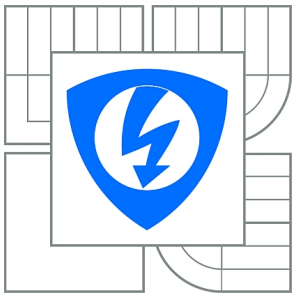
VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

BRNO UNIVERSITY OF TECHNOLOGY



FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ

ÚSTAV TELEKOMUNIKACÍ

FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION

DEPARTMENT OF TELECOMMUNICATIONS

PODPORA PROJEKTOVÁNÍ SÍTÍ

NETWORK DESIGN SUPPORT SOFTWARE

BAKALÁŘSKÁ PRÁCE

BACHELOR'S THESIS

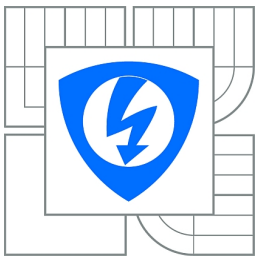
AUTOR PRÁCE — ALEŠ ŠPIDLA

AUTHOR

VEDOUCÍ PRÁCE — Ing. TOMÁŠ PELKA

SUPERVISOR

BRNO 2010



VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

Fakulta elektrotechniky a komunikačních technologií

Ústav telekomunikací

Bakalářská práce

bakalářský studijní obor
Teleinformatika

Student: Aleš Špidla ***ID:*** 111148
Ročník: 3 ***Akademický rok:*** 2009/2010

NÁZEV TÉMATU:

Podpora projektování sítí

POKYNY PRO VYPRACOVÁNÍ:

Úkolem studenta je v bakalářské práci podrobně popsat, porovnat a kriticky zhodnotit metodiky návrhu rozsáhlých počítačových sítí. Student navrhne a realizuje webovou aplikaci pro návrh sítí, tato aplikace bude implementovat nastudované metodiky včetně nástrojů pro usnadnění tvorby dokumentace a adresovacích plánů. Bude sloužit jako intuitivní průvodce návrháře sítě, výstupem této aplikace bude úplná dokumentace včetně adresního plánu.

DOPORUČENÁ LITERATURA:

[1] DONAHUE, Gary A. Network Warrior. 1st edition. [s.l.] : O'Reilly Media, Inc., 2007. 598 s. ISBN 978-0596101510.
[2] Cisco Systems, Inc.. Network Design and Case Studies. 2nd compl. edition. [s.l.] : Cisco Press, c1999. 1056 s. ISBN 1-57870-167-8.

Termín zadání: 29.1.2010 ***Termín odevzdání:*** 2.6.2010

Vedoucí práce: Ing. Tomáš Pelka

prof. Ing. Kamil Vrba, CSc.
Předseda oborové rady

UPOZORNĚNÍ:

ANOTACE

Jak již název napovídá, je práce zaměřena na podporu návrhu počítačových sítí. V práci jsou popsány kroky, které je třeba podniknout k úspěšnému navrhnutí počítačové sítě. Dále jsou zde zmíněny chyby, kterým je třeba se vyvarovat, různé doporučení od uložení zařízení do patch panelu, až po rozdělování adresního prostoru IP adres. Je zde zmíněná třívrstvá hierarchie sítě, kvalita služeb, problematika VLAN sítí a kaskádového zapojení přepínačů. Nemalá část práce se věnuje výhodám stohovatelných přepínačů jejich zařazení do sítě, dále popisuje výhody a druhy různých PoE (Power over Ethernet) zařízení. Za zmínku stojí také část kapitoly, která se věnuje IP sítím. Ta poukazuje na to, jak správně alokovat IP adresy a je zde také popsána nejvyužívanější metoda pro alokaci podsítí a to reverzní binární metoda.

Poslední část práce se věnuje popisu navržené aplikace, která umožní uživateli seznámit se s různými variantami přepínačů, VoIP telefonů, dozví se zde výhody a nevýhody různých přenosových médií nebo rozdíl mezi softwarovým nebo hardwarovým firewallem. Výstupem této aplikace je formulář, který bude sloužit pro zdokumentování sítě.

Klíčová slova: návrh sítě, QoS, stohování, PoE, IP adresy

ABSTRACT

The bachelor thesis is aimed at supporting of designing of computer networks. The thesis describes the steps which follows to successful propose of computer network. Furthermore, it discusses errors which should be avoided, the various recommendations from the positioning of devices in the patch panel, to allocating the address space of IP addresses. There is also mentioned three level hierarchy of networks, QoS, problems of VLANs and switches cascade connection. A large part describes the benefits of stackable switches, their inclusion in the network, and then describes the advantages of different kinds of PoE (Power over Ethernet) devices. Also noteworthy is the chapter, which deals with IP networks. It points out how to allocate IP addresses and it also describing the most frequently used method for allocating subnets which is reverse binary method.

The last part is devoted to the description of the application, which allows users to learn about different variants of switches, VoIP phones, find out the advantages and disadvantages of different transmission media, or the difference between software or hardware firewall. The output of this application is form, which can serve as network documentation.

Keywords: net design, QoS, stackable, PoE, IP adrress

ŠPIDLA, A. *Podpora projektování sítí: bakalářská práce*. Brno: FEKT VUT v Brně, 2010. 40 stran, 1 strana příloh. Vedoucí práce Ing. T. Pelka

Prohlášení

Prohlašuji, že svou bakalářskou práci na téma „Podpora projektování sítí“ jsem vypracoval samostatně pod vedením vedoucího bakalářské práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou všechny citovány v práci a uvedeny v seznamu literatury na konci práce. Jako autor uvedené bakalářské práce dále prohlašuji, že v souvislosti s vytvořením této bakalářské práce jsem neporušil autorská práva třetích osob, zejména jsem nezasáhl nedovoleným způsobem do cizích autorských práv osobnostních a jsem si plně vědom následků porušení ustanovení § 11 a následujících autorského zákona č. 121/2000 Sb., včetně možných trestněprávních důsledků vyplývajících z ustanovení § 152 trestního zákona č. 140/1961 Sb.

V Brně dne 31.5.2010

podpis autora

Poděkování

Děkuji vedoucímu práce Ing. Tomáši Pelkovi za užitečnou pomoc, cenné rady a zapůjčení materiálů při zpracování bakalářské práce.

V Brně dne 31.5.2010

podpis autora

Obsah

1 Úvod

Navrhnout správně a bez chyby počítačovou síť je někdy považováno za umění. I člověk, který se v oboru pohybuje několik let a má za sebou spoustu návrhu se může dopustit chyby, či na něco zapomenout. Následující práce poukazuje na hlavní body návrhu sítí, upozorňuje na chyby, kterým je třeba se vyvarovat, a nabízí řadu rad a tipů, které ulehčí jak návrh, tak následnou správu sítě. Práce popisuje, co je potřeba pro napsání dokumentace, co je potřeba zjistit ještě před navrhováním sítě a co všechno je potřeba sepsat, aby se z dokumentace dalo zjistit vše potřebné o navřené síti.

Dále se v práci popisují různé metody návrhu sítí, kvalita služeb QoS a její výhody, jsou zde zmíněny také virtuální sítě VLAN a jejich propojení. Užitečná je mimo jiné také kapitola ohledně stohovatelných přepínačů a přepínačů podporujících technologii PoE, které značně ulehčují práci na síti. Dále je v práci popsáno, jak vhodně alokovat IP adresy a jejich rozdělení do podsítí.

Cílem práce není naučit člověka, jak navrhnout správně počítačovou síť, protože to se naučí až praxí. Práce by měla právě pomoct při navrhování, aby nebylo na nic zapomenuto, a aby se nemusely řešit složité problémy právě špatně navržených sítí.

V závěru práce je popsaná navržená aplikace, která slouží jako průvodce pro návrh sítí, odkazuje na doporučené zařízení a obsahuje formulář, který by měl posloužit ke zdokumentování sítě.

2 Dokumentace

2.1 Požadavky

Návrh sítí obsahuje mnoho důležitých bodů, na které se snadno zapomíná, což může způsobit problémy nejen projektantovi, který síť navrhl, ale také správci dané sítě. V následujícím textu bude popsáno krok po kroku, co je nutné udělat, jaké použít technologie, na co by se nemělo zapomenout, či co je možné vynechat. Mezi základní a nejdůležitější části patří dokumentace, která pomáhá získat lepší orientaci v tom, co se právě dělá a ve výsledku z ní mohou čerpat správci při administraci, opravě či rozšíření sítě.

Na úvod návrhu sítě je třeba si uvědomit, že konečný návrh sítě musí odpovídat požadavkům, které byly zadány budoucím uživatelem sítě.

Patří zde mimo jiné:

- počet uživatelů
- druhy použitých koncových (VoIP telefony, síťové tiskárny s jejich umístěním)
- bezdrátové technologie
- prvky zabezpečení sítě (firewall apod.)
- jaké rozhraní mají síťové prvky podporovat apod.

To všechno by mělo být obsaženo v dokumentaci, stejně jako další kroky, které umožní navrhnout správně síť, jak pro malé tak pro rozsáhlejší firmy. Pokud člověk nikdy nedělal žádnou dokumentaci, je dobré, aby s tím začal, protože bez ní se v síti ztratí dřív, než ji vlastně celou navrhne. Je možné, že síť bude navržena, vše bude fungovat, ale pokud nastoupí na pozici správce sítě někdo, kdo nestál u návrhu, může vzniknout problém. Pokud síť funguje, je vše v naprostém pořádku, ale firmy se rozrůstají, lidé přicházejí a odcházejí a technologie jde nezadržitelným tempem kupředu. Právě proto je tak důležité projekt či návrh pečlivě zdokumentovat, aby z něj budoucí správci dané sítě mohli vycházet. Dokumentaci je nutno psát podrobně a srozumitelně s logickou strukturou, aby se v ní dokázal kdokoliv rychle zorientovat. A to bez ohledu na předchozí zkušenosti. Dobře napsaná dokumentace ulehčí mnoho a mnoho času při hledání zdrojů problémů. Důležitou součástí dokumentaci je topologické schéma sítě a také plán budovy s umístěním zásuvek, aktivních prvků, síťových tiskáren a dalších podstatných částí síťové infrastruktury.

Dokumentace musí obsahovat shrnutí požadavků, které daná síť musí splňovat. Jaké bude obsahovat síťové prostředky, počet uživatelů, jejich rozdělení do kanceláří,

kolik síťových zásuvek bude na jednoho uživatele, kde je umístěna serverovna, kolik serverů bude potřeba, jestli na každém patře nebo bude končit vše v jednom, kolik bude mít stanice ethernetových rozhraní, jaké propojení musí podporovat apod. Samozřejmě v některých bodech se liší dokumentace sítě navrhované do již existujícího prostředí – budovy, areálu od dokumentace sítě budované zároveň s budovou-areálem „na zelené louce“.

Zdokumentovat požadavky, které jsou na síť kladeny, je velice důležité, pro minimalizaci pozdějších konfliktů a nedorozumění se zadavatelem. Právě proto je na místě zmínka o tomto ne zrovna technickém tématu, protože díky dokumentaci se dá těmto problémům předejít.

V tuto chvíli jsou sepsány požadavky na síť. Ty jsou odeslány ke kontrole a až po potvrzení, že je vše v pořádku a všichni zúčastnění souhlasí, může se přistoupit k navrhování sítě.

2.2 Porty, stohování

Stěžejní a často opomíjený problém je konečný počet portů, který bude potřeba. Toto číslo samozřejmě nikdy není konečné, proto se musí počítat s dostatečnou rezervou. Při špatném navržení počtu portů hrozí nebezpečí, že nastoupí do firmy 5 nových zaměstnanců kteří potřebují přístup do sítě a není je kam „zapojit“. Vědět, kolik bude potřeba portů, je důležité především pro výběr aktivních prvků - přepínačů. Pokud přijde požadavek od zadavatele na 200 uživatelů, musí se počítat s tím, že daná síť se může rozrůstat. Obecně se bere v úvahu 15% růst, což z požadovaných 200 udělá 230 portů. K tomuto počtu je nutno připočíst počet síťových tiskáren, serverů, kamer, zabezpečovacích prvků atd., tedy všechny prvky, které je nutno zapojit do síťové infrastruktury. Pokud by bylo třeba 20 tiskáren, 10 kamer a 5 serverů, hned se jedná o 35 portů navíc. Jestliže se 15% růstem se zastavil počet portů na 230, tak už nastává problém, který vznikl mezi zadavatelem sítě a tím, kdo jí navrhuje. Znovu se zdůrazňuje potřeba jasného zadání požadavků na síť, co všechno má síť obsahovat, ať je jasné přesné číslo portů. Poté se k tomu číslu připočte 15% růst a dojdeme k číslu 270. V současné době lze koupit gigabitové přepínače s maximálním počtem portů, který odpovídá násobkům 48. Pro uvedený výpočet to vychází na šest 48 portových přepínačů. Z toho nám to vychází na 5 přepínačů pro uživatele a jeden pro servery, tiskárny a kamery.

Rozdělení přepínačů podle využití portů je individuální, ale doporučuje se oddělit alespoň stanice od serverů, kamer, wifi access pointů a podobných prvků. Když

po čase dojde na přepojovaní nebo výměnu kabeláže, je dobře patrné, kde co je a ušetří se tím starosti se zdlouhavým pátráním, kam který kabel vede.

Novější verze přepínačů lze propojit do stohu. Díky tomu se propojené přepínače chovají jako jeden logický přepínač, který používá jednu IP adresu. Celý stoh pak může být spravován, jako by se jednalo o jeden přepínač. U přepínače Cisco 3750 se toto propojení provádí pomocí speciálního stohovacího kabelu v zadní části přepínače, který disponuje rychlostí 32Gb/s. Pokud se bude stohování využívat, mělo by to opět být zapsáno v dokumentaci (více o stohovatelných přepínačích bude popsáno níže).

Následující citace popisuje potřebu vyhrazení trunk portů mezi přepínači:

Přepínače ve failover párech musí být vzájemně propojeny, obvykle vícegigabitovými linkami. Pokud používáte moduly FSM (Firewall Services Modules), měly by pro ně existovat vyhrazené trunky. Moduly CSM (Kontent Service Modules) by rovněž měly mít své vlastní trunky, stejně jako analyzátor RSPAN, pokud jej budete používat. Pokud budeme počítat s 2Gb/s EtherChannely pro každý z těchto trunků, právě jste alokovali 16 portů. [1]

Je důležité si toto uvědomit a dát si na to pozor, protože 16 portů už je docela velké číslo.

Jakmile je znám počet portů, které budou potřeba, je na čase sepsat seznam hardwaru potřebný pro splnění zadaných požadavků . Toto je nejlepší sepsat do přehledné tabulky, kde bude kromě názvu zařízení také jeho funkce, umístění a jaké rozhraní podporuje. Další tabulka by měla popisovat, co je připojeno do jednotlivých portů daných zařízení. U přepínačů je třeba také popsat trunk porty a porty, kde jsou zapojeny další VLAN sítě. Čím podrobnější tato tabulka bude, tím lépe se bude síť spravovat, případně řešit dané problémy. Tabulka obsahuje hlavní přepínač Cisco řady 6500,dva systémy firewallů a dva systémy pro sítě VPN s protokolem IPsec. Tyto systémy jsou integrovány se strojem Supervisit Engine. Obsahují duální rozhranní pro Gigabit Ethernet. Tento přepínač obsahuje 9 slotů, které je vhodné rozepsat do tabulky. Tím se vytvoří podrobný přehled použitých zařízení. Tento popis zobrazuje následující tabulka č.1.

Tabulka č.1: Příklad tabulky pro obsazení přepínače.

Název zařízení	**Funkce**	**Umístění**	**Rozhraní 10/100/1G**
Cisco 3750G-48TS	48portový 10/100/1000	Stojan 1	48
Cisco 3750G-48TS	48portový 10/100/1000	Stojan 1	48
Cisco 3750G-48TS	48portový 10/100/1000	Stojan 1	48
Cisco 3750G-48TS	48portový 10/100/1000	Stojan 1	48
Cisco 3750G-48TS	48portový 10/100/1000	Stojan 1	48
Cisco 3750G-48TS	48portový 10/100/1000	Stojan 2	48
Cisco ASA 5520	Firewall	Stojan 2	
Catalyst 2811	Internetový směrovač	Stojan 2	
Cisco 7800	Media Convergence Server	Stojan 2	

2.3 Rozpis IP adres

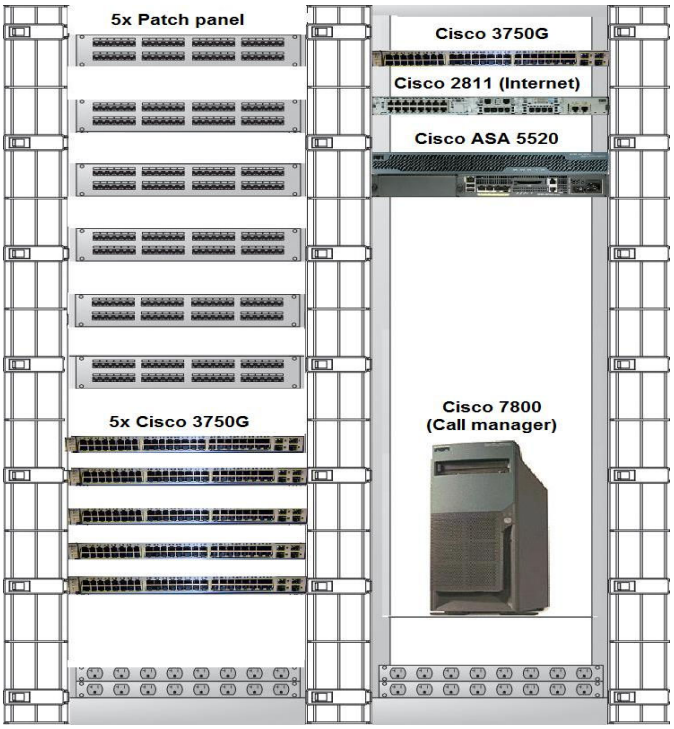
Další důležitou součástí dokumentace je rozpis IP adres pro jednotlivé zařízení. Měl by obsahovat veškeré VLAN sítě a použité zařízení od tiskáren až po Access pointy. Jak by mohla tabulka vypadat je zobrazeno v tabulce č. 2.

Tabulka č.2: Rozvržení IP adres.

IP adresa	Maska podsítě	VLAN	Popis
192.168.1.0	255.255.255.0		Síť
192.168.1.1	255.255.255.0	10	Stoh 1
192.168.1.2	255.255.255.0	10	Callmanager
192.168.1.3	255.255.255.0	10	AP 1.patro
192.168.1.4	255.255.255.0	10	AP 2.patro
192.168.1.7	255.255.255.0	10	Kamera č.1
192.168.1.8	255.255.255.0	10	Kamera č.2
192.168.1.9	255.255.255.0	10	Volné
192.168.1.9	255.255.255.0	10	Volné
192.168.10.2	255.255.255.240	20	Kopírka č.1
192.168.10.3	255.255.255.240	20	Kopírka č.2

2.4 Návrh rozmístění modulů ve stojanech

Tento návrh pomáhá předejít situaci, kdy se při instalaci modulů do stojanů zjistí, že je nedostatek místa. Kromě navržených zařízení nesmí být zapomenuto na patch panely, které u větších firem zabírají nemalé místo, napájení a kabely. Je dobré, když jsou kabely vedeny bokem případně v „tunelech“, aby nedošlo k situaci, kdy je 200 kabelů vedených přes sebe a jsou do sebe zapletené, což značně komplikuje připojování dalších zařízení nebo výměnu vadného kabelu. Proto je vhodné nechávat prostor mezi patch panely.



Obrázek č.1: Rozvržení modulů ve stojanech 1,2.

2.5 Napájení a chlazení

Co se týče požadavků na spotřebu a chlazení, je velice jednoduchý způsob, jak je zjistit. Stačí sečíst požadavky napájení jednotlivých modulů pro každou skříň. Místnost, kde budou rack skříně umístěny, musí splňovat tyto požadavky, aby nedocházelo k přehřátí modulů. Na většině stránkách prodejců lze nalézt jak popis napájení, tak také požadavky na chlazení. Je třeba používat maximální hodnoty a ne hodnoty v klidovém režimu, kdy zařízení nepracuje. Pozor také na omezení pro jednu skříň v prostorách, kde se budou skříně nacházet. Podobné omezení může nastat také v případě napájení, kdy se musí počítat s proudovým omezením napájecích modulů. Jak by mohla vypadat tabulka, která zobrazuje spotřebu energie, proud a tepelný výkon je zobrazeno v tabulce č.3. Z ní je patrné, že můžou být bez problému v jedné skříni použity všechny výše zmíněné přepínače i s rezervou, protože napájecí moduly obsažené ve skříních pro kolokační centra, jsou většinou dva s 20 A jističem a moduly z tabulka č.3 spotřebují maximálně 15 A. Při návrhu napájení a chlazení nesmí být opomenuto záložní napájení všech podstatných prvků síťové infrastruktury pro minimalizaci škod při výpadku napájení. U přepínačů, do kterých jsou připojena koncová zařízení napájená z těchto přepínačů pomocí PoE (Power over Ethernet) je nutno počítat s vyšší spotřebou a vyšším vyzářeným tepelným výkonem. Tabulka musí také obsahovat příkon a vyzářený tepelný výkon všech serverů, diskových polí apod.

Tabulka č. 3 Hodnoty spotřeby energie, BTU a proudu. [3]

Zařízení	**Spotřeba [W]**	**Maximální BTU/h**	**AC [A]**
Cisco 3750G-48TS	160	545,92	1,5-3
Cisco 3750G-48TS	160	545,92	1,5-3
Cisco 3750G-48TS	160	545,92	1,5-3
Cisco 3750G-48TS	160	545,92	1,5-3
Cisco 3750G-48TS	160	545,92	1,5-3
Celkem	800	2729,6	15

2.6 Pojmenování zařízení

K samotnému pojmenování zařízení slouží nejlépe pravidlo čím jednodušší tím lepší. Jedná se o velice individuální záležitost, ale je důležité, především u rozsáhlejších sítí, aby bylo z názvu patrné, kde se zařízení nachází, jeho pořadové číslo v daném místě a hlavně jakou plní funkci. Pojmenování by měla být dobře zapamatovatelná, ne složitěji než adresa IP.

3 Návrh sítí

3.1 Třívrstvý hierarchický model návrhu sítí

Hierarchické síťové topologie ohraničují provoz do jednotlivých lokálních oblastí. Tento model má tři vrstvy, které se nazývají přístupová, distribuční a vrstva jádra. Každá vrstva odděluje provoz v síti od ostatního provozu zasílaného mezi oblastmi dané LAN sítě. V současné době je tento model nejpoužívanější, protože v sobě ukrývá několik důležitých výhod. Protože je síťový provoz rozdělen do několika oblastí, dochází ke snížení počtu kolizních domén a tím pádem se zvyšuje výkon sítě. Vzniklé chyby jsou uzavřeny právě v oblasti, kde vznikly a je jednodušší je lokalizovat. Je zde také vyšší bezpečnost, protože provoz v síti je řízen právě mezi vrstvami sítě.

Přístupová vrstva

Rozděluje pomocí rozbočovačů a přepínačů hostitelská zařízení do různých segmentů sítě. Jsou zde poslední články sítě. U rozsáhlejší sítě, může přístupová vrstva obsahovat také směrovače, které zvyšují bezpečnost interní sítě.

Distribuční vrstva

Úlohou distribuční vrstvy je oddělit vysokorychlostní provoz páteřní sítě od pomalejší lokální sítě. Z toho je zřejmé, že jsou zde obsaženy směrovače. Díky „inteligenci“ směrovačů, kdy zkoumají obsah hlavičky příchozích paketů, urychlují činnost sítě, protože odesílají pakety pokud možno přímo do cíle. Zařízení v distribuční vrstvě provádí také směrování zpráv mezi jednotlivými virtuálními sítěmi VLAN. Dále se v této vrstvě provádí převody adres, seskupování adres a oblastí, zabezpečení síťového provozu, převody mezi protokoly IP a IPX, šifrování pro potřeby tunelování ve VPN sítích.

Vrstva jádra

Jedná se o páteřní vrstvu sítě, na kterou jsou napojeny jednotlivé segmenty LAN sítě. Může být složena z několika páteřních sítí, což je například u internetové sítě, která obsahuje páteřní sítě firem a regionální sítě. Páteřní sítě většinou propojují jednotlivé oblasti LAN sítí, například jednotlivé patra kancelářských budov. Páteřní síť by měla

být rychlá a přenos paketů mezi různými segmenty bez zbytečných přerušení. Toho se docílí právě pomocí distribuční vrstvy, která zajišťuje propojení jednotlivých segmentů LAN sítě. Směrovače distribuční vrstvy tedy zpracovávají adresy a proto se využívá přepínaných páteřních sítí.

3.2 Další možné typy sítí

Zhroucené jádro bez distribuční vrstvy

Tento případ se používá hlavně v případech, kdy se jedná o síť firmy, která se nachází v jedné budově. Přepínače jádra a přístupové přepínače mohou být rozděleny mezi patry, nebo je možné je umístit do serverovny, kde budou všechny pohromadě. Jelikož se jedná o malou firmu, je tento způsobu umístění lepší hlavně pro správce sítě, který má vše pohromadě.

Zhroucené jádro bez distribuční a přístupové vrstvy

Nejjednodušší je síť, která obsahuje pouze jednu vrstvu a to vrstvu jádra. Kabeláž se tedy vede od uživatelů nebo uživatelských zařízení přímo do přepínačů, ovšem musí splňovat limity pro délky vedení kabelů.

4 QoS - Quality of service – Kvalita služeb

Ať už kriticky důležitá aplikace sama zatěžuje šířku pásma sítě, nebo jestli je podobně náročnými aplikacemi sama dotčena, vždy je pro dnešní i budoucí provozuschopnost daného síťového provozu důležité navrhnout dobré řešení kvality služeb QoS. [2]

Kvalitu služeb určitě zná každý, kdo se trošku pohybuje mezi počítačovými sítěmi, nebo o ní minimálně slyšel. Jedná se o službu, která pomáhá upřednostnit na základě nastavené priority daný přenos, aby nedocházelo ke ztrátám paketů a zahlcení linky. Přenos s vyšší prioritou je odeslán dříve než ten s nižší. Důležité je předem si určit, který provoz by měl být upřednostňován před ostatními. Různé pakety, jako jsou TCP, UDP, FTP, HTTP a VoIP se liší právě různými potřebami pro přenos v síti od správného pořadí paketů v přijímací stanici, až po potřebu zajištění opravy v případě ztráty paketů.

Protokol TCP má schopnost upozornit odesílající stanici na to, že paket nedošel v pořádku nebo vůbec. Stanice tyto pakety znovu po tomto zjištění znovu odešle. Naopak UDP protokol žádné tyto informace neposkytuje, proto jsou aplikace založené na tomto protokolu háklivé na ztrátu paketů. Protokoly HTTP, FTP, SSH a telnet jsou založené na TCP protokolu. Ztráta paketů a prodleva času, kterou způsobuje právě opětovné odeslání ztraceného paketu nebývají problém. Naopak protokol VoIP si nemůže dovolit přijetí paketů v různém pořadí, například kvůli hlasovému přenosu.VoIP protokol je založený na TCP, UDP a RTP protokolech. Kvalita přenosu zvuku u VoIP protokolu je jedním z důvodů, proč byl QoS navržen.

4.1 Metody QoS

- FIFO - First in first out - pakety odcházejí v pořadí, v jakém přišly.
- WQF - Weigted fair queuing - pásmo se rozděluje podle váhy.
- CBWFQ - Clase based weigthed fair queuing - pásmo se dělí pomocí tříd.
- LLQ - Low latency queuing – spolu s CBWFQ vytváří prioritní fronty.
- IP RTP Prioritization – přídání low-latency do WFQ a CBWFQ, což je vhodné hlavně pro VoIP provoz. Provoz se zde definuje pomocí rozsahu UDP portů. [7]

4.2 Seznam protokolů a priorita služeb

Na začátku je třeba určit, jaké protokoly budou využity. Toto lze nejlépe zjistit softwarem pro zachytávání komunikace v síti, který jasně ukazuje, které protokoly jsou použity. Při přidělování priorit je třeba dbát na to, jestli je daný protokol opravdu tak důležitý. Například RTP protokol, který může být z hlediska důležitosti považován za prioritní, protože se využívá pro hlasový proud u VoIP, dokáže způsobit drobné komplikace, protože jej využívá mimo jiné také streamované video. V tomto případě je důležité nastavit sníženou prioritu právě pro video, aby nedocházelo k zhoršení kvality hlasového toku dat.

Určení správné priority není vždy tak lehké jak se může zdát. Administrátor musí vyhodnotit důležitost jednotlivých služeb a podle toho se rozhodovat, jak síťový provoz bude vypadat. Existují však již doporučené IP precedence, které pomohou určit priority a je dobré je dodržovat.

IP precedence 5 (DSCP: EF) zaručuje malé zpoždění, nízkou ztrátovost paketů a nízký jitter. Expedited Forwarding neboli urychlené posílání se používá hlavně pro služby v reálném čase, hlavně pro hlasové a video služby. IP precedence 3 (DSCP: AF)

by měla být u řídících paketů. Assured Forwarding, tedy zaručené posílání zařazuje pakety do jedné ze 4 tříd. Každé třídě je přidělena jedna ze tří priorit pro zahození paketu (drop precedence) v případě zahlcení přidělené paměti.

Výstupem návrhu QoS by měl být seznam, seřazený podle priority provozu. Hlasové pakety a pakety pro řízení hlasu by měly mít určitě vyšší prioritu než e-mail, http protokol nebo best effort (všechno ostatní), což jsou služby, které nemají žádné priority ani záruku doručení. Do této skupiny by měl patřit i protokol HTTP, ale existují výjimky, u kterých musí být prioritní provoz nastaven. Patří mezi ně například důležité webové aplikace. Nesmí se zapomínat také na to, že v případě kolize na síti a zahlcení linky musí být správce sítě schopen připojit se přes telnet nebo SSH protokol kamkoliv v síti bez omezení. Tyto protokoly nemají velké požadavky na provoz, takže jejich vysoká priorita nemá velký vliv na celkovou šířku pásma, proto by měly být hned za hlasovými službami.

Následující tabulka č.4 ukazuje hodnoty DSCP a přiřazené číslo precedence. IP precedence 6 a 7 se používají pro řízení mezi sítěmi a řízení sítě.

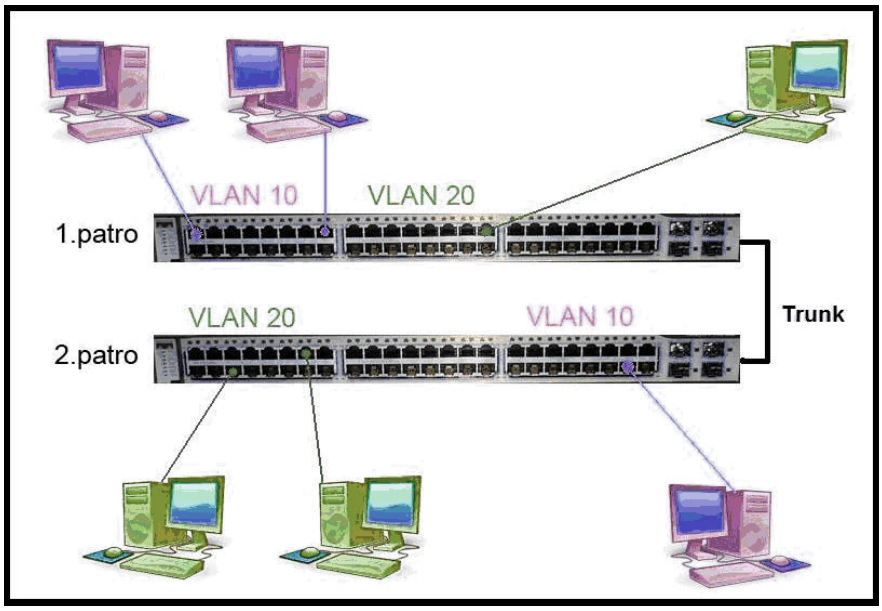
Tabulka č.4 Hodnoty DSCP.

PHB	**Třída**	**Priorita zahození paketu**			**Precedence**
Základní					0
AF (Zaručené posílání)		Nízká	Střední	Vysoká	
	1	AF 11	AF 12	AF 13	1
	2	AF 21	AF 22	AF 23	2
	3	AF 31	AF 32	AF 33	3
	4	AF 41	AF 42	AF 43	4
EF (Urychlené posílání)		EF			5

5 Virtuální sítě VLAN

Pokud je potřeba rozdělit uživatele, porty nebo například access pointy do odlišných sítí, nemusí se používat pro každou skupinu jednotlivý přepínač. V současné době se využívá sítí virtuálních neboli VLAN. Jedná se o to, že se vytvoří jednotlivé logické sítě nezávisle na fyzickém umístění. Ukázkový příklad je vyobrazen na obrázku č. 2. Jedná se o situaci, kdy je zapotřebí na dvou přepínačích v různých patrech vytvořit dvě skupiny počítačů, které patří do odlišných sítí. Pokud by nebyly použity VLAN sítě, musela by každá skupina mít svůj vlastní přepínač, což může být problém, protože jsou v různých patrech. Díky rozdělení do VLAN sítí můžou počítače komunikovat i s počítači připojených do druhého přepínače, musí však být ve stejné VLAN síti,

protože VLAN sítě mezi sebou nemůžou jen tak komunikovat. Komunikaci mezi sítěmi VLAN však lze zajistit pomocí přepínačů, což je popsáno níže.



Obrázek č.2: VLAN sítě v rozdílných přepínačích.

Výhody VLAN

- Jednodušší správa - pokud je zapotřebí přesunout zařízení do jiné sítě, stačí použít softwarové konfigurace a není třeba nic fyzicky přepojovat
- Vyšší bezpečnost - někdy je potřeba oddělit část sítě od zbytku a zamezit tam přístup. Toho se docílí právě díky VLAN. Dá se použít odděleného přepínače, ale VLAN řešení je určitě pohodlnější a praktičtější.
- Oddělení provozu - někdy je dobré oddělit některý síťový provoz od zbytku sítě. Například IP telefonie, access pointy nebo i síťové tiskárny můžou mít svou VLAN.

5.1 Komunikace a routing ve VLAN sítích

Můžou nastat dva případy, jak budou VLAN sítě navrženy. První způsob je, že budou obsazeny pouze v jednom přepínači, který má uložené informace o všech VLAN sítích a podle toho povoluje komunikaci. Druhý způsob, kdy jsou VLAN sítě ve dvou a více přepínačích, je značně složitější. Tady již musí být zajištěná komunikace mezi přepínači, což zajišťují protokoly ISL a 802.1q, které jsou popsány níže.

Routing je ve VLAN sítích to samé, co v klasických fyzických sítích. Jedná se o zajištění komunikace mezi jednotlivými sítěmi. V současné době se pro toto využívá L3 přepínače, které díky tomu, že obsahují směrovač, jsou schopny data směrovat bez externího směrovače připojeného přes trunk port k přepínači. Toto zapojení je známé jako „Router on stick“.

6 Stohování, kaskádové zapojení, trunk porty

6.1 Stohování a jeho výhody

Cisco StackWise, neboli technologie, díky které lze propojit směrovače do stohu. Tato technologie je určena pro přepínače Catalyst 3750, které jsou propojeny speciálním stohovacím kabelem, jak již bylo popsáno výše. Přepínače propojené do stohu sdílí stejný operační systém, tabulku MAC adres i informace o směrování. Díky tomu se jeví jako jedna logická jednotka, která má jedinou IP adresu. Tuto adresu nese master switch, jenž je určen automaticky nebo je zvolen správcem sítě. Pokud vypadne, je nahrazen jiným.

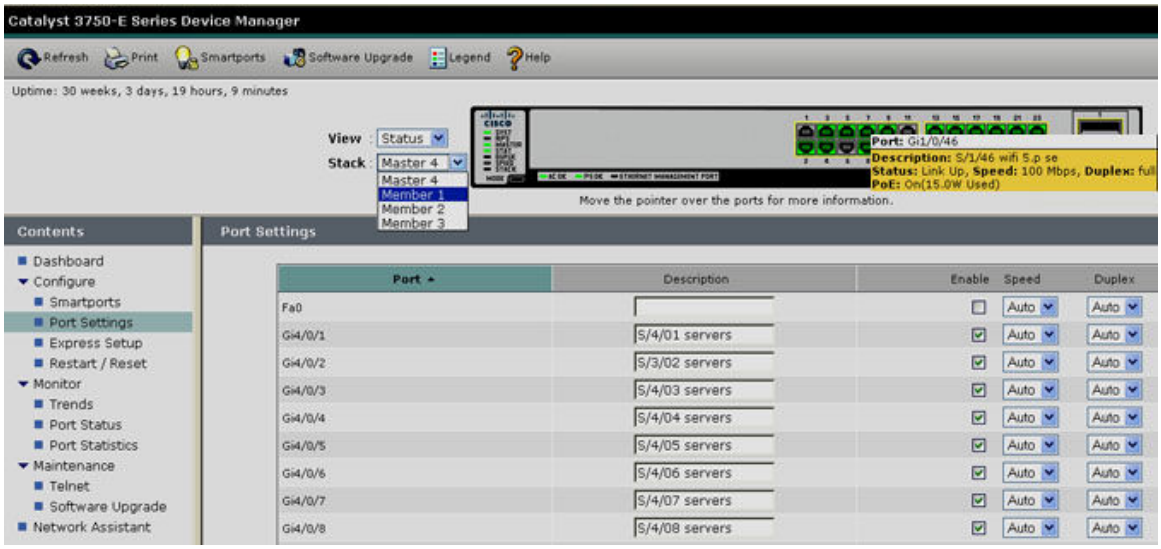
Do stohu může být zapojeno maximálně 9 přepínačů (u zařízení Cisco) s tím, že dojde k přerušení jednoho propojovacího modulu, nedojde k výpadku celého stohu, ale pouze poklesne propustnost na polovinu.

Nová technologie Cisco StackWise plus nabízí velikost propustnosti 64Gbps oproti původním 32Gbps. Používá ji zařízení 3750-E, ale tento přepínač je možné propojit do stohu i s 3750, ale v tom případě je použita technologie StackWise.

Výhod, které stohování přepínačů v distribuční vrstvě nebo v jádře přináší je mnoho. Mimo jiné jednodušší správu díky tomu, že se spravuje pouze jedno zařízení, nebo se zvyšuje odolnost proti výpadku.

Obrázek č.3 zobrazuje, jak snadno lze spravovat přepínače zapojené do stohu. V zobrazeném případě jsou ve stohu 4 přepínače, kde jeden je označen jako master a

ostatní jsou nazvány member 1, mebmer 2, member 3. Zelené porty značí obsazení, šedé naopak to, že nejsou využity. Najetím na obsazený port se zobrazí jeho popis a vlastnosti. Mimo jiné je se zde také jednoduše přidělují role jednotlivým portům, ale hlavně jsou všechny přepínače pod jednou IP adresou. Právě pro tuto jednoduchou správu je při navrhování rozsáhlejší sítě nutno zvážit nakoupení stohovatelných přepínačů, protože to ulehčí spoustu práce a času v následném nastavení i chodu sítě.



Obrázek č.3: Správa čtyř přepínačů ve stohu.

6.2 Kaskádové zapojení

Přepínače lze propojit kromě použití stohu také kaskádově. Jedná se o to, že další přepínač se k prvnímu připojí, jako by to byl klasický počítač. Nejsou tedy propojeny žádným speciálním kabelem, což značně snižuje rychlost přenosu dat (je možné propojit je pomocí trunk portů, ale toto řešení zabírá zbytečně moc portů, jak je popsáno výše). Proto je toto řešení považováno za provizorní, v případě náhlého nástupu například většího počtu zaměstnanců a následnému nedostatku RJ-45 zásuvek. Přepínač se tedy připojí přímo v kanceláři a ne do stohu v serverově.

6.3 Trunk porty

Trunk je propojení, které slouží ke komunikaci mezi více VLAN sítěmi současně. Jedná se tedy o přenos rámců ze zařízení, které je ve VLAN síti na jednom přepínači, do zařízení patřícího do stejné sítě na druhém přepínači. Rámec však pro tento přenos musí obsahovat zmínku o síti VLAN, což žádný z protokolů nad 2.vrstvou ani žádný z ethernetových protokolů nepodporuje. Proto byly vytvořeny protokoly ISL (Inter-Switch Link), jenž je přímo protokolem firmy Cisco a 802.1Q, vyvinutý organizací IEEE, které tuto úlohu plní.

Protože ne všechny přepínače podporují oba tyto protokoly, je potřeba po označení rámců, které mají být přeneseny přes trunk, aby se přepínače domluvili, jaký z těchto dvou protokolů bude použit. Rozdíl mezi oběma protokoly je v původu (Cisco a organizace IEEE), ale především v tom, že ISL podporuje pouze 1000 sítí, na rozdíl od 802.1Q, který podporuje až 4096 sítí. Další významný rozdíl je, jak je zacházeno s rámci. Zatímco protokol ISL zapouzdřuje rámce ethernetu na rámce ISL, protokol 802.1Q přidává k rámci hodnotu VLAN, čímž zaměňuje původní rámec.

Protokol ISL

Rámec zapouzdřený protokolem ISL je zobrazen na obrázku č.4 (velikost jednotlivých okének neodpovídá skutečné velikosti, kde největší část rámce tvoří DATA).

Hlavička ISL	Hlavička Ethernetu	Paket TCP	Hlavička Telnetu	Data	FCS

Obrázek č.4 Hlavička rámce zapouzdřeného protokolem ISL.

Pokud je použit protokol ISL při přenosu přes trunk, je původní rámec zapouzdřen do nového, který obsahuje na začátku navíc hlavičku ISL obsahující informace o VLAN a na konci kontrolní součet FCS (frame check sequence), který na rozdíl od původního počítá také s hlavičkou ISL. ethernetový.

S rozšířením ethernetového rámce, který byl vytvořen s určitou maximální velikostí, může dojít k situaci, kdy je rámec označen za vadný, kvůli své neobvykle velikosti, protože mu bylo přidáno 30 bajtů protokolem ISL.

Protokol 802.1Q

Tento protokol tím, že pouze pozměňuje původní rámec informací o VLAN síti, mění jeho velikost jen o 4 bajty, na rozdíl od 30 bajtů u protokolu ISL. Opět je to překročení maximální velikosti rámce, avšak ne tak velké. V obou případech však Cisco zařízení nemají problémy s jejich zpracováním.

Protokol DTP (Dynamic Trunking Protocol)

Jedná se o protokol, který některé zařízení Cisco používají pro automatické vytvoření trunků. DTP zjišťuje každých 30 vteřin, jaké trunk protokoly jsou podporovány na obou stranách a následně se pokusí trunk vytvořit.

7 Power over Ethernet - PoE

PoE technologie umožňuje menší koncové zařízení, jako jsou IP teleony, IP kamery nebo WiFi access pointy, napájet přes ethernetovou síť. Toto je zaručeno standardem IEEE 802.3af, která určuje požadavky na napájení přes ethernet. Aby bylo možné využít PoE technologii, je třeba, aby existovala dvě zařízení. Zařízení dodávající napětí a napájené zařízení.

- Zařízení dodávající napětí se značí PSE (Power sourcing equipment). Jedná se většinou o přepínače nebo směrovače, které pomocí síťového kabelu napájejí koncové zařízení. Ve standardu IEEE 802.3af je maximální výkon, který PSE dodává omezen na 15,4W.

- Napájená zařízení PD (Powered devices) jsou v současnosti většinou, jak již bylo zmíněno, IP telefony, IP kamery nebo wifi access pointy. Jejich maximální příkon je omezen na 12,95W.

7.1 PoE midspan

Ne všechny přepínače podporují PoE technologii. Pro rychlé zpřístupnění napájení přes ethernet se používá PoE injektor. Propojením přepínače s injektorem vzniká možnost napájení koncových zařízení přes porty v injektoru, který se tedy stává PSE zařízením. Výhodou je právě rychlé přizpůsobení přepínače PoE technologii.

7.2 PoE spillter

Další možným řešeni je zařízení zvané PoE splitter, které umožňuje napájet přes ethernet zařízení, která technologii PoE standardně nepoužívají. Lze sehnat také PoE splitter s měnitelným výstupním napětím.

7.3 Výhody PoE přepínačů

Cena

Díky využití pouze jednoho kabelu pro přenos dat i pro napájení odpadá nutnost napájecích kabelů a tedy i veškeré náklady ohledně zásuvek a elektroinstalace nezbytné pro napájení, které mohou být vysoké obzvlášť v těžko dostupných prostorech nebo u rozsáhlých hal.

Bezpečnost

PoE přepínače patří do SELV třídy zařízení pro malé napětí s nízkými bezpečnostními riziky. Přepínače jsou chráněny pře zkratem nebo jinou špatnou funkcí napájeného zařízení a to tak, že je možné na portech nastavit výkonové omezení. Bez něj by v případě zkratu mohl přestat fungovat celý přepínač a tím pádem i celá síť přes něj vedená.

PoE plus neboli Standard 802.3at

Díký nově vyvinutému standardu je možné přes síťový napájet koncová zařízení s požadovaným příkonem až 30W. Tím se rozšiřuje spektrum koncových zařízení, které mohou využívat PoE+ technologii (videotelefony, vysokorychlostní vysílače založené na technologii Wimax).

V dnešní době se již dají sehnat přepínače, které podporují jak stohování, tak PoE+ technologii. Jedním z takových je například přepínač GS724TPS. Ty lze však na rozdíl od přepínačů společnosti Cisco spojit do stohu s přenosem mezi přepínači 20GB/s (u Cisco přepínačů 32GB/s resp. 64GB/s) a počet přepínačů ve stohu je omezen na šest oproti devíti u Cisco přepínačů.

Rozdělení PD zařízení do tříd podle 802.3.af

Standard IEEE 802.3af rozděluje PB zařízení do několika tříd podle spotřebovaného příkonu. Díky těmto informacím, můžou být lépe určeny požadavky na daný přepínač, případně pro každý port, napájející dané zařízení přes ethernet, může být nastaveno výkonové omezení, jak bylo vysvětleno výše. Jednotlivé třídy zobrazuje tabulka č.5.

Tabulka č. 5. Třídy PB zařízení.

Třída	Využití	Maximální výkon na výstupu PSE	Maximální příkon na vstupu PD
0	Výchozí	15,4W	0,44 - 12,95W
1	Volitelné	4,0W	0,44 - 3,84W
2	Volitelné	7,0W	3,84 - 6,49W
3	Volitelné	15,4W	6,49 - 12,95W
4	Nepoužito	15,4W	Rezervováno

8 IP adresy

8.1 Privátní adresy

Každý už určitě někdy slyšel o skupině privátních adres, která je rozdělena do tří tříd. Tyto třídy vymezila organizace IANA

- Třída A 10.0.0.0 - 10.255.255.255
- Třída B 172.16.0.0 - 172.31.255.255
- Třída C 192.168.0.0 - 192.168.255.255

Vyznačené adresy by neměly být směrovány do internetu, protože každá síť, ať malá podniková, či globální internet, nesmí obsahovat dvě stejné adresy. Tedy každý uzel v síti musí obsahovat svou unikátní a jedinečnou adresu. Pokud by se tak stalo, paket by neprošel přes výchozí bránu, protože směrování by určilo, že odesilatel a cíl náleží do stejné sítě, i když tomu tak ve skutečnosti není.

Využití a rezervování IP adresních bloků popisuje dokument RFC 3330 [5]. Pro přiklad je uvedena adresa pro takzvanou zpětnou smyčku, nebo jedna z privátních adres.

127.0.0.0/16 - Tento blok je přidělen pro použití jako adresa zpětné smyčky internetového hostitele. Datagram odeslaný protokolem vyšší úrovně na libovolnou adresu v tomto bloku by měl dorazit ve smyčce zpět k hostiteli. Často jde o implementaci, která pro zpětnou smyčku používá pouze síť 127.0.0.1/32, ovšem žádné adres v tomto bloku by se nikdy neměly objevit nikde na žádné síti. [RFC1700, strana 5] [9]

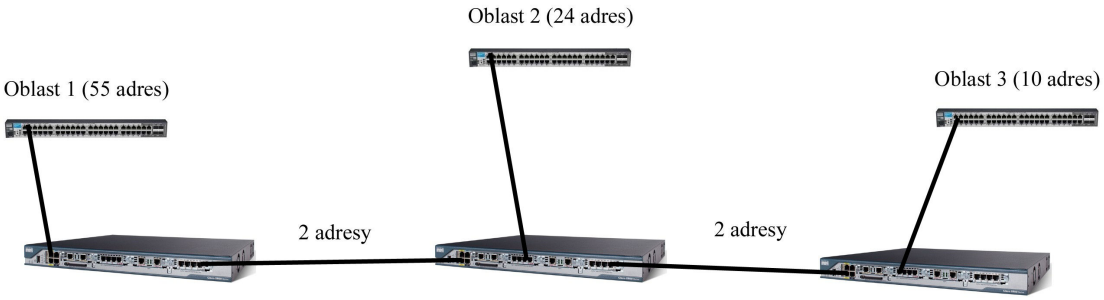
192.168.0.0/16 - Tento blok je vyčleněn pro použití v privátních sítích. Jeho použití je popsáno v [RFC1918] . Adresy v rámci tohoto bloku by se neměly objevit ve veřejném internetu. [10]

8.2 VLSM a CIDR

VLSM

Klasické pravidlo pro vytváření podsítí bylo vždy takové, že musely mít vždy stejnou velikost. To vedlo k neefektivnímu rozdělování IP adres a především k nevyužití sítí, které museli být vytvořeny. Toto řeší právě VLSM neboli adresování s maskou podsítě proměnné délky. Na následujícím případě (Obrázek č.5) je znázorněno, jak správně volit rozdělení podsítí a popsány právě výhody VLSM.

V první řadě je třeba si určit, kolik podsítí bude třeba, včetně počtu adres alokovaných pro danou podsíť. Pokud byla od poskytovatele internetu přidělena síť 210.10.0.0/24 rozdělíme ji na potřebný počet podsítí pomocí VLSM. Rozdělení na podsítě je vhodné si psát do tabulky, která by mohla vypadat jako tabulka č.6. Přidělování adres je vhodné dělat vzestupně nebo sestupně, v závislosti na počtu potřebných adres. Podle obrázku je největší oblast č.1, kde je potřeba 55 adres, tedy prefix o délce 6 bitů (musí se počítat také s určitou rezervou a také s adresou sítě a broadcastovou adresou). Další oblast požaduje 24 adres a poslední 10. Oblasti č. 4 a č.5 potřebují pouze čtyři adresy, protože se jedná o spojovací rozhraní.



Obrázek č.5: Síť a počty potřebných adres

Tabulka č.6: Adresní plán.

Oblast	Síť	Maska podsítě	Rozsah adres	Broadcast
1	210.1.30.64/26	255.255.255.192	210.1.30.65 až 210.1.30.126	210.1.30.127
2	210.1.30.32/27	255.255.255.224	210.1.30.33 až 210.1.30.62	210.1.30.63
3	210.1.30.16/28	255.255.255.240	210.1.30.17 až 210.1.30.30	210.1.30.31
4	210.1.30.4/30	255.255.255.252	210.1.30.5 až 210.1.30.6	210.1.30.7
5	210.1.30.0/30	255.255.255.252	210.1.30.1 až 210.1.30.2	210.1.30.3

Od poskytovatele internetu byla poskytnuta síť s prefixem /24. Z toho vyplývá, že na podsítě zbývá osm bitů. První podsíť potřebovala délku prefixu 6 bitů, což je 64 adres. Pokud by se nevyužilo VLSM, mohly by být vytvořené maximálně 4 adresy o délce tohoto prefixu, a i kdyby to stačilo, na spojovací linky je třeba pouze čtyř adres a zbylých 60 by zůstalo nevyužito. Zde je tedy jasně vidět výhoda využití VLSM. Pozor však na podmínku, že sítě musí začínat na hranicích podsítí s třídami.

CIDR

CIDR, neboli mezidoménové směrování bez tříd, se od VLSM liší tím, že nepracuje s podsítěmi, ale se skupinami hlavních sítí. Určuje, jak se odkázat na skupinu sítí pomocí jediné cesty.

9 IP sítě

9.1 Alokace IP adres

Pro alokaci adres, je třeba brát v potaz dvě užitečné, ale taky důležité pravidla, které pomohou předejít řadě problémů a také usnadní práci. První z nich říká, že při alokaci IP adres je třeba alokovat blok tak, aby se na něj dalo odkazovat pomocí jedné položky řízení přístupu a druhé pak nabádá k tomu, aby bylo vždy alokováno více adres, než je požadováno.
Pokud by bylo třeba připojit například 35 serverů do již vybudované sítě například 10.11.12.0/24, kde prvních 15 adres je již obsazeno, je dobré si promyslet, jak vhodně určit daný blok sítí a také kolik adres alokovat. Jednoduchým počtem lze zjistit, že je třeba alokovat 64 adres. Výsledný blok adres tedy musí být v násobcích 64. Jelikož prvních 15 adres je již obsazeno, je třeba začít adresou 10.11.12.64. Tímto byl alokován blok adres 10.11.12.64 - 10.11.12.127. Na tento rozsah je možné odkazovat se právě jednou položkou seznamu řízení přístupu, jak udává první pravidlo. Pokud by se použili adresy, které následují hned za využitými, odkazování na výsledný rozsah by bylo značně složitější.

Díky tomu, že byl alokován prostor pro servery podle hranic podsítí, je možné z nich udělat podsítě, aniž by se musely měnit IP adresy.

9.2 Alokace IP podsítí

Při alokování podsítí je také dobré vycházet z určitých pravidel, či doporučení, stejně jako je to u alokování adresovacího prostoru IP sítě.

- *Poskytnout největší možný zbývající adresovatelný prostor (tj. co největší možné podsítě ve zbývajícím prostoru).* [6]
- *Poskytnou co možná nejvíce podsítí, které lze rozšířit do okolního prostoru.* [6]

Existují metody, které jsou jednoduché, ovšem ne tak efektivní, i když se používají často, jako například sekvenční metoda. Tato metoda sebou nese spoustu problémů, jako například nutnost přečíslování z důvodu potřeby většího prostoru dané podsítě. Mnohem lepší je metoda dělení na polovinu, kdy v konečném stádiu je možné vždy rozšířit potřebnou podsíť. Princip metody je takový, že při alokaci nové sítě, se

nejmenší dostupný prostor rozdělí na polovinu. Výhodou je, že je možné největší dostupný prostor využívat po delší dobu, než bylo u sekvenční metody. Asi nejlepší, avšak matematicky asi nejnáročnější je reverzní binární metoda, která je také doporučována společností Cisco. Podsítě jsou alokovány binárním počítáním, ovšem s reverzní formou nejvýznamnějších a nejméně významných bitů. Jedná se o určitou šablonu, která by měla být použita bez ohledu na velikost výsledných podsítí. Tabulka č.7 znázorňuje vztah mezi běžnou binární metodou a reverzní binární metodou, která určuje pořadí sítí.

Tabulka č.7: Alokace podsítí reverzní binární metodou.

Běžná binární metoda		**Reverzní binární metoda**	
00000000	0	00000000	0
00000001	1	10000000	128
00000010	2	01000000	64
00000011	3	11000000	192
00000100	4	00100000	32
00000101	5	10100000	160
00000110	6	01100000	96
00000111	7	11100000	224

Pro lepší pochopení jsou v tabulce č.8 zobrazeny první tři kroky alokování sítě 192.168.1.0/24 podle zmíněné šablony a prefixem /28. Červeně jsou zde vyznačeny podsítě, které byly alokovány, což koresponduje s hodnotami v tabulce č.7. Modře jsou označeny podsítě, které ještě nebyly alokovány a černě jsou vyznačeny ty podsítě, které mohou být ještě rozděleny. [1]

Tabulka č.8: První tři kroky reverzní binární metody.

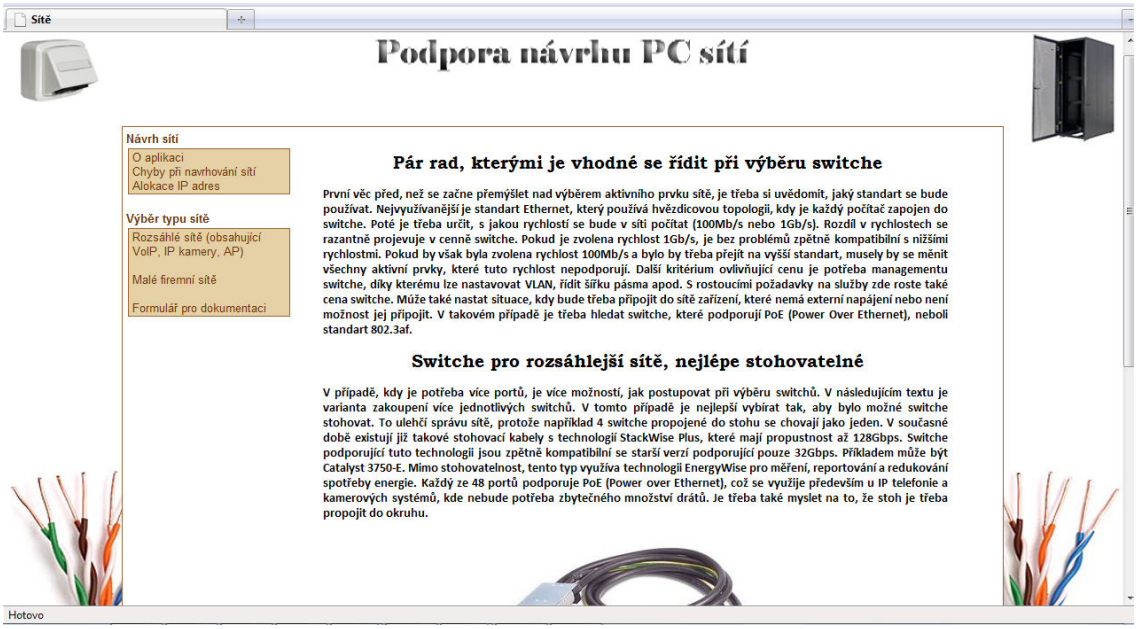
1.	**2.**	**3.**
192.168.1.0/25	192.168.1.0/26	192.168.1.0/26
	192.168.1.64/28	192.168.1.64/28
	192.168.1.80/28	192.168.1.80/28
	192.168.1.196/27	192.168.1.196/27
192.168.1.128/28	192.168.1.128/28	192.168.1.128/28
192.168.1.144/28	192.168.1.144/28	192.168.1.144/28
192.168.1.160/27	192.168.1.160/27	192.168.1.160/27
192.168.1.192/26	192.168.1.192/26	192.168.1.192/28
		192.168.1.208/28
		192.168.1.224 /27

Touto kapitolou končí část práce, která se zabývá problematikou navrhování počítačových sítí. V následující kapitole bude popsána webová aplikace, která byla vytvořena na základě informací z předešlé části.

10 Úvod do aplikace

Aplikace pro podporu počítačových sítí byla vytvořena na základě získaných informací během semestrálního projektu. Jedná se o stručného průvodce, který běží na serveru jako webová aplikace. Uživatel se zde dočte o tom, jaké jsou nejzákladnější chyby při navrhování sítí a to v kapitolách, které se věnují špatné domluvě, nevhodnému výběru zařízení nebo špatné adresaci v síti. Dále jsou v aplikaci popsány metody, jak správně navrhovat adresování, jaké zařízení vybrat apod. Více bude v popisu pro jednotlivé kapitoly.

Aplikaci je možno shlédnout na následujícím odkazu:
http://srv-126-boo.utko.feec.vutbr.cz/xspidl02/



Obrázek č.6: Ukázka aplikace

11 Technický popis aplikace

11.1 Struktura aplikace

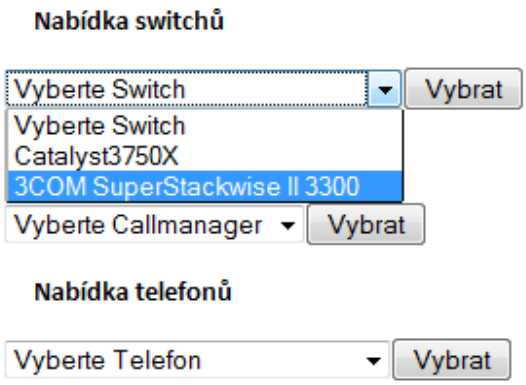
Úvodní strana aplikace se nějak neliší od klasických stránek. Jediné co zde je, tak je uvítání. Vše ostatní je na ostatních stránkách stejné a mění se pouze střed stránky v závislosti na vybraném odkazu. Toho je docíleno pomocí `vrch.php`, kde jsou umístěny meta-tagy, které slouží pro určení v jakém kódování se má zobrazovat, kdo je autorem, popis stránky a mnoho dalších vlastností. V části `spodek.php` je nadefinováno menu a spodní část stránek. Obě části se následně vkládají do ostatních částí aplikace, aby se nemusely znova definovat. Menu, nadpisy, zarovnání a další prvky jsou řešeny pomocí css stylů, na které se při psaní kódu odkazuje. Aplikace je celkově postavena na html kódu, do kterého se začleňují skripty z programovacího jazyka PHP.

11.2 Ukázka kódu

```
<?
$nazev = "switch"; //pojmenovani souboru -> např.
switch1.php
$zarizeni = array(1=>"Catalyst3750X", "3COM
SuperStackwise II 3300");  // seznam zarizeni
$vyberte ="Vyberte Switch";  // hlaska pro vyber
$count = 2;  //max počet položek

echo "<form><select id=\"".$nazev."\"
onchange='go(this)'>";
echo "<option value=\"\"
selected>".$vyberte."</option>";
for($a=1; $a<=$count; $a++) {echo ("\t<option
value=\"".$nazev.$a.".php\">".$zarizeni[$a]."</option>\n
");}
echo "</select><input onclick=\"go2('".$nazev."');\"
type=\"reset\" value=\"Vybrat\"></form>";
?>
```

Část kódu z `vel-vyber.php` slouží k vytvoření seznamu zařízení, kdy se po vybrání požadovaného zařízení zobrazí jeho popis.



Obrázek č.7: Výsledek skriptu pro výběr zařízení

Definice proměnných:

`$nazev` – pojmenování souboru (switch1.php)

`$zarizeni` – seznam zařízení

`$vyberte` – definice zobrazovaného textu

`$count` – maximální počet položek

Následný skript funguje tak, že v okně pro výběr je primárně nastavena hodnota `$vyberte`. Následuje cyklus pro načítání položek z pole `$zarizeni`. Hodnota value je složená z proměnných `$nazev` a `$a`, která se pomocí cyklu zvyšuje o jedničku, čímž se vytváří URL adresy, na které je uživatel směrován, například `switch1.php`, kde tel je hodnota `$nazev` a číslo 2 je hodnota `$a`.

12 Popis obsahu aplikace

Následující kapitola obsahuje stručný popis nejdůležitějších částí aplikace. První část se věnuje popisu chyb. V této části se uživatel dočte o nejčastějších chybách, které nastávají při navrhování počítačových sítí. Jedná se o problematiku při adresování, špatné domluvě a nevhodném výběru síťových zařízení.

Obrázek č.8: Ukázka aplikace – Časté chyby

Dále je v aplikaci popsán rozdíl mezi rozsáhlou a malou podnikovou sítí. Uživatel poté přesměrován na nejrozšířenější část aplikace, která se věnuje popisu, jak vybrat správně síťové zařízení. Z této části se uživatel dostane k doporučeným zařízením, kde jsou popsány výhody některých síťových zařízení, výhody či nevýhody hardwarových nebo softwarových firewallů a popis možností kabeláže.

V aplikaci je také možnost stažení formuláře, který ve výsledku bude sloužit jako výsledná dokumentace k navržené počítačové síti a uživatel si jej vyplní na základě zjištěných informací.

13 Závěr

Práce je rozdělena do dvou částí. V první části bylo cílem poukázat na věci, které jsou často v návrhu sítí zapomínány, jak ve výsledné dokumentaci, tak v samotném návrhu sítě. Správná výsledná dokumentace sítě je velice důležitá položka, protože se podle ní orientují současní i budoucí správci sítě. Měla by obsahovat vše od požadavků na síť, až po IP adresy použité v síti. Po prostudování práce je také zřejmé, že výběr správných komponentů, především směrovačů a přepínačů je velice důležitý. Technologie jde stále dopředu, proto jsou také tyto komponenty stále vyspělejší. V textu je zmíněno, že existují stohovatelné přepínače, které podporují PoE nebo modernější PoE plus, což ušetří čas i peníze, stejně jako správné určení priorit pro přenos pomocí QoS. Rovněž je důležité znát správné rozdělení IP adres, které je možno použít, které naopak ne. Teoreticky by mohly být použity všechny, ale problém může nastat při připojení na globální internet, kdy v síti nesmí být dvě totožné adresy. Práce se dále věnuje především doporučené metodě alokací podsítí a to reverzní binární metodě. Tato metoda je doporučována společností Cisco, i když je matematicky náročná, skrývá se v ní řada výhod.

Druhá část popisuje vytvořenou aplikaci na základě zjištěných informací. Tato aplikace slouží jako průvodce při navrhování sítí, ukazuje výhody a nevýhody různých síťových zařízení a a přenosových médií, upozorňuje na nejčastější chyby, které se při návrhu sítí objevují a obsahuje formulář, který ve finále slouží pro vytvoření dokumentace k síti. Aplikace poukazuje na nejnovější technologie v oblasti přepínačů, ale také se věnuje tomu, kde lze použít přepínače se slabším výkonem.

14 Seznam použité literatury

[1] DONAHUE, Gary. *Kompletní průvodce síťového experta*. Libor Pácl; Pavel Vaida. 1. vyd. Brno : Computer Press, a.s., 2009. 528 s. ISBN 978-80-251-2247-1.

[2] VELTE, Toby J., VELTE, Athony T. *Síťové technologie Cisco : Velký průvodce*. Libor Pácl; David Krásenský. 1. vyd. Brno : Computer Press, a.s., 2003. 759 s. ISBN 80-7226-857-0.

[3] *Cisco Catalyst 3750 Data Sheet* [online], Září 2009. Dostupné z: http://www.cisco.com/en/US/prod/collateral/switches/ps5718/ps5023/product_data_sheet0900aecd80371991.pdf [cit. 20.10.2009]

[4] *Cisco ASA 5500 Series Adaptive Security Appliances Data Sheet* [online], Září 2009. Dostupné z: http://www.cisco.com/en/US/prod/collateral/vpndevc/ps6032/ps6094/ps6120/product_data_sheet0900aecd802930c5.pdf [cit. 30.10.2009]

[5] IANA, *Special-Use IPv4 adresses* [online], Září 2002. Dostupné z: http://www.ietf.org/rfc/rfc3330.txt [cit. 20.10.2009]

[6] DONAHUE, Gary. *Síťové technologie Cisco*. 1. vyd. Libor Pácl, Pavel Vaida. Brno : Computer Press, a.s., 2009. ISBN 978-80-251-2247-1. Alokace podsítí IP, s. 473.

[7] *Cisco QoS, garance rychlosti, řazení do front* [online], Únor 2009. Dostupné na: http://www.samuraj-cz.com/clanek/cisco-qos-4-garance-rychlosti-razeni-do-front-queuing [cit. 12.11.2009]

[8] Redakce HW serveru. *Princip činnosti Power Over Ethernet* [online], Červen 2004. Dostupné na: http://hw.cz/ethernet/poe/popis_komunikace.html [cit. 30.11.2009]

[9] REYNOLDS, Joyce. *Assigned numbers* [online], Říjen 1994. Dostupné na: http://tools.ietf.org/html/rfc1700 [cit. 2009-12-13]

[10] REKHTER, Y., et al. *Address Allocation for Private Internets* [online], Leden 1996. Dostupné na: http://www.rfc-editor.org/rfc/rfc1918.txt [cit. 2009-12-03]

Abecední seznam použitých zkratek

AC	Alternating current - střídavý proud
AP	Access Point
BTU	British Thermal Unit - energetická jednotka rovna přibližně 1,06 kJ
CIDR	Classless Inter-Domain Routing
DSCP	Differentiated Services Code Point - šesti bitové pole v záhlaví IP
DTP	Dynamic Trunking Protocol
FCS	Frame Check Sequence
FTP	File Transfer Protocol
HTTP	Hypertext Transfer Protocol
IANA	Internet Assigned Numbers Autority - organizace přidělující IP adresy
IEEE	Institute of Electrical and Electonics Engineers
IP	Internet Protocol
IPsec	IP security
IPX	Internetwork Packet Exchange - síťový protokol podobný IP
ISL	Inter Switch Link - protokol navržený organizací Cisco pro tvoření trunku
LAN	Local Area Network
PD	Powered Devices
PoE	Power over Ethernet
PSE	Power Sourcing Equipment
QoS	Quality of Service
RTP	Real Time Protocol
SELV	Secured Extra-Low Voltage
SSH	Secure Shell - zabezpečený komunikační protokol v počítačových sítích
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
VLAN	Virtual LAN - zkratka pro virtuální sítě
VLSM	Variable Length Subnet Masking
VoIP	Voice Over Internet Protocol
VPN	Virtual Private Network

Seznam příloh

A Cd obsahující elektronickou podobu práce, použité obrázky v aplikaci a zdrojové kódy aplikace.

Příloha A

Stromová struktura obsahu CD:

Bakalářská práce → Elektronická podoba bakalářské práce
→ Zdrojové kódy aplikace → doc
→ obrázky
→ styl