**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. 4. 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

V tomto oddílu bych chtěl poděkovat hlavně panu Mgr. Milanu Haraštovy za umožnění a pomoc při vytváření maturitní práce.

Anotace

Cílem této maturitní práce je vytvořit schéma internetu v Packet traceru. Dále se práce věnuje základním pojmům v počítačových sítích a vysvětlení funkčnosti vytvořeného internetu.

Klíčová slova

Počítačová síť, router, switch, internet

Annotation

The goal of this work is to create schematic of internet in Packet tracer. Furthermore, the thesis deals with the basic terms in computer networks and the explanation of the functionality of the created internet.

Key word

Computer network, router, switch, internet,

Obsah

[1 Úvod 9](#_Toc164356863)

[2 Teoretická část práce 10](#_Toc164356864)

[2.1 Obecné informace o internetu 10](#_Toc164356865)

[2.1.1 Historie 10](#_Toc164356866)

[2.1.2 Kdo vlastní internet 10](#_Toc164356867)

[2.1.3 Klient/server model 11](#_Toc164356868)

[2.1.4 Referenční modely 11](#_Toc164356869)

[2.1.5 Služby internetu 11](#_Toc164356870)

[2.2 TCP/IP 11](#_Toc164356871)

[2.2.1 IPv4 12](#_Toc164356872)

[2.2.2 IPv6 13](#_Toc164356873)

[2.2.3 Další protokoly 13](#_Toc164356874)

[2.3 Síťové prvky 14](#_Toc164356875)

[2.3.1 Aktivní prvky 14](#_Toc164356876)

[2.3.2 Pasivní prvky 16](#_Toc164356877)

[3 Praktická část práce 18](#_Toc164356878)

[3.1 Packet tracer 18](#_Toc164356879)

[3.2 Síť LAN 18](#_Toc164356880)

[3.2.1 Nastavení ML switche 19](#_Toc164356881)

[3.3 Síť WAN 20](#_Toc164356882)

[3.3.1 Redundance 21](#_Toc164356883)

[3.4 Otestování funkčnosti internetu 21](#_Toc164356884)

[3.5 Služby internetu 22](#_Toc164356885)

[3.5.1 Webové stránky 22](#_Toc164356886)

[3.5.2 E-mail 24](#_Toc164356887)

[3.5.3 Ukládání souborů 24](#_Toc164356888)

[4 Závěr 26](#_Toc164356889)

[5 Použitá literatura 27](#_Toc164356890)

[6 Seznam obrázků 30](#_Toc164356891)

[7 Přílohy 32](#_Toc164356892)

Použité zkratky

ARPANET – Advanced Research Projects Agency NETwork

WWW – World wide web

HTTP – Hypertext Transfer Protocol

HTTPS – Hypertext Transfer Protocol Secure

HTML – Hypertext Markup Language

CERN - Conseil Européen pour la recherche nucléaire

CIX – Commercial Internet eXchange

IETF – Internet Engineering Task Force

IANA – Internet Assigned Numbers Authority

ICANN – Internet Corporation for Assigned Names and Numbers

RIR – Regional Internet registries

AFRINIC – African Network Information Center

ARIN – American Registry for Internet Numbers

APNIC – Asia-Pacific Network Information Centre

LACNIC – Latin American and Caribbean Internet Addresses Registry

RIPE NCC – Réseaux IP Européens – Network Coordination Centre

W3C – World Wide Web Consortium

OSI/ISO – International Organization for Standardization/Open Systems Interconnection

TCP – Transmission Control Protocol

IP – Internet Protocol

IPv4 – Internet Protocol version 4

NAT – Network address translation

DNS – Domain Name System

DHCP – Dynamic Host Configuration Protocol

ARP – Address Resolution Protocol

RARP – Reverse address Resolution Protocol

ICMP – Internet Control Message Protocol)

UDP – User Datagram Protocol

SSH – Secure Shell

MAC – Medium access control

PID – Process identifier

CAM – Content Addressable Memory

TP – Twisted pair

UTP – Unshielded twisted pair

STP – Shielded twisted pair

U/FTP – Unshielded, foil shielding twisted pair

SF/FTP Braided shielding, foil shielding twisted pair

CAT – Category

CCNA – Cisco Certified Network Associate

LAN – Local area network

WAN – Wide area network

VLAN – Virtual local area network

MLS – Multilayer switch

FTP – File transfer protocol

STP – Spanning Tree Protocol

CSS – Cascading Style Sheets

PHP – Hypertext Preprocessor

TLS – Transport Layer Security

SYN – Synchronization

FIN – Finish

ACK – Acknowledgement

SMTP – Simple mail transfer protocol

POP3 – Post Office Protocol version 3

# Úvod

Tématem maturitní práce je návrh struktury internetu v Packet traceru. Práce je rozdělená na dvě části, praktickou a teoretickou.

Teoretická část se věnuje stručné historii internetu, organizacím, které internet spravují, vymýšlejí  
a kontrolují protokoly pro komunikace na internetu. Dále se věnuje vysvětlení základních internetových protokolů v sadě TCP/IP jako jsou IPv4 a IPv6, TCP a UDP nebo ARP. Poslední část teoretické části se věnuje síťovým prvkům, jak aktivním tak pasivním. Je zde vysvětleno jak fungují routery a switche nebo kabely používané v počítačových sítích.

Praktická část se věnuje představení struktury internetu, kterou jsem navrhl. V této části je vysvětleno nastavení některých prvků, zapojení domácí nebo WAN sítě. Ukázání a vysvětlení komunikace některých internetových služeb jako jsou email, world wide web a používání FTP protokolu pro ukládání souborů.

# 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 „sít 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 a dalších.

### 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 (neměl 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 Barbaře a Utažské univerzitě. Později byly přidány další uzly po celý Spojených státech (40 v roce 1973).

Obsah obrázku skica, text, kresba, diagram

Popis byl vytvořen automaticky

Obrázek 1 – Síť ARPANET v březnu 1972 (Zdroj: Svět hardware)

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 vzájemnou komunikaci.

### Kdo vlastní internet

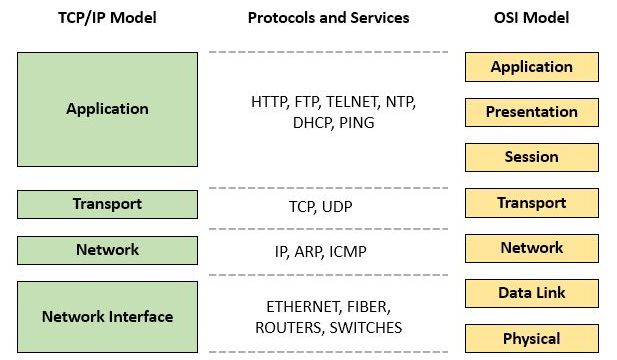
Internet je decentralizovaná síť, která není nikým vlastněna. Je to síť sítí, která propojuje nezávislé komerční, sítě dohromady. Přesto musejí existovat organizace, které budou tuto síť spravovat a vytvářet standardy protokolů. O protokoly se stará nezisková organizace Internet Engineering Task Force (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 kořenových DNS serverů. O samotné přidělování adres se starají Regionální Internetové Registry (RIR), které 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 model kde server slouží jako poskytovatel služby klientovy (webový server, emailový server, atd.), 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 slouží jako 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). 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 (Zdroj: Sabhi 2023)

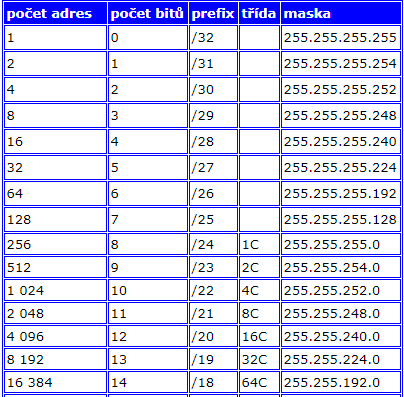
### Služby internetu

## TCP/IP

Aby počítače spolu mohli komunikovat, tak stejně jako lidi, musí „mluvit“ stejným jazykem. Pro počítače tento jazyk je definovaný v protokolech. Dnes nejpoužívanější 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 síti 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 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 prava) byte je pro zařízení, 192.168.1.1/23 – 23 -> 255.255.254.0 – první a druhý byte je pro zařízení. Masky taky označují počet subnetů. Prefix 24 má jeden subnet, 25 má 2 subnety, 26 čtyři atd, až do prefixu 32 (pouze jedna volná IP adresa). 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).



Obrázek 3 – tabulka prefixů s počtem IP adres (Zdroj: Maturita Formalita)

#### Privátní IP adresy

Privátní IP adresy jsou takové které nejsou přímo přístupné z internetu. 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 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. Rozsah adres u IPv6 je 2128 (přibližně 3,4 \* 1038). Hlavička je navržena jednodušeji než u IPv4, což umožňuje rychlejší a efektivnější komunikaci v síti. Dále 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 (název paketu ve třetí vrstvě) šifruje. Zápis IPv6 adres je rozdílný od IPv4, místo čtyř desítkových čísel od 0 do 255 používá IPv6 používá osm skupin čtyř hexadecimálních čísel, příklad IPv6 adresy je 2001:0db8:2231:aaec:0000:0000:4a4a:2100. Kvůli dlouhému zápisu existují pravidla pro zkrácení zápisu. Například minimálně dvě po sobě jdoucí části nul jsou nahrazeny „::“ (zápis 2001:0db8:2231:aaec::4a4a:2100), tento zápis ale nemůže být použit vícekrát na různých místech v adrese, takže v případě, že by adresa měla více míst, kde by se toto pravidlo dalo využít, je použito pro větší počet nul, a v případě, že by to byly dvě dvojice nul, tak je použito pro první z leva. Dalším pravidlem je, že když má část adresy nuly před posledním číslem, například :0001:, tak se nuly nepíšou (zápis :1:). Stejně jako předchůdce i IPv6 má část pro identifikaci sítě a zařízení, v tomto případě jsou ale zapisovány pouze prefixem, který označuje počet bitů pro síť. U adresy 2001:0db8:2231:aaec::4a4a:2100 s prefixem 64, by pro označení sítě platila část 2001:0db8:2231:aaec, zbylá část je pro identifikaci počítače. 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 protokol 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) k switchi nebo routeru (MAC adresa FFFF.FFFF.FFFF), zařízení „odpoví“ jestli se IP adresa v dotazu shoduje s adresou zařízení, adresou kterou má uloženou v paměti nebo vytvoří vlastní dotaz pro další zařízení která jsou k němu připojena.

#### ICMP

Internet Control Message Protocol slouží v operačních systémech k přenosu služebních informací (např. chybová hlášení, požadovaná služba není dostupná nebo potřebný počítač není dostupný). V sítích je využíván například v diagnostické službě ping, která posílá zprávy Echo Request a očekává Echo Reply.

#### 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 [bytů](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

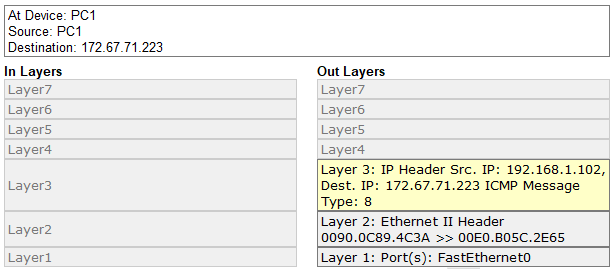
Routery jsou zařízení která pracují na třetí (síťové) vrstvě OSI/ISO modelu. Routery dokážou spojit dvě, nebo více, sítí dohromady. Na rozdíl od switchů, které pracují s MAC adresou, routery pracují i s IP adresou. Když chceme komunikovat se zařízením, počítač sám zjistí, jestli zařízení je součástí sítě nebo ne. Když je zařízení součástí sítě tak jako cílovou IP adresu a MAC adresu označí to zařízení se kterým chce komunikovat.

Obsah obrázku text, snímek obrazovky, číslo, Písmo

Popis byl vytvořen automaticky

Obrázek 4 – IP a MAC adresy při komunikaci se zařízením v síti

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.



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

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). 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 (název Lokální switch). Jak paket dále putuje 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. Další identifikátor, který routery používají se nazývá process identifier. PID je unikátní číslo které routery udělují procesům, které zpracovávají, vědí potom, co k čemu patří. PID také využívají operační systémy pro zjištění toho, který paket patří k jaké službě.

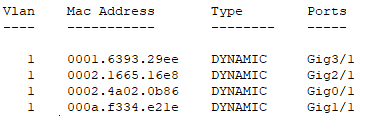
Obsah obrázku text, snímek obrazovky, Písmo, číslo

Popis byl vytvořen automaticky

Obrázek 6 – Obsah paketu po NATu na routeru

#### Switch

Switche 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 uzlu a port ke kterému je připojen.



Obrázek 7 – výpis z CAM tabulky

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, který má prohozené MAC a IP adresy. Proces se poté opakuje do konce přenosu.[[2]](#footnote-3)

|  |  |
| --- | --- |
| Obsah obrázku text, snímek obrazovky, Písmo, řada/pruh  Popis byl vytvořen automaticky  Obrázek 8 – část paketu s cílovou a zdrojovou MAC adresou | Obsah obrázku text, snímek obrazovky, Písmo, řada/pruh  Popis byl vytvořen automaticky  Obrázek 9 – část paketu s cílovou a zdrojovou IP adresou |

Obsah 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 – Obsah paketu na switchi

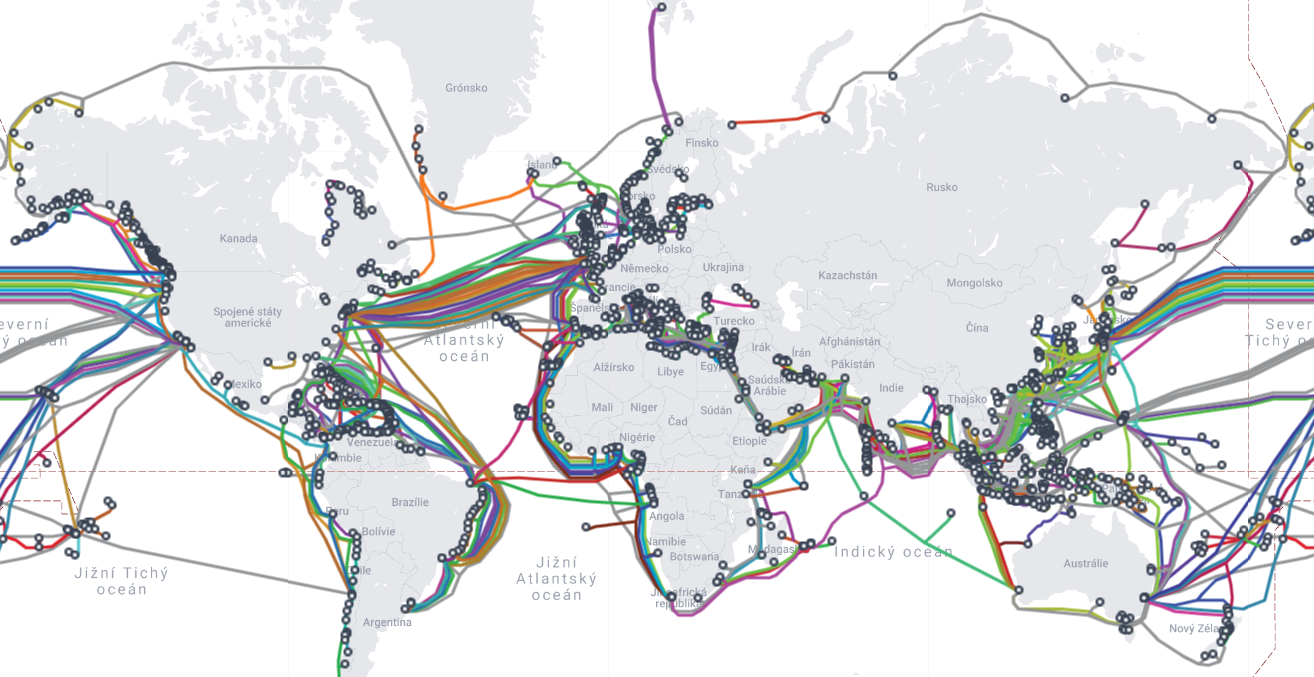
Obsah obrázku text, snímek obrazovky, Písmo, číslo

Popis byl vytvořen automaticky

Obrázek 12 – IP a MAC adresy po příchodu paketu na Laptop1

### 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.[[3]](#footnote-4)



Obrázek 13 – mapa podmořský kabelů (Zdroj: TeleGeography)

#### **Kroucená dvojlinka**

|  |  |
| --- | --- |
| undefined  Obrázek 14 – vodiče uvnitř kabelu (Zdroj: Wikipedie) | T568A and T568B Wiring Standards| Comms InfoZone  Obrázek 15 – normy pro TP (Zdroj: Comms express) |

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 párů – ethernet), podle stínění kabelů (UTP – nestíněná dvojlinka, STP -  stíněná dvojlinka) 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

Síť LAN (local area network) je malá počítačová síť, převážně pro 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 16 – schéma dvou domácích sítí Dům 1 a Dům 2

Samotný router, by mohl být nastaven manuálně providerem, nebo znova službou DHCP. To probíhá trochu složitěji. WR1 je připojen do switche, který se nachází někde v našem okolí (např. v paneláku). Ten je zase připojen do switche, který spojuje například město dohromady. Na tomto switchi (Městský switch) 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.

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

Popis byl vytvořen automaticky

Obrázek 17 – zapojení domácího routeru do lokálního switche

„Městský switch“ je dále připojen do multilayer switche, na kterém jsou znova vytvořeny dvě VLAN sítě. 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.

|  |  |
| --- | --- |
| Obsah obrázku text, diagram, snímek obrazovky, řada/pruh  Popis byl vytvořen automaticky  Obrázek 18 – schéma zapojení providera | Obsah obrázku text, snímek obrazovky, Písmo, číslo  Popis byl vytvořen automaticky  Obrázek 19 – dva rozsahy adres na DHCP serveru |

### Nastavení ML switche

Většina věcí v Packet traceru jde nastavit přes grafické rozhraní, to ale co je potřeba pro nastavení ML switche se zde nenachází, proto využijeme 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 sítě 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 jsou nastaveny následující 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 protokol (Routing Information Protocol), 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 Lokálních switchů přepneme příkazem switchport access vlan [id] na přístup do té VLAN, kterou tam chceme mít.[[4]](#footnote-5)

|  |  |
| --- | --- |
| Obsah obrázku text, řada/pruh, Písmo, software  Popis byl vytvořen automaticky  Obrázek 20 – mód access s přístupem do VLAN 10 na portu GIG1/1 | Obsah obrázku text, snímek obrazovky, Písmo, řada/pruh  Popis byl vytvořen automaticky  Obrázek 21 – mód access s přístupem do VLAN 20 na portu GIG2/1 |

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

Popis byl vytvořen automaticky

Obrázek 22 – mód trunk na portu GIG0/1

## Síť WAN

Obsah obrázku diagram, mapa, text

Popis byl vytvořen automaticky

Obrázek 23 – schéma internetu

Síť WAN (Wide area network) je síť která pokrývá území například několika států, největší takovouto sítí 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, serverů atd. Aby tyto prvky byly viditelné na našich počítačích je nutné aby měli veřejné IP adresy. Na obrázku víše je vidět schéma internetu, které bylo navrženo pro tuto práci. Nachází se zde 20 sítí které jsou navzájem propojené. Posledním článkem jsou servery poskytující služby jako DNS, webové stránky, FTP, email. Dále se zde nachází redundantně propojené switche, a routery které jednotlivé sítě oddělují.

### Redundance

Velice důležtou částí internetu je, když jeden prvek, např. switch, vypadne tak aby internet nepřestal fungovat. Pro zajištění téhle podmínky se využívá např. propojení prvků více než jednou cestou, tak zvanou redundancí. 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 protokol 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 automaticky  Obrázek 24 – STP na switchi: pomalejší cesta vypnuta | Obsah obrázku text, diagram, snímek obrazovky, řada/pruh  Popis byl vytvořen automaticky  Obrázek 25 – STP na switchi: pomalejší cesta zapnuta |

## Otestování funkčnosti internetu

Jednou 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 paket dostane do cíle, zde je potvrzen a vrací se zpátky na náš počítač.

Obsah obrázku text, snímek obrazovky, Písmo

Popis byl vytvořen automaticky

Obrázek 26 – ping na youtube

## Služby internetu

### Webové stránky

Webové stránky v internetu jsou tvořeny textovými 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 IP adresu (nefunguje DNS).

Obsah obrázku text, snímek obrazovky, software, Webová stránka

Popis byl vytvořen automaticky

Obrázek 27 – webová stránka youtube – generováno ChatGPT

#### HTTPS

HTTPS (Hypertext Transfer Protocol Secure) je protokol využívaný pro komunikaci webového klienta (prohlížeče) s webovým serverem. HTTPS se skládá ze svého předchůdce protokolu HTTP a protokolu TLS (transport layer security) pro zabezpečení. Pro komunikaci využívá port 443. Pokud použijeme doménu serveru (např. www.facebook.com) počítač nejdříve pošle DNS požadavek který jde na DNS server. Ve skutečnosti se využívá několika serverů. První se nachází hned v počítači kde jsou uložené stránky které jsme už navštívili. Když požadovanou stránku počítač nezná je požadavek poslán dál tak zvanému Rekurzivnímu resolveru, pokud nezná doménu tak pošle dotaz na kořenový (root) server. Ten nám sice neodpoví s IP adresu stránky, ale má záznamy o doménách nejvyšší úrovně (anglicky top level domain - .com, .cz a tak dále). TLD server odpoví s IP adresou autoritativního serveru na kterém jsou záznamy domén a IP adres. Resolver vytvoří požadavek který pošle na autoritativní server. Jestli se doména nachází v jeho záznamech tak odpoví IP adresou. Tu resolver pošle zpátky klientovy. V práci je tento proces velice zjednodušen a je vytvořen pouze autoritativní server který má v sobě záznamy o doménách.

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

Popis byl vytvořen automaticky

Obrázek 28 – DNS požadavek

Obsah obrázku text, snímek obrazovky, Písmo, číslo

Popis byl vytvořen automaticky

Obrázek 29 – DNS odpověď

Obsah obrázku text, snímek obrazovky, Písmo, číslo

Popis byl vytvořen automaticky

Obrázek 30 – záznamy na DNS serveru

Po tom, co se DNS paket vrátí zpátky na počítač je vytvořen TCP paket pro navázání komunikace se serverem. Prvně počítač pošle TCP paket s příznakem SYN, server odpoví nastavením příznaku SYN a ACK, nakonec počítač serveru oznámí že vše funguje správně nastavením příznaku ACK. Po úspěšném navázání komunikace je na počítači vytvořen HTTPS paket s HTTPS požadavkem. Jakmile požadavek přijde server začne generovat a posílat HTTPS odpovědi obsahující webovou stránku. Teprve po tom co všechny pakety dorazí na počítač bude stránka zobrazena v klientovy. Po obdržení veškerých data ze serveru, počítač pošle TCP paket s příznakem ACK a FIN tím serveru oznamuje že chce ukončit komunikaci. Server odpoví také ACK a FIN, a nakonec počítač znova potvrdí příznakem ACK.

|  |  |  |
| --- | --- | --- |
| Obrázek 31 – příznak SYN | Obrázek 32 – příznak ACK a SYN | Obrázek 33 – příznak ACK |
| Obrázek 34 – příznak ACK a FIN | | |

Tento proces se může zdát jako zdlouhavý ale není tomu tak, stránky se zobrazí přibližně za 120 milisekund a komunikace se ukončí za 180 milisekund, v případě že by počítač se serverem ještě nekomunikoval, a bylo by nutné vysílat ARP požadavky, tak se celá komunikace prodlouží přibližně o jednu sekundu.

### E-mail

Abychom mohli posílat email musí někde v internetu existovat server který bude naše požadavky zpracovávat. Tento server, nazývaný mail 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

Na 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. Jestli chceme odeslat email tak klikneme na tlačítko „Compose“ vložíme adresu uzivatele1, napíšeme zprávu a na druhém počítači zmáčkneme „Receive“ jestli vše proběhlo v pořádku tak se email zobrazí.

|  |  |
| --- | --- |
| Obsah obrázku text, snímek obrazovky, řada/pruh, Písmo  Popis byl vytvořen automaticky  Obrázek 35 – odesílání emailu uživateli | Obsah obrázku text, Písmo, snímek obrazovky, bílé  Popis byl vytvořen automaticky  Obrázek 36 – obdržený email |

#### Emailová komunikace

Když napíšeme email a zmáčkneme tlačítko „send“ tak je mezi naším počítačem a emailovým serverem vytvořeno TCP spojení a potom protokolem SMTP počítač na server posílá email. Simple Mail Transfer Protocol slouží pro přenos emailů mezi klientem a serverem. Při příjmu emailu je znova vytvořeno TCP spojení a klient využije protokol POP3. Post Office Protocol version 3 slouží pro příjem („stažení“) emailů ze serveru klientem.

### Ukládání souborů

|  |  |
| --- | --- |
| Obsah obrázku text, snímek obrazovky, Písmo  Popis byl vytvořen automaticky  Obrázek 37 – vložení souboru test\_FTP.txt na FTP server z PC1 | Obsah obrázku text, snímek obrazovky, Písmo  Popis byl vytvořen automaticky  Obrázek 38 – stažení souboru test\_FTP.txt na PC2 |

Pro vzdálené ukládaní souborů v Packet traceru je využit protokol FTP (File transfer protocol). Soubory ukládáme na sever, který je v práci pojmenován jako GitHub. Uložení souborů probíhá poměrně snadno. Na počítači otevřeme v záložce Desktop textový editor (text editor) do kterého napíšeme text a klávesovou zkratkou ctrl s ho uložíme. Dále otevřeme příkazový řádek kam napíšeme příkaz ftp github.com, následuje uživatelské jméno uzivatel a heslo 123. Nyní jsme přihlášení do FTP serveru příkazem put [nazev\_souboru.txt] na něj námi vytvořený soubor uložíme, že se soubor uložil můžeme ověřit tak že se do serveru podíváme. Když chceme soubor ze serveru stáhnout použijeme příkaz get [název\_souboru].

Obsah obrázku text, snímek obrazovky, software, číslo

Popis byl vytvořen automaticky

Obrázek 39 – uložený soubor test\_FTP.txt na PC2

#### Komunikace se serverem

Na FTP server se můžeme připojit jak pomocí doménového jména (github.com) nebo pomocí ip adresy. Když použijme doménu tak počítač nejdříve na DNS serveru zjistí IP adresu a poté naváže stejným postupem jako u HTTPS TCP spojení se serverem. Po založení TCP spojení server posílá první FTP paket s požadavkem na zadání uživatelského jména. Zadáním jména počítač posílá na server paket s uživatelským jménem, to je na serveru ověřeno, pokud jméno neodpovídá komunikace je ukončena, pokud je správně server posílá paket s požadavkem o heslo. Jestli zadáme i heslo správně tak server odpovídá zprávou „Logged in“.

|  |  |
| --- | --- |
| Obsah obrázku text, snímek obrazovky, řada/pruh, Písmo  Popis byl vytvořen automaticky  Obrázek 40 – FTP paket s uživatelským jménem | Obsah obrázku text, snímek obrazovky, řada/pruh, Písmo  Popis byl vytvořen automaticky  Obrázek 41 – FPT paket s heslem |

Při přenosu souborů počítač prvně serveru oznámí jaký typ souboru posílá (v tomto případě binární). Server potvrdí a klient oznámí serveru ať se přepne do pasivního módu. V pasivním módu si klient sám určí port ze kterého bude komunikovat, v aktivním se server připojí k náhodnému klientskému portu. Následuje uložení dat na server, FTP příkazem STOR oznámí klient, že chce ukládat soubor. Server odpoví, že je připraven na přesun souborů a je vytvořené TCP spojení a následně přenesení dat na FTP server. Po přenesení všech dat server oznamuje, že je přenos u konce a žádá o ukončení TCP spojení.

|  |  |
| --- | --- |
| Obsah obrázku text, snímek obrazovky, řada/pruh, Písmo  Popis byl vytvořen automaticky  Obrázek 42 – FTP paket s typem souboru | Obsah obrázku text, snímek obrazovky, řada/pruh, Písmo  Popis byl vytvořen automaticky  Obrázek 43 – FTP paket s příkazem STOR |

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

Popis byl vytvořen automaticky

Obrázek 44 – oznámení konce přenosu

# Závěr

Cílem práce bylo vytvořit schéma internetu a tohoto cíle se mi podařilo dosáhnout. O tom jak zapojení internetu vypadá můžeme jenom spekulovat, ale o moc rozdílné to pravděpodobně nebude. Během práce jsem se naučil lépe nastavovat switche pomocí příkazů což se velice hodí. Kromě nastavování jsem se ale také zlepšil v teorii sítí, lépe jsem porozuměl pojmům a dozvěděl jsem se co je v sítích dobré znát. Pokračováním práce by mohlo být rozšíření vytvořený internet o další funkce, ty jsou ale limitované tím co nám Packet tracer dovolí vytvořit.

# Použitá literatura

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, GitHub a Dark Web 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>

Router. In: *Wikipedia: the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation, 2001- [cit. 2024-04-02]. Dostupné z: <https://cs.wikipedia.org/wiki/Router>

Network address translation. In: *Wikipedia: the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation, 2001- [cit. 2024-04-03]. Dostupné z: <https://cs.wikipedia.org/wiki/Network_address_translation>

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>

Podmořský kabel. In: *Wikipedia: the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation, 2001- [cit. 2024-04-05]. Dostupné z: <https://cs.wikipedia.org/wiki/Podmořský_kabel>

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

ISO/IEC 11801. In: *Wikipedia: the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation, 2001- [cit. 2024-04-05]. Dostupné z: <https://en.wikipedia.org/wiki/ISO/IEC_11801>

ISO/IEC 11801. In: *Wikipedia: the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation, 2001- [cit. 2024-04-05]. Dostupné z: <https://cs.wikipedia.org/wiki/HTTPS>

Domain Name System. In: *Wikipedia: the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation, 2001- [cit. 2024-04-05]. Dostupné z: <https://cs.wikipedia.org/wiki/Domain_Name_System>

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

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. 2024-04-05]. Dostupné z: <https://cs.wikipedia.org/wiki/Kroucená_dvojlinka>

Tabulka ip adres a mask. Maturita Formalita  [online]. [cit. 2024-02-05]. Dostupné z: <http://maturitaformalita.4fan.cz/7-adresovani-v-tcp-ip-sitich-tridy-a-zapis-ip-adres-masky-koncepce-dalsiho-rozvoje/>

Mapa podmořských kabelů. TeleGeography  [online]. [cit. 2024-03-28]. Dostupné z: <https://www.submarinecablemap.com>

Justin Ellis , T568A-and-T568B-wiring-spec-standards. In: *comms express* [online- [cit. 2024-04-04]. Dostupné z: <https://www.comms-express.com/infozone/article/t568a-and-t568b/>

Yassine Sabhi, In: *Linkedin* [online]. [cit. 2024-04-04]. Dostupné z: <https://www.linkedin.com/posts/yassine-sabhi-5b2953206_the-osi-model-is-compared-to-the-tcpip-model-activity-7105472135212474369-cvlh>

Jan Vítek, 2019, Stav ARPANETu v březnu 1972. In: Svět hardware [online]. [cit. 2024-01-23]. Dostupné z: <https://www.svethardware.cz/pred-50-lety-byla-zaslana-prvni-zprava-pres-arpanet-pouze-dva-znaky/50519>

VILLANUEVA, John Carl. Active vs. Passive FTP Simplified. *JSCAPE* [online]. 2024 [cit. 2024-04-13]. Dostupné z: <https://www.jscape.com/blog/active-v-s-passive-ftp-simplified>

Baran Ivo, Kabel tvořený čtyřmi páry nestíněné kroucené dvojlinky. 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>

Fireship, 2021, DNS Explained in 100 Seconds, YouTube video [cit. 2024-04-12]. Dostupné z: <https://www.youtube.com/watch?v=UVR9lhUGAyU>

ARP and CAM Table. *GrayCampus* [online]. [cit. 2024-04-12]. Dostupné z: <https://www.greycampus.com/opencampus/ethical-hacking/arp-and-cam-cable>

Benefits of IPv6. *Catchpoint* [online]. [cit. 2024-04-03]. Dostupné z: <https://www.catchpoint.com/benefits-of-ipv6>

Google IPv6. *Google* [online]. [cit. 2024-04-03]. Dostupné z: <https://www.google.com/intl/en/ipv6/statistics.html>

IPv6 Subnetting Explained. *SubnettingPractice* [online]. [cit. 2024-04-18]. Dostupné z: <https://subnettingpractice.com/how-to-subnet-ipv6.html>

# Seznam obrázků

[Obrázek 1 – Síť ARPANET v březnu 1972 (Zdroj: Svět hardware) 10](#_Toc164356819)

[Obrázek 2 – Porovnání TCP/IP s OSI/ISO modelem (Zdroj: Sabhi 2023) 11](#_Toc164356820)

[Obrázek 3 – tabulka prefixů s počtem IP adres (Zdroj: Maturita Formalita) 12](#_Toc164356821)

[Obrázek 4 – IP a MAC adresy při komunikaci se zařízením v síti 14](#_Toc164356822)

[Obrázek 5 – IP a MAC adresy při komunikaci se zařízením mimo síť 14](#_Toc164356823)

[Obrázek 6 – Obsah paketu po NATu na routeru 15](#_Toc164356824)

[Obrázek 7 – výpis z CAM tabulky 15](#_Toc164356825)

[Obrázek 8 – část paketu s cílovou a zdrojovou MAC adresou 16](#_Toc164356826)

[Obrázek 9 – část paketu s cílovou a zdrojovou IP adresou 16](#_Toc164356827)

[Obrázek 10 – IP a MAC adresy v paketu na Laptop3 16](#_Toc164356828)

[Obrázek 11 – Obsah paketu na switchi 16](#_Toc164356829)

[Obrázek 12 – IP a MAC adresy po příchodu paketu na Laptop1 16](#_Toc164356830)

[Obrázek 13 – mapa podmořský kabelů (Zdroj: TeleGeography) 17](#_Toc164356831)

[Obrázek 14 – vodiče uvnitř kabelu (Zdroj: Wikipedie) 17](#_Toc164356832)

[Obrázek 15 – normy pro TP (Zdroj: Comms express) 17](#_Toc164356833)

[Obrázek 16 – schéma dvou domácích sítí Dům 1 a Dům 2 18](#_Toc164356834)

[Obrázek 17 – zapojení domácího routeru do lokálního switche 18](#_Toc164356835)

[Obrázek 18 – schéma zapojení providera 19](#_Toc164356836)

[Obrázek 19 – dva rozsahy adres na DHCP serveru 19](#_Toc164356837)

[Obrázek 20 – mód access s přístupem do VLAN 10 na portu GIG1/1 20](#_Toc164356838)

[Obrázek 21 – mód access s přístupem do VLAN 20 na portu GIG2/1 20](#_Toc164356839)

[Obrázek 22 – mód trunk na portu GIG0/1 20](#_Toc164356840)

[Obrázek 23 – schéma internetu 20](#_Toc164356841)

[Obrázek 24 – STP na switchi: pomalejší cesta vypnuta 21](#_Toc164356842)

[Obrázek 25 – STP na switchi: pomalejší cesta zapnuta 21](#_Toc164356843)

[Obrázek 26 – ping na youtube 21](#_Toc164356844)

[Obrázek 27 – webová stránka youtube – generováno ChatGPT 22](#_Toc164356845)

[Obrázek 28 – DNS požadavek 22](#_Toc164356846)

[Obrázek 29 – DNS odpověď 23](#_Toc164356847)

[Obrázek 30 – záznamy na DNS serveru 23](#_Toc164356848)

[Obrázek 31 – příznak SYN 23](#_Toc164356849)

[Obrázek 32 – příznak ACK a SYN 23](#_Toc164356850)

[Obrázek 33 – příznak ACK 23](#_Toc164356851)

[Obrázek 34 – příznak ACK a FIN 23](#_Toc164356852)

[Obrázek 35 – odesílání emailu uživateli 24](#_Toc164356853)

[Obrázek 36 – obdržený email 24](#_Toc164356854)

[Obrázek 37 – vložení souboru test\_FTP.txt na FTP server z PC1 24](#_Toc164356855)

[Obrázek 38 – stažení souboru test\_FTP.txt na PC2 24](#_Toc164356856)

[Obrázek 39 – uložený soubor test\_FTP.txt na PC2 25](#_Toc164356857)

[Obrázek 40 – FTP paket s uživatelským jménem 25](#_Toc164356858)

[Obrázek 41 – FPT paket s heslem 25](#_Toc164356859)

[Obrázek 42 – FTP paket s typem souboru 25](#_Toc164356860)

[Obrázek 43 – FTP paket s příkazem STOR 25](#_Toc164356861)

[Obrázek 44 – oznámení konce přenosu 25](#_Toc164356862)

# Přílohy

Příloha 1: Pomocný soubor pro vysvětlení fungování switche

Příloha 2: Nastavení ML a Městského switche

MLS:

vlan 10

name DUM\_1

vlan 20

name DUM\_2

int range fa0/1-24

switchport trunk enxapsulation dot1q

switchport mode trunk

ip routing

int vlan 1

ip add 192.168.1.1 255.255.255.0

no sh

ip helper-address 192.168.1.2

int vlan 10

ip add 192.168.10.1 255.255.255.0

no sh

ip helper-address 192.168.1.2

int vlan 20

ip add 192.168.20.1 255.255.255.0

no sh

ip helper-address 192.168.1.2

Městský switch:

int gig0/1

switchport mode trunk

int gig1/1

switchport access vlan 10

int gig2/1

switchport access vlan 20

vlan 10

name DUM\_1

vlan20

name DUM\_2

1. Google IPv6 adoption [↑](#footnote-ref-2)
2. Fungování switche vysvětleno použitím pomocné sítě (příloha 1) [↑](#footnote-ref-3)
3. Security magazín 2023 [↑](#footnote-ref-4)
4. Nastavení switchů v příloze 2 [↑](#footnote-ref-5)