**Maturitní práce**

**Návrh struktury internetu**

Studijní obor: 18-20-M/01 Informační technologie

Autor:

**Marek Borůvka** Podpis:

Vedoucí práce:

**Mgr. Harašta Milan**

Třída: **4.D** Školní rok: **2023/2024**

**ZÁVAZNÁ PŘIHLÁŠKA K ŘEŠENÍ MATURITNÍ PRÁCE**

Příjmení a jméno žáka: Marek Borůvka Třída: 4.D Školní rok: 2023/2024

Téma: **Návrh struktury internetu**

Vedoucí práce (VP): Mgr. Harašta Milan

Licenční ujednání:

1. Ve smyslu § 60 autorského zákona č. 121/2000 Sb. poskytuji Střední průmyslové škole, Česká Lípa, Havlíčkova 426, příspěvková organizace výhradní a neomezená práva (§46 a §47) k využití mé maturitní práce.
2. Bez svolení školy se zdržím jakéhokoliv komerčního využití mé práce.
3. V případě komerčního využití práce školou obdrží žák – autor práce odměnu ve výši jedné třetiny dosaženého zisku.
4. Pro výukové účely a prezentaci školy se vzdávám nároku na odměnu za užití díla.

V České Lípě dne: 6. 11. 2023

|  |
| --- |
| Termín odevzdání: 26. 5. 2024 |
| Kritéria hodnocení: 1. za vypracování od vedoucího práce,  2. za vypracování od oponenta práce,  3. obhajoba práce bude hodnocena komisí.  Výsledné hodnocení bude rozhodnutím komise s přihlédnutím k hodnocení bodů 1. až 3. |
| Požadavky: Žák odevzdá práci včetně příloh elektronicky v pdf souboru vedoucímu práce. |
| Vyjádření ředitele školy: Povoluji konat MP.  Ředitel školy stanovil délku obhajoby maturitní práce na 20 minut. |

Schváleno procesem Schvalování v MS Teams.

Charakteristika práce:

Cílem práce je popsat a emulovat strukturu internetu pomocí Packet traceru. Praktická část bude

obsahovat zjednodušenou a funkční strukturu internetu - úlohu v Packet traceru.

Licenční ujednání

Ve smyslu zákona č. 121/2000 Sb., O právu autorském, o právech souvisejících s právem autorským, ve znění pozdějších předpisů (dále jen autorský zákon) jsou práva k maturitním nebo ročníkovým pracím následující:

Zadavatel má výhradní práva k využití práce, a to včetně komerčních účelů.

Autor práce bez svolení zadavatele nesmí využít práci ke komerčním účelům.

Škola má právo využít práci k nekomerčním a výukovým účelům i bez svolení zadavatele a autora práce.

Prohlášení

Prohlašuji, že jsem svou ročníkovou práci vypracoval/a samostatně a použil/a jsem pouze prameny a literaturu uvedené v seznamu bibliografických záznamů.

Prohlašuji, že tištěná verze a elektronická verze práce jsou shodné.

Nemám závažný důvod proti zpřístupňování této práce v souladu s autorským zákonem.

V České Lípě dne ………………………………………………

Jméno a příjmení autora

Poděkování

Anotace

Klíčová slova

Annotation

Key word

Obsah

[1 Úvod 8](#_Toc163060078)

[2 Teoretická část práce 9](#_Toc163060079)

[2.1 Obecné informace o internetu 9](#_Toc163060080)

[2.1.1 Historie 9](#_Toc163060081)

[2.1.2 Kdo vlastní internet 9](#_Toc163060082)

[2.1.3 Klient/server model 10](#_Toc163060083)

[2.1.4 Referenční modely 10](#_Toc163060084)

[2.1.5 Služby internetu 10](#_Toc163060085)

[2.2 TCP/IP 10](#_Toc163060086)

[2.2.1 IPv4 10](#_Toc163060087)

[2.2.2 IPv6 11](#_Toc163060088)

[2.2.3 Další protokoly 11](#_Toc163060089)

[2.3 Síťové prvky 13](#_Toc163060090)

[2.3.1 Aktivní prvky 13](#_Toc163060091)

[2.3.2 Pasivní prvky 15](#_Toc163060092)

[3 Praktická část práce 16](#_Toc163060093)

[3.1 Packet tracer 16](#_Toc163060094)

[3.2 Síť LAN 16](#_Toc163060095)

[3.2.1 Nastavení ML switche 17](#_Toc163060096)

[3.3 Síť WAN 17](#_Toc163060097)

[3.3.1 Redundance 18](#_Toc163060098)

[3.4 Otestování funkčnosti internetu 18](#_Toc163060099)

[3.5 Služby internetu 18](#_Toc163060100)

[3.5.1 Webové stránky 18](#_Toc163060101)

[3.5.2 E-mail 19](#_Toc163060102)

[4 Závěr 20](#_Toc163060103)

[5 Citace 21](#_Toc163060104)

[6 Seznam obrázků 23](#_Toc163060105)

[7 Přílohy 24](#_Toc163060106)

Použité zkratky

# Úvod

Tématem maturitní práce je návrh struktury internetu. Práce je rozdělená na dvě části – praktickou  
a teoretickou.

Teoretická část se věnuje historii internetu, organizacím které spravují internet, protokolům díky kterým je komunikace na internetu možná nebo síťovým prvkům

Praktická část se věnuje představení struktury internetu, kterou jsem navrhl, vysvětlení jak funguje a k čemu jsou jednotlivé prvky,

# Teoretická část práce

## Obecné informace o internetu

Internet je celosvětová síť, která umožňuje komunikaci počítačům které k sobě nejsou fyzicky připojeny, někdy se taky internetu přezdívá jako „síti sítí“. Sítě, které internet může propojovat jsou soukromé nebo veřejné. Soukromé sítě jsou takové, kde majitel umožňuje přístup pouze vybraným uživatelům, jsou zabezpečeny heslem, např. domácí sítě, pracovní atd. Veřejné jsou takové kde mají přístup všichni bez nutnosti hesla, sítě v kavárnách, obchodech. Komunikace probíhá pomocí World Wide Webu (www), emailových serverů, sdílení souborů…

### Historie

Základem počítačových sítí je propojování paketů, tento princip vyvinul na začátku šedesátých letech Paul Baran, později nezávisle Donald Davies, který zavedl název „packet“. První moment kdy můžeme mluvit o jakémsi internetu byl projekt ARPANET. Původně vojenský projekt, který měl za cíl vyzkoušet nové technologie jako decentralizaci, neměla ústředny, rozdělení dat na packety, přepojování packetů a základy protokolů. Prvními uzly ARPANETu byly uzly na Kalifornské univerzitě v Los Angeles,SRI International, Kalifornské univerzitě v Santa Barbařea Utažské univerzitě. Později byly přidány další uzly po celý Spojených státech (40 v roce 1973). Obsah obrázku skica, text, kresba, diagram

Popis byl vytvořen automatickyObrázek 1 – Síť ARPANET v březnu 1972

V 1973 se připojilo Norsko a Spojené království. Zajímavostí je, že v této síti se začal šířit první vir s názvem Creeper, pro jeho odstranění také vznikl první antivir Reaper. V roce 1982 byl protokol TCP/IP standardizován pro komunikaci v ARPANETu což umožnilo komunikaci po celém světě. V roce 1989 se ve Spojených státech objevují první poskytovatelé internetového připojení. Vývoj polovodičů a optických sítí nabídl možnost komerčního využití počítačových sítí. V polovině roku 1989 MCI mail a Compuserve vytvořili první komerční přístup do internetu pro veřejnost. O několik měsíců později PSINet spustili jejich síť, která se stala jednou z páteřních sítí pozdějšího internetu. V prosinci 1990 Tim Bernes-Lee vydává WorldWideWeb (první internetový prohlížeč), HTTP protokol, HTML jazyk, HTTP web server (CERN httpd) a první webové stránky. V roce 1991 byl založen CIX, který dovolil komerčním sítím komunikaci vzájemnou komunikaci.

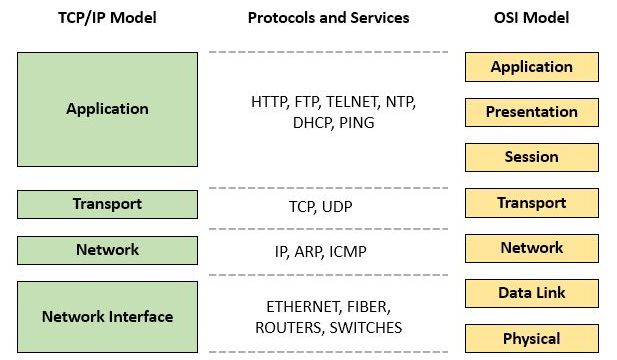
### Kdo vlastní internet

Internet je decentralizovaná síť a také není nikým vlastněn. Je to síť sítí, která propojuje nezávislé sítě dohromady. Přesto musejí existovat organizace, které budou tuto síť spravovat a vytvářet standardy protokolů. O protokoly se stará nezisková organizace Internet Engineering Task Force (IETF), česky Komise pro technickou stránku internetu. Tato organizace nemá zaměstnance, ale kdokoliv na světě se může přihlásit do pracovní skupiny nebo na IETF setkání. ICANN je organizace která je zodpovědná za dohled nad doménami první úrovně (.com, .net) a vytváří pravidla a standardy pro registrátory domén. IANA je pod organizací ICANN a má za úkol dohlížení na přidělování IP adres, číselné kódy protokolů a správu kořenového DNS serveru. O samotné přidělování adres se starají Regionální Internetové Registry (RIR) – ty se následně dělí do 5 registrů AFRINIC –pro Afriku, ARIN – Antarktika, Canada, USA, část Karibiku, APNIC – Asie a Pacifik, LACNIC – Latinská amerika, část Karibiku, RIPE NCC – Evropa, Rusko, Centrální a Západní Asie. O standarty pro World Wide Web se stará konsorcium W3C.

### Klient/server model

Je mode kde server slouží jako poskytovatel služby klientovy (webový server, emailový server…) který na server posílá požadavky a server mu odpovídá. Tento model nemusí být rozdělený, oba, server i klient, mohou být součástí stejného systému (počítače). Klient serveru neposkytuje svoje zdroje, pouze si „půjčuje“ od serveru, který čeká až bude klientem dotázán.

### Referenční modely

Referenční modely jsou příklad řešení komunikace v sítích. Existují dva modely, OSI/ISO a TCP/IP. OSI/ISO rozděluje komunikaci do sedmi vrstev (aplikační, prezenční, relační, transportní, síťová, linková, fyzická) zatím co TCP/IP model počet zmenšil na čtyři, někdy pět, vrstev (aplikační, transportní, síťová, síťové rozhraní (někdy se rozděluje na fyzickou a linkovou)). TCP/IP vychází z OSI/ISO a upravuje ho tak, aby byl více flexibilní a praktičtější na realizaci, zatím co OSI/ISO je spíše teoretický model.

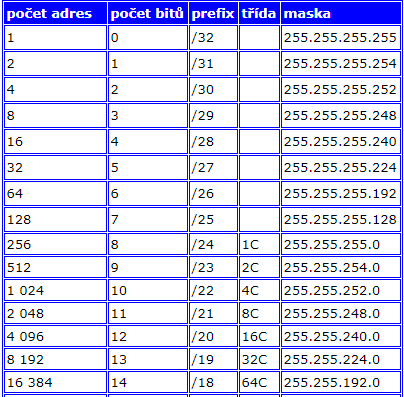
Obrázek 2 – Porovnání TCP/IP s OSI/ISO modelem

### Služby internetu

## TCP/IP

Aby počítače spolu mohli komunikovat, tak stejně jako lidi, musí „mluvit“ stejným jazykem. Pro počítače tento jazyk je definovaný v protokolech. Dnes používaná sada protokolů je zvaná TCP/IP. TCP/IP spojuje sady protokolů TCP (Transmission Control Protocol – „řízení provozu“) a IP (Internet Protocol – „protokol pro propojen sítí“).

### IPv4

Aby bylo možné počítače v síti od sebe rozeznat je nutné jim dát identifikátor, pro tento účel se používají ip adresy. U protokolu IPv4 tyto adresy jsou 32 bitové a jsou zapisovány v dot-decimal (volně přeloženo jako  
desítkový-tečkový) formátu např. 10.10.0.150. Celkový počet adres je 232 (přibližně 4 miliardy adres), ne všechny je ale možné používat, některé jsou rezervované pro privátní sítě, broadcast, loopback atd. Kvůli „malému“ počtu adres tohoto protokolu se ip adresy rozdělili do dvou velkých skupin, veřejné a soukromé (privátní) ip adresy. Adresy musí být v rámci sítí jedinečné, nesmí existovat dvě stejné veřejné ip adresy v internetu a stejně tak nesmí být dvě stejné privátní adresy v rámci jedné sítě. Masky v IPv4 protokolu slouží pro identifikaci, jaká část  
ip adresy slouží jako identifikátor sítě a která část jako identifikátor zařízení. Maska je binárně složena z jedniček a nul. Jedničky slouží pro nalezení sítě a nuly pro zařízení. Příklad 192.168.0.1/24 – prefix 24 odpovídá masce (zapsané v dot-decimal) 255.255.255.0 –> první (z leva) bajt je pro zařízení, 192.168.1.1/23 – 23 -> 255.255.254.0 – první a druhý bajt je pro zařízení. Masky taky označují počet subnetů. Prefix 24 má jeden subnet, 25 má 2 subnety, 26 čtyři atd. až do prefixu 32. Díky subnetům jsme schopní omezit naší síť na menší počet ip adres a tak zvýšit její bezpečnost. Pro výpočet subnetů musíme vědět kolik jednotlivé prefixy umožňují ip adres, musíme ale také mít na paměti, že z každého subnetu odečítáme dvě ip adresy které jsou rezervované pro bázi a broadcast. Báze je vždy první ip adresa broadcast poslední. Protokol IPv4 dále používá službu NAT (Network Address Translation – překlad síťových adres). Tato služba funguje tak, že se adresa zdroje (například náš počítat) přeloží na adresu routeru, který paket zpracuje, a pošle ho na další router, zde je znova přeložen. Při cestě zpátky se routery podívají do tabulky a podle adresy zjistí kam mají paket poslat.

Obrázek 3 – tabulka prefixů s počtem ip adres

#### Privátní ip adresy

Privátní ip adresy jsou takové které nejsou přímo přístupné z internetu, maskují se za jednu veřejnou ip adresu. Tyto adresy jsou vyhrazené a dělí se do tříd A,B a C. Ip adresy třídy A mají rozsah od 10.0.0.0 do 10.255.255.255, třída B 172.16.0.0 až 172.31.255.255, třída C 192.168.0.0 až 192.168.255.255. Privátní adresy jsou používány v domácích nebo firemních sítích. Výhodou privátních adres je bezpečnost, jelikož všechny počítače se díky překládání adres (NAT) „schovávají“ za adresu routeru. Další výhodou je, že se tyto ip adresy mohou opakovat v různých sítích, na rozdíl od veřejných, které musí být unikátní v celém internetu.

#### Veřejné ip adresy

Veřejné ip adresy jsou přístupné každému počítači a jejich adresa musí být unikátní. Veřejné adresy zpravidla slouží pro servery nebo routery které musí být identifikovatelné z jakéhokoliv místa (Google DNS: 8.8.8.8, YouTube server: 142.250.203.110). Tyto adresy v dnešní době už došli, proto se postupně začalo přecházet k nástupci IPv4, IPv6.

### IPv6

Internet Protocol verze 6 (IPv6) je nástupcem IPv4 a představuje klíčovou technologii pro budoucí rozvoj internetu a síťovou komunikaci. S nedostatkem dostupných IPv4 adres a rostoucím počtem připojených zařízení se IPv6 stává nezbytným řešením pro udržení a rozvoj internetu. IPv6 hlavička je navržena jednodušeji než u IPv4, což umožňuje rychlejší a efektivnější komunikaci v síti. Déle ve většině případů není potřeba NATu, jelikož adresní prostor je větší, což zjednodušuje správu sítě. Nevyužívání NAT by so mohlo zdát jako nebezpečné, ale není tomu tak. IPv6 podporuje IPsec protokol, který datagramy (třetí vrstva) šifruje. Celosvětová adopce IPv6 by se mohla zdát jako vzdálená budoucnost, ale opak je pravdou. Podle statistik Googlu celosvětově IPv6 protokol využívá k 25. únoru 2024 43,63% uživatelů Googlu. Nejvíc je IPv6 využívaná v Indii (72,02% uživatelů), v Česku tento protokol využívá 25,7% uživatelů.[[1]](#footnote-2)

### Další protokoly

#### ARP

Address Resolution Protocol zjišťuje fyzickou adresu MAC pomocí známé IP adresy. Opačný protkol RARP, který zjišťuje IP adresu podle MAC se dnes prakticky nepoužívá. Tento protokol je využívaný na routerech a switchích, když potřebují zjistit MAC adresy zařízení. Protokol funguje na bázi broadcast dotazu (pošle dotaz všem zařízením které jsou připojeny) od switche/routeru (MAC adresa FFFF.FFFF.FFFF), zařízení dále „odpoví“ jestli se IP adresa v dotazu shoduje s adresou zařízení.

#### ICMP

Internet Control Message Protocol slouží k přenosu služebních informací (např. chybová hlášení, požadován služba není dostupná nebo potřebný počítač není dostupný), je využíván např. v programu ping nebo traceroute.

#### TCP a UDP

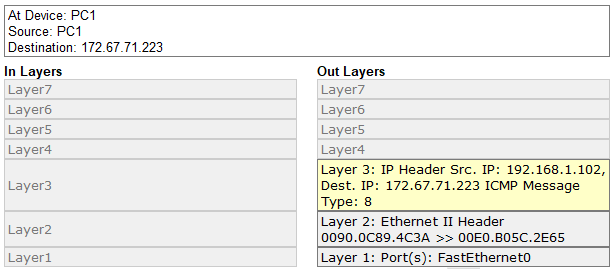
Protokoly TCP a UDP slouží pro přenos dat po síti. TCP je [spojově orientovaný](https://cs.wikipedia.org/wiki/Spojovan%C3%A1_komunikace) protokol, prvně musí být navázáno spojení, pro přenos toku [bajtů](https://cs.wikipedia.org/wiki/Bajt) na transportní vrstvě se [spolehlivým](https://cs.wikipedia.org/wiki/Spolehlivost_(po%C4%8D%C3%ADta%C4%8Dov%C3%A9_s%C3%ADt%C4%9B)) (ověřovaným) doručováním. Je využíván pro například WWW, email nebo SSH. UDP je bez záruky doručení (neověřovaný). Výhodou je menší zátěž přenosu, jelikož se neověřuje zda předchozí datagramy dorazily. Využívá se u DNS serverů, online her atd.

## Síťové prvky

### Aktivní prvky

#### Routery

Obsah obrázku text, snímek obrazovky, Písmo, číslo

Popis byl vytvořen automatickyObsah obrázku text, snímek obrazovky, číslo, Písmo

Popis byl vytvořen automatickyRoutery jsou zařízení která pracují na třetí (síťové) vrstvě OSI/ISO modelu. Routery dokážou spojit dvě, nebo více, sítí do hromady, tak aby spolu dokázali komunikovat počítače a jiné zařízení. Na rozdíl od switchů, které pracují s MAC adresou, routery pracují i s IP adresou. Když chceme komunikovat se zařízením, počítač sám zjistí, jestli zařízení je součástí sítě nebo ne. Když je tak jako cílovou IP adresu a Mac adresu označí to zařízení se kterým chce komunikovat. Když se ale zařízení nachází mimo naší síť (př. webový server github.com) tak jako cílovou IP adresu uvede adresu zařízení se kterým chceme komunikovat, ale MAC adresu uvede adresu brány (anglicky gateway) počítače. Gateway je jeden z módů, ve kterém mohou routery fungovat, jeho cílem je spojit dvě rozdílné sítě (na rozdíl od mostu (bridge) který spojuje stejnou síť na dvou různých místech (např. jiná budova).  
 V tomto případě Wireless Router1 je brána pro počítač PC1.   
Když paket odcházel z PC1 tak jako zdrojová IP a MAC adresa je adresa PC1, ale když paket došel na router tak se obě adresy změnili na adresu routeru. Tomu procesu se říká NAT (Network address translation). A jako cílová MAC adresa je zapsán další zařízení v pořadí (Switch1). Jak paket dále putují internetem tak se na routerech znova nepřekládá NATem (IP adresa zůstává našeho routeru) ale zdrojová MAC adresa se změní na adresou routeru který paket posílá a cílová na další zařízení. Aby routery poté věděli kam mají paket vrátit tak si obě adresy uloží do tabulky.

Obrázek 4 – Obsah paketu po NATu na routeru

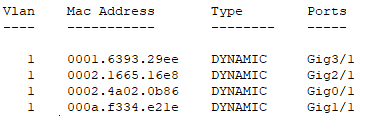
Obrázek 5 – IP a MAC adresy při komunikaci se zařízením mimo síť

Obrázek 6 – IP a MAC adresy při komunikaci se zařízením v síti

#### Switch

Obsah obrázku text, snímek obrazovky, Písmo, řada/pruh

Popis byl vytvořen automatickyObsah obrázku text, snímek obrazovky, Písmo, řada/pruh

Popis byl vytvořen automatickySwitche jsou aktivní prvky, které pracují na druhé (linkové) vrstvě OSI/ISO modelu. Nahradili dřívější huby. Výhodou switche od hubu je to, že switch dokáže identifikovat s kým chceme mluvit. To huby neumějí a posílají data (na druhé vrstvě známé jako rámce) všem uzlům kteří jsou s ním propojeni, to značně zpomaluje komunikaci v síti. Switch pro identifikaci uzlu používá takzvanou CAM (Content Addressable Memory) tabulku do které si switch ukládá záznam o MAC adrese portu uzlu. Když potom chceme komunikovat s například jiným počítačem v síti tak se do paketu zapíše zdrojová a cílová MAC a IP adresa.   
Switch zjistí jakému portu odpovídá Mac adresa a na ten pošle příchozí paket. Na cílovém počítači je paket přijat a vytvořen nový paket, který má prohozené MAC a ip adresy. Proces se poté opakuje do konce přenosu.[[2]](#footnote-3)

Obrázek 7 – část paketu s cílovou a zdrojovou MAC adresou

Obrázek 8 – část paketu s cílovou a zdrojovou IP adresou

Obrázek 9 – výpis z CAM tabulky

Obsah obrázku text, snímek obrazovky, Písmo, číslo

Popis byl vytvořen automatickyObsah obrázku text, snímek obrazovky, číslo, Písmo

Popis byl vytvořen automaticky

Obrázek 10 – IP a MAC adresy v paketu na Laptop3

Obsah obrázku text, snímek obrazovky, Písmo, číslo

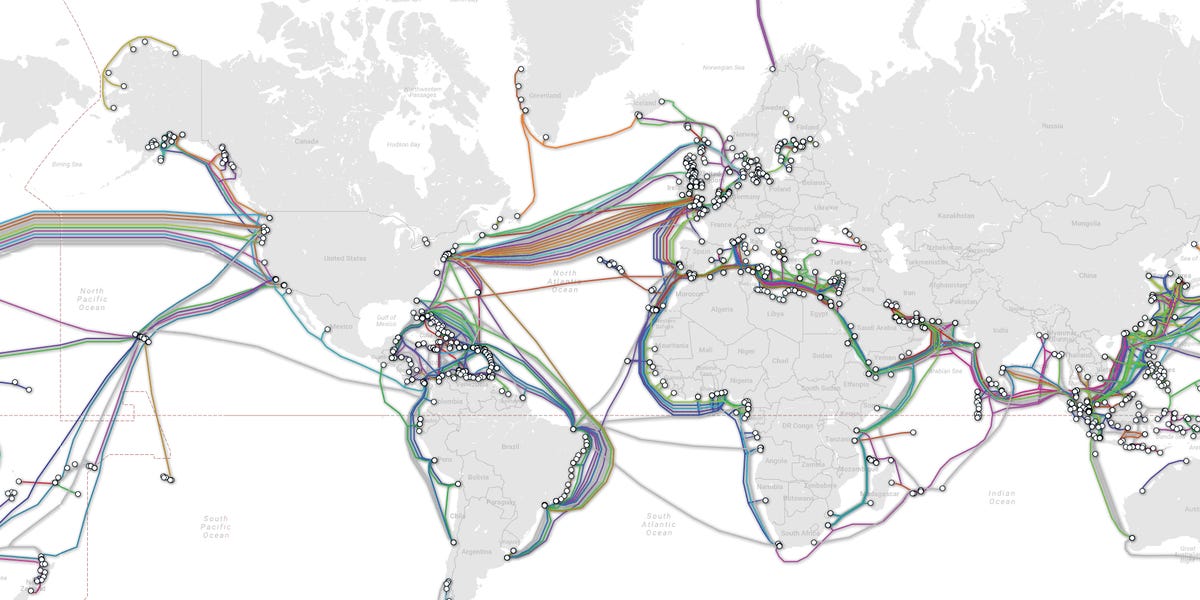
Popis byl vytvořen automaticky

Obrázek 11 – IP a MAC adresy po příchodu paketu na Laptop1

Obrázek 12 – Obsah paketu na switchi

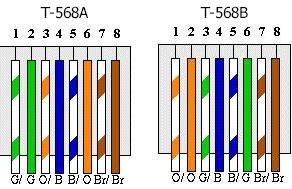
#### Servery

### Pasivní prvky

Pasivní síťové prvky jsou takové které v sítích pouze data přenášejí bez jakékoliv změny nebo úpravy. Většina těchto to prvků jsou kabely, koncovky, zásuvky nebo rozvaděče. V dnešní době bezdrátových přenosů mohou tyto prvky znít trochu zbytečně, přesto je přenos dat po kabelech na delší vzdálenosti nejefektivnější možností kterou známe. Abychom mohl komunikovat se zařízeními po celém světě tak jsou kontinenty propojen takzvanými Podmořskými kabely (anglicky Submarine communications cable).  
Po zemi jsou data přenášeny pozemními kabely. Alternativní přenosovou cestou jsou satelity, ty ale v současné době mají kapacitu pro pouze 1% přenosů.

Obrázek 13

#### undefined**Kroucená dvojlinka**

Kroucená dvojlinka (anglicky Twisted pair) je jedním ze základních kabelů používaných v počítačových sítích. Tvoří ho čtyři páry vodičů které jsou zakončeny konektorem RJ-45. Při připojování konektoru je důležité dbát na normu zapojení, ty jsou dvě T568A a T568B, v případě kdy by byla použita opačná norma na obou stranách tak by komunikace nefungovala. Kroucená dvojlinka se dělí podle počtu párů (25 párů – telekomunikace, 8 – ethernet), stínění kabelů (UTP – unshielded twisted pair, STP -  shielded twisted pair) nebo podle stínění párů (U/FTP – bez stínění, SF/FTP – oplétaný fólií a stíněný kabel). Verze TP kabelů se označují jak Cat, dnes standartě využívána verze 5e nebo vyšší jako 6, 6a, 7 nebo 8. Největším omezením u TP kabelů je nízká vzdálenost přenosu, u 5e je přenosová vzdálenost 100 metrů, u vyšších kategorií se pouze snižuje (Cat 8 přibližně 30 metrů).

#### Optické kabely

Optické kabely používají pro přenos dat světlo místo elektrického náboje. Optický kabel je složen z tenkého vlákna vyrobeného z čistého skla nebo plastu, které je schopné vést světlo. Vlákno je obaleno ochrannou vrstvou, která mu poskytuje mechanickou stabilitu a ochranu před vnějšími vlivy. Vnitřní jádro vlákna má vyšší index lomu než vnější obal, což umožňuje světlu, aby se v něm šířilo metodou totálního vnitřního odrazu. Zpoždění na 1000 km je přibližně 11 milisekund díky tomu že data v optických kabelech putují rychlostí světla. Kvůli odrazu světla uvnitř kabelu, se nedají moc ohýbat proto jsou více používané pro přenášení dat na dlouhé vzdálenosti.

# Praktická část práce

## Packet tracer

Packet tracer je software vyvinutý firmou Cisco Systems pro vizuální reprezentaci a simulaci počítačových sítí. Převážně je využívaný pro výuku a přípravu na CCNA (Cisco Certified Network Associate) zkoušky.

## Síť LAN

Obsah obrázku text, snímek obrazovky, Písmo, číslo

Popis byl vytvořen automatickySíť LAN (local area network) je malá počítačová síť, převážně domácí nebo firemní sítě. V této práci jsou použity dvě sítě, Dům 1 a Dům 2, které reprezentují domácí sítě. Pro správné fungování sítě, je nutné aby se všechny prvky v síti nakonfigurovaly. Toto nastavení může být provedeno buď manuálně, samy si na všech zařízeních nastavíme ip adresu, masku atd., nebo pomocí služby DHCP - Dynamic Host Configuration Protocol. Zařízení v  LAN síti nastavuje náš router (Wireless Router0 nebo 1). Obsah obrázku řada/pruh, diagram, snímek obrazovky, Vykreslený graf

Popis byl vytvořen automaticky

Obrázek 14 – dva rozsahy adres na DHCP serveru

Obrázek 15 – schéma dvou domácích sítí Dům 1 a Dům 2

Obsah obrázku text, diagram, snímek obrazovky, řada/pruh

Popis byl vytvořen automatickyObsah obrázku diagram, text, snímek obrazovky, mapa

Popis byl vytvořen automatickySamotný router, by mohl být nastaven manuálně providerem, nebo znova službou DHCP. To probíhá trochu složitěji. WR1 (náš domácí router) je připojen do switche, který se nachází někde v našem okolí (např. v paneláku). Ten je zase připojen do switche, který spojuje více paneláků dohromady. Na tomto switchi (Switch0) jsou vytvořeny dvě sítě VLAN. VLAN (Virtuální LAN) síť je speciální druh LAN sítě kde počítače od sebe nejsou odděleny routerem, ale pouze logicky na switchi. Tyto dvě VLANy nám tedy oddělí jednotlivé paneláky od sebe a každému může být nastavena jiná ip adresa, to nám pomůže se lépe vyznat v tom, kde se jednotlivé sítě nacházejí. Switch0 je dále připojen do multilayer switche, na kterém jsou znova vytvořeny dvě VLAN sítě, které musí odpovídat těm vytvořeným na Switch0. Zde je ale ještě nutné každé VLAN nastavit také adresy obou sítí. MLS totiž funguje podobně jako router, směruje pakety do správných portů, ale i z jiných sítí něž do kterých patří, narozdíl od normálního switche. Nakonec, samotné generování ip adres vzniká na DHCP serveru providera. Na tom jsou vytvořeny dva rozsahy pro obě sítě. Vlan10 pro Dům 1 a vlan20 pro Dům 2.

Obrázek 16 – schéma zapojení providera

Obrázek 17 – zapojení domácího routeru do „panelákového“ switche

### Nastavení ML switche

Obsah obrázku text, snímek obrazovky, Písmo, řada/pruh

Popis byl vytvořen automatickyObsah obrázku text, snímek obrazovky, Písmo, řada/pruh

Popis byl vytvořen automatickyObsah obrázku text, řada/pruh, Písmo, software

Popis byl vytvořen automatickyVětšina věcí se v packet traceru jde nastavit přes grafické rozhraní, to ale co je potřeba pro nastavení ML switche se zde nenachází, proto se využije možnosti nastavení přes příkazy. První dva příkazy, které se používají vždycky jsou en (zapnutí) a conf terminal (přístup do konfiguračního terminálu), teprve zde začíná samotné nastavování switche. Prvně na ML switchi vytvoříme dvě VLAN sítě příkazem vlan [id], v práci jsou použity id 10 a 20, zároveň si síť pojmenujeme příkazem name [nazev]. Int range f0/1-24 vybere všechny FastEthernet porty a příkazem switchport trunk encapsulation dot1q řekneme, že switch do framů (česky rámců) bude přidávat část identifikující VLAN, a příkaz switchport mode trunk přepne porty do módu trunk který dovoluje přenos mezi různými VLANy. Jelikož ML switch slouží částečně i jako router tak zapneme routování příkazem ip routing. Nyní nastavíme všechny VLAN sítě. Int vlan [id] nás dostane do rozhraní pro nastavení VLANu. Příkazem ip add [ip adresa] [maska] vlan přidáme do sítě do které chceme aby patřila. V práci nastavujeme tři VLAN sítě, 1, 10 a 20 s ip adresami 192.168.1.1, 192.168.10.1 a 192.168.20.1, všechny sítě mají masku s prefixem 24. Příkazem no sh zaručíme že VLAN bude zapnuta a posledním příkazem pro VLAN, ip helper-address 192.168.1.2 (adresa DHCP serveru), sítím nastavíme „pomocníka“ pro DHCP dotazy. Nakonec nastavíme RIP (Routing Information Protocol) protokol, který umožní routování mezi sítěmi. To buď jde graficky v záložce config, nebo příkazy router rip (přístup do rozhraní), network [ip adresa]. Aby nám ale vše fungovalo správně, tak na switchi, který je připojen do multilayer switche, jeden port nastavíme na trunk mód příkazem switchport mode trunk, tento port musí vést do MLS. Ostatní dva port, které vedou do každého „paneláku“ přepneme příkazem switchport access vlan [id] na přístup do té VLAN, kterou tam chceme mít.

Obrázek 18 – mód access s přístupem do VLAN 20 na portu GIG2/1

Obrázek 19 – mód trunk na portu GIG0/1

Obrázek 20 – mód access s přístupem do VLAN 10 na portu GIG1/1

## Síť WAN

Obsah obrázku diagram, mapa, Plán, řada/pruh

Popis byl vytvořen automatickySíť WAN (Wide area network) je celosvětová síť kterou nazýváme internetem. Naše lokální síť se většinou bude skládat z jednotek sítí, WAN se naopak skládá z tisíců. Tyto sítě jsou tvořeny z  routerů, switchů a serverů atd. Aby tyto prvky byly viditelné na našich počítačích je nutné aby měli veřejné ip adresy.

Obrázek 21 – schéma internetu

### Redundance

Velice důležtou částí internetu je, když jeden prvek, např. switch, vypadl tak aby internet nepřestal fungovat. Pro zajíštění téhle podmínky se využívá např. propojení prvků více než jednou cestou nebo tak zvanou redundancí, tj. propojení switchů více cestami. Redundatní propojení může být problematické kvůli vytvoření smyček. Smyčky jsou v sítích nebezpečné, jelikož kdyby k jednomu cíli existovalo více cest tak se pakety zacyklí a budou do nekonečna putovat po síti a zahlcovat ji. Toto řeší protokl STP (spanning tree protocol). Tento protokol u switchů zjistí nejrychlejší cestu a tu pomalejší uzavře a znova jí otevře pouze když dojde k znepřístupnění rychlejší cesty.

Obsah obrázku text, diagram, snímek obrazovky, řada/pruh

Popis byl vytvořen automatickyObsah obrázku text, diagram, snímek obrazovky, řada/pruh

Popis byl vytvořen automaticky

Obrázek 22 – STP na switchi: vypnutá pomalejší cesta

Obrázek 23 – STP na switchi: pomalejší cesta zapnuta

## Otestování funkčnosti internetu

Obsah obrázku text, snímek obrazovky, Písmo

Popis byl vytvořen automatickyJednou ze základních diagnostických pomůcek pro ověření funkčnosti internetu je příkaz ping. Ping nám umožní zjistit jestli náš počítač dokáže komunikovat s jiným počítačem, routerem nebo serverem. Příkaz využijeme otevřením příkazového řádku, napsáním ping [cíl]. Pro ukázku bude probíhat ping z PC1 na youtube.com. Když se ping vyšle z našeho počítače první zastávka je náš router. Zde je paket přeložen NATem, na routeru je do tabulky uložena ip adresa zdroje (počítače) a cíle (youtube.com). Adresa zdroje je nahrazena adresou routeru a paket pokračuje na další router. Tento proces pokračuje než se ping dostane do cíle, zde je ping potvrzen a vrací se zpátky na náš počítač.

Obrázek 24 – ping na youtube

## Obsah obrázku text, snímek obrazovky, software, Webová stránka Popis byl vytvořen automatickySlužby internetu

Obrázek 25 – webová stránka youtube – generováno ChatGPT

### Webové stránky

Webové stránky v internetu jsou tvořen textové jazyky HTML, CSS, JavaScript (případně PHP) a další. Dokumenty vytvořené těmi to jazyky jsou uloženy na webový serverech, odkud se posílají ke klientům (webovým prohlížečům). V práci můžete otevřít „webové stránky“ youtube.com, facebook.com, github.com a „darkweb“. První tři stránky jsou přístupné pod aliasem (například www.youtube.com). DarkWeb je přístupný pouze přes ipadresu (nefunguje DNS).

### E-mail

Abychom mohli posílat email musí někde v internetu existovat mail server. Tento server má za úkol předávat emaily od jednoho klienta k dalšímu (klientem rozumíme webovou aplikaci jako Gmail, Outlook a tak dále). Na mail serveru je přečtena „obálka“ našeho emailu obsahující naší a příjemcovu adresu. Ta je přeložena službou DNS na ip adresu. Mail Exchange zjistí cestu k příjemci a ze serveru email odejde ke klientovy.

#### Email v Packet traceru

Obsah obrázku text, snímek obrazovky, Písmo, číslo

Popis byl vytvořen automatickyNa mail serveru (název serveru gmail) nastavíme doménu na gmail.com a vytvoříme dva uživatele, uživatel (heslo 123) a uzivatel1 (heslo 11). Na obou počítačích v sekci desktop otevřeme záložku email a zde vyplníme informace o uživatelích a serveru. V praxi existují dva servery na přijímání a odesílání emailu, zde obě funkce vykonává ten samý server. Teď jestli chceme odeslat email tak klikneme na tlačítko „Compose“ vložíme adresu uzivatele1, napíšeme zprávu a na druhém počítači zmáčkneme „Receive“ a jestli vše proběhlo v pořádku tak se email zobrazí.

Obrázek 26 – emailové nastavení pro uzivatele

Obsah obrázku text, snímek obrazovky, řada/pruh, Písmo

Popis byl vytvořen automaticky

Obrázek 27 – odesílání emailu uzivateli

Obsah obrázku text, Písmo, snímek obrazovky, bílé

Popis byl vytvořen automaticky

Obrázek 28 – obdržený email

# Závěr

# Citace

What is a Public Network? ROUSE, Margaret. *Technopedia* [online]. 2023 [cit. 2024-01-23]. Dostupné z: <https://www.techopedia.com/definition/26424/public-network>

Internet. In: *Wikipedia: the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation, 2001- [cit. 2024-01-23]. Dostupné z: <https://en.wikipedia.org/wiki/Internet>

ARPANET. In: *Wikipedia: the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation, 2001- [cit. 2024-01-23]. Dostupné z: <https://en.wikipedia.org/wiki/ARPANET>

Internet protocol suite. In: *Wikipedia: the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation, 2001- [cit. 2024-01-23]. Dostupné z: <https://en.wikipedia.org/wiki/Internet_protocol_suite>

Creeper. In: *Wikipedia: the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation, 2001- [cit. 2024-01-23]. Dostupné z: <https://cs.wikipedia.org/wiki/Creeper>

Internet Engineering Task Force. In: *Wikipedia: the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation, 2001- [cit. 2024-01-23]. Dostupné z: <https://cs.wikipedia.org/wiki/Internet_Engineering_Task_Force>

ICANN. In: *Wikipedia: the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation, 2001- [cit. 2024-2024-01-24]. Dostupné z: <https://en.wikipedia.org/wiki/ICANN>

Internet Assigned Numbers Authority. In: *Wikipedia: the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation, 2001- [cit. 2024-01-24]. Dostupné z: <https://en.wikipedia.org/wiki/Internet_Assigned_Numbers_Authority>

Webové stránky YouTube, Facebook a GitHub generovány ChatGPT verze 3.5. Dostupné z: <https://chat.openai.com>

Packet Tracer. In: *Wikipedia: the free encyclopedia*[online]. San Francisco (CA): Wikimedia Foundation, 2001- [cit. 2024-03-30]. Dostupné z: <https://en.wikipedia.org/wiki/Packet_Tracer>

IEEE 802.1Q. In: *Wikipedia: the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation, 2001- [cit. 2024-03-30]. Dostupné z: <https://cs.wikipedia.org/wiki/IEEE_802.1Q>

IPv6. In: *Wikipedia: the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation, 2001- [cit. 2024-03-30]. Dostupné z: <https://en.wikipedia.org/wiki/IPv6>

What is a mail server?. In: *Cloudflare [*online]. [cit. 2024-02-21]. Dostupné z: <https://www.cloudflare.com/learning/email-security/what-is-a-mail-server/>

ICMP. In: *Wikipedia: the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation, 2001- [cit. 2024-04-01]. Dostupné z: <https://cs.wikipedia.org/wiki/ICMP>

NetworkChuck, 2020, What is a SWITCH? // FREE CCNA // Day 1, YouTube video [cit. 2024-04-02]. Dostupné z: <https://www.youtube.com/watch?v=9eH16Fxeb9o>

NetworkChuck, 2020, What is a ROUTER? // FREE CCNA // EP 2, YouTube video [cit. 2024-04-03]. Dostupné z: <https://www.youtube.com/watch?v=p9ScLm9S3B4>

ALEXANDR, Karel. Zlověstné ticho analytiků. Bezpečnost světa leží na dně oceánů, zapomeňte na raketový deštník. *Security magazín* [online]. 2023-11-29 [cit. 2024-04-04]. Dostupné: <https://www.securitymagazin.cz/security/zlovestne-ticho-analytiku-bezpecnost-sveta-lezi-na-dne-oceanu-zapomente-na-raketovy-destnik-1404071615.html>

Kroucená\_dvojlinka. In: *Wikipedia: the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation, 2001- [cit. 2024-04-04]. Dostupné z: <https://cs.wikipedia.org/wiki/Kroucená_dvojlinka>

Fiber-optic cable. In: *Wikipedia: the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation, 2001- [cit. 2024-04-05]. Dostupné z: v <https://en.wikipedia.org/wiki/Fiber-optic_cable>

# Seznam obrázků

[Obrázek 1 – Síť ARPANET v březnu 1972 9](#_Toc163146119)

[Obrázek 2 – Porovnání TCP/IP s OSI/ISO modelem 10](#_Toc163146120)

[Obrázek 3 – tabulka prefixů s počtem ip adres 10](#_Toc163146121)

[Obrázek 4 – Obsah paketu po NATu na routeru 13](#_Toc163146122)

[Obrázek 5 – IP a MAC adresy při komunikaci se zařízením mimo síť 13](#_Toc163146123)

[Obrázek 6 – IP a MAC adresy při komunikaci se zařízením v síti 13](#_Toc163146124)

[Obrázek 7 – část paketu s cílovou a zdrojovou MAC adresou 14](#_Toc163146125)

[Obrázek 8 – část paketu s cílovou a zdrojovou IP adresou 14](#_Toc163146126)

[Obrázek 9 – výpis z CAM tabulky 14](#_Toc163146127)

[Obrázek 10 – IP a MAC adresy v paketu na Laptop3 14](#_Toc163146128)

[Obrázek 12 – IP a MAC adresy po příchodu paketu na Laptop1 14](#_Toc163146129)

[Obrázek 11 – Obsah paketu na switchi 14](#_Toc163146130)

[Obrázek 13 15](#_Toc163146131)

[Obrázek 14 – dva rozsahy adres na DHCP serveru 16](#_Toc163146132)

[Obrázek 15 – schéma dvou domácích sítí Dům 1 a Dům 2 16](#_Toc163146133)

[Obrázek 16 – schéma zapojení providera 16](#_Toc163146134)

[Obrázek 17 – zapojení domácího routeru do „panelákového“ switche 16](#_Toc163146135)

[Obrázek 18 - mód access s přístupem do VLAN 20 na portu GIG2/1 17](#_Toc163146136)

[Obrázek 19 - mód trunk na portu GIG0/1 17](#_Toc163146137)

[Obrázek 20 – mód access s přístupem do VLAN 10 na portu GIG1/1 17](#_Toc163146138)

[Obrázek 21 – schéma internetu 17](#_Toc163146139)

[Obrázek 22 – STP na switchi: vypnutá pomalejší cesta 18](#_Toc163146140)

[Obrázek 23 – STP na switchi: pomalejší cesta zapnuta 18](#_Toc163146141)

[Obrázek 24 – ping na youtube 18](#_Toc163146142)

[Obrázek 25 – webová stránka youtube – generováno ChatGPT 18](#_Toc163146143)

[Obrázek 26 – emailové nastavení pro uzivatele 19](#_Toc163146144)

[Obrázek 27 – odesílání emailu uzivately 19](#_Toc163146145)

[Obrázek 28 – obdržený email 19](#_Toc163146146)

# Přílohy

Příloha 1: Pomocný soubor pro vysvětlení fungování switche

1. Google IPv6 adoption <https://www.google.com/intl/en/ipv6/statistics.html> [cit. 2024-04-03] [↑](#footnote-ref-2)
2. Fungování switche vysvětleno použitím pomocného sítě (příloha 1) [↑](#footnote-ref-3)