Zabezpečení prenosu dat v autonómnich systémech

Bc. Matúš Valentovič

Diplomová práce
2021

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
Akademický rok: 2020/2021

Studijní program: Inženýrská informatika
Forma studia: Kombinovaná
Obor/kombinace: Bezpečnostní technologie, systémy a management (knBT-T)

Podklad pro zadání DIPLOMOVÉ práce studenta

Jméno a příjmení:	**Bc. Matúš Valentovič**
Osobní číslo:	**A18368**
Adresa:	Stupavská ulica 3, Malacky, 90101 Malacky, Slovenská republika
Téma práce:	Zabezpečení přenosu dat v autonmních systémech
Téma práce anglicky:	Security of Data Transmission in Autonomous Systems
Vedoucí práce:	Ing. Miroslav Matýsek, Ph.D. Ústav počítačových a komunikačních systémů

Zásady pro vypracování:

1. Zpracujte literární rešerši na dané téma.
2. Popište vývoj BGP protokolu a topologie Internetu.
3. Popište komunikaci BGP protokolu s protokoly IGP – EIGRP, OSPF a RIP.
4. Popište rozšíření BGP protokolu pro MPLS VPN, IP Multicast, IPv6 a CLNS.
5. Popište zabezpečení BGP protokolu.
6. Navrhněte zabezpečenou konfiguraci sítě s BGP protokolem pomocí Cisco Packet Traceru.
7. Vyhodnoťte účinnost zabezpečení navrhované sítě s BGP protokolem.

Seznam doporučené literatury:

1. BOOKHAM, Colin. *Versatile Routing and Services with BGP: Understanding and Implementing BGP in SR-OS*. Indianapolis: WILEY, 2014. ISBN 978-1118875285.
2. ZHANG, Randy a Micah BARTELL. *BGP Design and Implementation*. Indianapolis: Cisco Press, 2016. ISBN 9781587144707.
3. TEARE, Diane, Bob VACHON a Rick GRAZIANI. *Implementing Cisco IP routing (ROUTE)*. Indianapolis: Cisco Press, 2015. Cisco Press foundation learning guide. ISBN 978-158-7204-562.
4. KOCHARIANS, Narbik. *CCIE routing and switching v5.0 official cert guide*. Fifth edition. Indianapolis: Cisco Press, 2015. ISBN 978-158-7144-912.
5. BEIJNUM, Iljitsch van. *BGP*. Sebastopol: O'Reilly, 2002. ISBN 978-0-596-00254-1.

Podpis studenta: Datum:

Podpis vedoucího práce: Datum:

Prohlašuji, že

- beru na vědomí, že odevzdáním diplomové práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že diplomová práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk diplomové/bakalářské práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně a jeden výtisk bude uložen u vedoucího práce;
- byl/a jsem seznámen/a s tím, že na moji diplomovou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – diplomovou práci nebo poskytnout licenci k jejímu využití jen připouští-li tak licenční smlouva uzavřená mezi mnou a Univerzitou Tomáše Bati ve Zlíně s tím, že vyrovnání případného přiměřeného příspěvku na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše) bude rovněž předmětem této licenční smlouvy;
- beru na vědomí, že pokud bylo k vypracování diplomové práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky diplomové/bakalářské práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem diplomové práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

- že jsem na diplomové práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně, dne Matúš Valentovič v.r.

ABSTRAKT

Internet sa stal kritickou komunikačnou infraštruktúrou, na ktorú sme čoraz viac odkázaní. Pretože svet smeruje do konvergovanej siete, kde sa hlas, video a dáta prenášajú rovnakou sieťou, narušenie internetu môže spôsobiť vážnejšie škody. Preto je mimoriadne dôležité chrániť internet pred možným prerušením služieb, aby sa zabezpečilo jeho nepretržité fungovanie. Border Gateway Protocol (BGP) je štandardný a jediný smerovací protokol používaný na Internete. BGP objavuje a udržiava informácie o smerovaní používané na prenos cez Internet, a preto sa všeobecne považuje za rozhodujúcu súčasť internetovej infraštruktúry. Cieľom tejto práce je poskytnúť dostatočné základné informácie pre pochopenie bezpečnostných problémov BGP a lepšie porozumieť rozdielom medzi existujúcimi návrhmi bezpečnosti BGP a výzvam, ktorým čelia pri navrhovaní a praktickom nasadení bezpečnejšieho BGP.

Klíčová slova: BGP, autonómne systémy, eBGP, iBGP, bezpečnosť

ABSTRACT

The Internet has become a critical communication infrastructure which we are increasingly reliant upon. As the world moves into a converged network where voice, video, and data are all transmitted over the same network, disruption of the Internet can cause more severe damage. Therefore, it is critical to protect the Internet from poten tial service disruption in order to ensure its continous functioning. The Border Gateway Protocol (BGP) is the standard and only routing protocol used on the Internet. BGP discovers and maintains routing information used for transmitting traffic across the Internet, thus, it is widely considered as a crucial component of the Internet infrastructure. This job aims to provide sufficient background information for understan ding BGP security issues, and to better understand the differences between existing BGP security proposals and the challenges faced in the design and practical deployment of a more secure BGP.

Keywords: BGP, Autonomous system, eBGP, iBGP, security

Rád by som sa poďakoval vedúcemu práce Ing. Miroslavu Matýskovi, PhD. a oponentovi za vedenie, pripomienky, rady a trpezlivosti, ktorú mi venovali.

OBSAH

ÚVOD

V dnešnej dobe je takmer všetko pripojené k internetu. Náš poskytovateľ internetu sa stará o to aby sme mali globálny prístup na Internet. Internet ako ho dnes nazývame a berieme ho ako štandardnú vec v našom živote je ale jedna komplexná sieť sietí, ktorá sa dlhé desaťročia vyvíjala na tú podobu, akú ju dnes my všetci poznáme. Tvorí ju komplex uzlov a autonómnych systémov, kde každý systém má svoje číslo. Tieto autonómne systémy fungujú na protokole BGP.

Informácie o smerovaní protokolu BGP si obvykle vymieňajú konkurenčné podnikateľské subjekty, poskytovatelia internetových služieb v otvorenom a nepriateľskom prostredí. BGP je teda veľmi zameraný na bezpečnosť, napríklad všetky susedné smerovače musia byť konfigurované manuálne a slušné implementácie BGP poskytujú bohatú sadu filtrov smerovania, ktoré umožňujú ISP brániť svoje siete a kontrolovať, čo inzerujú svojim konkurentom.

Cieľom tejto práce je poskytnúť prehľad o vývoji, komunikácii a bezpečnosti BGP sietí na platforme Cisco. Taktiež rozoberieme typy základných komunikačných štandardov BGP a popísať zabezpečenie sietí. Hlavným cieľom bolo zhodnotiť BGP siete z hľadiska vývoja bezpečnosti a návrhu fiktívnej sieti v programe Cisco Packet Tracer.

I. TEORETICKÁ ČÁST

1 VÝVOJ INTERNETU

Príbeh hovorí, že Internet - alebo skôr ARPANET (Advanced Research Projects Agency Network), ktorý je považovaný za pôvod dnešného internetu - bol vynájdený armádou ako sieť, ktorá vydrží jadrový útok. Takto sa to skutočne nestalo. Začiatkom 60. rokov minulého storočia Paul Baran, výskumný pracovník spoločnosti Rand Corporation, napísal niekoľko memoránd navrhujúcich digitálnu komunikačnú sieť na vojenské účely, ktorá by mohla fungovať aj naďalej po utrpení veľkého poškodenia nepriateľským útokom. Pomocou simulácií Baran dokázal, že sieť s iba trikrát alebo štyrikrát toľkými spojeniami, ako je minimum potrebné na prevádzku, sa blíži teoretickej maximálnej možnej odolnosti. To samozrejme znamená, že sieť sa prispôsobí v prípade zlyhania spojenia, čo telefónna sieť a jej jednoduché digitálne pripojenia nemohli urobiť, pretože každé pripojenie bolo nakonfigurované manuálne. Baran začlenil do svojej navrhovanej siete množstvo revolučných konceptov napríklad prepínanie paketov, prispôsobivé smerovanie, používanie digitálnych obvodov na prenos hlasovej komunikácie a šifrovanie v sieti.

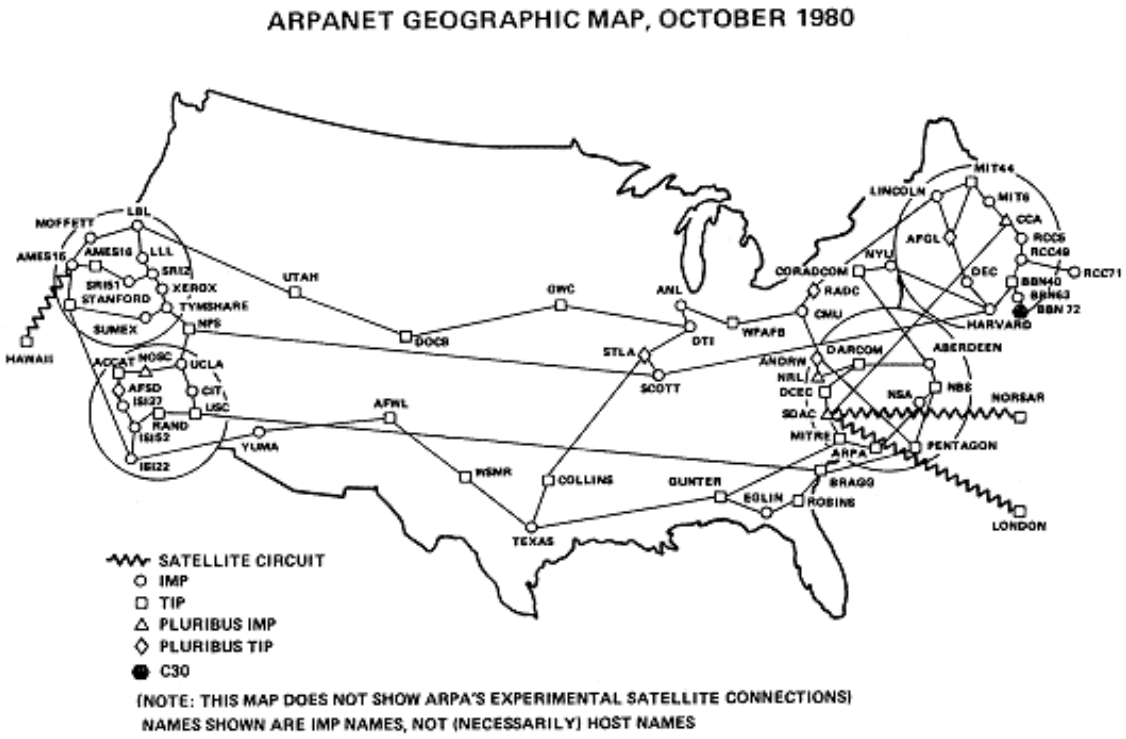
O niekoľko rokov neskôr ARPA (Advanced Research Projects Agency) ministerstva obrany bola nespokojná s tým, že mnohé univerzity a iné výskumné inštitúcie, ktoré pracovali na projektoch ARPA, si nedokázali ľahko vymieňať výsledky týkajúce sa práce s počítačom. Pretože sa používali počítače od mnohých rôznych dodávateľov s rôznymi operačnými systémami a jazykmi, bolo mimoriadne ťažké vytvoriť program vyvinutý na jednom počítači tak, aby bežal na inom počítači. ARPA požadovala sieť, ktorá by výskumníkom umožňovala prístup k počítačom umiestneným na rôznych výskumných inštitúciách po celých Spojených štátoch.

V 70. rokoch 20. storočia sa ARPANET naďalej vyvíjal. Pôvodný sieťový riadiaci protokol NCP (Network Control Protocol), bol nahradený dvoma rôznymi protokolmi. IP (Internet protocol), ktorý spája rôzne siete, a protokolom TCP (Transmission Control Protocol), s ktorými aplikácie komunikujú bez toho, aby sa museli zaoberať zložitosti internetovým protokolom. IP a TCP sa často uvádzajú ako TCP/IP, aby zahŕňali celú rodinu súvisiacich protokolov používaných na internete.

1.1 Topológia Internetu

Pretože išlo o „sieť sietí“, vždy bolo potrebné prepojiť rôzne siete, ktoré spolu tvoria globálny internet. Na začiatku sa každý jednoducho pripojil k ARPANETu, ale v priebehu rokov sa topológia internetu radikálne zmenila.

Na konci osemdesiatych rokov 20. storočia bol ARPANET nahradený sieťou medzi piatimi super počítačovými miestami NFSNET (National Science Foundation Network). Federálne internetové výmeny na východnom a západnom pobreží FIX (Federal Internet Exchange) východ a FIX západ ktoré boli vybudované v roku 1989 s cieľom pomôcť pri prechode z ARPANET na chrbticu NFSNET. Pôvodne boli FIX 10 Mbps, ale neskôr sa pridal FDDI (Fiber distributed data interface) s rýchlosťou 100 Mb/s, aby sa zvýšila šírka pásma. Komerčná internetová burza na západnom pobreží vznikla, pretože ľudia zodpovední za systémy FIX váhali s pripojením komerčných sietí.



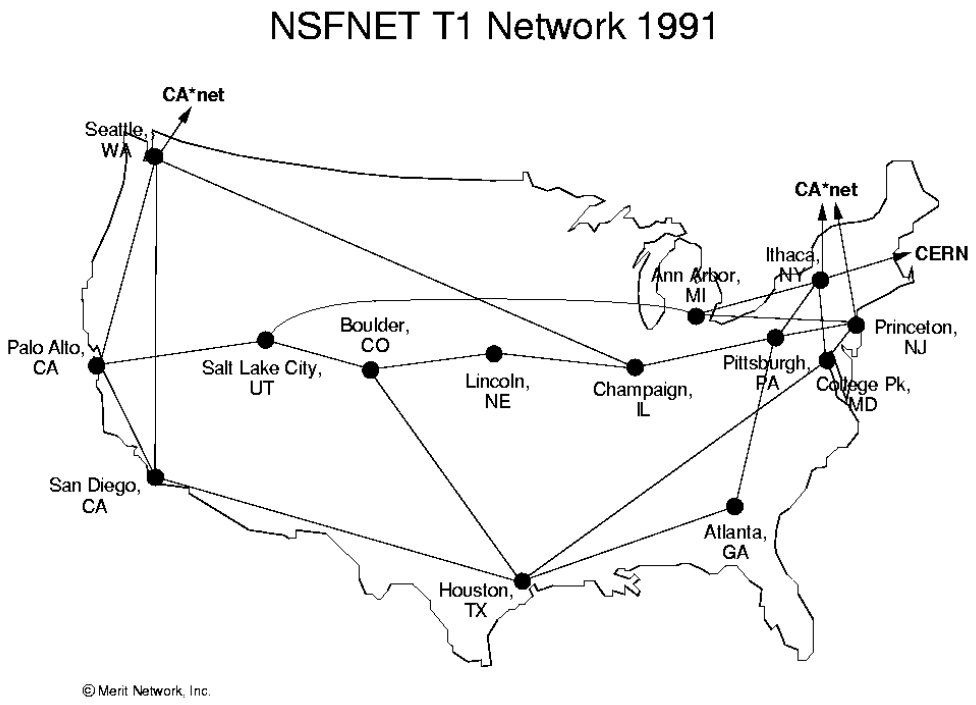
Obr. 1 Mapa APRANET v roku 1980 [1].

V roku 1992 spoločnosť MFS (Metropolitan Fiber Systems), postavila vo Washingtone oblasť, ktorá sa rýchlo stala miestom, kde mnoho rôznych prepojených komerčných sietí. Prepojenie na IX (Internet Exchange) alebo MAE (Metropolitan Area Exchange) je atraktívne, pretože mnoho sietí sa pripája k infraštruktúre IX alebo MAE, takže všetko čo je potrebné

je jediné fyzické pripojenie na prepojenie s mnohými inými sieťami. NAP (Network Access Points) boli vytvorené ako rozsiahle výmenné body, kde sa komerčné siete mohli vzájomne prepojiť bez toho, aby boli obmedzené politikou akceptovateľného použitia NSFNET. NAP sa použili aj na prepojenie s novou národnou výskumnou sieťou pre aplikácie s veľkou šírkou pásma VBNS (Very high Bandwidth Network Service) [1].

Objemy prenosu pre internetové výmeny v Európe a ázijsko-tichomorskom regióne boli v čase vytvárania NAP oveľa nižšie, takže tieto výmeny neboli nútené prijať drahé FDDI alebo ešte nezrelé ATM (Asynchronous transfer mode) technológie ako americké NAP. Pretože Ethernet je lacný, ľahšie konfigurovateľný ako ATM a bežne dostupný v niekoľkých rýchlostiach, väčšina internetových sietí iných ako NAP používa Ethernet. Existuje ich aj niekoľko, ktoré používajú rámcové relé, SMDS (Switched Multi-megabit Data Service) alebo SRP (Server Routing Protocol), zvyčajne, keď sa internetová burza neobmedzuje iba na jedno miesto alebo na malý počet miest, ale umožňuje pripojenie k akejkoľvek kancelárii ISP (Internet Service Provider) alebo k miestu prítomnosti POP (Point of Presence) v rámci metropolitnej oblasti.

V Európe má väčšina krajín internetovú výmenu. Z medzinárodného hľadiska sú hlavné LINX (The London Internet Exchange), AMS-IX (Amsterdam Internet Exchange) a DE-CIX (Deutsche Commercial Internet Exchange) vo Frankfurte. Internetové výmeny vo zvyšku sveta ešte nedosiahli rozsah v Spojených Štátoch a Európe. Používajú sa hlavne na výmeny vnútroštátnej prevádzky [2].



Obr. 2 Historická mapa infraštruktúry NSFNET [1].

1.2 Klasifikácia ISP

Všetci poskytovatelia internetových služieb nie sú rovnocennými. Od obrovských poskytovateľov s celosvetovými sieťami, až po malých, iba s jedným Ethernetom. Všeobecne sú poskytovatelia internetových služieb rozdelení do troch skupín:

1. Poskytovatelia internetových služieb triedy 1 sú takí veľkí, že za tranzit neplatia nikomu inému. Nemusia, pretože sa porovnávajú so všetkými ostatnými sieťami úrovne 1. Všetky ostatné siete musia platiť za tranzit aspoň jednému poskytovateľovi internetových služieb úrovne 1. Poskytovatelia internetových služieb úrovne 1 zaisťujú pripojenie k celému internetu.
2. Poskytovatelia internetových služieb triedy 2 majú veľkú vlastnú sieť, avšak nie sú však tak veľký, aby presvedčili všetky siete úrovne 1, aby s nimi spolupracovali. Dostanú tranzitnú službu od aspoň jedného poskytovateľa internetových služieb 1. úrovne.
3. Poskytovatelia internetových služieb triedy 3 nevytvárajú sieť, preto kupujú tranzitné služby od jedného alebo viacerých poskytovateľov internetových služieb úrovne 1 alebo 2, ktorí pôsobia v tejto oblasti. Ak sa pripájajú na iné siete, zvyčajne ide iba o jediný výmenný bod.

Spojenie medzi sieťami najvyššej úrovne 1 a menšou sieťou úrovni 2 je trochu rozmazaná, pričom niektoré siete úrovne 2 tvoria platené peeringovanie v sieťach úrovne 1. Pritom sa nazývajú úrovňou 1. Skutočný rozdiel spočíva v tom, že siete úrovne 2 majú vo všeobecnosti geograficky obmedzenú prítomnosť. Príkladom sú aj niektoré veľmi veľké európske siete s vlastným transatlantickým spojením, ktorý platia za tranzit skôr americkej sieti, než za prepojenie s veľkým počtom ďalších sietí v NAP v celých Spojených štátoch. Na druhej strane siete úrovne 2 nemusia vzájomne peerovať s mnohými sieťami úrovne 1.

V roku 1989 bolo v Európe založené fórum RIPE (Réseaux IP Européens) pre spoluprácu a bola otvorená všetkým stranám so záujmom o rozsiahle IP siete. Prácu vykonávali jednotliví dobrovoľníci vo svojom alebo v čase svojej organizácie [2].

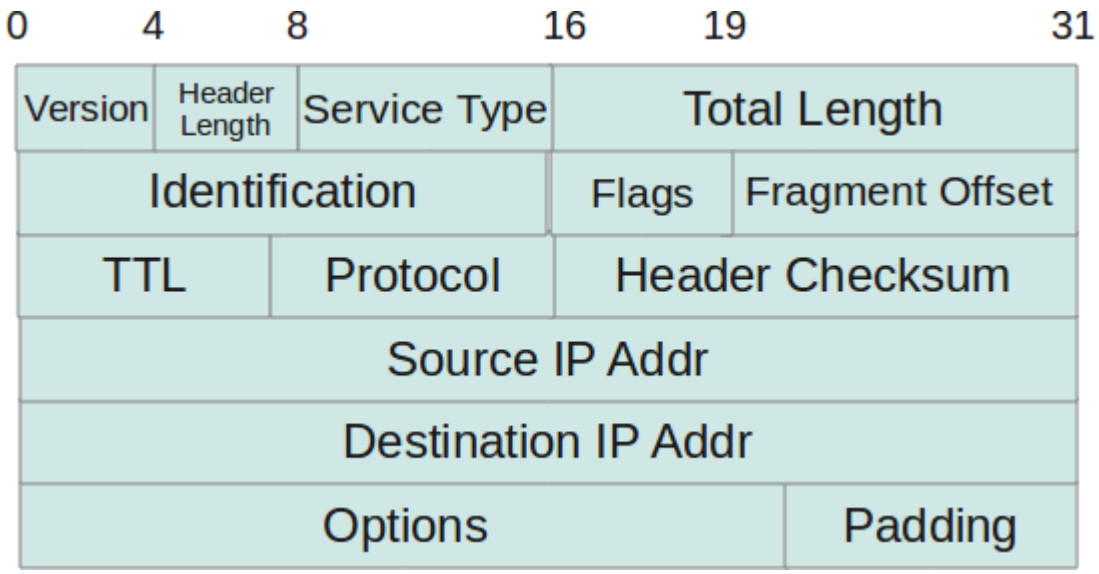
1.3 Protokol TPC/IP

Protokoly TCP/IP boli pôvodne vyvinuté ako súčasť výskumnej siete ARPANET. Táto pôvodná sieť, bola navrhnutá na používanie množstva protokolov, ktoré boli upravené z existujúcich technológií. Sieť ARPANET však mala nedostatky, či už koncepčne alebo v praktických záležitostiach, ako je kapacita. Vývojári novej siete uznali, že pokusy o použitie týchto existujúcich protokolov môžu nakoniec viesť k problémom, pretože ARPANET sa zväčšil na väčšiu veľkosť a bol prispôsobený pre novšie použitie a aplikácie.

V roku 1973 sa začal vývoj plnohodnotného systému pracovných protokolov na internete pre ARPANET. Mnoho ľudí si neuvedomuje, že v počiatočných verziách tejto technológie existoval iba jeden hlavný protokol, TCP. Bol vytvorený pre program kontroly prenosu. Prvá verzia tohto predchodcu moderného protokolu TCP bola napísaná v roku 1973, potom bola revidovaná a formálne zdokumentovaná v dokumente RFC (Request for Comments) 675, Špecifikácia programu kontroly internetového prenosu, december 1974 [3].

1.4 IP Protokol

IP je protokol alebo súbor pravidiel na smerovanie a adresovanie paketov údajov, aby mohli cestovať po sieťach a doraziť na správne miesto určenia. Prenos dát cez internet je rozdelený na menšie časti ktoré sa nazývajú pakety. Informácie IP sú pripojené ku každému paketu a tieto informácie pomáhajú smerovačom odosielať pakety na správne miesto. Každému zariadeniu, ktoré sa pripája na internet, je pridelená adresa IP a ako sú pakety smerované na adresu IP, ktorá je k nim pripojená, prichádzajú údaje tam, kde je to potrebné [4].



Obr. 3 Hlavička internetového protokolu IPv4 [5].

Prvých 32 bitov hlavičky je označuje: IP verziu, dĺžku internetového záhlavia a dĺžku hlavičky, celková dĺžka paketu IP vrátane záhlavia v bajtoch. Pole typy služieb QoS (Quality of Service) označujú kvalitu služby. Vo väčšine sietí sa obsah tohto poľa ignoruje.

Ďalších 32 bitov sa používa, keď je potrebné fragmentovať paket IP. Stáva sa to, keď maximálna veľkosť paketu na sieťovom spojení nestačí na prenos paketu ako celku. Router rozdelí paket na menšie pakety a prijímajúci hostiteľ môže neskôr zostaviť pôvodný paket pomocou informácií v poliach identifikátora, vlajky a odsadenie fragmentov [5].

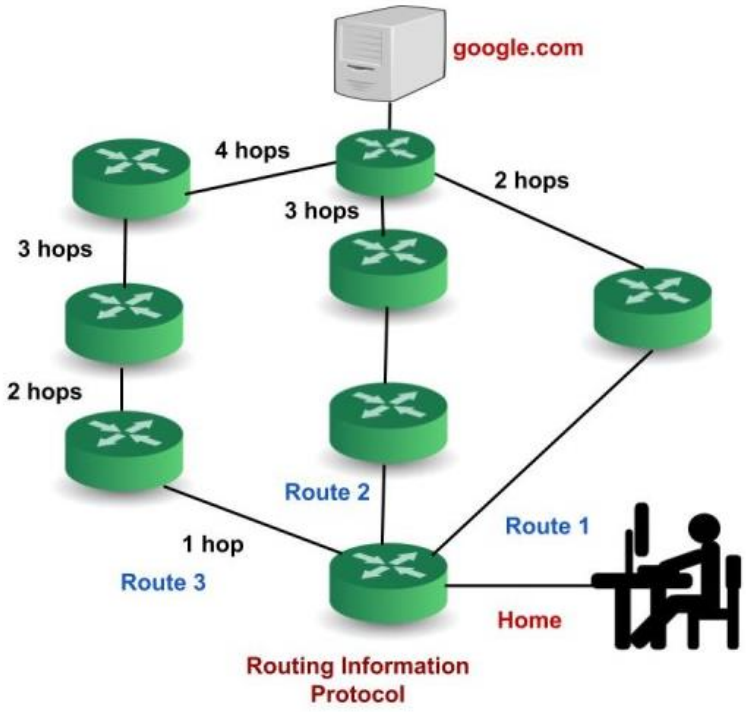
Prostredných 32 bitov obsahuje polia TTL (Time to Live), protokol a kontrolný súčet záhlavia. TTL je inicializovaný na dostatočne vysokej hodnote (zvyčajne 60) hostiteľským zdrojom a potom znižovaný každým smerovačom. Keď TTL dosiahne nulu, router vyhodí paket. Vykonáva sa tak preto, aby sa zabránilo tomu, aby pakety nezahltili sieť, keď existujú smerovacie slučky. V poli protokol sú uložené zvyčajne údaje TCP alebo UDP (User datagram Protocol) alebo riadiaca správa ICMP (Internet Control Message Protocol). Kontrolný súčet záhlavia sa používa na ochranu záhlavia pred neúmyselnými zmenami na ceste. Rovnako ako u všetkých kontrolných súčtov, prijímač vykoná výpočet kontrolného súčtu na základe prijatej informácie a ak je vypočítaný kontrolný súčet iný ako prijatý kontrolný súčet. Ak paket obsahuje neplatné informácie je vyradený. Posledné dve 32-bitové slová obsahujú adresu zdrojového systému, ktorý generoval paket, a cieľový systém, na ktorý je paket adresovaný.

Ak počas spracovania IP dôjde k chybám a systém zaznamenal chybu, odošle späť správu ICMP, aby informoval zdrojového hostiteľa o probléme.

1.5 Smerovací protokol

Smerovacia tabuľka musí preukázať skutočný spôsob, ako je všetko pripojené v danom čase vo sieťovej topológie. To znamená použitie protokolov dynamického smerovania, takže zmeny topológie, ako sú prerušenia káblov a zlyhané smerovače, sú okamžite zistené v celej sieti.

Jednoduchým smerovacím protokolom je smerovací informačný protokol RIP (Routing Information Protocol). Každá trasa v protokole RIP obsahuje, počet skokov, ktorý označuje vzdialenosť k cieľovej sieti. Smerovače majú možnosť vybrať najlepšiu cestu, keď dostanú viac trás do toho istého cieľa. Protokol RIP sa považuje za smerovací protokol vektorov vzdialenosti, pretože ukladá iba informácie o tom, kam posielať pakety pre určitý cieľ a koľko skokov je potrebných na to, aby sa tam dostali pričom overí najkrajšiu cestu [6].

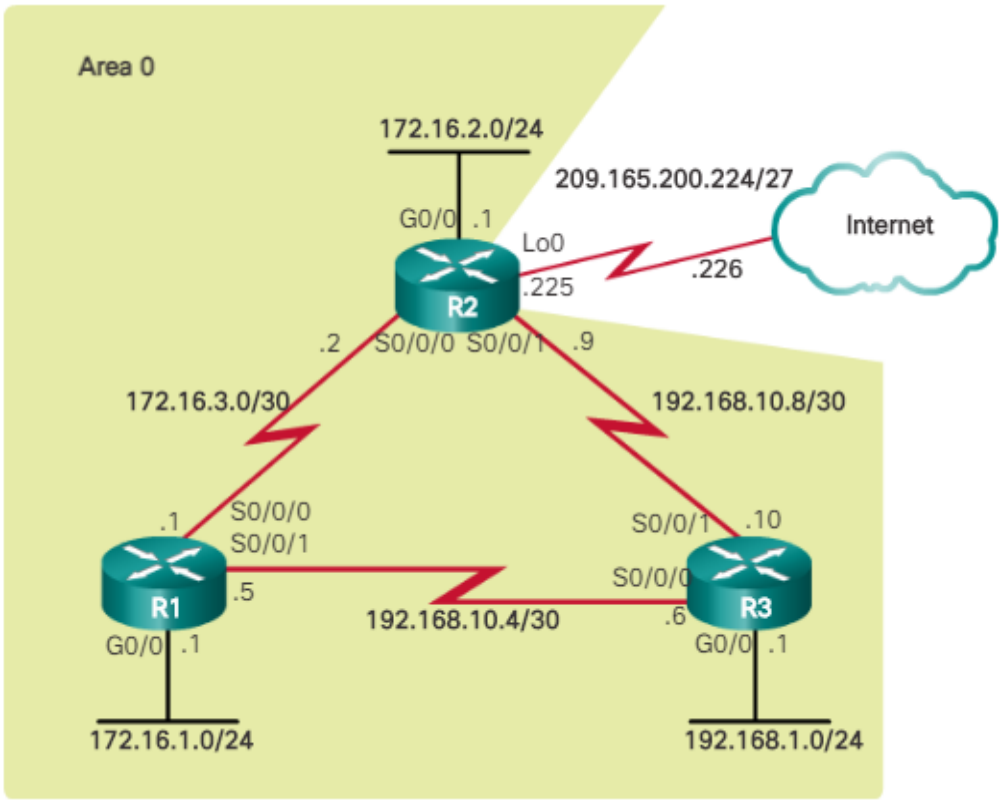


Obr. 4 Príklad počtu skokov protokolu RIP [6].

Namiesto pravidelného vysielania všetkých trás si OSPF (Open Shortest Path First) zachováva topologickú mapu siete a zasiela aktualizácie ostatným smerovačom v celej sieti iba vtedy, keď sa niečo zmení. Potom všetky smerovače prepočítajú mapu topológie pomocou

algoritmu SPF (Shortest Path First). Používa minimum prenosu smerovacieho protokolu, takže poskytuje lepší čas konvergencie.

Je zrejmé, že pravidelné vysielanie všetkých trás alebo uchovávanie informácií o topológii a o každom jednotlivom pripojení nie je možné realizovať v celom internete. Preto okrem protokolov vnútorného smerovania, ako sú RIP a OSPF na použitie v sieti jednej organizácie, sú potrebné aj externé protokoly na prenos informácií o smerovaní medzi organizáciami. Smerovače spájajúce jeden typ siete s druhým, boli nazývané brány v rodine smerovacích protokolov TCP / IP, takže zvyčajne hovoríme o protokoloch internej brány IGP (Interior Gateway Protocol) a protokole externej brány EGP (Exterior Gateway Protocol) [2].



Obr. 5 OSPF topológia [7].

1.6 Vývoj BGP protokolu

V roku 1984 bol protokol EGP bol formalizovaný v RFC 904. EGP ako smerovací protokol nie je príliš pokročilý. Nepodporuje napríklad topológiu so slučkami. Hlavným zámerom protokolu bolo pripojenie smerovačov ktoré boli pripojené k netransparentnej sieti a k zvyšku siete mali tieto ústredné brány informácie o dosiahnuteľnosti pre svoje systémy. EGP

vyžaduje stromovú štruktúru, v ktorej informácie tečú smerom nahor, v smere jadra alebo hlavnej sieti, alebo dole smerom k zbytku sieťam. Novinkou v EGP bola predstava rôznych smerovacích domén. V rámci ARPANET sa GGP (Gateway-to-Gateway Protocol) naďalej používal ako vnútorný protokol.

GGP je vo všeobecnosti podobný protokolu RIP v tom, že na určenie najlepších trás medzi zariadeniami používa algoritmus vektora vzdialenosti. GGP vyberie trasu s najkratším počtom preskokov.

V roku 1989 už nový protokol o hraničných susedoch už neumožňuje smerovačom nájsť susedov samostatne. Vyžadovalo ich manuálnu konfiguráciu a spustenie cez TCP. BGP (Border Gateway Protocol) Verzia 1, RFC 1105 stále mala predstavu o vzostupných, zostupných alebo horizontálnych vzťahoch, ako v prípade EGP. Toto obmedzenie bolo zrušené v BGP-2 (RFC 1163) spolu s hlavnými zmenami formátov správ. BGP-3 (RFC 1267) zaviedol okrem iného pole identifikátora BGP v otvorenej správe a definoval spôsob použitia tohto poľa na rozhodnutie, ktoré spojenie sa ukončí, keď dvaja susedia BGP iniciujú TCP reláciu súčasne. V roku 1994 BGP-4 (RFC 1654, neskôr RFC 1771) pridal CIDR (Classless Inter-Domain Routing), podporu agregácie, atribút lokálnej preferencie a dobu zadržania po pripojení.

Zatiaľ čo BGP bol ešte v začiatku vývoja, pracovalo sa na ešte zaujímavejšom prístupe k smerovaniu medzi doménami, na protokole IDPR (Inter-Domain Policy Routing) (RFC 1479). IDPR sa snaží pozerať na politiky zdrojovej a cieľovej siete a sietí medzi nimi, pokúša sa vyhovieť požiadavkám používateľov na určité služby a záruky QoS. Na rozdiel od BGP používa IDPR mechanizmus distribúcie prepojenia na distribúciu informácií o smerovaní. To umožňuje zdroju presnejšie uplatňovať svoje politiky. Za týmto účelom je všetka prevádzka tunelová. Tunelovanie skryje sieťovú vrstvu. S IDRP nie je problém pre poskytovateľa internetových služieb odosielať prenosy od jedného zákazníka cez jedno tranzitné spojenie a prenos od iného zákazníka cez iné tranzitné pripojenie, aj keď je cieľ v oboch prípadoch rovnaký. Poskytovateľ internetových služieb to môže spraviť, ak jeden tranzitný poskytovateľ internetových služieb ponúka oveľa lepšie služby, ale je tiež drahší. Jeden zákazník môže potrebovať lepšiu úroveň služieb, zatiaľ čo druhý nechce platiť príliš veľa.

V prípade BGP to nie je možné, pretože presmerovanie hop-by-hop zohľadňuje iba cieľovú adresu a dopravné toky, ktoré sa v určitom bode zišli, avšak sa nedajú neskôr oddeliť. Zdá sa, že IDPR stratil dynamiku skôr, ako sa mohol nasadiť. Hľadanie záruk QoS v IP bolo

vyzdvihnuté vývojom protokolu rezervácie zdrojov (RSVP, RFC 2205). RSVP neporušuje vzor hop-by-hop, ale namiesto toho používa iný prístup. Protokol umožňuje rezervovať zdroje na každom smerovači pozdĺž cesty, takže jednotlivé toky využívajú QoS ako normálne, hromadný prenos [2].

2 BGP PROTOKOL V SIETACH CISCO

BGP je smerovací protokol, ktorý sa najčastejšie používa medzi AS (Autonomous System) systémami. Je navrhnutý tak, aby fungoval cez spoľahlivý prepravný protokol. Používa na to ako transportný protokol TCP. Cieľovému portu TCP je pridelené 179 a miestnemu portu je pridelené náhodné číslo portu. Softvér Cisco podporuje verziu BGP 4 a túto verziu používali poskytovatelia internetových služieb ISP na pomoc pri budovaní Internetu. V RFC 1771 boli vysvetlené rady nových funkcií BGP, aby sa protokol mohol škálovať na použitie na internete. RFC 2858 zaviedla multi protokolové rozšírenia, ktoré umožnia BGP prenášať informácie o smerovaní pre IP multicastové trasy a viac rodín protokolov vrstvy 3, vrátane IPv4 (Internet Protocol version 4), IPv6 (Internet Protocol version 6) a CLNS (Connectionless-mode Network Service).

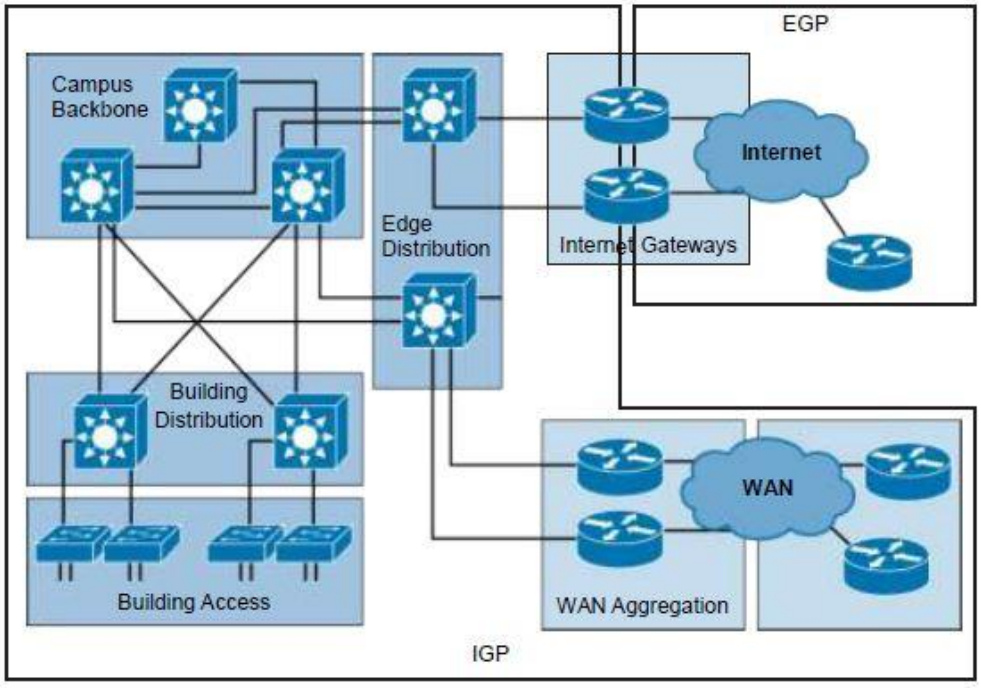
BGP sa používa hlavne na pripojenie miestnej siete k externej sieti na získanie prístupu na internet alebo na pripojenie k iným organizáciám. Pri pripájaní k externej organizácii sa vytvárajú externé peeringové relácie BGP, eBGP (External Border Gateway Protocol). Hoci sa BGP označuje ako protokol vonkajšej brány EGP, mnoho sietí v organizácii sa stáva tak zložitých, že BGP sa môže použiť na zjednodušenie vnútornej siete používanej v organizácii. Partneri BGP si v rámci tej istej organizácie vymieňajú informácie o smerovaní prostredníctvom interných peeringových relácií BGP, iBGP (lnternal Border Gateway Protocol).

BGP používa algoritmus smerovania vektorov cesty na výmenu informácií o dosiahnuteľnosti siete s ostatnými sieťovými zariadeniami ktoré komunikujú o BGP. Informácie o dosiahnuteľnosti siete sa vymieňajú medzi aktualizáciami smerovania členov BGP. Informácie o dosiahnuteľnosti siete obsahujú číslo siete, atribúty ktoré sú špecifické pre cestu a zoznam autonómnych systémových čísel, ktoré musí trasa dosiahnuť k cieľovej sieti. Tento zoznam je obsiahnutý v atribúte AS ceste. Algoritmus smerovania BGP cesta-vektor je a kombinácia algoritmu smerovania vzdialenosti vektora a detekcie slučky AS cesty [8].

2.1 Výmena smerovania BGP-IGP

AS predstavuje kolekciu sieťových zariadení pod spoločným správcom. Typickými príkladmi AS sú interná sieť podniku alebo sieťová infraštruktúra poskytovateľa internetových služieb. Protokoly smerovania sa dajú rozdeliť na základe toho, či si vymieňajú trasy v rámci AS alebo medzi rôznymi autonómnymi systémami:

- Protokoly vnútornej brány IGP: Používajú sa v organizácii a vymieňajú si trasy v rámci AS. Môžu podporovať malé, stredné a veľké organizácie, ale ich škálovateľnosť má svoje hranice. Protokoly môžu ponúknuť veľmi rýchlu konvergenciu a konfigurácia základných funkcií nie je zložitá. Najbežnejšie používanými IGP v podnikoch sú EIGRP a OSPF, rovnako ako RIP. V internej sieti poskytovateľa služieb sa bežne nachádza aj smerovací protokol s názvom IS-IS (Intermediate System-to-Intermediate System) [9].
- Protokoly vonkajšej brány EGP: Zabezpečujú výmenu trasy medzi rôznymi autonómnymi systémami. BGP je jediný EGP, ktorý sa dnes používa. Hlavnou funkciou BGP je výmena obrovského počtu trás medzi rôznymi autonómnymi systémami, ktoré sú súčasťou najväčšej siete, Internet.



Obr. 6 IGP vs BGP [9].

Existujú dva bežné spôsoby, ako vložiť trasy z IGP do BGP:

- Pomocou príkazu na redistribúciu
- Pomocou príkazu network

Trasy IGP môžu byť dynamicky pridané do BGP pomocou príkazu redistribute. Vždy by sa malo používať správne filtrovanie a sumarizáciu, aby sa znížilo možnému dopadu na nestabilitu IGP na BGP. Aj s týmito opatreniami dynamické prerozdeľovanie trás IGP na BGP sa nepodporuje kvôli svojej dynamickej povahe, a teda kvôli nedostatku administratívnej kontroly [9].

Príkaz network v BGP funguje odlišne od príkazu network IGP v softvéri Cisco IOS (Internetwork Operating System). Vo väčšine konfigurácií IGP sieťový príkaz viaže miestne rozhranie k smerovaciemu protokolu a pridá adresu rozhrania do IGP. S BGP príkaz network vytvorí trasu v tabuľke BGP, iba ak je už v smerovacej tabuľke IP adresa prítomná. To umožňuje, aby sa cesty IGP pridali do BGP semistaticky.

Redistribúcia trás BGP na IGP by sa mala používať iba s malou podskupinou internetových trás BGP alebo ak je malý počet trás BGP. Počas re distribúcie by sa malo nasadiť správne filtrovanie, aby sa minimalizoval počet prefixu v IGP [10].

2.2 Základy informačného smerovania

IP RIB (Routing Information Base) alebo smerovacia tabuľka IP je kritická databáza, ktorá poskytuje dôležité spojenie medzi riadiacou rovinou a dopravnou rovinou. Na jednej strane rôzne smerovacie zdroje, protokoly ako sú BGP a IS-IS, zaplňujú RIB svojimi cestami. Na druhej strane RIB poskytuje informácie na vytvorenie databázy preposielania. Niektoré metódy prepínania používajú RIB priamo na preposielanie.

Keď každý smerovací protokol prijíma aktualizácie a ďalšie informácie, vyberie najlepšiu cestu k danému cieľu a pokúsi sa nainštalovať túto cestu do smerovacej tabuľky. Ak existuje rovnaká cesta pre ten istý prefix, smerovač rozhodne, či trasy nainštaluje na základe administratívnych vzdialeností zahrnutých protokolov. IOS má preddefinované, ale konfigurovateľné administratívne vzdialenosti pre rôzne smerovacie protokoly, zdroje. Preferovaný je prefix zo smerovacieho zdroja, ktorý má menšiu administratívnu vzdialenosť.

IP RIB je organizovaný ako zbierka blokov sieťového deskriptora NDB (Network Descriptor Block). Každý NDB má jeden záznam v smerovacej tabuľke a predstavuje sieťovú predponu získanú prostredníctvom jedného z troch zdrojov:

- Adresy, masky nakonfigurované na lokálnom rozhraní smerovača. Stane sa z toho pripojená trasa, ktorá má najvyššiu preferenciu, administratívna vzdialenosť 0.

- Statická trasa nakonfigurovaná na smerovači. Statická trasa má predvolenú administratívnu vzdialenosť 1.
- Dynamický smerovací protokol, napríklad BGP.

NDB obsahuje informácie o sieťovej adrese, maske a administratívnej vzdialenosti, ako aj informácie potrebné na fungovanie protokolov dynamického smerovania, ako je napríklad re distribúcia trasy. Pretože každá predpona v NDB môže byť potenciálne dosiahnutá viacerými cestami, používajú sa aj bloky RDB (Routing Descriptor Blocks). S každou NDB môže byť spojená jedna alebo viac RDB na ukladanie skutočných informácií o nasledujúcom skoku. NDB v súčasnosti môže mať až osem RDB, ktoré nastavujú hornú hranicu počtu odkazov zdieľaných na zaťaženie miesta. Pretože NDB sú riadené jednotlivými smerovacími protokolmi, smerovacie protokoly určujú, koľko RDB sa má priradiť k NDB.

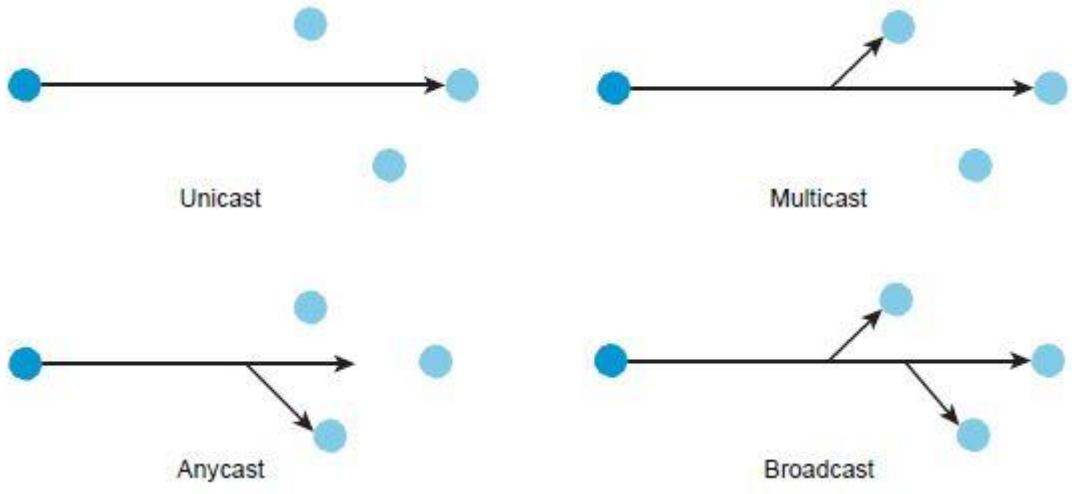
Databáza preposielania paketov je vytvorená na základe informácií obsiahnutých v tabuľke IP RIB a IP ARP (Address Resolution Protocol). V RIB sa vykonáva vyhľadávanie predpony, aby sa určila adresa nasledujúceho skoku a výstupné rozhranie. Skutočná hlavička L2 vrstvy je postavená na základe informácií z tabuľky IP ARP. Rámové relé a mapy ATM sú ďalšie príklady, ktoré sa používajú na mapovanie adries L3 vrstvy na adresy L2. Softvér Cisco IOS podporuje dva všeobecné typy vyhľadávacích operácií RIB:

- Classless - Vyhľadá sa najdlhší zhodný prefix. Ak nenájde zodpovedajúci prefix, použije sa predvolená trasa, ak je k dispozícii. IP Classless lookup je predvolené (aj keď sa stále zobrazuje v spustenej konfigurácii) od vydania softvéru Cisco IOS Release 11.3
- Classful - vyhľadávanie s najdlhšou zhodou. Supernety a predvolená trasa sa nezohľadňujú, ak smerovacia tabuľka obsahuje podsieť veľkej cieľovej sieti [10].

2.3 Typy prenosov

Použitím špecifického typu cieľovej adresy IP môže zariadenie vysielať prenos jednému príjemcovi, vybraným príjemcom alebo všetkým zariadeniam v rámci podsiete súčasne. Protokoly smerovania používajú rôzne typy prenosu na riadenie spôsobu výmeny informácií o smerovaní. Výber cieľovej adresy IP podľa rôznych typov adries umožňuje zariadeniu odoslať rôzne typy prenosu:

- Unicast: Unicast adresa je adresa, ktorá identifikuje jedinečný uzol v sieti. Komunikácia unicast sa vymieňa iba medzi jedným odosielateľom a jedným príjemcom. Zdrojové adresy môžu byť iba unicast adresy.
- Multicast: Multicastové adresy označujú skupinu rozhraní medzi rôznymi zariadeniami. Prenos, ktorý sa odosiela na adresu multicast, sa odosiela súčasne do viacerých cieľov. Rozhranie môže patriť do ľubovoľného počtu skupinových vysielacích skupín. V IPv4 je vyhradený rozsah adresného priestoru pre adresy multicast 224.0.0.0 až 239.255.255.255. Rezervované multicastové adresy IPv6 majú predponu FF00 :: / 8.
- Anycast: Anycast adresa je priradená rozhraniu na viac ako jednom uzle. Keď sa paket odošle na adresu anycast, presmeruje sa na najbližšie rozhranie, ktoré má túto adresu. Najbližšie rozhranie sa nájde podľa miery vzdialenosti konkrétneho smerovacieho protokolu. Všetky uzly, ktoré zdieľajú rovnakú adresu, by sa mali správať rovnako, aby sa služba ponúkala podobne bez ohľadu na uzol, ktorý obsluhuje požiadavku. Bežným prípadom použitia pre server anycast je internetový server DNS. Na celom svete existuje niekoľko inštancií toho istého servera a server anycast vám umožňuje dosiahnuť najbližší server jednoducho pomocou cieľovej adresy anycast.
- Broadcast: IPv4 vysielacie adresy sa používajú pri odosielaní prenosu na všetky zariadenia v podsieti. Informácie sa prenášajú z jedného odosielateľa do všetkých pripojených prijímačov. Adresa miestneho vysielania 255.255.255.255 sa používa, keď chcete komunikovať so všetkými zariadeniami v miestnej sieti. Cielená vysielacia adresa, ktorá je poslednou adresou IPv4 v každej sieti, umožňuje zariadeniu osloviť všetky zariadenia vo vzdialenej sieti. IPv6 nepoužíva vysielaciu adresu, ale namiesto toho používa adresy multicast [11].



Obr. 7 Štyri rôzne typy prenosov [11].

Protokoly včasného smerovania sa používali iba na prenos informácií o smerovaní. Vysielanie správ obsahujúcich smerovacie aktualizácie zbytočne využívalo iné zariadenia, ktoré boli pripojené k rovnakej sieti, pretože každé zariadenie muselo spracovať vysielacie pakety, kedy boli prijaté. Všetky moderné IGP používajú adresy multicast na zisťovanie susedov, výmenu informácií o smerovaní a zasielanie aktualizácií.

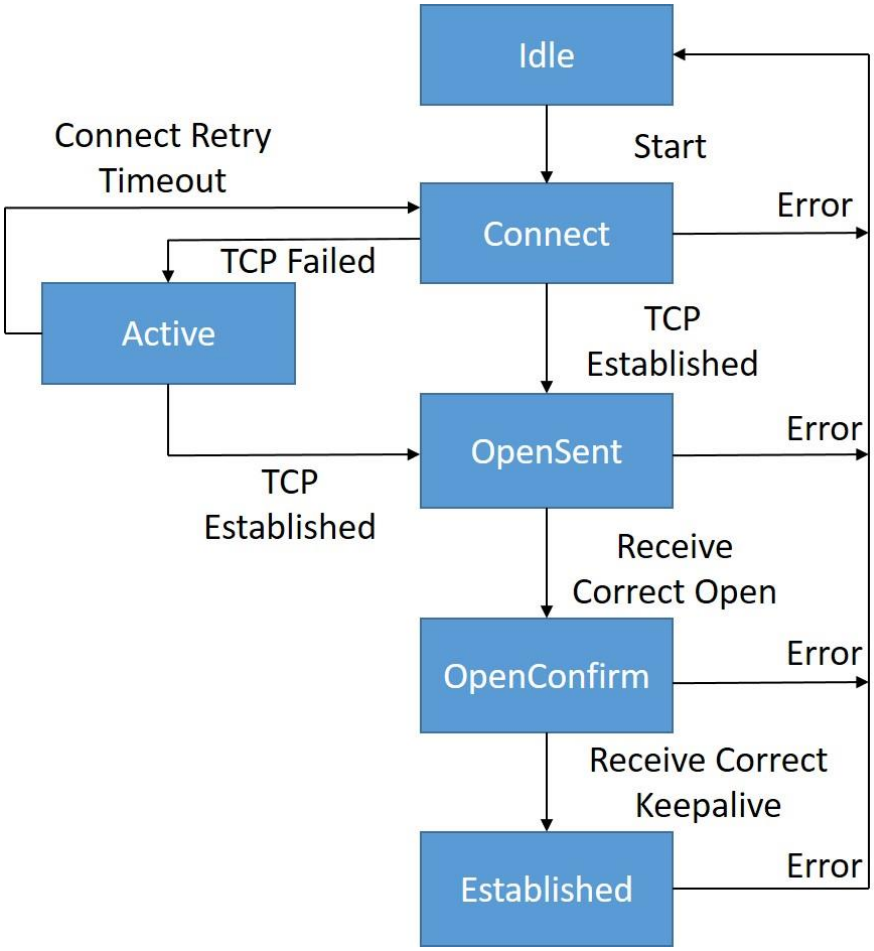
2.4 Vzťahy partnerov v BGP

Keď proces smerovania BGP vytvorí reláciu prenosu, prechádza nasledujúcim stavom zmeny:

- Idle: Počiatočný stav, do ktorého smerovací proces BGP vstupuje, keď je aktivovaný smerovací proces alebo keď je zariadenie resetované. V tomto stave zariadenie čaká na štartovaciu udalosť, napríklad na konfiguráciu rovného so vzdialeným rovnocenným. Keď zariadenie prijme žiadosť o pripojenie TCP od vzdialeného partnera, zariadenie iniciuje ďalšiu udalosť spustenia, aby počkalo na časovač, a až potom začne pripojenie TCP na vzdialený partner.
- Connect - Proces smerovania BGP zistí, že partner sa pokúša vytvoriť reláciu TCP s lokálnym partnerom BGP.
- Active - V tomto stave sa proces smerovania BGP pokúsi nadviazať reláciu TCP s rovnocenným zariadením pomocou časovača ConnectRetry. Počas procesu smero-

vania BGP je aktívny stav ignorovania. Ak proces smerovania BGP je prekonfigurovaný alebo ak sa vyskytne chyba, proces smerovania BGP uvoľní systémové prostriedky a vráti sa do nečinného stavu.

- OpenSent - Je nadviazané pripojenie TCP a proces smerovania BGP odošle správu otvorené do vzdialeného partnera a prejde do stavu otvoreného odosielania. Ak pripojenie zlyhá, proces smerovania BGP prejde do aktívneho stavu.
- OpenConfirm - Proces smerovania BGP prijíma správu zahájený a čaká na počiatočnú správu Keepalive zo vzdialeného partnera. Ak je prijatá oznamovacia správa, proces smerovania BGP prejde do stavu nečinnosti. Ak dôjde k chybe alebo zmene konfigurácie, ktorá má vplyv na reláciu rovnocenného procesu smerovania, BGP odošle správu s upozornením a chybovým kódom stroja konečných stavov FSM (Finite-State Machine) a potom prejde do nečinného stavu.
- Established - Počiatočný udržiavací príkaz je prijatý od vzdialeného partnera. Teraz je nadviazaný rovnocenný prenos so vzdialeným susedom a BGP začína výmenu aktualizačnej správy so vzdialeným partnerom. Časovač pozastavenia sa reštartuje po prijatí aktualizačnej alebo udržiavacej správy. Ak proces BGP dostane oznámenie o chybe, prejde do stavu nečinnosti.



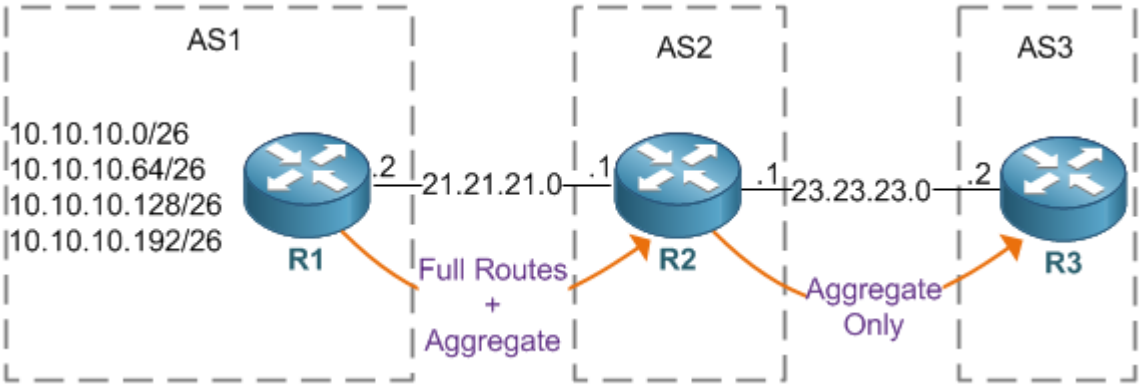
Obr. 8 Stavový stroj BGP [12].

2.5 Agregácie trasy BGP

BGP si ukladajú a vymieňajú smerovacie informácie a množstvo smerovacích informácií. Množstvo sa zvyšuje, keď je nakonfigurovaných viac zástupcov BGP. Použitie agregácie trás znižuje množstvo zahrnutých informácií. Agregácia je proces kombinovania atribútov niekoľkých rôznych trás, kde sa inzeruje iba jedna trasa. Agregované predpony používajú zásadu smerovania beztriedneho CIDR. Spôsobí to kombinovanie susedných sietí bez IP adries v smerovacích tabuľkách, kde je možné ich zhrnúť. Teraz je za potreby inzerovať menej trás.

Na implementáciu agregácie trasy, sú k dispozícii dve metódy. Môžete distribuovať agregovanú trasu do BGP alebo môžete použiť formu podmienenej agregácie. Základné prerozdeľovanie trás zahŕňa vytvorenie súhrnnej trasy a potom prerozdelenie trás do BGP. Podmie-

nená agregácia zahŕňa vytvorenie súhrnnej trasy a potom propagujú alebo potlačenie inzeruje určité trás na základe, informácií autonómnych systémových nastavení trás AS-SET alebo súhrnných informácií. Proces smerovania BGP môže v predvolenom nastavení propagovať trasy, ktoré nie sú nainštalované v databáze smerovacích informácií RIB do počítačov BGP. Trasa, ktorá nie je nainštalovaná v RIB, je neaktívnou trasou. Neaktívna inzercia trasy sa môže vyskytnúť napríklad vtedy, keď sa trasy inzerujú prostredníctvom spoločnej agregácii. Neaktívnu inzerciu trasy možno potlačiť, na konzistentné odovzdávanie údajov.



Obr. 9 Agregovaná BGP adresa pomocou komunít [13].

2.6 Politika riadenia zmien smerovania

Politiky smerovania pre peer zahŕňajú všetky konfigurácie prvkov, ako sú mapa trasy, distribučný zoznam, zoznam predpôn a zoznam filtrov, ktoré môžu mať vplyv na aktualizácie prichádzajúcich alebo odchádzajúcich smerovacích tabuliek. Vždy, keď dôjde k zmene v politike smerovania, relácia BGP musí byť vymazaná alebo obnovená, aby nová politika nadobudla účinnosť. Vykonanie resetovania prichádzajúcich zásielok umožňuje, aby sa uplatnili nové zásady prichádzajúcich údajov nakonfigurované v zariadení. Vykonanie odchádzajúcich resetov spôsobí, že nové miestne politiky odchádzajúcich nakonfigurované v zariadení sa prejavia bez resetovania relácie BGP. Keď sa počas resetovania odchádzajúcej politiky odošle nová sada aktualizácií, môže sa uplatniť aj nová prichádzajúca politika suseda. To znamená, že po zmene prichádzajúcej politiky musíte vykonať miestne resetovanie alebo miestne nastavenie resetovať na partnerskom zariadení. Zmeny odchádzajúcich zmien vyžadujú odchádzajúci reset na miestnom zariadení alebo prichádzajúci reset na rovnocennom zariadení [8].

Typy Resetu	Výhody	Nevýhody
Hard reset	Žiadna réžia pamäte	Prefix v tabuľkách BGP, IP a FIB (Forwarding Information Base) poskytnuté susedom sa stratia.
Odchádzajúci soft reset	Žiadna konfigurácia a žiadne ukladanie aktualizácii smerovacích tabuliek.	Neresetuje aktualizácie prichádzajúcich smerovacích tabuliek.
Dynamický vstupný soft reset	Nevymaže reláciu a vyrovnávaciu pamäť BGP. Nevyžaduje sa ukladanie aktualizácii smerovacích tabuliek a nemá žiadnu réžiu pamäte.	Obe zariadenia BGP musia podporovať schopnosť obnovenia trasy. **Poznámka**: Neresetuje aktualizácie odchádzajúcich smerovacích tabuliek.
Konfigurovaný prichádzajúci soft reset. Používa príkaz: **neighbor soft-reconfiguration**	Môže sa použiť, keď obe zariadenia BGP nepodporujú funkciu automatického obnovovania trasy. Príkaz bgp soft-reconfig-backup slúži na konfiguráciu prichádzajúcej soft rekonfigu-rácie pre rovnocenné zariadenia, ktoré ne-podporujú schopnosť obnovenia trasy.	Vyžaduje predkonfiguráciu. Uloží všetky prijaté (prichádzajúce) aktuali-zácie smerovacích poli-tík bez úprav. Je nároč-ný na pamäť.

Obr. 10 Výhody a nevýhody hard a soft resetov.

Následne po definovaní dvoch susedných zariadení, sa vytvorí spojenie BGP a zariadenia si vymenia informácie o smerovaní. Ak následne zmeníte filter, váhu, vzdialenosť, verziu alebo časovač BGP, alebo ak urobíte podobnú zmenu konfigurácie, musíte obnoviť spojenie BGP. Až potom sa zmena konfigurácie prejaví.

Soft reset resetuje smerovaciu tabuľku pre prichádzajúce a odchádzajúce smerovanie aktualizácie. Softvér Cisco podporuje mäkký reset bez predchádzajúcej konfigurácie. Tento mäkký reset umožňuje dynamickú výmenu požiadaviek na obnovenie trasy a smerovacích informácií medzi zariadeniami BGP a umožňuje následné čítanie príslušnej odchádzajúcej smerovacej tabuľky.

Existujú dva typy soft resetu:

- Ak sa soft reset používa na generovanie prichádzajúcich aktualizácií od suseda, nazýva sa to dynamický vstupný soft reset.
- Ak sa soft reset používa na odoslanie novej sady aktualizácií susedovi, nazýva sa odchádzajúci soft reset.

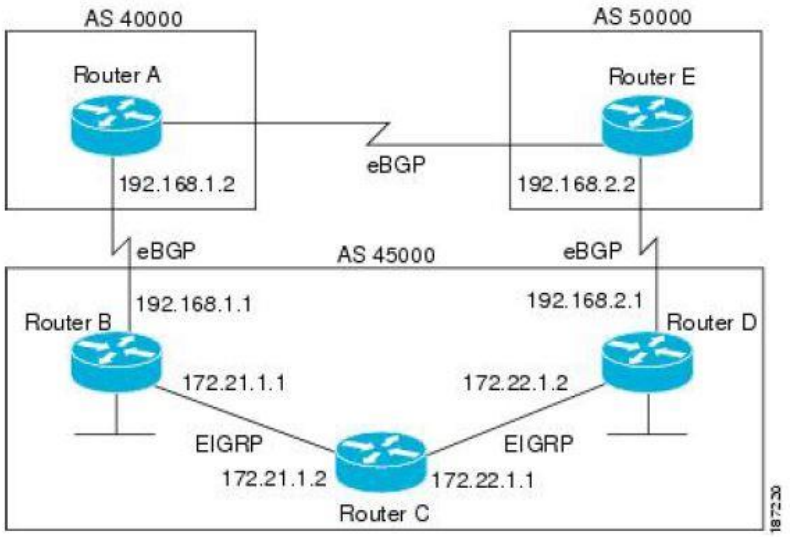
Ak chcete použiť mäkký reset bez konfigurácie, obaja partneri BGP musia podporovať schopnosť obnovenia soft trás, ktorá je inzerovaná v správe OPEN, odoslanej, keď partneri vytvoria reláciu TCP.

2.7 Skupiny BGP partnerov

V BGP sieti je často veľa susedov nakonfigurovaných s rovnakými aktualizačnými politikami, to znamená rovnaké odchádzajúce mapy trás, distribuované zoznamy, zoznamy filtrov, zdroj aktualizácií. Susedia s rovnakými aktualizačnými politikami môžu byť zoskupení do rovnocenných BGP skupín, aby sa zjednodušila konfigurácia a čo je dôležitejšie, aby sa aktualizácie stali efektívnejšími. Ak máte veľa partnerov, tento prístup sa dôrazne odporúča.

2.8 Zadné trasy BGP

V topológii siete BGP s dvoma hraničnými zariadeniami, ktoré používajú eBGP na komunikáciu s celým radom rôznych autonómnych systémov, nemusí byť použitie eBGP na komunikáciu medzi dvoma hraničnými zariadeniami najúčinnejšou metódou smerovania.



Obr. 11 Topológia zadných trás [8].

Na obrázku je smerovač B ako reproduktor BGP prijímať trasu do smerovača D cez eBGP. Táto trasa bude prechádzať najmenej dvoma autonómnymi systémami. Smerovač B a smerovač D sú tiež pripojený prostredníctvom siete EIGRP (Enhanced Interior Gateway Routing Protocol). Táto trasa má kratšiu cestu. Trasy EIGRP však majú predvolenú administratívnu vzdialenosť 90 a trasy eBGP majú predvolenú administratívnu vzdialenosť 20, takže BGP bude uprednostňovať trasu eBGP. Zmena predvolených administratívnych vzdialeností sa neodporúča, pretože zmena administratívnej vzdialenosti môže viesť k smerovacím slučkám. Ak chcete, aby program BGP uprednostnil trasu EIGRP, môžete použiť príkaz sieťového zadných tras. BGP považuje sieť zadanú príkazom: network backdoor za lokálne priradenú sieť, s výnimkou že nebude inzerovať určenú sieť v aktualizáciách BGP. Na obrázku to znamená, že smerovač B bude komunikovať so smerovačom D pomocou kratšej trasy EIGRP namiesto dlhšej trasy eBGP [8].

3 KOMUNIKÁCIA BGP PROTOKOLU

BGP je poštová služba na internete. Keď niekto vloží list do poštovej schránky, poštová služba danú časť pošty spracuje a zvolí rýchlu a efektívnu cestu na doručenie tohto listu príjemcovi. Podobne, keď niekto odosiela údaje cez internet, BGP je zodpovedná za prezeranie všetkých dostupných trás, po ktorých môžu údaje cestovať, a za výber najlepšej trasy, čo obvykle znamená preskakovanie medzi autonómnymi systémami. BGP je protokol, ktorý umožňuje fungovanie internetu. Robí to povolením smerovania údajov na internete. Keď používateľ v Singapure načíta web s pôvodnými servermi v Argentíne, BGP je protokol, ktorý umožňuje rýchlu a efektívnu komunikáciu [14].

3.1 Autonómne systémy BPG

Keď poskytovateľ internetových služieb ISP získa sieť, ktorá patrí do iného autonómneho systému AS, neexistuje žiadny bezproblémový spôsob presunu rovnocenných aplikácií BGP získanej siete do AS nadobúdajúceho ISP. Proces konfigurácie BGP kolegov s novým číslom AS môže byť časovo náročný a ťažkopádny. Zákazníci niekedy nechcú alebo nemôžu okamžite upraviť svoje vzájomné usporiadanie alebo konfiguráciu. Počas tohto druhu prechodného obdobia môže byť užitočné nakonfigurovať zariadenia s povoleným BGP v novom AS, aby sa v aktualizáciách BGP používalo pôvodné číslo AS. Toto predchádzajúce číslo AS sa nazýva miestne AS .

Použitie miestneho čísla AS umožňuje smerovacím zariadeniam v získanej sieti, aby vyzerali, že patria bývalému AS [15].

3.2 Implementácia EIGRP

EIGRP je pokročilý vektorový smerovací protokol navrhnutý spoločnosťou Cisco. Základná konfigurácia je jednoduchá a ľahko zrozumiteľná, preto sa bežne používa v menších sieťach. Jeho pokročilé funkcie, ktoré poskytujú rýchlu konvergenciu, vyššiu škálovateľnosť a podporu viacerých smerovaných protokolov, spĺňajú požiadavky v zložitých sieťových prostrediach. EIGRP podporuje IPv4 aj IPv6. Aj keď sa štandardná konfigurácia EIGRP medzi IPv4 a IPv6 líši, je možné ju zjednotiť pomocou novo zavedeného konfiguračného režimu EIGRP.

3.2.1 Vytvorenie susedských vzťahov EIGRP

EIGRP bol vyvinutý ako vylepšená verzia staršieho protokolu IGRP (Internal Gateway Routing Protocol) a má mnoho rovnakých vlastností ako pokročilý protokol IGP, napríklad vysokorýchlostná konvergencia, čiastočné aktualizácie a možnosť podpory viacerých sieťových vrstiev. Prvým krokom pri konfigurácii EIGRP je nadviazanie susedských vzťahov EIGRP v rôznych typoch rozhraní. Je dôležité vedieť ako ich overiť, či boli správne formované ich parametre, ako sú časovače Hello a Hold a rôzne technológie WAN, ktoré ovplyvňujú vytvorenie relácie.

3.2.2 Funkcie EIGRP

Medzi kľúčové funkcie, ktoré odlišujú EIGRP od ostatných smerovacích protokolov, patrí rýchla konvergencia, podpora maskovania podsietí s premenlivou dĺžkou VLSM (Variable-Length Subnet Mask), čiastočné aktualizácie a podpora protokolov viacerých sieťových vrstiev. Základný popis návrhu protokolu a architektúry bol uverejnený ako informačný RFC, ktorý umožňuje spoločnosti Cisco zachovať si kontrolu nad EIGRP a skúsenosťami so zákazníkmi a zároveň ju otvoriť iným dodávateľom na podporu prevádzkyschopnosti.

EIGRP je patentovaný protokol spoločnosti Cisco, ktorý kombinuje výhody protokolov smerovania stavu spojenia a vektorového smerovania vzdialenosti. EIGRP je však vektorový smerovací protokol. Obsahuje pokročilé funkcie, ktoré sa nenachádzajú v iných protokoloch vektorovej vzdialenosti, ako je RIP. Preto sa tento protokol označuje ako protokol vektora smerovania pokročilej vzdialenosti. Rovnako ako jeho predchodca IGRP, aj EIGRP sa ľahko konfiguruje a je prispôsobiteľný širokému spektru sieťových topológií. Čo robí EIGRP pokročilým vektorovým protokolom na diaľku, je pridanie niekoľkých funkcií nájdených v protokoloch o stave spojenia, ako je napríklad zistenie dynamického suseda. EIGRP je vylepšený IGRP z dôvodu jeho rýchlej konvergencie a záruky topológie bez slučiek za všetkých okolností. Medzi vlastnosti tohto protokolu patrí:

- **Rýchla konvergencia**: EIGRP používa difúzny aktualizačný algoritmus DUAL (Diffusing update algorithm) na dosiahnutie rýchlej konvergencie. Router so systémom EIGRP ukladá smerovacie tabuľky susedov, aby sa mohol rýchlo prispôsobiť zmenám v sieti. Ak v lokálnej smerovacej tabuľke neexistuje vhodná cesta a v topologickej tabuľke neexistuje vhodná záložná cesta, EIGRP požiada svojich susedov o nájdenie alternatívnej trasy. Tieto dotazy sa šíria, kým sa nenájde alternatívna cesta alebo kým sa nestanoví, že neexistuje iná alternatíva trasa.

- **Čiastočne aktualizácie**: EIGRP posiela skôr čiastočné spustené aktualizácie než pravidelné aktualizácie. Tieto aktualizácie sa odosielajú iba vtedy, keď sa zmení cesta alebo metrika trasy. Obsahujú informácie iba o tom, že sa zmenil odkaz, a nie o celej smerovacej tabuľke. Propagácia týchto čiastkových aktualizácií je automaticky ohraničená tak, aby sa aktualizovali iba tie smerovače, ktoré tieto informácie požadujú. Výsledkom je, že EIGRP spotrebuje podstatne menšiu šírku pásma ako IGRP. Toto správanie sa líši aj od link – state protokolu, ktorý odošle aktualizáciu zmien do všetkých smerovačov v oblasti.

- **Podpora viacerých sieťových vrstiev**: EIGRP podporuje IPv4 a IPv6 závislých modulov, ktoré sú zodpovedné za protokol požiadavky špecifické pre sieťovú vrstvu. Rýchla implementácia a sofistikovaná metrika EIGRP ponúkajú vynikajúci výkon a stabilitu pri implementácii v sieťach IPv4 a IPv6.

- **Použitie multicast a unicast**: Pri komunikácii medzi smerovačmi sa používa EIGRP vysielanie multicast a unicast. Výsledkom je, že koncové stanice nie sú ovplyvnené smerovaním aktualizácií alebo dopytov. Multicastová adresa použitá pre EIGRP pre IPv4 je 224.0.0.10 a multicastová adresa pre EIGRP pre IPv6 je FF00 :: A.

- **Podpora VLSM**: EIGRP je smerovací protokol bez tried, čo znamená, že inzeruje masku podsiete pre každú cieľovú sieť. To umožňuje EIGRP podporovať diskontinuálne podsiete a VLSM.

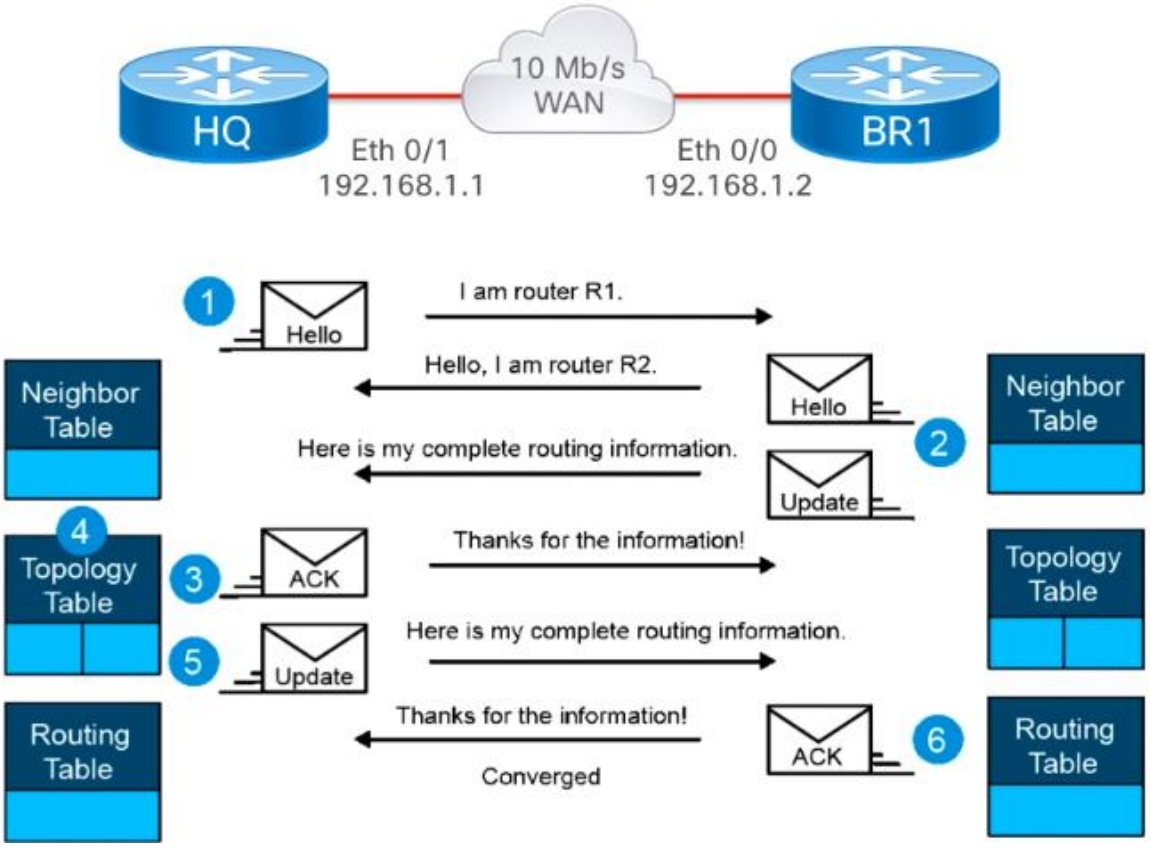
- **Bezproblémové pripojenie vo všetkých protokoloch a topológiách vrstvy dátového spojenia**: EIGRP nevyžaduje špeciálnu konfiguráciu na prácu so všetkými protokolmi 2. vrstvy. Iné smerovacie protokoly napríklad protokol OSPF, vyžadujú rôzne konfigurácie pre rôzne protokoly 2. vrstvy, ako napríklad Ethernet a Frame Relay. EIGRP bol navrhnutý tak, aby efektívne pracoval v prostrediach LAN (Local area network) aj WAN. Podpora siete WAN (Wide Area Network) pre vyhradené spojenia point-to-point a NBMA (non-broadcast multiple access) topológie sú štan-

dardom. EIGRP prispôsobuje rozdiely v typoch médií a rýchlostiach. Keď sa susediace spojenia vytvárajú cez spojenia WAN, môžu byť nakonfigurované tak, aby obmedzovali šírku pásma, ktorú protokol používa na pripojenia WAN siete.

- **Sofistikovaná metrika:** EIGRP predstavuje metrické hodnoty v 32-bitovom formáte na zabezpečenie dostatočnej diskrétnosti. EIGRP podporuje nerovnomerné vyvažovanie metrických záťaží, čo správcom umožňuje efektívnejšie rozdeľovať toky prenosu v ich sieťach [16].

3.2.3 Prehľad prevádzky EIGRP

Činnosť protokolu EIGRP je založený na informáciách uložených v troch tabuľkách: Susednej tabuľke, topologickej tabuľke a smerovacej tabuľke. Hlavnou informáciou uloženou v susednej tabuľke je skupina susedov, s ktorými smerovač EIGRP nadviazal spojenie. Pre susedov je charakteristická ich primárna IP adresa a priamo k nim pripojené rozhranie. Tabuľka topológie obsahuje všetky cieľové trasy inzerované susednými smerovačmi. Každý záznam v topologickej tabuľke je spojený so zoznamom susedov, ktorí inzerovali cieľ. Pre každého suseda sa zaznamenáva inzerovaná metrika. To je metrika, ktorú sused ukladá vo svojej smerovacej tabuľke na dosiahnutie konkrétneho cieľa. Ďalšou dôležitou informáciou je metrika, ktorú smerovač používa na dosiahnutie toho istého cieľa. Toto je súčet inzerovanej metriky od suseda plus náklady na prepojenie so susedom. Trasa s najlepšou metrikou k cieľu sa nazýva nástupca a je umiestnená v smerovacej tabuľke a inzerovaná ostatným susedom. Proces vytvárania a objavovania susedných trás prebieha súčasne s EIGRP.



Obr. 12 Prehľad prevádzky EIGRP [16].

Postup prenosu s použitím topológie:

1. Nový smerovač R1 príde na odkaz a pošle paket „Hello“ cez všetky svoje rozhrania nakonfigurované v EIGRP.
2. Smerovače, ktoré prijímajú paket „Hello“ (R2) na jednom rozhraní, odpovedajú aktualizačnými paketmi, ktoré obsahujú všetky trasy, ktoré majú vo svojich smerovacích tabuľkách, s výnimkou tých, ktoré sa naučili cez toto rozhranie (rozdelený horizont). R2 odošle aktualizačný paket do R1, ale susedský vzťah sa nestanoví, kým R2 neodošle ahoj paket do R1. Aktualizačný paket z R2 má inicializačný bit nastavený, čo naznačuje, že toto je inicializačný proces. Aktualizačný paket obsahuje informácie o trasách, ktoré pozná sused (R2), vrátane metriky, ktorú sused inzeruje pre každý cieľ.
3. Potom, čo si obe smerovače vymenili požiadavky a susedská susednosť bola nadviazaná, R1 odpovie na R2 paketom ACK, čo naznačuje, že prijala aktualizačné informácie.

4. R1 prispôsobí všetky aktualizačné pakety vo svojej topologickej tabuľke. Tabuľka topológie obsahuje všetky ciele inzerované susednými susednými smerovačmi. Uvádza zoznam všetkých cieľov, všetkých susedov, ktorí môžu dosiahnuť cieľ, a ich priradené metrický.
5. R1 odošle aktualizačný paket do R2.
6. Po prijatí aktualizačného paketu R2 pošle paket ACK do R1.

4 ROZŠÍRENIE BGP PROTOKOLU

Zdieľanie zaťaženia BGP Multipath Load Sharing pre eBGP a iBGP, umožňuje konfigurovať vyrovnávanie zaťaženia viacerých ciest pomocou externých ciest eBGP a interných BGP iBGP, v sieťach BGP, ktoré sú nakonfigurované na používanie protokolu MPLS (Multiprotocol Label Switching). Táto funkcia poskytuje vylepšené možnosti rozloženia záťaže a ponúkania služieb a je užitočná pre viacčlenné autonómne systémy a smerovače PE (Provider Edge), ktoré importujú cesty eBGP a iBGP z sietí s viacerými doménami a sub sietí.

4.1 Obmedzenia záťaže BGP s viacerými cestami v VPN-MPLS

- Podpora druhu adries

  Táto funkcia je nakonfigurovaná na základe VPN (Virtual Private Network) smerovania a preposielania VRF (Virtual Routing and Forwarding). Túto funkciu je možné nakonfigurovať iba v rámci rodiny adries IPv4 VRF.

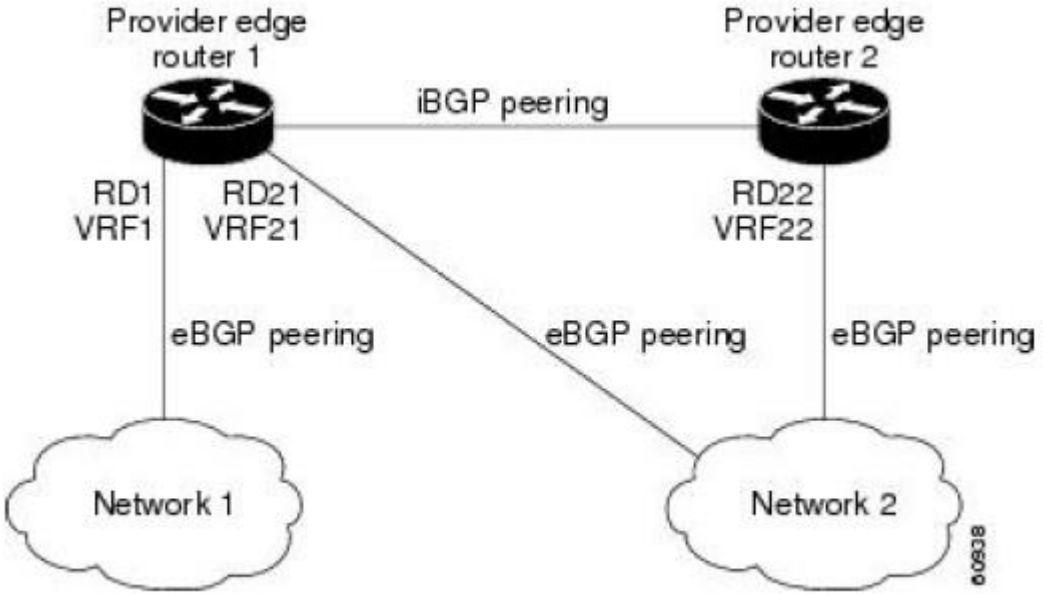
- Obmedzenie spotreby pamäte

  Každý záznam tabuľky smerovania viacerých ciest BGP použije ďalšiu pamäť. Je odporúčané, aby sa táto funkcia nepoužívala na smerovači s malým množstvom dostupnej pamäte a najmä ak smerovač obsahuje úplné smerovacie tabuľky na internete.

- Obmedzenie zrkadlových trás

  Ak je vo smerovacej tabuľke nainštalovaných viac ciest iBGP, odzrkadlené trasy budú propagovať iba jednu cestu. Ak má smerovač za odzrkadlenými trasami, všetky smerovače, ktoré sú pripojené k lokalitám s viacerými adresami, nebudú inzerované, pokiaľ pre každý VRF nie je nakonfigurovaný iný rozlišovač trasy.

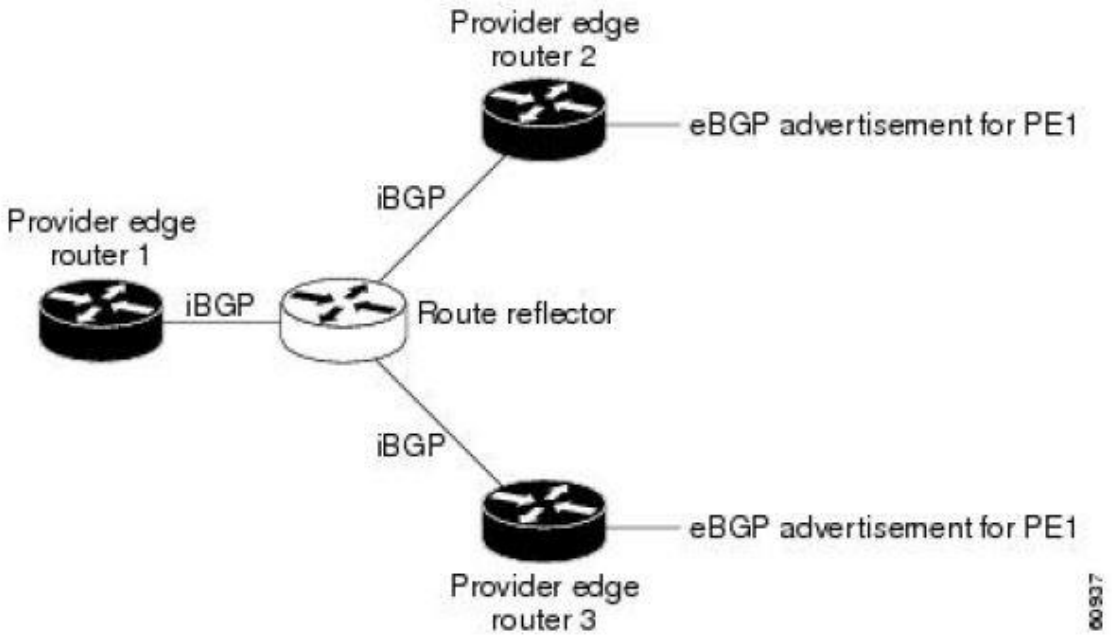
4.1.1 Záťaž eBGP a iBGP s viacerými cestami v sieti BGP MPLS



Obr. 13 Sieť poskytovateľa služieb BGP MPLS [8].

Smerovač 1 je možné nakonfigurovať pomocou zdieľania záťaže BGP pre viaceré cesty pre eBGP a iBGP vo funkcii VPN MPLS. Cesty iBGP a eBGP môžu byť vybrané ako multipathy a importované do VRF Network 1. CEF (Cisco Express Forwarding) použije viacnásobné cesty na vyrovnanie záťaže. IP adresa ktorá sa odosiela z Network 2 na smerovači 1. Smerovač 2, sa bude odosielať cez cesty eBGP. IP adresa, ktorá sa odosiela cez cestu iBGP, sa odosiela ako prenos MPLS a prenos MPLS, ktorý sa odosiela cez cestu eBGP, sa odošle ako prenos IP. Akýkoľvek prefix, ktorý je inzerovaný z Network 2, bude prijatý smerovačom 1 cez rozlišovač trasy RD (Route distinguisher) 21 a RD 22. Oznámenie cez RD 21 bude prenášaný v IP pakete a oznámenie prostredníctvom RD 22 bude prenášaný v MPLS pakete. Obe cesty môžu byť vybrané ako viaccestné pre VRF 1 a nainštalované do VRF 1 RIB.

4.1.2 Záťaž eBGP a iBGP s viacerými cestami pomocou zrkadlových tras



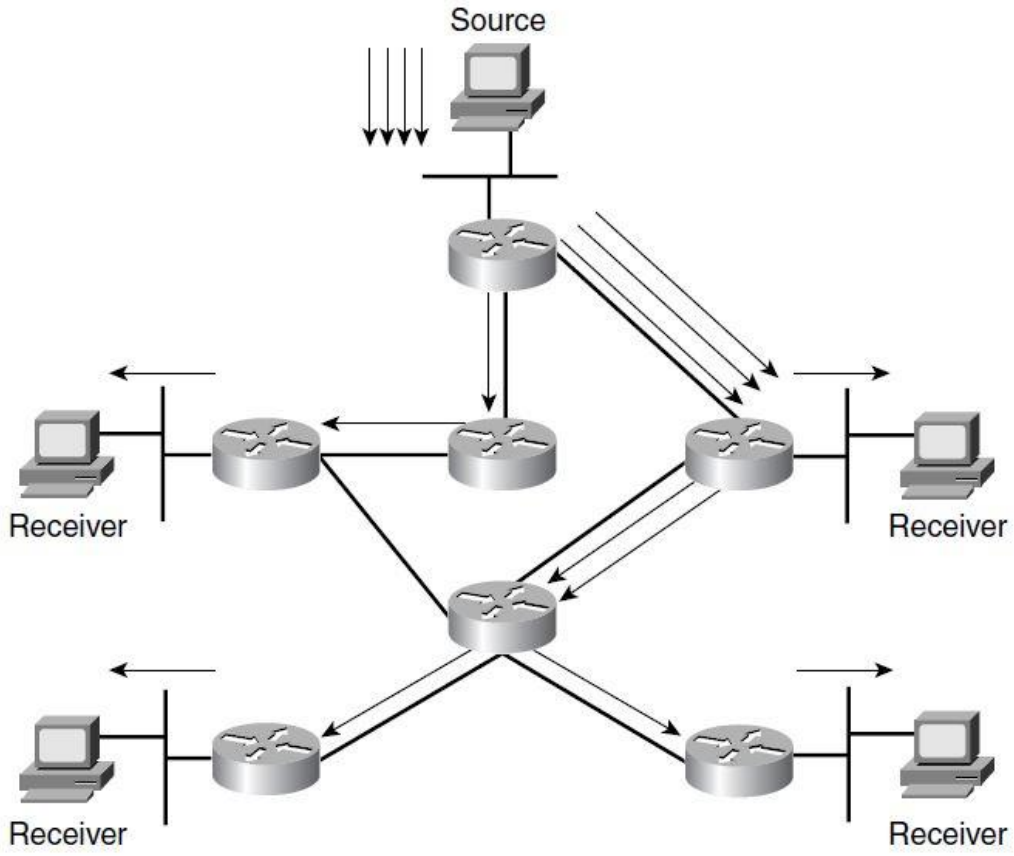
Obr. 14 Topológia so zrkadlovou trasy [8].

Obrázok zobrazuje topológiu, ktorá obsahuje tri smerovače a zrkadlovú trasu. Všetko je nakonfigurované na rovnocenné iBGP. Smerovač 2 a smerovač 3 propaguje rovnako preferovanú cestu eBGP k smerovaču 1. V predvolenom nastavení si zrkadlová trasa vyberie iba jednu cestu a inzeruje smerovač 1.

Aby sa všetky rovnaké cesty preferencií k smerovaču 1 inzerovali prostredníctvom zrkadlenia trasy, je dôležité nakonfigurovať každý VRF s iným RD. Prefix prijatý zrkadlením trasy sa rozpozná odlišne a inzeruje sa na smerovači 1 [8].

4.2 Rozšírenie IP multicast

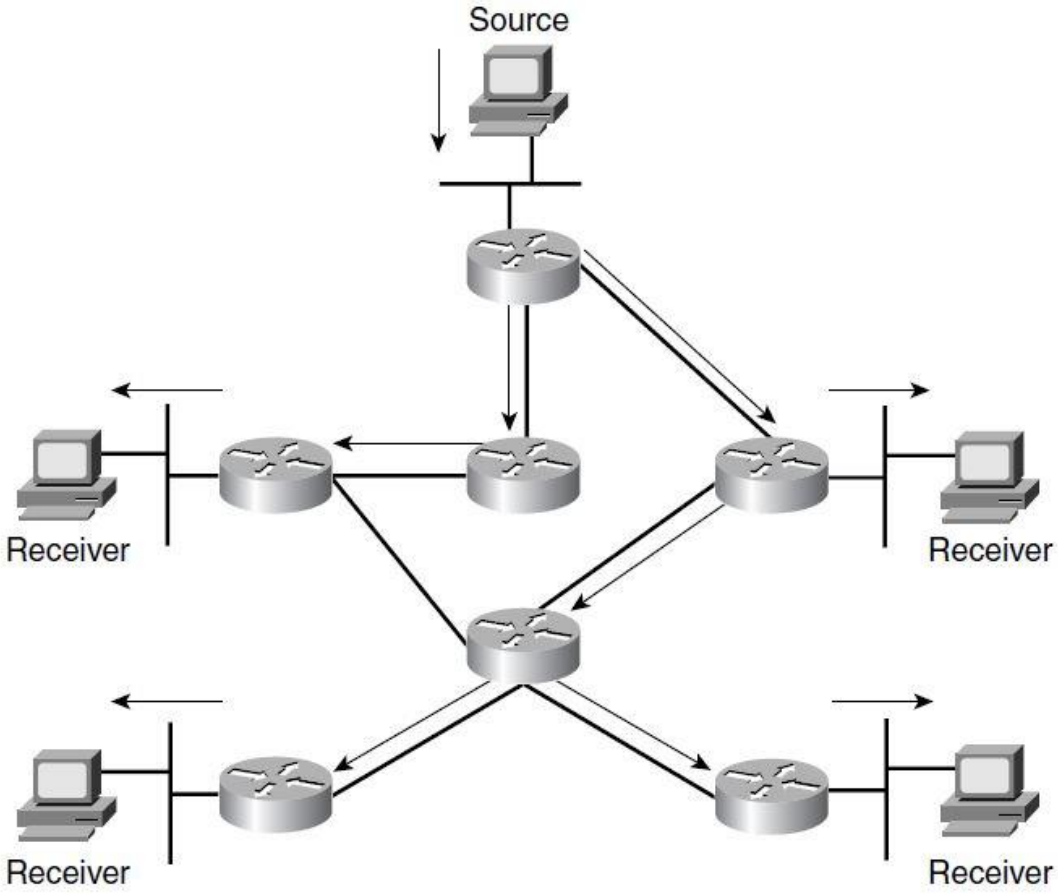
Tradičným modelom dodávania údajov pre počítačové siete sú jednosmerné prenosové toky. Tento model má jediný prijímač pre dátový tok. Tento spôsob doručovania údajov funguje veľmi dobre pre mnoho druhov komunikácie, ako sú webové stránky a e-mail. S inou triedou komunikácie však tento model poskytovania údajov čelí vážnym problémom so škálovaním. Príkladom tejto triedy komunikácie je streamovanie v reálnom čase alebo živé multimediálne vysielanie. Neefektívny obrazec prevádzky vedie k lineárnemu zvýšeniu prenosu v sieti pre každý ďalší prijímač, ktorý sa pripája k dátovému toku. Túto neefektívnosť možno vyriešiť implementáciou distribučných stromov multicastu.



Obr. 15 Neúčinnosť modelu jednosmerného doručovania [8].

4.2.1 Multicastové distribučné trasy

Koncepcia multicastu IP spočíva v tom, že vysielacie zdroje a poslucháči tvoria skupinu. Spanning tree spájajúci všetkých prijímačov, ktorý používajú zdroj ako root, používa iný distribučný model ako jednosmerové prenosy. V každej vetve stromu sa údaje replikujú a preposielajú v každej vetve. Použitie stromu rozosielania multicast MDT (Multicast Distribution Tree) vedie k významnému zníženiu prenosu údajov a rieši problém mierkového rastu lineárneho prenosu v sieti. Samotný zdroj je povinný poslať iba jeden tok, ktorý sa replikuje v každej vetve distribučného stromu. Tento proces rozdeľuje záťaž generovania dodatočných dát a optimalizuje umiestnenie replikácie dát jeho presunom čo najbližšie k prijímaču. To neznamená, že doručovanie založené na výberovom vysielaní nemá žiadne problémy so škálovaním. Hlavnými problémami sú fan-out a replikácia paketov.



Obr. 16 Efektivita modelu multicastového doručovania [8].

4.3 Podpora BGP pre IPv6

Vývoj IPv6 je vývojovým krokom od IPv4. Posledných 20 rokov vyšlo najavo niekoľko oblastí, ktoré je potrebné zlepšiť. Protokol IPv6 je vo väčšine aspektov veľmi podobný protokolu IPv4. Vylepšenia sa dajú rozdeliť do nasledujúcich všeobecných kategórií:

- Rozšírené adresovanie
- Automatická konfigurácia
- Zjednodušenie hlavičky
- Bezpečnosť
- QoS

V IPv4 sú adresy dlhé 32 bitov. To vytvára potenciál pre približne 4,2 miliardy adries. Kombinácia faktorov však viedla k významnej neefektívnosti vo využívaní adresy:

- Dimenzovanie podsiete
- Pridelenie aktuálnej adresy
- Klasické nasadenia
- Jedna osmina adresného priestoru je vyhradená triedou E, alebo je určená na multicast

4.3.1 Možnosti automatickej konfigurácie

Protokol IPv6 umožňuje hostiteľovi automaticky sa nakonfigurovať s globálne smerovacou adresou. Možnosti automatickej konfigurácie zahŕňajú použitie protokolu ICMPv6 (Internet Control Message Protocol version 6) na určenie miestnej podsiete. Hostiteľ potom automaticky nakonfiguruje 64-bitovú časť adresy, nazývanú identifikátor rozhrania, aby vytvoril jedinečnú adresu, ktorú je možné globálne smerovať.

4.3.2 Vylepšenie zabezpečenia

IPv4 neobsahuje zabudovanú autentifikáciu ani šifrovanie údajov. Protokol IPv4 poskytuje možnosť zahrnúť informácie z kontrolného súčtu, ktoré umožňujú overenie integrity údajov. Schopnosť šifrovania užitočného zaťaženia je riadená nad sieťovou vrstvou.

IPv6 poskytuje autentifikačnú hlavičku AH (Authentication Header) na vykonávanie autentifikácie s použitím IPSec (Internet Protocol Security) na šifrovanie údajov pomocou hlavičky zapuzdrenia bezpečnostného užitočného zaťaženia ESP (Encapsulating Security Payload). Hlavička ESP môže tiež poskytovať autentifikáciu, čím odstraňuje potrebu AH aj hlavičku ESP pri šifrovaní a autentifikácii. Schopnosť poskytovať šifrovanie založené na IPSec sa vyžaduje pre hostiteľov s podporou IPv6. Schopnosť vykonať kontrolný súčet je udržiavaná na transportnej vrstve pomocou TCP alebo UDP. Poskytuje overenie, šifrovanie a overenie integrity údajov.

4.4 Rozšírenia pre podporu CLNS

Používanie BGP sa rozšírilo aj za prostredie IP. Schopnosť spoločnostiam využívať BGP a efektívne spravovať veľké množstvo informácií o smerovaní sa dá využiť kdekoľvek inde. Primárny príklad toho, kde je možné využívať BGP, je v prostredí dátovej komunikačnej siete DCN (Data Communications Network). DCN je sieť pre správu sieťových prvkov synchrónnej optickej siete SONET (Synchronous Optical Network) a synchrónnej digitálnej hierarchie SDH (Synchronous Digital Hierarchy) NE (Network Elements). Sieťová služba

bez pripojenia CLNS (Connectionless-mode Network Service) sa používa na správu NE s metódou prístupu k prenosu súborov FTAM (File Transfer Access Method) a protokolom CMIP (Common Management Interface Protocol).

4.4.1 Škálovateľnosť DCN

Hlavnou výzvou škálovateľnosti, ktorej čelia siete IP, je množstvo informácií o prefixe, ktoré sa musia inzerovať. To platí aj pre prostredie DCN. Počet uzlov v sieti však vytvoril ďalšie obmedzenia. Sieť prostredia DCN sa skladá zo sieťových prvkov SONET alebo SDH, odložených multiplexorov ADM (Add/Drop Multiplexer). Počet NE v jednom krúžku SONET / SDH je v priemere okolo 10, ale môže sa pohybovať od 3 do 40. Typický DCN môže mať viac ako tisíc zvonení, čo vedie k desiatkam tisíc NE. To by nepredstavovalo problém, s výnimkou toho, že každý NE pôsobí ako prechodný systém IS (Intermediate System) a nie ako koncový systém ES (End System).

Kruhy SONET majú riadiaci kanál, nazývaný dátový komunikačný kanál DCC (Data Communications Channel), ktorý sa používa na odosielanie riadiacich správ medzi sieťovými prvkami. Tento riadiaci kanál má šírku pásma 192 kb/s.

4.4.2 Návrh siete DCN založený na BGP

Implementácia podpory CLNS v BGP sa spolieha na TCP, nie na TP4 (Transport Protocol 4), aby sa zabezpečilo pripojenie transportnej vrstvy. Rovnajúce sa relácie sú vytvárané medzi IP adresami, nie prístupovými bodmi k sieťovým službám NSAP (Network Service Access Point address). Tým sa zvyšuje zložitosť, pokiaľ ide o ďalší skok BGP pre NSAP. Tiež sa vyžaduje zavedenie IP do siete, aby sa mohli vytvoriť relácie TCP pre BGP [10].

5 ZABEZPEČENIE BGP PROTOKOLU

Zatiaľ čo sa používanie BGP na poskytovanie služieb v rámci autonómneho systému zvýšilo, zostáva protokolom na výmenu medzi trasami AS, preto musí BGP bežať na smerovačoch, ktoré sú na konci autonómneho systému alebo administratívnej domény. Miesto, kde sa autonómny systém pripája externe, sa často považuje za bezpečnostný obvod. Bez ohľadu na to, či je týmto externým pripojením zákazník, partnerský partner, poskytovateľ obsahu alebo čokoľvek iné, zabezpečenie tohto obvodu proti potenciálnym hrozbám alebo útokom má prvoradý význam. V súčasnosti sa na vykonávanie bezpečnostných opatrení na internete používa celý rad mechanizmov.

5.1 FlowSpec

Špecifikácia toku BGP (FlowSpec) umožňuje kódovanie informácií o špecifikácii toku do protokolu BGP NLRI (Network Layer Reachability Information) s viacerými protokolmi. Špecifikácia toku, ktorá sa skladá z niekoľkých zhodných kritérií, ako je zdrojový prefix, cieľový prefix, protokol alebo porty, ktoré sa môžu použiť na prenos IP triedy C. Spolu s informáciami o špecifikácii prúdov NLRI, rozšírené atribúty Spoločenstva poskytujú schopnosť definovať pravidlá pre obchodovanie so špecifikáciami prúdenia.

Zámerom je umožniť automatizované vytvorenie filtrov IP na zabránenie útokom DDoS (Distributed Denial of Service) v rámci AS a medzi AS a umožniť presmerovanie prenosu do iných kontextov smerovania za účelom potlačenia čistiacich zariadení. Špecifikácie toku sú určené na to, aby boli presnejšie smerovacie záznamy do unicast agregovaného prefixu, ktorý existuje v smerovacej tabuľke. Agregovaný prefix unicast môže prijať skupina a má sa nainštalovať sa do RIB / FIB, ale špecifikačné pravidlo môže potom prijať iná skupina, ktorá definuje špecifickejšie pravidlá toku, čo vedie k odlišnému správaniu vpred pre túto podmnožinu dopravy.

Ak sa identifikuje prenos pomocou identifikácie NLRI, je ďalším krokom vykonanie akcie pri tomto prenose. Komunita s rozšírenými obchodnými sadzbami obsahuje dvojbajtové číslo AS nasledované štyrmi bajtmi na určenie rýchlosti v bytoch za sekundu (vo formáte Fluteating Point IEEE). Miera nula sa používa na určenie akcie prerušenia a je jedinou sadzbou podporovanou v systéme SR-OS (Service Router Operating System). Spoločenstvo rozšírené o obchodné činnosti pozostáva zo šiestich bajtov, z ktorých sú v súčasnosti definované iba dva najmenej významné bity posledného bajtu. Bit „Terminal Action“ alebo „T“, ak je

nastavený na 1, predstavuje akciu „next-entry“. Ak je tento bit nastavený na nulu, hodnotenie obchodného filtra sa zastaví, keď sa použije toto pravidlo. Bit „Vzorka“ alebo „S“, ak je nastavený na 1, umožňuje prenos vzoriek a protokolovanie údajov pre túto špecifikáciu toku. Rozšírené komunity triedy Presmerovanie na VRF a Mark Traffic sú samovysvetľujúce, pričom na definovanie cieľového presmerovania VRF sa používa hodnota Route Target [17].

5.2 Podpora BGP pre kontrolu zabezpečenia TTL

Keď je funkcia TTL Security Check implementovaná pre BGP, predstavuje ľahký bezpečnostný mechanizmus na ochranu susedských relácií eBGP pred útokmi založenými na využití CPU (Central Processing Unit). Tieto typy útokov sú zvyčajne útoky typu DoS (Denial of Service), ktoré sa snažia vypnúť sieť zaplavením siete paketmi IP, ktoré obsahujú kované zdrojové a cieľové adresy IP.

Funkcia kontroly bezpečnosti TTL chráni reláciu susedstva eBGP porovnaním hodnoty v poli TTL prijatých paketov IP proti počtu skokov, ktorý je nakonfigurovaný lokálne pre každú susednú reláciu eBGP. Ak je hodnota v poli TTL prichádzajúceho IP paketu väčšia alebo rovná lokálne nakonfigurovanej hodnote, paket IP sa akceptuje a normálne spracuje. Ak je hodnota TTL v pakete IP menšia ako lokálne nakonfigurovaná hodnota, paket je ticho zahodený a negeneruje sa žiadna správa ICMP.

Aj keď je možné sfalšovať pole TTL v záhlaví paketu IP, nie je možné presne falšovať počet TTL, aby sa zhodoval s počtom TTL od dôveryhodného partnera, pokiaľ nebola narušená sieť, do ktorej dôveryhodný partner patrí. Funkcia kontroly zabezpečenia TTL podporuje priamo prepojené relácie susedov a susedné relácie eBGP vo viacnásobnom skoku obchodu. Relácia susedov BGP nie je ovplyvnená prichádzajúcimi paketmi, ktoré obsahujú neplatné hodnoty TTL. Relácia susedov BGP zostane otvorená a smerovač ticho zahodí neplatný paket. Relácia BGP však stále môže vypršať, ak sa pakety s udržiavacou frekvenciou nedostanú skôr, ako vyprší časovač relácie.

5.2.1 TTL Kontrola bezpečnosti susedných relácií BGP

Funkcia podpory BGP pre kontrolu zabezpečenia TTL je nakonfigurovaná pomocou príkazu neighbor ttl-security v konfiguračnom režime smerovača alebo v konfiguračnom režime rodiny adries. Ak je táto funkcia povolená, BGP vytvorí alebo udržiava reláciu, iba ak je hodnota TTL v hlavičke paketu IP rovnaká alebo väčšia ako hodnota TTL nakonfigurovaná pre reláciu peeringu. Povolenie tejto funkcie zabezpečí reláciu eBGP iba v prichádzajúcom

smere a nemá žiadny vplyv na odchádzajúce pakety IP alebo vzdialený smerovač. Argument počtu skokov sa používa na konfiguráciu maximálneho počtu skokov, ktorý oddeľuje dvoch susedov. Hodnota TTL je určená smerovačom z nakonfigurovaného počtu skokov. Hodnota tohto argumentu je číslo od 1 do 254.

5.2.2 Podpora kontroly TTL pre susedné relácie Multihop BGP

Funkcia podpory BGP pre kontrolu zabezpečenia TTL podporuje priamo pripojené relácie susedov aj relácie viacerých obchodov susedov. Ak je táto funkcia nakonfigurovaná pre reláciu suseda viacerých obchodov príkazom na konfiguráciu smerovača susedov: ebgp-multihop, nie je možné nakonfigurovať a na vytvorenie suseda nie je potrebný.

Tieto príkazy sa vzájomne vylučujú a na vytvorenie viacnásobného susedského spojenia je potrebný iba jeden príkaz. Ak sa pokúsite nakonfigurovať oba príkazy pre rovnakú reláciu, na konzole sa zobrazí chybové hlásenie.

Ak chcete nakonfigurovať túto funkciu pre existujúcu reláciu viacerých skokov, musíte najprv zakázať existujúcu susedskú reláciu príkazom: ebgp-multihop bez susedov. Keď povolíte túto funkciu pomocou príkazu: neighbor ttl-security, obnoví sa relácia susedov.

Táto funkcia by mala byť nakonfigurovaná na každom zúčastnenom smerovači. Aby sa maximalizovala efektívnosť tejto funkcie, argument počtu impulzov by mal byť presne nakonfigurovaný tak, aby zodpovedal počtu skokov medzi lokálnou a externou sieťou. Pri konfigurácii tejto funkcie pre reláciu viacerých obchodov so susedmi by ste však mali zvážiť aj zmenu cesty.

5.2.3 Výhody podpory BGP pre kontrolu zabezpečenia TTL

Funkcia BGP Support for TTL Security Check poskytuje efektívne a ľahko nasaditeľné riešenie na ochranu susedských relácií eBGP pred útokmi založenými na využití CPU. Ak je táto funkcia povolená, hostiteľ nemôže zaútočiť na reláciu BGP, ak hostiteľ nie je členom miestnej alebo vzdialenej siete BGP alebo ak hostiteľ nie je priamo spojený so sieťovým segmentom medzi miestnymi a vzdialenými sieťami BGP. Toto riešenie výrazne znižuje účinnosť útokov DoS proti autonómnemu systému BGP [8].

5.3 „Bogonové“ adresy

Pojem „Bogon“ (podvod) sa vzťahuje na IP adresu, ktorú si IANA (Internet Assigned Numbers Authority) alebo iný internetový register vyhradil, ale ešte ich nepridelil.

Adresy, ktoré neboli pridelené legitímnym používateľom, by nikdy nemali byť smerované a pakety, ktoré z týchto adries pochádzajú, sú s najväčšou pravdepodobnosťou falšované. S rastúcim internetom sa však neustále prideľujú nové adresy, takže filtre bogonových adries sa musia neustále aktualizovať. Ak tak neurobíte, môžu sa segmenty siete stať nedostupnými. V roku 2004 boli niektoré stránky na Novom Zélande zablokované, pretože používali adresy v rozsahu 222.x.x.x. Mnoho poskytovateľov internetových služieb považovalo tieto adresy za nepriradené, a preto neplatné, pretože nedokázali náležite aktualizovať svoj zoznam filtrov bogónov pomocou nedávno pridelených adries IP z APNIC (Asia Pacific Network Information Centre), autorizovaného registra pre novozélandský región.

Filtrovanie bogonových adries môže mať významný vplyv na bezpečnosť. Jedna štúdia zistila, že bogonové adresy sa použili ako zdrojové adresy IP pre viac ako 60% paketov, ktoré buď porušili pravidlá kontroly prístupu alebo detekcia narušenia. Ich odfiltrovanie má teda dvojaký vplyv na bezpečnosť:

- odstránenie paketov, ktoré môžu byť škodlivé
- zníženie zaťaženia systémov detekcie narušenia.

Existujú dva prístupy k zmierneniu šírenia a používania bogonových adries v smerovaní BGP: filtrovanie trasy a odhadzovanie paketov. Pretože adresy sa nepretržite prideľujú s pridávaním nových uzlov na internet, odporúča sa používať automatizované procesy na udržiavanie zoznamov bogonových adries na filtrovanie alebo vyradenie.

5.4 Pokyny na filtrovanie IPv4

Filtrovanie paketov odosielaných do smerovačov BGP a z nich je dôležitou súčasťou správy bezpečnosti pre BGP. Aktualizácie trasy môžu byť filtrované na základe atribútov trasy, cesty alebo komunity a filtre môžu byť navrhnuté tak, aby zakázali zadané predpony a predávali iné, alebo odovzdávali zadané predpony a odmietali ostatné. O použitej metóde sa môže rozhodnúť správca systému na základe požiadaviek na konfiguráciu a politiku. Táto časť sa zaoberá všeobecne prijatými postupmi uverejnenými v NISCC BGP (The National Infrastructure Security Co-ordination Centre).

1. Zakázať špeciálne predpony pridelené a vyhradené na budúce použitie - vyhradené predpony sa odložia a nepoužívajú na smerovanie. Napríklad 192.168.0.0/16 je určený na použitie v miestnej sieti, takže externý partner BGP by nikdy nemal mať túto IP adresu.

2. Zakázať nepridelené miesto (sivé / bogonové) - Nepriradené adresy neboli nikomu pridelené, a preto by nemali byť aktívne. Partner BGP s nepridelenou adresou je anomália, ktorá naznačuje buď chybu konfigurácie, alebo škodlivú aktivitu.
3. Zakázať nadmerne špecifické predpony - BGP znižuje objem aktualizačných správ konsolidáciou prefixu. Príliš špecifické prefixe spôsobujú veľké zvýšenie počtu správ vymieňaných medzi rovesníkmi. Odporúčania sa líšia, pokiaľ ide o to, ktoré prefixe by sa mali považovať za „príliš špecifické“, ale primeraným kritériom by mohli byť odporúčania s adresami prefixov v rozsahu / 25 - / 30.
4. Ak je to možné, súhrnné trasy - Trasy sa zhromažďujú pomocou kratšej predpony na kombinovanie viacerých adries. Napríklad 36.0.0.0/7 sa môže použiť namiesto 36.0.0.0/8 a 37.0.0.0/8, pretože sedem bitov binárneho 36 s vysokým poradím (0010 0100) je rovnakých ako sedem bitov s vysokým poradím pre binárne 37 (0010 0101). Agregácia adries šetrí miesto vo smerovacích tabuľkách a znižuje počet správ BGP, ktoré sa musia vymieňať.
5. Zakázať predvoľby výmenného bodu - Tieto predpony zahŕňajú predpony peeringovej siete AS, ktoré sú pripojené prostredníctvom výmenného bodu. Tie by nemali do svojho IGP alebo eBGP zavádzať blok adresy LAN výmenného bodu. Okrem toho, ak neoznámite predpony výmenných bodov, útočník bude ťažšie odosielať spoofing pakety medzi vzdialenými bodmi.
6. Zakázať trasy do interných priestorov IP - Interné adresy IP, ako napríklad adresy za sieťou NAT, by sa nikdy nemali vnímať ako prichádzajúce od externého partnera, a preto by sa mali zamietnuť.

5.5 Podpis MD5

Hashovací algoritmus MD5 (Message-Digest algorithm 5) sa môže použiť na ochranu relácií BGP vytvorením hashovaného kľúča na autentifikáciu správ TCP. MD5 prijíma správu s premenlivou dĺžkou a počíta pevnú dĺžku „Výberu“, 128-bitová kryptografická hodnota hash pre každý paket pomocou tajného kľúča, ktorý zdieľajú obidva konce relácie. Pretože MD5 je kryptografický algoritmus a nie jednoduchý kontrolný súčet, ako je CRC32 (Cyclic redundancy check 32), je výpočtovo ťažké určiť kľúč MD5 z hodnoty hash. MD5 je navrhnutý tak, že jedna bitová zmena paketu bude produkovať inú hashovaciu hodnotu, takže prijímajúci partner môže byť primerane istý, že v správach BGP neboli vykonané žiadne zmeny, vymazania alebo vloženia. Partneri BGP môžu pri každej správe obsahovať hodnotu MD5 a

prijímajúci rovnocenný partner skontroluje, či sa hodnota zhoduje s hodnotou vypočítanou pomocou zdieľaného tajného kľúča. Ak sa hodnoty nezhodujú alebo kontrolný súčet MD5 chýba, správa sa zahodí.

MD5 poskytuje ochranu proti útokom založeným na TCP, ako sú spoofing a únos relácie, pretože útočník musí poznať tajný kľúč použitý pri výpočte hash. Komerčné smerovače ponúkajú MD5, ako a konfiguračná možnosť a relatívne ľahko sa dá nastaviť pomocou jedného alebo dvoch príkazov v konfiguračných súboroch. Nevýhodou je, že tajný kľúč musí byť zdieľaný medzi každým párom rovesníkov a kľúče musia byť pravidelne aktualizované, aby sa zabránilo prasknutiu brutálnej sily útočníkom, ktorý nazhromaždil veľké množstvo správ. Pri veľkej prevádzke to môže byť drahé a časovo náročné. Ďalším dôvodom je to, že pretože MD5 používa zdieľaný tajný kľúč, kľúče sa musia zmeniť súčasne na oboch koncoch spojenia BGP, takže administratívne chyby môžu viesť k narušeniu smerovacích operácií. Pretože crackeri hesiel sú bežne dostupné a dajú sa použiť aj na praskanie kľúčov, mali by sa zvoliť silné kľúče.

5.6 IPsec

Pri vyhodnocovaní bezpečnosti konfigurácie BGP je dôležité mať na pamäti, že BGP je prenášaný štandardným protokolom TCP. Náročnejšia práca útočníka, nie sú kryptograficky bezpečná. Kedykoľvek má útočník prístup k nešifrovanej komunikácii medzi rovesníkmi BGP, sú tieto systémy náchylné na rôzne útoky založené na TCP, ako napríklad spoofing-attack. Jediným komplexným riešením týchto zraniteľností je kryptografický protokol, napríklad IPsec.

IPsec je protokol vrstvy IP, takže štandardný BGP môže používať IPsec bez úprav. Protokol IPsec môže poskytovať autentifikáciu aj šifrovanie údajov a preto by sa mohol použiť namiesto MD5 overenia. Ak je potrebná iba autentifikácia, vo vrstve IP sa môže použiť voľba AH (Authentication Header). Pridaná vrstva ochrany je k dispozícii pomocou možnosti ESP (Encapsulating Security Payload) na šifrovanie údajov odovzdaných v aktualizáciách BGP. Alternatívne tunelovanie IPsec môže poskytovať šifrovanie údajov BGP. Hlavnou nevýhodou IPsec je potreba koordinovať kľúče s rovesníkmi BGP, rovnako ako s MD5. Silné šifrovanie, ktoré sa používa s protokolom IPsec, môže byť náročné aj na zdroje, čo zvyšuje zaťaženie smerovačov, ktoré už môžu byť takmer preťažené. Vo väčšine prípadov by šifrovanie údajov BGP nemalo byť potrebné, pretože sa očakáva, že informácie sa budú rovnako

šíriť cez internet, takže používanie nákladu s vyššou úrovňou zabezpečenia môže byť iba kryptografické overenie.

5.7 Ochrana smerovača a fyzická bezpečnosť

Základnou súčasťou zabezpečenia BGP je ochrana smerovačov, na ktorých BGP beží. Obstarávanie a prevádzka smerovačov BGP by mali zahŕňať aspoň:

- Prevádzkujte smerovač v zabezpečenej uzamknutej miestnosti. Prístup by mali mať iba oprávnení správcovia systému. Tieto obmedzenia znižujú možnosť neoprávneného fyzického prístupu k smerovaču, ktorý uľahčilo by to dosiahnutie kompromisu.
- Ak chcete znížiť potenciál útokov odmietnutia služieb na základe vyčerpania smerovacích tabuliek, nakonfigurujte smerovače s maximálnym dostupným množstvom pamäte.
- Poskytnite nepretržité napájanie UPS (Uninterruptible Power Supply) pre všetky smerovače, aby ste znížili riziko zlyhania smerovača. Okrem úvah o tolerancii porúch UPS znižuje pravdepodobnosť útoku na napájanie.
- Implementujte politiku aktualizácie softvéru, aby ste zaistili, že záplaty budú začlenené do softvéru smerovača, len čo ich vydá predajca smerovača, a aby boli primerane otestované z hľadiska vhodnosti v miestnej sieti. Aktualizácia záplat poskytnutých predajcom je najúčinnejším prostriedkom zabezpečenia smerovačov proti neoprávnenému prístupu, útokom odmietnutia služieb a iným hrozbám [18].

II. PRAKTICKÁ ČÁST

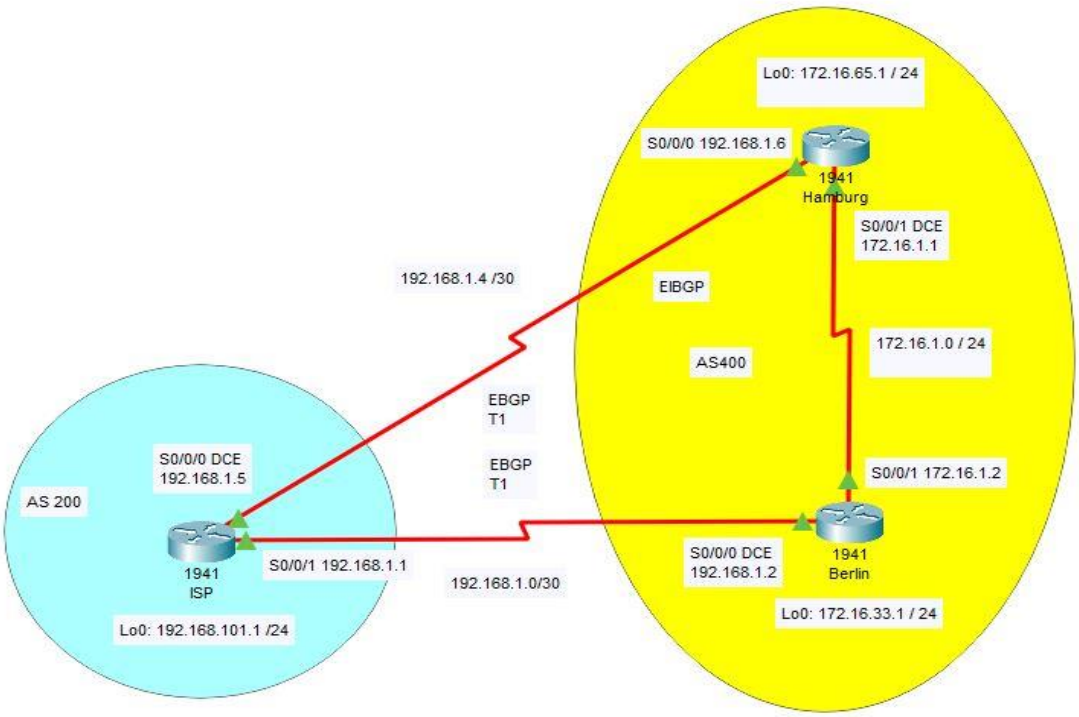
6 NÁVRH KONFIGURURÁCIE SIETE BGP POMOCOU SILULAČNÉHO PROGRAMU PACKET TRACER

Spoločnosť Cisco vytvorila aplikáciu Packet Tracer aby pomohla študentom zapojeným do akademického sieťového programu získať zručnosti v sieťových technológiách.

Packet Tracer je výkonná platforma pre simulovanie počítačových sietí inšpirujúca študentov k tomu, aby experimentovali. Nahradzuje fyzickú výbavu v laboratóriu a umožňuje študentom vytvárať siete s takmer neobmedzeným počtom zariadení, podporujúc zručnosti, objavovanie a riešenie problémov.

6.1 Návrh a topológia BGP siete

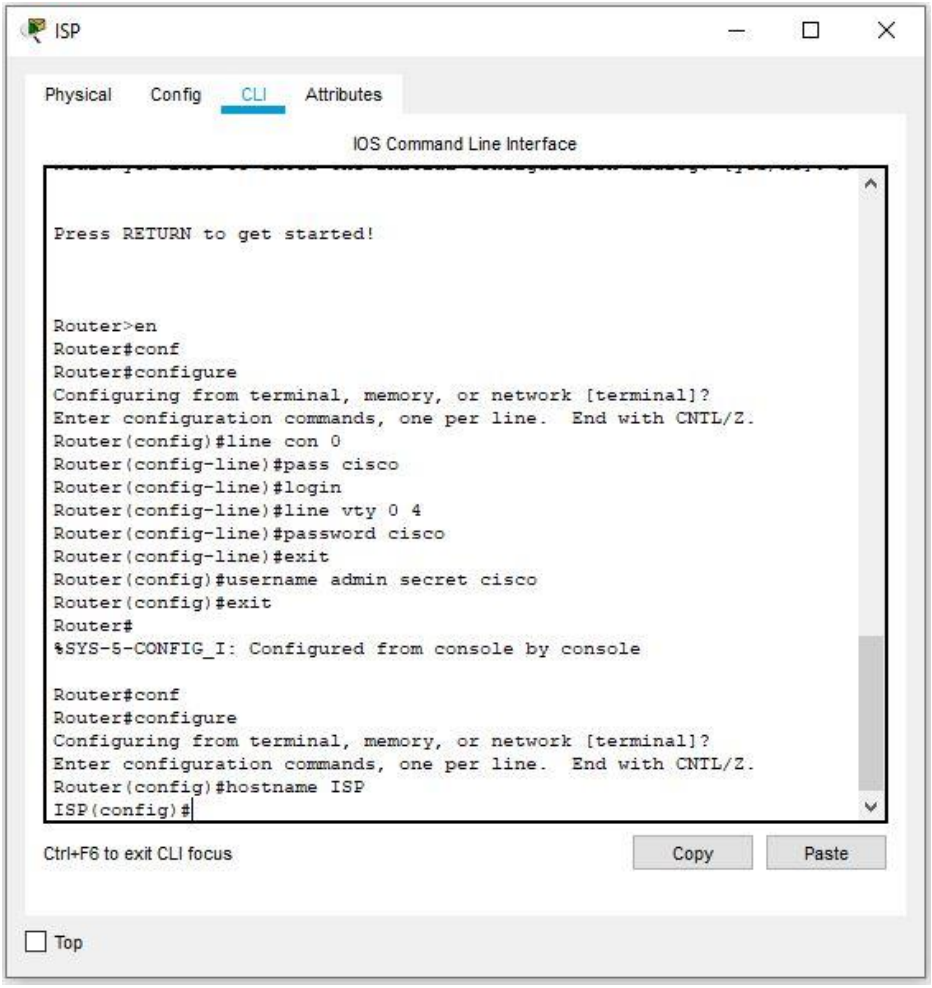
Cieľom návrhu siete BPG je zaistenie komunikácie vo fiktívnej podnikovej siete, ktorá je vytvorená v simulačnom programe. Podnik komunikuje medzi sebou cez medzinárodnú sieť. Každý zo smerovačov sa nachádza v inom meste.



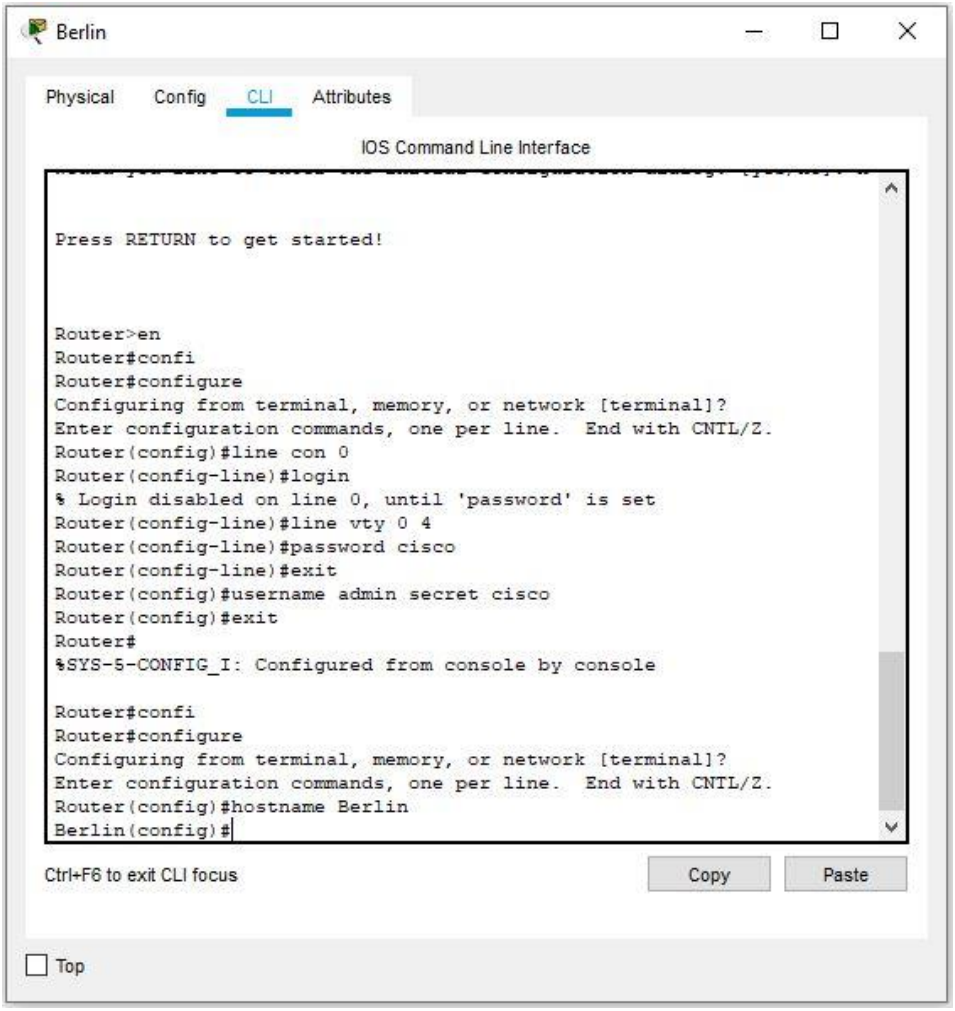
Obr. 17 Topológia siete.

6.2 Konfigurácia adresy rozhrania

Pri prvom prihlásení k prepínaču pomocou konzoly je za potreby na každom smerovači nastaviť vlastné meno a heslo. V tomto prípade sa použilo štandardné heslo Cisco. Ak heslo, ktoré sa zvolilo a nie je dostatočne zložité, zobrazí sa výzva na vytvorenie iného hesla. Nastavenie hesla sa aplikovalo na každý smerovač.

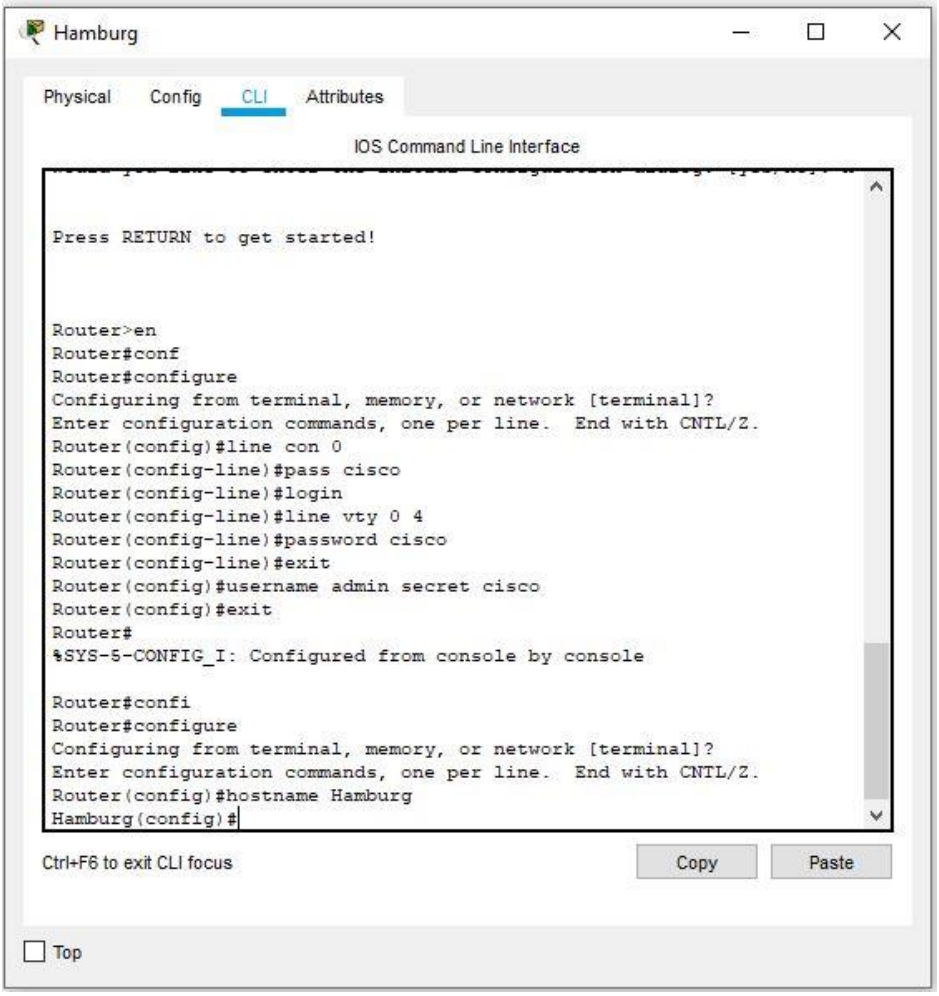


Obr. 18 Nastavenie mena a hesla na smerovači ISP.



Obr. 19 Nastavenie mena a hesla na smerovači Berlin.

Po nastavení hesla na smerovačoch, sa definovalo meno každého zariadenia pre lepšie rozpoznanie smerovačov na danej sieti. Každý smerovač bol premenovaný, podľa toho kde sa nachádza. V predvolenom nastavení smerovača sa každé jedno slovo zadané do zariadenia so systémom IOS, deteguje ako príkaz ale ak nie je to platný príkaz, považuje sa ako meno hostiteľa. Zariadenie sa pokúsi preložiť dané slovo na adresu IP v procese, ktorý môže trvať asi minútu. Preklad DNS sa zakázalo pomocou príkazu no ip domain-lookup. Príkaz sa aplikoval do všetkých zariadení v danej topológii.

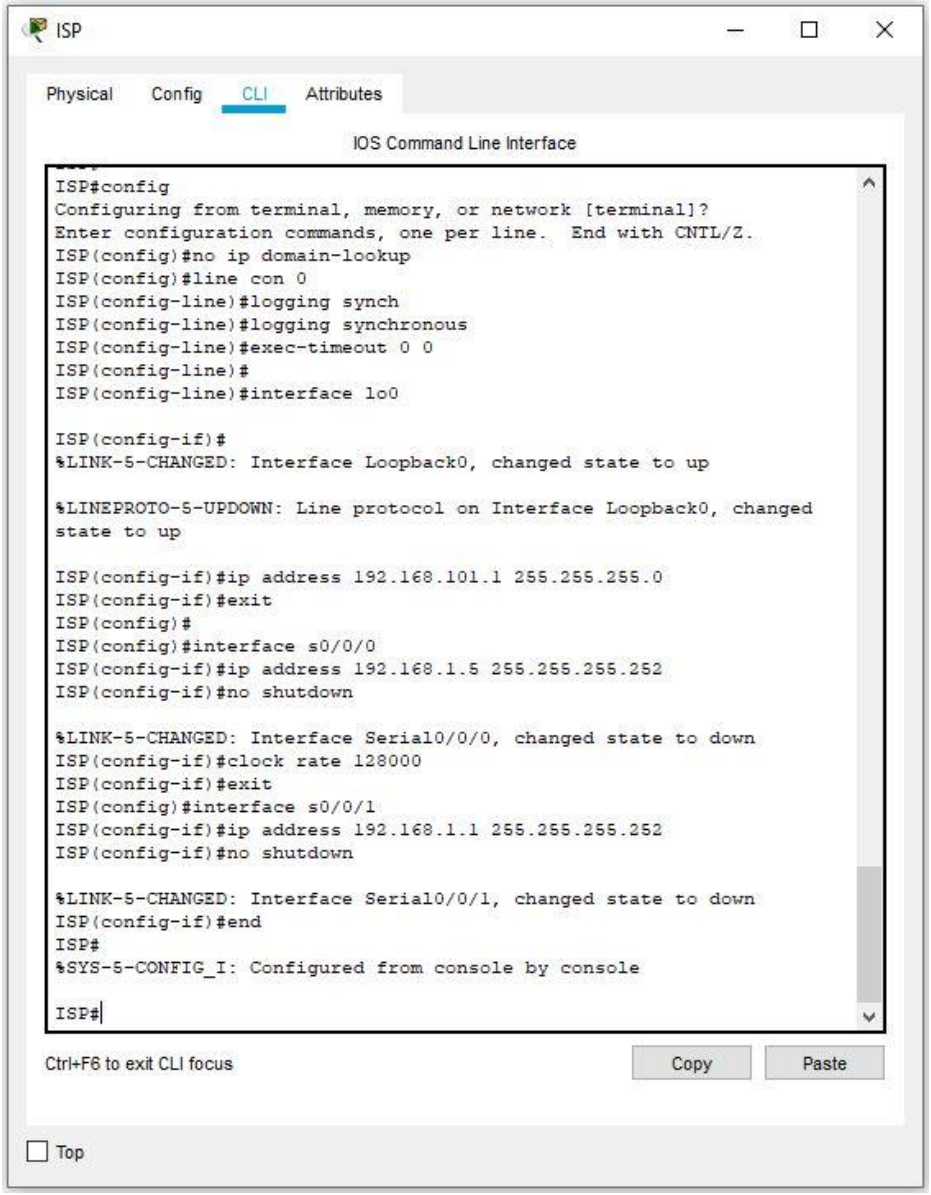


Obr. 20 Nastavenie mena a hesla na smerovaci Hamburg.

Na všetkých smerovačoch bolo definované rozhranie Lo0 zo statickou IP adresov. Toto rozhranie je označované ako Loopback. Internetový protokol určuje sieť so spätnou väzbou s adresou IPv4 127.0.0.0 s 8 bitovým prefixom . Väčšina implementácií IP podporuje rozhranie spätnej väzby, ktoré predstavuje funkciu spätnej väzby. Akákoľvek prevádzka, ktorú počítačový program pošle v sieti so spätnou väzbou, je adresovaná tomu istému počítaču. Najbežnejšie používaná adresa IP v sieti so spätnou slučkou je 127.0.0.1 pre IPv4 a ::1 pre IPv6. Štandardný názov domény pre adresu je localhost.

V ďalšom kroku sa zvolila konfigurácia sériového rozhrania. Ak by sa použilo pripojenie typu WAN typu back-to-back, je potrebné nastaviť príkazom clock rate rýchlosť hodín na sériovom rozhraní smerovača. Keď sú pripojené dva smerovače, jeden musí poskytovať taktovanie pre vzájomnú komunikáciu. Nastavenie hodinovej rýchlosti je dôležité pre synchronizáciu, pretože každý hodinový impulz signalizuje prenos bitu. V skutočnom svete

takmer každý poskytovateľ siete dodáva hodinový signál, ktorý nevyžaduje nastavenie žiadnej hodinovej rýchlosti na smerovači na konci zákazníka.

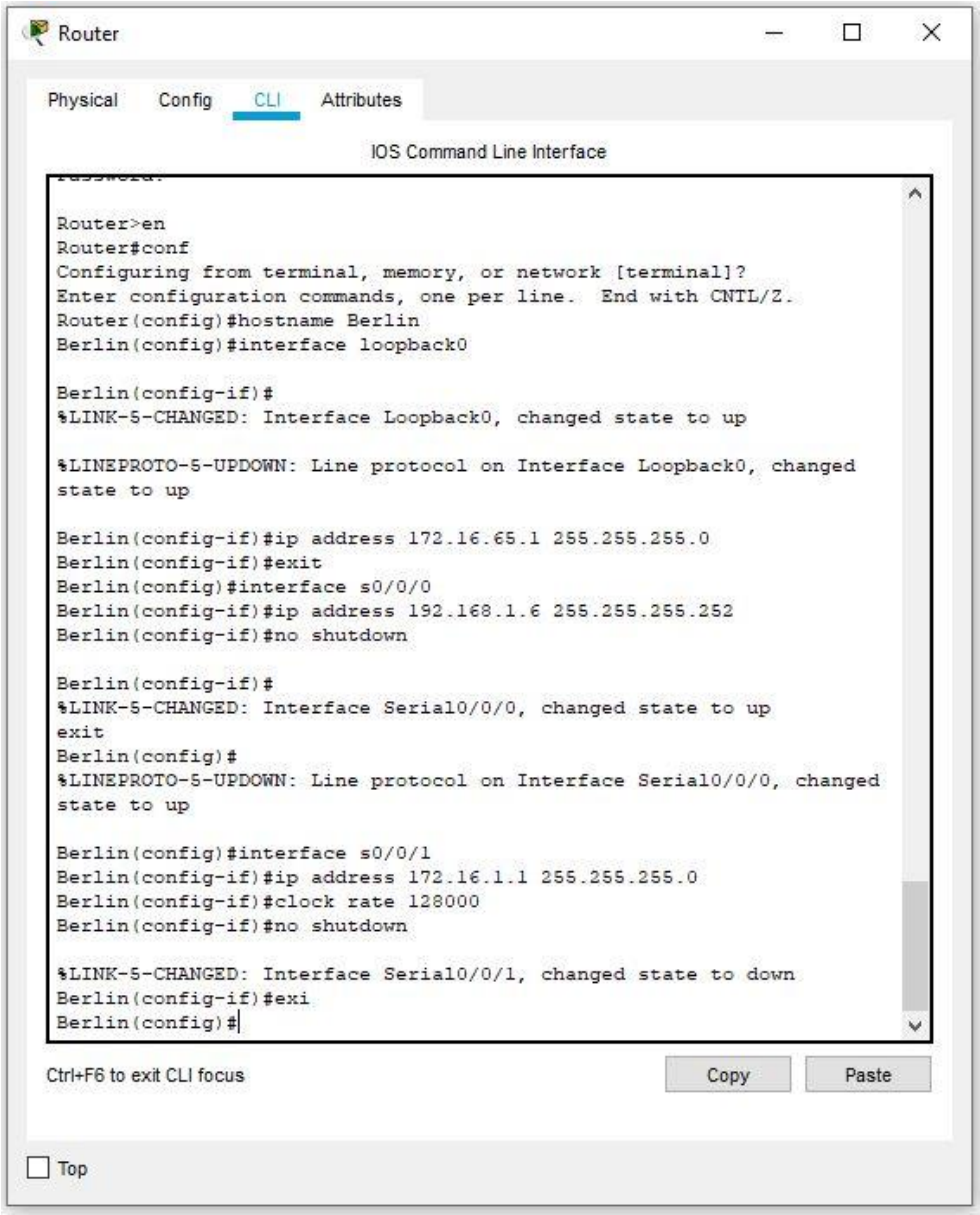


Obr. 21 Nastavenie Loopback0 a sériového rozhrania na smerovači ISP.

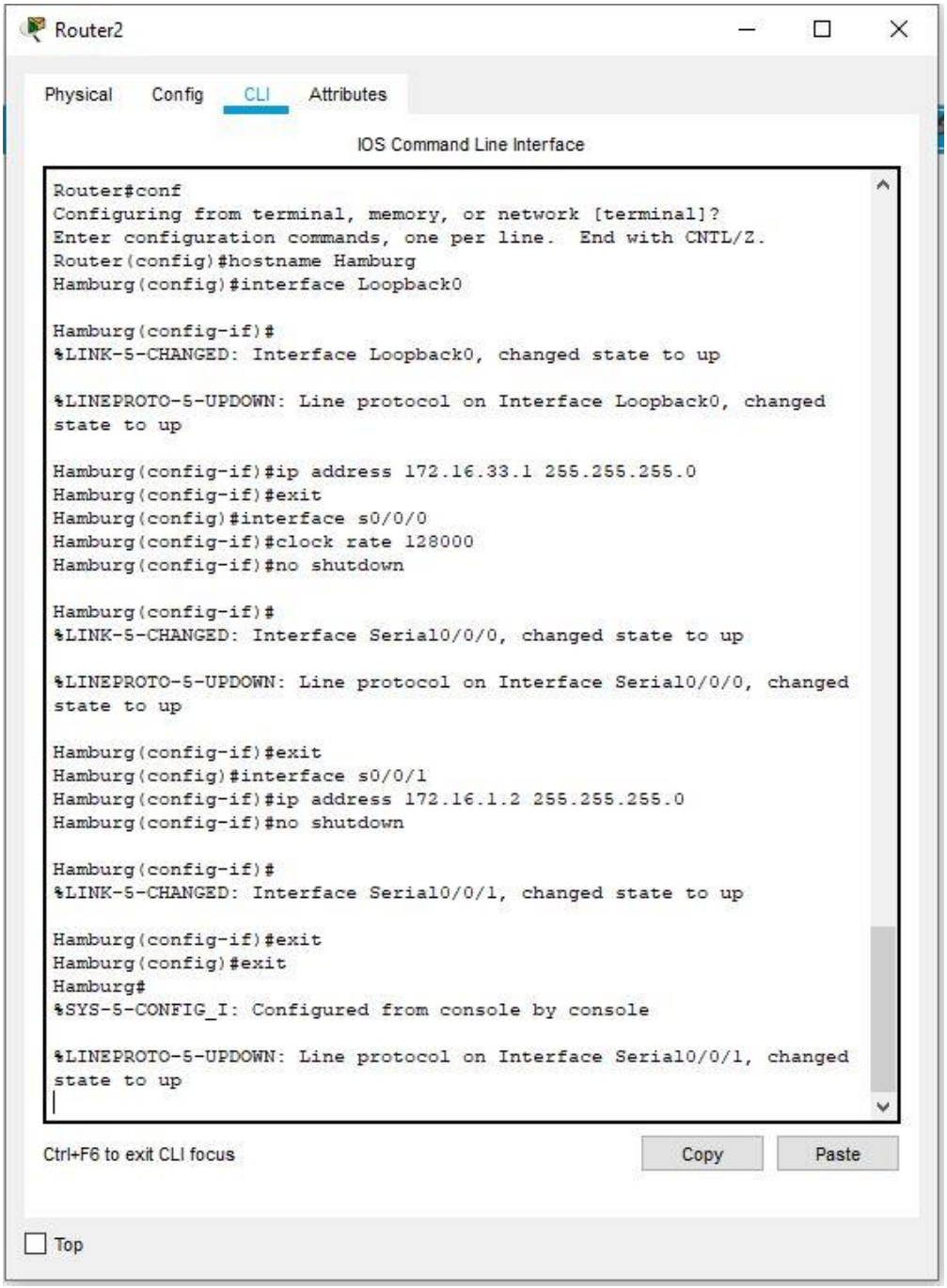
Pred prechodom na príkazy na nastavenie frekvencie hodín bolo dôležité poznať rozdiel medzi DTE (Data Terminal Equipment) a DCE (Data Communications Equipment). Kedykoľvek sú pripojené dva smerovače, vždy jeden bude fungovať ako DTE a druhý ako DCE. Po konfigurácii DTE alebo DCE boli aktivované sériové porty.

DTE zahŕňa každú jednotku, ktorá funguje buď ako zdroj alebo ako cieľ pre binárne digitálne údaje. Na fyzickej vrstve to môže byť terminál, mikropočítač, počítač, tlačiareň, fax, stroj alebo akékoľvek iné zariadenie, ktoré generuje alebo spracováva digitálne údaje. DTE potrebujú sprostredkovateľa na to, aby mohli komunikovať.

DCE Zahŕňa akúkoľvek funkčnú jednotku, ktorá vysiela alebo prijíma údaje vo forme zdroju hodín alebo digitálneho signálu prostredníctvom siete.

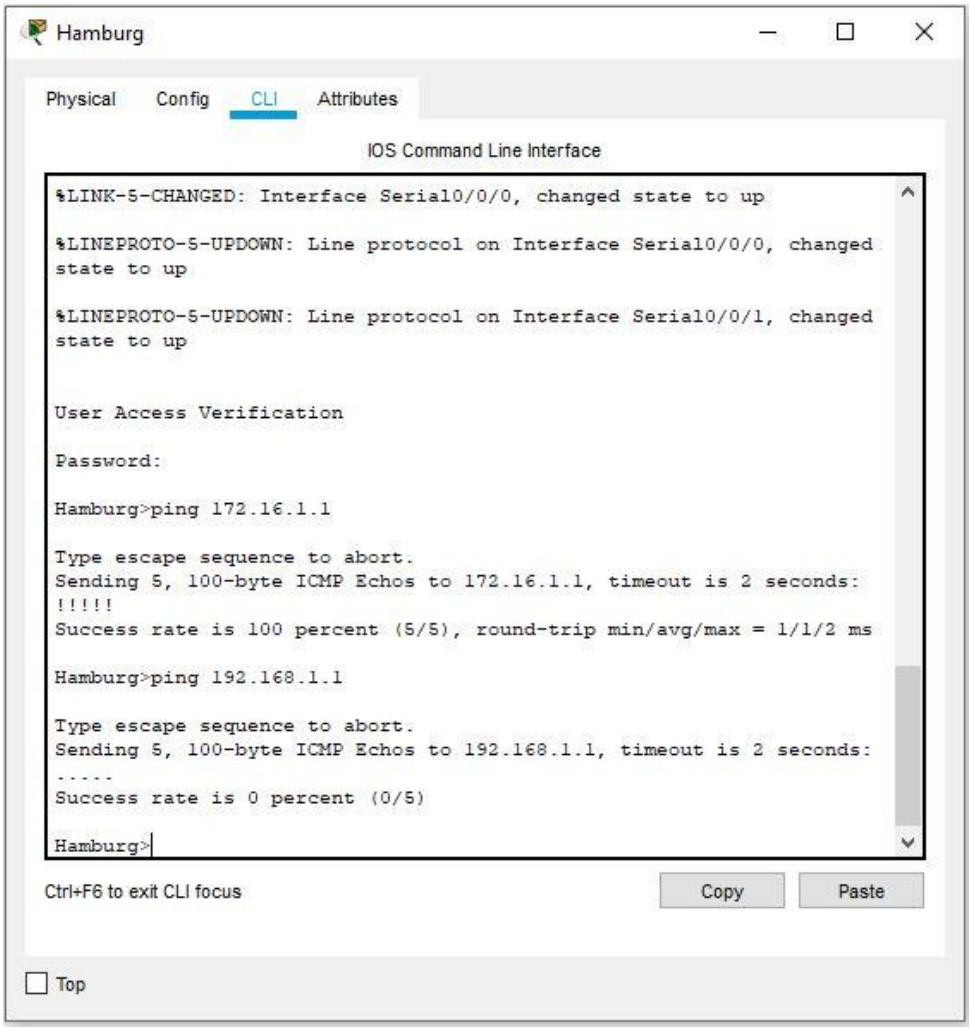


Obr. 22 Nastavenie Loopback0 a sériového rozhrania na smerovači Berlin.



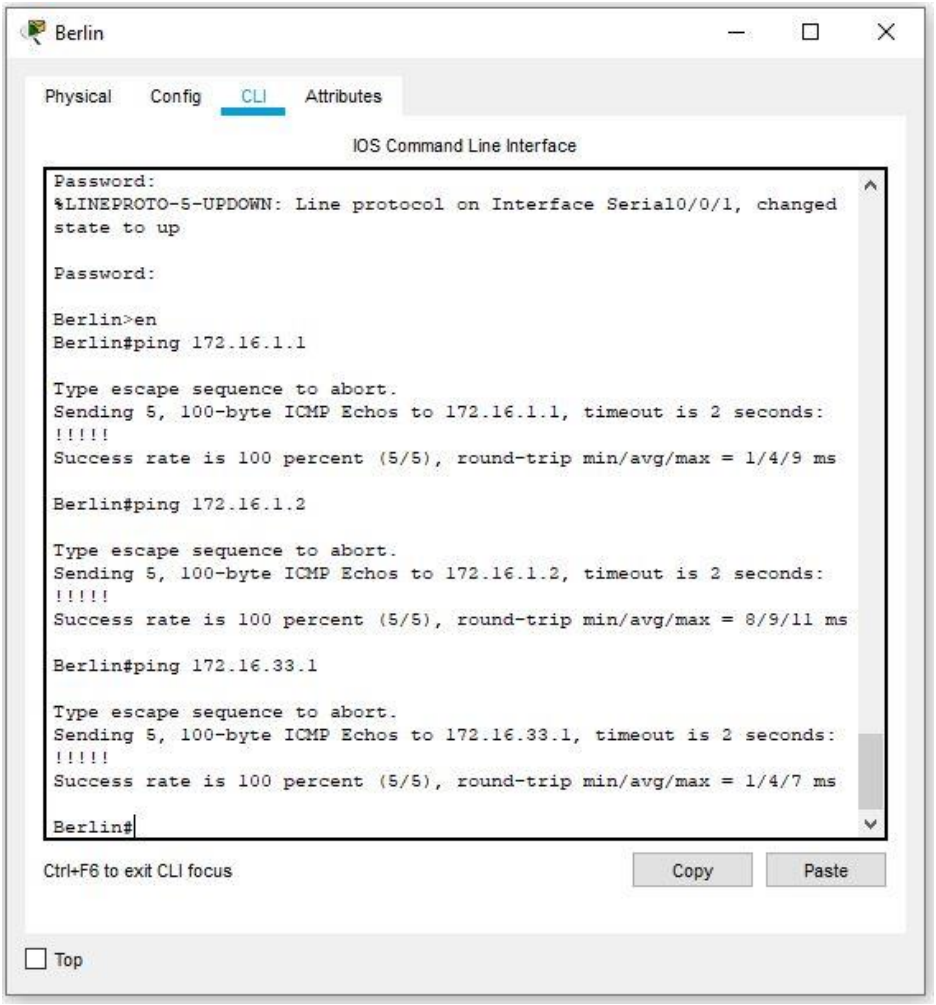
Obr. 23 Nastavenie Loopback0 a sériového rozhrania na smerovači Hamburg.

Pomocou príkazu ping bolo otestované pripojenie medzi priamo pripojenými smerovačmi. Na oboch smerovačoch Hamburg a Berlin je za potreby overiť pripojenie pomocou príkazu ping, svoju lokálnu IP adresu a adresu sériového spojenia ISP. Smerovač ISP nemohol dosiahnuť segment medzi Hamburg a Berlin.



Obr. 24 Testovanie spojenia smerovača Hamburg.

Príkaz ping odoslal postupnosť paketov požiadaviek na echo ICMP zadanému hostiteľovi. Je to jeden z najjednoduchších a najčastejšie používaných nástrojov na riešenie problémov. Ak by bol hostiteľ vynechaný z príkazového riadku a nachádzal by sa v privilegovanom režime EXEC (Execute Cisco IOS Commands), smerovač pošle výzvu na zadanie ďalších informácií.

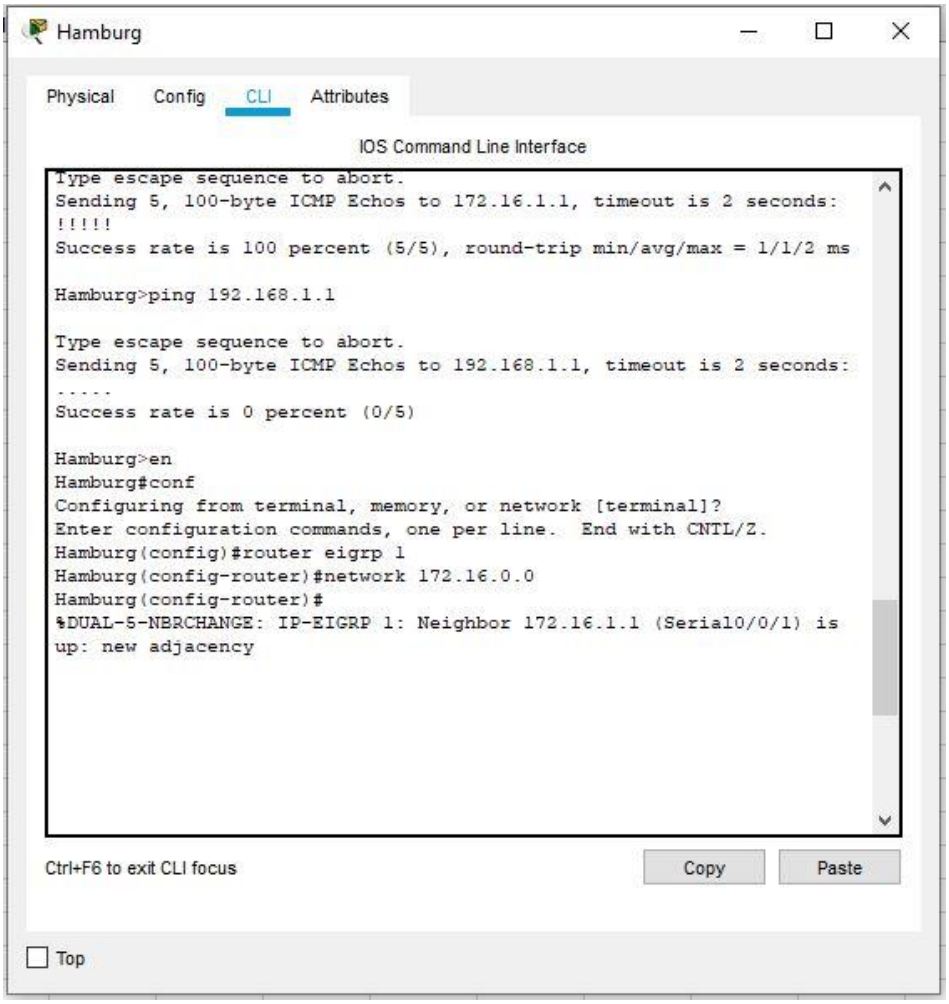


Obr. 25 Testovanie spojenia na smerovači Berlin.

6.3 Konfigurácia EIGRP

Autentifikácia paketov odosielaných medzi susedmi zaručuje, že zariadenie prijíma pakety iba zo zariadení, ktoré majú rovnaký vopred zdieľaný kľúč. Ak toto overenie nie je definované, je možné úmyselne alebo neúmyselne pridať do siete ďalšie zariadenie s rôznymi alebo konfliktnými informáciami o trase.

Overovanie pomocou protokolu EIGRP je konfigurovateľné na základe jednotlivých rozhraní. Pakety vymieňané medzi susedmi pripojenými cez rozhranie sú autentifikované. EIGRP podporuje autentifikáciu pomocou algoritmov súhrnu správ MD5, aby sa sledovalo zavedenie nepovolených informácií z neschválených zdrojov. V tomto prípade bolo nakonfigurovaná susedská autentizácia iba medzi smerovačmi Hamburg a Berlin.

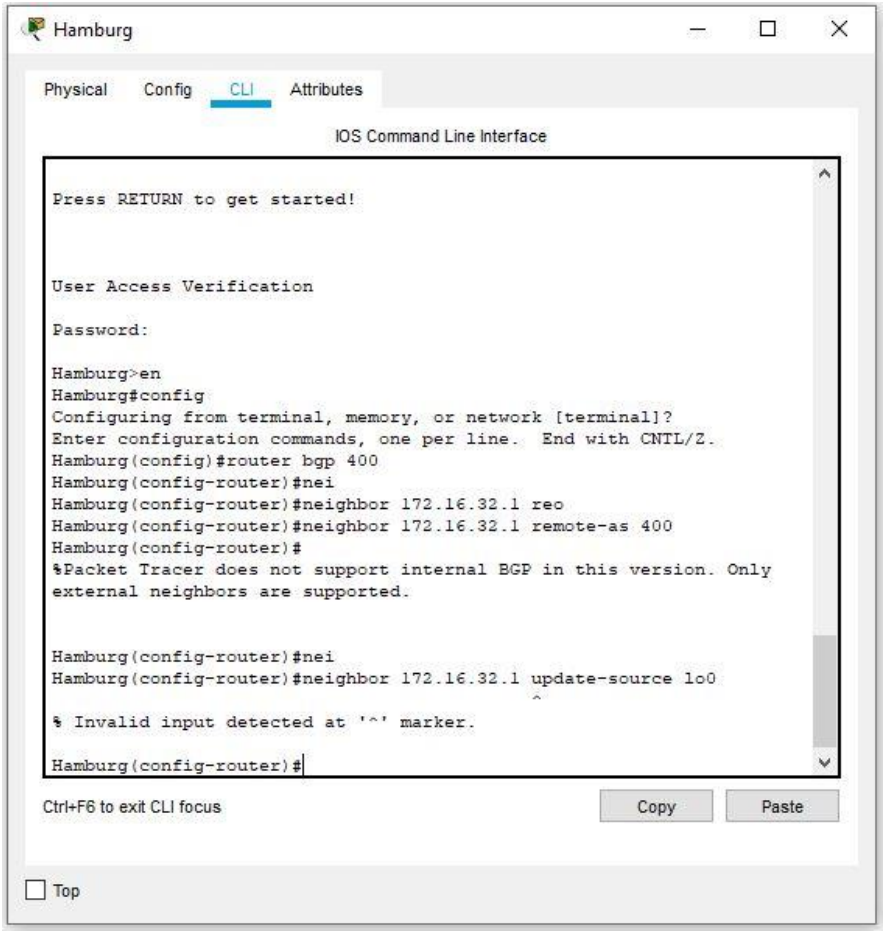


Obr. 26 Konfigurácia EIGRP medzi smerovačmi Berlin a Hamburg.

6.4 Konfigurácia IBGP a overenie susedov BGP

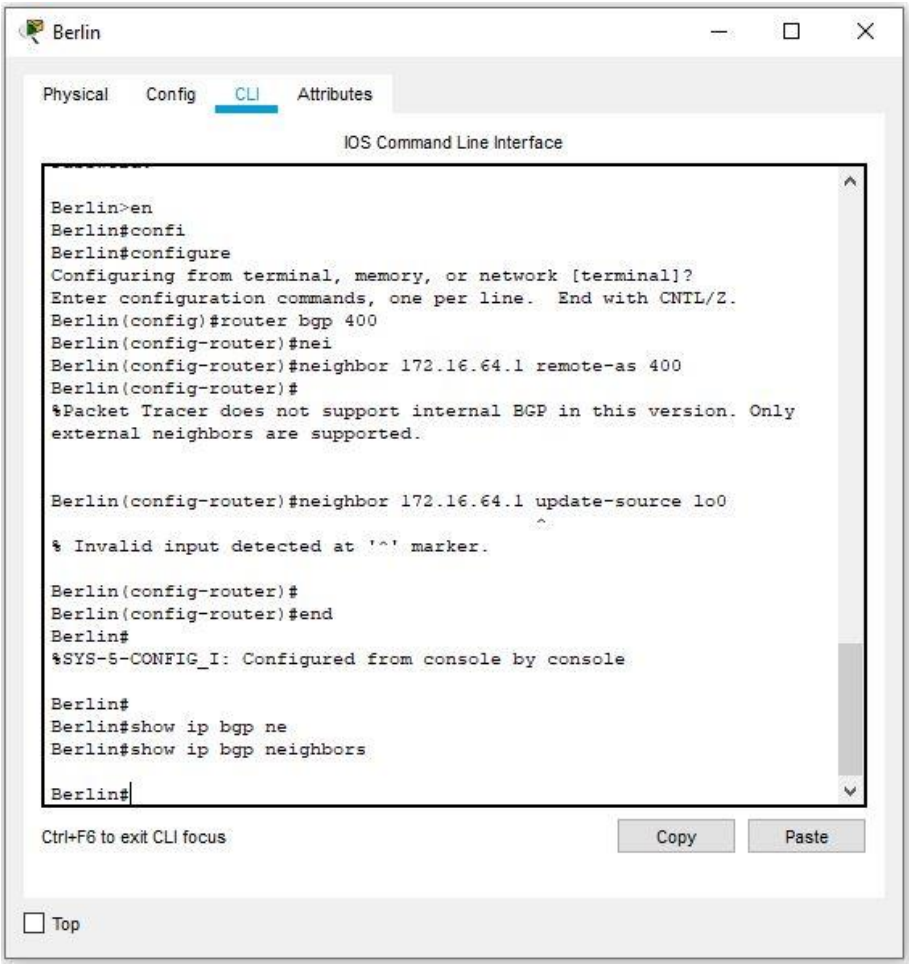
Ak existuje viac ciest k susedovi BGP, smerovač je možné použiť viac rozhraní na komunikáciu so susedom. Zdrojová adresa IP závisí od odchádzajúceho rozhrania. Príkaz update-source lo0 stanovil príkaz smerovaču, aby použil adresu IP rozhrania Loopback0 ako zdrojovú adresu IP pre všetky správy BGP odoslané tomuto susedovi. Mimo poskytovateľov internetových služieb sa väčšina správcov sietí zaoberá BGP oveľa menej ako s IGP, ak vôbec. A aj keď sa používa BGP, konfigurácie u malých poskytovateľov internetových služieb a od iných poskytovateľov sú zvyčajne úplne základné.

V tomto prípade sa nastavili IBGP protokoly na smerovačoch Berlin a Hamburg na AS 400.



Obr. 27 Príkaz nastavenia smerovania IBGP na smerovači Hamburg.

Program Packet Tracer vyvinutý spoločnosťou Cisco je iba ale simulačný. Protokoly a príkazy na nastavenie smerovania IBGP však ale nepozná. V tomto prípade je zobrazený príkaz neighbor 172.16.32.1 remote-as 400, ktorý určoval že smerovač Hamburg má vytvoriť susednú sieť IBGP 400.Tento príkaz nie je v programe definovaný. Taktiež ani príkaz update-source lo0, ktorý slúži na to, aby použil ip adresu rozhrania ako zdrojovú adresu, pre všetky správy BGP odoslané susednému smerovaču. Tieto príkazy boli zadané aj na smerovač Berlin, kde taktiež nespracoval príkaz.

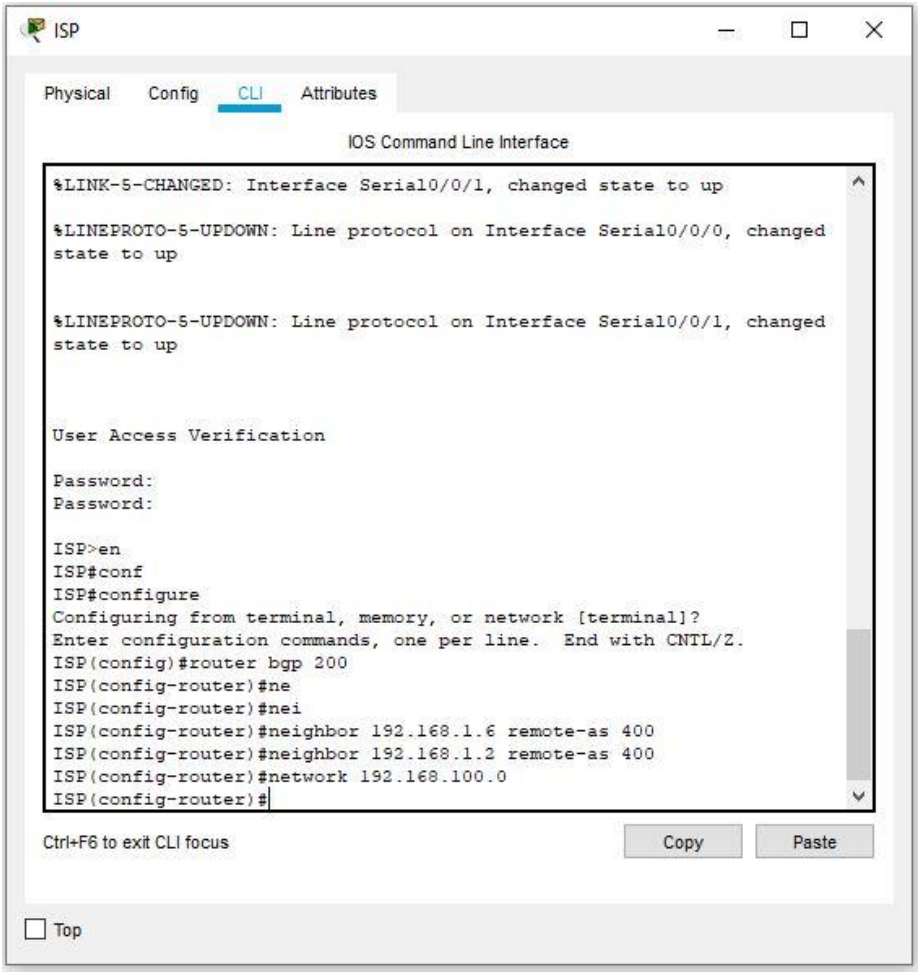


Obr. 28 Príklad nastavenia smerovania IBGP na smerovači Berlin.

Ak by bol zadaný platný príkaz smerovania IBGP, na fyzických smerovačoch, príkazom show ip bgp neighbors by sa overilo susedské spojenie. Konkrétne by zobrazil základné informácie ako sú, IP adresu susedského spojenia a v akej AS sa nachádza. Ďalej by zobrazil podrobné informácie o verzii BGP. Prepojenie medzi Berlin a Hamburg by malo identifikovať ako interné prepojenie naznačujúce partnerský vzťah IBGP.

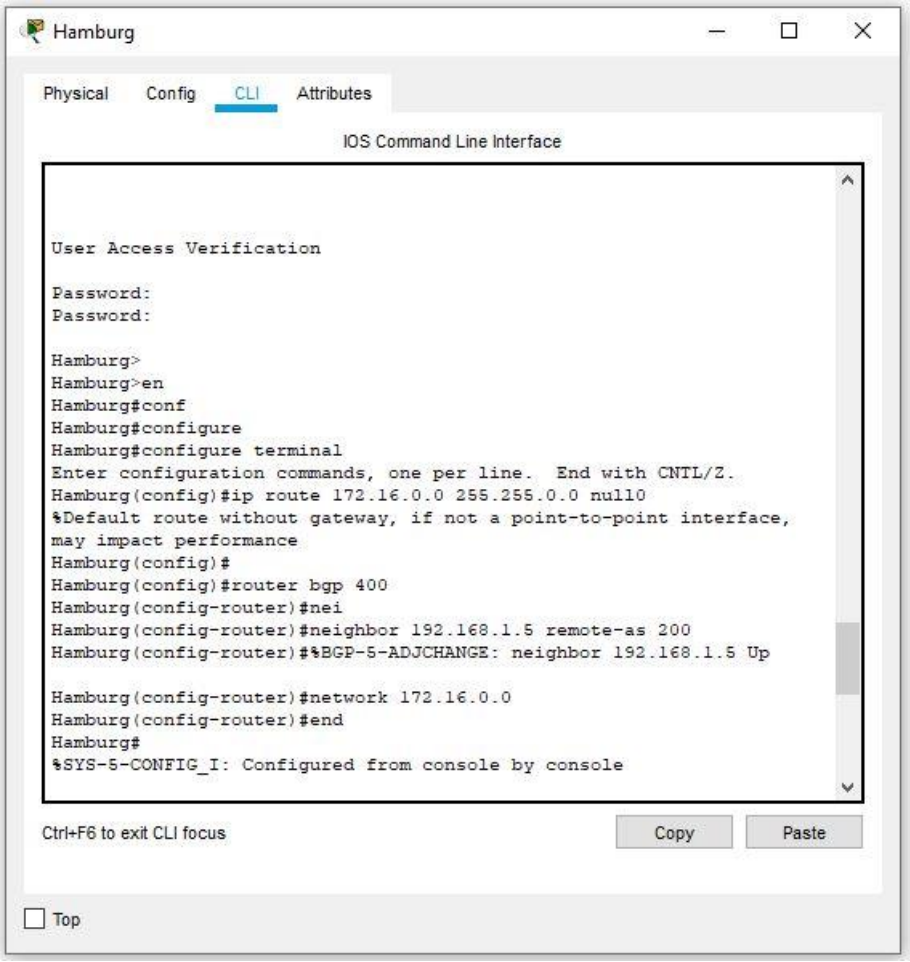
6.5 Konfigurácia EBGP a overenie susedov BGP

Partnerské vzťahy EBGP sú hlavnou súčasťou protokolu BGP na internete. EBGP je výmena sieťových predpôn medzi autonómnymi systémami.



Obr. 29 Nastavenie EBGP smerovania na ISP.

Pretože relácie EBGP sú takmer vždy vytvárané cez odkazy typu point-to-point, nebol dôvod v tejto konfigurácii používať kľúčové slovo update-source. Medzi rovesníkmi existuje iba jedna cesta. Ak táto cesta je neaktívna, alternatívne cesty nie sú k dispozícii.

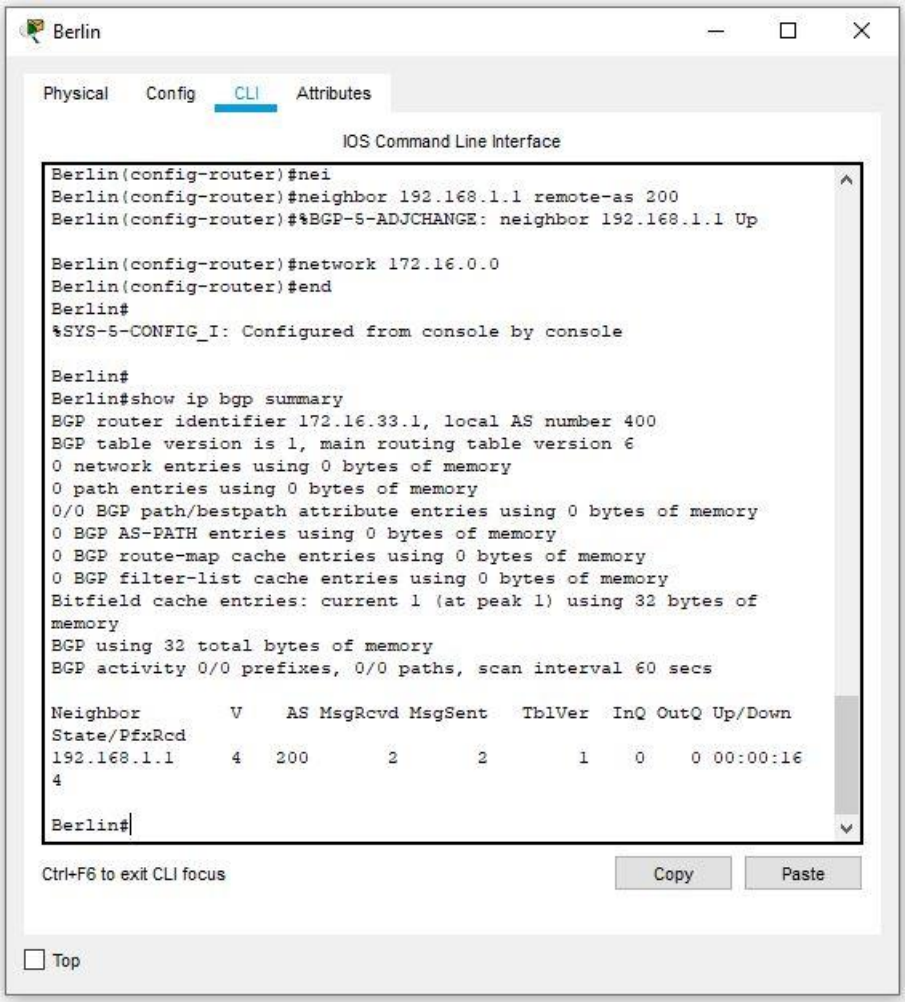


Obr. 30 Konfigurácia statickej trasy Hamburg.

Na vyššie uvedenom obrázku je zobrazený konfiguračný príkaz na určenie nulovej trasy. Nulová trasa znamená „upustiť od tejto premávky“. Jedným z dôvodov použitia nulovej trasy je bezpečnosť, ale je možné ju použiť aj na tento trik pre BGP. Používa sa aj na zabránenie smerovacích slučiek a na trvalé uloženie trás do smerovacej tabuľky.

6.6 Súhrnný výstup BGP

V tomto kroku bol príkaz show ip bgp neighbors použitý na overenie či smerovače Berlin a ISP dosiahli stanovený stav. Užitočným alternatívnym príkazom je príkaz: show ip bgp summary. Výstup by mal byť podobný nasledujúcemu.



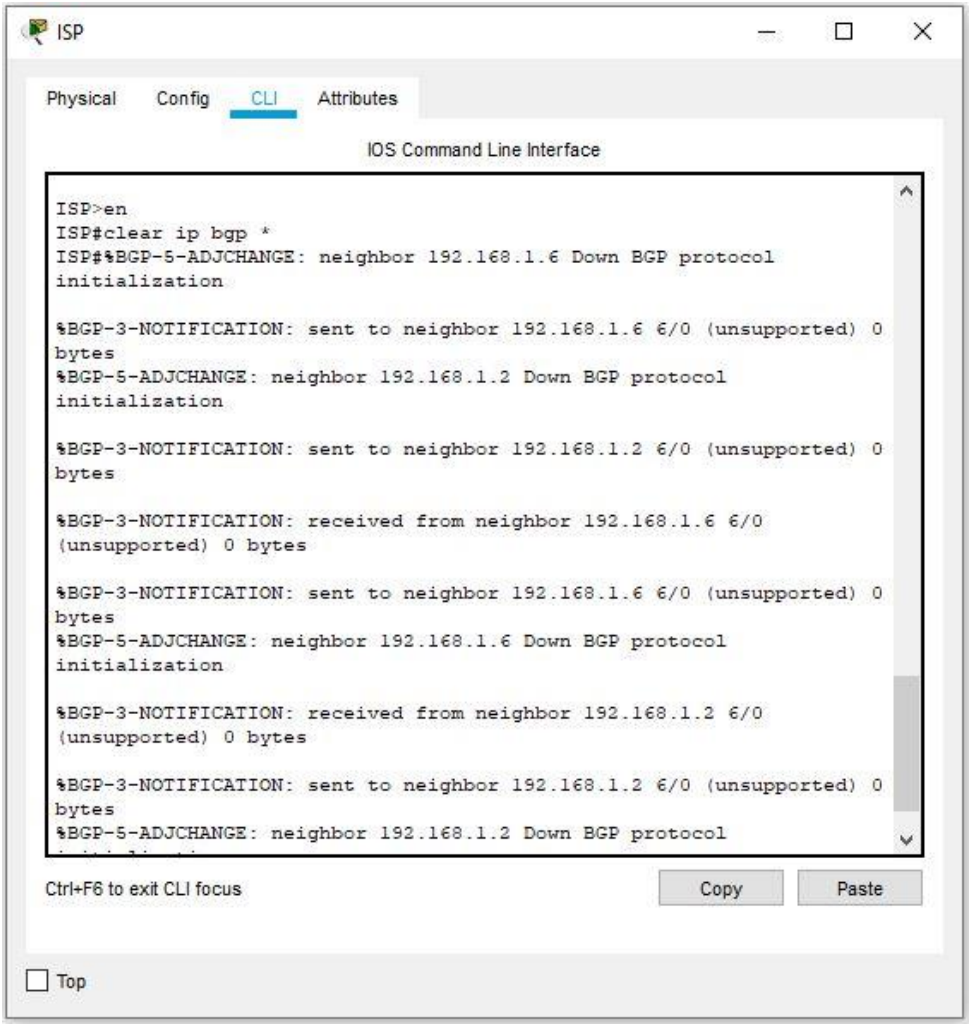
Obr. 31 Overenie stavu medzi smerovačmi Berlin a ISP.

V tabuľke boli generované údaje o smerovaní stavu spojenia. Identifikátor smerovača zobrazil AS 400. Verzia BGP je 1, verzia smerovacej tabuľky 6. V prípade že by boli nakonfigurované trasy IBGP, ostatné parametre výstupu by zobrazovali koľko sieťových a smerovacích položiek je k dispozícií. Nie sú ale žiadne záznamy v medzi pamäti.

Parametre výstupu zobrazujú: Identifikátor smerovača, v tomto prípade to je BGP 172.16.33.1, AS 400. Jedná sa o spojenie EBGP. Verziu BGP 6. Jedno susedné spojenie 192.168.1.1 v AS 200.

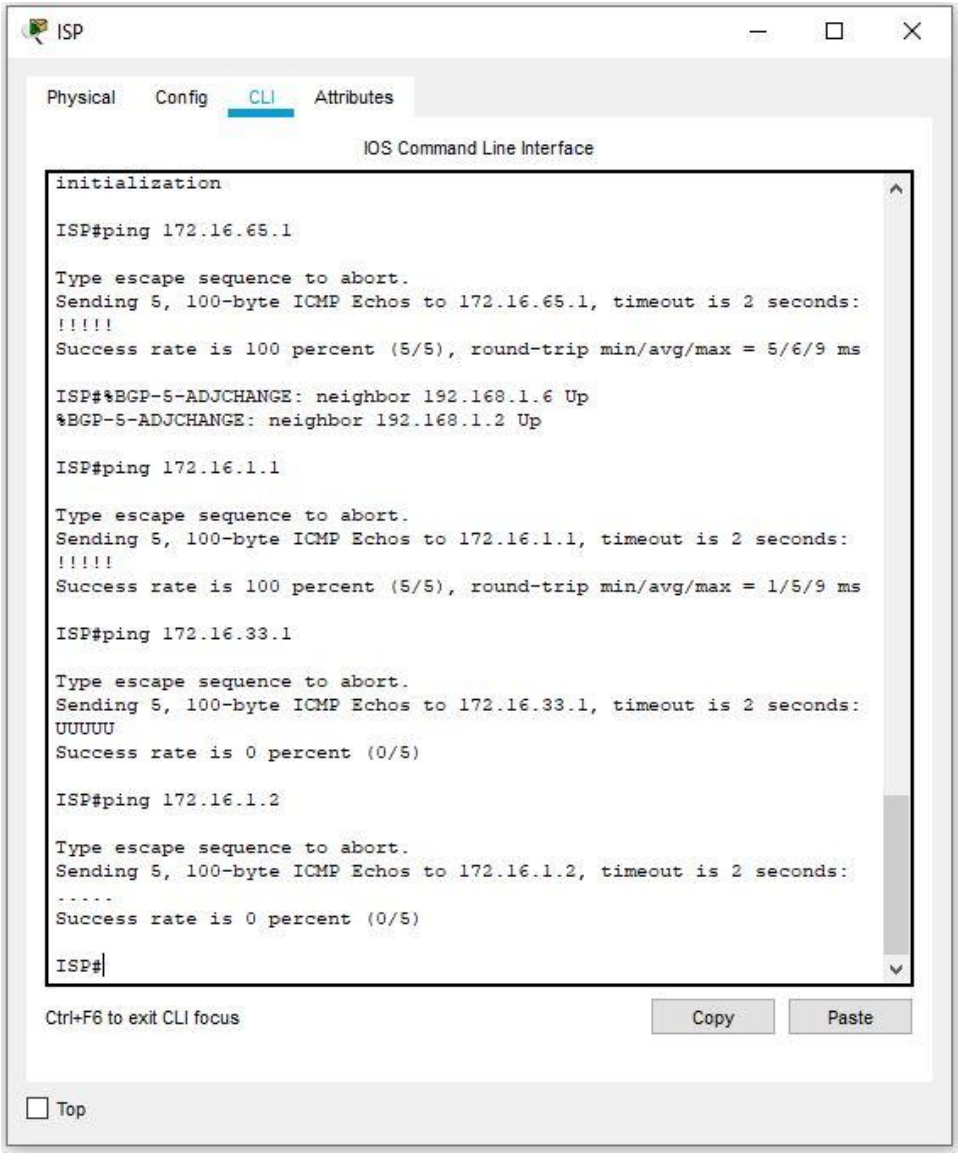
6.7 Overenie cesty

Boli resetované pripojenia BGP, pre možné zmeny politiky prichádzajúcich a odchádzajúcich smerovaní, pomocou príkazu clear ip bgp *. Je dôležité počkať aby sa nastavenia obnovia s každým smerovačom.



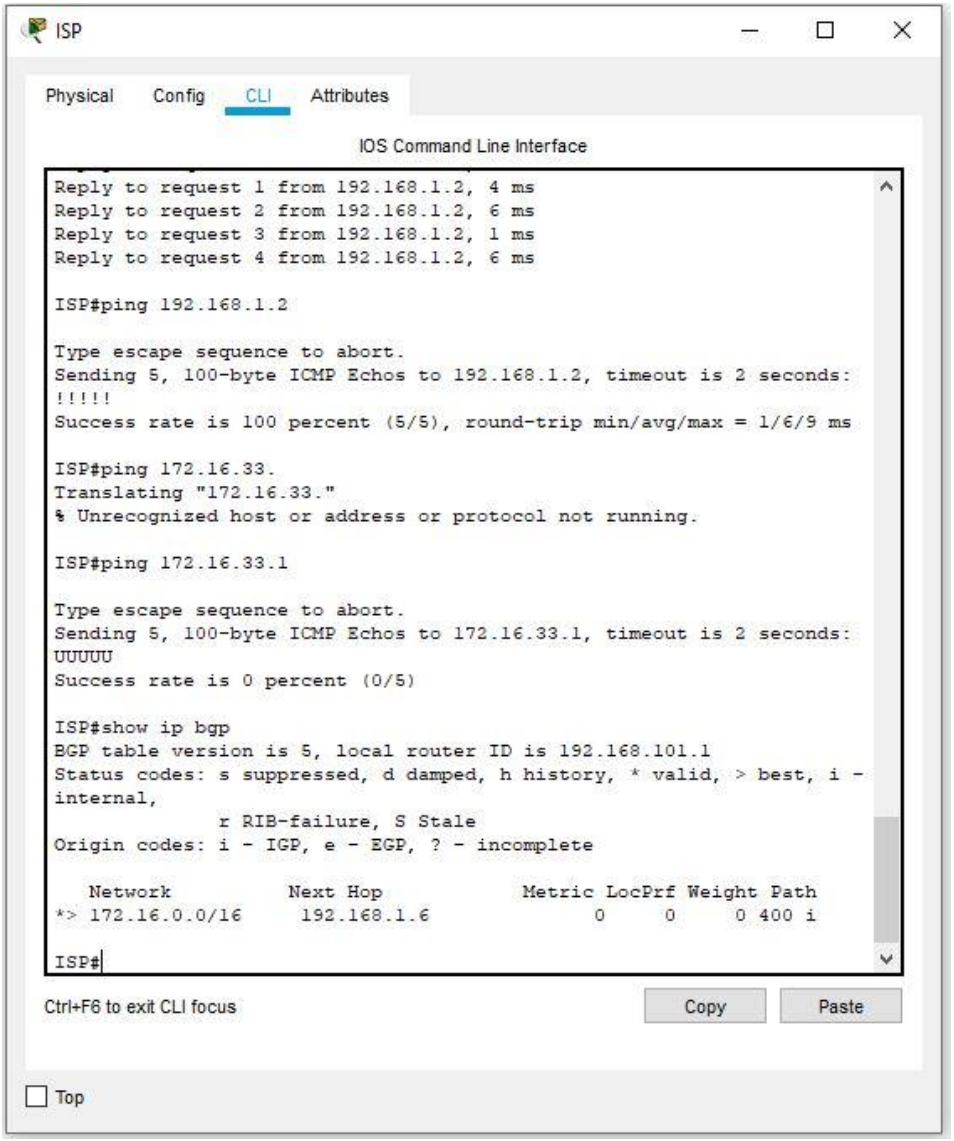
Obr. 32 Resetovanie pripojenia BGP na smerovači ISP.

V ďalšom kroku sa testovali na smerovači IPS spojenia pomocou príkazu ping.



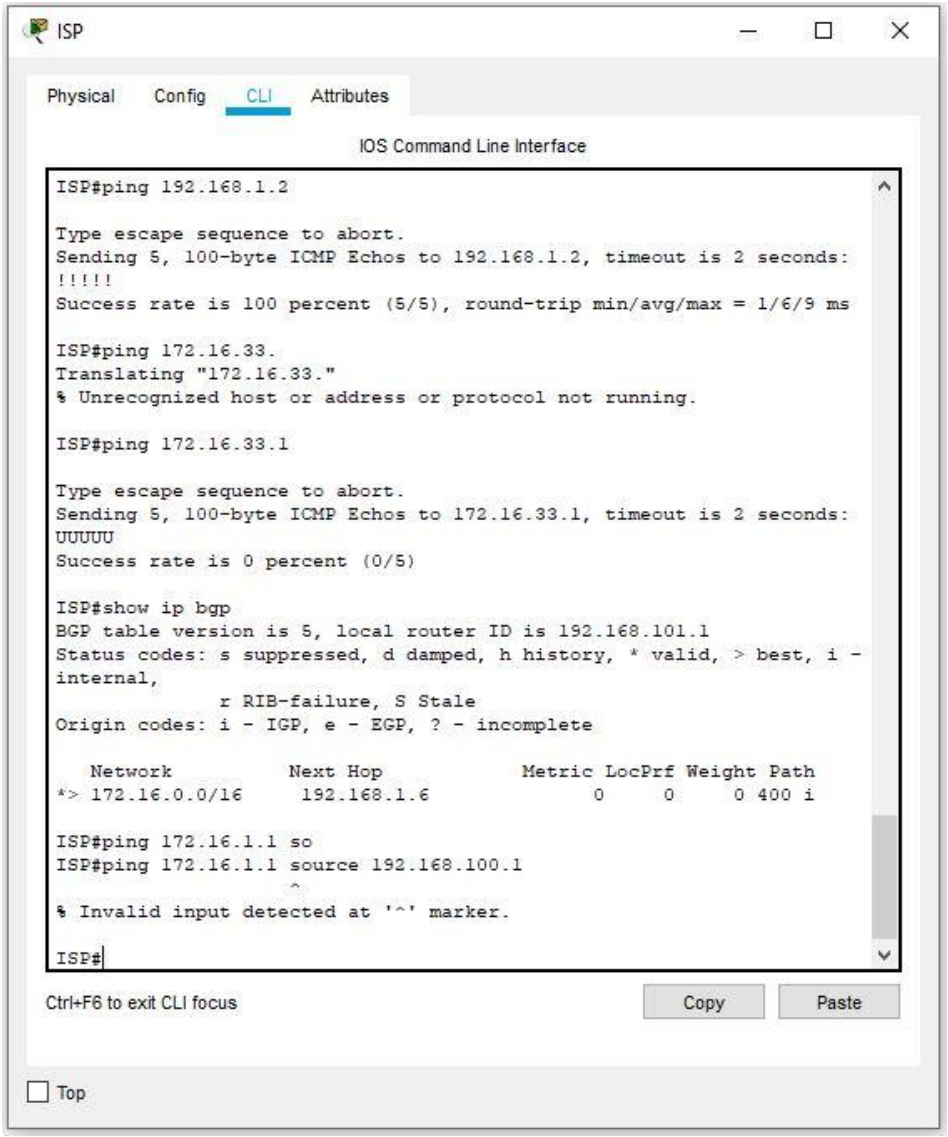
Obr. 33 Testovanie spojenia IPS.

Príkaz zobrazil pozitívne spojenie medzi ISP a smerovačom Hamburg. Taktiež spojenie medzi ISP a smerovačom Berlin funguje, avšak iba na priamom spojení, nie cez smerovač Hamburg. V prípade ak by boli definované IBGP smerovanie medzi Hambrug a Berlin, príkaz ping by fungoval aj na tomto smerovači.



Obr. 34 Zobrazenie položiek v smerovacej tabuľky.

Príkazom show ip bgp sú zobrazované položky v smerovacej tabuľke BGP. Znak šípky určuje že tabuľkový záznam je najlepší záznam, ktorý sa dá pre danú sieť použiť. Hviezda nám určuje že záznam v tabuľke je platný.

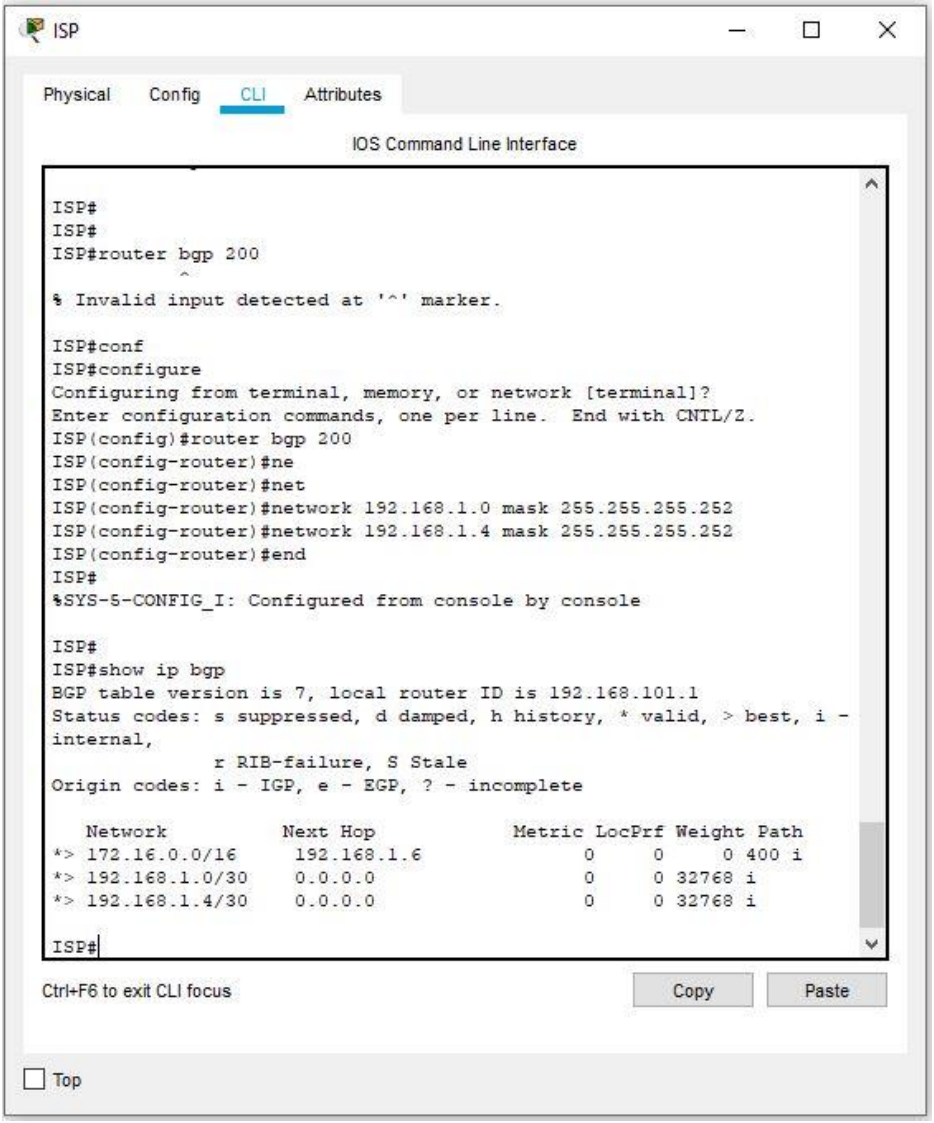


Obr. 35 Príklad použitia rozšíreného príkazu ping.

V tomto okamihu by mal byť smerovač ISP schopný dostať sa do každej siete pripojenej k Berlin a Hamburg adresy spätnej slučky 192.168.100.1. V tomto prípade ale nie je možné to realizovať, nakoľko konfiguráciu IBGP Cisco Packet Tracer nepodporuje.

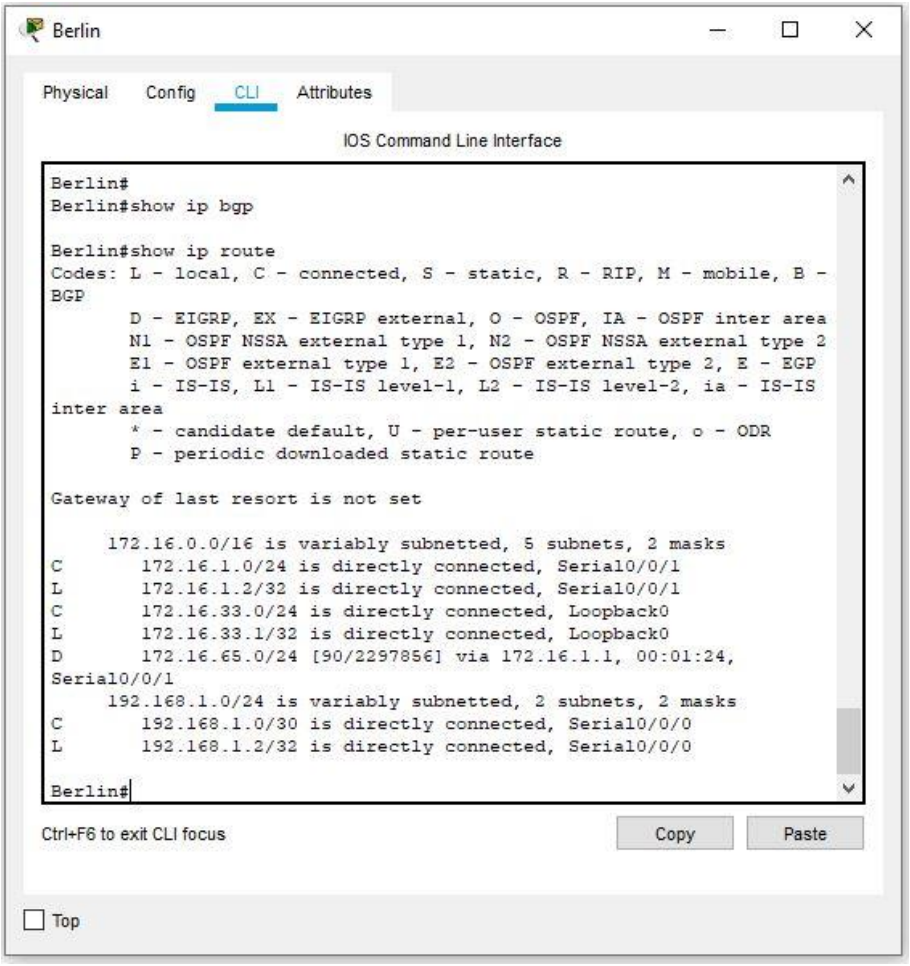
6.8 Konfigurácia funkcie next-hop

Smerovač Hamburg nevedel o prepojení medzi ISP a Berlin a Berlin nevedel o prepojení medzi ISP a Hamburg. Predtým, ako ISP mohol úspešne otestovať spojenie so všetkými internými sériovými rozhraniami AS 400, sa museli tieto sériové linky inzerovať cez BGP na smerovači ISP. To je možné vyriešiť aj pomocou protokolu EIGRP na smerovači Hamburg. Je to jedna z metód, aby ISP tieto odkazy inzeroval.



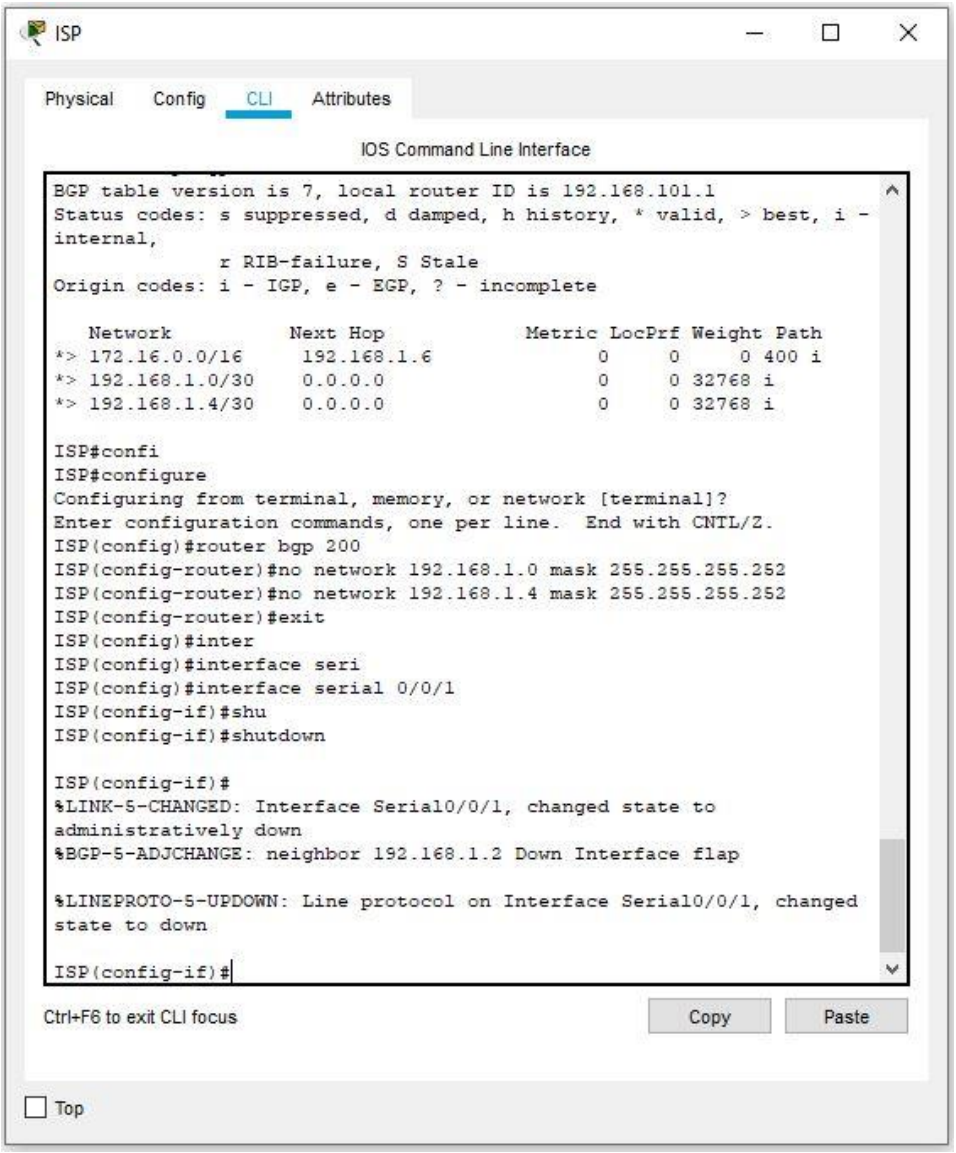
Obr. 36 Overenie, WAN odkazov do BGP na smerovači ISP

Po nastavení boli overené informácie príkazom: show ip bgp na smerovači ISP, či sa korektne vložili odkazy WAN do BGP.



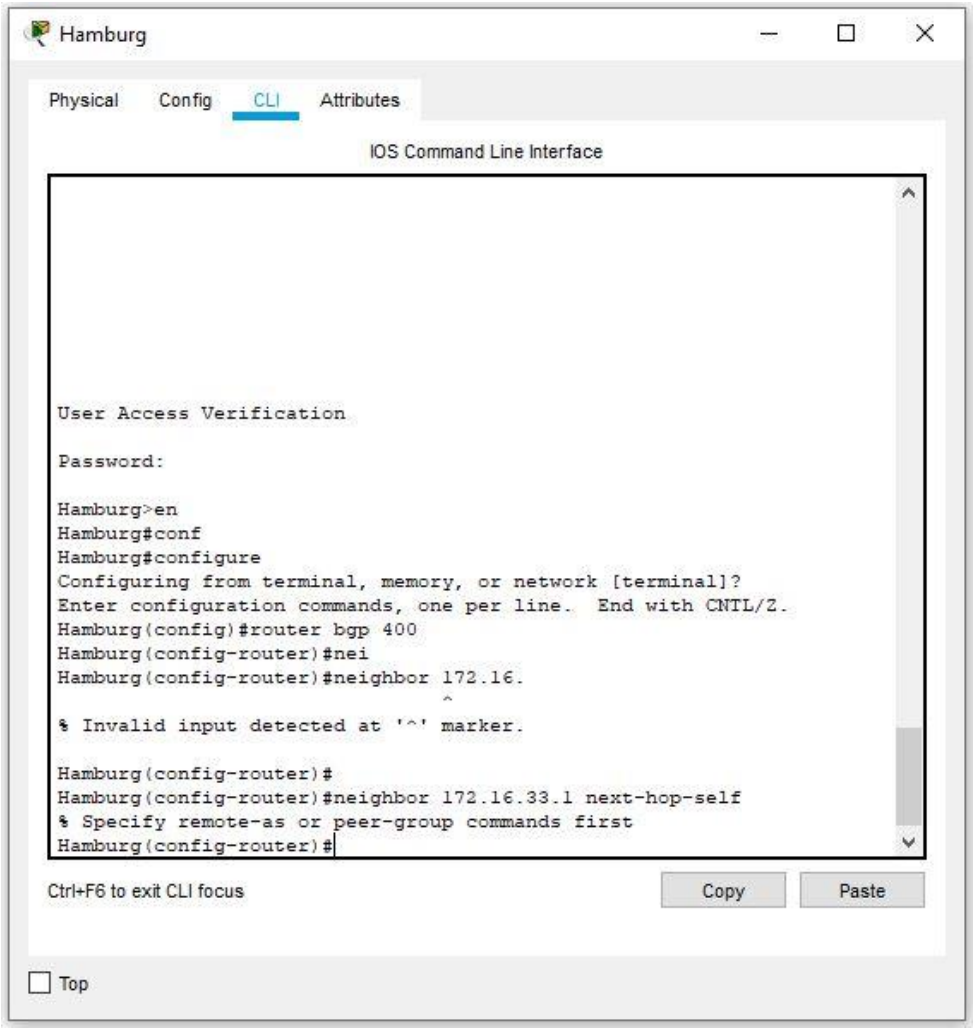
Obr. 37 Overenie EIGRP protokolu na smerovači Berlin

V ďalšom kroku je zobrazené či v smerovači Berlin je aktualizovaná smerovacia tabuľka o sieť EIGRP ktorá bola nastavená na ISP. Ako je vidieť v poslednom výpise, cesta je aktívna.



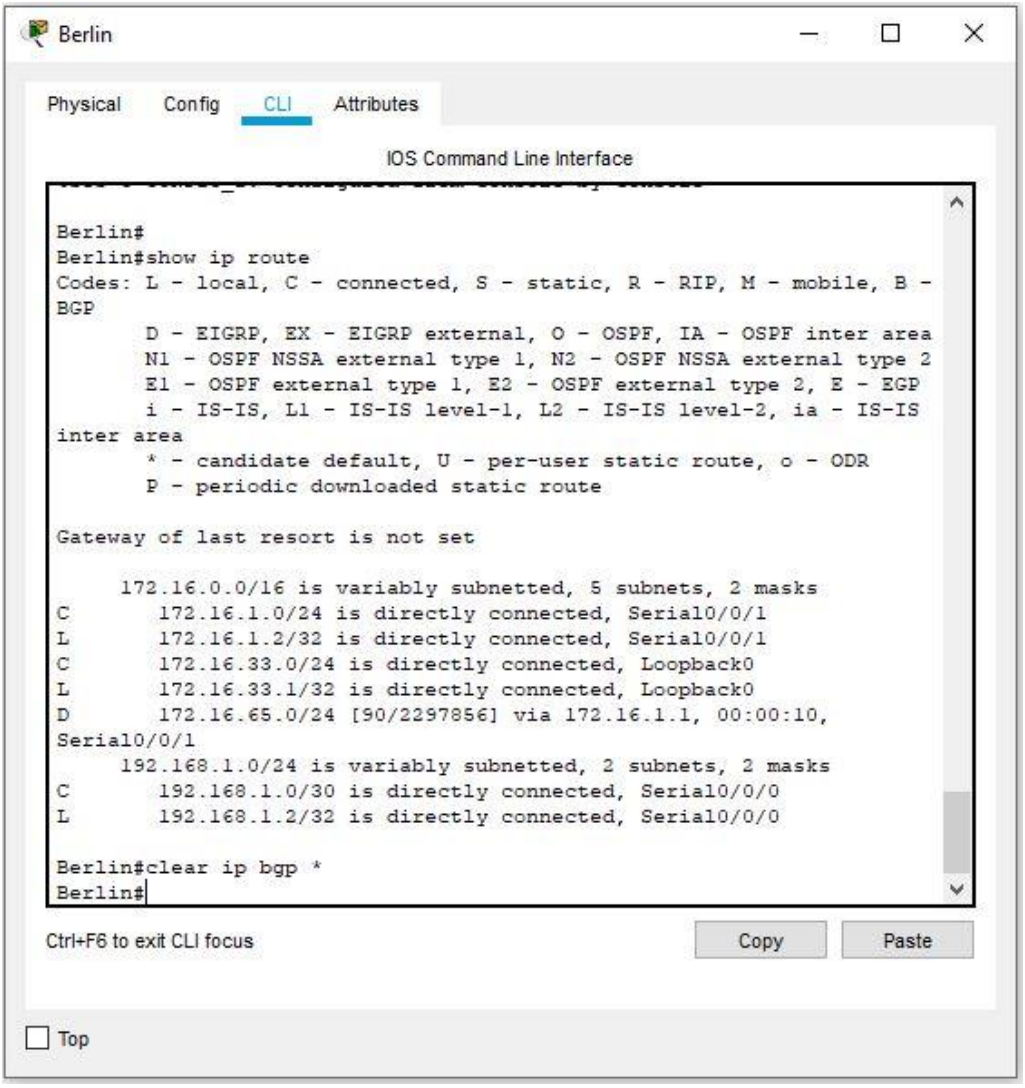
Obr. 38 Odstránenie liniek WAN na smerovači ISP.

Pre lepšie porozumenie príkazu next-hop-self, sa odstránili na ISP jeho dve WAN linky a vypli WAN spojenie medzi ISP a Berlin. Jedinou možnou cestou zo Berlin k ISP je cez smerovač Hamburg. Toto nastavenie avšak platí ak sú definované trasy cez IBGP.



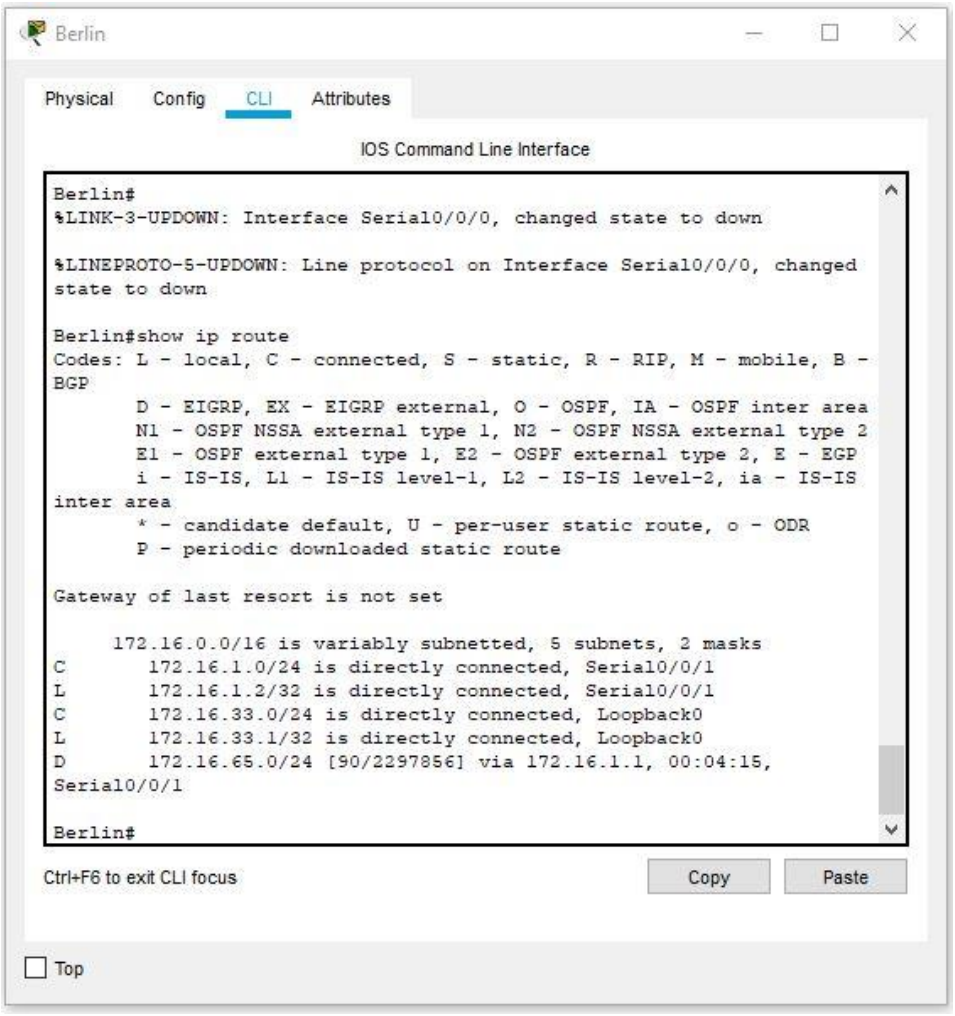
Obr. 39 Konfigurácia adries pomocou príkazu next hop self.

Pri zadávaní ďalších skokov EBGP sa adresy prenášali do IBGP nezmenené. Ak by sa chceli inzerovať ďalšie trasy, pomocou príkazu next-hop-self program Cisco Packet Tracer vypísal oznámenie že máme špecifikovať AS. Avšak príkazy nebolo možné zadať v tomto programe. V projekte sú závislé od sieti IBGP, ktoré neboli možné nakonfigurovať.



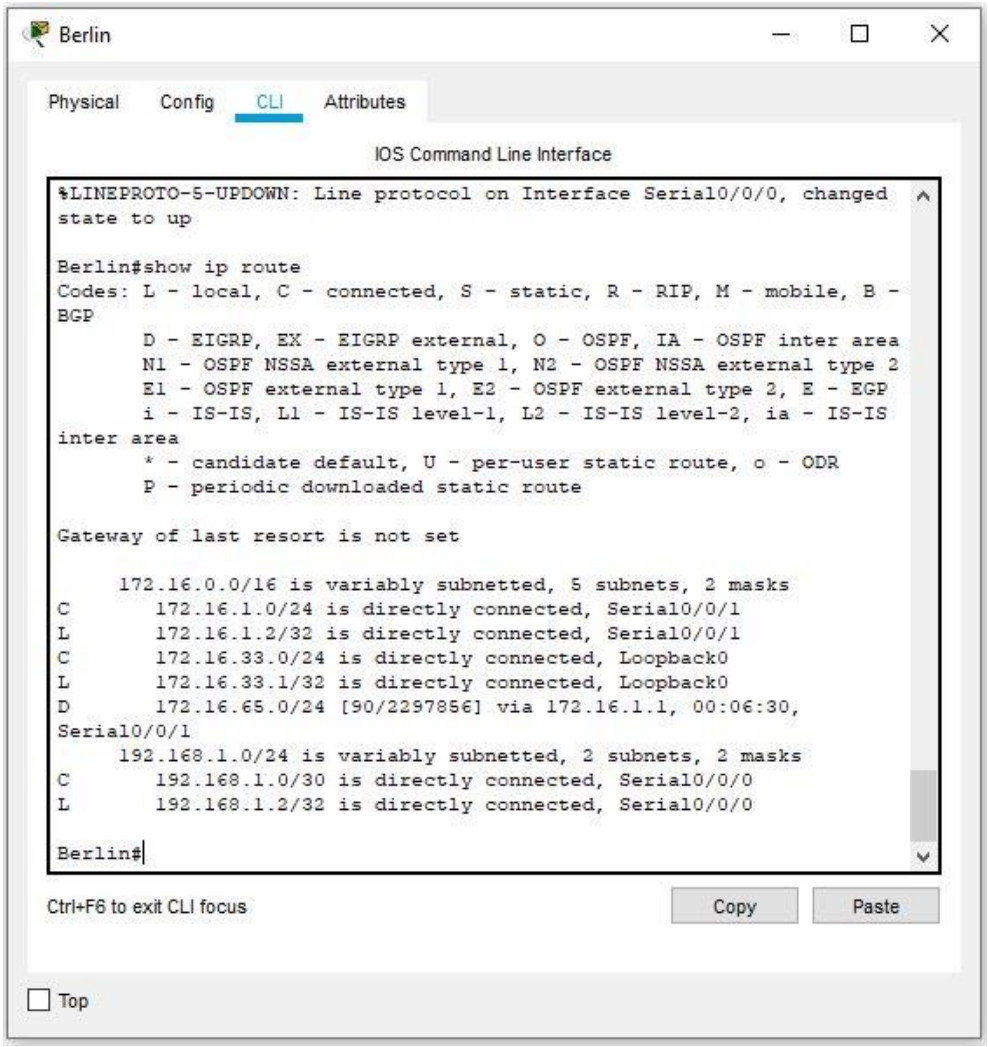
Obr. 40 Resetovanie pripojenia BGP na smerovači Berlin.

Na obrázku vyššie je zobrazené resetovanie pripojenia BGP. Pomocou ďalšieho príkazu by bolo možné zobraziť topologickú databázu BGP. Databáza ale neobsahuje žiadne smerovacie cesty s toho dôvodu že nemá nakonfigurované IBGP protokoly. Výstup s príkazového riadku bol použitý aj pri smerovači Hamburg avšak taktiež neúspešne. Ak by boli zadané protokoly IBGP, výpis by ho zobrazil. V tomto prípade by sa smerovač ISP dokázal pripojiť k smerovaču Berlín iba cez IBGP.



Obr. 41 Výpis smerovacej tabuľky Berlin.

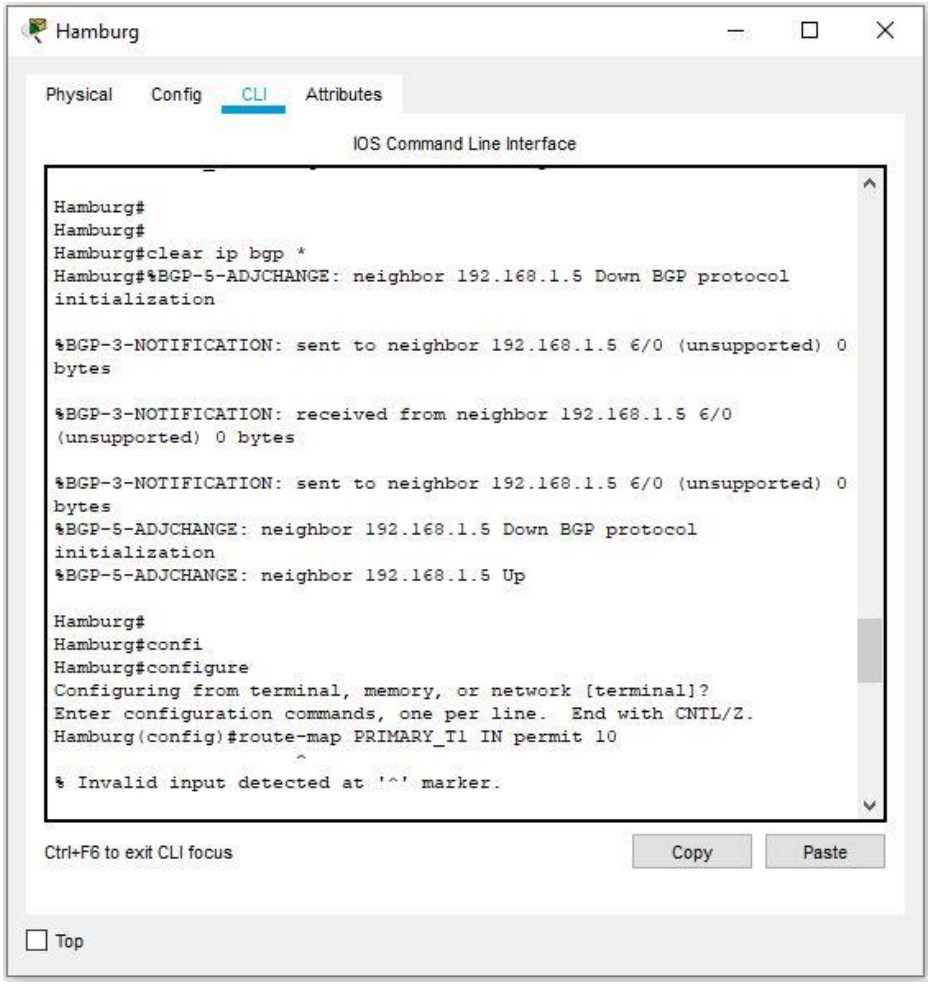
Vo výpise je vidieť že nie je aktívny sériový port s0/0/0. Aby bola možná realizácia komunikácie zo smerovačom Berlin, je zapotreby povoliť sériové pripojenie s0/0/1 na smerovači ISP.



Obr. 42 Overenie aktívnej trasy na smerovači Berlin.

6.9 Nastavenie miestnych preferencií BGP

Pretože hodnota miestnej preferencie je zdieľaná medzi susedmi IBGP, bola nakonfigurovaná jednoduchá mapa trasy, ktorá odkazuje na hodnotu miestnej preferencie na smerovače Hamburg a Berlin.



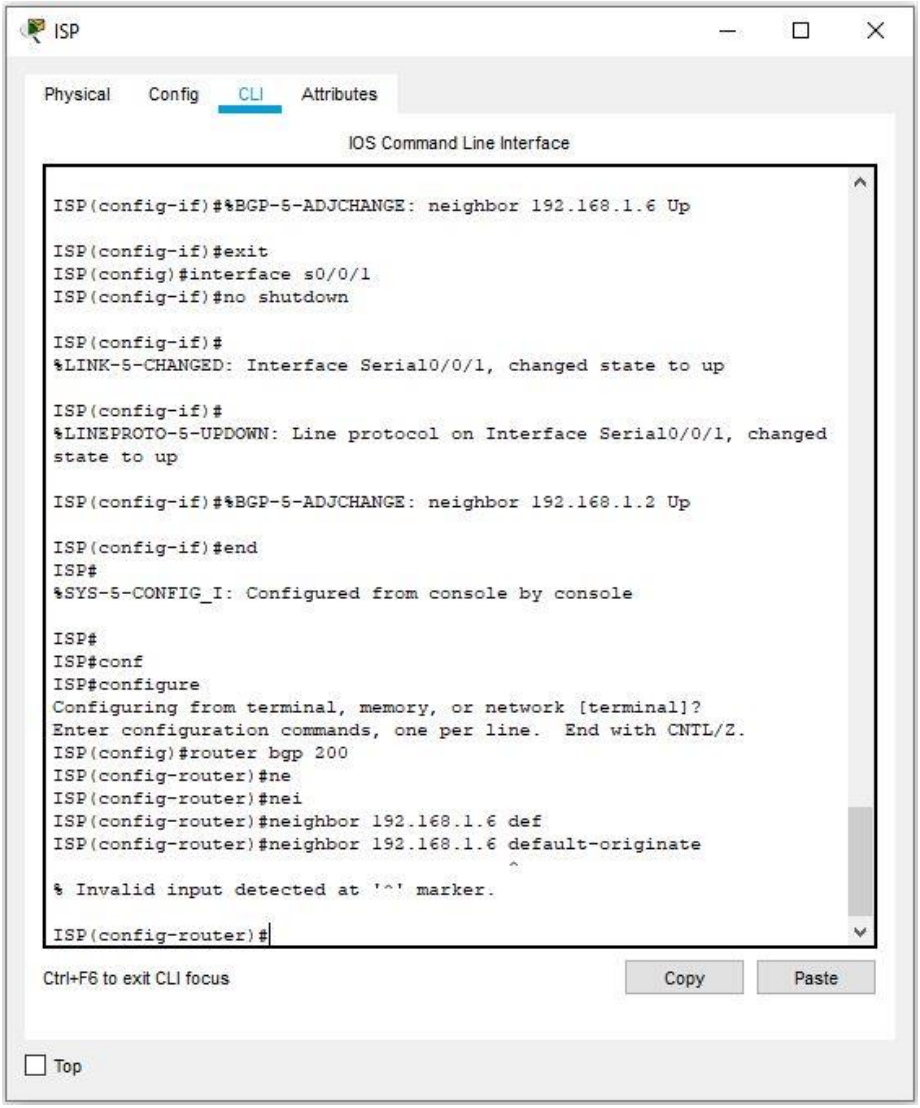
Obr. 43 Príklad konfigurácie pomocou príkazu route-map

V Cisco Packet Tracer, nebolo možné zadať príkaz route-map. Tento príkaz program nepoznal. V štandardnom výpise, ak by bol route-map povolený zobrazoval by zoznam ACL (Access Control List) ktorý by končil implicitným príkazom odmietnutia podľa návrhu konvencie. Ak počas pokusov o zhodu by dosiahol koniec mapy trasy, výsledok by závisel od konkrétnej aplikácie mapy trasy. Našťastie sa mapy trasy, ktoré sa používajú na prerozdelenie, správajú rovnakým spôsobom ako zoznamy ACL. Mapy trás často používajú zoznamy prístupových práv ako kritériá zhody.

Hlavným výsledkom vyhodnotenia prístupového zoznamu je odpoveď áno alebo nie. Zoznam ACL povoľuje alebo zakazuje vstupné údaje.

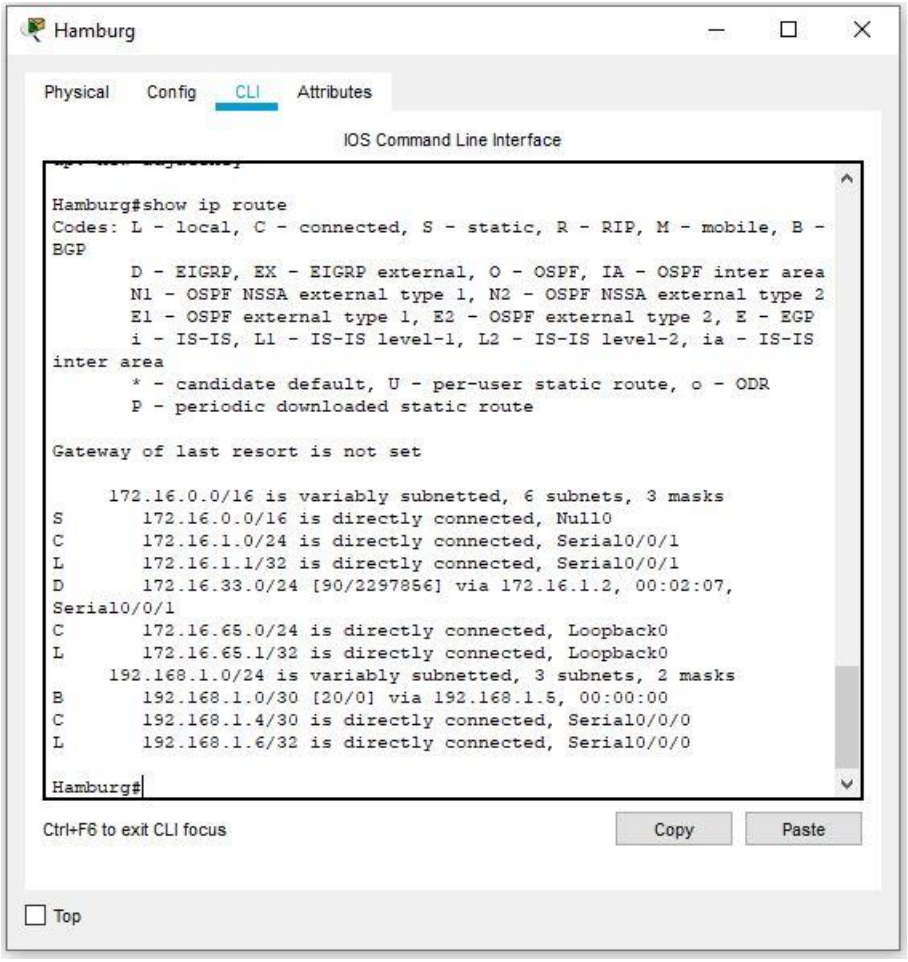
6.10 Stanovenie predvolenej trasy

V poslednom kroku je smerovač ISP nakonfigurovaný tak, aby vložil predvolenú cestu do smerovača Hamburg a Berlin pomocou BGP príkazu default-originate.



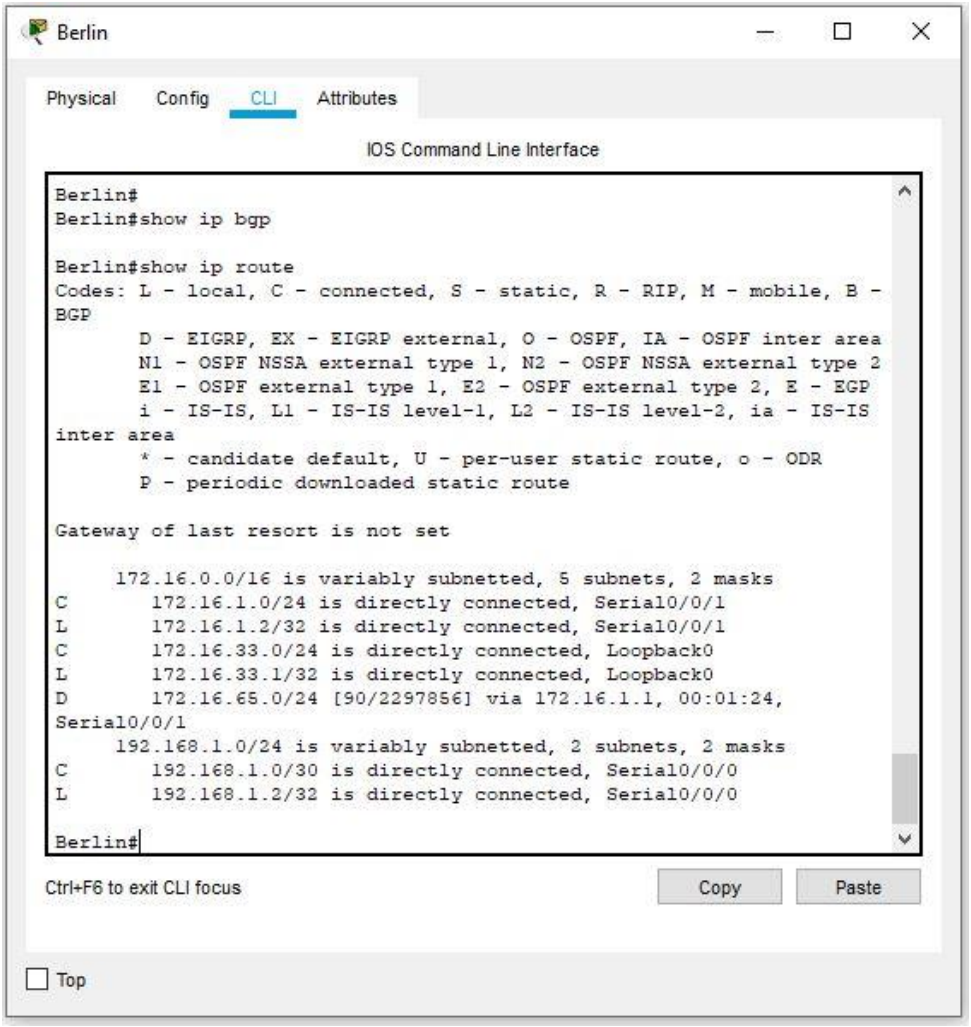
Obr. 44 Použitie príkazu default-originate na smerovači ISP.

Tento príkaz na stanovenie trasy avšak program nepozná.



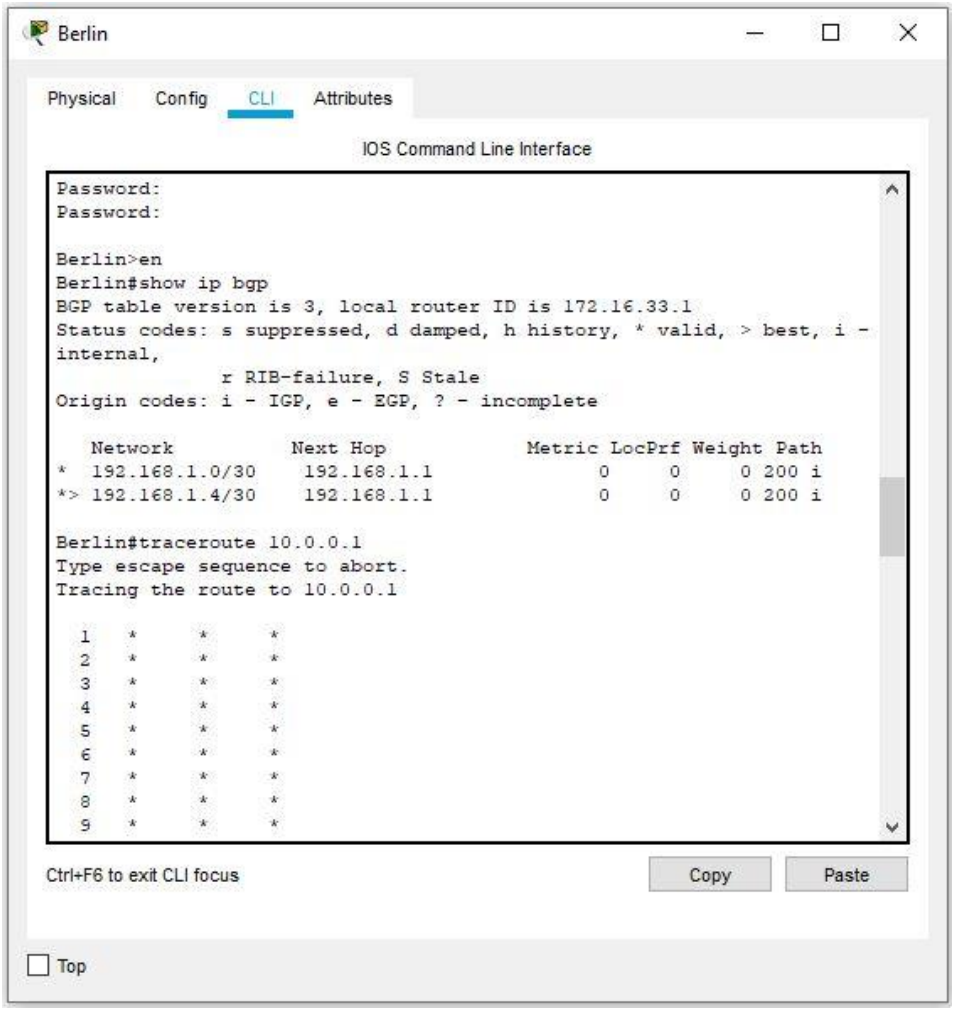
Obr. 45 Výpis príkazu ip route smerovača Hamburg.

Ak by boli stanovené predvolené trasy na smerovači ISP, výpis príkazu show ip route na smerovači Hamburg, by zobrazoval záznam vo výpise zoznamu adries na prvom mieste. Bol by označovaný ako B*, čo znamená že by sa jednalo o BGP protokol s predvolenou trasou.



Obr. 46 Výpis príkazu ip route smerovača Berlin.

Taktiež je vidieť, ak by bol použitý príkaz na stanovenie predvolenej trasy aj na tomto smerovači mali by sme záznam ktorý by bol označený ako B*. Tiež by znamenal že v zozname by bola adresa BGP s predvolenou trasou.



Obr. 47 Použitie príkazu traceroute.

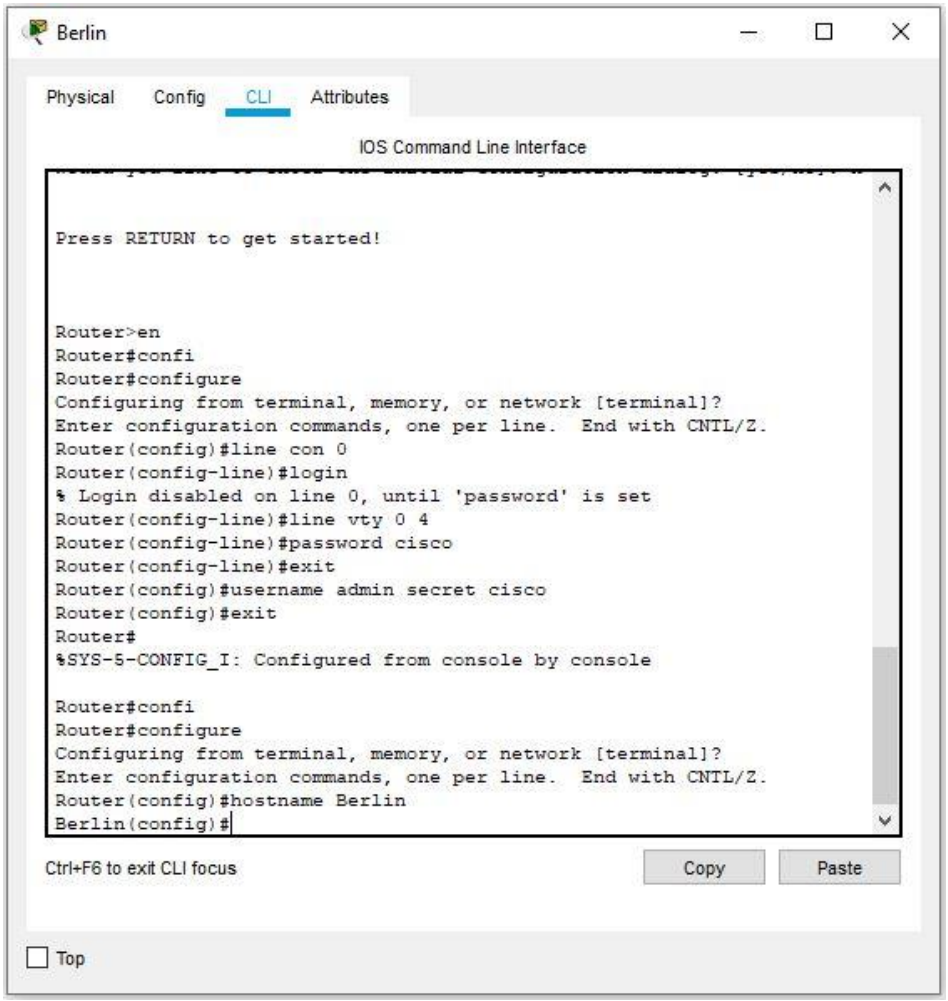
Na obrázku vyššie je vidieť že pomocou príkazu traceroute a IP adresy 10.0.0.1 bolo overené že pakety neprechádzajú a ani nepoužívajú predvolenú trasu cez smerovač Berlin. Je to zapríčinené z dôvodu obmedzenia príkazov v programe Cisco Packet Tracer.

7 VYHODNOTENIE ÚČINOSTI ZABEZPEČENIA BGP

V projekte bolo viacero úrovni zabezpečenia. Základné nastavenia smerovača ktoré boli vykonané obsahovali príkazy line con 0 a line vty 0 4.

Príkaz line con 0 slúžil na konfiguráciu pomocných portov na vzdialenú konfiguráciu a sledovanie smerovača pomocou telefonického modemu. Na rozdiel od hesiel pre konzoly a vty nebolo pomocné heslo nakonfigurované počas úvodného konfiguračného dialógu a malo by sa konfigurovať pomocou príkazu password v režime konfigurácie pomocnej linky.

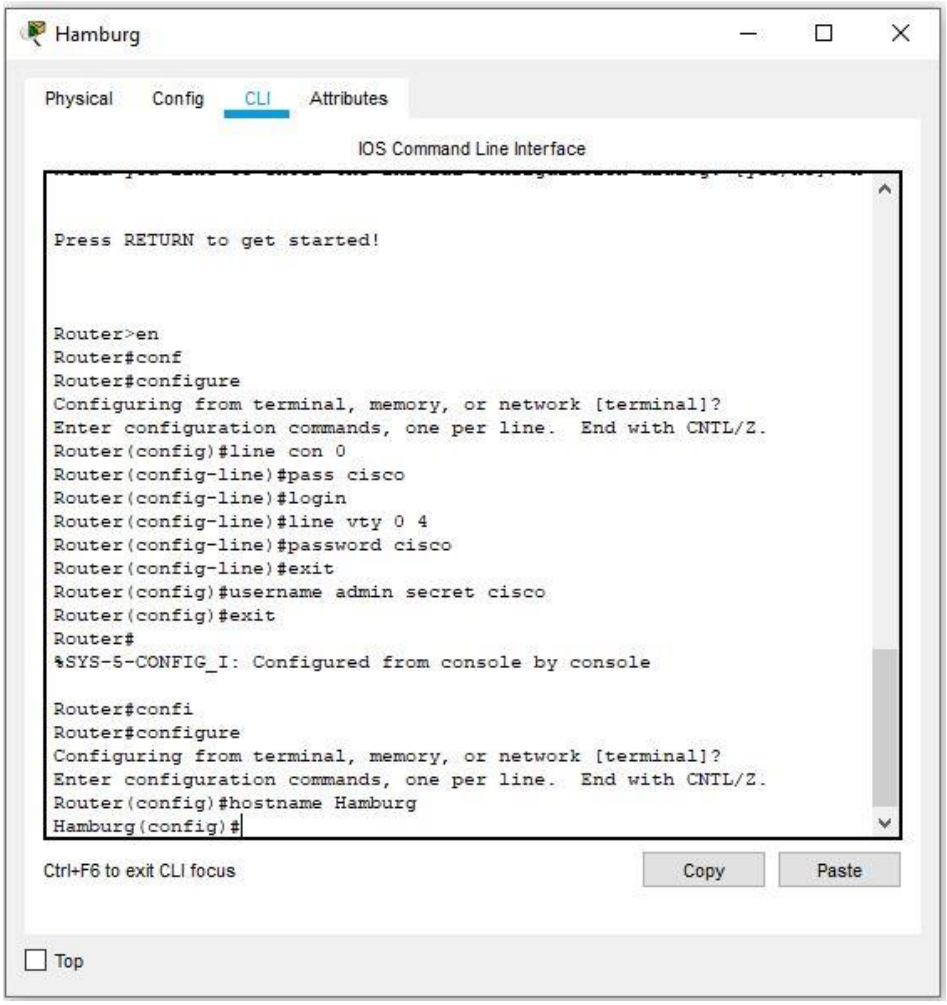
Nastavenie hesla na úrovni pomocného riadku je iba jedným z niekoľkých krokov, ktoré boli vykonané pri konfigurácii pomocného portu smerovača pre vzdialený prístup prostredníctvom dial-up.



Obr. 48 Zobrazenie konfigurácie line con 0 na smerovači Berlin.

Ako je zobrazené na výstupe z príkazového riadku hneď pod konfiguráciou pomocných portov bol zadaný príkaz line vty 0 4 s heslom cisco.

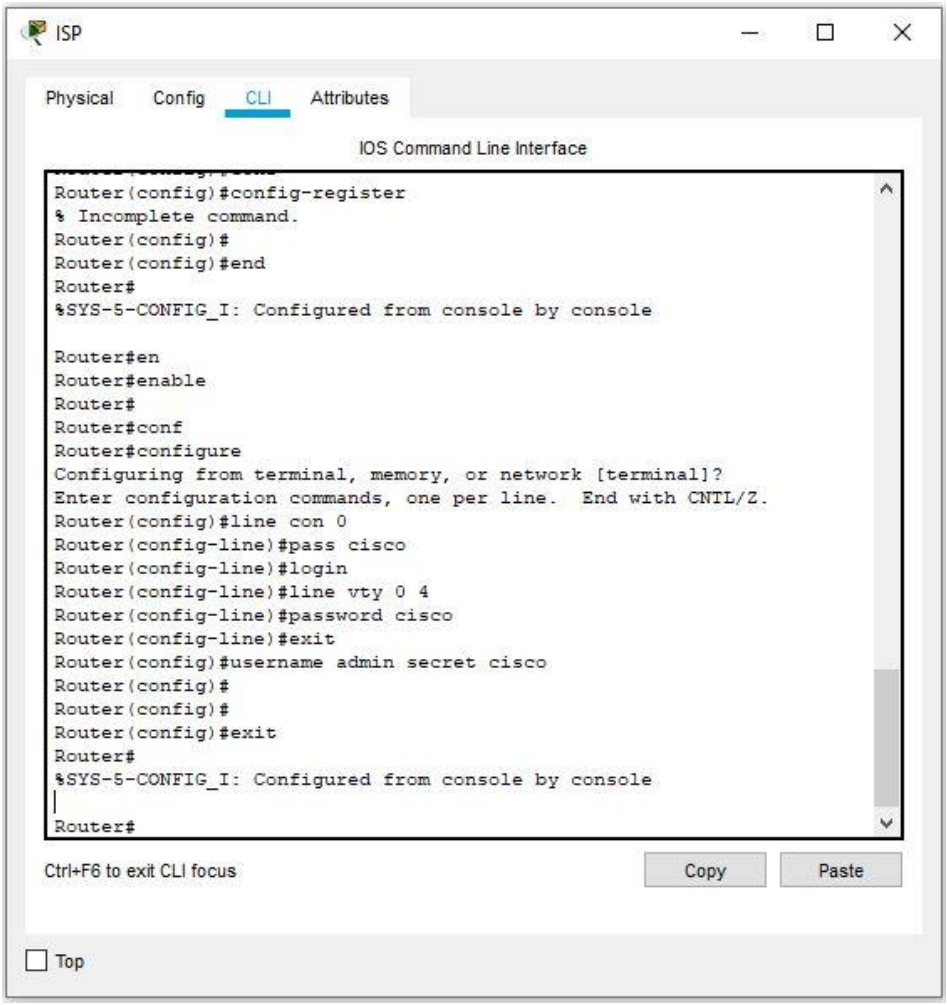
Pojem VTY (Virtual Teletype) znamená virtuálny typ písma. VTY je virtuálny port a používa sa na získanie prístupu Telnetu alebo SSH (Secure Shell Protocol) k zariadeniu. Pre získanie prístupu cez Telnet alebo SSH bolo nastavené v konzolovom príkaze heslo cisco. V skutočnosti by sa použilo silné heslo ktoré by spĺňalo požiadavky na silu hesla. VTY sa používa iba na prichádzajúce pripojenia k zariadeniu. Všetky tieto pripojenia sú virtuálne a nie je s nimi spojený žiadny hardvér. Abstrakt 0-4 znamená, že zariadenie môže umožniť 5 simultánnych virtuálnych pripojení, ktoré môžu byť Telnet alebo SSH. Svojím spôsobom môžeme povedať, že 5 (0-4) sú porty pripojenia k smerovaču alebo prepínaču. V skutočnosti je možné mať pripojovacie porty až 16 (0-15).



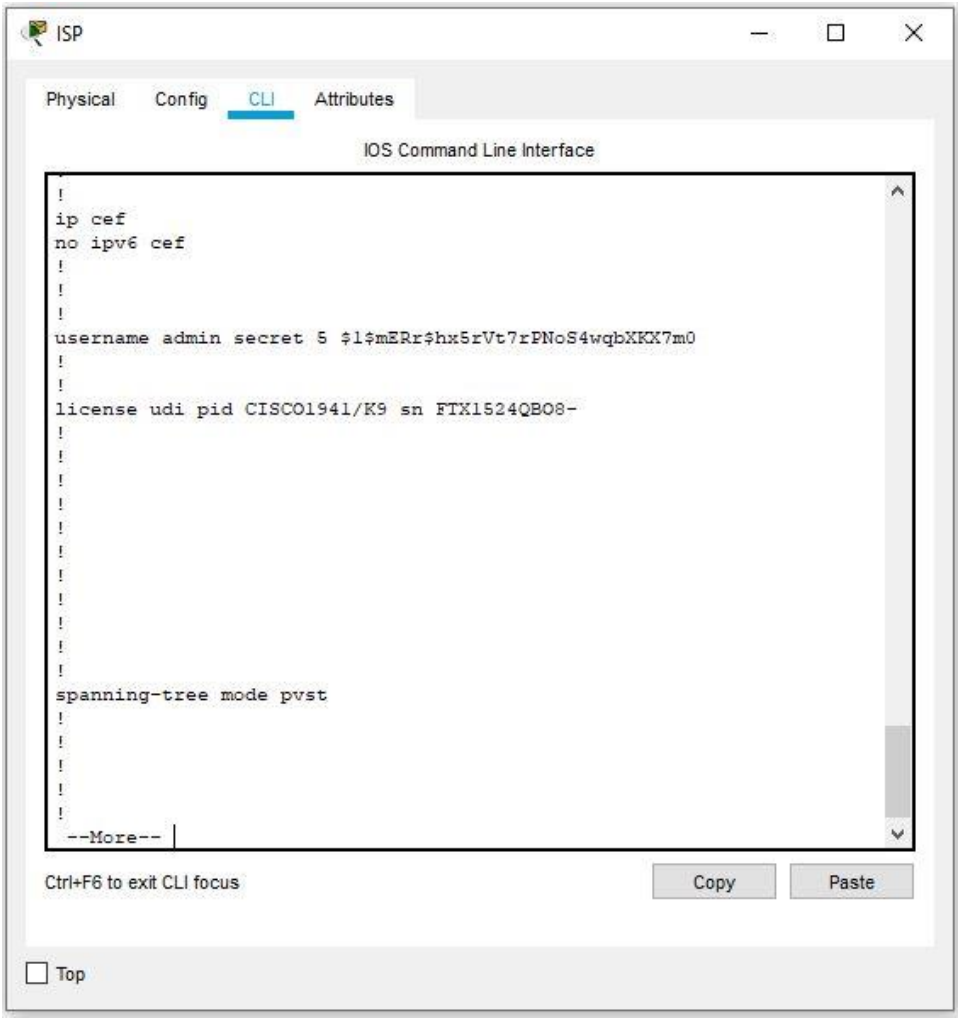
Obr. 49 Konfigurácia virtuálneho portu na smerovači Hamburg.

Príkazom username secret bola poskytnutá ďalšia vrstva zabezpečenia hesla používateľa. Je to lepšie zabezpečenie šifrovaním hesla pomocou reverzibilného šifrovania MD5 a ukladaním šifrovaného textu. Pridaná vrstva šifrovania MD5 je užitočná v prostrediach, v ktorých heslo prechádza cez sieť alebo je uložené na serveri TFTP (Trivial File Transfer Protocol).

Pomocou príkazu username secret bolo zadané meno používateľa a hash pomocou MD5, PBKDF2 (Password-Based Key Derivation Function 2), SHA-256 (Secure Hash Algorithm 256).



Obr. 50 Zobrazenie konfigurácie MD5.



Obr. 51 Zobrazenie parametrov MD5 na smerovači ISP.

Smerovače Cisco poskytujú ešte podrobnejšie zabezpečovacie funkcie na ochranu buď smerovača alebo aj celej dátovej komunikácie. V projekte boli zobrazené len tie najnákladnejšie, nakoľko vizualizačný program je obmedzený konfiguráciou ďalších BGP protokolov ktoré boli zmieňované v projekte.

ZÁVĚR

Každú sekundu milióny hostiteľov pošlú miliardy paketov cez internet ďalším hostiteľom. Poskytovatelia internetových služieb ISP používajú protokol BGP, aby sa navzájom informovali, ktorá IP adresa smeruje kam. Protokol BGP je tiež užitočný pre organizácie koncových používateľov, ktoré požadujú spoľahlivé pripojenie k internetu prostredníctvom dvoch alebo viacerých poskytovateľov internetových služieb. BGP je smerovací protokol, ktorý si vymieňa smerovacie informácie cez internet, a je jediným protokolom, ktorý dokáže pracovať so sieťou s veľkosťou internetu. Je to tiež jediný protokol, ktorý si dobre poradí s viacerými pripojeniami k nesúvisiacim smerovacím doménam. V prípade výpadku siete BGP prepočíta cestu tak, aby sa pakety mohli vyhnúť problémovej oblasti a nepretržite prúdiť. BGP je sprievodca po všetkých aspektoch. V práci sme popisovali, ako zabezpečiť BGP a ako sa dá BGP použiť na boj proti útokom DDoS. Aj keď príklady v tejto práci sú určené pre smerovače Cisco, diskutované techniky je možné aplikovať na akýkoľvek smerovač podporujúci protokol BGP.

SEZNAM POUŽITÉ LITERATURY

[1] Historical Maps of Computer Networks [online]. University of Manchester: Martin Dodge, 2007 [cit. 2021-02-07]. Dostupné z: https://personalpages.manchester.ac.uk/staff/m.dodge/cybergeography/atlas/historical.html.

[2] VAN BEIJNUM, Iljitsch. BGP: Building Reliable Networks with the Border Gateway Protocol. 1005 Gravenstein Highway North, Sebastopol, CA 95472: Published by O'Reilly & Associates, September 2002. ISBN 978-0596002541.

[3] The TCP/IP Guide: A Comprehensive, Illustrated Internet Protocols Reference. San Francisco, California: No Starch Press, 2005. ISBN 978-1593270476.

[4] What is the Internet Protocol? [online]. San Francisco, California, U.S.: Cloudflare, 2019 [cit. 2021-03-01]. Dostupné z: https://www.cloudflare.com/learning/network-layer/internet-protocol/.

[5] IP Protocol Header Fundamentals Explained with Diagrams [online]. Los Angeles: HIMANSHU ARORA, 2012 [cit. 2021-02-07]. Dostupné z: https://www.thegeekstuff.com/2012/03/ip-protocol-header/.

[6] What is RIP (Routing Information Protocol)? [online]. G-773, Ground Floor, Suncity, Sector 54, Gurugram, Haryana 122002, India: After Academy, 2020 [cit. 2021-02-07]. Dostupné z: https://afteracademy.com/blog/what-is-rip-routing-information-protocol.

[7] OSPF Network Topology [online]. San Jose: Cisco netacad, 2012 [cit. 2021-03-07]. Dostupné z: https://static-course-assets.s3.amazonaws.com/RSE503/en/index.html#8.2.1.1

[8] IP Routing: BGP Configuration Guide, Cisco IOS Release 15M&T [online]. 170West Tasman Drive San Jose, CA 95134-1706 USA: Cisco Systems, 2019 [cit. 2021-03-01]. Dostupné z: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_bgp/configuration/15-mt/irg-15-mt-book.html.

[9] KOCHARIANS, Narbik a Terry VINSON. CCIE routing and switching v5.0 official cert guide: volume 2. Fifth edition. Indianapolis, IN: Cisco Press, 2015. ISBN 978-1-58714-491-2

[10] ZHANG, Randy a Micah BARTELL. BGP Design and Implementation. 800 East 96th Street, 3rd Floor Indianapolis, IN 46240 USA: Cisco Press, December 2003. ISBN 978-1587051098.

[11] TEARE, Diane. Implementing Cisco IP routing (ROUTE) foundation learning guide. Indianapolis, IN: Cisco Press, c[2015]. ISBN 978-1-58720-456-2.

[12] Proceso de establecer una relación de pares BGP. In: Forum Huawei [online]. Shenzhen, China: Gustavo.HdzeF, 2019 [cit. 2021-02-07]. Dostupné z: https://forum.huawei.com/enterprise/es/proceso-de-establecer-una-re-laci%C3%B3n-de-pares-bgp/thread/505921-100235.

[13] BGP Aggregate-Address Using Communities. In: CCIE Blog [online]. London: deniart, 2008 [cit. 2021-02-07]. Dostupné z: https://ccieblog.co.uk/bgp/bgp-aggregate-address-using-communities.

[14] What Is BGP? [online]. San Francisco: Cloudflare, c2021 [cit. 2021-03-07]. Dostupné z: https://www.cloudflare.com/learning/security/glossary/what-is-bgp/.

[15] Autonomous Systems for BGP Sessions: Understanding the BGP Local AS Attribute [online]. Sunnyvale, California: Juniper Network, 2020 [cit. 2021-02-18]. Dostupné z: https://www.juniper.net/documentation/en_US/junos/topics/topic-map/autonomous-systems.html.

[16] 3.4 EIGRP Operation Overview. In: Stuck in active [online]. United States: Stuck in active, 2019 [cit. 2021-02-07]. Dostupné z: https://stucknactive.com/2019/03/12/3-4-eigrp-operation-overview/

[17] LUCENT, Alcatel a Colin BOOKHAM. Versatile Routing and Services with BGP: Understanding and Implementing BGP in SR-OS. 10475 Crosspoint Boulevard Indianapolis, IN 46256: John Wiley, 2014. ISBN 978-1118875285.

[18] SRIRAM, Kotikalapudi a Doug MONTGOMERY. Resilient Interdomain Traffic Exchange: BGP Security and DDoS Mitigation. NIST [online]. 100 Bureau Dr, Gaithersburg, MD 20899, United States: National Institute of Standards & Technology, 2019, 2019 [cit. 2021-02-07]. Dostupné z: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-189.pdf

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

ADM	Add/Drop Multiplexer
ACL	Acccess Control List
AH	Authentication Header
AMS-IX	Amsterdam Internet Exchange
APNIC	Asia Pacific Network Information Centre
ARP	Address Resolution Protocol
ARPANET	Advanced Research Projects Agency Network
AS	Autonomous System
ATM	Asynchronous Transfer Mode
BGP	Border Gateway Protocol
CEF	Cisco Express Forwarding
CIDR	Classless Inter-Domain Routing
CLNS	Connectionless-Mode Network Service
CMIP	Common Management Interface Protocol
CPU	Central Processing Unit
CRC32	Cyclic Redundancy Check 32
DCC	Data Communications Channel
DCE	Data Communications Equipment
DCN	Data Communications Network
DDoS	Distributed Denial of Service
DE-CIX	Deutsche Commercial Internet Exchange
DoS	Denial of Service
DTE	Data Terminal Equipment
DUAL	Diffusing Update Algorithm

eBGP	External Border Gateway Protocol
EGP	Exterior Gateway Protocol
EIGRP	Enhanced Interior Gateway Routing Protocol
ES	End System
ESP	Encapsulating Security Payload
EXEC	Execute Cisco IOS Commands
FDDI	Fiber Distributed Data Interface
FIB	Forwarding Information Base
FIX	Federal Internet Exchange
FSM	Finite-State Machine
FTAM	File Transfer Access Method
GGP	Gateway to Gateway Protocol
iBGP	lnternal Border Gateway Protocol
ICMP	Internet Control Message Protocol
ICMPv6	Internet Control Message Protocol version 6
IDPR	Inter Domain Policy Routing
IGP	Interior Gateway Protocol
IGRP	Internal Gateway Routing Protocol
IOS	Internetwork Operating System
IP	Internet Protocol
IPSec	Internet Protocol Security
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
IS	Intermediate System
IS-IS	Intermediate System to Intermediate System
ISP	Internet Service Provider

IX	Internet Exchange
LAN	Local Area Network
LINX	The London Internet Exchange
MAE	Metropolitan Area Exchange
MD5	Message-Digest Algorithm 5
MDT	Multicast Distribution Tree
MPLS	Multiprotocol Label Switching
MSF	Metropolitan Fiber Systems
NAP	Network Access Points
NBMA	Non-Broadcast Multiple Access
NPC	Network Control Protocol
NDB	Network Descriptor Block
NE	Network Elements
NFSNET	National Science Foundation Network
NISCC	The National Infrastructure Security Co-ordination Centre
NRLI	Network Layer Reachability Information
NSAP	Network Service Access Point Address
OSPF	Open Shortest Path First
PBKDF2	Password-Based Key Derivation Function 2
PE	Provider Edge
POP	Point of Presence
QoS	Quality of Service
RD	Route Distinguisher
RDB	Routing Descriptor Blocks
RFC	Request For Comments
RIB	Routing Information Base

RIP	Routing Information Protocol
RIPE	Réseaux IP Européens
SDH	Synchronous Digital Hierarchy
SHA-256	Secure Hash Algorithm 256
SMDS	Switched Multi Megabit Data Service
SONET	Synchronous Optical Network
SPF	Shortest Path First
SR-OS	Service Router Operating System
SRP	Server Routing Protocol
SSH	Secure Shell Protocol
TCP	Transmission Control Protocol
TFTP	Trivial File Transfer Protocol
TP4	Transport Protocol 4
TTL	Time to Live
UDP	User Datagram Protocol
UPS	Uninterruptible Power Supply
VBNS	Very high Bandwidth Network Service
VLSM	Variable Length Subnet Mask
VPN	Virtual Private Network
VRF	Virtual Routing and Forwarding
VTY	Virtual Teletype
WAN	Wide Area Network

SEZNAM OBRÁZKŮ