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

NÁVRH SPOLEHLIVÉ PODNIKOVÉ SÍTĚ S PODPOROU KVALITATIVNÍCH POŽADAVKŮ SLUŽEB

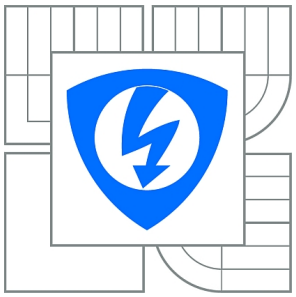
BAKALÁŘSKÁ PRÁCE
BACHELOR'S THESIS

AUTOR PRÁCE MARTIN KIŠKA
AUTHOR

BRNO 2012

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

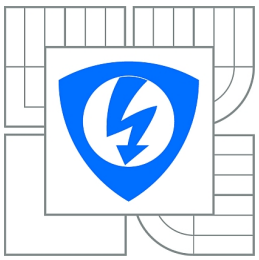
NÁVRH SPOLEHLIVÉ PODNIKOVÉ SÍTĚ S PODPOROU KVALITATIVNÍCH POŽADAVKŮ SLUŽEB

BAKALÁŘSKÁ PRÁCE
BACHELOR'S THESIS

AUTOR PRÁCE — MARTIN KIŠKA
AUTHOR

VEDOUCÍ PRÁCE — doc. Ing. VÍT NOVOTNÝ, Ph.D.
SUPERVISOR

BRNO 2012



VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

Fakulta elektrotechniky a komunikačních technologií

Ústav telekomunikací

Bakalářská práce

bakalářský studijní obor
Teleinformatika

Student: Martin Kiška ***ID:*** 128127
Ročník: 3 ***Akademický rok:*** 2011/2012

NÁZEV TÉMATU:

Návrh spolehlivé podnikové sítě s podporou kvalitativních požadavků služeb

POKYNY PRO VYPRACOVÁNÍ:

Prostudujte principy návrhu podnikových datových sítí z pohledu spolehlivosti funkčnosti síťové architektury. Seznamte se s technikami podpory kvalitativních požadavků služeb v sítích IP a jejich nasazením v různých úrovních síťové infrastruktury. Uvažujte jak linkovou, tak i síťovou vrstvu. Seznamte se s konkrétními síťovými prvky experimentální sítě laboratoře ÚTKO a s možnostmi podpory QoS u těchto síťových prvků. Dle nabytých znalostí a dle dostupné výbavy v laboratoři PA-427 navrhněte malou podnikovou intersíť, na které bude možno otestovat schopnost regenerace sítě po výpadku spoje či uzlu a vzájemné ovlivňování služeb při různé konfiguraci podpory QoS. Na základě výsledků navrhněte dvě laboratorní úlohy.

DOPORUČENÁ LITERATURA:

[1] SZIGETI, T., HATTINGH, CH., End-to-End QoS Network Design. Cisco Press, ISBN 1-58705-176-1, Indianapolis, USA
[2] MARCHESE M. QoS over Heterogeneous Networks. John Wiley & Sons, ISBN 978-0-470-01752-4, 2007

Termín zadání: 6.2.2012 ***Termín odevzdání:*** 31.5.2012

Vedoucí práce: doc. Ing. Vít Novotný, Ph.D.

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

UPOZORNĚNÍ:

ABSTRAKT

Práce se zabývá návrhem spolehlivé podnikové sítě s různými možnostmi zabezpečení proti smyčkám a podporou kvalitativních požadavků služeb na linkové a síťové vrstvě. Na základě teoretických znalostí je navrhnuta experimentální síť v laboratoři ústavu telekomunikací, která je složena z několika počítačů, VoIP telefonů, přepínačů a směrovačů. Při funkční sítí je pak testován výpadek jednotlivých uzlů a dopad na provoz v síti. V další části je pak síť testována při nastavení různých možností podpory QoS.

KLÍČOVÁ SLOVA

STP, RSTP, MSTP, UTP, STP, UPS, BPDU, VLAN, IntServ, RSVP, DiffServ, DSCP.

ABSTRACT

This work deals with creating a reliable corporate network and its variety capabilities against loops and supporting QoS on link and network layer. On the basis of theoretical knowledge is designed an experimental network in the laboratory of Institute of Telecommunications composed of several computers, VoIP pohones, switches and routers. Functinonal network is then tested to failure of individual nodes and the impact on network traffic. In another part of this bachelor thesis this network is tested using different QoS support options.

KEYWORDS

STP, RSTP, MSTP, UTP, STP, UPS, BPDU, VLAN, IntServ, RSVP, DiffServ, DSCP.

KIŠKA, Martin *Návrh spolehlivé podnikové sítě s podporou kvalitativních požadavků služeb*: bakalářská práce. Brno: Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, Ústav telekomunikací, 2012. 54 s. Vedoucí práce byl doc. Ing. Vít Novotný, PhD.

PROHLÁŠENÍ

Prohlašuji, že svou bakalářskou práci na téma „Návrh spolehlivé podnikové sítě s podporou kvalitativních požadavků služeb“ 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/nebo majetkových a jsem si plně vědom následků porušení ustanovení § 11 a následujících autorského zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů, včetně možných trestněprávních důsledků vyplývajících z ustanovení části druhé, hlavy VI. díl 4 Trestního zákoníku č. 40/2009 Sb.

Brno ....

(podpis autora)

Poděkování

Děkuji vedoucímu bakalářské práce doc. Ing. Vítu Novotném, Ph.D. za cenné rady, připomínky a metodické vedení práce. Dále bych rád poděkoval Ing. Radku Krkošovi za pomoc při řešení praktické části bakalářské práce.

OBSAH

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

ÚVOD

V dnešní době je snaha integrovat veškeré možné provozované služby do datových sítí. Dobře to jde rozpoznat v nově vystavěných budovách, kde jediná síť zprostředkovává veškerou hlasovou, obrazovou (video konference, IP kamery,...) a datovou (elektronická pošta, přenos souborů,...) komunikaci. Je zapotřebí, aby tato síť byla dostatečně spolehlivá a přenesla data bez zanesení chyby k příjemci. Například při zaslání emailu je nemyslitelné, aby druhé straně přišel pozměněn. Musí se taktéž řešit problémy, aby hovor přes takovou síť byl plynulý a ani jedna ze stran nezaregistrovala, že hovor neprobíhá přes síť se spojováním okruhů, ale přes síť se spojováním paketů. Stalo se Vám také, že jste se chtěli podívat na video přes Internet a každou chvíli se Vám přerušovalo? Není zrovna příjemné pozorovat videoklip od oblíbené písničky a stihnout u něj vypít šálek kávy. Při budování takové sítě se musí zvážit provoz na síti. Jednotlivé prvky se nesmí zbytečně zahlcovat a musí zvládat upřednostňovat hlasové pakety s vyšší prioritou, zároveň však doručovat kvalitně i pakety datové.

Zkvalitnění služeb se dosáhne zavedením podpory QoS (Quality of Service) v síťové infrastruktuře. Jedná se o rezervaci a řízení datových toků v telekomunikačních a počítačových sítích. Jednotlivé pakety jsou značkovány dle obsahu, který nesou. Směrovač pak dle značek rozlišuje pakety a dle nastavení s nimi zachází. Například paket obsahující hlasovou službu s vyšší prioritou může zaslat primárně jako první, aby nedocházelo k znekvalitnění probíhající služby.

V práci jsou vysvětleny jednotlivé metody pro zabezpečení spolehlivého a kvalitního přenosu dat po síti. Nabyté poznatky pak aplikuji při návrhu sítě a zapojení v laboratorním pracovišti na Ústavu telekomunikací.

V první části bakalářské práce se věnuji zejména fyzické a linkové vrstvě, teoreticky jsou zde probrány různé protokoly pro zachování sítě bez smyček a vytváření virtuálních lokálních sítí. V praktické části aplikuji jednotlivé protokoly na síťová zařízení v laboratoři a testuji jejich chování.

V druhé části bakalářské práce navazuji vrstvou další – síťovou. V teorii se věnuji jednotlivým možnostem zavedení podpory QoS v síti. Následně teoretické znalosti aplikuji v laboratoři. V praktické části sleduji chování sítě při stavu zahlcení, zda-li bude upřednostňovat požadované služby nad ostatní.

1 SLUŽBY TELEKOMUNIKAČNÍCH SÍTÍ

Na telekomunikačních sítích se setkáme s celou řadou služeb. Každá má přitom specifické nároky na provoz. Cílem dnešních sítí je pojmout co nejvíce služeb při zachování stávající kabelové infrastruktury a přitom je provozovat na dostatečně kvalitní úrovni tak, aby nedocházelo ke ztrátě uživatelských dat z důvodu nedostatečné kapacity sítě. V následujících kapitolách uvádím několik základních služeb a jejich nároky na síť.

1.1 Hlasová služba

Pro zachování hlasové služby je důležité zachovat minimální zpoždění průchodů paketů v sítích. Organizací ITU[1] a doporučením G.114 jsou doporučeny hodnoty menší než 150 ms na cestu jedním směrem, tudíž 300 ms tam a zpět. Důležitý je i *jitter*[2]. Ten by neměl přesáhnout 50 ms. Ztrátovost paketů[3] by neměla přesáhnout 1 %. Datový tok se pohybuje v závislosti na použitém kodeku (viz tab. 1.1), vzorkovací frekvenci a případně režii pro uskutečnění hovoru. Pro sestavení hovoru je zapotřebí například SIP[4] protokol.

Tab. 1.1: Přehled vybraných audio kodeků. [11]

Označení	Datový tok [kbit/s]	Vzorkovací kmitočet [kHz]
G.711	64	8
G.721	32	8
G.722	64	16
G.728	16	8
G.729	8	8

1.2 Video konference

Už z podstaty služby je jasné, že video konference má větší nároky na šířku pásma než služba hlasová. Požadavky na udržení co nejmenšího jitteru a zpoždění jsou shodné s hlasovou službou. Datová náročnost závisí na použitém kodeku a rozlišení.

[1] International Telecommunication Union - Mezinárodní telekomunikační unie.
[2] Změna zpoždění způsobena opožděním některých paketů oproti ostatním.
[3] Při zahlcení směrovače dochází k zahazování paketů.
[4] Session Initiation Protocol – protokol pro inicializaci relací.

Používají se například kodeky H.261, H.262, H.263 a H.264. Kodek H.264 má největší kompresní poměr a tak je nejvhodnější ho používat pro videokonference.

1.3 Video streaming

Na principu video streamingu pracuje například server www.youtube.com. Video, které si chcete přehrát se před samotným spuštěním přednačte do vašeho počítače (např. 5 sekund dopředu). Při sledování je přehrávání plynulé, protože veškeré zpoždění, ztráta paketů a jitter se odehrává 5 sekund před vašim aktuálním snímkem. Předpokládá se, že do té doby zpožděné snímky přijdou. Tímto způsobem ukládání do paměti počítače se uživateli zamezí pozorování krátkého výpadku přenosu dat přes síť.

1.4 Datové přenosy

Data potřebují pro přenos větší šířku pásma, ale zpoždění a jitter nehraje až takovou roli, jako u služeb hlasových. Služba je schopna se vypořádat se ztrátovostí paketů. Má zabezpečovací mechanizmy na opakované vyslání paketů a doručení celé zprávy bez chyb i při zahození paketů směrovačem při zahlcení. Pro přenos může použít protokol FTP (File Transfer Protocol).

Tab. 1.2: Požadavky hlavních služeb v reálném čase na sítích.

Služba	Datový tok	Zpoždění	Jitter	Ztrátovost paketů
Hovor	malý	malé	malý	malá
Video konference	střední	malé	malý	malá
Video streaming	střední	střední	malý	malá
Přenos dat	velký	střední	střední	malá

2 VYBUDOVÁNÍ SPOLEHLIVÉ SÍTĚ

V dnešní době si už většina lidí nedokáže představit svůj život bez přístupu na síť, ať už se jedná o ranní přečtení e-mailových zpráv, informací z intranetu nebo prohledávání pracovních databází. V obou případech očekává, že dostane to, co bude potřebovat. V těchto případech musí mít poskytovatel/firma vybudovanou kvalitní síťovou infrastrukturu, která mu zajistí přístup na síť i při výjimečných situacích. Poskytovatelé obvykle garantují dostupnost svých služeb na 99,999 %. Což znamená, že za rok provozu bychom se pouze 5 minut nemohli dostat na síť.

2.0.1 Zajištění nepřetržité dodávky elektrické energie

Pro zajištění neustálého provozu i při výpadku dodávky elektrického proudu je nutné zajistit náhradní zdroje elektrické energie. Ty pak udrží prvky v provozu i při výpadku elektrické energie dalších pár hodin. Ideálním řešením je nepřerušitelný zdroj energie UPS (Uninterruptible Power Supply). Veškerá zařízení, která by v případě výpadku měla zůstat v provozu, jsou zapojena přes UPS, které je následně zapojeno do sítě. UPS funguje na principu akumulátoru. V normálním provozu je akumulátor udržován v nabitém stavu. V případě výpadku je z něj čerpána energie pro zapojená zařízení. Tímto způsobem mohou být zálohovány jednotlivé přístroje, nebo celý okruh zásuvek. Je možné taktéž přímo zakoupit síťové prvky, které máji dva vstupy elektrické energie (v případě, když jeden nefunguje, nahradí ho druhý).

Obr. 2.1: Pohled na UPS zepředu a zezadu.

2.0.2 Strukturovaná kabeláž

Kabeláž slouží k propojení jednotlivých síťových prvků. Správnou volbou kabelů zajistíme dostatečnou kapacitu pro přenos na páteřních a přístupových linkách. Základní dělení je na optické a metalické kabely.

Metalické kabely jsou rozděleny do několika kategorií dle šířky pásma, rychlosti, protokolu přenosu, odstupu signálu od šumu, přeslechu na blízkém/vzdáleném konci a dalších vlastností. V dnešní době již historické kategorie 3 a 4 dosahovaly maximální rychlosti 16 Mbit/s a pro přenos využívaly šířku pásma do 100 MHz. Nejběžnější používanou kategorií i z ekonomických důvodů je kategorie 5E. Ta zvládá ve stejné šířce pásma 100 MHz až 1000 Mbit/s na vzdálenost do 100 metrů. Pro přenos využívá protokol 1000Base-T.

Existují i vyšší kategorie (např. 6, 6A a 7), které zvládají rychlosti přenosu až 10 Gbit/s, ale také používají větší šířku pásma. Shrnutí naleznete v tabulce 2.1.

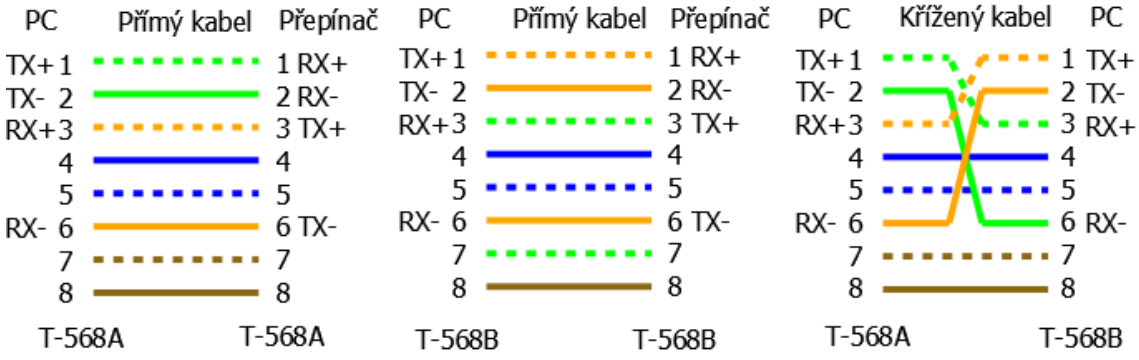
Zároveň ještě dělíme kabely na stíněnou kroucenou dvoulinku (STP – Shielded Twisted Pair) a nestíněnou kroucenou dvoulinku (UTP – Unshielded Twisted Pair). Kabely STP vyzařují méně do okolí a tak neovlivňují ostatní datové kabely. Jsou také odolnější proti vnějšímu záření. Jednotlivé kabely se skládají ze čtyř párů, kterou jsou ještě v páru kroucené, aby nevyzařovaly tolik do okolí (elektromagnetické záření se vzájemně vyruší).

Tab. 2.1: Rozdělení UTP kabelů na kategorie.

Kategorie	Frekvence [MHz]	Protokol	Rychlost
3	do 16	10BASE-T Ethernet	10 Mbit/s
4	do 20	10BASE-T Ethernet	16 Mbit/s
5	do 100	100BASE-TX Ethernet	100 Mbit/s
5E	do 100	1000BASE-T Ethernet	1 Gbit/s
6	do 250	1000BASE-T Ethernet	1 Gbit/s
6A	do 500	10GBASE-T Ethernet	10 Gbit/s
7	do 1200	10GBASE-T Ethernet	10 Gbit/s

Při propojování síťových prvků je důležité zvýšit pozornost i u zapojení jednotlivých pinů do konektoru RJ-45. U přímého kabelu musí jednotlivé piny souhlasit na obou stranách (1-1, 2-2, 3-3, ...). Přímým kabelem se propojuje např PC-přepínač a směrovač-přepínač. Je definován ve standardu T-568A.

U kříženého kabelu je nutné jednu koncovku zapojit s prohozeným 2. (pin 1 a 2) a 3. (pin 3 a 6) párem. Tímto se pak propojují prvky PC-PC, směrovač-směrovač, PC-směrovač a přepínač-přepínač. Je definován ve standardu T-568B například pro 100BASE-TX. Schématické znázornění naleznete na obrázku 2.2.



Obr. 2.2: Znázornění standardu T-568A a T-568B.

Novější síťové prvky jsou schopné automaticky detekovat jaký kabel je připojený (přímý nebo křížený) a dle toho změnit softwarově pořadí pinů na portu. V případě, že tuto funkci přepínač/směrovač umožňuje, je u portu napsána zkratka MDI/MDIX (Medium Dependent Interface/Medium Dependent Interface Crossover).

Pro přenos je možné využít i optické kabely, která mají mnoho výhod. Dosahují větších přenosových rychlostí na větší vzdálenosti. U metalických kabelů je možno dosáhnout rychlosti 1 Gbit/s u kategorie 5E na vzdálenost do 100 m, zatímco u optických jednovidových kabelů lze dosáhnout rychlosti 10 Gbit/s až do vzdálenosti 10 km. Jejich hlavní nevýhodou je minimální poloměr ohybu. Aby paprsek „nevyletěl“ mimo vlákno, musí mít větší poloměr ohybu než ±3 cm.

Při volbě kabelu pro spolehlivou síť je vhodné páteřní prvky zapojit přes optické kabely, stejně jako servery, kde je očekávána větší náročnost na průtok dat. Jsou také vhodné pro připojení vzdálenějších kanceláří (do 10 km). Optické kabely jsou chráněny proti elektromagnetickým vlivům silových elektrických kabelů (špičkové stavy při zapnutí výkonového přístroje), které mohou vést podél datového vedení.

Metalické kabely je pak vhodné vést do kanceláří, kde může dojít k opotřebení kabelu. V potaz musíme vzít i ekonomickou stránku věci, metalické kabely jsou výrazně levnější. Výhodou metalických kabelů je taktéž to, že mohou napájet připojené IP kamery a VoIP telefony na síti (PoE – Power over Ethernet).

2.0.3 Redundantní zapojení

Síť si můžeme hierarchicky rozdělit do několika vrstev: páteřní, distribuční a přístupovou. Redundantní zapojení[1] je důležité především v páteřní síti. Přes tuto část sítě proudí veškerý provoz na světovou síť Internet (vysoké hardwarové nároky) a je nutné v případě výpadku (přeseknutí kabelu, poruchy přístroje, . . .) mít záložní cestu ven. Redundantní zapojení taktéž snižuje nároky na propustnost síťových prvků – data

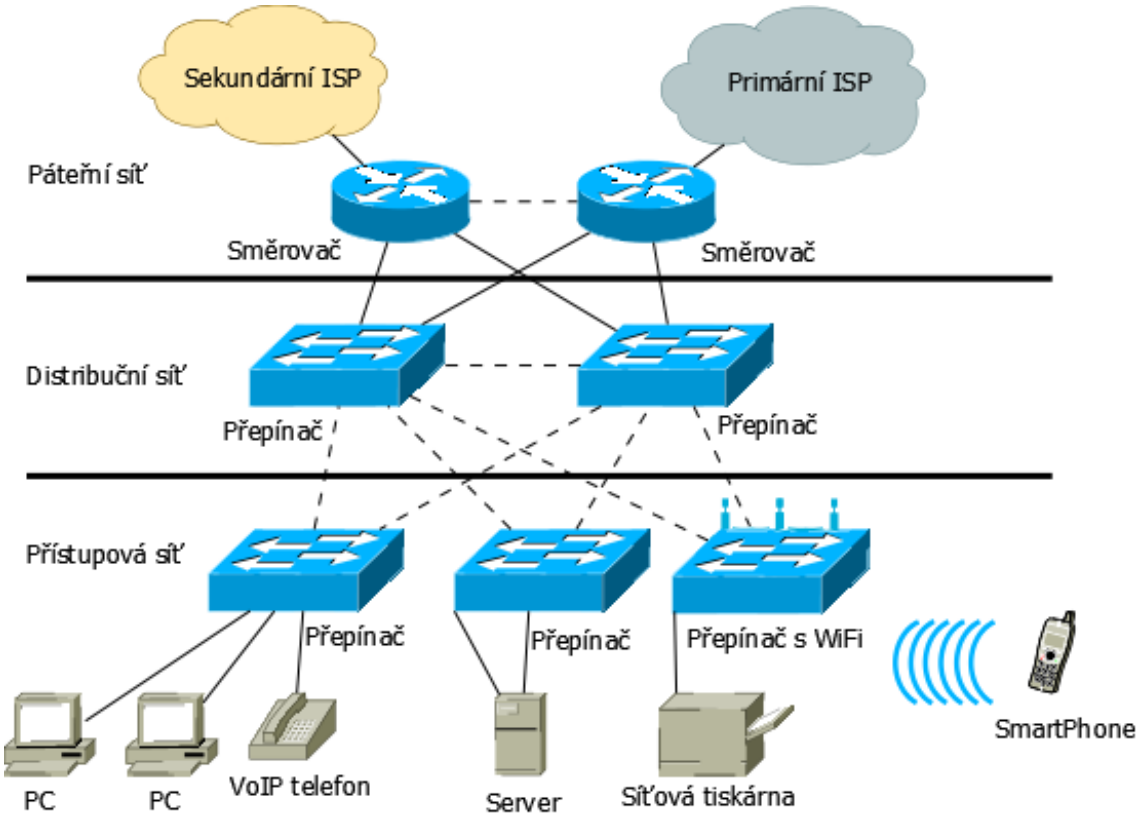
[1] Zapojení, kde je zajištěno propojení i v případě výpadku jedné z propojujících linek.

mohou téct odlišnými kabely a prvky. Můžeme být k Internetu připojeni i přes více poskytovatelů, abychom při výpadku jednoho měli stále přístup na celosvětovou síť.

V distribuční síti se používají především přepínače. Výpadek jednoho nesmí ovlivnit správný chod sítě. V této části sítě se řeší omezení provozu na síti. Může se filtrovat provoz směřující dovnitř i mimo síť pomocí ACL (Access List). Tímto způsobem jednoduše nastavíme politiku přístupu pro danou síť (uživatele).

V přístupové části sítě již řešíme samotný vstup do sítě. Jednotlivým zařízením přiřazujeme IP adresy. Ty můžeme přidělovat staticky (tiskárny, VoIP telefony, servery, ...) nebo dynamicky (PC, SmartPhone, ...). Můžeme taktéž povolit vstup jen hostům s určitou MAC[2] adresou.

U linek směřujících k serveru lze předpokládat větší datový tok. Server připojíme vícekrát s přepínačem a linky agregujeme[3]. Tím dosáhneme větší propustnosti.

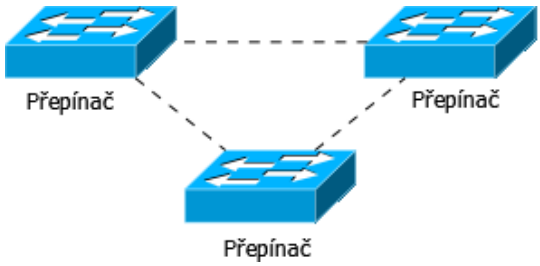


Obr. 2.3: Redundantní zapojení sítě

[2]Media Acces Control je jedinečný identifikátor síťového rozhraní.
[3]Topologicky je sloučíme do jedné.

2.1 Protokol STP na linkové vrstvě

Spanning tree protocol zajišťuje průchod rámce přes přepínače bez smyčky. V případě redundantního zapojení dle obrázku 2.4 si přepínače ukládají do své MAC tabulky MAC adresy, které přiřazuje k portům, ke kterým jsou připojeny. V případě zaslání všesměrového dotazu ze stanice ji první přepínač ihned rozešle na všechny své porty. Vzápětí mu přijde zpráva o nalezení hledané stanice na oba porty. První přepínač tak veškerou komunikaci pro určenou stanici přeposílá na oba porty, jelikož má u nich záznam, že cílová MAC adresa je dosažitelná přes oba. Tímto nežádoucím provozem může brzy dojít k zahlcení celé sítě. Jedná se o tzn. Broadcast Storm. Na linkové úrovni v rámci není políčko TTL (Time To Live) a rámec tak pořád koluje než najde svůj cíl. Každý síťový prvek musí na všesměrovou zprávu odpovědět a roste tak jeho nárok na procesorový čas. Zároveň dochází k přeposílání nesmyslných zpráv, které zbytečně zatěžují kapacitu linky.



Obr. 2.4: Zapojení přepínačů se smyčkou.

Účelem protokolu STP je udržovat topologii rozsáhlé sítě v redundantní infrastruktuře bez smyček. STP odesílá pravidelně zprávu Bridge Protocol Data Unit (BPDU). Tento rámec je odesílán implicitně každé 2 sekundy na všechny porty na rezervovanou skupinovou MAC adresu $_{16}$0180.C200.0000. Struktura rámce je zobrazena na obrázku 2.6. Na základě hodnoty BID (Bridge ID, viz obr. 2.5) v BPDU rámci (nejnižší priority a MAC adresa) se určí hlavní přepínač (*Root*). Ostatní si od něj odvodí cenu cesty. V případě, že přepínači přijde zpráva BPDU od *Root* přepínače na dva porty, port s nižší cenou nechá zapojený a uvede do role *Root*. Druhý port uvede do role *Non-designated*.

Bridge ID	
Priorita	MAC adresa
16 bitů	48 bitů

Obr. 2.5: Hodnota Bridge ID.

Cena cesty se kumuluje od *Root* přepínače až ke konečnému přepínač dle přenosové kapacity linek. Při průchodu přepínačem se zvýší cena cesty. Nejvhodnější je pak varianta s nejmenším součtem. Protokol STP je poměrně starý a při původním návrhu se nepočítalo s rychlostí linek větší než 1 Gbit/s. Proto byla doporučená cena linek změněna a to dokonce dvakrát v letech 1998 a 2001. Cenu linek naleznete v tabulce 2.2.

Pole	Velikost [B]
Protocol ID	2
Version	1
BPDU Type	1
Flags	1
Root Bridge ID	8
Root Path Cost	2
Sender Bridge ID	8
Port ID	2
Message Age	2
Maximum Age	2
Hello Time	2
Forward Delay	2

Obr. 2.6: Struktura rámce BPDU

Celý proces je poměrně časově náročný, trvá v rozmezí 30–50 sekund. Jednotlivé porty prochází pěti stavy: *Blocking, Listening, Learning, Forwarding a Disabled*, než začnou vysílat rámce.

Rychlost linky	Cena od 2001	Cena od 1998	Cena původní
10 Gbit/s	2000	2	1
2 Gbit/s	10000	3	1
1 Gbit/s	20000	4	1
100 Mbit/s	200000	19	10
10 Mbit/s	2000000	100	100

Tab. 2.2: Cena linek dle jejich rychlosti.

Po zvolení *Root* přepínače jeho všechny porty přejdou do role *Designated* a stavu *Forwarding* a začnou vysílat BPDU rámce na své porty. Na základě ceny cesty si ostatní přepínače nastaví své porty do různých rolí: *Root port* (má nejnižší cenu k *Root* přepínači), *Designated* (pro ostatní přepínače je přes tento port k *Root* přepínači nejnižší cena), nebo *Non-designated* (port má větší cenu cesty k *root* přepínači

než ostatní porty) – tento port rovnou uvedou do stavu *Blocking*, ve kterém zůstane. *Root* a *Designated* porty pak přejdou do stavu *Blocking*, kdy přijímají pouze BPDU rámce od *Root* přepínače, ostatní komunikaci zahazují. V tomto stavu setrvají 20 sekund (hodnota Max-Age v BPDU rámci). Poté přejdou do stavu *Listening*. V tuto chvíli přijímají a vysílají BPDU rámce, žádnou další komunikaci nepřipouští. V tomto stavu setrvají 15 sekund (Forward Delay). Dále pokračují do stavu *Learning*, kdy posílají a přijímají BPDU rámce a zároveň se učí MAC adresy. V tomto stavu setrvají 15 sekund (Forward Delay). Následně přejdou do stavu *Forwarding*, kdy již přijímají a posílají vše.

Při změně topologie se generují BPDU rámce s příznakem Topology Change Notification (TCN BPDU) a Topology Change Notification Acknowledgement (TCA BPDU).

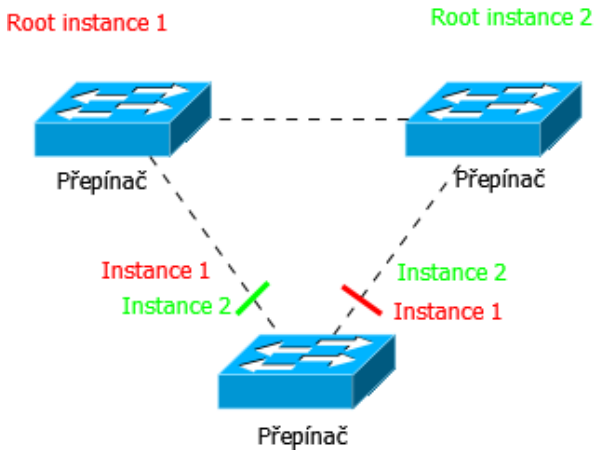
2.1.1 Rapid STP

Protokol RSTP (Rapid Spanning Tree Protocol) je definován ve standardu 802.1w. Byl vylepšen hlavně v rychlosti konvergence celé sítě. V praxi bylo zjištěno, že 30-50 sekundová prodleva po startu nebo změně topologie u protokolu STP je moc dlouhá. Protokol byl vylepšen. RSTP již nevyužívá časovačů. Používá vyjednávacích metod na základě nabídek a potvrzení (*Proposal/Agreement*). V praxi tento algoritmus konverguje v síti během 1-2 sekund. Dopředu lze označit některé porty jako tzv. *Edge port*. Takovým způsobem se označí porty, ke kterým se budou připojovat koncové stanice a ne síťové prvky. Ty pak hned po rozběhnutí RSTP přejdou do stavu *Forwarding* a jsou připraveny na komunikaci. Další změnou je, že port neprochází stavy *Listening* a *Learning*, ale jen stavy – *Discarding, Forwarding* a *Disabled*. Důležitá je i zpětná kompatibilita se standardem 802.1D (STP) – RSTP se degraduje na STP a celý proces konvergence znovu probíhá 30-50 sekund. Obě verze STP protokolu se liší v poli *Version* v BPDU rámci (STP – 1, RSTP – 2).[3]

2.1.2 Multiple STP

Myšlenkou MSTP je provozovat více STP instancí pro určité VLAN. Původně byl tento standard v samotné normě IEEE 802.1s, od roku 2003 se však přidal do standardu 802.1q, se kterým úzce souvisí. Po spuštění MSTP jsou všechny VLAN sítě zahrnuty do nulté instance MSTP. Přepínače, na kterých běží MSTP musí mít stejné namapování VLAN na instance MSTP. Vystupuje zde nový parametr – *Region*, pod který všechny přepínače musí patřit. Aby určené přepínače patřily do jednoho MSTP regionu, musí mít shodné tři parametry – jméno regionu, revizní číslo a mapování VLAN na instance.

Tímto jednoduchým způsobem můžeme staticky ovlivnit kterou cestou bude procházet Voice VLAN (spadá do instance 1), která se tak nemusí potkat s ostatními rámci jiných VLAN (instance 2). Schéma možného zapojení je na obrázku 2.7. [2]



Obr. 2.7: Zapojení přepínačů se smyčkou s dvěma instancemi STP.

2.1.3 Proprietární verze Spanning Tree Protocol

Firma Cisco vydala ještě další verze STP, jejich shrnutí naleznete níže.

- **Per-VLAN Spanning Tree (PVST)**
  Pro každou VLAN běží vlastní instance STP. Výhodou je možné rozdělení zátěže. Jako zapouzdřovací metodu používá proprietární Inter-Switch Link (ISL) trunk.[4]
- **Per-VLAN Spanning Tree Plus (PVST+)**
  Rozdíl oproti PVST je v použití trunku – 802.1q trunk. [5]
- **Rapid Per-VLAN Spanning Tree Plus (RPVST+)**
  Pro každou VLAN běží vlastní instance RSTP. [6]

V případě většího počtu VLAN v síti je nevhodné pro každou VLAN použít vlastní instanci. Toto řešení by příliš zatěžovalo procesor. V takové situaci je pak vhodné provozovat v síti Multiple STP.

[4] Více na http://www.cisco.com/en/US/tech/tk389/tk621/tk846/tsd_technology_support_sub-protocol_home.html

[5] Více na http://www.cisco.com/en/US/tech/tk389/tk621/tk847/tsd_technology_support_sub-protocol_home.html

[6] Více na http://www.cisco.com/en/US/tech/tk389/tk621/tk845/tsd_technology_support_sub-protocol_home.html

2.2 Výběr optimálního směrovacího protokolu

Pro správnou funkčnost sítě o sobě musí jednotlivé prvky na síťové vrstvě vědět, jedině tak jsou schopny správně směrovat pakety k cíli. Prvky si musí uchovávat aktuální topologii a každou změnu v topologii musí co nejdříve šířit k ostatním síťovým prvkům. Shrnutí interních směrovacích protokolů naleznete v tabulce 2.3 (IGP – Interior Gateway Protocol). Pro vybrání ideálního směrovacího protokol pro síť, se musí zvážit její rozsáhlost, počet připojených prvků, výkonnost směrovačů, rychlost konvergence[7], ...

Pro malé a střední sítě je vhodnější zvolit distanční směrové protokoly, které nejsou tak náročné na procesorový čas směrovačů. Avšak opakovaně zasílají kompletní směrovací tabulku, čímž roste zátěž linky. Pracují na bázi počtu přeskoků (hopů) k cíli. Jejich nastavení a správa je pro správce jednodušší, neumožňují však velkou variabilitu. Jako zástupce jmenuji především RIPv2.

Pro střední a velké sítě je vhodnější zvolit směrovací protokol, který funguje na základě stavu linky. Takový protokol zahltí síť ze začátku při vytváření kompletní topologie sítě, kterou si uchovává každý směrovač. Pak již dochází k zasílání aktualizací jen při změně stavu linky. Navíc je schopen pracovat i s dalšími vlastnostmi linky jako je šířka pásma, zpoždění atp. Pro takovou síť by byl vhodný například směrovací protokol OSPF.

Tab. 2.3: Rozdělení vnitřních směrovacích protokolů.

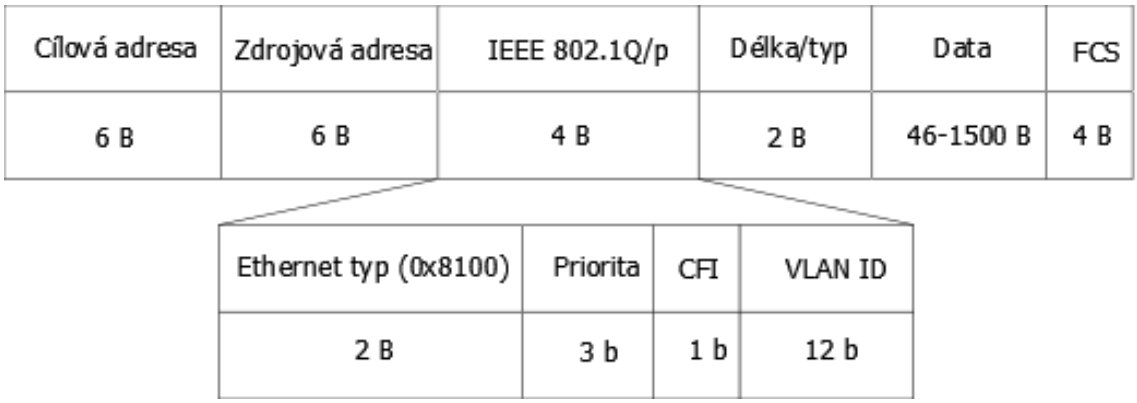
	Algoritmus			
	Vektor vzdálenosti		Stav linky	
Třídní	RIPv1	IGRP	–	–
Beztřídní	RIPv2	EIGRP	OSPFv2	IS-IS
IPv6	RIPng	EIGRP pro IPv6	OSPFv3	IS-IS pro IPv6

Na páteřní síti Internet se používají tzv. externí směrovací protokoly (EGP – Exterior Gateway Protocol). Oproti IGP jsou tyto protokoly „línější“, déle jim trvá reakce na změnu v síti. Jejich výhodou je naopak větší možnost nastavení politiky přístupu jednotlivých koncových sítí. Možnosti upřednostňovat některé linky při redundantním připojení na základě lokální preference. Jednotlivé přístupové sítě pak jsou děleny do autonomních oblastí, kde má každá přiděleno své unikátní číslo. Jako zástupce jmenuji BGP (Border Gateway Protocol).

[7]Doba, za kterou je všem prvkům známa topologie sítě.

3 VIRTUÁLNÍ LOKÁLNÍ SÍTĚ NA LINKOVÉ VRSTVĚ

Při vytváření firemních sítí nastal problém s fyzickým rozložením stanic v budovách a adresací. Bylo zapotřebí sloučit jednotlivé logické celky sídlící na více podlažích do jedné virtuální sítě na linkové úrovni a zamezit tak zbytečným všesměrovým zprávám, které bylo zbytečné zasílat všem stanicím. Dle standardu IEEE 802.1Q pro identifikaci různých sítí VLAN (Virtual Local Area Network) využívá techniky značení rámců. Pole je vkládáno za zdrojovou MAC adresu. Pro identifikaci VLAN se využívá 12 bitů, takže je možné označit až 4096 VLAN. Do tohoto standardu byl ještě implementován standard 802.1p (pojednává o prioritách). Na určení mu jsou přiděleny 3 bity.



Obr. 3.1: Struktura rámce 802.1Q/p na linkové vrstvě.

Jelikož přepínače pracují pouze na linkové vrstvě, navzájem se jednotlivé virtuální sítě nevidí (pracují jen s rámci) a nemohou mezi sebou komunikovat. Při komunikaci mezi jednotlivými virtuálními sítěmi je nutno připojit směrovač (nebo L3 přepínač[1]) do topologie a patřičně jej nastavit.

[1] L3 přepínač může pracovat na třetí vrstvě modelu TCP/IP. Podporuje i směrovací protokoly. Je řešen hardwarovou implementací (rychlejší zpracování a přeposlání dat) – řeší jen základní úkony.

3.1 Způsoby přiřazení virtuálních sítí

Přiřazení do virtuálních sítí se může lišit dle potřeb. Je důležité, aby koncová stanice byla stále ve správné VLAN, aby zbytečně nezahlcovala směrovač. Pro přiřazení do VLAN lze použít následující možnosti:

- VLAN dle portu na přepínači – jednotlivým portům na přepínači lze manuálně přiřadit, ke kterým virtuálním sítím budou přiřazeny.
- VLAN dle MAC adresy hostů – je to dynamické řešení, kdy na přepínači nastavíme, která MAC adresa bude přiřazena do které virtuální sítě. Když tento host změní zapojení a připojí se přes jiný port, zůstane pořád ve své VLAN.
- VLAN založené na síťové vrstvě – slučuje stanice jednoho protokolu do jedné virtuální sítě (IP, IPX, AppleTalk).
- VLAN definované politikou – sdružuje všechny způsoby zmíněny výše. Je nejpřizpůsobivější, jelikož umožňuje výběr VLAN definovat na základě kombinace různých kritérií.

V praxi se používá především přiřazení do VLAN sítě dle zapojení do portu na přepínači.

Při použití poslední možnosti tj. dynamické přidělení do VLAN musím přepínače podporovat standard 802.1x. Ten používá komunikační protokol Extensible Authentication Protocol (EAP). Připojený uživatel (NE koncový prvek) se pak musí autentizovat přepínači, který dále komunikuje s RADIUS serverem (Remote Authentication Dial In User Service). RADIUS server porovná zadané hodnoty (jméno a heslo) se svou databází a zjistí, do které VLAN uživatel patří a přiřadí jej do ní. Při zamítnutí znemožní přístup počítače do sítě.

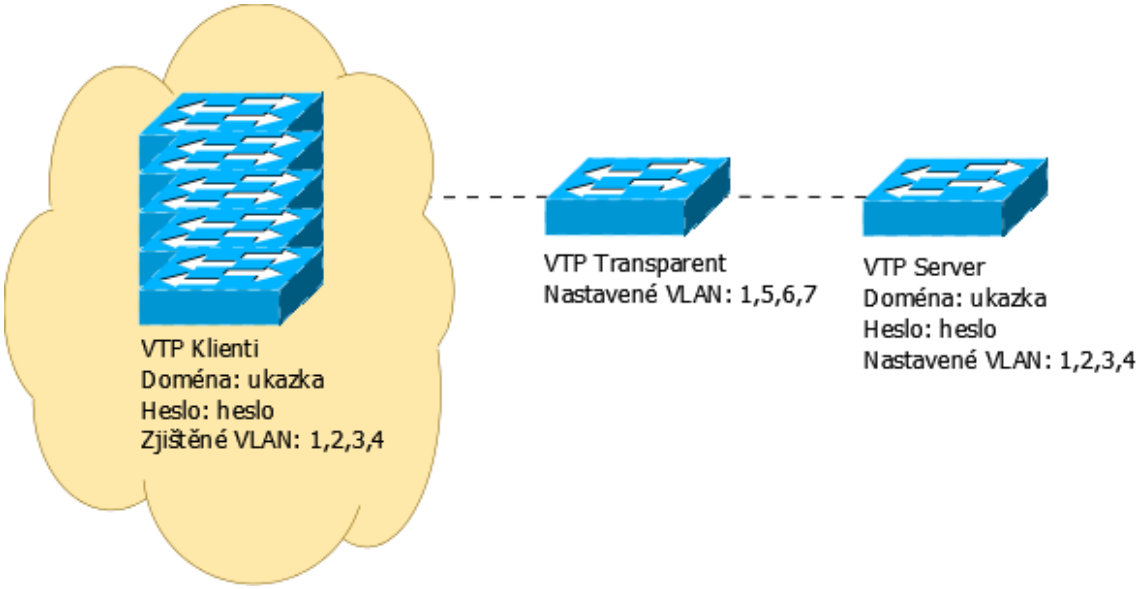
Návštěvníci firemní sítě mohou být na základě neúspěšné autentizace (nemají potřebné údaje ke vstupu do interní sítě) přepojeni do VLAN, která má přístup jen k Internetu, avšak ne k interním serverům.

Do této VLAN jsou připojeni i uživatelé, jejichž zařízení nepodporuje standard 802.1x. Tudíž nemají možnost komunikovat s RADIUS serverem přes protokol EAP.

3.2 Rozsáhlé sítě s VLAN

Při správě více přepínačů v síti je náročné při změně politiky přidělení VLAN aplikovat veškerá pravidla. Jednotlivé přepínače se musí nastavovat zvlášť. Firma Cisco přišla s řešením. Jedná se o proprietární VTP protokol (VLAN Trunking Protocol), který zajišťuje rozesílání založených VLAN v síti. Zvolí se hlavní přepínač – server. Ostatní přepínače jsou klienti. Všechny přepínače musí být přiřazeny do jedné domény s platným heslem. Klientské přepínače pak dostanou informace o vytvořených VLAN sítích od hlavního přepínače. Poté lze jednoduše upravovat jednotlivé VLAN v celé rozsáhlé síti na jednom přepínači.

Přepínač může být ještě v transparentním módu. To má za následek přeposílání VLAN ve směru od serveru na své ostatní porty, ale zároveň může mít nastavené své vlastní VLAN. Ty jsou nezávislé na nastavení serveru.



Obr. 3.2: Příklad použití VTP protokolu.

4 TECHNOLOGIE NA ZAJIŠTĚNÍ KVALITY SLUŽBY (QOS)

Pro začátek je nutné si uvědomit, že QoS neumožňuje zasílání provozu nad rámec možnosti linky (fyzického spoje). Je to jen sada možností, jak upřednostnit provoz specifikovaných dat na síti (VoIP, FTP, HTTP, ...) a lépe využít celé šířky pásma.

Z počátku provozu na síti nebylo zapotřebí QoS zřizovat. V 90. letech byl však již traffic[1] nadměrný a bylo nutné zajistit šířku pásma pro prioritní služby. V IP paketu bylo vyhrazeno 8bitové pole pro ToS (Type of Service). Tato služba umožňovala různé zacházení s paketem. V praxi se však moc nerozšířila.

Ve službě DiffServ toto 8bitové pole nahradilo pole DSCP (Differentiated Service Code Point). DSCP pole využívalo prvních 6 bitů a bylo možné rozdělit tok dat až do 64 tříd. Služba se ze začátku využívala především v transportní síti na globální úrovní. Klade menší nároky na hardware zařízení. V dnešní době se používá i v podnikových sítích.

Služba IntServ je vhodnější především pro interní podnikové sítě, jelikož pro správné fungování potřebuje velkou režii před zahájením spojení. Což by na celosvětové úrovni příliš zatěžovalo síťové prvky. V dnešní době se s ní již málokdy setkáte.

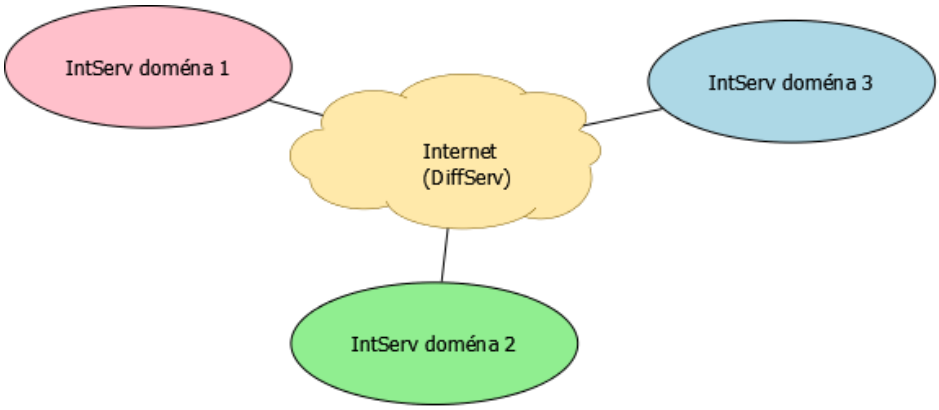
V případě nenastavení žádné z výše zmíněných služeb, uplatní se nenáročná služba Best-Effort. Ta má snahu jakýkoliv přijatý paket ihned odeslat, aniž by rozlišoval druh dat obsažených v paketu.

4.1 Integrated services – IntServ

Služba Intserv se rozšířila především v začátcích QoS. Pro správnou funkci musí být všechny síťové prvky pod kontrolou jednoho administrátora, který nastaví jednotnou QoS politiku. Z toho vyplývá, že je nemyslitelné rozšíření této služby na globální úrovni. IntServ funguje na bázi rezervace šířky pásma před uskutečněním samotné služby, kdy každý směrovač rezervuje část linky pro požadovanou službu. Celý tento proces je náročný na procesorový čas směrovačů v síti. Zároveň s přibývajícím počtem koncových stanic a provozovaných služeb rapidně roste provoz spojený s rezervací pásma.

Problém nastává při cestě paketu mimo IntServ doménu. Na globální úrovni se totiž používá služba DiffServ (zmíním se o ní v další kapitole). Na tu se IntServ namapuje a je tak zajištěna podpora kvality služeb napříč celou sítí – záleží již na nastavení správců DiffServ domény, jaké parametry služby IntServ přiřadí.

[1] Provoz na síti.



Obr. 4.1: Znázornění výskytu Intserv a DiffServ domény.

4.1.1 Protokol RSVP (Resource reSerVation Protocol)

Protokol pro rezervace prostředků dokáže dopředu zajistit pro data dostatečnou šířku pásma pro průchod sítí. Jeho první verze byla uvedena v roce 1997 (RFC 2205). Protokol je založený na bázi otázek a odpovědí. Odesílatel posílá zprávy *path* a příjemce odpoví zprávou *resv*. Zamluvení šířky pásma probíhá vždy v jednom směru a pak následně stejným způsobem v druhém směru, pokud je to zapotřebí (např. VoIP telefonie × sledování videa přes síť).

- *Path* – nese informaci od odesílatele nebo jiného uzlu sítě o parametrech rezervace, potvrzení nebo zamítnutí žádosti o rezervaci.
- *Resv* – specifikuje požadavky na vytvoření, změnu nebo zrušení rezervace prostředků.

Když zpráva *path* projde přes směrovače, znamená to, že směrovače jsou schopny rezervovat požadované parametry tímto směrem. Už jen zbývá potvrzení cílovou stanicí. Odpoví zpět zprávou *resv* a požadované parametry spojení jsou v jednom směru zaručeny.

Obr. 4.2: Průběh rezervace prostředků pro zajištění přesnosu.

Pro vyhrazení pásma v obou směrech se proces opakuje ještě jednou z opačné strany.

4.2 Differentiated services – DiffServ

Pro globální sítě bylo zapotřebí zvolit jiný přístup pro zajištění kvalitního přenosu. Metoda IntServ by kladla na směrovače ve světovém měřítku příliš velkou náročnost na procesorový čas. DiffServ jednotlivé toky paketů rozděluje do tříd. Tuto hodnotu zapisuje do prvních 6 bitů v IP paketu do pole ToS. Jedná se o tzv. kód služby DSCP. Představíme-li si síť s podporou DiffServ, tak kterýkoliv provoz směřující přes tuto síť se označkuje pouze na okrajových směrovačích (zapíše se hodnota do DSCP). V těch místech dojde k sdružení paketů stejného druhu do tříd služeb. Aneb směrovač nerozlišuje jednotlivé VoIP hovory jako IntServ, ale upřednostňuje celou skupinu hovorů. U ostatních směrovačů již probíhá prioritní směrování paketů jen na základě hodnoty v políčku DSCP.

4.2.1 Rozdělení provozu do tříd

Okrajový směrovač (BA, Behavior Aggregate) v DiffServ doméně nejdříve klasifikuje pakety do jednotlivých tříd a nastaví jim DSCP pole na určitou hodnotu. Vnitřní směrovače pak již neznačkují pakety (jsou již označkovány), ale jen pracují dle hodnoty v poli DSCP a nastaveného chování (PHB, Per Hop Behavior).

Provoz je rozdělen do tří základních tříd – Expedited Forwarding (EF), Assured Forwarding (AF) a Best Effort (BE). Třída AF se ještě dělí na další čtyři podtřídy, kde v každé jsou ještě tři podkategorie (malá, střední a velká pravděpodobnost zahození). Jednotlivé třídy (EF, AF1–AF4 a BE) se liší v prvních třech bitech DSCP pole. Tyto tři bity jsou zároveň využívány u pole ToS a služby IP Precedence, takže jsou obě služby navzájem kompatibilní. Rozdělení DSCP a IP Precedence naleznete v tabulce 4.1.

Pro QoS je doporučeno vyhradit maximálně 75 % šířky pásma na lince. Je důležité stanovit priority, kterou službu upřednostníme a kterou ne. Rozdělení se může lišit dle interního nařízení firmy. Avšak hlavní služby – hlasová, videokonferenční, směrovací proces atd. bývají celosvětově zařazeny do shodných tříd, primárně z důvodů globální jednotnosti.

Lze taktéž nastavit, že všechna data, která se nezařadí do nějaké třídy, budou přiřazena do třídy Best Effort.

Tab. 4.1: Dělení tříd u DiffServ se zpětnou kompatibilitou na ToS.

Třída	IP Precedence	Označení třídy	DSCP pole
Expedited Forwarding	5	EF	**101**110
Assured Forwarding:		AF:	
Class Selector 4 (CS4)	4	AF41	**100**010
		AF42	**100**100
		AF43	**100**110
Class Selector 3 (CS3)	3	AF31	**011**010
		AF32	**011**100
		AF33	**011**110
Class Selector 2 (CS2)	2	AF21	**010**010
		AF22	**010**100
		AF23	**010**110
Class Selector 1 (CS1)	1	AF11	**001**010
		AF12	**001**100
		AF13	**001**110
Best Effort	0	BE	**000**000

4.2.2 Optimální přidělení šířky pásma službám

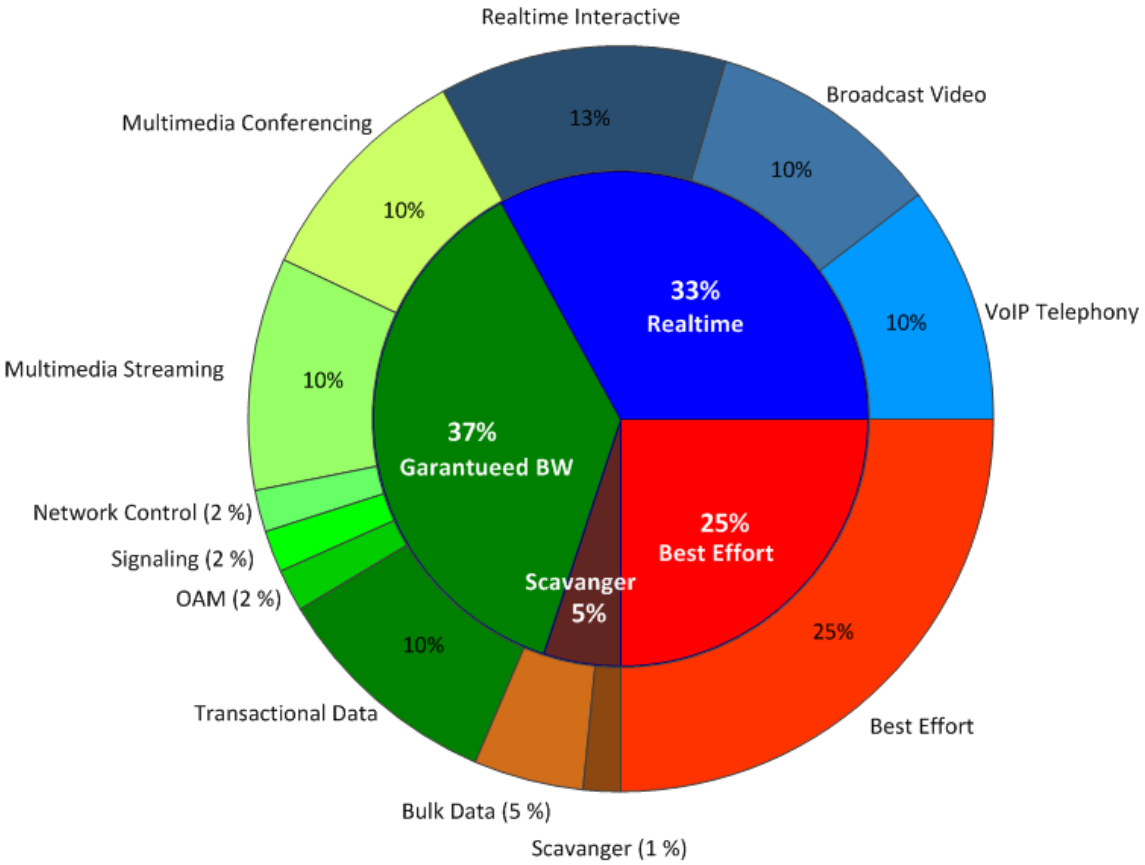
Při požadavku zavedení QoS ve firemní síti je potřeba analyzovat provoz na síti a zjistit, které služby a v jaké míře zatěžují síť. Na základě této analýzy, pak můžeme stanovit jednotlivým službám šířku pásma v procentech z rychlosti linky nebo přímo v kbit/s.

Firma Cisco vytvořila referenční model rozdělení šířky pásma pro kampusové sítě dle počtu požadovaných tříd. Existuje základní model, kde jsou služby rozděleny do 4 tříd. Těmi jsou Realtime, Garantueed BW, Scavanger a Best Effort. Podrobnější model obsahuje až 12 tříd. Oba modely si můžete prohlédnout na obrázku 4.3.

Model dělený na 12 tříd se ještě může lišit dle místa aplikování. V páteři sítě se používá lehce odlišné rozdělení. Optimální přiřazení DSCP jednotlivým třídám naleznete v tabulce 4.2.

Provoz můžeme identifikovat různě, ideálně na bázi IP adresy nebo portu – pakety směrovacího protokolu OSPF používají všesměrové adresy 224.0.0.5 a 224.0.0.6, hovorová signalizace protokolu SIP používá port 5060, IP adresy video serverů atd. Tento proces zatěžuje nejméně hardware směrovačů.

Pakety lze rozlišit taky na vyšších vrstvách – pakety pro přenos hlasu (RTP), pro přenos dat (FTP), pro administraci směrovačů (Telnet) atd. Nevýhodou však je celkové zpomalení operace a větší nárok na hardware směrovačů.



Obr. 4.3: Čtyř a dvanácti třídní model při zavádění podpory QoS.

Tab. 4.2: Přiřazení tříd DSCP aplikacím.

Služba	Označení třídy
VoIP Telephony	EF
Broadcast Video	CS5
Real-Time Interactive	CS4
Multimedia Conferencing	AF4
Multimedia Streaming	AF3
Network Control	CS6
Signaling	CS3
OAM	CS2
Transactional Data	AF2
Bulk Data	AF1
Best Effort	BE
Scavanger	CS1

4.3 Rozdělení provozu do front

Aby směrovač mohl zacházet s pakety, musí mít jednoznačně stanovená pravidla. Směrovač dle nastavení používá pro různé třídy odlišné fronty, podle kterých pak může upřednostňovat pakety s vyšší prioritou a zasílat je dříve.

- **First-In, First-Out (FIFO)**
  Tato fronta funguje na principu „kdo dřív přijde, ten dřív mele“. Aneb první příchozí paket na rozhraní bude přeposlán dále. Toto zacházení může způsobit nepříjemné zahazování VoIP paketů, když se například dostanou do toku s objemnými datovými pakety.

- **Priority Queueing (PQ)**
  Směrovač rozlišuje pakety až se čtyřmi prioritami – vysoká, střední, normální a malá. Pakety jsou do nich rozděleny a poté přeposílány. Tato metoda však nedokáže obsloužit všechny fronty. Když při provozu narostou data s vysokou prioritou, směrovač se je snaží pořád přeposílat, avšak k uvolnění paměti zahazuje pakety s nižší prioritou a tím může dojít až k výpadku uskutečněných nižších služeb.

- **Weighted Fair Queueing (WFQ)**
  V této skupině se dělí datové toky do více skupin – data náročná a nenáročná na šířku pásma. Pakety zde mají různou váhu a dle té dostanou přidělenou různou šířku pásma (například procentuálně). Pakety s vysokou prioritou pak mají definované procento šířky pásma pro přenos. Pakety s malou prioritou využívají zbylou šířku pásma. Tento mechanizmus nechává přistupovat k médiu všechny fronty a nedojde tím pádem k zahazování paketů při přílišném provozu paketů s vysokou prioritou.

- **Class-based WFQ (CBWFQ)**
  U této metody jsou pakety rozlišeny ještě v jednotlivých váhových frontách do tříd, dochází tak k lepšímu třídění.

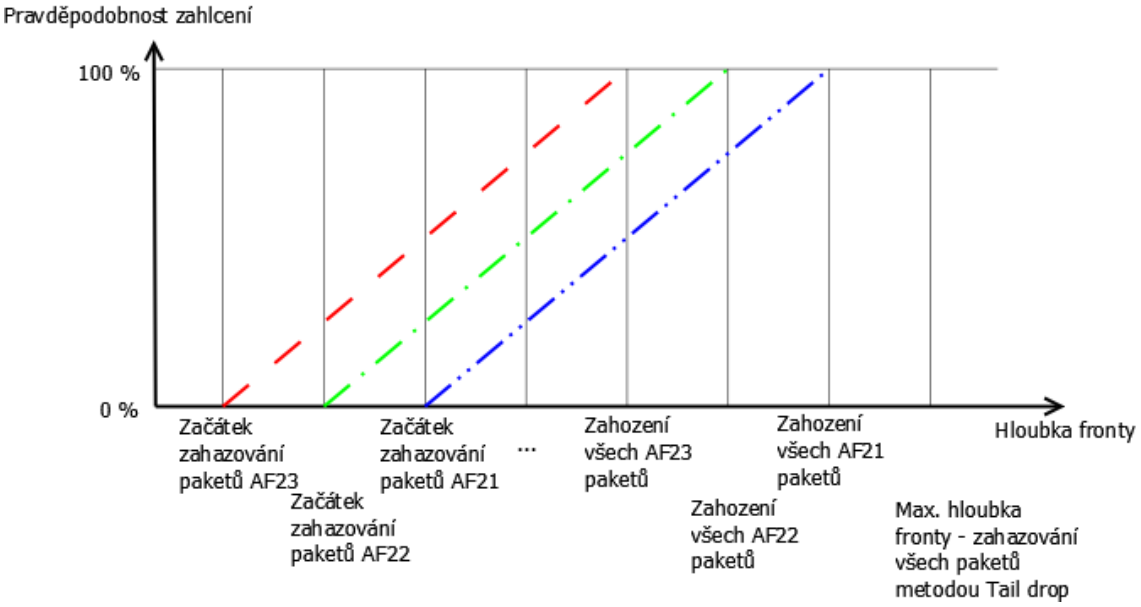
- **Low Latency Queueing (LLQ)**
  Původní název této fronty LLQ byl Priorit Queueing CBWFQ. Nevýhoda fronty CBFWQ je, že nedokáže striktně prioritizovat určité pakety (VoIP). Toto umí až fronta LLQ, která zaručuje prioritní obsloužení této fronty. Je vhodné ji používat zřídka a jen pro Real-Time služby.

4.4 Možnosti jak předejít zahlcení síťového prvku

Při běžném provozu je možné předejít stavu zahlcení síťového prvku detekcí obsazenosti příchozí vyrovnávací paměti. Náhodné zahazování paketů ve frontě (Random Early Detection – RED) ovlivňuje globální synchronizaci TCP protokolu. Pro ten je lepší, když se náhodně zahodí paket, než aby došlo ke stavu úplného zahlcení a zahazovaní metodou Tail Drop, která zahazuje všechny pakety. Toto náhodné zahození ovlivní, že pakety jsou znovu vyslány, ale nedojde k novému pomalému startu TCP (zvětšování posuvného okénka od 0).

Existuje ještě vážené náhodné zahazování paketů (Weighted Random Early Detection – WRED), které bere v potaz prioritu paketů (IP Precedenci nebo DSCP). Vždy je nejdříve zahazována třída s nižší prioritou. Viz obrázek 4.4.

Protože protokol UDP nepodporuje žádný zpětný pokus o znovu vyslání paketu, tak jej tyto metody (RED, WRED) nijak neovlivní.



Obr. 4.4: Zahazování metodou WRED (DSCP).

4.5 Protokoly TCP a UDP na transportní vrstvě

4.5.1 Transsmission Control Protocol

Protokol TCP zajišťuje *spolehlivý a spojově orientovaný* přenos IP paketů po síti. Na každou odeslanou zprávu musí příjemce odpovědět zprávou o doručení (ACK). Jelikož při průchodu zprávy paketovou sítí, (kde je každý paket směrován zvlášť), může dojít k zamíchání pořadí jednotlivých paketů jedné zprávy, je nutné číslovat vyslané zprávy i odpovědi na ně. Tohoto přenosu se využívá především u zpráv, kde není přípustné jejich narušení v průchodu přes datovou síť. Jedná se například o služby e-mail, FTP, HTTP a další.

4.5.2 User Datagram Protocol

Protokol UDP zajišťuje *nespolehlivý a nespojově orientovaný* přenos IP paketů po síti. Příjemce na zaslané zprávy neodesílá odpověď a tím zrychluje proces přenosu dat. Při průchodu sítí může dojít také k záměně pořadí paketů, ale jejich zpoždění v síti by mělo mnohem horší následek na kvalitu služeb, u kterých se protokol UDP používá. Jedná se zejména o služby v reálném čase – hlasová a video-konferenční služba. Výpadek malého množství paketů poznáme krátkým výpadkem hlasu.

5 NÁVRH EXPERIMENTÁLNÍ SPOLEHLIVÉ SÍTĚ

Při návrhu experimentální spolehlivé sítě jsem vycházel z vybavení laboratoře. Z těchto důvodů tuto síť nebylo možno zajistit například proti výpadku elektrické energie. Při sestavování sítě jsem se snažil zahrnout do topologie zařízení od více výrobců, abych si prakticky vyzkoušel odlišný postup nastavování. Vybíral jsem taková zařízení, která podporují standardy, které chci v této síti aplikovat a testovat (802.1D – STP, 802.1w – RSTP, 802.1s – MSTP a 802.1q – VLAN).

Jako směrovací prvek jsem zvolil Cisco směrovač 1812w (obr. 5.1), který disponuje dvěma FastEthernetovými porty s integrovaným přepínačem.

Pro redundantní síť jsem volil tři přepínače. Dva modely od ASUSu a jeden od Linksysu. U ASUSu jsem volil model GigaX 3112F (obr. 5.1), od Linksysu pak model SRW2008P (obr. 5.1).

Obr. 5.1: Vybrané síťové prvky do experimentální sítě, zleva: přepínač ASUS GigaX 3112F, přepínač Linksys SRW2008P a směrovač Cisco 1812W.

5.1 Schéma zapojení a adresace

Pro zapojení experimentální sítě jsem využil metalických kabelů. Všechny přístroje podporují u jednotlivých portů funkci MDI/MDIX, proto jsem mohl zapojit všude přímé UTP kabely. Topologické schéma naleznete na obrázku 5.2. K zařízením jsem se připojoval přes konzolový port pro základní nastavení, abych zprovoznil webové rozhraní. V něm jsem pak nastavil další parametry, tento postup jsem udělal u všech přepínačů. Směrovač jsem nastavoval přes příkazový řádek (CLI – Command Line), kterým jsem obsluhoval nainstalovaný systém Cisco IOS. Jednotlivým síťovým prvkům jsem pak přiřadil adresy dle tabulky 5.1.

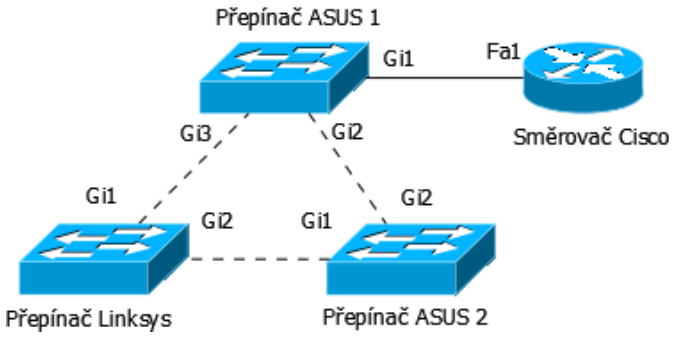
U přepínačů jsem do VLAN 2 přiřadil gigabitové porty 5 a 6, zatímco do VLAN 3 jsem přiřadil gigabitové porty 7 a 8. U trunkovacích linek mezi přepínači jsem nastavil značkování VLAN 2 a 3, zároveň jsem nastavil neznačkování nativní

VLAN 4. Totéž je nastaveno mezi směrovačem a přepínačem. Pro snadné nastavování přepínačů jsem ještě jeden port Gi4 na přepínači ASUS 1 nechal neznačkovaný pro přístup do nativní VLAN 4.

Jako nativní VLAN jsem úmyslně volil VLAN 4. Je to z důvodu bezpečnosti, aby se běžný uživatel neměl možnosti připojit na přepínače (všechny porty ve výchozím nastavení patří do VLAN 1).

Tab. 5.1: Adresace v experimentální sítí.

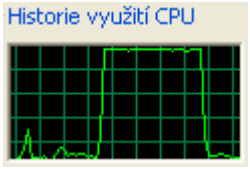
Síťový prvek	Síťové rozhraní	IP adresa	Síť	Komentář
Cisco	Fa1.2 (subint)	192.168.2.1	192.168.2.0/30	VLAN 2
	Fa1.3 (subint)	192.168.3.1	192.168.3.0/24	VLAN 3
	Fa1.4 (subint)	192.168.4.1	192.168.4.0/24	mgmt VLAN 4
ASUS 1	VLAN 4	192.168.4.2	192.168.4.0/24	mgmt VLAN 4
ASUS 2	VLAN 4	192.168.4.3	192.168.4.0/24	mgmt VLAN 4
Linksys	VLAN 4	192.168.4.4	192.168.4.0/24	mgmt VLAN 4



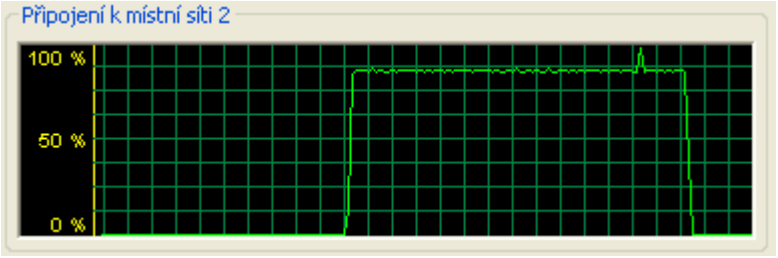
Obr. 5.2: Schéma zapojení v experimentální sítí.

5.2 Zahlcení v případě smyčky

V teoretické části (viz kapitola 2.1) jsem zmínil Broadcast storm a jeho dopad na provoz sítě. Když zapojíme schéma (obr. 5.2) bez připojeného směrovače, bude komunikace probíhat jen na linkové úrovni a může tak dojít k Broadcast storm. Na jakoukoliv komunikaci musí každý síťový prvek odpovědět. V případě ARP dotazu budou pakety permanentně kolovat přes síť tam a zpět. Nejen, že zabírají procesorový čas, jak lze vidět na obr. 5.3, ale také nadbytečně vytěžují linku viz obr. 5.4. Mnohdy může nastat situace, že ji zahltí tak, že se není možné připojit přes telnet k síťovým prvkům a musíme tedy zasáhnout manuálně a některé spoje odpojit. U mého pokusu kolovalo v síti kolem 150 000 paketů za sekundu (viz obr. 5.5).



Obr. 5.3: Vytížení procesoru při Broadcast storm.



Obr. 5.4: Vytížení linky při Broadcast storm.

Description	IP	Packets	Packets/s
Realtek RTL8139 Family Fast Ethernet Adapter (Microsoft's Packet Scheduler)	192.168.1.11	1341390	148585

Obr. 5.5: Počet paketů za sekundu při Broadcast storm.

5.3 Prověření funkce STP

Ještě předtím, než jsem zapojil přepínače do smyčky, jsem na každém přepínači musel povolit protokol STP, jelikož byl na všech přepínačích ve výchozím stavu zakázaný. Nechal jsem u něj výchozí nastavení priorit portů (128) a přepínače (32678). Očekávané chování bylo, že dle nejnižší MAC adresy se zvolí hlavní přepínač. V zapojení jsou přepínače s MAC adresami dle tabulky 5.2. Po výměně zpráv BPDU došlo ke zvolení *Root* přepínače, tím se stal ASUS 2.

Po zvolení *Root* přepínače si od něj ostatní přepínače začaly počítat cenu k jeho portům, tím zjistí nejlepší cestu. Když náhodou dojde k situaci, že cena cesty k hlavnímu přepínači je přes oba dva porty stejná, rozhoduje pak nastavená priorita portu. Když i ta je stejná, tak přepínač s nižší MAC adresou uvede port do stavu *Forwarding*. Jelikož MAC adresa přepínače Linksys je větší, tak uvedl port Gi2 do stavu *Blocking* (obr. 5.6), zatímco port Gi3 přepínače ASUS 1 je ve stavu *Forwarding*.

Až se přepínače úspěšně dohodly a začaly normálně posílat data sítí, jsem odpojil port Gi1 na Linksysu, který byl ve stavu *Forwarding*. Po změně topologie trvalo téměř 30 sekund, než se přepínače znovu dohodly a začaly posílat data po síti, jak je zdokumentováno na obrázku 5.7.

Tab. 5.2: MAC adresy přepínačů v laboratoři.

Síťový prvek	Priorita	MAC adresy
ASUS 1	32678	00:17:31:ce:9f:c6
ASUS 2	32678	00:17:31:ce:9f:c2
Linksys	32678	00:18:f8:9f:cc:63

Port	STP	Port Fast	Port State	Port Role	Speed	Path Cost	Priority	Designated Bridge ID
g1	Enabled	Disabled	Forwarding	Root	1000M	20000	128	32768-00:17:31:ce:9f:c2
g2	Enabled	Disabled	Blocking	Alternate	1000M	20000	128	32768-00:17:31:ce:9f:c6

Obr. 5.6: Zachycení stavu portů na přepínači Linksys po rozběhnutí STP protokolu.

```
c:\>ping 192.168.4.1 -n 10

Příkaz PING na 192.168.4.1 - 32 bajtů dat:
Odpověď od 192.168.4.1: bajty=32 čas < 1ms TTL=255
Odpověď od 192.168.4.1: bajty=32 čas < 1ms TTL=255
Odpověď od 192.168.4.1: bajty=32 čas < 1ms TTL=255
Vypršel časový limit žádosti.
Vypršel časový limit žádosti.
Vypršel časový limit žádosti.
Vypršel časový limit žádosti.
Vypršel časový limit žádosti.
Vypršel časový limit žádosti.
Odpověď od 192.168.4.1: bajty=32 čas=1ms TTL=255

Statistika ping pro 192.168.4.1:
Pakety: Odeslané = 10, Přijaté = 4, Ztracené = 6 (ztráta 60%),
Přibližná doba do přijetí odezvy v milisekundách:
    Minimum = 0ms, Maximum = 1ms, Průměr = 0ms
```

Obr. 5.7: Zachycení příkazu ping po odpojení portu Gi1 na přepínači Linksys ze stavu *Forwarding*, čekání na přepnutí portu Gi2 ze stavu *Blocking* na *Forwarding*.

5.3.1 Změna Root přepínače pomocí priority

U přepínače s nejvyšší MAC adresou (Linksys, viz tab. 5.2) jsem nastavil prioritu pro volbu hlavního přepínače na hodnotu 16384 (musí to být násobek čísla 4096). Hned poté se celý koloběh volby hlavního přepínače a portů rozběhl od začátku. S ohledem na prioritu byl zvolen *Root* přepínačem Linksys a port Gi2 u přepínače ASUS 1 se přepnul do role *Non-designated* a stavu *Blocking* (přepínač ASUS 2 má menší MAC adresu než přepínač ASUS 1). Lze to pozorovat na obrázku 5.9. Změna *Root* přepínače je uvedena na obrázku 5.8. Oba porty mají roli *Designated* a jsou ve stavu *Forwarding*.

Jelikož použité přepínače jsou různě staré, tak si na výpisech na obrázcích 5.6 a 5.9 můžete všimnout různé ceny cesty na gigabitových linkách. V reálné intersíti je nutné tyto parametry sjednotit.

Port	STP	Port Fast	Port State	Port Role	Speed	Path Cost	Priority	Designated Bridge ID
g1	Enabled	Disabled	Forwarding	Designated	1000M	4	128	16384-00:18:f8:9f:cc:63
g2	Enabled	Disabled	Forwarding	Designated	1000M	4	128	16384-00:18:f8:9f:cc:63

Obr. 5.8: Volba *Root* přepínače Linksys pomocí změněné priority.

Port	State	Root Cost	Path Cost	Priority
gigabitethernet1/0/1	Forwarding	4	19	128
gigabitethernet1/0/2	Alternate	4	4	128
gigabitethernet1/0/3	Forwarding	4	4	128

Obr. 5.9: Na přepínači ASUS 1 lze pozorovat přechod portu Gi2 do role *Non-designated* (stav *Blocking*), z důvodu vyšší MAC adresy.

5.3.2 Rapid Spanning Tree Protocol

Tento protokol jsem podstoupil stejné zkoušce jako STP. Na všech přepínačích jsem zapnul RSTP. Porty během pár sekund přešly do stavu *Forwarding*. Na přepínači Linksys byl totožně jako při protokolu STP port Gi2 ve stavu *Discarding* (u RSTP byl stav *Blocking* přejmenován na *Discarding*).

Poté jsem zadal příkaz `ping` s parametrem `-n` (počet vyslaných pingů) – `ping 192.168.3.11 -n 5`. Vypojil jsem port Gi1 na Linksysu, který byl ve stavu *Forwarding*, následně jeden ping vypadl. Avšak během nepatrné doby si RSTP poradilo se změnou topologie a port Gi2 byl rychle ve stavu *Forwarding*. Průběh příkazu ping můžete sledovat na obrázku 5.10. Na tomto příkladu demonstruji vylepšení protokolu RSTP v porovnání s protokolem STP a jeho rychlou obnovu po změně topologie sítě.

```
C:\>ping 192.168.3.11 -n 5

Příkaz PING na 192.168.3.11 - 32 bajtů dat:
Odpověď od 192.168.3.11: bajty=32 čas < 1ms TTL=128
Odpověď od 192.168.3.11: bajty=32 čas < 1ms TTL=128
Vypršel časový limit žádosti.
Odpověď od 192.168.3.11: bajty=32 čas < 1ms TTL=128
Odpověď od 192.168.3.11: bajty=32 čas < 1ms TTL=128

Statistika ping pro 192.168.3.11:
Pakety: Odeslané = 5, Přijaté = 4, Ztracené = 1 (ztráta 20%),
Přibližná doba do přijetí odezvy v milisekundách:
    Minimum = 0ms, Maximum = 0ms, Průměr = 0ms
```

Obr. 5.10: Rychlé znovuobnovení přenášení dat při použití RSTP po změně topologie.

5.3.3 Multiple STP

Stále vycházím ze stejného zapojení, viz obr. 5.2 a MAC adres dle tab. 5.2. Při nastavování MSTP jsem vycházel z výchozího nastavení, kdy všechny VLAN byly přiřazeny do STP instance 0. Zprovoznil jsem další STP instanci 1, do které jsem přidal VLAN 2. Všechny tři přepínače jsem připojil do domény se jménem *mstp*. Po tomto nastavení byl pro obě instance STP zvolen *Root* přepínačem ASUS 2 (nejnižší MAC adresa). Pak jsem na přepínači ASUS 1 nastavil *Bridge Root Priority* pro instanci 1 na 16384. K této hodnotě je ještě přičteno číslo instance, proto je ve výpise na obrázku 5.11 priorita 16385.

Instance ID	VLAN Group	MAC Address	Priority
0	1,3-4094	0017.31ce.9fc2	32768
1	2	0017.31ce.9fc6	16385

Obr. 5.11: Rozdíl *Root* přepínačů pro jednotlivé instance STP na ASUSu 1.

5.4 Prověření funkce VLAN

5.4.1 Komunikace v jedné VLAN

V teoretické části jsem uvedl, že pro komunikaci v jedné VLAN není zapotřebí v topologii směrovač. Do libovolných portů přepínačů náležících VLAN 2 (5 a 6) jsem připojil počítače s adresami dle tabulky 5.3. Nezáleží na tom, zda-li jsou obě PC připojena do jednoho stejného nebo do dvou různých přepínačů.

Pro ověření dostupnosti zařízení jsem na jednom počítači spustil v příkazové řádce příkaz `ping 192.168.2.11 -n 10`. Směrovač jsem odpojil zadáním příkazu `shutdown` pro rozhraní Fa1. Po zadání nedošlo k výpadku spojení a druhý počítač neustále odpovídal na příkaz `ping`.

Na tomto příkladu jsem demonstroval, že pro komunikaci v jedné VLAN není zapotřebí připojený směrovač v síti. K přepínání dochází na úrovni linkové vrstvy na bázi MAC adres a pole, které přidal standard 802.1Q.

Tab. 5.3: Přiřazené adresy počítačům při komunikaci v jedné VLAN.

PC	IP adresa	Síť
PC1 (VLAN3)	192.168.2.10	192.168.2.0/24
PC2 (VLAN3)	192.168.2.11	192.168.2.0/24

```
c:\>ping 192.168.2.11 -n 10

Příkaz PING na 192.168.2.11 - 32 bajtů dat:
Odpověď od 192.168.2.11: bajty=32 čas < 1ms TTL=128
Odpověď od 192.168.2.11: bajty=32 čas < 1ms TTL=128
Odpověď od 192.168.2.11: bajty=32 čas < 1ms TTL=128
Odpověď od 192.168.2.11: bajty=32 čas < 1ms TTL=128
Odpověď od 192.168.2.11: bajty=32 čas < 1ms TTL=128
Odpověď od 192.168.2.11: bajty=32 čas < 1ms TTL=128
Odpověď od 192.168.2.11: bajty=32 čas < 1ms TTL=128
Odpověď od 192.168.2.11: bajty=32 čas < 1ms TTL=128
Odpověď od 192.168.2.11: bajty=32 čas < 1ms TTL=128
Odpověď od 192.168.2.11: bajty=32 čas < 1ms TTL=128

Statistika ping pro 192.168.2.11:
Pakety: Odeslané = 10, Přijaté = 10, Ztracené = 0 (ztráta 0%),
Přibližná doba do přijetí odezvy v milisekundách:
    Minimum = 0ms, Maximum = 0ms, Průměr = 0ms
```

Obr. 5.12: Zachycení příkazu ping při komunikaci mezi zařízeními, která náleží do stejné VLAN.

5.4.2 Komunikace mezi různými VLAN

Chování jsem ověřil podobně jako u komunikace v jedné VLAN pomocí příkazu ping zadaném na jednom počítači. PC1 jsem zapojil do VLAN 2 a dle ní také adresoval. PC2 jsem zapojil do VLAN 3 a přiřadil odpovídající adresu (viz tab. 5.4). Opět nezáleží na tom, zda-li jsou obě PC připojena do jednoho nebo do dvou různých přepínačů.

Tab. 5.4: Přiřazené adresy počítačům při komunikaci mezi různými VLAN.

PC	IP adresa	Síť
PC1 (VLAN2)	192.168.2.10	192.168.2.0/24
PC2 (VLAN3)	192.168.3.11	192.168.3.0/24

Pro ověření dostupnosti zařízení jsem na PC1 spustil v příkazové řádce příkaz `ping 192.168.3.11 -n 10`. Směrovač jsem poté odpojil zadáním příkazu `shutdown` pro rozhraní Fa1. Po zadání došlo k výpadku spojení. To lze vidět na vypadnutí několika pingů. Na směrovači jsem poté opět rozhraní Fa1 zapnul příkazem `no shutdown`. Tím došlo zpátky k obnovení komunikace mezi různými VLAN (viz obr. 5.13).

Na tomto příkladu demonstruji průběh komunikace mezi různými VLAN. Každá je v jiné síti a tím pádem dochází k směrování na síťové vrstvě, kterou zprostředkovává směrovač.

Ještě zdůrazňuji, že jsem přepnul port přepínače, kterým je připojen ke směrovači do role *Edge port*. Z tohoto důvodu měření není ovlivněno chováním protokolu RSTP a port tak ihned přejde do stavu *Forwarding*.

```
c:\>ping 192.168.3.11 -n 10

Příkaz PING na 192.168.3.11 - 32 bajtů dat:
Odpověď od 192.168.3.11: bajty=32 čas < 1ms TTL=127
Odpověď od 192.168.3.11: bajty=32 čas < 1ms TTL=127
Odpověď od 192.168.3.11: bajty=32 čas < 1ms TTL=127
Vypršel časový limit žádosti.
Vypršel časový limit žádosti.
Vypršel časový limit žádosti.
Vypršel časový limit žádosti.
Odpověď od 192.168.3.11: bajty=32 čas < 1ms TTL=127
Odpověď od 192.168.3.11: bajty=32 čas < 1ms TTL=127
Odpověď od 192.168.3.11: bajty=32 čas < 1ms TTL=127

Statistika ping pro 192.168.3.11:
Pakety: Odeslané = 10, Přijaté = 6, Ztracené = 4 (ztráta 40%),
Přibližná doba do přijetí odezvy v milisekundách:
    Minimum = 0ms, Maximum = 0ms, Průměr = 0ms
```

Obr. 5.13: Zachycení příkazu ping při komunikaci mezi zařízeními, která jsou v rozdílných VLAN při odpojení od směrovače.

5.4.3 Zachycení rámce VLAN

Do topologie jsem mezi směrovač a přepínač ASUS 1 zapojil rozbočovač (HUB). Ten pracuje na fyzické vrstvě, jeho úkolem je kopírovat komunikaci z jednoho portu na všechny ostatní. K tomu jsem ještě připojil PC1, abych mohl přes program Wireshark analyzovat síťový provoz. Zachytil jsem pár paketů a podrobil je analýze. Na obrázku 5.14 je zdokumentován zachycený paket. Typ rámce je $_{16}0\times8100$ – značka pro užití 802.1Q rámce a VLAN ID je 3 (VLAN 3).

```
⊟ Ethernet II, Src: Cisco_12:4e:0b (00:14:f2:12:4e:0b), Dst: HonHaiPr_10:cd:b8 (00:22:68:10:cd:b8)
  ⊞ Destination: HonHaiPr_10:cd:b8 (00:22:68:10:cd:b8)
  ⊞ Source: Cisco_12:4e:0b (00:14:f2:12:4e:0b)
    Type: 802.1Q Virtual LAN (0x8100)
⊟ 802.1Q Virtual LAN, PRI: 0, CFI: 0, ID: 3
    000. .... .... .... = Priority: 0
    ...0 .... .... .... = CFI: 0
    .... 0000 0000 0011 = ID: 3
    Type: IP (0x0800)
```

Obr. 5.14: Zachycený rámec VLAN po zapojení HUBu do topologie.

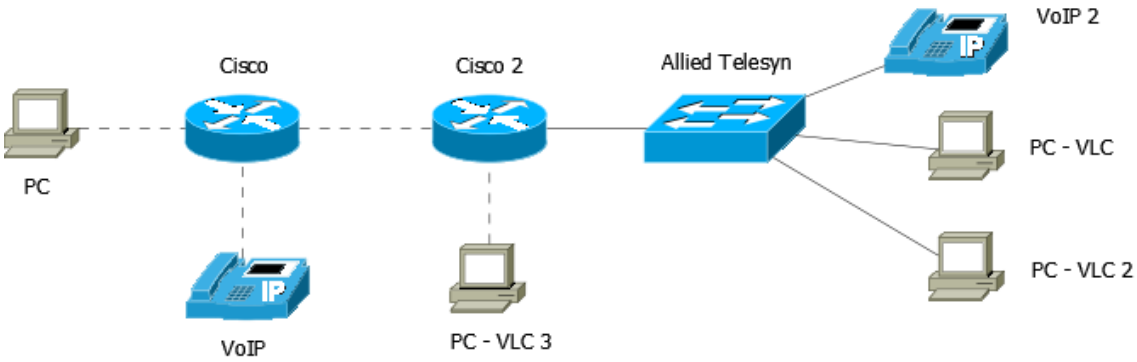
6 NÁVRH EXPERIMENTÁLNÍ SÍTĚ S PODPOROU QOS

Při návrhu této sítě jsem se snažil prozkoumat možnosti podpory QoS jak na linkové, tak i na síťové vrstvě. Z tohoto důvodu jsou zapojeny prvky, které podporují QoS na obou vrstvách – přepínače a směrovače. Jako směrovače jsem volil stejnou řadou, kterou jsem použil v předcházející úloze, tj. Cisco router 1812w. U této řady jsem použil i integrovaný přepínač. Abych prozkoumal možnosti nastavování dalších prvků, zvolil jsem jako přepínač Allied Telesyn – AT-8624T/2M (obr. 6.1).

Obr. 6.1: Přepínač Allied Telesyn – AT-8624T/2M.

6.1 Schéma zapojení a adresace

Experimentální síť byla navržena tak, aby zde provozované služby dostatečně vytěžovaly síťové prvky. Pro zlepšení situace jsem při testování snížil rychlost určitých linek na 10 Mbit/s, tím jsem dosáhl „úzkého“ hrdla, kde síťové prvky řeší podporu QoS jak na linkové, tak na síťové vrstvě. Schéma zapojení naleznete na obrázku 6.2. Adresaci síťových prvků a koncových zařízení uvádím v tabulce 6.1 a 6.2. Jako směrovací protokol jsem zvolil OSPF.



Obr. 6.2: Schéma zapojení pro testování podpory QoS.

Tab. 6.1: Adresace síťových prvků v experimentální sítí.

Síťový prvek	Síťové rozhraní	IP adresa	Síť	Komentář
Cisco	Fa0	192.168.0.1	192.168.0.0/24	
Cisco 2	Fa0	192.168.0.2	192.168.0.0/24	
	Fa1.1 (subint)	192.168.2.1	192.168.2.0/24	VLAN 1
	Fa1.3 (subint)	192.168.3.1	192.168.3.0/24	VLAN 3
	Fa1.4 (subint)	192.168.4.1	192.168.4.0/24	VLAN 4
	Fa1.5 (subint)	192.168.5.1	192.168.5.0/24	VLAN 5
	VLAN 1	192.168.7.1	192.168.7.0/24	
Allied Telesyn	VLAN 1	192.168.2.2	192.168.2.0/24	

Tab. 6.2: Adresace koncových zařízení v experimentální sítí.

Koncový prvek	IP adresa	Komentář
PC VLC	192.168.4.10	VLC server
PC VLC 2	192.168.3.10	VLC server, FTP klient
PC VLC 3	192.168.7.10	VLC server
VoIP	192.168.10.10	SIP klient
VoIP 2	192.168.5.10	SIP klient
PC	192.168.1.11	SIP a FTP server, VLC klient

6.2 Testování podpory QoS na linkové vrstvě

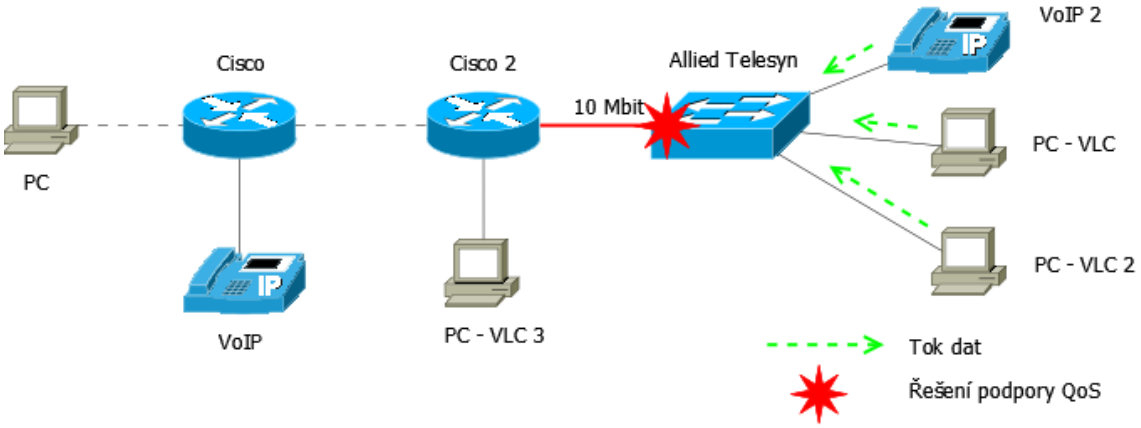
Pro možnost testování jsem jednotlivá koncová zařízení připojil do přepínače Allied Telesyn a přidal do různých VLAN. Nastavil jsem jim různou prioritu na linkové vrstvě. Veškerý tok dat jde do přepínače po 100 Mbit/s linkách a opouští ho po 10 Mbit/s lince – lze zde sledovat různé možnosti podpory QoS na linkové vrstvě (viz obrázek 6.3).

Přepínač Allied Telesyn má širokou škálu možností podpory QoS. Jelikož tento přepínač může pracovat i na 3. vrstvě, může pakety přeposílat i na základě hodnoty DSCP, ale tím se v této úloze budu zabývat až na směrovačích Cisco.

Provoz může rozdělit na základně hodnoty v políčku priorita až na 8 různých front. Podporuje i striktní frontu, která je obsloužena vždycky nejdřív. Z toho důvodů je vhodná především pro hlasový provoz.

6.2.1 Síť bez zajištěné podpory QoS

Ze začátku jsem vypnul veškerou podporu QoS jak na linkové, tak na síťové vrstvě. Poté jsem spustil video streaming z PC – VLC na PC a přenos souboru z počítače

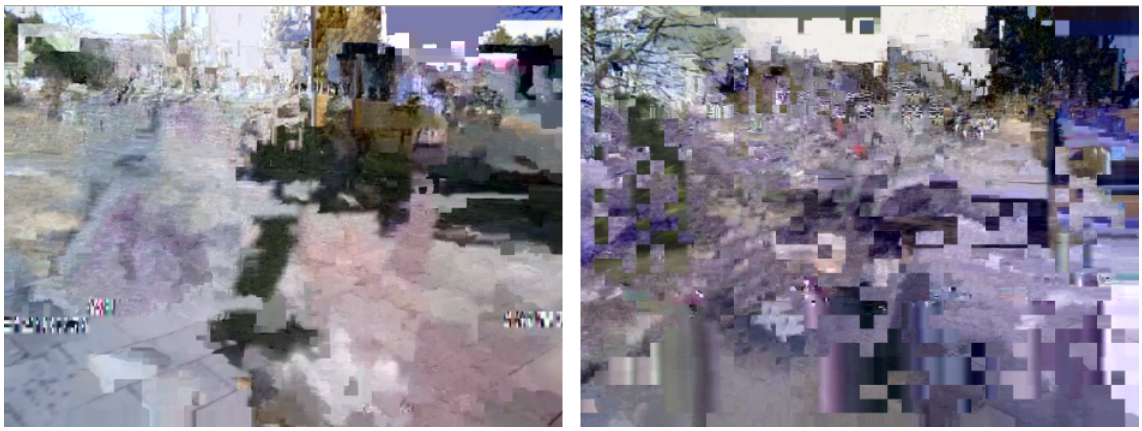


Obr. 6.3: Schéma zapojení pro testování podpory QoS na linkové vrstvě.

PC – FTP (PC – VLC 2) na PC. Vysílané video má datový tok 6,4 Mbit/s.

Zjistil jsem, že FTP přenos je schopen pomocí zpětné vazby TCP protokolu dostatečně omezit tzv. velikost okna. Obraz videa vypadl jen při začátku FTP přenosu, kde velikost okna roste exponenciálně. Ovšem poté již neroste tímto tempem a kolísá kolem takové hodnoty, aby neomezoval ostatní provoz na síti. Z tohoto důvodu jsem pro další testování podpory QoS místo FTP přenosu používal pouze video streaming, který zahltí síť UDP pakety bez zpětné vazby.

Začal jsem z PC – VLC 2 vysílat video na PC (místo FTP přenosu). Vysílal jsem dvě shodná videa – tzn. 12,8 Mbit/s. Na PC jsem pozoroval výpadky obou obrazů (viz obr. 6.4).



Obr. 6.4: Rozpad obrazu bez podpory QoS na linkové vrstvě.

Zdroj signálu zleva: PC – VLC, PC – VLC 2.

Do tohoto provozu jsem ještě volal mezi VoIP telefony. Na hovoru šlo poznat, že byl zpomalený a přerušovaný, občas nešlo rozumět vyslovenému slovu.

Rozdíl pingů mezi koncovými prvky PC a PC - VLC 2 byl v nezatíženém stavu ± 8 ms a v zatíženém stavu ± 230 ms (viz obr. 6.5).

```
Příkaz PING na 192.168.1.11 - 32 bajtů dat:
Odpověď od 192.168.1.11: bajty=32 čas=6ms  TTL=126
Odpověď od 192.168.1.11: bajty=32 čas=4ms  TTL=126
Odpověď od 192.168.1.11: bajty=32 čas=10ms  TTL=126
Odpověď od 192.168.1.11: bajty=32 čas=227ms  TTL=126
Odpověď od 192.168.1.11: bajty=32 čas=221ms  TTL=126
Vypršel časový limit žádosti.
```

Obr. 6.5: Rozdíl pingů v zatíženém a nezatíženém stavu.

6.2.2 Síť se zajištěnou podporou QoS na linkové vrstvě

Pro jednotlivá koncová zařízení připojená do přepínače Allied Telesyn jsem nastavil různou prioritu na linkové vrstvě. Prioritu jsem přiřazoval postupně od nejvyšší priority dle tabulky 6.3.

Tab. 6.3: Přiřazená priorita jednotlivým virtuálním sítím.

Koncový prvek	Priorita	VLAN
VoIP 2	Prioritní fronta	5
PC VLC	5	4
PC VLC 2	3	3

Znovu jsem spustil veškerý provoz na síti. Na přepínači jsem postupně nastavoval podporu QoS. Nejdříve jsem nastavil prioritní frontu pro VLAN 5 (VoIP VLAN) – hovor přestal být trhaný, slovu šlo dobře rozumět. Poté jsem nastavil prioritu pro VLAN 4 (PC VLC). Na PC šlo sledovat, že jedno video bylo přehráváno bez výpadků, zatímco u druhého stále docházelo k rozpadu obrazu. Při nastavení priority pro VLAN 3 nedošlo ke změně. Protože tato VLAN byla přiřazena do fronty s nejnižší prioritou, byly její pakety zahazovány (viz obr.6.6).

Obr. 6.6: Rozpad obrazu s podporou QoS na linkové vrstvě.

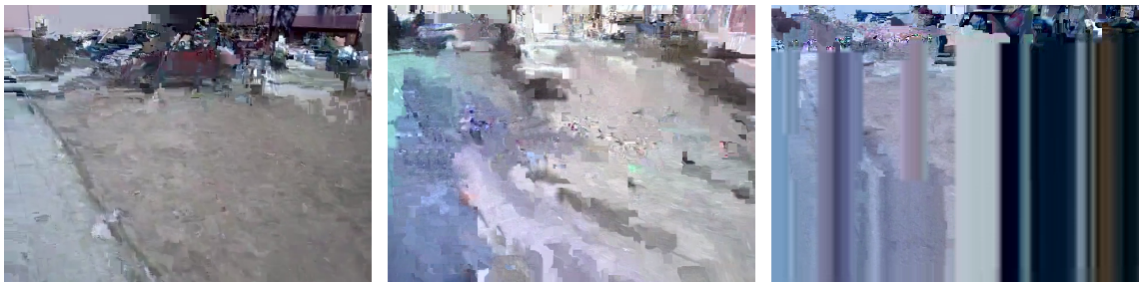
Zdroj signálu zleva: PC – VLC, PC – VLC 2.

6.2.3 Síť se zajištěnou podporou QoS na linkové, ale ne na síťové vrstvě

Při tomto pokusu jsem ještě přidal jeden video streaming, jehož tok šel z PC – VLC 3 rovnou do směrovače. Datový tok přidaného videa byl 900 kbit/s. Na L2 vrstvě byla řešena podpora QoS jako v předchozím případě, avšak směrovač ještě nebyl nastaven pro podporu QoS na vrstvě síťové.

Pro možnost sledování podpory QoS jsem ještě musel omezit linku mezi směrovači Cisco na 10 Mbit/s (obrázek 6.8).

Jelikož z přepínače byl datový tok do směrovače stále ± 10 Mbit/s a ve směrovači přibyl další datový tok 900 kbit/s, došlo střídavě k zahazování paketů od všech provozovaných služeb na síti a tím k nespokojenosti uživatelů. Rozpad obrazu můžete sledovat na obrázku 6.7.



Obr. 6.7: Rozpad obrazu s podporou QoS na linkové vrstvě a bez podpory QoS na síťové vrstvě.

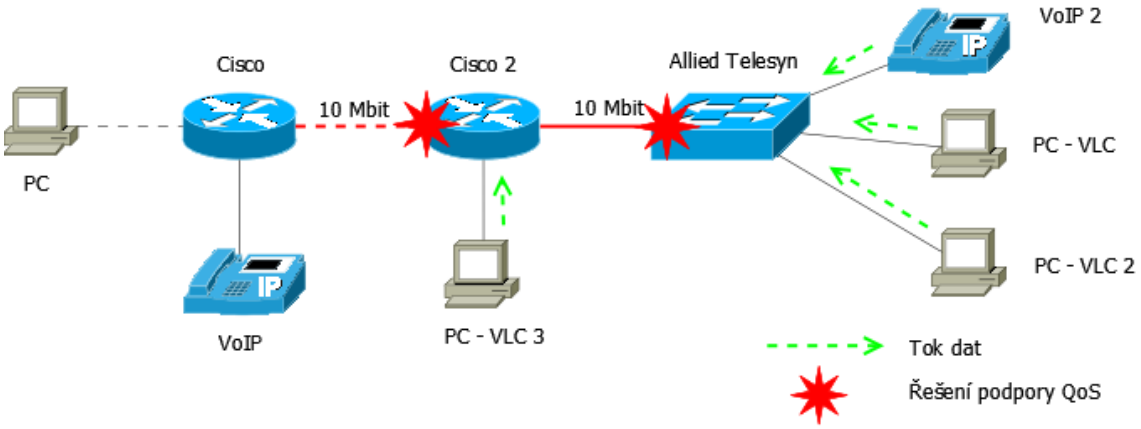
Zdroj signálu zleva: PC – VLC 3, PC – VLC a PC – VLC 2.

6.2.4 Síť se zajištěnou podporou QoS na linkové i síťové vrstvě

Pro zajištění podpory QoS na síťové vrstvě je nezbytné nastavit stejné parametry v celé síti. Veškeré označení probíhá na okrajových směrovačích. Zde máme různé možnosti označkování paketu. V mém případě jsem využil namapování pomocí hodnot políčka priority ve VLAN rámci, shody s porty RTP paketů, adresy zdrojové sítě a skupinové adresy směrovacího protokolu OSPF.

Vnitřní směrovače jsou určeny k rychlému přeposílání paketů. Je to umožněno tím, že již nemění políčko DSCP, ale jen ho přečtou a přiřadí do určené fronty.

Jelikož pakety již máme označkované, stačí jen upravit chování směrovače pro jednotlivé pakety na výstupních rozhraních (tj. mezi směrovači). Pro video streaming jsem rezervoval celkovou šířku pásma 7,3 Mbit/s, tím by měl být zajištěn přenos bez zahazování paketů pro video streaming z PC – VLC a PC - VLC 3 (tj. bez rozpadání obrazu) – fronta CBWFQ. Pro hovorovou službu jsem vyhradil pásmo 100 kbit/s s frontou LLQ (Low Latency Queueing). Tato služba je vždy obsloužena dříve než ostatní. Paketům směrovacího protokolu OSPF jsem přiřadil nejvyšší prioritu – Expedited Forwarding (EF) a přiřadil jim šířku pásma 100 kbit/s (fronta CBWFQ). Tímto rozdělením jsem dodržel pravidlo, že by šířka pásma přidělená pro podporu QoS neměla přesahovat ± 75 % kapacity linky.



Obr. 6.8: Schéma zapojení pro testování podpory QoS.

V případě, že by jedna služba nevyužívala svou kapacitu linky naplno, kdykoliv ji může služba s nižší prioritou využít. (výjma fronty LLQ).

Uplatnil jsem politiku QoS na vstupní a výstupní rozhraní, kde jsem různým provozům přiřadil různou prioritu a šířku pásma, viz tabulka 6.4.

Zdůrazňuji, že provoz z PC – VLC 2 jsem nijak neoznačoval. Z toho vyplývá, že byl automaticky přiřazen do výchozí fronty typu FIFO, nazývané Best Effort.

Tab. 6.4: Přiřazená priorita jednotlivým virtuálním sítím.

Služby	Priorita	Šířka pásma [kbit/s]	Typ fronty
Pakety OSPF	EF	100	CBWFQ
VoIP	AF31	100	LLQ
Video streaming	AF21	7300	CBWFQ

Mnou očekávané chování bylo, že VoIP hovor a dvě videa vysílaná z PC – VLC a PC – VLC 3 budou přenesena bez problémů, stejně jako pakety směrovacího protokolu OSPF.

Správné značení paketů šlo ověřit na směrovači. Ten u jednotlivých tříd vypisoval počet paketů se shodou a bitový tok. Nejmenší počet paketů byl ve třídě OSPF. Příčinou je občasné vyslání Hello paketu (každých 10 sekund). Zatímco ostatní třídy měly počet paketů úměrný datovému toku videové a hlasové službě.

Správnou funkčnost okrajového směrovače lze sledovat také na obrázku 6.9, lze si všimnout pozměněné hodnoty DSCP u provozované video služby. Paket byl zachycen programu Wireshark na PC.

```
⊟ Internet Protocol, Src: 192.168.4.10 (192.168.4.10), Dst: 192.168.1.11 (192.168.1.11)
    Version: 4
    Header length: 20 bytes
  ⊞ Differentiated Services Field: 0x48 (DSCP 0x12: Assured Forwarding 21; ECN: 0x00)
```

Obr. 6.9: Analýza hodnoty DSCP.

Správné chování podpory QoS lze pak sledovat na obrázku 6.10. Dvě videa byla přenesena bez výpadku obrazu, zatímco tok videa, který nebyl přiřazen do prioritní fronty (byl automaticky zahrnut do výchozí fronty), byl zahazován a tudíž docházelo k rozpadu obrazu. Při hovoru nedocházelo k přerušování spojení.

Obr. 6.10: Rozpad obrazu s podporou QoS na linkové i síťově vrstvě.

Zdroj signálu zleva: PC – VLC 3, PC – VLC a PC – VLC 2.

7 LABORATORNÍ ÚLOHY

Součástí zadání bakalářské práce byl kromě vlastního prozkoumání problematiky také návrh a realizace dvou laboratorních úloh pro studenty druhého ročníku do předmětu Architektura sítí. Při vytváření laboratorních úloh jsem vycházel z praktické části bakalářské práce.

První laboratorní úloha – zajištěné spolehlivé sítě na linkové vrstvě se zabývá zamezení výskytu smyček v síti. V teoretické části jsou uvedeny výhody redundantních topologií a funkce různých verzí spanning tree protokolu. Studenti jsou také zasvěceni do virtuálních lokálních sítí a jejich výhod při rozdělení provozu na linkové vrstvě. Jsou zde zmíněna i rizika v případě výskytu smyček – vytížení kapacity linky a procesorů jednotlivých koncových a síťových prvků.

V praktické části úlohy si studenti zapojí danou topologii – mají přístup přímo k hardwaru. Vyzkouší si nastavování různých síťových prvků od různých výrobců v příkazovém řádku i webovém rozhraní. Ověří si v praxi rychlost konvergence protokolů pro zajištění redundantní topologie bez smyček – STP a RSTP. V druhé části vytvářejí virtuální lokální sítě (VLAN). Studenti by si měli uvědomit nutnost výskytu síťového prvku pracujícího na síťové vrstvě pro možnost směrování mezi jednotlivými virtuálními lokálními sítěmi a pochopit, z jakého důvodu zde musí být.

Druhá laboratorní úloha – zajištění kvalitativní podpory služeb (QoS) se zabývá zajištěním kvalitativní podpory služeb na linkové i síťové vrstvě. V teoretické části se studenti seznámí se strukturou ethernetového rámce typu 802.1Q a využití pole Type of Service v IP paketu. Dočtou se o původním využití tohoto pole – IP Precedence, o technologii IntServ a poté o technologii DiffServ, která se v dnešní době používá.

V praktické části úlohy testují tři typy služeb - dostupnost (ping), video streaming a hovor. Ze začátku zahltí síť a pozorují výpadek u hovoru, video streamingu a prodloužení odezvy pingu (případně jeho úplné ztráty). Postupně v síti nastavují síťové prvky pro podporu QoS na linkové a síťové vrstvě. Veškeré nastavení priorit a rozdělení do tříd si ihned ověří na změně kvality probíhajících služeb. Síťové prvky od různých výrobců rovněž nastavují pomoci příkazové řádky a webového rozhraní.

8 ZÁVĚR

Obsahem této práce je rozbor možností pro vybudování spolehlivé sítě s virtuálními lokálními sítěmi s podporou kvalitativních požadavků služeb. Tuto problematiku jsem nejdříve teoreticky nastudoval a poté testoval v praxi.

Pro ověření teoretických poznatků jsem v laboratoři Ústavu telekomunikací sestavil z dostupných síťových prvků experimentální síť, kde jsem prakticky ověřil funkci jednotlivých protokolů. Výsledky jsem následně zdokumentoval v praktické části práce. Z těchto zkušeností usuzuji, že je nejvhodnější použít na linkové vrstvě protokol RSTP pro zajištění redundantní topologie bez smyček s rychlou odezvou na změnu topologie. V případě výskytu přepínačů, které tento novější protokol nepodporují, je možné použít jeho původní verzi STP, ten ovšem od roku 2004 již není součástí standardu 802.1D. Může však dojít k 30-50 sekundovým výpadkům sítě při změně topologie. V případě nepoužití těchto protokolů hrozí celkové zhroucení sítě, dochází k nežádoucímu vytížení linek a procesorů síťových i koncových prvků.

Na linkové vrstvě jsem vytvářel virtuální lokální sítě a zkoumal jejich výhody při aplikování v síti. Dochází k logickému rozdělení sítě a omezení všesměrových zpráv, které jsou v síti ve velkém množství nežádoucí. Pro směrování mezi více virtuálními sítěmi musí být připojen prvek pracující na síťové vrstvě.

Při použití virtuálních lokálních sítí je vhodné použít protokol MSTP pro zachování redundantní topologie bez smyček, který je schopen staticky dělit provoz na linkách.

V další části práce jsem se věnoval možnostem podpory QoS na linkové a síťové vrstvě. Vytvořil jsem další experimentální síť, ve které jsem testoval zahlcení sítě se zabezpečenou podporou QoS i bez ní na různých vrstvách. Z mých výsledků docházím k závěru, že je nezbytné podporovat QoS jak na linkové, tak i na síťové vrstvě. Při aplikaci podpory QoS do datové sítě je důležité nejdříve analyzovat provoz v síti. Na základě této analýzy můžeme rozdělit provoz do tříd a přiřadit jim patřičnou prioritu a šířku pásma.

Ze získaných zkušeností jsem navrhl dvě laboratorní úlohy pro výuku studentů. Cílem první úlohy je seznámit studenty s možnostmi zajištění redundantního zapojení bez vzniku smyček a pochopení problematiky virtuálních lokálních sítí. Cílem druhé úlohy je seznámit studenty s možnostmi zabezpečení podpory QoS jak na linkové, tak i na síťové vrstvě. Studenti dostanou zároveň příležitost seznámit se s nastavením síťových prvků různých výrobců – Cisco, Linksys, Asus a Allied Telesyn.

LITERATURA

[1] BOUŠKA, Petr. *Cisco IOS* [online]. © 2005-2012 [cit. 2011-11-23]. Dostupné z: http://www.samuraj-cz.com/serie/cisco-ios/.

[2] Spanning Tree Protocol. *Understanding Multiple Spanning Tree Protocol (802.1s)* [online]. 17. 4. 2007 [cit. 2011-11-23]. Dostupné z: http://www.cisco.com/en/US/tech/tk389/tk621/technologies_white_paper09186a0080094cfc.shtml.

[3] Spanning Tree Protocol. *Understanding Rapid Spanning Tree Protocol (802.1w).* [online]. 24. 10. 2006 [cit. 2011-11-23]. Dostupné z: http://www.cisco.com/en/US/tech/tk389/tk621/technologies_white_paper09186a0080094cfa.shtml.

[4] HELD, Gilbert. *Quality of service in a Cisco networking environment.* Chichester: John Wiley, 2002, 184 s. ISBN 04-708-4425-6.

[5] HUCABY, David. *Konfigurace směrovačů Cisco.* Vyd. 1. Brno: Computer Press, 2004, 632 s. ISBN 80-7226-951-8.

[6] KEAGY, Scott. *Integrating voice and data networks.* Vyd. 1. Indianapolis: Cisco Press, 2000, 779 s. ISBN 15-787-0196-1.

[7] NOVOTNÝ, Vít. *Architektura sítí* [online]. Brno, 2011 [cit. 2012-05-21]. Dostupné z: https://www.vutbr.cz/www_base/priloha.php?dpid=57265. Skriptum. FEKT VUT v Brně.

[8] PUŽMANOVÁ, Rita. *TCP/IP v kostce.* 2. upr. a rozš. vyd. České Budějovice: Kopp, 2009, 619 s. ISBN 978-80-7232-388-3.

[9] SZIGETI, Tim a Christina HATTINGH. *End-to-end QoS network design.* 2. upr. a rozš. vyd. Indianapolis: Kopp, 2009, 619 s. ISBN 15-870-5176-1.

[10] TRULOVE, James a Christina HATTINGH. *Sítě LAN: hardware, instalace a zapojení.* 1. vyd. Praha: Grada, 2009, 384 s. ISBN 978-80-247-2098-2.

[11] Voip Think. *Codec Summary table* [online]. [cit. 2012-05-21]. Dostupné z: http://www.en.voipforo.com/codec/codecs.php.

[12] WANG, Zheng. *Internet QoS: architectures and mechanisms for quality of service.* San Francisco: Morgan Kaufmann, c2001, xv, 239 s. ISBN 15-586-0608-4.

SEZNAM SYMBOLŮ, VELIČIN A ZKRATEK

ACK	Acknowledgement
ACL	Access List
AF	Assured Forwarding
BA	Behaviour Aggregate
BE	Best Effort
BGP	Border Gateway Protocol
BPDU	Bridge Protocol Data Unit
CBWFQ	Class Based Weighted Fair Queueing
DiffServ	Differentiated Services
DSCP	Differentiated Service Code Point
EAP	Extensible Authentication Protocol
EF	Expedited Forwarding
EGP	Exterior Gateway Protocol
FCS	Frame Check Sequence
FIFO	First-In, First-Out
FTP	File Transfer Protocol
HTTP	Hyper Text Transfer Protocol
IGP	Interior Gateway Protocol
IntServ	Integrated Services
IP	Internet Protocol
ISL	Inter-Switch Link
ISP	Internet Service Provider
ITU	International Telecommunication Union
LLQ	Low Latency Queueing

MAC	Media Access Control
MDI	Medium Dependent Interface
MDIX	Medium Dependent Interface Crossover
MSTP	Multiple Spanning Tree Protocol
OAM	Operations, Administration and Management
OSPF	Open Shortest Path First
PHB	Per Hop Behaviour
PoE	Power over Ethernet
QoS	Quality of Service
RED	Random Early Detection
RSTP	Rapid Spanning Tree Protocol
RSVP	Resource reSerVation Protocol
RTP	Real-Time Transport Protocol
SIP	Session Initiation Protocol
STP	Spanning tree protocol
STP	Shielded Twisted Pair
TCP	Transsmission Control Protocol
ToS	Type of Service
UDP	User Datagram Protocol
UPS	Uninterruptible Power Supply)
UTP	Unshielded Twisted Pair
VLAN	Virtual local area network
VoIP	Voice over IP
VTP	VLAN Trunking Protocol
WFQ	Weighted Fair Queueing
WRED	Weighted Random Early Detection