Návrh firemní sítě v Packet Traceru pro středně velkou firmu

Lukáš Králík

Bakalářská práce
2017

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2016/2017

ZADÁNÍ BAKALÁŘSKÉ PRÁCE
(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Lukáš Králík**
Osobní číslo:	**A14247**
Studijní program:	**B3902 Inženýrská informatika**
Studijní obor:	**Informační technologie v administrativě**
Forma studia:	**prezenční**
Téma práce:	**Návrh firemní sítě v Packet Traceru pro středně velkou firmu**
Téma anglicky:	**A Draft Corporate Network in Packet Tracer for a Mid-sized Company**

Zásady pro vypracování:

1. **Zpracujte literární rešerši na dané téma.**
2. **Nakonfigurujte v prostředí Cisco Packet Traceru počítačovou síť pro středně velkou firmu.**
3. **Pro konfiguraci aktivních prvků použijte VLSM, VLAN, VTP a STP protokoly.**
4. **Na hraničním směrovači nakonfigurujte OSPF směrovací protokol.**
5. **Firemní síť zabezpečte na hraničním směrovači pomocí ACL.**
6. **Ve firemní síti nakonfigurujte webový server a IP telefonii.**

Rozsah bakalářské práce:

Rozsah příloh:

Forma zpracování bakalářské práce: **tištěná/elektronická**

Seznam odborné literatury:

1. **LAMMLE, Todd. CCNA: výukový průvodce. Vyd. 1. Brno: Computer Press, 2015. 1016 s. ISBN 978-80-251-4602-6.**
2. **WALLACE, Kevin. Cisco VoIP: autorizovaný výukový průvodce. Vyd. 1. Brno: Computer Press, 2009. Samostudium. 528 s. ISBN 978-80-251-2228-0.**
3. **EMPSON, Scott. CCNA kompletní přehled příkazů: autorizovaný výukový průvodce. Vyd. 1. Brno: Computer Press, 2009. 336 s. ISBN 978-80-251-2286-0.**
4. **CARROLL, Brandon. Bezdrátové sítě Cisco: autorizovaný výukový průvodce. Vyd. 1. Brno: Computer Press, 2011. 480 s. ISBN 978-80-251-2884-8.**
5. **ODOM, Wendell, Rus HEALY a Naren MEHTA. Směrování a přepínání sítí: autorizovaný výukový průvodce. Vyd. 1. Brno: Computer Press, 2009. 879 s. ISBN 978-80-251-2520-5.**

Vedoucí bakalářské práce: **Ing. Miroslav Matýsek, Ph.D.**
Ústav počítačových a komunikačních systémů

Datum zadání bakalářské práce: **3. února 2017**

Termín odevzdání bakalářské práce: **30. května 2017**

Ve Zlíně dne 3. února 2017

doc. Mgr. Milan Adámek, Ph.D.
děkan

Ing. Miroslav Matýsek, Ph.D.
ředitel ústavu

Prohlašuji, že

- beru na vědomí, že odevzdáním diplomové/bakalářské práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že diplomová/bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk diplomové/bakalářské práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně a jeden výtisk bude uložen u vedoucího práce;
- byl/a jsem seznámen/a s tím, že na moji diplomovou/bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – diplomovou/bakalářskou práci nebo poskytnout licenci k jejímu využití jen připouští-li tak licenční smlouva uzavřená mezi mnou a Univerzitou Tomáše Bati ve Zlíně s tím, že vyrovnání případného přiměřeného příspěvku na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše) bude rovněž předmětem této licenční smlouvy;
- beru na vědomí, že pokud bylo k vypracování diplomové/bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky diplomové/bakalářské práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem diplomové/bakalářské práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

- že jsem na diplomové/bakalářské práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně, dne 29.5.2017

.....
podpis diplomanta

ABSTRAKT

Práce je zaměřena na tvorbu počítačové sítě středně velkého rozsahu v simulačním prostředí Packet Tracer, výhradně pomocí Cisco IOS a aktivních prvků společnosti Cisco na úrovni CCNA. První část popisuje operační systém od firmy Cisco, základní tvorbu podsítí s IP adresací. Dále se řeší směrování v sítích, tvorba VLAN, zabezpečení pomocí ACL a IP telefonie. Druhá část se zabývá tvorbou počítačové sítě pro fiktivní středně velkou firmu a konfigurací všech aktivních prvků v dané síti spolu s IP telefony. Práce taktéž obsahuje kompletní nastavení, které bylo použito pro konfiguraci aktivních prvků.

Klíčová slova: Cisco, VLSM, Vlan, Směrování, ACL, VoIP

ABSTRACT

The work is focused on the creation of mid-sized computer network in the Packet Tracer simulation environment, exclusively using Cisco IOS and active devices from Cisco company on the CCNA level. The first part describes the Cisco operating system, the basic subnetting with IP adressing. The next is solution of network routing, creation of VLAN, ACL security and IP telephony. The second part describes the creation of a computer network for a fictitious mid-sized company and configuration of active devices in the network together with IP phones. The work also contains the complete settings that were used to configure the all active devices.

Keywords: Cisco, VLSM, Vlan, Routing, ACL, VoIP

Poděkování:

Rád bych touto cestou poděkoval Ing. Miroslavu Matýskovi, PhD. Za cenné rady a připomínky, při zpracování mé bakalářské práce. Velké díky patří rodičům, kteří nade mnou nezlomili hůl, podporovali mě ve studiu a především babičce, které jsem dělal společnost každý víkend po celou dobu mého studia ve Zlíně. Rád bych, taky vyzdvihl připomínky Ing. Lukáše Urbančoka, o tom jak počítačové sítě fungují v praxi.

"*You, me, or nobody is gonna hit as hard as life, but it ain't about how hard you hit, it's about how hard you can get hit and keep moving forward, how much you can take and keep moving forward. That's how winning is done*" (Rocky Balboa, Sylvester Stallone)

Prohlašuji, že odevzdaná verze bakalářské/diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

OBSAH

ÚVOD

Hlavním cílem této práce je vytvoření počítačové sítě pro středně velkou firmu. Nejdříve je však nutné pochopit jak počítačové sítě pracují především z pohledu Cisco, jelikož tato síť kompletně využívá aktivní prvky a konfigurace od této společnosti. Síť je navržena tak, aby byly splněny všechny zásady pro zpracování, a aby odpovídala skutečnému nastavení, které se v praxi využívá.

Práce se dělí na dvě části. V první části se popisuje Cisco IOS, který se využívá na přepínačích a směrovačích. Následně je vysvětlena tvorba podsítí, především pomocí VLSM. Dále je popsáno, jak se řeší směrování v počítačových sítích a které protokoly jsou vhodné pro nasazení v menších či větších sítích. Důležitý je popis Spanning tree protokolu, který popisuje smyčky, které mohou nastat při zapojení tří a více přepínačů dohromady. V neposlední řadě se řeší zabezpečení sítě a filtrování packetů pomocí ACL. Jako poslední jsou popsány virtuální sítě VLAN a technologie VoIP, která se často využívá ke komunikaci ve firemním prostředí.

Druhá část popisuje tvorbu počítačové sítě. Řeší se VLSM adresace stanic pro zaměstnance, dále adresace VoIP telefonů a ostatní IP adresy, které jsou použity jak v dané síti tak i mimo ní v Internetu. Dále je práce zaměřena především na to jak daná síť funguje tím se, nemyslí jednotlivá konfigurace, ale již to jak síť funguje v ostrém provozu. Popisují se tu především přiložené obrázky, které mapují funkčnost již nastavených aktivních prvků, koncových stanic a serverů. V příloze jsou pak uvedeny veškeré konfigurace, které byly použity pro nastavení aktivních prvků.

I. TEORETICKÁ ČÁST

1 SYSTÉM CISCO IOS

Jedná se o jádro operačního systému společnosti Cisco, které je zakomponované do aktivních prvků, jenž nám umožňují, směrování, přepínání a celkovou komunikaci v počítačových sítích. První verzi tohoto systému vytvořil pan William Yeager roku 1986, která sloužila pro provoz síťových aplikací. Operační systém je nejčastěji využíván na směrovačích Cisco, ale i na přepínačích např. typu Catalyst 2960 a 3560.

Hlavní funkce Cisco IOS směrovačů:

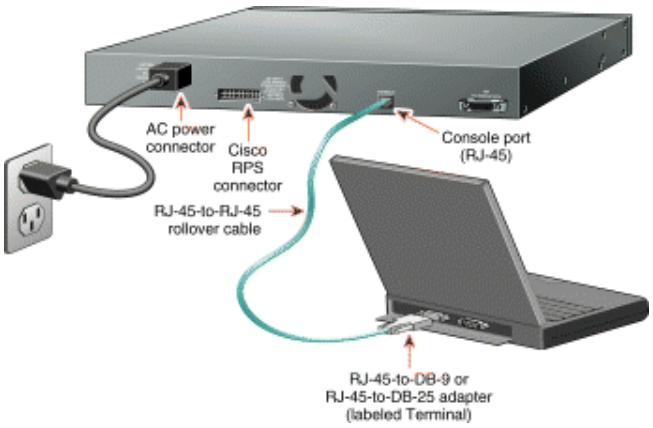
- Aktivace síťových protokolů.
- Vytváří propojení mezi zařízeními.
- Poskytuje zabezpečení proti neoprávněné manipulaci.
- Zajišťuje škálovatelnost a lepší redundanci sítě při její rozšiřování [1].

1.1 Připojení k zařízení s Cisco IOS

Aby se aktivní prvek mohl konfigurovat, je potřeba nejprve navázat spojení. Existuje několik možností jak se připojit k danému zařízení. Buďto fyzicky nejčastěji pomocí konzole, která má port RJ-45, případně webovým rozhraním, ale taky virtuálně sadou protokolů SSH a Telnet [2].

1.1.1 Port konzole

Jde o propojení PC a aktivního prvku pomocí rollover cable. Do aktivního prvku je připojen port RJ-45, jenž je většinou umístěn na zadní straně daného zařízení a na straně PC je zapojen do portu COM [2].



Obr. 1. Schéma zapojení konzole [3].

1.1.2 Webové rozhraní

Tato volba umožňuje konfiguraci a monitoring přes vnitřní zabudované rozhraní. Je nutné mít nainstalovaný IOS, který podporuje toto rozhraní a mít ho povolené. Následně můžeme volit mezi nezabezpečeným protokolem HTTP případně zabezpečeným HTTPS [2].

1.1.3 Protokol SSH

Tento protokol slouží pro šifrovanou komunikaci po síti. Primární funkcí SSH je vytvoření vzdáleného shellu, který umožňuje následnou konfiguraci aktivního prvku. SSH nahrazuje zastaralý protokol Telnet, který není šifrovaný. Pro správné navázaní spojení je však nutné použít externí program typu Putty, jenž je volně dostupný a zajišťuje kompletní vytvoření příkazové řádky [4].

1.1.4 Protokol Telnet

Jedná se o zcela nezabezpečený protokol. Nemá žádnou vlastnost šifrování či ochranu hesel. Veškerá komunikace přes tento protokol je jednoduchá pro zachycení a zcela čitelná. Nedoporučuje se při konfiguraci Cisco zařízení používat tento protokol, jako alternativu je vhodné zvolit výše zmíněný SSH. Pro správné nastavení je potřeba taktéž použít program typu Putty [4].

1.2 Režimy Cisco zařízení

Práce v Cisco IOS zahrnuje celkem tři režimy, které slouží k získávání informací, konfiguraci a ověřování daného nastavení. Konfigurace probíhá pomocí příkazové řádky, která ovlivňuje uživatelský režim, privilegovaný režim a režim globální konfigurace [5].

1.2.1 Uživatelský režim

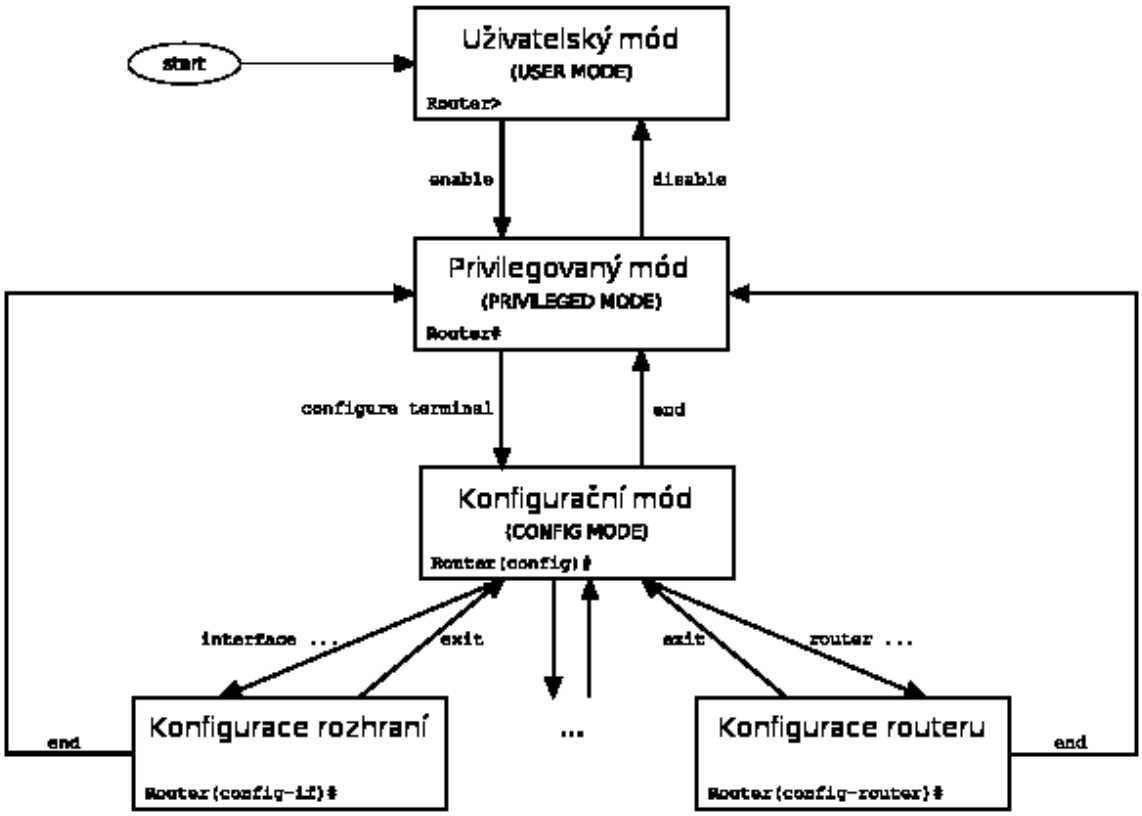
Jedná se o nejnižší stupeň v této hierarchii, je zde povoleno minimum příkazů, které nemají vliv na nastavení aktivního prvku, jde především o příkazy pro sledování. Do tohoto módu se dostaneme ihned po připojení k danému zařízení, tento režim slouží jako vstupní brána k další konfiguraci [1].

1.2.2 Privilegovaný režim

Jde o druhý stupeň této hierarchie. Pokud se chceme dostat do tohoto režimu z uživatelského, musí se zadat příkaz *„enable“*. Zde je přístup k ostatním příkazům aktivního prvku a je možné zde vykonávat práci se soubory. V tomto módu je často nutné ukládat danou konfiguraci příkazem *„copy running-config startup config“*, jenž uloží provedené nastavení, které bude k dispozici při dalším spuštění směrovače [1].

1.2.3 Režim globální konfigurace

Nejvyšší stupeň této hierarchie. Do tohoto režimu se dostaneme příkazem „*configure terminal*“, zde již probíhá veškerá konfigurace, která ovlivňuje celý systém. Při zadávání příkazu dochází k okamžitému přepsání hodnot v nastavení [1].



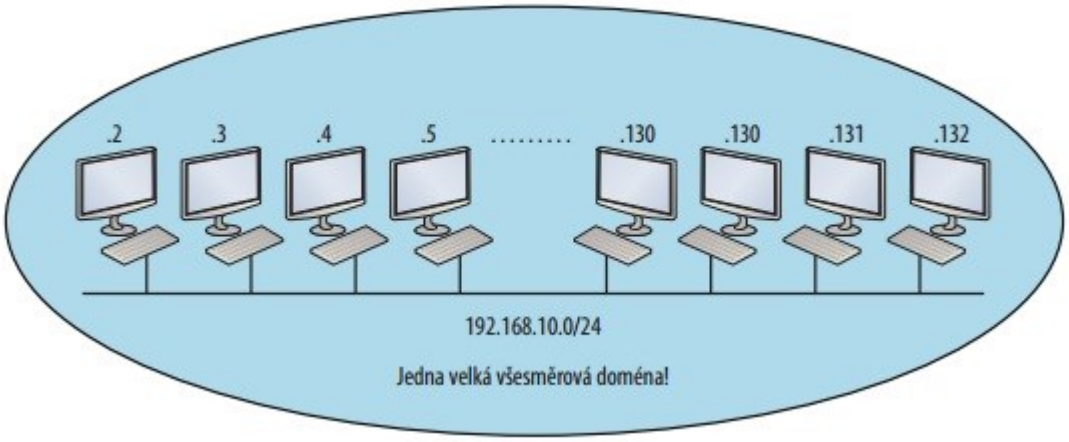
Obr. 2. Přehled uživatelských režimů [6].

2 ZÁKLADY TVORBY PODSÍTÍ

2.1 Počítačová síť

Aby vznikla počítačová síť, musí k tomuto účelu sloužit minimálně dvě, někdy tři zařízení, které jsou spolu navzájem propojené a jejichž hlavní náplni je přenášet a sdílet informace. Spojení je navázáno pomocí optických kabelů, kroucené dvoulinky či bezdrátově [7].

Dnes se nejčastěji setkáme se sítí, která je založena na technologii Ethernetu. Aby se dalo komunikovat v těchto sítích, využívá se protokol TCP/IP. Tento protokol přidělí IP adresy ve formátu IPv4 a IPv6, které slouží pro identifikaci zařízení v dané síti [8].



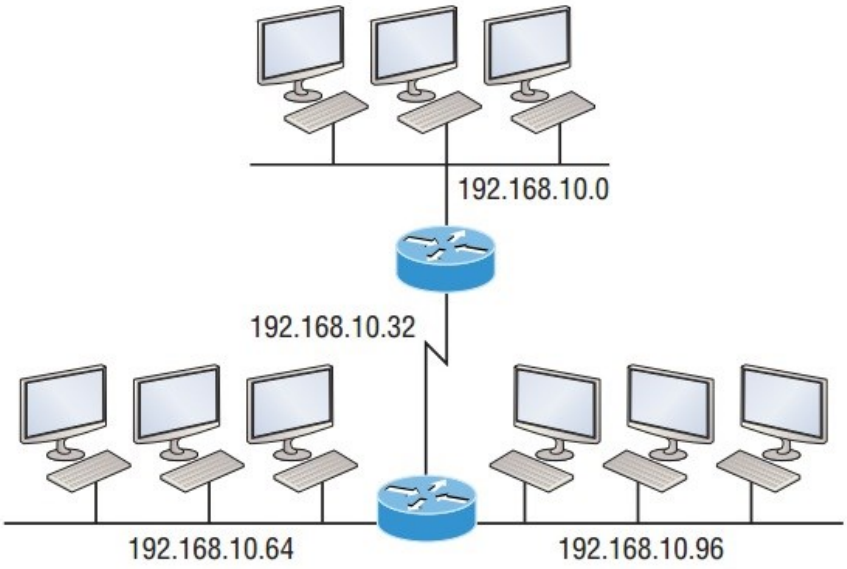
Obr. 3. Jedna síť [1].

2.1.1 Podsíť

Podsítě jsou tvořeny z důvodu dělení na menší lépe upravovatelné celky, které se identifikují protokolem IP. Protokol IP přidělí dané podsítí určitý rozsah adres, který je možné uplatnit pouze v této podsíti.

Důvody dělení na podsítě:

- Problémy, které vzniknou v dané podsítí, jsou omezené a neovlivní tak okolní sítě.
- Větší bezpečnost sítě.
- Menší náročnost, na CPU směrovačů.
- Dělení na celky usnadní budoucí práci [9].



Obr. 4. Rozdělení na podsítě [1].

2.1.2 Maska podsítě

Pomocí masky podsítě se určuje, která část IP adresy je síťová a která je určená pro cílové zařízení v síti. Network ID je hodnota v dekadické či binární soustavě, která je stále stejná pro danou síť a nemění se. Host ID je adresa, jenž se mění a je přiřazena každému hostovi v dané síti [8].

Třída	Formát	Výchozí maska podsítě
A	*síť.uzel.uzel.uzel*	255.0.0.0
B	*síť.síť.uzel.uzel*	255.255.0.0
C	*síť.síť.síť.uzel*	255.255.255.0

Obr. 5. Výchozí masky podsítí [1].

2.2 Beztřídní směrování CIDR

Z důvodů vyčerpání veřejných IP adres muselo dojít k řešení, které by tomuto způsobu zamezilo. Jedna z možností jak tomuto zabránit je zavedení IPv6, který používá 128 bitový prostor pro adresu. Přechod na tento protokol, ale není vůbec jednoduchý a místo toho poskytuje řešení beztřídní směrování mezi doménami (CIDR). Sítě, které jsou tvořeny touto metodou, se nazývají „*slash x*“ z důvodu dělení lomítkem za IP adresou. Význam CIDRu je ten, že pracujeme se všemi adresami bývalých tříd A, B a C rovnocenně.

Síť má tvar například 192.168.1.0/24 lomítko s hodnotou 24 udává, že 24 bitů slouží pro identifikaci sítě a 8 bitů je vyčleněno pro koncové hostitele. Při tvorbě třídních adres to znamená síť třídy C [7].

Pokud ovšem chceme pracovat s CIDR notaci na zařízeních Cisco musíme mít na paměti, že teoreticky se dá dosáhnout maximální hodnoty /32, jelikož IP adresa je rozdělena do čtyř oktetů po osmi bitech. Prakticky jde dosáhnout maximální hodnoty /30 [1].

2.2.1 Příklad tvorby podsítě adresy typu C

Adresa typu C nabývá velikosti 8 bitů pro koncové uživatele. Velikost prefixů, které lze u třídy C použít jsou v rozsahu od /24-/30.

Máme síťovou adresu 192.168.10.0/25

Maska sítě je 255.255.255.128

1. Jaká je velikost podsítí? Hodnota 128 má zapnutý pouze jeden bit to znamená $2^1 = 2$
2. Kolik je hostitelů v dané podsítí? Zde je vypnuto 7 bitů to znamená, že dostaneme $2^7 = 128$, ale musíme brát v potaz, že vždy odečítáme velikost bloku o 2. Celkem lze, získat 126 hostů. Nepočítá se totiž s adresou podsítě a všesměrovou adresou.
3. Jaký je platný rozsah podsítě? Máme 2 podsítě, z nichž každá má 126 hostů.
4. Jaká je všesměrová adresa podsítě? Jedná se o poslední použitelnou adresu dané podsítě. Slouží pro všesměrové vysílání u první podsítě, nabývá hodnoty 127 [1].

Tab. 1. Tabulka rozsahu podsítí [1].

Podsíť	**0**	**128**
První hostitel	1	129
Poslední hostitel	126	254
Všesměrové vysílání	127	255

2.3 VLSM

VLSM je způsob, kterým lze pracovat s maskami podsítí s proměnnou délkou. Tyto masky dokážou pracovat se směrovacími protokoly jako EIGRP, OSPF a RIP verze 2. Hlavní výhodou tohoto způsobu práce s maskami je, že se ekonomicky používá prostor pro adresy IP. Menší nevýhodou je nefunkčnost VLSM se starším směrovacím protokolem RIP verze 1, jelikož tento protokol nepodporuje ukládání informací o podsítích [1].

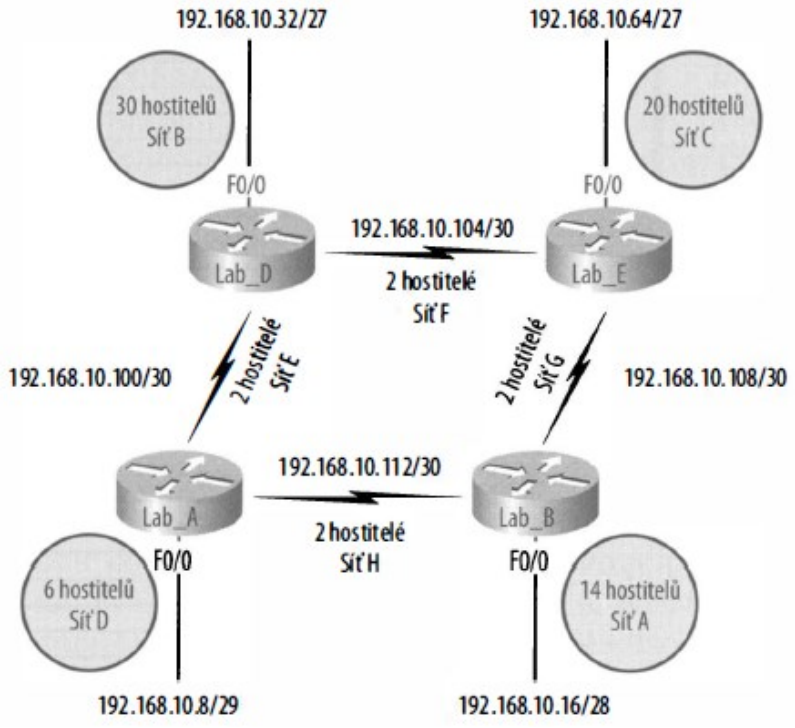
2.3.1 Implementace VLSM

Abychom vhodně implementovali VLSM je nejdříve nutné pochopit, jak pracují tyto masky v sítích třídy C. Pro lepší pochopení, slouží tabulka přiložená níže.

Tab. 2. Velikost bloků [1].

Prefix	Maska	Hostitelé	Velikost bloku
/25	128	126	128
/26	192	62	64
/27	224	30	32
/28	240	14	16
/29	248	6	8
/30	252	2	4

VLSM funguje následovně. Pokud máme síť, například s IP adresou 192.168.10.0 za masku si následně volíme, podle velikosti bloku, který bude v dané síti potřebný. Když potřebujeme síť, pro 25 uživatelů použijeme blok velikosti 32, ale musíme vzít v potaz, že použitelných je pouze 30 IP adres. Pro 11 hostitelů postačí blok velikosti 16, ale použitelných bude pouze 14 IP adres. Samozřejmě lze používat i větší velikost bloků tím by se, ale popřela funkce VLSM jenž má zabránit plýtváním IP adres. Pří plánování IP adresace je zapotřebí počítat s tím, že se daná síť bude rozrůstat. V tomto případě je možné zvolit větší blok, který by mohl sloužit pro budoucí rozsah sítě [1].



Obr. 6. Příklad sítě s VLSM [10].

3 SMĚROVÁNÍ IP

Směrování IP neboli IP přeposílání řeší proces přeposílání paketů do odlišné podsítě. Když dojde k odeslání paketu. IP provede kontrolu, zjistí IP adresu doručení spolu se síťovou maskou a provede výpočet ANDing, jde o proces, který určí, zda je daný paket zasílán do stejné sítě či nikoliv. Pokud je adresa ve stejné síti dojde k odeslání paketu na danou adresu, pokud nikoliv je paket odeslán na výchozí bránu směrovače.

Výchozí brána je IP adresa směrovače, který je připojený nejen k lokální, ale i další síti. Směrovač porovnává svojí směrovací tabulku a snaží se podle ní určit nejlepší cestu pro odeslání paketu. Paket může projít přes mnoho směrovačů, než dorazí do cílové destinace. Jakmile paket doputuje do cílové destinace, IP použije část hostitelské IP adresy a dodá ho na koncové zařízení v dané síti [7].

3.1 Statické směrování

Statické směrování je založené na práci daného administrátora sítě, který vkládá do směrovací tabulky IP adresy a masky dané sítě, které definují cesty, pro zasílání paketů. Statické směrování je do určité míry výhodnější než dynamické, jelikož poskytuje lepší přehled a kontrolu nad trasami pro, zasílaní paketů. Nevýhoda nastává při každé aktualizaci, kdy se daná trasa mění nebo upravuje. Proto je statické směrování vhodné pouze pro malé sítě [7].

3.2 Dynamické směrování

Dynamické směrování používá ke směrování paketů protokoly, které mezi sebou komunikují a vyměňují si informace o změnách ve směrovací tabulce automaticky. Používá se především ve větších sítích, ale je možné tuto volbu použít i v sítích menších rozměrů. Hlavní výhody dynamického směrování:

- Menší nároky na administrátora.
- Pokud dojde k poruše, ostatní směrovače si vymění informace a dojde ke změně trasy.
- Snížení rizika vzniku chyb ve směrovací tabulce [7].

3.3 Protokoly distance-vector

Směrovací protokoly typu distance-vector jsou primární volbou pro dynamické směrování v menších sítích. Jsou založeny na algoritmech z šedesátých let minulého století, které byly vyvinuty pro směrování ARPanetu. Tyto protokoly využívají algoritmus, jenž se nazýva Bellman-Fordův. Hlavní funkcí distance-vector protokolu je přístup ke všem informacím na síti, tak aby o nich věděl každý směrovač nebo koncové zařízení. Směrovače mají ve směrovací tabulce uloženy adresu bran spolu s jejich metrikou. Metrika je celková vzdálenost neboli počet přeskoků do cílové destinace. Algoritmus určí nejkratší trasu do cílové destinace. Pokud dojde ke změně a aktualizaci ve směrovací tabulce a směrovač zjistí, že trasa sousedního směrovače má nižší metriku je zvolena trasa s menšími nároky.

Nevýhody distance-vector:

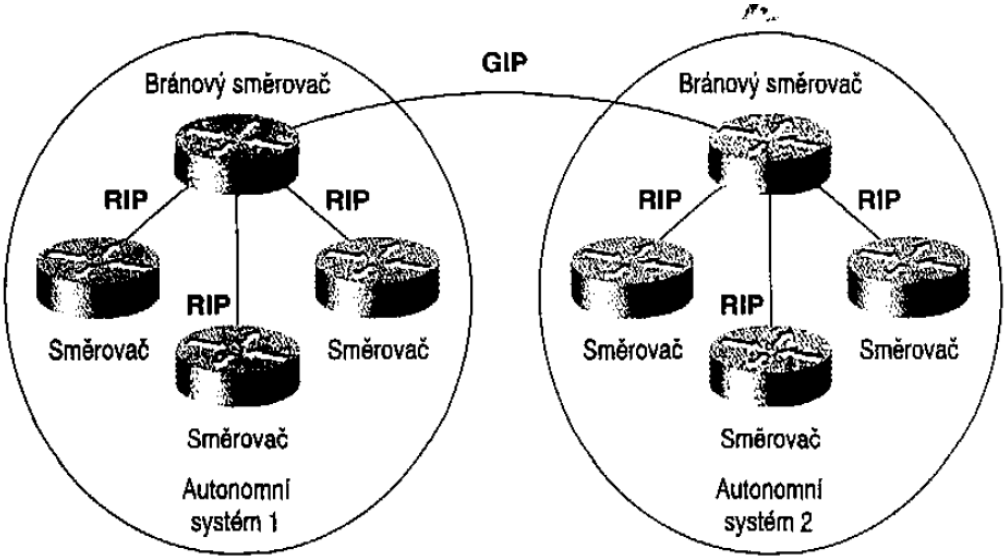
- Vysoká náchylnost na směrovací smyčky.
- Maximální počet přeskoků je 15.
- Není vhodné pro velké sítě [7].

3.3.1 RIP verze 1

Jedná se o jeden z nejstarších směrovacích protokolů. Prvního nasazení se dostal ve firmě Xerox a sloužil jako doplněk protokolu GIP (Gateway Information Protocol). Tento protokol měl za úkol vyměňovat směrovací informace mezi vzdálenými sítěmi. Firma Xerox, doplnila do této architektury jednoduchý směrovací protokol, který počítal cesty uvnitř autonomních systémů. Protokol byl založen na práci pana Fulkersona, Bellmana, Forda a byl pojmenován Routing Information Protocol (RIP). Jednalo se tedy o doplněk protokolu GIP.

Nevýhody protokolu RIP 1:

- Nepodporuje cesty delší než 15 přeskoků.
- Počítá cesty pouze podle předem dané metriky.
- Pomalá konvergence.
- Vysoká náročnost na aktualizace směrovacích tabulek.
- Nepodporuje VLSM.
- Nemožnost dynamického vyrovnání záteže [11].



Obr. 7. Spolupráce protokolů GIP a RIP v síti [11].

3.3.2 RIP verze 2

Jedná se o vylepšenou verzi protokolu RIP 1. RIP 2, byl poprvé představen roku 1993. Prvotní myšlenka nebyla vytvořit nový protokol pouze vylepšit starou verzi. Hlavní novinkou bylo představení síťové funkce, které zahrnovala práci s podsítěmi. I přes úspěšnou aktualizaci se nepodařilo odstranit nedostatky starší verze jako počet přeskoků na 15. Přesto tento protokol najde uplatnění i v dnešní době v sítích menších rozměrů. Momentálně bývá nahrazen protokolem se stavem linky OSPF.

Nové vlastnosti protokolu:

- Práce s maskami podsítí a podpora VLSM.
- Více směrové vysílání zpráv RIP-2 [11].

Jelikož protokol RIP verze 2, zdědil většinu vlastností po svém předchůdci, nepodařilo se odstranit některé důležité omezení:

- Neumožňuje podporu alternativních cest, jelikož udržuje ve své směrovací tabulce pouze jednu cestu. Pokud dojde k přerušení dané cesty, musí čekat na aktualizaci, podle které začne teprve vyhledávat jinou cestu [11].

3.3.3 Vlastnosti pouze RIP verze 2

1. Pracuje na transportní vrstvě UDP, port 520.
2. Verze, kterou používá Cisco, umožňuje směrování do stejné podsítě více trasami.

3. Podpora VLSM.
4. Vyvolává aktualizace při změně cesty [1].

3.4 Protokol EIGRP

Jedná se o protokol, který byl vytvořený přímo firmou Cisco. Jde o inovaci protokolu IGRP. Od svého předchůdce se, ale výrazně liší, podporuje VLSM a CIDR. Jeho funkce jsou nejbohatší a nejrobustnější ze všech směrovacích protokolů. EIGRP je hybrid, který má nejlepší vlastnosti z protokolů s vektorem vzdálenosti a stavem linky díky této kombinaci vznikl unikátní protokol, který se nedá zařadit do běžné kategorie protokolů. Obsluha a nastavení je náročnější, přesto je možné nasadit EIGRP s protokoly IPv4, IPv6, AppleTalk a IPX [11].

Hlavní výhody protokolu EIGRP:

- Podpora IPv4 a IPv6.
- Beztřídní protokol stejně jako RIPv2 či OSPF.
- Podporuje VLSM a CIDR.
- Podporuje souhrnné cesty.
- Efektivně zjišťuje sousedy.
- Vybírá trasu pomocí difúzního aktualizačního algoritmu DUAL.
- Nevyužívá všesměrové vysílání [1].

3.4.1 Nové prvky EIGRP

- Dynamicky pozná směrovače, které jsou nově připojeny do sítě.
- Identifikuje cesty, které se staly nedosažitelné či neschopné provozu.
- Opět pozná směrovač, který byl nedostupný [11].

Přenosový protokol RTP

Jedná se o protokol, jehož hlavní funkcí je rychlá aktualizace a přesné doručení dat. Tento protokol zajišťuje přenášení zpráv mezi kompatibilními směrovači [1].

DUAL algoritmus

- Zajišťuje záložní trasu, pokud je dostupná.
- Podporuje VLSM.
- Zajišťuje obnovu dynamických tras.

- Ptá se sousedů na neznámé alternativní cesty [1].

3.4.2 Vlastnosti EIGRP

- Pracuje na transportní vrstvě IP.
- Podpora časovače Hold, který zjišťuje selhání z důvodu neobdržení žádné zprávy, případně ani paketu Hello.
- Úplná aktualizace proběhne, pouze při rozpoznání nového souseda jinak se zasílají částečné aktualizace [1].

3.5 Protokoly link-state

Protokoly link-state, jsou vylepšenou verzí dynamického směrování. Algoritmy jsou založeny na funkci, která mapuje topologie dané sítě a snaží se udržet databázi link-state, která je základem této mapy. Pokud dojde k nějaké změně, databáze se aktualizuje. Tato metoda je mnohem účinnější než distance-vector, ale má taky svou nevýhodu. Pokud link-state databáze doroste vysokých rozměrů, dojde k vysokým nároku na procesor a paměť směrovače. Konvergence neboli šíření aktualizovaných informací je mnohem rychlejší než u distance-vector. Zástupci této skupiny jsou především OSPF a IS-IS [7].

3.6 OSPF Vznik

Jedná se o jeden z nejsilnějších a vlastnostmi nejbohatší otevřený směrovací protokol. Na druhou stranu je velmi složitý což je jeho největší nevýhodou, jelikož provoz sítě s protokolem OSPF je mnohem náročnější než s jiným protokolem. Tento protokol byl vytvořen v 80. letech minulého století, původní verze byla označována, jako OSPF verze 1, ale jelikož došlo k velké úpravě a zdokonalení starší verze vznikl nový protokol OSPF verze 2. Podobu verze 2 popisuje dokument volně otevřený standart RFC 2328 [11].

3.6.1 OSPF

Rozsáhlejší sítě, vyžadují propracovanější protokoly pro tento účel se využívá protokol OSPF. Je to protokol z rodiny link-state. Tento protokol není náchylný na směrovací smyčky a je mnohem efektivnější jako ostatní protokoly. Největší výhodou, která zvyšuje účinnost je rozdělení sítě na oblasti, což umožňuje hierarchickou strukturu pro směrovací tabulky. Každý směrovač patří do určité oblasti, kde spravuje ve své

databázi brány pouze své oblasti. Pokud chceme směrovat mimo oblast, potřebujeme proto směrovač hranice oblasti (ABR), který spojuje ostatní oblasti. Průchod přes páteřní oblast zmenšuje velikost směrovacích tabulek a snižuje čas, který je potřebný pro přepočet tras při změně [7].

Hlavní výhody OSPF:

- Možnost vytvořit oblasti a autonomní systémy.
- Minimální provoz aktualizací.
- Velice pružný, všestranný a škálovatelný protokol.
- Podporuje VLSM a CIDR.
- Neomezený počet přeskoků.
- Otevřený standard, který se nasazuje do sítí s více dodavateli aktivních prvků [1].

3.6.2 OSPF verze 3

Jedná se o protokol, který je novým nástupcem starší verze. Nevýhodou je, že je mnohem složitější a pracuje s protokolem IPv6. Základ je velice podobný mezi oběma protokoly, přesto došlo k určitým zásadním změnám v konfiguraci. Pro směrovací proces se nepoužívá již příkaz network, ale nyní se konfiguruje přímo dané zařízení (interface).

Hlavní změny:

- Změna konfigurace nastavuje se přímo daný interface.
- Autentizace již není přímou součástí jelikož IPv6 podporuje protokoly AH a ESP.
- Změna názvosloví OSPF verze 2 používá komponentu síť OSPF verze 3 používá název linka.
- Sítě v LSA OSPF verze 2 vyjadřuje sítě hodnotami [adresa, maska] OSPF verze 3 vyjadřuje hodnotou [prefix, délka prefixu]
- Rozsah rozesílání plošných zpráv v OSPF verze 3 může být jeden ze tří typů a to linkový lokální rozsah, rozsah v oblasti slouží pro plošné zasílání v jedné oblasti. Posledním typem je rozsah v autonomním systému jedná se o plošné rozesílání v celé směrovací doméně [12].

4 SPANNING TREE PROTOKOL

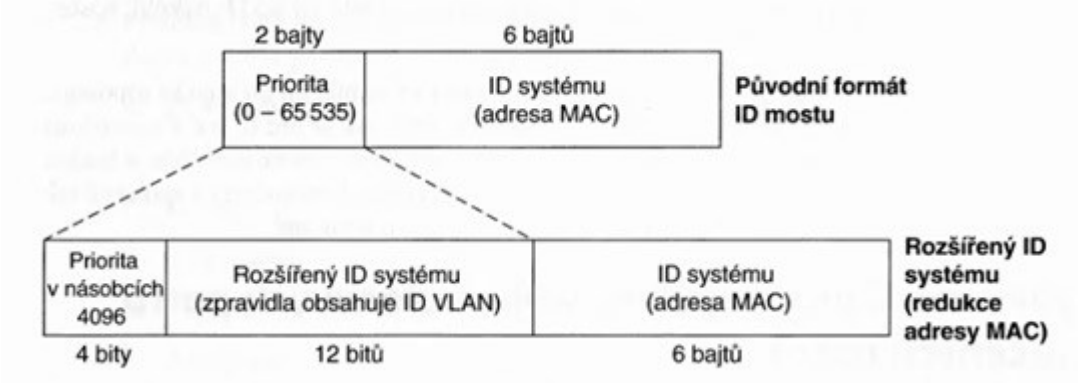
Jedná se o protokol, který využívají přepínače mezi sebou ke komunikaci, jenž má zabránit smyčkám v logické topologii sítě. STP (Spanning tree protocol) rozhoduje, které porty budou ve stavu blokovaném neboli (blocking) stavu. Ostatní porty jsou ve stavu rozesílaní neboli (forwarding) tímto se zajistí trasa bez smyček do každé ethernetové části dané sítě. STP rozhoduje o tom, které porty povolí a které zakáže pomocí tří kroků. Jedná se o volbu kořenového přepínače, volbu kořenového portu na každém přepínači a volbu určitého portu každého segmentu [12].

4.1 Volba kořenového přepínače

Kořenovým přepínačem může být pouze jeden. Výběr kořenového přepínače probíhá pomocí volby (election). Následně každý přepínač na začátku vytvoří kontaktní zprávu Hello, kterou odešle. Hello je datová jednotka mostového protokolu. Jakmile je zpráva rozeslána, přepínač prohlašuje, že chce být kořenovým přepínačem. Když dojde k přijetí nadřazené kontaktní zprávy (superior Hello), jde o zprávu s nižším ID mostu, přestane daný přepínač vytvářet a vysílat zprávy Hello a tím přestává být kořenem. Místo toho se začnou šířit zprávy s větší prioritou od většího kandidáta. Později nastane útlum zasílání zpráv Hello a zůstane pouze jeden přepínač s nejlepším ID mostu, který se stane vítězem a kořenovým přepínačem.

ID mostu se dělí na dvě části:

- Standardní volbu ID mostu tvoří 2 bajtová priorita, který se stanovuje zvlášť v nastavení každého přepínače a ovlivňuje tak celkovou volbu STP.
- Případně pomocí MAC adresy. To znamená, že každý přepínač má jedinečnou ID mostu a při volbě tak musí jeden z nich zvítězit [12].



Obr. 8. ID mostů podle IEEE 802.1d. [12].

4.2 Volba kořenového portu

Jakmile dojde k volbě kořenového přepínače, musí ostatní přepínače určit svůj kořenový port (root port). Volba vypadá následovně:

1. Kořenový přepínač vytvoří zprávu, Hello, kterou odešle. Výchozí nastavení časovače Hello, jsou 2 sekundy.
2. Pokud dojde k přijetí zprávy Hello, dojde k přeposlání zprávy Hello, ale nejdříve se v ní aktualizuje pole: cena (cost, náklady), ID mostu ze kterého zpráva Hello přišla a dojde k aktualizaci odesílajícího portu spolu s číslem odesílajícího portu.
3. Porty, které přejdou do blokovaného stavu zprávy, Hello dále nerozesílají.
4. Všechny porty, které zprávu Hello obdrží, se stane kořenovým portem, ten který má nejmenší vypočítanou cenu.

Přepínač u každé zprávy Hello, stanovuje nejmenší cenu na cestu, která slouží k dosažení kořenového přepínače. Proto je potřeba přečíst hodnoty cen ve zprávě a sečíst v ní vlastní náklady na port STP [12].

Rychlost Ethernetu	Cena podle původní IEEE	Cena podle revidované IEEE
10 Mb/s	100	100
100 Mb/s	10	19
1 Gb/s	1	4
10 Gb/s	1	2

Obr. 9. STP výchozí ceny portů podle normy IEEE 802.1d. [12].

Pokud přepínač obdrží více zpráv Hello, které mají stejnou vypočtenou cenu. Rozhodne se následovně:

- Zvolí nejnižší hodnotu ID přepínače, který zprávu odeslal.
- Zvolí nejnižší prioritu portu vedlejšího přepínače, jelikož vedlejší přepínač přidal svou vlastní prioritu ke zprávě a teprve ji poslal dále.
- Zvolí nejnižší interní číslo portu od odesílajícího přepínače. Číslo je uvedeno v přijatých zprávách Hello.

4.3 Volba určeného portu

Jakmile se dokončí konvergence, bude do každé částí sítě LAN posílat zprávy Hello jenom jeden přepínač. Jedná se o určený přepínač (designated switch) daného segmentu sítě. Příslušný port tohoto segmentu je určený port (designated port). Jde o port, který má nejnižší náklady na přístup k danému segmentu oproti ostatním portům. Určený port se taky označuje jako předávací a v každém síťovém segmentu může být pouze jeden [12].

4.4 Pět stavů portů STP podle IEEE 802.1d

Při změně topologie sítě například přidáním nového přepínače může dojít k ovlivnění stavu jednotlivých portů. Zde jsou vypsané stavy, které mohou nastat [13].

4.4.1 Disabled

Tento port neposílá a ani se nezúčastňuje přeposílání rámců protokolu STP. Tento port prakticky ani nefunguje [1].

4.4.2 Blocking

Tento port rámce nepředává, pouze poslouchá datové jednotky přemosťovacího protokolu. Tento stav zamezuje vzniku smyček. Stav blokování dostávají standardně všechny porty po zapnutí přepínače [1].

4.4.3 Listening

Port ve stavu naslouchání pracuje s datovými jednotkami přemosťovacího protokolu. Dříve než předá datový rámec, prozkoumá síť, zda neobsahuje žádné smyčky. Port v tomto stavu předává rámce bez zaplnění tabulky MAC [1].

4.4.4 Learning

Port v tomto nastavení pracuje s datovými jednotkami přemosťovacího protokolu a zjišťuje všechny možné cesty v dané síti. Port v tomto stavu naplňuje tabulku MAC adres, prozatím ale nepřeposílá datové rámce. Zpoždění předávání je stav, který zjišťuje, jak dlouho trvá přechod z naslouchání do režimu zjišťování případně z režimu zjišťování do režimu předávání. Defaultní nastavení zpoždění je zde na hodnotě 15 sekund [1].

4.4.5 Forwarding

Tento port přijímá a odesílá všechny datové rámce na přemostěném portu [1].

4.5 CST (Common spanning tree) 802.1d

Jde o první standart protokolu STP, který je omezený svou rychlostí. Výhodou je, že je málo náročný na prostředky mostů. Pokud se v přepínané síti s použitím redundantních linek, použije protokol CST proběhne výběr pomocí STP, který rozhodne o volbě kořenového mostu v dané síti. Taktéž se stane kořenovým mostem pro všechny VLAN sítě a ostatní mosty v sítí k němu vytvoří jedinou cestu [1].

4.6 PVST+

Jedná se o přímé vylepšení protokolu STP firmou Cisco. Toto vylepšení vzniklo z důvodu snížení konvergence, která byla nastavena na hodnotu 50 sekund. Protokol PVST+ umožňuje vytvořit samostatný protokol STP pro každou síť VLAN. To umožňuje si zvolit kořenový most pro každou VLAN síť zvlášť. Nevýhodou je vysoká náročnost na procesor i paměť přepínače [1].

4.7 RSTP

Protokol RSTP je novější rozvinutá verze protokolu STP, jenž nám umožňuje řešit problémy a rychlost s konvergencí, která byla problémová u tradičního protokolu STP. Menší nevýhodou je jeho náročnost na procesor a paměť z důvodu rychlé konvergence. Vlastnosti protokolu:

- Urychluje přepočítání při změně topologie na 2 vrstvě.
- Velice rychlý a aktivní, nepoužívá časovače zpoždění standardu 802.1d.
- Nahrazuje standard 802.1d, ale je zde zachována zpětná kompatibilita.
- Většina parametrů a termíny ze standardu 802.1d zůstává stejná [1].

5 ZABEZEPEČENÍ POMOCÍ ACL

V dnešní době veškerá komunikace přes Internet probíhá pomocí protokolu TCP/IP. Tento protokol po sítí zasílá malé části zvané pakety. V dobách, kdy začínal Internet, se začalo používat filtrování paketů, které se dodnes zachovalo a používá se především na směrovačích firmy Cisco. Tyto paketové filtry jsou první obranou spolu v kombinaci s jinými firewallovými technologiemi. Dnes se s touto implementací setkáme pod názvem přístupové seznamy. Filtrování paketů je jedna z prvních věcí, která by se měla použít pro kontrolu paketů. Na ten se nastaví určitá pravidla, která určují, zda daný paket může projít dál, nebo se zahodí [4].

Vlastnosti přístupových seznamů:

- Definují seznam pomocí pravidel „*permit*“ (povolit) či „*deny*“ (zakázat).
- Identifikace je pomocí čísel či jména.
- Nové pravidlo se přidá vždy na konec seznamu.
- Využití přístupových seznamů zpomaluje aktivní prvek má vliv na výpočetní výkon [14].

5.1 Dělení přístupových seznamů

Přístupové seznamy se dají rozdělit do dvou částí a to na standardní přístupové seznamy a rozšířené přístupové seznamy. Je potřeba zmínit, že k nim patří i pojmenované přístupové seznamy, které nejsou novým typem, ale chovají a vytvářejí se odlišně jako dva zmíněné předtím.

Výhody přístupových seznamů:

- Chrání před falšováním IP adres, které přichází do sítě.
- Chrání před falšováním IP adres, které odchází ze sítě.
- Chrání před útoky Dos.
- Blokuje a filtruje zprávy ICMP jak příchozí tak odchozí [1].

5.1.1 Standardní přístupové seznamy

Tento přístupový seznam filtruje síťový provoz pomocí zdrojové IP adresy daného paketu. Veškerá rozhodnutí se odvíjí od zdrojové IP adresy. Přístupové seznamy se vytvářejí pomocí čísel access-list od 1 do 99 případně v rozšířeném formátu 1300 až 1999. Ve výsledku to znamená, že povolí nebo zakáže celou sadu protokolů [1].

5.1.2 Rozšířené přístupové seznamy

Jedná se o složitější variantu přístupových seznamů, která nám ale poskytuje mnohem lepší a jemnější definování cílových požadavků. Seznam analyzuje zdrojovou a cílovou IP adresu. Tímto je možné některým uživatelům poskytnout či odejmout přístup například k některým službám v Internetu [1].

5.1.3 Pojmenované přístupové seznamy

Jde o jiný postup při tvorbě přístupových seznamů. Ve velkých počítačových sítích může správa přístupových seznamů dorůst neúnosné meze. Jelikož se předchozí přístupové seznamy značí číslem, může se stát, že při velkém množství se stanou listy nepřehledné a ani nebudeme vědět, co se pod daným číslem skrývá, zda daný list je aktivní nebo ne a zda ho mohu smazat či upravit. Tento problém právě řeší pojmenované seznamy, jenž umožňují slovně popsat daný seznam, který slouží pro okamžitou orientaci [1].

6 VIRTUÁLNÍ SÍTĚ LAN

Virtuální sítě LAN jsou jednoznačně definované porty na přepínači, které tvoří novou doménu všesměrového vysílání. Pomocí portů případně propojení několika přepínačů můžeme vytvořit virtuální sítě, které mezi sebou budou či nebudou komunikovat [12].

První sítě VLAN vznikly kolem roku 1995, ale masivního nasazení se jim dostalo až o několik let později a to především ve firmách malého a středního rozsahu. Hlavní důvody zavedení VLAN sítí byly:

- Seskupení uživatelů do jedné podsítě, která byla přiřazena danému útvaru například oddělení lidských zdrojů, tímto krokem se oddělila síť od ostatních.
- Zavedením VLAN se snížil počet broadcastů v síti.
- Zmenšily se kolizní domény, jednalo se především o dobu, kdy se huby používaly místo přepínačů [15].

6.1 Praktické výhody VLAN sítí

1. Snížena tvorba broadcastů tím, že se vytvoří menší podsíť, vznikne nová broadcastová doména, která zlepší výkon sítě a sníží provoz (traffic).
2. Lepší správa jedná se o jednoduchou správu, aby správce dostal zařízení do určité VLAN sítě stačí mu přiřadit port dané VLAN sítí. Tímto, odpadá práce s fyzickým přepojováním HW, vše se řeší SW.
3. Zabezpečení tím, že se vytvoří oddělené virtuální sítě, ke kterým není přístup, vznikají, lepší zabezpečené celky.
4. Snížení finančních prostředků díky tomu, že se na daném přepínači, dá vytvořit několik virtuálních sítí [15].

6.2 Zařazení komunikace do VLAN

Přiřazení do určité VLAN sítě probíhá na přepínači. Přepínače, které mají povolenou tvorbu VLAN sítí mají vždy defaultně nastavenou síť VLAN 1 tato síť se nedá vypnout ani smazat. Pokud se neprovede změna nastavení, jsou všechny porty na přepínači přidány do sítě VLAN 1. Existuje mnoho možností jak přiřadit komunikaci k dané VLAN, ale nejčastěji se používá přiřazení pomocí portu a podle MAC adresy [15].

6.2.1 Přiřazení podle portu

Port je přímo ručně přiřazen administrátorem do dané VLAN sítě. Port a veškerá komunikace, která přes port prochází, spadá do přiřazené VLAN sítě. To znamená, jestliže k danému portu připojíme přepínač tak ostatní zařízení, které jsou na přepínači připojena, budou spadat do stejné VLAN sítě. Toto řešení je nejjednodušší a zároveň nejbezpečnějším jedná se o jednoduchou a přehlednou správu [15].

6.2.2 Přiřazení podle MAC adresy

Port se přiřazuje do určité VLAN sítě pomocí MAC adresy. Jedná se o dynamický způsob správy, kdy se vede tabulka MAC adres pro každé zařízení společně s VLAN síti. Výhoda spočívá v tom, že pokud přepneme zařízení do jiného portu, zařízení se automaticky přiřadí do správné VLAN sítě. Veškerou správu zpracovává přepínač, který vyhledává dané informace v tabulce MAC adres [15].

6.3 Identifikace sítí VLAN

Aby přepínače mohly identifikovat VLAN sítě a sledovat veškeré rámce pří průchodu a správně je přiřadit musí zvolit z více metod, které se používají pro trunkování [1].

6.3.1 Směrování ISL

Jedná se o způsob značkování od firmy Cisco nevýhodou je podpora pouze na zařízeních firmy Cisco a to ještě na přepínačích vyšší třídy např. 3750. Tento způsob funguje na principu zabalení celého rámce do nové hlavičky a kontrolního součtu. Nevýhodou je to, že se tím zvětšuje komunikace a každý rámec je tak o 30 B větší. Momentálně firma Cisco od tohoto způsobu odstupuje a přechází čistě na 802.1q [15].

6.3.2 IEEE 802.1q

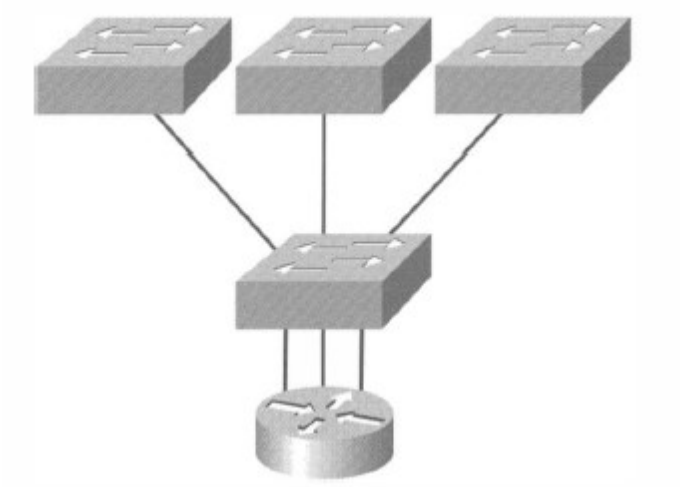
Tento protokol je možné znát také pod názvem trunking protokol případně dot1q tagging. Jde o metodu, která je dostupná na všech přepínačích, jenž umožňují tvorbu VLAN. Tento způsob je založený na tzv. tágování, kdy se vezme originální rámec a jeho hlavička se rozšíří o informaci velikosti 4 B. První značka určuje, že se jedná o protokol 802.1q dále v pořadí se určí priorita podle 802.1p poté následuje MAC adresa a číslo VLAN [15].

6.4 Směrovač mezi sítěmi VLAN

Pokud je potřeba zajistit mezi hostiteli komunikaci spolu se sítěmi VLAN je nutné proto použít zařízení, které pracuje na 3. Vrstvě. Aby se zajistila taková komunikace, existují dvě možnosti jak toto řešení uskutečnit.

6.4.1 Port pro každou VLAN síť

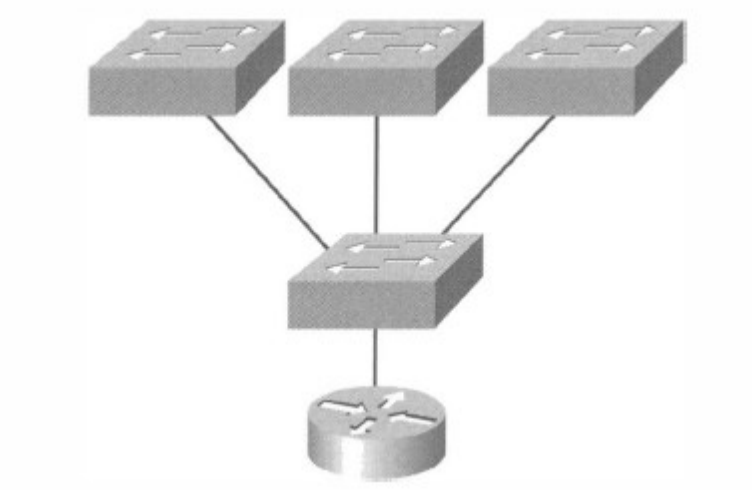
Jde o využití jednoho portu, který je přímo využíván jednou VLAN sítí. Výhodou je to, že veškerá komunikace probíhá přes daný port a nemusí se dělit s žádnou jinou VLAN sítí o šířku pásma. Nevýhoda je při použití více VLAN sítí kdy počet portů neustále narůstá a toto řešení se jeví jako neekonomické [1].



Obr. 10. Jeden port pro jednu VLAN síť [10].

6.4.2 Směrování na tyči neboli trunk

Jde o způsob, kdy se všechny VLAN sítě dělí o jeden port tzv. trunk. Tento způsob, umožňuje komunikaci pouze přes jedno místo, což má za následek snížení šířky pásma pro přenos. Proto tento se doporučuje volit GigabitEthernet, jenž umožňuje větší přenos po sítí. Výhodou tohoto způsobu je ekonomický, ale na druhou stranu veškerý provoz putuje přes jediný port, který když selže, ovlivní to všechny VLAN sítě, které danému trunku patří [1].



Obr. 11. Směrovač na tyči [10].

6.5 VTP protokol

Jedná se o protokol, který umožňuje vedlejším přepínačům získávat informace o nastavení sítě VLAN. Jednoduše stačí provést nastavení na jednom přepínači a ostatní přepínače si pomocí VTP protokolu dynamický zjistí veškeré informace. VTP oznamuje u každé VLAN sítě její ID, jméno a typ, ale již neuvádí informace o portech pro jednotlivé VLAN. To znamená, že se pomocí příkazu „*switch port access vlan*“, musí znovu přiřadit. Cisco přepínače dokážou pracovat se třemi režimy VTP [12].

6.5.1 Server

Je nejvyšší instance, bez, které nelze provádět výměnu informací o VLAN. V každé doméně musí být jeden server, který rozesílá informace o VLAN v dané doméně. Přepínač, který je zvolený jako server vytváří a maže VLAN sítě v dané doméně. Pokud, chceme změnit nějaké informace, je nutné to provést na serveru, od kterého se pak předají informace o změně pomocí VTP v dané doméně. Nastavení v serverovém režimu jsou uloženy v paměti NVRAM [10].

6.5.2 Klient

Přepínač v tomto režimu dostává informace z VTP serveru, za předpokladu, že se nachází ve stejné doméně. Přepínač dále odesílá a přijímá aktualizace. Dalo by se říct, že pracuje jako server, ale v tomto nastavení nemůže tvořit, odstraňovat či měnit VLAN sítě.

Důležité je taky vědět, že informace přijaté ze serveru VTP nejsou uloženy v paměti NVRAM. Kdyby se přepínač restartoval, nastala by, ztráta informací o VLAN [10].

6.5.3 Transparentní mód

Přepínač v tomto nastavení není součástí VTP domény a ani nesdílí informace o sítích VLAN. Pracuje samostatně. Vytváří a maže VLAN sítě, změny se projevují pouze lokálně. Toto nastavení pracuje jako prostředník, aby vzdálené přepínače byly schopné přijmout informace o VLAN sítích z VTP serveru pomocí přepínače, který se nezúčastňuje stejného přiřazení sítí VLAN [10].

7 VOIP

Jde o několik druhů technologií, které nám umožňují využít sítě IP pro hlasové aplikace jako je telefonování, telekonference a zasílání rychlých hlasových zpráv. VoIP, přesně definuje, jakým způsobem dojde k přenosu hlasového volání přes sítě IP, včetně digitalizace, paketizace datových a hlasových proudů. Služba VoIP převádí náš hlas na digitální signál a tento signál dále putuje sítěmi, které jsou založené na protokolu IP. VoIP umožňuje přímé volání z počítače, VoIP telefonu případně z analogového telefonního přístroje, který je připojený přes zvláštní adaptér. VoIP je taky možné využívat pomocí bezdrátových hotspotů na místech jako jsou parky, kavárny či letiště a umožňují se připojit k Internetu [16].

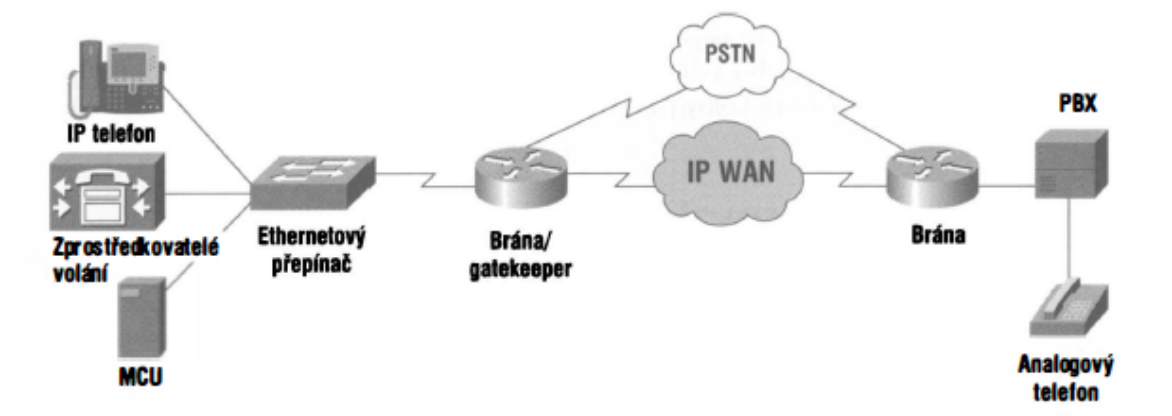
7.1 Využití VoIP ve firmách

Výhody, které z nasazení VoIP ve firmách plynou, se neustále mění. Nejdříve se jednalo o návrat investic, který byly vynaložené pro zavedení VoIP a taky zaměření na úspory, které z toho vedly, jelikož došlo k volání, které je osvobozené od poplatků telefonních společností. Momentálně hlasové technologie umožňují několik výhod, které je možné kombinovat a využít tak nejlépe pro svojí firemní činnost.

- Snížení nákladů a eliminace za meziměstské hovory.
- Směrové volání do cílové destinace může vést více trasami díky, tomu je možné zvolit nejvhodnější trasu, kde jsou nejmenší náklady případně se zaměřit na volání podle denní doby.
- Jednotné zasílání zpráv jde o zvýšení produktivity a zlepšení komunikace. Jde o centralizované místo, které spojuje různé média a tím podporuje čtení emailů, poslech hlasové pošty a přehled faxových zpráv.
- Zabezpečení citlivých polí hlaviček signalizace a ochranu paketů v případě, že by došlo k neoprávněnému přístupu [16].

7.2 Součást sítě VoIP

Následující obrázek popisuje základní součásti paketové hlasové sítě a komponenty sítě VoIP.



Obr. 12. Součásti sítě VoIP [17].

- Telefony IP jedná se o koncové prvky, které se využívají pro hlasovou komunikaci.
- Správce (Gatekeeper) jedná se o směrovač, který zajišťuje funkci řízení CAC (Call Admission Control) jde o správu, překlad adres a řízení šířky pásma.
- Brána (Gateway) hlavní funkcí brány je překládání sítí VoIP mezi sítěmi, které nejsou založeny na technologii VoIP.
- Jednotka MCU (Multipoint Control Unit) zajišťuje komunikaci v reálném čase tak aby bylo možné propojit účastníky videokonference z celého světa.
- Ethernetové přepínače s podporou hlasu – jedná se o přepínače, které dokážou připojenému IP telefonu poskytnout informace o podsíti, případně zajišťují napájení IP telefonů.
- Zprostředkovatelé volání – Jedná se o sadu funkcí, které měly dříve na starost telefonní ústředny. Příkladem může být CCM (Cisco Call Manager.) [17].

7.3 Protokoly VoIP

Aby bylo možné zajistit komunikaci hlasové brány a serverů CCM musí se zvolit jeden ze tří protokolů, které umožňují komunikaci zařízení v sítí VoIP, jedná se o H.323, MGCP a SIP [16].

7.3.1 H.323

Jde o nejdokonalejší protokol z těchto zmíněných. Nejedná se o jeden jediný protokol, ale o množinu více protokolů. Tato množina byla definovaná společnosti ITU (International Telecommunication Union) a schválena v únoru 1996. Tato sada měla za účel využít sítě IP stejně, jako se využívají telefonní sítě. V současnosti je protokol H.323

nejčastěji využíván pro hlasový přenos a videokonference. H.323 dále specifikuje protokoly:

- H.225 – tento signalizační protokol se využívá pro připojení mezi dvěma koncovými body.
- H.245 – tento protokol je využíván jako výměnná stanice, která předává zprávy v obou směrech komunikace. Zprávy, které se přenášejí jsou:

1. Informace o řízení toku.
2. Indikace a obecné příkazy.
3. Pracuje s logickými kanály, které slouží k přenosu datových toků médií.
4. Podpora kodeků [16].

7.3.2 MGCP

MGCP je protokol založený na principu klient-server. Výhoda spočívá v centralizované správě bran, jenž zajišťují vhodné řešení pro IP telefony. Informace, které slouží pro vytáčení, jsou přímo uloženy v úložišti samotného agenta volání. MGCP využívá pro přenos dat prostý text. MGCP byl specifikován v definici RFC 2705 byl poté několikrát upraven a vylepšen a nyní se nachází pod definicí RFC 3661[16].

7.3.3 SIP

Protokol SIP byl vytvořen skupinou MMUSIC a slouží jako alternativa ke známějšímu protokolu H.323. SIP je založený na stejné logice jako Internetový protokol WWW (World wide web) a proto ho lze velice snadno implementovat. SIP funguje na principu peer-to-peer, kde uživatelští agenti využívají relace mezi sebou. Oproti protokolu H.323, ale využívá pro svojí komunikaci textové zprávy, které jsou kódované pomocí ASCI znaků [16].

II. PRAKTICKÁ ČÁST

8 SOUPIS POŽADAVKŮ POČÍTAČOVÉ SÍTĚ

Návrh této počítačové sítě je založený na požadavcích smyšlené společnosti, která vystupuje pod jménem Firma.cz. Po konzultaci s jednatelem společnosti byly stanovené podmínky, o tom jak by počítačová síť měla vypadat a jaké vlastnosti by měla splňovat. Stanovené podmínky pro firemní sít:

- Zajištění komunikace pro Prodej, Administrativa a IT oddělení.
- Možnost volání v celé firemní síti.
- Zabezpečení sítě, tak aby zaměstnanci nemohli chodit na weby typu Facebook.
- Připojení do Internetu přes jednu veřejnou IP adresu.
- Vytvoření firemního webového serveru.
- Vytvoření firemního emailového serveru.
- Zajistit funkčnost celé sítě.

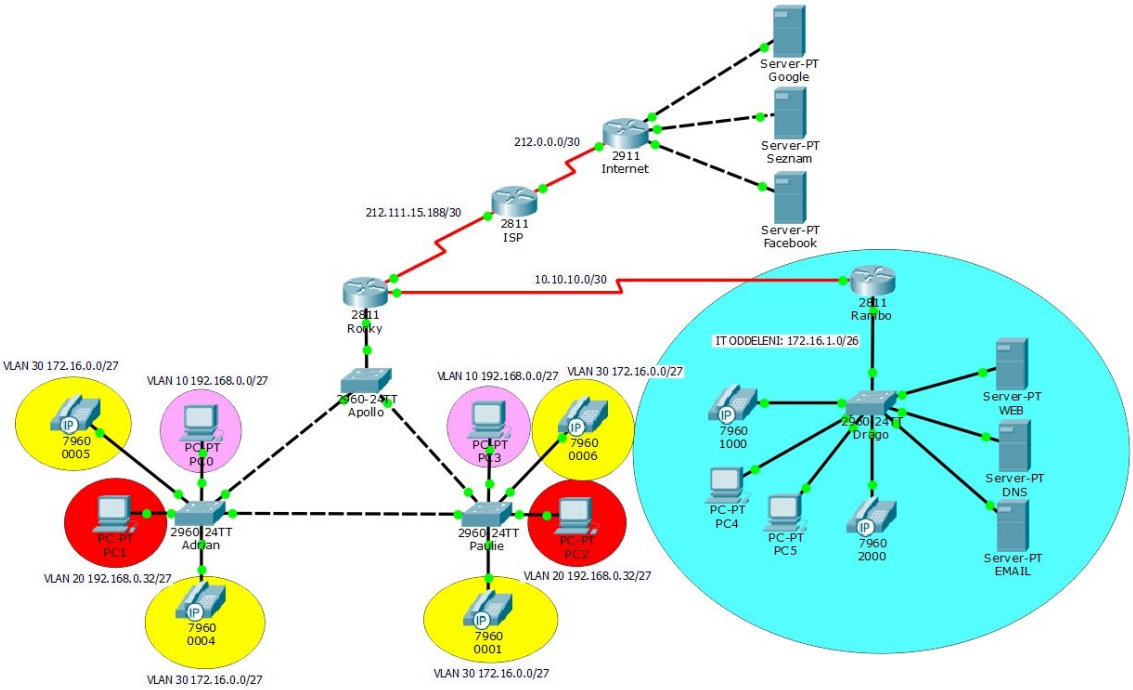
8.1 Celkový přehled použitých technologií pro návrh firemní sítě

Níže je popsán seznam hlavních použitých protokolů a technologií, které byly využity pro návrh dané sítě.

- VLSM, ACL.
- VLAN, VTP, STP.
- OSPF, DHCP, NAT.
- DNS, WEB, MAIL.
- VoIP a Webové servery na Internetu.

9 GRAFICKÉ SCHÉMA POČÍTAČOVÉ SÍTĚ

Níže je grafická podoba nakonfigurované firemní sítě v simulačním prostředí Packet Tracer. Jedná se o fyzickou typologii, jak jsou aktivní prvky a počítačové stanice zapojeny. Včetně dvou směrovačů v Internetu a tří serverů.



Obr. 13. Grafické schéma počítačové sítě

10 VLSM A IP ADRESACE ZAMĚSTNANCŮ

Pro návrh hlavní části počítačové sítě, jenž slouží pro zaměstnance, byla použita adresa 192.168.0.0/24. Tato adresa byla dále rozdělena pomocí VLSM na dvě podsítě pro VLAN Prodej a pro VLAN Administrativa. Obě tyto sítě pracují s maskou 255.255.255.224, což umožňuje připojit 30 uživatelů do obou VLAN sítí.

Celková kapacita sítě je pro 254 uživatelů. Aktuálně DHCP server poskytuje IP adresy, které dokážou přiřadit IP adresy 60 uživatelům PC stanic. Momentální využití adresace, je cca na 25% a pro budoucí růst je ponechaná značná rezerva.

Tab. 3. VLSM adresace zaměstnanců

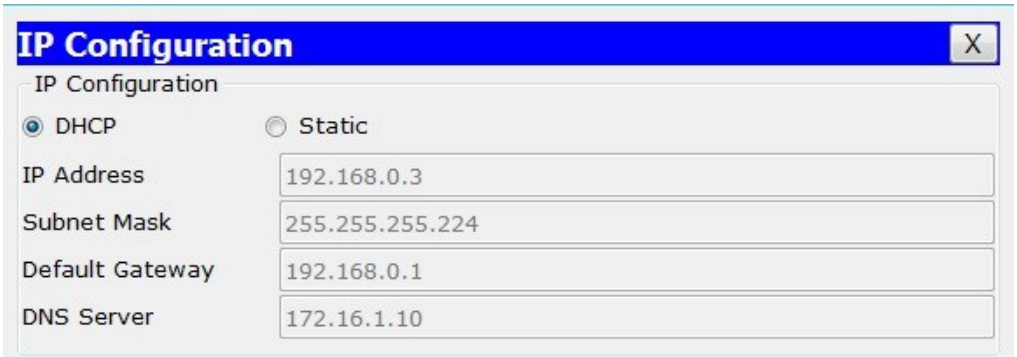
Název sítě	IP adresa sítě	Maska	Platný rozsah
Prodej	192.168.0.0	255.255.255.224	192.168.0.1-30
Administrativa	192.168.0.32	255.255.255.224	192.168.0.33-62

10.1 DHCP server pro klienty

DHCP server je nastavený jak na směrovači Rocky tak na směrovači Rambo. Tyto DHCP servery pak dále poskytují IP adresy všem koncovým zařízením ve VLAN 10, VLAN 20 a pro VoIP telefonii. V sítí, kde se nachází IT oddělení, funguje DHCP server pouze pro VoIP telefony.

```
ip dhcp pool Vlan10
 network 192.168.0.0 255.255.255.224
 default-router 192.168.0.1
 dns-server 172.16.1.10
ip dhcp pool Vlan20
 network 192.168.0.32 255.255.255.224
 default-router 192.168.0.33
 dns-server 172.16.1.10
ip dhcp pool VOIP
 network 172.16.0.0 255.255.255.224
 default-router 172.16.0.1
 option 150 ip 172.16.0.1
```

Obr. 14. DHCP nastavení směrovače Rocky



Obr. 15. DHCP protokol na koncových stanicích

10.2 IP adresace VoIP

Pro přehlednou správu počítačové sítě byly pro VoIP telefony zvoleny adresy z B rozsahu 172.16.0.0/27 a 172.16.1.0/26. Tyto IP adresy jsou přidělovány pomocí DHCP serverů, které běží na obou směrovačích. Adresa 172.16.0.0/27 je čerpána v sítí pro Prodej a Administrativu a je zde zvolen dost velký rozsah, který nebrání budoucímu rozšíření.

Adresa 172.16.1.0/26 je přidělena celé síti, kde se nachází IT oddělení, které si zde veškerou adresaci řeší samostatně staticky, kromě VoIP. Tento adresní prostor je použit jak pro VoIP, tak i počítačové stanice včetně serverů. VoIP telefony si z tohoto rozsahu berou pouze adresy, které byly vyhrazeny pomocí příkazu „*ip dhcp excluded-adress*“ a platný rozsah je tedy až od adresy 172.16.1.41 – 172.16.1.62.

Tab. 4. IP adresace sítě IT oddělení a VoIP zaměstnanců

Název sítě	IP adresa sítě	Maska	Platný rozsah
VoIP zaměstnanci	172.16.0.0	255.255.255.224	172.16.0.1-30
VoIP IT oddělení	172.16.1.0	255.255.255.192	172.16.1.41-62
IT oddělení	172.16.1.0	255.255.255.192	172.16.1.1-40

11 KONFIGURACE NATU

Aby celá firemní síť mohla vystupovat na Internetu je na hraničním směrovači nastavený přetížený NAT, který všechny adresy, jenž má přidělené, převede na jednu veřejnou adresu 212.111.15.189, která je nastavena na sériové lince 0/0/1. Při konfiguraci sítě, kde jsou zaměstnanci, je nutné nastavit NAT na jednotlivé sub interfacy, jelikož každá síť má vlastní VLAN. Pro IT oddělení tento způsob není nutný.

```
Rocky#show ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
icmp 212.111.15.189:1  192.168.0.3:1      77.75.77.39:1      77.75.77.39:1
icmp 212.111.15.189:2  192.168.0.3:2      77.75.77.39:2      77.75.77.39:2
tcp 212.111.15.189:1026192.168.0.3:1026   77.75.77.39:80     77.75.77.39:80
tcp 212.111.15.189:1027192.168.0.3:1027   77.75.77.39:80     77.75.77.39:80
tcp 212.111.15.189:1028192.168.0.3:1028   77.75.77.39:80     77.75.77.39:80
tcp 212.111.15.189:1029192.168.0.3:1029   77.75.77.39:80     77.75.77.39:80
tcp 212.111.15.189:1030192.168.0.3:1030   216.58.201.99:80   216.58.201.99:80
tcp 212.111.15.189:1031192.168.0.3:1031   216.58.201.99:80   216.58.201.99:80
tcp 212.111.15.189:1032192.168.0.3:1032   216.58.201.99:80   216.58.201.99:80
```

Obr. 16. Přehled komunikace PC stanice na Internetu

Obrázek popisuje komunikaci počítačové stanice, která má IP adresu 192.168.0.3. Jak nejdříve zasílá příkaz ping na server Seznam.cz, který má IP adresu 77.75.77.39. Dále stejná počítačová stanice zasílá přes webový prohlížeč dotaz pro zobrazení obsahu stránek Seznamu a Googlu, který má adresu 216.58.201.99. Veškerá komunikace, v Internetu probíhá pod adresou 212.111.15.189.

```
Rocky#show ac
Rocky#show access-lists
Standard IP access list NAT
    10 permit 172.16.1.0 0.0.0.63
    20 permit 192.168.0.0 0.0.0.31
    30 permit 192.168.0.32 0.0.0.31
```

Obr. 17. Přehled sítí, které využívají NAT

K využití technologie NAT, je nejdříve nutné vytvořit access-list, který má definované IP adresy sítí, pro které se má překlad adres použít. Jakmile je access-list vytvořen uvedete se NAT do provozu příkazem „*ip nat inside source list NAT interface Serial0/0/1 overload*“.

12 ZABEZPEČENÍ POMOCÍ ACL

Vzhledem ke stanoveným požadavkům ohledně navštěvování nevhodných stránek na Internetu, byl vytvořen ACL, který zamezuje komunikaci na server Facebook pro všechny zaměstnance. Toto omezení neplatí pro IT oddělení, které si může služeb Facebooku využívat bez omezení. Z důvodu toho, že Facebook na Internetu vystupuje až pod 36 adresami, které je možné dohledat na Internetu, byl zvolen tento způsob zamezení komunikace s tímto serverem, který popisuje přiložený obrázek.

```
Extended IP access list Facebook
    10 deny ip 192.168.0.0 0.0.0.31 31.13.84.0 0.0.0.255 (138 match(es))
    20 deny ip 192.168.0.32 0.0.0.31 31.13.84.0 0.0.0.255 (72 match(es))
    30 permit ip any any (53 match(es))
```

Obr. 18. Nastavený access list pro Facebook

12.1 Zamezení přístupu na Facebook

Pro zamezení přístupu na Facebook, byl adresám 192.168.0.0 a 192.168.0.32 odepřen permanentní přístup do sítě 31.13.84.0, která patří Facebooku. Jedná se však pouze o jednu adresu ze zmíněných 36. Omezení je opět nutno nastavit na jednotlivé sub interfacy, jelikož se jedná o sítě, které mají vlastní VLAN.

Obr. 19. Zamezený přístup na Facebook

Z obrázku je možné vidět, že komunikace se serverem Facebook selhala. Požadavek byl vyslán z PC stanice, která patří do VLAN 10 a má adresu 192.168.0.2.

12.2 Zamezení stanice v přístupu na firemní server

Vzhledem k tomu, že ve firemní sítí se IP adresy na serveru nemění, je zde nastavený mnohem efektivnější ACL, který zabraňuje stanici z VLAN 10 s adresou 192.168.0.2 přístup na webový firemní server. Z obrázku níže je možné vidět, že je dané stanici zakázán webový protokol na adrese 172.16.1.9.

```
Rambo#show access-lists
Extended IP access list 110
    10 deny tcp host 192.168.0.2 host 172.16.1.9 eq www (153 match(es))
    20 permit ip any any (91 match(es))
```

Obr. 20. Nastavený access list pro zákaz stanice 192.168.0.2

Obr. 21. Zamezený přístup stanice 192.168.0.2 na webový server firmy

Z obrázku jde vidět selhaný pokus při přístupu na webový server počítačové stanice 192.168.0.2 z VLAN 10, které byl odepřen přístup a firemní stránky se tak nezobrazily.

13 NASTAVENÍ FIREMNÍCH SERVERŮ

Ve firemní síti, se nachází celkem tři servery. Webový server, na kterém jsou oficiální firemní stránky, dále DNS server, který překládá IP adresy na doménová jména a emailový server, který slouží pro komunikaci v celé firemní síti.

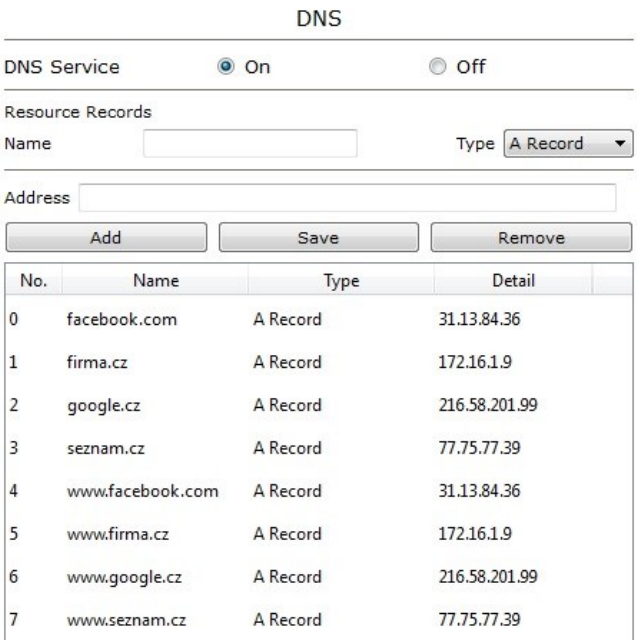
13.1 Firemní webový server

Tento server má v sítí adresu 172.16.1.9 a běží na něm webová adresa firmy, která má název Firma.cz. Na tento server mají přístup všechny stanice kromě jedné s adresou 192.168.0.2. Níže přiložený obrázek zobrazuje firemní stránky, které běží v prohlížeči stanice, která patří do VLAN 20 a má adresu 192.168.0.34.

Obr. 22. Firemní webové stránky

13.2 DNS server

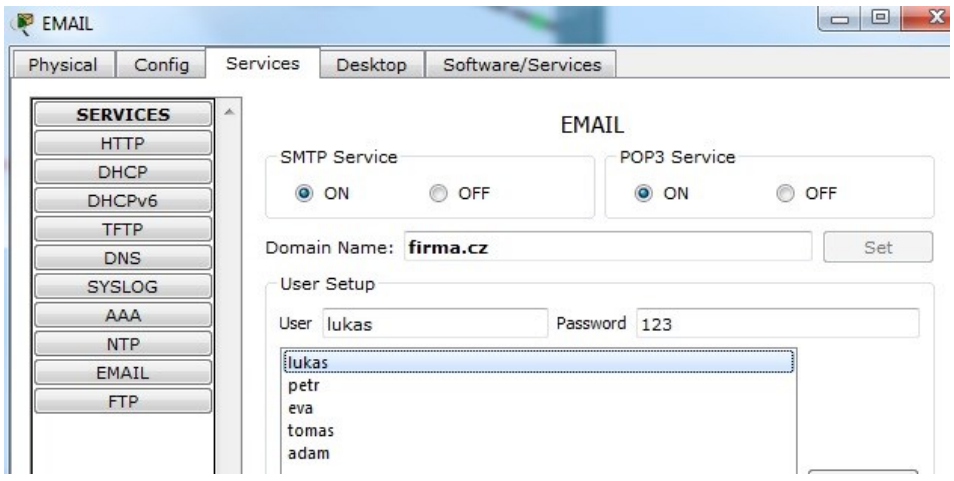
Tento server překládá veškeré IP adresy na doménová jména. Na tomto serveru jsou uloženy adresy Firma.cz, Seznam.cz, Google.cz a Facebook.com. Vzhledem k tomu, že Packet Tracer nepodporuje na koncových stanicích více DNS serverů bylo zvoleno toto řešení, kde jsou uloženy všechny webové adresy. Google, Seznam a Facebook mají přidělené originální adresy, pod kterýma je možno dohledat tyto stránky v reálu. Pokud by ve firemní síti neběžel DNS server, webové stránky by fungovaly, ale pro zobrazení obsahu stránek by se musela zadávat IP adresa každého serveru.



Obr. 23. Přehled všech adres uložených v DNS

13.3 Emailový server

Na tomto serveru běží emailová komunikace celé sítě. Každý uživatel má za svým jménem doménovou adresu firma.cz. Adresa tohoto serveru je 172.16.1.11, tuto adresu je taky nutné vložit do nastavení při konfiguraci emailového klienta na každé stanici.



Obr. 24. Přehled uživatelů emailového serveru

Obr. 25. Výsledný přehled emailové komunikace

Výsledný obrázek popisuje emailovou komunikaci mezi uživateli. Jedná se o email zaslaný ze sítě IT oddělení do sítě, kde jsou zaměstnanci. Komunikace funguje v celé firemní síti.

14 NASTAVENÍ VTP A STP PROTOKOLU

Aby ve firemní síti nedocházelo ke smyčkám, které by mohli vytvořit broadcastovou bouři, je na přepínači Apollo nastaven Spanning Tree Protocol, který je aplikován na všechny VLAN sítě, které jsou zde vytvořeny.

```
spanning-tree mode pvst
spanning-tree vlan 10,20,30,99 priority 4096
```

Obr. 26. Nastavení Spanning Tree Protokolu

14.1 Nastavení VTP

Na přepínači Apollo je taktéž použit protokol VTP. Přepínač Apollo je nastavený jako server s doménou FIRMA a dále přeposílá informace o VLAN sítích na směrovače Adrian a Paulie, které se nacházejí ve stejné doméně a mají nastavení jako klienti. Pokud chceme měnit nebo přidávat VLAN sítě stačí pouze změny provést na přepínači Apollo. Heslo do domény FIRMA je firma.

```
Apollo#show vtp status
VTP Version                     : 2
Configuration Revision          : 8
Maximum VLANs supported locally : 255
Number of existing VLANs        : 9
VTP Operating Mode              : Server
VTP Domain Name                 : FIRMA
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0x07 0x52 0x77 0xC9 0x94 0xE6 0xCA 0x8B
Configuration last modified by 0.0.0.0 at 3-1-93 00:02:29
```

Obr. 27. Nastavení VTP serveru přepínače Apollo

```
Adrian#show vtp status
VTP Version                     : 2
Configuration Revision          : 8
Maximum VLANs supported locally : 255
Number of existing VLANs        : 9
VTP Operating Mode              : Client
VTP Domain Name                 : FIRMA
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0x07 0x52 0x77 0xC9 0x94 0xE6 0xCA 0x8B
```

Obr. 28. Nastavení VTP klienta přepínače Adrian

15 NASTAVENÍ PROTOKOLU OSPF

Protokol OSPF propojuje síť zaměstnanců spolu s IT oddělením. Je nastaven na směrovačích Rocky a Rambo. OSPF přenáší informace o sítích VLAN do sítě, kde je IT oddělení a z IT oddělení zpátky do sítě zaměstnanců. Spojení probíhá po sériové lince, která využívá IP adresu 10.10.10.0/30. Aby mohla síť IT oddělení přistupovat do Internetu je nutné na hraničním směrovači Rocky povolit redistribuci sítí příkazem „*default-information originate*“.

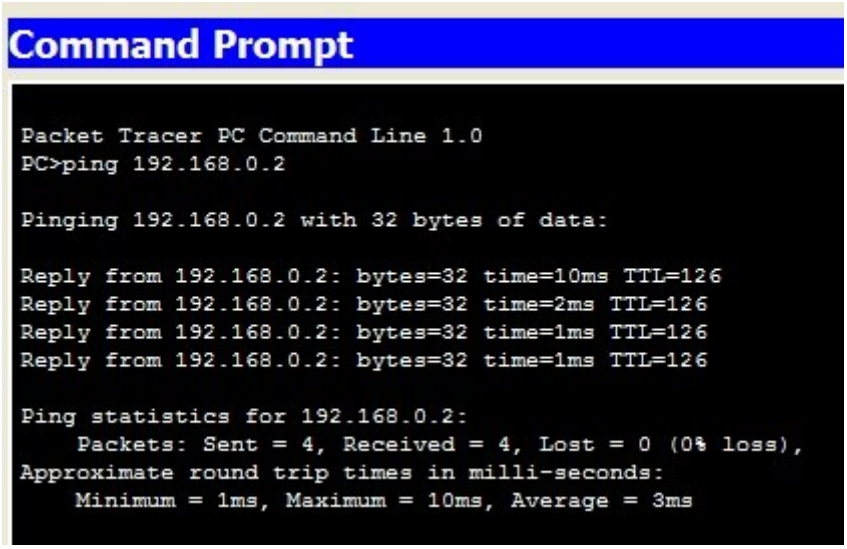
```
router ospf 1
 router-id 1.1.1.1
 log-adjacency-changes
 network 10.10.10.0 0.0.0.3 area 1
 network 192.168.0.0 0.0.0.31 area 1
 network 192.168.0.32 0.0.0.31 area 1
 default-information originate
```

Obr. 29. Nastavení OSPF na směrovači Rocky

```
router ospf 1
 router-id 2.2.2.2
 log-adjacency-changes
 network 10.10.10.0 0.0.0.3 area 1
 network 172.16.1.0 0.0.0.63 area 1
```

Obr. 30. Nastavení OSPF na směrovači Rambo

Obrázek níže zobrazuje úspěšný příkaz ping, který byl zaslaný ze sítě IT oddělení z adresy stanice 172.16.1.3 do sítě zaměstnanců na adresu 192.168.0.2, která patří do VLAN 10. Bez nastavení směrovacího protokolu mezi sítěmi by příkaz ping nebyl možný.



Obr. 31. Přehled úspěšného pingu

16 NASTAVENÍ VOIP

V celé firemní síti je nastavená VoIP telefonie, která umožňuje volat zaměstnancům mezi sebou, ale taky do sítě, kde je IT oddělení a můžou se tak řešit technické problémy mnohem efektivněji pomocí hlasové komunikace. V síti zaměstnanců je pro VoIP vytvořen VLAN 30 s názvem VOIP. Pro IT oddělení je VoIP v defaultním nastavení VLAN 1. Pro komunikaci mezi sítěmi je na směrovačích Rocky a Rambo nastaven příkaz „*session target ipv4:10.10.10.1-2*“, který umožní telefonování do obou sítí, bez tohoto příkazu by fungovala telefonie pouze v síti, kde jsou zaměstnanci nebo v síti IT oddělení. Komunikace mezi sítěmi by nebyla možná.

```
dial-peer voice 1 voip
 destination-pattern ....
 session target ipv4:10.10.10.2
!
telephony-service
 max-ephones 6
 max-dn 6
 ip source-address 172.16.0.1 port 2000
 auto assign 4 to 6
 auto assign 1 to 5
!
ephone-dn 1
 number 0001
!
ephone-dn 2
 number 0002
!
ephone-dn 3
 number 0003
```

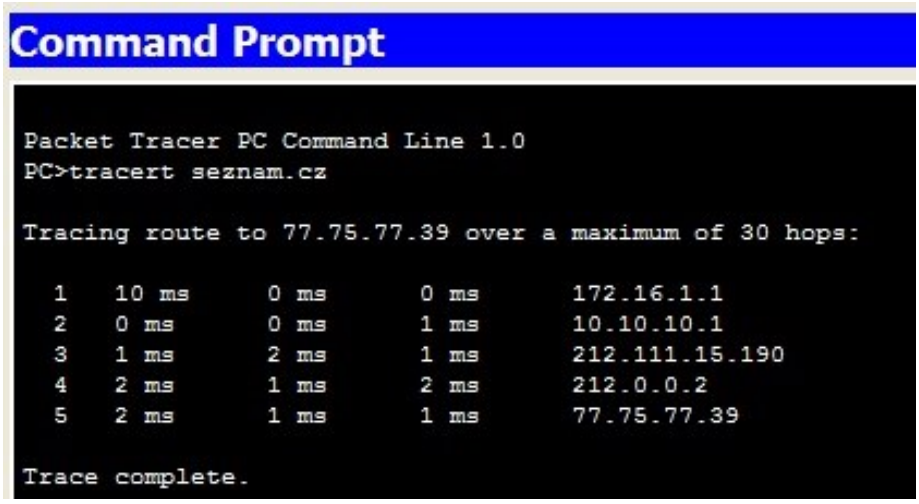
Obr. 32. Nastavení VoIP na směrovači Rocky

Obr. 33. Telefonní komunikace mezi sítěmi

Obrázek níže zobrazuje telefonní spojení sítě IT oddělení a zaměstnanců. Hovor je vytvořen ze sítě zaměstnanců s číslem 0005 a je spojen s telefonem v IT oddělení, který má číslo 2000.

17 KOMUNIKACE V INTERNETU

Pro kompletní ověření firemní sítě, byly do Packet Traceru přidělané dva směrovače ISP a Internet. Jedná se o směrovače, které jsou nastaveny pouze tak, aby prošla komunikace na servery Facebook, Seznam a Google. Neřeší se zde žádná bezpečností politika ani protokoly. Aby se uskutečnilo spojení se servery z hraničního směrovače Rocky, vede defaultní routa „*ip route 0.0.0.0 0.0.0.0 212.111.15.190*„ na ISP. ISP pak dále přeposílá informace směrovači Internet, na který vedou celkem tři statické cesty. Pro každý server jedna. Příkaz „*ip route 216.58.201.0 255.255.255.0 212.0.0.2*“ je statická cesta pro server Google.cz. Tyto servery pak zobrazují jednoduchý textový obsah „Vítejte na Googlu“. Pokud se daný obsah zobrazí, bylo úspěšně navázané spojení do Internetu.



Obr. 34. Mapování cesty na server Seznam.cz

Z daného obrázku je možné vidět příkaz „*tracert*“, který zobrazuje cestu ze stanice s IP adresou 172.16.1.2 na server Seznam.cz, který se nachází na adrese 77.75.77.39. Cesta začíná na defaultní bráně počítačové stanice, ze které byl příkaz vyslán, IP adresa brány je 172.16.1.1. Dále vede spojení na IP adresu 10.10.10.1 sériové linky směrovače Rocky. Cesta dále vede na IP adresu 212.111.15.190, jenž je adresa sériové linky směrovače ISP. Poté se pokračuje na adresu 212.0.0.2, která náleží sériové lince směrovače Internet. Ze směrovače Internet pak vede finální cesta na adresu 77.75.77.39, která patří Seznam.cz

ZÁVĚR

V této práci byl proveden návrh sítě pro středně velkou firmu v simulačním prostředí Packet Tracer na úrovni CCNA. Hlavním cílem byla konfigurace všech aktivních prvků podle zadání, které tato firemní síť využívá.

Při tvorbě této práce v simulačním prostředí Packet Tracer byly uplatněny teoretické poznatky, které se převedly do praktické části. Vzhledem k tomu, že Packet Tracer má rozdílné chování na rozdíl od reálných aktivních prvků, které se využívají v praxi, bylo by vhodnější provádět simulaci v mnohem propracovanějším prostředí než je Packet Tracer, jelikož tento program postrádá absenci některých příkazů. Ideálním řešením je emulační prostředí GNS3. V tomto emulačním prostředí se přímo pracuje s binárními soubory IOSu.

Aby počítačová síť fungovala správně, je nutné již od začátku navrhnout přehledný postup, který umožní jednoduchou správu sítě a případně budoucí rozšíření o další technologie, bez zbytečných problémů a složitého přenastavení. Práce může být do budoucna rozšířena o zabezpečení sítě především proti fyzickým útokům a živelným pohromám. Dále může být nastaveno vzdálené připojení pomocí VPN klienta. Daná síť se může rozšířit o další koncové periferie, jako jsou tiskárny, notebooky pro, které je možné vytvořit novou Wi-Fi síť. Vzhledem k tomu, že ve firemní sítí funguje služba VoIP, která má větší nároky na datový provoz, může při rozšiřování sítě dojít ke snížení kvality ostatních služeb. Proto by bylo vhodné se zaměřit na QoS této sítě a stanovit priority dle toho, co má v síti největší přednost.

CONCLUSION

In this work was made a draft computer network for a mid-sized company in the Packet Tracer simulation environment on CCNA level. The main goal was to configure all active devices according to the assignments used by this company network.

During the creation of this work in the Packet Tracer simulation environment, the theoretical knowledge has been applied, which has been transformed into a practical part. Since Packet Tracer has different behaviors, as opposed to real-life active devices, it would be preferable to perform simulation in a much more sophisticated environment than Packet Tracer, as this program lacks the absence of some commands. The ideal solution is the GNS3 emulation environment. In this emulation environment, IOS binaries work directly.

In order for the computer network to function properly, it is necessary to propose a clear procedure from the beginning to make it easy to manage the network and possibly future enhancements to other technologies, without unnecessary problems and complicated re-setup. Work may be extended in the future to network security, especially against physical attacks and natural disasters. In addition, remote VPN client connections can be set. The network may be extended by other end devices, such as printers, laptops for which you can create a new Wi-Fi network. Due to the fact that the company's VoIP service, which has more data traffic, it may decrease the quality of other services while expanding the network. Therefore, it would be advisable to focus on the QoS of this network and to prioritize it according to what has the highest priority in the network.

SEZNAM POUŽITÉ LITERATURY

[1] LAMMLE, Todd. *CCNA: výukový průvodce*. Brno: Computer Press, 2015. ISBN 978-802-5146-026.

[2] BOUŠKA, Petr. *Cisco IOS 5 - komunikace se switchem* [online]. 2007 [cit. 2017-05-05]. Dostupné z: http://www.samuraj-cz.com/clanek/cisco-ios-5-komunikace-se-switchem/

[3] *Obrázek* [online]. [cit. 2017-05-26]. Dostupné z: http://docstore.mik.ua/univercd/illus/2/66/28066.gif

[4] THOMAS, Thomas M. *Zabezpečení počítačových sítí bez předchozích znalostí*. Brno: CP Books, 2005. Cisco systems. ISBN 80-251-0417-6.

[5] *CCNA kompletní přehled příkazů: autorizovaný výukový průvodce*. Brno: Computer Press, 2009. ISBN 978-80-251-2286-0.

[6] *Obrázek* [online]. [cit. 2017-05-05]. Dostupné z: https://upload.wikimedia.org/wikipedia/commons/thumb/0/04/Cisco-router-1.svg/600px-Cisco-router-1.svg.png

[7] SHINDER, Debra Littlejohn. *Počítačové sítě: nepostradatelná prírucka k pochopení sítové teorie, implementace a vnitrních funkcí [sic]*. Praha: SoftPress, c2003. Cisco systems. ISBN 80-864-9755-0.

[8] BOUŠKA, Petr. *TCP/IP - adresy, masky, subnety a výpočty* [online]. 2007 [cit. 2017-05-05]. Dostupné z: http://www.samuraj-cz.com/clanek/tcpip-adresy-masky-subnety-a-vypocty/

[9] *Network subnets* [online]. [cit. 2017-05-05]. Dostupné z: https://www.ibm.com/support/knowledgecenter/cs/SS2GNX_5.1.1/com.ibm.tivoli.tpm.net.doc/network/tnet_cfgsubnets.html

[10] LAMMLE, Todd. *CCNA: výukový průvodce přípravou na zkoušku 640-802*. Brno: Computer Press, 2010. ISBN 978-802-5123-591.

[11] SPORTACK, Mark A. *Směrování v sítích IP: [autorizovaný výukový průvodce : samostudium : kompletní zdroj informací o směrování a protokolech v sítích IP]*. Brno: Computer Press, 2004. Cisco systems. ISBN 80-251-0127-4.

[12] ODOM, Wendell, Rus HEALY a Naren MEHTA. *Směrování a přepínání sítí: autorizovaný výukový průvodce*. Brno: Computer Press, 2009. Samostudium. ISBN 978-80-251-2520-5.

[13] BOUŠKA, Petr. *Cisco IOS 9 - Spanning Tree Protocol* [online]. 2007 [cit. 2017-05-05]. Dostupné z: http://www.samuraj-cz.com/clanek/cisco-ios-9-spanning-tree-protocol/

[14] BOUŠKA, Petr. *Cisco IOS 8 - ACL - Access Control List* [online]. 2007 [cit. 2017-05-05]. Dostupné z: http://www.samuraj-cz.com/clanek/cisco-ios-8-access-control-list/

[15] BOUŠKA, Petr. *VLAN - Virtual Local Area Network* [online]. 2007 [cit. 2017-05-05]. Dostupné z: http://www.samuraj-cz.com/clanek/vlan-virtual-local-area-network/

[16] WALLACE, Kevin. *Cisco VoIP: autorizovaný výukový průvodce*. Brno: Computer Press, 2009. Samostudium. ISBN 978-802-5122-280.

[17] WALLACE, Kevin. *VoIP bez předchozích znalostí*. Brno: Computer Press, 2007. Cisco systems. ISBN 978-80-251-1458-2.

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

ACL	Access Control List
CCM	Cisco Call Manager
CIDR	Classless Inter-Domain Routing
COM	Hardwarové rozhraní
CPU	Central Processing Unit
CST	Common Spanning Tree
DOS	Denial of Service
EIGRP	Enhanced Interior Gateway Routing Protocol
GIP	Gateway Information Protocol
H.225	Telekomunikační protokol
H.245	Telekomunikační protokol
H.323	Telekomunikační protokol
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
HW	Hardware
ICMP	Internet Control Message Protocol
IOS	Internetwork Operating System
IPV4	Internet Protocol version 4
IPV6	Internet Protocol version 6
ISL	Inter-Switch Link
ITU	International Telecommunication Union
MAC	Media Access Control
MCU	Multipoint Control Unit
MGCP	Media Gateway Control Protocol

OSPF	Open Shortest Path First
PVST+	Per Vlan Spanning Tree Plus
RIP1	Routing Information Protocol version 1
RIP2	Routing Information Protocol version 2
RJ-45	Kabel typu UTP a STP
RSTP	Rapid Spanning Tree Protocol
RTP	Reliable Transport Protocol
SIP	Session Initation Protocol
SSH	Secure Shell
STP	Spanning Tree Protocol
SW	Software
TCP/IP	Transmission Control Protocol/Internet Protocol
VLAN	Virtual Local Area Network
VLSM	Variable Length Subnet Mask
VOIP	Voice Over Internet Protocol
VTP	Vlan Trunk Protocol

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM PŘÍLOH

P I: Návrh počítačové sítě v Packet Traceru – na CD

P II: Konfigurační soubory aktivních zařízení – na CD