Univerzita Karlova
Pedagogická fakulta

BAKALÁŘSKÁ PRÁCE

2021 Marcel Poláček

Univerzita Karlova

Pedagogická fakulta

Katedra informačních technologií a technické výchovy

BAKALÁŘSKÁ PRÁCE

Laboratoř pro výuku a testování síťových prvků

Lab for learning and testing network devices

Marcel Poláček

Vedoucí práce: prof. Ing. Boris Šimák, CSc.

Studijní program: Specializace v pedagogice

Studijní obor: B – IT

UNIVERZITA KARLOVA
PEDAGOGICKÁ FAKULTA
Katedra informačních technologií a technické výchovy

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

akademický rok 2020/2021

Jméno a příjmení studenta: **Marcel Poláček**

Studijní program: **B7507 Specializace v pedagogice**

Studijní obor: **Informační technologie se zaměřením na vzdělávání**

Název tématu práce v českém jazyce:

Laboratoř pro výuku a testování síťových prvků

Název tématu práce v anglickém jazyce:

Laboratory for teaching and testing network elements

Jazyk práce: **český jazyk**

Stručná charakteristika tématu:

Cílem práce je vytvořit prostředí pro testování síťových prvků bez nutnosti jejich hardwarových součástí, a tak zpřístupnit jejich testování a výuku institucím bez nutnosti pořizovat daný hardware. Součástí práce bude také vytvoření vzorové výukové laboratoře s vybranými síťovými prvky, které bude možné konfigurovat za použití standardního PC, nebo levné varianty. (RaspberryPi apod.).

Zásady pro vypracování:

Proveďte rozbor možných řešení s ohledem na reálné parametry síťových prvků. Definujte základní požadavky na znalosti v oblasti síťových technologií.Výstupem práce budou návrhy řešení virtualizace síťových prvků praktickou výuku počítačových sítí.

Předpokládaná struktura práce:

Uvod – definice základních pojmů a principů v oblasti síťových technologií,
Návrh koncepce virtuální realizace síťových prvků
Relaizace virtuální laboratoře pro testování síťových prvků
Vytvoření vzorové úlohy s příklady možnosti testování, nebo konfigurování daných sítí či navržených sítí.
Zhodnocení navrženého řešení a směry dalšího rozvoje navržené laboratoře.

Seznam doporučené literatury:

Při řešení budou využívány primární a sekundárních informačních zdroje, včetně elektronických, dle tematické orientace práce.

SOSINSKY, Barrie, Pojsl JOSEF a Vaida PAVEL. Mistrovství – počítačové sítě. Brno: Computer press, 2010. ISBN 978-80-251-3363-7.

VELTE, Toby J. a Anthony T. VELTE. Síťové technologie Cisco: velký průvodce. Brno: Computer Press, 2003. ISBN 978-807-2268-573.

TRULOVE, James. Sítě LAN: hardware, instalace a zapojení. Praha: Grada, 2009. Profesionál. ISBN 9788024720982.

Vedoucí bakalářské práce: prof. Ing. Boris Šimák, CSc.

Oponent bakalářské práce:

Předpokládaný rozsah bakalářské práce[1]: 60 normostran

[1] Minimální rozsah bakalářské práce činí standardně 40 normostran (72 000 znaků vč. mezer) vlastního textu.

Prohlašuji, že jsem bakalářskou práci na téma Laboratoř pro výuku a testování síťových prvků vypracoval pod vedením vedoucího práce samostatně za použití v práci uvedených pramenů a literatury. Dále prohlašuji, že tato práce nebyla využita k získání jiného nebo stejného titulu.

Praha

.....

podpis

Touto cestou bych chtěl poděkovat panu prof. Ing. Borisu Šimákovi, CSc. za odborné vedení, náměty a vylepšení této bakalářské práce.

Zároveň bych chtěl poděkovat Soně Poláčkové za jazykovou korektoru a Josefu Koumarovi za cenné nápady a inspiraci.

ANOTACE

Tato práce se zabývá základními typy a vlastnostmi komunikačních technologií. Součástí je také charakteristika a praktické využití jednotlivých prvků. Důležitou částí práce je rozbor daných technologií a jejich následné testování v laboratořích pro výuku či k simulaci sítě. Cílem této práce je objasnit a vytvořit techniky, jak co nejefektivněji a věrohodně simulovat síťové prvky a jejich provoz.

KLÍČOVÁ SLOVA

počítačové sítě, operační systémy, telekomunikační technologie, přenos dat, laboratoř pro testovaní sítí, virtualizace a emulace síťových zařízení

ANNOTATION

This work deals with the basic types and properties of this technology. It also includes the characteristics and practical usage of individual technologies. An important part of the thesis is the analysis of the network technologies and their subsequent testing in laboratories for teaching or a network simulation. The aim of this work is to clarify and create techniques to simulate network elements and their operation as efficiently and reliably as possible.

KEYWORDS

computer networks, operating systems, telecommunication technologies, data transmission, laboratory for network testing, virtualization and emulation network devices.

1 Obsah

2 Úvod

Síťová infrastruktura definuje a určuje komunikaci mezi zařízeními. Je velmi mnoho typů sítí, a také velmi mnoho způsobů, jak je budovat. Existují však některé standardy, které je nutné, nebo přinejmenším vhodné, dodržovat. Dnes tak tvoří nedílnou součást moderní doby a nároky na jejich provoz a fungování jsou každým rokem čím dál větší.

Koncová zařízení zahrnují počítače, notebooky, servery, tiskárny, chytré telefony nebo například IoT[1], tudíž jakékoliv zařízení připojené k veřejné či neveřejné síti.

Proto je nutné v dané problematice edukovat odborníky a také testovat nové nebo stávající sítě. Je kladen stále větší důraz i na znalosti uživatelů v této oblasti. V této práci se k tomuto účelu rozebírají základní termíny a techniky využívané v této oblasti pro následné aplikace v tematických úlohách, pro experimentální či edukační účely. Vzhledem k faktu, že hardwarové prvky jsou velmi drahé, a proto je jejich testovaní ekonomicky výhodné pouze pro velké subjekty či univerzity, budou v práci využity i emulační programy pro zajištění maximální cenové dostupnosti, zejména pro edukační účely.

Cíl práce je najít a vytvořit řešení, které splňuje výše zmíněné požadavky, aby bylo výsledné řešení maximálně možno dostupné pro všechny instituce.

[1] Internet věcí (anglicky – Internet of Things) jsou fyzická zařízení, často menších rozměrů, vytvořená pro určitý účel (termostat, kamera apod.), a která jsou připojena k internetu.

3 Základní síťové prvky

Síťové prvky jsou zařízení umožňující komunikaci na určité síťové vrstvě modelu sítě [1]. Mezi nejčastěji používané prvky patří směrovač (router), přepínač (switch) a přístupový bod (access point). V této práci se bude nadále využívat jejich anglické pojmenování. Mezi laickou veřejností se tato zařízení nejčastěji používají ve sloučené a menší verzi. Bez těchto zařízení se žádná síť neobejde, a je proto důležité vyvíjet stále nové a lepší technologie i z důvodu exponenciálních růstů síťového provozu. V domácnostech se často využívá jeden prvek či jedno zařízení slučující funkce více zařízení, který obsahuje uživatelsky příjemné prostředí pro nastavení. Ve větších institucích se již setkáme s mnoha typy switchů, jak na vrstvě L2 nebo L3 síťového modelu, routerů a z důvodu kvalitního bezdrátového připojení i s velkým množstvím access pointů.

3.1 Switch

Aktivní síťový prvek pracující na druhé síťové vrstvě se nazývá switch. Rozděluje se na dva hlavní typy – bez možnosti konfigurace, nebo s přístupem ke konzoli k zařízení pro jeho nastavení. Switch se v základním nastavení chová deterministicky, pokud není nijak upraven. Podle CAM tabulky [2], která je vytvořena na základě znalosti adres koncových zařízení, směřuje rámce na daného příjemce, kterému jsou určeny.

Switch může mít i možnost PoE[2], která se dá využít pro napájení například bezpečnostních kamer, přístupových zařízení apod. Existují různé velikosti přepínačů od domácích, zpravidla kolem 8 až 16 portů, až po industriální, do 48 portů. Rovněž jsou vybaveny různými typy konektorů (portů), které mohou být nejčastěji typu RJ45 nebo různých řad modulů SFP (SFP, SFP+, QSFP apod.) [3]. Méně často se mohou přepínače rozdělovat podle přístupu k přenosu. Nejvyužívanější jsou dva přístupy, cut-through nebo store and forward [4]. Každá metoda je vhodná pro specifickou formu přenášení dat. V případě požadavku rychlého přenosu dat s krátkou odezvou ale s větší chybovostí, je vhodná metoda cut-through, v případě požadavku na stabilní připojení s kontrolními mechanismy, je doporučeno využít metodu store and forward [4].

[2] Power over Ethernet – je způsob přenosu elektrické energie (slaboproudé) po ethernetových rozvodech provedených pomocí kabelu UTP nebo STP.

3.1.1 Funkce Switche

Zařízení je uzpůsobeno pro propojování koncových zařízení, jako jsou například tiskárny nebo počítače. Dražší switche podporují i technologii VLAN, díky které mohou jednotlivým portům přiřadit i síť virtuální. Switche na úrovní L3 jsou schopny i základního směrování, jako je například interVLAN routing[3].

3.2 Router

Router je aktivní síťový prvek pracující na třetí síťové vrstvě. Díky tomu je schopen zpracovávat pakety a je tedy hlavním zařízením mezi interní a externí (internet) sítí. Můžeme se setkat i s verzí switche pracující současně na vrstvách L2 i L3. Takový switch je mnohem mocnější a kombinuje výhody switche a doplňuje jej o základní funkce routeru. V domácích podmínkách se toto zařízení často nesprávně označuje jako prvek s wi-fi a mnoha switch porty. Toto označení je ale zavádějící. Správné označení je proto router+switch+ap, které jsou realizované pouze v jednom zařízení pro jednoduchost a menší rozměry. Router je tedy zařízení, které slouží pro směrování paketů mezi sítěmi, ať už interními nebo externími (WAN). Velmi často pomíjená vlastnost těchto zařízení je jejich samotný výpočetní výkon, tj. velikost paměti RAM, počet a takt procesorů, jenž má vliv na schopnost obsluhovat velký počet připojení. V menších provedeních má router pouze dva porty (pro síť WAN a interní), v praxi se ale využívá i více portů pro např. failover [5], připojení k více ISP providerů. Tato zařízení jsou také vybavena bránou (síťovým firewallem), díky které je možné filtrovat provoz a zajistit tak větší bezpečnost interní sítě.

3.2.1 Funkce Routeru

Umožňuje rozdělit síť do podsítí (subnetů). Umožňuje hierarchicky členit síť, ve které se nachází koncové zařízení. Funkce routeru je i bezpečnostní, kdy je možné při použití technologie NAT chránit koncová zařízení a nepřipojit je tak přímo do veřejné sítě.

3.3 Access point

Zařízení, které se ve velké míře využívá k vytváření bezdrátových sítí, se nazývá access point. V dnešní době je tato technologie často upřednostněna před pevným kabelovým připojením. Vyznačuje se velikou dostupností a velmi jednoduchým připojením. Často některé koncové stanice, zejména mobily, a i některé notebooky nejsou vybaveny síťovou kartou pro kabelové připojení a mají pouze bezdrátové síťové rozhraní. Nevýhoda této technologie je úzce

[3] *Inter-VLAN Routing* – způsob distribuce VLAN a základních routovacích cest [online]. Dostupné z: https://www.ciscopress.com/articles/article.asp?p=3089357&seqNum=4

vymezené bezlicenční pásmo, případně i nestabilita při připojení více klientů. V neposlední řadě je i cena, kdy pokrytí kvalitním signálem může vyjít i na desítky tisíc korun, v závislosti na technologii a výrobci. V ideálním případě je dobré tuto technologii kombinovat, kdy zařízení se stálou pozicí jsou připojeny drátově a ostatní koncové stanice jsou připojeny bezdrátově nebo kombinují obě možnosti. Tím se sníží nároky na bezdrátovou síť. Kabelové připojení je také ve většině případů rychlejší.

3.3.1 Funkce Access pointu

Aktivní síťový prvek pro bezdrátové připojení koncových stanic. V současné době využívá bezlicenční pásmo na frekvencích 2,4GHz a 5GHz ve standardech 802.11 a,b,g,n,ac nebo nejnovější standard ax. Existují také bezlicenční pásma na vyšších frekvencích, například 60GHz. Ty jsou ale určené především pro spoje P2P, tedy bezdrátová spojení dvou bodů (sítí).

4 Topologie sítě

Topologie je schéma propojení jednotlivých uzlů sítě. Topologie sítě mohou být různé, některé typy topologie ale skoro zanikly z důvodu přechodu na jinou technologii. Existují propojení podle logického nebo fyzického modelu. Nedílnou součástí topologie je užitá strukturovaná kabeláž, díky které se spojují koncová zařízení do sítě.

4.1 Základní topologie

Existují tři základní druhy topologie. První a nejstarší je sběrnicová technologie, dnes již málo využívaná. V dnešní době se nejčastěji setkáme se zapojením do hvězdy, do kruhu nebo s kombinací pro zajištění maximální dostupnosti a případné alternativní trasy pro fail over linku, kdy je i možné zapojovat jednu trasu více spoji a tím vytvořit linku s větší propustností, tak i se záložními cestami v případě přerušení kabelu.

4.1.1 Zapojení do sběrnice

Nejstarší technika propojení koncových stanic je zapojení do sběrnice. Na technologii je výhodná úsporná forma připojení koncových zařízení, které sdílí jeden okruh (kabel), a tudíž sítě s touto topologií nejsou drahé na výstavbu. Také je možné použít koaxiální kabely v rozvodech pro televizní signál, čehož dodnes využívají někteří operátoři pomocí technologie DOCSIS. Tato technologie ale využívá mnohem vyšší frekvence než klasický koaxiální ethernet z 90. let. V historii se pro propojení stanic využíval koaxiální kabel zakončený buď

stanicí, HUBem, nebo terminátorem[4]. Čím více je připojených bodů, tím přibývá broadcoastů a v případě neřízené komunikace taky kolizí. Pro komunikaci se v sítích typu Ethernet používá metoda CSMA/CD (Carrier-sense multiple access/collision detect) nebo CSMA/CA (Carrier-sense multiple access/collision avoid). Platí proto nerovnice, kdy čím více máme komunikujících klientů, tím menší je přenosová rychlost a s tím i odezva.

4.1.2 Zapojení do hvězdy

Toto zapojení se nejčastěji používá pro připojení koncových zařízení. Je to velmi oblíbené řešení, kdy se ve středu nachází switch, případně i router. Výhoda tohoto zapojení je, že každý má svůj vyhraněný komunikační okruh (v tomto případě celý kabel), a tak se linka na spoji mezi koncovým bodem a středem hvězdy s nikým dalším nesdílí. Nevýhoda zapojení spočívá v drahé realizaci, kdy je potřeba velké množství zásuvek (portů) a kabelů pro připojení každého koncového zařízení.

4.1.3 Zapojení do kruhu

Toto zapojení je charakteristické pro odolnost vůči výpadku jednoho bodu. Oproti předchozím topologiím se v případě výpadku neovlivní komunikace v síti a ostatní stanice komunikují dál. Využívá se zejména na propojovacích trasách mezi routery nebo switchi, pro realizaci mezi koncovými stanicemi je tato varianta velmi nákladná a vyžadovala by minimálně dvě síťová rozhraní v každé stanici.

4.1.4 Kombinované zapojení

V praxi se můžeme setkat i s kombinací hvězdy a kruhu. Vysoce dostupné sítě by se takto i měly plánovat, a tím tak předcházet výpadku, který by ovlivnil nedostupnost dané sítě.

5 Strukturovaná kabeláž a standardy

Nedílnou součástí jakékoliv sítě je strukturovaná kabeláž. Pomocí ní je možné rozvádět danou síť po místnostech, patrech, ale i v ulicích a mezi městy. Její plánování je velmi důležité i z toho důvodu, že většina kabeláže se skrývá pod omítky nebo pod zem, a tak změny či vylepšení kabeláže nejsou jednoduché. Je proto výhodné dané rozvody realizovat do servisních kanálů nebo tzv. husích krků, které umožňují výměnu kabelů, či přidání dalších. Strukturovanou kabeláž můžeme dělit i podle různé různých druhů přenosového media.

[4] Terminátor – je zakončení na koaxiálním kabelu pro správné zakončení nevytvářející přeslechy [online]. Dostupné z: https://networkencyclopedia.com/terminator/

Zpravidla se jedná o metalické kabely typu UTP nebo STP [6], pro rychlejší a páteřní spoje se využívají i optické kabely, multimode nebo singlemode[5], v závislosti na vzdálenosti.

Standard, popisující hlavní parametry kabeláže, je označen jako EIA/TIA[6] 568. V současné době se ale prosadily revize EIA/TIA 568-B nebo EIA/TIA 568-C. Nejlepší možná volba je v současné době, pro budování moderních sítích, varianta EIA/TIA 568-C, kterou podporuje většina techniků.

5.1 Standard EIA/TIA 568-C a její součásti

Tento standard se rozděluje do čtyř částí, C.0, C.1, C.2 a C.3. Tyto části standardu detailněji popisují jednotlivá přenosová média a stanovují jim parametry. Odděluje tak nároky na kabeláž od ostatních požadavků na danou síť.

5.1.1 Kategorie UTP kabelů

Označení kabelu	Průřez [mm^2]	Impedance [Ω] 10% odchylka	Frekvenční pásmo [MHz]	Využívaný standard pro komunikaci
CAT 1 / Kategorie 1	0,128-0,823	-	Telefonní pásmo pro zvonkové rozvody	Telefonní rozvody/ zvonkové rozvody
CAT 2 / Kategorie 1	0,128-0,324	-	≤ 1,5 MHz	Analogový telefon
CAT 3 / Kategorie 1	0,205-0,324	100Ω	≤ 16 MHz	10BaseT, 4/16 Token Ring
CAT 4 / Kategorie 1	0,205-0,324	100Ω	≤ 20 MHz	10BaseT, 4/16 Token Ring
CAT 5+5e / Kategorie 1	0,205-0,324	100Ω	≤ 100 MHz	100BaseTX, ATM, 1000BaseT (4)
CAT 6 / Kategorie 1	0,205-0,324	100Ω	≤ 500 MHz	1000BaseTX
Ex. CAT 6 /	0,205-0,324	100Ω	≤ 500 MHz	10GBaseT
CAT 7 / Kategorie 7	0,324	100Ω	≤ 1200 MHz	10GBaseT, multimédia

Tabulka 5-1 Výkonnostní kategorie UTP kabelů

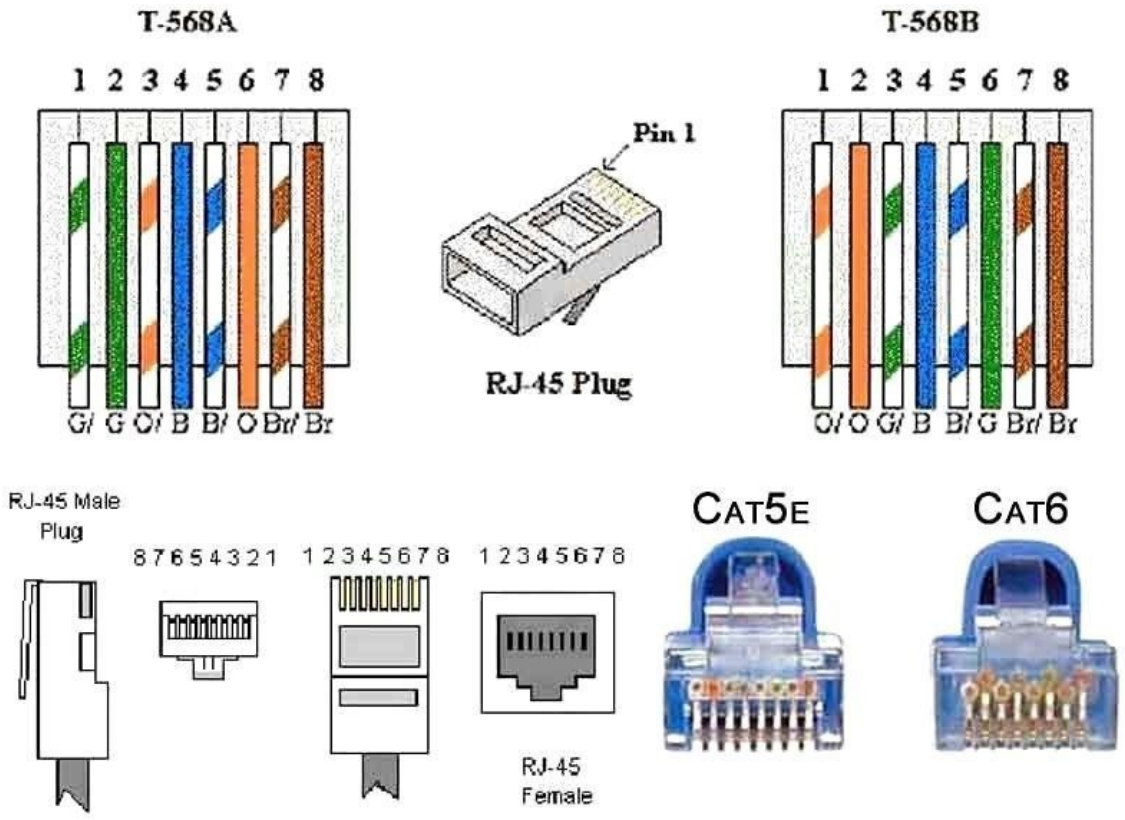
[5] Technologie komunikace na optických vláknech – Fiber *Optic Cable Types* [online]. Dostupné z: https://community.fs.com/blog/single-mode-cabling-cost-vs-multimode-cabling-cost.html

[6] Podrobnější specifikace normy a parametrů [online]. https://www.csd.uoc.gr/~hy435/material/TIA-EIA-568-B.2.pdf

V dané tabulce *5-1* je v dnešní době využívaný přednostně typ kabelů CAT 5e nebo vyšší. Omezující faktor komunikace je šířka pásma. Rychlost přenosu přímo závisí na druhu kódování.

5.1.2 Konektory

Standard počítá s využitím konektoru označení RJ45. Existuje několik druhů zapojení samotných kabelů. Mezi hlavní standardy se řadí způsob zapojení podle normy T568A nebo T568B. U některých institucí se můžeme setkat i s různými modifikacemi, které jsou realizovány z bezpečnostních důvodů. Piny totiž v případě špatného zapojení nemusí fungovat maximální možnou rychlostí, nebo vůbec. Konektor má osm pinů pro čtyři páry kroucené dvojlinky. Pro rychlost 100BaseTX stačí pouze dva páry.



Obrázek 5-1 Zapojení kabelů do RJ45 konektoru

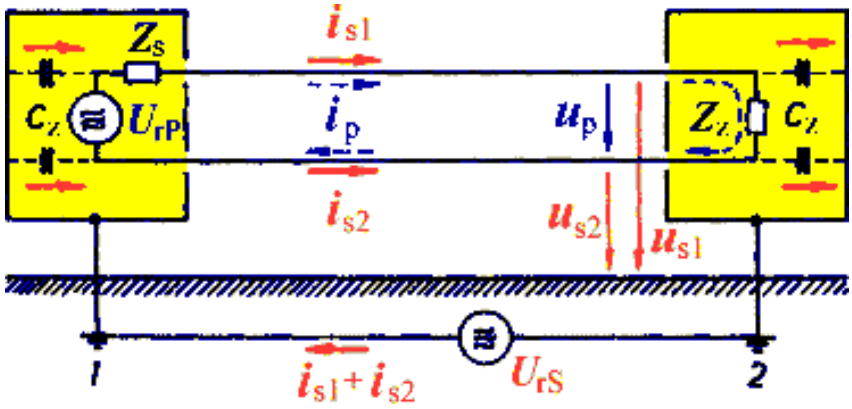
(zdroj: https://www.pinterest.com/pin/378443174942791961/)

Při vytváření kabelů je zapotřebí použít speciální kleště, které všech osm pinů nalisují do umístěných kabelů. Tento proces je nevratný a v případě špatného kontaktu je nutné konektor ustřihnout i s vodiči a nahradit ho novým. Proto by se při instalaci mělo počítat

s rezervou a v rozvodech nechávat na koncích kabel o pár desítek centimetrů delší pro pozdější úpravy. Při nacvakování konektorů je dobré zkoušecím přístrojem kabel otestovat a ujistit se, že všechny piny dokonale vodí elektrický signál a jsou správně pospojovány. Také se ověří nenarušení vedení na celé trase.

5.2 Kroucená dvoulinka

Kroucená dvojlinka se v současných sítích používá nejčastěji, i když je v případě modernizace nahrazována optickou přípojkou. Má ale nesporné výhody, je všestranná, není drahá a snadno se instaluje. Kroucený pár kabelů, který je typický pro kroucenou dvojlinku, má délku zkrutu podle přesné délky z důvodu eliminace vlivu rušivého elektromagnetického pole. To by ovlivňovalo druhý vodič a zároveň zkrátilo dosah vedení. Tento způsob vedení datových kabelů je využit i v kabelu typu UTP nebo STP.



Obrázek 5-2 Rušivý soufázový signál na vedení

(zdroj: http://www.elektrorevue.cz/clanky/02032/Image279.gif)

Proudy i_s a napětí u_s na vodičích se společným zemnícím kabelem mají stejný směr a vytváří tak soufázový rušivý signál, který vzniká zejména vlivem parazitních zemních potenciálů označených jako U_{rS}.

5.3 Elektrická charakteristika elektricky vodivých kabelů

Jakýkoliv telekomunikační kabel musí mít přesně stanovené hodnoty jeho vlastností a odporů, aby bylo možné správně signál přenést. Vzájemnou kvalitu spojení ovlivňuje i samotný průřez vodičů nebo jejich vzájemná poloha. Charakteristická impedance[7] je hodnota, která s těmito faktory pracuje. Pro datové sítě se nejčastěji využívají kabely s hodnostou 100, 120, nebo 150

[7] *Twisted-Pair Impedance* [online]. Dostupné z: https://www.allaboutcircuits.com/tools/twisted-pair-impedance-calculator/

Ω. Standardní UTP kabel má impedanci 100 Ω. V případě stíněné verze, označované jako STP, má impedanci 150 Ω. Důležitým parametrem je také útlum na vedení v dB [decibel].

Vzorec pro výpočet útlumu je $10 \log_{10}$ = (vstupní výkon P / výstupní výkon P).[8]

5.4 Optické kabely

Optické kabely mají jedinečné vlastnosti a schopnosti, které se velmi liší od UTP/STP kabeláže. Tato technologie má své výhody, ale i nevýhody, oproti metalicky vodivým kabelům. Hlavní problém UTP nebo STP kabeláže je její omezená kapacita přenosu v závislosti na vzdálenosti (útlumu). U těchto kabelů při použití standardu CAT5e nebo vyšší není problém dosáhnout rychlosti 1Gbit/s do cca 100 m. Při vyšších rychlostech pomocí SFP modulů v řádu jednotek až desítek Gigabitů ale rapidně klesá maximálně možná délka linky. Tyto nevýhody metalické kabeláže částečně řeší využití optických kabelů.

Optické kabely jsou schopné přenášet optický signál od několika metrů (v případě multimode kabelu) po několik kilometrů (v případě jednovidového kabelu). Výhoda je také v nevodivých částech kabelu, kdy data nejsou ovlivňovány rušením nebo přeslechy. V neposlední řadě jsou tyto technologie výhodné pro ISP[9] providery, kdy nemusí mít v některých rozvodech aktivní síťové prvky, a tak nejsou závislé na elektrické energii.

Velkou nevýhodou je ale jejich cena, která je sice vyvážena šířkou pásma a přenosových schopností, nicméně zakončování, spojování, a i samotné aktivní prvky jsou dražší než při metalické verzi. Při spojování je nutné použít drahých svářeček, které dokáží spojit dvě vlákna tak, aby ve spoji nevznikaly odrazy či útlum.

V současnosti je velmi moderní technologie FTTH neboli Fiber To The Home. Princip spočívá v zavedení optického kabelu přímo k zákazníkovi, což je pro poskytovatele finančně náročnější, nicméně výhody této technologie jsou do budoucna jedinečné. V častějším případě se setkáme s metodou FTTC (Fiber to the courb) nebo FTTP (Fiber to the point). Tyto technologie jsou víceméně shodné, jsou postaveny na principu předsunutého bodu, do kterého je přivedený optický kabel, a na posledních pár metrů k připojení koncového zařízení je použita technologie přes UTP nebo ADSL, pokud zvažujeme pouze drátové možnosti spojení.

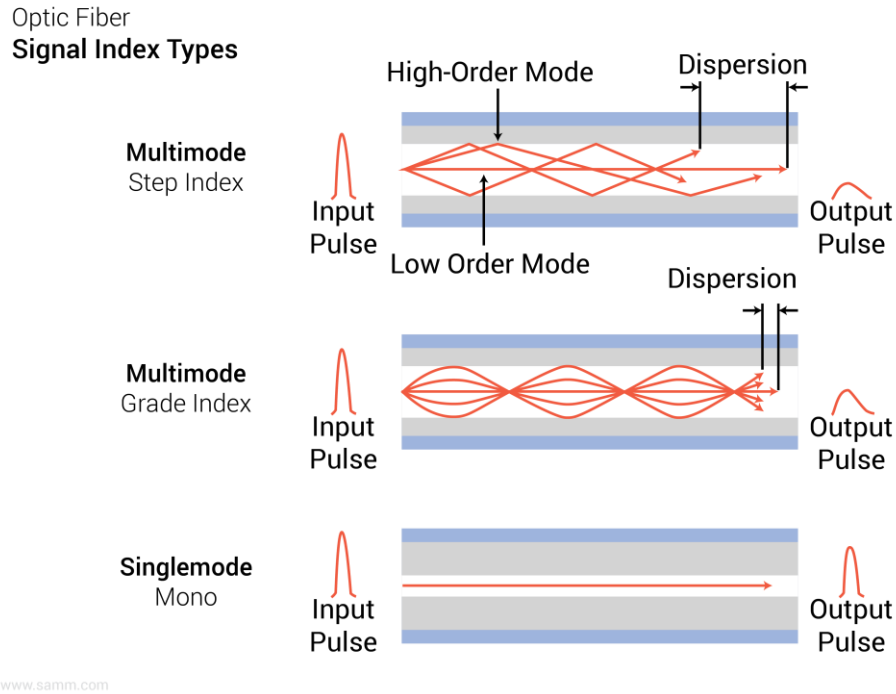
[8] Aplikace pro výpočet technických údajů a simulace pro telekomunikační technologie - http://matlab.feld.cvut.cz/
[9] ISP – Internet Service Provider, poskytovatel internetového připojení

Optické připojení je v současné době nejlepší přístup, jak připojit klienty k veřejné síti WAN, nicméně i metalická kabeláž má svoji budoucnost. Pro připojení koncových stanic (počítačů apod.) je to v současné době jediná forma připojení, které je úměrné cenou a rychlostí.

5.4.1 Konstrukce optických kabelů

Tyto kabely se vždy skládají z optického vlákna a několika druhů izolace. Existují dva typy ochrany optických vláken, těsné nebo volné. Těsná sekundární ochrana je přilepena přímo na optické vlákno, zatímco volná varianta má kabely umístěny volně v chránicí izolaci.

Důležitým parametrem je průměr, který určuje vlastnosti. Nejčastěji se používají vícevidová vlákna o rozměrech 62,5/125 µm. První číslo udává průřez vlákna a druhé průřez jeho obalu. Celkový průměr má kolem 900 µm, ale většinu tvoří sekundární izolace.



Obrázek 5-3 Typy optických kabelů

(zdroj: https://telecom.samm.com/Data/EditorFiles/images/blog/what-is-fiber-optic/fiber-optic-cable-types-signal-indexing-01.png)ém

Pro přenos optiského signálu pomocí optického kabelu se využívá síťové rozhraní s polovodičovou laserovou diodou, která do daného vlákna vyzařuje světlo o vlnové délce 800-1550 nm. Optické kabely mají výhodu ve velké šířce pásma a malém útlumu. Přibližně platí čím větší vlnová délka, tím menší útlum.

	Vícevidové vlákno 62,5/125µm		Jednovidové vlákno 8µm	
Vlnová délka nm	850	1300	1310	1550
Útlum (dB/km)	3,5	1	0,5	0,4

Tabulka 5-2 Závislost vzdálenosti na typu optickém kabelu

Šířka pásma závisí na konstrukčním uspořádání, na materiálu optického vlákna a na vlnové délce optického signálu. V současnosti se na meziměstská spojení používají již výhradně optické kabely, případně je součástí kabelu i měděné jádro pro přívod elektrické energie. To se využívá například pro napájení aktivních síťových prvků na trase.

Základními parametry optického vlákna[10]

- šířka pásma [MHz . km];
- numerická apertura (NA);
- disperze;
- útlum [dB];
- ztráty na makroskopických neregularitách;
- minimální poloměr ohybu;
- obsah OH;
- u jednovidových vláken parametr MFD.

U jednovidových vláken je mezní vlnová délka λ_c (cutoff wavelength), což je nejkratší vlnová délka, při které se vlákno projevuje jako jednovidové. To znamená, že jednovidové vlákno se může v závislosti na vlnové délce optického paprsku stát mnohovidovým. Přechod z jednovidového do mnohovidového režimu se uskutečňuje postupně. Prakticky je do jednovidového vlákna vždy vysílán paprsek s vlnovou délkou větší, než je mezní vlnová délka λ_c.

6 Bezdrátové síťové technologie

V dnešní moderní době se již neobejdeme bez bezdrátových technologií a zejména bez připojení k síti pomocí Wi-Fi. Tento způsob připojení je poměrně mladý,

[10] Zdroj a podrobnější specifikace – Optoelektrotechnika, parametry optických vláken [online] https://publi.cz/books/185/06.html

nicméně již za tu dobu se vyvíjel velmi rychle i z důvodu, že tento způsob připojení je stále více preferovaný. Nikdy však nebude technicky možné vyrovnat se kvalitativně pevnému připojení. Jsou však situace, kdy je toto připojení vhodnější a snazší. Moderní zařízení jako smartphony nejsou ani vybaveny ethernetovým portem. Budování sítí se pomocí bezdrátových technologií zjednodušuje a díky nim je možné pokrýt veškerou potřebnou oblast signálem bez nutnosti velkého množství kabelů a přípojných bodů.

6.1 Princip bezdrátových sítí

Základním principem je přenos elektromagnetických vln neboli mikrovln, vygenerovaných ve vysílači a přijatých přijímačem. Různé úrovně vln zastupují jednotlivé hodnoty, ze kterých lze vyčíst jejich úrovně. Samotný přenos je velmi sofistikovaný a obsahuje mnoho synchronizačních, řídících, ale i mnohdy šifrovacích mechanismů. Zařízení mohou být vybaveny i více anténami pro zajištění větší propustnosti. Tato technologie je označována jako MIMO[11] (Multiple In, Multiple Out) a udává se v hodnotách A x B, kdy A je číslo udávající počet antén přijímacích a B počet antén odesílacích.

Radiové vysílání probíhá vždy na tzv. nosné frekvenci, což je základní frekvence, která je definována a standardizována. Tyto standardy vyjadřují skupinu nosných frekvencí jako pásma frekvencí. Ty se dělí na pásma licencované a nelicencované. Základní rozdíl mezi nimi je v jejich dovoleném využívání. Je totiž velmi mnoho systémů bezdrátových spojení, pro které je poměrně malý interval frekvencí pro dané užití. Některé frekvence jsou vhodné pro rozhlasové stanice a některé jsou vhodné pouze pro P2P spoje. V každém státě existuje proto úřad, jenž tyto příděly kmitočtů rozděluje. V České republice je takovou institucí Český telekomunikační úřad, označován zkratkou ČTÚ. Tento úřad definuje, jaké frekvence jsou vyčleněny rozhlasovým, televizním a mobilním operátorům, meteorologickým stanicím, ale i jaké jsou bezlicenční frekvence neboli frekvence, na které není potřeba získat licenci od daného úřadu. Celosvětově rozděluje kmitočtové příděly jednotlivým státům mezinárodní telekomunikační unie ITU.

[11] Podrobnější popis technologie MIMO – Intel Wirelles products [online] https://www.intel.com/content/www/us/en/support/articles/000005714/wireless/legacy-intel-wireless-products.html

7 Protokol TCP/IP

Vznik tohoto standardu se přisuzuje instituci nazvané ARPANET. Hlavním cílem této organizace bylo decentralizovat telekomunikační síť, která byla v této době centralizovaná. Základní vlastností decentralizace je absence centrální autority.

Přenos dat v hostitelské telekomunikační síti byl bod - bod. Nicméně však v danou chvíli ~~linku~~ vedení není možné využít pro další spojení. V této době existovalo spojení na základě přepojování okruhů (circuit switching) hojně využívané v telekomunikacích.

V současné době je tato technologie klíčová pro datovou komunikaci. Obsahuje mnoho protokolů a síťová komunikace je rozdělena na vrstvy, původně ISO/OSI o sedmi vrstvách, dnes se využívá spíše zjednodušená varianta modelu TCP/IP o čtyřech základních vrstvách.

7.1 Architektura TCP/IP

V současnosti se pracuje s dvěma modely síťové architektury.

Vrstva	RM ISO/OSI	TCP/IP
L1	Fyzická vrstva	Vrstva síťového rozhraní
L2	Spojová (Linková) vrstva	
L3	Síťová vrstva	Síťová vrstva
L4	Transportní vrstva	Transportní vrstva
L5	Relační vrstva	Aplikační vrstva
L6	Prezentační vrstva	
L7	Aplikační vrstva	

Tabulka 7-1 Jednotlivé vrstvy ISO/OSI + TCP/IP

Ve výše uvedené tabulce je vidět, jak se novější model TCP/IP vyvinul a zjednodušil tak předchozí model ISO/OSI. Hlavní nevýhodou ISO/OSI metody je její odtrženost od reality. Při tvorbě TCP/IP byl kladen důraz na jednoduchost a efektivnost přenosových mechanismů sítě. Přenos dat u této architektury je prováděn na nespolehlivém principu, což znamená, že odesílatel odesílá data a předpokládá, že je příjemce dostupný nebo že vůbec existuje. V základu tato metoda nerozlišuje rozdíly mezi daty, tudíž ani prioritu, a tak mají všichni komunikující stejné podmínky a žádný z nich není upřednostněn. V praxi se ale tyto

parametry nastavují z důvodu zajištění vysoké dostupnosti, kdy se některé typy komunikace, například rychlost připojení, omezuje tak, aby důležité služby byly vždy dostupné.

7.2 Adresování v TCP/IP, IPv4

Potřeba rozlišit a určit každému zařízení v síti jeho adresu je technologie, která by se mohla přirovnat k přiřazování poštovních adres zásilkám. Velmi obdobný je princip adresace a doručování dat v počítačové síti. Zařízení musí být jedinečně očíslováno v dané síti, aby nedošlo ke kolizím, podobně jako nesmí mít stejné adresy a jméno dva příjemci v ulici. Vycházelo se tedy z předpokladu vytvořit systém jedinečné identifikace objektů na různých síťových vrstvách. Potřebujeme tedy znát, ke komu se chceme připojit (IP adresa serveru nebo brány), potřebujeme dopravit zprávu na zařízení v jeho síti a například i identifikovat jakou službu chceme využít. (např.: http server s portem 80 nebo 443). To všechno je realizováno pomocí adresace.

Z výše zmíněného příkladu je patrné, že adresace zasahuje všechny vrstvy síťového modelu. V tabulce níže jsou uvedeny typy adres, které jsou přiřazeny k dané vrstvě.

Vrstva podle TCP/IP	Identifikátor
Vrstva síťového rozhraní	48bitové adresy MAC
Síťová vrstva	IP adresy
Transportní vrstva	Čísla portů
Aplikační vrstva	URL odkazy

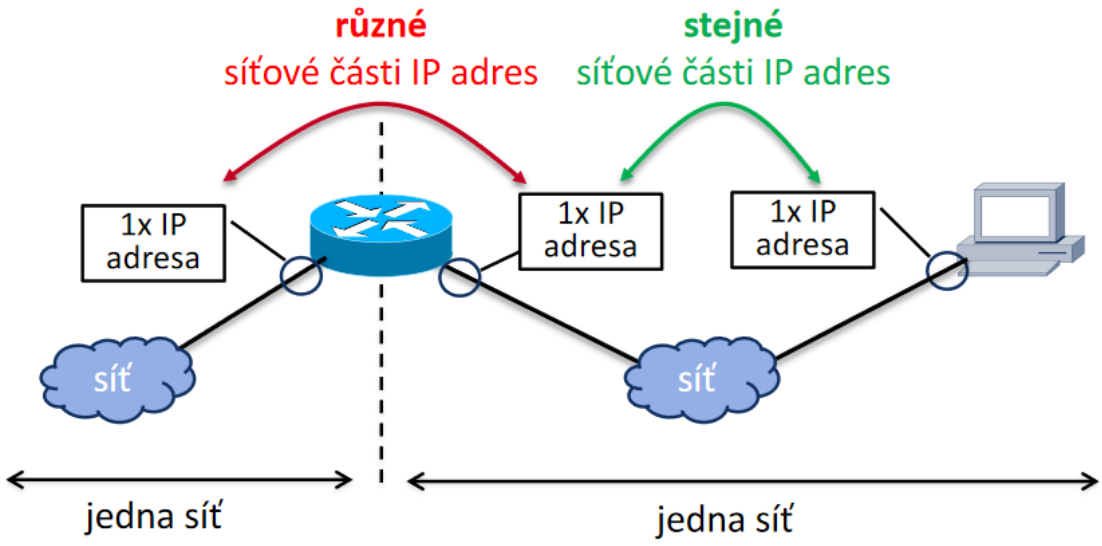
Tabulka 7-2 Vrstvy v TCP/IP

7.2.1 Adresace ve vrstvě síťového rozhraní

Na této úrovní se vyskytují 2 adresy. Linková adresa MAC[12] a síťová adresa IPv4 nebo IPv6. Adresy MAC jsou předem definované, občas označované jako hardwarové adresy, které jsou definovány z jedinečného rozsahu, jež je přidělen danému výrobci síťové karty. MAC adresa je tedy jedinečná a neměly by se objevit zařízení se stejnou adresou. U IP adresy je tato skutečnost o trochu složitější. V minulosti byla i IP adresa součást jedinečného balíku adres, z kterého byl po požádání přiřazen dané instituci požadovaný rozsah adres a následně byl z celkového rozsahu adres vyřazen. V minulosti, kdy tento typ adres vznikal, nebylo počítáno s velmi vysokým nárustem požadavku na tuto adresaci a v současnosti je již počet možných

[12] MAC adresa - 48 bitů dlouhé číslo, které se zapisuje jako 6 dvojic šestnáctkových čísel oddělených dvojtečkami či pomlčkami (https://www.itnetwork.cz/site/zaklady/fyzicky-prenos-mac-adresy-a-protokoly/)

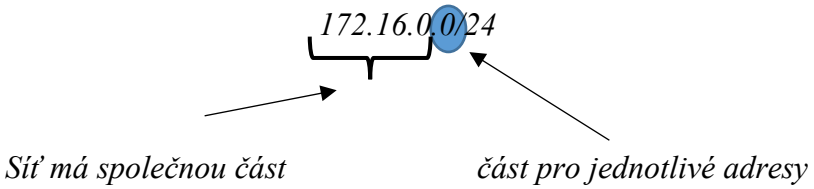
jedinečných adres vyčerpán. Celkem jich v dané verzi IPv4 je 2^{32} neboli 4294967296 adres. V případě IPv6, které je 128bitové, je adres 2^{128} a to je již velmi dostatečné i na současnou poptávku. Rozsah adres je taky také snížen o adresy, které jsou vyčleněné pro adresaci uvnitř sítě, případně speciální služby jako NAT (network address translation). Rozsah adres v současnosti již nedostačuje, a tak byl rozšířen o adresaci v IPv6. Bohužel, nasazení této verze je pomalé a velmi mnoho správců sítě ji neumí nebo nemůže nastavit z důvodu nekompatibility síťových prvků. Proto byl vytvořen systém NAT, který dokáže veřejné adresy přeložit na neveřejné a tím navýšit rozsah těchto adres. Nevýhoda je ztráta viditelnosti koncového bodu za NAT adresou a závislost překladu adres z hlediska náročnosti výpočtu. Výhoda spočívá v bezpečnosti, kdy je koncový bod schovaný za NATem, a tudíž nemusí čelit přímým dotazům z veřejné sítě.



Obrázek 7-1 Mapa adresace v síti

Zdroj: https://www.earchiv.cz/l225/gifs/NSWI045v3_4.pdf

Na obrázku 7-1 můžeme vidět návrh jednoduché sítě. Na ní lze vidět, jak se provádí adresace v jednom segmentu či velmi malé síti o jednom routeru a dvou sítích. Každá síť má svoji masku, která uvádí maximální počet adres určených pro danou síť. Zkráceně se píše za IP adresu sítě.



Ve výše zmíněném příkladu je tedy rozsah sítě od 172.16.0.1 do 172.16.0.255, kdy poslední adresa z rozsahu je vždy vyhrazená pro broadcoastovou (všesměrovou) komunikaci. Takže reálně použitelný rozsah je do 172.16.0.254. Ve veškeré IP konfiguraci fungují pravidla založená na dvojkové soustavě. To znamená, že je vždy maximálně 255 adress jednom segmentu, kdy binárně je tato hodnota 11111111. Zároveň lze z IP adresy a masky zjistit logickým součinem AND adresu sítě. Občas se lze setkat i s takzvanou wildcard maskou která je inverzní o standardní masku.

Maska s prefixem x.x.x.x/24 má tedy dekadický přepis 255.255.255.0 a binární 11111111. 11111111.11111111.00000000. Wildcard je její inverze a tedy dekadicky 0.0.0.255 nebo binárně 00000000. 00000000. 00000000.11111111.

Volba masky je individuální. Pro větší sítě je možné zvolit větší rozsah, a tudíž menší číslo masky. Je ale také vhodné sítě nevytvářet velké z důvodu rozsáhlých broadcoastových domén. V tabulce níže jsou uvedeny všechny rozsahy a masky v IPv4.

CIDR (velikost vnitřní domény)	Dekadicky	Počet adres	Třída	Subnet
/1	128.0.0.0	2147483646	128 A	2
/2	192.0.0.0	1073741822	64 A	4
/3	224.0.0.0	536870910	32 A	8
/4	240.0.0.0	268435454	16 A	16
/5	248.0.0.0	134217726	8 A	32
/6	252.0.0.0	67108862	4 A	64
/7	254.0.0.0	33554430	2 A	128
/8	255.0.0.0	16777214	1 A	256
/9	255.128.0.0	8388606	128 B	512
/10	255.192.0.0	4194302	64 B	1024
/11	255.224.0.0	2097150	32 B	2048
/12	255.240.0.0	1048574	16 B	4096
/13	255.248.0.0	524286	8 B	8192
/14	255.252.0.0	262142	4 B	16384
/15	255.254.0.0	131070	2 B	32768
/16	255.255.0.0	65534	1 B	65536
/17	255.255.128.0	32766	128 C	131072
/18	255.255.192.0	16382	64 C	262144
/19	255.255.224.0	8190	32 C	524288
/20	255.255.240.0	4094	16 C	1048576
/21	255.255.248.0	2046	8 C	2097152

/22	255.255.252.0	1022	4 C	4194304
/23	255.255.254.0	510	2 C	8388608
/24	255.255.255.0	254	1 C	16777216
/25	255.255.255.128	126	1/2 C	33554432
/26	255.255.255.192	62	1/4 C	67108864
/27	255.255.255.224	30	1/8 C	134217728
/28	255.255.255.240	14	1/16 C	268435456
/29	255.255.255.248	6	1/32 C	536870912
/30	255.255.255.252	2	1/64 C	1073741824
/31	255.255.255.254	0	1/128 C	
/32	255.255.255.255	1		

Tabulka 7-3 Velikosti prefixů a počty IP adres

7.2.2 Adresace na transportní vrstvě

Přestože jeden připojený bod má sice svoji adresu, která je jedinečná, pro navázání komunikace s danou aplikací nestačí mít pouze adresu IP, a proto existují takzvané porty. Každá aplikace používá tedy pro komunikaci definovaný port, který může být buď standardizovaný nebo náhodně vygenerovaný. V případě standardizovaných portů se jedná o předem určené rozmezí portů, které lze využít. Většinou se jedná o webové porty, přenosové porty a podobně, o kterých se předpokládá, že budou dotazovány ostatními a využívány pro tyto aplikace. Ostatní porty jsou generovány náhodně z definovaného rozmezí a slouží pouze pro komunikaci. Rozmezí portů je od 0 do 65535, tedy 16 bitů velký rozsah. Čísla od 0 do 1023 jsou vyhrazená a mají pevně daný účel pro definovanou službu.

7.2.3 Adresace na aplikační vrstvě

Adresování na aplikační vrstvě se využívá k identifikaci různých objektů, jako například videa nebo obrázky, které jsou umístěné v různých místech v síti. V této vrstvě jsou 3 identifikátory. URN (Uniform Resource Name), URL (Uniform Resource Locator) a URC (Uniform Resource Citation) [7].

8 Směrování v IP sítích

Směrování je velmi důležitá část počítačových sítí. V současné době jsou sítě velmi rozlehlé a nároky na směrování neboli routování, jsou vysoké. Na této technice je postaveno veškeré směrování ve větších firmách, ISP providerech i routing mezi státy a kontinenty. Směrování je poměrně náročné na procesor a paměť ve směrovacích zařízeních. Proto je nutné každou síť navrhnout tak, aby nebyla rychlost sítě omezená daným zařízením.

Součástí této technologie je tedy výpočet optimálních cest, vytváření směrovacích tabulek, forwarding mezi sítěmi, průběžné výpočty a aktualizace sousedních propojů.

8.1 Směrovací protokoly

Existuje několik protokolů, které se starají o co nejlepší směrování daných dat. Směrovací algoritmy jsou velmi složité na výpočet, a proto se musí aplikovat správně. Špatné nastavení může vyvolat velké odezvy nebo velmi mnoho synchronizačních a dotazovacích funkcí, jež budou danou síť zahlcovat. Tyto algoritmy můžeme klasifikovat jako distance-vector (výměna vektorů mezi směrovači) nebo link-state (stavu okruhu mezi směrovači). Mezi hlavní směrovací protokoly patří RIP, BGP, IGRP+EIGRP a OSPF.

8.1.1 Směrovací protokol RIP

U RIP (Routing Information Protocol) protokolu existují dvě verze tohoto protokolu. RIPv1 se dnes již nemá využívat. Společnost Cisco ve svých dokumentech doporučuje při konfiguraci přímo přepnout na RIPv2, které řeší různé nedostatky i z hlediska bezpečnosti. Poslední verze je RIPng, nicméně mnoho routerů tento protokol nepodporuje. Tento protokol využívá pro hledání sousedních tras metodu distance-vector, ve volném překladu vektor vzdálenosti. K tomuto propočtu je aplikováván Bellman-Ford algoritmus uvedený níže, který porovnává metriky dané sítě.

```
bellman-ford(vrcholy, hrany, zdroj)

// krok 1: inicializace grafu
for each v in vrcholy
if v=zdroj then v.vzdálenost := 0
else v.vzdálenost := nekonečno
v.předchůdce := null

// krok 2: opakovaně relaxovat hrany
for i from 1 to size(vrcholy)-1
for each h in hrany    // h je hrana z u do v
u := h.počátek
v := h.konec
if u.vzdálenost + h.délka < v.vzdálenost
v.vzdálenost := u.vzdálenost + h.délka
v.předchůdce := u

// krok 3: kontrola záporných cyklů
for each h in hrany
u := h.počátek
v := h.konec
if u.vzdálenost + h.délka < v.vzdálenost
error "Graf obsahuje záporný cyklus."
```

Z algoritmu je patrné, že je velmi jednoduchý a v základu pracuje na principu oceňování jednotlivých tras čísly. Podle daných čísel se pak následně rozhoduje, jaká trasa je pro daný tok dat nejvhodnější. V praktickém užití je vhodný do menších sítí, kde není mnoho cest a routerů, a proto se s ním nesetkáme v univerzitní nebo ISP síti.

8.1.2 Směrovací protokol BGP

BGP neboli Border Gateway Protocol, je směrovací protokol o variantách exterior gateway protocol, vhodný pro směrování v oblasti ISP, a interior gateway protocol, vhodný pro interní směrování. Nicméně je tento protokol vhodný pro rozlehlé sítě nebo přímo ISP sítě. Prakticky se s ním setkáme na ISP úrovni velmi často, protože jej lze velmi dobře využívat i v rozsáhlých směrovacích oblastech bez jejich zahlcení, při vytváření routovacích tabulek. Tento protokol je velmi složitý a pro vytvoření směrovací tabulky posuzuje až 11 atributů, díky kterým určuje nejvýhodnější trasu. Některé atributy je ale možné použít jen na určitých zařízeních daných výrobců. Mezi hlavní parametry patří Weight (cena cesty), Local preference (lokální preference), originate, anebo třeba AS path lenght (délka trasy). Níže je uvedena tabulka všech atributů dle priorit.

Priority	Attribute
1	Weight
2	Local Preference
3	Originate
4	AS path length
5	Origin code
6	MED
7	eBGP path over iBGP path
8	Shortest IGP path to BGP next hop
9	Oldest path
10	Router ID
11	Neighbor IP address

Tabulka 8-1 BGP atributy dle priority

Oproti ostatním protokolům, které se používají, posuzuje více atributů naráz, a proto se jedná o velmi efektivní protokol nasazovaný ve velkých sítích.

8.1.3 Směrovací protokol IGRP+EIGRP

IGRP (Interior Gateway Routing Protocol) a jeho další verze EIGRP (Enchanted Interior Gateway Routing Protocol) jsou protokoly, které vymyslela a aplikovala firma Cisco a jsou oproti ostatním uvedeným protokolům Cisco proprietární, a tedy jejich plná aplikace je možná pouze na síťových zařízeních od firmy Cisco. Tyto routovací protokoly jsou vhodné jak pro menší, tak i středně velké sítě. Původní protokol IGRP vznikl v 80. letech 20. století jako

odezva na potřebu routovat větší sítě, které už výše zmíněný protokol RIP nedokázal usměrňovat. Protokol RIP totiž umožňuje maximálně 16 hopů (počet maxima povolených přesměrování mezi jednotlivými routery) na síť. Porovnává tedy čtyři hlavní parametry:

- *Internetwork delay* – reprezentuje výpočet zpoždění a odezvy na dané trase.
- *Bandwidth* – porovnává rychlost dané linky a posuzuje s ostatními. Rozsah rychlosti je od 1200 b/s do 10 Gb/s.
- *Reliability* – hodnota udávající stabilitu linky. Maximální hodnota je 255, což znamená jako maximálně stabilní a dostupná.
- *Administrative Distance* – Označuje atraktivitu spojenebo spojů mezi dvěma routery, jehož hodnota je mezi 1 až 255, kdy platí, že čím menší číslo okruh má, tím více atraktivní je.

Protokol IGRP zasílá informace pouze routerům, které jsou součástí autonomního systému a jeho součástí jsou 3 typy routovacích cest:

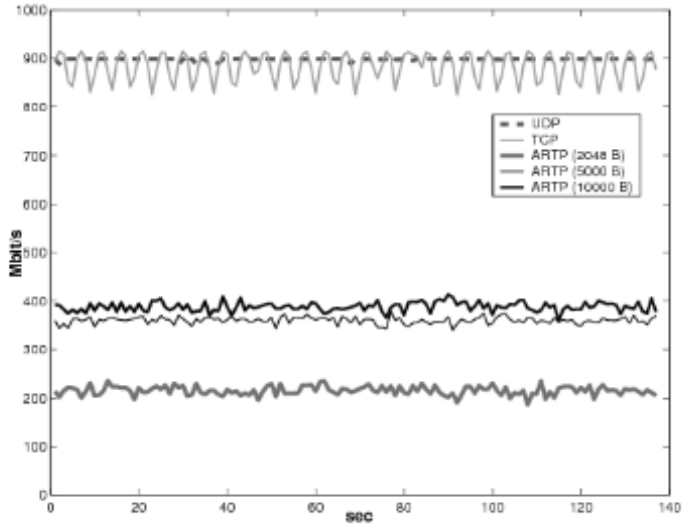
- Interior Routes – Okruhy, které jsou lokálně připojené a které jsou inzerované k routingu.
- Exterior Routes – Okruhy, jenž jsou součástí externí sítě, nazývané default networks, a které nejsou součástí autonomního systému.
- System Routes – Okruhy, které jsou součástí autonomního systému.

8.1.4 Směrovací protokol OSPF

Routovací protokol OSPF neboli Open Shortest Path First, který spadá do skupiny interior gateway protokolů, je využíván převážně ve velkých sítích u poskytovatelů internetu neboli ISP. Fungování tohoto protokolu je založeno na rozdělení jednotlivých sítí do takzvaných oblastí (area network) a očíslování každého směrovacího routeru jedinečným ID (router ID). Každý router si pak předává směrovací tabulku se svými sousedy, na základě jejich oblasti a ID. Tyto údaje se nastavují manuálně, a tak nehrozí případné kolize v jedné síti (pouze pokud jsou hodnoty špatně manuálně zadány).

8.2 Transportní protokoly

Transportní protokoly se nachází nad směrovacími. Rozlišujeme dva druhy transportních protokolů. Transportní protokoly bez spojení a transportní protokoly se spojením. Transportní protokoly bez spojení (UDP – User Datagram Protocol) zajišťují pouze přenos daných dat, ale nezajišťují žádné kontrolní mechanismus a opravy poškozených dat. Oproti tomu Transportní protokoly se spojením (TCP – Transmission Control Protocol) dokáží nejen ud ržovat a navázat spojení, ale zajišťují i samotnou kontrolu dat proti ztrátám či dokáže pomocí kontrolních funkcí zjistit poškozená data a požádat o jejich opětovné poslání.



Obrázek 8-1 Porovnání rychlostí různých protokolů

Zdroj: https://www.fi.muni.cz/~xrebok/DOCs/PUBs/Olomouc05_1.pdf

8.2.1 UDP – User Datagram Protocol

Protokol UDP je jedním z nejznámějších a funguje velmi jednoduše. Je definovaný jako nespolehlivý a nespojovaný protokol a hodí se zejména na přenos dat, u kterých nevadí jejích poškození či přímo ztráta. Proto je vhodný zejména pro přenos živého video streamu nebo zvuku. Jediné, co UDP v podstatě zajišťuje, je multiplexování[13] a demultiplexování datagramů podle čísel portu. Níže je popsán princip komunikace pomocí protokolu UDP.

8.2.2 TCP – Transmission Control Protocol

TCP protokol je spojovaný a spolehlivý pro přenos dat. Spolu s UDP patří mezi nejpoužívanější. Dokáže řídit tok dat nebo například kontrolovat zahlcení sítě. Jeho hlavní použití je v případech, kde chceme docílit úspěšných přenosů souborů bez poškozených dat.

[13] Multiplex – sloučení více frekvencí, pomocí různých metod, do jednoho signálu nebo přenosového média. https://www.earchiv.cz/a96/a651k150.php3

8.2.3 Adresování na transportní vrstvě

Jak už bylo zmíněno výše, v případě komunikace je potřeba znát nejen IP adresu, ale musí být známy i čísla komunikačních portů, které komunikaci otevírají. Konkrétní entitu tedy tvoří kombinace IP a transportní adresy neboli číslo portu. Podmínkou je přímá viditelnost ve veřejné síti, protože pro správnou komunikaci je potřeba znát nejen uzel, ale i konkrétní entity v daném uzlu. Porty mohou definovat i službu, kterou zprostředkovávají. Proto jsou některé porty vyhrazené pro komunikaci užívající určité protokoly. Hlavní význam tohoto standardu je spojení určitého portu s určitou službou, která je díky portu předem známá. Například weby používají port 80 nebo 443 v případě zabezpečeného způsobu spojení. Prohlížeč dopředu ví, že v případě vyhledávání webové stránky se bude dotazovat na jeden z těchto portů. Tyto porty se někdy označují jako dobře známé porty[14](well-known-ports). Porty dělíme do tří kategorií. Dobře známé porty, v rozsahu od 0 až do portu 1023, jsou vymezené k přesnému účelu a službě. Registrované porty od 1024 do 49151 nemají sice přímo definovanou službu, nicméně je možné jim pevně některou přiřadit. Poslední rozsah je vyhrazen pro dynamické porty, které jsou od portu 49152 až po konečný možný 65535. Tyto porty nemají vyhrazené přesné využití a lze je použít pro jakékoliv účely. V dalším případě máme sockety, spojující IP adresu a port[15], které běží na úrovni dané aplikace a zahrnují i problematiku portů.

8.2.4 Zajištění spolehlivosti a detekce chyb

Data, která se přenášejí přes počítačovou síť, nemusí přijít vždy v pořádku z toho důvodu, že se stále jedná o zpracování elektrických signálů, které mohou být ovlivněny mnoha faktory. Chyby mohou nastat například v pozměnění dat, shluku chyb nebo dokonce ve výpadku celých bloků dat. O co nejlepší detekci chyb se starají matematické postupy jako jsou parita, kontrolní součty nebo CRC polynomy[16]. Hlavním principem je kontrola dat jako je paket nebo rámec. V případě poškozených dat se pak celý paket zahazuje a žádá o znovu zaslání konkrétních dat. Ke každému bloku dat se připíše hodnota pořadí bloku, který příjemce dokáže přečíst a porovnat s příchozími daty.

První metodou je parita neboli paritní bit. Tato metoda je velmi jednoduchá na výpočet i porovnání. Kontrola parity se provádí na binární úrovni, kdy porovnávají jednotlivé hodnoty, které se odesílají. Podle nich se určí, zdali se jedná o sudou paritu (v případě že počet binárních

[14] Výpis všech definovaných portů. https://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xhtml

[15] Socket – Adresace socketů v TCP/IP [Online] https://www.ibm.com/docs/en/aix/7.2?topic=addresses-socket-in-tcpip

[16] *Zabezpečení datových přenosů pomocí CRC* [online]. Dostupné z: https://moodle.fel.cvut.cz/pluginfile.php/85912/mod_resource/content/1/CRC_navod.pdf

1 je sudý) nebo o lichou paritu (v případě že počet binárních hodnot 1 je lichý). Zároveň se pro účinnější fungování sestavuje jakási matice podélné a příčné parity tak, aby byla kontrola jednotlivých bitů jak horizontálně, tak i vertikálně podle stejnolehlých bitů všech řádků. Výsledkem je, že každý sloupec a řádek má přiřazenou konkrétní hodnotu parity (lichá nebo sudá). Nevýhoda této metody spočívá v její chybovosti, kdy každý druhý poškozený bit vygeneruje falešně správný paritní bit (chyby ve dvou bitech se vzájemně vyruší), a proto je pravděpodobnost výskytu chybové parity větší než u ostatních metod.

Druhou metodou kontroly dat je kontrolní součet. Oproti paritě nepracuje s určováním lichých a sudých počtů bitů. Dokáže detekovat více chyb než parita, nicméně i u této metody se vyskytují chybové stavy. Blok dat se v této metodě sečte (AND), případně se použije metoda XOR, a výsledek se použije jako bezpečnostní údaj pro kontrolu správnosti dat.

Poslední jmenovanou metodou je CRC[17] algoritmus neboli Cyclic Redundancy Check. Tato metoda využívá posloupnosti bitů a implementuje je jako polynomy. Základní vlastností je volba klíče, který také následně generuje polynom a udává se jako číslo CRCx, kde x = hodnota klíče. Tedy pokud je kontrolní součet CRC8, kontrolní součet má řídící polynom stupně 8. CRC je založeno na dělení v konečném tělese, tedy u výsledných koeficientů se provádí pouze operace modulo 2. Tento algoritmus detekce je velmi účinný. Lze s ním detekovat jak chyby v lichých počtech bitů, tak i shluky chyb do velikosti N, kdy N je stupeň daného polynomu. Pravděpodobnost shluky chyb o velikosti x > N+1 je 99.99999998 % za použití CRC32, přitom složitost výpočtu pro tento polynom je minimální.

9 Kryptografie a šifrování

Kryptografie a šifrování jsou technologie, která zajišťují data proti nedovolenému čtení, ať už při přenosu přes síť, nebo při ukládání na úložná média, jako jsou USB Flash disky nebo interní úložiště. V dnešní době je velmi doporučeno mít důležitá a citlivá data při přenosu přes síť v zašifrované podobě. Současně i některé instituce vynucují šifrování disků koncových stanic, jako jsou například notebooky. Šifrování je součástí kryptografie a stará se o transformaci dat tak, aby bylo zajištěno jejich zabezpečení před nedovoleným čtením. Výsledkem je, že danou šifru může rozluštit pouze ten, kdo má k šifře klíč. Existují ale i jiné metody, které nepoužívají klíč, ale nějakou matematickou funkci označovanou jako hash, kam se řadí například MD5, SHA nebo SHA2.

[17] CRC – technický popis technologie a specifikace chybovosti. https://tools.ietf.org/html/rfc3385

9.1 Šifry a klíče

Šifra je jinak kryptografický algoritmus, který je dán pomocí jasně definovaných předpisů. Provádí funkci jak šifrovací, tak dešifrovací, což je funkce inverzní. Vzhledem k faktu, že algoritmus není před ostatními utajen, protože všichni používají ten samý, je bezpečnost v samotném výstupu algoritmu zajištěna pomocí klíče, nikoliv v algoritmu samotném. Existuje několik druhů klíčů, které se i pro větší bezpečnost mohou navzájem doplňovat. V základu máme 2 druhy klíčů. Private (soukromý) klíč, je typ klíče který například při HTTPS[18] komunikaci zůstává a nikam se neodesílá. Public (veřejný) klíč, který se mezi odesílatelem a příjemcem navzájem vymění. Oba zmíněné klíče jsou takzvaně asymetrické a jedná se tedy o asymetrický způsob šifrování. Odesílatel může data zašifrovat veřejným klíčem, ale příjemce musí pro dešifrování použít klíč privátní.

9.2 Bezpečnost šifer

Tento parametr udává, jak moc je určitý druh šifry bezpečný a odolný proti prolomení. Obvykle se vyjadřuje v bitech, kdy n bitů je mocnina 2, tedy v matematickém vyjádření 2^n. Výraz udává počet možných klíčů neboli možností. V současné době je tento způsob tipování klíče jen velmi málo obvyklý. Zpravidla se lze spíš setkat s více sofistikovanými způsoby než jen tipovat všechny možnosti klíče. Šifrovací algoritmy mají předem definovány délku klíče, velmi často se udává i v názvu samotného algoritmu, jako například AES128, AES256 nebo RSA1024.

Délka klíče je horní hranice bezpečnostní šifry, která určuje i samotnou složitost daného algoritmu. Platí zde přímá úměra, kdy: čím je délka klíče větší, tím je náročnější danou šifru prolomit. Je ale nutné brát ohledy na výpočetní výkon, kdy při použití příliš složitého šifrovacího algoritmu můžeme zpomalit, nebo přímo úplně zahltit dané zařízení. Dolní hranice šifry by měla být v nejlepším případě stejná jako horní hranice šifry. Nicméně u některých typů šifer existuje řada zranitelností, které bezpečnost daného algoritmu snižují. U šifrovacího algoritmu 3DES, který měl například horní hranici bezpečnosti navrženou na 168 b, byla při objevení bezpečnostních nedostatků snížena jeho dolní hranice bezpečnosti na 112 b.

9.3 Nejrozšířenější kryptografické algoritmy a jejich doporučené varianty

V současné době jsou nejrozšířenější takové algoritmy, které jsou v dané zemi schválené a doporučené institucí, která se stará o kybernetickou bezpečnost státu. V České republice je pro tyto účely instituce NÚKIB neboli Národní úřad pro kybernetickou a informační

[18] HTTPS – Hypertext Transfer Protocol Secure, zabezpečená forma připojení využívající protokol HTTP

bezpečnost. Jelikož se jedná o technologie, které se po určité době mohou změnit, jsou použité informace a doporučení v této části platné v období psaní této práce. Pro zjištění aktuálních doporučení lze navštívit webové stránky NÚKIBu. (https://www.nukib.cz)

Schválené symetrické algoritmy

a) Schválené blokové a proudové šifry
    1. Advanced Encryption Standard (AES) s využitím délky klíčů 128, 192 a 256 bitů
    2. Twofish s využitím délky klíčů 128 až 256 bitů
    3. Serpent s využitím délky klíčů 128, 192, 256 bitů
    4. Camellia s využitím délky klíčů 128, 192 a 256 bitů
    5. SNOW 2.0, SNOW 3G s využitím délky klíčů 128, 256 bitů
    6. ChaCha20 s délkou klíče 256 bitů a se zatížením klíče menším než 256 GB

Doporučení je použití blokových šifer a v jejich případě využití algoritmu AES s klíčem o délce 256 bitů. V případě algoritmu 3DES je doporučeno přejít na variantu AES[19].

Schválené asymetrické algoritmy

a) Digital Signature Algorithm (DSA) s využitím délky klíčů 3072 bitů a více, délky parametru cyklické podgrupy 256 bitů a více
b) Elliptic Curve Digital Signature Algorithm (EC-DSA) s využitím délky klíčů 256 bitů a více
c) Digital Signature Algorithm (DSA) s využitím délky klíčů 2048 bitů, délky parametru cyklické podgrupy 224 bitů – dosluhující
d) Elliptic Curve Digital Signature Algorithm (EC-DSA) s využitím délky klíčů 224 bitů – dosluhující
e) Diffie-Hellman (DH) s využitím délky klíčů 3072 bitů a více, délky parametru cyklické podgrupy 256 bitů a více
f) Elliptic Curve Diffie-Hellman (ECDH) s využitím délky klíčů 256 bitů a více
g) Elliptic Curve Integrated Encryption System–Key Encapculation Mechanism (ECIES-KEM) s využitím délky klíčů 256 bitů a více

[19] *MINIMÁLNÍ POŽADAVKY NA KRYPTOGRAFICKÉ ALGORITMY* [online]. Dostupné z: https://www.nukib.cz/download/uredni_deska/Kryptograficke_prostredky_doporuceni_v1.0.pdf

Podrobný výpis všech algoritmů uvedených výše je k dispozici na stránkách NÚKIBu nebo na url:https://www.nukib.cz/download/uredni_deska/Kryptograficke_prostredky_doporuceni_v1.0.pdf .

Algoritmy hashovacích funkcí

a) Schválené hašovací funkce
    1. SHA-2
    2. SHA-2562.SHA-384
    3. SHA-5124.SHA-512/256b

b) Doporučené hašovací funkce
    1. SHA3
    2. SHA3-256
    3. SHA3-3843.SHA3-512
    4. SHAKE1285.SHAKE256

10 Významní výrobci síťových prvků

Na trhu je již v současné době mnoho výrobců daných prvků, mezi kterýma může být nejen velký cenový rozdíl, ale i kvalitativní. Teoreticky lze prvky rozdělit do několika kategorií. Od modelů pro osobní použití, domácnost, malou/střední/velkou firmu, instituci a samotné ISP a telekomunikační providery. Síťové prvky se liší technickými parametry a cenou. V případě osobních nebo domácích prvků se v dnešní době jedná i o několik set korun (zařízení typu router+switch+ap). Tato zařízení se ve velké míře vyskytují v domácnostech a ve velmi malých provozovnách. Jsou velmi levná, ale také i velmi málo výkonná. Zpravidla si dokážou poradit jen s několika málo bezdrátovými klienty a jejich rychlost nebude vysoká. Na trhu se lze ale setkat i s modely, které mohou stát i tisíce korun. Liší se hlavně v přenosových rychlostech a v lepších bezdrátových standardech, jako je třeba systém dual-band (2,4GHz + 5GHz) neboli standard bgn+ac.

V případě rozlehlejších sítí, jako jsou třeba firemní sítě, sítě v nemocnicích a úřadech či dokonce sítě samotných poskytovatelů, se lze setkat již se zařízeními větších rozměrů, standardizovaných maximální šířkou (výškou) tak, aby šli namontovat do racku[20]. Mezi hlavní výrobce těchto prvků jsou firmy Cisco, Mikrotik, Motorola, Ericsson, Huawei, HP, Aruba network, 3com, Netgear, Juniper, nebo například Ubiquity. Tyto společnosti mají různé

[20] Rack – skříň, převážně kovová, pro namontování síťových prvků, serverů nebo strukturované kabeláže. Zpravidla je vybavena i aktivním chlazením.

cenové politiky a je mezi nimi i kvalitativní rozdíl. Tyto firmy by bylo možné rozdělit na několik kategorií. Některé jsou totiž zaměřené pouze na určitý segment svých zařízení a některé jen doplňují své portfolio produktů o síťové řešení. V této práci se v praktické části budeme věnovat prvkům od společnosti Cisco a Mikrotik, jako jedněch z nejčastěji používaných, a také na kterých se velmi často zajišťuje odborná výuka nebo laboratorní cvičení.

10.1 Operační systémy na síťových prvcích

U každého síťového zařízení běží po zavedení operační systém, zpravidla vyvinutý danou společností, který ovládá a řídí zařízení a jeho provoz. Velmi často jsou tyto systémy založené na Linuxovém jádru. Ty lze i později přenést a případně emulovat pro nasimulování dané situace mimo reálnou síť. Každý síťový prvek je tedy v jistém slova smyslu počítač, který má vlastní procesor, operační paměť, a i svůj operační systém. Rozděluje se na dva hlavní typy, které ovlivňují celkové fungování zařízení. V prvním případě je prvek nespravovatelný (no management) a chová se v síti tak, jak byl výrobcem nakonfigurován v jeho operačním systému, a nelze jej nikterak měnit či přehrávat. S těmito prvky se lze většinou setkat na úrovni L2 s levnějšími typy přepínačů. Tyto přepínače (switche) vykonávají základní přepínání a nelze je nastavovat. Jejich výhoda je v jednoduchosti zapojení, kdy stačí přepínač zapojit do elektrické energie a daný prvek plně funguje, jako konfigurovatelný přepínač v defaultním nastavení.

Druhou variantou jsou spravovatelné prvky (management). Tyto prvky jsou zpravidla dražší, ale poskytují nespočet funkcí navíc, které jsou obzvláště u větších sítí nezbytně nutné. I na těchto prvcích běží operační systém výrobce prvku, který ale oproti nespravovatelným síťovým prvkům lze nastavovat a měnit jeho chování. Tento operační systém má své prostředí pro konfiguraci. U některých zařízení se setkáme se sériovým portem (console port), přes který lze prvek nastavovat pomocí sériového portu na počítači či za použití redukce přes USB. Některé nové prvky ale již tento styl propojení nemají a spoléhají na čistě webové nebo jiné síťové rozhraní. V tomto případě prvek automaticky spouští tuto službu při spuštění jeho systému.

10.1.1 Cisco Internetwork Operating System (IOS)

Cisco IOS je operační systém vyvinutý firmou Cisco v 80. letech 20. století. Prostředí tohoto systému se většinou konfiguruje přes konzoli v příkazovém prostředí, ať už připojením přes sériový port telnetem (nezabezpečené spojení), nebo SSH. Systém obsahuje i webové prostředí,

které je ale nutné pomocí příkazu, ip http server, zapnout. Tento systém je výjimečný v konfiguračním prostředí konzole, která obsahuje různé úrovně (módy) [8]:

- User EXEC Mode
- Privileged EXEC Mode
- Global Configuration Mode
- ROM Monitor Mode
- Setup Mode

10.1.2 Mikrotik RouterOS

Systém od společnosti Mikrotik, RouterOS, je podobně jako systém od firmy Cisco založen na linuxovém systému. Rozdíl je v konfiguračním prostředí, kdy produkty od této firmy podporují obě varianty konfigurace v příkazovém prostředí nebo ve webové variantě, kde lze zároveň i obraz konzole spustit. Tyto prvky lze také konfigurovat pomocí programu winbox. V případě větší sítě lze nainstalovat i na některý prvek doplněk The Dude, který umožní lepší správu všech zařízeních a také grafické znázornění všech síťových zařízení.

11 Virtualizační programy pro testování a rozdíly ve virtualizaci

Existuje mnoho způsobů virtualizace síťových prvků. Lze je virtualizovat jako virtuální stroj ve virtualboxu nebo VMware, či získat program pro virtualizaci sítě, který dané prvky automaticky virtualizuje, a může je i graficky vizualizovat.

11.1 Síťová simulace

Síťová simulace je druh systému, lépe řečeno programu, který dané prvky simuluje. Pomocí algoritmů vypočítává jednotlivé interakce a komunikace mezi jednotlivými prvky. Prvky tedy nejsou reálné, jen pracují v programu, který je celistvý. Výhoda těchto programů je jejich jednoduchost, celistvost (není potřeba instalovat prvky a obrazy operačních systémů), výkonnost a v neposlední řadě jsou i méně náročné pro hostující systém. Nevýhoda spočívá v někdy nepřesném provedení daných nastavení a simulované prvky se tak nemusí chovat vždy stejně jako ty opravdové.

11.2 Síťová emulace

Síťová emulace je oproti simulaci věrohodnější. Funguje na principu emulace reálných operačních systémů daných prvků. Každý prvek je tedy samostatná instance a entita, která má vlastní operační systém, který má dedikovanou paměť, procesor a určité rozhraní. Prvky se chovají velmi věrohodně. Největší nevýhoda síťové emulace je její náročnost. Systém, na kterém emulační software běží, musí být výkonný, zejména musí mít dostatečně

dimenzovanou paměť RAM. Nicméně pro emulaci několika prvků středně výkonný počítač stačí. Výhoda tohoto řešení je v jeho přesnosti, napodobit reálné prvky a jejich vzájemnou komunikaci, kterou lze i analyzovat pomocí různých programů.

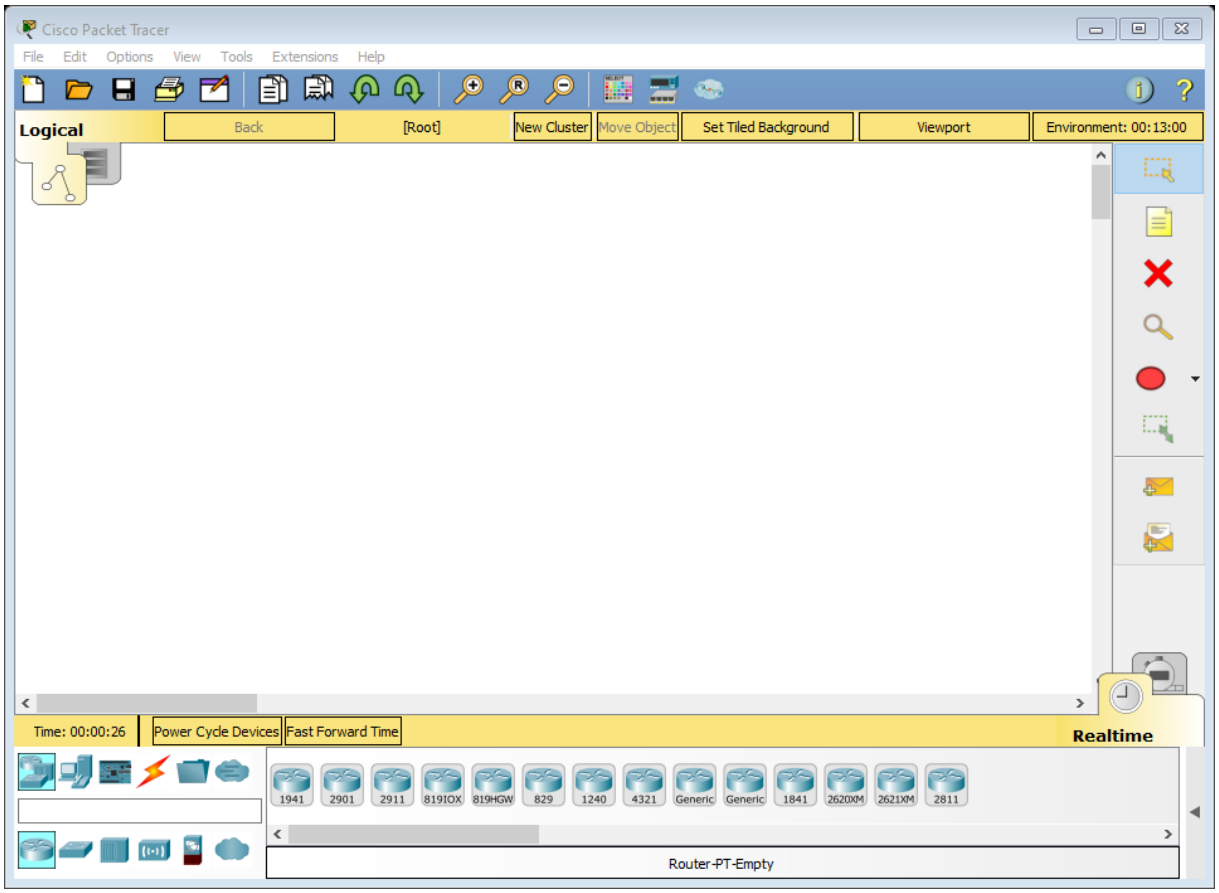
11.3 Příklady systémů pro virtualizaci a jejich prostředí

Pro potřeby virtuální síťové laboratoře je nutné využít virtualizačních či simulačních programů. Jejich vzájemné výhody i nevýhody byly zmíněny v této práci výše. Hlavní výhoda této laboratoře spočívá v její dostupnosti jak fyzické, tak i ekonomické. Pro možnosti výuky jsou nároky na vybudování laboratoře vysoké, protože je nutné mít pro každého studenta samostatné zařízení pro konfiguraci a testování. Síťové prvky mají vlastní operační systém a lze je i virtualizovat samostatně ve virtualizačních programech jako je VirtualBox nebo vmware. Pro možnosti více prvků není ale tato varianta příliš intuitivní a nelze v ní vytvářet síťovou hierarchii. Proto se tato práce zaměřuje i na grafické znázornění a vizualizaci.

11.3.1 Cisco Packet Tracer

Cisco Packet Tracer je program vyvinutý společností Cisco pro účely výuky počítačových sítí na jejich hardwarových zařízeních. Program nevyžaduje zvláštní nastavení počítače a jeho podpora je jak pro systémy Windows, tak i pro Linuxové distribuce. Program je veřejně dostupný na stránkách společnosti nebo ze zdroje: https://www.netacad.com/courses/packet-tracer . Po přihlášení do kurzu Introduction to Packet Tracer lze po získání přihlašovacích údajů daný program aktivovat a zadarmo využít. Školní instituce mohou zažádat o vlastní výukové prostředí (classroom), kdy je vybrán lektor, který kurz vede podle prezentací od této společnosti. Program slouží pro přípravu na Cisco certifikaci CCNA nebo profesionální variantu CCNP. Lektor ale musí být certifikovaný společností a nelze bez něj tyto kurzy vyučovat a následně certifikovat.

Program pro standardní úlohy zabere maximálně 300 MB RAM a vytížení procesoru je závislé na úlohách, které program zpracovává. Na interním úložném médiu zabere maximálně 1 GB

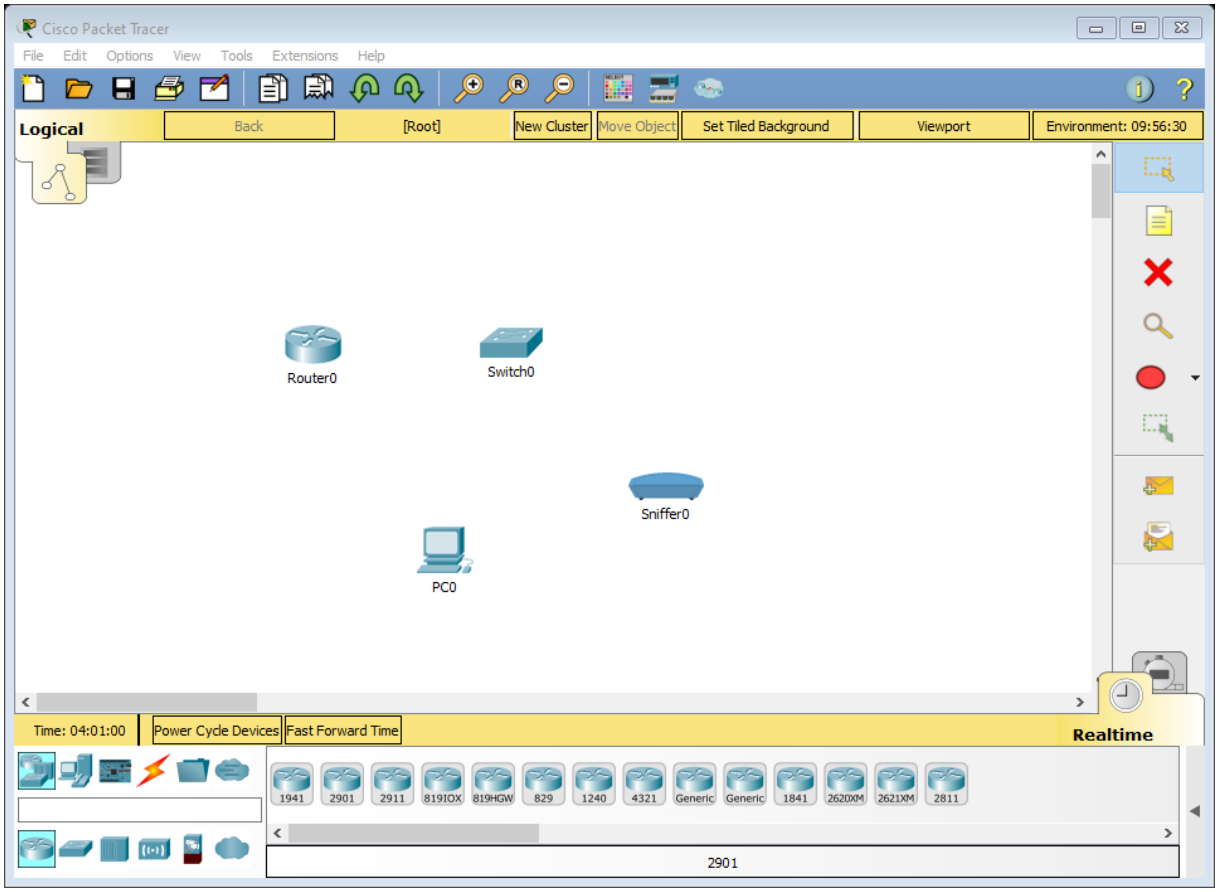


Obrázek 11-1 GUI programu Cisco Packet Tracer

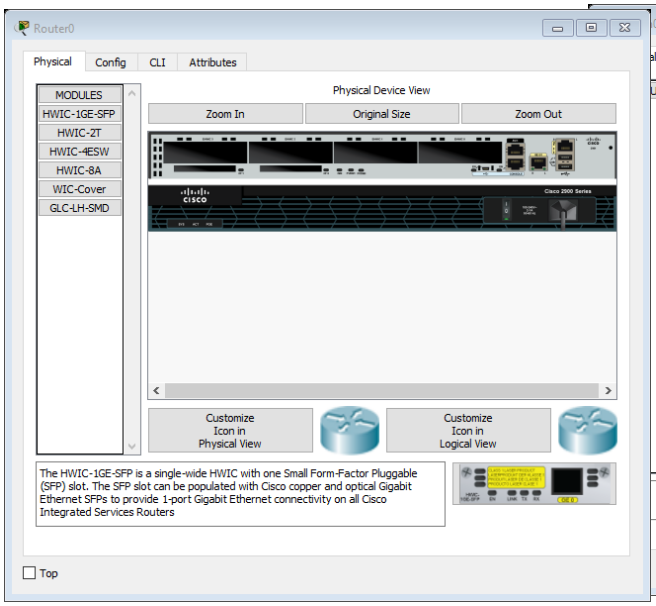
prostoru. Úlohy lze ukládat a případně exportovat a otevřít v jiném Packet Traceru. Pro možnosti výuky jde tedy vytvořit sadu cvičení, která je možno naimportovat a následně již provádět jejich konfiguraci a nezdržovat se samotným navrhováním rozmístění a propojení samotných hardwarových prvků.

Prostředí obsahuje několik kategorií zařízení, která obsahují dané prvky, jenž spadají do dané kategorie. V tomto programu se setkáme pouze se zařízeními od společnosti cisco a několika počítači, telefony a servery. Pracovní prostředí je libovolně velké a prvky se ze spodní lišty natahují do pracovní plochy programu, kde probíhá i následná konfigurace. Na obrázku č. 11-3 a č. 11-4 lze vidět jednotlivé prvky a jejich možnosti konfigurace. Veškerá konfigurace daných prvků se tedy realizuje v tomto daném oknu, které je pro každý prvek oddělené. V defaultním nastavení se prvky nacházejí s minimální konfigurací. U některých prvků lze za vypnutého stavu přidat další porty (sériové, SFP nebo další RJ45). Pro konfiguraci je možné využít karty config pro základní nastavení. Veškeré nastavení se provádí

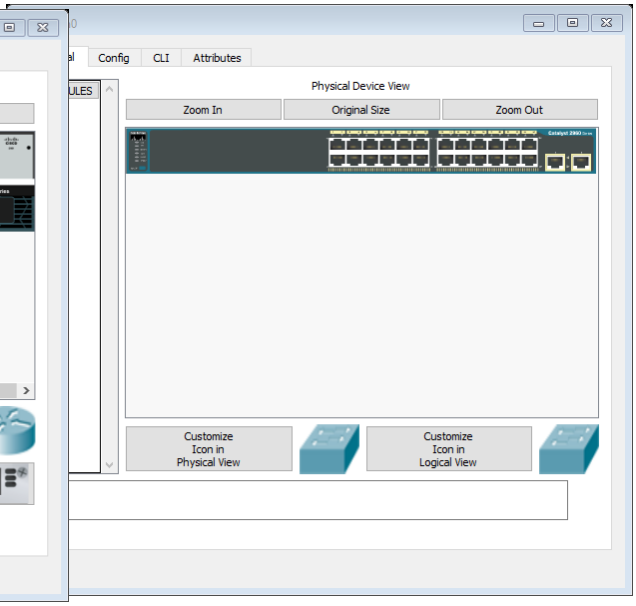
na kartě CLI, což je simulace konzolového portu, a funguje to stejně, jako kdyby se prvek nastavoval přímo přes sériový kabel. Pro rozšiřující možnosti lze zvolit a přidat do zařízení další porty pomocí okna moduly (uvedeno na obrázku 11-3 pod označením modules).



Obrázek 11-2 Umístěné Cisco prvky v programu Packet Tracer (PT)

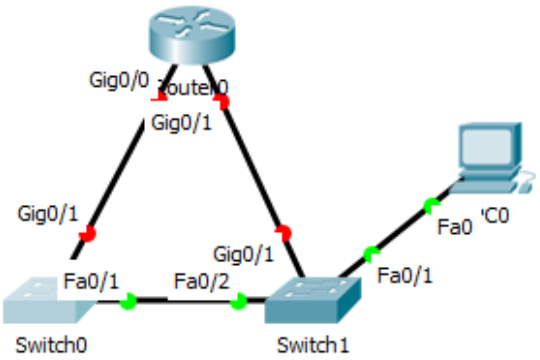


Obrázek 11-3 Konfigurační okno Cisco Routeru v PT



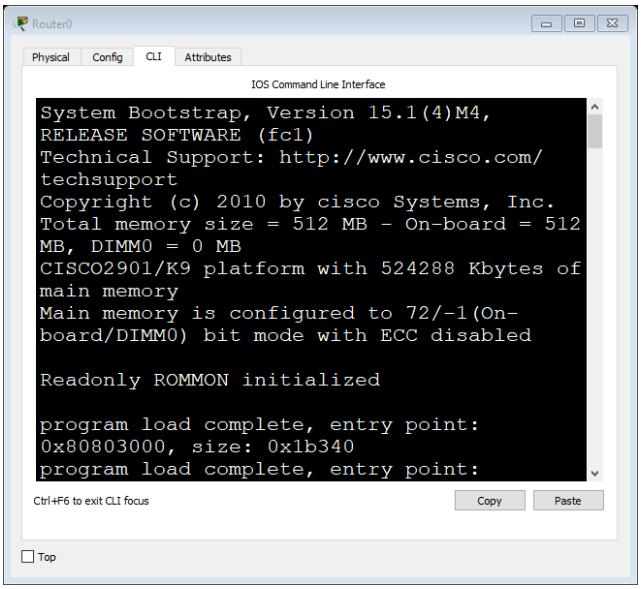
Obrázek 11-2 Konfigurační okno Cisco Switche v PT

Pracovní prostředí je velmi intuitivní a v oknech se lze velmi jednoduše orientovat. Grafické propojení jednotlivých zařízení je realizováno v hlavním okně, kde se dané linky konfigurují pomocí výběru třetí ikony z pravého dolního rohu (obrázek 11-4).



Obrázek 11-4 Zapojení prvků v PT

V grafickém zobrazení lze při spojení jednotlivých prvků vidět, zdali je linka a port shutdown/ no shutdown (podle barvy červená/zelená). Dále jsou vidět již připojené porty, jejich označení a popis daných prvků.



Obrázek 11-5 CLI rozhraní Cisco routeru v PT

V CLI rozhraní lze konfigurovat daný prvek. Každé zařízení má simulovaný systém, který se snaží chovat maximálně věrohodně k danému reálnému operačnímu systému. Konfigurace je stejná jako při práci se standardními prvky od společnosti cisco. Po načtení se dostaneme do enable módu. Veškeré provedené konfigurace lze uložit, stejně jako na reálných prvcích

po vyvolání příslušného příkazu, pro každý prvek zvlášť. V programu lze také uložit vše pomocí karty file.

11.3.2 NS 1/2/3 (Network Simulator)

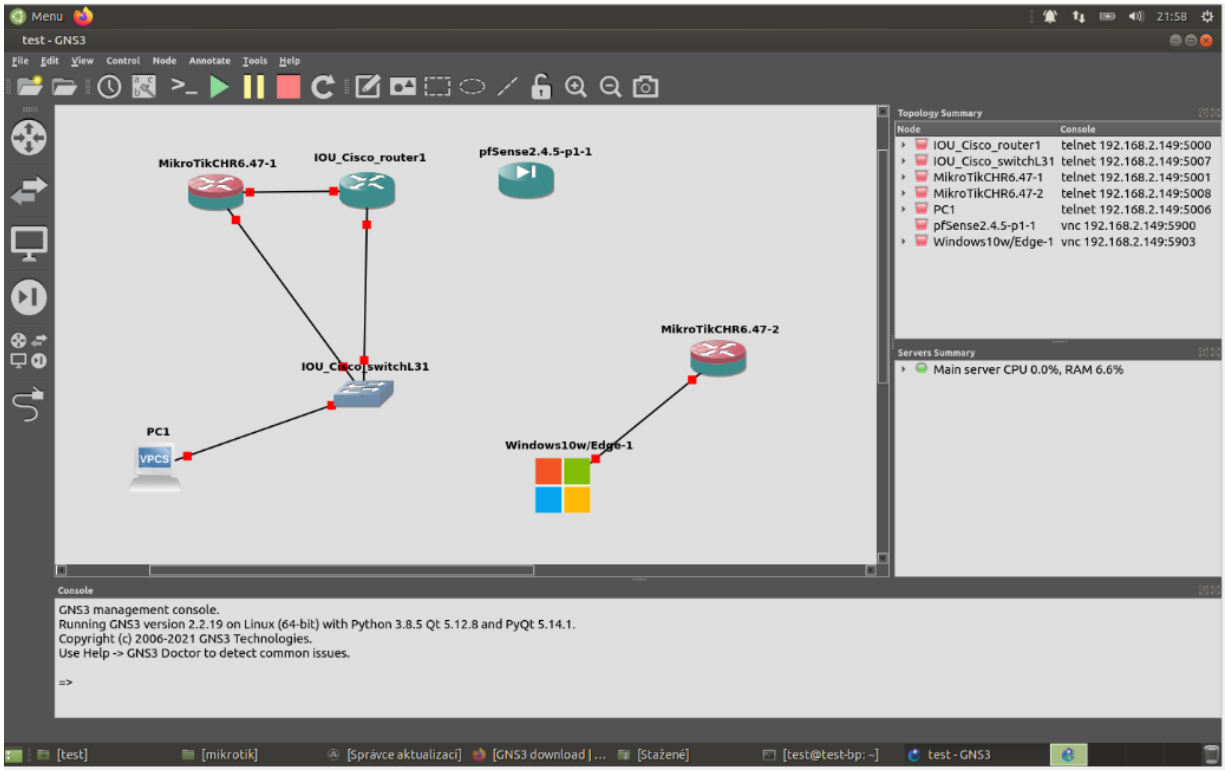
Network simulator je program pro Linuxové systémy napsaný v programovacím jazyce C++ a Pythnu. Doposud existují tři verze. Nyní se již používá pouze třetí verze. Program je zcela bezplatný a lze jej stáhnou z této adresy (https://www.nsnam.org/releases/ns-3-33/download/). Program podporuje IP a non-IP sítě. Velká výhoda spočívá v simulaci i bezdrátových technologií, jako jsou například WiFi a WiMAX. Program umožnuje simulaci telekomunikačních technologií LTE na 1. a 2. síťové vrstvě. Disponuje také základním statickým a dynamickým směrováním.

Tento program je určený spíše pro simulaci dané sítě a infrastruktury, propojení vzájemných bodů a testování konfigurace. Neobsahuje příliš mnoho technologií a modulů pro detailnější konfiguraci síťových prvků. Program je také vhodný pro analyzování koncových protokolů.

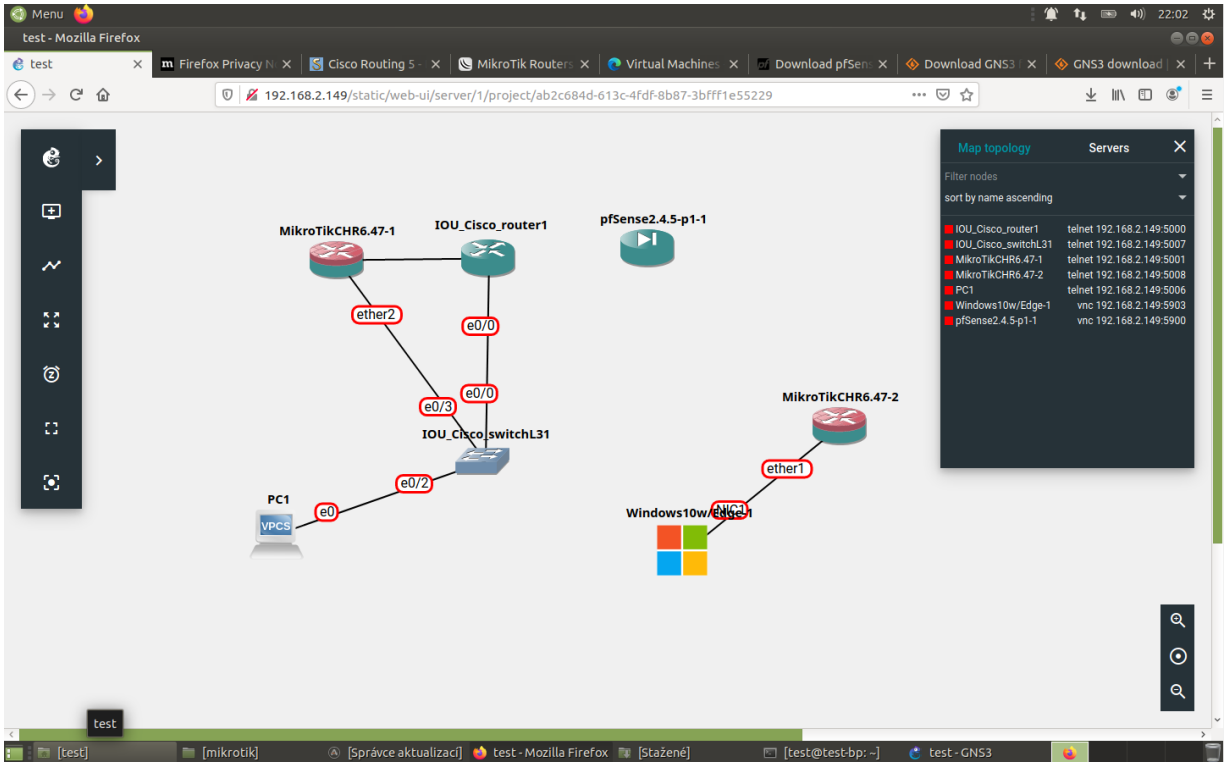
11.3.3 GNS (Graphical Network Simulator)

Graphical Network Simulator je jeden z nejvíce využívaných síťových emulátorů podporovaný jak systémy s operačním systémem Windows, tak i Linuxové distribuce Debian a Ubuntu. Je založený na virtualizaci reálných obrazů, a proto je pro jeho spuštění potřeba splnění alespoň minimálních parametrů[21]. Netýká se nastavení v podobě externího výpočetního bodu, na který se klienti pouze připojují. GNS má tedy výhodu v možnosti nainstalování tohoto programu na výpočetně slabé prostředí a ve využití externího výpočetního serveru ke všem úkonům. V případě serverově řešené emulace je možnost sestavovat síť přes instalovaný program, nebo i bez nutnosti cokoliv instalovat využít webové prostředí. Rozdíly mezi webovým a aplikačním rozhraním není veliké. V obou případech se veškeré výpočty a virtualizace zpracovávají v serverové části, a tedy lze využívat pouze verzi bez aplikace, a tím šetřit úložné místo v koncové stanici. Změny se propisují automaticky a lze i otevřít více instancí na jednu laboratoř. Pro připojení ke konzoli není potřeba instalace aplikace podporující toto spojení. Pro připojení na vzdálenou plochu operačních systémů, podporující pouze GUI prostředí (Windows apod.), je nutné nainstalovat program vnc. GNS3 automaticky namapuje každému prvku port, přes který lze využít vzdálené spojení odkudkoliv (telnet/vnc), viz obr. 11-7. IP adresa je shodná v případě jedné serverové části GNS.

[21] Minimální parametry pro GNS3 – minimálně 2 logické CPU s podporou virtualizace a 4 GB RAM, 1 GB na instalaci samotného programu + prostor pro nainstalování obrazů operačních systémů.



Obrázek 11-6 Programové prostředí GNS3



Obrázek 11-7 Webové prostředí GNS v Mozille Firefox

12 Aplikace technologie GNS3 do laboratoře

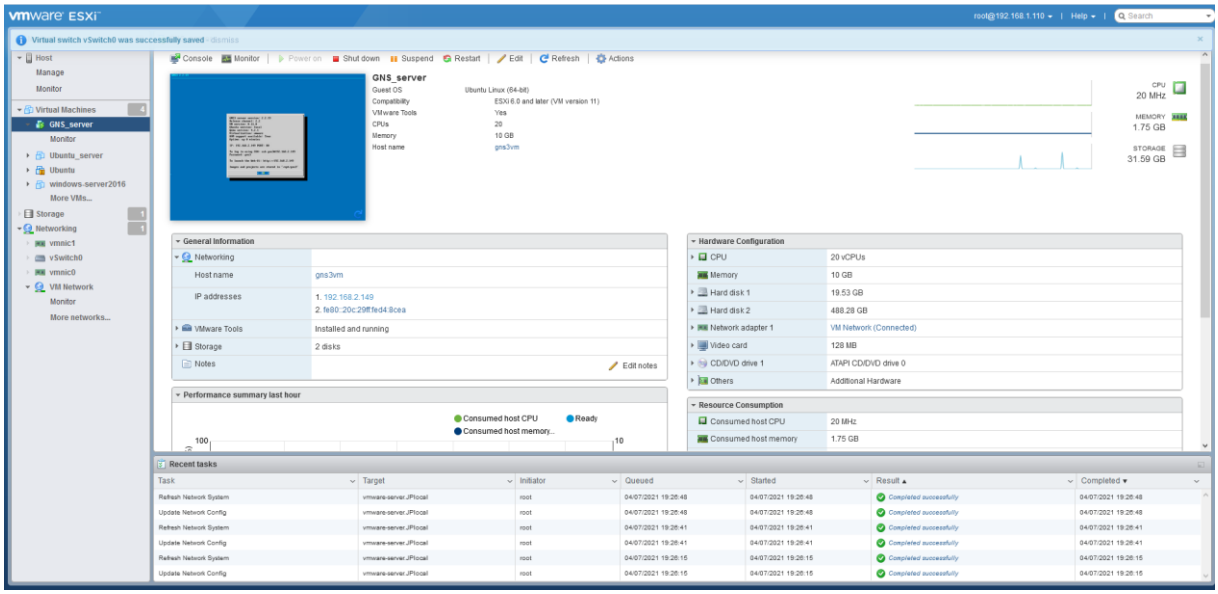
V této části se bude vycházet z předpokladu přenesení virtualizace veškerých síťových prvků na serverovou část a připojení koncového uživatele pomocí aplikace nebo webového prostředí na vybraný server. Nasazení aplikace do laboratorního prostředí vyžaduje serverovou a aplikační část. U serverové části je nutné zajistit výkon daného serveru, jelikož veškerý výpočet provádí pouze server. Velmi záleží na pracovním prostředí, kdy virtualizovaná síť s jedním osobním počítačem se systémem Windows 10 zabere alespoň 2 GB RAM. V případě prostředí s více osobními počítači bude nárok na velikost paměti RAM veliký. Standardní cvičení by mohlo vyžadovat serverovou paměť o velikosti 10 GB/jedno prostředí (uživatel). Pro dobré fungování laboratoře o 15studentech je potřeba aspoň 192 GB RAM.

Co se týká parametrů CPU, je vhodné vybrat ze serverových řad (Intel Xeon) alespoň 1 jádro na osobu. Pokud má server 2 CPU o 6fyzických a 6dalších logických jádrech, je možné vytvořit nezávislé prostředí až pro 30 studentů. Tento parametr je ale velmi závislý na použitých zařízeních ve virtualizaci. Nezbytná je ovšem podpora virtualizace, bez které nelze tyto programy spustit. Pro dobrý výkon je také dobré zvážit využití rychlých SSD disků, zvláště pro více uživatelů pracujících ve sejných časech.

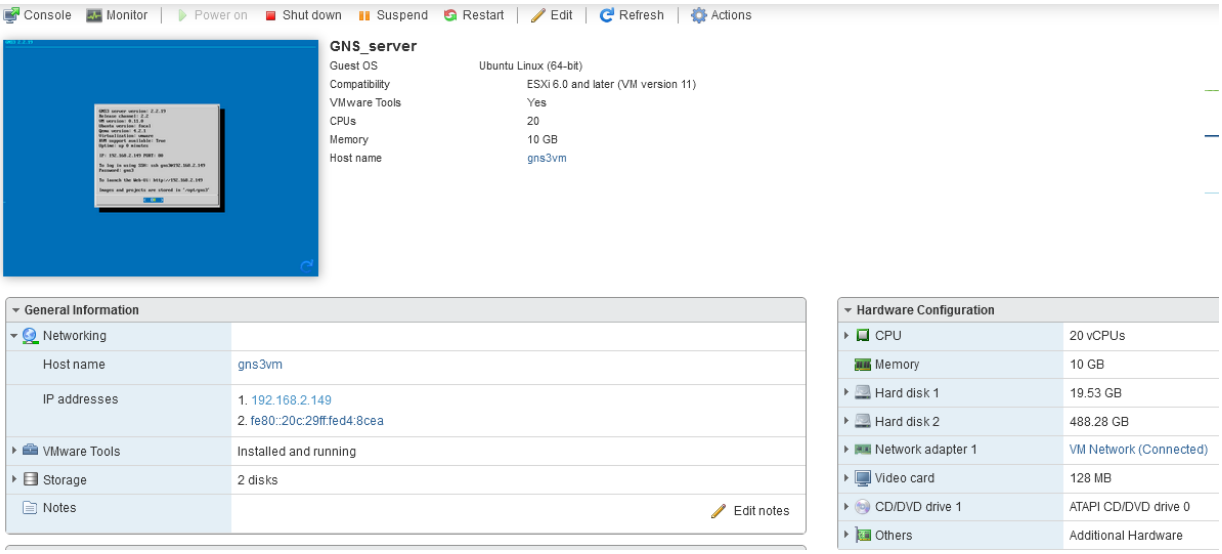
12.1 Instalace serverové části

Pro instalaci GNS serveru je možné zvolit jednu ze dvou možností. První možnost je tuto instanci nainstalovat jako mateřský systém přímo na daný hardware. Tato možnost je jednodušší, ale není příliš doporučovaná vzhledem k tomu, že celý server je vyhrazen pouze pro tento systém. Druhá možnost využívá virtualizačního systému pro obsluhu a zavedení operačního systému GNS serveru. Možný výběr je z linuxových systémů ProxMox nebo Vmware. Pro server využijeme vmware ESXi, což je specializovaný operační systém pro serverovou virtualizaci. Samotný vývojář programu GNS vydává speciální image systémů pro instalaci na těchto systémech. Zdarma je ke stažení z odkazu (https://www.gns3.com/software/download-vm). Po naimportování VM obrazu do systému VMware se stane součástí virtualizační platformy, a pokud není potřeba upravit parametry (velikost paměti RAM, počet CPU a podobně), je možné jej přímo spustit. Prostředí vmware lze vidět na obrázku 12-1 a samotné nastavení virtuálního stroje s nainstalovanou instancí GNS na obrázku 12-2. Na obrázku 12-3 je vidět samotné prostředí operačního systému, na kterém běží, a automaticky se spouští, aplikace GNS. Operační systém je linuxová distribuce systému Ubuntu bez grafického rozhraní s možností připojení pomocí SSH na konzoli OS.

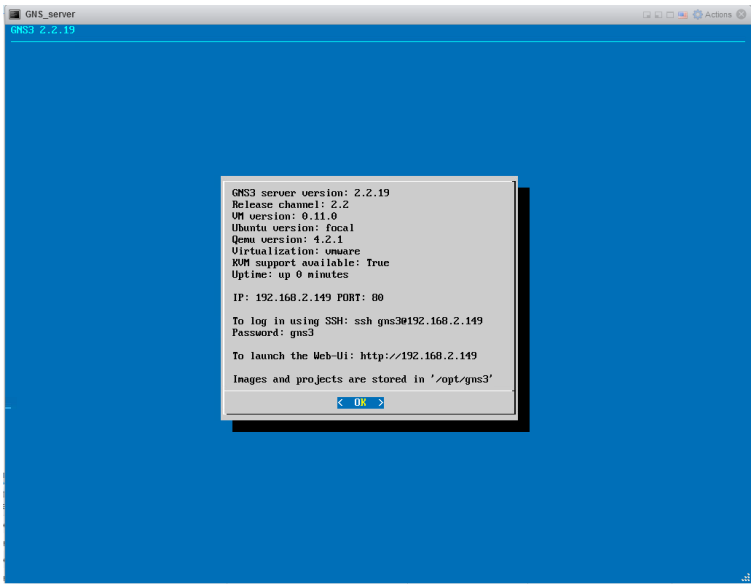
Pro konfiguraci samotného GNS je možné využít konzoli OS nebo webové a aplikační rozhraní pod definovanou IP adresou.



Obrázek 12-1 Prostředí vmware ESXi



Obrázek 12-2 GNS server ve vmware



Obrázek 12-3 Operační systém Ubuntu s předinstalovaným systémem GNS3

```
gns3@gns3vm:~$ ls
CiscoIOUKeygen3f.py  GNS3  iourc.txt
gns3@gns3vm:~$ cd GNS3/
gns3@gns3vm:~/GNS3$ ls
appliances  configs  symbols
gns3@gns3vm:~/GNS3$ cd configs/
gns3@gns3vm:~/GNS3/configs$ ls
ios_base_startup-config.txt         iou_l2_base_startup-config.txt  vpcs_base_config.txt
ios_etherswitch_startup-config.txt  iou_l3_base_startup-config.txt
gns3@gns3vm:~/GNS3/configs$ ..
bash: ..: command not found
gns3@gns3vm:~/GNS3/configs$ cd
gns3@gns3vm:~$ cd GNS3/appliances/
gns3@gns3vm:~/GNS3/appliances$ ls
gns3@gns3vm:~/GNS3/appliances$ ls -a
.  ..
gns3@gns3vm:~/GNS3/appliances$ cd
gns3@gns3vm:~$ cd GNS3/symbols/
gns3@gns3vm:~/GNS3/symbols$ ls
microsoft.svg
gns3@gns3vm:~/GNS3/symbols$ cd
gns3@gns3vm:~$ ls m-a
ls: cannot access 'm-a': No such file or directory
gns3@gns3vm:~$ ls -a
.   .bash_history  .bash_profile  .cache              .config  .iourc     .local    .sudo_as_admin_successful
..  .bash_logout   .bashrc        CiscoIOUKeygen3f.py  GNS3     iourc.txt  .profile  .wget-hsts
gns3@gns3vm:~$ sudo
usage: sudo -h | -K | -k | -V
usage: sudo -v [-AknS] [-g group] [-h host] [-p prompt] [-u user]
usage: sudo -l [-AknS] [-g group] [-h host] [-p prompt] [-U user] [-u user] [command]
usage: sudo [-AbEHknPS] [-r role] [-t type] [-C num] [-g group] [-h host] [-p prompt] [-T timeout] [-u user] [VAR=value]
            [-i|-s] [<command>]
usage: sudo -e [-AknS] [-r role] [-t type] [-C num] [-g group] [-h host] [-p prompt] [-T timeout] [-u user] file ...
gns3@gns3vm:~$ sudo ls
CiscoIOUKeygen3f.py  GNS3  iourc.txt
gns3@gns3vm:~$ sudo ls -a
.   .bash_history  .bash_profile  .cache              .config  .iourc     .local    .sudo_as_admin_successful
..  .bash_logout   .bashrc        CiscoIOUKeygen3f.py  GNS3     iourc.txt  .profile  .wget-hsts
gns3@gns3vm:~$
```

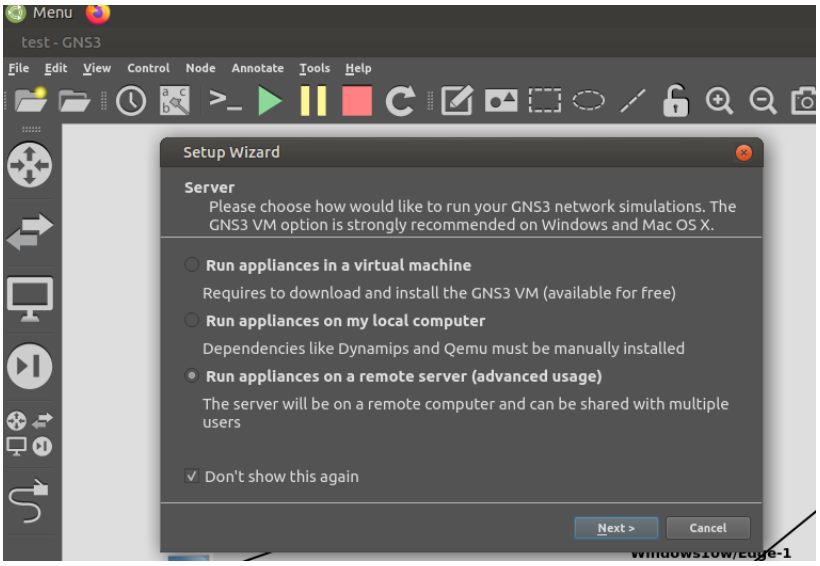
Obrázek 12-4 Příkazové prostředí v GNS3

V případě nainstalování GNS3 serveru je možné přejít na instalaci klientských stanic a přes některou naimportovat obrazy síťových prvků nebo PC. Všechny se instalují do adresáře /opt/gns3.

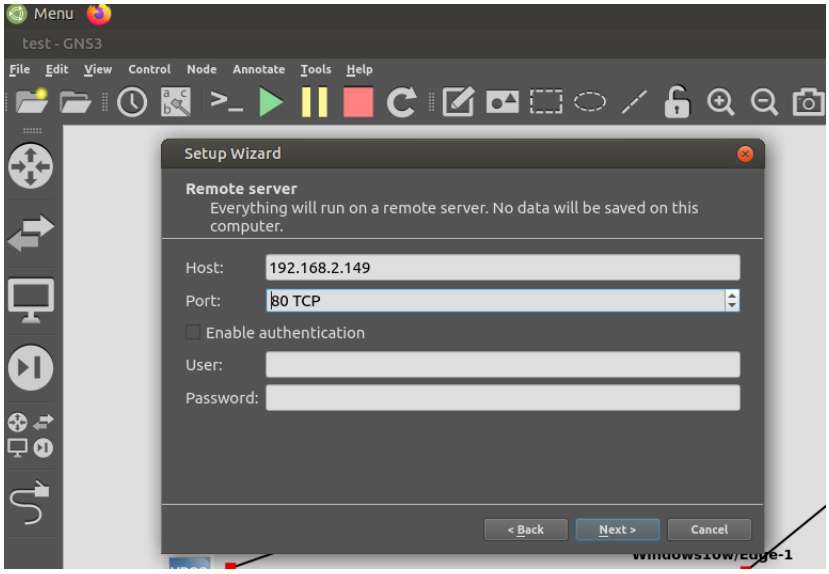
12.2 Instalace klientské části

V případě výběru aplikačního prostředí GNS jej lze stáhnout zdarma z oficiálních webových stránek (https://www.gns3.com/software/download). Podpora je napříč všemi systémy,

Windows, Linux a i MacOS. Po nainstalování a spuštění programu se zobrazí dialogové okno nastavení. Pro laboratoř se serverovou částí se zvolí možnost: Run appliances on a remote server. V další části se zadá IP adresa serveru a port přístupu na aplikaci. Po dokončení je instalace a nastavení připraveno k použití.



Obrázek 12-5 Instalace a nastavení programu GNS3



Obrázek 12-6 Instalace a nastavení IP serveru v GNS3

13 Příklady laboratorních cvičení

V této části budou nastíněna některá základní a pokročilá cvičení z oblasti telekomunikačních a počítačových sítí. Konfigurace bude zaměřená na konfigurování síťových prvků od společnosti Cisco nebo Mikrotik a osobních počítačů se systémem Windows nebo Linux. Cvičení budou vytvořena jak v prostředí Cisco packet tracer, tak v emulačním prostředí GNS3,

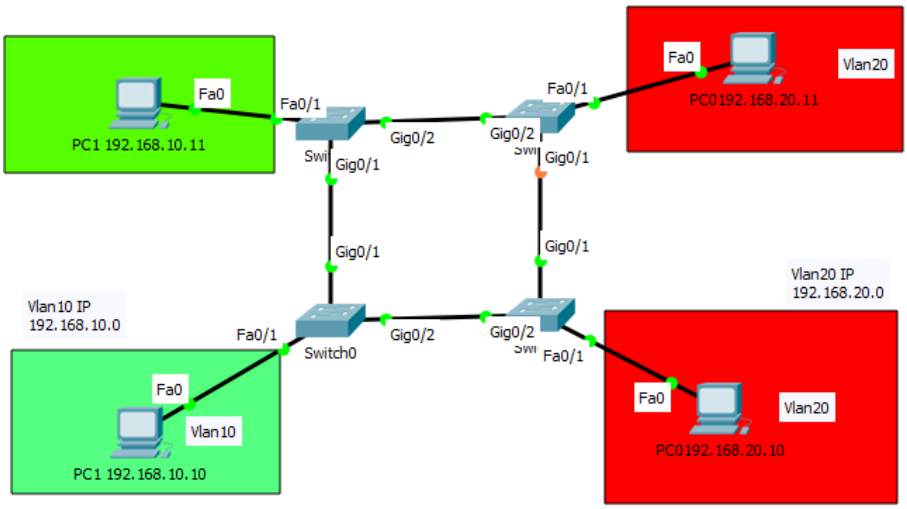
za použití serverové a klientské části. Vzájemně tak bude možné porovnat výhody a nevýhody daných řešení v laboratořích. Ke každému úkolu bude stanoveno zadání, podle kterého lze postavit celou síť včetně konfigurace. Je také možné síť sestavit, později naimportovat a na daných prvcích provádět konfiguraci.

13.1 Úloha 1 – nastavení VLAN a jednoduché zapojení

Zadání

V první úloze bude zadána jedna z nejzákladnějších úloh pro propojení a zajištění konektivity. Nadále bude potřeba vytvořit virtuální sítě pro rozdělení provozu mezi počítači.

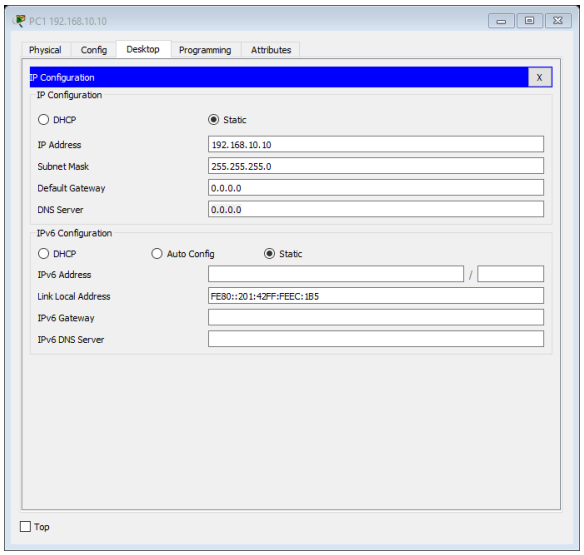
Vytvoříme infrastrukturu o čtyřech prvcích typu switch a vzájemně propojenou a případně zapojenou agregační linku, která v případě výpadku jiné dokáže provoz převzít (failover). Do každého switche bude také připojen alespoň jeden osobní počítač. Dva počítače budou zapojeny ve vlan10 a zbylé ve vlan20. Může být vzájemně zajištěno vyjednávání, aktualizace vlan a vytvoření záložních tras pomocí HSRP (Hot Standby Router Protocol), jako funkce inter-VLAN routing (funkce pracující na L3). Na všech zařízeních bude nastavena IP adresa tak, aby jej šlo nastavovat i na dálku za pomoci protokolu telnet nebo SSH.



Obrázek 13-1 Úloha 1 - schéma zapojení

Řešení

V první řadě nakonfigurujeme porty na počítačích. Přidělíme jim statickou IP adresu napsanou pod počítačem a shodnou s adresou sítě. V případě přidání IP adresy PC v packet traceru je postup jednoduchý, při výběru počítače se na kartě vybere možnost IP config a zadá se IPv4 nebo IPv6. Okno konfigurace IP adres pro dané zařízení je zobrazeno na obrázku 13-2. Obdobně nastavíme i ostatní počítače dle popsaných parametrů.



Obrázek 13-2 Nastavení IP adresy v PT

Obecná konfigurace switchů pro nastavení VLAN, IP adres a přístupu pomocí SSH.

```
SWITCH(config)#vlan 10 // vytvoření/přepnutí do VLAN 10
```

Nyní jsme v konfiguraci sítě VLAN a můžeme nastavit několik parametrů, dobré je nastavit jméno VLAN pro snadnější orientaci.

```
SWITCH(config-vlan)#name net1 // pojmenování VLANy
```

Z vlastností, které můžeme nastavit pro celou síť VLAN, zmíním pouze změnu IP MTU (maximální velikost přenášených paketů – payload rámce), standardní je 1500B pro Ethernet (rámec má velikost 1518B).

```
SWITCH(config-vlan)#mtu 2000 // možné hodnoty 576 až 18190 (podle typu switche)
```

Změny se uloží při opuštění konfigurace.

```
SWITCH(config-vlan)#exit // o úroveň výš
```

Zrušit VLANu můžeme standardně. Při zrušení síť VLAN však nedojde k odstranění vazeb, které na ni existují (jako zařazení portů do VLANy).

```
SWITCH(config)#no vlan 10 // smazání VLAN 10
```

Pozn.: VLAN vytvoříme také tím, když ji použijeme na určitém místě. Například pokud port zařadíme do neexistující VLAN, u prvků od firmy Cisco se daná VLAN automatiky vytvoří.

Nastavení IP adresy pro VLAN

VLAN neboli virtuální LAN je forma nastavení, kdy mohu v daném zařízení nastavit více jak jednu síť, a tak zvýšit bezpečnost i dostupnost.

```
SWITCH(config)#interface vlan 10 // přepnutí na interface dané vlany 10
SWITCH(config-if)#ip address 192.168.10.1 255.255.255.0 // nastavení IP adresy ve vlaně 10
SWITCH(config-if)#no shutdown // spuštění interface
```

Přiřazení portu do VLAN

Standardně jsou všechny porty zařazeny do VLAN 1. Pokud chceme nakonfigurovat přístupový port s pevným zařazením do VLANy, postupujeme následovně.

```
SWITCH(config)#interface f0/1 // přepnutí na port FastEthernet 1
SWITCH(config-if)#switchport mode access // nastavení portu do přístupového módu
SWITCH(config-if)#switchport access vlan 10 // zařazení do VLANy 10
```

Konfigurace Trunku

Aby se zachovala informace o zařazení do VLAN, a aby se přenášela data v různých sítích VLAN mezi přepínači, je třeba mezi nimi zřídit mód trunk. Pomocí tohoto modu lze přes port propouštět více než jednu VLANu. Ten se nastavuje na obou stranách, na portu, kterým jsou switche propojeny mezi sebou nebo portech v případě etherchannel. Můžeme využít standard IEEE802.1q (rozšíření rámce o hodnotu nesoucí číslo VLANy) nebo Cisco proprietální ISL (tagování rámce přiřazenou VLANou), které je podporováno pouze u vyšších Cisco switchů. Také je možné vyjmenovat VLANy, které se mohou trunkem přenášet, v opačném případě je v defaultním nastavení přenos všech známých vlan v systémovém souboru vlan.dat.

```
SWITCH(config)#interface f0/1 // přepnutí na port FastEthernet 1
SWITCH(config-if)#switchport trunk encapsulation dot1q // metoda encapsulation pro tagovací rámce
SWITCH(config-if)#switchport trunk allowed vlan 2-200 // povolení VLANy se přenáší
SWITCH(config-if)#switchport trunk native vlan 10 // určení nativní VLAN
SWITCH(config-if)#switchport mode trunk // nastavení portu do TRUNK modu
SWITCH(config-if)#no shutdown // spuštění portu
```

Přístup pomocí protokolu SSH

Telnet má nevýhodu, že se veškerá data (včetně hesel) zasílají nešifrovaná, takže je možno je odposlechnout a získat. Vhodnější je použít šifrované řešení, a tedy SSH. Abychom však mohli SSH použít, potřebujeme verzi IOSu, která obsahuje šifrování a následně pak při prvním nastavení vytvořit šifrovací klíč, podle kterého se šifra vypočítá. Potom musíme vytvořit uživatele, nastavit parametry SSH a vlastní nastavení přístupu. Vzdálený přístup pomocí SSH se nastavuje obdobně jako telnet, pouze zvolíme jiný port.

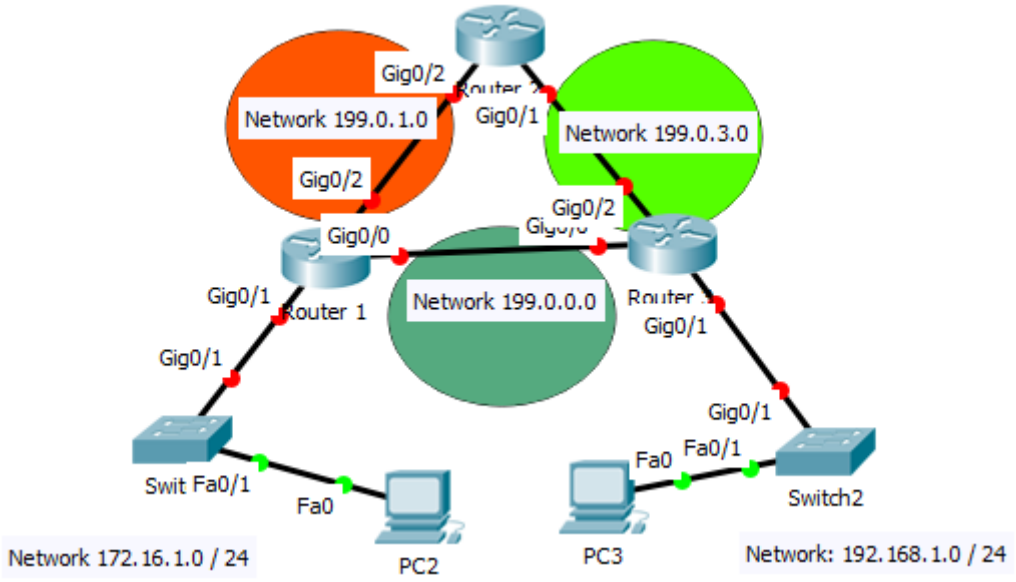
```
SWITCH(config)#aaa new-model                        // zapnutí AAA
SWITCH(config)#username cisco secret Heslo          // vytvoření uživatele
s heslem uloženým pomocí MD5 hashe
SWITCH(config)#ip ssh time-out 60                   // parametry SSH - vypršení
session
SWITCH(config)#ip ssh authentication-retries 2 // parametry SSH - počet
pokusů o přihlášení
SWITCH(config)#ip ssh version 2                     // parametry SSH - verze
SWITCH(config)#ip domain name firma.local          // jméno domény pro vytvářený
certifikát
SWITCH(config)#crypto key generate rsa // pokud ještě nemáme, vygenerujeme
klíč
SWITCH(config)#line vty 0 1 // konfigurace linky s ID 0 až 1 (různé
podle možnosti a daných interface určitého zařízení
SWITCH(config-line)# transport input ssh // výběr konzolového vstupu
protokolem SSH
```

13.2 Úloha 2 – nastavení routingu pomocí protokolu RIP

Druhá úloha bude nastavování základního routingu mezi routery. Využívat se bude nejjednoduššího protokolu RIP, případně RIPv2. Konektivita se prověří zasláním pingu mezi jednotlivými body. V rozšiřující verzi je možné připojit i jiného výrobce do sítě a otestovat tak funkčnost i na jiných systémech.

Zadání

Síť bude obsahovat dva počítače připojené do přepínače. Přepínače budou v defaultním nastavení, případně lze použít L3 přepínače a připojit se do routování. Tři routery budou vzájemně propojeny a budou simulovat síť ve větší instituci, kde je potřeba základního a jednoduchého routingu.



Obrázek 13-3 Úloha 2 - schéma zapojení

Řešení

Tato úloha je velmi jednoduchá a vyžaduje jen několik málo příkazů. Routovací protokol RIP je jednoduchý na implementaci do méně rozlehlých sítí. Z výše uvedených parametrů je možné nastavit maximálně 15 skoků, a to je u tohoto protokolu omezující. V síti o 3 routrech je ale toto řešení nejjednodušší. V této variantě je možné použít i statické směrování, které je ze všech nejbezpečnější, ale nedokáže vyjednat žádné změny, a tak se všechny musí manuálně upravit.

Přepínače v této úloze lze zanechat v defaultním nastavení. Na routrech se nastaví porty a IP adresy dle adresy sítí. Konfigurace pro Router1 je popsána níže. Obdobně se provede konfigurace i na ostatních routrech.

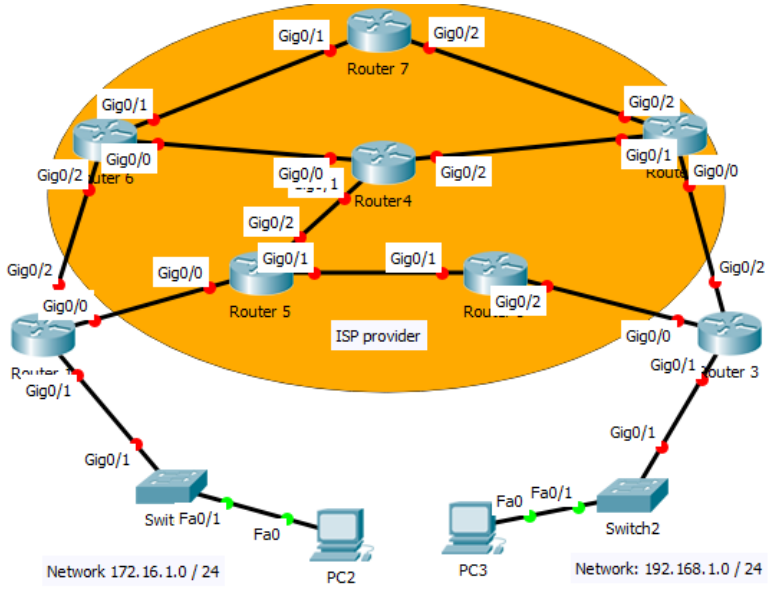
```
Router>enable
Router#configure terminal // konfigurační mód
Router(config)#interface GigabitEthernet 0/1 // Vybrání interfacu
Router(config-if)#no shutdown // zapnutí interfacu
Router(config-if)#ip address 172.16.1.1 255.255.255.0 // přidělení interfacu
IP adresu
Router(config-if)#exit
Router(config)#interface GigabitEthernet 0/0
Router(config-if)#ip address 199.0.0.1 255.255.255.0
Router(config-if)#no shutdown

Router(config)#router rip // zapnutí dynamického routingu technologií RIP
Router(config-router)#network 199.0.0.0 // přidání sítě do RIP tabulky
Router(config-router)#network 172.16.1.0 // přidání sítě do RIP tabulky
```

13.3 Úloha 3 – nastavení směrování pomocí protokolu BGP

Pomocí této úlohy lze vyzkoušet routování, které využívají zejména hlavní ISP provideři. Síť proto bude tvořit zejména mnoho routerů zastupujících jednotlivé přípojné body od ISP. Správnost redistribuce IP adres a konektivity se prověří pingem napříč body.

Zadání

Síť obsahuje 8 vzájemně propojených routerů. Pomocí protokolu BGP se provede routing a na základě zadání bude rozhodnuto o verzi BGP (iBGP nebo eBGP).



Obrázek 13-4 Úloha 3 - schéma zapojení

Řešení

Pro vyřešení tohoto úkolu je potřeba nastavit všechny směrovače do modu BGP, kdy každému routeru musíme přiřadit AS, což je identifikátor jednotlivých zařízení. V tomto případě můžeme využít různé AS a tím vytvořit verzi eBGP. Rozsah IP adres zvolíme z veřejného rozsahu libovolně. Známé jsou dvě sítě 17216.1.0/24 a 192.168.1.0/24, které by na konci nastavení měly být navzájem dostupné a propojené.

Příkazy Cisco IOSu pro konfiguraci BGP

```
ROUTER(config)#router bgp 100 // aktivuje BGP, 300 je číslo AS
ROUTER(config-router)#neighbor 190.0.0.1 remote-as 200 //určí sousedy, s kterými se vytvoří spojení, v daném AS
ROUTER(config-router)#neighbor 190.0.0.1 next-hop-self // nastaví danou adresu jako next hop
ROUTER(config-router)#neighbor 190.0.0.1 send-community // odešle community atributy sousedovi
ROUTER(config-router)#neighbor 190.0.0.1 update-source loopback 1 // jako zdrojový interface nastavíme loopback, pro IBGP můžeme chtít, aby spojení
```

```
stále běželo a nebyl definovaný specifický interface, proto můžeme použít
adresu loopback (127.0.0.1) což je softwarový port, který je vždy up
ROUTER(config-router)#neighbor 190.0.0.1 route-reflector-client  // nastaví,
že tento router je reflector, a určí jeho klienta
ROUTER(config-router)#no synchronization // vypne synchronizaci
ROUTER(config-router)#bgp always-compare-med // donutí router porovnávat
metriky cest z jiných AS

ROUTER#clear ip bgp * // vymaže BGP tabulky a session, *=(all) znamená
všechny, jinak se zadávají IP adresy
```

Zařazení prefix do routovacího procesu

```
ROUTER(config-router)#redistribute static     // vloží prefixy statických
route, zahrne je také do BGP tabulky
ROUTER(config-router)#network 172.16.0.1 mask 255.255.255.0 // které lokálně
naučené sítě (musí existovat v routovací tabulce) má zveřejnit a distribuovat
mezi ostatními.
```

Sumarizace adres v BGP

```
ROUTER(config-router)#redistribute static // možnost agregace
ROUTER(config-router)#network 198.10.0.0 mask 255.255.255.0 // třetí možnost
agregace (také dohromady s ip route)
```

Show příkazy – kontrola konfigurace

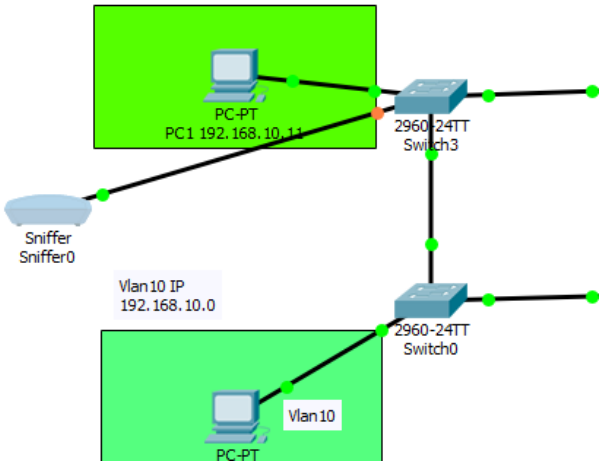
```
ROUTER#show ip bgp          // zobrazí routy, nejlepší je označena >
ROUTER#show ip bgp summary // souhrn všech spojení (seznam BGP sousedů)
ROUTER#show ip bgp path     // všechny cesty v DB
ROUTER#show bgp neighbor     // připojené sousední routery s informací
o reflektoru
ROUTER#show ip prefix-list // zobrazí prefix list
```

14 Sledování a analýza síťového provozu

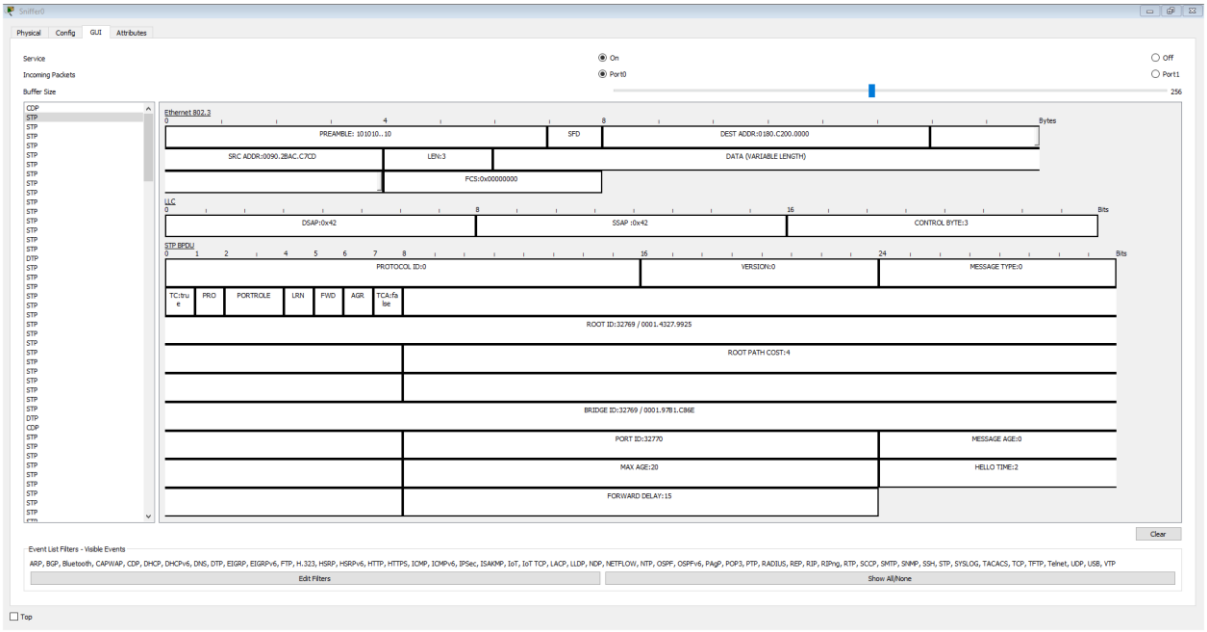
Pro sledování síťového provozu existují speciální programy, které tuto činnost usnadní. Na výběr je z několika možností, ale mezi jedny z nejpoužívanějších programů patří program WireShark. Lze také využít specializované operační systémy, jako je například Kali linux.

14.1 Funkce sledování provozu v Packet traceru

V případě packet traceru nelze nainstalovat program, který by byl schopný odchytávat komunikaci na daných portech. Částečně k tomu slouží objekt nazvaný sniffer, který provede základní výpis protokolů vyskytujících se v síti.



Obrázek 14-1 Sniffer v Packet traceru



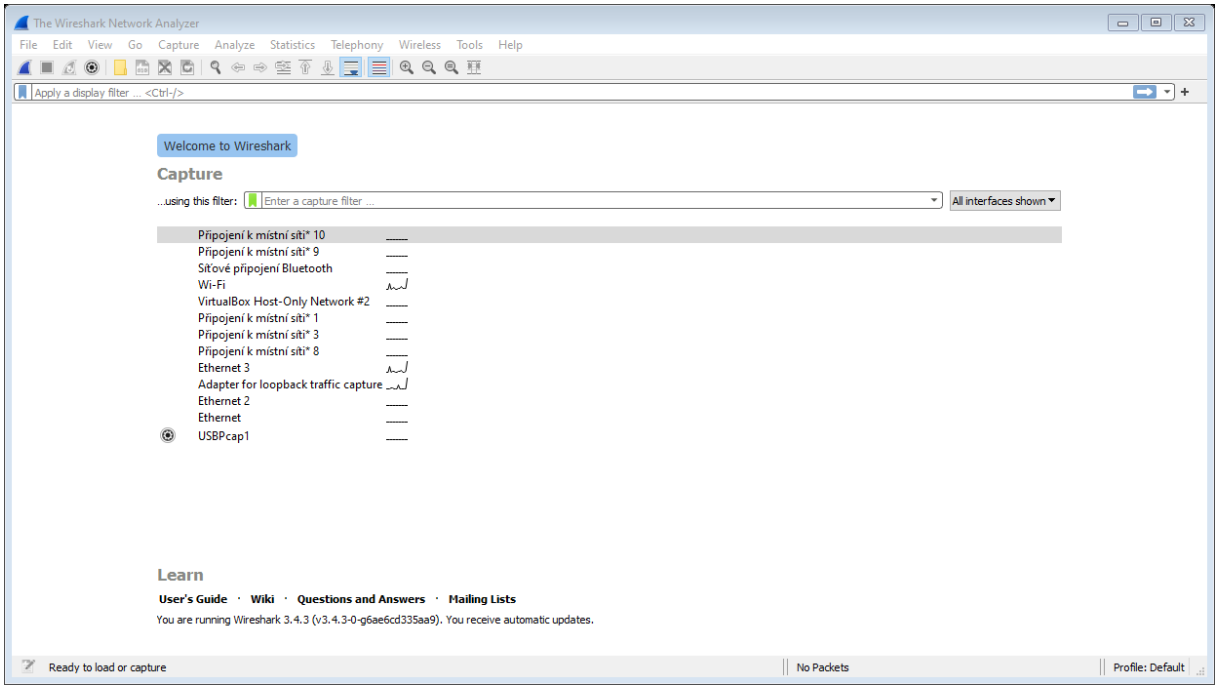
Obrázek 14-2 Prostředí Sniffru pro analýzu a sledování síťového provozu

Na obrázku 14-2 lze vidět zachycení některých protokolů na síti z úkolu 1. Konkrétně zde můžeme vidět CDP (Cisco Discovery Protocol) a STP (Spanning Tree Protocol). Program je schopný vygenerovat i vizualizaci datových rámců nebo paketů. Nicméně je toto pouze simulace a reálný provoz se na daných linkách neobjevuje. Navíc neobsahuje podrobnější parametry, jak reálně rámce a pakety vypadají.

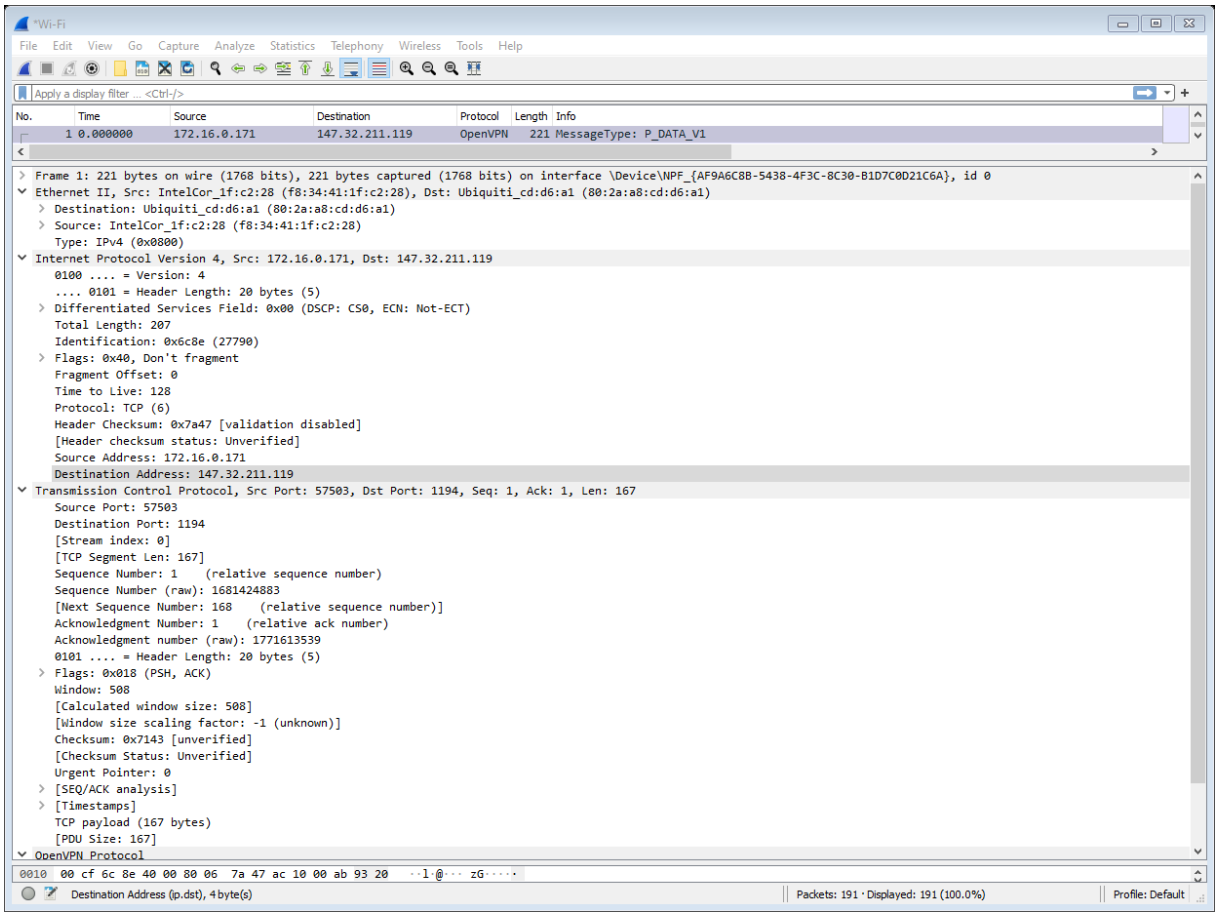
14.2 Program Wireshark pro sledování provozu

Tento program funguje jako aplikace v prostředí operačního systému. Podpora tohoto programu je jak pro systémy běžící na platformě Windows, tak i pro systémy s operačním

systémem na bázi Linuxu. V prostředí programu lze určit, jaká cesta by měla být sledována. Lze tak vybrat z různých síťových adaptérů v případě, že počítač obsahuje více portů nebo adaptérů pro připojení sítě (obrázek 14-3). V aplikaci lze filtrovat jednotlivé protokoly, anebo vyhledat komunikaci mezi jednotlivými IP adresami. Program funguje na principu chache, které se po zapnutí tlačítka sledování sítě naplňuje zachycenými daty. Následně je lze uložit a vyexportovat k podrobnější analýze. Na obrázku 13-4 lze vidět zachycení protokolu OpenVPN a jeho podrobný výpis nesených informací na různých síťových vrstvách. V porovnání s funkcí obsaženou v programu Packet traceru je v programu Wireshark zobrazená skutečná podoba síťové komunikace. V programu Packet tracer z funkčních důvodů nelze program Wireshark využít, proto je pro sledování síťového provozu řešení s emulovanou sítí v programu GNS3 mnohonásobně edukačně lepší než využití simulátoru Packet tracer.



Obrázek 14-3 Prostředí v aplikaci Wireshark po spuštění programu



Obrázek 14-4 Zachycení paketu s protokolem OVPN

15 Závěr

V této práci se zhodnotily a uvedly příklady využití virtualizace nebo simulace pro výuku a testování různých síťových úloh. Teoretická část se věnovala základním principům a funkcím, které se následně využily v praktické části. Funkce této laboratoře je umožnění praktických cvičení na jakémkoliv zařízení bez nutnosti fyzického hardwaru. To řeší mnoho problémů, které nastávají ve výuce, kdy není například možné vykonávat cvičení ve škole nebo student nemá časové dispozice k osobní účasti v laboratoři. Benefit spočívá také v možnosti kdykoliv práci uložit nebo přenést a následně ji vypracovat v jiný čas bez nutnosti fyzické účasti v laboratoři. Výhody jsou i na straně koncových zařízení, kdy je možné cvičení vykonávat na zařízení, které je velmi málo výkonné, s minimálními nároky. Laboratoř je tedy možné využívat i mimo rozvrh a každý má kdykoliv možnost cvičit různé konfigurace bez nutnosti fyzického navštívení laboratoře. Ukázané řešení je možné nadále vylepšovat přidáváním dalších operačních systémů a síťových prvků. Limitujícím faktorem je pouze hardwarové vybavení serveru, na které jsou při větším počtu uživatelů vyvíjeny vysoké nároky. V porovnání ceny serveru oproti reálným hardwarovým prvkům vychází server cenově lépe. Výhodou je také aktuálnost, kdy je možné kdykoliv upgradovat systém a nahrát nové zařízení. U fyzického hardwaru je nutné koupit hardware nový. Ten postupem času stárne a stává se zastaralým. V neposlední řadě je velmi nákladné nakoupit tolik zařízení, aby byl počet dostatečný pro plnohodnotné cvičení pro každého jednotlivce. Tak je možné zajistit plnohodnotnou výuku pro každého studenta bez nutnosti, aby více studentů sdílelo jeden hardware.

V práci byla vytvořena virtuální laboratoř za použití volně dostupných technologií, které byly modifikovány, nastaveny a rozšířeny o vlastní moduly a funce. Součást je i sada ilustrativních úloh, vytvořených podle osobních zkušeností a znalostí, v závislosti na teoretické části tak, aby splňovaly základní požadavky na praktické znalosti v jednotlivých úrovních. Nesporná výhoda spočívá v možnosti využití laboratoře odkudkoliv, kde je k dispozici připojení do sítě internet (v případě zajištění přístupu na server i ze sítě WAN).

V práci je možné nadále rozšiřovat o další virtualizované prvky různých typů a výrobců. Také je zde prostor pro vytvoření dalších laboratorních úloh pro cvičení více konkrétních funkcí. Řešení má výhodu v neomezené možnosti dalšího rozvoje a vytváření nových úloh, bez nutnosti programových či systémových změn.

16 Seznam použitých informačních zdrojů

[1] *Báječný svět počítačových sítí, část III. - Síťové architektury [online]. Dostupné z: https://www.earchiv.cz/b05/b0500001.php3*

[2] *Router Switching metody a související termíny – CAM, FIB, CEF [online]. Dostupné z: https://www.samuraj-cz.com/clanek/cisco-router-switching-metody-a-souvisejici-terminy-cam-fib-cef/*

[3] *Small form-factor pluggable transceiver. In: Wikipedia: the free encyclopedia [online]. San Francisco (CA): Wikimedia Foundation, 2001 - Dostupné z: https://en.wikipedia.org/wiki/Small_form-factor_pluggable_transceiver*

[4] *Switching modes [online]. Dostupné z: https://www.networkacademy.io/ccna/ethernet/store-and-forward-vs-cut-through-switching*

[5] *Configuring Active/Standby Failover [online]. Dostupné z: https://www.cisco.com/c/en/us/td/docs/security/asa/asa90/configuration/guide/asa_90_cli_config/ha_active_standby.html*

[6] *Difference Between UTP and STP Cables [online]. Dostupné z: https://techdifferences.com/difference-between-utp-and-stp-cables.html*

[7] *WWW Names and Addresses, URIs, URLs, URNs, URCs [online]. [cit. 2021-04-19]. Dostupné z: https://www.w3.org/Addressing/URL/Addressing.html*

[8] *Cisco command hierarchy* [online]. Dostupné z: https://www.cisco.com/E-Learning/bulk/public/tac/cim/cib/using_cisco_ios_software/02_cisco_ios_hierarchy.htm

16.1 Odborné publikace a dokumenty

SOSINSKY, Barrie, Pojsl JOSEF a Vaida PAVEL. Mistrovství – počítačové sítě. Brno: Computer press, 2010. ISBN 978-80-251-3363-7.

VELTE, Toby J. a Anthony T. VELTE. Síťové technologie Cisco: velký průvodce. Brno: Computer Press, 2003. ISBN 978-807-2268-573.

TRULOVE, James. Sítě LAN: hardware, instalace a zapojení. Praha: Grada, 2009. Profesionál. ISBN 9788024720982.

SAMURAJ – webový portál s databází konfigurací síťových prvků společnosti Cisco [online]. ©2021 [cit. 09.04.2021]. Dostupné z: https://www.samuraj-cz.com/

CISCO – webový portál s popisem konfiguračních možností všech zařízení společnosti Cisco, používající operační systém IOS [online]. ©2021 [cit. 09.04.2021]. Dostupné z: https://www.cisco.com/c/en/us/td/docs/switches/wan/mgx/mgx_8850/software/mgx_r3/rpm/rpm_r1-1/configuration/guide/appc.html

17 Seznam obrázků

18 Seznam tabulek

19 Použité technologie

1. Packet tracer
2. VMware – virtualizační serverový operační systém
3. GNS3
4. IOS Cisco firmware
5. Mikrotik OS
6. Windows 10 – edice pro testování
7. Kali linux OS
8. Ubuntu MATE – operační systém vhodný pro minipočítače RaspberryPi
9. Server DELL 610R – 2 CPU Xeon (2x12 core) 2,6 GHz

Univerzita Karlova, Pedagogická fakulta

M. Rettigové 4, 116 39 Praha 1

Evidenční list žadatelů o nahlédnutí do listinné podoby práce

Jsem si vědom/a, že závěrečná práce je autorským dílem a že informace získané nahlédnutím do zveřejněné závěrečné práce nemohou být použity k výdělečným účelům, ani nemohou být vydávány za studijní, vědeckou nebo jinou tvůrčí činnost jiné osoby než autora.

Byl/a jsem seznámen/a se skutečností, že si mohu pořizovat výpisy, opisy nebo rozmnoženiny závěrečné práce, jsem však povinen/povinna s nimi nakládat jako s autorským dílem a zachovávat pravidla uvedená v předchozím odstavci tohoto prohlášení.

Poř. č.	Datum	Jméno a příjmení	Adresa trvalého bydliště	Podpis
1.				
2.				
3.				
4.				
5.				
6.				
7.				
8.				
9.				
10.				

Univerzita Karlova, Pedagogická fakulta
M. Rettigové 4, 116 39 Praha 1

Prohlášení žadatele o nahlédnutí do listinné podoby práce před její obhajobou

Závěrečná práce:

Druh závěrečné práce: Bakalářská práce

Název závěrečné práce: Laboratoř pro výuku a testování síťových prvků

Autor práce: Marcel Poláček

Jsem si vědom, že závěrečná práce je autorským dílem a že informace získané nahlédnutím do zveřejněné závěrečné práce nemohou být použity k výdělečným účelům, ani nemohou být vydávány za studijní, vědeckou nebo jinou tvůrčí činnost jiné osoby než autora.

Byl jsem seznámen se skutečností, že si mohu pořizovat výpisy, opisy nebo rozmnoženiny závěrečné práce, jsem však povinen s nimi nakládat jako s autorským dílem a zachovávat pravidla uvedená v předchozím odstavci tohoto prohlášení.

Jsem si vědom, že pořizovat výpisy, opisy nebo rozmnoženiny dané práce lze pouze na své náklady.

V Praze dne ……

Jméno a příjmení žadatele	
Adresa trvalého bydliště	

.....

podpis