ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE
Fakulta elektrotechnická
Katedra telekomunikační techniky

Simulátor síťového prostředí

Network Environment Simulator

Vedoucí práce: Ing. Pavel Bezpalec, Ph.D.
Diplomant: Bc. Daniel Rantoš

Praha, Červen 2018

Čestné prohlášení

Prohlašuji, že jsem zadanou diplomovou práci zpracoval sám s přispěním vedoucího práce a používal jsem pouze literaturu v práci uvedenou. Dále prohlašuji, že nemám námitek proti půjčování nebo zveřejňování mé diplomové práce nebo její části se souhlasem katedry.

V Praze dne 25. 5. 2018

.....
Bc. Daniel Rantoš

ZADÁNÍ DIPLOMOVÉ PRÁCE

I. OSOBNÍ A STUDIJNÍ ÚDAJE

Příjmení: **Rantoš** Jméno: **Daniel** Osobní číslo: **420407**

Fakulta/ústav: **Fakulta elektrotechnická**

Zadávající katedra/ústav: **Katedra telekomunikační techniky**

Studijní program: **Elektronika a komunikace**

Studijní obor: **Komunikační systémy a sítě**

II. ÚDAJE K DIPLOMOVÉ PRÁCI

Název diplomové práce:

Simulátor síťového prostředí

Název diplomové práce anglicky:

Network Environment Simulator

Pokyny pro vypracování:

Podrobně analyzujte možnosti dostupných simulátorů a emulátorů síťového prostředí. Zaměřte se zejména na možnost propojení simulované/emulované sítě s reálnými síťovými prvky. Svá zjištění doprovoďte experimentem. Vytvořte výukové pracoviště s podklady pro laboratorní výuku.

Seznam doporučené literatury:

[1] Banks, J. at al.: Discrete-Event System Simulation, 5th edition. Prentice Hall, 2009. ISBN: 978-0-13606-212.7.
[2] GNS3. Dostupné na http://www.gns3.com [on-line], GNS3 2007-2017.
[3] Cisco PacketTracer - simulation tool. Dostupný na http://www.netacad.com [on-line]. Cisco Inc. 2017.
[4] eNSP. Dostupné na http://www.ensp.com [on-line]. Huawei Inc. 2017.

Jméno a pracoviště vedoucí(ho) diplomové práce:

Ing. Pavel Bezpalec, Ph.D., katedra telekomunikační techniky FEL

Jméno a pracoviště druhé(ho) vedoucí(ho) nebo konzultanta(ky) diplomové práce:

Datum zadání diplomové práce: **04.01.2018** Termín odevzdání diplomové práce: **25.05.2018**

Platnost zadání diplomové práce: **30.09.2019**

Ing. Pavel Bezpalec, Ph.D. podpis vedoucí(ho) práce	podpis vedoucí(ho) ústavu/katedry	prof. Ing. Pavel Ripka, CSc. podpis děkana(ky)

III. PŘEVZETÍ ZADÁNÍ

Diplomant bere na vědomí, že je povinen vypracovat diplomovou práci samostatně, bez cizí pomoci, s výjimkou poskytnutých konzultací. Seznam použité literatury, jiných pramenů a jmen konzultantů je třeba uvést v diplomové práci.

. | Datum převzetí zadání

Podpis studenta

Anotace

Tato diplomová práce se nejprve zabývá teoretickými principy spojitých a diskrétních simulací a následně analýzou a možnostmi propojení simulátorů a emulátorů síťového prostředí s fyzickými síťovými prvky. Jako reálné i emulované síťové prvky byla použita zařízení od výrobců Cisco a Huawei. Dále bylo vytvořeno výukové pracoviště a tři laboratorní úlohy, ve kterých byl kladen důraz právě na využití propojení virtuální a externí sítě. Jednotlivé úlohy, tématicky zaměřené na směrovací protokol OSPF a multicast jsou rozděleny do několika částí: zadání s topologií, rozbor a postupný návod. V příloze je uvedena celá konfigurace. Laboratorní úlohy byly realizovány v emulátorech datových sítí GNS3 a eNSP.

Klíčová slova

Simulace, simulátor, emulátor, GNS3, Dynamips, eNSP, Cisco Packet Tracer, Cisco VIRL

Summary

This diploma thesis first deals with theoretical principles of continuous and discrete-event simulations, then, with the analysis and possibilities of interconnection of simulators and emulators of network environment with the real network system. Both the real and emulated network elements were used as devices manufactured by Cisco and Huawei Companies. In addition, a training centre and three laboratory tasks were created in which the emphasis was placed on the use of virtual and external network connections.Each task, thematically focused on the OSPF and multicast routing protocols, is divided into several parts: assignment for typology designs, analysis, and gradual guidance.The complete configuration is listed in the appendix. Laboratory tasks were performed in emulators of the data networks GNS3 and eNSP.

Index Terms

Simulation, simulator, emulator, GNS3, Dynamips, eNSP, Cisco Packet Tracer, Cisco VIRL

Poděkování

Děkuji vedoucímu práce Ing. Pavlu Bezpalcovi, Ph.D. za velmi užitečnou metodickou pomoc a cenné rady při zpracování této diplomové práce.

Dále bych chtěl poděkovat celé mé rodině včetně přítelkyně za podporu, trpělivost a povzbuzování při psaní této práce.

Obsah

Seznam obrázků

Seznam tabulek

Úvod

Síťové technologie jsou neoddělitelnou součástí dnešní doby. Jejich využití našlo uplatnění téměř v každém odvětví. Postupem času však přestalo stačit sítě pouze navrhovat a implementovat. Takto realizovaná síť se může chovat neočekávaně a v nejhorším případě může nastat i její celková nefunkčnost. Pokud bychom takovou neodzkoušenou síť začali využívat v produkčním prostředí, mohlo by to mít nedozírné následky v podobě snížené kvality poskytované služby.

Abychom těmto problémům zabránili, je třeba síť před nasazením do ostrého provozu řádně otestovat. K analýze sítě není většinou třeba pořizovat drahé aktivní síťové prvky. Místo nich lze využít simulátory nebo emulátory síťových prostředí. Díky nim můžeme virtualizovat část nebo i celou síť. Poskytují velmi propracované prostředí, které umožňuje věrně napodobit chování fyzických zařízení a ušetřit značné finanční prostředky, které bychom museli vynaložit pořízením těchto síťových prvků.

Některé nástroje umožňují propojení s externí sítí. Této funkce můžeme využít při testování sítí složených z prvků od více než jednoho výrobce nebo připojení virtualizované sítě k již fungující topologii a sledování jejich chování.

Pro sledování provozu v datových sítích se hojně využívá software Wireshark, který je schopen odchytávat komunikaci na síťových rozhraních a následně provést podrobnou analýzu zachycených paketů. Pokročilejší nástroje umožňují integraci s tímto programem. V praxi to má za následek možnost odchytávání síťové komunikace přímo v simulované síti.

Tento typ softwaru nemusí nutně používat jen odborníci v oboru síťových technologií. Hojně se využívají i ve výuce. Asi nejznámějším výukový softwarem v tomto oboru je Packet Tracer, který je poskytován zdarma v rámci studijního programu Cisco Networking Academy. Jako další simulátory můžeme uvést neméně známý GNS3 či eNSP od společnosti Huawei.

Cílem této práce je porovnání vybraných simulátorů a emulátorů síťového prostředí se zaměřením na možnost propojení s externí sítí a toto propojení patřičně otestovat. Dále vytvoření laboratorního pracoviště a několik laboratorních úloh, které mají demonstrovat možnosti propojení daných nástrojů s externí sítí.

Samotné úlohy jsou rozděleny na zadání včetně topologie, rozbor a postup řešení. Jsou realizovány v prostředí simulátoru GNS3 a částečně i eNSP a koncipovány ve smyslu "krok za krokem". Nicméně od studenta se očekávají základní znalosti v dané problematice (model TCP/IP, adresování v IPv4 sítích, základní konfigurační příkazy v IOS apod.). Náročnost je přibližně na úrovni CCNP (Cisco Certified Network Professional). Úplné konfigurace jednotlivých síťových prvků jsou uvedeny v příloze.

1 Simulace

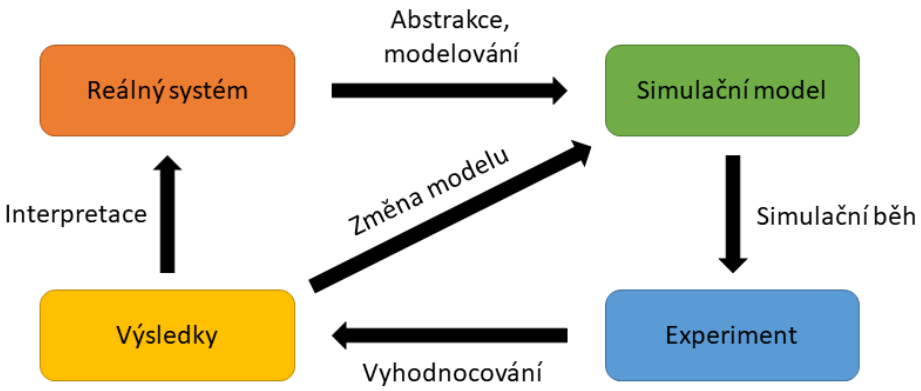
S pojmem simulace se lze setkat v mnoha souvislostech. Nejčastěji se však za simulaci považuje metoda získávání nových znalostí o prostředí či objektech, které jsou zkoumané. Toto získávání znalostí se děje realizací pokusů nad jejich modely. Simulace je v podstatě napodobování chování systému pomocí počítačového modelu [26].

Simulace nemusí nutně sloužit pouze pro získávání nových poznatků. Choi a Kang ve své publikaci [9] dělí simulace do dvou oblastí:

- Analytické simulace, které se zabývají experimentováním a získáváním nových poznatků a znalostí.
- Simulace virtuálního prostředí, jejímž cílem je vzdělání a zábava.

Cílem simulace tedy bývá studium chování reálného systému. Modely zde vystupují jako zjednodušené zobrazení reality vytvářené pomocí počítače. Složité reálné systémy nelze dokonale popsat modelem zcela přesně. Proto zde přichází zjednodušení a snaha o zachycení prvků a souvislostí, které jsou relevantní.

Pokud se jedná o systém, který již existuje, motivací pro modelování obvykle bývá snaha o předvídání důsledků změn v tomto systému. Může se jednat o změny vstupních charakteristik některých částí systému i o změnu struktury systému. Simulace však může poskytnout cenné poznatky i ve fázi návrhu zcela nového systému a může tak pomoci při rozhodování o jeho budoucí podobě [11].



Obr. 1.1: Princip simulace [16]

1.1 Historie simulací

Simulace jako metoda byla vyvinuta v polovině 20. století pro vojenské účely. Poprvé byla nasazena v projektu Manhattan ve 2. světové válce pro modelování procesu nukleární detonace. Konkrétně byla aplikována metoda Monte Carlo.

Dnešní pojetí simulace představuje disciplínu, která vznikla právě z této metody. Postupem času se simulace oddělila a stala se samostatnou disciplínou, ale i přesto je s metodou Monte Carlo často spojována. Jejich rozdílnost lze nalézt v účelu využití. Zatímco metoda Monte Carlo se zabývá statistickými odhady, simulace napomáhá ke zkoumání složitých dynamických systému [14].

Existuje několik definic pojmu simulace [15]:

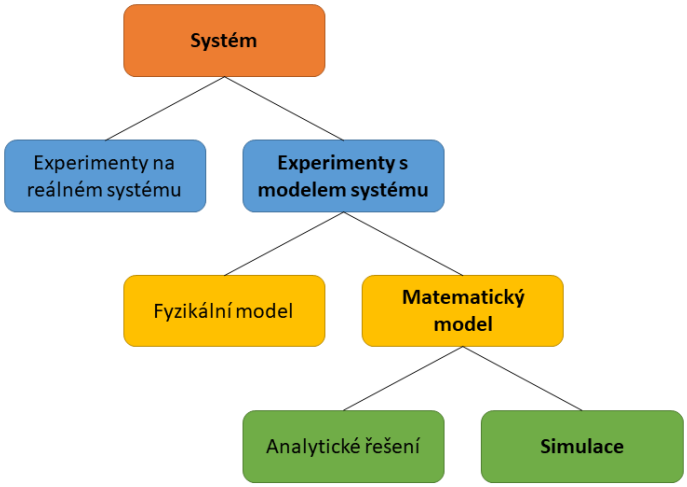
- **Shannon:** Simulace je proces tvorby modelu reálného systému a provádění experimentů s tímto modelem za účelem dosažení lepšího pochopení chování studovaného systému či za účelem posouzení různých variant činnosti systému.
- **Naylor:** Simulace je numerická metoda, která spočívá v experimentování s matematickými modely reálných systémů na číslicových počítačích.
- **Dahl:** (uvádí se jako nejznámější definice) Simulace je výzkumná metoda, jejíž podstata spočívá v tom, že zkoumaný dynamický systém nahradíme jeho simulátorem (modelem) a s ním provádíme pokusy (experimenty) s cílem získat informaci o původním zkoumaném systému.
- **Cendelín, Kindler:** Simulace je technika pro výzkum dynamických systémů, jejíž podstata spočívá v tom, že zkoumaný systém nahradíme jeho simulačním modelem a s tímto modelem provádíme experimenty proto, abychom získali informace o původním zkoumaném systému. Originál (zkoumaný systém) se v simulaci nazývá simulovaným systémem a simulační model se nazývá simulující systém nebo také simulátor [23].

1.2 Systém

Jedním ze základních pojmů simulace je systém. Jedná se o skupinu objektů se vzájemně definovanými vztahy mezi sebou. Tento popis lze rozšířit o faktory, které ovlivňují systém z vnějšku. Zmíněné externí faktory tvoří okolí systému (system enviroment) [32]. Zkoumané objekty jsou reprezentovány prvky (entitami). Mohou to být procesory, pevné disky, síťová rozhraní atp. Pro popis charakteru jednotlivých elementů entity se používají atributy. Podoba atributů nabývá různých hodnot od čísel, přes pravdivostní hodnoty, až po textové popisy [22].

Stav systému je dán souhrnem stavových proměnných a proměnných systému v určitém časovém okamžiku. Stavové proměnné jsou spjaté s jednotlivými objekty, kdežto proměnné systému se vážou k systému jako celku [9].

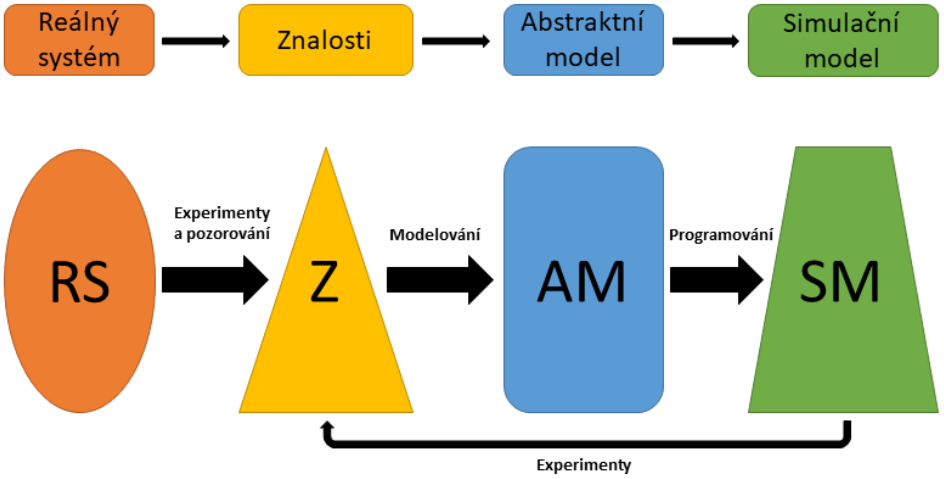
Jak již bylo výše zmíněno, systémy můžeme dělit např. z pohledu časového hlediska na statické či dynamické nebo z pohledu predikovatelnosti následujícího stavu na deterministické či stochastické. Existuje celá řada dalších kriterií, podle kterých lze systémy kategorizovat. Tato práce se zabývá především systémy dynamickými [22], [32].



Obr. 1.2: Možnosti zkoumání systému [21]

1.3 Model systému

Modelem systému se myslí popis reálného systému. Tvorba modelu neboli modelování je proces převodu vybraných entit reálného systému na objekty modelu, který musí zachovávat vlastnosti modelovaného systému. Příkladem takového popisu je mapa, která představuje zjednodušenou reprezentaci části zeměkoule [22]. Složité systémy však nelze dokonale modelovat a využívá se zjednodušený popis [28].



Obr. 1.3: Modelování [28]

1.4 Spojitá simulace

Spojité simulace (angl. continuous simulations nebo continuous system simulations) jsou charakterizovány tím, že stav systému (hodnoty stavových proměnných) se v čase mění průběžně - spojitě na rozdíl od diskrétních simulací, kde nenastává změna stavu systému v čase spojitě, ale diskrétně v určitých okamžicích. Pro popis chování spojitého modelu lze zvolit diferenciální rovnice. Nevýhodou spojitých simulací je především vysoká výpočetní náročnost. Jako příklad úloh řešené pomocí spojitých simulací můžeme uvést řešení elektrických a elektronických obvodů nebo sledování fyzikální veličiny jako je teplota, rychlost a podobně [26], [11].

1.5 Diskrétní simulace

V některých situacích je vhodné zkoumat pouze změny systému, ke kterým dochází při výskytu určitých událostí, jelikož změny, ke kterým dochází v reálném systému mezi těmito událostmi, jsou z hlediska zkoumání nezajímavé či nejsou relevantní. V tomto případě tedy zaznamenáváme pomocí modelu pouze tyto události a časové okamžiky v nichž nastávají. V anglické literatuře se setkáme výhradně s pojmem Discrete-Event Simulation [11].

1.5.1 Událost

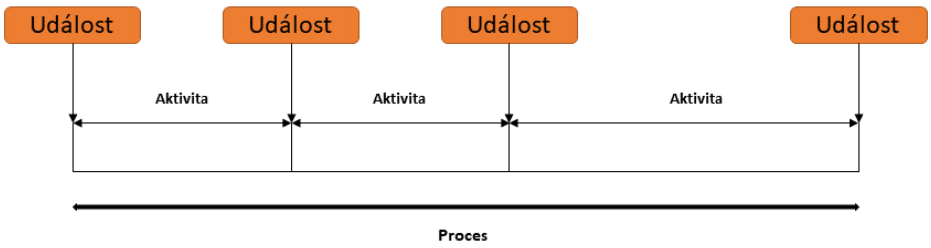
Událost představuje ústřední pojem techniky diskrétní simulace. Pomocí události se vyjadřuje změna stavu systému. Může to být např. příchod paketu či zvednutí sluchátka telefonu. V reálném světě může událost trvat určitou dobu, avšak pro potřeby simulace se tento čas zanedbává, tj. je atomická a má nulovou dobu trvání [26].

1.5.2 Kalendář událostí

Pro plánování spuštění jednotlivých událostí se využívá kalendář událostí (Future Event List). Kalendář vytváří a aktualizuje posloupnost událostí probíhajícího experimentu. Jednotlivé položky jsou řazeny vzestupně dle doby, kdy přijdou na řadu.V případe více událostí se stejným časem je výběr řízen prioritami [22].

1.5.3 Proces

Proces představuje sled událostí, které na sebe dle určité logiky navazují. Jednotlivé události mohou v procesu oddělovat prostředky, které vyjadřují čekání (aktivity reprezentující čekání ve frontě nebo operace zpracování paketu). Procesy v systému probíhají paralelně a v určitých případech spolu mohou komunikovat [22], [26].



Obr. 1.4: Proces [26]

1.5.4 Typy diskrétních simulací

Existují tři základní modelovací techniky vycházející z pojmů proces, aktivita a událost. Většina simulačních programů implementuje událostní či procesní přístup. Aplikace modelování na základě aktivit se ukázala být nevýkonnou ve většině simulačních scénářů [18].

- **Event-Scheduling** je technika modelování založená na událostním přístupu. Události popisují změnu stavu systému např. pokud přijde paket na rozhraní směrovače, zvýší se počet paketů čekajících na zpracování. Simulace představuje skupinu seřazených událostí, které jsou spolu s přiřazeným simulárním časem umísťovány do kalendáře událostí [18]. Následně jsou jednotlivé události vykonávány v tomto pořadí:
  1. Vybrání první položky kalendáře
  2. Inkrementace simulárního času na čas události
  3. Provedení události
  4. Zneplatnění (vymazání) záznamu v kalendáři
  5. Vybrání další položky z kalendáře nebo konec simulace, pokud je kalendář prázdný
- **Process-Interaction** je přístup na základě procesů. Je jednodušší než modelování událostmi, ale jeho nevýhodou je menší flexibilita a nižší programová kontrola. Od modelování na základě událostí se liší tím, že na rozdíl od atomického provedení bloku události, jednotlivé části procesů mohou začít a skončit v různých okamžicích [26].
- **Activity-Scanning** je metoda založená na základě aktivit. Simulární čas je inkrementován po diskrétních úsecích a zároveň se hledá splnění určité podmínky aktivitou. Pokud je podmínka splněna, dojde ke zpracování a obnovení stavu systému. Tato metoda je nejméně používaný princip modelování [33].

– **Three Phase Approach** je kombinací metody Activity Scanning a plánování událostí. Zůstal princip kontroly podmínek aktivit v určitý okamžik, ale pohyb v čase je realizován plánováním událostí [33].

1.6 Generátory náhodných čísel

K realizaci simulace je třeba získat vstupní náhodné proměnné. Obecně jsou dvě možnosti, jak tyto proměnné získat [15]:

– Přímo z reálného systému a jejich následné použití v simulaci. Tento způsob však není zpravidla vhodný, protože při simulačních experimentech je potřeba řádově tisíce až statisíce hodnot.
– Pozorováním reálného systému a zjištěním pravděpodobnostních zákonností, kterými se příslušné procesy řídí (tj. stanovení typu rozdělení náhodné proměnné a odhadnutí parametrů). Při simulaci se následně generují hodnoty řídící se daným rozdělením pomocí vhodného generátoru.

Historicky se náhodná čísla získávala pomocí tabulek náhodných čísel. Tento způsob se však v současnosti využívá minimálně a je vhodný pouze ke generování posloupnosti malého rozsahu. Další možností jsou generátory mechanické - házení kostkou. Generátory založené na fyzikálních jevech (rozpad radioaktivního materiálu atp.) lze označit za pravé generátory náhodných čísel. Nelze totiž předpovědět, kdy dojde k rozpadu. Na druhou stranu práce s radioaktivním materiálem je velmi nebezpečná a vyžaduje vysokou opatrnost. Nejpoužívanějšími jsou generátory aritmetické využívající rekurentní vzorce. Jejich nevýhoda je ta, že získaná čísla nelze označit za zcela náhodná, jelikož jde o výpočet a nikoliv o náhodu. Vygenerovaná čísla označujeme jako čísla pseudonáhodná [36].

Nejznámějším generátorem pseudonáhodných čísel je lineární kongruenční generátor, který je zároveň jedním z nejstarších [36]. Tento generátor (i pseudonáhodné generátory obecně) potřebuje ke své práci úvodní vstupní data, která se následně doplní do výpočetního algoritmu a poté je provedeno samotné generování dle vztahu:

$$x_{n+1} = (ax_n + c) \bmod m; \quad n \geq 0$$

kde $0 <$ m modul
$2 \leq$ a $<$ m násobitel
$0 \leq$ c $<$ m inkrement
$0 \leq x_0 <$ m seed

Posloupnost pseudonáhodných čísel z intervalu $\langle 0,$ m$)$ je generována podle výše uvedeného rekurentního vzorce (smíšený lineární kongruenční generátor). Vydělením modulem m dostaneme výběr hodnot z rovnoměrného rozdělení na intervalu (0,1).

Vedle tohoto generátoru existují např. multiplikativní kongruenční generátor či aditivní lineární kongruenční generátor [25].

Parametry je nutné vhodně zvolit, aby perioda generátoru byla dostatečně veliká, ale výpočet netrval příliš dlouho.

Generování náhodných nezávislých čísel s požadovaným statistickým rozdělením probíhá ve dvou krocích:

– Primární generátor vygeneruje posloupnost náhodných čísel s rovnoměrným rozdělením v intervalu (0,1): U(0,1)

– Z této posloupnosti vhodnou transformací vytvoříme posloupnost čísel s požadovaným rozdělením a parametry. Rozložení U(0,1) je možno použít ke generování náhodných čísel z libovolného rozložení použitím inverzní distribuční funkce tohoto rozložení [21].

Generátor musí mít dostatečně dlouhou periodu (posloupnost generovaných hodnot se nesmí opakovat). Vygenerovaná posloupnost by se měla co nejvíce přibližovat posloupnosti náhodných čísel a generování by mělo být dostatečně rychlé [15].

1.7 Výhody a nevýhody simulace

Často bývá metoda simulace přeceňována a očekává se, že poskytne řešení na všechno. Je to ale pouze možná alternativa. Stručně lze popsat aplikaci simulace do čtyř bodů [12]:

– Systém je velmi složitý a nelze jej pochopit statickým zkoumáním. Je zapotřebí sledovat dynamiku modelu.
– Nutnost vylepšení stávajícího systému.
– Testování nových myšlenek a nápadů.
– Získávání nových znalostí bez zasahování do reálného systému.

Mezi největší výhody použití simulace je cena. Experimenty s reálným systémem jsou mnohdy finančně náročné (nákup síťových prvků atp.). Dalším benefitem simulace je možnost manipulace s časem. Některé reálné procesy trvají velmi dlouho dobu, což ztěžuje jejich zkoumání. Díky simulaci lze např. rok vnímat jako minutu a zároveň lze manipulovat rychlostí simulárního času [12]. Simulační nástroje též mnohdy poskytují vizualizační prostředky, které umožňují ještě lepší chápání chování systému a popřípadě i zachytávání chyb či nedostatků. Na druhou stranu je často velmi složité navrhnout a vytvořit model složitého systému. Důležitým aspektem je také správné modelování (generování) vstupních dat. Důsledkem experimentů složitějších modelů je vysoká výpočetní náročnost [26].

V případě dostupnosti analytického postupu je jeho použití vhodnější než metoda simulace. Jeho výsledkem je přesná hodnota a mnohdy je výpočetně méně složitý než simulace. Pokud však systém zahrnuje prvky náhodnosti a reflektuje průběh času, je vhodnějším kandidátem simulace [14].

2 Simulátory a emulátory

Simulátor z definice simulace pouze napodobuje funkčnost reálného systému. V praxi se simulátory využívají k získávání nových poznatků o reálných systémech, které modelují. Ne vždy však simulátor pokrývá veškeré funkční prvky reálného systému. Tato vlastnost může mít celou řadu příčin například: systém je příliš složitý a využívá se zjednodušení nebo pro potřeby zkoumání jsou některé funkce reálného systému nezajímavé.

Jiná situace nastává, pokud reálný systém dokonale známe, ale nemáme ho k dispozici. Jeho funkce však potřebujeme a musíme je realizovat prostředky, které k dispozici máme. V tomto případě se uplatní technika zvaná emulace. Emulátor transformuje instrukce systému tak, aby mohl fungovat i na jiných prostředcích, než pro které byl původně určen. Typickým příkladem je emulace her na počítačích, které jsou však určené pro herní konzole.

Rozdíl mezi simulací a emulací je především v tom, k čemu slouží - simulace k získání nových poznatků o určitém systému, zatímco emulace umožňuje jeho provoz na jiných prostředcích, než pro které byl původně určen.

V této kapitole budou popsány čtyři simulátory a emulátory síťového prostředí, jejich výhody a nevýhody a na konci kapitoly je uvedeno shrnutí zaměřené na vhodnost použití v praxi a také možnosti propojení s fyzickou infrastrukturou či jinou externí sítí.

Těmito simulátory respektive emulátory jsou:

- Cisco Packet Tracer
- Cisco Virtual Internet Routing Lab (VIRL)
- Huawei enterprise Network Simulator Platform (eNSP)
- Graphical Network Simulator-3 (GNS3)

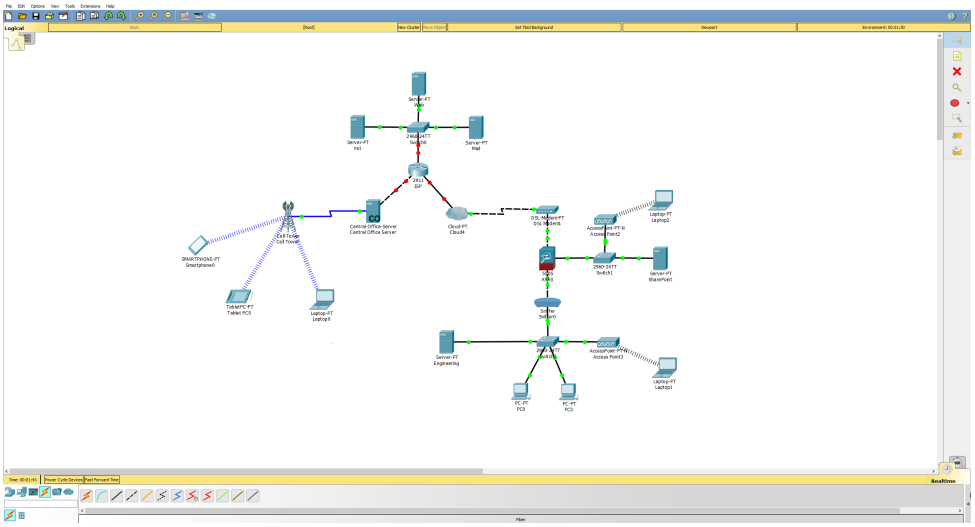
2.1 Cisco Packet Tracer

Simulátor Packet Tracer od společnosti Cisco je jeden z nejznámějších simulátorů datových sítí. Byl vyvinut v rámci vzdělávacího programu Cisco Networking Academy, který je známý po celém světě a jeho prostřednictvím probíhá vzdělávání především v oblasti počítačových sítí a informační bezpečnosti. Je navržen tak, aby nenáročnou a zároveň profesionální formou podporoval vzdělání a zvýšil interakci mezi studenty a instruktory.

Poskytuje velice podrobnou simulaci datových sítí s velikou škálou zařízení a nastavení doprovázené intuitivní grafickou reprezentací. Základní konfiguraci zařízení jako je konfigurace IP adres, pojmenování zařízení, zapnutí rozhraní atd. lze provést i v grafickém režimu. Pro pokročilejší konfiguraci je k dispozici rozhraní příkazového řádku. Díky celé škále zařízení, které lze v programu simulovat, můžeme testovat výstavbu bezdrátové sítě včetně připojení IoT zařízení. Podporován je také hardwarový firewall Cisco ASA 5505. V simulačním režimu umožňuje odchytávání a zobrazování obsahu paketů vybraných komunikačních protokolů (ICMP, ARP, DHCP, DNS apod.), ale ne na takové úrovni, jako třeba analyzátor síťového provozu WireShark. Software umožňuje návrh fyzického rozmístění zařízení v rackové skříni, místnosti, budovy, města (příklad rozmístění fyzický zařízení v rackové skříni je na obr. 2.2) a také možnost nahrání vlastního pozadí (např. plán datového centra).

Jedna z velikých nevýhod simulátoru je provázanost se vzdělávacím programem Networking Academy a tudíž je zajištěna funkčnost pouze těch konfigurací, které jsou v akademii vyučovány. V praxi tedy často můžeme narazit na situaci, kdy nám simulátor oznámí, že konfigurační příkaz není podporován i když ve fyzickém zařízení podporován je (např. jednosměrná autentizace protokolem CHAP). Jakékoliv propojení s fyzickou sítí též není podporováno.

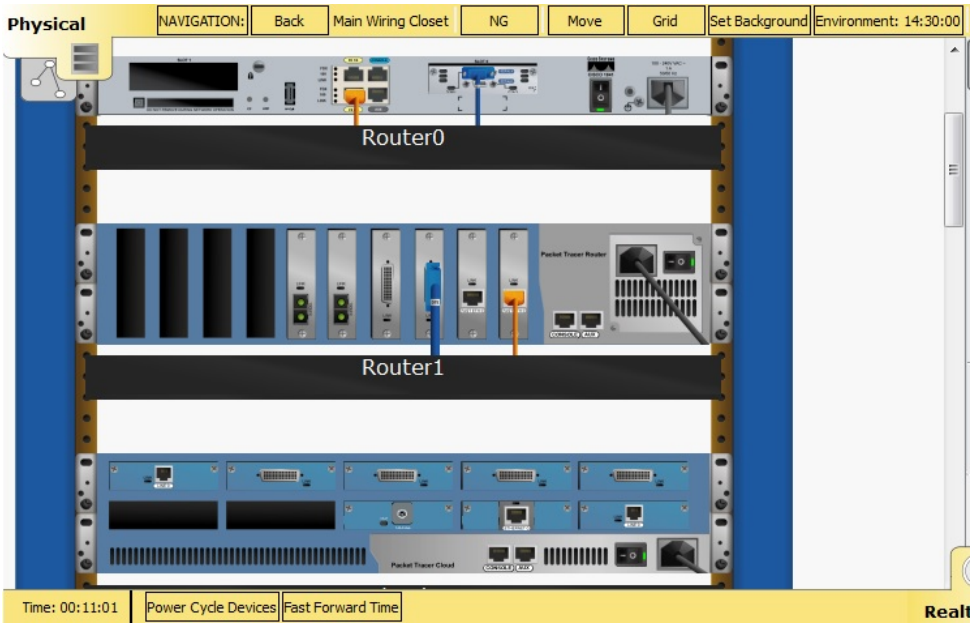
Packet Tracer je k dispozici zdarma všem studentům, instruktorům a absolventům programu Cisco Networking Academy. Lze se zdarma zaregistrovat do vzdělávacího kurzu Introduction to



Obr. 2.1: Grafické prostředí simulátoru Cisco Packet Tracer

Packet Tracer a tím získat k softwaru přístup. Po instalaci je vyžadováno přihlášení pomocí uživatelského jména a hesla do akademie. Bez přihlášení software umožní maximálně 10x uložit konfigurovanou topologii.

Díky své rozšiřitelnosti existuje pro tento simulátor mnoho předpřipravených laboratorních úloh, návodů a videí. Packet Tracer je multiplatformní software. Podporovány jsou systémy Microsoft Windows 7, 8.1, 10 a Linux Ubuntu 14.04. Dále existují verze pro mobilní zařízení na bázi iOS i Android.



Obr. 2.2: Návrh rozmístění fyzických zařízení v rackové skříni [6]

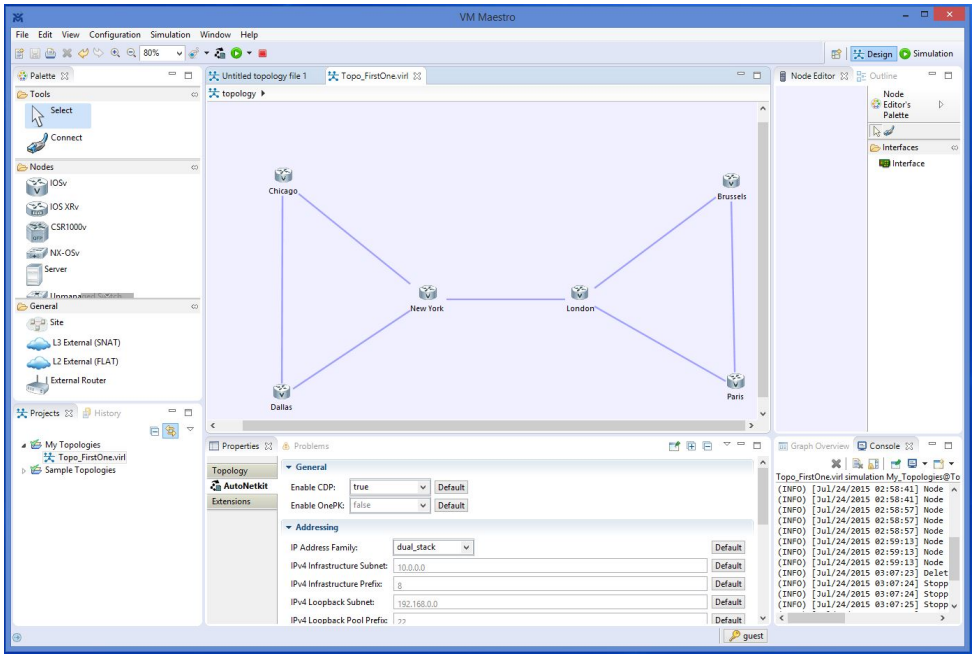
2.2 Cisco VIRL

Cisco VIRL (Cisco Virtual Internet Routing Lab) je další simulační nástroj z dílny společnosti Cisco. Packet Tracer byl cílen především na studenty vzdělávacího programu Cisco Networking Academy, VIRL je určen pro skutečné profesionály v oboru. Síťové prvky nejsou simulovány, ale emulovány. Tento nástroj je založen na bázi OpenStack platformy, což je virtualizační platforma určená pro provoz cloudů. Nechybí podpora připojení externí sítě. Nástroj je distribuován buď jako připravený obraz virtuálního počítače s operačním systémem Linux Ubuntu pro hypervisory od společnosti VMWare (ESXi, Workstation, Player a Fusion) nebo jako obraz ISO, který lze nainstalovat na jakýkoliv hardware splňující požadavky pro provoz. Obrazy virtuálních počítačů nejsou kompatibilní s VirtualBoxem.

Součástí simulátoru jsou i řádně licencované operační systémy IOS, které jsou přizpůsobené pro běh ve virtuálním prostředí. Nemusíme si je tedy obstarávat jako v případě simulační platformy GNS3. Další výhodou oproti této platformě je fakt, že VIRL umožňuje emulovat i L2 přepínače. Pro běh virtuálních síťových prvků jsou využívány hypervisory KVM a QEMU. K dispozici je emulace celé řady zařízení včetně série Nexus, určené pro datová centra [34], [10].

VIRL je pouze server. Abychom jej mohli využívat, je zapotřebí instalace grafického nástroje VM Maestro (obr. 2.3). Tento software slouží ke konfiguraci a návrhu topologií. Topologie je reprezentována XML souborem.

Simulační nástroj je vyvíjen primárně společností Cisco, ale je podporován i komunitou, která pořádá webináře či publikuje články kolem dění okolo této platformy. Na adrese https://learningnetwork.cisco.com/groups/virl lze najít plno užitečných materiálů či řešení problémů. Tento simulátor je v rámci mé práce jediný, který je placený.

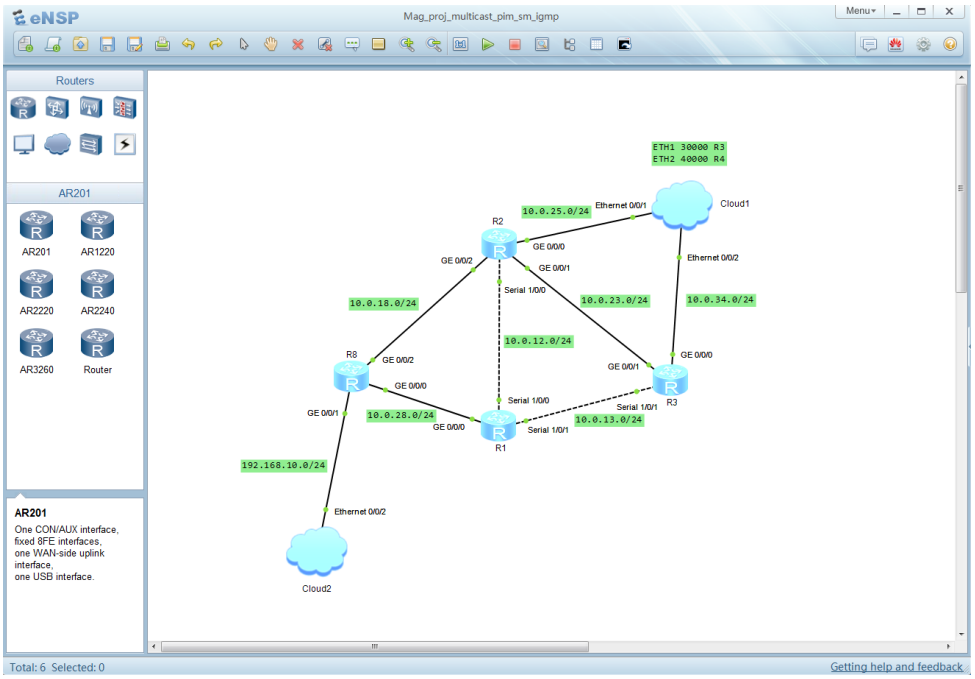


Obr. 2.3: Grafické prostředí nástroje VM Maestro [4]

2.3 eNSP

eNSP neboli Enterprise Network Simulation Platform je emulační nástroj od společnosti Huawei Technologies Co. Ltd. Společnost se především zabývala vývojem technologií pro mobilní komunikace, nicméně v posledních letech výrazně stoupá produkce směrovačů a ethernetových

přepínačů Huawei na úkor společnosti Cisco Systems, Inc. Tento růst zejména způsobuje poměr cena/výkon který je výrazně příznivější, než u produktů společnosti Cisco. Ta i nadále zůstává světovou jedničkou na poli směrovačů a ethernetových přepínačů. V závislosti na tomto faktu bylo třeba vyvinout simulační nástroj, ve kterém by si síťoví odborníci mohli testovat konfiguraci sítě na bázi Huawei prvků.



Obr. 2.4: Grafické prostředí simulátoru Huawei eNSP

V roce 2012 byl představen simulátor eNSP. Pro jeho získání je třeba registrace na webových stránkách Huawei. Po stažení není software nijak omezován. Aktivní síťové prvky nejsou simulovány, ale emulovány a tím je zajištěna ještě větší míra podobnosti chování oproti fyzickým prvkům, než je tomu u simulací. Jako hypervisor je využíván software VirtualBox od společnosti Oracle, který je zdarma dostupný bez jakékoliv registrace a hojně využívaný k testování. Pokud požadujeme propojení s fyzickou sítí nebo s jiným simulátorem např. GNS3, je k dispozici nástroj Cloud, který nám propojení umožní. Díky tomuto nástroji můžeme do simulované topologie připojovat také virtuální počítače a napodobit tak reálnou topologii, která se neskládá pouze z aktivních síťových prvků, ale také například z virtuálních serverů. K dispozici máte šest typů směrovačů od jednoúčelových s pevně danou konfigurací až po složitější víceúčelové, které lze pomocí modulů poskládat dle potřeby. Dále nám simulátor nabízí 3 typy ethernetových přepínačů, firewally, přístupové body a koncová zařízení. V eNSP je na rozdíl od Packet Traceru v grafickém režimu podporováno pouze přidávání a odebírání modulů. Veškerou konfiguraci je tedy nutné provádět v příkazovém řádku. Konfigurační příkazy jsou velmi obdobné, jako je tomu u síťových prvků společnosti Cisco. Síťovým inženýrům díky této vlastnosti nepůsobí veliké problémy přejít od výrobce Cisco k Huawei.

Společně se samotným simulačním softwarem se nainstaluje i celá řada ukázkových topologií včetně kvalitní dokumentace, kde lze nalézt veškeré podrobnosti k ovládání a funkcím.

Tento emulační nástroj je vydáván pouze pro operační systém Microsoft Windows. Ačkoliv je v dokumentaci uvedeno, že je podporována i verze Windows 10, po instalaci se setkáte s problémem, že emulované síťové prvky nejdou spustit.

Je to dáno verzí VirtualBoxu. Problém se děje, když je VirtualBox instalován společně s emulátorem i když VirtualBox instalujete samostatně. Pro spolehlivý chod bude eNSP rámci této práce provozován na operačním systému Microsoft Windows 7 viz kapitola Výukové pracoviště

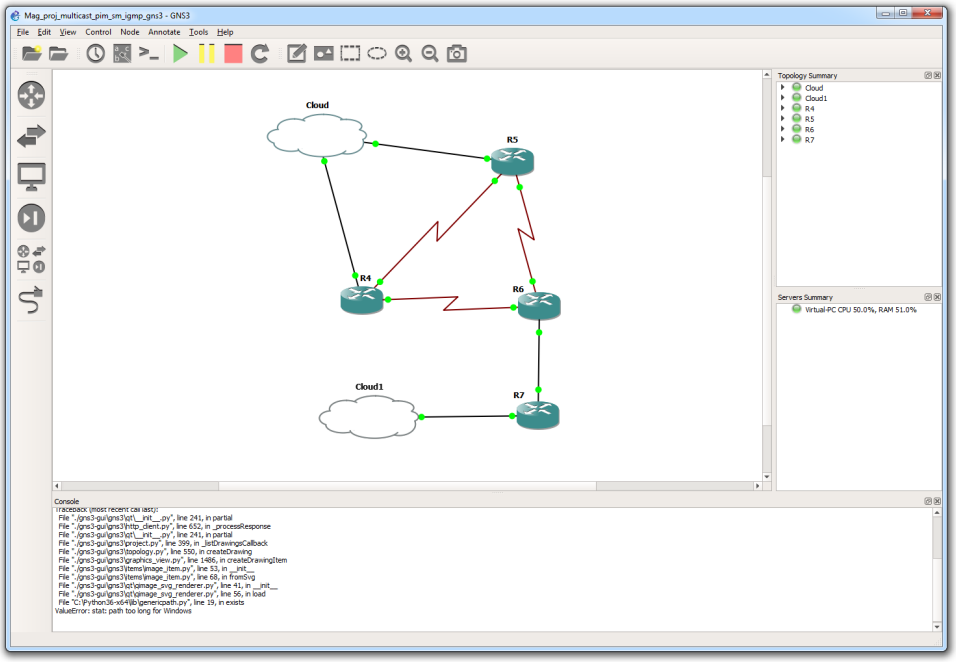
2.4 GNS3

Simulátor GNS3 (Graphic Network Simulator) na rozdíl od výše zmíněných simulátorů nevyvíjí technologická společnost, ale komunita. Z tohoto faktu plynou nesporné výhody, zejména ta, že nejsou podporována zařízení pouze od jednoho výrobce. Emulovány mohou být směrovače, bezpečnostní brány a další zařízení. Problém je ovšem s emulací přepínačů a jak ho řešit je nastíněno v další části této práce. Základem emulačního nástroje je několik emulátorů (Dynamips a další). Díky tomu, že síťové prvky nejsou simulovány, ale emulovány, je jejich chování velmi podobné fyzickým zařízením.

GNS3 funguje na principu klient-server. Serverovou část lze provozovat na jiném počítači, než klientskou. Tato funkce je vhodná ve chvíli, kdy počítač nedisponuje dostatečnou hardwarovou výbavou a také v případě, že na topologii (projektu) pracuje více lidí a je potřeba jí mezi nimi sdílet.

Nástroj je velice využívaný pro studijní účely a přípravu k Cisco certifikacím, jako je např. CCNA či CCNP. Používají jej také odborníci v oblasti síťových technologií k testování provozu a chování sítí (např. při kybernetickém útoku), jelikož jeho velkou předností je možnost propojení simulované sítě se sítí reálnou přes síťové rozhraní hostitelského počítače. Další velkou předností je možnost připojení virtualizovaného počítače ve VirtualBoxu nebo VMWaru přímo k simulované síti.

Emulátor je po registraci na webu k dispozici zdarma pro celou řadu platforem [2]. Na webu též nalezneme velmi obsáhnou dokumentaci. GNS3 je open-source projekt.



Obr. 2.5: Prostředí simulátoru GNS3

2.4.1 Dynamips

Dynamips je nástroj pro emulaci operačního systému IOS od společnosti Cisco. Jeho hlavní funkcí je přeložit instrukce IOS, které jsou určené pro procesory MIPS (Microprocessor without Interlocked Pipeline Stages) na instrukce, které jsou schopné zpracovat dnes běžné procesory od společnosti Intel či AMD [27].

Emulátor je kompatibilní s operačními systémy Windows, Linux i MacOS. Jako úplně první byl emulován směrovač Cisco 7200.

Ačkoliv Dynamips umožňuje emulovat směrovače, neumožňuje emulovat přepínače. Je to dáno velikou náročností emulace obvodů ASIC (Application Specific Integrated Circuit), což jsou obvody určené pro specifické aplikace, které přepínače využívají ke zrychlení přepínání rámců.

Pokud potřebujeme v topologii využívat přepínač, máme několik možností, jak tuto situaci vyřešit. Použít základní přepínač, který je součástí instalace GNS3. Umožňuje omezené nastavení, ale podporuje i virtuální sítě. Další možností je osadit směrovač modulem EtherSwitch a takto modifikovaný směrovač používat jako přepínač. Ale ani toto řešení nenahradí plnohodnotný přepínač. Seznam omezení lze nalézt na webových stránkách GNS3. Poslední možností je použití jiného simulačního prostředí [35].

Emulátor podporuje pouze vybrané řady směrovačů Cisco: 1700, 2610, 2620, 2691, 3620, 3640, 3660, 3725, 3745 a 7206. Pouze typ 7206 má podporu IOS verze 15, všechny ostatní typy podporují maximálně verzi 12.4. Dynamips nepodporuje příkaz Reload. Pro restart směrovače je třeba zvolit z rozevíracího menu zařízení položku Reload viz obr. 3.3.

GNS3 využívá vedle tohoto emulátoru ještě další, jejich shrnutí je uvedeno v tabulce 2.1.

Emulátor	**Emulovaná zařízení**
Qemu	Cisco ASA, Juniper, Linuxové stanice, apliance na bázi IOS, IOU
Pemu	Cisco PIX firewall
VirtualBox	Windows a Linux stanice, Juniper

Tab. 2.1: Další emulátory podporované v GNS3 [35]

2.4.2 Idle-PC

Emulátor Dynamips nedokáže určit, kdy směrovač vykonává efektivní činnost (čte záhlaví paketu apod.) nebo pouze čeká na určitou akci (výpis do konzoly, přepočet směrovací tabulky atd.) - je v tzv. režimu nečinné smyčky. Důsledkem toho emulátor posílá hostitelskému procesoru i instrukce, které jednoduše znamenají, aby vyčkával a tím způsobují vyšší využití procesoru, než je skutečně nutné. Této nepříznivé situaci by měl zabránit výpočet hodnoty Idle-PC a následné použití.

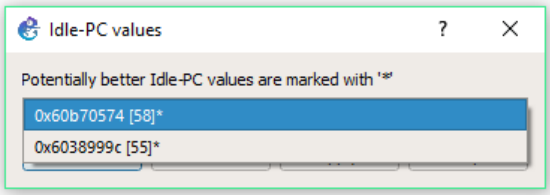
Výpočet hodnoty Idle-PC spočívá v tom, že se provede analýza na spuštěném směrovači a určí se nejpravděpodobnější body v kódu, které reprezentují nečinnou smyčku v rámci instrukcí operačního systému IOS.

Hodnota Idle-PC se váže na konkrétní IOS a je reprezentována hexadecimálně. Bude se lišit pro rozdílné verze IOS obrazů a to i pokud se bude jednat o totožnou verzi s rozdílným balíkem funkcí.

Může nastat případ, kdy hodnota Idle-PC není nalezena. Avšak při opětovném spuštění analýzy se vypočítají správné hodnoty. Novou analýzu lze spustit kliknutím pravým tlačítkem myši na směrovač a zvolením Idle-PC nebo Auto Idle-PC. Varianta Idle-PC vygeneruje několik hodnot, přičemž u některých se bude nacházet znak hvězdičky. Takto označené hodnoty poukazují

na potenciálně nejlepší nalezené výsledky. Auto Idle-PC vygeneruje pouze jednu hodnotu a tato hodnota se automaticky použije pro všechny virtuální směrovače s danou verzí IOS (tato varianta je použita při automatickém nastavení Idle-PC při importu binárního obrazu operačního systému IOS).

Po výpočtu a nastavení hodnoty (probíhá při importu binárního obrazu IOS nebo lze nastavit později) emulátor příležitostně uspává virtuální směrovač ve chvíli, kdy se nachází v režimu nečinné smyčky, což snižuje využití hostitelského procesoru, aniž by se snížil výkon virtuálního směrovače [35].



Obr. 2.6: Příklad vypočtených hodnot Idle-PC

2.4.3 Cloud

Nástroj Cloud poskytuje v GNS3 stejnou funkci, jako je tomu v případě simulátoru eNSP, tedy připojení simulované sítě do jiné ať už fyzické či také simulované. V níže zmíněných laboratorních úlohách bude využito jak propojení s fyzickou sítí (fyzickým směrovačem) tak propojení s další simulovanou sítí.

Pro testování konfigurace a chování sítě je propojení emulátoru s jinou sítí velmi výhodné. Umožňuje analyzovat chování původní sítě a k ní připojené simulované sítě bez toho, aniž bychom museli pořizovat další často drahé aktivní síťové prvky na testování. Emulace síťových prvků se totiž velmi blíží chování fyzických zařízení.

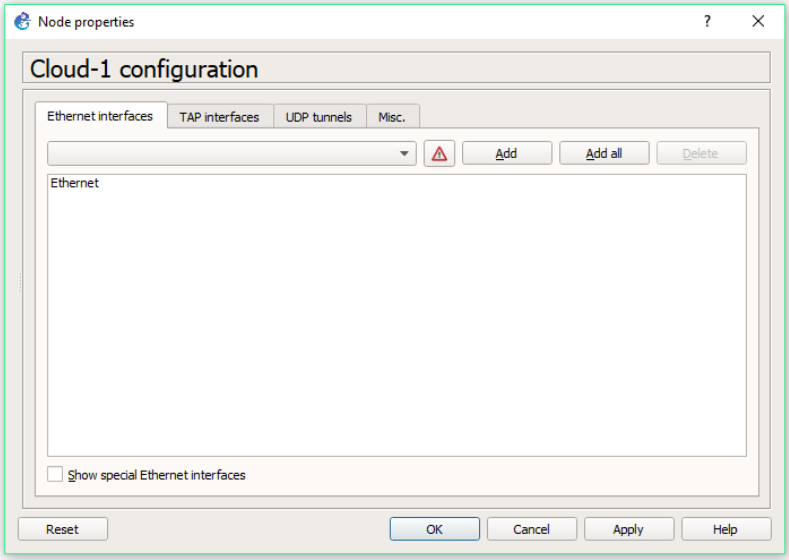
Na obr. 2.7 je konfigurační okno nástroje Cloud. Vidíme, že simulovanou síť můžeme propojit s jinou sítí několika způsoby. Pokud je požadováno propojení s fyzickou sítí (např. internet nebo LAN), využijeme k tomu fyzické adaptéry hostitelského počítače (Ethernet interfaces). Dále máme k dispozici připojení přes TAP rozhraní (TAP interfaces), což jsou pouze virtuální rozhraní, které spravuje jádro operačního systému a UDP tunely (UDP Tunnels), které jsou využívány v úlohách Lab 3 - Multicast, PIM Sparse mode a Lab 2 - Multicast, PIM Dense mode k propojení s emulátorem eNSP.

Pomocí UDP tunelů lze propojit i virtuální sítě, které se nacházejí na odlišných hostitelích. Tato funkce byla vyzkoušena propojením dvou simulovaných sítí realizovaných na odlišných hostitelských počítačích, které byly připojeny do stejné LAN sítě s využitím VPN.

V poslední záložce různé (Misc.) můžeme měnit jméno konkrétní instance nástroje Cloud. V simulované topologii můžeme mít i více instancí toho nástroje. Ne nutně musíme propojovat pouze sítě, ale díky tomuto nástroji můžeme do topologie připojit i virtuální počítače.

2.4.4 Platformy

Jak již bylo zmíněno výše, GNS3 je multiplatformní software. Jsou podporovány operační systémy Windows, Linux i mac OS X. Software lze stáhnout jako instalační soubor nebo jako obraz virtuálního počítače s již připravenou a plně funkční instalací. Obraz je připravený pro VirtualBox, VMWare Workstation či VMWare ESXi.



Obr. 2.7: Konfigurace nástroje Cloud

Emulátor zdaleka neumožňuje emulovat pouze aktivní síťové prvky Cisco. Podporuje například i zařízení Juniper, MikroTik, či méně známý Sophos. Velikou výhodou je podpora tzv. apliancí. Apliance je předpřipravený obraz operačního systému. Z webových stránek stačí stáhnout aplianci, kterou potřebujeme a importovat do GNS3. Pro využívání apliancí je nutné mít stažen připravený virtuální počítač s GNS3, jinak nepůjde apliance importovat. K dispozici nejsou pouze aktivní síťové prvky, ale i standardní operační systémy jako Microsoft Windows či Linux Ubuntu [2].

2.5 Porovnání

Každý z výše uvedených simulátorů, respektive emulátorů, má své klady i zápory. V této podkapitole je uvedeno shrnutí vlastností jednotlivých nástrojů, především se zaměřením na možnost propojení s externí sítí a také využití v praxi.

Simulátor Packet Tracer vyniká svou jednoduchostí. Je vázán na vzdělávací program Cisco Networking Academy a také dostupný pouze jeho studentům, lektorům či absolventům. Jako doplňkový vzdělávací nástroj k tomuto programu je dostačující. Zaručeně v něm totiž fungují pouze konfigurační příkazy, o kterých je zmínka ve vzdělávacím programu. Pokud se jedná například o konfiguraci jednosměrné autentizace protokolem CHAP, směrovač vypíše chybu o nepodporovaném příkazu, ačkoliv ve fyzickém směrovači tento příkaz podporovaný je. Simulátor je vyvíjen společností Cisco a jsou tedy podporována pouze zařízení od tohoto výrobce s tím, že nabídka použitelných zařízení je pevně definována a další zařízení přidat nelze. Zařízení jsou pouze simulována, nikoliv emulována. Jakékoliv propojení s fyzickou sítí není podporováno.

Packet Tracer není vhodný pro plánování a testování sítí, které mají být nasazeny do reálného provozu, naopak pro studium a pochopení fungování datových sítí je dostačující a hojně využíván.

Cisco VIRL není na rozdíl od Packet Traceru pouze software. Je to celá platforma pracující na principu klient-server. Jako klient je využíván grafický nástroj VM Maestro umožňující návrh, stavbu a konfiguraci topologie. Součástí platformy jsou licencované aktuální obrazy IOS upravené pro běh ve virtuálním prostření [34]. Nechybí možnost propojení do jiné sítě mimo platformu či integrace s jinými zařízeními jako jsou virtuální počítače či zařízení jiných výrobců např. Juniper, Fortinet, Arista, Alcatel, Citrix a další. Topologie jsou ukládány ve formě XML souborů

a umožňují snadný export. VIRL je placený nástroj. Pro osobní použití je v současnosti cena 199 dolarů za rok s omezením na 20 uzlů v topologii [1].

V dnešní době je tato virtualizační platforma to nejlepší, co lze pro simulaci datových sítí na bázi Cisco síťových prvků získat.

Emulační nástroj eNSP je značně pokročilejším nástrojem, než Packet Tracer. Ke své funkci potřebuje hypervisor VirtualBox, ve kterém jsou vytvářeny virtuální aktivní síťové prvky. Zařízení jsou v tomto nástroji emulována. Díky tomu poskytují věrnější chování, než u simulovaných prvků. Volitelným sofwarem je WireShark - analyzátor síťového provozu, kterým lze analyzovat probíhající komunikaci mezi jednotlivými zařízeními. eNSP je vyvíjen společností Huawei. Obdobně jako v případě Packet Traceru máme předem definovaná zařízení, která lze používat. Emulátor disponuje nástrojem Cloud. Tento nástroj poskytuje propojení s vnější sítí. Vnější síť může být fyzická síť, jiná simulovaná síť či pouhé propojení s virtuální počítačem. Příklad využití nástroje Cloud k propojení s jinou simulovanou sítí a připojení virtuálního počítače je demonstrován v úloze Lab 3 - Multicast, PIM Sparse mode.

eNSP je vhodný pro analýzu a testování chování síťových topologií založených na aktivních síťových prvcích Huawei. Nechybí však propojení s dalšími sítěmi realizovanými mimo simulátor. Existuje tedy možnost testovat i sítě, které jsou složeny ze zařízení více výrobců.

Čtvrtým simulačním nástrojem zmíněným v této práci je GNS3. Od předchozích se liší v jedné zásadní věci. Není vyvíjený žádnou technologickou společností, ale komunitou. Díky tomu nejsou v softwaru předem definována zařízení, která lze v simulovaných topologiích použít. Po instalaci je k dispozici pouze pár aktivních prvků, ale žádný není směrovač. K tomu, abychom mohli využívat v topologii směrovače, musíme disponovat operačním systémem IOS nebo stáhnout připravenou aplianci z webu. Apliance vyžaduje instalaci do předpřipraveného obrazu virtuálního počítače. Tento obraz je rovněž dostupný ke stažení na webu [2]. K dispozici je celá řada apliancí, nejen pro zařízení od společnosti Cisco, ale i Juniper, Sophos či Fotinet a další [3]. Simulátor disponuje nástrojem Cloud, který pracuje shodně jako v případě simulátoru eNSP. Podporuje několik hypervisorů, které jsou využívány dle konkrétního typu emulovaného zařízení. Na webových stránkách je k dispozici bohatá dokumentace.

GNS3 je velmi mocný nástroj k emulaci datových sítí. Je velmi hodně využíván jak ke studiu, tak k analýze a testování. Podporuje propojení s externími sítěmi či integraci analyzátoru WireShark.

V praktické části diplomové práce je využíván především tento emulátor. V úlohách Lab 3 - Multicast, PIM Sparse mode a Lab 2 - Multicast, PIM Dense mode je využito propojení s emulátorem eNSP [30].

	Cisco Packet Tracer	Cisco VIRL	Huawei eNSP	GNS3
Aktuální verze	7.1.1	1.5	1.2.00.510	2.1.4
Propojení s externí sítí	Ne	Ano	Ano	Ano
Přidání zařízení od jiných výrobců	Ne	Ano	Ne	Ano
Emulace zařízení	Ne	Ano	Ano	Ano
Propojení s VM přímo v simulátoru	Ne	Ano	Ne	Ano
Dostupnost	Zdarma[1)]	199$/rok[2)]	Zdarma[3)]	Zdarma[4)]
Dostupnost připraveného virt. počítače	Ne	Ano	Ne	Ano
Vyvíjen výrobcem zařízení	Ano	Ano	Ano	Ne
Vzorové topologie obsažené v instalaci	Ano	Ano	Ano	Ne
Multiplatformní nástroj	Ano	Ano	Ne	Ano

1) Zdarma pro studenty, instruktory a absolventy programu Cisco Networking Academy
2) Cena platí pro variantu Personal Edition s omezením na 20 uzlů v topologii [1]
3) Zdarma po registraci
4) Zdarma po registraci, je nutné disponovat operačními systémy pro síťové prvky

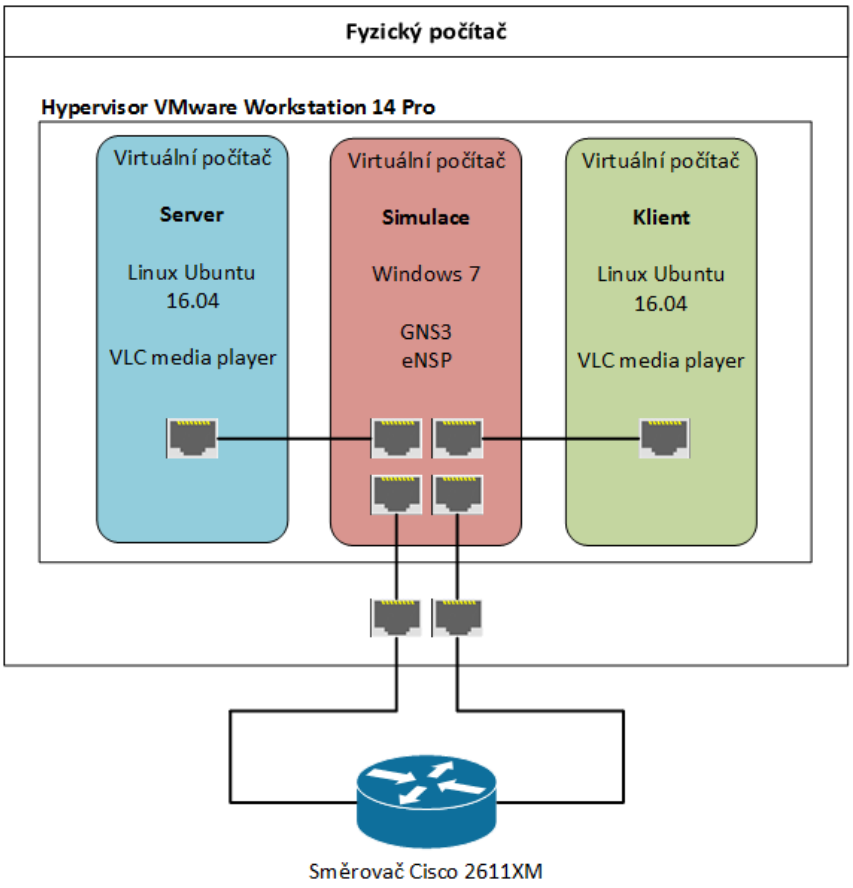
Tab. 2.2: Porovnání simulátorů

3 Výukové pracoviště

Výukové pracoviště je díky použití virtualizace velice variabilní a lze jej přizpůsobit konkrétním potřebám dané řešenou laboratorní úlohou. Nicméně je třeba dodržet několik zásad jak po hardwarové, tak softwarové stránce, aby simulační resp. emulační software fungoval správně [2], [5]:

- Simulace jsou realizovány v operačním systému Microsoft Windows 7 Professional. Je to dáno omezením softwaru eNSP, který na operačním systému Windows 10 běží s chybami, které zabraňují spuštění emulovaných síťových prvků.
- Pro spolehlivý chod emulátoru eNSP je hypervisor VirtualBox instalován společně s emulátorem (VirtualBox je součástí instalačního balíku), aby nedošlo k nekompatibilitě verzí.
- Software GNS3 i eNSP musejí být spuštěny jako správce. Pouze v režimu správce je zajištěn plný přístup k síťovým rozhraním.
- Z webových stránek softwaru GNS3 lze stáhnout již hotový virtuální počítač s předinstalovaným softwarem. Tato varianta použita není. Místo toho byl stažen pouze instalační soubor a nainstalován na námi vytvořený virtuální počítač.
- Jako fyzické zařízení je v laboratorních úlohách použit směrovač Cisco 2611XM, je možno použít jakýkoliv konfigurovatelný Cisco Router (např. 1841, 2801, 1941, 2911)
- Fyzický směrovač je konfigurován dodávaným konzolovým kabelem, ke kterému je připojen převodník Serial-USB, jelikož fyzický počítač nedisponuje sériovým portem.
- Síťové karty počítače musejí pracovat v promiskuitním režimu. Tento režim zajišťuje síťovému rozhraní přijímat i pakety, které nejsou určené přímo pro něj. Pokud by byl promiskuitní režim vypnutý, síťová karta by filtrovala provoz a k operačnímu systému by se dostaly pouze pakety, které jsou určené jen pro dané rozhraní a žádné jiné. V praxi by to například znamenalo, že by při dynamickém směrování nefungovala výměna směrovacích tabulek mezi směrovači ve fyzické a simulované síti, jelikož by probíhala filtrace paketů nesoucí tuto informaci a síťová karta by tyto pakety zahazovala.
- Každou z úloh lze modifikovat podle toho, kolik máme k dispozici fyzických zařízení. Od toho se také odvíjí požadavky na počet síťových rozhraní virtuálního počítače, přes které bude probíhat komunikace s fyzickými prvky v topologii a také počet ethernetových portů, kterými musí tyto prvky disponovat.
- Hardwarové požadavky na virtuální počítač ve kterém bude simulace realizována závisejí na počtu emulovaných síťových prvků. Laboratorní úlohy vytvořené v rámci této práce byly simulovány na virtuálním počítači s těmito parametry:
  - Operační systém: Windows 7 Professional 64-bit
  - Operační paměť: 6 GB
  - Kapacita pevného disku: 60 GB
  - Procesor: 4 jádra
  - Počet síťových rozhraní: 4 - v úloze Lab 3 - Multicast, PIM Sparse mode jsou dvě rozhraní použita k připojení serveru respektive klienta na testování streamování hudby. Další 2 rozhraní jsou použita v úloze Lab 1 - Typy oblastí ve směrovacím protokolu OSPF pro připojení fyzického směrovače.
- Parametry fyzického počítače jsou následující:
  - Operační systém: Windows 10 Pro 64-bit
  - Operační paměť: 16 GB
  - Kapacita pevného disku: 240 GB
  - Procesor: i7 8700, 12 jader, 3,2 GHz

  - Počet síťových rozhraní: 2 - rozhraní jsou použita v úloze Lab 1 - Typy oblastí ve směrovacím protokolu OSPF pro připojení fyzického směrovače.
- Jako hypervisor byl použit VMware Workstation 14 Pro, což je profesionální placený nástroj umožňující vytvářet virtuální počítače. Pro potřeby výuky je zcela dostačují i zdarma dostupný hypervisor VirtualBox.

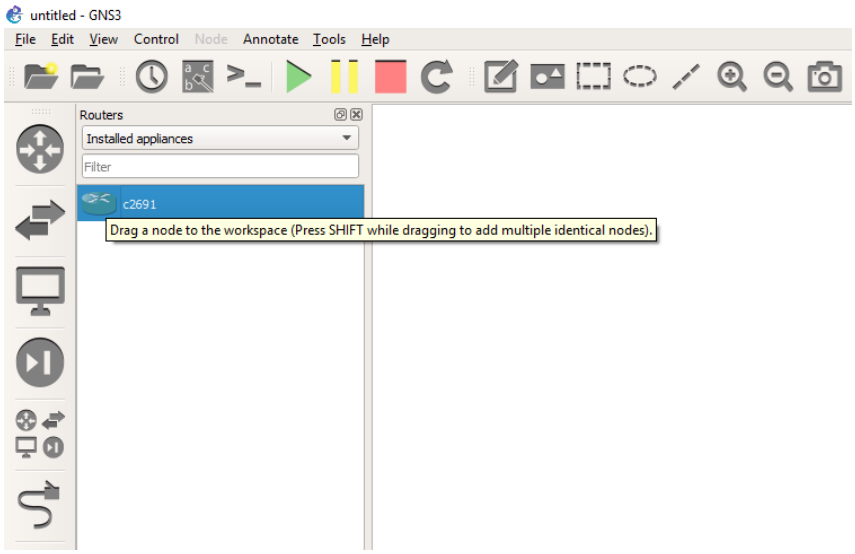


Obr. 3.1: Schéma výukového pracoviště

3.1 Práce v prostředí GNS3

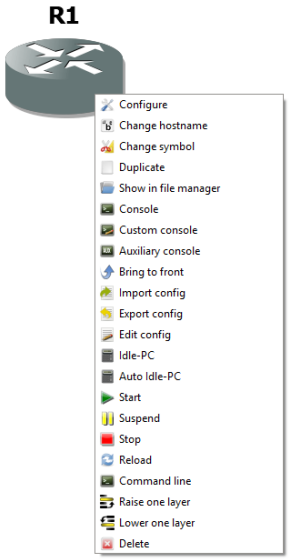
Práce v softwaru je velmi jednoduchá a intuitivní. Jak již bylo zmíněno výše, lze využít celou řadu předpřipravených apliancí. Pokud disponujeme binárním obrazem operačního systému Cisco IOS, lze ho přidat v horní liště kliknutím na položku Edit - Preferences - IOS routers. Při importu se automaticky nastaví typ zařízení, hardwarové parametry a můžeme přidat další rozšiřující rozhraní. Na stejném místě lze přidat virtuální počítače [19].

Pokud chceme do topologie přidat další zařízení, stačí vybrat kategorii v levém menu a po zobrazení nabídky zařízení ho přetáhnout na pracovní plochu. Postup je zobrazen na obr. 3.2



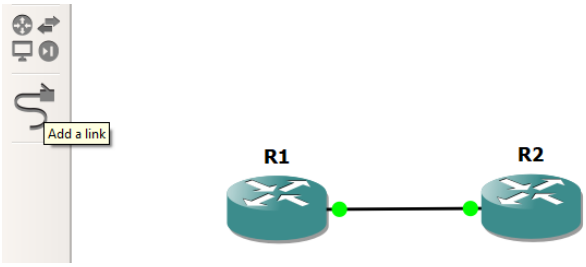
Obr. 3.2: Přidání zařízení do topologie

Po vložení směrovače na pracovní plochu, klikneme na zařízení pravým tlačítkem myši. Zobrazí se nabídka umožňující další práci se směrovačem (zapnutí, restart, import konfigurace a další). Celý výpis nalezneme na obr. 3.3. Stejná nabídka se také nachází v horní liště - položka Node.



Obr. 3.3: Konfigurace směrovače

Propojení zařízení s jiným probíhá tak, že zvolíme ikonu propojení obr. 3.4, klikneme na zařízení, zvolíme port a následně klikneme na druhé zařízení a také zvolíme port. Tím se nám zařízení propojí. Typ propojení se vybere automaticky na základě vybraných rozhraní.

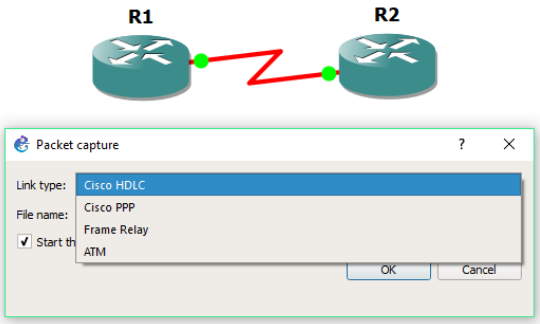


Obr. 3.4: Propojení zařízení

V základním nastavení software nezobrazuje popisky připojených rozhraní. V praxi nám však tyto popisky usnadňují orientaci v topologii. Zapínací tlačítko se nachází v horní liště a na obr. 3.5 je barevně vyznačeno.

Obr. 3.5: Zobrazení popisků připojených rozhraní

GNS3 umožňuje spolupráci s analyzátorem síťové komunikace Wireshark. Díky tomu můžeme zachytávat a analyzovat komunikaci mezi jednotlivými zařízeními. Stačí kliknout pravým tlačítkem myši na propojení a zvolit Start capture. Zobrazí se nám dialog pro výběr typu protokolu linkové vrstvy. U ethernetového spojení máme na výběr pouze Ethernet. U sériového spojení je na výběr Cisco PPP, Cisco HDLC, ATM a Frame Relay.



Obr. 3.6: Typy zapouzdření u sériové linky

Poklepáním na levé tlačítko myši na zařízení se otevře příkazový řádek (v případě směrovače) nebo nastavení v grafickém režimu (v případě základního přepínače).

4 Laboratorní úlohy

Jedním z cílů této práce byla tvorba podkladů pro laboratorní výuku. V této kapitole jsou vytvořeny tři laboratorní úlohy, které svou obtížností odpovídají úrovni Cisco Certificate Network Professional. V každé z nich je kladen důraz na využití propojení mezi simulovanou sítí v softwaru GNS3 s externí sítí. Jednotlivé úlohy obsahují zadání s topologií, rozbor a postup řešení. Témata jednotlivých úloh jsou:

- Typy oblastí ve směrovacím protokolu OSPF
- Multicast, PIM Dense mode
- Multicast, PIM Sparse mode

4.1 Lab 1 - Typy oblastí ve směrovacím protokolu OSPF

V rámci této úlohy budou konfigurovány různé typy koncových oblastí směrovacího protokolu OSPF a vysvětleny rozdíly mezi nimi.

4.1.1 Zadání a topologie

Zadání:

- V prostředí emulačního softwaru GNS3 a jednoho fyzického směrovače realizujte dynamické směrování protokolem OSPF a EIGRP.
- Uvažujte topologii dle obr. 4.1
- Část sítě, ve které pracuje protokol OSPF, rozdělte do několik oblastí.
- Nastavte redistribuci směrovacích informací mezi směrovacími protokoly.
- Nakonfigurujte jednotlivé typy koncových oblastí.
- Zaměřte se na vliv typu koncové oblasti na velikost a obsah směrovacích tabulek.

4.1.2 Rozbor úlohy

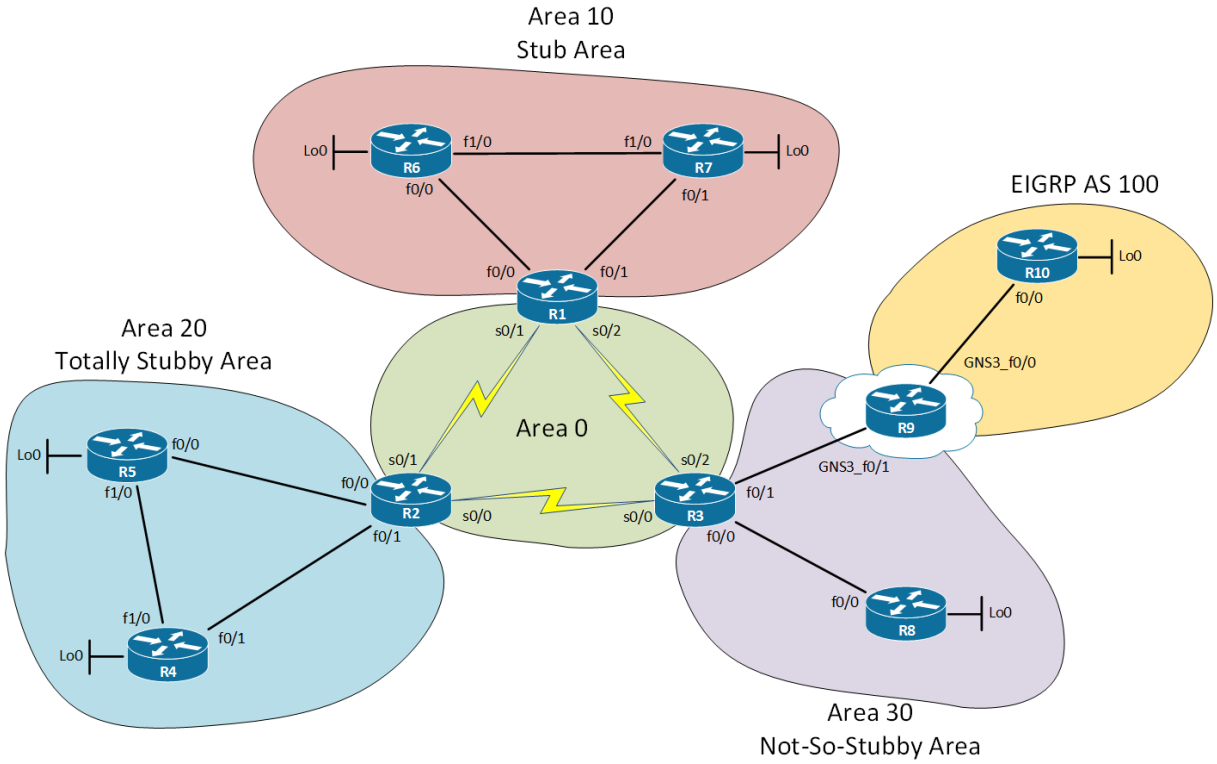
V této úloze budete konfigurovat devět virtuálních a jeden fyzický směrovač. Směrovače R1, R2 a R3 budou propojeny sériovým kabelem. R1 bude zdroj hodinového signálu pro spoje R1-R2 a R1-R3. R2 bude zdroj hodinového signálu pro R2-R3. R9 (Cisco 2611XM) bude připojen k R3 a R10 přes fyzická síťová rozhraní hostitelského počítače a dále pomocí nástroje Cloud připojeny do simulované sítě. Pro připojení R9 k fyzickým síťovým rozhraním hostitele využijte ethernetové porty FastEthernet 0/0 a FastEthernet 0/1 viz obr. 4.3

Jako emulovaná zařízení použijte devět směrovačů typu Cisco 2961. Na směrovačích R4, R5, R6, R7, R8, R10 bude nakonfigurováno virtuální rozhraní Loopback 0 pro další rozšíření topologie.

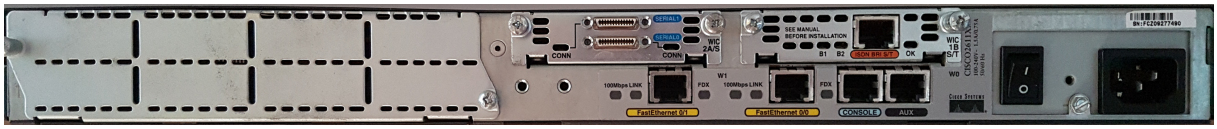
Směrovače budou v síti se směrovacím protokolem OSPF jednoznačně identifikovány parametrem router-id, který vychází z pojmenování směrovače, např. R1 - 1.1.1.1, R2 - 2.2.2.2, atp.

Pro přesnější porozumění jednotlivým typům koncových oblastí je nejprve zapotřebí definovat nejdůležitější typy LSA (Link-state advertisement), což jsou pakety nesoucí topologické informace (informace o stavu linky). Každý typ LSA popisuje jinou část topologie [31].

Typ 1 - Router (Směrovač) Každý směrovač vytvoří toto LSA sám pro sebe a rozešle (záplava). Popisuje směrovač, jeho rozhraní a seznam sousedních směrovačů na každém rozhraní (vše v jedné dané oblasti).



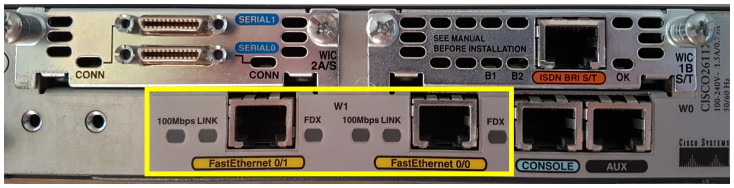
Obr. 4.1: Topologie laboratorní úlohy



Obr. 4.2: Směrovač Cisco 2611XM

Typ 2 - Network (Síť) Reprezentuje tranzitní podsíť, pro kterou byl zvolen DR (Designated Router). Pokud v podsíti nebyl zvolen DR, toto LSA se nevytváří.

Typ 3 - Net Summary (Souhrn sítě) Hraniční směrovače oblastí (ABR) nezasílají z jedné oblasti do druhé LSA typu 1 a 2, ale místo toho zasílají LSA typu 3. LSA typu 3 reprezentují podsítě první oblasti popsané LSA typu 1 a 2 a jedná se o vektor s údaji o podsíti, masce a ceně, se kterou ABR danou podsíť dosáhne.



Obr. 4.3: Použité porty na směrovači Cisco 2611XM

Zařízení	Rozhraní	IP adresa	Adresa podsítě	Oblast	DCE/DTE
R1	f0/0	172.16.1.17	172.16.1.16 /30	10	-
	f0/1	172.16.1.13	172.16.1.12 /30	10	-
	s0/1	192.168.1.1	192.168.1.0 /30	0	DCE
	s0/2	192.168.1.5	192.168.1.4 /30	0	DCE
R2	f0/0	172.16.1.1	172.16.1.0 /30	20	-
	f0/1	172.16.1.5	172.16.1.4 /30	20	-
	s0/0	192.168.1.9	192.168.1.8 /30	0	DCE
	s0/1	192.168.1.2	192.168.1.0 /30	0	DTE
R3	f0/0	172.16.1.29	172.16.1.28 /30	30	-
	f0/1	172.16.1.25	172.16.1.24 /30	30	-
	s0/0	192.168.1.10	192.168.1.8 /30	0	DTE
	s0/2	192.168.1.6	192.168.1.4 /30	0	DTE
R4	f0/1	172.16.1.6	172.16.1.4 /30	20	-
	f1/0	172.16.1.9	172.16.1.8 /30	20	-
	Lo0	172.16.1.33	172.16.1.33 /32	20	-
R5	f0/0	172.16.1.2	172.16.1.0 /30	20	-
	f1/0	172.16.1.10	172.16.1.8 /30	20	-
	Lo0	172.16.1.37	172.16.1.37 /32	20	-
R6	f0/0	172.16.1.18	172.16.1.16 /30	10	-
	f1/0	172.16.1.21	172.16.1.20 /30	10	-
	Lo0	172.16.1.41	172.16.1.41 /32	10	-
R7	f0/1	172.16.1.14	172.16.1.12 /30	10	-
	f1/0	172.16.1.22	172.16.1.20 /30	10	-
	Lo0	172.16.1.45	172.16.1.45 /32	10	-
R8	f0/0	172.16.1.30	172.16.1.28 /30	30	-
	Lo0	172.16.1.49	172.16.1.49 /32	30	-
R9	f0/0	10.11.12.1	10.11.12.0 /30	-	-
	f0/1	172.16.1.26	172.16.1.24 /30	30	-
R10	f0/0	10.11.12.2	10.11.12.0 /30	-	-
	Lo0	10.11.12.5	10.11.12.4 /32	-	-

Tab. 4.1: Tabulka IP adres

Typ 4 - ASBR Summary (Souhrn hraničního směrovače autonomního systému) ASBR vytvoří LSA typu 5 při zanášení externí cesty typu E1 (uvažuje jak externí tak interní metriku) a plošně je rozešle. Jakmile se LSA typu 5 dostane do hraničního směrovače oblasti ABR, který je má rozeslat do své oblasti, vytvoří LSA typu 4, jejíž součástí je i metrika, podle níž ABR dosáhne ASBR, který původní LSA typu 5 vytvořil.

Typ 5 - AS External (Externí k autonomnímu systému) Vytvoří se při zanášení externí cesty typu E2 směrovačem ASBR, které je následně plošně rozesláno. Externí cesta typu E2 uvažuje pouze externí metriku (metriku kterou určil směrovací protokol, ze kterého externí cesta pochází.)

Typ 7 - NSSA External (Externí k oblasti NSSA) LSA typu 7 vytváří ASBR uvnitř oblasti NSSA místo LSA typu 5. Hraniční směrovače oblastí ABR převádějí LSA typu 7 při odesílání do jiné oblasti na typ 5.

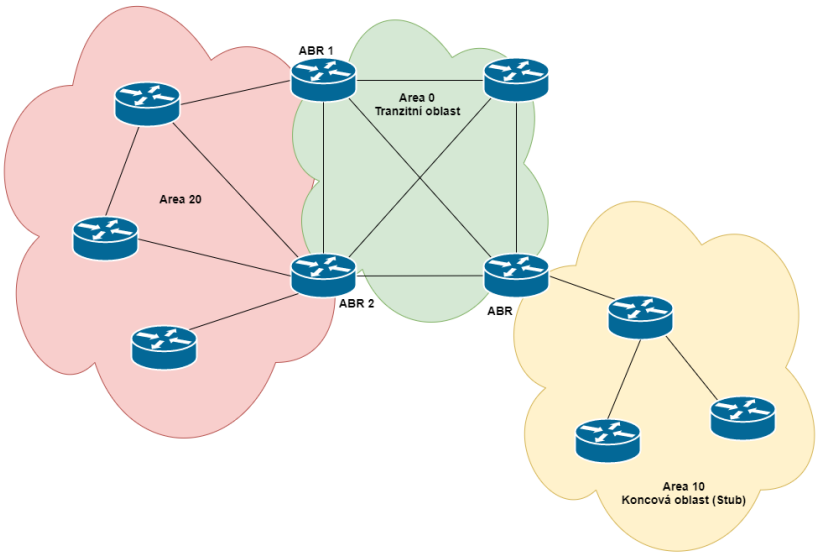
Typy oblastí

Obecně můžeme oblasti v OSPF dělit na 2 základní typy:

- **Tranzitní oblast** - taková, kterou prochází provoz z jedné oblasti do druhé.
- **Koncová oblast (Stub area, Stubby area)** - je oblast, ve které provoz končí nebo začíná, ale nikdy jí neprochází (v rámci sítě s OSPF protokolem).

Koncové oblasti můžeme dál dělit na:

- Koncovou oblast (stub, stubby)
- Plně koncovou oblast (totally stubby)
- Oblast NSSA (Not-So-Stubby Area)
- Úplnou oblast NSSA (totally NSSA)



Obr. 4.4: Princip oblastí v OSPF protokolu

Koncová oblast (stub, stubby area)

- obecný standard
- Area 0 nelze nastavit jako stub
- v oblasti nesmí ležet hraniční směrovač autonomního systému (Autonomous System Boundary Router, ASBR)
- všechny směrovače v oblasti musí být shodně nakonfigurovány jako stub
- přes oblast nesmí procházet virtuální link
- nezanášejí se LSA typu 5

Plně koncová oblast (Totally stubby area)

- proptietární rozšíření společnosti Cisco
- dále rozvíjí princip stub oblasti
- do oblasti toho typu se nepropagují cesty z ostatních oblastí
- ve směrovací tabulce směrovače v Totally stubby area jsou obsaženy pouze cesty uvnitř oblasti a defaultní cestu.
- nezanášejí se LSA typu 5 a 3

Oblast NSSA (Not-So-Stubby Area)

- typ koncové oblasti, ve které se provádí redistribuce
- v oblasti smí ležet ASBR, který provádí redistribuci
- podobné vlastnosti jako stub oblast, připouští, aby z ní byly propagovány externí cesty
- nezanášejí se LSA typu 5
- umožňuje vytváření LSA typu 7 uvnitř oblasti

Úplná oblast NSSA (totally NSSA)

- rozšíření NSSA oblasti
- nezanášejí se LSA typu 5 a 3
- umožňuje vytváření LSA typu 7 uvnitř oblasti

V této laboratorní úloze budou konfigurovány oblasti typu Stub, Totally Stub a Not-So-Stubby. Cílem konfigurace koncových oblastí je snižovat množství komunikace, velikost topologické databáze (Link State Database - LSDB) a v důsledku toho i velikost směrovací tabulky. LSDB obsahuje orientovaný graf sítě vytvořený pomocí informací v jednotlivých LSA. Nad touto databází se následně spouští algoritmus SPF, jehož výsledkem je nalezení nejkratších cest do každé podsítě a odstranění smyček v topologii sítě. V případě, že je směrovač ve více oblastech, udržuje pro každou oblast samostatnou LSDB [31].

4.1.3 Postup

Proveďte zapojení celé sítě podle zadané topologie včetně fyzického směrovače. Fyzický směrovač poznáte tak, že je v topologii umístěn v oblaku.

Směrovače pojmenujte podle informací v topologii [17].

```
Router# hostname R1
R1#
```

IP adresy přidělte a nastavte zařízením dle tabulky 4.1.

Příklad konfigurace síťového rozhraní na Cisco směrovači [17]:

```
R1# configure terminal
R1(config)# interface fastethernet0/0
R1(config-if)# ip address 172.16.1.17 255.255.255.252
R1(config-if)# no shutdown
R1(config-if)# exit
```

V případě konfigurace sériového rozhraní je ještě potřeba nastavit na **DCE** takt, který se zadává v jednotkách bit/s. Pro zobrazení všech podporovaných rychlostí zadejte příkaz:

```
R1(config-if)# clock rate ?
```

Zvolte např. hodnotu 64000 neboli 64 kbit/s.

```
R1(config-if)# clock rate 64000
```

Pro kontrolu správného nastavení IP adres a masek vyzkoušejte ping v rámci dvoubodových lokálních podsítí mezi směrovači (R1 → R2, R1 → R6, R6 → R7, atp.).

Směrování protokolem OSPF

Konfigurace směrovacího protokolu OSPF začíná příkazem:

```
R4(config)# router ospf <ID procesu>
```

kde ID procesu je číslo od 1 do 65 535, které nijak nesouvisí s číslem oblasti, do které směrovač patří a slouží pouze k oddělení OSPF procesů v rámci zařízení. Má pouze lokální charakter a tudíž na různých směrovačích v rámci sítě může být zadáno různé ID procesu.

Následuje zadání parametru router-id, což je identifikátor směrovače v rámci sítě, ve které probíhá směrování pomocí OSPF.

```
R4(config-router)# router-id 4.4.4.4
```

U protokolu OSPF musíte nakonfigurovat všechny přímo připojené podsítě, inverzní masky a oblast, do které patří. Inverzní maska (Wildcard mask) je speciální zápis síťové masky. Jedná se o opak ke klasické masce. Místo jedniček v binárním zápise se v tomto případě počítají nuly. Například klasické masce 255.255.255.0 odpovídá inverzní maska 0.0.0.255. V rámci OSPF směrovacího procesu jednotlivé inverzní masky určují, na kterých rozhraních směrovače bude směrovací proces aktivován. Existuje i obecnější zápis v podobě samých nul u čísla sítě a inverzní masky, který aktivuje směrovací proces na všech rozhraních.

Konfigurace protokolu OSPF na směrovači R4 bude vypadat následovně:

```
R4(config)# router ospf 1
R4(config-router)# router-id 4.4.4.4
R4(config-router)# network 172.16.1.4 0.0.0.3 area 20 // síť mezi R4 a R2
R4(config-router)# network 172.16.1.8 0.0.0.3 area 20 // síť mezi R4 a R5
R4(config-router)# network 172.16.1.33 0.0.0.0 area 20 // síť na virtuálním
                                                        rozhraní Loopback 0
```

Směrování protokolem EIGRP

Pro demonstraci koncové oblasti typu NSSA bude v části topologie nastaven směrovací protokol EIGRP. Konfigurace je obdobná jako u OSPF,

```
R10(config)# router EIGRP <číslo autonomního systému>
```

kde číslo autonomního systému je číslo od 1 do 65 535, které musejí mít všechny směrovače ve stejném autonomním systému shodné.

U protokolu EIGRP se na rozdíl od OSPF síť nedělí na oblasti a tudíž se ani do konfigurace neuvádějí. Zadávají se tedy pouze adresy podsítí a inverzní masky (inverzní maska má zde stejný význam, jako v případě OSPF směrovacího procesu), které budou podléhat směrování v protokolu EIGRP.

Konfigurace protokolu EIGRP na směrovači R10 bude vypadat následovně:

```
R10(config)# router eigrp 100
R10(config-router)# no auto-summary // vypnutí automatické sumarizace
R10(config-router)# network 10.11.12.0 0.0.0.3 // podsíť mezi R10 a R9
R10(config-router)# network 10.11.12.5 0.0.0.0 // podsíť na virtuálním
                                                  rozhraní Loopback 0
```

Redistribuce směrovacích informací

Redistribucí se rozumí předávání směrovacích informací z jednoho protokolu do druhého a naopak. Tento proces bude probíhat na fyzickém směrovači R9, který je připojen jak k síti s protokolem OSPF, tak i EIGRP.

Konfigurace redistribuce z EIGRP do OSPF bude vypadat následovně:

```
R10(config)# router ospf 1
R10(config-router)# redistribute eigrp 100 subnets
```

Směrovač provádí redistribuci z EIGRP (autonomní systém číslo 100) do OSPF. U redistribuovaných cest je výchozí hodnota metriky v OSPF rovna 20. Dále je součástí příkazu volba subnets, která umožní redistribuci podsítí. Bez této volby se redistribuují pouze cesty pro třídní sítě. Nyní je ještě potřeba nastavit redistribuci v opačném směru, tedy z OSPF do EIGRP:

```
R10(config)# router eigrp 100
R10(config-router)# redistribute ospf 1 metric 1000 1000 245 245 1500
```

Směrovač provádí redistribuci z OSPF (číslo procesu 1) do EIGRP. EIGRP musí definovat metriku, protože ta nemá žádnou výchozí hodnotu. Hodnoty metriky mají následující význam: Šířka pásma (1000), zpoždění (1000), zatížení (245), spolehlivost (245), MTU (1500). Dále nebudeme metriku rozebírat, jelikož to není cílem této úlohy.

Pro kontrolu dostupnosti všech podsítí v topologii použijte následující příkaz

```
R1(config)# show ip route
```

Koncové oblasti

Jak již bylo uvedeno v úvodu, v této laboratorní úloze budou konfigurovány tři typy koncových oblastí: Stub, Totally Stub a Not-So-Stubby Area (NSSA). Nejdříve si však zobrazte velikost a obsah směrovací tabulky bez toho, aniž byste konfigurovali oblast jako koncovou [7].

```
R6# show ip route
Gateway of last resort is not set

172.16.0.0/16 is variably subnetted, 13 subnets, 2 masks
O IA    172.16.1.49/32 [110/85] via 172.16.1.17, 00:00:04, FastEthernet0/0
O       172.16.1.45/32 [110/2] via 172.16.1.22, 00:00:04, FastEthernet1/0
C       172.16.1.41/32 is directly connected, Loopback0
O IA    172.16.1.37/32 [110/85] via 172.16.1.17, 00:00:04, FastEthernet0/0
O IA    172.16.1.33/32 [110/85] via 172.16.1.17, 00:00:04, FastEthernet0/0
O IA    172.16.1.28/30 [110/84] via 172.16.1.17, 00:00:04, FastEthernet0/0
O IA    172.16.1.24/30 [110/84] via 172.16.1.17, 00:00:05, FastEthernet0/0
C       172.16.1.20/30 is directly connected, FastEthernet1/0
C       172.16.1.16/30 is directly connected, FastEthernet0/0
O       172.16.1.12/30 [110/11] via 172.16.1.22, 00:00:05, FastEthernet1/0
O IA    172.16.1.8/30 [110/85] via 172.16.1.17, 00:00:05, FastEthernet0/0
O IA    172.16.1.4/30 [110/84] via 172.16.1.17, 00:00:05, FastEthernet0/0
O IA    172.16.1.0/30 [110/84] via 172.16.1.17, 00:00:07, FastEthernet0/0
10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
O E2    10.11.12.5/32 [110/20] via 172.16.1.17, 00:00:07, FastEthernet0/0
O E2    10.11.12.0/30 [110/20] via 172.16.1.17, 00:00:07, FastEthernet0/0
192.168.1.0/30 is subnetted, 3 subnets
O IA    192.168.1.8 [110/138] via 172.16.1.17, 00:00:07, FastEthernet0/0
O IA    192.168.1.0 [110/74] via 172.16.1.17, 00:00:07, FastEthernet0/0
O IA    192.168.1.4 [110/74] via 172.16.1.17, 00:00:07, FastEthernet0/0
```

```
R6# show ip route summary
IP routing table name is Default-IP-Routing-Table(0)
IP routing table maximum-paths is 16
Route Source    Networks    Subnets     Overhead    Memory (bytes)
connected       0           3           216         408
static          0           0           0           0
ospf 1          0           15          1080        2040
Intra-area: 2 Inter-area: 11 External-1: 0 External-2: 2
NSSA External-1: 0 NSSA External-2: 0
internal        3                                   3468
Total           3           18          1296        5916
```

Je patrné, že směrovač R6 má ve směrovací tabulce záznamy o všech podsítích v rámci topologie včetně externích (příznak E2) a velikost směrovací tabulky je 5916 bytů. Konfigurací oblasti 10 jako Stub by se tato velikost měla zmenšit a ve směrovací tabulce by měly zmizet záznamy o externích podsítích. Do koncové oblasti typu Stub se totiž nezanášejí LSA typu 5, což jsou informace o externích podsítích. Místo toho hraniční směrovač ABR vytvoří a oznámí výchozí (default) cesty. Interní směrovače v oblasti pak podle výchozích cest zasílají pakety

vždy do uvedeného hraničního směrovače a v důsledku toho mohou i zmenšit velikost směrovací tabulky.

Určení oblasti 10 jako Stub vypadá následovně:

```
R6(config)# router ospf 1
R6(config-router)# area 10 stub
```

Toto nastavení musíte provést na všech směrovačích v dané oblasti, tedy na R6, R7 a R1. Po konfiguraci proveďte ověření, že ve směrovací tabulce opravdu chybí záznamy o externích sítích, byla přidána výchozí cesta a také, že se velikost směrovací tabulky opravdu zmenšila.

```
R6# show ip route
Gateway of last resort is 172.16.1.17 to network 0.0.0.0

172.16.0.0/16 is variably subnetted, 12 subnets, 2 masks
O IA    172.16.1.49/32 [110/85] via 172.16.1.17, 00:00:05, FastEthernet0/0
C       172.16.1.41/32 is directly connected, Loopback0
O IA    172.16.1.37/32 [110/85] via 172.16.1.17, 00:00:05, FastEthernet0/0
O IA    172.16.1.33/32 [110/85] via 172.16.1.17, 00:00:05, FastEthernet0/0
O IA    172.16.1.28/30 [110/84] via 172.16.1.17, 00:00:05, FastEthernet0/0
O IA    172.16.1.24/30 [110/84] via 172.16.1.17, 00:00:05, FastEthernet0/0
C       172.16.1.20/30 is directly connected, FastEthernet1/0
C       172.16.1.16/30 is directly connected, FastEthernet0/0
O       172.16.1.12/30 [110/20] via 172.16.1.17, 00:00:06, FastEthernet0/0
O IA    172.16.1.8/30 [110/85] via 172.16.1.17, 00:00:06, FastEthernet0/0
O IA    172.16.1.4/30 [110/84] via 172.16.1.17, 00:00:06, FastEthernet0/0
O IA    172.16.1.0/30 [110/84] via 172.16.1.17, 00:00:06, FastEthernet0/0
192.168.1.0/30 is subnetted, 3 subnets
O IA    192.168.1.8 [110/138] via 172.16.1.17, 00:00:07, FastEthernet0/0
O IA    192.168.1.0 [110/74] via 172.16.1.17, 00:00:07, FastEthernet0/0
O IA    192.168.1.4 [110/74] via 172.16.1.17, 00:00:07, FastEthernet0/0
O*IA 0.0.0.0/0 [110/11] via 172.16.1.17, 00:00:07, FastEthernet0/0
```

```
R6# show ip route summary
IP routing table name is Default-IP-Routing-Table(0)
IP routing table maximum-paths is 16
Route Source    Networks    Subnets     Overhead    Memory (bytes)
connected       0           3           216         408
static          0           0           0           0
ospf 1          1           13          1008        1904
Intra-area: 2 Inter-area: 12 External-1: 0 External-2: 0
NSSA External-1: 0 NSSA External-2: 0
internal        2                                   2312
Total           3           16          1224        4624
```

Velikost směrovací tabulky se zmenšila z 5916 bytů na 4624 byty a jako poslední záznam směrovací tabulky byla přidána výchozí cesta.

Nyní bude oblast 20 nakonfigurována jako Totally Stubby. Tento typ oblasti je proprietárním rozšířením společnosti Cisco a rozvádí dál myšlenku Stub oblasti v tom, že se do této oblasti

nezanášejí kromě LSA typu 5 ani LSA typu 3. V praxi to znamená, že směrovač ve směrovací tabulce má pouze záznamy o podsítích v rámci oblasti a výchozí bránu, což ještě více zmenšuje velikost směrovací tabulky oproti Stub oblasti.

Konfigurace je obdobná jako u Stub oblasti a opět je nutné jí provést na všech směrovačích v dané oblasti, tedy na R4, R5 a R2:

```
R4(config)# router ospf 1
R4(config-router)# area 20 stub no-summary
```

Zobrazení směrovací tabulky a její velikosti:

```
R4# show ip route
Gateway of last resort is 172.16.1.5 to network 0.0.0.0

172.16.0.0/16 is variably subnetted, 5 subnets, 2 masks
O       172.16.1.37/32 [110/2] via 172.16.1.10, 08:15:14, FastEthernet1/0
C       172.16.1.33/32 is directly connected, Loopback0
C       172.16.1.8/30 is directly connected, FastEthernet1/0
C       172.16.1.4/30 is directly connected, FastEthernet0/1
O       172.16.1.0/30 [110/11] via 172.16.1.10, 08:15:14, FastEthernet1/0
O*IA 0.0.0.0/0 [110/11] via 172.16.1.5, 08:15:14, FastEthernet0/1
```

```
R4# show ip route summary
IP routing table name is Default-IP-Routing-Table(0)
IP routing table maximum-paths is 16
Route Source    Networks    Subnets     Overhead    Memory (bytes)
connected       0           3           216         408
static          0           0           0           0
ospf 1          1           2           216         408
Intra-area: 2 Inter-area: 1 External-1: 0 External-2: 0
NSSA External-1: 0 NSSA External-2: 0
internal        1                                   1156
Total           2           5           432         1972
```

Velikost tabulky se dále zmenšila z 4624 byty (Stub oblast) na pouhých 1972 byty. Pokud porovnáme velikost směrovací tabulky bez konfigurace oblasti jako koncové a při nastavení oblasti jako Totally Stubby zjistíme, že se velikost zmenšila na $\frac{1}{3}$. Je tedy patrné, že konfigurace koncových oblastí se z hlediska počtu směrovacích záznamů a velikosti směrovacích tabulek velmi vyplácí.

Jako poslední typ koncové oblasti bude konfigurována oblast typu NSSA (Not-So-Stubby Area). Tato oblast má na rozdíl od ostatních typů výhodu v tom, že může obsahovat ASBR a tedy i generovat externí cesty uvnitř oblasti.

Jako oblast typu NSSA bude konfigurována oblast 30, ve které leží směrovač R9 provádějící redistribuci směrovacích informací mezi OSPF a EIGRP protokolem.

```
R4(config)# router ospf 1
R4(config-router)# area 30 nssa
```

Totéž proveďte na zbylých dvou směrovačích v oblasti 30.

Na R3 nastavte, aby byla generována výchozí cesta přes tento směrovač

```
R3(config-router)# area 30 nssa default-information-originate
```

Směrovací tabulka bude vypadat následovně:

```
R8# show ip route
Gateway of last resort is 172.16.1.29 to network 0.0.0.0

172.16.0.0/16 is variably subnetted, 13 subnets, 2 masks
C       172.16.1.49/32 is directly connected, Loopback0
O IA    172.16.1.45/32 [110/85] via 172.16.1.29, 00:00:38, FastEthernet0/0
O IA    172.16.1.41/32 [110/85] via 172.16.1.29, 00:00:38, FastEthernet0/0
O IA    172.16.1.37/32 [110/85] via 172.16.1.29, 00:00:38, FastEthernet0/0
O IA    172.16.1.33/32 [110/85] via 172.16.1.29, 00:00:38, FastEthernet0/0
C       172.16.1.28/30 is directly connected, FastEthernet0/0
O       172.16.1.24/30 [110/20] via 172.16.1.29, 00:00:39, FastEthernet0/0
O IA    172.16.1.20/30 [110/85] via 172.16.1.29, 00:00:39, FastEthernet0/0
O IA    172.16.1.16/30 [110/84] via 172.16.1.29, 00:00:39, FastEthernet0/0
O IA    172.16.1.12/30 [110/84] via 172.16.1.29, 00:00:39, FastEthernet0/0
O IA    172.16.1.8/30 [110/85] via 172.16.1.29, 00:00:39, FastEthernet0/0
O IA    172.16.1.4/30 [110/84] via 172.16.1.29, 00:00:39, FastEthernet0/0
O IA    172.16.1.0/30 [110/84] via 172.16.1.29, 00:00:42, FastEthernet0/0
10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
O N2    10.11.12.5/32 [110/20] via 172.16.1.29, 00:00:42, FastEthernet0/0
O N2    10.11.12.0/30 [110/20] via 172.16.1.29, 00:00:42, FastEthernet0/0
192.168.1.0/30 is subnetted, 3 subnets
O IA    192.168.1.8 [110/74] via 172.16.1.29, 00:00:42, FastEthernet0/0
O IA    192.168.1.0 [110/138] via 172.16.1.29, 00:00:42, FastEthernet0/0
O IA    192.168.1.4 [110/74] via 172.16.1.29, 00:00:42, FastEthernet0/0
O*N2 0.0.0.0/0 [110/1] via 172.16.1.29, 00:00:42, FastEthernet0/0
```

Opět můžete nalézt výchozí cestu zanášenou ABR a také dvě externí cesty typu N2 (OSPF NSSA external type 2). V ostatních oblastech pokud nejsou nastaveny jako Stub popřípadě Totally Stub se tyto záznamy zobrazí s příznakem E2 (OSPF external type 2). Je to dáno tím, že ABR převádí LSA typu 7 na typ 5. V případě, že by v jiné části sítě probíhala také redistribuce, záznamy typu E2 bychom ve směrovací tabulce nenašli. Oblast typu NSSA stejně jako ostatní druhy koncových oblastí nezanáší LSA typu 5.

V této laboratorní úloze byly konfigurovány tři typy koncových oblastí směrovacího protokolu OSPF a vysvětleny a ověřeny rozdíly mezi nimi. Pro demonstraci chování NSSA oblasti byl v části sítě nastaven protokol EIGRP a také redistribuce mezi OSPF a EIGRP protokoly.

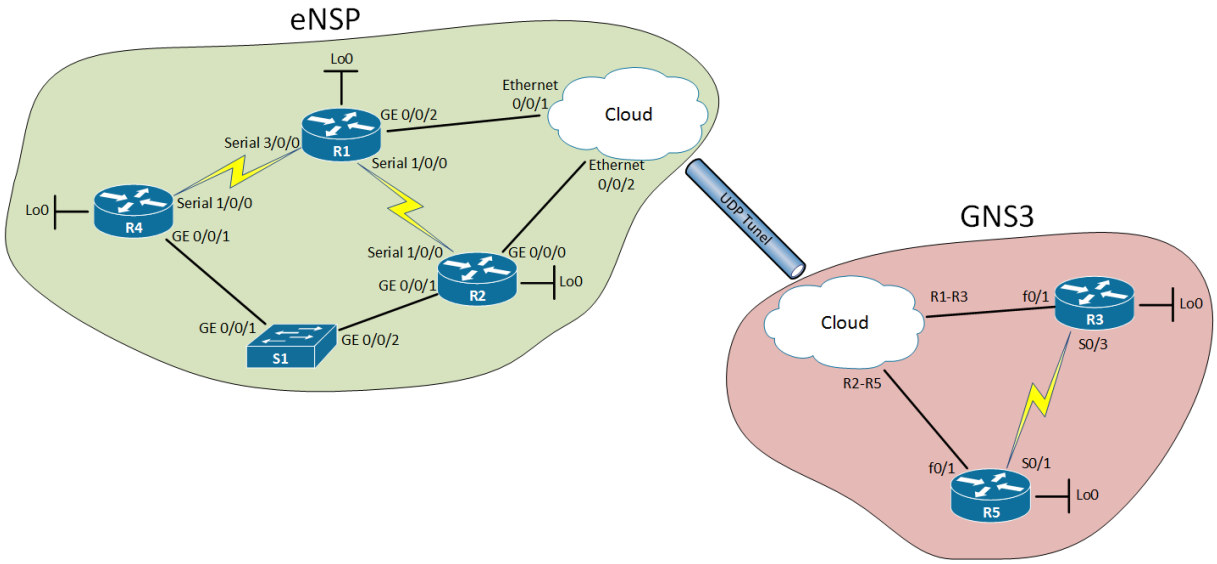
4.2 Lab 2 - Multicast, PIM Dense mode

V této úloze proběhne seznámení s konfigurací aktivních síťových prvků od společnosti Huawei. Úloha je koncipována tak, že část sítě je emulována v GNS3 a část v nástroji eNSP. Propojení obou sítí je realizováno nástrojem Cloud jímž oba nástroje disponují. Po seznámení s principy konfigurace síťových prvků Huawei bude v obou částech sítě konfigurován multicast se směrovacím protolem PIM v režimu Dense mode a ověřena jeho funkčnost.

4.2.1 Zadání a topologie

Zadání:

- V prostředí emulačního softwaru GNS3 a eNSP realizujte multicastové vysílání protokolem PIM v režimu Dense mode.
- Na směrovačích R2 a R4 nakonfigurujte IGMP protokol.
- Uvažujte topologii dle obr. 4.5.
- Nejdříve konfigurujte část v emulátoru eNSP a až poté v GNS3.
- Dynamické směrování v zadané topologii realizujte protokolem OSPF.
- Pro propojení obou sítí využijte nástroj Cloud.
- Ověřte funkčnost multicastového směrování.



Obr. 4.5: Topologie laboratorní úlohy

4.2.2 Rozbor úlohy

V této úloze budou konfigurovány čtyři virtuální směrovače Huawei a dva směrovače Cisco. Propojení bude realizováno nástrojem Cloud. Mezi emulátory bude vytvořen UDP tunel. Směrovač R1 bude sloužit jako zdroj taktu pro sériové spoje R1-R4 a R1-R2. Směrovač R3 bude zdroj taktu pro spoj R3-R5. Na každém směrovači bude nakonfigurováno virtuální rozhraní Loopback, které bude sloužit pro identifikaci směrovače v rámci směrovacího protokolu OSPF.

Zařízení	Rozhraní	IP adresa	Adresa podsítě	DCE/DTE	Typ
R1	Serial 1/0/0	10.0.12.1	10.0.12.0 /24	DCE	Huawei AR2220
	Serial 3/0/0	10.0.14.1	10.0.14.0 /24	DCE	
	GE 0/0/2	10.0.13.1	10.0.13.0 /24	-	
	lo0	10.0.1.1	10.0.1.1 /32	-	
R2	Serial 1/0/0	10.0.12.2	10.0.12.0 /24	DTE	Huawei AR2220
	GE 0/0/0	10.0.25.2	10.0.25.2 /24	-	
	GE 0/0/1	10.0.24.2	10.0.24.0 /24	-	
	Lo0	10.0.2.2	10.0.2.2 /32	-	
R3	s0/3	10.0.35.3	10.0.35.0 /24	DCE	Cisco 2691
	f0/1	10.0.13.3	10.0.13.0 /24	-	
	Lo0	10.0.3.3	10.0.3.3 /32	-	
R4	Serial 1/0/0	10.0.14.4	10.0.14.0 /24	DTE	Huawei AR1220
	GE 0/0/1	10.0.24.4	10.0.24.0 /24	-	
	Lo0	10.0.4.4	10.0.4.4 /32	-	
R5	s0/1	10.0.35.5	10.0.35.0 /24	DTE	Cisco 2691
	f0/1	10.0.25.5	10.0.25.0 /24	-	
	Lo0	10.0.5.5	10.0.5.5 /32	-	
S1	GE 0/0/1	-	-	-	Huawei S5700
	GE 0/0/2	-	-	-	

Tab. 4.2: Tabulka IP adres

Multicast

Multicast je z definice komunikace jednoho zdroje s více cíli. Jako přiřazení můžeme použít streamování videa, kdy zdroj vysílá video stream a příjemci toho streamu jsou jen cíle, které o to mají zájem. V praxi se ovšem tento typ komunikace často řeší tak, že se vytvoří spojení pro každého příjemce zvlášť. To ovšem způsobuje zatížení jak zdroje, tak i infrastruktury, která musí přenášet duplicitní data. Multicast řeší doručování paketů více příjemcům co možná nejefektivnějším způsobem a to tak, aby paket šel přes každý uzel v síti pouze jednou. Kopie paketů se vytváří pouze na směrovačích, kde se cesty k příjemcům rozdělují.

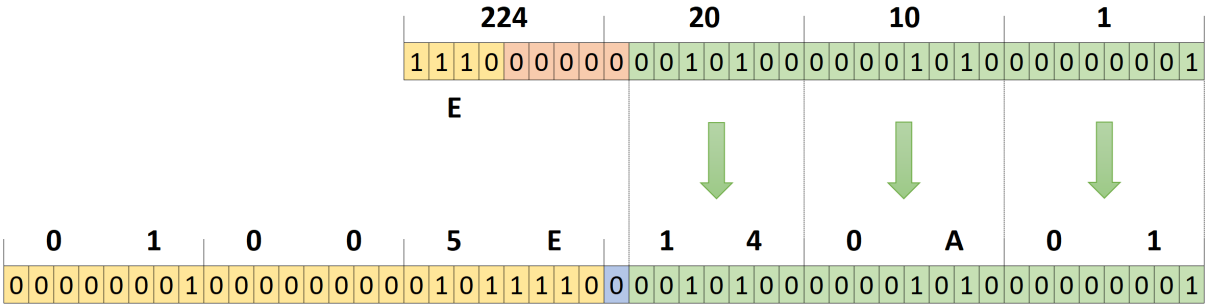
Zdroj dat odesílá pakety na multicastovou adresu (třída D, rozsah: 224.0.0.0 – 239.255.255.255). Tato adresa neidentifikuje pouze jednoho příjemce, ale skupinu příjemců. Zdrojová adresa je vždy unicastová. Na rozdíl od unicastového vysílání, které je iniciováno zdrojem je multicastové vysílání iniciováno příjemci. K tomu, aby se příjemci přihlásili do multicastové skupiny a tedy i k přijímání paketů, slouží protokol IGMP. Směrovač tedy musí zjišťovat, do kterých přímo připojených sítí má multicast odesílat. Směrovač periodicky odesílá do přímo připojených sítí dotaz na multicastovou adresu 224.0.0.1 a stanice odpovídají s informací, kterou skupinu chtějí přijímat na adresu skupiny, kterou chtějí přijímat. V případě, že stanice zaregistruje odpověď od jiné stanice na stejnou multicastovou adresu, odpověď sama neposílá.

Pro zabránění posílání multicastových paketů ve smyčkách se používá metoda RPF (Reverse Path Forwarding). Směrovač přijímá provoz pouze ze směrů, ze kterých vede zpáteční cesta

ke zdroji vysílání. Tato metoda je založena na standardních směrovacích protokolech (OSPF, EIGRP atp.) a využívá unicastovou směrovací tabulku [31], [8].

Multicast MAC adresa

Každá multicast MAC adresa začíná vždy 01:00:5E následně se přidá 0 a posledních 23 bitů multicastové IP adresy se přímo zkopíruje do multicastové MAC adresy. Princip je vyznačen na obr. 4.6. Z obrázku vyplývá, že 5 bitů se z multicastové IP adresy nepřevádí. Přiřazení IP adres k MAC adresám tedy není jednoznačné, 2^5=32 IP adres se mapuje vždy na jednu MAC adresu [20].



Obr. 4.6: Převod multicastové IP adresy na multicastovou MAC adresu

Multicast adresní rozsahy

- **224.0.0.0 až 224.0.0.255** - určené pro síťové protokoly uvnitř LAN, mají TTL = 1
- **224.0.1.0 až 238.255.255.255** - globální multicast adresy, které se používají mezi organizacemi a přes internet
- **239.0.0.0 až 239.255.255.255** - adresy určené pro použití uvnitř organizace (LAN)

PIM

PIM (Protocol Independent Multicast) je protokol sloužící k multicastovému směrování paketů. Existuje ve dvou variantách - Dense mode (hustý režim) a Sparse mode (řídký režim). V rámci této úlohy si popíšeme pouze Dense mode, jelikož bude i konfigurován.

Dense mode předpokládá, že multicastový provoz chce přijímat většina stanic v síti. Hodí se tam, kde jsou zdroje a přijímače blízko u sebe (co do počtu směrovačů mezi nimi). Pokud je směrovač nakonfigurován v tomto režimu, odesílá multicastový provoz na všechna rozhraní (mimo toho, ze kterého přišel).

Tento režim PIM protokolu funguje na principu záplavy, kdy je síť nejdříve zaplavena multicastovým provozem a následně se multicastový provoz omezuje tím, že směrovače posílají informaci o tom, že nechtějí multicastový provoz přijímat. Pokud směrovač zjistí (protokolem IGMP), že k žádnému jeho rozhraní není připojen zájemce o multicastový provoz, odešle směrovači na vyšší úrovni (blíže ke zdroji zpráv) žádost, aby mu multicastový provoz neposílal. Tento typ zprávy se nazývá „Prune“ (odříznutí). Tím dojde k odříznutí větve v distribučním stromu od multicastového provozu. Pokud je třeba obnovit zasílání, musí odříznutý směrovač odeslat zprávu „Graft“ směrovači vyšší úrovně. Tím dojde k obnovení zasílání multicastového provozu [31].

IGMP

Internet Group Management Protocol má za cíl informovat směrovače v síti, že některé koncové stanice mají zájem přijímat multicastový provoz v rámci určité multicastové skupiny. Existují tři verze tohoto protokolu IGMPv1, IGMPv2 a IGMPv3. V této úloze budeme využívat IGMPv2 a proto si teď popíšeme jeho funkci.

Směrovač periodicky zjišťuje informace o tom, zda je na některém z jeho rozhraní zájem o přijímání multicastového provozu (jednotlivých skupin). Zprávy, které vysílá, se nazývají Membership query. Aby nedocházelo k zahlcení v případě více odpovědí najednou, stanice neodpoví na tuto zprávu ihned, ale počká náhodnou dobu. Pokud během této doby zareaguje jiná stanice odpovědí Membership report, ve které je zasíláno přihlášení k dané multicastové skupině a multicastová skupina se shoduje s tou, kterou chce přijímat i čekající stanice, odpověď již neposílá. Zprávy Membership query jsou posílány na multicastovou adresu 224.0.0.1 (všichni hosté v lokální síti), čímž je zaručeno to, že dotazy slyší všechny stanice v rámci lokální sítě. Zprávy Membership report jsou zasílány na adresy požadovaných multicastových skupin s TTL 1.

Pokud stanice již nechce přijímat provoz z určité multicastové skupiny, pošle zprávu o zrušení členství Leave group na její skupinovou adresu. Po přijmutí této zprávy směrovačem je odeslána zpráva Group Specific query, která zjišťuje, zda v síti existuje alespoň jedna stanice, která má zájem přijímat provoz v rámci dané multicastové skupiny. Pokud taková stanice existuje, záznam v multicast směrovací tabulce zůstane, pokud ne, je smazán [31].

4.2.3 Aktivní síťové prvky Huawei

Jelikož je většina síťových prvků v úloze od společnosti Huawei, proběhne nejdříve seznámení se základními principy konfigurace těchto prvků.

Na první pohled jsou konfigurační příkazy velmi podobné příkazům na konfiguraci prvků Cisco. Jsou tu ovšem drobné rozdíly, které je nutné si osvětlit. Po připojení ke směrovači se dostaneme do tzv. user-view. Tento režim lze přirovnat k privilegovanému módu u IOS. V tomto režimu jsou omezené možnosti konfigurace (ping, tracert, save, show atp.). Pro zobrazení nápovědy platí stejná pravidla, jako u IOS od společnosti Cisco, tedy stačí zadat otazník např.:

```
<Huawei>?
arp-ping            ARP-ping
backup              Backup information
batch-cmd           Batch commands
board-channel-check Board-Channel-Check enable/disable
capture-packet      enable capturing packet
cd                  Change current directory
...
```

Po zadání příkazu:

```
<Huawei>system-view
```

se dostanete do tzv. system-view, což je mód, který lze přirovnat ke konfiguračnímu módu u IOS. V tomto režimu už lze konfigurovat název zařízení, rozhraní, směrování, vzdálený přístup atp. V tabulce 4.3 nalezneme porovnání nejdůležitějších příkazů.

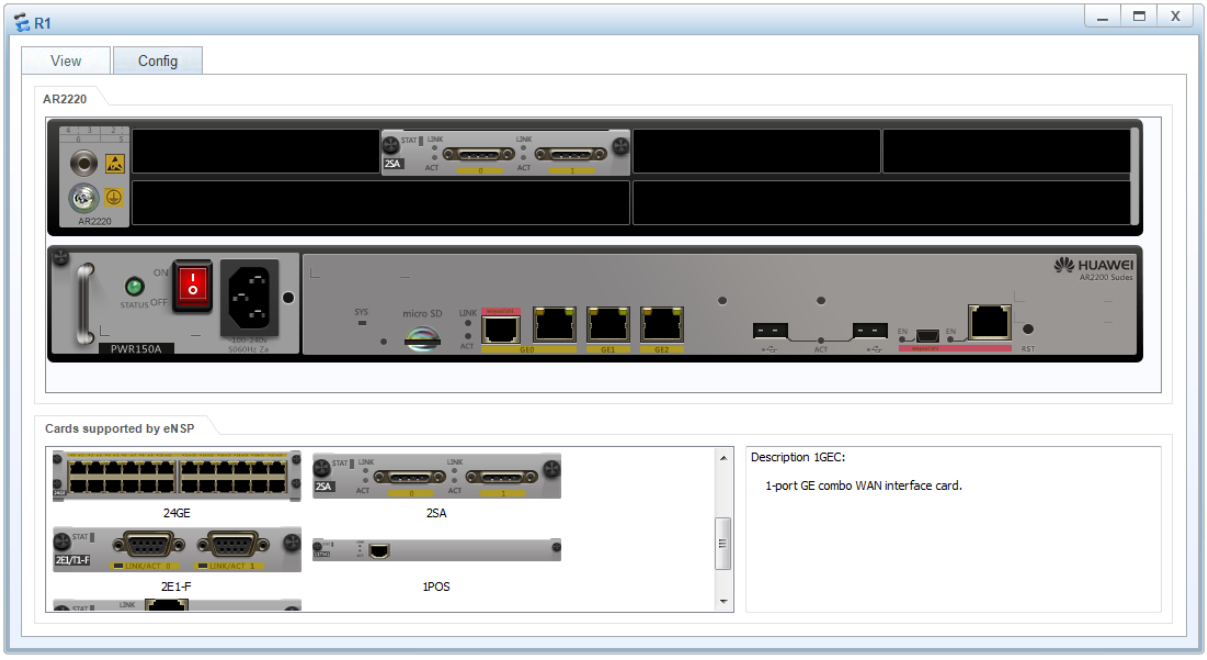
Ve směrovačích Huawei jsou defaultně zapnuta všechna rozhraní a tudíž je není nutno zapínat jako v případě IOS. U sériových rozhraní jsou při startu načteny defaultní hodnoty a nepotřebují žádné dodatečné nastavování jako např. clock rate u IOS.

Cisco iOS	Huawei
traceroute	tracert
show	display
show ip route	display ip routing-table
copy running-config startup-config	save
reload	reboot
no	undo
erase	delete
hostname	sysname
router ospf	ospf

Tab. 4.3: Tabulka některých příkazů pro konfiguraci prvků Cisco a Huawei [24]

4.2.4 Postup

Proveďte zapojení obou částí sítě podle zadané topologie. Směrovače Huawei nemají v základní konfiguraci sériové porty, proto je nutné přidat je ještě před konfigurací. Klikněte pravým tlačítkem myši na ikonu směrovače a zvolte "Settings". Zobrazí se obrázek směrovače viz obr. 4.7. Směrovač vypněte (nejčastěji červené velké tlačítko). Pod obrázkem směrovače jsou dostupné moduly, které je možno vložit do volných šachet. Vyberte modul 2AS a přesuňte do volné šachty. Dbejte na to, abyste modul vložili do správné šachty. Pokud ho vložíte do nesprávné, nebudou vám souhlasit čísla rozhraní podle topologie.



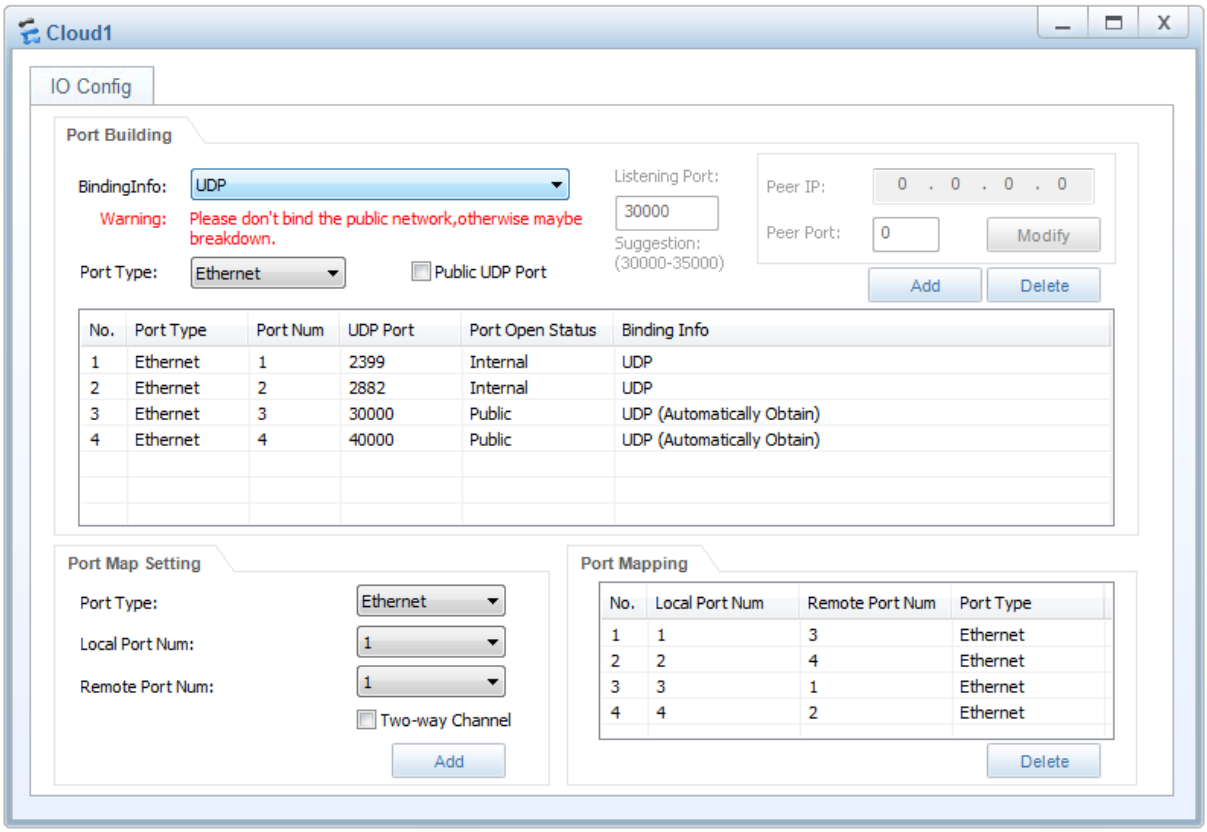
Obr. 4.7: Huawei směrovač

Směrovače pojmenujte podle informací v topologii [17].

```
[Huawei] sysname R1
[R1]
```

```
Router# hostname R3
R3#
```

Nástroj Cloud nastavte v emulátoru eNSP podle obr. 4.8. Důležité je především shodné nastavení veřejných (public) portů. Čísla vnitřních portů (internal) jsou generována automaticky a tudíž se může stát, že nebudou odpovídat portům zobrazených na obrázku. Následně je třeba nastavit mapování portů. Platí, že jednomu veřejnému portu je přidělen jeden interní. Jelikož je to obousměrná cesta, zaškrtněte pole "Two-way Channel".

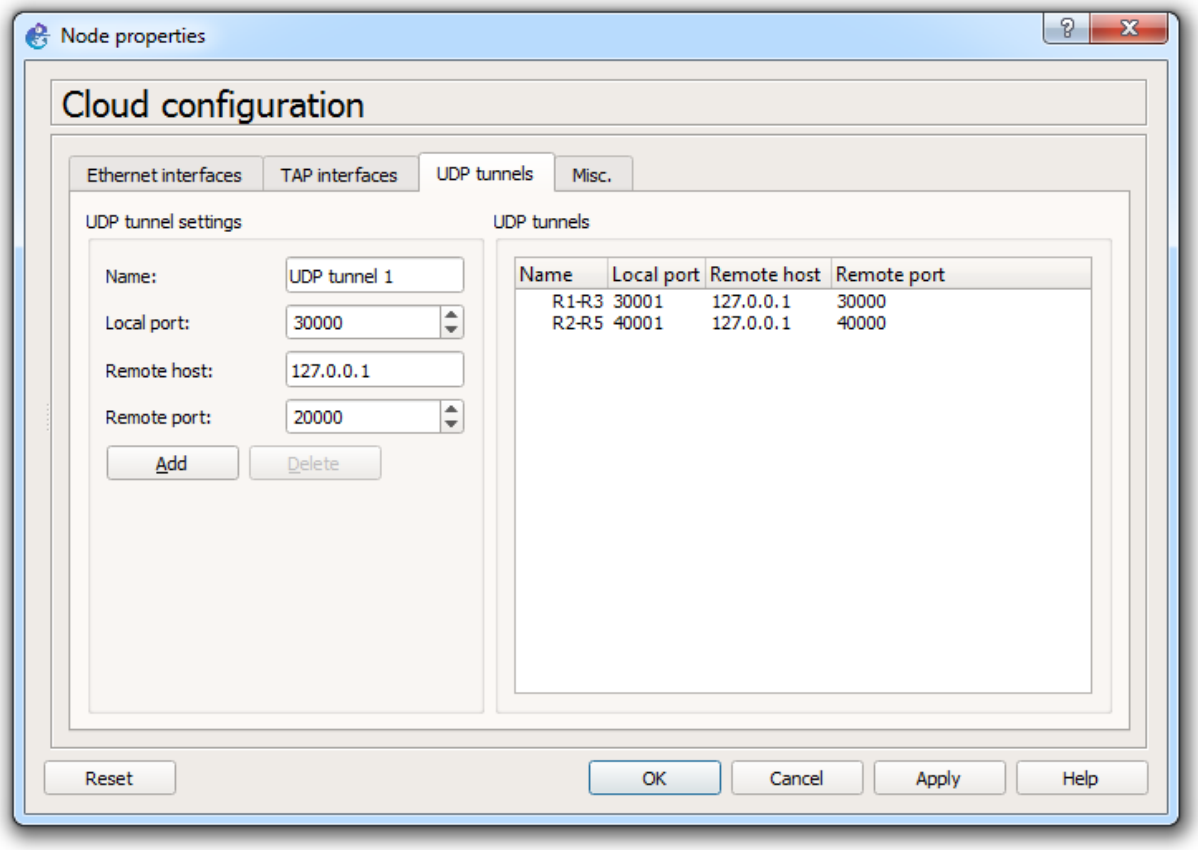


Obr. 4.8: Konfigurace nástroje Cloud v eNSP

V emulátoru GNS3 nastavte nástroj Cloud podle obr. 4.9. Zde si můžete čísla vnitřních a vnějších portů zvolit. V tomto případě se již předpokládá, že cesta je oboustranná, a proto není nutno nastavovat nic dalšího.

Pokud špatně nastavíte nástroje Cloud, nebude fungovat propojení mezi oběma částmi sítě.

IP adresy přidělte a nastavte zařízením dle tabulky 4.2.



Obr. 4.9: Konfigurace nástroje Cloud v GNS3

Příklad konfigurace síťového rozhraní na Cisco směrovači [17]:

```
R3# configure terminal
R3(config)# interface fastethernet0/0
R3(config-if)# ip address 172.16.1.17 255.255.255.252
R3(config-if)# no shutdown
R3(config-if)# exit
```

Příklad konfigurace síťového rozhraní na Huawei směrovači:

```
[R1] interface fastethernet0/0
[R1] ip address 172.16.1.17 255.255.255.252
[R1] quit
```

Po konfiguraci všech síťových rozhraní proveďte kontrolu konektivity mezi směrovači, abyste ověřili správnost konfigurace jak síťových prvků, tak nástrojů Cloud.

Multicast

Nejprve je třeba povolit multicastové směrování paketů globálně na celém směrovači. Následně na každém rozhraní definovat multicastový směrovací protokol a jeho režim (PIM, režimu Dense mode) [13].

Příklad konfigurace multicastu na Huawei směrovači R1:

```
[R1] multicast routing-enable
[R1] interface GigabitEthernet 0/0/2
[R1-GigabitEthernet0/0/2] pim dm
[R1-GigabitEthernet0/0/2] interface Serial 1/0/0
[R1-Serial1/0/0] pim dm
[R1-Serial1/0/0] interface Serial 3/0/0
[R1-Serial3/0/0] pim dm
```

Příklad konfigurace multicastu na Cisco směrovači R5:

```
R5(config)#ip multicast-routing
R5(config)#interface serial 0/1
R5(config-if)#ip pim dense-mode
R5(config-if)#interface fastEthernet 0/1
R5(config-if)#ip pim dense-mode
```

Proveďte kontrolu, zda je protokol PIM aktivován na všech požadovaných rozhraní:

```
 [R1]display pim interface
 VPN-Instance: public net
 Interface           State NbrCnt HelloInt   DR-Pri     DR-Address
 GE0/0/2             up    1      30         1          10.0.13.3
 S1/0/0              up    1      30         1          10.0.12.2
 S3/0/0              up    1      30         1          10.0.14.4
```

PIM je aktivován na 3 rozhraních v rámci směrovače R1 a ke každému rozhraní je připojen jeden soused (NbrCnt). Směrovač s nejvyšší IP adresou funguje v daném segmentu sítě jako Designated Router (DR).
Zobrazte ještě podrobné informace o PIM protokolu na rozhraní g0/0/2 směrovače R1.

```
[R1]display pim interface GigabitEthernet 0/0/2 verbose
VPN-Instance: public net
Interface: GigabitEthernet0/0/2, 10.0.13.1
PIM version: 2
PIM mode: Dense
PIM state: up
PIM DR: 10.0.13.3
PIM DR Priority (configured): 1
PIM neighbor count: 1
PIM hello interval: 30 s
PIM LAN delay (negotiated): 500 ms
PIM LAN delay (configured): 500 ms
PIM hello override interval (negotiated): 2500 ms
PIM hello override interval (configured): 2500 ms
PIM Silent: disabled
PIM neighbor tracking (negotiated): disabled
PIM neighbor tracking (configured): disabled
```

```
PIM generation ID: 0X5325911
PIM require-GenID: disabled
PIM hello hold interval: 105 s
PIM assert hold interval: 180 s
PIM triggered hello delay: 5 s
PIM J/P interval: 60 s
PIM J/P hold interval: 210 s
PIM state-refresh processing: enabled
PIM state-refresh interval: 60 s
PIM graft retry interval: 3 s
PIM state-refresh capability on link: capable
PIM dr-switch-delay timer : not configured
Number of routers on link not using DR priority: 0
Number of routers on link not using LAN delay: 0
Number of routers on link not using neighbor tracking: 2
ACL of PIM neighbor policy: -
ACL of PIM ASM join policy: -
ACL of PIM SSM join policy: -
ACL of PIM join policy: -
```

V základním nastavení se Hello pakety posílají každých 30 sekund. V případě, že soused nepošle Hello paket více než 105 sekund, což je 3,5 násobek intervalu mezi posíláním Hello paketů, je odstraněn ze seznamu sousedů (zrušen stav sousednosti).

Můžete zobrazit seznam sousedů, kteří mají navázán vztah sousednosti se směrovačem R1 v rámci protokolu PIM

```
[R1]display pim neighbor
VPN-Instance: public net
Total Number of Neighbors = 3

Neighbor        Interface           Uptime   Expires  Dr-Priority  BFD-Session
10.0.13.3       GE0/0/2             00:01:56 00:01:26 1            N
10.0.12.2       S1/0/0              00:01:14 00:01:28 1            N
10.0.14.4       S3/0/0              00:01:09 00:01:35 1            N
```

Uptime značí čas, který uběhl od ustanovení stavu sousednosti a Expirates čas, za který tento stav vyprší, pokud od souseda nepřijde Hello paket.

IGMP

Uživatelé přijímací multicast budou připojeni k přepínači S1. Povolte IGMP protokol na rozhraních směrovačů R2 a R4, které jsou připojené k přepínači S1.

```
[R2]interface GigabitEthernet 0/0/1
[R2-GigabitEthernet0/0/1]igmp enable

[R4]interface GigabitEthernet 0/0/1
[R4-GigabitEthernet0/0/1]igmp enable
```

Dále ke stejným rozhraním přiřaďte statickou multicastovou IGMP skupinu. Tím zajistíte, že tato rozhraní budou vždy předávat multicastový provoz s cílovou IP adresou skupiny 225.1.1.1. Směrovač sám ovšem tyto pakety přijímat nebude a ani na ně nebude reagovat.

```
[R2]interface GigabitEthernet 0/0/1
[R2-GigabitEthernet0/0/1]igmp static-group 225.1.1.1

[R4]interface GigabitEthernet 0/0/1
[R4-GigabitEthernet0/0/1]igmp static-group 225.1.1.1
```

Zobrazte podrobné informace o nastavení protokolu IGMP na rozhraní GigabitEthernet 0/0/1 směrovače R2.

```
[R2]display igmp interface GigabitEthernet 0/0/1
Interface information of VPN-Instance: public net
 GigabitEthernet0/0/1(10.0.24.2):
   IGMP is enabled
   Current IGMP version is 2
   IGMP state: up
   IGMP group policy: none
   IGMP limit: -
   Value of query interval for IGMP (negotiated): -
   Value of query interval for IGMP (configured): 60 s
   Value of other querier timeout for IGMP: 0 s
   Value of maximum query response time for IGMP: 10 s
   Querier for IGMP: 10.0.24.2 (this router)
```

V základním nastavení se používá IGMP verze 2. Dále je třeba určit tzv. dotazovače. Dotazovač je zvolený směrovač v segmentu sítě, ke kterému je připojeno více směrovačů a jeho úkolem je odesílání zpráv Membership query. Pomocí zpráv Membership query se směrovač snaží zjistit, zda je k některému jeho rozhraní připojen hostitel, který požaduje příjem vícesměrového provozu z některé skupiny. Ve vašem případě byl zvolen dotazovačem směrovač R2. Jako dotazovač se standardně volí směrovač s nejnižší IP adresou v daném segmentu sítě.

Dále si zobrazte statické IGMP skupiny na směrovači R2 a proveďte kontrolu správného nastavení.

```
[R2]display igmp group static
Static join group information of VPN-Instance: public net
Total 1 entry, Total 1 active entry
Group Address   Source Address  Interface            State     Expires
225.1.1.1       0.0.0.0         GE0/0/1              UP        never
```

Dotazovač mimo jiného vytváří i IGMP směrovací tabulku. Ta je generována pouze v případě, že na rozhraní je nakonfigurován IGMP a nikoliv PIM. IGMP směrovací tabulku tedy na směrovači R4 nezobrazíme.

```
[R2]display igmp routing-table
Routing table of VPN-Instance: public net
 Total 1 entry

 00001. (*, 225.1.1.1)
       List of 1 downstream interface
       GigabitEthernet0/0/1 (10.0.24.2),
       Protocol: STATIC
```

Nastavte interval dotazování neboli interval, jak často má posílat dotazovač zprávy Membership query na 20 sekund. Standardní hodnota je 60 sekund.

```
[R2]interface GigabitEthernet 0/0/1
[R2-GigabitEthernet0/0/1]igmp timer query 20
```

Ověřte, že se položka "Value of query interval for IGMP (configured):"změnila z 60 s na 20 s.

```
[R2]display igmp interface GigabitEthernet 0/0/1
Interface information of VPN-Instance: public net
GigabitEthernet0/0/1(10.0.24.2):
IGMP is enabled
Current IGMP version is 2
IGMP state: up
IGMP group policy: none
IGMP limit: -
Value of query interval for IGMP (negotiated): -
Value of query interval for IGMP (configured): 20 s
Value of other querier timeout for IGMP: 0 s
Value of maximum query response time for IGMP: 10 s
Querier for IGMP: 10.0.24.2 (this router)
```

OSPF

OSPF je v dnešní době nejvyužívanější IGP protokol pro unicastové směrování. To je důvod, proč ho využijeme i v této úloze.

Jako router-id použijte IP adresu rozhraní Loopback0.

Ukázka konfigurace OSPF na Huawei směrovači:

```
[R1] ospf 1 router-id 10.0.1.1
[R1-ospf-1] area 0
[R1-ospf-1-area-0.0.0.0] network 10.0.1.1 0.0.0.0
[R1-ospf-1-area-0.0.0.0] network 10.0.14.0 0.0.0.255
[R1-ospf-1-area-0.0.0.0] network 10.0.13.0 0.0.0.255
[R1-ospf-1-area-0.0.0.0] network 10.0.12.0 0.0.0.255
```

Ukázka konfigurace OSPF na Cisco směrovači:

```
R3(config)# router ospf 1
R3(config-router)# router-id 10.0.3.3
R3(config-router)# network 10.0.3.3 0.0.0.0 area 0
R3(config-router)# network 10.0.13.0 0.0.0.255 area 0
R3(config-router)# network 10.0.35.0 0.0.0.255 area 0
```

Po konfiguraci OSPF protokolu zobrazte směrovací tabulku na každém směrovači a ověřte správnost nastavení.
Pro Huawei směrovače použijte příkaz:

```
[R1] display ip routing-table protocol ospf
```

pro Cisco směrovače:

```
R3#show ip route ospf
```

Nyní máte nakonfigurovanou celou síť a můžete vyzkoušet funkčnost multicastového směrování. Proveďte simulaci multicastového vysílání ze zdrojové adresy 10.0.3.3 (tedy ze směrovače R3) s cílovou adresou 225.1.1.1:

```
R3#ping
Protocol [ip]:
Target IP address: 225.1.1.1
Repeat count [1]: 100
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Interface [All]: fastethernet0/1
Time to live [255]:
Source address: 10.0.3.3
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 1, 100-byte ICMP Echos to 225.1.1.1, timeout is 2 seconds:
Packet sent with a source address of 10.0.3.3
..........
```

Zobrazte směrovací tabulky PIM protokolu na směrovači R2. Měly by v ní být 2 záznamy. První záznam (*, 225.1.1.1) se generuje po nastavení statické IGMP skupiny na rozhraní. Druhý záznam (10.0.3.3, 225.1.1.1) je vygenerován ve chvíli, kdy směrovač obdrží multicastový paket. Na ostatních směrovačích kromě R4 najdeme pouze druhý záznam, jelikož nemají nastavenou žádnou statickou IGMP skupinu.

```
[R2]display pim routing-table
VPN-Instance: public net
Total 1 (*, G) entry; 1 (S, G) entry

(*, 225.1.1.1)
Protocol: pim-dm, Flag: WC EXT
UpTime: 01:50:01
Upstream interface: NULL
Upstream neighbor: NULL
RPF prime neighbor: NULL
Downstream interface(s) information: None
(10.0.3.3, 225.1.1.1)
Protocol: pim-dm, Flag: EXT ACT
UpTime: 00:00:05
```

```
Upstream interface: Serial1/0/0
Upstream neighbor: 10.0.12.1
RPF prime neighbor: 10.0.12.1
Downstream interface(s) information:
Total number of downstreams: 1
1: GigabitEthernet0/0/0
Protocol: pim-dm, UpTime: 00:00:05, Expires:  -
```

V této úloze byl nakonfigurován multicastový směrovací protokol PIM v režimu Dense mode, nastavena statická IGMP skupina a prověřena funkčnost nastavení.

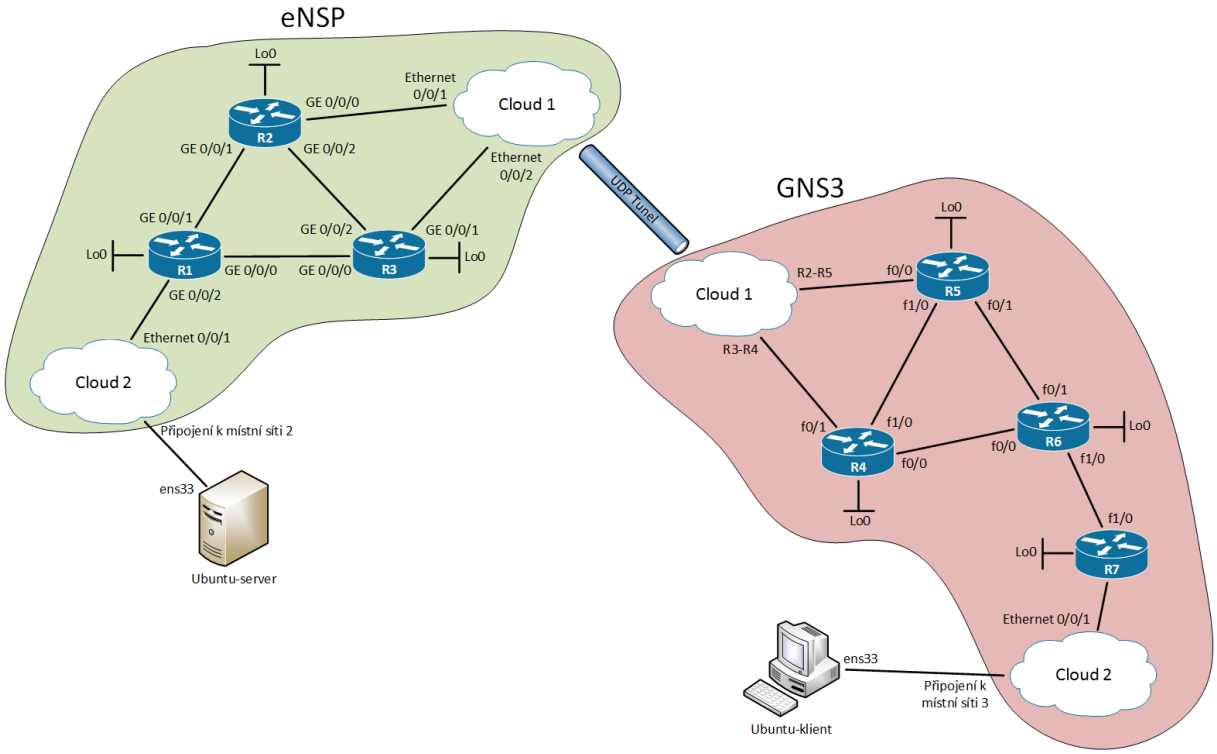
4.3 Lab 3 - Multicast, PIM Sparse mode

Tato úloha je obdobně jako Lab 2 - Multicast, PIM Dense mode koncipována tak, že část sítě je emulována v GNS3 a část v nástroji eNSP. Propojení obou sítí je realizováno nástojem Cloud, jímž oba nástroje disponují. V obou částech sítě bude konfigurován multicast se směrovacím protokolem PIM v režimu Sparse mode a ověřena jeho funkčnost.

4.3.1 Zadání a topologie

Zadání:

- V prostředí emulačního softwaru GNS3 a eNSP realizujte multicastové vysílání protokolem PIM v režimu Sparse mode.
- Směrovač R2 nakonfigurujte jako Rendezvous point.
- Uvažujte topologii dle obr. 4.10.
- Nejdříve konfigurujte část v simulátoru eNSP a až poté v GNS3.
- Dynamické směrování v zadané topologii realizujte protokolem OSPF.
- Pro propojení obou sítí využijte nástroj Cloud.
- Ověřte funkčnost multicastového směrování.



Obr. 4.10: Topologie laboratorní úlohy

4.3.2 Rozbor úlohy

V této úloze budete konfigurovat tři virtuální směrovače Huawei a čtyři směrovače Cisco. Propojení bude realizováno nástrojem Cloud. Mezi emulátory bude vytvořen UDP tunel. Na každém směrovači bude nakonfigurováno virtuální rozhraní Loopback, které bude sloužit pro identifikaci směrovače v rámci směrovacího protokolu OSPF.

Zařízení	Rozhraní	IP adresa	Adresa podsítě	Typ
R1	GE 0/0/0	10.0.13.1	10.0.13.0 /24	Huawei AR2220
	GE 0/0/1	10.0.12.1	10.0.12.0 /24	
	GE 0/0/2	192.168.10.100	192.168.10.0 /24	
	Lo0	10.0.1.1	10.0.1.1 /32	
R2	GE 0/0/0	10.0.25.2	10.0.25.0 /24	Huawei AR2220
	GE 0/0/1	10.0.12.2	10.0.12.2 /24	
	GE 0/0/2	10.0.23.2	10.0.23.0 /24	
	Lo0	10.0.2.2	10.0.2.2 /32	
R3	GE 0/0/0	10.0.13.3	10.0.13.0 /24	Huawei AR2220
	GE 0/0/1	10.0.34.3	10.0.34.0 /24	
	GE 0/0/2	10.0.23.3	10.0.23.0 /24	
	Lo0	10.0.3.3	10.0.3.3 /32	
R4	f0/0	10.0.46.4	10.0.46.0 /24	Cisco 2691
	f0/1	10.0.34.4	10.0.34.0 /24	
	f1/0	10.0.45.4	10.0.45.0 /24	
	Lo0	10.0.4.4	10.0.4.4 /32	
R5	f0/0	10.0.25.5	10.0.25.0 /24	Cisco 2691
	f0/1	10.0.56.5	10.0.56.0 /24	
	f1/0	10.0.45.5	10.0.45.0 /24	
	Lo0	10.0.5.5	10.0.5.5 /32	
R6	f0/0	10.0.46.6	10.0.46.0 /24	Cisco 2691
	f0/1	10.0.56.6	10.0.56.0 /24	
	f1/0	10.0.67.6	10.0.67.0 /24	
	Lo0	10.0.6.6	10.0.6.6 /32	
R7	f0/0	192.168.20.100	192.168.20.0 /24	Cisco 2691
	f1/0	10.0.67.7	10.0.67.0 /24	
	Lo0	10.0.7.7	10.0.7.7 /32	
Ubuntu-server	ens33	192.168.10.2	192.168.10.0 /24	VM Ubuntu 16.04
Ubuntu-klient	ens33	192.168.20.2	192.168.20.0 /24	VM Ubuntu 16.04

Tab. 4.4: Tabulka IP adres

Randezvous point bude na adrese 10.0.2.2 (směrovač R2). Budou také využity dva virtuální počítače, jeden jako zdroj multicastového provozu (streamované hudby) a druhý jako příjemce. Propojení virtuálních počítačů se simulovanou sítí bude opět realizováno nástrojem Cloud.

Multicast

Obecný popis a princip multicastového vysílání a IGMP protokolu je uveden v laboratorní úloze Lab 2 - Multicast, PIM Dense mode. V této úloze je uveden pouze popis multicastového směrovacího protokolu PIM v režimu Sparse mode.

PIM Sparse mode

Tento režim protokolu PIM vychází z opačné představy než režim Dense mode. Předpokládá, že klienti, kteří chtějí přijímat multicastový provoz, se v síti nacházejí velmi řídce. Pokud je PIM nastaven v tomto režimu, posílá multicastový provoz pouze směrovačům, které si o něj požádají. Neplýtvá se tak prostředky, které by musely být vynaloženy k přenosu multicastového provozu do všech sítí jako je tomu u Dense mode.

Režim Sparse mode vyžaduje, aby byl v síti nakonfigurován (automaticky nebo manuálně) tzv. Randezvous point (RP) - bod setkání. RP je směrovač v síti, o kterém musí vědět všechny ostatní směrovače, jelikož oznamuje zdroje multicastového provozu a vytváří cestu od zdroje ke členům skupiny. Princip protokolu je následující [31]:

- Zdroj multicastového provozu posílá do RP vícesměrové pakety.
- RP tyto vícesměrové pakety zahazuje, jelikož neobdržel žádost (PIM Join) od dalšího směrovače nebo lokálních hostitelů v síti, že má zájem přijímat multicastový provoz.
- Ve chvíli kdy má klient zájem přijímat multicastový provoz, vyšle ke směrovači žádost (Membership report).
- Směrovač odešle do RP zprávu PIM Join s žádostí o přijímání multicastového provozu.
- RP začne posílat multicastový provoz pro danou skupinu (uvedena ve zprávě Membership report a následně PIM Join) směrem ke směrovači, který jej žádal.

4.3.3 Postup

Proveďte zapojení obou částí sítě podle zadané topologie.

Směrovače pojmenujeme podle informací v topologii [17].

```
[Huawei] sysname R1
[R1]
```

```
Router# hostname R3
R3#
```

Nástroj Cloud nastavte v emulátoru eNSP obdobně, jako v Lab 2 - Multicast, PIM Dense mode. Důležité je především shodné nastavení veřejných (public) portů. Čísla vnitřních portů (internal) jsou generována automaticky a proto se může stát, že nebudou odpovídat portům zobrazených na obrázku. Následně je třeba nastavit mapování portů. Platí, že jednomu veřejnému portu je přidělen jeden interní. Jelikož je to obousměrná cesta, zaškrtněte pole "Two-way Channel".

V emulátoru GNS3 nastavte nástroj Cloud obdobně jako v Lab 2 - Multicast, PIM Dense mode. Zde si můžeme čísla vnitřních a vnějších portů zvolit. V tomto případě se již předpokládá, že cesta je oboustranná a tudíž není třeba nastavovat nic dalšího.
Pokud špatně nastavíte nástroje Cloud, nebude fungovat propojení mezi oběma částmi sítě.

IP adresy přidělte a nastavte zařízením dle tabulky 4.4.

Příklad konfigurace síťového rozhraní na Cisco směrovači [17]:

```
R5# configure terminal
R5(config)# interface fastethernet0/0
R5(config-if)# ip address 10.0.45.5 255.255.255.0
R5(config-if)# no shutdown
R5(config-if)# exit
```

Příklad konfigurace síťového rozhraní na Huawei směrovači:

```
[R1] interface fastethernet0/0
[R1] ip address 10.0.12.1 255.255.255.0
[R1] quit
```

Pro unicastové směrování je v této úloze použit OSPF protokol. OSPF je v dnešní době nejvyužívanější IGP protokol a proto ho využijeme i v této úloze.

Jako router-id použijte IP adresu rozhraní Loopback0.

Ukázka konfigurace OSPF na Huawei směrovači:

```
[R3] ospf 1 router-id 10.0.3.3
[R3-ospf-1] area 0
[R3-ospf-1-area-0.0.0.0] network 10.0.3.3 0.0.0.0
[R3-ospf-1-area-0.0.0.0] network 10.0.34.0 0.0.0.255
[R3-ospf-1-area-0.0.0.0] network 10.0.13.0 0.0.0.255
[R3-ospf-1-area-0.0.0.0] network 10.0.23.0 0.0.0.255
```

Ukázka konfigurace OSPF na Cisco směrovači:

```
R5(config)# router ospf 1
R5(config-router)# router-id 10.0.5.5
R5(config-router)# network 10.0.5.5 0.0.0.0 area 0
R5(config-router)# network 10.0.25.0 0.0.0.255 area 0
R5(config-router)# network 10.0.45.0 0.0.0.255 area 0
R5(config-router)# network 10.0.56.0 0.0.0.255 area 0
```

Po konfiguraci OSPF protokolu zobrazte směrovací tabulku na každém směrovači s ověřte správnost nastavení.

Pro Huawei směrovače použijte příkaz:

```
[R1] display ip routing-table protocol ospf
```

Pro Cisco směrovače:

```
R3#show ip route ospf
```

Po konfiguraci všech síťových rozhraní proveďte kontrolu konektivity mezi směrovači, abyste ověřili správnost konfigurace jak síťových prvků tak nástrojů Cloud.

Multicast

Nejprve je třeba povolit multicastové směrování paketů globálně na celém směrovači. Následně musíte na každém rozhraní definovat multicastový směrovací protokol a jeho režim (PIM v režimu Sparse mode)

Příklad konfigurace multicastu na Huawei směrovači R3:

```
[R3] multicast routing-enable
[R3] interface GigabitEthernet 0/0/2
[R3-GigabitEthernet0/0/2] pim sm
[R3-GigabitEthernet0/0/2] interface GigabitEthernet 1/0/0
[R3-Serial1/0/0] pim sm
[R3-Serial1/0/0] interface GigabitEthernet 3/0/0
[R3-Serial3/0/0] pim sm
```

Příklad konfigurace multicastu na Cisco směrovači R5:

```
R5(config)#ip multicast-routing
R5(config)#interface fastEthernet 0/1
R5(config-if)#ip pim sparse-mode
R5(config-if)#interface fastEthernet 0/1
R5(config-if)#ip pim sparse-mode
R5(config-if)#interface fastEthernet 0/1
R5(config-if)#ip pim sparse-mode
```

Proveďte kontrolu, zda je protokol PIM aktivován na všech požadovaných rozhraní:

```
[R3]display pim interface
VPN-Instance: public net
Interface           State NbrCnt HelloInt   DR-Pri     DR-Address
GE0/0/0             up    1      30         1          10.0.13.3       (local)
GE0/0/1             up    1      30         1          10.0.34.4
GE0/0/2             up    1      30         1          10.0.23.3       (local)
Loop0               up    0      30         1          10.0.3.3        (local)
```

PIM je aktivován na čtyřech rozhraních v rámci směrovače R3 a ke každému rozhraní je připojen jeden soused (NbrCnt) kromě rozhraní Loopback0, které je pouze virtuální.

Můžete zobrazit seznam sousedů, kteří mají navázán vztah sousednosti se směrovačem R3 v rámci protokolu PIM

```
[R3]display pim neighbor
VPN-Instance: public net
Total Number of Neighbors = 3
```

```
Neighbor        Interface           Uptime   Expires  Dr-Priority  BFD-Session
10.0.13.1       GE0/0/0             00:03:44 00:01:35 1            N
10.0.23.2       GE0/0/1             00:03:31 00:01:25 1            N
10.0.34.4       GE0/0/2             00:03:50 00:01:28 1            N
```

Uptime značí čas od ustanovení stavu sousednosti a Expirates čas, za který tento stav vyprší, pokud od souseda nepříjde Hello paket.

V teoretické části úlohy bylo uvedeno, že PIM v režimu Sparse mode využívá tzv. Randezvou Point (RP). RP je místo (směrovač), kde se setkávají zdroje a příjemci multicastového provozu. RP oznamuje zdroje a vytváří cestu od zdroje ke členům skupiny. Zdroj vysílá multicastový provoz na tento bod a ten následně rozposílá provoz příjemcům.

V této úloze bude Randezvous point nastaven staticky na každém směrovači v simulované síti. RP bude směrovač R2 (IP adresa rozhraní Loopback0, tedy 10.0.2.2). Lze ovšem i nastavit, aby byl volen automaticky.

Příklad konfigurace statického RP na Huawei směrovači R3:

```
[R3] pim
[R3] static-rp 10.0.2.2
```

Příklad konfigurace statického RP na Cisco směrovači R5 [29]:

```
R5(config)#ip pim rp-address 10.0.2.2
```

IGMP protokol v této úloze není potřeba konfigurovat. Příjemce multicastového provozu (Ubuntu-klient) je připojen ke směrovači R7 (Cisco). Na Cisco směrovačích se IGMP protokol zapne automaticky ve chvíli, kdy aktivujeme na rozhraní protokol PIM.

Testování

Zapněte virtuální počítače, přihlaste se (uživatel student, heslo student) a vyzkoušejte ping do simulované sítě (IP adresa, maska i brána jsou přednastaveny). Spusťte VLC media player na Ubuntu-server a nastavte streamování připravené hudební nahrávky:

- Media → Stream
- Vyberte připravenou nahrávku → tlačítko Add, nahrávka je umístěna v adresáři /home/student/Music → klikněte na tlačítko Stream
- Potvrďte výběr nahrávky → Next
- Vyberte New Destination - RTP/MPEG Transport Stream a přidejte tlačítkem Add
- Vyplňte multicastovou IP adresu - 239.1.1.1. Zapamatujte si tuto IP adresu a předvyplněný port → Next
- Zaškrtněte položku Active Transcondig a vyberte Audio - MP3 → Next
- Zaškrtněte položku Stream all elementary streams a Genereate stream outpus string doplňte do následujícího tvaru:

```
:sout=#transcode{vcodec=none,acodec=mp3,ab=128,channels=2,samplerate=44100,
ttl=20} :sout-all :sout-keep
```

- Nastavení dokončíte kliknutím na tlačítko Stream. Kliknutím se aktivuje vysílání multicastového provozu s cílovou adresou 239.1.1.1

Nyní je nastavený zdroj vysílání. Na virtuálním počítači Ubuntu-klient zapněte VLC media player a nastavte ho na přijímání streamu:

- Media → Open Network Stream
- Do pole Network URL vyplňte multicastovou IP adresu a port ve tvaru:

```
rtp://239.1.1.1:5004
```

- Přehrávání spustíte tlačítkem Play

Pokud je vše správně nastaveno, uslyšíte hudební stream vysílaný počítačem Ubuntu-server. V případě problémů lze využít analyzátor síťového provozu Wireshark.

V této úloze byl nakonfigurován multicast se směrovacím protokolem PIM v režimu Sparse mode a následně otestována funkčnost na reálném streamování hudby a jejího příjmu.

Vyhodnocení

Cílem této práce byla analýza možností propojení simulátorů a emulátorů síťových prostředí s externí sítí (fyzická či také virtualizovaná). Pro tyto účely jsem po dohodě s vedoucím práce zvolil čtyři simulační nástroje - GNS3, Cisco Packet Tracer, Huawei eNSP a Cisco VIRL. Cisco VIRL nebyl otestován z důvodu jeho zpoplatnění. Této analýze a následnému porovnání se věnuje druhá kapitola.

Jako první jsem testoval simulátor Packet Tracer. Neumožňuje propojení s externí sítí. Jako jediný z testovaných simulátorů síťové prvky skutečně pouze simuluje. V praxi to má za následek nefunkčnost některý konfiguračních příkazů, které ve fyzických zařízeních podporovány jsou. Tento simulátor je velmi svázán s programem Cisco Networking Academy a je vhodným vzdělávacím nástrojem k pochopení fungování datových sítí. Nejvhodnější se pro účely simulací datových sítí jeví GNS3, který je zdarma a po dohodě s vedoucím práce jsem v něm navrhl laboratorní úlohy. Jeho nevýhodou je nutnost disponovat obrazy operačního systému Cisco IOS. Tato nevýhoda je částečně kompenzována připravenými apliancemi síťových prvků. K tomu, abychom je mohli využívat, musíme mít stažený oficiální virtuální počítač s připravenou instalací softwaru GNS3. Pomocí nástroje Cloud lze GNS3 propojit s externí sítí. Pro návrh některých laboratorních úloh jsem využil i emulační nástroj eNSP. Umožňuje propojení virtualizované sítě s externí (fyzická případně také virtuální). Vzhledem k tomu, že ho vyvíjí společnost Huawei, lze simulace provádět pouze na zařízeních od tohoto výrobce a výběr zařízení nelze měnit. Cisco VIRL je platforma distribuovaná především jako obraz virtuálního počítače určeného pro hypervisory od společnosti VMWare. Pracuje na principu klient-server. Síťové prvky jsou emulovány a k dispozici je též podpora propojení s jinou sítí mimo platformu. K dispozici jsou řádně licencované operační systémy IOS. Nechybí ani podpora vysoce výkonných přepínačů řady Nexus. Tento nástroj ocení především odborníci v oboru, kteří potřebují analyzovat složité topologie.

Vytvořil jsem výukové pracoviště složené ze tří virtuálních počítačů a aktivních síťových prvků od společnosti Cisco. Toto pracoviště jsem podrobně popsal v kapitole 3. Jelikož je umístěno převážně ve virtuálním prostředí, je zaručena vysoká míra flexibility a přizpůsobení daným potřebám.

Pro vytvořené výukové pracoviště jsem navrhl tři laboratorní úlohy zaměřené na směrovací protokol OSPF a Multicast. V úlohách jsem kladl důraz na využití propojení mezi virtuální a fyzickou či jinou sítí a v případě potřeby lze tyto úlohy snadno modifikovat např. využitím více fyzických zařízení.

Literatura

[1] Cisco Virtual Internet Routing Lab Personal Edition (VIRL PE) 20 Nodes. https://learningnetworkstore.cisco.com/virtual-internet-routing-lab-virl/cisco-personal-edition-pe-20-nodes-virl-20, [Online; citováno 2018-03-26].

[2] Dokumentace k programu GNS3. https://gns3.com/support/docs, [Online; citováno 2017-10-15].

[3] GNS3 Marketplace. https://www.gns3.com/marketplace, [Online; citováno 2018-03-24].

[4] Grafické prostředí nástroje VM Maestro. http://www.showconfig.net/wp-content/uploads/2015/07/virl_interface.jpg, [Online; citováno 2018-03-24].

[5] Huawei Enterprise Network Simulation Platform. http://support.huawei.com/enterprise/en/network-management/ensp-pid-9017384/, [Online; citováno 2017-10-17].

[6] Návrh rozmístění fyzických zařízení v rackové skříni. http://magiken.com/magiken-lab/2017/01/09/cisco-packet-tracer%E5%88%A9%E7%94%A8%E6%89%8B%E5%BC%95%E3%81%8D4/, [Online; citováno 2018-03-24].

[7] OSPF Stub Areas. https://networkingjournalblog.wordpress.com/2016/09/06/ospf-stub-areas/, [Online; citováno 2017-09-20].

[8] Bouška, P.: TCP/IP - skupinové vysílání IP Multicast a Cisco. https://www.samuraj-cz.com/clanek/tcpip-skupinove-vysilani-ip-multicast-a-cisco/, [Online; citováno 2017-11-10].

[9] Byoung Kyu Choi, D. K.: *Modeling and Simulation of Discrete Event Systems*. Hoboken: Wiley, 2013, ISBN 9781118732854.

[10] Carroll, B.: Cisco VIRL vs. GNS3 – How They Compare. http://globalconfig.net/cisco-virl-vs-gns3-compare/, [Online; citováno 2018-03-26].

[11] Charvát, K.: Diskrétní simulace v MS Excel. https://vskp.vse.cz/15760_Diskr, [Online; citováno 2018-04-03].

[12] Chung, C. A.: *Simulation modeling handbook: a practical approach*. Boca Raton: CRC Press, 2004, ISBN 0849312418.

[13] Dave HUCABY, S. M.: *Konfigurace směrovačů Cisco: [autorizovaný výukový průvodce : podrobný přehled příkazů, protokolů a nastavení]*. Brno: Computer Press, 2004, ISBN 80-722-6951-8.

[14] Dlouhý, M.: *Simulace podnikových procesů*. Praha: Computer Press, 2011, ISBN 9788025134498.

[15] Dorda, M.: Generování pseudonáhodných čísel při simulaci. http://homel.vsb.cz/~dor028/Aplikace_4.pdf, [Online; citováno 2018-04-01].

[16] Dorda, M.: Úvod do modelování a simulace systémů. http://homel.vsb.cz/~dor028/Aplikace_2.pdf, [Online; citováno 2018-04-03].

[17] EMPSON, S.: *CCNA kompletní přehled příkazů: autorizovaný výukový průvodce*. Brno: Computer Press, 2009, ISBN 978-802-5122-860.

[18] Fishman, G. S.: *Discrete-Event Simulation Modeling, Programming, and Analysis*. New York, NY: Springer New York, 2001, ISBN 9781475735529.

[19] Fuszner, M.: GNS3 Tutorial. `https://www.csd.uoc.gr/~hy435/material/GNS3-0.5-tutorial.pdf`, [Online; citováno 2017-03-04].

[20] Grygárek, P.: IP Multicast. `http://www.cs.vsb.cz/grygarek/SPS/lect/multicast/multicast.html`, [Online; citováno 2017-11-03].

[21] Hampl, P.: Prezentace z předmětu Teorie hromadné obsluhy. `https://moodle.fel.cvut.cz`, [Online; citováno 2018-04-01].

[22] Ivan Křivý, E. K.: *Simulace a modelování*. Ostrava: Ostravská univerzita, Přírodovědecká fakulta, 2001, ISBN 9788070428092.

[23] Jiří Cendelín, E. K.: *Modelování a simulace*. Plzeň: Západočeská univerzita, 1994, ISBN 8070821655.

[24] Khan, R.: Cisco Vs Huawei CLI Commands. `http://www.networksheaven.com/tutorials/cisco-vs-huawei-cli-commands`, [Online; citováno 2017-10-25].

[25] Kořínková, M.: Simulace výrobního procesu. `https://vskp.vse.cz/id/1601`, [Online; citováno 2018-04-01].

[26] Larionova, V.: Diskrétní simulace pro metodu BORM v nástroji OpenCABE. `https://dspace.cvut.cz/handle/10467/63143`, [Online; citováno 2018-04-03].

[27] Neumann, J. C.: *The Book of GNS3 : Build Virtual Network Labs Using Cisco, Juniper, and More*. No Starch Press, 2015, ISBN 978-1-59327-695-9.

[28] Peringer, P.: Modelování a simulace. `http://www.fit.vutbr.cz/study/courses/IMS/public/prednasky/IMS.pdf`, [Online; citováno 2018-04-03].

[29] Perkin, R.: Multicast for CCIE – Lesson 1 – Static RP. `http://www.rogerperkin.co.uk/multicast/multicast-for-ccie-static-rp/`, [Online; citováno 2017-11-28].

[30] Raio, M.: Connecting Huawei eNSP to GNS3. `https://gns3.com/news/article/connecting-huawei-ensp-to-gns3`, [Online; citováno 2017-11-02].

[31] Rus HEALY, N. M., Wendell ODOM: *Směrování a přepínání sítí: autorizovaný výukový průvodce*. Brno: Computer Press, 2009, ISBN 978-80-251-2520-5.

[32] Udo W. Pooch, J. A. W.: *Discrete event simulation: a practical approach*. Boca Raton: CRC Press, 1992, ISBN 9780849371745.

[33] Vangheluwe, H.: Discrete Event Modelling and Simulation. `http://www.cs.mcgill.ca/~hv/classes/MS/discreteEvent.pdf`, [Online; citováno 2018-04-05].

[34] Wang, J.: Why Cisco VIRL is Better Than GNS3. `https://www.speaknetworks.com/cisco-virl-better-gns3/`, [Online; citováno 2018-03-26].

[35] Welsh, C.: *GNS3 Network Simulation Guide*. Packt Publishing, 2013, ISBN 978-1-78216-081-6.

[36] Zouhar, P.: Generátor náhodných čísel. `https://www.vutbr.cz/www_base/zav_prace_soubor_verejne.php?file_id=27715`, [Online; citováno 2018-04-01].

Seznam příloh

A Struktura CD