Střední průmyslová škola,
Česká Lípa, Havlíčkova 426, příspěvková organizace

tel.: **487 833 123**
fax: **487 833 101**
email: **sps@sps-cl.cz**
web: **www.sps-cl.cz**

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

Použité zkratky

1 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 kterou jsem navrhl, vysvětlení jak funguje a k čemu jsou jednotlivé prvky,

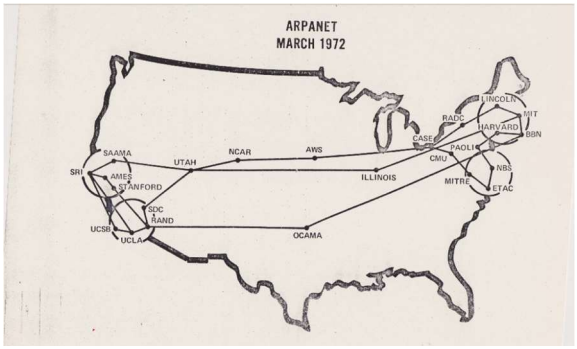
2 TEORETICKÁ ČÁST PRÁCE

2.1 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…

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



Obrázek 1 - Síť ARPANET v březnu 1972

2.1.2 Kdo vlastní internet

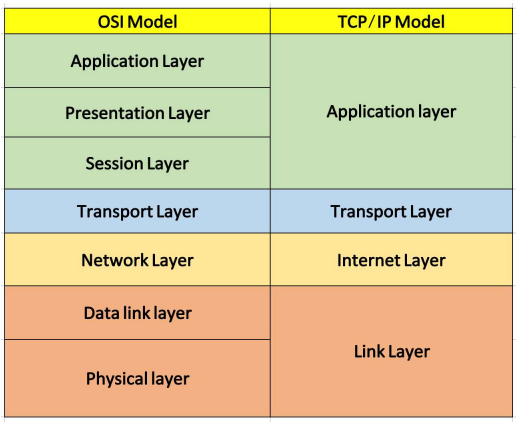
Internet je decentralizovaná síť a také není nikým vlastněn. Je to síť sítí, která propojuje nezávislé sítě dohromady. Přesto musejí existovat organizace, které budou tuto síť spravovat a vytvářet standardy protokolů. O protokoly se stará nezisková organizace Internet Engineering Task Force (IETF), česky 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.

2.1.3 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.

2.1.4 Referenční model ISO/OSI

Je model řešení komunikace v počítačových sítích pomocí vrstev. Vypracovala ho organizace ISO (mezinárodní organizace pro normalizaci). Standardizovat architekturu počítačových sítí a usnadnit komunikaci mezi různými zařízeními od různých výrobců. Nespecifikuje realizaci sys témů, ale uvádí principy vrstev. ISO/OSI se dělí do sedmi vrstev, aplikační, prezentační, relační, transportní, síťová, spojová, fyzická. V sítích se využívá TCP/IP model, který využívá čtyři vrstvy. Linková vrstva pracuje v lokální síti.



2.1.5 Služby internetu

2.2 Protokoly

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“)

2.2.1 TCP/IP

2.2.2 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 2^{32} (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

počet adres	počet bitů	prefix	třída	maska
1	0	/32		255.255.255.255
2	1	/31		255.255.255.254
4	2	/30		255.255.255.252
8	3	/29		255.255.255.248
16	4	/28		255.255.255.240
32	5	/27		255.255.255.224
64	6	/26		255.255.255.192
128	7	/25		255.255.255.128
256	8	/24	1C	255.255.255.0
512	9	/23	2C	255.255.254.0
1 024	10	/22	4C	255.255.252.0
2 048	11	/21	8C	255.255.248.0
4 096	12	/20	16C	255.255.240.0
8 192	13	/19	32C	255.255.224.0
16 384	14	/18	64C	255.255.192.0

Obrázek 2 - tabulka prefixů s počtem ip adres

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.

2.2.2.1 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.

2.2.2.2 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.

2.2.3 IPv6

Protokol IPv6 vznikl už v roce 1998 jako nástupce protokolu IPv4, ale jako internetový standart byl potvrzen až v roce 2017. IPv6 používá 128 bitové adresy umožňující až 2^{128} přibližně 340 sextilionů ($3{,}4 * 10^{38}$) ip adres. Použitelných adres je ale méně, protože některé z nich museli být vyřazeny pro speciální využití.

Pakety jsou navržené tak aby nebylo nutno je překládat službou NAT což zjednodušuje konfiguraci.

2.3 Síťové prvky

2.3.1 Aktivní prvky

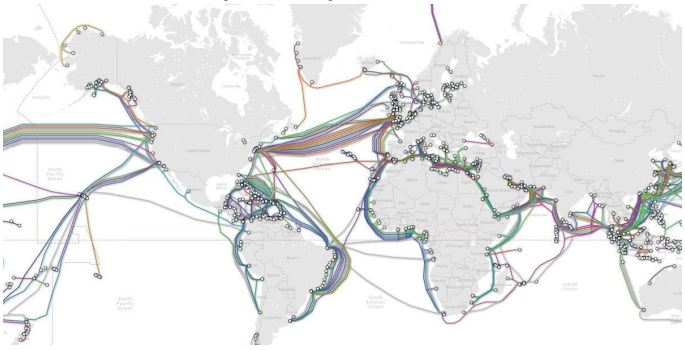
2.3.1.1 Routery

2.3.1.2 Switche

2.3.1.3 Servery

2.3.2 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.



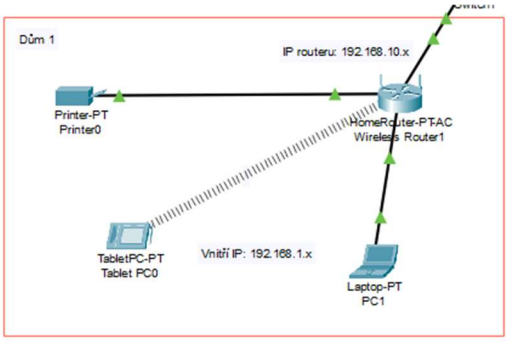
3 PRAKTICKÁ ČÁST PRÁCE

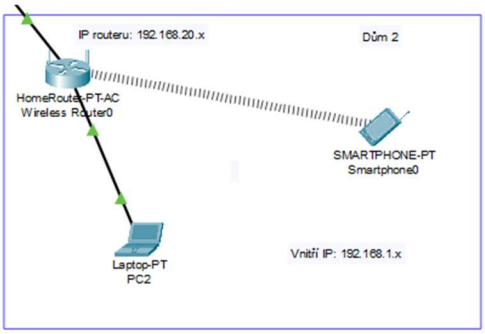
3.1 Packet tracer

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

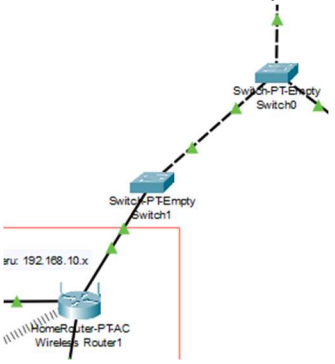
3.2 Síť LAN

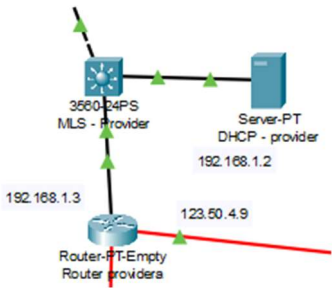
Síť LAN (local area network) je malá počítačová síť, převážně domácí nebo firemní sítě. V této práci jsou použity dvě sítě, Dům 1 a Dům 2, které reprezentují domácí sítě. Pro správné fungování sítě, je nutné aby se všechny prvky v síti nakonfigurovaly. Toto nastavení může být provedeno buď manuálně, 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).





Samotný 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 zásobníky pro obě sítě. Vlan10 pro Dům 1 a vlan20 pro Dům 2.





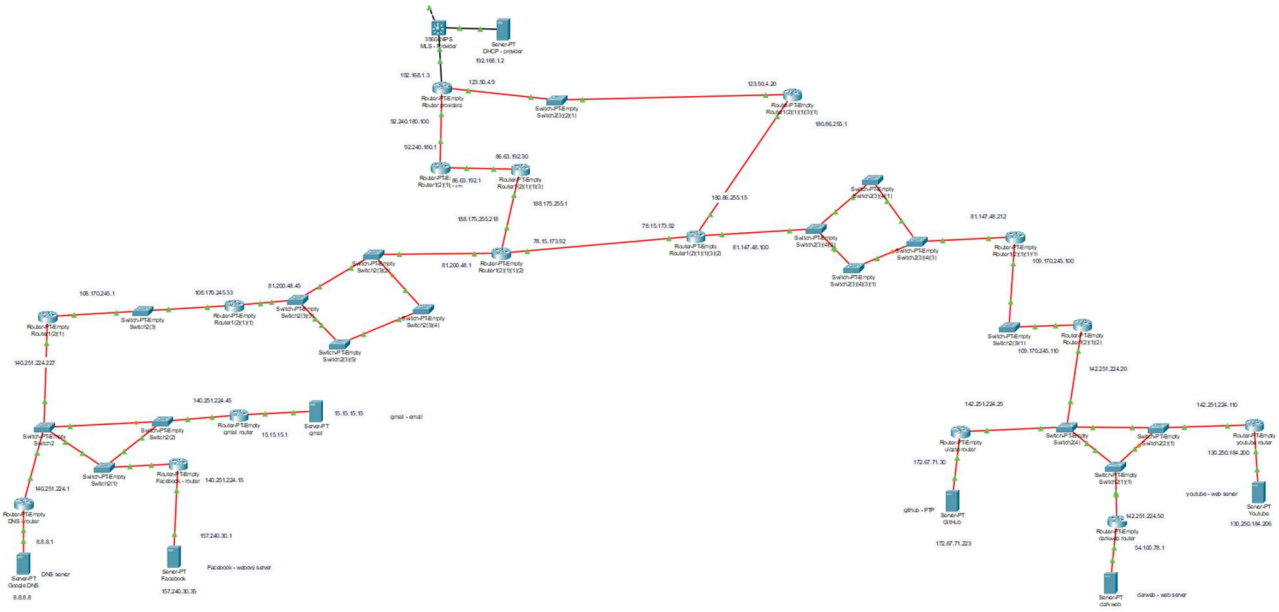
Pool Name	Default Gateway	DNS Server	Start IP Address	Subnet Mask	Max User
vlan20	192.168.20.1	8.8.8.8	192.168.20.3	255.255.2...	253
vlan10	192.168.10.1	8.8.8.8	192.168.10.3	255.255.2...	253

3.2.1 Nastavení ML switche

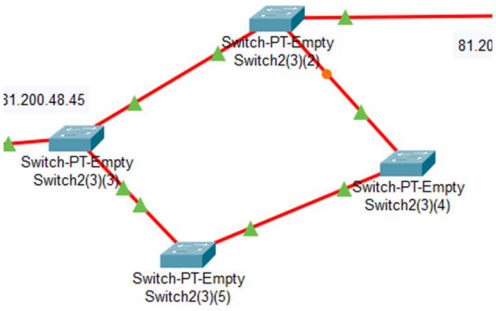
Většina věcí se v packet traceru jde nastavit přes grafické rozhraní, to ale co je potřeba pro nastavení ML switche se zde nenachází, proto se využije možnosti nastavení přes příkazy. První dva příkazy, které se používají vždycky jsou en (zapnutí) a conf terminal (přístup do konfiguračního terminálu), 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.

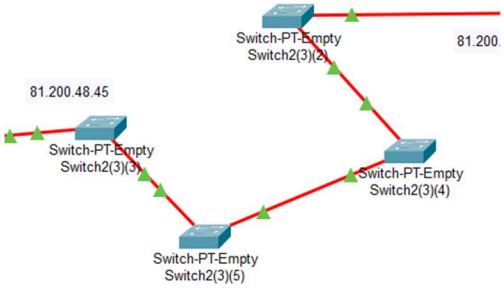
3.3 Síť WAN

Síť 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.



Velice důležtou částí internetu je, když jeden prvek, např. switch, vypadl tak aby internet nepřestal fungovat. Pro zajištění téhle podmínky se využívá např. propojení prvků více než jednou cestou nebo tak zvanou redundancí, tj. propojení switchů více cestami. Redundatní propojení může být nebezpečné 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.





3.4 Otestování funkčnosti internetu

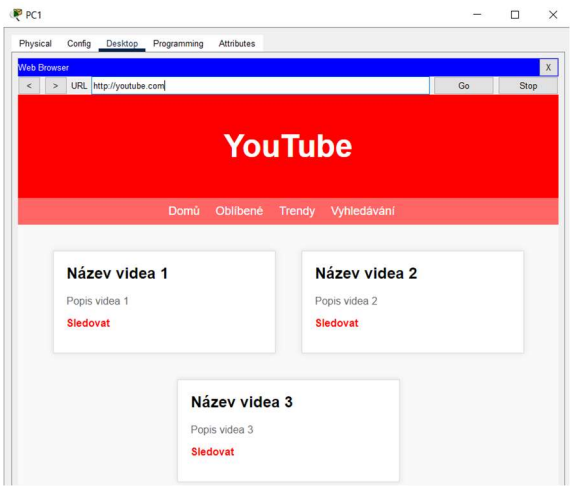
Jedním ze základních diagnostických pomůcek pro ověření funkčnosti internetu je příkaz ping. Ping nám umožní zjistit jestli náš počítač dokáže komunikovat s jiným počítačem, routerem nebo serverem. Příkaz využijeme otevřením příkazového řádku, napsáním ping [cíl]. Pro ukázku bude probíhat ping z PC1 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.

```
C:\>ping www.youtube.com

Pinging 130.250.184.206 with 32 bytes of data:

Reply from 130.250.184.206: bytes=32 time=10ms TTL=119
Reply from 130.250.184.206: bytes=32 time<1ms TTL=119
Reply from 130.250.184.206: bytes=32 time<1ms TTL=119
Reply from 130.250.184.206: bytes=32 time<1ms TTL=119

Ping statistics for 130.250.184.206:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 10ms, Average = 2ms
```

3.5 Služby internetu

3.5.1 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).



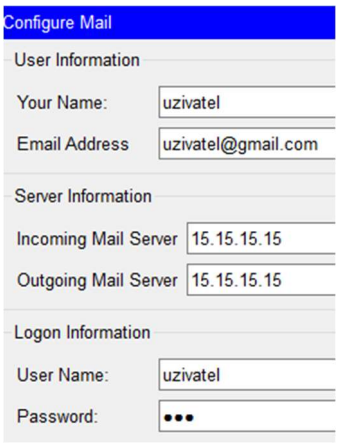
3.5.2 E-mail

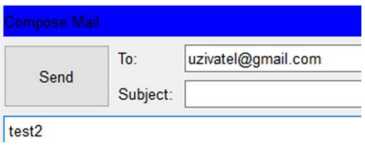
Webová stránka youtube.com – Generováno ChatGPT

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.

3.5.2.1 Email v Packet traceru

Na mail serveru (název serveru gmail) nastavíme doménu na gmail.com a vytvoříme dva uživatele, uživatel a uzivatel1. 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.





4 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/