*			*75*	*65001 100 i*
***>**		***100.100.100.21***			***150***	***65001 100 i***
*	*100.100.100.0/30*	*100.100.100.25*			*75*	*65001 100 i*
***>**		***100.100.100.21***			***150***	***65001 100 i***
*	*100.100.100.4/30*	*100.100.100.25*			*75*	*65001 100 i*
***>**		***100.100.100.21***			***150***	***65001 100 i***
*	*100.100.100.12/30*	*100.100.100.25*	*0*		*75*	*65001 ?*
***>**		***100.100.100.21***	***0***		***150***	***65001 ?***

*	*100.100.100.16/30*	*100.100.100.25*		*75*	*65001 ?*
***>**		***100.100.100.21***		***150***	***65001 ?***
*	*140.140.0.0/22*	*100.100.100.25*	*2297856*	*75*	*65001 ?*
***>**		***100.100.100.21***	***2297856***	***150***	***65001 ?***
*>	*150.150.0.0/24*	*0.0.0.0*	*0*	*32768*	*i*
*	*180.180.0.0/23*	*100.100.100.25*		*75*	*65001 ?*
***>**		***100.100.100.21***		***150***	***65001 ?***

5.4 Změna AS cesty

Atribut *AS-Path* nese informaci o autonomních systémech, přes které cesta vede. Výběr nejlepší cesty lze pomocí něj ovlivnit přidáním několika autonomních systémů do cesty nebo provedením filtrace podle jejich původu a jejich pozdějších úprav.



Obrázek 28 Výběr cest – AS-Path[33]

5.4.1 Změna AS cesty přidáním čísla AS

Změna cesty pomocí atributu AS-Path spočívá v přidání čísla autonomního systému, které už v cestě je. Tím se cesta mezi eBGP směrovači prodlouží.

(router) **neighbor** [*ip-adresa*] **route-map** *název-mapy* **in**

Cisco IOS umožňuje u eBGP spojení přidávat příchozí i odchozí cesty pomocí směrovací

[33] MĚŘIČEK, Tomáš. *Metodika nasazení protokolu BGP pro směrování mezi autonomními uzly*. Hradec Králové, 2012. Diplomová práce. Univerzita Hradec Králové, Fakulta informatiky a managementu, Katedra informačních technologií. str. 53

mapy. V rámci iBGP spojení přidání AS nefunguje. Uvnitř směrovací mapy se potom použije příkaz **set as-path prebend** [*číslo*-AS] [*číslo*-AS] [...] a několik totožných AS. Zpravidla se přidává číslo autonomního systému, ve kterém se nastavovaný směrovač nachází. Při výběru cesty je potom upřednostněna cesta s nižším počtem přeskoků. Při nesprávném použití, např. vložením čísla AS, který se na dané cestě nenachází, může dojít ke zkolabování dané sítě.

Nastavení AS cesty na směrovači R5:

R5#sh run
router bgp 500
neighbor 100.100.100.17 remote-as 300
neighbor 100.100.100.17 route-map AS-PATH-PREPEND out
neighbor 100.100.100.26 remote-as 700
neighbor 100.100.100.26 route-map AS-PATH-PREPEND out
no auto-summary
!
route-map AS-PATH-PREPEND permit 10
set as-path prepend 500 500

Výpis BGP tabulky směrovače R2:

R2#sh ip bgp

	Network	*Next Hop*	*Metric*	*LocPrf*	*Weight*	*Path*
*>	*0.0.0.0*	*100.100.100.5*	*0*		*0*	*100 i*
*>	*100.100.100.12/30*	*0.0.0.0*	*0*		*32768*	*?*
*>	*120.110.100.0/24*	*100.100.100.22*			*0*	*600 700 i*
*****		***100.100.100.18***			***0***	***500 500 500 700 i***
*>	*220.220.0.0/23*	*100.100.100.14*	*2297856*		*32768*	*?*

5.4.2 Změna AS cesty pomocí filtrace

Pomocí regulárního výrazu se u vybraného spojení s BGP partnerem v požadovaném směru vybere konkrétní cesta, která se na základě atributu AS-Path odfiltruje.

(router) **ip as-path access-list** [*číslo-acl*] [**permit | deny**] [*regulární-výraz*]

(router) **neighbor** [*ip-adresa*] **filter-list** *číslo-acl* [**in | out**]

Chybné nastavení může způsobit nedoručení požadovaných BGP aktualizací nebo výskyt černých děr (data po cestě zmizí) a tím výpadek v síti.

Tabulka 6 Výběr cest – regulární výrazy pro filtraci[34]

Regulární výraz	Význam
^$	Všechny místní cesty
.*	Všechny cesty
^100$	Cesty začínající a končící v AS 100
_100$	Cesty pocházející z AS 100
^100_	Cesty přijaté z AS 100
_100_	Cesty procházející AS 100

Nastavení směrovače ISP:

ISP#sh run

router bgp 100

network 0.0.0.0

neighbor 100.100.100.2 remote-as 200

neighbor 100.100.100.6 remote-as 300

neighbor 100.100.100.6 filter-list 1 out

no auto-summary

!

ip as-path access-list 1 deny ^200$

*ip as-path access-list 1 permit .**

Směrovač ISP je nastaven tak, aby směrovač R2 neinformoval o žádné síti směrovače R1.

Ke kontrole nastavení filtrace slouží příkaz **sh ip bgp regexp** [*regulární-výraz*].

ISP#sh ip bgp regexp ^200$

	Network	*Next Hop*	*Metric*	*LocPrf*	*Weight*	*Path*
*>	*100.100.100.8/30*	*100.100.100.2*	*0*		*0*	*200 ?*
*>	*210.210.0.0*	*100.100.100.2*	*65*		*0*	*200 ?*

[34] HOONG, Yap Chin. *CCNP ROUTE Complete Guide*. 1st Edition. United States of America: CreateSpace Independent Publishing Platform, 2010. ISBN 1453807667. str. 240

6 FILTROVÁNÍ BGP AKTUALIZACÍ

Podle [3], [8]. BGP směrovače mohou přijímat velké množství směrovacích aktualizací. Toto množství je kvůli optimalizaci protokolu potřeba rozumně omezit pomocí metod pro jejich filtraci. K filtraci aktualizací lze použít prefix listy, směrovací mapy a distribuční seznamy.

6.1 Směrovací mapy

Směrovací mapy lze využít v následujících případech:

- Redistribuce – Při použití redistribuce z jednoho protokolu do druhého je téměř vždy nutné využít filtrování cest pomocí směrovacích map. Oproti distribučním seznamům přinášejí směrovací mapy výhodu v podobě možnosti použití příkazu **set** k upravení konkrétních cest.
- Výběr cest – Směrovací mapy umožňují vybrat konkrétní zdrojovou a cílovou IP adresu, směrovací protokol i uživatelskou aplikaci. Výběr trasy k cílové adrese lze, v případě shody cesty s nastavenými požadavky, upravit.
- Překlad síťových adres (NAT) – Směrovací mapy umožňují jednodušší kontrolu překládaných adres.
- BGP – Směrovací mapy slouží k filtrování jednotlivých příchozích a odchozích BGP cest a k manipulaci s jednotlivými atributy cest.

6.1.1 Nastavení směrovacích map

Ve směrovací mapě se může vyskytovat jeden nebo více příkazů **route-map** se stejným názvem mapy. Jednotlivé příkazy se vykonávají podle nastaveného pořadí a jejich logika je podobná konstrukci if – else z programovacích jazyků. Příkaz **route-map** je možné doplnit příkazem **match** sloužícím k identifikaci konkrétní cesty a několika příkazy **set** sloužícími ke změně parametrů dané cesty. Jednotlivé příkazy **route-map** musí zvolenou akci buď povolit (**permit**) nebo zamítnout (**deny**). U redistribuce se, v případě nalezení shody u konkrétní cesty v příkazu **route-map**, následující zpracování téže cesty zastaví. Cesta bude redistribuována při zadání parametru **permit**, jinak k redistribuci nedojde. Na konci příkazu **route-map** je zamítací pravidlo **deny any**, které zbylé cesty zakáže. Pokud se v příkazu **route-map** s parametrem **permit** příkaz **match** nevyskytne, budou zbývající cesty povoleny.

(router) **route-map** *název-mapy* [**permit | deny**] [*pořadové-číslo*]

A. Příkaz **match**

Slouží k identifikaci konkrétní cesty. Cestu lze potom porovnat pomocí:

1. IP adresy

match ip address [*...číslo-acl* | *název*] | **prefix-list** *jméno-prefixu* [*jméno-prefixu*]

Porovnává všechny cesty s číslem sítě ve standardním nebo rozšířeném přístupovém seznamu nebo prefix seznamu. Je možné kombinovat více seznamů najednou. V případě shody s alespoň jedním seznamem znamená shodu celé cesty.

2. Délky paketu

   match length *min max*

   Shoda na základě délky paketu 3. vrstvy.

3. Rozhraní

   match interface *typ číslo*

   Pro cesty s přeskokem přes dané rozhraní.

4. Přeskoku

   match ip next-hop [*...číslo-acl* | *název*]

   Pro jakékoliv cesty s nastavenou IP adresou přeskoku.

5. Cílové IP adresy

   match ip route-source [*...číslo-acl* | *název*]

   Pro cesty se zdrojovou IP adresou směrovače nebo serveru.

6. Metriky cesty

   match metric *metrika*

   Pro cesty, které mají nastavenou danou hodnotu metriky.

7. Typu cesty

   match route-type [**external | internal | level-1 | level-2 | local**]

   Pro konkrétní typ cesty.

8. Komunity

   match community [*číslo-komunity* | *název*]

   Pro cesty se stejnou komunitou.

9. Znaku

   match tag *znak*

   Pro cesty se stejnou hodnotou znaku.

B. Příkaz **set**

Slouží k nastavení parametrů konkrétní cesty. Nastavitelné parametry jsou:

1. Metrika

   set metric *metrika*

   Pro nastavení metriky cesty.

2. Typ metriky

   set metric-type [**external | internal | type-1 | type-2**]

Pro nastavení typu metriky cílového směrovacího protokolu.

3. Výchozí rozhraní

   set default interface *typ číslo*

   Pro nastavení výchozího rozhraní sloužícího paketům, které prošly směrovací mapou a nemají nastavenou trasu cesty.

4. Rozhraní

   set interface *typ*

   Pro nastavení rozhraní cest, které prošly směrovací mapou.

5. Výchozí IP přeskok

   set ip default next-hop *ip-adresa*

   Pro nastavení výchozího přeskoků paketů, které prošly směrovací mapou a nemají nastavenou trasu cesty.

6. Ověření výchozího IP přeskoku

   set ip default next-hop verify-availability

   Pro zamezení výskytu černé díry v případě nedostupnosti přeskoku.

7. IP adresa přeskoku

   set ip next-hop *ip-adresa*

   Pro nastavení přeskoku cest, které prošly směrovací mapou.

8. Ověření IP adresy přeskoku

   set ip next-hop verify-available

   Pro zjištění dostupnosti přeskoku.

9. VRF (Virtual Routing and Forwarding)

   set ip vrf

   Pro určení kam poslat paket, který prošel směrovací mapou, když je přeskok pojmenován VRF.

10. Přeskok

    set next-hop

    Pro určení přeskoku cesty.

11. Typ oblasti

    set level [**level-1 | level-2 | stub-area | backbone**]

    Pro nastavení typu oblasti (area) sloužící k importování cest (platí pro cesty OSPF a IS-IS).

12. AS cesta

    set as-path [**tag | prebend** *znak-as-cesty*]

Pro změnu cesty přes autonomní systémy (u BGP).

13. Automatická značka

    set automatic-tag

    Pro nastavení automatického značkování cest.

14. Komunita

    set community {*číslo-komunity* [**additive**] [*známá-komunita*] | **none**}

    Pro nastavení atributu komunity (u BGP).

15. Místní preference

    set local-preference *atribut-bgp*

    Pro nastavení místní preference (u BGP).

16. Váha

    set weight *bgp-váha*

    Pro nastavení váhy cesty (u BGP).

17. Původ

    set origin *kód-bgp původu*

    Pro nastavení původu cesty (u BGP).

18. Znak

    set tag

    Pro nastavení znaku cesty cílového směrovacího protokolu.

6.2 Distribuční seznamy

Distribuční seznamy rozvíjejí možnosti seznamů přístupových (access listů). Přístupové seznamy je možné aplikovat jen na jedno rozhraní, směrovače ale většinou využívají rozhraní více, v takovém případě jsou přístupové seznamy neefektivní. Přístupové seznamy zároveň nijak neovlivňují odchozí provoz v síti, nemají tedy vliv na odchozí aktualizace. Naproti tomu distribuční seznamy se aplikují uvnitř samotného směrovacího protokolu. Umožňují tedy ovlivnit veškeré směrovací aktualizace. Pomocí přístupového seznamu se vybere konkrétní síť a pomocí distribučního seznamu směrovač přístupový seznam aplikuje do směrovacího protokolu. Distribuční seznamy umožňují filtrování směrovacích aktualizací podle příchozích a odchozích rozhraní nebo redistribuce z jiného směrovacího protokolu.

Postup při filtrování směrovacích aktualizací pomocí distribučního seznamu:

1. Směrovač obdrží aktualizaci nebo se připraví na odeslání aktualizace o jedné nebo více sítích.

2. Směrovač vybere rozhraní, na které dorazila příchozí aktualizace, nebo z něhož by měla být aktualizace odeslána.
3. Směrovač určí, jestli je filtr (distribuční seznam) určen pro zvolené rozhraní.
4. Pokud filtr není pro dané rozhraní určen – paket se odešle běžným způsobem.
5. Pokud je filtr určen pro dané rozhraní – směrovač zkontroluje shodu u všech přístupových seznamů nacházejících se v distribučním seznamu pro směrovací aktualizace.
6. V případě shody cesty s přístupovým seznamem se daná cesta buď povolí, nebo zakáže.
7. Při nenalezení shody v přístupovém seznamu jsou zbylé cesty zahozeny.

6.2.1 Nastavení distribučních seznamů

(router) **distribute-list** [*číslo-acl* | *jméno*] **out** [[*jméno-rozhraní směrovací-proces*] | [*směrovací-proces parametr*]]

Příkaz slouží k aplikaci distribučního seznamu do konkrétního směrovacího protokolu. *Číslo-acl* určuje číslo standardního seznamu, *jméno* jeho název. K použití přístupového seznamu na odchozí spojení je nutné zadat příkaz **out**, volitelnými příkazy je potom možné zvolit jméno výchozího rozhraní, na kterém bude filtrace provedena. Dále je možné zadat název směrovacího procesu nebo parametr *static* | *connected*, od kterého budou aktualizace filtrovány a bude redistribuovaný, případně upřesnit *parametr* v podobě čísla autonomního systému nebo směrovacího procesu.

(router) **distribute-list** [*číslo-acl* | *jméno*] | [**route-map** | *znak-mapy*] **in**
[*typ-rozhraní číslo-rozhraní*]

Slouží k použití přístupového seznamu na příchozí rozhraní (**in**). Je možné jej doplnit nepovinnými parametry *znak-mapy* a *typ-rozhraní*. *Znak-mapy* slouží u protokolu OSPF k výběru směrovací mapy, která určí jaká síť bude uložena do směrovací mapy a jaká bude filtrována. *Typ-rozhraní* upřesní *typ* a *číslo-rozhraní*, ze kterého jsou aktualizace filtrovány.

distribute-list out – Filtruje aktualizace odcházející z rozhraní daného směrovače.

distribute-list in – Filtruje aktualizace přicházející na zvolené rozhraní směrovače.

6.3 Seznamy IP prefixů

K filtraci se v některých případech dají, jako alternativa přístupových seznamů, použít seznamy IP prefixů. Výhody seznamů IP prefixů jsou:

- Oproti přístupovým seznamům výrazný nárůst výkonu v načtení a hledání v rozsáhlých seznamech.

- Možnost budoucí modifikace seznamu. Samotný seznam není potřeba odstranit celý, stačí pouze doplnit příkazy na požadované místo pomocí pořadového čísla nebo je případně odebrat.
- Oproti přístupovým seznamům uživatelsky přívětivější a přehlednější prostředí.
- Větší flexibilita.

6.3.1 Nastavení seznamů IP prefixů

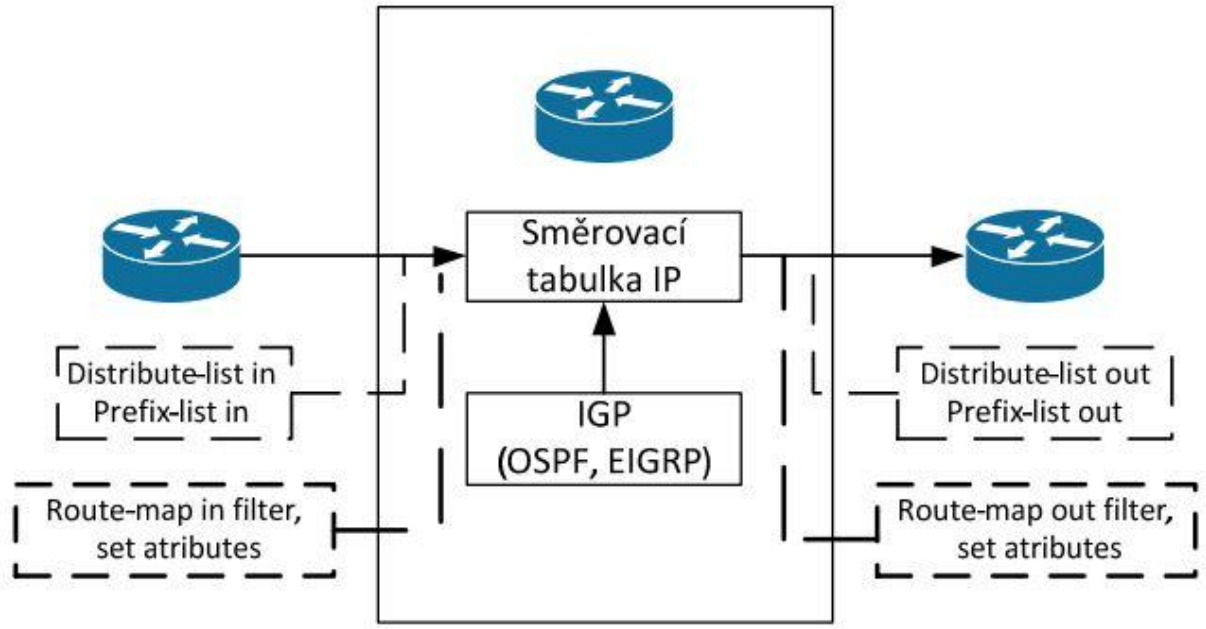
Nastavení se podobá nastavení směrovací mapy.

(router) **ip prefix-list** *název-seznamu* [**seq** *pořadové-číslo*] [**permit | deny**] *síť/délka* [**ge** *ge-hodnota*] [**le** *le-hodnota*]

Příkaz se skládá z názvu seznamu a jednoho nebo více příkazů odlišitelných od sebe pomocí pořadového čísla, které umožňuje vložení příkazu na požadované místo nebo jeho odstranění. Pokud není zadán parametr **seq**, je jeho výchozí hodnota nastavena na 5 a pro další příkazy je inkrementována o hodnotu 5. Akce **permit** nebo **deny** určují jestli je daná cesta shodná nebo ne. Parametr *síť/délka* určuje shodu s konkrétní sítí. Nepovinnými příkazy **ge** a **le** lze parametr rozšířit o porovnání délky sítě s prefixem. Hodnota **ge** *20* (greater - větší než) vybere všechny sítě s délkou prefixu od /20 do /32. Hodnota **le** *20* (lesser – menší než) vybere všechny sítě s délkou prefixu od hodnoty parametru *síť/délka* do hodnoty parametry /20 (*délka* < *ge* < *le* <= 32).

6.4 Kombinování filtračních metod

K filtraci je možné použít více filtračních metod najednou, proto je potřeba znát, které metody se provedou dříve, a které naopak později.



Obrázek 29 Kombinování filtračních metod[35]

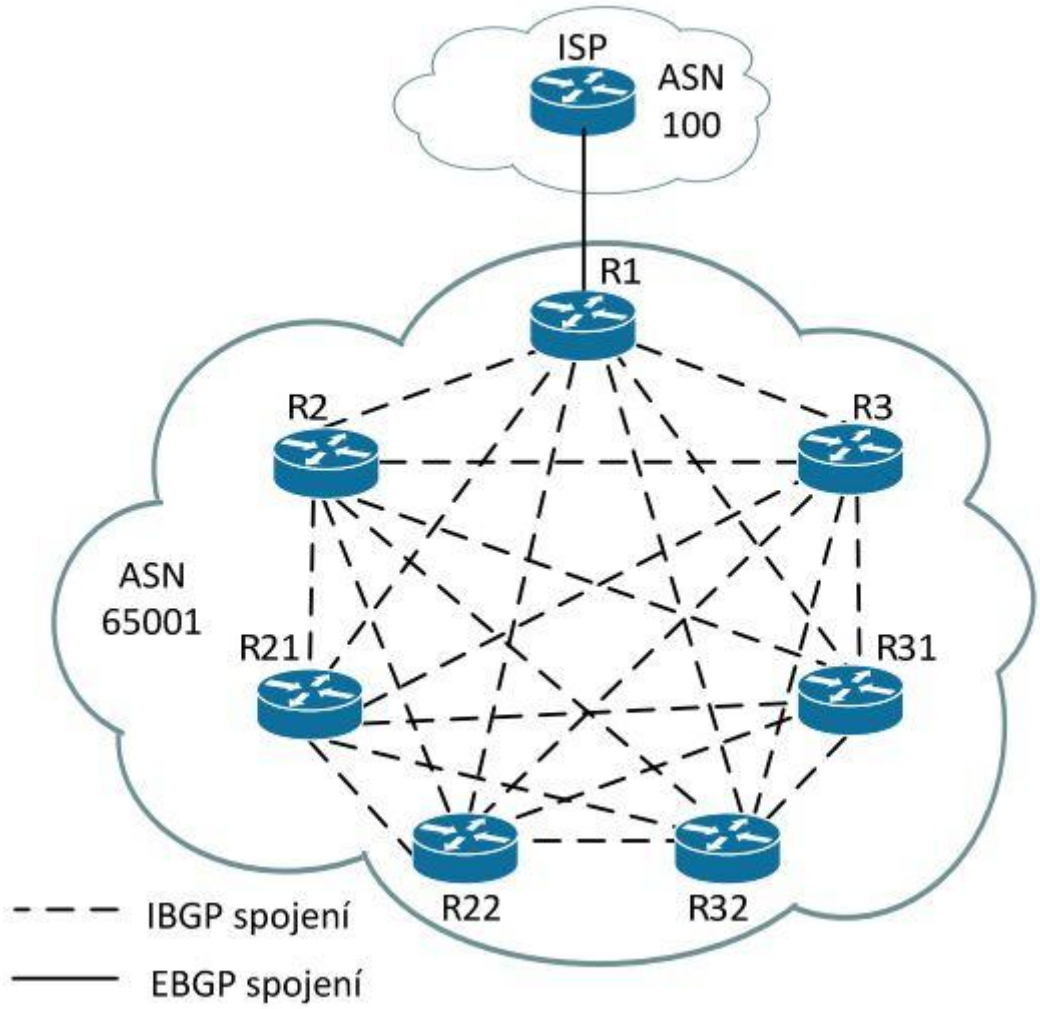
1. Nejprve se provede filtrace cesty podle vstupního distribučního seznamu (Distribute-list in), nebo seznamu IP prefixů (Prefix-list in).
2. Potom se aplikuje vstupní filtr směrovací mapy (Route-map in), který zároveň, v případě použití protokolu BGP, nastaví atributy vybraných cest.
3. Při odchozí filtraci se nejprve provedou příkazy směrovací mapy (Route-map out).
4. Následně se aplikuje distribuční list (Distribute-list out) nebo seznam prefixů (Prefix-list out).

[35] TEARE, Diane. *Implementing Cisco IP routing (ROUTE): foundation learning guide : foundation learning for the ROUTE 642-902 exam*. Indianapolis: Cisco Press, c2010, ISBN 978-1-58705-882-0. str: 398

7 REFLEKTORY CEST

Podle [16], [17]. Použití reflektorů cest rozdělí rozsáhlý autonomní systém na menší podčásti. Partneři uvnitř jednoho autonomního podsystému mají mezi sebou vztah iBGP, zatímco mezi autonomními podsystémy jsou ve vztahu eBGP. Použitím reflektorů cest dojde ke snížení velikosti topologické sítě a k urychlení konvergence BGP.

Reflektory cest (RR – Route Reflector) slouží k výraznému snížení iBGP spojení mezi směrovači uvnitř jednoho autonomního systému. Při použití *n* směrovačů uvnitř autonomního systému je mezi nimi potřeba zajistit *n*(n-1)/2* spojů.

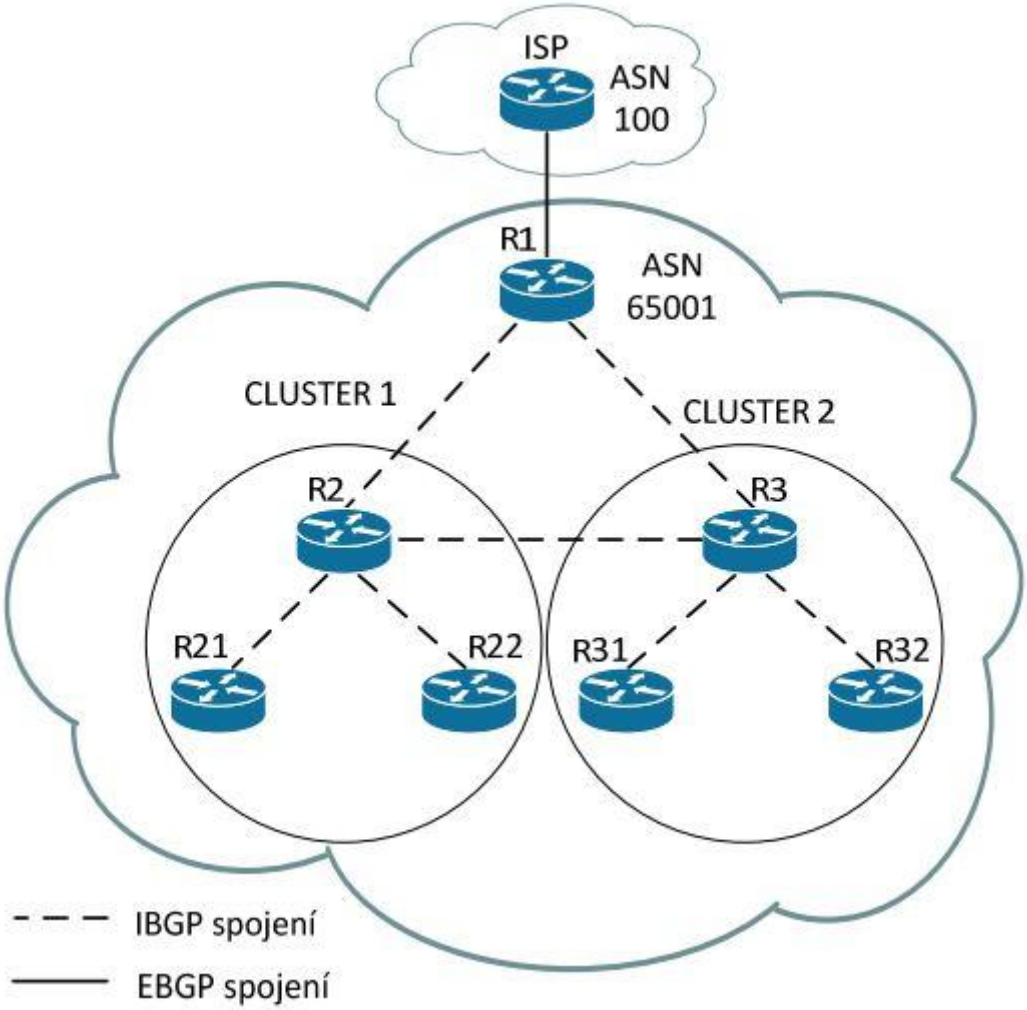


Obrázek 30 Reflektory – iBGP full-mesh spojení (bez reflektoru)[36]

Při použití 7 směrovačů jako na Obrázek 30 je tedy zapotřebí 21 spojů. V rozsáhlé síti potom hrozí výrazné snížení šířky pásma a na jednotlivé směrovače jsou kladeny extrémní

[36] MĚŘIČEK, Tomáš. *Metodika nasazení protokolu BGP pro směrování mezi autonomními uzly*. Hradec Králové, 2012. Diplomová práce. Univerzita Hradec Králové, Fakulta informatiky a managementu, Katedra informačních technologií. str. 63

systémové požadavky.



Obrázek 31 Reflektory – topologie reflektorů cest[37]

Při použití reflektorů cest podle Obrázek 31 klesne počet spojení mezi směrovači z 21 na 7. Při použití reflektorů cest se jeden autonomní systém skládá z jednoho nebo více rozdělených částí, tzv. clusterů. Uvnitř jednoho clusteru se nachází jeden nebo, v případě redundantního spojení, více RR směrovačů. Zbylé směrovače uvnitř clusteru nazýváme klienty a směrovače mimo cluster neklienty. Spojení mezi klienty uvnitř clusteru zajišťuje RR směrovač. RR směrovače musí být vzájemně spojeny pomocí full-mesh spojení. Pokud se nějaký směrovač nenachází v clusteru a není reflektorem, musí být s ostatními RR směrovači také ve stavu full-mesh.

Směrovače R2 a R3 jsou reflektory cest (RR). Směrovače R21 a R22 jsou klienty směrovače

[37] MĚŘIČEK, Tomáš. *Metodika nasazení protokolu BGP pro směrování mezi autonomními uzly*. Hradec Králové, 2012. Diplomová práce. Univerzita Hradec Králové, Fakulta informatiky a managementu, Katedra informačních technologií. str. 64

R2 a směrovače R1, R3, R31, R32 jsou neklienty směrovače R2 a naopak. RR směrovače pracují s odlišnou logikou, zatímco klienti a neklienti fungují stejně jako při iBGP spojení. Po přijmutí aktualizace RR směrovač nejprve informuje své klienty.

Tabulka 7 Pravidla RR směrovače[38]

Umístění, z něhož se RR o prefixu dozví	Oznamují se cesty klientům?	Oznamují se cesty neklientům?
Klient	Ano	Ano
Neklient	Ano	Ne
eBGP	Ano	Ano

7.1 Atributy reflektorů cest

BGP atributy sloužící při použití reflektorů cest k zabránění výskytu směrovacích smyček uvnitř autonomního systému:

- CLUSTER_LIST – Před odesláním cesty se do trasy cesty uloží ID clusteru, kterým cesta prochází. RR směrovač ignoruje všechny aktualizace, u kterých se vyskytuje ID lokálního clusteru.
- ORIGINATOR_ID – Atribut je vytvořen RR směrovačem a nese informaci o ID směrovače v místním autonomním systému. Když směrovač uvidí svoje BGP ID v atributu přijaté cesty, cestu ignoruje. Při použití více RR směrovačů v jednom clusteru je potřeba nastavit na RR směrovači CLUSTER_ID.

7.2 Nastavení reflektoru cest

(router) **neighbor** *ip-adresa* **route-reflector-client**

Příkaz uvnitř BGP procesu nastaví příslušný směrovač na RR směrovač. *Ip-adresa* označí sousední směrovač jako klienta. Při použití více RR směrovačů v jednom clusteru se na všech RR směrovačích použije příkaz **bgp cluster-id** *id-clusteru*. Po nastavení klientů už nelze hodnotu cluster ID změnit.

[38] MĚŘIČEK, Tomáš. *Metodika nasazení protokolu BGP pro směrování mezi autonomními uzly*. Hradec Králové, 2012. Diplomová práce. Univerzita Hradec Králové, Fakulta informatiky a managementu, Katedra informačních technologií. str. 64

Zapojení na Obrázek 31:

Nastavení směrovače R2 jako RR směrovače:

R2#sh run
router bgp 65001
no synchronization
bgp cluster-id 1
network 2.2.2.0 mask 255.255.255.0
network 100.100.100.4 mask 255.255.255.252
network 100.100.100.12 mask 255.255.255.252
network 100.100.100.16 mask 255.255.255.252
network 100.100.100.20 mask 255.255.255.252
neighbor 100.100.100.5 remote-as 65001
neighbor 100.100.100.14 remote-as 65001
neighbor 100.100.100.18 remote-as 65001
neighbor 100.100.100.18 route-reflector-client
neighbor 100.100.100.22 remote-as 65001
neighbor 100.100.100.22 route-reflector-client
no auto-summary

Nastavení směrovače R3 jako RR směrovače:

R3#sh run
router bgp 65001
no synchronization
bgp cluster-id 2
bgp log-neighbor-changes
network 3.3.3.0 mask 255.255.255.0
network 100.100.100.8 mask 255.255.255.252
network 100.100.100.12 mask 255.255.255.252
network 100.100.100.24 mask 255.255.255.252
network 100.100.100.28 mask 255.255.255.252
neighbor 100.100.100.9 remote-as 65001
neighbor 100.100.100.13 remote-as 65001
neighbor 100.100.100.26 remote-as 65001
neighbor 100.100.100.26 route-reflector-client

neighbor 100.100.100.30 remote-as 65001

neighbor 100.100.100.30 route-reflector-client

no auto-summary

Výpis směrovací tabulky směrovače R31:

R31#sh ip route

Gateway of last resort is 100.100.100.1 to network 0.0.0.0

1.0.0.0/24 is subnetted, 1 subnets

B 1.1.1.0 [200/0] via 100.100.100.9, 00:02:40

32.0.0.0/24 is subnetted, 1 subnets

B 32.32.32.0 [200/0] via 100.100.100.30, 00:01:58

2.0.0.0/24 is subnetted, 1 subnets

B 2.2.2.0 [200/0] via 100.100.100.13, 00:02:40

100.0.0.0/30 is subnetted, 8 subnets

B 100.100.100.4 [200/0] via 100.100.100.9, 00:02:40

B 100.100.100.0 [200/0] via 100.100.100.9, 00:02:40

B 100.100.100.12 [200/0] via 100.100.100.25, 00:02:47

B 100.100.100.8 [200/0] via 100.100.100.25, 00:02:47

B 100.100.100.20 [200/0] via 100.100.100.13, 00:02:41

B 100.100.100.16 [200/0] via 100.100.100.13, 00:02:41

B 100.100.100.28 [200/0] via 100.100.100.25, 00:02:20

C 100.100.100.24 is directly connected, Serial0/0

3.0.0.0/24 is subnetted, 1 subnets

B 3.3.3.0 [200/0] via 100.100.100.25, 00:02:48

21.0.0.0/24 is subnetted, 1 subnets

B 21.21.21.0 [200/0] via 100.100.100.18, 00:02:14

22.0.0.0/24 is subnetted, 1 subnets

B 22.22.22.0 [200/0] via 100.100.100.22, 00:02:14

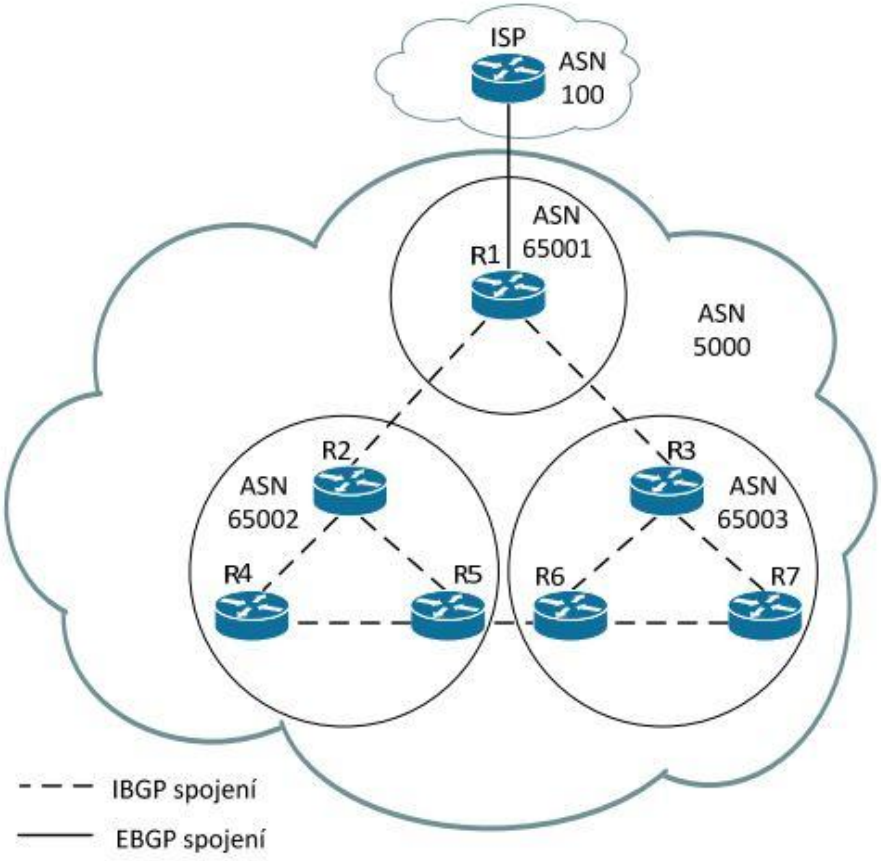
31.0.0.0/24 is subnetted, 1 subnets

C 31.31.31.0 is directly connected, Loopback0

B 0.0.0.0/0 [200/0] via 100.100.100.1, 00:02:14*

8 KONFEDERACE

Podle [18], [19]. Konfederace rozdělují rozsáhlé autonomní systémy na menší podčásti. Partneři uvnitř jednoho autonomního podsystému mají mezi sebou vztah iBGP, mezi autonomními podsystémy jsou potom ve vztahu eBGP. Pomocí konfederací dojde také ke zmenšení topologické sítě a k urychlení konvergence BGP. Konfederace tedy mají stejný význam jako reflektory cest. Při použití konfederací jsou jednotlivé směrovače uvnitř autonomního systému rozděleny do několika individuálních konfederací. Uvnitř jedné částečné konfederace jsou směrovače ve vztahu iBGP, partneři v různých částečných konfederacích jsou ve vztahu eBGP. Směrovače uvnitř částečné konfederace jsou ve vztahu full-mesh. iBGP a eBGP partneři se chovají stejně, jako by byli normálními iBGP a eBGP partnery, platí pro ně stejná pravidla. Zavedení konfederace do síťové topologie přináší výrazné snížení počtu spojení mez iBGP směrovači, tím zároveň snižuje nároky na jednotlivé směrovače. V původní topologii (viz Obrázek 30) se 7 směrovači bylo zapotřebí 21 spojů.



Obrázek 32 Konfederace – topologie[39]

[39] MĚŘIČEK, Tomáš. *Metodika nasazení protokolu BGP pro směrování mezi autonomními uzly*. Hradec Králové, 2012. Diplomová práce. Univerzita Hradec Králové, Fakulta informatiky a managementu, Katedra informačních technologií. str. 67

Zavedením konfederace podle Obrázek 32 klesne počet spojení z 21 na 9.

8.1 Atributy konfederací

K zabránění výskytu směrovacích smyček v konfederačním autonomním systému slouží atribut AS_PATH. Atribut AS_PATH je tvořen čtyřmi segmenty – AS_SET, AS_SEQUENCE, AS_CONFED_SET, AS_CONFED_SEQUENCE. Směrovače nacházející se uvnitř konfederace zaznamenávají částečné autonomní systémy do segmentu AS_CONFED_SEQUENCE. Při použití konfederací se v atributu AS_PATH využívají segmenty AS_CONFED_SET a AS_CONFED_SEQUENCE zabraňující vzniku směrovacích smyček. Při oznámení iBGP cesty do jiného konfederačního autonomního systému musí nejprve konfederační eBGP partner zkontrolovat, jestli se již dílčí autonomní systém v segmentu AS_CONFED_SEQUENCE nevyskytuje. Pokud ano, tuto cestu neoznámí. Rozdíl mezi AS_CONFED_SET a AS_CONFED_SEQUENCE spočívá pouze v neseřazeném nebo seřazeném seznamu autonomních systémů v lokální konfederaci nacházejícím se v přijaté aktualizační zprávě.

8.2 Nastavení konfederace

(router) **bgp confederation identifier** *číslo-AS*

(router) **bgp confederation peers** *číslo-dílčího-AS*

První příkaz nastaví konfederaci. Pomocí druhého příkazu se identifikují všechny sousední dílčí autonomní systémy uvnitř BGP procesu, který je identifikován jako místní dílčí autonomní systém.

Zapojení na Obrázek 32:

Nastavení konfederace na směrovači R1:

R1#sh run

router bgp 65001

no synchronization

bgp log-neighbor-changes

bgp confederation identifier 5000

bgp confederation peers 65002 65003

network 1.1.1.0 mask 255.255.255.0

network 100.100.100.0 mask 255.255.255.252

network 100.100.100.4 mask 255.255.255.252

network 100.100.100.8 mask 255.255.255.252

neighbor 100.100.100.1 remote-as 100

neighbor 100.100.100.6 remote-as 65002
neighbor 100.100.100.10 remote-as 65003
default-information originate
no auto-summary

Nastavení konfederace na směrovači R2:
R2#sh run
router bgp 65002
no synchronization
bgp log-neighbor-changes
bgp confederation identifier 5000
bgp confederation peers 65001 65003
network 2.2.2.0 mask 255.255.255.0
network 100.100.100.4 mask 255.255.255.252
network 100.100.100.12 mask 255.255.255.252
network 100.100.100.16 mask 255.255.255.252
neighbor 100.100.100.5 remote-as 65001
neighbor 100.100.100.14 remote-as 65002
neighbor 100.100.100.18 remote-as 65002
no auto-summary

Nastavení konfederace na směrovači R3:
R3#sh run
router bgp 65003
no synchronization
bgp log-neighbor-changes
bgp confederation identifier 5000
bgp confederation peers 65001 65002
network 3.3.3.0 mask 255.255.255.0
network 100.100.100.8 mask 255.255.255.252
network 100.100.100.24 mask 255.255.255.252
network 100.100.100.28 mask 255.255.255.252
neighbor 100.100.100.9 remote-as 65001
neighbor 100.100.100.26 remote-as 65003

neighbor 100.100.100.30 remote-as 65003

no auto-summary

Výpis směrovací tabulky směrovače R4:

R4#sh ip route

Gateway of last resort is 100.100.100.1 to network 0.0.0.0

1.0.0.0/24 is subnetted, 1 subnets

B 1.1.1.0 [200/0] via 100.100.100.5, 00:04:47

2.0.0.0/24 is subnetted, 1 subnets

B 2.2.2.0 [200/0] via 100.100.100.13, 00:04:52

100.0.0.0/30 is subnetted, 10 subnets

B 100.100.100.36 [200/0] via 100.100.100.22, 00:03:45

B 100.100.100.32 [200/0] via 100.100.100.38, 00:02:28

B 100.100.100.4 [200/0] via 100.100.100.13, 00:04:52

B 100.100.100.0 [200/0] via 100.100.100.5, 00:04:47

C 100.100.100.12 is directly connected, Serial0/0

B 100.100.100.8 [200/0] via 100.100.100.5, 00:04:49

C 100.100.100.20 is directly connected, Serial0/1

B 100.100.100.16 [200/0] via 100.100.100.13, 00:04:36

B 100.100.100.28 [200/0] via 100.100.100.25, 00:02:31

B 100.100.100.24 [200/0] via 100.100.100.10, 00:03:18

3.0.0.0/24 is subnetted, 1 subnets

B 3.3.3.0 [200/0] via 100.100.100.10, 00:04:26

4.0.0.0/24 is subnetted, 1 subnets

C 4.4.4.0 is directly connected, Loopback0

5.0.0.0/24 is subnetted, 1 subnets

B 5.5.5.0 [200/0] via 100.100.100.22, 00:03:48

6.0.0.0/24 is subnetted, 1 subnets

B 6.6.6.0 [200/0] via 100.100.100.38, 00:03:02

7.0.0.0/24 is subnetted, 1 subnets

B 7.7.7.0 [200/0] via 100.100.100.30, 00:02:17

B 0.0.0.0/0 [200/0] via 100.100.100.1, 00:04:26*

9 ZÁVĚR

Práce byla vytvořena pomocí vlastních zkušeností získaných během studia CCNA od společnosti Cisco, následného samostudia a s použitím uvedené literatury.

V první kapitole byly popsány základní pojmy zahrnující autonomní systémy a používané typy interních a externích směrovacích protokolů. Ve druhé kapitole byl podrobně popsán protokol BGP s jeho vlastnostmi, typy spojení, možnostmi jeho použití a nasazení, zprávami a atributy jeho cest. Třetí kapitola představila možnosti základní konfigurace BGP sítě se základními konfiguračními příkazy. Ve čtvrté kapitole jsem se zaměřil na problematiku redistribuce, která patří mezi komplikované oblasti při konfiguraci interních a externích směrovacích protokolů. Pátá kapitola byla zaměřena na manipulaci s jednotlivými cestami v BGP. Šestá kapitola se zabývá filtrací BGP aktualizací, která se využívá k zabránění propagování nepotřebných cest. V sedmé kapitole jsem se zaměřil na reflektory cest používané ke snížení systémových nároků na zařízení a k celkovému urychlení konvergence sítě. V osmé kapitole byly popsány konfederace, sloužící stejně jako reflektory cest ke snížení systémových nároků na zařízení a k celkovému urychlení konvergence sítě.

Praktická část byla vytvořena v programu GNS3 stažitelného na internetových stránkách http://www.gns3.net/. Na směrovačích byly aplikovány IOS používané v univerzitní Cisco laboratoři.

K nastavení protokolu BGP je, na rozdíl od většiny IGP protokolů, potřeba mít pokročilé znalosti v oblasti routingu srovnatelné alespoň s úrovní kurzu CCNA 4 od společnosti Cisco. Chybně nastavený protokol BGP může negativně ovlivnit chod významné části Internetu, zatímco nesprávné nastavení IGP protokolů ovlivní nanejvýš sítě v několika propojených společnostech. Jako hlavní rozdíly při konfiguraci lze uvést nutnost zavedení komplikované redistribuce cest a s ní související problémy s filtrací a manipulací těchto cest.

10 POUŽITÁ LITERATURA

1. GRYGÁREK, Petr. Směrování v počítačových sítích a v Internetu. *Katedra informatiky: Fakulta elektrotechniky a informatiky, VŠB-TUO* [online]. [2012/2013] [cit. 2013-04-05]. Dostupné z: http://www.cs.vsb.cz/grygarek/SPS/lect/routing-ucitele.pdf
2. GRYGÁREK, Petr. Směrovací protokol BGP. *Katedra informatiky: Fakulta elektrotechniky a informatiky, VŠB-TUO* [online]. [2012/2013] [cit. 2013-04-05]. Dostupné z: http://www.cs.vsb.cz/grygarek/SPS/lect/BGP/BGP.html
3. PALÚCH, Peter. Border Gateway Protocol (BGP): BSCI Module 6. *Katedra informačných sietí: Fakulta riadenia a informatiky ŽU* [online]. [12-Sep-2011] [cit. 2013-04-05]. Dostupné z: http://www.kis.fri.uniza.sk/~palo/prednasky/ccnp-route-v6/ROUTE_M6-BGP.pdf
4. Regional Internet registry. In: *Wikipedia: the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation, 2001- [cit. 2013-04-05]. Dostupné z: http://en.wikipedia.org/wiki/Regional_Internet_registry
5. MAHEL, Aleš. Směrování a směrovací protokoly. *Neoo72* [online]. [21-Jun-2009] [cit. 2013-04-05]. Dostupné z: http://www.neoo72.ic.cz/doc/pos/10_protokoly.pdf
6. PETERKA, Jiří, Směrování v TCP/IP sítích - IV. *EArchiv.cz: archiv článků a přednášek Jiřího Peterky* [online]. 1992, 41/92 [cit. 2013-04-05]. Dostupné z: http://www.earchiv.cz/a92/a241c110.php3
7. 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.
8. TEARE, Diane. *Implementing Cisco IP routing (ROUTE): foundation learning guide : foundation learning for the ROUTE 642-902 exam*. Indianapolis: Cisco Press, c2010, xxix, 945 s. ISBN 978-1-58705-882-0.
9. BOUŠKA, Petr. Cisco Routing 5 - BGP - Border Gateway Protocol. *SAMURAJ-cz* [online]. 2009 [cit. 2013-04-05]. Dostupné z: http://www.samuraj-cz.com/clanek/cisco-routing-5-bgp-border-gateway-protocol/
10. HOONG, Yap Chin. *CCNP ROUTE Complete Guide*. 1st Edition. United States of America: CreateSpace Independent Publishing Platform, 2010. ISBN 1453807667.
11. SANJEEV. BGP Message Types. *A New Beginning* [online]. 2012 [cit. 2013-04-05]. Dostupné z: http://choudharysanjeev.blogspot.cz/

12. INETDAEMON. BGP Notification Message. INETDAEMON ENTERPRISES. *InetDaemon.Com: Free Online IT Tutorials and Internet Training* [online]. © 1995-2012 [cit. 2013-04-05]. Dostupné z: http://www.inetdaemon.com/tutorials/internet/ip/routing/bgp/operation/messages/notification.shtml
13. CISCO SYSTEMS, Inc. *Cisco IOS XE IP Routing: BGP Configuration Guide* [online]. Release 2. San Jose: Cisco Systems, Inc., © 2009-2010 [cit. 2013-04-05]. Dostupné z: http://www.cisco.com/en/US/docs/ios/ios_xe/iproute_bgp/configuration/guide/2_xe/irg_xe_book.pdf
14. WHITE, Russ, Danny MCPHERSON a Sangli SRIHARI. *Practical BGP*. Boston: Addison-Wesley, 2005, xii, 434 p. ISBN 03-211-2700-5.
15. ODOM, Wendell, Rus HEALY a Naren MEHTA. *Směrování a přepínání sítí: autorizovaný výukový průvodce*. Vyd. 1. Brno: Computer Press, 2009, 879 s. ISBN 978-80-251-2520-5.
16. BATES, T., R. CHANDRA a E. CHEN. BGP Route Reflection: An Alternative to Full Mesh IBGP. *The Internet Engineering Task Force* [online]. 2000 [cit. 2013-04-05]. Dostupné z: http://www.ietf.org/rfc/rfc2796.txt.pdf
17. BATES, T., E. CHEN a R. CHANDRA. BGP Route Reflection: An Alternative to Full Mesh Internal BGP. *The Internet Engineering Task Force* [online]. 2006 [cit. 2013-04-05]. Dostupné z: http://www.ietf.org/rfc/rfc4456.txt.pdf
18. TRAINA, P., D. MCPHERSON a J. SCUDDER. Autonomous System Confederations for BGP. *The Internet Engineering Task Force* [online]. 2001 [cit. 2013-04-05]. Dostupné z: http://www.ietf.org/rfc/rfc3065.txt.pdf
19. TRAINA, P., D. MCPHERSON a J. SCUDDER. Autonomous System Confederations for BGP. *The Internet Engineering Task Force* [online]. 2007 [cit. 2013-04-05]. Dostupné z: http://www.ietf.org/rfc/rfc5065.txt.pdf
20. MĚŘIČEK, Tomáš. *Metodika nasazení protokolu BGP pro směrování mezi autonomními uzly*. Hradec Králové, 2012. Diplomová práce. Univerzita Hradec Králové, Fakulta informatiky a managementu, Katedra informačních technologií. Vedoucí práce Mgr. Josef Horálek.
21. HAMOUZ, Ondřej. *Směrování mezi autonomními systémy s využitím protokolu BGP*. Ústí nad Labem, 2011. Bakalářská práce. Univerzita J. E. Purkyně v Ústí nad Labem, Přírodovědecká fakulta. Vedoucí práce Mgr. Jindřich Jelínek.

22. HANKO, Adam. *Snižování doby konvergence protokolu BGP* [online]. Olomouc, 2011 [cit. 2013-04-05]. Dostupné z: http://theses.cz/id/ya5cej/diplom.pdf. Diplomová práce. Přírodovědecká fakulta Univerzity Palackého, Katedra informatiky. Vedoucí práce Doc. Ing. Lence Carr-Motyčková, CSc.
23. CISCO SYSTEMS, Inc. *Cisco* [online]. © 1992-2013 [cit. 2013-04-05]. Dostupné z: http://www.cisco.com/en/US/tech/tk365/tk80/tsd_technology_support_sub-protocol_home.html

Příloha 1 Konfigurace – Redistribuce – připojení k jednomu ISP

```
hostname ISP
!
no ip domain lookup
!
interface Loopback0
ip address 1.1.1.1 255.255.255.0
!
interface FastEthernet0/0
ip address 100.100.100.1 255.255.255.252
duplex auto
speed auto
!
interface FastEthernet0/1
ip address 100.100.100.5 255.255.255.252
duplex auto
speed auto
!
router bgp 65101
no synchronization
bgp log-neighbor-changes
network 0.0.0.0
neighbor 100.100.100.2 remote-as 65001
neighbor 100.100.100.6 remote-as 65001
default-information originate
no auto-summary
!
ip route 0.0.0.0 0.0.0.0 Loopback0
!
end
```

```
hostname R2
!
no ip domain lookup
!
interface Loopback1
ip address 140.140.0.1 255.255.255.128
!
interface Loopback2
ip address 140.140.0.129 255.255.255.128
!
interface Serial0/0
ip address 100.100.100.10 255.255.255.252
!
interface Serial0/1
ip address 100.100.100.13 255.255.255.252
clock rate 128000
!
interface Serial0/2
ip address 100.100.100.21 255.255.255.252
!
router eigrp 1
redistribute bgp 65001 metric 64 1000 255 1 1500
network 100.100.100.20 0.0.0.3
no auto-summary
!
router bgp 65001
no synchronization
bgp log-neighbor-changes
bgp redistribute-internal
network 140.140.0.0 mask 255.255.255.128
network 140.140.0.128 mask 255.255.255.128
aggregate-address 140.140.0.0 255.255.255.0 summary-only
redistribute eigrp 1
neighbor 100.100.100.9 remote-as 65001
neighbor 100.100.100.14 remote-as 65001
no auto-summary
!
end
```

```
hostname R4
!
no ip domain lookup
```

```
hostname R1
!
no ip domain lookup
!
interface FastEthernet0/0
ip address 100.100.100.2 255.255.255.252
duplex auto
speed auto
 !
interface Serial0/0
ip address 100.100.100.9 255.255.255.252
clock rate 128000
!
interface FastEthernet0/1
ip address 100.100.100.6 255.255.255.252
duplex auto
speed auto
!
interface Serial0/1
ip address 100.100.100.17 255.255.255.252
!
router bgp 65001
no synchronization
bgp log-neighbor-changes
network 0.0.0.0
neighbor 100.100.100.1 remote-as 65101
neighbor 100.100.100.5 remote-as 65101
neighbor 100.100.100.10 remote-as 65001
neighbor 100.100.100.18 remote-as 65001
default-information originate
no auto-summary
!
ip route 0.0.0.0 0.0.0.0 FastEthernet0/0 210
ip route 0.0.0.0 0.0.0.0 FastEthernet0/1 220
!
end
```

```
hostname R3
!
no ip domain lookup
!
interface Loopback3
ip address 160.160.0.1 255.255.255.192
!
interface Loopback4
ip address 160.160.0.65 255.255.255.192
!
interface Serial0/0
ip address 100.100.100.14 255.255.255.252
!
interface Serial0/1
ip address 100.100.100.18 255.255.255.252
clock rate 128000
!
interface Serial0/2
ip address 100.100.100.25 255.255.255.252
!
router eigrp 2
redistribute bgp 65001 metric 64 100 255 1 1500
network 100.100.100.24 0.0.0.3
no auto-summary
!
router bgp 65001
no synchronization
bgp log-neighbor-changes
bgp redistribute-internal
network 160.160.0.0 mask 255.255.255.192
network 160.160.0.64 mask 255.255.255.192
aggregate-address 160.160.0.0 255.255.255.128 summary-only
redistribute eigrp 2
neighbor 100.100.100.13 remote-as 65001
neighbor 100.100.100.17 remote-as 65001
```

```
!
interface Loopback5
ip address 200.200.0.129 255.255.255.192
!
interface Loopback6
ip address 200.200.0.1 255.255.255.128
!
interface Loopback7
ip address 200.200.0.193 255.255.255.224
!
interface Loopback8
ip address 200.200.0.225 255.255.255.224
!
interface Loopback9
ip address 200.200.1.1 255.255.255.240
!
interface Serial0/0
ip address 100.100.100.22 255.255.255.252
ip summary-address eigrp 1 200.200.0.0 255.255.254.0 5
clock rate 128000
!
router eigrp 1
network 100.100.100.20 0.0.0.3
network 200.200.0.0 0.0.0.127
network 200.200.0.128 0.0.0.63
network 200.200.0.192 0.0.0.31
network 200.200.0.224 0.0.0.31
network 200.200.1.0 0.0.0.15
no auto-summary
!
end

hostname R6
!
no ip domain lookup
!
interface Loopback10
ip address 180.180.1.129 255.255.255.224
ip ospf network point-to-point
!
interface Loopback11
ip address 180.180.0.1 255.255.255.128
ip ospf network point-to-point
!
interface Loopback12
ip address 180.180.1.1 255.255.255.192
ip ospf network point-to-point
!
interface Loopback13
ip address 180.180.0.129 255.255.255.128
ip ospf network point-to-point
!
interface Loopback14
ip address 180.180.1.65 255.255.255.192
ip ospf network point-to-point
!
interface Serial0/0
ip address 100.100.100.30 255.255.255.252
clock rate 128000
!
router ospf 1
log-adjacency-changes
area 1 range 180.180.0.0 255.255.254.0
network 100.100.100.28 0.0.0.3 area 0
network 180.180.0.0 0.0.0.127 area 1
network 180.180.0.128 0.0.0.127 area 1
network 180.180.1.0 0.0.0.63 area 1
network 180.180.1.64 0.0.0.63 area 1
network 180.180.1.128 0.0.0.31 area 1
!
end
```

```
no auto-summary
!
end

hostname R5
!
no ip domain lookup
!
interface Serial0/0
ip address 100.100.100.26 255.255.255.252
clock rate 128000
!
interface Serial0/1
ip address 100.100.100.29 255.255.255.252
!
router eigrp 2
redistribute ospf 1 metric 64 100 255 1 1500
network 100.100.100.24 0.0.0.3
no auto-summary
!
router ospf 1
log-adjacency-changes
redistribute eigrp 2 subnets
network 100.100.100.28 0.0.0.3 area 0
default-information originate
!
end
```

Příloha 2 Konfigurace – Redistribuce – Připojení ke dvěma ISP

```
hostname ISP1
!
no ip domain lookup
!
interface Loopback0
ip address 1.1.1.1 255.255.255.255
!
interface FastEthernet0/0
ip address 100.100.100.1 255.255.255.252
duplex auto
speed auto
!
router bgp 65101
no synchronization
bgp log-neighbor-changes
network 0.0.0.0
network 100.100.100.0 mask 255.255.255.252
neighbor 100.100.100.2 remote-as 65001
default-information originate
no auto-summary
!
ip route 0.0.0.0 0.0.0.0 Loopback0
!
end
```

```
hostname ISP2
!
no ip domain lookup
!
interface Loopback0
ip address 1.1.1.1 255.255.255.255
!
interface FastEthernet0/0
ip address 100.100.100.5 255.255.255.252
duplex auto
speed auto
!
router bgp 65102
no synchronization
bgp log-neighbor-changes
network 0.0.0.0
network 100.100.100.4 mask 255.255.255.252
neighbor 100.100.100.6 remote-as 65001
default-information originate
no auto-summary
!
ip route 0.0.0.0 0.0.0.0 Loopback0
!
end
```

```
hostname R1
!
no ip domain lookup
!
interface FastEthernet0/0
ip address 100.100.100.2 255.255.255.252
duplex auto
speed auto
!
interface Serial0/0
ip address 100.100.100.9 255.255.255.252
!
interface Serial0/1
ip address 100.100.100.17 255.255.255.252
clock rate 128000
!
router eigrp 2
redistribute ospf 1 metric 64 100 255 1 1500
network 100.100.100.16 0.0.0.3
no auto-summary
!
router ospf 1
log-adjacency-changes
redistribute eigrp 2 subnets
redistribute bgp 65001 subnets
network 100.100.100.8 0.0.0.3 area 0
default-information originate
!
router bgp 65001
no synchronization
bgp log-neighbor-changes
network 100.100.100.0 mask 255.255.255.252
redistribute eigrp 2
redistribute ospf 1
neighbor 100.100.100.1 remote-as 65101
neighbor 100.100.100.1 route-map PRI-ISP-IN in
neighbor 100.100.100.1 route-map PRI-ISP-MED-OUT out
neighbor 100.100.100.13 remote-as 65001
neighbor 100.100.100.13 next-hop-self
no auto-summary
!
ip route 0.0.0.0 0.0.0.0 FastEthernet0/0
!
route-map PRIMARY-ISP-IN permit 10
set local-preference 150
!
route-map PRIMARY-ISP-MED-OUT permit 10
```

```
hostname R2
!
no ip domain lookup
!
interface FastEthernet0/0
ip address 100.100.100.6 255.255.255.252
duplex auto
speed auto
!
interface Serial0/0
ip address 100.100.100.13 255.255.255.252
!
interface Serial0/1
ip address 100.100.100.21 255.255.255.252
clock rate 128000
!
router eigrp 1
redistribute ospf 1 metric 64 100 255 1 1500
network 100.100.100.20 0.0.0.3
no auto-summary
!
router ospf 1
log-adjacency-changes
redistribute eigrp 1 subnets
redistribute bgp 65001 subnets
network 100.100.100.12 0.0.0.3 area 0
default-information originate
!
router bgp 65001
no synchronization
bgp log-neighbor-changes
network 100.100.100.4 mask 255.255.255.252
redistribute eigrp 1
redistribute ospf 1
neighbor 100.100.100.5 remote-as 65102
neighbor 100.100.100.5 route-map SEC-ISP-IN in
neighbor 100.100.100.5 route-map SEC-ISP-MED-OUT out
neighbor 100.100.100.9 remote-as 65001
neighbor 100.100.100.9 next-hop-self
no auto-summary
!
ip route 0.0.0.0 FastEthernet0/0
!
route-map SECONDARY-ISP-IN permit 10
set local-preference 100
!
route-map SECONDARY-ISP-MED-OUT permit 10
```

```
set metric 50
!
end

hostname R3
!
no ip domain lookup
!
interface Loopback1
ip address 192.40.0.65 255.255.255.240
ip ospf network point-to-point
!
interface Loopback2
ip address 192.40.0.1 255.255.255.224
ip ospf network point-to-point
!
interface Loopback3
ip address 192.40.0.33 255.255.255.224
ip ospf network point-to-point
!
interface Serial0/0
ip address 100.100.100.10 255.255.255.252
clock rate 128000
!
interface Serial0/1
ip address 100.100.100.14 255.255.255.252
clock rate 128000
!
router ospf 1
log-adjacency-changes
area 3 range 192.40.0.0 255.255.255.128
network 100.100.100.8 0.0.0.3 area 0
network 100.100.100.12 0.0.0.3 area 0
network 192.40.0.0 0.0.0.31 area 3
network 192.40.0.32 0.0.0.31 area 3
network 192.40.0.64 0.0.0.15 area 3
!
end

hostname R5
!
no ip domain lookup
!
interface Loopback7
ip address 192.50.0.1 255.255.255.128
!
interface Loopback8
ip address 192.50.0.161 255.255.255.240
!
interface Loopback9
ip address 192.50.0.129 255.255.255.224
!
interface Serial0/0
ip address 100.100.100.18 255.255.255.252
ip summary-address eigrp 2 192.50.0.0 255.255.255.0 5
!
router eigrp 2
network 100.100.100.16 0.0.0.3
network 192.50.0.0 0.0.0.127
network 192.50.0.128 0.0.0.31
network 192.50.0.160 0.0.0.15
no auto-summary
!
end

set metric 75
!
end

hostname R4
!
no ip domain lookup
!
interface Loopback4
ip address 192.60.0.193 255.255.255.224
!
interface Loopback5
ip address 192.60.0.1 255.255.255.128
!
interface Loopback6
ip address 192.60.0.129 255.255.255.192
!
interface Serial0/0
ip address 100.100.100.22 255.255.255.252
ip summary-address eigrp 1 192.60.0.0 255.255.255.0 5
!
router eigrp 1
network 100.100.100.20 0.0.0.3
network 192.60.0.0 0.0.0.127
network 192.60.0.128 0.0.0.63
network 192.60.0.192 0.0.0.31
no auto-summary
!
end
```

Příloha 3 Konfigurace – Výběr cest – místní preference, metrika, váha cesty

```
hostname ISP
!
no ip domain lookup
!
interface Loopback0
ip address 1.1.1.1 255.255.255.0
!
interface Serial0/0
ip address 100.100.100.1 255.255.255.252
clock rate 128000
!
interface Serial0/1
ip address 100.100.100.5 255.255.255.252
!
router bgp 100
no synchronization
bgp log-neighbor-changes
network 0.0.0.0
network 100.100.100.0 mask 255.255.255.252
network 100.100.100.4 mask 255.255.255.252
neighbor 100.100.100.2 remote-as 65001
neighbor 100.100.100.6 remote-as 65001
no auto-summary
!
ip route 0.0.0.0 0.0.0.0 Loopback0
!
end
```

```
hostname R1
!
no ip domain lookup
!
interface FastEthernet0/0
ip address 100.100.100.21 255.255.255.252
duplex auto
speed auto
!
interface Serial0/0
ip address 100.100.100.2 255.255.255.252
!
interface FastEthernet0/1
ip address 100.100.100.25 255.255.255.252
duplex auto
speed auto
!
interface Serial0/1
ip address 100.100.100.9 255.255.255.252
clock rate 128000
!
interface Serial0/2
ip address 100.100.100.13 255.255.255.252
!
router eigrp 1
redistribute bgp 65001 metric 64 100 255 1 1500
network 100.100.100.12 0.0.0.3
no auto-summary
!
router bgp 65001
no synchronization
bgp log-neighbor-changes
redistribute eigrp 1
neighbor 100.100.100.1 remote-as 100
neighbor 100.100.100.1 route-map PRI-ISP-IN in
neighbor 100.100.100.1 route-map PRI-ISP-MED-OUT out
neighbor 100.100.100.10 remote-as 65001
neighbor 100.100.100.22 remote-as 1000
neighbor 100.100.100.22 route-map WEIGHT-FA0/0 in
neighbor 100.100.100.26 remote-as 1000
neighbor 100.100.100.26 route-map WEIGHT-FA0/1 in
no auto-summary
!
route-map PRIMARY-ISP-IN permit 10
set local-preference 150
!
route-map WEIGHT-FA0/1 permit 10
set weight 75
!
route-map WEIGHT-FA0/0 permit 10
set weight 150
!
route-map PRIMARY-ISP-MED-OUT permit 10
set metric 50
!
end
```

```
hostname R2
!
no ip domain lookup
!
interface Serial0/0
ip address 100.100.100.6 255.255.255.252
clock rate 128000
!
interface Serial0/1
ip address 100.100.100.10 255.255.255.252
!
interface Serial0/2
ip address 100.100.100.17 255.255.255.252
!
router eigrp 2
```

```
hostname R3
!
no ip domain lookup
!
interface Loopback1
ip address 140.140.1.129 255.255.255.224
!
interface Loopback2
ip address 140.140.0.1 255.255.255.128
!
interface Loopback3
ip address 140.140.1.1 255.255.255.192
!
interface Loopback4
ip address 140.140.0.129 255.255.255.128
```

```
redistribute bgp 65001 metric 64 100 255 1 1500
network 100.100.100.16 0.0.0.3
no auto-summary
!
router bgp 65001
no synchronization
bgp log-neighbor-changes
redistribute eigrp 2
neighbor 100.100.100.5 remote-as 100
neighbor 100.100.100.5 route-map SEC-ISP-IN in
neighbor 100.100.100.5 route-map SEC-ISP-MED-OUT out
neighbor 100.100.100.9 remote-as 65001
no auto-summary
!
route-map SECONDARY-ISP-IN permit 10
set local-preference 100
!
route-map SECONDARY-ISP-MED-OUT permit 10
set metric 75
!
end
```

```
hostname R4
!
no ip domain lookup
!
interface Loopback6
ip address 180.180.0.129 255.255.255.192
!
interface Loopback7
ip address 180.180.0.1 255.255.255.128
!
interface Loopback8
ip address 180.180.0.193 255.255.255.224
!
interface Loopback9
ip address 180.180.0.225 255.255.255.224
!
interface Loopback10
ip address 180.180.1.1 255.255.255.240
!
interface Serial0/0
ip address 100.100.100.18 255.255.255.252
ip summary-address eigrp 2 180.180.0.0 255.255.254.0 5
clock rate 128000
!
router eigrp 2
network 100.100.100.16 0.0.0.3
network 180.180.0.0 0.0.0.127
network 180.180.0.128 0.0.0.63
network 180.180.0.192 0.0.0.31
network 180.180.0.224 0.0.0.31
network 180.180.1.0 0.0.0.15
no auto-summary
!
end
```

```
!
interface Loopback5
ip address 140.140.1.65 255.255.255.192
!
interface Serial0/0
ip address 100.100.100.14 255.255.255.252
ip summary-address eigrp 1 140.140.0.0 255.255.252.0 5
clock rate 128000
!
router eigrp 1
network 100.100.100.12 0.0.0.3
network 140.140.0.0 0.0.0.127
network 140.140.0.128 0.0.0.127
network 140.140.1.0 0.0.0.63
network 140.140.1.64 0.0.0.63
network 140.140.1.128 0.0.0.31
no auto-summary
!
router bgp 65001
no synchronization
bgp log-neighbor-changes
redistribute eigrp 2
no auto-summary
!
end
```

```
hostname R5
!
no ip domain lookup
!
interface Loopback0
ip address 150.150.0.1 255.255.255.0
!
interface FastEthernet0/0
ip address 100.100.100.22 255.255.255.252
duplex auto
speed auto
!
interface FastEthernet0/1
ip address 100.100.100.26 255.255.255.252
duplex auto
speed auto
!
router bgp 1000
no synchronization
bgp log-neighbor-changes
network 150.150.0.0 mask 255.255.255.0
neighbor 100.100.100.21 remote-as 65001
neighbor 100.100.100.21 route-map WEIGHT-FA0/0 in
neighbor 100.100.100.25 remote-as 65001
neighbor 100.100.100.25 route-map WEIGHT-FA0/1 in
no auto-summary
!
route-map WEIGHT-FA0/1 permit 10
set weight 75
!
route-map WEIGHT-FA0/0 permit 10
set weight 150
!
end
```

Příloha 4 Konfigurace – Výběr cest – AS-Path

```
hostname ISP
!
no ip domain lookup
!
interface Loopback0
ip address 1.1.1.1 255.255.255.0
!
interface Serial0/0
ip address 100.100.100.1 255.255.255.252
clock rate 128000
!
interface Serial0/1
ip address 100.100.100.5 255.255.255.252
!
router bgp 100
no synchronization
bgp log-neighbor-changes
network 0.0.0.0
neighbor 100.100.100.2 remote-as 200
neighbor 100.100.100.6 remote-as 300
neighbor 100.100.100.6 filter-list 1 out
no auto-summary
!
ip route 0.0.0.0 0.0.0.0 Loopback0
!
ip as-path access-list 1 deny ^200$
ip as-path access-list 1 permit .*
!
end
```

```
hostname R1
!
no ip domain lookup
!
interface Serial0/0
ip address 100.100.100.2 255.255.255.252
!
interface Serial0/1
ip address 100.100.100.9 255.255.255.252
clock rate 128000
!
router ospf 1
log-adjacency-changes
redistribute bgp 200 subnets
network 100.100.100.8 0.0.0.3 area 0
default-information originate
!
router bgp 200
no synchronization
bgp log-neighbor-changes
redistribute ospf 1
neighbor 100.100.100.1 remote-as 100
no auto-summary
!
end
```

```
hostname R2
!
no ip domain lookup
!
interface Serial0/0
ip address 100.100.100.6 255.255.255.252
clock rate 128000
!
interface Serial0/1
ip address 100.100.100.13 255.255.255.252
!
interface Serial0/2
ip address 100.100.100.17 255.255.255.252
!
interface Serial0/3
ip address 100.100.100.21 255.255.255.252
clock rate 128000
!
router eigrp 1
redistribute bgp 300 metric 64 100 255 1 1500
network 100.100.100.12 0.0.0.3
no auto-summary
!
router bgp 300
no synchronization
bgp log-neighbor-changes
redistribute eigrp 1
neighbor 100.100.100.5 remote-as 100
neighbor 100.100.100.18 remote-as 500
neighbor 100.100.100.22 remote-as 600
no auto-summary
!
end
```

```
hostname R3
!
no ip domain lookup
!
interface Loopback1
ip address 210.210.0.129 255.255.255.192
ip ospf network point-to-point
!
interface Loopback2
ip address 210.210.0.193 255.255.255.192
ip ospf network point-to-point
!
interface Loopback3
ip address 210.210.0.1 255.255.255.128
ip ospf network point-to-point
!
interface Serial0/0
ip address 100.100.100.10 255.255.255.252
!
router ospf 1
log-adjacency-changes
area 1 range 210.210.0.0 255.255.255.0
network 100.100.100.8 0.0.0.3 area 0
network 210.210.0.0 0.0.0.127 area 1
network 210.210.0.128 0.0.0.63 area 1
network 210.210.0.192 0.0.0.63 area 1
!
end
```

```
hostname R4
!
no ip domain lookup
!
interface Loopback4
ip address 220.220.1.1 255.255.255.128
!
interface Loopback5
```

```
hostname R5
!
no ip domain lookup
!
interface Serial0/0
ip address 100.100.100.18 255.255.255.252
clock rate 128000
!
```

```
ip address 220.220.1.129 255.255.255.128
!
interface Loopback6
ip address 220.220.0.1 255.255.255.0
!
interface Serial0/0
ip address 100.100.100.14 255.255.255.252
ip summary-address eigrp 1 220.220.0.0 255.255.254.0 5
clock rate 128000
!
router eigrp 1
network 100.100.100.12 0.0.0.3
network 220.220.0.0
network 220.220.1.0 0.0.0.127
network 220.220.1.128 0.0.0.127
no auto-summary
!
end
```

```
hostname R6
!
no ip domain lookup
!
interface Serial0/0
ip address 100.100.100.22 255.255.255.252
!
interface Serial0/1
ip address 100.100.100.29 255.255.255.252
clock rate 128000
!
router bgp 600
no synchronization
bgp log-neighbor-changes
neighbor 100.100.100.21 remote-as 300
neighbor 100.100.100.30 remote-as 700
no auto-summary
!
end
```

```
interface Serial0/1
ip address 100.100.100.25 255.255.255.252
!
router bgp 500
no synchronization
bgp log-neighbor-changes
neighbor 100.100.100.17 remote-as 300
neighbor 100.100.100.17 route-map AS-PATH-PREPEND out
neighbor 100.100.100.26 remote-as 700
neighbor 100.100.100.26 route-map AS-PATH-PREPEND out
no auto-summary
!
route-map AS-PATH-PREPEND permit 10
set as-path prepend 500 500
!
end
```

```
hostname R7
!
no ip domain lookup
!
interface Loopback0
ip address 120.110.100.1 255.255.255.0
!
interface Serial0/0
ip address 100.100.100.26 255.255.255.252
clock rate 128000
!
interface Serial0/1
ip address 100.100.100.30 255.255.255.252
!
router bgp 700
no synchronization
bgp log-neighbor-changes
network 120.110.100.0 mask 255.255.255.0
neighbor 100.100.100.25 remote-as 500
neighbor 100.100.100.29 remote-as 600
no auto-summary
!
end
```

Příloha 5 Konfigurace – Reflektory cest

```
hostname ISP
!
no ip domain lookup
!
interface Loopback0
ip address 10.10.10.1 255.255.255.0
!
interface Serial0/0
ip address 100.100.100.1 255.255.255.252
clock rate 128000
!
router bgp 100
no synchronization
bgp log-neighbor-changes
network 0.0.0.0
network 100.100.100.0 mask 255.255.255.252
neighbor 100.100.100.2 remote-as 65001
no auto-summary
!
ip route 0.0.0.0 0.0.0.0 Loopback0
!
end
```

```
hostname R1
!
no ip domain lookup
!
interface Loopback0
ip address 1.1.1.1 255.255.255.0
!
interface Serial0/0
ip address 100.100.100.2 255.255.255.252
!
interface Serial0/1
ip address 100.100.100.5 255.255.255.252
clock rate 128000
!
interface Serial0/2
ip address 100.100.100.9 255.255.255.252
!
router bgp 65001
no synchronization
bgp log-neighbor-changes
network 1.1.1.0 mask 255.255.255.0
network 100.100.100.0 mask 255.255.255.252
network 100.100.100.4 mask 255.255.255.252
network 100.100.100.8 mask 255.255.255.252
neighbor 100.100.100.1 remote-as 100
neighbor 100.100.100.6 remote-as 65001
neighbor 100.100.100.10 remote-as 65001
default-information originate
no auto-summary
!
ip route 0.0.0.0 0.0.0.0 Serial0/0
!
end
```

```
hostname R2
!
no ip domain lookup
!
interface Loopback0
ip address 2.2.2.1 255.255.255.0
!
interface Serial0/0
ip address 100.100.100.6 255.255.255.252
!
interface Serial0/1
ip address 100.100.100.13 255.255.255.252
clock rate 128000
!
interface Serial0/2
ip address 100.100.100.17 255.255.255.252
!
interface Serial0/3
ip address 100.100.100.21 255.255.255.252
!
router bgp 65001
no synchronization
bgp cluster-id 1
bgp log-neighbor-changes
network 2.2.2.0 mask 255.255.255.0
network 100.100.100.4 mask 255.255.255.252
network 100.100.100.12 mask 255.255.255.252
network 100.100.100.16 mask 255.255.255.252
network 100.100.100.20 mask 255.255.255.252
neighbor 100.100.100.5 remote-as 65001
neighbor 100.100.100.14 remote-as 65001
neighbor 100.100.100.18 remote-as 65001
neighbor 100.100.100.18 route-reflector-client
neighbor 100.100.100.22 remote-as 65001
neighbor 100.100.100.22 route-reflector-client
no auto-summary
!
end
```

```
hostname R3
!
no ip domain lookup
!
interface Loopback0
ip address 3.3.3.1 255.255.255.0
!
interface Serial0/0
ip address 100.100.100.10 255.255.255.252
clock rate 128000
!
interface Serial0/1
ip address 100.100.100.14 255.255.255.252
!
interface Serial0/2
ip address 100.100.100.25 255.255.255.252
!
interface Serial0/3
ip address 100.100.100.29 255.255.255.252
!
router bgp 65001
no synchronization
bgp cluster-id 2
bgp log-neighbor-changes
network 3.3.3.0 mask 255.255.255.0
network 100.100.100.8 mask 255.255.255.252
network 100.100.100.12 mask 255.255.255.252
network 100.100.100.24 mask 255.255.255.252
network 100.100.100.28 mask 255.255.255.252
neighbor 100.100.100.9 remote-as 65001
neighbor 100.100.100.13 remote-as 65001
neighbor 100.100.100.26 remote-as 65001
neighbor 100.100.100.26 route-reflector-client
neighbor 100.100.100.30 remote-as 65001
neighbor 100.100.100.30 route-reflector-client
no auto-summary
!
end
```

```
hostname R21
!
no ip domain lookup
!
interface Loopback0
ip address 21.21.21.1 255.255.255.0
!
interface Serial0/0
ip address 100.100.100.18 255.255.255.252
clock rate 128000
!
router bgp 65001
no synchronization
bgp log-neighbor-changes
network 21.21.21.0 mask 255.255.255.0
network 100.100.100.16 mask 255.255.255.252
neighbor 100.100.100.17 remote-as 65001
no auto-summary
!
end
```

```
hostname R22
!
no ip domain lookup
!
interface Loopback0
ip address 22.22.22.1 255.255.255.0
!
interface Serial0/0
ip address 100.100.100.22 255.255.255.252
clock rate 128000
!
router bgp 65001
no synchronization
bgp log-neighbor-changes
network 22.22.22.0 mask 255.255.255.0
network 100.100.100.20 mask 255.255.255.252
neighbor 100.100.100.21 remote-as 65001
no auto-summary
!
end
```

```
hostname R31
!
no ip domain lookup
!
interface Loopback0
ip address 31.31.31.1 255.255.255.0
!
interface Serial0/0
ip address 100.100.100.26 255.255.255.252
clock rate 128000
!
router bgp 65001
no synchronization
bgp log-neighbor-changes
network 31.31.31.0 mask 255.255.255.0
network 100.100.100.24 mask 255.255.255.252
neighbor 100.100.100.25 remote-as 65001
no auto-summary
!
end
```

```
hostname R32
!
no ip domain lookup
!
interface Loopback0
ip address 32.32.32.1 255.255.255.0
!
interface Serial0/0
ip address 100.100.100.30 255.255.255.252
clock rate 128000
!
router bgp 65001
no synchronization
bgp log-neighbor-changes
network 32.32.32.0 mask 255.255.255.0
network 100.100.100.28 mask 255.255.255.252
neighbor 100.100.100.29 remote-as 65001
no auto-summary
!
end
```

Příloha 6 Konfigurace – Konfederace

```
hostname ISP
!
no ip domain lookup
!
interface Loopback0
ip address 10.10.10.1 255.255.255.0
!
interface Serial0/0
ip address 100.100.100.1 255.255.255.252
clock rate 128000
!
router bgp 100
no synchronization
bgp log-neighbor-changes
network 0.0.0.0
network 100.100.100.0 mask 255.255.255.252
neighbor 100.100.100.2 remote-as 5000
no auto-summary
!
ip route 0.0.0.0 0.0.0.0 Loopback0
!
end
```

```
hostname R1
!
no ip domain lookup
!
interface Loopback0
ip address 1.1.1.1 255.255.255.0
!
interface Serial0/0
ip address 100.100.100.2 255.255.255.252
!
interface Serial0/1
ip address 100.100.100.5 255.255.255.252
clock rate 128000
!
interface Serial0/2
ip address 100.100.100.9 255.255.255.252
clock rate 128000
!
router bgp 65001
 no synchronization
bgp log-neighbor-changes
bgp confederation identifier 5000
bgp confederation peers 65002 65003
network 1.1.1.0 mask 255.255.255.0
network 100.100.100.0 mask 255.255.255.252
network 100.100.100.4 mask 255.255.255.252
network 100.100.100.8 mask 255.255.255.252
neighbor 100.100.100.1 remote-as 100
neighbor 100.100.100.6 remote-as 65002
neighbor 100.100.100.10 remote-as 65003
default-information originate
no auto-summary
!
ip route 0.0.0.0 0.0.0.0 Serial0/0
!
end
```

```
hostname R2
!
no ip domain lookup
!
interface Loopback0
ip address 2.2.2.1 255.255.255.0
!
interface Serial0/0
ip address 100.100.100.6 255.255.255.252
!
interface Serial0/1
ip address 100.100.100.13 255.255.255.252
clock rate 128000
!
interface Serial0/2
ip address 100.100.100.17 255.255.255.252
!
router bgp 65002
no synchronization
bgp log-neighbor-changes
bgp confederation identifier 5000
bgp confederation peers 65001 65003
network 2.2.2.0 mask 255.255.255.0
network 100.100.100.4 mask 255.255.255.252
network 100.100.100.12 mask 255.255.255.252
network 100.100.100.16 mask 255.255.255.252
neighbor 100.100.100.5 remote-as 65001
neighbor 100.100.100.14 remote-as 65002
neighbor 100.100.100.18 remote-as 65002
no auto-summary
!
end
```

```
hostname R3
!
no ip domain lookup
!
interface Loopback0
ip address 3.3.3.1 255.255.255.0
!
interface Serial0/0
ip address 100.100.100.10 255.255.255.252
!
interface Serial0/1
ip address 100.100.100.25 255.255.255.252
clock rate 128000
!
interface Serial0/2
ip address 100.100.100.29 255.255.255.252
!
router bgp 65003
no synchronization
bgp log-neighbor-changes
bgp confederation identifier 5000
bgp confederation peers 65001 65002
network 3.3.3.0 mask 255.255.255.0
network 100.100.100.8 mask 255.255.255.252
network 100.100.100.24 mask 255.255.255.252
network 100.100.100.28 mask 255.255.255.252
neighbor 100.100.100.9 remote-as 65001
neighbor 100.100.100.26 remote-as 65003
neighbor 100.100.100.30 remote-as 65003
no auto-summary
!
end
```

```
hostname R4
!
no ip domain lookup
!
interface Loopback0
ip address 4.4.4.1 255.255.255.0
!
interface Serial0/0
ip address 100.100.100.14 255.255.255.252
!
interface Serial0/1
ip address 100.100.100.21 255.255.255.252
clock rate 128000
!
router bgp 65002
no synchronization
bgp log-neighbor-changes
bgp confederation identifier 5000
bgp confederation peers 65001 65003
network 4.4.4.0 mask 255.255.255.0
network 100.100.100.12 mask 255.255.255.252
network 100.100.100.20 mask 255.255.255.252
neighbor 100.100.100.13 remote-as 65002
neighbor 100.100.100.22 remote-as 65002
no auto-summary
!
end
```

```
hostname R5
!
no ip domain lookup
!
interface Loopback0
ip address 5.5.5.1 255.255.255.0
!
interface Serial0/0
ip address 100.100.100.18 255.255.255.252
clock rate 128000
!
interface Serial0/1
ip address 100.100.100.22 255.255.255.252
!
interface Serial0/2
ip address 100.100.100.37 255.255.255.252
!
router bgp 65002
no synchronization
bgp log-neighbor-changes
bgp confederation identifier 5000
bgp confederation peers 65001 65003
network 5.5.5.0 mask 255.255.255.0
network 100.100.100.16 mask 255.255.255.252
network 100.100.100.20 mask 255.255.255.252
network 100.100.100.36 mask 255.255.255.252
neighbor 100.100.100.17 remote-as 65002
neighbor 100.100.100.21 remote-as 65002
neighbor 100.100.100.38 remote-as 65003
no auto-summary
!
end
```

```
hostname R6
!
no ip domain lookup
!
interface Loopback0
ip address 6.6.6.1 255.255.255.0
!
interface Serial0/0
ip address 100.100.100.26 255.255.255.252
!
interface Serial0/1
ip address 100.100.100.33 255.255.255.252
clock rate 128000
!
interface Serial0/2
ip address 100.100.100.38 255.255.255.252
clock rate 128000
!
router bgp 65003
no synchronization
bgp log-neighbor-changes
bgp confederation identifier 5000
bgp confederation peers 65001 65002
network 6.6.6.0 mask 255.255.255.0
network 100.100.100.24 mask 255.255.255.252
network 100.100.100.32 mask 255.255.255.252
network 100.100.100.36 mask 255.255.255.252
neighbor 100.100.100.25 remote-as 65003
neighbor 100.100.100.34 remote-as 65003
neighbor 100.100.100.37 remote-as 65002
no auto-summary
!
end
```

```
hostname R7
!
no ip domain lookup
!
interface Loopback0
ip address 7.7.7.1 255.255.255.0
!
interface Serial0/0
ip address 100.100.100.30 255.255.255.252
clock rate 128000
!
interface Serial0/1
ip address 100.100.100.34 255.255.255.252
!
router bgp 65003
no synchronization
bgp log-neighbor-changes
bgp confederation identifier 5000
bgp confederation peers 65001 65002
network 7.7.7.0 mask 255.255.255.0
network 100.100.100.28 mask 255.255.255.252
network 100.100.100.32 mask 255.255.255.252
neighbor 100.100.100.29 remote-as 65003
neighbor 100.100.100.33 remote-as 65003
no auto-summary
!
end
```