VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

Fakulta elektrotechniky
a komunikačních technologií

BAKALÁŘSKÁ PRÁCE

Brno, 2016 Miroslav Šiklóši

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ
FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION

ÚSTAV TELEKOMUNIKACÍ
DEPARTMENT OF TELECOMMUNICATIONS

TŘI SCÉNÁŘE SIMULACE GLOBÁLNÍHO CHOVÁNÍ INTERNETU
THREE SCENARIOS OF SIMULATION OF GLOBAL INTERNET BEHAVIOR

BAKALÁŘSKÁ PRÁCE
BACHELOR'S THESIS

AUTOR PRÁCE
AUTHOR
Miroslav Šiklóši

VEDOUCÍ PRÁCE
SUPERVISOR
Ing. Jan Jeřábek, Ph.D.

BRNO 2016

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ

Bakalářská práce

bakalářský studijní obor **Teleinformatika**
Ústav telekomunikací

Student: Miroslav Šiklóši ***ID:*** 164414
Ročník: 3 ***Akademický rok:*** 2015/16

NÁZEV TÉMATU:

Tři scénáře simulace globálního chování Internetu

POKYNY PRO VYPRACOVÁNÍ:

V rámci semestrálního projektu nastudujte problematiku fungování Internetu především z pohledu autonomních systémů (AS), BGP protokolu, tranzitu, peeringu, možností odpojování či připojování konkrétních AS, toků dat a jejich ovlivňování, systému DNS a samozřejmě bezpečnosti. Vytipujte vhodné simulační prostředí (GNS3, NS3 či jiný simulátor). Navrhněte topologii sítě a obrysy minimálně tří názorných a smysluplných scénářů a řešení rozpracujte. V rámci bakalářské práce proveďte kompletní implementaci navržených scénářů ve vybraném simulačním prostředí a vytvořte dokumentaci ve formě detailních laboratorních návodů.

DOPORUČENÁ LITERATURA:

[1] TEARE, Diane. Implementing Cisco IP routing (ROUTE): foundation learning guide : foundation learning for the ROUTE 642-902 exam. Indianapolis: Cisco Press, 2010, xxix, 945 s. ISBN 978-1-58705-882-0.

[2] Dynamic Network Services: Internet Performance, Research [online]. Dyn, ©2015 [cit. 2015-09-11]. Dostupné z: http://research.dyn.com/.

[3] JEŘÁBEK, Jan. Pokročilé komunikační techniky. Skriptum FEKT Vysoké učení technické v Brně, 2015. s. 1-193.

Termín zadání: 1.2.2016 ***Termín odevzdání:*** 1.6.2016

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

doc. Ing. Jiří Mišurec, CSc., *předseda oborové rady*

ABSTRAKT

Cieľom tejto bakalárskej práce bolo vytvoriť tri laboratórneho úlohy v simulačnom prostredí GNS3. Teoretická časť práce obsahuje základné informácie potrebné na vypracovanie a pochopenie jednotlivých úloh. Prvá úloha je zameraná na komplexnú konfiguráciu BGP protokolu na Cisco smerovačoch. Druhá úloha poukazuje na rozdiely medzi tranzitným a peeringovým spojením. Tretia úloha demonštruje základné princípy fungovania bezpečnostného rozšírenia systému DNS.

KĽÚČOVÉ SLOVÁ

Active Directory, Autonómny systém, BGP, Cisco, DNS, DNSSEC, GNS3, Iperf3, tranzit, peering, Windows Server

ABSTRACT

The goal of this bachelor thesis was to create three laboratory tasks in simulation enviroment GNS3. Teoretical part of thesis contains basic informations to accomplish those tasks. First task is oriented to komplex configuration of BGP protocol on Cisco routers. Second task shows differencies between transit and peering connection. Last task is demonstrating basic principals of security extension of DNS system.

KEYWORDS

Active Directory, Autonomous system, BGP, Cisco, DNS, DNSSEC, GNS3, Iperf3, transit, peering, Windows Server

ŠIKLÓŠI, Miroslav *Tři scénáře simulace globálního chování Internetu*: bakalárska práca. Brno: Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, Ústav telekomunikací, 2016. 65 s. Vedúci práce bol prof. Ing. Jan Jeřábek, Ph.D.

VYHLÁSENIE

Vyhlasujem, že som svoju bakalársku prácu na tému „Tři scénáře simulace globálního chování Internetu“ vypracoval samostatne pod vedením vedúceho bakalárskej práce, využitím odbornej literatúry a ďalších informačných zdrojov, ktoré sú všetky citované v práci a uvedené v zozname literatúry na konci práce.

Ako autor uvedenej bakalárskej práce ďalej vyhlasujem, že v súvislosti s vytvorením tejto bakalárskej práce som neporušil autorské práva tretích osôb, najmä som nezasiahol nedovoleným spôsobom do cudzích autorských práv osobnostných a/alebo majetkových a som si plne vedomý následkov porušenia ustanovenia § 11 a nasledujúcich autorského zákona Českej republiky č. 121/2000 Sb., o práve autorskom, o právach súvisiacich s právom autorským a o zmene niektorých zákonov (autorský zákon), v znení neskorších predpisov, vrátane možných trestnoprávnych dôsledkov vyplývajúcich z ustanovenia časti druhej, hlavy VI. diel 4 Trestného zákoníka Českej republiky č. 40/2009 Sb.

Brno ....

podpis autora

POĎAKOVANIE

Rád by som poďakoval vedúcemu bakalárskej práce pánovi Ing. Janu Jeřábkovi, Ph.D. za odborné vedenie, konzultácie, trpezlivosť a podnetné návrhy k práci.

Brno ....

podpis autora

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

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

POĎAKOVANIE

Výzkum popsaný v tejto bakalárskej práci bol realizovaný v laboratóriách podporených projektom SIX; registračné číslo CZ.1.05/2.1.00/03.0072, operačný program Výzkum a vývoj pro inovace.

Brno . . . . . .

. . . . . .

podpis autora

EVROPSKÁ UNIE
EVROPSKÝ FOND PRO REGIONÁLNÍ ROZVOJ
INVESTICE DO VAŠÍ BUDOUCNOSTI

OBSAH

ZOZNAM OBRÁZKOV

ZOZNAM TABULIEK

ÚVOD

V dnešnej dobe pri vytváraní nových sieťových riešení nestačí sieť len navrhnúť a implementovať, ale pred nasadením do reálnej siete je veľmi dôležité každé navrhnuté riešenie otestovať. Neotestované riešenia by mohli mať katastrofálne dopady nielen na použitý hardvér, ale hlavne na bezpečnosť siete a dát. Vyhnutie sa takýmto situáciám je možné použitím vhodného simulačného prostredia, ktoré je schopné otestovať skutočnosti bez nutnosti nákupu reálneho hardvéru alebo ohrozenia bezpečnosti. Simulačné prostredie nemusí slúžiť len na testovanie, ale je tiež vhodné pre študentov a ľudí zaujímajúcich sa o problematiku počítačových sietí. V poslednej dobe sa stále viac obľúbeným stáva simulačné prostredie GNS3 (Graphical Network Simulator-3), ktoré dokáže simulovať nielen rôzne sieťové prvky, ale tiež rôzne koncové stanice.

Cieľom tejto bakalárskej práce je vytvoriť laboratórne úlohy v simulačnom prostredí GNS3, ktoré sa zameriavajú na správanie globálneho Internetu, funkcie smerovacieho protokolu BGP, ovplyvňovaniu toku dát a systém DNS.

V teoretických častiach práce sa nachádzajú základné informácie potrebné na vypracovanie a pochopenie jednotlivých laboratórnych úloh. V úvode každej laboratórnej úlohy sa nachádza stručný opis danej problematiky spolu s obrázkom topológie, za ktorým nasleduje opis postupu riešenia a ukážka použitých príkazov s odpoveďami na zadané otázky. V prílohe sa nachádza celá konfigurácia v kopírovateľnom formáte.

Laboratórne úlohy sú koncipované s predpokladom na základné znalosti konfigurácie Cisco smerovačov, Linux terminálu a práce s OS Microsoft Windows 8.1 a Microsoft Windows Server 2012 R2.

1 SIMULAČNÉ PROSTREDIE GNS3

GNS3 je grafický sieťový simulátor, ktorý umožňuje emuláciu komplexných sietí. [1] Podobne ako VMWare alebo VirtualBox umožňujú emulovať rôzne operačné systémy, GNS3 emuluje sieťové prvky.[2] K tomu využíva rôzne emulátory, ktoré sú zhrnuté v tabuľke 1.1.[3]

Tab. 1.1: Typy emulátorov v GNS3

Emulátor	**Emulované zariadenia**
Dynamips	Cisco smerovače
Qemu	Cisco ASA firewall, Juniper a Vyatta smerovače, Linuxové stanice
Pemu	Variácia Qemu emulátoru využívaná pre emuláciu PIX firewallu
VirtualBox	Juniper a Vyatta smerovače, Linux a Windows stanice

GNS3 je vhodný nástroj nielen pri príprave na Cisco certifikácie (CCNA, CCNP a CCIE), ale svoje využitie má aj vo firemnej sfére ako testovacie prostredie. Veľkou výhodou je obrovská komunita ľudí, ktorí sa o svoje skúsenosti delia na oficiálnom fóre.

Dynamips

Dynamips je emulátor operačných systémov IOS od firmy Cisco, ktorý vytvoril Christopher Fillot.[4] Prekladá inštrukcie z IOS obrazu, pôvodne určené pre MIPS (Microprocessor without Interlocked Pipeline Stages) procesory na inštrukcie kompatibilné s procesormi Intel (Integrated Electronics) a AMD (Advanced Micro Devices). Vďaka tomu je kompatibilný s operačnými systémami Windows, Linux a MacOS (Macintosh Operating System).

V súčasnej dobe nie je schopný emulovať Cisco prepínače. Problém je v tom, že prepínače spracovávajú niektoré operácie hardvérovo. Možným riešením je použiť EtherSwitch modul v smerovači, ale ani takéto riešenie nezabezpečí všetky funkcie reálneho prepínača.

Qemu a Pemu emulátory

Qemu (Quick Emulator) je open-source emulátor Cisco ASA firewallov, Linuxových staníc a smerovačov Juniper a Vyatta. Emuluje CPU využitím dynamického binárneho prekladu.[5]

Pemu emulátor je variáciou Qemu emulátoru. Je využívaný na emuláciu staršieho Cisco PIX firewallu.

VirtualBox

Oracle VM VirtualBox je výkonný virtualizačný nástroj využívaný nielen na súkromné účely, ale taktiež vo firemnej sfére. Je kompatibilný s operačnými systémami Windows, Linux a MacOS. Umožňuje virtualizáciu rôznych verzií operačných systémov Windows, Linux, BSD, Solaris a iných.[6]

Využitím VirtualBoxu je možné do simulovanej siete implementovať rôzne virtualizované stanice.

2 SMEROVANIE V INTERNETE

2.1 Čo je Internet

Internet je počítačová sieť prepájujúca stovky miliónov počítačových zariadení po celom svete.[7] Umožňuje komunikáciu a výmenu dát medzi koncovými systémami. Koncové systémy sú prepojené prostredníctvom siete komunikačných liniek a paketových prepínačov. Existuje niekoľko druhov prepínačov paketov, ale dva najčastejšie typy prepínačov v dnešnom Internete sú smerovače (routers) a prepínače spojovej vrstvy (switches). Oba typy prepínačov predávajú pakety smerom k ich konečnému cieľu. Prepínače spojovej vrstvy sa väčšinou používajú v prístupových sieťach, pričom smerovače sa väčšinou používajú v jadre siete. Postupnosť komunikačných spojení a paketových prepínačov, ktorými prejde paket z vysielacieho koncového systému k prijímaciemu koncovému systému, sa nazýva trasa alebo cesta cez sieť.

Koncové systémy pristupujú do Internetu prostredníctvom poskytovateľov internetových služieb (Internet Service Provider, ISP), vrátane miestnych ISP, ako napríklad miestne káblové alebo televízne spoločnosti, firemné a univerzitné ISP. Každý poskytovateľ internetových služieb je sám o sebe sieť paketových prepínačov a komunikačných liniek. Poskytovatelia internetových služieb ďalej poskytujú prístup do Internetu poskytovateľom tým, že pripojujú webové stránky (resp. servery, na ktorých bežia) priamo do Internetu.

Internet je hlavne vzájomné prepojenie koncových systémov, takže poskytovatelia, ktorí poskytujú prístup ku koncovým systémom, musia byť tiež prepojení. Títo poskytovatelia nižšej úrovne sú navzájom prepojení prostredníctvom národných a medzinárodných poskytovateľov vyššej úrovne (napríklad AT&T, Level 3 Communications, Sprint, NTT).

Existuje niekoľko rozdelení počítačových sietí. Podľa veľkosti, resp. množstva koncových zariadení, sa delia na siete typu Personal Area Network (PAN), Local Area Network (LAN), Metropolitan Area Network (MAN) a Wide Area Network (WAN).[8]

2.2 Autonómne systémy

Internet je v súčasnosti natoľko rozsiahly a premenlivý, že nie je reálne možné udržiavať v smerovačoch úplnú informáciu o jeho celej topológii.[9] Navyše by tieto informácie boli veľmi nestabilné, pretože by sa menili s výpadkom alebo zapojením linky kdekoľvek na svete. Preto bolo rozhodnuté riešiť smerovanie v Internete hierarchickým spôsobom. Predpokladom jeho použitia je rozdelenie Internetu do tzv. autonómnych systémov (AS).

Autonómny systém je skupina sietí a smerovačov, ktoré sú pod spoločnou správou a riadia sa spoločnou smerovacou politikou. Príkladom autonómneho systému môže byť autonómny systém jedného konkrétneho poskytovateľa Internetu (ISP) alebo veľkej firmy.

Každý AS má svoj jedinečný 32-bitový (kedysi 16-bitový) identifikátor - Autonomous System Number (ASN). Označenie sa zapisuje v podobe X.Y, kde X a Y sú 16-bitové čísla, poprípade pomocou jedného 32-bitov dlhého čísla.

Vyhradené pre 16-bitové ASN:

- 64512 - 65534 - Vyhradené pre privátne účely.
- 0, 54272 - 64511 a 65535 - Vyhradené pre organizáciu IANA

Pre 32-bitové ASN sú vyhradené tieto čísla:

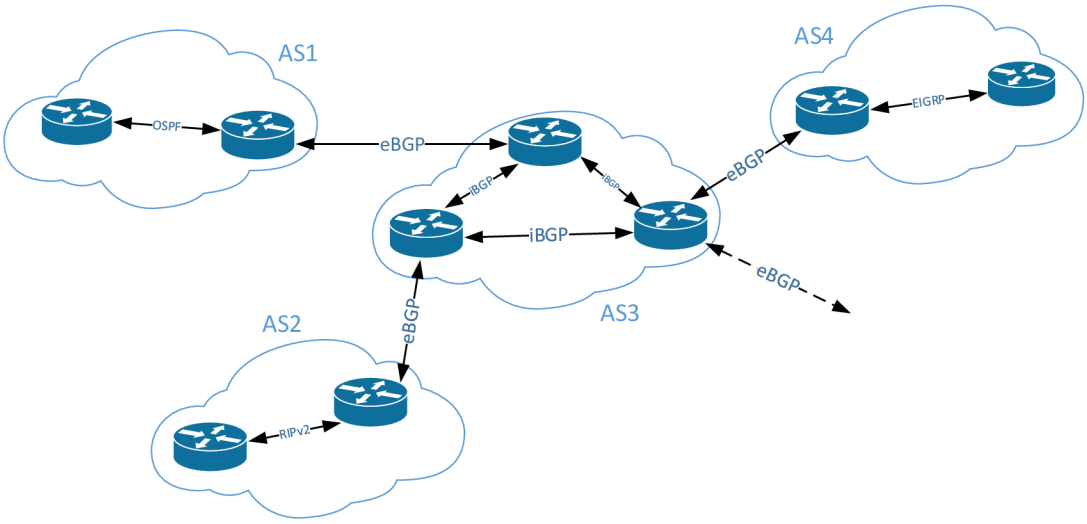
- 0.Y - Vyhradené pre ASN so 16-bitovým identifikátorom, kde Y je pôvodný identifikátor
- 1.Y a 65535.65535 - Vyhradené pre organizáciu IANA

Pri smerovaní v rámci jednotlivých autonómnych systémov sa používajú tzv. vnútorné smerovacie protokoly (Interior Gateway Protocol, IGP).[10] Pri smerovaní medzi AS sa používajú vonkajšie smerovacie protokoly (Exterior Gateway Protocol, EGP). Namiesto IGP sa v rámci autonómnych systémov niekedy využíva iBGP (Internal BGP). Najčastejším dôvodom jeho použitia je potreba prenosu smerovacích informácii medzi hraničnými smerovačmi v jednom AS.

Medzi AS sa pri použití BGP protokolu niekedy využíva označenie Exterior BGP (eBGP), ale jednoduché BGP väčšinou postačuje.

Na obr. 2.1 je znázornená možná situácia zapojenia autonómnych systémov a použitia niektorých smerovacích protokolov. V rámci jednotlivých AS sú použité niektoré IGP protokoly, napríklad v AS1 to je OSPF, v AS2 to je protokol RIPv2, v AS3 je ale využitý vyššie spomínaný protokol iBGP. AS3 v tomto obrázku môže predstavovať tranzitný AS. Celý AS3 je možné si predstaviť ako jeden virtuálny smerovač so štyrmi externými portmi.

Princíp hierarchického smerovania spočíva v tom, že z pohľadu externých smerovacích protokolov sú autonómne systémy chápané ako základné jednotky, ktorých štruktúra nie je mimo hranice AS známa. Pri každom AS sa evidujú len adresy sietí, ktoré AS obsahuje. AS sú číslované celosvetovo jednoznačnými šestnásťbitovými číslami. Cieľom je vždy doručiť paket určený pre niektorú zo sietí vo vnútri AS na jeho hranicu. O ďalšie smerovanie paketu v rámci AS sa potom postará hraničný smerovač, ktorý pozná topológiu (alebo aspoň cesty ku všetkým sieťam) svojho AS.



Obr. 2.1: Príklad použitia eBGP, iBGP a IGP protokolov

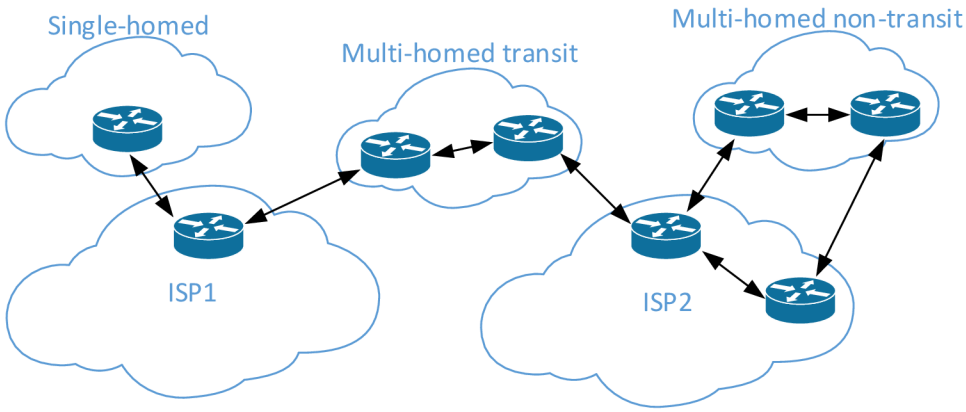
(Každý AS propaguje všetky svoje siete, ktoré majú byť z vonkajšej strany dostupné. Keďže týchto sietí môže byť veľa, je výhodné, keď tieto siete majú spoločný prefix a môžu byť propagované spoločne ako jedna veľká supersieť.)

2.2.1 Typy autonómnych systémov

Autonómne systémy môžeme podľa počtu liniek, ktorými sa pripájajú k ostatným AS, rozdeliť na single-homed a multi-homed. Single-homed AS je k inému AS pripojený jednou linkou, pričom multi-homed AS je k jednému alebo viacerým (častejšie) okolitým AS pripojený viacerými linkami. Multi-homed AS ešte delíme na tranzitné a netranzitné. Tranzitné sú tie AS, ktoré povoľujú prechod prevádzke, ktorá v ňom nezačína ani nekončí. Príkladom rozdelenia je obr. 2.2.

2.3 BGP Protokol

Smerovanie medzi autonómnymi systémami prebieha výmenou smerovacích informácií medzi hraničnými smerovačmi. Túto komunikáciu na hraničných smerovačoch zabezpečuje v súčasnosti prakticky jediný používaný smerovací protokol - Border Gateway Protocol (BGP). Pomocou BGP si hraničné smerovače vymieňajú informácie o sieťach v jednotlivých autonómnych systémoch a o tom, cez ktoré AS je



Obr. 2.2: Príklad rôznych typov AS

možné sa dostať k jednotlivým sieťam.[11] V dnešnej dobe sa takmer výhradne používa protokol BGP vo verzii 4, ktorá bola opísaná v RFC 4271 v roku 2006.

Protokol BGP podporuje beztriedne adresovanie (CIDR). S každým prefixom (adresou siete, resp. jej prvých bitov) sa šíri aj dĺžka príslušného prefixu. Vďaka tomu môže BGP realizovať aj agregáciu adries.

2.3.1 Vyhľadávanie ciest a smerovacia politika

Protokol BGP nepracuje s grafom prepojení jednotlivých smerovačov a sietí, ako napríklad OSPF, ale s grafom prepojení AS. V ňom sú následne vyhľadávané cesty medzi sieťami v rôznych AS. Cestou k určitej sieti sa v terminológii BGP rozumie postupnosť čísel autonómnych systémov, cez ktoré je možné sa dostať k cieľovej sieti.

BGP nemá, na rozdiel od vnútorných smerovacích protokolov (IGP), jednoznačnú metriku, podľa ktorých by za každých okolností automaticky volil najkratšie cesty do jednotlivých cieľových sietí. Pri smerovaní medzi autonómnymi systémami totiž smerujeme prevádzku cez cudzie AS, ktorých poskytovatelia majú rôzne prevádzkové a obchodné podmienky. Na základe všetkých týchto faktorov protokol určí smerovaciu politiku (routing policy). Smerovacia politika určuje napríklad:

- do ktorých autonómnych systémov necháme prechádzať prevádzku cez náš autonómny systém,
- z ktorých zdrojových autonómnych systémov necháme prechádzať prevádzku cez náš autonómny systém,

- ktorou výstupnou linkou z nášho autonómneho systému necháme prevádzku odchádzať k daným sieťam.

Keďže je potrebné pri konfigurácii BGP protokolu zahrnúť všetky faktory smerovacej politiky, je konfigurácia omnoho viac manuálna ako pri protokoloch triedy IGP. Protokoly triedy IGP si väčšinou susedné smerovače vyhľadávajú automaticky a predpokladá sa, že všetky nájdené smerovače spolu môžu komunikovať a jednotlivé cesty do cieľových sietí nie sú obmedzené žiadnymi ďalšími podmienkami než minimálna hodnota metriky. Pri protokole BGP sú naopak susedné smerovače konfigurované manuálne, tak ako transformácie prevádzané medzi jednotlivými susedmi.

Z pohľadu počtu preskokov, resp. cien spojov alebo inej metriky nie je smerovanie v Internete ideálne. Ale ideálne smerovanie v praxi nie je z viacerých dôvodov dosiahnuteľné a kvôli potrebe aplikácie rôznych smerovacích politík ani žiadané. Základnou technickou komplikáciou pre dosiahnutie optimálneho smerovanie je absencia spoločne interpretovateľnej metriky – každý vnútorný smerovací protokol používa svoju, od ostatných odlišnú metriku (napr. kompozitná metrika, hop-count, cena).

2.3.2 Funkcie BGP

Vnútorné smerovacie protokoly sa rozdeľujú na link-state a distance-vector. Z pohľadu úrovne znalosti topológie siete, spôsobu odovzdávania a obsahu smerovacích informácií, sa protokol BGP radí medzi ne. Niekedy je označovaný ako protokol špeciálnej triedy, nazývanej path-vector. Path-vector je postupnosť čísel autonómnych systémov, cez ktoré vedie cesta k danej sieti. Spolu s cestou je šírený aj jej path-vector, ktorý sa postupne predlžuje ako prechádza jednotlivými autonómnymi systémami. Aby sa cesta nezacyklila, môže sa číslo každého AS objaviť v path-vector maximálne jedenkrát. Prípadné cyklické cesty sa odstraňujú tak, že autonómny systém zahadzuje cesty, ktoré v path-vectore už majú jeho vlastné AS číslo.

Path-vector taktiež slúži k výberu najkratšej cesty do jednotlivých sietí. Najkratšia cesta je analogicky tá, ktorá prechádza najmenším počtom autonómnych systémov. Pri výbere sú teda preferované cesty, ktorých path-vector je kratší.

Smerovacie informácie (routing updates) sa v BGP vymieňajú vždy medzi susednými, tzv. peer smerovačmi. Susedia (peer routers), s ktorými si bude tieto informácie vymieňať, sa každému BGP smerovaču priraďujú manuálne pri jeho konfigurácii. Aby výmena týchto informácií bola spoľahlivá, prebieha s použitím protokolu TCP na porte 179. Pri naviazaní spojenia medzi susednými smerovačmi sa medzi nimi vymenia kompletné smerovacie informácie, ktoré sú obom známe. Potom už prebieha len inkrementálna výmena.

Každý BGP smerovač si periodicky (väčšinou raz za minútu) testuje dostupnosť každého svojho suseda pomocou tzv. keepalive správ. V prípade, že sused prestane

byť aktívny, musí smerovač odstrániť všetky cesty vedúce cez neho a informovať o zmene všetkých ostatných susedov.

2.3.3 Správy v BGP

V BGP protokole existujú 4 typy správ, ktoré si môžu susedné smerovače vymieňať. Tieto správy sa vymieňajú pomocou k tomuto účelu naviazaného TCP spojenia a majú spoločnú hlavičku. V hlavičke je okrem iného aj pole podporujúce autentifikáciu susedov.

Protokol BGP definuje tieto správy:

- OPEN – správa, vymieňaná pri naväzovaní väzby medzi susednými smerovačmi. V nej sa napríklad dohaduje verzia používaného BGP protokolu, a taktiež sa navzájom informujú o AS číslach, do ktorých patria.
- UPDATE – správa je určená pre propagovanie alebo odvolanie cesty. Po naviazaní spojenia sú pomocou tejto správy zaslané všetky cesty, ktoré chce smerovač oznámiť susednému smerovaču (plný update). Takisto sú od suseda prijaté všetky ním propagované cesty. Pri ďalšej komunikácii medzi nimi sa odosielajú už len dáta pre pridanie alebo odobratie určitých ciest, ktoré sú, resp. už nie sú k dispozícií.
- KEEPALIVE – správa vymieňaná periodicky pre overenie funkčnosti linky medzi susednými smerovačmi. Typicky sa vysiela každých 60 sekúnd. Spojenie sa považuje za nefunkčné v prípade, že od suseda neprišla správa KEEPALIVE po dobu HoldTime – predtým dohodnutá pomocou správy OPEN.
- NOTIFICATION – správy tohto typu sa používajú pre informovanie susedných smerovačov o dôvode ukončenia spojenia.
- ROUTE REFRESH - umožňuje BGP smerovaču požiadať susedný BGP smerovač o nové preposlanie smerovacej tabuľky, podobne ako pri zahájení relácie. Toto je nutné pri zmene smerovacej politky aby nedošlo k resetu BGP spojenia, čo by mohlo viesť k vymazaniu tejto cesty zo smerovacích tabuliek. V prípade, že susedný smerovač nepozná správu Route Refresh, je možné použiť techniku soft rekonfigurácie tzn., že si všetky prijaté cesty uloží do samostatnej tabuľky.

Informácie o cestách získaných od susedných smerovačov sa ukladajú do databázy. Do každej siete potom volí smerovač niektorú z uložených ciest, ako záznam smerovacej tabuľky. Cesty, ktoré smerovač sám používa, potom propaguje svojim susedom.

2.3.4 Atribúty v BGP

Hlavným ovládacím mechanizmom v BGP sú jeho metriky, resp. atribúty, pomocou ktorých sa určuje nastavenie ciest, prioritizácia a všetky nastavenia potrebné pre správnu funkčnosť smerovača. Tieto atribúty sa potom delia na Well-known a Optional.

Well-known atribúty:

- Každý smerovač im musí rozumieť
- Delia sa na Mandatary a Discretionary – povinné a nepovinné. Mandatory atribúty musia byť obsiahnuté vo všetkých updatoch smerovačov, pričom Discretionary sú voliteľné a môžu sa v updatoch objaviť.

Optional atribúty:

- Sú nepovinné tzn., že smerovače si ich môžu, ale nemusia vymieňať.
- Delia sa na Transitive a Non-transitive – preposielateľné a nepreposielateľné.
- Transitive sú propagované ostatným susedným smerovačom a v prípade, že nie sú rozpoznané, smerovač nastaví Partial bit, čím označí, že atribút nebol rozpoznaný.
- Non-transitive – v prípade, že nie sú smerovačom rozpoznané, zahodí ich. Rozpoznané atribúty potom propaguje susedným smerovačom na základe ich významu.

Najčastejšie používané BGP Path atribúty:[12]

- ORIGIN (1) – Well-known mandatory
- AS_PATH (2) – Well-known mandatory
- NEXT_HOP (3) – Well-known mandatory
- MULTI_EXIT_DISC (4) – Optional non-transitive
- LOCAL_PREF (5) – Well-known discretionary
- ATOMIC_AGGREGATE (6) – Well-known discretionary
- AGGREGATOR (7) – Optional transitive
- COMMUNITY (8) – Optional transitive
- ORIGINATOR_ID (9) – Optional non-transitive
- CLUSTER_LIST (10) – Optional on-transitive
- 255 – Reserved for development

ORIGIN atribút

Atribút Origin určuje pôvod prichádzajúcej aktualizácie. Ako je spomenuté vyššie, ide o Well-known povinný BGP path atribút, a preto musí byť vždy rozpoznaný a poslaný ďalej ostatným susedným BGP smerovačom. Môže obsahovať jednu z týchto troch hodnôt:

- IGP – update prišiel z interného protokolu autonómneho systému.
- EGP – update prišiel z vonku autonómneho systému
- Incomplete – pôvod update-u nie je známy

V prípade, že má BGP viac možností výberu cesty pri rovnakých atribútoch, tak je ORIGIN jeden z faktorov pri rozhodovaní o výbere najlepšej cesty. IGP je najvyššie hodnota, ktorá sa pri výbere uprednostní pred ostatnými ORIGIN atribútmi. Za ním nasleduje EGP a najnižšiu hodnotu má atribút Incomplete.

AS_PATH atribút

Ide o Well-known povinný atribút popisujúci cestu, ktorou prejde paket k dosiahnutiu cieľa. To znamená, že sú v ňom postupne za sebou uvedené čísla všetkých autonómnych systémov, cez ktoré paket prejde počas cesty zo zdrojového do cieľového AS. Príklad podoby konečného atribútu môže byť 2819 5588 12389 12880.

Pomocou umelého predlžovania ciest, prijatých od určitého susedného BGP smerovača, je možné prioritizovať a riadiť prichádzajúcu prevádzku do autonómneho systému. Tento spôsob sa nazýva AS_PATH prepending.

NEXT_HOP atribút

Je Well-known povinný atribút, ktorý určuje adresu ďalšieho BGP smerovača na ceste k cieľovej sieti. IP adresa nevyjadruje "bežný next hop", ale IP adresu hraničného smerovača v ďalšom autonómnom systéme, takže sa v rámci jedného autonómneho systému nebude meniť. V prípade, že smerovač nepozná cestu k next hop-u, nie je možné vložiť smer do smerovacej tabuľky.

LOCAL_PREF atribút

Well-known nepovinný atribút, ktorý stanovuje priority pre určitú cestu. Používa sa vo vnútri jedného AS. Atribút je stanovený každým hraničným smerovačom AS a následne je distribuovaný spolu s cestou do vnútra AS. Používa sa pre výber medzi niekoľkými hraničnými smerovačmi vo vnútri AS, pre prioritizáciu odchádzajúcej prevádzky cez vybraný smerovač. Taktiež sa používa pre prioritizáciu jedného z BGP peerov pred druhým, pre odchádzajúcu prevádzku v rámci jedného hlavného BGP smerovača.

MULTI_EXIT_DISC atribút

Jedná sa o Optional non-transitive atribút, ktorý je veľmi podobný atribútu LOCAL_PREF. Rozdielom je, že atribút MED sa používa pre prirotizáciu cestu smerujúcu do autonómneho systému. Preferuje nižšiu hodnotu. Ovplyvňuje hraničné smerovače susedného AS, a to úpravou cesty, čiže do ktorého hraničného smerovača daného AS majú smerovať všetku prevádzku.

2.3.5 Kritéria výberu cesty

Smerovač po prijatí update-u od všetkých susedných smerovačov začne zostavovať smerovaciu tabuľku, pričom najlepšiu cestu vyberá na základe nasledujúceho algoritmu (postupne od hora dole; čím vyššie je atribút postavený, tým je dôležitejší):

1. Vyraď cesty nesynchronizované s IGP a cesty s nedostupnou NEXT_HOP adresou.
2. Vyšší Weight (lokálny atribút, nastavuje sa väčšinou na Cisco smerovačoch).
3. Vyšší LOCAL_PREF.
4. Originate - preferuj cestu pochádzajúcu z tohto smerovača.
5. Kratší AS_PATH.
6. Nižší ORIGIN (IGP < EGP < Incomplete).
7. Nižší MED.
8. Preferuj eBGP pred iBGP.
9. Pre IGP preferuj nižší NEXT_HOP.
10. Pre EGP preferuj najstaršiu cestu.
11. Nižšie ID BGP smerovača.
12. Kratší Cluster-list atribút.
13. Nižšia IP adresa susedného BGP smerovača.

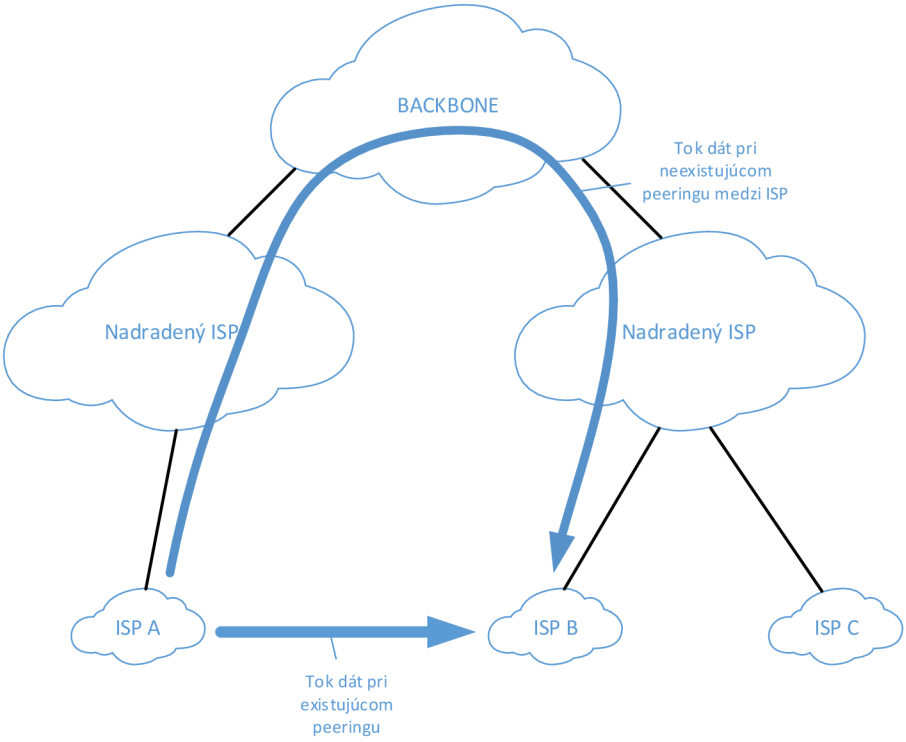
Uvažujú sa len konvergované cesty bez slučiek.

2.4 Tranzit a peering

Tranzitom sa nazýva stav, kedy je poskytovateľ, napr. druhej úrovne pripojený, do siete poskytovateľa prvej úrovne.[13] Podobne sa jedná o tranzit aj v prípade koncového zákazníka, ktorý je pripojený k svojmu ISP.

Peering, alebo inak povedané vzájomná výmena dát na nižších úrovniach hierarchického usporiadania, má veľký význam pri hierarchickom pripájaní jednotlivých ISP. Túto situáciu znázorňuje obr. 2.3. V prípade, že by chcel zákazník poskytovateľa A komunikovať so zákazníkom poskytovateľa B, musela by ich vzájomná prevádzka postupne prejsť v hierarchickej štruktúre až na takú úroveň, na ktorej by existovalo prepojenie medzi jednotlivými "vetvami". Taká možnosť, samozrejme, musí existovať, inak by Internet nebol súvislý resp. jeden z poskytovateľov by prakticky neponúkal pripojenie do celého Internetu.

Situácia, kedy by komunikácia medzi spomínanými koncovými bodmi prebiehala cez najvyššie vrstvy nie je efektívna, pretože sa tým viac vyťažujú linky jednotlivých ISP. Riešením je peering na nižších úrovniach hierarchického usporiadania.



Obr. 2.3: Schéma toku dát

3 DNS

Domain Name Service, skrátene DNS, je hierarchická štruktúra doménových mien, ktorá podobne ako systém IP adries, slúži k označeniu konkrétneho miesta v sieti Internet.[14] Potreba zavedenia tohto systému vyplýva z rozdielneho spôsobu identifikácie staníc v sieti. Počítače sa navzájom identifikujú pomocou číselných označení - IP adries. Pre bežného užívateľa siete je naopak jednoduchšie identifikovať zariadenia pomocou domén - je jednoduchšie si zapamätať textový reťazec, napríklad www.google.com, než IP adresu napr. 173.194.122.18.

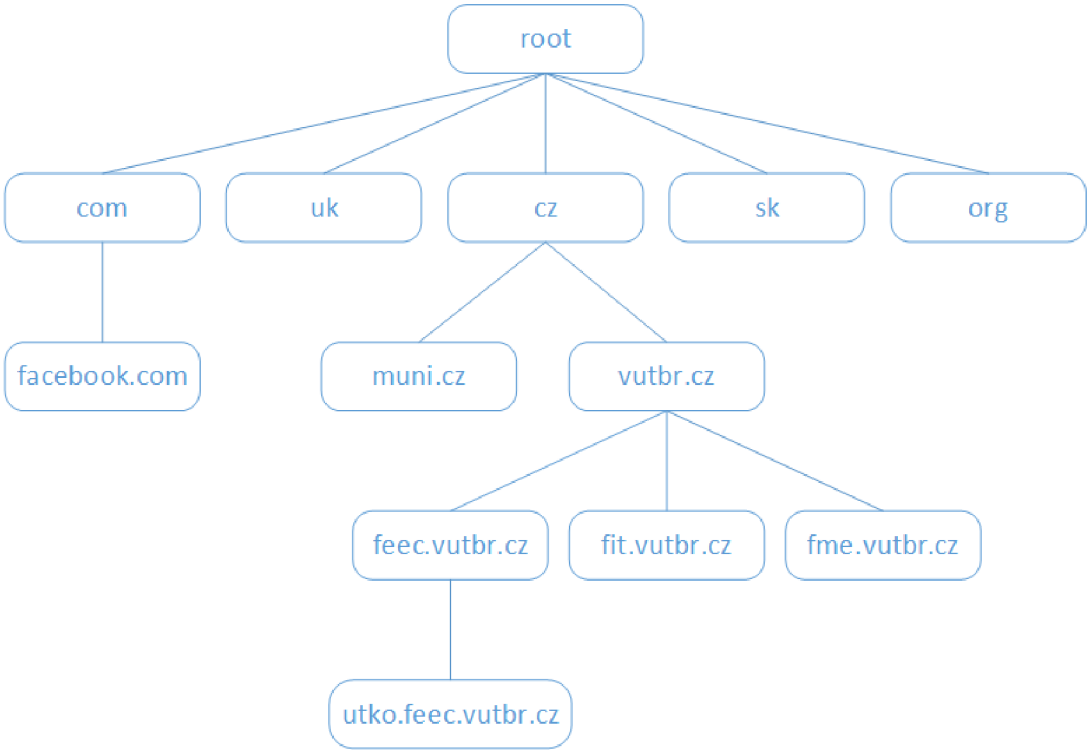
Služba DNS využíva transportné porty UDP a TCP na porte 53 (platí pre oba transportné protokoly, UDP aj TCP). Systém je založený na princípe klient - server.

Na obrázku 3.1 je znázornená hierarchická štruktúra doménových mien. V doménach sa môžu nachádzať aj subdomény, ktoré sa môžu ďalej deliť (vutbr.cz -> FEKT, FIT, FSI atď.) pre lepšiu údržbu a jednoduchšiu identifikáciu. Pri doménových menách platí naopak, ako je zvykom, vyhodnocovanie sprava doľava, tzn. od najvyššej úrovne (root) po najnižšiu. Celková dĺžka DNS názvu môže byť maximálne 255 znakov, pričom každý z čiastkových reťazcov môže mať maximálne 63 znakov. Také dlhé názvy sa však používajú len výnimočne, väčšinou sú reťazce kratšie (4 až 10 znakov), aby boli jednoduchšie zapamätateľné. Výnimkou boli donedávna domény najvyššej úrovne, kde boli reťazce dlhé 2 až 4 znaky, ale už existujú aj tzv. generické domény, napr. .berlin apod.

3.1 Štruktúra DNS

Aby sa systém DNS vysporiadal s otázkou rozsahu, používa veľké množstvo serverov, organizovaných hierarchicky a distribuovaných po celom svete. Žiadny z jednotlivých DNS serverov neobsahuje všetky mapovania pre všetkých hostiteľov v Internete. Mapovanie je rozložené medzi všetkými DNS servermi. Existujú tri triedy DNS serverov: koreňové DNS servery, DNS servery domény najvyššej úrovne (top-level domain, TLD) a autoritatívne DNS servery. Tieto triedy sú usporiadané v tzv. stromovej hierarchii.

Existuje však ešte ďalší typ DNS serveru - miestny DNS server. Miestny DNS server nepatrí striktne do hierarchie serverov, ale pre architektúru DNS je aj napriek tomu dôležitý. Každý ISP, ako napríklad univerzita, spoločnosť alebo verejný ISP, má lokálny DNS server. Keď sa hostiteľ pripojí k ISP, ten mu poskytne IP adresu jedného alebo niekoľkých svojich lokálnych DNS serverov (väčšinou pomocou protokolu DHCP - Dynamic Host Configuration Protocol).



Obr. 3.1: Ukážka hierarchickej štruktúry DNS

3.1.1 Koreňové DNS servery

Koreňové DNS servery spravujú doménu root (najvyššia možná doména). Každý server je z dôvodu bezpečnosti a spoľahlivosti vlastne sieť replikovaných serverov. Koreňové servery sú využívané bežnými DNS servermi na presmerovávanie na miestne doménové servery.

Správnu funkciu DNS sytému v Internete zabezpečuje 13 koreňových DNS serverov (sú označované A až M) a sú spravované dvanástimi organizáciami (operátormi) vybranými autoritou IANA. Nejedná sa ale o 13 fyzických serverov. Každý operátor používa nadmerné množstvo výpočtovej techniky pre zabezpečenie spoľahlivosti v prípade hardvérovej alebo softvérovej chyby. Tieto servery sa nachádzajú po celom svete v desiatkach krajín. Sú prepojené anycast-om, ktorý poskytuje zvýšenú výkonnosť a väčiu odolnosť proti chybám.

3.1.2 Servery domény najvyššej úrovne

Tieto servery sú zodpovedné za domény najvyššej úrovne, ako napríklad .com, .org, .net a .gov a všetky domény najvyšších úrovní jednotlivých zemí, ako sú napríklad .uk, .cz a .sk. Servery najvyššej úrovne .com udržuje spoločnosť VeriSign Global Registry Services, pre doménu .edu to je zase spoločnosť Educause. Štátne domény sú

spravované organizáciami v konkrétnom štáte, napríklad v Českej Republike spravuje register domény .cz organizácia Cz.NIC.

3.1.3 Autoritatívne DNS servery

Každá organizácia s verejne prístupnými hostiteľmi (ako sú napríklad webové a poštové servery) musí poskytovať verejne prístupné záznamy DNS, ktoré mapujú mená týchto počítačov na IP adresy. Tieto DNS záznamy sú uložené v autoritatívnom DNS servery organizácie.[15] Organizácia sa môže rozhodnúť uchovávať tieto záznamy vo svojom vlastnom autoritatívnom DNS servery alebo môže platiť za uloženie týchto záznamov v autoritatívnom DNS servery niektorého z poskytovateľov služieb. Väčšina univerzít a veľkých firiem musí implementovať a udržovať svoj vlastný primárny a sekundárny (záložný) autoritatívny DNS server.

3.1.4 Práca DNS serverov

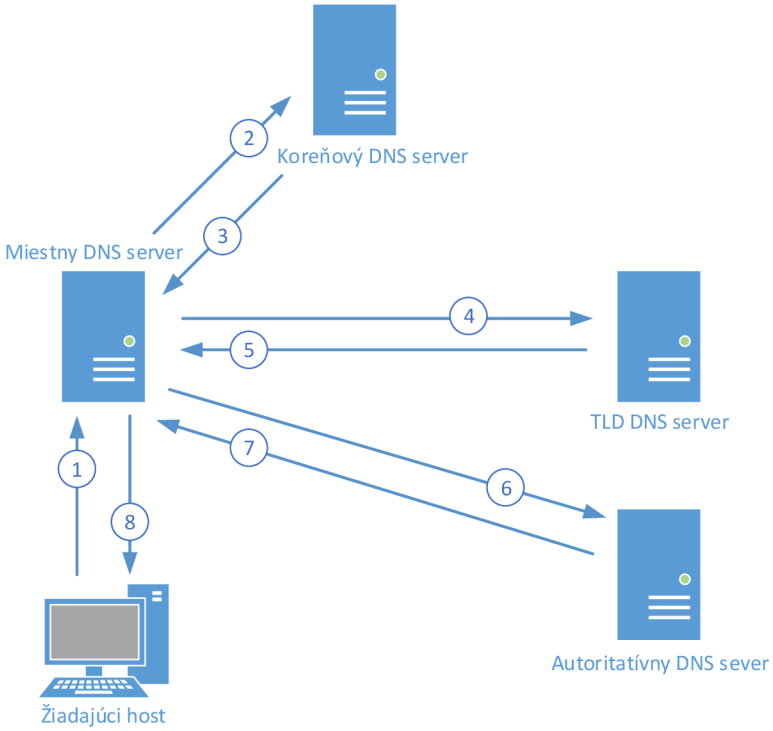
Hlavnou náplňou práve DNS serverov je riešenie dotazov, ktoré zadávajú užívatelia. Tieto dotazy sa týkajú prekladu domén na IP adresu a naopak, tzv. reverzný preklad. Umožňujú tým používať k identifikácii vzdialených staníc doménové mená namiesto IP adries, čo je pre koncových užívateľov oveľa pohodlnejšie a jednoduchšie.

Každá koncová stanica má vo svojej sieťovej konfigurácii zadanú adresu lokálneho DNS serveru, na ktorý sa obracia s dotazmi. Táto adresa je väčšinou pridelená pomocou DHCP. Pokiaľ počítač hľadá určitú informáciu v DNS (napríklad IP adresu k danému názvu), pošle dotaz práve na svoj lokálny DNS server. Ten, rovnako ako ostatné servery, obsahuje súbor s adresami serverov pre domény vyššej úrovne. Pokiaľ teda sám nepozná odpoveď na daný dotaz, obrátiť sa s dotazom na server vyššej úrovne.

Dotazy môžu byť riešené buď rekurzívne, alebo nerekurzívne. Rekurzívny dotaz znamená, že pokiaľ server, ktorý je posielaný dotaz, nepozná odpoveď, obrátiť sa na server vyššej úrovne, sám nájde na daný dotaz, uloží si ho do pamäte a pošle späť koncovej stanici. O tento typ dotazov sa starajú tzv. cache servery. Naopak, aby nedošlo k preťaženiu systému, tak o nerekurzívne dotazy sa starajú hlavne primárne servery. V prípade nerekurzívneho dotazu, pokiaľ nepozná odpoveď, pošle len zoznam serverov, kam sa obrátiť. Inak povedané, pokiaľ nepozná odpoveď na dotaz, daný dotaz ho nezaujíma.

Hlavnou úlohou DNS serverov je poskytnúť informáciu (hlavne IP adresu) k zadanému doménovému menu. Existuje ale aj tzv. reverzný dotaz, ktorý preloží zadanú IP adresu na doménové meno, pod ktorým je zaregistrovaná. Pri tomto type dotazu je však problém s opačným usporiadaním IP adresy a doménového mena.

IP adresa má v ľavej časti najvšeobecnejšie informácie, ktoré sa smerom doprava konkretizujú (zľava doprava adresa siete, podsiete a konkrétnej koncovej stanice), pričom doména má najvšeobecnejšie informácie, ktoré sa smerom doprava konkretizujú. Tento problém rieši DNS tým, že pri reverznom dotaze obráti poradie bajtov IP adresy. K obrátenej adrese potom pripojí doménu in-addr-arpa a výslednú doménu hľadá štandardným spôsobom. Obrátenie adresy umožňuje preposielať dotaz správcom zodpovedajúcich sietí a podsietí.



Obr. 3.2: Interakcia rôznych DNS serverov

3.2 Zabezpečenie DNS

Služba DNS je verejná a využíva ju každý užívateľ komunikujúci v sieti Internet. Odpovede DNS serverov sú väčšinou prijímané ako dôveryhodné. DNS komunikácia však prebieha cez nezabezpečené dátové kanály, kde je možné odpovede zachytiť, zmeniť alebo podvrhnúť, čím sa útočník môže dostať k citlivým dátam napadnutých užívateľov (napríklad k prihlasovacím údajom do rôznych služieb). Ďalším slabým miestom je tiež cache pamäť záložných DNS serverov. V tomto prípade môže útočník podvrhnúť škodlivé informácie a DNS server ďalej neoveruje platnosť týchto záznamov a na dotazy odpovedá uloženou hodnotou bez toho, aby sa ďalej dotazoval

autoritatívneho DNS serveru. Útoky tohto typu (cache poisoning) viedli k vytvoreniu štandardov na podpisovanie DNS správ - TSIG a DNSSEC.[16][17]

Pri zabezpečovaní služby DNS je potrebné dbať na zachovanie jej základného charakteru - je to verejná služba dostupná každému užívateľovi v Internete. Z toho vychádzajú dve základné úlohy, ktoré je potrebné splniť pri zabezpečovaní DNS:

- Integrita dát - dáta sa behom prenosu nezmenia.
- Autentizácia zdroja - príjemca môže dôverovať odosielateľovi dát.

Pre zaistenie integrity dát a autentizácie zdroja dát sa používa systém verejných kľúčov a podpisovania záznamov DNSSEC. Pri podpisovaní záznamov súkromným kľúčom sa využíva technika TSIG.[18][19]

3.2.1 Bezpečnostné riziká v DNS

Medzi základné triedy útokov na systémy DNS patrí:

- **Odpočúvanie paketov** - útočník pri tomto útoku sleduje komunikáciu a v prípade dotazu na DNS vráti nesprávnu, poprípade upravenú odpoveď, čím môže napríklad presmerovať prevádzku na server s inou IP adresou (napríklad na iný e-mailový server, čím môže získať citlivé dáta). Riešením je zaistenie integrity paketov DNS podpisovaním záznamov DNSSEC.
- **Hádanie ID paketu a predikcia odpovede** - identifikačné číslo DNS paketu a číslo portu klienta sú len 16-bitové hodnoty, cieľový port serveru je známy (53). Počet možných kombinácií týchto čísel je teda 2^{32}, čo je pomerne malé číslo pri útoku hrubou silou. Sledovaním sieťovej prevádzky je možné tieto hodnoty predvídať alebo hádať.
- **Reťazenie mien (otrávenie pamäte cache)** - základom tohto typu útoku je vloženie nesprávnej informácie do pamäte cache. To je možné dosiahnuť zmenou informácií v poli RDATA, hlavne v záznamoch CNAME, NS a DNAME. Útočník vnúti klientovi na jeho dotaz odpoveď, ktorá je upravená - napríklad s nesprávnou IP adresou autoritatívnych serverov DNS.
  Väčšine týchto útokov je možné zabrániť kontrolou podpisov použitím DNSSEC, kedy resolver môže overiť, či odosielateľ pozná tajný kľúč, ktorého odpovedajúci verejný kľúč je aj s overením prístupný na verejnom mieste v DNS.
- **Znemožnenie služby (Denial of Service)** - typ útoku, ktorý bráni prístupu k službám. Základným princípom je zaplavenie spojenia veľkým množstvom paketov. Mechanizmy DNSSEC a TSIG tieto útoky nerieši, práve naopak zhoršujú, pretože podpisovanie a overovanie jednotlivých záznamov je výpočtovo náročná operácia. Riešenie tohto typu útokov prebieha na úrovni konfigurácie DNS serveru (obmedzenie počtu dotazov) alebo na úrovni siete (kontrola počtu naviazaných spojení z jednej IP adresy).

- **Odmietnutie domény** - súvisí s otázkou, či overovať neexistenciu domény. Jedná sa o problém, či by mal byť resolver schopný detekovať zrušenie dát útočníkom v odpovedi DNS. DNSSEC vie určiť, ktoré autoritatívne názvy existujú v zóne a ktoré autoritatívne záznamy existujú pre dané názvy pomocou záznamov NSEC a NSEC3.

3.2.2 Podpisovanie transakcií - TSIG

TSIG (Transaction Signatures) popisuje overovanie transakcií DNS využitím symetrickej kryptografie. Je opísaný v štandarde RFC 2845 z roku 2000, aktualizovaný bol v roku 2003 a nazvaný GSS-TSIG (viď. RFC 3645). Využíva overovanie so zdieľaným tajným kľúčom a jednocestnou hashovacou funkciou HMAC-MD5. Narozdiel od DNSSEC nezaisťuje autentizáciu a integritu samotných dát, len príjemcu a odosielateľa - dátové prenosy (transakcie) medzi nimi.

Podpisovanie TSIG využíva typ záznamu TSIG, ktorý obsahuje overovací kód (hash) celého názvu DNS spolu s názvom algoritmu, času podpisu a iných údajov. Záznam TSIG je jedinečný pre každú odosielanú správu, preto sa neukladá do pamäte cache, ani sa neobjavuje v zónových súboroch.

TSIG zaisťuje overovanie zdroja a integritu dát pomocou kryptografického súčtu HMAC-MD5. Po zostavení paketu DNS sa spočíta kontrolný súčet a vloží TSIG záznam. Príjemca po prijatí správy skontroluje typ hašovacieho algoritmu, názov použitého kľúča a platnosť overovacieho kódu. Spočíta overovací kód záznamu a porovná s hodnotou v správe.

Pri použití TSIG sa predpokladá použitie kľúča pre každú dvojicu DNS serverov, čo je nevhodné pre servery komunikujúce s veľkým množstvom ďalších serverov. Problémom je taktiež distribúcia kľúčov, keďže sa jedná o súkromný kľúč, ktorý je nutné druhej strane predať bezpečným spôsobom.

Mechanizmus TSIG je možné pre resolvery, ktoré sa dotazujú len menšieho počtu serverov. Taktiež je vhodný pre záložné servery, ktoré sa dotazujú len jedného konkrétneho serveru. Pre overovanie komunikácie s verejnými servermi sa používa DNSSEC.

3.2.3 Podpisovanie záznamov - DNSSEC

DNSSEC je rozšírenie protokolu DNS pre zabezpečenie prenosu dát v systéme DNS použitím asymetrického šifrovania. Narozdiel od mechanizmu TSIG, ktorý používa symetrické šifrovanie, DNSSEC používa dva kľúče - súkromný kľúč, pri podpisovaní záznamov a verejný kľúč, pre overenie daného podpisu.

Pre potreby DNSSEC boli do DNS pridané nové záznamy - záznam DNSKEY pre uloženie verejného kľúča, RRSIG obsahujúci podpis konkrétneho záznamu, NSEC pre sekvenčné usporiadanie záznamov v doméne a záznam DS pre overenie podpisu záznamu DNSKEY pomocou vyššej autority.

Pri použití DNSSEC, zónový súbor obsahuje okrem záznamov zóny (typy A, MX, CNAME apod.) taktiež elektronický podpis ku každému z týchto záznamov. Inak povedané, podpísaný kontrolný súčet (hash) záznamu sa uloží do záznamu RRSIG, ktorý sa použije k overeniu integrity záznamu a autentizácii vlastníka. Ten sa overuje proti verejnému kľúču, ktorý sa nachádza v zázname DNSKEY.

Oba kľúče sa generujú súčasne, a preto sú algoritmicky závislé - k danému súkromnému kľúču patrí konkrétny verejný kľúč. Pomocou nich je možné záznamy podpísať a následne skontrolovať, či je tento podpis platný. Aby bola zabezpečená plná autentizácia, je nutné overiť, že kľúč pre podpis zóny ZSK (Zone Signing Key) nie je podvrhnutý útočníkom (ktorý podpíše záznamy svojím kľúčom a ponúkne k overeniu svoj platný verejný kľúč). K tomu sa používa kľúč pre overenie týchto kľúčov KSK (Key Singing Key), ktorý taktiež používa asymetrickú šifru. Tieto dva páry kľúčov tvoria základ systému zabezpečenia DNSSEC.

Každý zónový súbor teda obsahuje po dva záznamy typu DNSKEY a RRSIG. Prvý záznam RRSIG obsahuje podpis daného záznamu a jeho platnosť overuje pomocou verejného kľúča ZSK v zázname DNSKEY. Druhý záznam RRSIG obsahuje podpis verejného kľúča ZSK, ktorého platnosť je možné overiť pomocou záznamu DNSKEY obsahujúceho verejný kľúč KSK. Ten je následne možné overiť pomocou záznamu DS, ktorý je súčasťou nadradenej zóny. Záznam DS je podpísaný súkromným kľúčom ZSK nadradenej zóny. Takto postupne vzniká tzv. reťazec dôvery (chain of trust), v ktorom jednotlivé zónové súbory postupne odkazujú podľa hierarchie až ku koreňovým zónovým súborom.

3.2.4 Záznamy DNSSEC

Rozšírenie DNS sa začalo vyvíjať v roku 1999, kedy sa pre podpisovanie používali záznamy typu KEY, SIG a NXT, ktoré sa dnes už nepoužívajú. V roku 2005 boli totiž nahradené záznamy typu DNSKEY, RRSIG a NSEC (v roku 2008 nahradený aktualizovaným typom záznamov NSEC3).

- **Záznam DNSKEY (DNS Key Record)** - obsahuje verejný kľúč, pomocou ktorého sa overujú záznamy podpísané zodpovedajúcim privátnym kľúčom. Súčasťou záznamu je taktiež typ kľúča, použitý algoritmus pre overovanie a ďalšie.
- **Záznam RRSIG (Resource Record Signature)** - obsahuje elektronický podpis jednotlivých záznamov v podpísanej zóne, inak povedané, podpis RR-

SIG sa nevzťahuje k jednotlivým záznamom, ale k celej množine záznamov, ktoré majú rovnaké doménové meno, typ. triedu a TTL. Z týchto údajov a obsahu záznamov je vypočítaný podpis. Záznam RRSIG preto obsahuje meno podpisujúcej autority, typ použitého algoritmu, dobu platnosti podpisu a príznak, ktorý odkazuje na overujúci verejný kľúč.

- **Záznam NSEC (Next-Secure Record)** - obsahuje ďalšie doménové meno záznamu v doméne a typ záznamu DNS, ktoré sa vzťahujú k tomu doménovému menu. Záznam NSEC ukazuje na ďalšie doménové meno, čím ukazuje že medzi súčasným a nasledujúcim doménovým menom nie je žiadna položka. Použitie tohto záznamu vyžaduje zoradenie jednotlivých záznamov DNS podľa doménových mien.
- **Záznam DS (Delegation Signer)** - odkazuje na záznam DNSKEY a používa sa k overeniu kľúča v tomto zázname. Obsahuje odkaz na kľúč DNSKEY, typ použitého algoritmu a odtlačok kľúča (digest) v DNSKEY. Pomocou neho môže resolver overiť kľúč v zázname DNSKEY. Záznamy DNSKEY a DS majú rovnakého vlastníka (obsahujú rovnaké doménové meno), ale sú uložené na rôznych miestach. Napríklad záznam DS pre doménu fekt.vutbr.cz sa nachádza v zónovom súbore vutbr.cz, pričom zodpovedajúci záznam DNSKEY je uložený v zóne fekt.vutbr.cz.
- **Záznam NSEC3 (Next-Secure Record version 3)** - na rozdiel od NSEC nepoužíva pre radenie kanonické mená (ktoré sú nevhodné z hľadiska bezpečnosti), ale číselnú hodnotu hašovacej funkcie, ktorú aplikuje na pôvodné meno. Výsledné číselné hodnoty sú numericky zoradené do zoznamu (tzv. hash order), ktorý je radený rovnako, ako v prípade použitia kanonickým mien. Záznam NSEC3 obsahuje informácie o použitej hašovacej funkcii, inicializačnej sekvencii, počet iterácií hašovacej funkcie nad pôvodným doménovým menom, ukazovateľ na ďalšie hašované meno a bitovú mapu, ktorá obsahuje zoznam typov DNS vytvorených pre dané doménové meno.

4 IPERF

Iperf je jednoduchý nástroj na aktívne meranie priepustnosti siete.[20] Vytvára TCP (Transmission Control Protocol) a UDP (User Datagram protokol) toky dát. Užívateľ je schopný nastaviť rôzne parametre, ktoré môžu byť využité nielen pri testovaní siete, ale tiež pri jej ladení a optimalizovaní. Je podporovaný na viacerých platformách, ako napríklad Linux, Unix a Windows.

Priepustnosť medzi dvoma koncovými bodmi je schopný merať jednosmerne aj obojsmerne. Pri UDP toku dát umožňuje upravovať veľkosť prenášaných datagramov a poskytuje výsledky priepustnosti datagramov a straty paketov. Pri TCP toku dát meria priepustnosť užitočného zaťaženia (payload-u).

Existuje aj obdobný nástroj s grafickým užívateľským rozhraním (GUI) pomenovaný Jperf. Napriek tomu je v súčasnosti stále viac preferovaný Iperf.

4.1 Iperf3

Iperf3 je nová verzia nástroju Iperf, vytvorená od nuly, s cieľom menšieho a jednoduchšie kódového základu. Zahŕňa niekoľko funkcií z nástrojov ako nuttcp a netperf, ktoré chýbali v pôvodnom nástroji Iperf. [21] Iperf3 nie je spätne kompatibilné s Iperf.

Pre uskutočnenie Iperf3 testu je nutné zriadiť server aj klient. Iperf3 server sa spúšťa príkazom **iperf3 -s** [**options**], klient sa spúšťa príkazom **iperf3 -c** ***server*** [**options**]. Server je možné okrem klasického módu (parameter -s) spustiť v móde na pozadí. To sa nastaví použitím parametru -D namiesto parametru -s.

Medzi ďalšie parametre patrí napríald parameter intervalu (-i), parameter nastavenia veľkosti TCP okna (-w) a parameter doby prenosu (-t). Všetky parametre je možné nájsť v manuálových stránkach Linuxu.[22]

5 VYPRACOVANIE LABORATÓRNYCH ÚLOH

Táto kapitola obsahuje popis a návody troch laboratórnych úloh. Podrobné konfigurácie prvej a druhej laboratórnej úlohy sa nachádzajú v prílohe práce. Riešenie tretej laboratórnej úlohy prebieha v grafickom rozhraní OS Windows, preto príloha neobsahuje konfiguračné súbory tejto úlohy. Konfiguračné súbory jednotlivých použitých zariadení sa nachádzajú na priloženom CD.

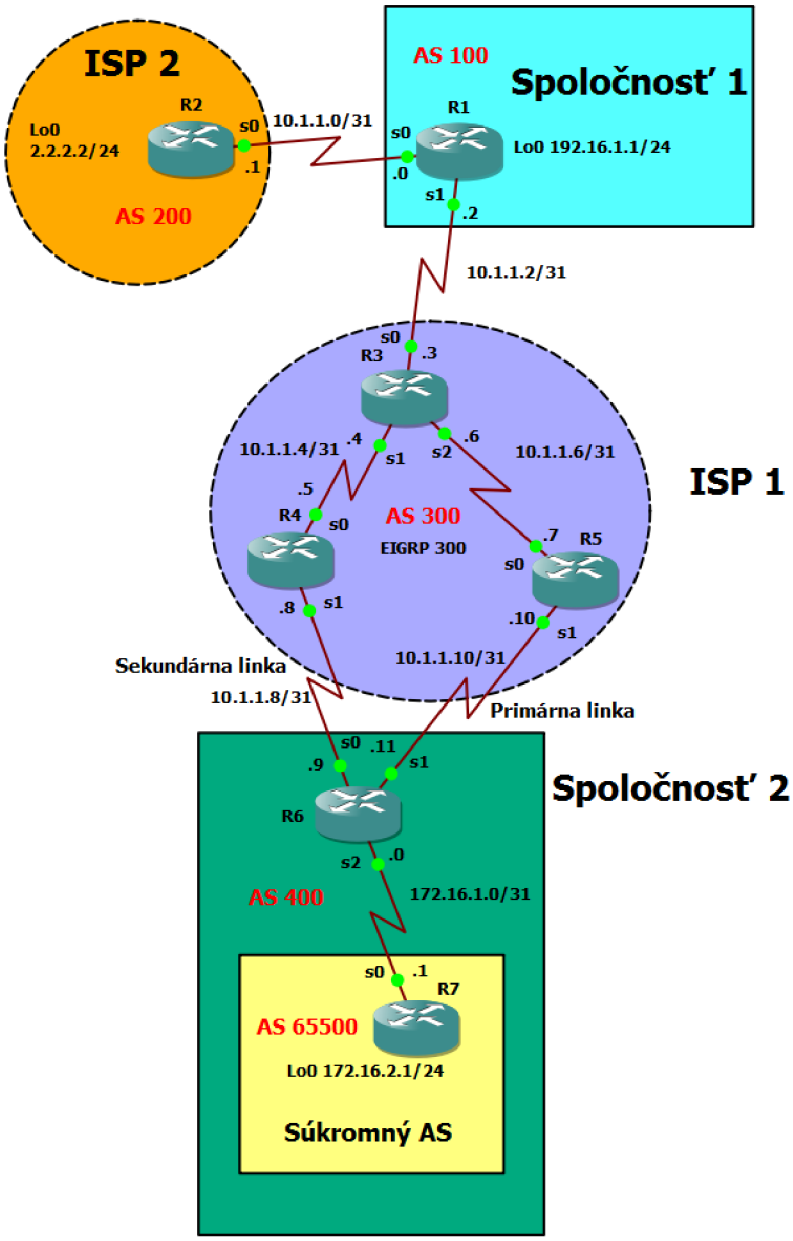
Jednotlivé laboratórne úlohy sú vypracované v simulačnom prostredí GNS3 vo verzii 1.4.6. Operačný systém použitého hosťujúceho počítača je MS Windows 10 Pro 64-bit.

Smerovače použité v prvej a druhej laboratórnej úlohe sú Cisco 1700 s Cisco IOS vo verzii 12.4. V druhej laboratórnej úlohe sa nachádzajú virtualizované stanice, na ktorých je nainštalovaný operačný systém Linux Debian 32-bit bez grafického užívateľského rozhrania (GUI) pre zníženie potrebného výpočtového výkonu. V tretej laboratórnej úlohe sa nachádzajú virtualizované stanice spojené ethernetovým prepínačom. Na jednej virtualizovanej stanici je nainštalovaný OS MS Windows Server 2012 R2, na druhej je nainštalovaný OS MS Windows 8.1 32-bit. Jednotlivé virtualizované stanice sú implementované prostredníctvom programu VirtualBox. Do tretej laboratórnej úlohy je zakomponovaná práca s programom Wireshark pre ukážku princípu fungovania DNSSEC záznamov.

5.1 Laboratórna úloha č.1 - Komplexná konfigurácia protokolu BGP

5.1.1 Ciele úlohy

V topológii tejto úlohy sa nachádzajú 2 spoločnosti a 2 poskytovatelia internetu (ISP - Internet Service Provider), viď obr. 5.1. Spoločnosť 1, reprezentovaná smerovačom R1, s prideleným verejným číslom Autonómneho systému 100 má pripojenie do Internetu zabezpečené pripojením k dvom navzájom nezávislým ISP. Spoločnosť 2, reprezentovaná smerovačom R6, s prideleným verejným číslom Autonómneho systému 400 má pripojenie k tranzitnému ISP 1 zabezpečené dvomi linkami - primárnou a sekundárnou. Vo vnútri AS Spoločnosti 1 sa nachádza súkromný AS s číslom 65500 reprezentovaný smerovačom R7, ktorý slúži na testovanie nimi vyvíjaného softvéru. ISP 1 s číslom AS 300 je reprezentovaný smerovačmi R3, R4 a R5, medzi ktorými je nakonfigurované EIGRP. ISP 2 s číslom AS 200 je reprezentovaný smerovačom R2, pričom spojenie s ISP 1 si predstavte cez nezobrazené AS.



Obr. 5.1: Topológia laboratórnej úlohy č.1

Pri konfigurácii pre zrýchlenie postupu používajte príkaz **clear ip bgp ***, ktorým reštartujete BGP na danom smerovači. V reálnych situáciách používajte výhradne soft reset, ktorý nereštartuje BGP spojenie, ale len urýchli zmenu v BGP tabuľkách.

5.1.2 Postup riešenia

1. **Konfigurácia IP adries na rozhraniach**
   - Pre ušetrenie času sú IP adresy vopred nakonfigurované, správnosť kon-

Tab. 5.1: Tabuľka adries k laboratórnej úlohe č.1

Smerovač	Rozhranie	IP Adresa rozhrania
R1	Serial 0	10.1.1.0/31
	Serial 1	10.1.1.2/31
	Loopback 0	192.168.1.1/24
R2	Serial 0	10.1.1.1/31
	Loopback 0	2.2.2.2/24
R3	Serial 0	10.1.1.3/31
	Serial 1	10.1.1.4/31
	Serial 2	10.1.1.6/31
R4	Serial 0	10.1.1.5/31
	Serial 1	10.1.1.8/31
R5	Serial 0	10.1.1.7/31
	Serial 1	10.1.1.10/31
R6	Serial 0	10.1.1.9/31
	Serial 1	10.1.1.11/31
	Serial 2	172.16.1.0/31
R7	Serial 0	172.16.1.1/31
	Loopback 0	172.16.2.1/24

figurácie si môžete overiť porovnaním s tabuľkou 5.1.

- Vyskúšajte si sami nakonfigurovať IP adresy na smerovači R7 podľa tabuľky 5.1.

2. **Konfigurácia EIGRP v AS 300**
   - Do EIGRP vložte IP adresy liniek medzi smerovačmi R3 a R4, R3 a R5.
   - Overte funkčnosť EIGRP. Prečo na smerovači R3 nevypíše žiadnu EIGRP smerovaciu tabuľku?
3. **Konfigurácia iBGP**
   - Naviažte iBGP susedstvo medzi R3 a R4, R3 a R5 a taktiež medzi R4 a R5 v AS 300.
   - Overte BGP susedstvá.
4. **Konfigurácia eBGP**
   - Naviažte eBGP susedstvá medzi hraničnými smerovačmi jednotlivých AS (medzi R1 a R2, R1 a R3, R4 a R6, R5 a R6, R6 a R7).
   - Overte ping medzi sieťami 192.168.10/24 a 172.16.2.0/24. Prečo nefunguje, hoci jednotlivé smerovače majú tieto siete v tabuľkách BGP?
   - Pridajte do eBGP záznamy o sieťach na linkách medzi hraničnými smerovačmi (stačí na jednom z každej dvojice).

- Overte susedstvá medzi hraničnými smerovačmi a ešte raz ping medzi sieťami 192.168.10/24 a 172.16.2.0/24.

5. **Private AS (Súkromný AS)**
   - V BGP tabuľkách smerovačov R3, R4 a R5 si všimnite, že majú pri ceste k sieti 172.16.2.0/24 uvedený AS 65500, ktorý ale patrí do rozsahu súkromných čísiel AS a ISP by to mal filtrovať.
   - Nastavte filtrovanie posielania privátnych čísiel autonómnych systémov.
   - Overte, že smerovače už nemajú informácie o súkromnom AS, ale sieť 172.16.2.0/24 aj napriek tomu ostala v BGP tabuľkách.
   - Príkazom **ping** overte, že medzi týmito sieťami ostala plná konektivita.
6. **Non-transit AS (Netranzitný AS)**
   - Všimnite si, že smerovač R3 smeruje prevádzku do siete 2.2.2.0/24 cez smerovač R1, pričom AS 100 je súkromný a má zabezpečené pripojenie do Internetu cez dvoch rôznych ISP (AS 200 a AS 300). Zabezpečte, aby cez smerovač R1 prechádzali len dáta, ktoré smerujú z/do sietí v AS 100.
   - Overte, že smerovač R1 viac nepreposiela záznamy o sieti 2.2.2.0/24. *Poznámka: Predpokladajme, že konektivita medzi R2 a R3 existuje cez ďalšie AS v Internete, ktoré sa v tejto topológii nenachádzajú, a teda úpravou nastavení na R1 by sieť 2.2.2.0/24 úplne nezmizla z BGP tabuliek, len by sa upravila cesta k nej.*
7. **MD5 autentifikácia**
   - Medzi smerovačmi R1 a R2 nastavte overovanie záznamov pomocou MD5 autentifikácie. Pre demonštráciu priebehu nakonfigurujte najskôr smerovač R1 a všimnite si správy v konzole. Následne nakonfigurujte aj smerovač R2.
8. **Nastavenie preferovanej cesty z/do AS 400**
   - Ktorou cestou prebieha pripojenie z/do AS 400? Cez smerovač R4 alebo R5 a prečo?
   - Nastavte cestu cez R5 ako preferovanú a cestu cez R4 ako záložnú.
   - Ktorou cestou prebieha pripojenie z/do AS 400 teraz? Cez smerovač R4 alebo R5 a prečo?
9. **Demonštrácia výpadku linky**
   - V simulačnom prostredí GNS3 kliknite pravým tlačidlom na linku medzi smerovačmi R1 a R3, zvoľte **Start Capture**, vyberte port **Serial0** na smerovači **R3** a potvrďte **Ok**, čím spustíte zachytávanie paketov v programe Wireshark.
   - Spustite príkaz **ping** s vyšším počtom opakovaní (minimálne 200) a vypnutím linky medzi R3 a R5 počas priebehu pingu overte presmerovanie prevádzky cez záložnú linku (cez smerovač R4). Po skončení pingu za-

stavte zachytávanie paketov v programe Wireshark a pozrite sa na priebeh komunikácie.

5.1.3 Príklady použitých príkazov a odpovede

1. **Konfigurácia IP adries na rozhraniach**
   - Konfiguráciu IP adries je možné skontrolovať použitím príkazu:

     ```
     R1#show ip interface brief
     ```

2. **Konfigurácia EIGRP v AS 300**
   - Príklad overenia EIGRP na smerovači R4, viď obr. 5.2.
   - Pri smerovaní majú prednosť priamo pripojené linky pred záznamami smerovacích protokolov, preto smerovač R3 nevypíše žiadne záznamy v EIGRP smerovacej tabuľke. Taktiež sa v tejto topológii, za priamo pripojenými smerovačmi, nenachádzajú žiadne siete, o ktorých by sa mohol smerovač R3 cez EIGRP naučiť.

```
R4#show ip route eigrp
     10.0.0.0/31 is subnetted, 5 subnets
D       10.1.1.6 [90/2681856] via 10.1.1.4, 00:11:50, Serial0
```

Obr. 5.2: Výpis zo smerovača R4 pri overení EIGRP

3. **Konfigurácia iBGP**
   - Všimnite si, že smerovače R4 a R5 nie sú priamo spojené žiadnou linkou, BGP susedstvá je totiž možné nastaviť aj v takomto prípade, podmienkou je konektivita medzi danými smerovačmi (tú zabezpečuje EIGRP nastavené v predchádzajúcom kroku).
   - Overenie BGP susedstiev:

     ```
     R3#show ip bgp neighbors
     ```

4. **Konfigurácia eBGP**
   - Hoci jednotlivé smerovače vedia ako sa dostať k sieťam 192.168.1.0/24 a 172.16.2.0/24, nemajú konektivitu k jednotlivým next-hopom (môžete si to overiť zobrazením smerovacej tabuľky).
   - Overenie BGP susedstiev:

     ```
     R3#show ip bgp neighbors
     ```

5. **Private AS(Súkromný AS)**
   - Filtrovanie čísiel súkromných AS nastavíte príkazom:

```
R6(config)#router bgp 400
R6(config-router)#neighbor 10.1.1.8 remove-private-as
```

6. **Non-transit AS(Netranzitný AS)**
   - Najvhodnejším riešením je použiť as-path access-list, ktorý zabezpečí, že smerovač bude informovať len o sieťach pochádzajúcich z jeho vlastného AS.
     Poznámka: Aby ste to zabezpečili, pri vytváraní access-listu použite parameter ^$.
7. **MD5 autentifikácia**
   - Pri nastavení MD5 autentifikácie zvoľte ľahko-zapamätateľné heslo (napríklad AAA).
8. **Nastavenie preferovanej cesty z/do AS 400**
   - Spojenie momentálne prebieha cez smerovač R4 pretože má nižšiu IP adresu. Môžete to overiť pomocou príkazu **traceroute**.
   - Pre úpravu preferovanej cesty upravte atribút LOCAL_PREF. Tento atribút sa používa vo vnútri jedného AS tzn., že je distibuovaný spolu s cestou do vnútra daného AS. Pre nastavenie preferovanej cesty smerom von z AS 400, upravte LOCAL_PREF na smerovači R6 pre nastavenie preferovanej cesty do AS 400 uskutočnite túto úpravu na smerovačoch R4 a R5. Využite vhodne nastavenú route-mapu. Nezabudnite, že pri výbere cesty je preferovaná vyššia hodnota (predvolená hodnota je 100).
   - Správnosť nastavenia si overte v BGP tabuľkách a taktiež príkazom **traceroute** z IP adresy 192.168.1.1 na adresu 172.16.2.1 a opačne.
9. **Demonštrácia výpadku linky**
   - V zachytenom priebehu komunikácie programom Wireshark si všimnite správy **BGP Update**, po ktorých sa ping znovu rozbehol.

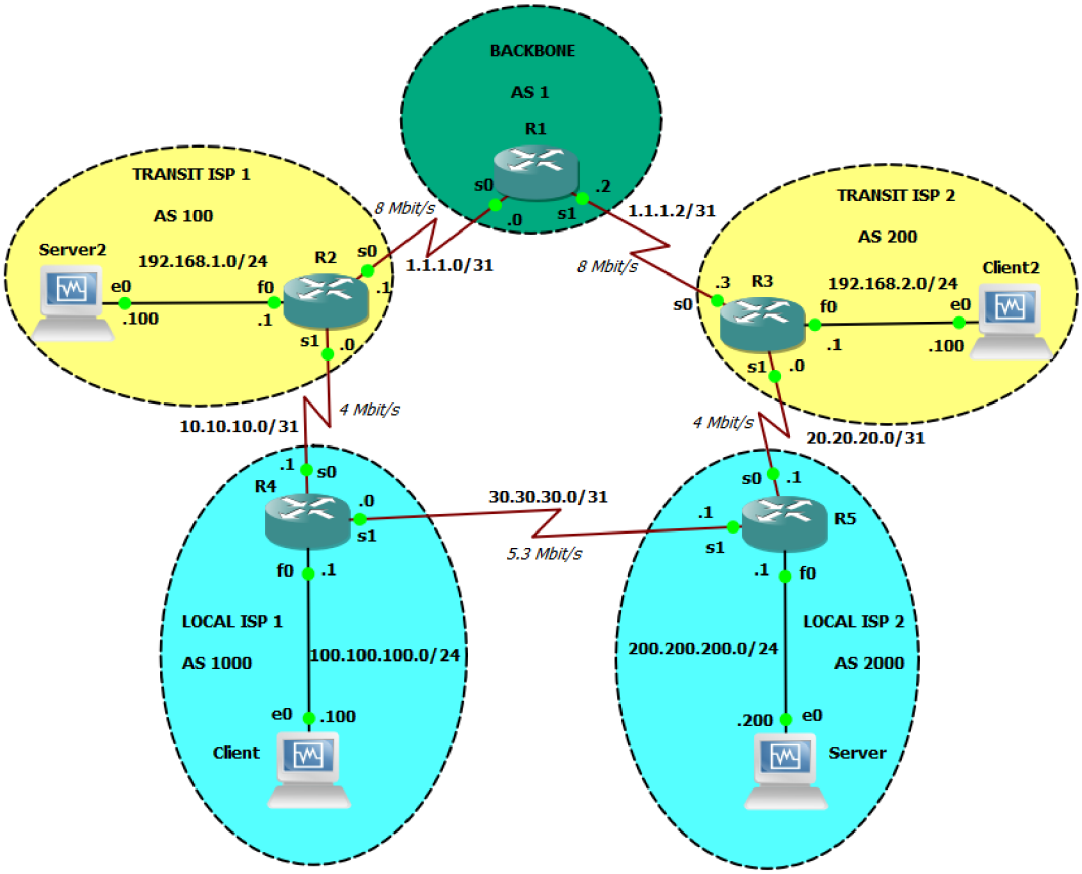
5.2 Laboratórna úloha č.2 - Porovnanie tranzitu a peeringu

Prihlasovacie údaje do linuxových staníc:

Login: **bachelor**

Heslo: **aaa**

Heslo pre užívateľa **root: aaa**.



Obr. 5.3: Topológia laboratórnej úlohy č. 2

5.2.1 Ciele úlohy

Podstatou tejto laboratórnej úlohy je prakticky si overiť poznatky o rozdieloch medzi tranzitnými a peeringovými spojeniami. V topológii, zobrazenej na obr. 5.3, sa nachádza Backbone network (prekl. Chrbticová sieť) s číslom Autonómneho systému 1 a reprezentovaná smerovačom R1. K AS 1 sa pripájajú dvaja tranzitný ISP prvej úrovne s číslami Autonómnych systémov 100 a 200. Sú reprezentovaný smerovačmi R2 a R3, ku ktorým sú pripojené dve linuxové stanice, generujúce prevádzku na pozadí. Poslednú úroveň znázorňujú lokálny ISP s číslami Autonómnych systémov 1000 a 2000. Sú reprezentovaní smerovačmi R4 a R5, ku ktorým sa pripájajú ďalšie dve linuxové stanice predstavujúce konečných užívateľov. Medzi lokálnymi ISP je vytvorená linka predstavujúca peering.

Z dôvodu použitia nižšej rady smerovačov Cisco a obmedzeným hardvérovým možnostiam pri simulácii je na linkách medzi AS 1 a tranzitnými ISP obmedzená rýchlosť na 8 Mbit/s. Z rovnakých dôvodov je medzi tranzitnými a lokálnymi ISP obmedzená rýchlosť na 4 Mbit/s a 5.3 Mbit/s na peeringovej linke medzi lokálnymi

Tab. 5.2: Tabuľka adries k laboratórnej úlohe č.2

Zariadenie	Rozhranie	IP Adresa rozhrania
R1	Serial0	1.1.1.0/31
	Serial1	1.1.1.2/31
R2	Serial0	1.1.1.1/31
	Serial1	10.10.10.0/31
	FastEthernet0	192.168.1.1/24
R3	Serial0	1.1.1.3/31
	Serial1	20.20.20.0/31
	FastEthernet0	192.168.2.1/24
R4	Serial0	10.10.10.1/31
	Serial1	30.30.30.0/31
	FastEthernet0	100.100.100.1/24
R5	Serial0	20.20.20.1/31
	Serial1	30.30.30.1/31
	FastEthernet0	200.200.200.1/24
Client	eth0:avahi	100.100.100.100/24
Client2	eth0:avahi	192.168.2.100/24
Server	eth0:avahi	200.200.200.200/24
Server2	eth0:avahi	192.168.1.100/24

ISP. Je nutné si uvedomiť, že v reálnych situáciach sa rýchlosti na týchto linkách môžu pohybovať v rádoch desiatok Mbit/s, pre potreby tejto laboratórnej úlohy ale také vysoké rýchlosti nie sú potrebné.

5.2.2 Postup riešenia

1. **Konfigurácia IP adries**
   - IP adresy smerovačov sú vopred nastavené, ich konfiguráciu porovnajte s tabuľkou 5.2.
   - Na linuxových staniciach nastavte IP adresu a predvolenú bránu podľa topológie.
   - Overte, že rozhranie Serial1 na smerovači R4 je vypnuté.
   - Použitím príkazu **ping** overte konektivitu medzi Clientom a Serverom.
2. **Demonštrácia tranzitného spojenia**
   - Príkazom **traceroute** si overte cestu medzi stanicami **Client** a **Server**. Všimnite si vyššie hodnoty odozvy a zdôvodnite ich.
   - Na oboch serveroch spustite **Iperf3** server. Následne na stanici **Client**

spustite Iperf3 klient a všimnite si prenosovú rýchlosť.

- Spustite Iperf3 server na stanici **Server2** a Iperf3 klient na stanici **Client2** s upravenými parametrami, aby ste demonštrovali prevádzku na pozadí. Použite Linux manuálové stránky.
- Opäť spustite Iperf3 klient na stanici **Client** a pozorujte zmeny v rýchlosti prenosu. Zmenu zdôvodnite.

3. **Demonštrácia peeringového spojenia**
   - Zapnite rozhranie Serial1 na smerovači R4 a počkajte na naviazanie BGP susedstva medzi smerovačmi R4 a R5.
   - Príkazom **traceroute** si overte cestu medzi stanicami **Client** a **Server**. Všimnite si nižšie hodnoty odozvy a zdôvodnite ich.
   - Spustite Iperf3 klient na stanici **Client** a pozorujte zmeny prenosovej rýchlosti. Zdôvodnite.

5.2.3 Príklady použitých príkazov a odpovede

1. **Konfigurácia IP adries**
   - Konfiguráciu rozhraní na smerovačoch overte nasledujúcim príkazom:

     ```
     show ip interface brief
     ```

   - Na linuxových staniciach nastavte IP adresu a predvolenú bránu príkazmi:

     ```
     ifconfig eth0:avahi 100.100.100.100/24
     route add default gw 100.100.100.1 eth0:avahi
     ```

     *Poznámka: Pre nastavenie IP adresy a predvolenej brány linuxových staníc musíte mať práva superužívateľa, do ktorého sa dostanete zadaním **su** a vložením príslušného hesla.*

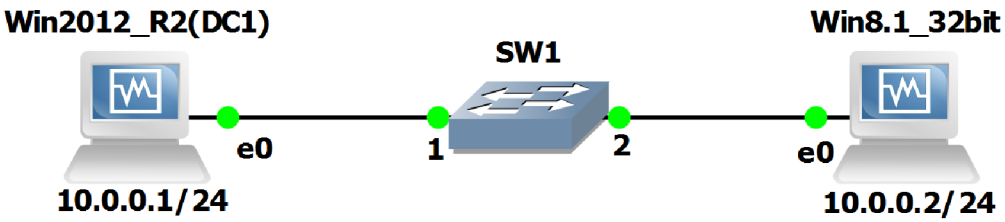
2. **Demonštrácia tranzitného spojenia**
   - Vyššie hodnoty odozvy sú spôsobené prechodom cez väčšie množstvo zariadení.
   - Na stanici **Server2** nastavte Iperf3 server na pozadí a na stanici **Server** nastavte klasický Iperf3 server.
   - Na stanici **Client** spustite Iperf3 klient bez upravenia parametrov:

     ```
     iperf3 -c 200.200.200.200
     ```

   - Po spustení prenosu medzi stanicami **Client2** a **Server2** došlo k poklesu rýchlosti prenosu pri spustení Iperf3 medzi stanicami **Client** a **Server** pretože určitá časť linky obsadila prevádzka medzi stanicami Server2 a Client2.

3. **Demonštrácia peeringového spojenia**
    - Peering je v súčasnosti veľmi dôležitou zložkou v sieťovej architektúre moderného Internetu, pretože vzájomným prepojením nižších vrstiev zabezpečuje kratšiu odozvu a rýchlejšie prenosy a taktiež uvoľňuje linky na vyšších vrstvách, čím pomáha znižovať celkové náklady.

5.3 Laboratórna úloha č.3 - Demonštrácia DNSSEC



Obr. 5.4: Topológia laboratórnej úlohy č.3

Prihlasovacie údaje na Windows Server 2012 R2

Login: **Bachelor**

Heslo: **Qwert123**

Prihlasovacie údaje na Windows 8.1

Login: **Bakalaris**

Heslo: **aaa**

5.3.1 Ciele úlohy

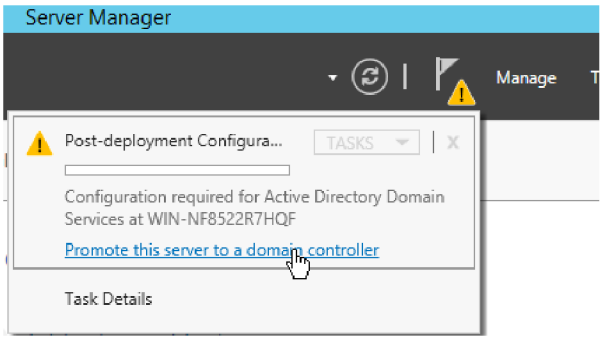
DNSSEC je bezpečnostné rozšírenie služby DNS, ktoré je v posledných rokoch postupne nasadzované do všetkých domén. Z toho dôvodu narastá pravdepodobnosť, že sa s týmto rozšírením študenti stretnú vo svojom budúcom zamestnaní. Táto laboratórna úloha preto poukazuje na základné princípy funkcie bezpečnostného rozšírenia DNSSEC.

Ako môžete vidieť na obr. 5.4, v topológii tejto laboratórnej úlohy sa nachádza Windows Server 2012 R2 ako Domain Controller a DNS server a Windows 8.1 ako klient.

5.3.2 Konfigurácia zariadení

Konfigurácia DC1

1. Nakonfigurujte IP adresu **10.0.0.1**, masku podsiete **255.255.255.0** a preferovaný DNS server **10.0.0.1**.
2. Upravte názov počítača na **DC1**. Následne server reštartujte.
3. Nainštalujte **Active Directory Domain Services**.
   - V okne **Server Manager** klinite na **Add Features and Roles**.
   - V okne **Add Roles and Features Wizard** kliknite **3-krát Next**. Následne v okne **Select server roles** kliknite na zaškrtávacie políčko položky **Active Directory Domain Services**.
   - V následne otvorenom okne klinite na **Add Features**.
   - **3-krát** kliknite na **Next**, nakoniec kliknite na **Finish**.
   - Kliknite na notifikačnú vlajku v pravej hornej časti okna Server Manager a zvoľte **Promote this server to a domain controller**.



Obr. 5.5: Povýšenie serveru na Domain Controller

   - V okne **Active Directory Domain Services Configuration Wizard**, v záložke **Deployment Configuration**, zvoľte možnosť **Add a new forest** a pomenujte ho **bachelor.local**.
   - Kliknite na **Next** a v záložke **Domain Controller Options** vložte a potvrďte heslo **Qwert123**. Skontrolujte, že možnosti **Domain Name System (DNS) server** a **Global Catalog (GC)** sú zvolené a klinite na **Next**.
   - Kliknite **5-krát Next** a nakoniec **Install**.
   - Následne sa počítač automaticky reštartuje. Po spustení sa prihláste pod lokálnym kontom.
   - Pre potreby laboratórnej úlohy je nutné vytvoriť administrátorský účet. Kliknite na položku **Tools > Active Directory Users and Computers**. V otvorenom okne dvojklikom otvorte **bachelor.local**, pravým kliknite na **Users**, prejdite na možnosť **New** a vyberte **User**.
   - V otvorenom okne **New Object – User** vytvorte používateľa **Bakalaris** a klinite na **Next**.

- Vložte a potvrďte heslo **Qwert123**.
- Prezrite si možnosti nastavenia hesla pre daného užívateľa. Pre túto laboratórnu úlohu zvoľte možnosť **Password never expires**, kliknite na **Next** a následne **Finish**.
- Dvojklikom otvorte vytvoreného užívateľa Bakalaris, prejdite do záložky **Member of**, kliknite **Add**, napíšte **domain admins**, overte kliknutím na **Check names** a potvrďte kliknutím na **OK**.
- Prejdite do okna **Start >Administrator > Sign out**.
- Kliknite na **Other user** a prihláste sa cez novovytvoreného užívateľa. Nezabudnite pred login vložiť názov domény **(BACHELOR\Bakalaris > Qwert123)**.

4. Nakonfigurujte DNS zónu **sec.bachelor.local**.
   - V okne Server Manager kliknite na **Tools > DNS**.
   - V okne DNS Manager kliknite pravým tlačidlo myši na **Forward Lookup Zones >New Zone**.
   - V okne New Zone Wizard kliknite **3-krát Next** a pomenujte novú zónu **sec.bachelor.local**.
   - Pridajte nový zdrojový DNS záznam do zóny sec.bachelor.local kliknutím pravým tlačidlom na zónu a z kontextovej ponuky vyberte **New Host (A or AAAA)**.
   - Pomenujte ho **dc1**, IP adresu nastavte **10.0.0.1** a kliknite na **Add Host**. Overte si, že záznam **dc1.sec.bachelor.local** bol úspešne pridaný a kliknite na **OK**.
   - Ukončite pridávanie kliknutím na **Done**.
5. Povolenie **Vzdialenej plochy** na **DC1**.
   - V okne Server Manager kliknite na **Local Server**.
   - Kliknite na **Disabled** vedľa Remote Desktop.
   - V okne System Properties, v záložke **Remote**, zakliknite **Allow remote connections to this computer** a odkliknúť Allow connections only from computers running Remote Desktop with Network Level Authentification (recommended).
   - Kliknite na **Select Users > Add** a pridajte užívateľa **BACHELOR\Bakalaris**. Potvrďte kliknutím 3-krát **OK**.

Konfigurácia klienta Windows 8.1

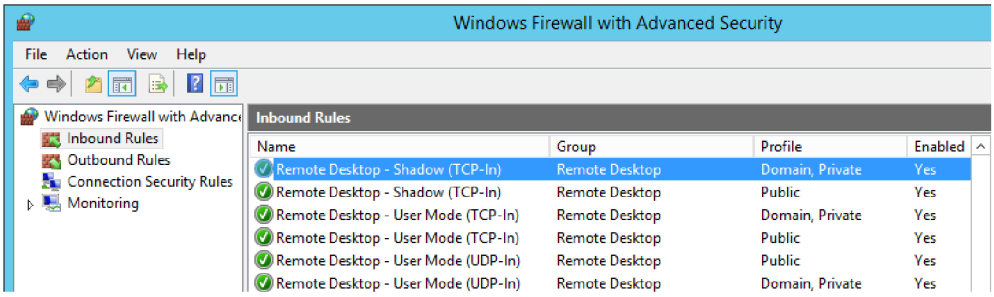
1. Nastavte IP adresu počítača **10.0.0.2**, masku podsiete 2**55.255.255.0** a preferovaný DNS server **10.0.0.1**.
2. Pripojte PC do domény **bachelor.local**.
   - Kliknite na **Štart**, napíšte **sysdm.cpl** a potvrďte.

- V okne **Vlastnosti systému** kliknite na **Zmeniť**, zvoľte **Členstvo**, vpíšte **bachelor.local** a potvrďte **OK**.
- Po vyzvaní sa prihláste použitím prihlasovacích údajov užívateľa **Bakalaris**.
- Po úspešnom prihlásení do domény uvidíte správu **Vitajte v doméne Bachelor**, 2-krát potvrďte a následne potvrďte aj reštart počítača.
- Po reštartovaní kliknite na šípku doľava > **Other user** a prihláste sa ako **BACHELOR\Bakalaris**.

5.3.3 Postup riešenia

Dotaz na nepodpísanú zónu bez vyžadovaného DNSSEC overenia

1. V simulačnom prostredí GNS3 kliknite pravým tlačidlom na linku medzi serverom a prepínačom, zvoľte **Start Capture**, vyberte port na prepínači a potvrďte **Ok**.
   Poznámka: GNS3 neumožňuje spustiť Wireshark na rozhraniach VirtualBoxu.
2. Do príkazového riadku na Windows 8.1 vpíšte príkaz **resolve-dnsname dc1.sec.bachelor.local –server dc1 –dnssecok**.
   *Poznámka: Parameter **dnssecok** v tomto príkaze oznamuje DNS serveru, že rozumie DNSSEC a server mu môže poslať bezpečnostné záznamy. Keďže zóna nie je podpísaná, v odpovedi sa nebude nachádzať žiadny podpis (RRSIG).*
3. Overte funkčnosť pripojenia Vzdialenej plochy k doménovému kontroleru DC1 príkazom **mstsc /v:dc1.sec.bachelor.local**.
   Poznámka: Ak pripojenie k Vzdialenej ploche nebude fungovať, vo firewalle povoľte pravidlá pre Vzdialenú plochu pre všetky typy sietí (v reálnej situácii toto v žiadnom prípade nerobte!), viď obr. 5.6.



Obr. 5.6: Nastavenie firewallu na Windows servery

4. Po vyzvaní vložte login a heslo užívateľa Bakalaris.
5. Okno s informáciou o probléme s overením vzdialeného počítača potvrďte kliknutím na **Áno**.

6. Overte, že ste sa úspešne pripojili k Vzdialenej ploche doménového kontrolera a ukončite reláciu.
7. Vypnite zachytávanie paketov v programe Wireshark a pozrite sa na priebeh komunikácie medzi serverom a klientom.

Podpísanie zóny na DC1

1. Na servery DC1 spustite DNS Manager, kliknite na **Forward Lookup Zones > sec.bachelor.local**, kliknite pravým tlačidlom na zónu sec.bachelor.local, **DNSSEC > Sign the Zone**.
2. Zakliknite **Use default settings to sign the zone** a pokračujte, až kým vám nevypíše **The zone has been successfully signed** a potvrďte kliknutím na **Finish**.
3. Obnovte DNS Manager a všimnite si, že pribudli rôzne záznamy ako napríklad DNSKEY, RRSIG a NSEC3.

Dotaz na podpísanú zónu bez vyžadovaného DNSSEC overenia

1. V simulačnom prostredí GNS3 spustite zachytávanie paketov.
2. Do príkazového riadku na klientskom počítači vložte príkaz **resolve-dnsname dc1.sec.bachelor.local –server dns1 –dnssecok**.
3. Pre overenie, že DNSSEC overovanie nie je momentálne vyžadované, vložte do príkazového riadku príkaz **Get-DnsClientNrptPolicy**.
4. Vypnite zachytávanie paketov v programe Wireshark a pozrite sa na priebeh komunikácie.

Dotaz na podpísanú zónu s vyžadovaným DNSSEC overením

1. V okne Server Manager spustite **Group Policy Management**, presuňte sa do **Domains > bachelor.local > Group Policy Objects**, kliknutím pravým tlačidlom na **Default Domain Policy** a zvoľte **Edit**.
2. V okne Group Policy Management Editor sa presuňte do **Computer Configuration > Policies > Windows Settings > Name Resolution Policy**. V panely **Create Rules** a vyberte **Suffix > sec.bachelor.local**.
3. V záložke DNSSEC zakliknite **Enable DNSSEC in this rule** a pod **Validation** zaklknite **Require DNS clients to check that name and address data has been validated by the DNS server**.
4. V spodnej časti kliknite na **Create** a overte, že pravidlo pre sec.bachelor.local bolo pridané do tabuľky **Name Resolution Policy Table**.
5. Potvrďte kliknutím na **Apply** a zatvorte Group Policy Management Editor.
6. Na servery vložte do **Windows PowerShell** nasledujúce príkazy:

```
gpupdate /force
```

```
Get-DnsClientNrptPolicy
```

7. Overte, že Zásady skupiny boli obnovené a že hodnota **DnsSecValidationRequired** pre Namespace sec.bachelor.local je **True**.
8. Aktualizujte Zásady skupiny aj na Windows 8.1 a overte NRPT zásadu.
   Poznámka: NRPT (Name Resolution Policy Table) je používaný na vyžiadanie DNSSEC overenia.
9. V simulačnom prostredí GNS3 spustite zachytávanie paketov.
10. Na Windowse 8.1 vložte do príkazového riadku príkazy:
    resolve-dnsname –name dc1.sec.bachelor.local –type soa –server dns1 -dnssecok
    resolve-dnsname –name sec.bachelor.local –type dnskey –server dns1 -dnssecok.
11. Vypnite zachytávanie paketov v programe Wireshark a pozrite sa na priebeh komunikácie. V položke Information si všimnite položky SOA a DNSKEY.

BONUS: Podpísanie zóny s vlastnými parametrami

1. Zrušte podpis zóny sec.bachelor.local. Otvorte DNS Manager a presuňte sa do **Forward Lookup Zones > sec.bachelor.local**, kliknite pravým tlačidlom na zónu sec.bachelor.local a kliknite na **DNSSEC > Unsign the Zone**.
2. Obnovte DNS Manager a overte, že zóna sec.bachelor.local neobsahuje DNSSEC záznamy.
3. Znovu kliknite pravým tlačidlom na zónu sec.bachelor.local a presuňte sa do **DNSSEC > Sign the Zone**.
4. V otovrenom okne kliknite na **Next**, v ďalšom okne zvoľte **Customize zone signing parameters** a znovu kliknite na **Next**.
5. V okne Key Master overte, že je zvolená možnosť **The DNS server DC1 is the Key Master** a kliknite na **Next** 2-krát.
6. V okne Key Signing Key (KSK) kliknite na exitujúci KSK kľúč a kliknite na **Remove**.
7. Pridajte nový KSK kľúč kliknutím na **Add**. V okne New Key Signing Key (KSK) si prezrite parametre, ktoré je možné upraviť a upravte hodnotu **DNSKEY RRSET signature provider validity period (hours)** na Vami zvolenú hodnotu.
8. Postupným klikaním na **Next** sa dostanete na koniec konfigurácie podpísania zóny. Prezrite si jednotlivé okná a parametre v nich.
9. Potvrďte kliknutím na **Finish** a obnovte DNS Manager. Týmto ste nastavili DNSKEY s vlastnými parametrami.

6 ZÁVER

V bakalárskej práci sa nachádzajú tri laboratórne úlohy. Tie sú vytvárané v simulačnom prostredí GNS3, ktorý emuláciou sieťových prvkov a rôznych koncových staníc dokáže simulovať komplexné sieťové topológie.

Laboratórne úlohy sú vytvorené s predpokladom základných znalostí konfigurácie Cisco smerovačov, práce v Linux termináli a práce s OS Microsoft Windows 8.1 a Microsoft Windows Server 2012 R2. Postupy riešenia rátajú s určitou samostatnosťou pri ich vypracovávaní, ale obsahujú aj príklady príkazov s vysvetleniami a odpoveďami na kontrolné otázky. Pre lepšiu predstavu obsahuje každá úloha obrázok topológie, tabuľku adries a stručný opis danej problematiky. Celú konfiguráciu je následne možné pozrieť v prílohe.

Prvá laboratórna úloha zameraná na konfiguráciu BGP protokolu má komplexný charakter. Znázorňuje situáciu s niekoľkými rôznymi Autonómnymi systémami, ktoré majú rôzne požiadavky na pripojenie. Úloha slúži na doplnenie znalostí práce s BGP protokolom.

Druhá laboratórna úloha pojednáva o rozdieloch medzi tranzitným a peeringovým spojením. Jej podstatou je porovnanie rýchlostí spojenia a odozvy, k čomu je použitý nástroj Iperf. Ten je využitý nielen na meranie týchto parametrov, ale tiež slúži na generovanie prevádzky na pozadí.

Tretia laboratórna úloha sa venuje základným princípom bezpečnostného rozšírenia systému doménových mien DNSSEC. Úloha je zameraná na DNSSEC záznamy DNSKEY, RRSIG a iné.

LITERATÚRA

[1] FUSZNER, Mike *GNS3 - Graphical Network Simulator* [online]. [cit. 30.05.2016]. Dostupné z URL: <https://www.csd.uoc.gr/~hy435/material/GNS3-0.5-tutorial.pdf>

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

[3] BARNIAK, Martin *Návrh nových laboratorních úloh pro prostředí GNS3*: diplomová práca. BRNO: Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, Ústav telekomunikací, 2015. 140 s. Vedúci práce bol Ing. Jan Jeřábek, Ph.D.

[4] *Dynamips / Dynagen Tutorial* [online]. [cit. 30.05.2016]. Dostupné z URL: <http://www.iteasypass.com/Dynamips.htm>

[5] Wikipedia contributors *QEMU* [online]. Posledná úprava 11.05.2016 [cit. 30.05.2016]. Dostupné z URL: <https://en.wikipedia.org/w/index.php?title=QEMU&oldid=719818210>

[6] Oracle *VirtualBox* [online].[cit. 30.05.2016]. Dostupné z URL: <https://www.virtualbox.org/>

[7] KUROSE, James F a Keith W ROSS. *Počítačové sítě*, 1. vyd. Brno: Computer Press, 2014, 622 s. ISBN 978-80-251-3825-0.

[8] *Rozdelenie sietí* [online].[cit. 30.05.2016]. Dostupné z URL: <http://www.sieteblb.wbl.sk/Rozdelenie-sieti.html>

[9] *Směrovací protokol BGP* [online]. [cit. 15.12.2015]. Dostupné z URL: <http://www.cs.vsb.cz/grygarek/SPS/lect/BGP/BGP.html>

[10] JEŘÁBEK, Jan. *Pokročilé komunikační techniky. Skriptum FEKT Vysoké učení technické v Brně*, 2015. s. 1-193.

[11] *Popis protokolu BGP a jeho využití* [online]. [cit. 15.12.2015]. Dostupné z URL: <http://isp-servis.cz/clanky.html>

[12] *Border Gateway Protocol (BGP) Parameters* [online]. Posledná úprava 03.11.2015 [cit. 15.12.2015]. Dostupné z URL: <http://www.iana.org>

[13] DANĚK, M. *Směrovací mechanizmy mezi autonomními systémy Internetu.* Brno: Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, 2015. 71 s. Vedoucí bakalářské práce doc. Ing. Vít Novotný, Ph.D.

[14] JELÍNEK, Ondřej *Lokace stanice v síti Internet pomocí analýzy doménových názvů*: bakalářská práce. Brno: Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, Ústav telekomunikací, 2013. 45 s. Vedoucí práce byl doc. Ing. Dan Komosný, Ph.D.

[15] Wikipedia a prispievatelia. *Domain Name System* [online]. Posledná úprava 11.12.2015 [cit. 15.12.2015]. Dostupné z URL: <`https://en.wikipedia.org/w/index.php?title=Domain_Name_System&oldid=694808227`>

[16] CZ.NIC *O DNSSEC* [online]. [cit. 30.05.2016]. Dostupné z URL: <`http://www.dnssec.cz/`>

[17] CZ.NIC *JAK FUNGUJE DNSSEC* [online]. [cit. 30.05.2016]. Dostupné z URL: <`http://www.dnssec.cz/page/444/jak-funguje-dnssec/`>

[18] Wikipedia contributors *Domain Name System Security Extensions* [online]. Posledná úprava 05.05.2016 [cit. 30.05.2016]. Dostupné z URL: <`https://en.wikipedia.org/w/index.php?title=Domain_Name_System_Security_Extensions&oldid=718788008`>

[19] RAFTERY, James *Securing your DNS information with Transaction Signatures (TSIG)* [online]. [cit. 30.05.2016]. Dostupné z URL: <`http://romana.now.ie/james/tsig.html`>

[20] Wikipedia contributors *Iperf* [online]. Posledná úprava 18.05.2016 [cit. 30.05.2016]. Dostupné z URL: <`https://en.wikipedia.org/w/index.php?title=Iperf&oldid=720901726`>

[21] *Iperf* [online]. [cit. 30.05.2016]. Dostupné z URL: <`https://iperf.fr/iperf-doc.php#3doc`>

[22] *iPerf 3 user documentation* [online]. [cit. 30.05.2016]. Dostupné z URL: <`http://software.es.net/iperf/`>

[23] TEARE, Diane. *Implementing Cisco IP routing (ROUTE): foundation learning guide : foundation learning for the ROUTE 642-902 exam. Indianapolis: Cisco Press*, 2010, xxix, 945 s. ISBN 978-1-58705-882-0.

[24] Dynamic Network Services: Internet Performance, Research [online]. Dyn, ©2015 [cit. 2015-09-11]. Dostupné z URL: <http://research.dyn.com/>.

[25] *BGP Best Path Selection Algorithm* [online]. Posledná úprava 18.11.2015 [cit. 15.12.2015]. Dostupné z URL: <http://www.cisco.com/c/en/us/support/docs/ip/border-gateway-protocol-bgp/13753-25.html>

[26] *Step-by-Step: Demonstrate DNSSEC in a Test Lab* [online]. Posledná úprava 25.03.2014 [cit. 30.05.2016]. Dostupné z URL: <https://technet.microsoft.com/en-us/library/hh831411.aspx?f=255&MSPPError=-2147217396>

[27] Wikipedia contributors *Dynamips* [online]. Posledná úprava 17.02.2016 [cit. 30.05.2016]. Dostupné z URL: <https://en.wikipedia.org/w/index.php?title=Dynamips&oldid=705353836>

[28] *GNS3 Vault* [online]. [cit. 30.05.2016]. Dostupné z URL: <http://gns3vault.com/>

ZOZNAM SYMBOLOV, VELIČÍN A SKRATIEK

AMD	Pokročilé mikro zariadenia - Advanced Micro Devices
AS	Autonómny systém - Autonomous System
ASA	Adaptívne zabezpečovacie zariadenie - Adaptive Security Appliance
ASN	Číslo autonómneho systému - Autonomous System Number
AT&T	American Telephone and Telegraph
BGP	Smerovací protokol - Border Gateway Protocol
BSD	Berkeley Software Distribution
CCIE	Cisco Certified Internetwork Expert
CCNA	Cisco certifikovaný sieťový Cisco Certified Network Associate
CCNP	Cisco certifikovaný sieťový profesionál - Cisco Certified Network Professional
CIDR	Beztriedne medzidoménové smerovanie - Classless Inter-Domain Routing
CNAME	Záznam kanonického mena - Canonical Name record
CPU	Centrálny procesorová jednotka - Central Processing Unit
DHCP	Protokol dynamickej konfigurácie koncového uzla – Dynamic Host Configuration Protocol
DNAME	Záznam poverenia - Delegation Name record
DNS	Systém názvov domén - Domain Name System
DNSSEC	Bezpečnostné rozšírenie systému názvov domén - Domain Name System Security Extensions
DS	Delegation Signer
eBGP	Vonkajšie susedstvo BGP smerovačov - External BGP
EIGRP	Smerovací protokol – Enhanced Interior Gateway Routing Protocol
GNS3	Grafický sieťový simulátor - Graphical Network Simulator-3

GUI	Grafický užívateľské rozhranie - Graphical User Interface
IANA	Autorita pri prideľovanie čísel na Internete - Internet Assigned Numbers Authority
iBGP	Vnútorné susedstvo BGP smerovačov - Internal BGP
ID	Identifikátor - Identificator
Intel	Integrovaná elektronika - Integrated Electronics
IOS	Sieťový operačný systém - Internetwork Operating System
IP	Internet Protocol
ISP	Poskytovateľ internetového pripojenia - Internet Service Provider
LAN	Lokálna sieť - Local Area Network
KSK	Kľúč podpisu kľúča - Key Signing Key
MacOS	Operačný systém Macintosh – Macintosh Operating System
MAN	Metropolitná sieť - Metropolitan Area Network
MD5	Message-Digest algorithm
MIPS	Procesor bez automaticky spojeného zreťazeného spracovania - Microprocessor without Interlocked Pipeline Stages
MS	Microsoft
NS	Záznam názvu autoritatívneho serveru - Name Server record
NSEC	Next Secure Record
NSEC3	Next Secure Record version 3
NTT	Nippon Telegraph and Telephone
OS	Operačný systém - Operating system
OSPF	Smerovací protokol - Open Shortest Path First
PAN	Osobná sieť - Personal Area Network
PIX	Súkromná internetová ústredňa - Private Internet eXchange
QEMU	Rýchly emulátor - Quick Emulator

RFC	Žiadosť o komentáre - Request For Comments
RIPv2	Smerovací protokol verzia 2 - Routing Information Protocol version 2
RRSIG	Záznam zdrojového podpisu - Resource Record Signature
TCP	Vysielací kontrolný protokol – Transmission Control Protocol
TLD	Doména najvyššej úrovne - Top Level Domain
TSIG	Podpisovanie transakcií - Transaction Signature
UDP	Používateľský datagramový protokol – User Datagram Protocol
WAN	Rozsiahla sieť - Wide Area Network
ZSK	Kľúč podpisu zóny - Zone Signing Key

ZOZNAM PRÍLOH

A KONFIGURÁCIA LABORATÓRNYCH ÚLOH

V tejto prílohe sa nachádzajú použité príkazy z každej úlohy v kopírovateľnom tvare.

A.1 Laboratórna úloha č.1 - Komplexná konfigurácia protokolu BGP

1. **Konfigurácia IP adries na rozhraniach**

```
Smerovač R1:
interface serial0
ip address 10.1.1.0 255.255.255.254
no shutdown
interface serial1
ip address 10.1.1.3 255.255.255.254
no shutdown
interface loopback0
ip address 192.168.1.1 255.255.255.0

Smerovač R2:
interface serial0
ip address 10.1.1.2 255.255.255.254
no shutdown
interface loopback0
ip address 2.2.2.2 255.255.255.0

Smerovač R3:
interface serial0
ip address 10.1.1.3 255.255.255.254
no shutdown
interface serial1
ip address 10.1.1.4 255.255.255.254
no shutdown
interface serial2
ip address 10.1.1.6 255.255.255.254
no shutdown

Smerovač R4:
interface serial0
```

```
ip address 10.1.1.5 255.255.255.254
no shutdown
interface serial1
ip address 10.1.1.8 255.255.255.254
no shutdown
```

```
Smerovač R5:
interface serial0
ip address 10.1.1.7 255.255.255.254
no shutdown
interface serial1
ip address 10.1.1.10 255.255.255.254
no shutdown
```

```
Smerovač R6:
interface serial0
ip address 10.1.1.9 255.255.255.254
no shutdown
interface serial1
ip address 10.1.1.11 255.255.255.254
no shutdown
interface serial2
ip address 172.16.1.0 255.255.255.254
no shutdown
```

```
Smerovač R7:
interface serial0
ip address 172.16.1.1 255.255.255.254
no shutdown
interface loopback0
ip address 172.16.2.1 255.255.255.0
no shutdown
```

2. **Konfigurácia EIGRP v AS 300**

```
Smerovač R3:
router eigrp 300
network 10.1.1.4 0.0.0.1
network 10.1.1.6 0.0.0.1
```

```
Smerovač R4:
router eigrp 300
network 10.1.1.4 0.0.0.1

Smerovač R5:
router eigrp 300
network 10.1.1.6 0.0.0.1
```

3. **Konfigurácia iBGP**

```
Smerovač R3:
router bgp 300
neighbor 10.1.1.5 remote-as 300
neighbor 10.1.1.7 remote-as 300

Smerovač R4:
router bgp 300
neighbor 10.1.1.4 remote-as 300
neighbor 10.1.1.7 remote-as 300

Smerovač R5:
router bgp 300
neighbor 10.1.1.5 remote-as 300
neighbor 10.1.1.6 remote-as 300
```

4. **Konfigurácia eBGP**

```
Smerovač R1:
router bgp 100
neighbor 10.1.1.1 remote-as 200
neighbor 10.1.1.3 remote-as 300
network 192.168.1.0 mask 255.255.255.0

Smerovač R3:
router bgp 200
neighbor 10.1.1.0 remote-as 100
network 2.2.2.0 mask 255.255.255.0

Smerovač R3:
router bgp 300
neighbor 10.1.1.2 remote-as 100
```

```
Smerovač R4:
router bgp 300
neighbor 10.1.1.9 remote-as 400

Smerovač R5:
router bgp 300
neighbor 10.1.1.11 remote-as 400

Smerovač R6:
router bgp 400
neighbor 10.1.1.8 remote-as 300
neighbor 10.1.1.10 remote-as 300
neighbor 172.16.1.1 remote-as 65500

Smerovač R7:
router bgp 65500
neighbor 172.16.1.0 remote-as 400
network 172.16.2.0 mask 255.255.255.0
```

5. **Private AS(Súkromný AS)**

```
Smerovač R6:
router bgp 400
neighbor 10.1.1.8 remove-private-as
neighbor 10.1.1.10 remove-private-as
```

6. **Non-transit AS(Netranzitný AS)**

```
Smerovač R1:
ip as-path access-list 1 permit \^{}\$

neighbor 10.1.1.1 filter-list 1 out
neighbor 10.1.1.3 filter-list 1 out
```

7. **MD5 autentifikácia**

```
Smerovač R1:
router bgp 100
neighbor 10.1.1.1 password AAA

Smerovač R2:
router bgp 200
neighbor 10.1.1.0 password AAA
```

8. **Nastavenie preferovanej cesty z/do AS 400**

```
Smerovač R4:
route-map secondary permit 10
set local-preference 150
exit
router bgp 300
neighbor 10.1.1.9 route-map secondary in

Smerovač R5:
route-map primary permit 10
set local-preference 200
exit
router bgp 300
neighbor 10.1.1.11 route-map primary in

Smerovač R6:
route-map primary permit 10
set local-preference 200
exit
route-map secondary permit 20
set local-preference 150
exit
router bgp 400
neighbor 10.1.1.10 route-map primary in
neighbor 10.1.1.8 route-map secondary in
```

9. **Demonštrácia výpadku linky**

```
Ping s vyšším počtom opakovaní
Smerovač R1:
ping 172.16.2.1 source loopback 0 repeat 200

Vypnutie linky medzi R3 a R5
Smerovač R3:
interface serial2
shutdown
```

A.2 Laboratórna úloha č.2 - Porovnanie tranzitu a peeringu

Konfigurácia smerovačov

```
Smerovač R1:
hostname R1
Interface Serial0
ip address 1.1.1.0 255.255.255.254
no shutdown
Interface Serial1
ip address 1.1.1.2 255.255.255.254
no shutdown
router bgp 1
network 1.1.1.0
network 1.1.1.0 mask 255.255.255.254
network 1.1.1.2 mask 255.255.255.254
neighbor 1.1.1.1 remote-as 100
neighbor 1.1.1.3 remote-as 200

Smerovač R2:
hostname R2
interface FastEthernet0
ip address 192.168.1.1 255.255.255.0
no shutdown
speed 10
interface Serial0
ip address 1.1.1.1 255.255.255.254
no shutdown
clock rate 8000000
interface Serial1
ip address 10.10.10.0 255.255.255.254
no shutdown
interface Serial2
ip address 10.10.10.2 255.255.255.254
no shutdown
router bgp 100
network 1.1.1.0 mask 255.255.255.254
network 10.10.10.0 mask 255.255.255.254
```

```
network 10.10.10.2 mask 255.255.255.254
network 192.168.1.0
neighbor 1.1.1.0 remote-as 1
neighbor 10.10.10.1 remote-as 1000
neighbor 10.10.10.3 remote-as 100

Smerovač R3:
hostname R3
interface FastEthernet0
ip address 192.168.2.1 255.255.255.0
speed 10
interface Serial0
ip address 1.1.1.3 255.255.255.254
no shutdown
clock rate 8000000
interface Serial1
ip address 20.20.20.0 255.255.255.254
no shutdown
router bgp 200
network 3.3.3.0 mask 255.255.255.0
network 20.20.20.0 mask 255.255.255.254
network 192.168.2.0
neighbor 1.1.1.2 remote-as 1
neighbor 20.20.20.1 remote-as 2000

Smerovač R4:
hostname R4
interface FastEthernet0
ip address 100.100.100.1 255.255.255.0
no shutdown
speed 10
interface Serial0
ip address 10.10.10.1 255.255.255.254
no shutdown
clock rate 4000000
interface Serial1
ip address 30.30.30.0 255.255.255.254
no shutdown
clock rate 5300000
```

```
router bgp 1000
network 30.30.30.0 mask 255.255.255.254
network 100.100.100.0 mask 255.255.255.0
neighbor 10.10.10.0 remote-as 100
neighbor 30.30.30.1 remote-as 2000

Smerovač R5:
hostname R5
interface FastEthernet0
ip address 200.200.200.1 255.255.255.0
no shutdown
speed 10
interface Serial0
ip address 20.20.20.1 255.255.255.254
no shutdown
clock rate 4000000
interface Serial1
ip address 30.30.30.1 255.255.255.254
no shutdown
router bgp 2000
network 200.200.200.0
neighbor 20.20.20.0 remote-as 200
neighbor 30.30.30.0 remote-as 1000
```

1. **Konfigurácia IP adries**

```
Client:
ifconfig eth0:avahi 100.100.100.100/24
route add default gw 100.100.100.1 eth0:avahi

Client2:
ifconfig eth0:avahi 192.168.2.100/24
route add default gw 192.168.2.1 eth0:avahi

Server:
ifconfig eth0:avahi 200.200.200.200/24
route add default gw 200.200.200.1 eth0:avahi

Server2:
ifconfig eth0:avahi 192.168.1.100/24
```

```
route add default gw 192.168.1.1 eth0:avahi

Smerovač R4:
Interface Serial1
shutdown
```

2. **Demonštrácia tranzitného spojenia**

```
Server:
iperf3 -s

Server2:
iperf3 -D

Client2:
iperf3 -c 192.168.1.100 -w 100K -t 60 -i 0.5

Client:
iperf3 -c 200.200.200.200
```

3. **Demonštrácia peeringového spojenia**

```
Smerovač R4:
Interface Serial1
no shutdown

Client:
iperf3 -c 200.200.200.200
```

B OBSAH PRILOŽENÉHO CD

Priložené CD obsahuje elektronickú verziu bakalárskej práce a priečinok s jednotlivými vypracovanými laboratórnymi úlohami vo forme GNS3 topológií.

```
/
├── 164414 ..... Priečinok s praktickou časťou práce
│   ├── Lab1 ..... Priečinok obsahujúci súbory k prvej laboratórnej úlohe
│   │   ├── project-files ..... Priečinok s projektovými súbormi
│   │   │   └── dynamips ..... Priečinok s konfiguračnými súbormi
│   │   └── Lab1.gns3 ..... Spustiteľný GNS3 súbor
│   ├── Lab2 ..... Priečinok obsahujúci súbory k druhej laboratórnej úlohe
│   │   ├── project-files ..... Priečinok s projektovými súbormi
│   │   │   ├── dynamips ..... Priečinok s konfiguračnými súbormi
│   │   │   └── virtualbox ..... Priečinok použitých VM
│   │   └── Lab2.gns3 ..... Spustiteľný GNS3 súbor
│   └── Lab3 ..... Priečinok obsahujúci súbory k tretej laboratórnej úlohe
│       ├── project-files ..... Priečinok s projektovými súbormi
│       │   ├── dynamips ..... Priečinok s konfiguračnými súbormi
│       │   └── virtualbox ..... Priečinok použitých VM
│       └── Lab3.gns3 ..... Spustiteľný GNS3 súbor
└── BP_Siklosi_164414 ..... Elektronická verzia bakalárskej práce
```