Česká zemědělská univerzita v Praze
Technická fakulta

Zhodnocení možností využití subnettingu a VLAN v prostředí komerčních sítí

bakalářská práce

Vedoucí práce: Ing. Zdeněk Votruba, Ph.D.
Autor práce: Karel Truneček

PRAHA 2019

Česká zemědělská univerzita v Praze
Technická fakulta

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Autor práce:	Karel Truneček
Studijní program:	Zemědělské inženýrství
Obor:	Informační a řídicí technika v agropotravinářském komplexu
Vedoucí práce:	Ing. Zdeněk Votruba, Ph.D.
Garantující pracoviště:	Katedra technologických zařízení staveb
Jazyk práce:	Čeština
Název práce:	**Zhodnocení možností využití subnettingu a VLAN v prostředí komerčních sítí**
Název anglicky:	**Evaluate the possibilities of using subnetting and VLAN in commercial network environments**
Cíle práce:	Cílem práce je porovnat a posoudit vhodnost nasazení VLAN v komerčních počítačových sítí v alternaci s možností subnettingu. Pro obě uvedené služby definujte kritéria použití a bezpečnostní parametry.
Metodika:	1. Úkol 2. Cíl práce 3. Metodika 4. Důvody a možnosti pro organizaci počítačových sítí na logické vrstvě 5. Subnetting 6. VLAN 7. Zásady a pravidla pro použití 8. Bezpečnostní specifika 9. finanční náročnost a závěr
Doporučený rozsah práce:	30 až 40 stran textu včetně obrázků, grafů a tabulek
Klíčová slova:	počítačové sítě, subnetting, VLAN, bezpečnost

Doporučené zdroje informací:

1. firemní literatura CISCO
2. firemní literatura TP-Link
3. James F. Kurose, Keith W. Ross: Počítačové sítě, CPress, 2014, 3. vydání
4. JIROVSKÝ, V. Vademecum správce sítě. Praha: Grada, 2001. ISBN 80-7169-745-1.
5. KERŠLÁGER, M. -- HORÁK, J. Počítačové sítě pro začínající správce. Brno: Computer Press, 2003. ISBN 80-7226-876-7.

Předběžný termín obhajoby: 2018/19 LS - TF

Elektronicky schváleno: 29. 1. 2018
doc. Ing. Jan Malaťák, Ph.D.
Vedoucí katedry

Elektronicky schváleno: 9. 3. 2018
doc. Ing. Jiří Mašek, Ph.D.
Děkan

Čestné prohlášení

Prohlašuji, že jsem diplomovou/bakalářskou práci na téma: Zhodnocení možností využití subnettingu a VLAN v prostředí komerčních sítí vypracoval samostatně a použil jen pramenů, které cituji a uvádím v seznamu použitých zdrojů. Jsem si vědom, že odevzdáním bakalářské práce souhlasím s jejím zveřejněním dle zákona č. 111/1998 Sb., o vysokých školách a o změně a doplnění dalších zákonů, ve znění pozdějších předpisů, a to i bez ohledu na výsledek její obhajoby. Jsem si vědom, že moje bakalářská práce bude uložena v elektronické podobě v univerzitní databázi a bude veřejně přístupná k nahlédnutí. Jsem si vědom, že na moji bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů, ve znění pozdějších předpisů, především ustanovení § 35 odst. 3 tohoto zákona, tj. o užití tohoto díla.

V Praze dne: …….. ……..

Karel Truneček

Poděkování

Děkuji Ing. Zdeňku Votrubovi, Ph.D., vedoucímu bakalářské práce, za odborné vedení a cenné rady, čímž přispěl k vypracování této bakalářské práce.

Zhodnocení možností využití subnettingu a VLAN v prostředí komerčních sítí

Abstrakt: Cílem práce je porovnat a posoudit vhodnost nasazení VLAN v komerčních počítačových sítích v alternaci s možností subnettingu. V práci je v teoretické části vysvětleno několik základních pojmů, které jsou klíčové pro správné pochopení obou metod. Následně jsou v práci rozebrány obě metody, včetně jejich výhod a nevýhod a jejich správná konfigurace. Závěrem práce je v praktické části provedeno několik testů na malé síti rozdělené pomocí subnettingu a VLAN.

Klíčová slova: počítačové sítě, subnetting, VLAN, CIDR, bezpečnost

Evaluate the possibilities of using subnetting and VLAN in commercial network environments

Summary: The aim of this work is to compare and assess the suitability of VLAN deployment in commercial computer networks in alternation with subnetting. In the theoretical part of the thesis, several basic concepts are explained, which are crucial for the correct understanding of both methods. Subsequently, both methods are analyzed, including their advantages and disadvantages and their correct configuration. Finally, at the end of the work there are several tests on a small network divided by subnetting and VLAN.

Key words: computer networks, subnetting, VLAN, CIDR, safety

Obsah

Seznam obrázků:

Seznam tabulek:

Seznam použitých zkratek:

ARPA – Advanced Research Projects Agency

CIDR – Classless Inter-Domain Routing

DHCP – Dynamic Host Configuration Protocol

DNS – Domain Name System

IEEE – Institute of Electrical and Electronics Engineers

IMAP – Internet Message Access Protocol

IP – Internet Protocol

IPX/SPX – Internetwork Packet Exchange (IPX) / Sequenced Packet Exchange (SPX)

LAN – Local Area Network

MAC – Media Access Control

MAN – Metropolitan area network

POP3 – Post Office Protocol

PVID – Port VLAN ID

QOS – Quality of Service

RIPE NNC – Réseaux IP Européens Network Coordination Centre

SMTP – Simple Mail Transfer Protocol

TCP/IP – Transmission Control Protocol / Internet Protocol

UDP – User Datagram Protocol

VLAN – Virtual Local Area Network

WAN – Wide Area Network

1. Úvod

Žijeme v době, kdy se stále rychleji rozvíjí komunikační a informační technologie. Právě proto v dnešním světě hraje oblast počítačových sítí velmi důležitou úlohu. Asi si nikdo neuměl v 70-80 letech představit, jak velký bude mít tehdy začínající projekt ARPANET, z kterého se později vyvinul Internet tak, jak ho známe dnes, vliv na budoucnost komunikace po celém světě. To samozřejmě nevzniklo přes noc. Byl to dlouhý vývoj, který se skládal z mnoha střípků technologie, která po mnoha letech společně tvořily něco tak složitého a komplexního, jako je právě Internet, bez kterého si mnoho lidí neumí dnešní svět ani představit. Za tyto střípky lze beze sporu považovat i technologie, které jsou předmětem této práce – Subneting a VLAN. K Subnettingu se často řadí i podobná technologie, která na jeho základě vznikla, tzv. CIDR. Ani jedna z těchto technologií se sice v dnešní době nepoužívají čistě k tomu, k čemu původně vznikaly, ale i tak se pro ně dnes najde široké využití při rozdělování sítí. Správnou konfigurací těchto technologii lze v lokálních sítích podstatně zvýšit bezpečnost i výkonnost sítě a usnadnit její spravování. Jak už to tak bývá, tak i v tomto případě mají obě tyto technologie své opodstatnění a uplatnění. Na základě jejich výhod a nevýhod, které jsou v práci uvedeny se musí správce sítě rozhodovat jaké technologii dá v konkrétním případě přednost.

2. Cíl práce

Cílem práce je porovnat a posoudit vhodnost použití Subnettingu nebo VLAN. V práci je tak vysvětlen princip i výhody a nevýhody obou technologii. Čtenář by tedy měl po přečtení být schopen posoudit vhodnost nasazení metod a být schopen je bez problémů nakonfigurovat.

3. Metodika

V práci je zprvu vysvětleno několik základních pojmů, které jsou nezbytné k pochopení principu fungování subnettingu a VLAN. Následně je v práci vysvětlen samotný princip a konfigurace těchto technologií, které jsou následně navzájem porovnány. Závěrem práce je demonstrováno využití těchto technologií na malé síti, kde byla k rozdělení sítě na podsítě prvně využita technologie subnetting a následně VLAN. Na obou sítích byla ověřena správnost zapojení a změřena přenosová rychlost.

4. Teoretická část

V první půlce teoretické části jsou vysvětleny základní termíny jako Ethernet, TCP/IP, LAN, MAC adresa, IP protokol, převod z a do binární soustavy atd. To vše směřuje k druhé půlce teoretické části, a to sice k důvodu vzniku, principu a konfigurace subnettingu a VLAN.

4.1 Ethernet

Pod pojmem Ethernet si lze představit definici nebo standard, jak mají počítačové sítě jako LAN nebo MAN správně fungovat. Za vznikem Ethernetu stojí především společnosti Xerox, DEC a Intel, které se v 80. letech zabývaly novým konceptem technologie kabelových sítí (kroucená dvojlinka, optické kabely a koaxiální kabely). Ethernet je tedy protokol převážně lokálních sítí, který je z větší části standardizován jako IEEE 802.3. Zjednodušeně řečeno je Ethernet pro lokální sítě to, čím je Internet pro celosvětové sítě. Ethernet od svého vzniku v 80. letech pokračoval ve svém vývoji a je pravděpodobné, že v dohledné budoucnosti zůstane nejrozšířenější, takto využívanou technologii pro lokální sítě. Jeho dominantní postavení bylo dáno především tím, že byl první široce používanou vysokorychlostní technologii LAN. Síťoví administrátoři se s ním tedy brzy důvěrně seznámili. Další výhodou je, že Ethernet je jednodušší a levnější, než jeho předchůdci – token ring, FDDI, nebo ATM. Začátkem 20. století prošel Ethernet jednou zásadní změnou. Zařízení nadále využívají hvězdicovou technologii, ale hub byl nahrazen přepínačem. (1)

4.2 Transmission Control Protocol / Internet Protocol

Dále jen TCP/IP. Protokol začal vznikat již na konci 60. let ve společnosti ARPA (Advanced Research Projects Agency) ministerstva obrany USA, která si tyto protokoly nechávala vyvinout pro jejich vznikající síť ARPANET. Již tehdy se jednalo o zárodek vzniku něčeho většího, něčeho, co dnes nazýváme Internet. Protokol byl plně uveden v provoz až 1.1.1983. TCP/IP je v dnešní době nejrozšířenější internetový přenosový protokol, na kterém je založena komunikace zařízení připojených do veřejné sítě. (2)

S nadsázkou se dá říct, že se jedná o „Chytrý protokol na hloupé síti“, protože komunikace probíhá po aktivních zařízeních připojených do sítě, ale ty se neustálé mění (odpojují a zapojují), proto protokol musí být dostatečně „inteligentní“ aby našel cestu do cílové adresy i na tak dynamicky proměnlivé síti jako je Internet. Za opak tohoto

protokolu se dá považovat IPX/SPX, který se využívá výhradně v lokálních sítí, kde se aktivní zařízení nemění.

TCP/IP se liší s jeho předchůdcem ISO/OSI především v tom že tvůrci TCP/IP považovali spolehlivost doručení datových paketů problémem koncových účastníků komunikace a mělo by být tedy řešeno až na úrovni transportní vrstvy. TCP/IP na rozdíl od ISO/OSI počítá jen se čtyřmi vrstvami sítě.

Nejnižší vrstvou je vrstva síťového rozhraní (Network Interface Layer). Ta má na starost vše, co je spojeno s přímým vysíláním a příjmem datových paketů. Typickým příkladem této vrstvy je právě Ethernet.

Další vyšší vrstvou je tzv. Síťová vrstva (Network Layer). Tato vrstva má na starosti především komunikaci mezi jednotlivými uzly. Jejím hlavním úkolem je tedy adresování a směřování. Hlavním protokolem této vrstvy je IP protokol.

Třetí vrstvou TCP/IP je transportní vrstva (Transport Layer), někdy také označována právě jako TCP vrstva, protože je nejčastěji realizována TCP protokolem. Tato vrstva zajišťuje především komunikaci mezi koncovými uživateli a zároveň zajišťuje spolehlivost přenosu.

Poslední, nejvyšší vrstvou je Aplikační vrstva (Application Layer). Pro tuto vrstvu jsou typické programy, které komunikují s transportní vrstvou. Jako jsou např. POP3, IMAP nebo SMTP, které slouží pro přijímání a odesílání e-mailů. Dále jsou zde typické protokoly jako DNS, Telnet apod. (2) (3)

4.3 Local Area Network

Local Area Network, zkráceně LAN označuje počítačovou síť pokrývající malé geografické území (domy, kanceláře atd.), kde jsou všechny příslušné prvky propojené do jednoho jednotně adresovaného segmentu. Takže všechna zařízení na lokální síti mají IP adresu ze stejného intervalu hodnot. Přenosové rychlosti jsou vysoké, řádově až desítky Gb/s. Zprvu sítě LAN s osobními počítači využívaly pro svoji jednoduchost protokol IPX/SPX. S nástupem World Wide Webu, ale byl nahrazen protokolem TCP/IP.

Typickým základním aktivním prvkem u lokálních sítí je router, který spojuje dvě sítě. Ten má jeden vstup zvaný WAN a několik dalších výstupů LAN, do kterých se připojují koncová zařízení v lokální síti. Router zároveň pomocí DHCP protokolu dynamicky přiděluje jednotlivým zařízením IP adresy. Další typické aktivní prvky využívané v lokálních sítí jsou například switch, síťové karty atd. (4) (5) (6)

4.4 Media Access Control adresa

Více známá pod zkratkou MAC adresa nebo fyzická adresa je celosvětově jedinečné číslo přiřazené výrobcem síťového prvku sloužící k identifikaci zařízení. Adresa se dělí na dvě poloviny. První polovina adresy definuje typ síťového prvku a výrobce (je tedy u všech karet daného typu a výrobce stejná). Druhou polovinu potom tvoří jedinečnou část adresy pro každý síťový prvek. Adresu tvoří 48 bitů, což umožnuje 2^{48} neboli 281 474 976 710 656 možných jedinečných adres. (6)

MAC adresa by se podle standartu měla zapisovat jako trojice čtyř hexadecimálních čísel oddělených tečkou. Mnohem častěji se ale setkáme se zápisem šestice dvojciferných čísel jednotlivě oddělených pomlčkou nebo dvojtečkou (např.: 44-8A-5B-B1-E5-42 nebo 44:8A:5B:B1:E5:42). MAC adresu využívají především protokoly na 2. síťové vrstvě. Typickým protokolem postaveném na MAC adrese je přenosový protokol IPX/SPX. (6)

4.5 IP adresa

Aby jednotlivá zařízení připojená do tak velké sítě jako je World Wide Web mohla mezi sebou komunikovat, bylo za potřebí je jednoznačně identifikovat. K tomu slouží IP protokol. Při každém přenosu dat po internetu je nutné znát IP adresu odesílatele a příjemce. O adresování a směrování datových paketů se pak starají směrovače (routery), které mají svoji vlastní IP adresu.

V dnešní době je nejrozšířenější IPv4, která vznikla roku 1981. Počet jedinečných IP adres je konečný, u verze IPv4 jich je 2^{32}= 4 294 967 296. Jeden z největších problémů internetu v současnosti je, že IPv4 adresy došly nebo docházejí (záleží na regionu). Právě kvůli tomu začaly vznikat technologie jako subnetting, CIDR a rozdělení na vnitřní a veřejné sítě. IPv4 je adresa tvořena 32bitovým číslem rozděleným tečkou po čtyřech jednotlivých oktetech.

IPv4 adresa se dělí na tři základní části. Prvních osm bitů je číslo sítě, druhých osm bitů je číslo podsítě a poslední dvě osmice bitů tvoří číslo síťového rozhraní.

Pro práci se subnettingem nebo CIDRem je důležité si uvědomit, že počítač nepracuje s dekadickou soustavou, ale s binární. Takže IP adresa například 192.168.1.5 vypadá pro počítač takto: 11000000.10101000.00000001.00000101. Jinak řečeno, každé dekadické číslo oddělené tečkou se převede samostatně do binární soustavy. (1) (7)

4.5.1 Binární zápis IP adresy

Bez základní znalosti, jak pracovat s binárním kódem a převádět ho do dekadické soustavy a obráceně je nemožné pochopit princip a konfiguraci subnettingu a CIDRu. Binární (dvojková) soustava je číselná soustava, která používá pouze dvě číslice (0,1) na rozdíl od běžně používané dekadické (desítkové), která používá deset číslic (0,1,2,3,4,5,6,7,8,9). Tato soustava má poziční číselnou soustavu se základem 2. Konkrétní číslo je vyjádřeno mocninou čísla 2. Čísla zapsaná ve dvojkové soustavě se nazývají binární čísla. Zápis ve dvojkové soustavě bývá doplněn o znak „b“ nebo „2“ použitý jako dolní index za poslední číslicí, případně zkratkou BIN. Každý počítač na světě pracuje na základě binární soustavy. Tyto dva stavy 0 a 1 odpovídají stavu elektrického obvodu (bez napětí = 0, pod napětím = 1). Také se pomocí těchto dvou mohou vyjádřit stavy logického výroku (nepravda = 0, pravda = 1). (6)

4.5.1.1 Převod z dekadické do binární soustavy

Nejsnáze lze převést číslo z desítkové do dvojkové soustavy postupným dělením. Číslo, které se převádí je děleno neustále dvojkou až k nule, přičemž se zapisují zbytky po celočíselném dělení. Výsledek jsou právě zbytky po dělení (1,0), které se zapisují od posledního děleného čísla po první.

Princip převodu do jiných soustav je vždy stejný, ale převáděné číslo musí být děleno vždy příslušným číslem soustavy. Při převodu například do šestnáctkové soustavy je číslo děleno šestnáctkou. (6)

Konkrétní příklad:

Je zapotřebí převést číslo $55_{(10)}$ v dekadické soustavě do binární:

55:2= 27 => 1

27:2= 13 => 1

13:2= 6 => 1

6:2= 3 => 0

3:2= 1 => 1

1:2= 0 => 1

Výsledek je tedy: $110111_{(2)}$.

4.5.1.2 Převod z binární do desítkové soustavy

U tohoto převodu stačí použít rovnici $x = \sum_{i=0}^{k-1} x_i \cdot 2^i$. Kde nabývající hodnoty x jsou 1 a 0 z původního tvaru binárního čísla a mocnitel i se zvětšuje vždy o 1 ke každé vyšší bitové pozici.

Konkrétní příklad:

Je zapotřebí převést číslo $110111_{(2)}$ v binární soustavě do dekadické:

$1 \cdot 2^5 + 1 \cdot 2^4 + 0 \cdot 2^3 + 1 \cdot 2^2 + 1 \cdot 2^1 + 1 \cdot 2^0 = 32 + 16 + 0 + 4 + 2 + 1 = 55$

Výsledek je tedy: $55_{(10)}$.

Tento postup může být uplatněn i při převodu do jiných soustav, ale vždy se musí násobit číslo příslušným číslem soustavy. Například při převodu do osmičkové soustavy je násobeno osmičkou.

Zjednodušeně si lze napsat nad čísla mocniny čísla 2 a sečíst pouze ty, pod kterými je číslo 1. Pro lepší představu je přiložena Tabulka 1 – Převod binárního čísla do desítkového.

Tabulka 1 – Převod binárního čísla do desítkového

mocniny čísla 2	32	16	~~8~~	4	2	1
číslo v bin. soustavě	1	1	0	1	1	1

32+16+4+2+1= 55

V praxi je samozřejmě nejrychlejší a nejjednodušší použít kalkulačku, která tyto převody umí.

4.5.2 Další parametry adresace

V těchto podkapitolách jsou vysvětleny termíny jako maska sítě, brána sítě, třídy IPv4 adres a pravidla přidělování IP adres na kterých je v podstatě založen subnetting a CIDR.

4.5.2.1 Maska sítě

Slouží právě k rozdělení sítě na jednotlivé podsítě. Určuje, která část IP adresy je síťová a která je pro síťové rozhraní. V binárním tvaru obsahuje jedničky tam, kde se v adrese nachází číslo sítě a podsítě a nuly tam, kde je číslo síťového rozhraní. Běžně se setkáte se zápisem masky v desítkové soustavě, např.: 255.255.255.0 v binární soustavě je zápis: 11111111. 11111111. 11111111.00000000. (8)

4.5.2.2 Brána sítě

Takto je označován uzel, který má v síti nejvyšší postavení. Tvoří ho zpravidla aktivní hardwarový prvek tzv. směrovač (nejčastěji router), který přeposílá datové pakety do koncových zařízení. Přes toto zařízení pak probíhá veškerá komunikace v dané síti. Všechna zařízení pak do něj zapojená spadají implicitně do dané sítě. Směrovač má dvě adresy, jednu vnější (veřejnou) přes kterou komunikuje s ostatními aktivními prvky a druhou implicitní bránu (default gateway), přes kterou komunikuje s koncovými zařízeními do něj zapojenými. (9)

4.5.2.3 Třídy IPv4 adres

Podle toho, jak jsou jednotlivé sítě rozlehlé, rozlišujeme tři hlavní třídy IP adres – A, B a C. Jak vypadá rozdělení IP adresy je zobrazeno na Obrázku 1. Třídy IP adres rozděluje maska sítě, kterou určuje prvních několik bitů IP adresy.

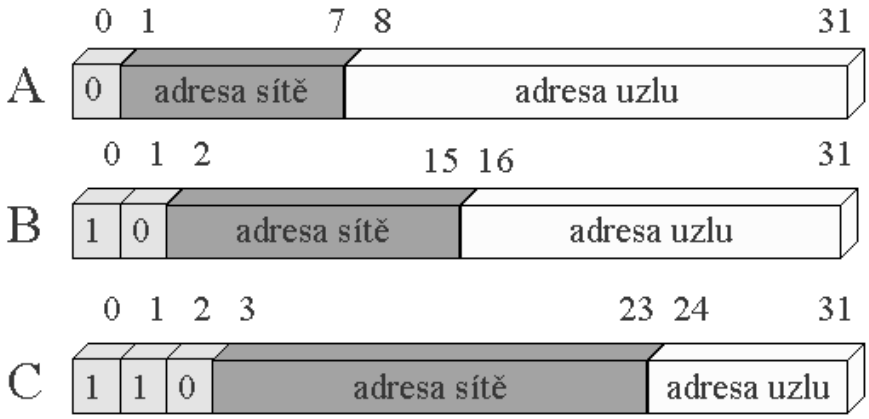
IP adresa třídy A je určena pro malý počet velkých sítí. Dovoluje adresování jen 126 sítích, ale v každé z nich může být až 16 miliónů počítačů, maska sítě je 255.0.0.0.

IP adresa třídy B je pro střední počet středních sítí. Může adresovat až 16 tisíc sítí a 65 tisíc počítačů v každé síti, maska sítě je 255.255.0.0. První dva bajty tvoří adresu sítě a další dva adresu počítače.

IP adresa třídy C se využívá tam, kde je třeba velký počet malých sítí. Dokáže adresovat až 2 milióny sítí a 254 počítačů v každé síti, maska sítě je 255.255.255.0. První tři bajty jsou adresou sítě a jeden bajt adresou počítače.

Dále byla definována třída D pro skupinové vysílání (multicasting) a třída E zůstala jako rezerva. (7)

Obrázek 1 – Rozdělení IP adresy na jednotlivé třídy



Zdroj: http://www.earchiv.cz/a95/a511c503.php3

4.5.2.4 Pravidla přidělování IP adres

Musí být dodrženy dvě základní pravidla. Pokud se dvě a více síťových rozhraní nachází ve stejné síti, musí mít jejich IP adresy stejnou síťovou část (Network ID) a pochopitelně jedinečné klientské části (Host ID). Pokud se dvě síťová rozhraní nachází v různých sítích, musí mít jejich IP adresy různou síťovou část (Network ID) a klientská část může i nemusí být stejná. (10)

Pro přidělování IP adres v sítích slouží tzv. Dynamic Host Configuration Protocol, zkráceně DHCP. Na hardwarovém zařízení, nejčastěji routeru, je spuštěný DHCP server, který všem zařízením do něj zapojených propůjčuje na určitou dobu jedinečnou IP adresu a v případě potřeby zapůjčení prodlužuje. Zároveň všem zařízením přiděluje i masku sítě, primární a sekundární DNS server a výchozí bránu. DHCP je protokol z rodiny TCP/IP, díky tomu může jednotlivým zařízením přidělovat automaticky potřebné parametry, čímž podstatně centralizuje a usnadňuje správu sítě. Na routeru je vždy i možnost vypnutí DHPC serveru a jednotlivým zařízením přidělit IP adresu a ostatní parametry ručně, tzv. staticky. (11)

4.6 Využití rozdělení sítě na podsítě

Subnetting nebo CIDR se převážně využívá ve společnostech, kde je zapotřebí softwarově rozdělit síť na podsítě. Čímž lze velice usnadnit správu sítě. Zařízení zapojená do jiných podsítí mezi sebou nemůžou komunikovat, to má pozitivní vliv na bezpečnost. Také se zvyšuje i výkonnost sítě, protože v jednotlivých podsítích dochází ke snížení zahlcení sítě a kolizí. (8)

„*Dělení sítě na subnety je důležité nejen proto, že naši síť "fyzicky" oddělíme od jiných sítí, ale také z výkonových důvodů. Řada informací se v rámci lokální sítě (subnetu) šíří pomocí broadcastů, tedy vysílání všem zařízením, což je značná režie pro síť i zařízení.*“ (8)

4.7 Důvod vzniku subnettingu a CIDRu

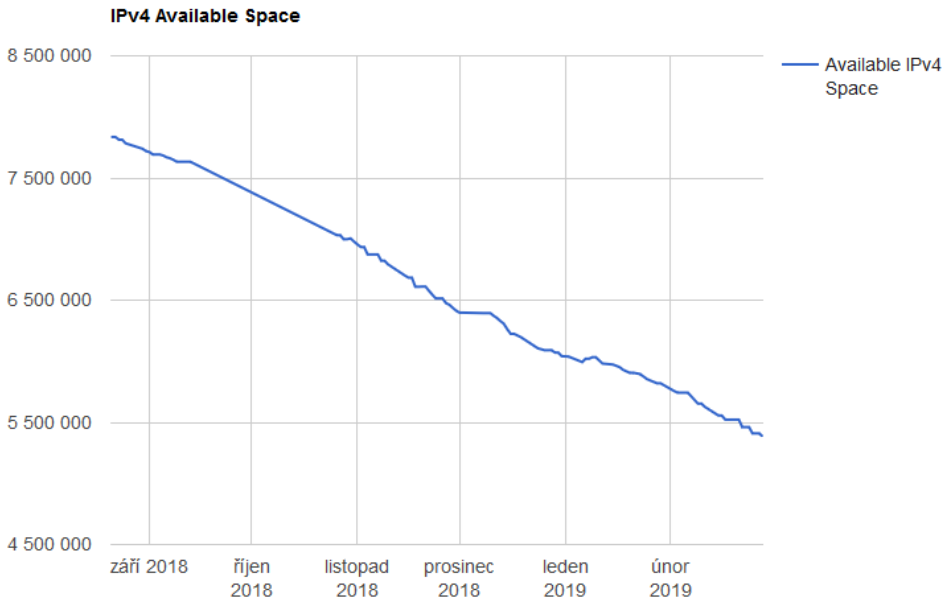
Když se poprvé začaly rozdělovat IP adresy vznikla tehdy prvotní myšlenka, že IP adresy budou přidělovány po celých „blocích“ protože nikdo nemohl čekat tak dynamický rozvoj internetu. Takže úspěšnému žadateli o IP adresy do jeho společnosti pro jednotlivá zařízení byl přidělen nejbližší vyšší počet IP adres. To znamenalo, že když si podnikatel zažádal o 400 IP adres dostal IP adresy třídy B, což znamenalo 65 536 IP

adres. Samozřejmě netrvalo dlouho a IP adresy začaly docházet. Další myšlenkou bylo přidělit více nejbližších menších bloků. Takže náš žadatel by dostal dva bloky IP adres třídy C, to by znamenalo 2x 255 adres. Ani tato metoda už tehdy bohužel nestačila, a tak se začalo nasazovat několik úsporných řešení, které se používají do dnes. (10)

Jednou z prvotních technologii bylo dynamické přidělování IP adres DHCP serverem. Došlo sice k úspoře adres, ale i tak se hledaly jiné lepší způsoby. Jedním z dalších řešení bylo zavedení právě tzv. Subnettingu, který dělil bloky adres na více částí pro více sítí. Další variantou byl CIDR, který umožnoval ještě podrobnější dělení síťové a klientské části. (11)

Tyto metody byly později v této problematice zastíněny technologii vnějších a vnitřních (resp. privátních a veřejných) IP adres, které se využívají až do dnes. I tato metoda je v dnešní době nedostačující, jak je evidentní z Obrázku 2 (pro Evropu) a jediné co může pomoci je zvětšení adresního prostoru čili přechod na IPv6. (10)

Obrázek 2 – RIPE NNC – září 2018 / únor 2019



Zdroj: http://opendata.labs.lacnic.net/ipv4stats/graphs/ipv4avail.html

4.8 Subnetting

Subnetting byl první metodou, jak rozdělovat síť na podsítě. Jeho největší výhodou byla jednoduchost a fakt, že rozdělení probíhalo pouze softwarově za pomoci vhodně nastavené masky sítě a IP adres jednotlivých zařízení. K rozdělení není třeba žádný další aktivní prvek. Největší nevýhodou subnetingu je, že dokáže rozdělit síť jen na omezený

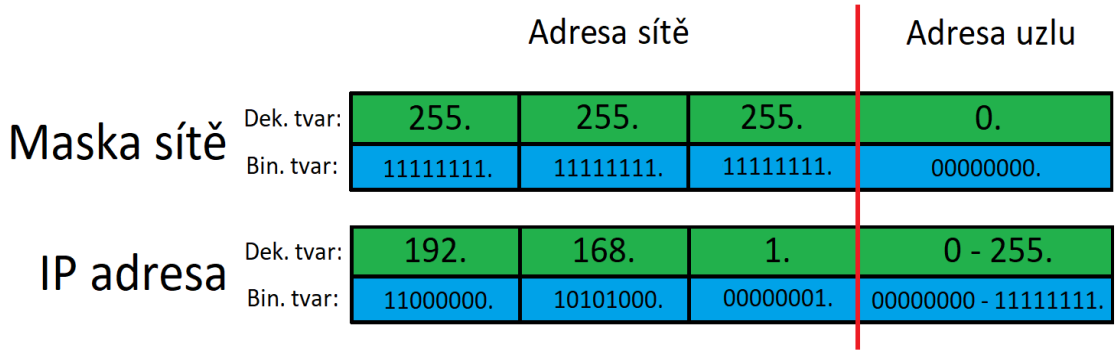
počet podsítí. Konkrétně jen násobky dvou. To znamená, že IP adresu třídy C dokáže rozdělit jen na 2, 4, 8, 16, 32, 64 podsítí. (10)

4.8.1 Princip subnettingu

Jak je zmíněno výše, IP adresa je rozdělena do 4 částí po 8 bitech. Tyto čtyři části IP adresy jsou pomocí třídy adres A, B a C pevně rozděleny na dvě části − na adresu sítě a uzlu. Subnetting mi pomocí masky sítě umožňuje změnit kolik bitů v rámci jedné části IP adresy bude přiděleno pro adresu sítě a kolik pro adresu uzlu. Jelikož je počet bitů v IP adrese neměnný, tak z logiky věci vyplývá, že když bude odebráno několik bitů, které byli původně přiděleny pro adresu uzlu a budou použity pro adresu podsítě, tak se počet bitů pro adresy uzlů sníží. Jinak řečeno, zvětšuje se adresa sítě na úkor adresy uzlu (čím více podsítí, tím méně v nich může být zapojeno jednotlivých zařízení). Jelikož je subnetting vázán rozdělováním sítě po celých blocích (8 bitech), lze síť rozdělovat omezeně. To znamená, že IP adresu třídy C, kde je k dispozici posledních 8 bitů pro adresu uzlů (254 dostupných IP adres pro jednotlivá zařízení v dané síti), je možno rozdělit pouze na 2, 4, 8, 16, 32, 64 podsítí. Protože každý bit masky sítě, přísluší stejnému bitu v IP adrese, a právě maska sítě definuje rozdělení IP adresy na část síťovou a část uzlovou. Na pozici, kde jsou jedničky je část síťová a na zbylých pozicích, kde jsou nuly, je část uzlová. (10)

Viz Obrázek 3, kde síť není rozdělena na podsítě. Takže maska sítě je 255.255.255.0 a IP adresa je například 192.168.1.0-255. Adresa sítě je 192.168.1. a poslední osmice bitů je uzlová část, ve které může být zapojeno 0 až 255 zařízení. S takovouto sítí se lze běžně setkat v domácnostech.

Obrázek 3 – Maska sítě a IP adresa



Zdroj: vlastní

4.8.2 Rozdělení sítě na podsítě pomocí subnettingu

První krok při rozdělení sítě na podsítě je změna masky sítě. Pomocí vzorce [$2^N = počet\ podsítí$] je možné vypočítat počet bitů, které budou přiděleny z uzlové části do síťové. Konstanta čísla 2, představuje počet možných stavů, které mohou nastat na dané pozici (1,0) a proměnná N je mocnina, kterou je číslo umocněno, aby výsledek byl počet potřebných podsítí. Toto číslo je potom shodné s potřebným počtem bitů. Tyto bity představují v masce sítě jedničky od nejvyšší bitové pozice do nejnižší, doplněné nulami. Samotná maska sítě je spočítána jako převod tohoto binárního čísla do dekadické soustavy. Bity, které se v IP adrese shodují s jedničkovými bity masky sítě, které definují počet nově vzniklých podsítí, nabývají všech možných kombinací 1 a 0. Počet kombinací jedniček a nul exponenciálně vzrůstá s počtem používaných bitů pro síťovou část. Aby bylo jednoznačně určeno, jaké zařízení bude zapojeno, do které podsítě, musí mít statickou IP adresu z rozsahu IP adres dané podsítě.

Rozsah IP adres v daných podsítích je dán převodem adresy podsítě a zároveň uzlové části z binární soustavy do dekadické, kde jsou bity, které tvoří síťovou část doplněny o nuly (nejnižší možná IP adresa v podsíti) a pak o jedničky (nejvyšší možná IP adresa v podsíti). Od maximálního možného počtu IP adres je nutnost vždy odečíst dvě, protože nultá (00000000) a poslední (11111111) IP adresa se nikdy nepoužívá pro vlastní účely! V Tabulce 2 je uvedena maska sítě a počet možných IP adres pro všechny podsítě pro IP adresu třídy C a v Tabulce 3 je znázorněn převod masky sítě z binárního tvaru do dekadického.

Tabulka 2 – Maska sítě a počet IP adres pro danou podsíť

Počet podsítí	Maska sítě	Počet IP adres
1	255.255.255.0	254
2	255.255.255.127	126
4	255.255.255.192	62
8	255.255.255.224	30
16	255.255.255.240	14
32	255.255.255.248	6
64	255.255.255.252	2

Zdroj: vlastní

Tabulka 3 – Převod masky sítě z binárního tvaru do dekadického

Maska sítě binárně				Maska sítě dekadicky			
11111111.	11111111.	11111111.	00000000	255.	255.	255.	0.
11111111.	11111111.	11111111.	10000000	255.	255.	255.	128.
11111111.	11111111.	11111111.	11000000	255.	255.	255.	192.
11111111.	11111111.	11111111.	11100000	255.	255.	255.	224.
11111111.	11111111.	11111111.	11110000	255.	255.	255.	240.
11111111.	11111111.	11111111.	11111000	255.	255.	255.	248.
11111111.	11111111.	11111111.	11111100	255.	255.	255.	252.

Zdroj: vlastní

4.8.3 Příklad využití subnettingu

Je dána IP adresa třídy C – 192.168.1.X, kterou je nutno rozdělit na 4 podsítě.

Maska sítě:

[2^N = *počet podsítí*] = [2^2=4]

Pro síťovou část budou zapotřebí 2 bity a pro uzlovou část zbude 6 => 11000000_{BIN} = 192_{10}. Viz Obrázek 4.

Obrázek 4 – Maska sítě pro 4 podsítě

Zdroj: vlastní

Rozsah IP adres v jednotlivých podsítích:

První dva bity IP adresy, které se shodují s prvními dvěma bity masky sítě určují tedy adresu podsítě. Všechny možné stavy, které mohou nastat kombinací 1 a 0 v těchto dvou bitech určují adresy jednotlivých podsítí. Adresa první podsítě je [00], druhé [01], třetí [10] a čtvrté [11]. Rozsah IP adres pro danou podsíť se vypočítá převodem do dekadické soustavy, kde je zbytek bitů doplněn o nuly pro nejnižší IP adresu a o jedničky pro nejvyšší IP adresu. Jak je uvedeno v Tabulce 4.

Tabulka 4 – Rozsah IP adres pro 4 podsítě

Maska sítě:	255.255.255.	11	000000		Rozsah IP adres pro podsítě
IP adresa:	192.168.1.	00	000000 - 111111	=	192.168.1.0 - 192.168.1.63
		01	000000 - 111111	=	192.168.1.64 - 192.168.1.127
		10	000000 - 111111	=	192.168.1.128 - 192.168.1.191
		11	000000 - 111111	=	192.168.1.192 - 192.168.1.255

Zdroj: vlastní

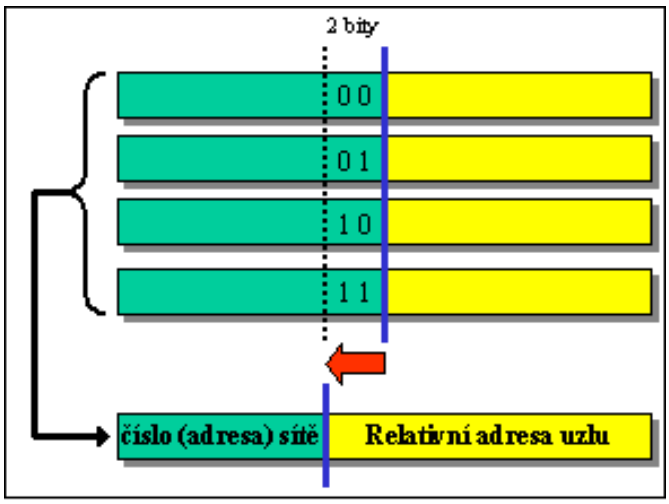
V každé podsítí není možné využít nejnižší a nejvyšší IP adresu. Tyto dvě IP adresy jsou určeny pro adresu podsítě a broadcoast. Zařízení, která budou zapojena do první podsítě musí mít IP adresu z rozsahu 192.168.1.1 až 192.168.1.62, v druhé podsítí 192.168.1.65 až 192.168.1.126, ve třetí 192.168.1.129 až 192.168.1.190 a ve čtvrté 192.168.1.193 až 192.168.1.254.

4.9 Supernetting

Funkce supernettigu je agregace podsítí neboli jejich sdružování. Supernetting můžeme považovat za pravý opak subnettingu, protože posouvá pomyslnou dělící čáru mezi uzlovou a síťovou částí naopak doleva k vyšším bitům (viz Obrázek 5). Výsledná síť je poté tvořena několika původně samostatnými IP adresami, které jsou díky supernettingu spojeny. V případě použití subnettingu zůstává informace o poloze dělící čáry pouze lokální. Tomu tak nemůže být i u supernettingu. Informace o poloze dělící čáry musí být dostupná a mít celosvětově a jednoznačně definovaný charakter. (12)

Aby byla umožněna práce s IP adresami, kde je právě tato dělící čára libovolně umístěna bylo za potřebí změnit koncept IP adres v rámci protokolů TCP/IP. Ke každé takovéto IP adrese musela být přiřazena její vlastní maska sítě, která definuje umístění právě této dělící čáry. Právě tento nový koncept o použití supernettingu a vzniku masek IP adres dostal pojmenování Classless Inter-Domain Routing neboli CIDR. V dnešní době se supernatting používá jen velmi výjimečně u rozsáhlých sítí. (12) (13)

Obrázek 5 – Supernetting



Zdroj: http://www.earchiv.cz/anovinky/ai1681.php3

„*CIDR také obsahuje mechanismus agregace, který dovoluje spojit několik spojitých síťových rozsahů do jednoho supernetu. Použití agregace šetří místo a prostředky při routování.*“ (14)

4.9.1 Využití supernettingu

Supernatting lze použít v případě, kdy je zapotřebí spojit několik síťových adres menších sítí v jedinou síťovou adresu.

Například je dána síť s 900 uzly, která je místo jediné adresy třídy B složena z 4 adres třídy C. Supernattingem můžeme posunout pomyslnou dělící čáru o dvě pozice k vyššímu bitu a udělat jedinou síťovou adresu (o dvě pozice protože [2^2=4]). (12)

4.10 Classless Inter-Domain Routing

Technologie CIDR vznikla v roce 1993. Stejně jako subnetting umožnuje CIDR softwarově rozdělovat sítě, ale daleko podrobněji. Při využití CIDRu v podstatě úplně zaniká význam tříd IP adres, protože CIDR už není vázán na jednotlivé bloky IP adresy. CIDR je podstatně náročnější na výpočet než subnetting, proto se mu v praxi dává přednost pouze, když je podrobnější rozdělení sítě než na 2, 4, 8, 16, 32 atd. podsítí nevyhnutelné. (10) (15)

4.10.1 Princip CIDRu

Za adresu sítě se přidává lomítko se zápisem buďto celé masky sítě nebo jednoho čísla (tzv. CIDR Notation). Oba dva zápisy jsou totožné, protože CIDR Notation určuje, kolik bitů v masce sítě od leva jsou jedničky a zbytek jsou nuly. Příklad zápisu: 192.168.1.1/28 je stejné jako 192.168.1.1/255.255.255.240. Protože maska sítě je v binárního tvaru: 1111111.1111111.1111111.11110000. Poslední jednička je zleva přesně 28. bit a číslo $11110000_2 = 240_{10}$. CIDR Notation oddělený lomítkem za IP adresou určuje, do jaké podsítě daná IP adresa připadá. Číslo sítě se spočítá jako logický součin celého bloku osmice bitů (kde končí síťová a začíná uzlová část adresy) IP adresy a masky sítě v binárním tvaru. Ostatní bloky IP adresy zůstanou beze změny. (13)

4.10.2 Rozdělení sítě na podsítě pomocí CIDRu

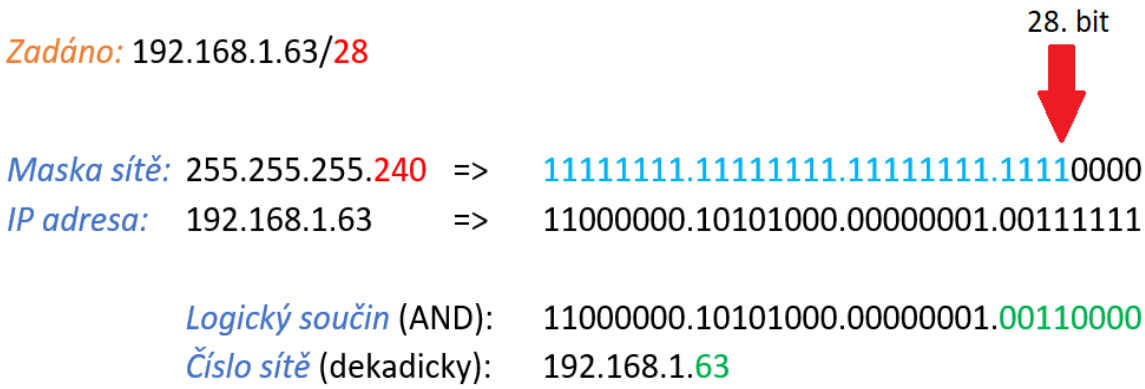
Pro správné určení masky sítě bude v případě CIDRu lepší postupovat obráceně než u subnettingu. První je zapotřebí si určit kolik zařízení bude společně zapojeno do jednotlivých podsítí. Výpočet je podobný jako u výpočtu podsítí subnettingu, až na to, že

je první počítána velikost uzlové části adresy neboli počet nul masky sítě. [$2^N = počet\ zařízení\ v\ podsíti$], kde konstanta čísla 2 opět představuje počet možných stavů na dané pozici (1,0), proměnná N je mocnina, kterou je konstanta umocňována tak, aby výsledek byl nejbližší vyšší počet možných zapojených zařízení do dané podsítě. V každé podsíti, stejně jako u subnettingu, nesmíme použít nejnižší a nejvyšší IP adresu, které jsou opět použity pro adresu sítě a broadcoast.

CIDR Notation je vypočítán odečtením všech nulových bitů od maximálního počtu bitů masky sítě (32). Rozsah IP adres pro každou podsíť začíná přesně tam, kde končí rozsah IP adres pro předchozí podsíť.

Pro lepší pochopení polohy CIDRu Notation a výpočtu čísla sítě je přiložen Obrázek 6.

Obrázek 6 – CIDR Notation – příklad



Zdroj: vlastní

4.10.3 Příklad využití CIDRu

Má být navržena síť sestávající ze 4 podsítí, ve které má být minimum připojených uzlů. V první podsíti je 6 PC, v druhé 14 PC, ve třetí 29 PC a ve čtvrté je 10 PC. IP adresa je 192.168.1.X.

Maska sítě / CIDR Notation:

1) 6 PC- [2^N = počet zařízení v podsíti] = (2^3=8) 8-2 = 6 dostupných IP adres.

CIDR Notation: 32-3= 29

Maska sítě: 11111111. 11111111. 11111111.11111000 => 255.255.255.248

Rozsah IP adres: 192.168.1.1 / 29 – 192.168.1.6 / 29

2) 14 PC- [2^N = počet zařízení v podsíti] = (2^4=16) 16-2 = 14 dostupných IP adres.

CIDR Notation: 32-4= 28

Maska sítě: 11111111. 11111111. 11111111.11110000 => 255.255.255.240

Rozsah IP adres: 192.168.1.9 / 28 – 192.168.1.22 / 28

3) 29 PC- [2^N = počet zařízení v podsíti] = (2^5=32) 32-2 = 30 dostupných IP adres.

CIDR Notation: 32-5= 27

Maska sítě: 11111111. 11111111. 11111111.11100000 => 255.255.255.224

Rozsah IP adres: 192.168.1.25 / 27 – 192.168.1.55 / 27

4) 10 PC- [2^N = počet zařízení v podsíti] = (2^4=16) 16-2 = 14 dostupných IP adres.

CIDR Notation: 32-4= 28

Maska sítě: 11111111. 11111111. 11111111.11110000 => 255.255.255.240

Rozsah IP adres: 192.168.1.58 / 28 – 192.168.1.71 / 28

Zařízení tedy připojená do první podsítě musejí mít IP adresu 192.168.1.1/29 až 192.168.1.6/29, do druhé 192.168.1.9/28 až 192.168.1.22/28, do třetí 192.168.1.25/27 až 192.168.1.55/27 a do čtvrté 192.168.1.58/28 až 192.168.1.71/28.

4.11 Porovnání subnettingu a CIDRu

Subnetting i CIDR mají jednu velkou společnou výhodu. Jejich realizace probíhá pouze softwarově, takže nepotřebují žádná další drahá hardwarová zařízení. Vše závisí tedy pouze na zručnosti administrátora sítě. Konfigurace subnettingu a CIDRu se, ale už podstatně liší. Jak už je zmíněno výše, subnetting dokáže rozdělit síť pouze na omezený počet podsítí s předem určeným počtem koncových zařízení. CIDR umožnuje díky libovolnému posouvání pomyslné dělící čáry podstatně detailnější dělení podsítě ovšem je složitější na konfiguraci a výpočet. CIDR má navíc tu výhodu, že při přidání další podsítě do sítě, která již je rozdělena na podsítě, nemusí nutně dojít k překonfigurování celého zapojení, pokud je v síti dostatek nevyužitých IP adres pro nová zařízení, která budou v nově vzniklé podsíti. U subnettingu bez ohledu na počet nevyužitých IP adres v síti, musí při přidání nové podsítě dojít k překonfigurování všech existujících IP adres v síti. Naopak je u CIDRu ale pravděpodobnější, že bude muset dojít k složité překonfiguraci sítě, když bude zapotřebí přidat několik zařízení do existující podsítě. Protože ty bývají dimenzovány právě tak, aby byl počet volných IP adres co nejmenší.

Vezměme si výše uvedený příklad s využitím CIDRu. Je patrné, že při využití CIDRu je značně ušetřen počet používaných IP adres. Při využití subnettingu by bylo zapotřebí použít celou adresu třídy C, 255 IP adres pro 64 PC. Většina IP adres by v jednotlivých podsítích zůstala nevyužita. V první podsíti by zůstalo 56 nevyužitých IP adres, v druhé podsítí 48, ve třetí podsítí 33 a ve čtvrté podsítí by zůstalo 52 nevyužitých IP adres, do kterých lze ale připojit bez problému potenciální další zařízení. Při použití CIDRu je využito jen 72 IP adres pro 59 PC. U typické adresy třídy C by tedy zůstalo 183 volných IP adres pro případné další podsítě. Při rozhodování, kterou technologii je nejlepší využít je nutné myslet do budoucnosti. Jestli je opravdu nutné detailnější dělení než umožňuje subnetting, jestli se do podsítí budou spíše přidávat nová zařízení nebo celé podsítě atd. Všechny tyto aspekty musí být zváženy, protože můžou v budoucnosti usnadnit mnoho práce.

4.12 VLAN

Virtuální LAN slouží především k logickému rozdělení sítě bez ohledu na fyzické uspořádání. K realizaci je ale zapotřebí hardwarové zařízení, což je hlavní rozdíl oproti subnettingu, nebo CIDRu, kde konfigurace probíhá pouze softwarově. VLANy, ale mají jednu velkou výhodu.

Subnetting a CIDR, který je založený na IP adrese pracuje na 3. síťové vrstvě. V praxi to tedy znamená, že při použití Subettingu nebo CIDRu komunikace mezi zařízeními v jiných podsítích stále probíhá, ale až koncové zařízení pozná, jestli se jedná o datové pakety, které jsou nebo nejsou určeny pro tuto podsíť a data „zahodí“ nebo pošle dál. Služba VLAN, ale probíhá již na nižší 2. síťové vrstvě, protože její realizaci uskutečňuje hardwarové zařízení, které rovnou adresuje datové pakety do podsítí, kam jsou určeny. To je z hlediska bezpečnosti mnohem lepší. Umožňuje tedy ještě dokonalejší rozdělení podsítí. Za další výhodu VLAN oproti subnettingu lze považovat snadnější uživatelskou konfiguraci. (16) (18)

4.12.1 Důvod vzniku VLAN

Technologie VLAN začala vznikat v polovině 90. let minulého století. Jejich původní důvod vývoje by se dal shrnout do tří bodů: 1. Redukce nákladů na konfigurační změny, 2. Virtuální pracovní skupiny, 3. Redukce zatížení všesměrových vysílání. První důvod se už nevyužívá, protože vznikla celá řada softwarových nástrojů, které se upřednostňují

před využitím VLAN v této oblasti a s nástupem Cloudů zanikl i druhý důvod vývoje. Skutečnost je tedy taková, že v dnešní době má uplatnění pouze třetí důvod.

VLAN se tedy v současnosti využívají především k redukce zatížení všesměrových vysílání neboli zabránění multicastingu. Pod pojmem multicasting si lze představit tedy všesměrové vysílání z jednoho zdroje do více stanic, což vede samozřejmě k zahlcení sítě daty, která většina koncových uživatelů nevyužívá. Typickým příkladem multicastingu je televizní či radiové vysílání, streaming, videokonference atd. Díky službě VLAN lze této komunikaci vyhradit vlastní VLAN, po které bude tato komunikace izolovaně probíhat a nebude zbytečně zatěžovat celou síť. (16) (17)

4.12.2 Princip VLAN

Jak už bylo zmíněno výše, tak k realizaci VLAN je zapotřebí hardwarové zařízení. To představuje tzv. managovatelný switch, nebo popřípadě managovatelný router, který má několik číslovaných vstupních portů. Managovatelný switch při spuštění vytváří VLAN číslo 1, která představuje první podsíť, do které lze připojit koncová zařízení a pomocí dalšího nastavení, které probíhá pomocí uživatelské aplikace spárované s managovatelným switch, lze přidat další VLAN. Existují čtyři základní metody, které zařazují zařízení do konkrétních VLAN – 1. Podle portu, 2. Podle MAC adresy, 3.Podle protokolu, 4. Podle autentizace. (17)

4.12.2.1 Podle portu

Díky jednoduchosti, rychlosti a snadnému spravování je tento způsob zařazení zařízení nejpoužívanější ze všech. Switch adresuje datové pakety na konkrétní porty, ke kterým jsou přiděleny jednotlivé VLAN. S touto jednoduchostí, ale přichází i nevýhoda. Switch u této metody nijak nekontroluje, co za koncové zařízení je právě připojeno do portu. To znamená, že při obyčejném přepojení kabelu se může potenciální útočník dostat do kterékoli VLAN. Následující konkrétní metody zařazení zařízení podle portu (MTU VLAN a Port Based VLAN) jsou popsány na managovatelných switch od společnosti TP–LINK.

MTU VLAN

Jediné nastavení, které je zde nutné je definice čísla portu, do kterého je přiváděna konektivita, tzv. uplink port. Každému dalšímu portu je pak napevno přidělena jedna VLAN. Veškerá komunikace pak procházející přes tento port spadá do dané VLAN.

Pokud je do takového portu zapojen další switch, tak všechna zařízení, do něj zapojena se budou nacházet v jedné VLAN.

Port Based VLAN

U této metody nelze nastavit, který port je uplinkový. Vytváří se zde pouze jednotlivé VLAN a k nim jsou následně přiřazovány porty. Každý port může být přiřazen v jednu chvíli pouze k jedné VLAN. To znamená, že pokud je do switch přiveden pouze jeden kabel s konektivitou, tak k internetu má přístup pouze ta skupina zařízení, které se nacházejí ve stejné VLAN.

4.12.2.2 Podle MAC adresy

Jak už název napovídá, tak u tohoto způsobu se zařazují zařízení do VLAN podle jejich zdrojové MAC adresy. Při konfiguraci jsou vytvářeny jednotlivé VLAN a ke každé vytvořené VLAN existuje tabulka, ve které je seznam MAC adres všech zařízení, které do ní patří. Tabulku lze tak považovat za tzv. „white list“. Touto metodou je v podstatě eliminován největší problém předchozí metody, protože u tohoto způsobu zařazení zařízení nezáleží, na kterém portu je které zařízení připojeno. Switch při připojení nového zařízení kontroluje v tabulce MAC adres do které VLAN patří. To vše jde ale na úkor rychlosti komunikace a složitosti spravování.

4.12.2.3 Podle protokolu

Tato metoda nevyžaduje v podstatě žádnou konfiguraci. Switch dynamicky přepojuje koncová zařízení do VLAN podle právě používaného protokolu. Koncové zařízení se tedy bude nacházet v jiné VLAN, pokud například bude uživatel posílat e-maily a zase v jiné, pokud bude uživatel vyhledávat přes prohlížeč na internetu. Switch zde, ale musí pracovat s aplikačními protokoly, takže se dostává opět na 3. vrstvu i když normálně pracuje na 2. vrstvě. To sice switch zpomaluje, ale umožňuje využití více nástrojů, jak optimalizovat komunikaci, jako je například QOS. Toto zařazení má tedy své uplatnění na velkých sítí, kde je velké množství používaných služeb.

4.12.2.4 Podle autentizace

Poslední nejsložitější, ale za to nejbezpečnější způsob zařazení. Pro autorizaci zařízení je používán protokol IEEE 802.1x, který představuje způsob ověřování přenosů. K ověřování se používá často tzv. RADIUS server. Podle informací zařadí server zařízení

do dané VLAN. U této metody nezáleží na místě zapojení ani na fyzickém zařízení. Jedná se o velice univerzální metodu.

802.1Q

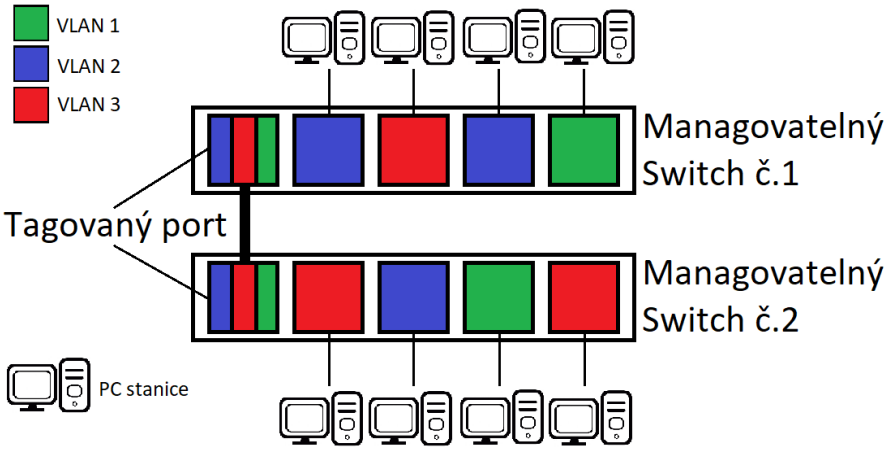
U této metody je možnost propojit více managovatelných switch, protože už pracuje s tagovanými a netagovanými porty. Tagovanými porty se propojují switch a do netagovaných portů se zapojují koncová zařízení. Blíže je tato technologie vysvětlena níže. Množství dostupných VLAN je zde naddimenzováno až do čísla 4094. V praxi se ale poslední VLAN nepoužívá! Do jednotlivých VLAN mohu uplingový port přiřadit víckrát!

První krok je vybrání VLAN, která bude konfigurována a následné vybrání portů, které do ní spadají. V PVID Setting je pak zapotřebí znovu zvolit porty, které mezi sebou mohou komunikovat. Uplinkový port se v tomto kroku nepřidává nikam, protože je zapotřebí ho použít ve více VLAN, v kterých je požadována konektivita.

4.12.3 Trunking protokol

Aby byla realizována komunikace v rámci VLAN mezi dvěma nebo více switch, byl vytvořen Trunking protokol. Ten využívá tzv. tagované porty přes které je možné switch navzájem propojit. Tagovaný port je nutno vybrat v nastavení. U takto propojených switch zůstává i nastavení VLAN, takže zařízení v prvním switch ve VLAN 1 může komunikovat se zařízením v druhým switch, které je také ve VLAN 1. Typické zapojení pomocí tagovaného portu je zobrazeno na Obrázku 7. (17)

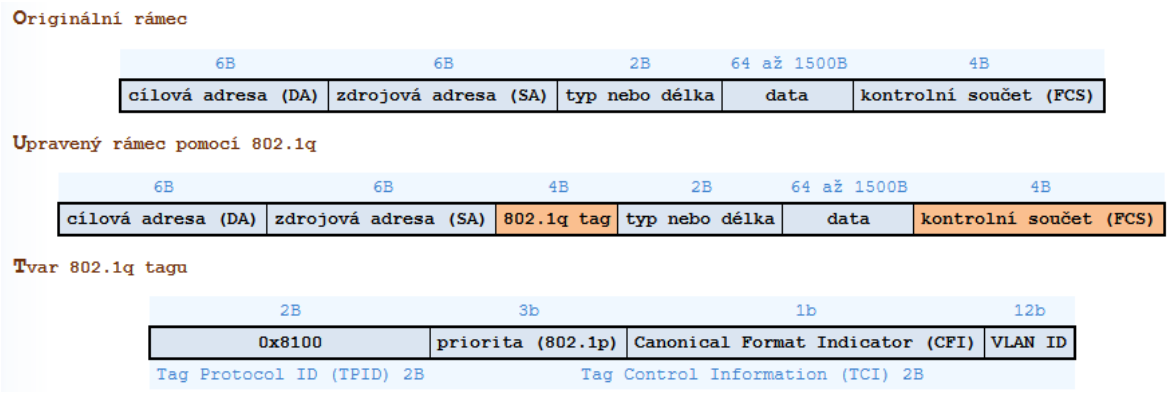
Obrázek 7 – VLAN – Tagovaný port



Zdroj: vlastní

Trunking protokol upravuje datové pakety procházející po tagovaném portu a vkládá do nich navíc informaci, z které VLAN je každý datový paket. Takto upravený paket umí přečíst pouze managovatelný switch na tagovaném portu. Úpravy datových paketů standardizuje IEEE 802.1q. Jak vypadá datový paket procházející po tagovaném portu je na Obrázku 8. (18)

Obrázek 8 – VLAN – Upravený datový paket



Zdroj: https://www.samuraj-cz.com/clanek/vlan-virtual-local-area-network/

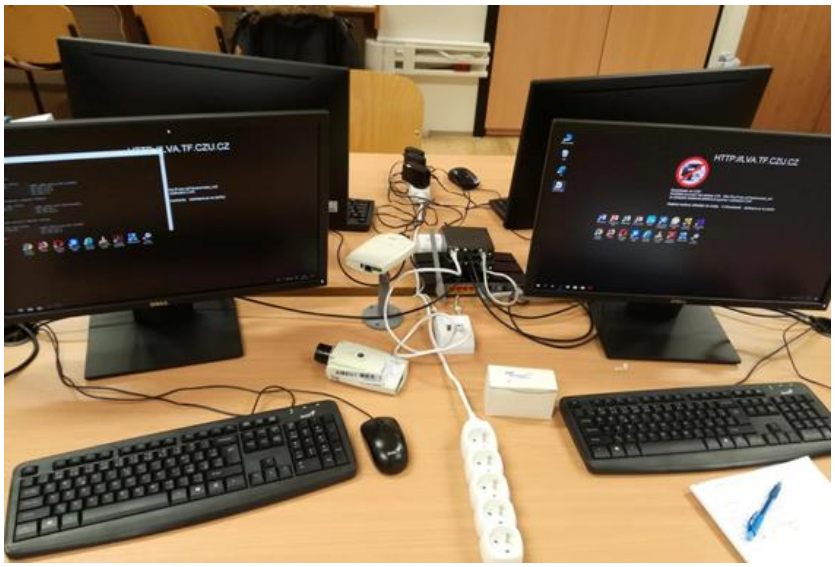
5. Praktická část

Tato část práce je zaměřena na praktické porovnání subnettingu a VLAN. Na vytvořené síti byla otestována funkčnost a změřena rychlost sítě při reálném využití obou metod.

5.1 Využité komponenty a softwary

Konfigurace zapojení probíhala v laboratoři na malé síti o 4 stejných počítačových stanicích (viz Obrázek 9). Při zapojení s užitím subnettingu byli zapojeny do switch části routeru a při zapojení VLAN byli použity dva managovatelné switch se stejnou maximální přenosovou rychlostí jako router. Ke konfiguraci switch byla využita příslušná aplikace TP-LINK Easy Smart Configuration Utility. K měření rychlosti přenosu uvnitř sítě byla využita aplikace TamoSoft Throughput Test a pro měření rychlosti ven ze sítě byl využit test rychlosti na stránkách www.adsl.cz.

Obrázek 9 – Fotografie – Pracoviště



Zdroj: vlastní

5.1.1 Počítačové stanice

Počítačové stanice se skládají z:

Operační systém: Windows 10 Enterprise (verze 1803)

Typ systému: 64 bitový operační systém

Procesor: Intel(R) Core(TM) i5-8400 CPU @ 2.80GHz 2.81GHz

Operační paměť (RAM): 16 GB

Grafická karta: NVIDIA Quadro P620

ID produktu: 00329-10180-22135-AA445

Na každé stanici je nainstalován webový prohlížeč Mozilla Firefox, TamoSoft Throughput Test a TP-LINK Easy Smart Configuration Utility.

5.1.2 TP-Link TL-WR1043ND Ultimate WLAN Gigabit Router

U tohoto routeru od společnosti TP-LINK byla využita pouze jeho switch část pro zapojení počítačových stanic.

Přenosové rychlosti pro HUB/Switch: 1 000 Mb/s

Počet portů HUB/Switch: 4

Napájení: 12 V / 1,5 A

Kód výrobce: TL-WR1043ND

5.1.3 Switch TP-Link TL-SG105E

Při zapojení byly využity dva tyto managovatelné switch od společnosti TP-LINK. K jejich konfiguraci byla využita příslušná aplikace.

Přenosová rychlost LAN: 1 000 Mb/s

Počet portů: 5

Napájení: 9 V / 0,6 A

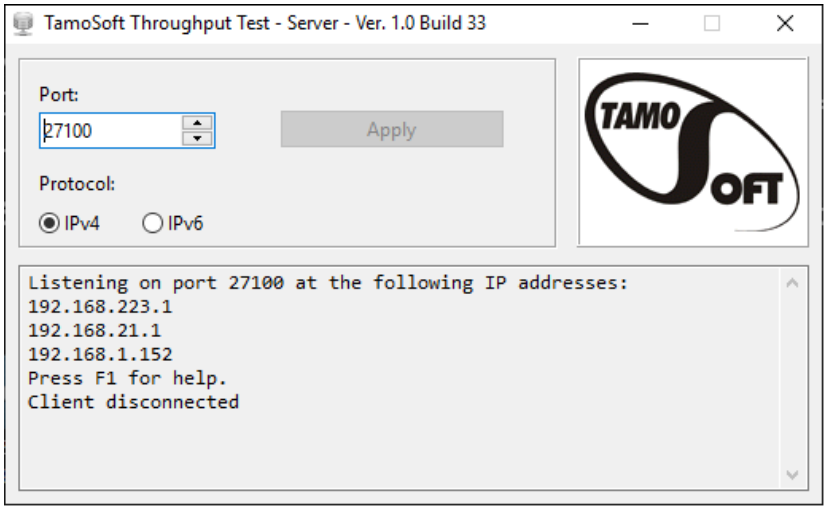
Kód výrobce: TL-SG105E

5.1.4 TamoSoft Throughput Test

TamoSoft Throughput Test je freewarový nástroj pro testování výkonu bezdrátové nebo kabelové sítě od společnosti TamoSoft. Tento nástroj průběžně odesílá datové toky TCP a UDP v rámci sítě a měří důležité hodnoty, jako jsou například vstupní a výstupní datové hodnoty a ztráta paketů. Výsledky zobrazuje v numerických i grafických formátech. Podporuje IPv4 i IPv6 a umožňuje uživateli vyhodnotit výkon sítě v závislosti na nastavení QoS (Quality of Service).

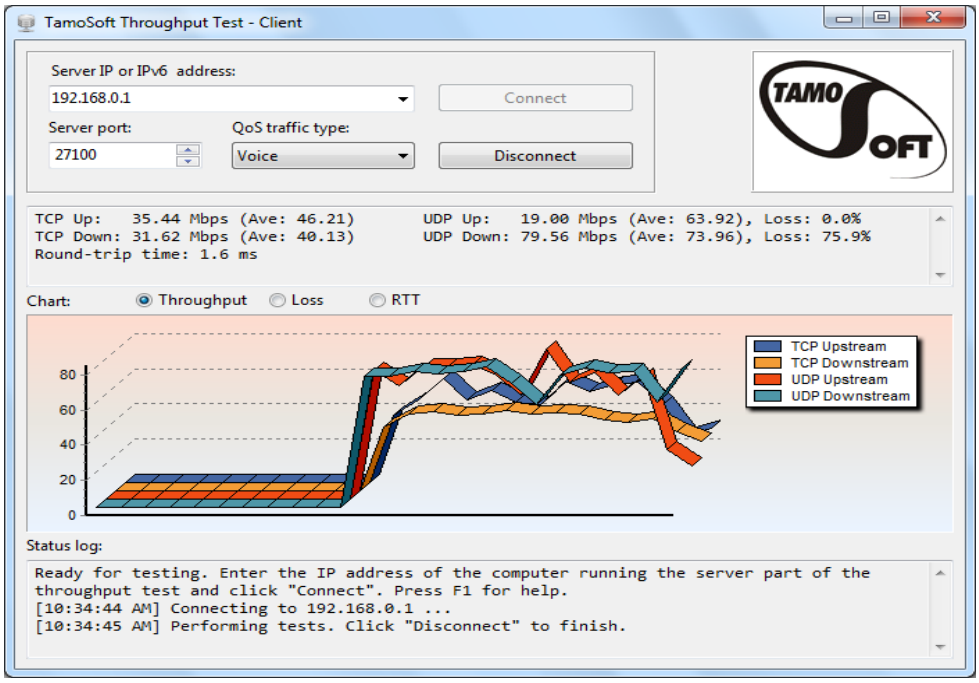
Pro provedení testu sítě používá aplikace dva komponenty: server a klienta. Uživatelské prostředí pro server je na Obrázku 10 a pro klienta na Obrázku 11. Serverová část aplikace naslouchá připojení od klienta a klient se připojí k serveru. Jakmile je spojení navázáno, klient a server odesílají data v obou směrech a klientská část aplikace vypočítává a zobrazuje výsledky.

Obrázek 10 – TamoSoft Throughput Test – SERVER



Zdroj: https://www.tamos.com/products/throughput-test/

Obrázek 11 – TamoSoft Throughput Test – CLIENT



Zdroj: https://www.tamos.com/products/throughput-test/

Na klientské části musí být nastavena IP adresa počítače, mezi kterým je měřena rychlost komunikace. Server port se musí shodovat na klientské i serverové části. Stisknutím tlačítka Connect na klientské části aplikace je spuštěn test a tlačítkem Disconnect je zastaven.

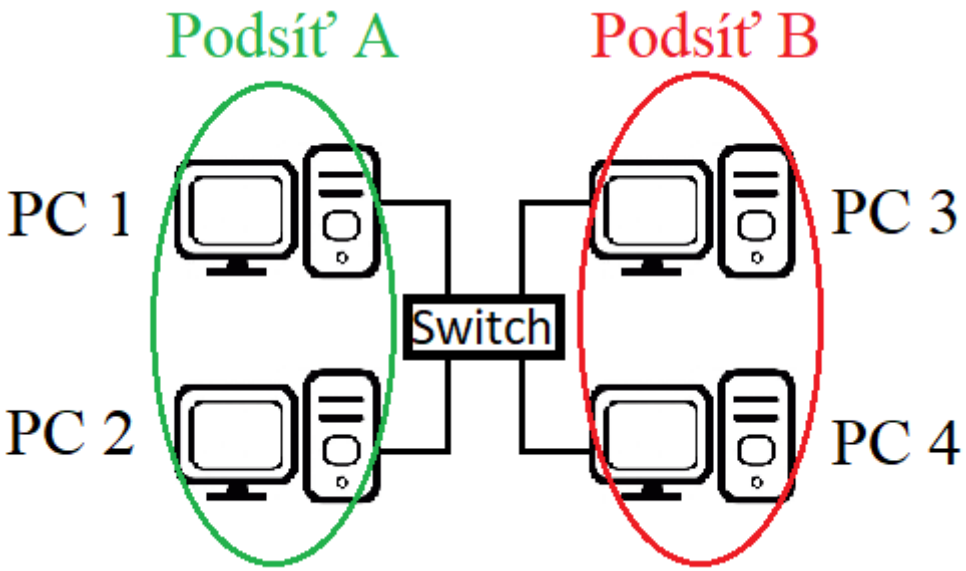
Pod tímto nastavením se nachází panel, na kterém se numericky zobrazují naměřené výsledky. Jak pro TCP, tak pro UDP je zobrazena přenosová rychlost v daný okamžik a v závorce průměrná hodnota za celou dobu měření. Software zároveň zobrazuje procento ztracených paketů.

Součástí je i grafické zobrazení. Horizontální osa je určena pro čas a vertikální pro přenosovou rychlost. Na zobrazeném grafu je vidět průběh přenosu za posledních 60 vteřin.

5.2 Zapojení subnettingu

Všechny počítačové stanice se původně nacházely v jedné síti. Správnou konfigurací masky sítě a IP adres byli tyto čtyři stanice rozděleny do dvou podsítí (A podsíť a B podsíť), kde v každé podsítí byli dvě počítačové stanice. Pro lepší pochopení jsou počítače navíc očíslovány (PC1, PC2, PC3, PC4), jak je zobrazeno na Obrázku 12.

Obrázek 12 – Subnetting – Dvě podsítě



Zdroj: vlastní

5.2.1 Konfigurace subnettingu:

PC 1:		**PC 3:**	
IP adresa:	192.168.1.51	*IP adresa:*	192.168.1.151
Maska podsítě:	255.255.255.128	*Maska podsítě:*	255.255.255.128
Výchozí brána:	192.168.1.1	*Výchozí brána:*	192.168.1.1
Upřed. server DNS:	8.8.8.8	*Upřed. server DNS:*	8.8.8.8

PC 2:		**PC 4:**	
IP adresa:	192.168.1.52	*IP adresa:*	192.168.1.152
Maska podsítě:	255.255.255.128	*Maska podsítě:*	255.255.255.128
Výchozí brána:	192.168.1.1	*Výchozí brána:*	192.168.1.1
Upřed. server DNS:	8.8.8.8	*Upřed. server DNS:*	8.8.8.8

5.2.2 Test pomocí funkce ping

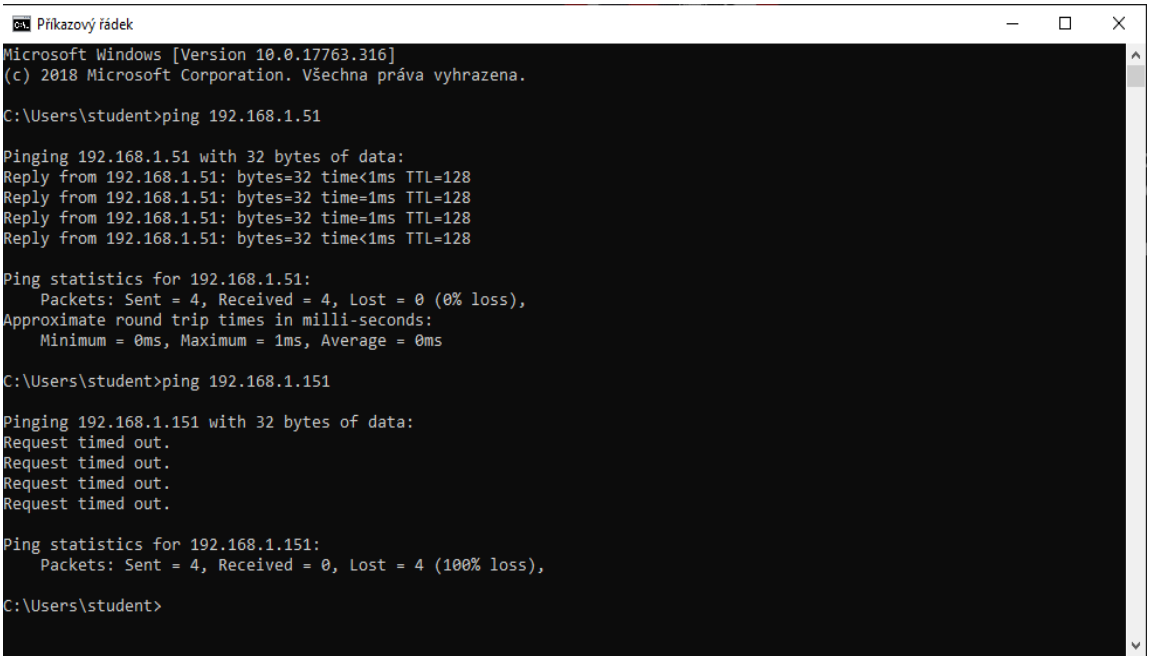
Jak už bylo uvedeno výše, počítače v jiných podsítích mezi sebou nemohou komunikovat. Správnost konfigurace lze tedy snadno ověřit úspěšným navázáním komunikace mezi počítači ve stejné podsíti a neúspěšnou komunikací mezi počítači v různých podsítí.

Tento test lze snadno provést pomocí příkazového řádku a příkazu ping. Ping vyšle dotaz na specifikovanou IP-adresu a čeká, zda mu dané zařízení odpoví.

Z PC 2 by tedy měl tento příkaz vrátit pozitivní hodnoty (odpověď od cílové adresy včetně počtu přenesených bytů a časem přenosu) pokud bude volán PC 1 a negativní hodnoty (tzv „Request timed out.“) pokud bude volán PC 3 nebo PC 4.

Na Obrázku 13 je zobrazen příkazový řádek, kde je z PC 2 (IP adresa: 192.168.1.52) volán nejprve počítač ve stejné podsítí PC 1 (IP adresa: 192.168.1.51) a následně počítač v druhé podsítí PC 3 (IP adresa: 192.168.1.151).

Obrázek 13 – CMD – Test pomocí funkce ping



Zdroj: vlastní

5.2.3 Test přenosové rychlosti uvnitř sítě

K tomuto testu byl využit výše popsaný software TamoSoft Throughput. Test přenosové rychlosti probíhal mezi dvěma stanicemi ve stejné podsíti – PC3 a PC4, které byli propojeny přes switch část gigabitového routeru. V Tabulce 5 jsou zapsány průměrné hodnoty za 60 vteřin měření, které proběhlo celkem desetkrát.

Tabulka 5 – Subnetting – Naměřené hodnoty – rychlost přenosu uvnitř sítě

	TCP		UDP		Lost packets	
	UP [Mb/s]	DOWN [Mb/s]	UP [Mb/s]	DOWN [Mb/s]	UP	DOWN
1	*855,70*	*858,27*	*691,86*	*698,25*	*0,0%*	*0,1%*
2	*854,94*	*860,08*	*695,81*	*691,84*	*0,0%*	*0,0%*
3	*852,58*	*846,85*	*681,53*	*691,65*	*0,0%*	*6,8%*
4	*854,97*	*858,45*	*677,89*	*703,07*	*0,0%*	*4,2%*
5	*856,49*	*853,35*	*678,30*	*699,33*	*0,0%*	*5,8%*
6	*855,73*	*856,27*	*681,74*	*690,89*	*0,0%*	*5,6%*
7	*858,97*	*862,60*	*679,21*	*699,01*	*0,0%*	*4,2%*
8	*858,65*	*857,39*	*689,81*	*691,58*	*0,0%*	*0,0%*
9	*847,19*	*860,10*	*689,71*	*688,57*	*0,0%*	*6,7%*
10	*858,96*	*857,55*	*686,97*	*684,12*	*0,0%*	*4,4%*
Průměr:	**855,42**	**857,09**	**685,28**	**693,83**	**0,00%**	**3,78%**

Zdroj: vlastní

Z tabulky je zřejmé, že naměřené hodnoty přenosových rychlostí TCP a UDP se nijak výrazně nelišily. Což se dalo předpokládat vzhledem k velikosti sítě. TCP se jednoznačně projevil jako rychlejší oproti UDP jak v uploadu, tak v downloadu. Ovšem procenta ztracených paketů se v downloadu značně mění.

Průměrná hodnota uploadu z deseti měření je u TCP 855,42 Mb/s a 857,09 Mb/s při downloadu. U UDP jsou průměrné hodnoty nižší, a to sice 685,28 Mb/s při uploadu a 693,83 Mb/s při downloadu.

5.2.4 Test přenosové rychlosti ven ze sítě

Pro tento test byl využit webový test rychlosti na stránkách www.adsl.cz. Testem lze získat tři základní hodnoty kvality připojení – download (stahování dat), upload (odesílání dat) a ping (rychlost odezvy). Měření proběhlo pětkrát na počítačové stanici PC 1 a pětkrát na počítačové stanici PC 3. Výsledné hodnoty jsou v Tabulce 6.

Tabulka 6 – Subnetting – Naměřené hodnoty – rychlost přenosu ven ze sítě

	PC 1			PC 3		
	Upload [Mb/s]	Download [Mb/s]	Ping [ms]	Upload [Mb/s]	Download [Mb/s]	Ping [ms]
1	49,15	44,94	4	46,20	44,04	4
2	45,10	45,03	4	48,15	45,22	4
3	49,52	43,80	4	50,02	48,13	4
4	47,88	46,01	4	47,30	47,02	4
5	49,53	46,70	4	48,90	44,36	4
Průměr:	**48,24**	**45,30**	**4**	**48,11**	**45,75**	**4**

Zdroj: vlastní

Naměřené hodnoty se po celou dobu měření výrazně nelišily ani na počítačové stanici PC 1 tak na počítačové stanici PC 3. Průměrná hodnota z obou stanic je u uploadu tedy 48,175 Mb/s, u downloadu 45,525 Mb/s. Ping zůstal na 4ms.

5.3 Zapojení VLAN

Při využití VLAN byly využity dva managovatelné switch, které byly navzájem propojeny přes tagovaný port. Na zapojení byl proveden test pomocí funkce ping a měření přenosové rychlosti uvnitř a ven ze sítě. Následně byl proveden i test přenosové rychlosti uvnitř sítě při zapojení pouze s jedním managovatelným switch. Výsledky byly porovnány, aby bylo zjištěno, jestli má propojení dvou switch přes tagovaný port výrazný vliv na přenosovou rychlost.

5.3.1 Zapojení s dvěma managovatelnými switch

V tomto případě byly počítačové stanice rozděleny do dvou VLAN (A, B) s využitím dvou managovatelných switch, které byli propojeny přes tagovaný port. Počítačovým stanicím byla přidělena IP adresa dynamicky od DHCP serveru. Pro zapojení byly využity výše zmíněné gigabitové managovatelné switch.

IP adresy počítačových stanic přidělené DHCP serverem:

PC 1 – *IP adresa:* 192.168.1.105

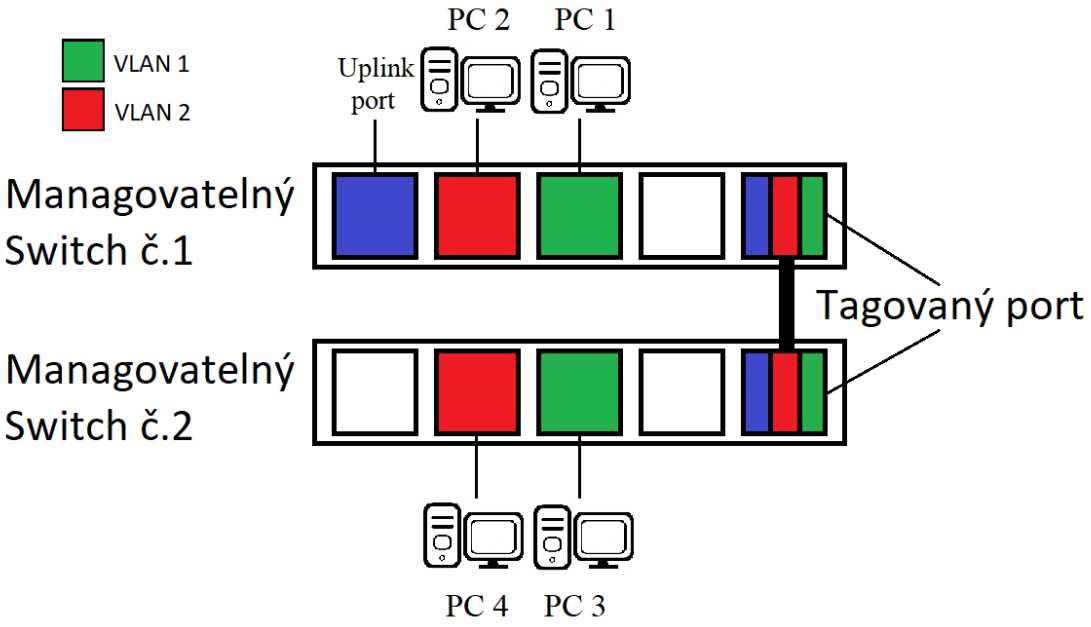
PC 2 – *IP adresa:* 192.168.1.196

PC 3 – *IP adresa:* 192.168.1.193

PC 4 – *IP adresa:* 192.168.1.197

Zapojení je znázorněno na Obrázku 14.

Obrázek 14 – VLAN – Dva managovatelné switch



Zdroj: vlastní

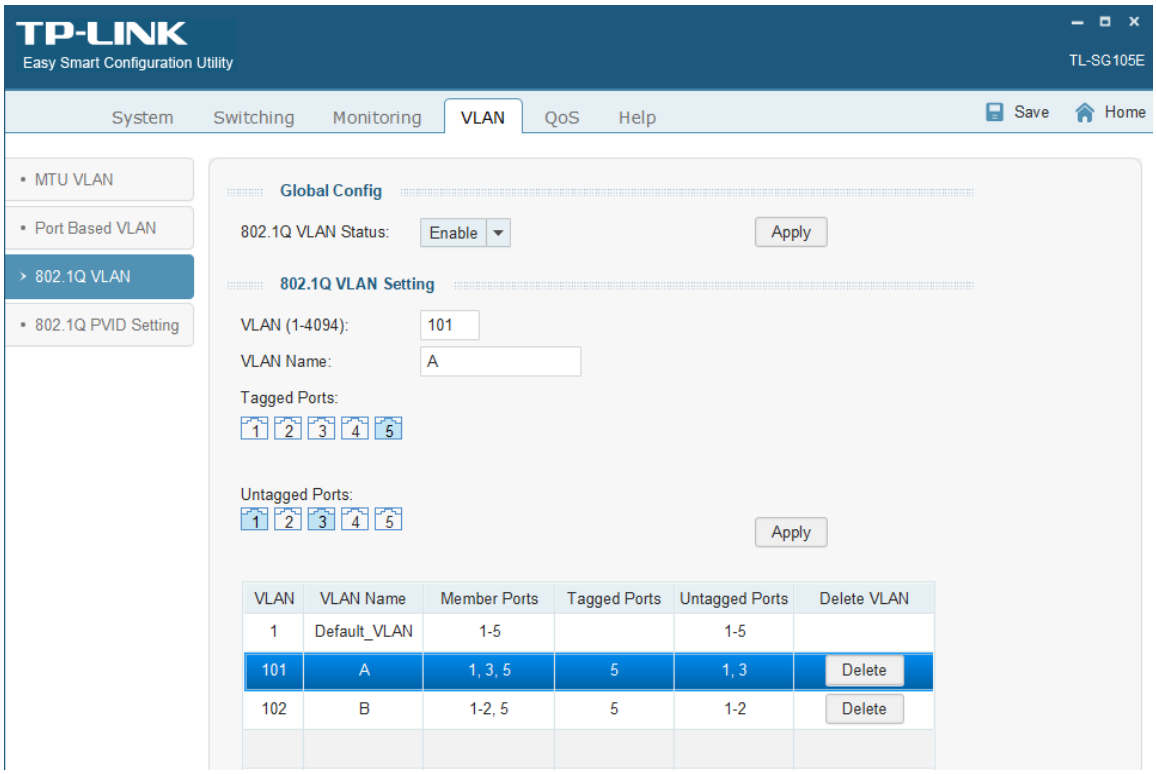
5.3.2 Konfigurace VLAN

Pro konfiguraci byla v příslušné aplikaci využita metoda 802.1Q. Oběma switch byly přiděleny přihlašovací údaje a IP adresy. Managovatelný switch č.1 dostal IP adresu 192.168.1.221 a managovatelný switch č.2 dostal IP adresu 192.168.1.222.

V konfiguraci 802.1Q VLAN bylo pro VLAN A zvoleno číslo 101, jako tagovaný port vybrán port č.5 a jako netagované porty byly vybrány porty č.1 a č.3. Pro VLAN B bylo zvoleno číslo 102, jako tagovaný port byl opět vybrán port č. 5 a jako netagované porty byly vybrány porty č.1 a č.2. V konfiguraci PVID Setting byl port č.2 přidělen do PVDI 102 a port č.3 do PVID 101, aby byla zachována konektivita na obou VLAN port č.1 nebyl přidělen ani do jedné VLAN.

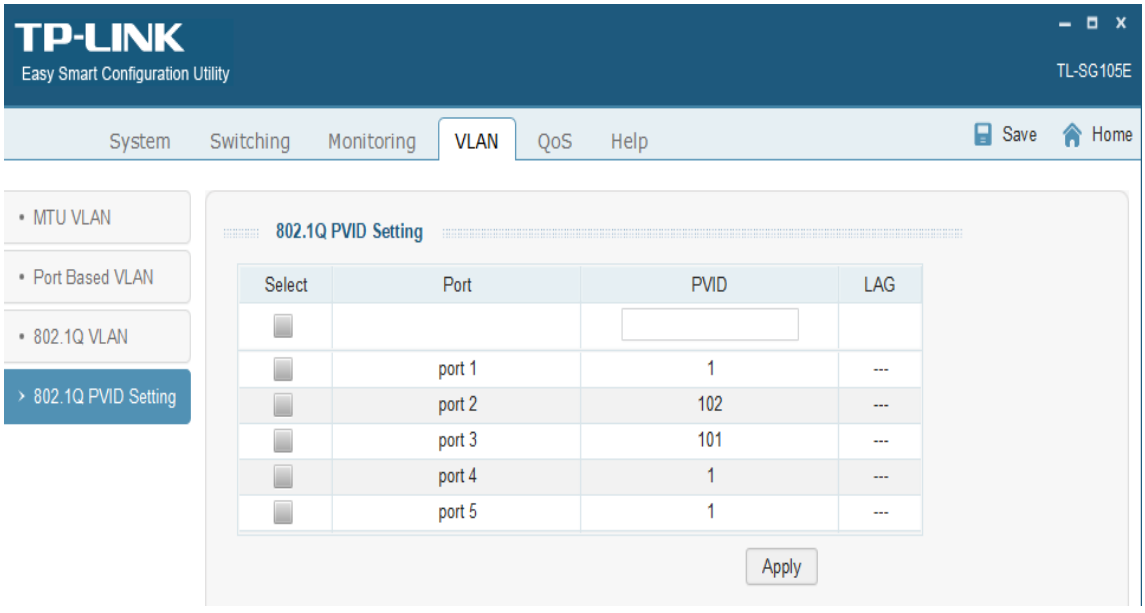
Oba managovatelné switch byly nakonfigurovány totožně. Nastavení 802.1Q VLAN pro VLAN A je zobrazeno na Obrázku 15 a 802.1Q PVID Setting je zobrazeno na Obrázku 16.

Obrázek 15 – Konfigurace – 801.1Q VLAN



Zdroj: vlastní

Obrázek 16 – Konfigurace – 801.1Q PVID Setting

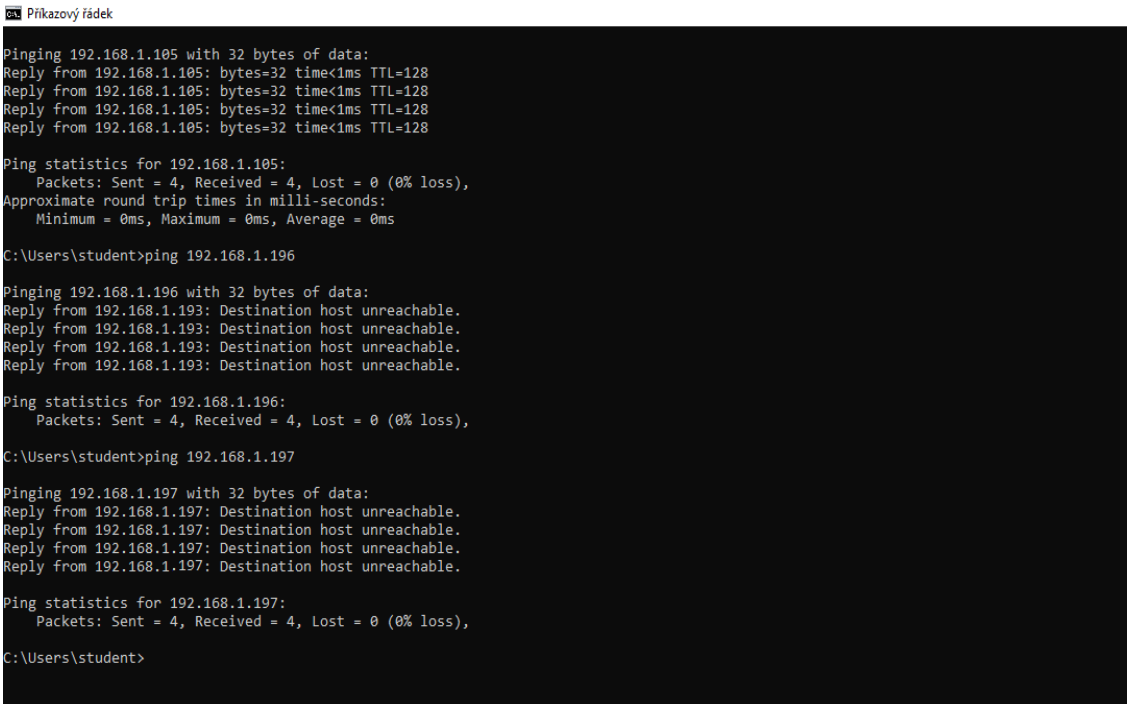


Zdroj: vlastní

5.3.3 Test pomocí funkce ping

Správnost konfigurace byla opět ověřena pomocí příkazového řádku a funkce ping. Na Obrázku 17 je zobrazen příkazový řádek, kde je z počítačové stanice PC 3 (IP adresa 192.168.1.193) volána počítačová stanice PC 1 (IP adresa 192.168.1.105), která se nachází ve stejné VLAN, tudíž dostává pozitivní hodnoty (odpověď od cílové adresy včetně počtu přenesených bytů a časem přenosu). Následně je z té samé počítačové stanice volán PC 2 (IP adresa 192.168.1.196) a PC 4 (IP adresa 192.168.1.197) od kterých dostává negativní hodnoty („Reply from 192.168.1.193 / 197: Destination host unreachables“), protože se nacházejí v jiné VLAN.

Obrázek 17 – VLAN – Test pomocí funkce ping



Zdroj: vlastní

5.3.4 Test přenosové rychlosti uvnitř sítě

K zjištění přenosové rychlosti byl opět využit software TamoSoft Throughput, který byl spuštěn na dvou počítačových stanicích zapojených do jedné VLAN. Test probíhal desetkrát po dobu 60 vteřin. Průměrné naměřené hodnoty jsou v Tabulce 7.

Tabulka 7– VLAN (dva switch) – Naměřené hodnoty – rychlost přenosu uvnitř sítě

	TCP		UDP		Lost packets	
	UP [Mb/s]	**DOWN [Mb/s]**	**UP [Mb/s]**	**DOWN [Mb/s]**	**UP**	**DOWN**
1	*860,09*	*858,68*	*695,33*	*711,01*	*0,0%*	*0,1%*
2	*853,86*	*868,58*	*696,88*	*710,80*	*0,0%*	*0,2%*
3	*863,99*	*864,03*	*695,23*	*710,84*	*0,0%*	*0,0%*
4	*859,18*	*866,14*	*700,94*	*706,78*	*0,0%*	*0,1%*
5	*857,78*	*885,91*	*699,52*	*712,35*	*0,2%*	*0,0%*
6	*855,23*	*873,12*	*698,13*	*709,89*	*0,0%*	*0,1%*
7	*856,75*	*877,38*	*696,44*	*711,27*	*0,0%*	*0,0%*
8	*859,34*	*880,01*	*697,61*	*712,68*	*0,0%*	*0,2%*
9	*861,45*	*882,26*	*700,31*	*709,93*	*0,0%*	*0,1%*
10	*859,06*	*869,38*	*696,36*	*710,87*	*0,0%*	*0,0%*
Průměr:	**858,67**	**872,55**	**697,68**	**710,64**	**0,02%**	**0,08%**

Zdroj: vlastní

Z naměřených hodnot si lze povšimnout, že TCP se opět projevil v uploadu i v downloadu jako rychlejší než UDP. Procenta ztracených paketů byli však takřka nulová, ani při jednom měření nebyly vyšší než 0,2 %.

Průměrná hodnota uploadu u TCP je 858,67 Mb/s a u downloadu 857,09 Mb/s. Pomalejší UDP má průměrný upload 697,68 Mb/s a download 710,64 Mb/s.

5.3.5 Test přenosové rychlosti ven ze sítě

Na stránkách www.adsl.cz byly opět naměřeny tři základní hodnoty kvality připojení – download, upload a ping. Měření proběhlo pětkrát na počítačové stanici PC 1 a pětkrát na počítačové stanici PC 4. Výsledné hodnoty jsou v Tabulce 8.

Tabulka 8– VLAN – Naměřené hodnoty – rychlost přenosu ven ze sítě

	PC 1			PC 4		
	Upload [Mb/s]	Download [Mb/s]	Ping [ms]	Upload [Mb/s]	Download [Mb/s]	Ping [ms]
1	49,03	48,94	4	48,15	47,56	4
2	49,29	48,47	4	49,55	48,36	4
3	48,61	44,25	4	50,01	48,45	4
4	50,58	49,65	4	47,42	45,05	4
5	45,87	43,25	4	47,95	46,47	4
Průměr:	**48,68**	**46,91**	**4**	**48,62**	**47,18**	**4**

Zdroj: vlastní

Hodnoty se nijak výrazně nelišily na počítačové stanici PC 1 ani na počítačové stanici PC 4. Průměrná hodnota z obou stanic vyšla u uploadu 48,65 Mb/s a u downloadu 47,045 Mb/s. Ping zůstal po celou dobu měření na 4ms.

5.3.6 Přenosvá rychlost uvnitř sítě v zapojení s jedním managovatelným switch

V tomto zapojení byly dvě počítačové stanice PC 3 a PC 4 zapojeny do jednoho managovatelného switch bez jakékoliv konfigurace, protože managovatelný switch při spuštění vytváří na všech portech VLAN číslo 1.

Na takto zapojené síti bylo pomocí softwaru TamoSoft Throughput změřena přenosová rychlost mezi těmito dvěma počítačovými stanicemi. Výsledné hodnoty jsou v Tabulce 9.

V tom to zapojení je průměrná hodnota uploadu u TCP 843,24 Mb/s a u downloadu 844,88 Mb/s. U UDP byl naměřen průměrný upload 697,48 Mb/s a download 710,32 Mb/s.

Z naměřených hodnot je zřejmé, že přenosová rychlost mezi počítačovými stanicemi není nijak výrazně zpomalena při zapojení s využitím dvou managovatelných switch do sebe. Dokonce se projevila ve výsledných hodnotách jako rychlejší. U TCP byli rozdíly minimální a u UDP takřka totožné. Pro běžné uživatele jsou tyto minimální rozdíly přenosových rychlostí zanedbatelné.

Tabulka 9 – VLAN (jeden switch) – Naměřené hodnoty – rychlost přenosu uvnitř sítě

	TCP		UDP		Lost packets	
	UP [Mb/s]	**DOWN [Mb/s]**	**UP [Mb/s]**	**DOWN [Mb/s]**	**UP**	**DOWN**
1	*847,50*	*839,94*	*700,80*	*712,19*	*0,0%*	*0,0%*
2	*835,72*	*840,02*	*685,45*	*713,89*	*0,0%*	*0,0%*
3	*850,23*	*843,96*	*697,72*	*713,04*	*0,0%*	*0,3%*
4	*839,86*	*838,42*	*700,30*	*717,33*	*0,0%*	*0,0%*
5	*834,61*	*851,27*	*696,75*	*714,89*	*0,0%*	*0,0%*
6	*857,55*	*855,75*	*700,81*	*712,28*	*0,0%*	*0,1%*
7	*847,63*	*858,71*	*693,99*	*712,28*	*0,0%*	*0,2%*
8	*836,44*	*839,48*	*699,95*	*697,17*	*0,0%*	*0,1%*
9	*837,94*	*833,16*	*695,59*	*712,51*	*0,0%*	*0,1%*
10	*844,91*	*848,04*	*703,43*	*697,66*	*0,2%*	*0,0%*
Průměr:	**843,24**	**844,88**	**697,48**	**710,32**	**0,02%**	**0,08%**

Zdroj: vlastní

5.4 Zhodnocení naměřených výsledků

Při pohledu na získané hodnoty z měření přenosové rychlosti uvnitř sítě je zřejmé že výsledky se nijak výrazně nelišily ani při jednom zapojení. U TCP se upload pohyboval vždy v rozmezí 834 Mb/s až 861 Mb/s a download v rozmezí 833 Mb/s až 885 Mb/s. UDP se ve všech měření projevilo jako pomalejší, upload se pohyboval v rozmezí 681 Mb/s až 717 Mb/s. Za zmínku ale stojí procenta ztracených paketů. Při použití VLAN nepřekročily 0,3 %, ale u subnettingu stoupaly hodnoty i až na 6,8 %. Zásadní vliv na měření měla samozřejmě minimální velikost sítě.

I při měření přenosové rychlosti ven ze sítě se hodnoty v podstatě opět nelišily ani v jednom zapojení. Upload se pohyboval v rozmezí 47 Mb/s až 51 Mb/s, download v rozmezí 43 Mb/s až 49 Mb/s a ping zůstal na 4ms.

Pro běžného uživatele by tak rozdílné hodnoty byly naprosto nepodstatné. Z hlediska přenosové rychlosti se tedy neprojevila ani jedna metoda jako úspěšnější.

6. Závěr

Cílem práce bylo porovnat a posoudit vhodnost nasazení VLAN v komerčních počítačových sítích v alternaci s možností subnettingu. Z teoretického hlediska se jeví obě metody velice odlišně, hlavně z pohledu jejich principu fungování, konfigurace a financí. Z praktického hlediska, ale byly naměřené výsledky přenosové rychlosti v podstatě totožné, výrazné změny byly pouze v procentech ztracených paketů. U VLAN byla procenta ztracecných paketů takřka nulová, naopak u subnetingu procenta stoupala až do 6-7%.

Subnetting, nebo CIDR pracují v podstatě na stejném základě. Jedná se o softwarové rozdělení sítě na podsítě za pomoci správného nastavení statické IP adresy a masky sítě u všech zařízení. Výhodami této metody je, že k vytvoření podsítě není zapotřebí žádný další aktivní prvek a spolehlivost fungování. Naopak nevýhodou se může jevit složitost určení IP adresy, výpočtu masky sítě a faktu, že při přidání nebo odebrání podsítě nebo zařízení může dojít ke složitému překonfigurování celé sítě, včetně všech zařízení do ní připojených.

Naopak u VLAN je vždy zapotřebí další aktivní prvek, který provádí rozdělení sítě. Samotná konfigurace sítě pak probíhá v jednoduché uživatelské aplikaci. Za výhody VLAN může být považována jednodušší konfigurace, větší flexibilita zapojení a fakt, že služba VLAN probíhá na nižší druhé síťové vrstvě a tudíš managovatelný switch rovnou adresuje datové pakety do podsítí, kam jsou určeny. Jako nevýhoda se může jevit nutnost pořízení dalšího dražšího aktivního prvku.

Pokud pomineme tuto finanční nevýhodu, lze VLAN považovat za výhodnější ve všech ohledech. Subnetting má jistě stále své opodstatnění a řadu využití, ale na větších a komplikovanějších sítích se více uplatní větší flexibilita konfigurace a jednodušší spravování VLAN.

7. Reference

1. **Kurose F. James, Ross W. Keith.** *Počítačové sítě.* Brno : Computer Press, 2014. 978-80-251-3825-0.

2. **Sochor, Tomáš.** *Počítačové sítě II.* Ostrava : Ostravská univerzita v Ostravě, 2009.

3. **Peterka, Jiří.** Síťový model TCP/IP. *eArchiv.cz.* [Online] 1992. [Citace: 3. únor 2019.] http://www.earchiv.cz/a92/a231c110.php3.

4. —. LAN vs. WAN. *eArchiv.cz.* [Online] 1996. [Citace: 18. Prosinec 2018.] http://www.earchiv.cz/a96/a615k150.php3.

5. **doc. RNDr. Eva Hladká, Ph.D., Mgr. Jan Fousek.** Lokální sítě (LAN). *Základy IT gramotnisti .* [Online] [Citace: 28. Listopad 2018.] https://is.muni.cz/do/ics/el/sitmu/law/html/lokalni-site-lan.html.

6. **Odom, Wendell.** *Počítačové sítě bez předchozích znalostí.* Brno : CP Books, a.s., 2005. 80-251-0538-5.

7. **Shinder, Debra Littlejohn.** *Počítačové sítě.* Praha : SoftPress, 2003. 80-86497-55-0.

8. **Bouška, Petr.** Co je network a subnet (síť a podsíť). *SAMURAJ-cz.* [Online] 5. září 2007. [Citace: 25. Listopad 2018.] https://www.samuraj-cz.com/clanek/tcpip-adresy-masky-subnety-a-vypocty/.

9. **Peterka, Jiří.** Brouter, gateway. *eArchvi.cz.* [Online] 1993. [Citace: 26. Listopad 2018.] http://www.earchiv.cz/a93/a343c120.php3.

10. **Votruba, Zdeněk.** Online záznam přednášky. *Adresace sítě – AV záznam z 2.přednášky.* Praha : autor neznámý, 2018.

11. **Vozňák, Daniel.** Jak funguje a k čemu slouží DHCP. *eABM.* [Online] 26. leden 2017. [Citace: 14. únor 2019.] http://blog.eabm.cz/jak-funguje-a-k-cemu-slouzi-dhcp/.

12. **Peterka, Jíři.** Supernetting. *eArchiv.cz.* [Online] 1999. [Citace: 15. únor 2019.] http://www.earchiv.cz/anovinky/ai1681.php3.

13. **Bouška, Petr.** Adresy a jejich výpočty v počítačových sítích založených na TCP/IP. *SAMURAJ-cz.* [Online] 21. červenec 2010. [Citace: 26. listopad 2018.] https://www.samuraj-cz.com/clanek/adresovani-v-ip-sitich/.

14. —. Síťové třídy. *SAMURAJ-cz.* [Online] 21. červenec 2010. [Citace: 12. Prosinec 2018.] https://www.samuraj-cz.com/clanek/adresovani-v-ip-sitich/.

15. **Peterka, Jiří.** CIDR, alias; Classless InterDomain Routing. *eArchiv.cz.* [Online] 1996. [Citace: 12. prosinec 2018.] http://www.earchiv.cz/anovinky/ai1681.php3.

16. **Lammle, Todd.** *CCNA - Výukový průvodce přípravou na zkoušku.* Praha : Computer Press, 2010. 978-80-251-2359-1.

17. **Votruba, Zdeněk.** Online záznam přednášky. *VLAN – TGT26Z přednáška VLAN.* Praha : autor neznámý, 2018.

18. **Bouška, Petr.** Co je to VLAN. *SAMURAJ-cz.* [Online] 2. červen 2007. [Citace: 12. únor 2019.] https://www.samuraj-cz.com/clanek/vlan-virtual-local-area-network/.