Univerzita Hradec Králové
Fakulta informatiky a managementu
Katedra informačních technologií

Simulátory provozu na počítačových sítích

Bakalářská práce

Autor: Jakub Slavíček
Studijní obor: Aplikovaná informatika

Vedoucí práce: Ing. Karel Mls, Ph.D.

Hradec Králové 04 2020

Prohlášení:

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

vlastnoruční podpis

V Hradci Králové dne 9.5.2020

Poděkování:

Rád bych tímto poděkoval svému vedoucímu práce, Ing. Karlu Mlsovi, Ph.D., za velkou ochotu, věnovaný čas a užitečné rady při realizaci této práce. Dále bych rád poděkoval své přítelkyni, která mi byla velkou oporou, a také celé své rodině za projevenou trpělivost a podporu, které se mi dostalo nejen během psaní této bakalářské práce, ale i během celého studia.

Anotace

Tato bakalářská práce se zabývá úvodem do síťové problematiky, vysvětlení základních pojmů. Dále popisuje instalaci a manipulaci s existujícími simulátory počítačových sítí z pohledu malé sítě, které jsou ve výsledku testovány a porovnány mezi sebou. Jedná se o přehled nejpoužívanějších a nejzajímavějších síťových simulátorů, které jsou v současné době k dispozici na softwarovém trhu. Dále poskytuje manuál pro používání těchto nástrojů, od stahování a instalace po vytvoření simulace ukázkové malé sítě.

Klíčová slova

síťové útoky, síťová bezpečnost, DoS, PAN, LAN, WAN, MAN, GAN, simulátory počítačových sítí, počítačová síť

Title

Traffic simulators for computer networks

Annotation

The bachelor thesis deals with an introduction to problematice of computer network, explanation of basic terms. The thesis also describes the installation and manipulation of existing data flow generators on a computer network from the perspective of a small network, which is ultimately tested and compared between themselves. It is an overview of the most used and interesting network simulators currently available on the software market. It also provides a manual for using these tools, from downloading and installing to creating a sample small network simulation.

Keywords

network attacks, network security, DoS, PAN, LAN, WAN, MAN, GAN, data flow generators, computer network

Obsah

Seznam zkratek a pojmů

Pro sjednocení oborové komunikace a lepší srozumitelnosti je potřeba nejprve upřesnit základní pojmy a vysvětlit zkratky, které se v bakalářské práci budou objevovat.

Carrier Sense Multiple Access with Collision Detection (CSMA-CD) je přístupová metoda u ethernetových sítí. Tato metoda se snaží předcházet tomu, aby do sítě vysílalo více počítačů najednou, jelikož by pak docházelo k rušení.

Cisco Configuration Professional (CCP nebo také Cisco CP) je nástroj pro správce sítí. Nabízí uzamčení routeru na jedno kliknutí, inovativní funkci hlasového a bezpečnostního auditu pro kontrolu a doporučení změn v konfiguraci routeru a mnoho dalších nástrojů pro zjednodušení a zrychlení práce.

Cisco Service Device Manager (CISCO SDM) zjednodušuje konfiguraci routeru a zabezpečení pomocí inteligentních průvodců, což zákazníkům umožňuje rychle a snadno nasadit, konfigurovat a monitorovat přístupový router Cisco, aniž by museli znát rozhraní příkazového řádku softwaru Cisco IOS.

Domain Name System (DNS) je internetový standard zahrnutý v TCP/IP. DNS slouží k překladu jmen objektů na IP adresy či jiné zdrojové záznamy. Jména objektů se označují jako doménová jména (domain name) a nejčastěji se jedná o jména hostitelů (hostname), jsou to alfanumerické řetězce, které jsou lépe zapamatovatelné než IP adresy.

Fotonické služby představují soubor pokročilých služeb optických sítí, které umožnují čistě optický přenos bez konverze na elektrický signál. Jsou tak určeny pro nejnáročnější aplikace.

IP Adresa je logická adresa zařízení v síti. Skládá se ze 4 částí (oktetů) a každá část má 8 bitů, které se oddělují tečkou. Adresy se zapisují v dekadické či binární formě. Dekadická forma je lepší pro čitelnost, ale binární je lepší pro výpočty. Teoretický adresní rozsah je od 0.0.0.0 do 255.255.255.255

ISO/OSI je referenční model a definuje sedm vrstev pro počítače komunikující v síti. Vrstvy jsou řazeny podle vztahu k systému a k uživateli – nejnižší vrstvy pracují na hardwarové úrovni a nejvyšší pak maximálně komunikují s uživatelem.

Maska podsítě pomáhá k rozdělení sítě na podsítě. Z masky podsítě lze zjistit, jaká část je síťová (adresa sítě, broadcast) a která je určena pro hosty. Maska podsítě se zapisuje stejně jako IP adresa, pouze s rozdílem, že pokud se zde z pravé strany objeví

nula musí již doprava pokračovat samé nuly. Jedničky v masce jsou část, která je pro danou podsíť stále stejná a říká se jí síťová část. Nuly jsou část, která je proměnná a určuje adresu hosta v dané podsíti a je to část hosta. Příkladem jednoduché masky je 255.255.255.0, která určuje, že prvních 24 bitů adresy je síťová část a posledních 8 bitů je část hosta.

Microsoft Office (MS Office) je balík, který obsahuje kancelářské programy jako především jsou Word pro psaní dokumentů, Excel jako tabulkový procesor, či PowerPoint pro prezentace.

Model je v oblasti počítačů jde o matematickou nebo grafickou napodobeninu objektů reálného světa. Modely mohou sloužit jednak k simulaci některých jevů v abnormálních nebo dlouhodobých podmínkách.

Simulace je napodobení procesu nebo objektu pomocí matematického popisu. Simulace umožňuje pomocí změny vstupních nebo jiných podmínek zkoumat změny a varianty chování objektu a předpovídat tak jeho reálnou činnost. Počítač je ideálním prostředkem pro provádění simulací vzhledem k tomu, že simulování reálných dějů vyžaduje množství ovlivňujících faktorů a jejich neurčitosti obrovskou výpočetní sílu. [3]

Systém je skupina počítačů a periférií, navzájem propojených v síti.

TCP/IP je podobný model jako předchozí ISO/OSI, ale je pouze čtyřvrstvý. Obsahuje vrstvu síťového rozhraní, síťovou, transportní a aplikační.

Virtual local area network (VLAN) je virtuální síť typu LAN

Virtual private network (VPN) obecně znamená systém propojení počítačů do zabezpečené soukromé sítě i tehdy, když jsou na různých místech v internetu. Mezi počítači se vytvoří šifrovaný tunel, kterým teče veškerá komunikace mezi počítači ve virtuální síti. S takovým využitím VPN se lze nejčastěji setkat v zaměstnání, když se ze vzdáleného místa zaměstnanec chce bezpečně připojit do firemní sítě.

Visual Basic (VBA) je objektově orientovaný programovací jazyk, který se převážně používá v Excelu. Primárně umožňuje vytváření uživatelsky definovaných funkcí, automatizaci procesů, či různé výpočty. [24]

Seznam obrázků

Seznam tabulek

1 Úvod

Informační technologie se v dnešní době objevuje skoro všude kolem nás. Informační technologii obsahují především mobilní telefony, počítače, notebooky, ale už i televize, moderní stolní budíky i hodinky. Informační technologie se z profesního hlediska dělí na dvě strany. První strana je, kde lidé používají databáze, programují software, a na straně druhé se lidé starají o počítačovou síťovou infrastrukturu. Tato bakalářská práce se bude zabývat druhou stránkou informační technologie, a to počítačovou sítí.

S rozvojem informačních technologií, a především počítačových sítí, došlo k masivnímu šíření sdílení informací pomocí informačních technologií. Avšak díky této vymoženosti se otevřelo nové pole působnosti pro útočníky, v tomto případě jsou to konkrétněji kybernetičtí útočníci. Počítačové sítě, po kterých jsou dnes informace hojně sdíleny, se staly obětí nejrůznějších útoků, jejichž cílem je tyto informace získat. Důvodem mohou být konkurenční boje společností, krádež či pouhá pomsta nespokojeného zaměstnance.

Mezi základní protiopatření před kyberútokem je velmi důležité mít nainstalovaný antivirový software. Antivirový software je bezpečností software, který zajišťuje bezpečnost pomocí detekování škodlivých aplikací a případně jejich pozdější odstranění z počítače. Většinu času provozu antivirový software provádí preventivní opatření a skenuje oblasti disků nebo každého stahovaného souboru do zařízení. Bohužel si ale často uživatelé myslí, že nainstalovaný antivirový software stačí ke stoprocentní ochraně svého zařízení a poté se diví, že mohli být napadeni právě oni. Antivirový software zastupuje pouze „*Objevování známých škodlivých vzorců a špatného chování v programech. Objevování známých škodlivých vzorců v dokumentech a webových stránkách. Objevování známých škodlivých vzorců v síťových paketech. Snaží se přizpůsobit a objevit nová špatná chování nebo vzorce založené na zkušenostech s dříve známými*.“ [10] Proto dochází ke školení na téma o bezpečnosti při práci na počítači či jiném koncovém zařízení sítě, a to především v zaměstnáních. [10]

S ukázkami, jak útoky fungují a jak jim předcházet úzce souvisejí simulátory datových toků, které se staly nepostradatelnou metodou při tvorbě počítačových sítí. Zde je možné vytvořit topologii sítě a na ní zkoušet různé modelové situace, ať už pro

produktivitu sítě, tak i bezpečnost. Je možné si vyzkoušet i jak útokům předcházet, či když útok nastane, jak rychle znovu nastartovat síť po výpadku. Díky stálé potřebě růstu počítačových sítí je možné s přispěním zvyšujícího se výkonu hardwarových prvků tvořit rychlejší, přesnější a složitější síťové topologie. A k tomu jsou užitečným pomocníkem síťové simulátory jako nástroje pro jejich modelování a testování.

Při zkoumání chování sítí, vývoji nových síťových protokolů a testování nových postupů nelze také vždy pracovat na fyzických zařízeních a je třeba použít simulátory. Důvodem je častá neproveditelnost testovacích scénářů v reálném prostředí z důvodu vysokých finančních nákladů, společně s mobilitou a umístěním testovaných objektů. Navíc většina měření není opakovatelná a vyžaduje vysokou spolehlivost. I zde mohou simulátory výrazně pomoci.

Teoretická část této práce bude popisovat rozdělení počítačové sítě, typy síťového hardwaru a softwaru. V kapitole 5.2 budou popsané dopady kybernetických útoků a obecné informace o útocích. V kapitole 5.3 bude popsáno několik konkrétních příkladů útoků. Nakonec v kapitole 6 bude představena vzorová síťová topologie a k ní půdorys objektu se zobrazenými koncovými zařízeními a síťovými prvky.

V praktické části budou popsány vybraní zástupci simulátorů datových toků, ukázán postup jejich instalace, popsané základní prostředí aplikace a vytvoření topologie sítě. Na závěr popisu každého simulátoru bude krátké shrnutí, které bude obsahovat výhody a nevýhody daného simulátoru. Na konci praktické části bakalářské práce bude provedeno porovnání vybraných simulátorů podle předem stanovených kritérií.

2 Cíl práce

Cílem bakalářské práce je porovnání a testování vlastností a funkčnosti existujících generátorů datových toků na počítačových sítích z pohledu zabezpečení malé sítě.

V rámci praktické části bude představena instalace generátorů datových toků a manipulace s nimi. Na konci práce bude provedeno shrnutí vlastností daných simulátorů a jejich porovnání pomocí předem definovaných kritérií.

3 Metodika zpracování

V rámci bakalářské práce byly prohledány informační zdroje na internetu za účelem nalezení dostupných simulátorů počítačové sítě, ze kterých byly dále vybráni typičtí zástupci dané skupiny softwarových nástrojů. Na vybraných simulátorech je v praktické části popsána jejich instalace, práce s nimi, a nakonec provedeno vícekriteriální porovnání za pomoci testovacích kritérií. Konkrétní reprezentanti skupin simulátorů byli vybráni podle předem stanovených parametrů.

Bakalářská práce je rozdělena na úvodní část, kde jsou popsány počítačová sítě, síťový hardware a software. V navazujících kapitolách jsou diskutovány známé typy útoků na počítačovou síť, jejich dopady s konkrétními příklady a způsoby preventivní obrany. V šesté kapitole je popsána topologie sítě a praktické využití dané sítě v reálném světě. Další kapitoly jsou zaměřeny na popis konkrétních vybraných simulátorů počítačové sítě, jejich instalace, popis prostředí, postup, jak vytvořit síťovou topologii v dané aplikaci a krátké zhodnocení dané aplikace. V závěru bakalářské práce je provedeno porovnání vybraných simulátorů podle předem stanovených kritérií.

V textu jsou přednostně používány původní názvy zařízení a pojmů. To znamená, že názvy jsou primárně v anglickém jazyce a v případně potřeby jsou pro srozumitelnost nebo pro občasné vysvětlení daného názvu přeloženy do českého jazyka.

Nedílnou částí teoretické části práce je literární rešerše diskutované problematiky.

4 Počítačová síť

4.1 Úvod do počítačové sítě

Počítačová síť vznikne v momentě, když se dohromady propojí minimálně dva počítače pomocí telekomunikačního systému za účelem sdílení dat, programů nebo periferních zařízení. Propojení počítačů je realizováno pomocí speciálních kabeláží nebo bezdrátově. V praxi je nejrozšířenější síť založena na technologii Ethernet a používá protokol TCP/IP. [21]

Síť se může rozdělit podle více kritérií. Nejčastěji se však dělí podle rozlehlosti, od nejmenší po nejrozsáhlejší to jsou PAN, LAN, MAN, WAN a nejrozsáhlejší je síť GAN. Pro praktickou činnost není dělení sítí podle velikosti tak důležité, navíc může být obtížné rozhodnout kde končí síť LAN a začíná MAN, či kde síť MAN přechází do sítě WAN. [4]

Síť PAN neboli Personal Area Network je osobní síť s dosahem pouze několik metrů. Tyto sítě jsou používané pro propojení osobních zařízení typu mobilní telefon, laptop nebo PDA. Pro osobní počítačovou síť je nejdůležitější odolnost vůči rušení a nízká spotřeba energie. O něco větší je síť LAN neboli Local Area Network, která pokrývá malé geografické území (domácnost, malé firmy). Síť LAN může být kabelová i bezdrátová. Standardně se pro kabelovou LAN používá Ethernet a pro bezdrátovou je to Wi-Fi. *„První sítě LAN vznikly na konci 70. let 20. století. Sloužily k vysokorychlostnímu propojení sálových počítačů.“* [20] Síť MAN neboli Metropolitan Area Network je velmi podobná síti LAN, ale tato síť mívá velmi vysokou rychlost a propojuje jednotlivé LAN sítě. Síť MAN nepřekračuje jednotlivé hranice města či metropolitní oblasti. Mnohem rozsáhlejší síť je WAN neboli Wide Area Network, která pokrývá dlouhé vzdálenosti za pomoci telefonních linek, optických kabelů nebo satelitních spojení. Nakonec je zde nejrozsáhlejší síť GAN neboli Global Area Network. Z jmenovaných sítí je nejrozsáhlejší, především díky použití satelitů a bezdrátových technologií a tím se stává prakticky neomezená. Základní přenosové rychlosti bývají v řádech Mb/s. Klasickým příkladem sítě GAN je právě Internet. [20]

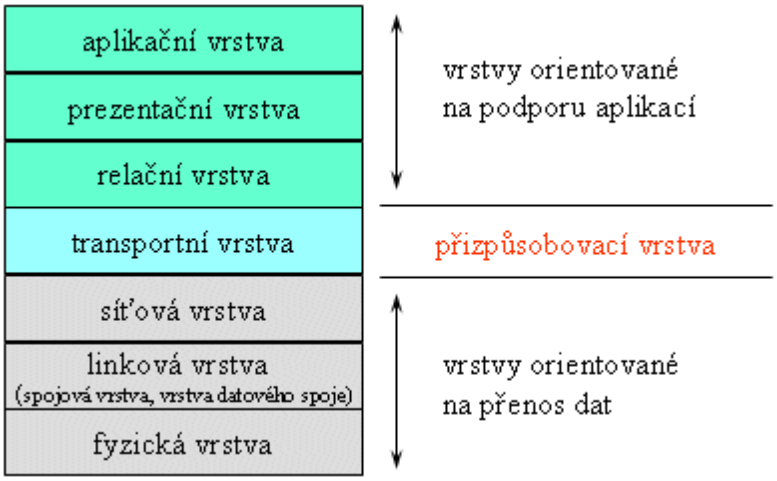
Od roku 2015 začíná budování nového internetového připojení a tím je satelitní síť StarLink od Elona Muska a firmy SpaceX. Firma SpaceX plánuje vyslat celkem 11 924 družic, které budou rozmístěny do určitých vzdáleností od Země. Nejbližších 7518

satelitů bude přibližně ve výšce 320 km na zemským povrchem, o něco výše je v plánu dalších 1584 satelitů, a to ve výšce 550 km. Poslední část, a to nejvzdálenějších 2825 satelitů, ve výšce 1110–1325 km. V dubnu 2020 firma SpaceX zažádala o změnu vzdálenosti nejvzdálenějších satelitů, a to na 540–570 km od Země, k čemuž zatím nebylo rozhodnuto. Koncový uživatel se k síti StarLink bude připojovat pomocí speciálního terminálu s anténou. Potřebné k připojení bude pouze, aby terminál měl přímý výhled na oblohu a přívod elektrické energie, přičemž terminál se bude moci pohybovat. To znamená, že terminál bude možné připojit i na auto, loď nebo letadlo. SpaceX avizuje začátek komerčního poskytování služby telekomunikačním firmám a dalším zákazníkům v druhé polovině roku 2020. V tomto momentě (konec dubna 2020) bylo vysláno celkem 360 satelitů sítě StarLink pro testovací a komerční použití. [25]

4.2 Typy síťového hardwaru

4.2.1 Model ISO/OSI

Hlavním účelem v počítačové síti je vzájemné propojování jednotlivých koncových zařízení. V dnešních sítích je IP protokol používán jako implementace ISO (International Standards Organization) standardu OSI (Open Systems Interconnection). Vzhledem ke složitosti problémů je síťová komunikace rozdělena do sedmi vrstev, jak je vidět na Obrázek 1, kde nejnižší tři vrstvy poskytují paketově orientovaný přenos uživatelských dat. Poté je zde transportní vrstva, která je také jinak nazývaná jako přizpůsobovací vrstva, a nakonec model obsahuje nejvyšší tři vrstvy, které se zaměřují na podporu aplikací. Princip spočívá v tom, že vyšší vrstva převezme úkol od podřízené vrstvy, zpracuje jej a předá vrstvě nadřízené. Při praktické práci se sítí není tento model zcela využíván. Umožňuje však pochopit principy práce síťových prvků a zároveň patří k základní terminologii sítí. [13]



Obrázek 1 Sedmivrstvá architektura ISO/OSI. [14]

Proces začíná vrstvami orientovanými na přenos dat, kterými jsou fyzická, linková a síťová vrstva. První zmíněná neboli fyzická vrstva, popisuje elektrické či optické signály používané při komunikaci mezi počítači. Na fyzické vrstvě je tvořen fyzický okruh za pomoci dalších zařízení, mezi které patří modemy, routery a huby. Nad fyzickou vrstvou je vrstva linková, která v případě sériových linek zajišťuje výměnu dat mezi sousedními počítači a v případě lokálních sítí výměnu dat v dané síti. Základní jednotkou linkové vrstvy je datový rámec, který se skládá ze záhlaví (Header), přenášených dat (Payload) a zápatí (Trailer). Datový rámec má v záhlaví uloženou linkovou adresu příjemce, odesílatele a další řídící informace. V zápatí je uložen kontrolní součet z přenášených dat, pomocí něhož lze zjistit, zda během přenosu nedošlo ke ztrátě či porušení dat. V přenášených datech je zpravidla nesen paket síťové vrstvy. Poslední vrstva orientovaná na přenos dat je síťová vrstva, která se stará o přenos dat mezi vzdálenými počítači v síti WAN. Základní jednotkou přenosu je paket, který je dále zabalen linkovou vrstvou do datového rámce. Paket se skládá ze záhlaví a datového pole. Zápatí se u paketů vykytuje jen velmi zřídka. V rozsáhlých sítích typu WAN se mezi počítači často nachází jeden či více routerů. Po přijetí vybalí router paket z datového rámce a před odesláním jej opět zabalí do jiného datového rámce.

Po vrstvách zabývajících se přenosem dat je přizpůsobovací vrstva, která obsahuje vrstvu transportní. Síťová vrstva zabezpečí spojení mezi vzdálenými počítači, to znamená, že transportní vrstva nevidí žádné modemy, repeatery, bridge či routery na cestě. Z tohoto pohledu zcela spoléhá na služby nižších vrstev. Úkolem transportní vrstvy

je zajištění spojení mezi aplikacemi na jednotlivých počítačích. Mezi dvěma počítači může probíhat více transportních spojení současně a jednotlivé aplikace jsou jednoznačně adresovány. Jednotka přenosu se nazývá transportní paket a skládá se ze záhlaví a datové části.

Poslední částí modelu jsou vrstvy orientované na podporu aplikací, kam spadají relační vrstva, prezentační vrstva a aplikační vrstva. První zmíněná vrstva zajišťuje výměnu dat mezi aplikacemi. Stará se zejména o synchronizaci akcí nebo korektní uzavírání souborů. Základní jednotkou je relační paket, který se vkládá jako data do transportního paketu. Prezentační vrstva je zodpovědná za reprezentaci a zabezpečení dat. *„Reprezentace dat může být na různých počítačích různá. Např. se jedná o problém, zdali je nejvyšší bit v bajtu zcela vlevo nebo vpravo atp. Zabezpečením se rozumí šifrování, zabezpečení integrity dat, digitální podepisování atd.“* [9] Na vrcholu všech vrstev je vrstva aplikační, která říká, jak mají být data přebírána a předávána od aplikačních programů a v jakém formátu. [9]

4.2.2 Topologie sítí

Topologie sítě je způsob propojení mezi přímo připojenými prvky v síti. Fyzická topologie odpovídá několika logickým neboli reálným topologiím, kde je každá na jiné úrovni abstrakce.

Síťová topologie se stále mění, nejčastěji když se uzly a propojení připojují k síti či se zvyšuje kapacita sítě, aby zvládla zvýšený provoz. Ruční sledování topologie sítě je velmi namáhavé až často nemožné. Přesné informace o topologii jsou však nezbytné pro:

*„**Simulace:** pro simulování skutečné sítě, musí být nejprve získána topologie sítě.*

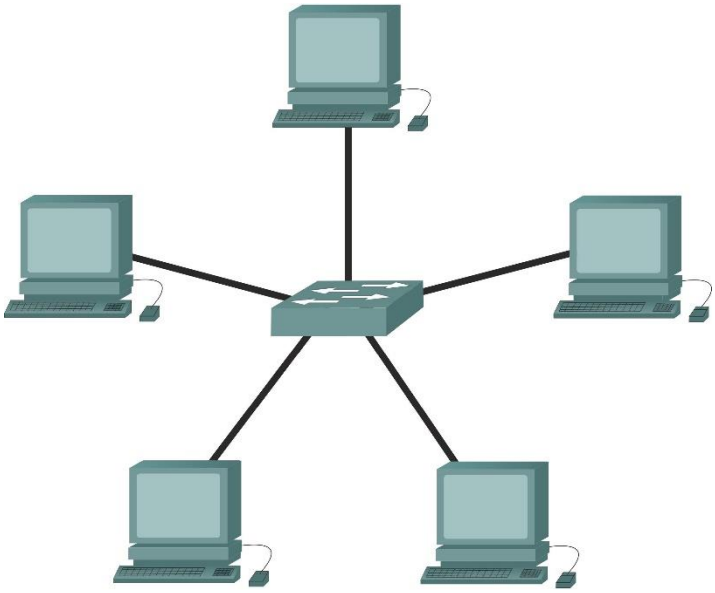
***Správa sítě:** Informace o topologii jsou užitečné při rozhodování, zda přidat nové routery a zjistit, zda je aktuální hardware správně nakonfigurován. Rovněž umožňuje správcům sítě najít překážky a selhání v síti.*

***Umístění:** Mapa sítě pomáhá uživatelům určit, kde jsou v síti, takže se mohou rozhodnout, kam umístit servery a ke kterému poskytovateli připojení se připojí.*

***Algoritmy podporující topologii:** Informace o topologii umožňují novou třídu protokolů a algoritmů, které využívají znalosti topologie ke zlepšení výkonu. Příklady zahrnují politiku citlivou na topologii a směrování QoS a algoritmy skupinové komunikace s výběrem procesní skupiny s vědomím topologie.“* [11]

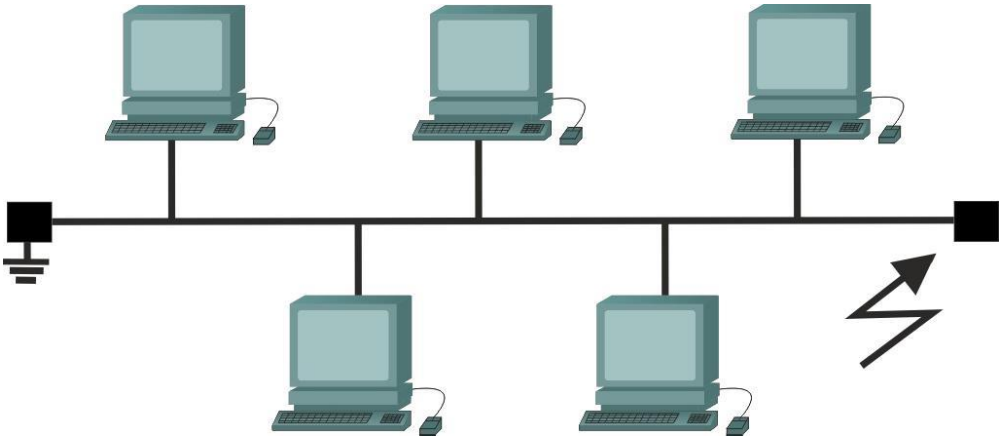
Síťovou topologii si lze představit jako tvar či strukturu dané sítě. Tento předdefinovaný tvar nemusí nutně korespondovat se skutečným fyzickým rozvržením prvků, zapojených v síti. V počítačových sítích jsou tři hlavní topologie, a jimi jsou hvězdicová neboli strom, sběrnicová a prstencová neboli kruh. [11]

U první z nich, jak již název napovídá jsou zařízení uspořádána do takzvané hvězdice či stromu, jak je vidět na Obrázek 2. Signál je vysílán ze zdrojového počítače a pomocí hubu je rozesílán do všech ostatních zařízení v síti. Pokud při této topologii selže centrální bod neboli hub, přestane fungovat celá síť, ale pokud selže jen kabel ke koncovému zařízení, či přestane fungovat cílové zařízení, tak je mimo provoz komunikace pouze pro dané zařízení. Ostatní části sítě jsou oddělené, a tato chyba je nezasáhne. [9]



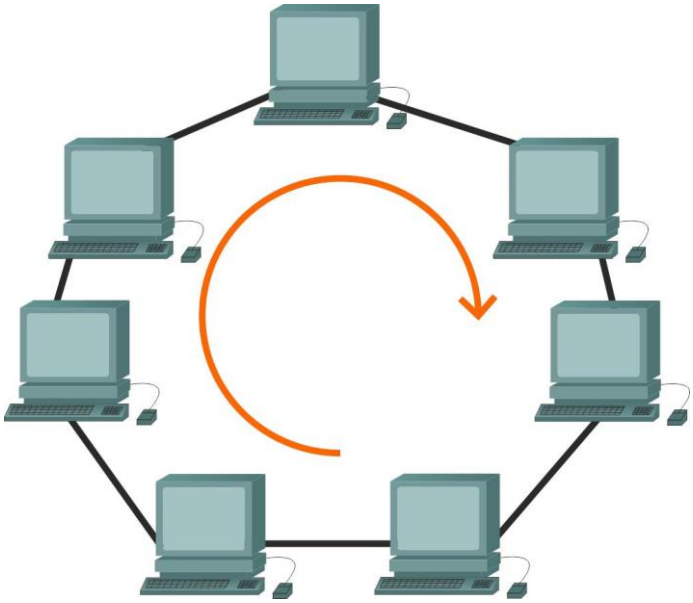
Obrázek 2 Hvězdicová topologie. [23]

Sběrnicové topologii se také říká lineární sběrnice. Je to nejjednodušší a nejčastější způsob zapojení počítačů do sítě. Skládá se z hlavního kabelu, nazývaného také jako páteř nebo segment, který v řadě propojuje všechny počítače v síti, jako je ukázáno na Obrázek 3. Komunikace probíhá tak, že počítače adresují data konkrétnímu cílovému zařízení a posílají je po kabelu ve formě elektrických signálů. Velkou výhodou této topologie je, že když vypadne jedno ze zařízení, tak zbytek sítě funguje dále. Když ale dojde k přerušení hlavního vedení, tak dochází k nefunkčnosti celé sítě. [9]



Obrázek 3 Sběrnicová topologie. [23]

Poslední jmenovanou topologií je prstencová, která propojuje počítače pomocí kabelu v jediném okruhu (Obrázek 4). Signál prochází ve smyčce v jednom směru všechny počítače. V této topologii počítače fungují jako repeatery a to znamená, že signál zesilují a posílají ho do dalšího počítače. Kvůli procházení signálu všemi počítači, může mít selhání jednoho velký vliv na celou síť a to tak, že pokud jedno zařízení přestane pracovat, nebo nastane chyba na jednom z přenosových kabelů, tak v daném místě se komunikace přeruší a dojde ke ztrátě informací, které byly zrovna poslány. [9]



Obrázek 4 Prstencová topologie. [23]

V Tabulka 1 jsou vidět vybrané výhody a nevýhody daných topologií sítě a jejich rozsah použití.

Tabulka 1 Výhody a nevýhody topologií sítě

Topologie	Výhody	Nevýhody	Rozsah použití
Hvězdicová	Spolehlivá, rychlá	Nutnost koncentrátoru (switchů)	Dnes nejpoužívanější
Sběrnicová	Nízké pořizovací náklady	Poruchovost, obtížné vyhledávání místa závady, porucha kabeláže vyřadí celou síť	Dožívá ve starších kabeláží
Prstencová	Pravidelné předávání zpráv v kruhu	Stejné jako u sběrnicové topologie, porucha kabeláže vyřadí celou síť, ale řeší se zdvojením vedení	Používají ji méně rozšířené sítě IBM Token Ring a FFDI

4.2.3 Aktivní prvky sítě

Počítačová síť se skládá z aktivních a pasivních síťových prvků. Mezi pasivní síťové prvky patří kabeláž a konektory. Mezi aktivní prvky patří zařízení, která odesílají, přijímají a přeposílají informace přes komunikační kanál. Použité aktivní prvky a komunikační protokol určují, jakým způsobem data fyzicky putují po síti. [20]

Mezi aktivní síťové prvky patří repeater (zesilovač či opakovač), transceiver (převodník), hub (rozbočovač), switch (přepínač), bridge (most), router (směrovač) a gateway (brána). Nejjednodušším aktivním prvkem v síti je repeater nazývaný také jako zesilovač nebo opakovač, protože pouze zesiluje či opakuje procházející signál. Jedná o krabičku se dvěma stejnými konektory. Je využíván v místech, kde je kabel dlouhý tak, že na konci by již nebyl dostatečně silný signál. Nejčastější je u koaxiálních sítí. Velmi podobným prvkem je transceiver, který plní stejnou funkci jako repeater, ale navíc ještě dokáže převést signál z jednoho typu kabelu na jiný jako například z kroucené dvojlinky na optický kabel. Hub byl dříve nezbytným prvkem v síti s hvězdicovou topologií. Dnes ho nahradily switche, které mají stejnou funkci a výrazně eliminují nevýhodu plynoucí z metody CSMA-CD. Základní funkcí hubu je, že rozbočuje signál, nebo větví síť. Switch oproti hubu odděluje komunikující uzly sítě tak, že pro ně vytvoří virtuální okruh a ostatní

uzly pak nejsou zahlcovány cizími pakety. Tím pádem nedochází ke zpomalování sítě, jak je tomu u hubu, a přenos informací probíhá maximální rychlostí. Dalším podobným prvkem v síti je bridge, který odděluje od sebe určité části sítě. Oproti switchi je bridge starším zařízením, jehož úkol je oddělení síťových segmentů a plní dvě funkce. První z nich je filtrace paketů, vycházející z toho, že si bridge přečte cílovou adresu paketu a propustí ho pouze do té části sítě, kde je cíl paketu, tím pádem se snižuje zatížení sítě a síť může být rychlejší a plynulejší. Druhou funkcí je propojování dvou sítí různých standardů. Jelikož bridge pracují v linkové vrstvě ISO/OSI modelu, který byl již vysvětlen v předchozí kapitole, tak víme, že fyzické rozdíly sítí bridge neovlivňují. Dále je zde nejinteligentnější prvek v síti, a to je router. Router pracuje na úrovni síťové vrstvy ISO/OSI modelu. Shromažďuje informace o připojených sítích a poté vybere nejvýhodnější cestu pro posílaný paket. Má zabudovanou filtraci paketů, kterou doplňuje o inteligentní směrování. U vnitřních sítí LAN není router typický, mnohem častěji je použit při připojování sítí k internetu.[4] K propojení dvou rozdílných sítí slouží gateway, která je sice pomalejší než bridge nebo router, ale dokáže překládat mezi sítěmi „hovořící různými jazyky“. Umožňuje komunikaci mezi odlišným prostředím, architekturami a přetváří data, tak aby se přizpůsobila aplikaci v jiné síti, která data přijímá. [1]

4.3 Síťový software

Dále k síťovému hardwaru, který byl popsán v kapitole 4.2, je důležitým bodem v sítí software. Tím je tvořena provozuschopná síť, kde po propojení připraveného hardwaru pomocí kabeláže přichází na řadu software a všechna zařízení v síti se musí správně nakonfigurovat a připravit k provozu sítě.

Síťový software se rozděluje na dvě kategorie. První je peer-to-peer a druhá je klient-server. Hlavní rozdíl mezi těmito kategoriemi je použití serveru. První zmíněná kategorie peer-to-peer nepoužívá server, ale klienti komunikují pouze mezi sebou. Poté druhý typ klient-server u kterého již z názvu vyplývá, že zde klienti komunikují výhradně přes server. [4]

4.3.1 Peer-to-peer

Peer-to-peer nebo také jako klient-klient je označení architektury počítačových sítí, ve které spolu komunikují přímo jednotliví klienti. Čistá peer-to-peer architektura

vůbec nezná pojem server, všechny uzly sítě jsou si rovnocenné. V praxi se však často pro zjednodušení návrhu v protokolu objevují specializované servery, které ovšem slouží pouze pro počáteční navázání komunikace, „seznámení“ klientů navzájem, popřípadě jako Proxy server v případě, že spolu z nějakého důvodu nemohou koncové uzly komunikovat přímo. Dnes se označení peer-to-peer vztahuje hlavně na výměnné sítě, prostřednictvím kterých si mnoho uživatelů může vyměňovat data.

Výhody:

Jednou ze základních výhod peer-to-peer sítí je fakt, že s rostoucím množstvím uživatelů celková dostupná přenosová kapacita roste, zatímco u modelu klient-server se musí uživatelé dělit o konstantní kapacitu serveru, takže při nárůstu uživatelů klesá průměrná přenosová rychlost. Nejčastějším obsahem šířeným po výměnných sítích jsou hudební nahrávky ve formátu MP3, filmy ve formátu MPEG a software.

Nevýhody:

Dnešní anonymní výměnné sítě umožňují (legální i nelegální) výměnu souborů s prakticky nulovou mírou odpovědnosti jednotlivých uživatelů. Někteří kritici poukazují na to, že se prostřednictvím výměnných sítí může distribuovat dětská pornografie či podporovat terorismus a na základě toho žádají o regulaci či přímo zákaz takových sítí. Zastánci naopak argumentují tím, že možnost zneužití technologie k nezákonným účelům nesmí bránit jejímu legálnímu využívání a že je třeba dodržovat princip presumpce neviny.

4.3.2 Klient-server

Klient-server je síťová architektura, která odděluje klienta a server, kteří spolu komunikují přes počítačovou síť. Klient-server aplikace obsahují jak klienta, tak i server a dělí se na dvě části. První z nich je serverová a druhou je klientská. Popisuje vztah mezi dvěma počítačovými programy, v nichž první program (klient) žádá o služby jiný program (server). Na tomto modelu je založen například přístup na e-mail, web, přístup k databázi a umožňuje zařízením sdílet soubory. Tento model používá většina obchodních či firemních aplikací, dále ho pak používají i tyto internetové protokoly HTTP, SMTP, Telnet, DNS a další. Každá instance klienta může posílat žádost o data jednomu nebo více připojeným serverům. Na druhé straně, servery akceptují tyto žádosti, zpracují je a vrátí klientovi požadovanou informaci.

Výhody:

Ve většině případů architektura klient-server rozdělí jednotlivé úkoly a zodpovědnosti počítačového systému mezi několik počítačů které spolu komunikují pouze prostřednictvím sítě. Tím vzniká další výhoda, a to snadnější údržba. Například je možné nahradit, opravit, modernizovat, přemístit server, aniž by to klienti poznali, nebo tím byli nějak ovlivněni. Tato nezávislost na klientech se nazývá zapouzdření. Všechny údaje jsou uloženy na serverech, které jsou mnohem bezpečnější než většina klientů. Servery mohou lépe kontrolovat přístup a zdroje, to zaručuje, že přistupovat a měnit data mohou pouze oprávnění klienti. Mnoho klient-server aplikací, které jsou dnes k dispozici, je navrženo s ohledem na vyšší bezpečnost, uživatelskou přívětivost a snadné používání.

Nevýhody:

Velkým problémem je přetěžování sítě. Vzhledem k tomu, že počet souběžných požadavků klientů na daný server se zvyšuje, server se může snadno přetížit. Naproti tomu u peer-to-peer sítí se šířka pásma zvětšuje s množstvím klientů, protože každý klient tvoří uzel sítě. Architektura klient-server není tak robustní jako sítě peer-to-peer. Pokud dojde k výpadku serveru, žádosti klientů nemohou být splněny. V peer-to-peer sítích jsou zdroje obvykle distribuovány mezi více uzlů. Dokonce i když více uzlů přeruší sdílení dat, mělo by být možné stáhnout data od zbývajících uzlů.

5 Útoky na počítačovou síť

Útok na počítačovou síť je „*Činnost realizovaná za účelem narušit, blokovat, znehodnotit nebo zničit informace uložené v počítači anebo na počítačové síti, či počítač anebo počítačovou síť samotnou. Útok na počítačové síti je určitým druhem kybernetického útoku.*“ [8]

Kybernetické útoky jsou čím dál častější a způsobují značnou škodu. Jeden z aktuálně nejznámějších útoků byl koncem roku 2019 na nemocnici v Benešově. „*11. prosince 2019 došlo v noci ke kyberútoku na strategické ICT systémy středočeské nemocnice v Benešově. Přímým důsledkem bylo totální ochromení infrastruktury nemocnice, kdy zkolabovala počítačová síť, nemocniční a laboratorní přístroje na ní napojené a bylo nutné zrušit plánované operace.*“ [19] Toto je jeden z důvodů, proč se kybernetické útoky začínají řadit mezi nejzávažnější rizika moderní společnosti. Je ale jasné, že se riziko bude stále zvyšovat s přibýváním zařízení připojených k internetu. Jsou to zařízení, která mohou být napadena jako cílové zařízení anebo jen využita pouze jako přestupní stanice, ze které bude proveden útok na jiné zařízení v síti. Toto si bohužel mnoho uživatelů zařízení neuvědomuje, a tak ohrožují soukromí i bezpečnost ostatních uživatelů. Neohrožují tím jen svoje soukromí, ale i svých blízkých, či v zaměstnání může být prozrazeno obchodní tajemství nebo podnikatelský plán.

Dříve byly počítače využívány pouze odborníky nebo lidmi, kteří je využívali ke svému povolání a znali i bezpečnostní stránku jejich užívání. V dnešní době jsou tato zařízení využívána kýmkoli, dokonce i batolaty, která si hrají s mobilními telefony či notebooky a vůbec nevědí, co bezpečnost v internetu znamená a ulehčují tak útočníkům přístupy k určitým zařízením a případným dalším útokům.

V dnešní době je útok buď proveden přímo útočníkem nebo nabízen jako služba, kde si uživatel koupí software na realizaci útoku a dostane ho včetně podpory. Jedná se o CaaS (Crime as a Service). „*Inovace Crime as a Service nepřináší pouze nástroje a služby v oblasti kybernetického zločinu do rukou širšího okruhu subjektů ohrožujících hrozbu, ale také z kybernetického útoku vytváří podnik, který může poskytnout živobytí pro kariérního zločince. Kromě toho restrukturalizuje činnosti v oblasti počítačové kriminality a vede útočníky hlouběji do podzemí, protože činnosti související s počítačovou kriminalitou mohou být nyní nabízeny jako nezávislé, modulární komponenty*

v dodavatelském řetězci pro počítačovou kriminalitu, přičemž útočníci těží z každé komponenty.“ [6]

Útoky lze dělit na vnitřní a vnější. Vnitřní útok znamená, že počítač, ze kterého je proveden útok, musí být připojen do vnitřní sítě firmy. Většinou se jedná o zaměstnance, nebo zaměstnance externí firmy, aby nebylo nápadné, co právě dělá. Vnější útok znamená, že útočník nemá fyzický přístup do vnitřní sítě firmy. Na tomto útoku je velká výhoda anonymita útočníka, ale o to větší musí mít zkušenosti, aby mohl do sítě proniknout.

Další dělení útoků je na aktivní a pasivní, podle toho, co chce útočník dělat. Při aktivním útoku chce někomu uškodit, systém nebude pracovat, jak by měl, či nastane změna probíhající komunikace. Všechny aktivní útoky musí mít vždy pozitivní prospěch pro útočníka. V pasivním útoku může docházet pouze k odposlouchávání probíhající komunikace. Tomuto útoku se nejlépe dá zabránit, pokud napadená zařízení používají šifrovanou komunikaci. Šifrovaná komunikace je vždy lepší, ať je uživatel napaden útokem, ale i v případě prevencí. [8]

5.1 Dopady kybernetických útoků

Dopady kybernetických útoků mohou být finanční nebo nefinanční a výše dopadů se odvíjí od zkušenosti útočníka a úrovně zabezpečení v síti dané společnosti. Útoky se zpravidla vždy projeví negativně na zisku společnosti, úniku informací, tempu jejího růstu a v krajních případech mohou vést i ke krachu nebo nucené likvidaci. Útočník může mít za cíl: [12]

- zamezení přístupu k informačnímu systému (webové stránky, e-shop),
- vniknutí do objednávkového systému a vytvářet falešné objednávky a v tomto případě i finanční ztrátu společnosti,
- smazání, pozměnění nebo zašifrování dat tak, aby se společnost nedostala k napadeným informacím (o zaměstnancích, klientech, produktech či výrobních plánech),
- ukradení citlivých informací a následně je prodat na černém trhu, či využít ve vlastní prospěch,
- ovládnutí systému a pomocí něho vytvořit další útok na jinou společnost za účelem lepšího skrytí své identity či šíření malwaru,

- ovládnutí systému a vložení do něho škodlivého kódu a poté nabídnutí firmě, že škodlivou část odstraní nebo upozorní společnost na danou chybu. [12]

5.2 Obecné informace o útocích, jejich typech a obraně

5.2.1 Typy útoků

Mezi nejčastější typy útoků patří odposlech při přenosu dat na síti, které poté útočník využije ve svůj prospěch. Útočníci se mohou vydávat za někoho jiného prostřednictvím emailu, kde se vydávají například za banku a zjišťují přihlašovací údaje k internetovému bankovnictví. Dalším typem útoku je zahlcení zdrojů zaplavováním MAC adres. Mezi tyto způsoby útoku patří spamming, DoS nebo DDoS, kde je útok prováděn hrubou silou, takže zaplní zdroje a poté získá snazší přístup k cílovému zařízení. Další možností, jak zaútočit, jsou automatizované programové útoky, mezi které patří viry, či trojské koně. [8]

5.2.2 Obrana

Obrana proti útokům je složitá a čím šikovnější je útočník, tím je těžší se bránit jeho útokům. Základními obranami před útoky na zařízení je zapnutý firewall a aktivovaná antivirová ochrana. Pro znemožnění, nebo alespoň pro ztížení přístupu k zařízení je používání VLAN a VPN. Pro ztížení odposlouchání komunikace či krádeži dat přenášených přes počítačovou síť je základem šifrovaná komunikace. To znamená, že i když útočník bude odposlouchávat komunikaci, tak nebude moci získané informace nijak zhodnotit, protože jsou pro něho neúplné a bez klíče k šifrování nejdou lehce rozluštit. Dále lze útokům předcházet neotvíráním příloh a odkazů v e-mailech, u kterých je odesílatel neznámým nebo je emailová adresa podezřelá. [5]

5.2.3 Zabezpečení LAN

Síť LAN se dá nejlépe zabezpečit tak, že správce dané sítě vypíše seznam povolených IP a MAC adres a zamezí tak přístupu jiných uživatelů (potenciálních útočníků). Dále lze nastavit omezení počtu MAC adres a tím předejít přepnutí do HUB modu a tím lehčímu napadení zařízení.

5.2.4 Firewall

Firewall zabezpečuje rozhraní mezi veřejnou a soukromou sítí. Dále definuje pravidla přístupu k zařízení. Dokáže omezit přístup na předem stanovené části vnitřní sítě. Rozhoduje, zda určité programy dostanou přístup k internetu a tím eliminuje samovolné stahování dalších programů. Kontroluje přístupy a zaznamenává statistiky. [8]

5.3 Konkrétní typy útoků

5.3.1 DoS attack

DoS attack neboli Denial of Service Attack česky přeložené jako odmítnutí služby nebo DDoS, který je stejný, pouze více distribuovaný, a proto Distrubuted Denial of Service Attack. DoS je technika útoku na omezení přístupu k internetové službě nebo stránce zahlcením komunikační linky nebo celého serveru požadavky. Projev tohoto útoku lze vysledovat v nadměrném nárůstu času na dotaz, nebo nemožnosti připojení se ke službě. [8]

5.3.2 MAC Flooding

MAC Flooding je typ útoku, při kterém dochází k úmyslnému zahlcení vnitřní paměti switche. Jakmile se paměť zaplní falešnými adresami, začnou se MAC adresy ukládat i na prostor, kde byly uloženy korektní adresy a switch začne pracovat jako hub. Poté už je lehké zachytávat data. Nejlepší obrana je nastavení omezení počtu MAC adres společně s limitem nastaveným na zadání nových MAC adres z jednoho zařízení.

5.3.3 Malware

Malware je typ útoku, vznikající spojením dvou anglických slov malicious jako škodlivý a software. Většina malwarů má společné to, že se snaží na napadeném zařízení skrývat, aby přežil i restart zařízení. Lze takto označit jakýkoliv software, který při spuštění začne škodit systému. [5]

Malware se rozděluji do tří kategorií. První z nich je Drive-by download malware, dalším je Phishing a poslední kategorií je Trojanizovaná aplikace. U Drive-by download malware k napadení zařízení stačí pouze navštívení infikované webové stránky, která automaticky začne se stahováním viru, který samovolně infikuje zařízení. Phishing je

druhým typem malwaru, kde útok je založen na oklamání uživatele a získání jeho citlivých údajů, jako jsou hesla, kontaktní údaje nebo čísla kreditních karet. Útok je založen na rozesílání podvodných emailů s odkazem na klamavou webovou stránku, která je identická s originální webovou stránkou, kde je uživatel vyzván tyto citlivé údaje zadat. Většinou se útočník vydává za banku, školu či jinou instituci, tak aby email vypadal důvěryhodně. [5]

Poslední kategorií je Trojanizovaná aplikace vyskytující se na neoficiálním, ale i oficiálním marketu, úložišti či přenositelném disku. „J*edná se o program vložený do informačního systému bez vědomí oprávněného uživatele, který monitoruje specifické činnosti, o které projevuje útočník zájem. Jedná se například o znaky, které oprávněný uživatel stiskl na klávesnici (zejména hesla) nebo stránky, které navštívil. Tyto údaje předává útočníkovi k dalšímu zpracování. Ten tak může získat přístupové informace k navštíveným webovým stránkám, bankovním účtům nebo kontům elektronické pošty.*“ [5] Jedná se o nejčlenitější část malwaru, která se rozděluje podle způsobu řízení útoku.

První z Trojanizovaných útoků je virus neboli kód přidávající se do spustitelného souboru, který dokáže mazat soubory, odposlouchávat komunikaci a dělat různé úkony, podle toho, jak je virus napsán. Šíření daného viru funguje tak, že když je infikovaný soubor spuštěn, snaží se zapisovat do dalších aplikací. Toto ale antiviry často identifikují, a proto není brán jako velká hrozba. Macrovirus je kód napsaný v jazyce VBA, který se kopíruje do souborů MS office. Funguje stejně jako virus, proto je snadno detekován a moc se nevyužívá, případně jen ke stažení jiného malwaru. Worm je dalším typem malwaru, ale oproti virusu je již dokončeným programem, který se sám rozesílá pomocí e-mailu nebo se šíří po síti, kde vyhledává zranitelnosti například užití výchozích či slabých hesel, nezabezpečených sdílených adresářů. „*Jedná se o samostatný program schopný vytvářet své kopie, které rozesílá do dalších počítačových systémů či sítí. Zde vyvíjí další činnost, pro kterou byl naprogramován. Často slouží k vyhledávání bezpečnostních skulin v systémech nebo v poštovních programech.*“ [5]

Díky takovýmto virům si útočník může zobrazovat soubory, použít ho jako keylogger pro zaznamenávání zpráv, nebo získá přístup k portu k následnému DDOS útoku, tím pádem je zařízení využito jen jako prostředník. Dalším typem je spyware, který se vyznačuje odesíláním dat bez vědomí uživatele útočníkovi. Nejčastěji se jedná o statistiky návštěvnosti, nešifrovaná hesla nebo čísla kreditních karet. Jedním z typů útoků,

kde se většinou sám útočník ohlásí, že napadl zařízení je ransomware. Lze ho poznat tak, že se uživatel nemůže dostat ke svým souborům a v tento moment přichází útočník s tím, že napadl zařízení a požaduje výkupné za obnovení přístupu.

6 Návrh síťové topologie

V této kapitole bakalářské práce bude představena konkrétní topologie sítě, která bude využita pro danou práci. Dále se vybraná topologie převede do reálného pohledu, což znamená, kde lze takovou síť využít. Na konci této části bude popsáno, jaká zařízení budou v síti používána.

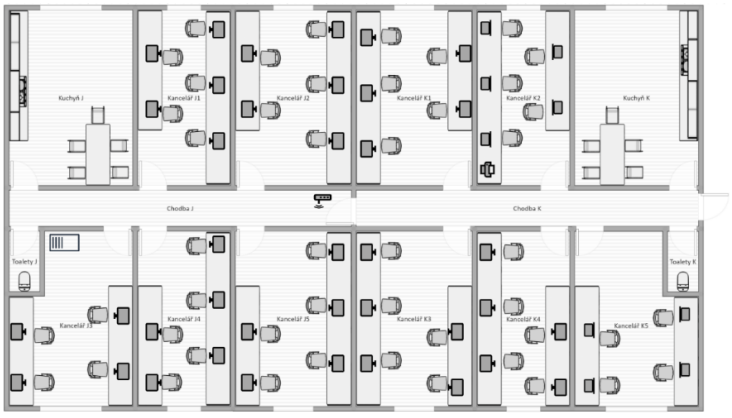
Nejprve je navržena topologie sítě spolu s rozdělením adresního prostoru jako základ pro tuto práci. V simulované síti budou rozmístěna všechna koncová zařízení. Poté se přechází k propojení všech zařízení a následné postupné základní konfiguraci u každého zařízení a testování konektivity, zda spolu veškerá potřebná zařízení komunikují.

6.1 Topologie sítě

Topologie sítě bude vytvořena pro malé podniky či rodinné domy. Konkrétní návrh je pro budovu s jedním patrem, kde je toto patro rozděleno na 2 části (levá a pravá). Stejnou topologii lze použít i pro dvoupatrové domy, kde místo levé a pravé části bude první a druhé podlaží.

6.2 Popis místností

V této části šesté kapitoly bude navržené a popsané možné rozložení navržené topologie infrastruktury do reálného světa. V tomto případě to bude pouze jedno patro, které bude rozděleno na levou a pravou část. Na Obrázek 5 Půdorys objektu a umístění jednotlivých koncových zařízení a síťových prvků je vidět grafický půdorys návrhu objektu.



Obrázek 5 Půdorys objektu a umístění jednotlivých koncových zařízení a síťových prvků.

Zdroj: vlastní zpracování

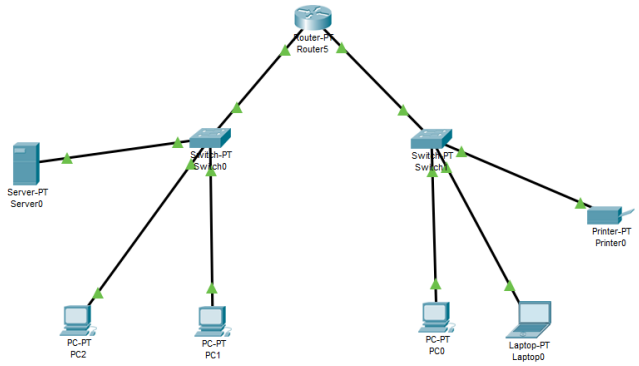
Obrázek 6 Zařízení použita v půdorysu topologie[16]

V nákresu půdorysu objektu byla použita následující koncová zařízení: stolní počítač, laptop, tiskárna, směrovač a server (Obrázek 6). V kuchyních a toaletách nejsou naistalována žádná koncová zařízení.

Objekt je rozdělen do dvou částí, každá z nich obsahuje 5 kanceláří, kuchyň a toaletu. První část je umístěna vlevo, kde jsou místnosti označené písmenem J, zatím co v druhé části jsou označené písmenem K.

Internet je do budovy přiváděn přes router, který je umístěn na chodbě v krajní části budovy J. Router dále směruje na připravené switche do obou místností, a tím rozděluje svoji síť na dvě podsítě. První podsíť je v části budovy J, kde budou dále naistalována zařízení jako jsou desktopové počítače a server. Druhá podsíť bude v části K, kde dále budou instalovány další desktopové počítače, laptopy a tiskárna.

Hlavní důvod rozdělení infrastruktury je z bezpečnostního hlediska, kde část J je pro IT oddělení a potřebuje být více zabezpečená a oddělená od dalších sítí. Část K je pro zbylá oddělení, kde pracují i méně zaškolení zaměstnanci pro bezpečnost sítě. Toto rozdělení umožňuje lepší zabezpečení infrastruktury v části J, pokud by se podařilo útočníkovi napadnout část K. Jak je navrženo rozdělení topologie sítě je vyobrazeno na Obrázek 7, kde je zřetelné rozdělení do dvou LAN sítí pomocí routeru a switchů.



Obrázek 7 Návrh vzorové síťové topologie.
(Zdroj: vlastní zpracování v aplikaci Cisco Packet Tracer)

7 Simulátory počítačových sítí

Tato bakalářská práce je psána za účelem porovnání vybraných simulátorů provozu na počítačových sítích od instalace až po implementaci definované síťové topologie, tak aby uživatel rychle dokázal posoudit, který ze simulátorů je pro něho a jeho práci nejvhodnější, jak z pohledu manipulace, tak i jeho funkcí a výstupu.

Porovnávání simulátorů v praktické části bude následující. Postupně budou představeny všechny tři simulátory počítačových sítí, jako takové, kde budou z pohledu uživatele uvedeny obecné informace o softwaru a dále budou postupně popsané kroky, jak se s daným simulátorem pracuje. Začíná se instalací, stejně jak uživatel bude postupovat. Již od stránek, kde lze daný simulátor stáhnout a za jakých podmínek. Pokračuje se průběhem celé instalace, která je pro většinu uživatelů stejná. Po instalaci softwaru se již přejde přímo do aplikace. Nejdříve bude popsána a vysvětlena vizuální stránka aplikace a poté se začne vytvářet předem definovaná síťová topologie, která byla představena v předchozí kapitole a odpovídá menší firmě, která je rozdělená na kanceláře a kde je několik pracovišť nebo střední až větší dům. Na konci každého simulátoru bude krátké shrnutí, kde budou popsané výhody a nevýhody daného simulátoru.

Na konci bakalářské práce bude provedeno porovnání simulátorů, podle definovaných kritérií aplikovaných na každém simulátoru, kde bude každé rozhodnutí bude vysvětleno, tak aby uživatel dokázal pochopit, zda dané kritérium je pro něho pozitivní nebo negativní. Nakonec bude sepsané krátké porovnání simulátorů mezi sebou pro větší přehlednost na jednom místě.

Síťové simulátory se v dnešní době používají velmi často – jak již k rozvržení budoucí sítě na konkrétních prostorech, tak pro modelování provozu při daném toku dat a v neposlední straně pro simulaci útoků a testování protiopatření. V oblasti komunikací a počítačových sítí je simulace sítí technika, při které se pomocí simulačních programů testují zadané topologie a uvnitř nich se sledují a analyzují vzájemné vztahy mezi různými subjekty (koncová zařízení, routery, switche) i přenášené pakety či datové linky.

Simulovat se dají jak klasické drátové sítě, tak i bezdrátové a satelitní sítě. Tato bakalářská práce se zaměřuje pouze na klasické drátové sítě, z důvodu, že v této práci jde o porovnání simulátorů, než jejich podrobnější funkce a fungování dalších sítí. Většina simulátorů pracuje s nejpoužívanějšími standardy, jako jsou IPv4, IPv6, UDP a TCP.

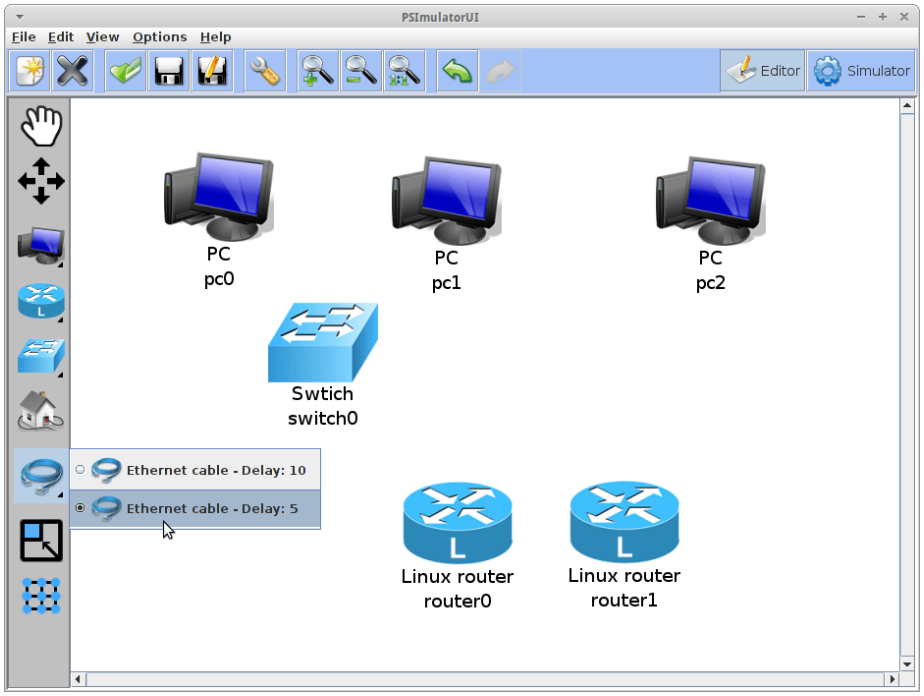
Simulátory síťové topologie jsou dostupné jak komerčně, tak i zdarma. Pro tuto práci byly použity simulátory, které se dají získat zdarma.

Simulátory jsou vybrány podle předem definovaných kritérií. Jako první kritérium je, aby daný simulátor byl zdarma (podmínka pro všechny vybrané simulátory). Druhým kritériem je známost a využívanost daného simulátoru ve školním prostředí. Čemuž odpovídá Cisco Packet Tracer, který je jeden z nejznámějších simulátorů na školní půdě, a to už z důvodu, že pro výukové účely je zdarma a nabízí různé certifikace. Dalším kritériem pro výběr testovaného simulátoru je, aby byl od nezávislého dodavatele, a přitom dostatečně podobný profesionálnímu. Simulátor GNS3 od Jeremyho Grossmana, je velmi podobný Packet Traceru od Cisca a také je v něm možné se připravit na certifikační zkoušky přímo na Cisco. Jako poslední simulátor byl vybrán OMNET++, který je rozdílný v implementaci síťové topologie, jak již bylo řečeno jako další kritérium vybrání třetího simulátoru. Pro práci s tímto simulátorem je potřeba znát programovací jazyk C#, ale není to jediný v čem je tento simulátor rozdílný. Je rozdílný vlastně už od začátku, to znamená už od instalace, která je prováděna pomocí příkazového řádku, a ne instalační aplikací.

K dispozici jsou i další simulátory počítačových sítí, konkrétně Boson NetSim, VIRL, EVE-NG. Boson NetSim je placený síťový simulátor. Veškeré zakoupené úkoly a zadání jsou implementovány přímo v aplikaci NetSim a uživatel je do aplikace nemusí nijak importovat ani vytvářet. Přidání zařízení v simulátoru je velmi podobné jako v GNS3. Velkou nevýhodou tohoto simulátoru je, že uživatel nevidí informace o přenášených datech a stav propojení sítě. Jinak je aplikace velmi podobná jako Cisco Packet Tracer. Z těchto důvodů nebyl Boson NetSim vybrán mezi prakticky testované simulátory. Dalším dostupným simulátorem je VIRL, který je velmi podobný simulátoru GNS3 a jeho největší výhodou je, že obsahuje obrazy softwarů, které se dají použít i do jiných simulátorů. Naopak nevýhodou je cena, která je pro osobní používání 199 USD ročně. Podobnost se simulátorem GSN3 je hlavním důvodem, proč tento simulátor nebyl vybrán do podrobného porovnávání. Poslední zmíněný simulátor je EVE-NG, který je rozdílný oproti ostatním v tom, že topologie navrhuje, připojuje a spravuje pomocí klienta HTML5. To znamená, že uživatel nemusí stahovat a instalovat samotnou aplikaci a bude to provádět prostřednictvím webového rozhraní. Nevýhodou tohoto simulátoru je, že nemá dostupné žádné softwarové obrazy síťového zařízení a uživatel si je musí sehnat

jinak, jak již bylo psáno dříve například od VIRL. Simulátor EVE-NG nebyl do bakalářské práce zahrnut z důvodu, že nesplňuje podmínku funkční vybavenosti aplikace a také vzhledem ke značné podobnosti k Cisco Packet Traceru a GNS3. [15]

Pro úplnost je třeba uvést i simulátor, který byl vyvinut v České republice, konkrétněji na Fakultě informačních technologií ČVUT v Praze. Tento simulátor se nazývá PSimulator, byl naprogramován v roce 2016 a je volně dostupný na GitHubu. Bohužel to byl jen školní projekt a po jeho dokončení se přestal aktualizovat a podporovat. [22] Z tohoto důvodu ho převzal Roland Kübert a pár aktualizací bylo provedeno. Poslední aktualizace software byla v roce 2019, ale není zde žádná podpora při problémech ani řádná dokumentace k simulátoru. Z tohoto důvodu nebyl jediný český zástupce mezi simulátory vybrán do testování a porovnávání simulátorů v bakalářské práci. Pro lepší představivost – PSimulator vypadá prakticky stejně jako Cisco Packet Tracer a GNS3 v odlehčené verzi (Obrázek 8).



Obrázek 8 Ukázka pracovního prostředí aplikace PSimulator. [22]

Veškeré instalace, simulace a testy na simulátorech byly provedeny na zařízení Lenovo ThinkPad E590 s verzí systému Windows 10 Pro s 64bitovým operačním systémem. Procesor byl Intel Core i7-8565U CPU @ 1,80 GHz 2,00 GHz a pamětí 16 GB RAM

7.1 Cisco Packet Tracer

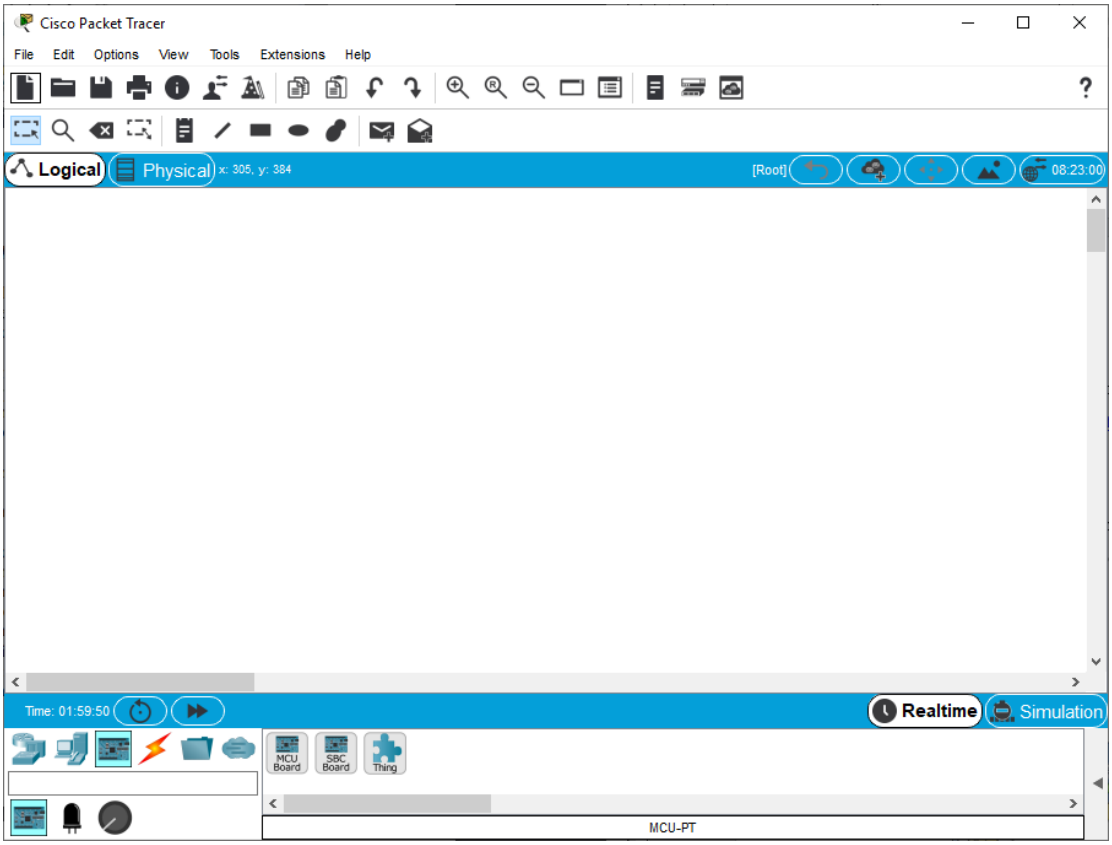
Cisco Packet Tracer je grafický síťový simulační software od společnosti Cisco, dostupný pro studenty Cisco Networking Academy, kde po absolvování výukového programu lze získat světově uznávaný certifikát Cisco CENT (Certified Entry Networking Technician), Cisco CNA (Certiffied Network Associate) a Cisco CNP (Certified Network Professional). [18]

Tento software je k dispozici zdarma pro všechny Cisco Networking Academy vyučující, studenty a absolventy na výuku síťové komunikace, tvorbu simulací, vizualizaci a animaci síťového provozu. Umožňuje navrhovat a konfigurovat počítačové sítě a učí řešit problémy s tím spojené. [2]

7.1.1 Instalace softwaru

Tento simulátor lze stáhnout z webové adresy: https://www.netacad.com/portal/self-enroll/c/920448, kde se uživatel zaregistruje tím, že vyplní údaje jako jméno, příjmení, emailovou adresu. Dalším krokem je potvrzení emailové adresy tak, že na zadaný email přijde zpráva s potvrzujícím linkem. Poté je možné se přihlásit do výukového prostředí netacad.com a na adrese https://www.netacad.com/portal/resources/packet-tracer stáhnout zdarma poslední verzi Cisco Packet Traceru. Simulátor je dostupný pro operační systémy Windows (x32 a x64), Linux a macOS.

Po stažení instalačního balíčku a spuštění instalace se spustí průvodce instalací a za jeho pomoci lze bezproblémově instalovat program. Po instalaci je Cisco Packet Tracer připraven k použití.



Obrázek 9 Základní prostředí Cisco Packet Tracer 7 po instalaci.
(Zdroj: vlastní zpracování v aplikaci Cisco Packet Tracer)

7.1.2 Popis prostředí

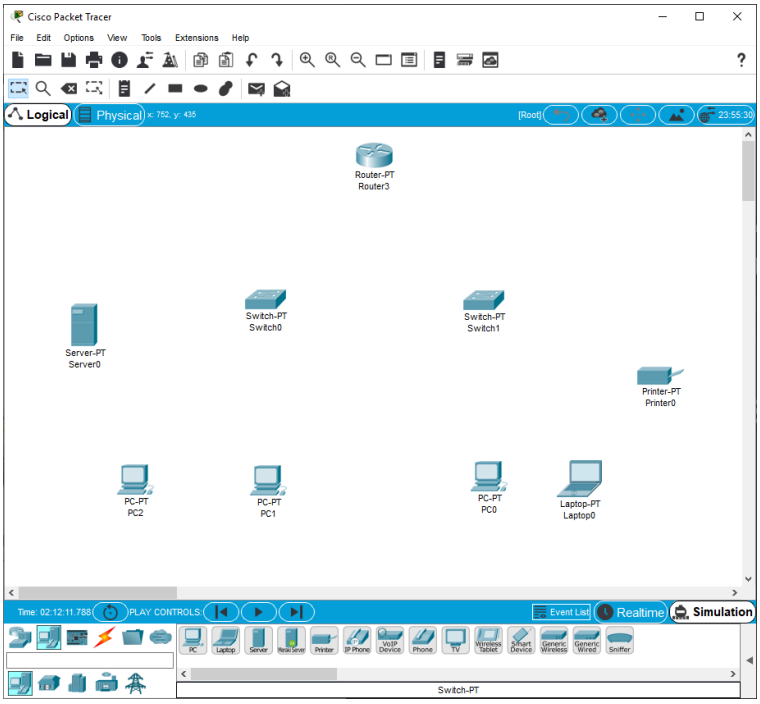
Prostředí simulátoru je rozděleno do několika částí (Obrázek 9). V horní části obrazovky jsou umístěny čtyři lišty. První z nich je Hlavní Menu s dostupnými příkazy aplikace a pod ní je lišta s ikonami pro rychlý přístup k vybraným činnostem. Pod těmito lištami je umístěna lišta pro práci s návrhovým prostředím. Jsou zde například volby pro výběr, kontrolu, mazání, změnu velikosti objektů, přidání poznámky. Na poslední liště je umístěn přepínač mezi logickým a fyzickým pracovním prostředím.

Ve fyzickém prostředí lze vytvářet nové budovy, města, kanceláře nebo místnosti. Lze je přemístit, nastavit jejich pozadí či přepnout do nového prostředí. Logické prostředí je obdobné tomu fyzickému s tím rozdílem, že je zde možné přecházet mezi místnostmi. Největší pracovní prostor aplikace zaujímá hlavní pracovní okno, kde probíhá většina práce se simulátorem. Vytváří se zde simulovaná síť, probíhá její testování a zobrazují se zde pomocné informace. Dalším prvkem je zde přepínač mezi simulací a pracovním oknem v reálném čase.

V režimu simulace se testuje navržená síť. Režim simulace obsahuje ovládání rychlosti simulace, zobrazují se zde statistiky a zaznamenávají se jednotlivé události s ohledem na simulační čas. V levém dolním rohu jsou dva řádky obsahující síťové prvky. První řádek je obecnější, nabízí výběr mezi síťovými prvky, koncovými zařízeními, komponenty a typy spojení. Ve druhém řádku jsou již konkrétní zařízení jako je router, switch, hub, koncové zařízení; dále jsou zde připraveny celé domy, města, továrny a prvky pro IoT. Ve zbytku dolní části je okno obsahující konkrétní typ zařízení z vybrané skupiny, který lze použít pro simulací sítě. Jsou zde jako koncová zařízení například počítač, server, televize. Pro kabeláž je zde například konzole, měděný či optický kabel, telefonní linka, USB, lze použít i automatický výběr, co Cisco Packet Tracer navrhuje, že by se pro konkrétní propojení mělo použít.

7.1.3 Vytvoření síťové topologie

Vytvoření síťové topologie začíná přidáním hlavních prvků do pracovního okna. Jednotlivé prvky jsou zobrazeny v dolní části aplikace (Obrázek 10). To znamená routery, switche a nějaká koncová zařízení jako jsou počítač, laptop, tiskárna nebo server. Zatím se pouze přidají zařízení, která se rozmístí podle navržené topologie a poté se začínají postupně propojovat všechny prvky pro dosažení požadované síťové topologie.



Obrázek 10 Návrh topologie bez použití propojení.
(Zdroj: vlastní zpracování v aplikaci Cisco Packet Tracer)

Po propojení dvojice zařízení se na obou koncích propojení zobrazí kontrolka indikující stav připojení v daném místě. Zelená barva značí funkční spojení, červená barva signalizuje spojení nefunkční. Kontrolu spojení lze provést také umístěním kurzoru nad vybrané zařízení, kdy se zobrazí stav linky "Up" pro aktivní spojení, nebo „Down“ pro spojení neaktivní.

Jelikož pouze propojení zařízení nestačí, musí se všechna zařízení nakonfigurovat, podobně jako v případě reálného hardware. Poklepáním na ikonu routeru se lze dostat do jeho konfiguračního nastavení a zde vybrat záložku Config. Zde je okno rozděleno do tří částí. První vlevo je navigační menu, druhé vpravo je okno, kde se upravují parametry zařízení a poslední okno dole je pro ovládání konfigurace pomocí příkazového řádku. V navigačním okně se dá přepnout do záložky „FastEthernet0/0“ kde jsou zapojené kabely s dalšími zařízeními. V tomto okně se nastaví IP adresa a maska podsítě.

Když jsou na routeru nastavena všechna rozhraní, může se přejít ke konfiguraci koncových zařízení. To je obdobné nastavení routeru. Po poklepání na ikonu koncového zařízení je uživatel přesměrován do konfiguračního nastavení, kde vybere záložku Config. Zde se vyplní „Gateway“, což znamení výchozí bránu, přes kterou se přechází do sítě Internet. Do tohoto pole se zadá IP adresa příslušného routeru. Poté je potřeba nastavit IP adresu daného zařízení, které se provede ve záložce „FastEthernet0“ podle toho, kam je zapojen kabel. V této záložce se vyplní maska podsítě, DNS server a IP adresa, která musí souhlasit se síťovým rozpětím routeru.

Nyní je topologie připravena na test spojení. Kliknutím na ikonu obálky se znaménkem plus se pošle jednorázový test spojení pomocí příkazu ping směrem k serveru. Server odpoví a zašle potvrzovací zprávu. Kurzor se změní na obálku, se kterou postupně uživatel klikne na osobní počítač a pak na server. V informační liště na pravé straně spodního panelu lze získat informace o stavu a pozici zaslané zprávy. Zde je také možnost provést test na opačnou stranu, ze serveru na osobní počítač. Testování spojení je zaznamenáváno a automaticky ukládáno jako scénář pro pozdější zopakování testu.

Program umožňuje prohlížení jednotlivých fází simulace a jejich animaci. Po odeslání zprávy se uživatel přepne do Simulation Mode, klikne na Edit Filters a vybere z nabízených protokolů jen na ICMP, pro zobrazení pouze těchto paketů. Spuštěním simulace tlačítkem Play lze sledovat průběh konkrétní simulace, kdy je současně zobrazen stav paketu v textové podobě s podrobnými informacemi a v pracovním okně

animované zobrazení s označením úspěšnosti přenosu zeleným zaškrtnutím nebo červeným křížkem. Aktuálně probíhající přenos je v textové části označen obrázkem oka. Přidání dalších zpráv pro posílání je zařazeno do fronty zpráv. Další informace o průběhu komunikace mezi těmito zařízeními lze sledovat povolením protokolu ARP v simulačním módu, ve výše zmíněném Edit Filters. Naplnění tabulek ARP je zobrazeno v pracovním okně po kliknutí nástrojem Inspect (ikona Lupy) z pravého svislého menu na vybrané zařízení. Vymazání tabulek ARP uživatel provede kliknutím na Power Cycle Devices, který provede vypnutí všech zařízení a tím i reset jejich konfigurací.

7.1.4 Shrnutí

Práce se simulátorem od firmy Cisco je pohodlná, od instalace až po dokončení modelu počítačové sítě. Instalace je prováděna pomocí instalačního asistenta, kde uživatel pouze vybírá jak a kam instalovat. Při spuštění aplikace Cisco Packet Tracer je možné si spustit úkoly, které s programem naučí zacházet, nebo si na webových stránkách Netacad.com lze zdarma projít lekce, které naučí pracovat s aplikací, a ještě přidá informace o sítových technologiích, které jsou zakončené certifikátem.

Cisco Packet Tracer umožňuje síťovou simulaci a vizualizaci. Je to velmi dobrý nástroj pro porozumění použití síťových protokolů, ale ne jejich využití v reálné síti. Dále lze tento nástroj využít k poukázání rozdílů mezi síťovými zařízeními jako jsou routery, huby, switche. [7]

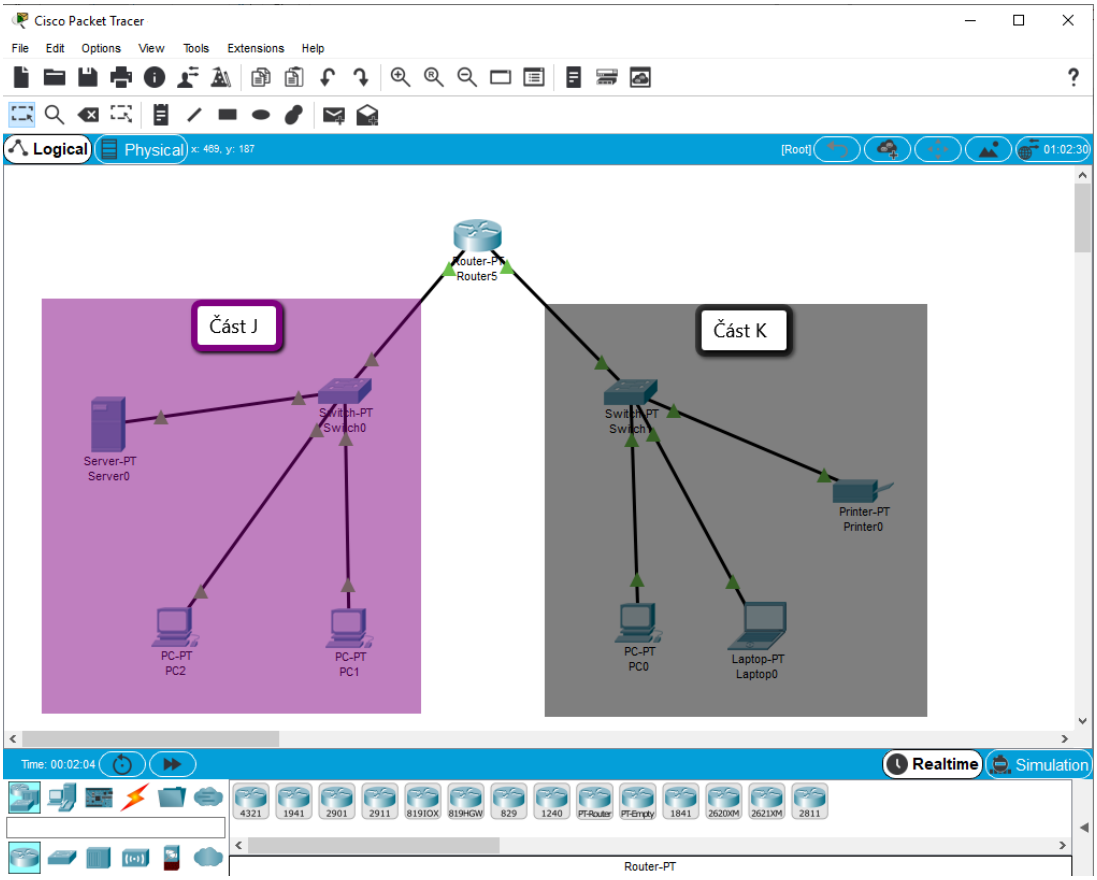
Výhody:

První výhodou Cisco Packet Traceru je jednoduchý průvod instalací a pomoc s prvním použitím aplikace. Aplikace je zdarma dostupná, kde jediná podmínka je, aby se uživatel registroval na stránkách Cisco, kde si poté může zdarma stáhnout aplikaci pro vybrané platformy. Když se uživatel zaregistruje, dostane možnost využít zdarma video kurzy, které Cisco nabízí. Pokud je již aplikace nainstalovaná, je vidět velmi přehledné grafické zpracování aplikace a jednoduchá manipulovatelnost s prvky a jako důležitým bodem je zde na výběr velké množství zařízení a síťového propojení.

Nevýhody:

Jako jednu z nevýhod má Cisco Packet Tracer tu, že aplikace není v českém jazyce, ale umožňuje mezinárodní jazyky, jako jsou angličtina, němčina či španělština.

Cisco SDM neumožňuje jednoduše nastavit základní konfiguraci zabezpečení síťové topologie, ale pouze je možné simulovat provoz na síti. Tento nedostatek částečně napravuje novější verze Cisco CCP. S tímto trochu souvisí i to, že do Cisco Packet Traceru není možné instalovat žádné rozšiřující programy.



Obrázek 11 Rozdělení topologie v aplikaci Cisco Packet Tracer.
(Zdroj: vlastní zpracování v aplikaci Cisco Packet Tracer)

7.2 GNS3

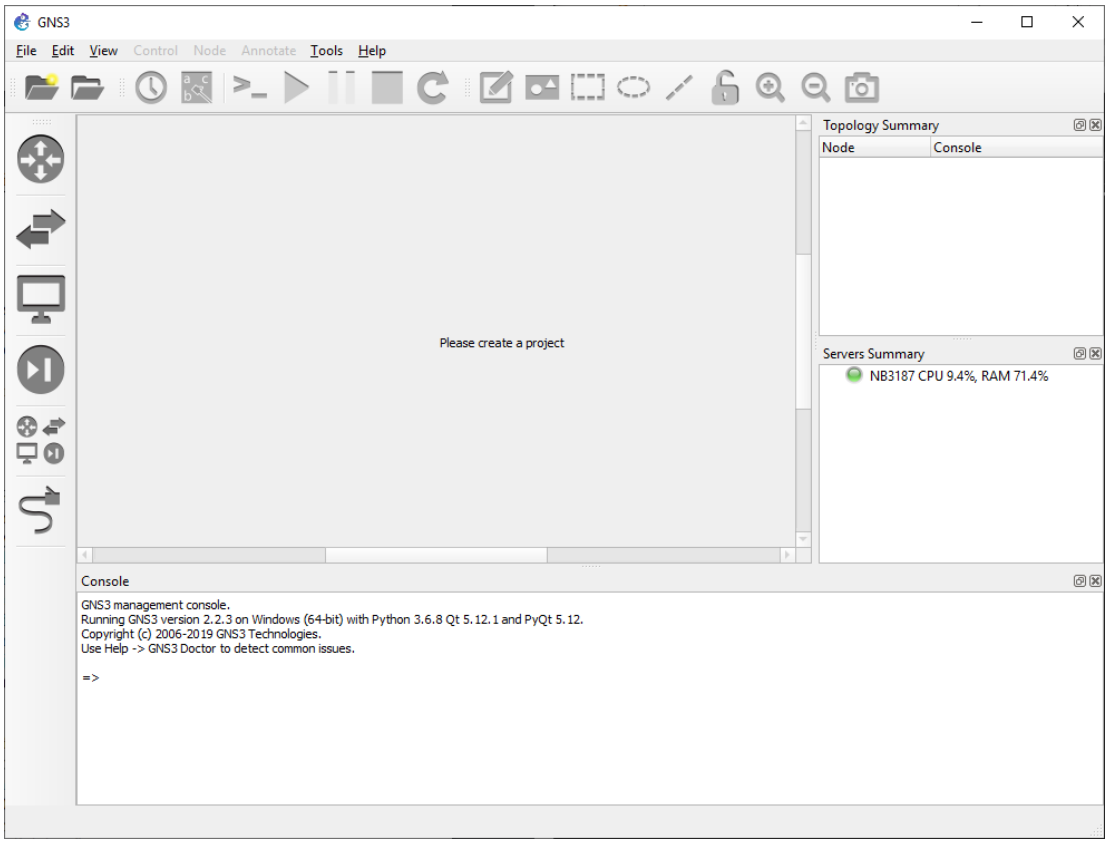
GNS neboli Graphical Network Simulator je multiplatformní aplikace pro simulaci počítačové sítě zaměřená hlavně na podporu Cisco softwaru. Aplikace je založena na programovacím jazyce Python. Tento simulátor je možné provozovat jak v systému Windows, na unixových systémech, tak i na macOS X. Program je poskytován zdarma a je vyvíjen pro laboratorní účely jako testovací a výukové prostředí. Používá množství protokolů a příkazů. Jediným omezením je nutnost vlastnit operační systém

firmy Cisco. První vydání projektu skupiny GNS3 Technologies bylo v roce 2007, jednalo se o GNS3 ve verzi 0.3.

Přímo na stránkách GNS3 (https://www.gns3.com/) je záložka Trénink, kde je umožněno objednání a absolvování certifikačního kurzu, anebo přejít do GNS3 akademie, kde je možné objednání a absolvování dalších kurzů. [17]

7.2.1 Instalace softwaru

Tento simulátor lze stáhnout z webové stránky: https://www.gns3.com/software/download, kde si lze vybrat simulátor pro dané operační systémy. Celou instalací provádí průvodce, kde stačí jen potvrzovat nabízené možnosti a odsouhlasit licenční podmínky a umístění programu. Důležité před koncem instalace je přidání dalších programů, které s GNS3 pracují, jako jsou Dynamips a Qemu. Po dokončení instalace přídavných programů a samostatné instalace GNS3 je simulátor připraven k použití a spustí se aplikace (Obrázek 12).



Obrázek 12 Základní prostředí GNS3 po instalaci.
(Zdroj: vlastní zpracování v aplikaci GNS3)

7.2.2 Popis aplikace

V dané aplikaci je nejvíce prostoru pro pracovní a vizuální plochu vytvořené sítě. To má většina těchto aplikací stejné; dále jsou zde ikony zobrazující síťová zařízení vlevo v panelu. První označuje routery, druhá switche a třetí jsou pro koncová zařízení. Dále v panelu na pravé straně se zobrazují zařízení již použitá v navrhované síti a vytížení počítače. Nakonec v horním panelu jsou dvě lišty. První z nich je Hlavní Menu s dostupnými příkazy aplikace jako jsou Soubor, Úprava, Pohled a další. Pod touto lištou jsou ikony pro rychlý přístup k vybraným činnostem.

7.2.2.1 Emulace Hardware

Grafické uživatelské rozhraní GNS3 umožňuje pohodlně vytvářet virtualizované síťové laboratoře s různými routery, switchi a koncovými zařízeními. Do GNS3 si lze přidat Cisco IOS, pomocí kterého lze udělat síťovou topologii realističtější. Ostatní aplikace tuto možnost nemají. GNS3 využívá hypervisor, který emuluje hardware, na kterém běží Cisco IOS. Emulace hardware je v případě GNS3 velice zásadní, neboť umožňuje spouštět aktuální image konkrétního IOS přímo na PC. Veškeré konfigurační příkazy a jejich výstupy vychází z reálných IOS, a tedy lze říct, že veškeré protokoly nebo funkce, podporované zvolenou verzí IOS, jsou k dispozici pro použití v navržených modelech sítí.

7.2.2.2 Simulované operační systémy

Kromě emulace hardware GNS3 integruje simulované operační systémy, které mohou být propojeny s ostatním GNS3 zařízením. Příkladem může být Cisco IOU, což je v podstatě IOS pro Unix. IOU se skládá z několika binárních souborů pro Linux, které emulují vlastnosti klasického Cisco IOS. Dále je možné do GNS3 integrovat QEMU a obrazy virtuálních systémů z VirtualBoxu, jako např. Linux, BSD, nebo Windows. Například pro nasazení Apache web serveru na Linuxu stačí pouze přidat virtuální stroj (VM), na kterém běží Linux a Apache. Následně tento VM vložit do GNS3, připojit k okolním zařízením a poté je možné testovat prohlížení webu z jiného VM. Vše v rámci uživatelského prostředí GNS3.

7.2.2.3 Dynamips Hypervisor

Pro emulování Cisco hardwaru používá GNS3 aplikaci Dynamips. Tato aplikace byla vytvořena v roce 2005. Autorem je Christophe Fillot z Francie a v chodu je udržována Fláviem J. Saraivem a dalšími. Dynamips hypervisor může emulovat Cisco router hardware v sériích 1700, 2600, 3600, 3700 a 7200. Díky aplikaci Dynamips je možné snadno a rychle konfigurovat tyto modely routerů s různými emulovanými Cisco síťovými sloty a WAN rozhraním. Virtuální vstupně / výstupní karty umožňují přidat k našim zařízením více ethernetových rozhraní, switchovací moduly a sériové porty. Dokonce je možné nastavovat paměť jednotlivým zařízením, na základě požadavků použité verze Cisco IOS.

7.2.3 Vytvoření síťové topologie

Než se začne s přidáváním zařízení do simulačního prostředí, musí si uživatel přidat nějaký router. Bez tohoto kroku by byla možnost vytvoření pouze menší sítě, ve které není router, ale pouze switche a koncová zařízení. Přidání routeru do aplikace GNS3 lze provést následujícím postupem:

- spustit program GNS3,
- v horní liště zvolit „Edit“ a v seznamu „Preferences“,
- zde zvolit záložku Dynamimp a v ní podzáložku IOS routers,
- v dolní části okna kliknout na New a následně vybrat cestu k IOS, který je určen pro nahrání (z vlastních fyzických zařízení, nebo pomocí Cisco online účtu),
- program by měl sám rozpoznat zařízení, které náleží k tomuto IOS a doplnit název,
- nastavit velikosti RAM a Flash,
- poté lze přidat moduly (ethernetové nebo sériové),
- nakonec nastavit Idle-PC, to je velmi důležité a sníží to značné vytížení procesoru. Lze změnit později v nastavení zařízení.

Nyní se již možné se pustit do vytvoření topologie sítě. Po spuštění GNS3 se zobrazí dialog pro vytvoření nového projektu nebo otevření dříve uloženého. Začne se pojmenováním nového projektu a zvolením cesty, kam se má projekt uložit. Tímto se

projekt uloží a v hlavní části aplikace je bílé pole, které značí prostor pro přidávání zařízení. Na levé straně hlavního okna programu je řada ikon s motivem zařízení, které daná ikona seskupuje – routery, switche, koncová zařízení, firewally, pak je zde ikona, která zobrazí seznam všech zařízení dohromady a ikona s motivem kabelu s koncovkou, kterou lze využít při spojování zařízení (Obrázek 13).

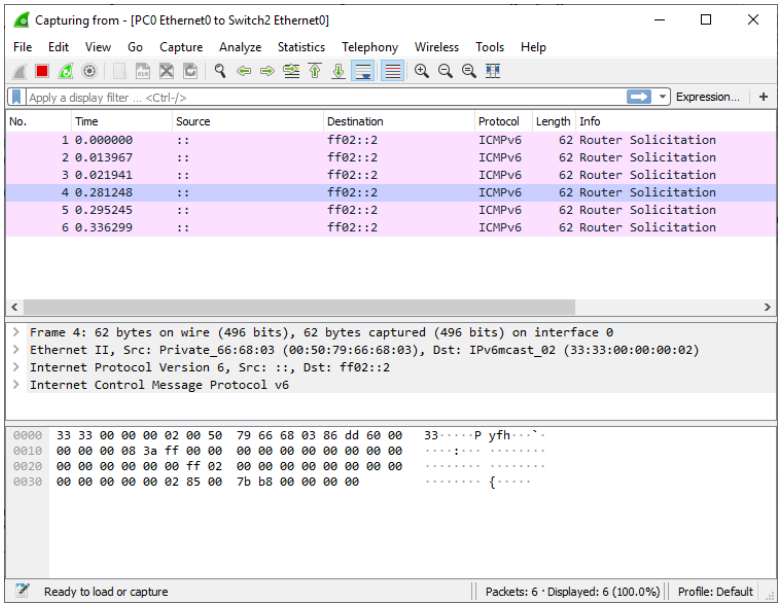
Obrázek 13 Ikony pro zařízení stejného typu.
(Zdroj: vlastní zpracování v aplikaci GNS3)

Po přidání zařízení jim lze upravit název nebo jejich vizuální stránku, a to tak, že na objekt uživatel klikne pravým tlačítkem myši a zvolí „Change symbol“. Objeví se okno, kde je filtr, pomocí kterého má možnost vyhledávat určitý obraz zařízení a poté je zde okno, kde jsou skupiny „Classic“, uchovávající klasické obrázky zařízení. Další skupinou jsou „Affinity-circle-blue“ „Affinity-circle-grey“ a „Affinity-circle-red“, označující logo daného zařízení v kruhu a poslední slovo značí jakou bude mít barvu – zda modrou, šedou anebo červenou. Poslední skupinou jsou „Affinity-square-blue“, „Affinity-square-grey“ a „Affinity-square-red“. To je stejné jako předchozí kategorie s jediným rozdílem, že jak již podle názvu vyplývá, logo zařízení nebude v kruhu ale ve čtverci. Když jsou všechna zařízení přidána na pracovní plochu, upraveny jejich názvy a ikony, je na čase je propojit kabelem. Propojení vzniká tak, že uživatel klikne na poslední ikonu z levé strany ikon. Vybere jedno zařízení a místo kam kabel zapojí. Poté tuto stejnou aktivitu udělá i u druhého zařízení, se kterým to první bude komunikovat. Pokud je kabel zapojen do obou zařízení, rozsvítí se u kabelu kontrolka. Červená, pokud dané zařízení není v provozu a zelená, pokud v provozu je.

V tomto kroku by měla být připravena topologie k použití. Již stačí pouze spustit funkci Play v horním panelu, a i ostatní zařízení, která svítí dosud červeně, by se měla rozsvítit zeleně, pokud jsou správně zapojena, a to z toho důvodu, že uživatel spustil provoz. Dokud provoz nebyl spuštěn, bylo vidět na pravé straně aplikace, že koncová zařízení jsou ve stavu Off podle jejich červeného osvětlení. Pokud jsou spuštěny všechny uzly, tak se koncová zařízení zapnou a kontrolky se rozsvítí zeleně.

Pokud uživatel chce vidět pakety, které probíhají na určitém uzlu sítě, tak na pravé straně aplikace v okně „Topology Summary“ může otevřít nějaké koncové zařízení tak, že klikne na šipku vedle něho. Zde se ukáže spojení, které má. Aby viděl, jaké pakety

probíhají na určitém uzlu, tak klikne na toto spojení pravým tlačítkem myši a vybere „Start capture“. Otevře se vyskakovací okno, ve kterém je typ linky a název souboru, kdyby si to chtěl později uložit. Otevře se aplikace Wireshark (Obrázek 14), která byla instalována již při instalaci programu GNS3. Pokud uživatel spustí všechny uzly, vidí zde, co vše proběhlo na vybraném uzlu. Pokud klikne na nějaký z vypsaných balíčků, vypíše další informace.



Obrázek 14 Ukázka prostředí aplikace Wireshark.
(Zdroj: vlastní zpracování v podpůrné aplikaci Wireshark)

7.2.4 Shrnutí

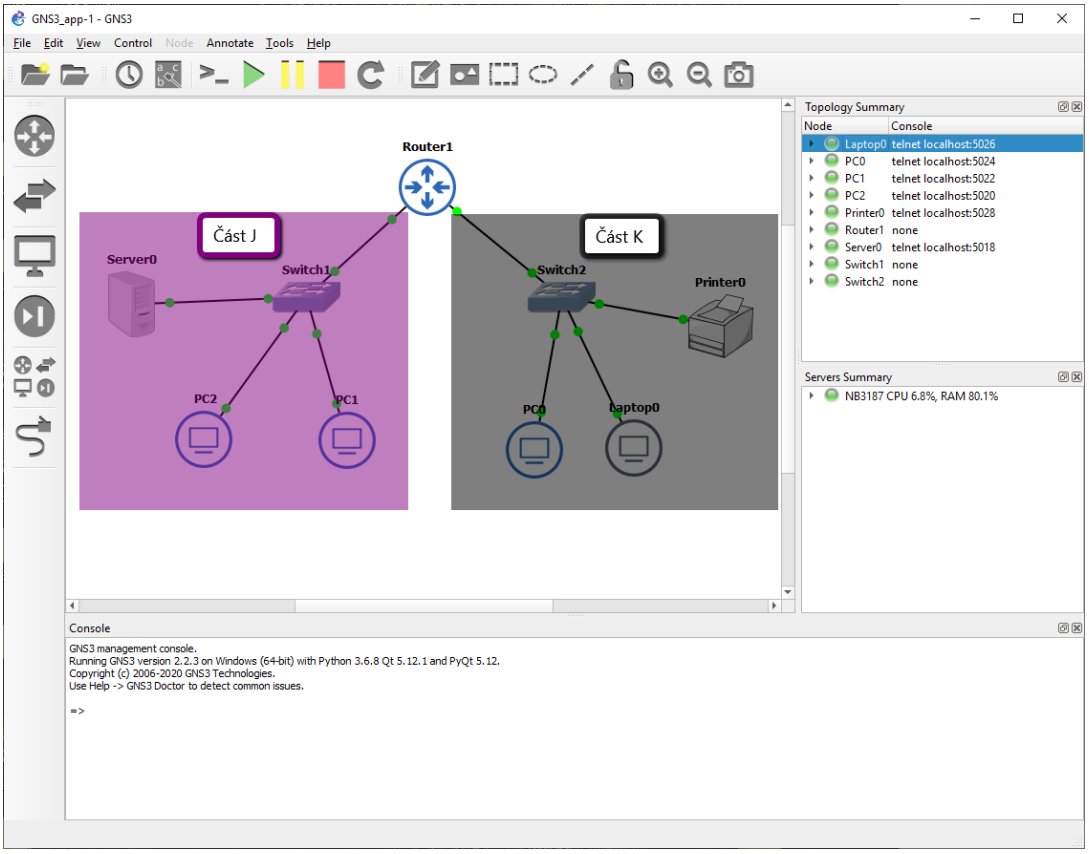
Použití tohoto simulátoru je vhodné k získání zkušeností se zařízeními síťové komunikace, pro testování a experimentování se softwarem reálných zařízení nebo pro ověřování správnosti konfigurací zařízení. Pohodlná instalace, která je prováděna pomocí průvodce nabízí programy, které je potřeba stáhnout k plné funkčnosti aplikace. To pak přináší výhodu v průběhu používání aplikace GNS3, protože doplňující programy jsou již instalovány a nemusejí se hledat na internetu a manuálně přidávat do programu. Ovládání a práce se simulátorem nečiní větší obtíže. Pracovní prostředí je přehledně uspořádáno. Práce programu s operační pamětí počítače je z důvodu náročnosti ošetřena vestavěnými nástroji, přidání a zprovoznění velkého množství síťových prvků je časově náročné z důvodu častého čekání na reakci počítače.

Výhody:

První výhodou aplikace GNS3 je, že je zdarma dostupná na webových stránkách aplikace. Po stáhnutí aplikace a spuštění instalace se otevře jednoduchý průvodce, který uživateli pomůže projít celou instalaci simulátoru. GNS3 je open-source grafický simulátor a díky tomu si ho uživatel může poupravit svým potřebám. GNS3 umožňuje konkrétně upravit hardware díky IOS image, který lze do simulátoru nahrát.

Nevýhody:

Aplikace GNS3 je vytvořena pouze pro studijní účely a nelze ji použít pro produkční prostředí, a to z důvodu propustnosti sítě, které je v rozsahu 1,5 až 800Mb/s. Jak je již popsáno ve výhodách, že si uživatel může nahrát vlastní IOS image, tak je to i menší nevýhoda, že si ten image musí vytáhnout buď z vlastních fyzických zařízení, nebo pomocí Cisco online účtu. Webové stránky aplikace GNS3 žádný IOS image nenabízí. Jednou z hlavních nevýhod, která se týká podobnosti reálné sítě je ta, že je zde pouze jeden druh kabelu na spojování zařízení. Pro české uživatele má GNS3 také nevýhodu, jak je již uvedeno i u aplikace Cisco Packet Tracer, že není dostupná v českém jazyce.



Obrázek 15 Rozdělení topologie v aplikaci GNS3.
(Zdroj: vlastní zpracování v aplikaci GNS3)

7.3 OMNET++

OMNET++ je open-source grafický simulátor, založený na komponentách jazyka C++. Hlavní použití spočívá v modelování počítačových sítí, drátový i bezdrátových, modelování ad-hoc sítí, síťových protokolů, modelování výkonu, fotonických sítí. Jsou poskytovány prostřednictvím modelových rámců vyvinutých jako nezávislé projekty. OMNET++ nabízí IDE založené na Eclipse, grafické běhové prostředí a řadu dalších nástrojů. Existují rozšíření pro simulaci v reálném čase, emulaci sítě, integraci databáze, integraci SystemC a několik dalších funkcí. OMNeT ++ je distribuován na základě akademické veřejné licence. [26]

Komponenty:

- knihovna simulačního jádra (C++),
- popis technologie NED,
- simulační IDE založené na platformě Eclipse,
- interaktivní simulační runtime GUI (Qtenv),
- rozhraní příkazového řádku provádění simulace (Cmdenv),
- dokumentace, ukázkové simulace.

INET Framework lze považovat za standardní knihovnu modelů protokolů OMNeT ++. INET obsahuje modely pro internetový zásobník a mnoho dalších protokolů a komponent. Rámec INET je udržován týmem OMNeT ++ pro komunitu, využívající záplaty a nové modely přispívané členy komunity.

OMPETPP pracuje na následujících operačních systémech. Simulační jádro OMNeT ++ je standardní C ++ a běží v podstatě na všech platformách, kde je k dispozici moderní kompilátor C ++. Simulační IDE vyžaduje Windows, Linux nebo macOS. [26]

7.3.1 Instalace softwaru

V současné době je k dispozici verze softwaru 5.5.1, a je možno si vybrat instalaci pro Linux, Windows, Mac OS, Docker nebo Core bez IDE. Tento simulátor lze stáhnout z webové stránky: https://omnetpp.org/download/, kde si lze vybrat pro kterou platformu je potřeba aplikaci stáhnout. Balíček se stáhne ve formátu zip, který se musí extrahovat do složky, lze využít externí programy, jako jsou Winzip nebo 7zip.

7.3.1.1 Instalace OMNET++

Balíček kromě souborů OMNeT ++ obsahuje kompilátor C ++, prostředí pro vytváření příkazového řádku a všechny knihovny a programy vyžadované programem OMNeT ++. Uživatel zkopíruje archiv OMNeT ++ do adresáře, do kterého ho chce nainstalovat. Vybere adresář, jehož úplná cesta neobsahuje žádné mezery; například neumisťovat OMNeT ++ pod Program Files.

7.3.1.2 Konfigurace a nastavení

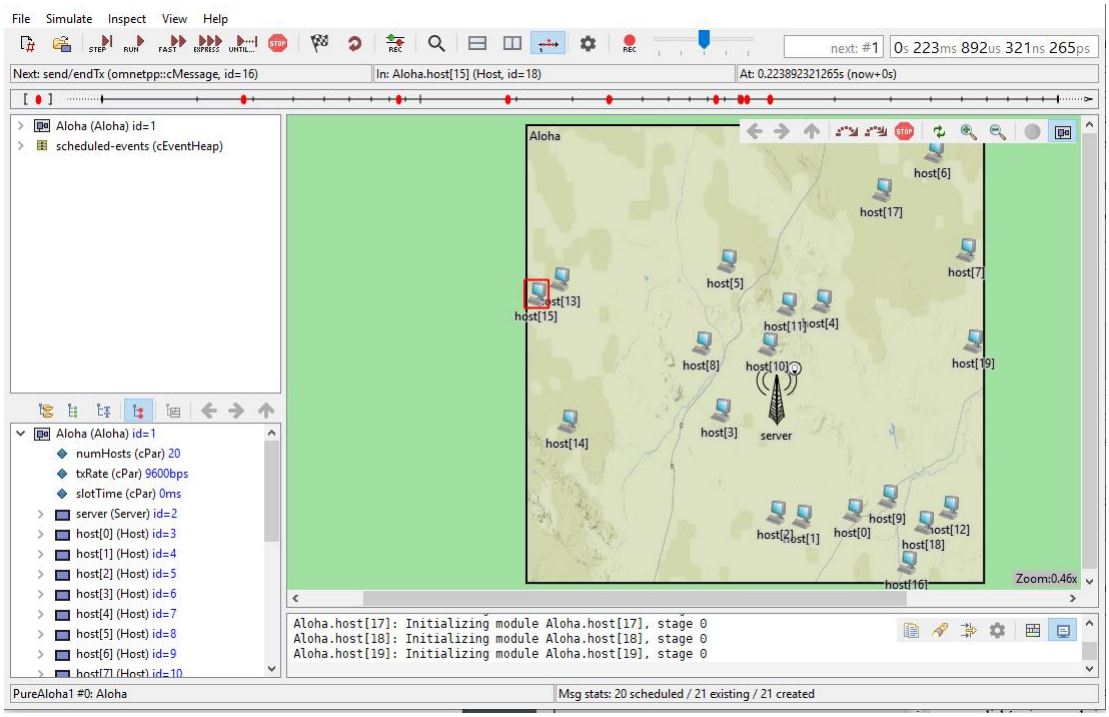
Spuštěním mingwenv.cmd se spustí konzole s bash shell MSYS, s nastavenou cestou k adresáři omnetpp-5.5/bin, kde pomocí shellu začne extrahovat potřebné soubory. Když extrakce souborů skončí, vyzve program ke stisknutí jakéhokoliv tlačítka k pokračování. Následují další dva kroky, které je do shellu potřeba napsat:

```
$ ./configure
$ make
```

Procesy vytvoří binární i ladicí soubory. Pokud jsou tyto kroky hotové, nastává ověření instalace. Vyzkoušejí se všechny vzory a zkontrolují se jejich správná funkce. Například jako první ve složce „samples“ je příklad „aloha“. Kontrola se provede následujícími kroky:

```
$ cd samples/aloha
$ ./aloha
```

První z kroků v shellu převede uživatele do složky aloha v samples. Druhý spustí vzorový příklad aloha. Podle výchozího nastavení bude spuštěn pomocí grafického prostředí Qtenv. Měla by se otevřít GUI okna a dialogy (Obrázek 16).



Obrázek 16 GUI okno příkladu aloha.
(Zdroj: vlastní zpracování v aplikaci OMNET++)

Ve vzorovém příkladu jsou již předpřipraveny komponenty, propojení a předpřipravené toky zpráv s vizualizací. Pro základní fungování programu je toto velmi dobré, že nabízí připravenou síť a uživatel může zkoušet funkce a vlastní síť si vytvoří později.

7.3.1.3 Spuštění aplikace

OMNET++ přichází s Eclipse-based Simulací IDE. IDE by se mělo spustit po zadání následujícího příkazu do příkazového řádku:

```
$ omnetpp
```

Spouštění aplikace přes příkazový řádek je pouze doporučeno. Lze aplikaci spustit i pomocí zástupce pro spuštění IDE. Lze to učinit pomocí souboru „omnetpp.exe“ ve složce omnetpp-5.5.1/ide. K instalaci je dobré si stáhnout i průvodce instalací v pdf formě, který je sice v anglickém jazyce, ale je podrobnější než tento popis. (viz příloha (num)).

7.3.2 Popis prostředí

Vývojové prostředí pro simulace je podobné jako u většiny dalších IDE, to znamená, že je rozděleno na několik částí. Horní část vyplňuje lišta se všemi dostupnými funkcemi a nástroji programu, pod ní je lišta s ikonami pro urychlení výběru funkcí a nástrojů. V levé části se nachází okno Project Explorer sloužící pro vytváření a editaci souborů a jejich zařazování do přehledné struktury projektu simulace. Pod ním je okno zobrazující vlastnosti aktuálně vybraného souboru. V prostředním, centrálním okně probíhá tvorba simulace, kdy lze přepínat mezi návrhovým prostředím a prostředím psaním zdrojového kódu. V pravé části aplikace se nachází paleta nástrojů pro tvorbu. Dolní část je vyhrazena záložkám zobrazujícím chyby kompilace simulace, parametry modulů, jejich hierarchii a závislosti, záložku konsole, logování událostí. Všechna tato okna lze libovolně přesouvat a individuálně upravit tak, aby plně vyhovovala pohodlné práci uživatele.

7.3.3 Vytvoření síťové topologie

Vytvoření začne spuštěním aplikace OMNET++, buď pomocí příkazového řádku, nebo pomocí souboru, jak již bylo popsáno. Založení nového projektu se provede pomocí posloupnosti příkazů File => New => OMNET++ project. Zde se zadává název projektu a cesta, kam se projekt uloží. Poté se přejde k dalšímu kroku, kde se aplikace zeptá, zda uživatel chce čistě prázdný projekt, nebo připravit složky src (zdroj) a simulation (složka pro simulace). Dále zde jsou další dvě možnosti již s předpřipravenými vzorovými topologiemi a simulací.

7.3.4 Shrnutí

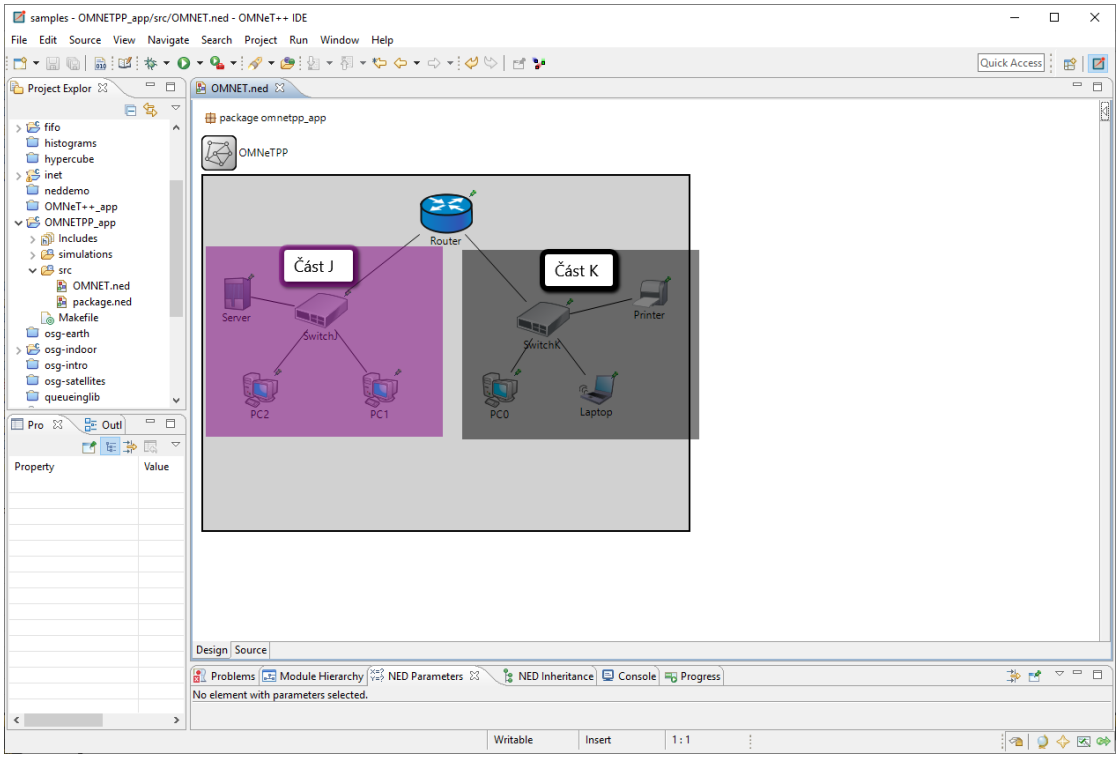
Celkově lze zhodnotil OMNET++ jako výborný nástroj, kde si uživatel dokáže vyzkoušet různé simulace na předem připravených a propracovaných projektech. K vytvoření vlastní simulace je již složitější cesta a uživatel musí znát i programování, aby si simulaci dokázal napsat. OMNET++ má hezky zpracovanou grafickou stránku simulací a velkou množinu možností co uživatel může dělat. Instalace aplikace je trochu složitější, ale zato je připraven dokument, kde je to krok po kroku napsané, jak má uživatel postupovat, takže s instalací nejsou větší problémy.

Výhody:

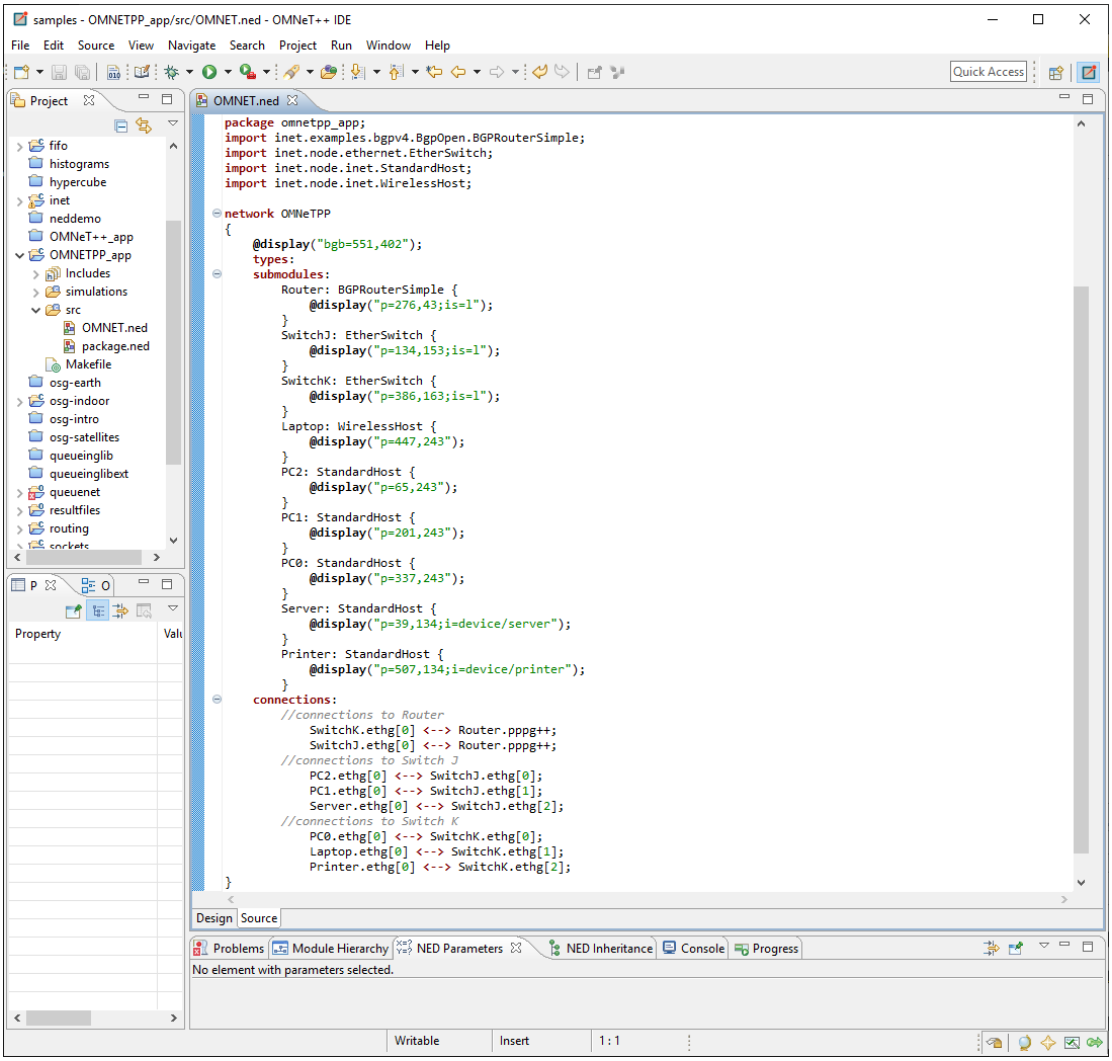
Výhodou aplikace OMNET++ je, že je zdarma dostupná, má velkou škálu možností, co v simulacích lze dělat, ale za podmínky, že si to uživatel připravil.

Nevýhody:

Nevýhodou aplikace OMNET++ je již při začátku, kde je složitější instalace a trvá déle než u jiných simulátorů. Hlavní nevýhodou je, že uživatel si své simulace musí napsat v kódu a není zde například možnost to v GUI připravit a poté upravit část vygenerovaného kódu, která by byla potřeba. OMNET++ má nevýhodu, jak je již napsáno i u aplikací Cisco Packet Tracer a GNS2, že není dostupný v českém jazyce.



Obrázek 17 Rozdělení topologie v aplikaci OMNET++
(Zdroj: vlastní zpracování v aplikaci OMNET++)



Obrázek 18 Topologie sítě v aplikaci OMNET++ pomocí kódu
(Zdroj: vlastní zpracování v aplikaci OMNET++)

8 Srovnávací kritéria simulátorů

V této kapitole je seznam kritérií s jejich podrobnějším popisem pro vysvětlení. Kritéria budou aplikována na každý simulátor síťové topologie pomocí tabulky, pod kterou bude každý bod kritéria popsán na simulátorech. Výhody a nevýhody simulátorů se mohou pro každého uživatele měnit podle jeho priorit kritérií a oblíbenosti stylů používání aplikace a vyhledávání dokumentace.

Porovnávací kritéria:

- Hardwarové požadavky
    - Zde budou vypsány minimální požadavky na systém
- Ovládání simulátorů
    - Simulátor může být ovládán pomocí GUI anebo si uživatel musí topologii naprogramovat.
- Instalace
    - Při instalaci bude zaměřeno na získání instalačního balíčku, poté jestli se simulátor instaluje pomocí dialogového okna, kde uživatel projde instalaci pomocí myši, nebo instalace probíhá v příkazovém řádku. Posledním bodem instalace je, jestli instalační balíček obsahuje všechny potřebné knihovny a aplikace, které jsou potřebné k plnohodnotnému běhu simulátoru.
- Dokumentace
    - V tomto bodě kritérií bude řešeno, jestli vydavatelé k simulátoru mají i dokumentaci, která je volně dostupná na internetu a podle které by se uživatel mohl řídit. Dále jestli jsou nějaké návody či úkoly, jak vytvořit topologii sítě a základní konfigurace. Na závěr porovnávání dokumentace bude, jestli je nápověda uvnitř aplikace.
- Technická podpora
    - Důležitým bodem jsou fóra a komunity pro aplikace, aby se měl uživatel kde poradit, pokud potřebuje pomoc, jak pokračovat nebo mu část funguje špatně nebo jinak, než by chtěl.
- Možnosti návrhu sítě

    - Pro jednoduchost práce se simulátorem je důležité, aby již obsahoval obrazy síťového softwaru, které uživatel bude moct použít v aplikaci a nemusí je hledat jinde.
- Vizualizace topologie sítě
    - Vizualizace sítě je důležitá, aby uživatel simulátoru viděl, jakou síť vytvořil a mohl spouštět simulace.
- Vizualizace toku dat –
    - Vizualizace toku dat je pro uživatele, aby viděl, jak data procházejí různými cestami a sítě a aby jej mohl analyzovat.

9 Porovnání simulátorů

V porovnání simulátorů budou představeny minimální požadavky na hardware. Poté bude poukázáno na ovládání simulátorů, zda se dají ovládat pomocí myši přes GUI, nebo si uživatel musí vše programovat. Na to naváže typ instalace, jestli uživatel provede instalaci pomocí dialogového okna anebo přes příkazovou řádku. Jedním z dalších kritérií byla dokumentace, do které patří dokumentace simulátoru na webu přímo od vydavatele, fórum, zda vydavatel poskytuje návody, jak se simulátorem pracovat a jestli má uvnitř aplikace nápovědu. Velmi podobným tématem je technická podpora aplikace, kde je nejdůležitější fórum nebo nějaká komunita, kam má uživatel možnost napsat svůj problém a lidé mu tam pomohou ho vyřešit.

Tabulka 2 Základní porovnání simulátorů

	Cisco Packet Tracer	GNS3	OMNET++
Hardware			
procesor	2 jádra	2 jádra	Neurčeno
HD	500 MB	1 GB	400 MB
RAM	2 GB	4 GB	512 MB
Ovládání simulátoru			
GUI	✓	✓	✗
Instalace			
Instalační soubor	Dostupný po registraci	Dostupný po registraci	Volně dostupný
Instalační Okno	✓	✓	✗
Příkazová řádka	✗	✗	✓
Obsahuje požadované programy a knihovny	✗	✗	✓
Dokumentace			
Online od vydavatele	✗	✓	✓
Návody	✓	✓	✓
Nápověda v aplikaci	✓	✓	✓
Technická podpora			

Fórum/komunita	✓	✓	✓
Vybavení			
Obraz síťového SW	✓	✗	✗
Vizualizace			
Topologie sítě	✓	✓	✓
Toku dat	✓	✓	✗

Z porovnávací tabulky (Tabulka 2) je zřejmé, že OMNET++ má nejmenší paměťovou náročnost z představených simulátorů. V části kritérií Hardwarové požadavky je také vidět, že Cisco Packet Tracer je méně náročný než GNS3, který potřebuje minimálně dvojnásobný prostor v úložišti i větší paměť RAM.

Při ovládání systému je OMNET++ rozdílný od ostatních vybraných simulátorů, kde uživatel v OMNET++ si musí vše naprogramovat v C++ a poté si to může v okně prohlédnout, oproti tomu v Cisco Packet Traceru a GNS3 lze vytvořit topologii a spravovat všechna zařízení pomocí GUI.

Instalační soubor lze volně stáhnout pouze pro simulátor OMNET++, kde si uživatel vybere, na kterém OS bude simulátor instalovat. U Cisco Packet Traceru i GNS3 se uživatel nejdříve musí registrovat a až poté lze stáhnout instalační balíček. Průběh instalace je také rozdílný pouze u simulátoru OMNET++, který je instalován pomocí příkazového řádku. Podobné to má Cisco Packet Tracer, který by byl instalován v Linuxu. Ve Windows lze instalovat Cisco Packet Tracer i GNS3 pomocí dialogového okna, které lze jednoduše proklikat. U některých simulátorů jsou potřebné další komponenty. Pro Cisco Packet Tracer je to Macromedia Flash Player. U simulátoru GNS3 to jsou Dynamips, Qemu a Wireshark, které se nainstalují v průběhu instalačního procesu aplikace. Poslední simulátor OMNET++ obsahuje požadované knihovny a aplikace přímo v zipu, který lze stáhnout na oficiálních stránkách. Z pohledu běžného uživatele je instalace jednodušší pomocí dialogového okna i přes to, že se uživatel musí pro získání instalačního souboru registrovat na oficiálních stránkách simulátorů.

Dokumentace je převážně pro všechny simulátory stejná, jen s rozdílem, že Cisco Packet Tracer nemá žádnou online dokumentaci přímo od vydavatele, ale pouze umožňuje nápovědy v aplikaci nebo v návodech například v Netacadu.

V rámci technické podpory jsou na internetu fóra nebo komunity, kam uživatelé mají možnost sepsat vlastní problém a jiní odborníci se snaží pomoci s problémem, či vysvětlit dotaz a takováto oficiální komunita je u všech tří simulátorů.

Mezi vybavení přímo v aplikaci vyniká Cisco Packet Tracer, kde si uživatel nemusí shánět obrazy síťového softwaru na internetu, ale tyto jsou obsaženy přímo v aplikaci. U ostatních simulátorů si je uživatel musí obstarat a u OMNET++ si je lze navíc naprogramovat.

Vizualizaci topologie sítě mají všechny tři simulátory, s jedním rozdílem, kde v případě OMNET++ ji uživatel musí naprogramovat a až poté když spustí vizualizaci, tak se zobrazí. Oproti tomu v Cisco Packet Traceru a GNS3 je vizualizace topologie sítě od spuštění aplikace a uživatel tam postupně přidává zařízení a vidí průběžný stav topologie a rozmístění sítě v aplikaci. Vizualizaci toku dat chybí v simulátoru OMNET++, který má k dispozici pouze export datových souborů, které se dají nahrát do jiných aplikací, aby zobrazily grafický výsledek, tento postup jde udělat v aplikaci Matlab. Ostatní dva simulátory mají vizualizaci toků dat, jen s tím rozdílem, že Cisco Packet Tracer zobrazuje data prostřednictvím interního prostředí a GNS3 k tomu používá externí aplikaci Wireshark, která je instalována současně se simulátorem.

10 Závěry a doporučení

Cílem této bakalářské práce bylo představit simulátory datových toků s následným porovnáním. Pro tuto práci byly vybrány typičtí představitelé tří různých skupin simulátorů, a to Cisco Packet Tracer, GNS3 a OMNET++.

V úvodní kapitole byla vysvětlena počítačová síť včetně síťového hardwaru a softwaru. V rámci síťového hardwaru byl popsán ISO/OSI model, topologie sítí a aktivní prvky kabeláže.

V další kapitole byly popsány útoky na počítačovou síť. Konkrétněji jaké dopady může takový útok mít, jaké typy útoků existují a základní obrana, jak útokům předcházet. Na konci dané kapitoly byly představeny konkrétní útoky, jak se vyznačují a k čemu pro útočníka jsou.

V šesté kapitole byla navržena síťová topologie pro malou firmu, ke které byl navržen i půdorys s jednotlivým umístěním koncových zařízení a síťových prvků. Pro lepší představení rozložení síťové topologie do reálného světa.

V praktické části byly představeny již zmíněné simulátory datových toků, u kterých byla popsána jejich instalace, popis základního prostředí aplikace, vytvoření topologie a na závěr byly ke každému simulátoru napsány výhody a nevýhody daného simulátoru.

V poslední části bakalářské práce bylo zpracováno porovnání vybraných simulátorů a popsání každého porovnávacího kritéria.

Simulátory datových toků nemusejí být využity pouze k vytváření topologií pro určité prostory nebo představy a učení se konfigurovat zařízení, ale i jako místo, kde lze vyzkoušet bezpečnostní opatření zařízení a důležitých částí sítě před útoky, které se v simulátorech dají také aplikovat. Lze si vyzkoušet i rychlé znovunastartování síťové infrastruktury, když už k nějakému útoku dojde.

Na tuto bakalářskou prací by bylo možné navázat testováním jiných simulátorů, nebo objektivnější výsledky s probráním určitou skupinou lidí. Důvodem porovnání kritérií více lidmi by mohlo mít výsledek, že jsou lidé, kteří raději pracují v příkazové řádce, nebo rádi programují a v tomto momentě by pro ně byl patrně nejlepší simulátor OMNET++. Podobně rozdílné názory by mohly být i na dokumentaci a na hardwarové

požadavky. V současné situaci, kdy platí omezení spojená s opatřeními proti šíření COVID-19 i na vysokých školách, nebylo možné uspořádat takové přímé setkání a hodnocení a online získání názorů nebylo prakticky možné. Z pohledu autora je nejvhodnější alternativou simulátor Cisco Packet Tracer, který sice nemá online dokumentaci, kterou zbylé dva simulátory mají velmi dobře zpracovanou, ale zato nabízí zdarma dostupné online kurzy pro studenty a integraci do dalších certifikovaných CCNA kurzů.

11 Seznam použité literatury

[1] BIGELOW, S. J. Mistrovství v počítačových sítích. 1. vyd. Brno: Computer Press, 2004. 990 s. ISBN 80-251-0178-9.

[2] FREZZO, Dennis C., et al. Psychometric and evidentiary approaches to simulation assessment in Packet Tracer software. In: Networking and Services, 2009. ICNS'09. Fifth International Conference on. IEEE, 2009. p. 555-560.

[3] HAVLENKA Jiří a kolektiv. Výkladový slovník výpočetní techniky a komunikací. Praha: Vydavatelství a nakladatelství Computer Press, 1997. ISBN 80-7226-023-5.

[4] HORÁK, Jaroslav; KERŠLÁGER, Milan. Počítačové sítě pro začínající správce. Computer press, 2003.

[5] HRŮZA, Petr. Kybernetická bezpečnost. Univerzita obrany, 2012.

[6] HUANG, Keman; SIEGEL, Michael; MADNICK, Stuart. Cybercrime-as-a-service: identifying control points to disrupt. 2017.

[7] JAVID, Sheikh Raashid. Role of packet tracer in learning computer networks. International Journal of Advanced Research in Computer and Communication Engineering, 2014, 3.5: 6508-6511.

[8] JIRÁSEK, Petr; NOVÁK, Luděk; POŽÁR, Josef. Výkladový slovník kybernetické bezpečnosti. Policejní akademie ČR v Praze, 2015.

[9] KLEMENT, Milan. Úvod do problematiky počítačových sítí. Olomouc: Univerzita Palackého v Olomouci, 2015, 64 s. Studijní opora. ISBN 978-80-244-4570-0.

[10] KORET, Joxean; BACHAALANY, Elias. The antivirus hacker's handbook. John Wiley & Sons, 2015.

[11] SIAMWALLA, Rachit; SHARMA, Rosen; KESHAV, Srinivasan. Discovering internet topology. Unpublished manuscript, 1998.

[12] ŠULC, Vladimír. Kybernetická bezpečnost. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2018, 147 s. ISBN 978-80-7380-737-5.

[13] VOLKERT, Thomas, et al. Requirements-oriented path selection for multipath transmission. In: Proceedings of the Joint ITG and Euro-NF Workshop on Visions of Future Generation Networks (EuroView), Würzburg, Bayern/Germany. 2012.

12 Internetové Zdroje

[14] © Jiří Peterka, 2015 Dostupné z: https://www.earchiv.cz/anovinky/ai1552.php3

[15] 5 Best Network Simulators for Cisco Exams: CCNA, CCNP, CCIE. CBT Nuggets [online]. Copyright © [cit. 28.04.2020]. Dostupné z: https://www.cbtnuggets.com/blog/career/career-progression/5-best-network-simulators-for-cisco-exams-ccna-ccnp-and-ccie

[16] Creately. Creately - Your Documents [online]. Dostupné z: https://app.creately.com/diagram/9IHA7zyHX5p/edit

[17] Getting Started with GNS3 – GNS3. GNS3 documentation [online]. Dostupné z: https://docs.gns3.com/1PvtRW5eAb8RJZ11maEYD9_aLY8kkdhgaMB0wPCz8a38/index.html

[18] Introduction to Packet Tracer. CCNA Network Information [online]. Dostupné z: https://www.ccna-study.com/2019/05/introduction-to-packet-tracer.html

[19] Kyberútoky na nemocnice jsou v době koronaviru smrtícím nebezpečím | SECURITY MAGAZÍN. SECURITY MAGAZÍN [online]. Copyright © 2014 [cit. 21.04.2020]. Dostupné z: https://www.securitymagazin.cz/security/kyberutok-na-nemocnici-v-benesove-a-rusky-virus-ryuk-bude-se-situace-opakovat-1404065040.html

[20] Počítačové sítě a jejich typy <články -> SAMURAJ-cz.com. SAMURAJ-cz.com - počítačové sítě, Cisco, Microsoft, VMware, administrace [online]. Copyright © 2005 [cit. 03.11.2019]. Dostupné z: https://www.samuraj-cz.com/clanek/pocitacove-site-a-jejich-typy/

[21] POTÁČEK, Jiří. Počítačová síť. In: KTD: Česká terminologická databáze knihovnictví a informační vědy (TDKIV) [online]. Praha: Národní knihovna ČR, 2003- [cit. 2020-04-14]. Dostupné z: https://aleph.nkp.cz/F/?func=direct&doc_number=000000052&local_base=KTD.

[22] Psimulator2 – a graphical network simulator | Open-Source Routing and Network Simulation. Open-Source Routing and Network Simulation | [online]. Copyright © 2020 [cit. 28.04.2020]. Dostupné z: https://www.brianlinkletter.com/psimulator2-graphical-network-simulator/

[23] Topologie počítačových sítí. Úvodní strana [online]. Dostupné z: http://ijs2.8u.cz/index.php?option=com_content&view=article&id=9&Itemid=116

[24] Visual Basic docs – začínáme, výukové programy, reference. | Microsoft Docs. [online]. Copyright © Microsoft 2020 [cit. 14.04.2020]. Dostupné z: https://docs.microsoft.com/cs-cz/dotnet/visual-basic/

[25] Vše o konstelaci Starlink – ElonX. ElonX – SpaceX, Tesla a další projekty Elona Muska [online]. Copyright © 2020. Všechna práva vyhrazena. [cit. 29.04.2020]. Dostupné z: https://www.elonx.cz/vse-o-konstelaci-starlink/

[26] What is OMNeT++?. OMNeT++ Discrete Event Simulator [online]. Copyright © 2001 [cit. 05.01.2020]. Dostupné z: https://omnetpp.org/intro/

14 Přílohy

1) Install guide pro OMNET++
2) Network in Packet Tracer
3) Network in GNS3
4) Network in OMNET++

Oskenované zadání práce

Zadání bakalářské práce

Autor:	**Jakub Slavíček**
Studium:	I1600606
Studijní program:	B1802 Aplikovaná informatika
Studijní obor:	Aplikovaná informatika
Název bakalářské práce:	**Simulátory provozu na počítačových sítích**
Název bakalářské práce AJ:	Traffic simulators for computer networks

Cíl, metody, literatura, předpoklady:

Cíl práce: Porovnání a testování vlastností a funkčnosti existujících generátorů datových toků na počítačových sítích z pohledu zabezpečení malé sítě. Obsah: 1. Úvod 2. Počítačová síť a útoky 3. Prevence před útoky, jejich simulace 4. Generátory datových toků na počítačových sítí 5. Závěr 6. Seznam použitých zdrojů

BARFORD, Paul, et al. A signal analysis of network traffic anomalies. In: Proceedings of the 2nd ACM SIGCOMM Workshop on Internet measurment. ACM, 2002. p. 71-82. HOQUE, Nazrul, et al. Network attacks: Taxonomy, tools and systems. Journal of Network and Computer Applications, 2014, 40: 307-324. ERLACHER, Felix; DRESSLER, Falko. Testing IDS using GENESIDS: Realistic Mixed Traffic Generation for IDS Evaluation. In: Proceedings of the ACM SIGCOMM 2018 Conference on Posters and Demos. ACM, 2018. p. 153-155. BEHAL, Sunny; KUMAR, Krishan. Characterization and Comparison of DDoS Attack Tools and Traffic Generators: A Review. IJ Network Security, 2017, 19.3: 383-393.

Garantující pracoviště:	Katedra informačních technologií, Fakulta informatiky a managementu
Vedoucí práce:	Ing. Karel Mls, Ph.D.
Oponent:	prof. RNDr. Peter Mikulecký, Ph.D.
Datum zadání závěrečné práce:	21.10.2014