Možnosti nastavení kvality služeb na přepínačích a směrovačích Cisco

Bc. Michal Pecha

Diplomová práce
2015

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2014/2015

ZADÁNÍ DIPLOMOVÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Bc. Michal Pecha**
Osobní číslo:	**A13448**
Studijní program:	**N3902 Inženýrská informatika**
Studijní obor:	**Počítačové a komunikační systémy**
Forma studia:	**prezenční**
Téma práce:	**Možnosti nastavení kvality služeb na přepínačích a směrovačích Cisco**
Téma anglicky:	**The Possibilities of Setting Service Quality on Cisco Routers and Switches**

Zásady pro vypracování:

1. **Popište vlastnosti, funkci a využití kvality služeb (QoS).**
2. **Popište algoritmy řazení do front a možnosti kontroly zahlcení sítě.**
3. **Popište základní konfiguraci VoIP.**
4. **Na dostupných zařízeních otestujte různá nastavení QoS.**
5. **Proveďte zhodnocení dosažených výsledků.**

Rozsah diplomové práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. **WALLACE, Kevin. Cisco VoIP: autorizovaný výukový průvodce. Vyd. 1. Brno: Computer Press, 2009, 527 s. ISBN 978-80-251-2228-0.**
2. **HUCABY, Dave, Steve MCQUERRY a Andrew WHITAKER. Cisco router configuration handbook. 2nd ed. Indianapolis, IN: Cisco Press, c2010, xxii, 641 s. ISBN 978-1-58714-116-4.**
3. **MCQUERRY, Steve, David JANSEN a Dave HUCABY. Cisco LAN switching configuration handbook. 2nd ed. Indianapolis, Ind.: Cisco Press, c2009, xx, 333 s. ISBN 978-1-58705-610-9.**
4. **SOSINSKY, Barrie A. Mistrovství - počítačové sítě: [vše, co potřebujete vědět o správě sítí]. Vyd. 1. Brno: Computer Press, 2010, 840 s. ISBN 978-80-251-3363-7.**
5. **SZIGETI, Tim, Christina HATTINGH, Robert BARTON a Kenneth BRILEY. End-to-End QoS Network Design: Quality of Service for Rich-Media & Cloud Networks. 2nd edition. Indianapolis, Ind: Cisco Press, 2013, 1040 s. ISBN 15-871-4369-0.**

Vedoucí diplomové práce: **Ing. Jiří Korbel, Ph.D.**
Ústav počítačových a komunikačních systémů

Datum zadání diplomové práce: **12. ledna 2015**

Termín odevzdání diplomové práce: **15. května 2015**

Ve Zlíně dne 6. února 2015

L.S.

doc. Mgr. Milan Adámek, Ph.D.
děkan

Ing. Miroslav Matýsek, Ph.D.
ředitel ústavu

Prohlašuji, že

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

Prohlašuji,

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

Ve Zlíně .....

podpis autora

ABSTRAKT

Diplomová práce se zabývá problematikou kvality řízení služeb na směrovačích a přepínačích společnosti Cisco. Celá práce se skládá ze dvou částí. V teoretické části je čtenář uveden do problematiky kvality řízení služeb a IP telefonie. Je zde řešen vliv kvality služeb na ip telefonii a jaké jsou možnosti nastavení. Dále jsou řešeny možnosti řazení do fronty na zařízeních Cisco a principy hodnocení IP hovorů.V projektové části jsou pak otestovány různé možnosti nastavení kvality služeb ve dvou typech zapojení.

Klíčová slova: Kvalita řízení služeb, voice over ip, QoS, VoIP, Cisco, směrovač, přepínač

ABSTRACT

This diploma thesis is consider of problems quality of service and voice over IP on Cisco routers and switches. The whole paper consists of two parts. The theoretical part contains informations about quality of service and voice over IP. There is solved affect the quality of service for IP telephony, and what are the options configuration. Further possibilities are solved queuing for Cisco devices and evaluation principles voice over IP. In the project part are tested differend ways to configure of quality of service on two types of schemas.

Keywords: Quality of Service, Voice over IP, QoS, VoIP, Cisco, router, switch

Mé poděkování patří vedoucímu práce panu Ing. Jiřímu Korbelovi, Ph.D. za ochotu, se kterou mi poskytl cenné rady k diplomové práci a podporu.

Dále bych chtěl poděkovat mojí rodině, která mě podporovala během celého studia a poskytla mi kvalitní zázemí pro studium i psaní této práce.

Moto:

„Buď slušný k lidem, stoupáš-li nahoru. Mohl bys je potkat, až půjdeš dolů.“
Jimmy Durante

OBSAH

ÚVOD

V dnešní době jsou počítačové sítě jednou ze složek kritické infrastruktury a na jejich správném fungování závisí většina firem, bank, institucí. Na internetu se obsluhuje internetové bankovnictví, komunikuje s přáteli, telefonuje, vyřizují se objednávky a zkrátka téměř vše co lze zdigitalizovat je na internetu možné najít. S tím ruku v ruce jde také jeho bezpečnost a kvalita poskytovaných služeb. A právě na kvalitu služeb je tato práce zaměřena.

V úvodu práce jsou popsány vlastnosti QoS (Quality of Service), její funkce a též pro praktické využití v síti. Dále je popisována kvalita služeb ve vztahu k IP telefonii, která se postupem času začíná více a více prosazovat. Svědčí o tom také fakt, že s příchodem mobilních sítí 4. generace se čím dál více uvažuje o přenesení hlasových služeb do datového prostoru a využívalo by se i zde IP telefonie. S tím jde ruku v ruce také fakt, že se neustále zvyšuje datový provoz na síti a tím pádem je zde dobré nastavení kvality služeb neocenitelné.

Hlavní část je zaměřena na konkrétní zařízení společnosti Cisco, na kterých jsou zkoumány jejich algoritmy pro automatické řízení služeb jak na směrovačích tak také na přepínačích fungujících na 2. a 3. vrstvě modelu OSI. Vyústěním práce je otestování různých nastaveních na směrovačích a přepínačích podle možností daných zařízeních.

I. TEORETICKÁ ČÁST

1 QUALITY OF SERVICE

Quality of Service (QoS) v počítačových sítích popisuje širokou oblast přístupů a nástrojů pro sítě s přepínáním paketů. Každého z nás jistě napadne, že se jedná o službu, která upřednostňuje jedny pakety ve frontě před druhými a dosahuje tak lepšího výsledku. Tohle je ovšem jen jedna její část. QoS má i jiné vlastnosti, kterými jsou: komprese, politika zahazování paketů, profilování, řízení, příznaky a jiné.

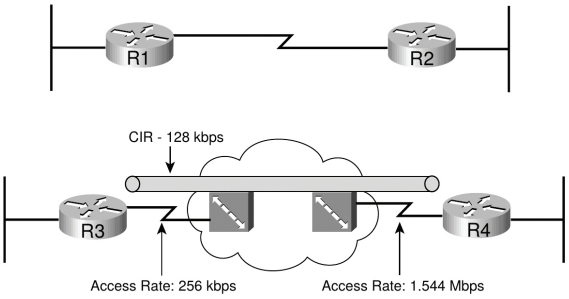
Na začátek je vhodné se podívat na 4 nejdůležitější vlastnosti, kvůli kterým bylo řízení kvality služeb (QoS) zavedeno a čím jsou charakteristické. Jsou jimi:

- Bandwidth (šířka pásma)
- Delay (zpoždění)
- Jitter (rozptyl zpoždění)
- Packet loss (ztrátovost paketů)

Použití těchto nástrojů QoS může zlepšit vlastnosti přenosu některých služeb a naopak, u některých služeb může dojít k jejich zhoršení. Je důležité se dobře zamyslet nad tím, které služby zvýhodníme a jaký vliv bude mít tento zásah na ostatní provoz a nakolik je to ovlivní. [6] Proto bude dobré se s jednotlivými vlastnostmi blíže seznámit.

1.1 Bandwidth - šířka pásma

Šířka pásma je v počítačové terminologii definována číslem, které udává, kolik bitů za sekundu je možné přenést zvoleným přenosovým kanálem. V některých případech odpovídá šířka pásma rychlosti linky nebo hodnotě clock rate na zvoleném rozhraní. Příkladem může být sériové propojení mezi směrovači. V ostatních případech je šířka pásma menší než je rychlost přenosového kanálu. (Obr. 1.1)



Obr. 1.1 Propojení Point to Point [6]

V síti, kde je projení mezi směrovači R1 a R2 řešeno přímou linkou, je šířka pásma rovna fyzické rychlosti linky nebo hodnotě clock rate. Například, máme-li linku s rychlostí 64kbps, můžeme očekávat odesílací rychlost 64kbps. Na přijímací straně můžeme očekávat tu samou rychlost. Také, ale nemůžeme očekávat, že přeneseme více bitů rychleji, než nám umožňuje nastavená hodnota clock rate. Opět to platí v obou směrech.[6]

U sítě, kterou vidíme na obr. 1.1 mezi směrovači R3 a R4 je situace mnohem komplikovanější. Takzvané úzké hrdlo je zde CIR (Committed information rate) - což je šířka pásma, kterou je schopný poskytovatel připojení garantovat mezi DTE (data terminal equipent) a každým koncovým VC (virtual circuit). Tuto logiku zajišťuje 8. vrstva referenčního modelu OSI.
Šířka pásma u více přístupové sítě není jednoduchá záležitost. Vidíme to na první pohled z obrázku. Směrovač R3 přistupuje do sítě s rychlostí 256kpbs, kdežto směrovač R4 je připojen optickou linkou T1 s rychlostí 1,544Mbps. Pro zdárný průběh přenosu pracujeme v tomto případě s protokolem Frame Relay. Když bude směrovač R3 odesílat data, musí je odesílat rychlostí, kterou je připojen, jinak by funkce 1. vrstvy přestaly fungovat. Stejně tak směrovač R4 musí odesílat data rychlostí T1. Jednou z velkých výhod Frame Relay je, že „dostanete něco za nic“ - to v praxi znamená, že si zaplatíte nějakou hodnotu CIR, ale dostanete více než máte zaplaceno. Ve skutečnosti designeři počítačových sítí předpokládají, že v průměru je k dispozici jeden a půl až dvojnásobek CIR, pro každý VC. Pokud by ovšem směrovače R3 a R4 odesílaly příliš mnoho dat a přepínače poskytovatele měly plné fronty, rámce jsou zahozeny a musí být odeslány znovu.[6]

1.1.1 Vliv QoS na šířku pásma

Nejlepší QoS nástroj pro nastavení šířky pásma je mít větší šířku pásma, což ale neřeší problém. Ve skutečnosti to může způsobit konvergentním sítím (sítě s hlasem, videm a daty) skrytý problém se zpožděním, a proto je lepší využít nástrojů QoS. Pokud je ovšem možné použít větší šířku pásma, tak to může pomoci se zlepšením kvality spojení. [6]

komprese Základem komprese je snížení počtu bitů, které je potřeba přenášet. K dispozici je velmi zjednodušený modelový příklad, kdy na vstupu je 80kpbs linka a na výstupu 64kpbs linka. V případě, že by směrovač nevyužíval komprese, bude výstupní linka plně vytížena a pro odesílání bude potřebovat celých 64kps a fronta bude zcela

zaplněna. Využije-li se však na směrovači komprese, tak bude stačit na odesílání dat jen 40kpbs.[6]

řízení přijetí hovoru (CAC) CAC je nástroj, který určuje, zda budou do sítě připojeny nové hlasové a video hovory. Přístup může být povolován na základě mnoha faktorů. Například, v síti může být povoleno použití pouze tří konkurenčních VoIP kodeků G.729A. CAC kontroluje každý nový hovor, a pokud již v síti existují 3 hovory se zvoleným kodekem, je hovor odmítnut. Důvodem nastavení takového CAC je může být, že pokud by se do sítě připojil další hovor se stejným kodekem, mohlo by dojít k degradaci kvality hovoru a takové chování je nežádoucí. Pokud je hovor odmítnut, tak je přesměrován na jinou trasu podle VoIP dial plánu, pro danou instanci.[6]

Fronta Frontové nástroje můžou mít vliv na šířku pásma a to tak, že se rozhoduje podle toho, jaký typ provozu přijde na vstup. Základem je vytvoření mnoha front a pakety jsou do front řazeny podle řídícího frontového algoritmu (queue-servicing algorithm). Tento algoritmus může obsahovat vlastnost, která garantuje minimální šířku pásma pro jednotlivé fronty nebo frontu. [6]

1.2 Delay - zpoždění

Zpoždění by se dalo definovat jako doba mezi prvním odesláním paketu a jeho přijetí v místě určení. Zpoždění v počítačové síti vzniká prakticky na každém zařízení, přes které je paket posílán a řada QoS nástrojů s tím pracuje. Na některých zařízeních se vytvoří menší zpoždění a na jiném významnější, ale s tím nic neuděláme. Celkové zpoždění se skládá z následujících typů zpoždění: [6]

- Serializované zpoždění (Serialization Delay) - Jedná se o fixní zpoždění, které je definováno jako čas, který je potřebný pro zakódování bitů paketu na fyzickém rozhraní. Pokud je linka rychlá, bity budou zakódovány rychleji, pokud je ovšem linka pomalá, bude proces trvat déle. Vliv na to má také délka paketu. Kratší paket bude rychleji zpracovaný než dlouhý paket.
  Pro výpočet serializovaného zpoždění je k dispozici vzorec:

$$\frac{\#\text{bity k odeslání}}{\text{rychlost linky}}$$

- Propagační zpoždění (Propagation Delay) - Je definován jako čas, který je potřebný k přenesení jednoho bitu z jednoho konce bitu na druhý. Pokud se signál šíří optickým nebo metalickým vedením, není fyzikálně možné okamžitě dostat signál z jednoho konce kabelu na druhý. Toto zpoždění je tedy ovlivněno pouze

délkou linky.
K výpočtu se používá následující vzorec:

$$\frac{\text{Délka linky (m)}}{2,1 * 10^8\ m/s}$$

Hodnota $2,1 * 10^8$ se používá pro přesnější hodnotu zpoždění, protože to lépe odpovídá reálné hodnotě, že obecně udávaná rychlost světla ve vákuu $3 * 10^8$.

- Zpoždění ve frontě (Queuing Delay) - Toto zpoždění vzniká čekáním ve frontě, než mohou být pakety odeslány. Je tedy definováno jako čas, který paket stráví ve frontě.

- Zpoždění směrování (Forwarding Delay) - Je to zpoždění, které vzniká ve směrovači nebo přepínači. Nejedná se však o celou dobu, po kterou je paket v zařízení, ale pouze o čas, který potřebuje na to, aby z analyzoval paket a určil na které rozhraní jej poslat.

- Zpoždění tvarování (Shaping Delay) - Zpoždění tohoto typu (pokud je nastaveno) je způsobeno tím, že pokud cesta v síti nebyla natrasována, tak jsou pomaleji obslouženy fronty. Důvodem k tomuto nastavení je, že se zabrání zahazování paketů, ovšem za cenu pomalejšího odesílání paketů.

- Zpoždění sítě (Network Delay) - je způsobeno prvky sítě, ke které jsme připojení, například k operátorovi.

1.2.1 Vliv QoS na zpoždění

Tak jako u šířky pásma, i zde platí, že nejlepším nástrojem na pro vyřešení problémů se zpožděním je mít co největší šířku pásma. Právě šířka pásma má největší vliv na snížení serializovaného zpoždění. To z toho důvodu, že pakety jsou rychleji odesílány a tím se i sníží zpoždění ve frontách.
Protože větší šířka pásma nevyřeší všechny problémy spojené se zpožděním, máme tu také QoS nástroje, které nám je pomáhají vyřešit.

Fronta - plánování Jeden z nejoblíbenějších nástrojů, pro řešení problémů se zpožděním. Rozhodování probíhá i jiným způsobem než je pouze čas doručení. Jde o to, že se nepoužívá jedna FIFO fronta, ale jiné frontové nástroje vytvoří více front a pakety jsou umísťovány do těchto různých front a jsou i odlišným způsobem obsluhovány. To umožňuje dříve odeslat pakety služeb, které jsou více náchylné na zpoždění a pakety

služeb, u kterých to tolik nevadí, tak je pozdržet. Tato technika sice nesníží zpoždění u všech paketů, jako například je tomu u zvětšení šířky pásma, ale má nižší cenu.[6]

Fragmentace linky a prokládání Funkce tohoto nástroje je užitečná pro snížení zpoždění serializace paketů na linku, která závisí na rychlosti linky a velikosti paketů. Pokud se směrovač rozhodne odeslat paket a odešle první bit, tak pokračuje do té doby, doku jej neodešle celý. To je nepříjemnost pro paket, který je citlivý na zpoždění a musí čekat, zvláště tehdy, odesílá-li se paket s velkou délkou. Díky tomuto nástroji, je možné první dlouhý paket přerušit, odeslat druhý paket, citlivý na zpoždění, a po té pokračovat v odesílání prvního paketu, který bude tímto mechanismem rozdělen na části, v tomto příkladě na dvě.[6]

Komprese Komprese pracuje s paketem nebo jeho hlavičkou a zkomprimuje data na menší velikost. V příkladu je 1500 bajtový paket, který bude zkomprimován na velikost 750 bajtů. To znamená, že se o polovinu sníží čas k serializaci, než by k tomu bylo v případě nezkomprimovaného paketu.
Komprese tedy sníží zpoždění u serializace, protože je potřeba odeslat menší počet bitů. Může mít však i opačný efekt, a to taký, že se zvýší zpoždění vlivem komprese a dekomprese paketů.[6]

Tvarování trasy Ačkoliv má tvarování trasy efekt většího zpoždění, jeho přínos je ve snížení ztrátovosti paketů.
Je zde zmíněn z důvodu jeho negativního vlivu na zpoždění.[6]

1.3 Jitter - rozptyl zpoždění

V síti s paketovým provozem a s proměnnými složkami zpoždění vždy dojde k rozptylu zpoždění. Otázkou je, zda to má vliv na degradaci služby, protože předpokládají nějaký rozptyl v doručení. Jsou ale služby, jako je například přenos hlasu, které vyžadují, aby byly přenášeny konzistentním a jednotným způsobem, například každých 20ms. Pakety by také měly dorazit do cíle se stejnými rozestupy.
Rozptyl zpoždění je tedy definován jako změna v doručení paketů. To znamená, jaká je změna v prodlení při doručování po síti. [6]

1.4 Packet Loss - ztrátovost paketů

Posledním z charakteristických vlastností QoS je ztrátovost paketů. Směrovače zahazují, ztrácí nebo ničí pakety z různých důvodů a techniky QoS s tím nemohou nic udělat. Mohou však svými nástroji přispět k jejich minimalizaci.

V dnešních sítích je počet paketů zahozených v důsledku bitových chyb velmi malý, je to přibližně jeden z miliardy přenesených bitů (hodnota bit error rate [BER] je 10^{-9} nebo lepší). Mnohem více chyb je z důvodu přeplněných zásobníků a front.[6]

1.4.1 Vliv QoS na ztrátovost paketů

Tak jako v předešlých doporučeních, i zde je jedním z možných řešení dostatečná šířka pásma. Což má vliv na velikost fronty, větší šířka pásma umožní rychlejší obsloužení fronty.

Fronta Aby se předcházelo přeplnění front, je dobré mít dostatečnou velikost fronty. Krátká fronta může být velmi rychle naplněna.

Random Early Detection (RED) RED využívá vlastnosti protokolu TCP. Touto vlastností je windowing (okno), což znamená, jaké množství TCP dat může uživatel odeslat bez toho aniž by obdržel potvrzení. Hodnota TCP okna pro každé odlišné TCP spojení se zvětšuje nebo zmenšuje na základě mnoha faktorů. RED této vlastnosti využívá tak, že velikost okna upravuje tak, aby nedocházelo k přeplnění fronty a celkové množství paketů poslaných do sítě byl menší. Když fronty nejsou naplněny, nemusí RED upozorňovat odesílatele, aby zpomalili, protože to není nutné. [6]

2 QUALITY OF SERVICE A VOICE OVER IP

Aplikace v reálném čase, například hlasové aplikace, mají různé vlastnosti a požadavky od tradičních datových aplikací. Vzhledem k tomu, že se jedná o aplikace v reálném čase, hlasové aplikace tolerují minimální odchylku velikosti zpoždění ovlivňující doručování jejich hlasových paketů. Hlasový přenos také není tolerantní vůči ztrátě paketů a jitteru, přičemž oba tyto faktory nepřijatelným způsobem degradují kvalitu hlasového přenosu doručovaného koncovému uživateli. Aby bylo možné efektivně přenášet hlasový přenos přes protokol IP, jsou nutné mechanismy zajišťující spolehlivé doručování hlasových paketů. Funkce Cisco IOS QoS kolektivně tyto techniky zahrnují, což umožňuje zajišťovat prioritní služby odpovídající striktním požadavkům na doručování hlasových paketů.

Komponenty QoS pro Cisco Undefied Communications jsou poskytovány prostřednictvím správy přenosu v síti IP, front a možností tvarování v rámci infrastruktury sítě IP společnosti Cisco.

Následuje několik funkcí Cisco IOS umožňujících plnit požadavky komplexního mechanismu QoS a rozlišen služeb pro doručování hlasových paketů:

- Komprese hlavičky - používá se v souvislosti s protokolem RTP (Real-time Transport Protocol) a TCP (Transmission Control Protocol). Slouží ke kompresi objemově velkých hlaviček protokolu RTP nebo TCP. Výsledkem je využití menší dostupné šířky pásma pro hlasový přenos. Výsledkem je odpovídající snížení zpoždění.

- FRTS (Frame Relay Traffic Shaping) - zpozdí nadměrný přenos dat pomocí vyrovnávací paměti nebo mechanismu fronty k pozdržení paketů a tvarování toku v případě, že je rychlost zdrojových dat vyšší než očekávaná.

- FRF.12 (a vyšší) - zajišťuje předvídatelnost hlasového přenosu. Cílem je zajištění lepší propustnosti nízkorychlostních linek Frame Relay prokládáním hlasového přenosu citlivého na zpoždění na jednom virtuálním okruhu (VC, virtual circuit) fragmenty dlouhého rámce na jiném okruhu VC s využitím stejného rozhraní.

- Funkce fallback sítě JTS - zajišťuje mechanismus pro monitorování zahlcení v síti IP a v případě zahlcení sítě buď přesměruje volání do sítě JTS, nebo volání odmítne.

- Priorita IP RTP a Frame Relay IP RTP - zajišťuje striktní schéma využívání fronty na základě priorit umožňující data citlivá na zpoždění (například hlasová

data) vyřadit z fronty a odeslat před ostatními pakety standardně vyřazováním z ostatních front. Tyto funkce jsou užitečné zejména u pomalých linek WAN, včetně Frame Relay, Multilink PPP [MLP] a T1 ATM. Funguje s WFQ (weighted fair queuing) a CBWFQ (Class-Based WFQ)

- CoS (Class of Service) mezi IP a ATM - zahrnuje sadu funkcí, které mapují charakteristiky mezi sítí IP a režimem ATM. Nabízí diferenciální třídy služeb v rámci celé sítě WAN, nikoli pouze ve směrované části. Nabízí pro aplikace důležité pro chod firmy výjimečné služby v době vysokého využití sítě a jejího zahlcení.

- LLQ (Low Latency Queuing) - zajišťuje striktní využívání fronty na základě priority na virtuálních okruzích ATM VC a sériových rozhraních. Tato funkce umožňuje nakonfigurovat stav priority pro třídu v rámci CBWFQ a není limitována na čísla portů UDP (User Datagram Protocol), jako Priorita IP RTP.

- MLP - umožňuje multilink zapouzdření a fragmentaci velkých paketů, aby byly dostatečně malé na to, aby byly uspokojeny požadavky na zpoždění v rámci přenosu v reálném čase. MLP také zajišťuje speciální přenosovou frontu pro menší pakety citlivé na zpoždění, přičemž je umožňuje odeslat dříve než jiné toky.

- Protokol RSVP (Resource Reservation Protocol) - podporuje rezervování prostředků v rámci sítě IP, přičemž umožňuje koncovým systémům požadovat ze sítě záruky QoS. Pro sítě podporující VoIP může protokol RSVP (ve spojení s funkcemi zajišťujícími využívání front, tvarování přenosu dat a signalizace hlasových hovorů) zajišťovat řízení CAC (call admission control) pro přenos hlasu. Společnost Cisco také zajišťuje podporu protokolu RSVP pro LLQ a Frame Relay.[1]

2.1 Přínos QoS pro VoIP

Aby bylo zajištěno, že VoIP bude přijatelnou náhradou za standardní telefonní služby JTS, musí zákazníci přijímat stejně konzistentně vysokou kvalitu hlasového přenosu, jakou mají k dispozici v případě základních telefonních služeb. Stejně tak jako jiné aplikace v reálném čase je síť VoIP extrémně citlivá na problémy související s šířkou pásma a zpožděním. Aby bylo zajištěno, že přenos VoIP bude pro příjemce srozumitelný, nesmí být hlasové pakety zahozeny, nadměrně zpožděny ani ovlivněny proměnlivým zpožděním (jitter). Aby bylo nasazení sítě VoIP úspěšné, musí síť zajišťovat přijatelnou úroveň kvality hlasu. To znamená, že musí být splněny požadavky na přenos dat v síti VoIP z hlediska problémů týkajících se šířky pásma, latence a jitteru.

QoS nabízí schopnost sítě zajišťovat vylepšené služby pro vybraný síťový přenos přes nejrůznější podpůrné technologie, včetně Frame Relay, ATM, sítí Ethernet a 802.1, SONET a sítí se směrováním na IP. VoIP zaručuje přenos hlasu ve vysoké kvalitě pouze v případě, že mají pakety signalizačního a zvukového kanálu přednost před jinými druhy síťového přenosu.

Funkce QoS konkrétně zajišťují vylepšené a lépe předvídatelné síťové služby implementací následujících služeb:

- Podpora zaručené šířky pásma - návrh sítě takovým způsobem, aby byla vždy k dispozici nezbytná šířka pásma pro podporu hlasového a datového přenosu.
- Zlepšení charakteristiky ztrát - návrh například sítě Frame Relay, aby možnost zahození rámce (DE, discard eligibility) nebyla faktorem pro rámce obsahující hlas, aby byla zachována úroveň hlasu pod úrovní CIR (committed information rate).
- Zabránění a správa zahlcení sítě - zajištění, aby infrastruktura sítí LAN a WAN podporovala objem přenášených dat a objem dat pro hlasová volání
- Tvarování síťového přenosu - používání nástrojů pro tvarování přenosu společnosti Cisco k zajištění bezproblémového a konzistentního doručování rámců do sítě WAN.
- Nastavení priorit přenosu v rámci sítě - označení hlasového přenosu jako prioritního a zařazování hlasových dat nejprve do fronty. [1]

2.2 Požadavky a zabezpečení QoS

Aby byly dodrženy specifické požadavky sítě s QoS na kvalitní přenos hlasu a videa, byla stanovena základní kritéria, kdy při jejich dodržení se předejde problémů s kvalitou hlasu a videa. Těmito základními požadavky jsou:

- Celkové zpoždění: 150ms nebo méně
- Rozptyl zpoždění (jitter): 30ms nebo méně
- Ztrátovost paketů: 1 procento nebo méně

Hlavním cílem je implementace QoS takovým způsobem, aby byl k dispozici mnohem více konzistentní a stabilní přenosový mechanismus pro přenos hlasových paketů.

Zatím co technika best-effort může velmi dobře pracovat s daty, hlasový přenos potřebuje mnohem citlivější přístup pro optimální funkčnost.

Funkce QoS se skládají z těchto tří stupňů:

- Klasifikace přenosu
- Značkování přenosu
- Řazení do front

Klasifikace přenosu je proces, při kterém dochází k identifikaci paketů, které jsou citlivé na čas přenosu. Identifikační přenos musí být proveden jako první, protože zařízení musí být jednoznačně schopná identifikovat takový přenos. Vytvořením VLAN pro hlas tento proces zjednodušuje, protože lze předpokládat, že libovolný paket ve VLAN může být označen jako hlasový.

Značkování přenosu je proces, při kterém dochází k označení kritických paketů, takže zbývající části sítě jsou schopny je jednoduchým způsobem poznat a dát jim přednost před ostatním přenosem. Telefony Cisco tyto pakety označují pomocí hodnoty CoS (Class of Service). CoS je pole v hlavičce ethernetového rámce na 2 vrstvě, které je přiřazena hodnota třídy 0-7. Vyšší hodnotě CoS je přiřazena vyšší priorita. Ve výchozím nastavení, je hodnota CoS nastavena na 5. Pokud data nejsou označena hodnotou CoS, je jim automaticky přiřazena hodnota 0. Tato hodnota je směrovači využívána pro řazení do front.
Telefony Cisco mohou také IP pakety označovat identifikátorem ToS (Type of Service). Význam ToS je podobný jako u CoS, ale je využíván k identifikaci zařízeními pracujících na 3 vrstvě, jako jsou L3 přepínače a směrovače.

Řazení do front je proces řazení některých typů přenosu přes LAN nebo WAN rozhraní. K dispozici je několik různých technik řazení do fronty. V textu jim bude věnována pozornost.[7]

2.3 Typy QoS

Jak se potřeby aplikací pracujících na síti vyvíjely a potřebovaly různé úrovně nastavení QoS, tak dnes je možné v síti implementovat tři typy nastavení QoS:

- Best-Effort
- Integrated Services (IntServ)

- Differentiated Services (DivServ)

2.3.1 Best-Effort

Důvod, proč je uvedena technika Best-Effort je ta, že je to velmi často využíváno jako výchozí nastavení. Na druhou stranu, Best-Effort neklade žádné nároky na implementaci koncových zařízení. Nepoužívá žádný z QoS mechanismů, ale pracuje na základě jednoduché logiky, kdy ten kdo dříve přijde, tak je dříve obsloužen. To samozřejmě neřeší požadavky na QoS v dnešních sítích.

2.3.2 Integrated Services (IntServ)

Model IntServ pracuje na principu rezervace. Například, pokud chce uživatel provést volání pomocí VoIP s datovým tokem 80kpbs přes datovou síť, tak se podle modelu IntServ rezervuje na každém síťovém zařízení, mezi dvěma koncovými stanicemi, 80kpbs šířku pásma. K tomuto procesu využívá protokol RSVP (Resource Reseration Protocol). Po dobu trvání hovoru, nemůže využívat vyhrazenou šířku pásma, v tomto případě 80kpbs, nikdo jiný kromě aktuálně probíhajícího VoIP hovoru. Přestože je model IntServ jediný, který poskytuje garantovanou šířku pásma, tak má také problém se škálovatelností. Je-li k dispozici dostatečné množství rezervací, tak se šířka pásma jednoduše vyčerpá.[7]

2.3.3 RSVP

Resource Reseration Protocol definuje zprávy použité pro signalizaci zdroje řízení přístupů a rezervace zdrojů podle IntServ. Pokud aplikace vyšle signalizuje, že požaduje určitou úroveň služby, tak pokud jsou volné zdroje k dispozici, síťová zařízení tuto RSVP rezervaci přijmou.

Jestliže je třeba zajistit, že bude k dispozici zaručená kvalita služeb, tak síťová zařízení musí identifikovat pakety, které patří do rezervovaných toků a poskytnou odpovídající přístup k frontám. Když dojde k potvrzení službou o novém datovém toku, Cisco IOS nastaví síťový klasifikátor po cestě směrování paketů a povolí síťovým zařízením identifikovat takové pakety, pro které bude provedena rezervace. Tak bude zaručena požadovaná kvalita služeb. Cisco IOS používá stávající QoS nástroje.[6]

2.3.4 Úrovně RSVP

Pokud jsou od sítě požadovány určité úrovně, tak musí být nejdříve definovány.

V současné době RSVP definuje tři odlišné úrovně:

- Garantované QoS
- Řízené zatížení síťových prvků
- Úrovně Best-Effort

Garantovaná úroveň služeb QoS je použita tehdy, je-li požadována šířka pásma pro datový tok se stabilním zpožděním. Tato služba umožní poskytnout obě zpoždění a šířku pásma. Tento typ RSVP služby se využívá pro hlasové brány, když potřebují rezervovat šířku pásma pro hlasové toky.

Řízené zatížení síťových prvků se velmi podobá chování službě Best-Effort při nepřetížené síti na stejných zařízeních. Pokud aplikace dobře pracuje na nepřetížené síti, tak úroveň služby RSVP řízeného zatížení pracuje správně. Pokud je síť správně nakonfigurovaná na řízené zatížení, tak aplikace mohou počítat s následujícími parametry:

- Velmi malá ztrátovost - pokud síť není přetížená, tak nedochází k zaplnění front a tudíž nedochází ani k zahazování paketů ve frontě. Pakety jsou zahozeny jen tehdy, dojde-li k chybě během přenosu.
- Velmi malé zpozdění a jitter - jestliže není síť přetížená, tak opět nedochází k zaplnění front a zpoždění ve frontách je mnohem více proměnlivou složkou jak zpoždění tak jitteru.

Best-Effort pracuje stejným způsobem jak bylo popsáno u této služby výše, tedy negarantuje žádnou prioritu datovému toku. Je s ním zacházeno jako s ostatními datovými toky, které na směrovači jsou.[6]

2.3.5 Differentiated Services (DivServ)

DiffServ je technika, která je založená na principu následujícího skoku. To znamená, že na každém směrovači nebo přepínači se na základě informací uložených v hlavičce paketu rozhoduje jak se s takovým paketem naloží. Všechny informace, které k tomuto rozhodování jsou potřebné, si každý paket nese ve své hlavičce. Paket sám o sobě nemůže rozhodnout jak se s ním bude zacházet, ale na základě příznaků, klasifikačních a značkovacích údajů, které mohou být používány pro rozhodování na jednotlivých zařízeních v sítích, podle zvolené metodiky QoS. Každé zařízení v cestě může mít jiné nastavení.

Toto rozhodování se může odehrávat na dvou vrstvách OSI modelu. Nyní budou blíže přiblíženy.

2.3.6 QoS klasifikace na druhé vrstvě

Rámce na druhé vrstvě nemají žádný mechanismus, na základě, kterého by bylo možné určit prioritu nebo důležitost rámce. Tudíž přepínač na druhé vrstvě může pouze přesměrovat rámce podle techniky Best-Effort.

Pokud rámce putují z přepínače na přepínač, tak je zde technika kterou lze pro klasifikaci použít. Mezi přepínači lze pro přenos rámců použít více VLAN a na ně aplikovat tzv. trunk. Trunk rámce zabalí a přidá k němu údaj o zdrojové VLAN. Mimo to může přidat také pole, které indikuje hodnotu CoS (Class of Service) každého rámce. Právě tato hodnota umožní na přepínačích využít nastavení QoS. Poté co je trunk doručen a rozbalen na koncovém přepínači, tak je informace CoS zahozena.[8]

Dvě trunk zapouzdření řeší CoS odlišně:

IEEE 802.1Q Každý rámec je označen 12-bitovým VLAN ID a polem User. Pole User obsahuje tři 802.1p bity, které označují rámec CoS. Ten může mít hodnotu od 0 do 7, kdy nejnižší hodnota znamená nejnižší prioritu doručení a naopak nejvyšší hodnota znamená nejvyšší prioritu doručení. Rámce, které prochází výchozími VLANy neobsahují pole VLAN ID ani User a jsou přenášeny s defaultními nastaveními CoS, které je na přepínači. [8]

Inter-Switch Link (ISL) Každý rámec je označen 15-bitovým VLAN ID. Kromě toho je zde pole Type, které má velikost 4 bity a je používáno jako pole User. Spodní 3 bity pole User jsou používány jako CoS hodnota. Ačkoli ISL není založeno na standardech, tak přepínače Catalyst umí vzít hodnotu CoS z 802.1p z trunku 802.1Q a vložit jej do pole User u trunku ISL. Tím je zajištěno, že je hodnota CoS propagovaná mezi různými druhy zapouzdření. [8]

2.3.7 QoS klasifikace na třetí vrstvě s DSCP

Na začátku bylo definována hlavička IP, která obsahuje 1 bajtové pole služby type of service (ToS). Samotné pole je dále rozděleno a 3 nejvyšší bity jsou definovány jako pole priority, IP Precedence (IPP). Úplný seznam hodnot původního 3 bitového pole IPP z bajtu ToS je zobrazen v tabulce 2.1. [4]

Technologie DiffServ vyžaduje pro označení paketů více než 3 bity, a proto zavedla

Tab. 2.1 Hodnoty a názvy pole IPP [4]

Název	Desítková hodnota	Binární hodnota
Rutinní (Routine)	Priorita 0	000
Prioritní (Priority)	Priorita 1	001
Okamžitý (Immediate)	Priorita 2	010
Bleskový (Flash)	Priorita 3	011
Bleskový potlačený (Flash Override)	Priorita 4	100
Kritický (Critic/Critical)	Priorita 5	101
Řízení internetové sítě (Internetwork Control)	Priorita 6	110
Řízení sítě (Network Control)	Priorita 7	111

novou standardní definici bajtu ToS. Samotný bajt ToS byl přejmenován na pole Differentiated Services (DS) a pole IPP bylo nahrazeno 6 bitovým polem (nejvyšší bity 0-5) nazývaným pole Differentiated Services Code Point (DSCP). Později byly nadefinovány 2 nejnižší bity pole DS, které se používají ve funkci explicitního oznamování zahlcení QoS Explicit Congestion Notification (ECN). [4]

Porovnání bajtu ToS a DS je zobrazeno v tabulce 2.2

Tab. 2.2 Formát bajtu ToS a DS [8]

ToS	P2	P1	P0	T3	T2	T1	T0	Zero
DS	DS5	DS4	DS3	DS2	DS1	DS0	ECN1	ECN0
	(Class Selector)			(Drop Precendence)				

Jak lze vidět, odlišné jsou jen názvy jednotlivých bitů. Ve skutečnosti je DSCP zpětně kompatibilní s IPP, takže zařízení, které neumí pracovat s DiffServ stále může mít nějaké informace o QoS.

DSCP je rozdělen do 3 bitového class selektoru a 3 bitového Drop Precedence hodnoty. V tabulce 2.3 je zobrazeno, v jaké relaci jsou mezi sebou IPP, chování DSCP per-hop, kódové názvy DSCP a hodnoty.

Tab. 2.3 Mapování polí IP Precedence a DSCP [8]

IP Precedence (3 bity)			DSCP (6 bitů)				
Název	Hodnota	Bity	Per-hop chování	Class selector	Drop Precedence	Kódový název	DSCP bity (desítkově)
Routine	0	000	Default			Default	000000 (0)
Priority	1	001	AF	1	1: Nízké	AF11	001010 (10)
					2: Střední	AF12	001100 (12)
					3: Vysoké	AF13	001110 (14)
Immediate	2	010	AF	2	1: Nízké	AF21	010010 (18)
					2: Střední	AF22	010100 (20)
					3: Vysoké	AF23	010110 (22)
Flash	3	011	AF	2	1: Nízké	AF31	011010 (26)
					2: Střední	AF32	011100 (28)
					3: Vysoké	AF33	011110 (30)
Flash Override	4	100	AF	2	1: Nízké	AF41	100010 (34)
					2: Střední	AF42	100100 (36)
					3: Vysoké	AF43	100110 (38)
Critical	5	101	EF			EF	101110 (46)
Internetwork Control	6	110					(48-55)
Network Control	7	111					(56-63)

Tři class selector bity (DS5 až DS3) klasifikují pakety do jedné z osmi tříd:

- Třída 0, je výchozí třída, nabízí pouze best-effort směrování
- Třídy 1 až 4 jsou nazývány assured forwarding (AF) service level. Výšší hodnota AF třídy značí výskyt přenosu s vyšší prioritou.
  Pakety v AF třídě mohou být zahozeny. Pokud je to nezbytné, budou zahozeny

pakety s nižší hodnotou. Například, paket AF s třídou 4 bude mít přednost v doručení před AF paketem s třídou 3.

- Třída 5 je známá jako expedited forwarding (EF), těmto paketům jsou dány nadstandardní služby. U EF je nejmenší pravděpodobnost zahození a je obvykle rezervovaná pro časově kritické aplikace jako je třeba přenos hlasu.
- Třídy 6 a 7 jsou nazývány jako řízení internetové sítě a řízení sítě a jsou určeny právě pro řízení síťového provozu. Obvykle je používají přepínače a směrovače na sdílení informací o směrovacích protokolech, Spanning Tree Protocol. To zajišťuje včasné doručení paketů a udržuje síť stabilní a v provozu.[8]

Každá třída je v DCSP reprezentována také třemi úrovněmi zahazovacích preferencí, které jsou v DS2 ažd DS0, kde DS0 má obvykle hodnotu 0:

- Nízká (1)
- Střední (2)
- Vysoká (3)

V rámci třídy mají pakety, které jsou označeny vyšší drop precedence, mají vyšší pravděpodobnost, že budou zahozeny, před těmi, které mají tuto hodnotu nižší. Jinými slovy, nižší hodnota dá lepší službu. To dává k dispozici jemnější nástroj pro rozhodování, které pakety mohou být zahozeny, je-li to nezbytné. [8]

2.4 Kontrola zahlcení sítě (Congestion management)

Funkce kontroly zahlcení sítě umožňují řídit zahlcení sítě pomocí řazení paketů, které přijdou na rozhraní a rozhoduje se podle priorit, které tyto pakety mají. To znamená, že se musí vytvářet fronty, které se naplňují na základě klasifikace paketů a pomocí plánování paketů ve frontě pro přenos sítí. Kontrola zahlcení sítě QoS nám dává 4 typy front, kdy nám každá z nich dává možnost vytvořit různé množství front a tím umožnit větší či menší diferenciaci provozu a určit pořadí, ve kterém se bude provoz odbavovat.

V období s nízkým zatížením sítě, kdy nehrozí zahlcení sítě, se pakety odesílají takřka okamžitě. V době, kdy dochází k zahlcení sítě, jsou pakety rychleji přijímány než odesílány. Pokud použijeme některý z nástrojů pro kontrolu zahlcení sítě, tak jsou pakety řazeny do front, které jsou obslouženy, jakmile dojde k uvolnění rozhraní. Následně jsou naplánovány k odeslání na základe stanovených priorit, které jsou na zařízení a rozhraních nakonfigurovány. Směrovač určuje pořadí přenosu paketu podle toho, ve které frontě je umístěn a v jakém nastavení vůči sobě jsou. [9]

2.4.1 Proč používat kontrolu zahlcení sítě?

V heterogenních sítích používají aplikace mnoho různých protokolů, což vede k potřeba stanovit prioritu provozu, aby byly upřednostněny časově závislé aplikace (hlasový hovor) před méně náročnými aplikacemi na čas doručení, jakým je například přenos datového souboru. Různé typy přenosů sdílející datové cesty spolu mohou v síti komunikovat, v případě, že ovlivňují výkon aplikace. Pokud je vaše síť navržena tak, že podporuje mezi dvěma směrovači sdílet jednu datovou cestu pro různé druhy provozu, je dobré použít techniku kontroly zahlcení sítě, aby bylo zajištěno spravedlivé zacházení napříč různými druhy přenosu. [9]

2.4.2 Algoritmy řazení do front

FIFO je nejjednodušší řadící algoritmus, kde jsou pakety řazeny do jedné fronty a obsluhovány v pořadí v jakém byly přijaty. [10] Je-li použito FIFO, tak může špatné chování zdroje spotřebovat celou šířku pásma, může způsobit zpoždění časově citlivých dat nebo důležitého provozu, nebo můžou být pakety důležitého přenosu zahozeny, protože méně významný přenos naplnil frontu.

Pokud nejsou nastaveny žádné frontové strategie, tak s výjimkou sériového rozhraní na E1 (2048Mbps) a nižších se používá FIFO jako výchozí. (Sériové rozhraní E1 a nižší používají jako výchozí strategii WFQ).

FIFO je nejrychlejší frontová technika a je efektivní pro velké linky, které mají malé zpoždění a minimální zahlcení. [9]

PQ (Priority Queuing) PQ algoritmus je také velmi jednoduchý. Každému paketu je přiřazena priorita a je zařazen do hierarchické struktury front organizovaných podle priority. Nejdříve se odbaví fronta s nejvyšší prioritou a až jsou odbaveny všechny pakety, tak se pokračuje s odbavením fronty s nižší prioritou. To se provádí do té doby, dokud se fronta nevyprázdní nebo dokud nejsou pakety ve frontě s vyšší prioritou.

Pakety mohou být odeslány z nižší fronty pouze tehdy, jsou-li odeslány všechny pakety z front s vyšší prioritou. Dojde-li paket do fronty s vyšší prioritou, je z této fronty odeslán přednostně, před pakety z fronty s nižší prioritou.

U tohoto algoritmu se může stát, že pakety ve frontě s nižší prioritou zastarají, pokud probíhá neustálý provoz ve frontách s vyšší prioritou. V takovém případě se může stát, že pakety z fronty s nižší prioritou nebudou nikdy odeslány. [9]

Round Robin (RR) Algoritmus fronty typu round-robin pracuje tak, že používá více front, do kterých řadí příchozí pakety a odesílá je tzv. kruhovým způsobem. V každém kole odešle jeden paket z každé fronty. Nemůže se tedy stát, že by některá fronta nebo paket zastaraly, protože jsou v každém kole obslouženy všechny fronty.

Pokud mají všechny pakety stejnou velikost, tak budou mít všechny fronty sdílenou šířku pásma rovnoměrně. Pokud ale budou ve frontách pakety s různou velikostí, tak bude šířka pásma bude mezi frontami rozdělena nerovnoměrně.

Nevýhodou round-robin algoritmu je to, že zde neexistuje přednostní odbavení. [9]

Weighted Round Robin (WRR) Tento algoritmus je rozšířením algoritmu round-robin o prioritizaci.

U WRR jsou pakety rozděleny do tříd (hlas, přenos souborů, atd) a zařazeny do fronty podle příslušné hodnoty CoS. Pakety jsou stále odesílány kruhovým způsobem, tak jako u RR, ale zde je jim dána „váha“. Například, máme tři fronty, první s váhou 4, druhou s váhou 2 a třetí s váhou 1. Odesílání probíhá tak, že když je odbavována první fronta, tak algoritmus podle váhy zjistí, že může odeslat až 4 pakety z této fronty, pak pokračuje do druhé fronty a zde zjistí, že může odeslat až 2 pakety a u třetí fronty může odeslat jen jeden paket. Tak je zajištěna priorita a zároveň jsou obslouženy všechny fronty.

Některé implementace WRR algoritmu používají pro odesílání místo počtu paketů, počet bajtů, které mohou v každém cyklu odeslat. Příkladem takovéto implementace je Cisco custom queuing (CQ).

V následujícím příkladu si ukážeme, jaký problém může nastat v případě, kdy se odesílání řídí počtem bajtů. Mějme následující nastavení

- MTU na rozhraní 1500 bajtů
- počet bajtů na odeslání z fronty v každém cyklu (Treshold) 3000 bajtů (dvojnásobek MTU)

V příkladě odešle router první dva pakety s celkovou velikostí 2999 bajtů. Protože je stále ještě v povoleném limitu, který je 3000 bajtů, tak může odeslat další paket z povolené velikosti MTU. Výsledkem je, že byla o 50 procent přetížena šířka pásma než bylo povoleno. Jak můžeme vidět, WRR algoritmus nealokuje šířku pásma přesně.[9]

Deficit Round Robin (DRR) U tohoto algoritmu jde opět o úpravu nevýhod toho předešlého, tedy WRR. Řeší zde problém s nepřesnou alokací šířky pásma. Cisco modifikovalo DRR do algoritmu MDRR, který je použit u zařízení Cisco 12000 series.

Deficit Round Robin používá počítadlo, které udává kolik bajtů bylo odesláno nad rámec povoleného limit, nazývaný deficit. Tento spočítaný přečerpaný limit se v dalším cyklu zohlední, a to tak, že se od Tresholdu odečte deficit a zůstane číslo udávající počet bajtů, které je možné v tomto cyklu odeslat. Ukážeme si to na příkladu: [9]

- Treshold je 3000 bajtů
- Velikost paketů: 1500, 1499, 1500
- Celkem k odeslání v cyklu: 4499 bajtů
- Deficit = (4499 - 3000) = 1499 bajtů
- V dalším cyklu může být odesláno pouze (treshold - deficit) = (3000 - 1499) = 1501 bajtů

2.4.3 Princip činnosti front ve směrovačích Cisco

Směrovače Cisco mohou nad pakety, které čekají na výstup přes dané rozhraní, provádět při vhodné konfiguraci takzvané *inteligentní řazení do front* (fancy queuing). Jestliže například směrovač bude přijímat po několik dalších sekund 5Mbps provozu, jejž by bylo potřeba odvysílat přes jednu stejnou sériovou linku T1, určitě jej nezvládne všechen odeslat. Zařadí proto pakety do jedné nebo více softwarových front, které pak může řídit - může tedy ovlivnit, jaké pakety opustí rozhraní jako další a které pakety budou zahozeny.[4]

Softwarové a hardwarové fronty Fronty, které nad rozhraním vytvoří určitý nástroj pro obsluhu front, se nazývají *softwarové fronty*, protože jsou implementovány softwarově. Jakmile, ale je plánovač front převezme ze softwarové fronty další paket, neznamená to, že by okamžitě odcházel přes rozhraní ven. Namísto toho směrovač vezme paket ze softwarové fronty rozhraní a zařadí jej do malé hardwarové fronty typu FIFO, definované nad každým rozhraním. Tuto oddělenou finální frontu nazývá společnost Cisco vysílací fronta (transmit queue, TX queue) nebo vysílací okruh (transmit ring, TX ring), podle modelu směrovače; obecně se jim pak říká hardwarové fronty.

Hardwarové fronty mají následující vlastnosti:[4]

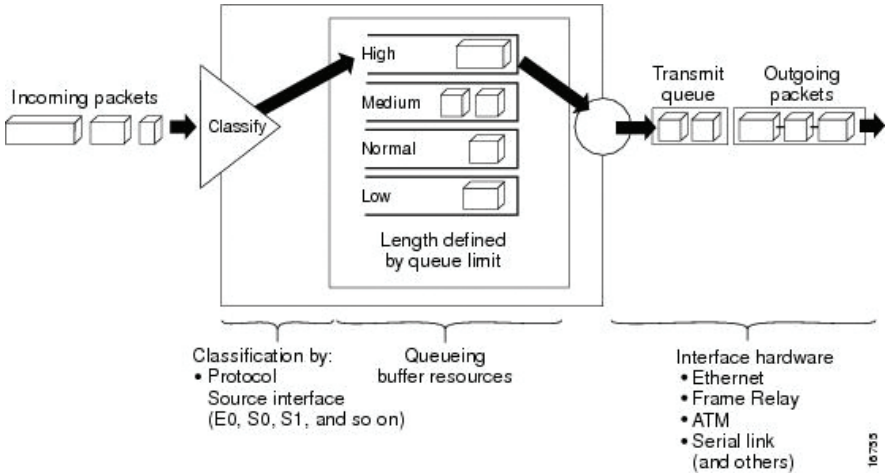
- Jakmile dané rozhraní dokončí odeslání paketu, může se zakódovat a přes stejné rozhraní odeslat další paket z hardwarové fronty, a to bez nutnosti softwarového přerušení procesoru; tím se plně využije šířka pásma rozhraní.
- Vždy používá logiku FIFO
- Jejich činnost nelze ovlivnit nástroji systému IOS pro práci s frontami.
- Pokud je v provozu nástroj pro práci s frontami, zkracuje systém IOS automaticky délku hardwarové fronty oproti výchozí hodnotě.
- Kratší hardwarová fronta znamená, že se pakety budou delší dobu zdržovat v řízené softwarové frontě; tím má frontový software větší kontrolu nad provozem opouštějícím dané rozhraní.
- U hardwarových front můžeme manipulovat pouze s jedinou vlastností, a sice s jejich délkou.

PQ (Priority Queuing) PQ umožňuje definovat, jakým způsobem bude provoz na síti priorizován. Používá ke konfiguraci čtyři druhy priorit, vysokou, střední, normální a nízkou. Můžeme definovat sérii filtrů, které jsou založeny na charakteristice paketu a směrovač je umístí do jedné z front; fronta s nejvyšší prioritou je odbavována první a to do té doby, doku není prázdná. Poté jsou odbavovány ostatní fronty v sekvenci.

Během přenosu dává PQ prioritním frontám absolutní přednost před frontami s nižšími prioritami; důležitý přenos dostane nejvyšší prioritu a má vždy přednost před méně důležitými přenosy. Pakety jsou klasifikovány na základě uživatelsky specifikovaných kritérií a vloženy do jedné ze čtyř výstupních front (vysoká, střední, normální a nízká) podle přiřazené priority. Pakety které nejsou klasifikovány jsou automaticky zařazeny do fronty normální. Celý proces ilustruje obrázek (Obr. 2.1).

Když jsou pakety nachystány na odeslání z rozhraní, PQ na rozhraní oskenuje všechny pakety sestupně podle priorit. Fronta s vysokou prioritou je skenována jako první, následuje fronta se střední prioritou a tak dále. Paket, který je první na výstupu z fronty s nejvyšší prioritou je zvolen pro přenos. Celý proces se opakuje pro každé odeslání paketu.

Maximální délka fronty je definována limitem délky. Když je fronta delší než je povolený limit, tak jsou všechny ostatní pakety zahozeny. [9]



Obr. 2.1 Priority Queuing [9]

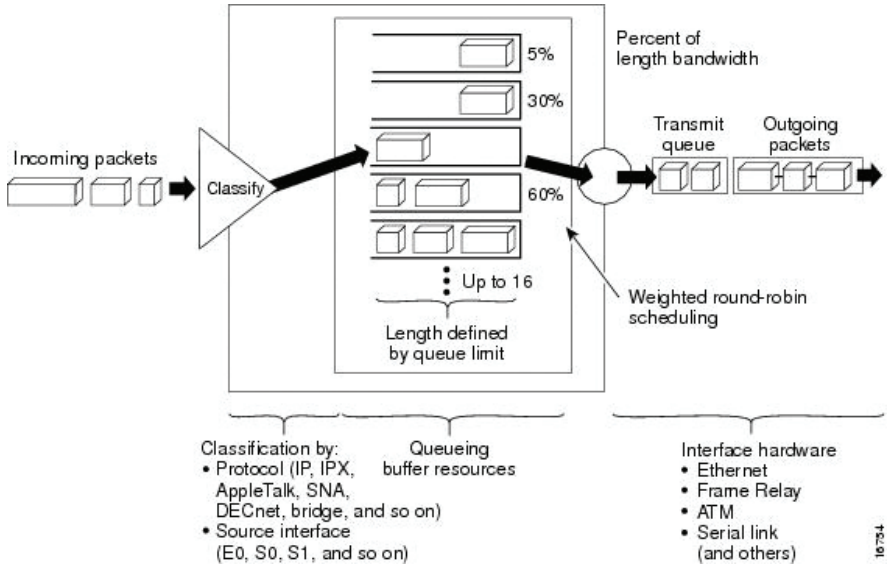
CQ (Custom Queuing) CQ umožňuje zadat určitý počet bajtů, které předá pokaždé, když je fronta obsluhována a tím umožní sdílení síťových zdrojů mezi aplikacemi se specifickými minimálními požadavky na šířku pásma nebo na latenci. Můžeme také určit maximální počet paketů v každé frontě.

CQ řídí provoz pomocí specifikování počtu paketů nebo bajtů, které mohou být obslouženy v každé třídě provozu. To je řešeno podobným způsobem, jako je tomu u cyklického round-robin algoritmu, odesíláním v přidělené šířce pásma každé fronty před tím než se přesune k další frontě. Pokud je fronta prázdná, tak směrovač pokračuje odesláním paketů z fronty, která je připravena na přenos.

Když je na rozhraní povoleno CQ, tak si systém vytvoří 17 výstupních front. Tyto fronty jsou označeny 1 až 16. U každé fronty je možné nastavit počet bajtů, které specifikují kolik bajtů dat je systém schopný doručit ze stávající fronty před tím než se přesune k další frontě.

Fronta s číslem 0 je systémovou frontou a musí být vyprázdněna před všemi ostatními frontami. Tato fronta má nejvyšší prioritu doručení a posílají se přes ní keepalive pakety a signální pakety. Žádný jiný provoz nemůže tuto frontu používat.

Fronty 1 až 16 prochází systém sekvenčním způsobem, podle pravidel round-robin, a odebírá z každé fronty nastavený počet bajtů v každém cyklu. Když se zpracovává konkrétní fronta, tak jsou pakety odesílány dokud, počet odeslaných bajtů nedojde povolené hranice nebo dokud se fronta nevyprázdní. Celý proces ilustruje obrázek 2.2.[9]



Obr. 2.2 Custom Queuing [9]

WFQ (Weighted Fair Queueing) WFQ bylo vyvinuto, aby řešilo problémy s řazením do fronty, kterými jsou:

- Fronta FIFO způsobuje zastarávání, zpoždění a jitter
- PQ způsobuje zastarávání front s nižšími prioritami a trpí všemi problémy fronty FIFO v každé ze čtyř vnitřních front, které používá pro stanovení priorit.
- CQ způsobuje velké zpoždění a také trpí všemi problémy, které má fronta FIFO u všech 16 front, které jsou použity pro klasifikaci provozu.

Hlavními myšlenkami WFQ jsou:

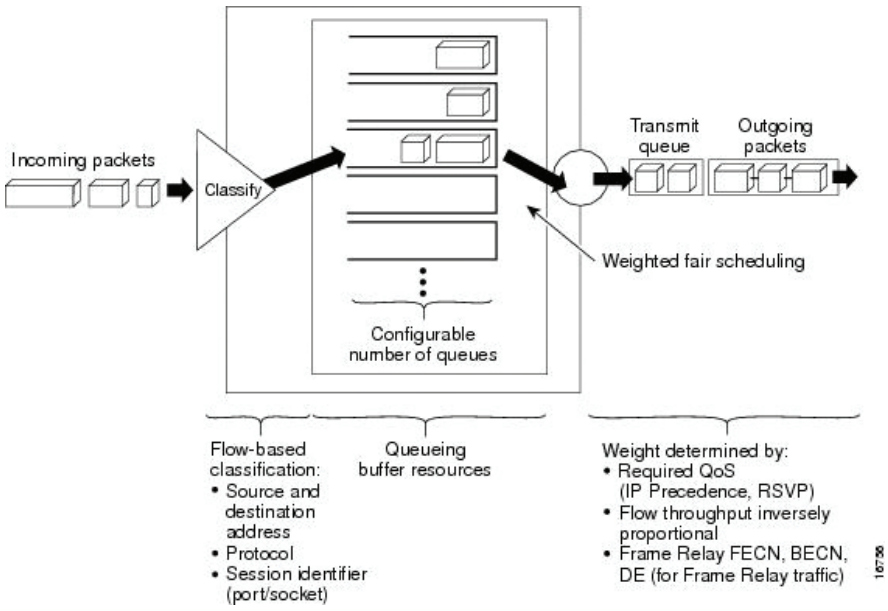
- Dedikovat fronty v každém proudu, aby nedocházelo k zastarávání, zpoždění nebo jitteru ve frontě.
- Spravedlivé přidělování šířky pásma mezi všemi toky v síti a tím získat minimální zpoždění při plánování a garantování služeb.
- Použít IP precedence jako váhu, když se přiděluje šířka pásma. [10]

WFQ má čtyři typy, které si blíže popíšeme. Jsou jimi:

- Flow-Based Weighted Fair Queueing
- Distributed Weighted Fair Queueing
- Class-Based Weighted Fair Queueing
- Distributed Class-Based Weighted Fair Queueing

Flow-Based Weighted Fair Queueing je obecně označována zkratkou WFQ. WFQ je dynamická plánovací metoda, která poskytuje férový přístup k alokaci šířky pásma celého síťového provozu. WFQ aplikuje techniku priorit nebo vah k identifikaci provozu, aby bylo možné klasifikovat provoz do konverzací, aby bylo možné rozhodnout, nakolik každá z konverzací vytěžuje šířku pásma ve vztahu k ostatním provozům. Je založen na Flow-base algoritmu, který simultánně plánuje interaktivní provoz do front a snižuje tím čas odezvy a spravedlivě dělí zbylou šířku pásma mezi vysoké toky šířky pásma. Jinými slovy, WFQ umožní přenos s nízkými nároky, jako je Telnet, před přenosem, na který jsou kladeny vysoké nároky na přenos, jako je FTP spojení. Dojde-li k souběžnému přenosu souborů, WFQ zajistí to, aby byla rovnoměrně využita kapacita linky. To znamená, že mají k dispozici srovnatelnou šířku pásma.[9]

Na následujícím obrázku (Obr. 2.3) je ukázáno, jak WFQ pracuje:



Obr. 2.3 Weighted Fair Queueing [9]

Datové toky jsou identifikovány na základě následujících informací, které jsou uloženy v IP hlavičkách a TCP nebo UDP hlavičkách:

- Zdrojová IP adresa
- Cílová IP adresa
- Číslo protokolu (identifikuje TCP nebo UDP)
- Pole Type of service
- Zdrojové číslo portu TCP nebo UDP

- Cílové číslo portu TCP nebo UDP

WFQ používá pevný počet front. Výchozí počet front se stanovuje podle šířky pásma na rozhraní. Počet front může být nastaven v rozsahu 16 až 4096 front a hodnota musí být mocninou 2. [10]

DWFQ (Distributed Weighted Fair Queueing) DWFQ je speciální vysokorychlostní verze WFQ, která se používá na zařízeních VIP. Podporují ji následující řady zařízení, které mají procesory VIP2-40 nebo vyšší:

- Cisco 7000 series s RSP7000
- Cisco 7500 series

U DWFQ máme dvě formy:

- Flow-based. U této formy jsou pakety klasifikovány po proudech. Pakety se stejnou zdrojovou IP adresou, cílovou IP adresou, zdrojovým TCP nebo UDP portem, cílovým TCP nebo UDP portem, protokol a ToS pole patří do stejného proudu.
  Každému proudu odpovídá oddělená výstupní fronta. Pokud jsou pakety přiřazeny do nějakého proudu, jsou také umístěny do fronty k příslušnému proudu. Když dojde k přetížení, DWFQ přidělí stejnou šířku pásma každé aktivní frontě.
- Class-based. V této formě jsou pakety řazeny do front podle toho, v jaké QoS skupině se nachází a nebo podle pole ToS u IP precedence.
  Skupiny QoS nám umožňují nastavovat zásady QoS. Jedná se o interní klasifikaci paketů, kterou používá směrovač k rozhodování, jak jsou pakety ovlivňovány různými nastaveními QoS, jako je DWFQ a CAR.[10]

CBWFQ (Class-Based Weighted Fair Queueing) CBWFQ je rozšířením standardní WFQ funkcionality a poskytuje podporu pro uživatelsky definované třídy přenosu. Definujeme zde třídy přenosu podle shody několika kritérií, která zahrnují protokoly, access control listy (ACL) a vstupní rozhraní. Pakety, které splňují daná kritéria třídy pak tvoří její provoz. Pro každou třídu je vyhrazena fronta FIFO, a provoz, který do dané třídy patří je směrován do příslušné fronty.

Poté, co byla třída definována, ji můžeme přiřadit vlastnosti, které třídu charakterizují. Přiřadíme ji šířku pásma, váhu a maximální počet paketů. Šířka pásma přidělená třídě je garantovanou šířkou pásma pro doručování během zahlcení.

K další charakterizaci třídy, může také posloužit nastavení limity třídy, která udává maximální počet paketů, které je možná naakumulovat ve frontě třídy. Pakety, které patří do třídy jsou podřazené šířce pásma a limitu fronty, které danou třídu charakterizují.

Tail drop je u CBWFQ třídy použita do té doby, dokud nejsou explicitně nastaveny zásady třídy tak, aby používaly k zahazování paketů techniku WRED a to ve smyslu předcházení zahlcení sítě. [10]

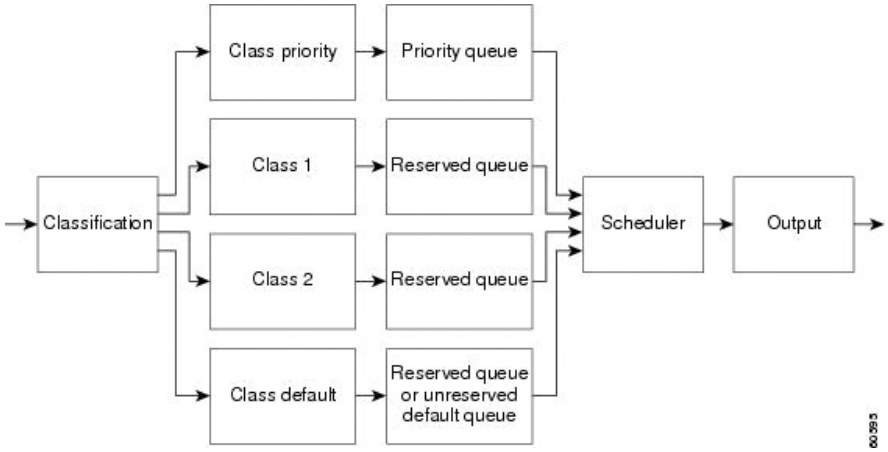
DCBWFQ (Distributed Class-Based Weighted Fair Queueing) DCBWFQ rozšiřuje funkce standardní WFQ funkcionality o podporu uživatelsky definovaných tříd přenosu u VIP.

LLQ (Low Latency Queueing) VoIP požaduje pro svou práci prioritní frontu. Můžeme použít libovolný frontový nástroj, který efektivně přiřadí VoIP nejvyšší prioritu, ale je doporučováno použít právě LLQ a to z toho důvodu, že je flexibilní a snadno se nastavuje.

Nejflexibilnější metodou, která splňuje požadavky na VoIP, je právě LLQ. LLQ používá konfigurační nástroj MQC na nastavení priorit určitých tříd a k zajištění minimální garantované šířky pásma pro třídy ostatní. Během zahlcení sítě je prioritní fronta hlídána na nastavené rychlosti tak, že prioritní přenos nemá monopol na celé šířce pásma. (Pokud má prioritní přenos monopol na šířku pásma, tak zabraňuje tomu, aby byla dodržena garantovaná šířka pásma pro ostatní fronty.) Pokud je LLQ správně nastaveno, tak by provoz na prioritní frontě neměl překročit nastavenou rychlost.

LLQ také umožňuje přesně určit hloubku fronty, kdy by měl směrovač zahazovat pakety, když jich hodně čeká v každé jednotlivé třídě fronty. K dispozici je také výchozí třída, která se používá pro všechen neklasifikovaný přenos. Na obrázku 2.4 je zobrazeno, jak LLQ pracuje.

Na obrázku (Obr. 2.4) je všechen odchozí provoz na rozhraních nebo subrozhraních (pro Frame Relay a ATM) nejdříve klasifikován pomocí MQC. Jsou zde čtyři třídy: jedna s nejvyšší prioritou, dvě s garantovanou šířkou pásma a výchozí třída. Třída prioritního přenosu je umístěna do prioritní fronty a třída s garantovanou šířkou pásma je umístěna do rezervované fronty. Provozu výchozí třídy může být poskytnuta rezervovaná fronta nebo může být zařazena do nerezervované výchozí fronty, kde každý datový tok bude mít k dispozici přibližně stejnou nerezervovanou a volnou šířku pásma. Služba



Obr. 2.4 LLQ operace [11]

plánování front pracuje tak, že přenos prioritní fronty probíhá do té doby, dokud není překročená nastavená priorita šířky pásma a tuto šířku pásma nepotřebuje rezervovaná fronta (značí to zahlcení). Rezervované fronty jsou obsluhovány podle jejich vyhrazené šířky pásma, které plánovač používá pro výpočet vah. Váha se používá k určení, jak často má být vyhrazená fronta obsluhována a kolik bajtů je možné v daném čase odbavit. Plánovač služeb je založen na WFQ algoritmu. [11]

2.5 Předcházení zahlcení sítě (Congestion avoidance)

Všechny nástroje pro předcházení zahlcení sítě pracují s hloubkou fronty, což není nic jiného než je počet paketů, které mohou ve frontě být, a kdy se začne se zahazováním paketů.

2.5.1 WRED (Weighted Random Early Detection)

Jakmile se fronta zaplní a systém IOS nemá kam zařadit nově příchozí pakety, začne je zahazovat. Tomuto jevu se říká tail drop (zahazování posledních). Vzhledem k nárazové povaze vysílání datových paketů se při zaplnění fronty často stává, že se takto zahodí několik paketů najednou.

Tail drop může mít ale pro síťový provoz velmi neblahé důsledky, zejména pro provoz TCP. Když se totiž pakety začnou ztrácet, ať už je důvod jakýkoli, zpomalí odesílatelé TCP svou rychlost odesílání. Když potom dojde k tail drop a ztratí se větší množství paketů, spojení TCP se zpomalí ještě více. Ve většině sítí navíc „běhá“ mnohem větší objem provozu TCP než UDP, takže po zahození posledních několika paketů klesá i celková provozní výkonnost sítě.

Je proto zajímavé, že celkovou propustnost sítě můžeme zvýšit, pokud několik paketů

zahodíme už v okamžiku, kdy se fronta začíná zaplňovat, a pokud nebudeme čekat na tail drop se všemi negativními důsledky. Pro tyto účely navrhla společnost Cisco mechanismus WRED (vážené náhodné včasné detekce), který průběžně sleduje délku fronty a jisté procento v ní zahazuje, s cílem zvýšení celkového výkonu sítě. Jakmile se fronta prodlužuje, začne WRED zahazovat více a více paketů a předpokládá, že tímto malým snížením nabízené provozní zátěže (nabízené kapacity) zabrání úplnému zaplnění fronty.

Mechanismus WRED provádí svá rozhodnutí na základě několika číselných parametrů. Za prvé využívá změřenou průměrnou délku fronty, podle níž stanovuje, jestli je již fronta dostatečně zaplněná a jestli má zahazovat pakety. Poté WRED porovná průměrnou hloubku s minimální a maximální prahovou hloubkou a na základě výsledku provádí při zahazování různé operace, které nám zobrazuje tabulka 2.4. Pokud je průměrná hloubka fronty velmi vysoká nebo naopak velmi nízká, jsou tyto operace zřejmé, i když výraz „plné zahazování“ v tabulce může být trochu překvapivý. Je to ale v pořádku: jakmile průměrná hloubka fronty překročí maximální prahovou hodnotu, začne WRED zahazovat všechny nové pakety. Na první pohled to může vypadat jako popsané tail drop, ve skutečnosti tomu tak ale není, protože samotná fronta ještě třeba zaplněna není. Pro rozlišování nazývá tedy WRED tuto kategorii „plným zahazováním“.

Tab. 2.4 Kategorie zahazování v mechanismu WRED [4]

Porovnání průměrné hloubky fronty a prahových hodnot	Operace	Název podle WRED
Průměr <= minimální práh	Nezahazují se žádné pakety.	Nezahazovat (no drop)
Minimální práh < průměrná hloubka <= maximální práh	Zahazuje se jisté procento paketů. Když se průměrná hloubka zvyšuje od minimálního po maximální práh, zvyšuje se úměrně procento zahozených od 0 do maximálního procenta	Náhodné zahazování (random drop)
Průměrná hloubka > maximální práh	Zahazují se všechny nové pakety; podobné jako tail drop	Plné zahazování (full drop)

Dokud se průměrná hloubka fronty pohybuje mezi oběma prahovými hodnotami, zahazuje WRED jisté procento paketů. Jeho přesná hodnota roste lineárně s růstem průměrné hloubky fronty od minimální po maximální prahovou hodnotu.

Posledním z číselných parametrů, které mají vliv na činnost logiky mechanismu WRED, je MPD (mark probability denominator), z něhož odvozujeme maximální procentní podíl zahození. Systém IOS vypočítá procento zahození pro případ dosažení maximální prahové hodnoty z jednoduchého vzorce 1/MPD; budeme-li mít příklad, kdy jmenovatel MPD bude roven 10, pak dostaneme hodnotu 1/10 a míra zahazování se proto bude pohybovat od 0 do 10 procent - úměrně růstu průměrné hloubky fronty od minimální po maximální prahovou hodnotu. Konkrétní zahazované pakety vybírá WRED náhodně.[4]

2.6 Měření kvality zvuku

K určení kvality signálu lze použít několik metod, například:

- MOS (Mean Opinion Score)
- PSQM (Perceptual Speech Quality Measurement)
- PESQ (Perceptual Evaluation of Speech Quality)

2.6.1 MOS

MOS je hodnotící systém pro kvalitu hlasu. Skóre MOS je generováno, když posluchači vyhodnocují předem nahrané věty, které jsou zpracovány různými způsoby, například kompresními algoritmy. Posluchači potom větám přiřadí hodnoty od 1 do 5, kde 1 znamená nejhorší a 5 nejlepší. Pro testy MOS v angličtině se používá věta „Nowadays, a chicken leg is a rare dish“. Používá se proto, že obsahuje širokou škálu zvuků charakteristických pro lidskou řeč, například dlouhé samohlásky, krátké samohlásky a tvrdé a měkké zvuky.

Z testovacího skóre je následně vypočteno průměrné skóre. Výsledky testů jsou subjektivní, protože vycházení z názorů posluchačů. Jsou relativní také proto, že skóre 3,8 z jednoho testu nelze přímo porovnat se skóre 3,8 z jiného testu. Je proto nutné vytvořit standard pro všechny testy, například G.711, aby bylo možné testy normalizovat a přímo porovnávat.[1]

2.6.2 PSQM

PSQM je automatizovaný způsob měření aktuální kvality řeči. software PSQM se obvykle nachází v systémech řízení volání IP, které jsou někdy integrovány do systémů SNMP (Simple Network Management Protocol).

Vybavení a software, které mohou měřit metodu PSQM, jsou k dispozici od dodavatelů

z řad třetích stran. Nejsou implementovány do zařízení Cisco. Měření probíhá porovnáváním kvality řeči, která byla na jednom konci odeslána, s výslednou řečí na druhém konci komunikačního kanálu. Systémy PSQM jsou nasazovány jako komponenty pracující v reálném čase. Měření metodou PSQM probíhají během vlastní konverzace v síti. Tento automatizovaný testovací algoritmus má více než 90 procentní přesnost v porovnávání se subjektivními poslechovými testy, například MOS. Skóre je vyhodnocováno na stupnici od 0 až do 6,5, kde 0 představuje nejlepší výsledek a 6,5 výsledek nejhorší. Metoda PSQM byla původně navržena pro přenos hlasu s okruhovým přepínáním, nepočítá se u ní s problémy se zpožděním nebo jitterem, ke kterým dochází v systémech přenosu hlasu využívající techniku přepínání paketů.[1]

2.6.3 PESQ

Metoda PESQ byla vyvinuta specificky pro testování kvality hlasu mezi hovořícím a poslouchajícím účastníkem v podmínkách skutečné sítě, například VoIP, POTS (Plain old Telephone service), ISDN (Integrated services digital network) a GSM (Global System for Mobile Communication). Metoda měření PESQ byla vyvinuta oddělením KPN Research - nyní TNO Telecom (Nizozemí) a společností BT (British Telecommunications) zkombinováním dvou pokročilých metod měření kvality hlasu: PSQM+ a PAMS (Perceptual Analysis Measurement System).

Z metody PESQ se vyvinulo doporučení P.862 organizace ITU-T, které je považováno za aktuální normu pro měření kvality hlasu. Metoda PESQ dokáže počítat s chybami kodeku, chybami filtrování, problémy způsobenými jitterem a zpožděním obecně, kterými se využívání sítí VoIP vyznačuje. Kombinuje to nejlepší z metody PSQM a z metody, která má název PAMS. Skóre měření metodou PESQ je v rozsahu od 1 (nejhorší) do 4,5 (nejlepší), přičemž 3,8 je považováno za kvalitu obvyklou u placených služeb (přijatelná kvalita v tradičních telefonních sítích). Metoda PESQ je určena k měření pouze jednoho aspektu kvality hlasu. Skóre PESQ neodráží faktory, které jsou typické pro obousměrnou komunikaci, například nízká hlasitost, zpoždění, ozvěna a vedlejší tón.[1]

II. PROJEKTOVÁ ČÁST

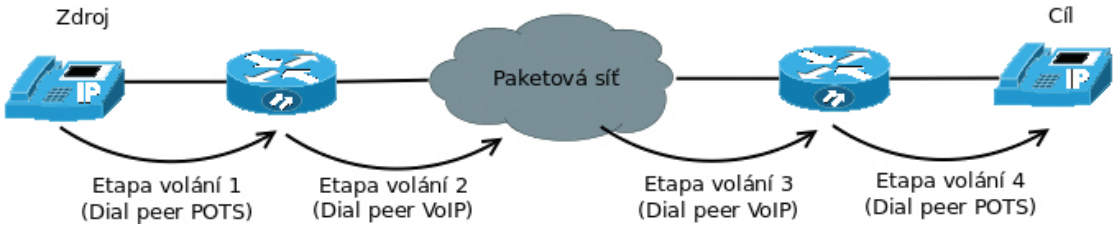
3 ZÁKLADNÍ KONFIGURACE VOICE OVER IP

konfigurace VoIP, aby správně fungovala na směrovačích Cisco nebo přístupovém serveru, tak se skládá z následujících šesti kroků:

Krok 1 Nejdříve je potřeba nastavit IP síť tak, aby byla schopná pracovat s hlasem v reálném čase. Pro jemné doladění sítě, aby VoIP správně pracoval, obsahuje řadu protokolů a funkcí, pro zlepšení QoS. Pro nastavení IP síť v hlasovém real-time provozu je třeba zvážit celý rozsah sítě. Poté vybrat a nakonfigurovat odpovídající nástroje QoS.

Krok 2 Pokud je v plánu používání VoIP v prostředí Frame Relay, je třeba při konfiguraci VoIP vzít v úvahu některé další faktory, aby provoz přes Frame Relay probíhal hladce. Příkladem může být, že veřejné Frame Relay cloudy neposkytují záruky pro QoS.

Krok 3 konfigurace dial peerů. K definování deal pearů se používá příkaz **dial-pear voice**, v konfiguračním módu. Každý dial peer definuje charakteristiky spojené s call legs (etapy volání). Call legs jsou logická spojení mezi libovolnými dvěma telefonními zařízeními, jako jsou brány, směrovače, správci Cisco Unified Communication Managers či koncové telefonní přístroje. End-to-End volání se zakládá ze čtyř dial peerů, dva z pohledu přístupu k serveru zdroje a dva z perspektivy přístupu cílového serveru, tak jak zobrazuje obrázek 3.1. Aby bylo možné uskutečnit volání mezi dvěma koncovými zařízeními z libovolné strany a odesílat hlasové pakety tam a zpět, musí být nakonfigurovány všechny čtyři dial peery. Dial peery se používají jen při ustanovení spojení. Jakmile je spojení funkční, dial peer se již nepoužívají.[1]



Obr. 3.1 LLQ operace [1]

Pro VoIP se používají dva typy dial peerů:

- Dial peer POTS - připojují se k tradiční telefonní síti. Ukazují na konkrétní hlasový port, který spojuje okrajovou síť či přístroj a také poskytují adresu (telefonní číslo nebo rozsah čísel) okrajové síti či přístroji. Při konfiguraci dial peeru POTS, je potřeba přidělit telefonní číslo a logické rozhraní.

K tomu se používá příkaz **destination-pattern**, pomocí něj se propojí telefonní číslo s POTS peerem. Pomocí příkazu **port** se spáruje zase konkrétní logické rozhraní s POTS peerem. Volitelná je možnost použít příkaz **direct-inward-dial**, kterým se získají informace o volaném čísle.

- Dial peer VoIP - spojuje se přes síť IP. Přiřazují cílovou adresu ke směrovači v následující etapě nebo cílovému směrovači podle použité technologie. Při konfiguraci dial peeru VoIP se musí nastavit cílové telefonní číslo a cílovou IP adresu. K tomu se používá příkaz **destination-pattern**, který spojí cílové telefonní číslo s VoIP peerem. Příkaz **session target** přiřadí VoIP peeru cílovou IP adresu.

Krok 4 Konfigurace number expansion (rozbalení čísla). Ke konfiguraci se používá příkaz **num-exp** a rozbaluje částečné telefonní číslo na plné telefonní číslo nebo nahrazuje číslo jiným číslem. S volaným číslem manipuluje tabulka rozbalení čísel. Protože k rozbalení čísla dochází před nalezením odpovídajícího odchozího dial peeru tak, aby bylo volání úspěšné, musí se cílový vzor odchozího dial peeru nakonfigurovat pomocí rozbaleného čísla, a nikoli s využitím původního čísla. [1]

Krok 5 Optimalizace dial peeru a konfigurace síťového rozhraní. VoIP dial peer je možné využít k dalším nastavením jako je nastavení kodeku, voice activity detection (VAD) a další parametry QoS (pouze pokud je nastaveno RSVP). Pokud je ovšem RVSP nastaveno, tak je ke konfiguraci možné použít příkazy **req-qos** nebo **acc-qos**, kterými je možné nastavit QoS. Příkazem **codec** se určuje, pomocí jakého kodeku se bude komunikovat. Příkaz **vad** zase zakazuje použití voice activation detection a přenos silence paketů.

Krok 6 Konfigurace hlasových portů. Obecně platí, že příkazem voice-port se definuje určitý voice-port signálního typu. Jsou podporováný následující hlasové signální typy:

- FXS (The Foreign Exchange Station interface) - rozhraní FXS připojuje směrovač nebo přístupový server k zařízením koncových uživatelů, jako jsou telefony, faxy či modemy.
- FXO (Foreign Exchange Office interface) - rozhraní FXO se používá pro trunkované neboli vázaná připojení k CO JTS nebo PBX bez podpory signalizace E&M.
- E&M - trunkové obvody vzájemně propojují telefonní přepínače. Nepřipojují na síť zařízení koncových uživatelů. Nejběžnější formou analogového trunkového obvodu je rozhraní E&M, jež pro přenášení informací o hovo-

rech využívá speciální signalizační cesty oddělené od trunkových hlasových cest.[1]

4 TESTOVÁNÍ NASTAVENÍ

4.1 Vybavení laboratoře

Pro potřeby testování byly zvoleny následující síťové prvky:

- 2x směrovač Cisco Catalyst 2801
- 2x přepínač Cisco Catalyst 2960S
- 2x Cisco IP Phone 7942G
- 4x PC

Jednotlivá zapojení, podle kterých se měření prováděla, jsou zobrazeny v jednotlivých sekcích níže.

V sítích se vyskytovaly různé rychlosti linek. Nejpomalejší provoz byl veden ze směrovačů, které umožňovaly přenosové rychlosti 100Mbps na rozhraních FastEthernet a na sériových linkách byla nastavena rychlost 2Mbps. Přepínače umožňovaly mnohem větší rychlosti a to 1Gbps, případně 10Gbps, která však pro testování nebyla využita. Oba směrovače již disponovaly nejnovější dostupnou verzí IOSu v plné verzi, takže odpadla nutnost instalace IOS s podporou CUCME (Cisco Unified Communications Manager Express). Podle databáze společnosti Cisco (`http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucme/ requirements/guide/33matrix.html`) si můžeme ověřit, že součástí IOSu je CUCME ve verzi 7.0(1), to odpovídá verzi IOSu 12.4(22)T. Dále byly použity IP telefony Cisco 7942G, které pracují s kodeky G.711 μ-law a G.729a.[12]

Aby bylo dosaženo různých stupňů zátěže, tak klienti určitou rychlostí generovaly UDP pakety, které byly odesílány na PC, který sloužil jako server. Počet vláken a se v průběhu měření lišil, protože bylo potřeba ji upravovat podle potřeb zatížení. Využíván byl nástroj iPerf3, který se pro tuto činnost velmi osvědčil a je dostupný z webu: `http://software.es.net/iperf/`

4.2 Metodika testování

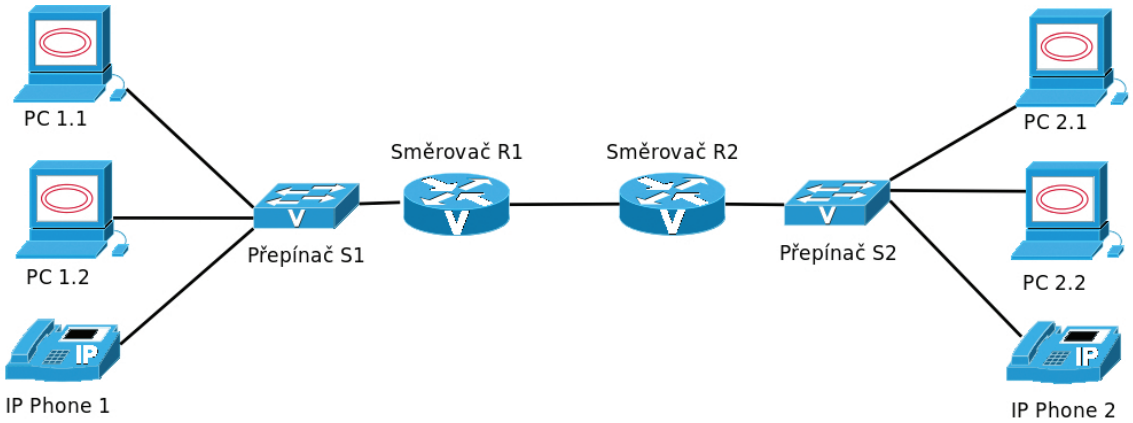
Testování probíhalo tak, že bylo třeba zatížit v kritickém místě síť a sledovat, jaký vliv má zahlcení sítě na kvalitu hovoru při různých nastaveních QoS. Provoz byl v obou typech sítí generován z PC 1.1 a PC 1.2 na PC 2.1. Stejným směrem bylo vyhodnocování hovoru, které probíhalo na IP telefonu 2.

K hodnocení hovorů byla využita metodika MOS LQK, která je součástí softwaru telefonu. Lze ji nalézt v menu, položka Call statistic. Společnost Cisco využívá k hodnocení hovoru proprietární algoritmus CVTQ (Cisco Voice Transmission Quality. Je odvislý od verze MOS LQK a hodnotící stupnice je v souladu s ITU standardem P.564. Tento standard definuje hodnotící metody a přesné výkonnostní cíle, které předpovídají skóre kvality hlasu na základě skutečného zatížení sítě.[13]

Telefony použité k testování disponovaly kodeky G.711 μ-law a G.729r8 a proto byla všechna měření provedena na těchto dvou kodecích.

4.3 Testování QoS na směrovačích Cisco Catalyst 2801

Na obrázku 4.1 je zobrazena testovací topologie zapojení se směrovači. Bylo otestováno řazení do front, které směrovače umožňovaly: FIFO, WFQ, CBWFQ a LLQ. Všechny konfigurace jsou součástí přílohy.



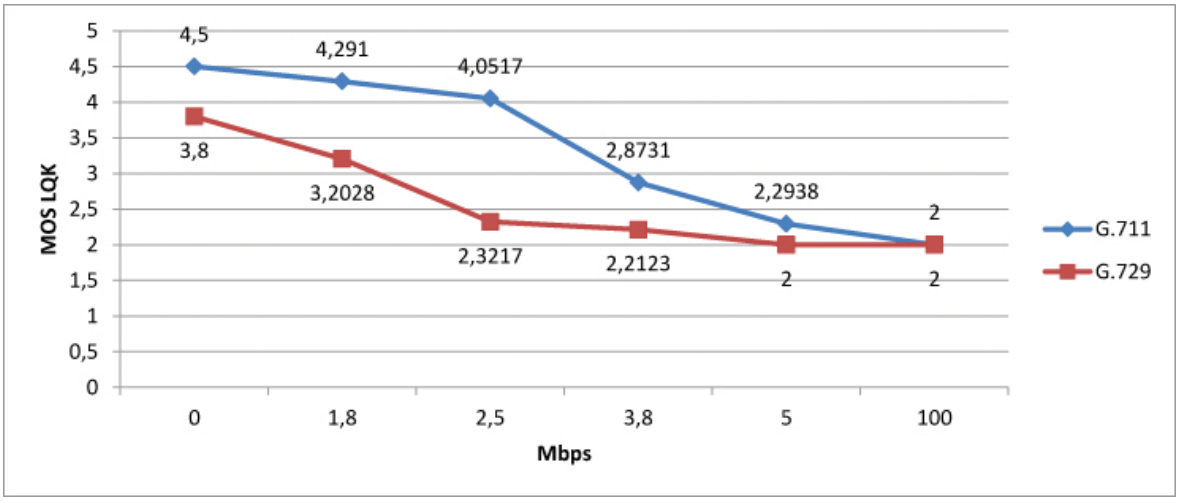
Obr. 4.1 Testovací konfigurace se směrovači

Síť byla rozdělena na dvě části, které byly navzájem propojeny sériovou linkou o kapacitě 2Mbps. Důvodem zvolení tohoto propoje bylo, aby v síti bylo slabé místo, na kterém by bylo možné otestovat chování sítě. Propojení mezi směrovačem a přepínačem umožňovalo rychlost 100Mbps a propojení mezi přepínači a koncovými zařízeními bylo na 1Gbps. Na směrovač R1 byl nastaven CUCME, který se staral o signalizaci.

Dále byl z PC 1.1 a z PC 1.2, které obstarávaly funkci klienta, generován provoz směrem k PC 2.1, který zastával funkci serveru. Kvalita hlasu byla měřena na několika úrovních zatíženích sítě: 0Mbps, 1,8Mbps, 2,5Mbps, 3,7Mbps, 5Mbps a 100Mbps. Při některých měřeních se zátěž sítě drobně odchylovala od stanovených hranic, nicméně na testování to nemělo znatelný vliv.

4.3.1 Měření kvality hovoru při různých nastaveních QoS

FIFO V tomto nastavení byla kvalita služby vypnuta. Cílem byl, jak se chová kvalita hovoru při postupném zatížení sítě, v případě, kdy není aktivní žádný nástroj QoS. Aby bylo možné tuto vlastnost ověřit, bylo nutné nejprve vypnout WFQ, protože se automaticky aktivuje v případě, kdy je šířka pásma rozhraní nižší než 2Mbps. Slouží k tomu příkaz **no fair-queue**.



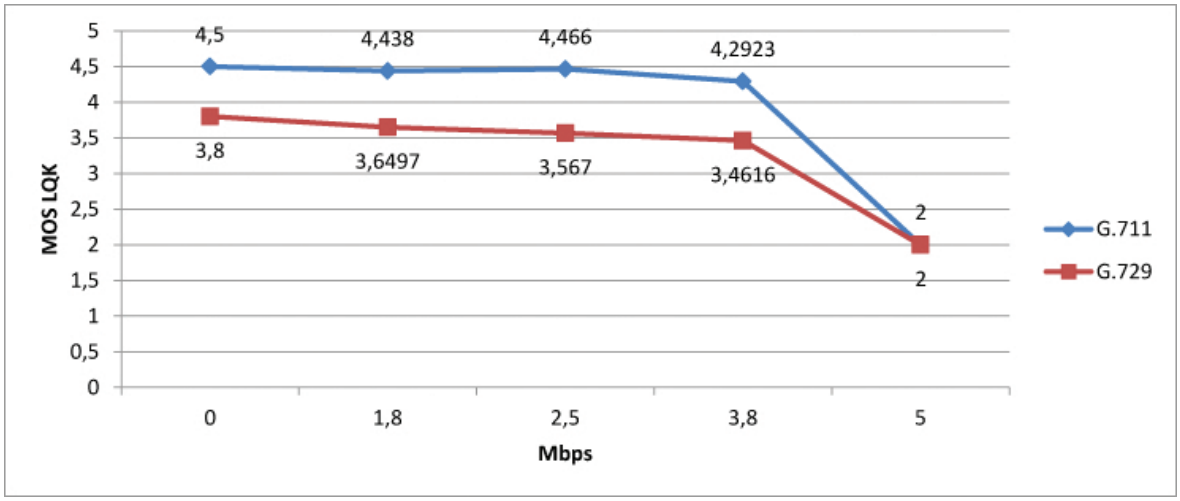
Obr. 4.2 Graf průběhu zátěže sítě při použití FIFO

Z obrázku 4.2 je možné vidět, že se oba kodeky chovají přibližně lineárně, přesně podle předpokladu. Ačkoli kodek G.729 nemá takové nároky na šířku jako kodek G.711, tak překvapivě dosahuje horších výsledků. Překvapující je, že kodek G.711 nemá minimální hodnotu MOS LQK, při zatížení sítě 1,5 násobku kapacity sítě (v tomto případě 3Mbps).

WFQ Dalším testovaným algoritmem bylo WFQ. To se zapíná nad konkrétním rozhraním pomocí příkazu **fair-queue** [congestive-discard-treshold [dynamic-queues [reservable-queues]]], kde congestive-discard-treshold značí hranici, za kterou začne zahazovat pakety agresivnějších toků. Dynamic-queues je hodnota udávající počet dynamický front (hodnota musí být mocninou 2 a v rozsahu 16 až 4096). Reservable-queues značí počet rezervovaných front, například pro protokol RSVP (0 do 1000, výchozí nastavení je 0).

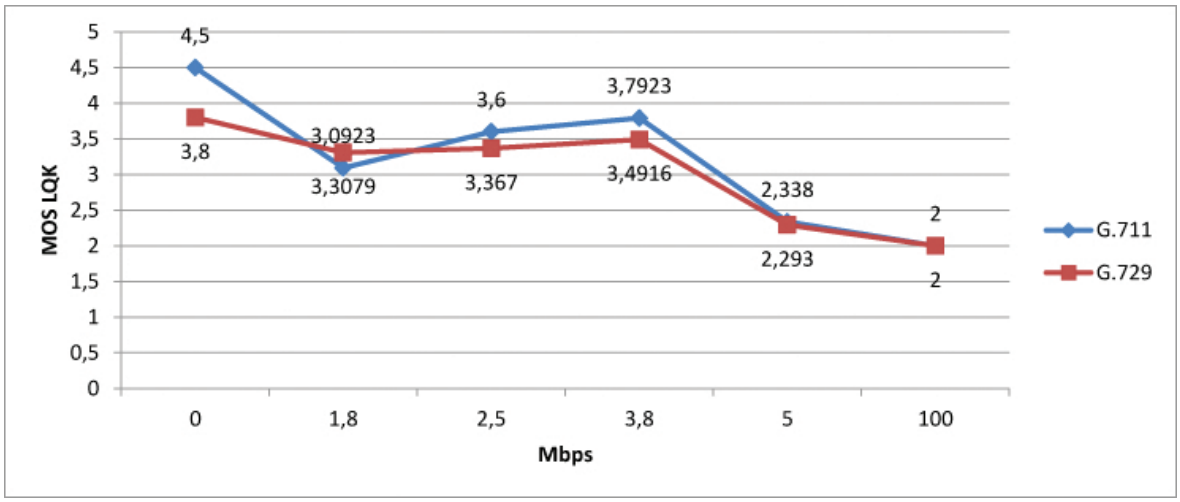
Při prvním testu této fronty, byla zvolena vysoká prahová hodnota, při které se začne se zahazováním paketů. Použit k tomu byl příkaz **fair-queue** 800 256 0. Na obrázku 4.3 je vidět, že při zvolené dostatečně vysoké prahové hodnotě, se pásmo rozdělí férově mezi toky a kvalita hovoru je na velmi dobré úrovni.

U následujícího testu byla pozornost zaměřena na to, jak se bude kvalito hovoru



Obr. 4.3 Graf WFQ při zvolené vysoké prahové hodnotě

chovat, při zvolení nízké prahové hodnoty pro zahazování paketů. Použit byl příkaz **fair-queue** 6 256 0, výsledek zobrazuje obrázek 4.4. Na první pohled se může chování MOS tvářit překvapivě. Nicméně při porovnání s předchozím měřením lze říci, že toto chování způsobuje prahová hodnota, při které jsou pakety zahazovány. Pro ověření správnosti úsudku bylo měření několikrát opakováno vždy se stejným výsledkem.



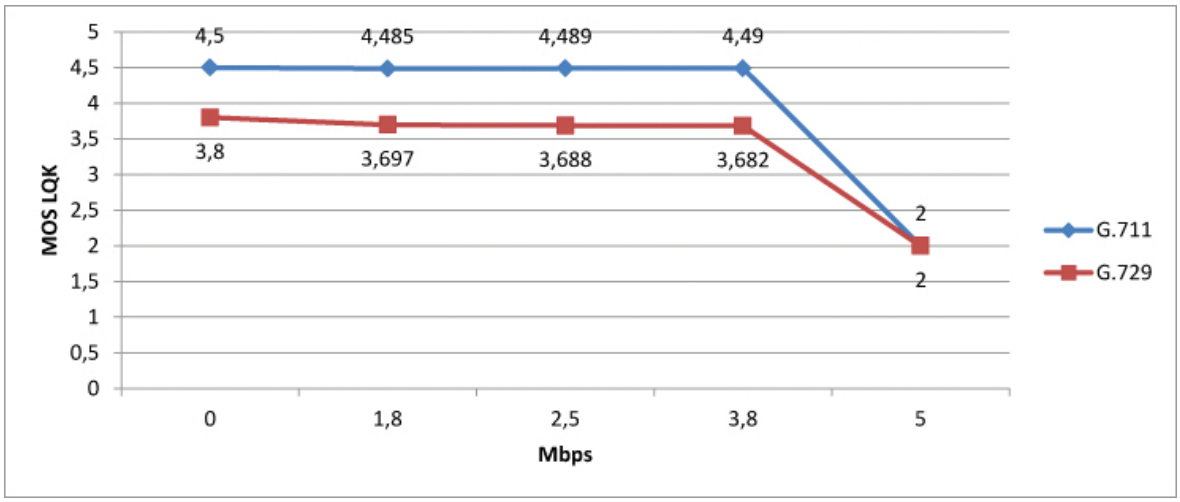
Obr. 4.4 Graf WFQ při zvolené nízké prahové hodnotě

V posledním testovaném nastavení bylo zvoleno minimální množství front, které lze u WFQ nastavit v kombinaci s rozumnou prahovou hodnotou. Použit byl příkaz **fair-queue** 400 16 0. Výsledkem bylo téměř identické chování jako u prvního měření, kdy bylo zvoleno větší množství front a vysoká prahová hodnota. Příčinu v takovémto chování by mohlo být možné hledat v tom, že pro testování byl použit jen jeden styl komunikace. V případě většího množství komunikace by se mohlo stát, že by byly zahazovány i hlasové data, což by mělo negativní vliv na kvalitu hovoru.

Závěrem lze konstatovat, že je důležité správně nastavovat parametry WFQ, protože kombinace všech faktorů má vliv na kvalitu hovoru. Dále do toho promlouvá také typ síťového provoz a bezesporu i jeho množství. Je dobré mít tyto informace na paměti.

CBWFQ V nástroji CBWFQ je pro každou frontu vyhrazena jistá šířka pásma a pro pakety ve výchozí frontě class-default je možné použít původních funkcí WFQ. CBWFQ je rozšířeno o prioritní frontu a konfiguruje se pomocí příkazu **bandwidth**. Pomocí map tříd provádí klasifikaci a pomocí map zásad vytváří množiny tříd, které se nad daným rozhraním mohou používat. CBWFQ nastavujeme podle následujících příkazů: **bandwidth** bandwidth-kpbs | textbfpercent procento, kde lze šířku pásma udávat číselnou hodnotou v kpbs a nebo použít procentuální vyjádření. Příkazem **queue-limit** sezi-of-queue nastavíme maximální délku fronty CBWFQ a příkazem **max-reserved-bandwidth** percent vyjadřujeme procentní podíl šířky pásma, kterou je možné rezervovat pro fronty CBWFQ kromě výchozí fronty class-default (výchozí hodnota 75 procent).

Pro ověření správné funkčnosti CBWFQ byly zvoleny tři případy rezervace šířky pásma pro VoIP. Zarezervováno byly šířky pásma 50kpbs, 250kpbs a 500kpbs. Použit k tomu byl výše zmíněný příkaz **bandwidth**. Výsledek lze vidět na obrázku 4.5.



Obr. 4.5 Graf CBWFQ při rezervaci šířky pásma pro VoIP

Ve všech případech se CBWFQ chovalo očekávaným způsobem a kvalita hovoru byla na vynikajícVšechny konfigurace jsou součástí přílohy.í úrovni.

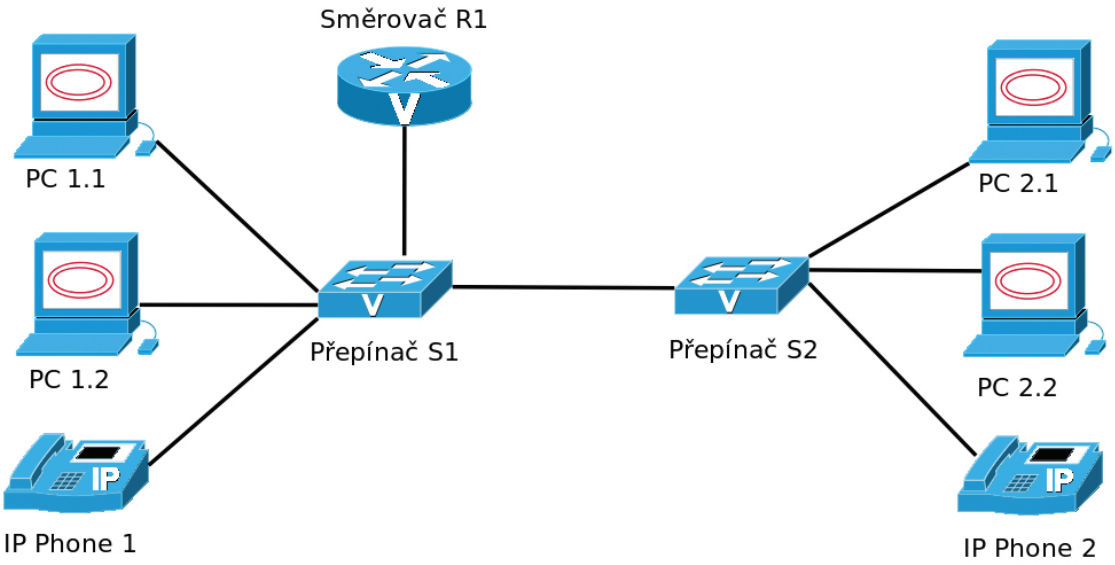
LLQ LLQ je velmi podobné CBWFQ, ale liší se v tom, že místo definování šířky pásma je zde definována priorita. Tudíž místo příkazu **bandwidth** se využívá příkazu

priority.

Opět se zde provedlo stejné měření jako tomu bylo u nástroje CBWFQ. Předpoklad byl takový, že by výsledkem měly být hodnoty MOS shodné s měřením u CBWFQ. Toto očekávání se naplnilo, ale přece jen zde jedna drobná změna byla, a to ta, že díky prioritnímu zpracování je zde o něco menší zpoždění, a proto je vhodnější využití LLQ tak, kde nám záleží na co nejdřívějším doručení.

4.4 Testování QoS na přepínačích Cisco Catalyst 2960S

Na obrázku 4.6 je zobrazena testovací topologie zapojení s přepínači. Testovány byly technologie autoQoS, SRR a vliv velikosti bufferu. Všechny konfigurace jsou součástí přílohy.



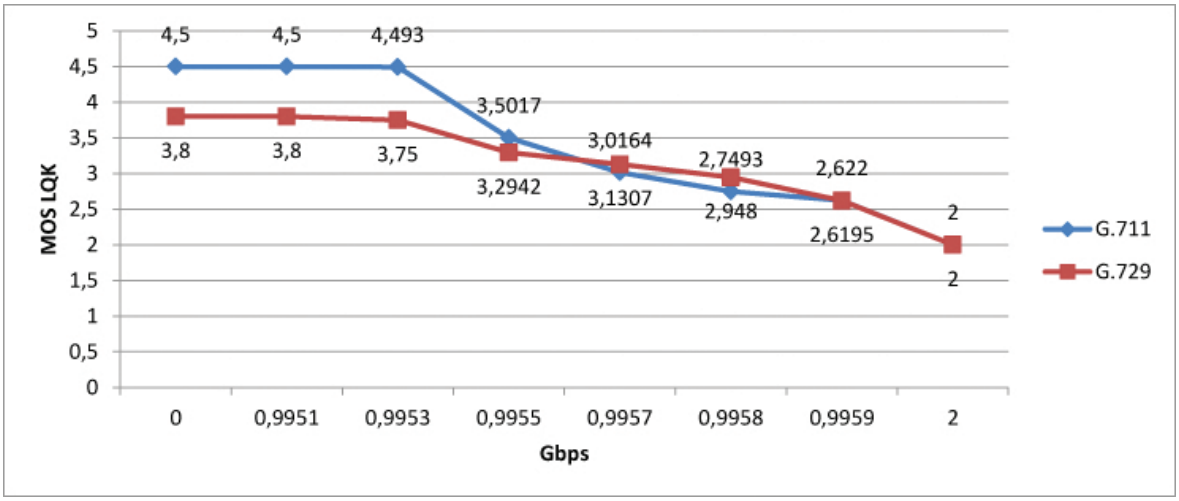
Obr. 4.6 Testovací konfigurace s přepínači

Oproti předchozímu nastavení byla upravena metodiky měření. Jelikož bylo propojení realizováno mezi dvěma přepínači s linkou o rychlosti 1Gbps, bylo třeba upravit nastavení na vypovídající hodnoty. Toho bylo dosaženo testováním a hledáním optimálních odečítacích hodnot. Výsledkem je sada hodnot na hranici kapacity linky (0,9953Gbps), konečná hodnota na stavu 2Gbps a počáteční hodnota na zatížení 0Gbps.

4.4.1 Měření kvality hovoru při různých nastaveních QoS

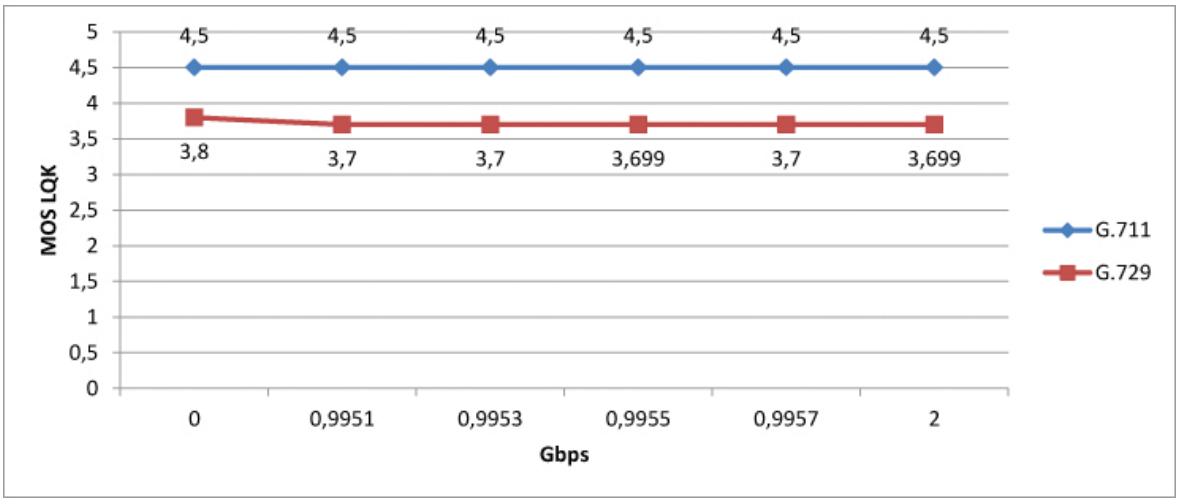
Bez použití QoS U toho nastavení bylo primárním cílem zjistit, jak se chová kvalita hlasu na síti bez všech podpůrných mechanismů, které QoS nabízí. Také si tím zjistit, na jakých hodnotách se začíná kvalita hlasu zhoršovat a určit si tak základ metodiky pro následující měření. Mechanismy QoS lze vypnout jednoduchým příkazem **no mls**

qos. Výsledek měření lze vidět na obrázku 4.7. Z něj je patrné, že se kvalita hovoru začala velmi rychle zhoršovat, když se dosáhlo vytížení kapacity linky na 0,9953Gbps. Při zahlcení linky došlo ke snížení kvality hovoru na nejnižší možnou hodnotu.



Obr. 4.7 Průběh zatížení sítě bez mechanismů QoS

auto QoS nejjednodušší nastavení kvality služeb QoS je aktivování automatického nastavení. Konfiguruje se na konkrétní rozhraní, ke kterému je připojen IP telefon, a to příkazem **auto qos voip cisco-phone**. Dále je třeba také aktivovat rozhraní, které směřuje k dalšímu přepínači, aby se dokázali dohodnout. Slouží k tomu příkaz **auto qos voip trust**. Jak je patrné z obrázku 4.8



Obr. 4.8 Průběh zatížení sítě s nastavením auto QoS

Předpokladem u tohoto nastavení bylo, že se samo nakonfiguruje a bude poskytovat nejvyšší kvalitu přenosu hlasu. Tento předpoklad se splnil a bylo ověřeno i to, že je to vhodný nástroj v případy, kdy si autor konfigurace není zcela jist nastavením nebo se zaobírá velmi specifickými problémy.

SRR SRR je plánovač, který obsluhuje příchozí i výstupní frontu a řídí se podle toho, jakou rychlostí je schopen data odesílat. Je možné určit, jak velkou část dostupné šířky pásma bude přiděleno každé frontě. K nastavení se používají příkazy **srr-queue bandwidth shape** weight1 weight2 weight3 weight4, kde je možné váhy nastavit na hodnoty 0 až 65535 a **srr-queue bandwidth share** weight1 weight2 weight3 weight4, kde je možné váhy nastavit na hodnoty 1 až 255.

V prvním testu byla pozornost zaměřena na chování plánovače, když se použije výchozí nastavení. Podle společnosti Cisco by takovéto nastavení mělo fungovat správně. Použity byly příkazy **srr-queue bandwidth shape** 25 0 0 0 a **srr-queue bandwidth share** 25 25 25 25. Výsledek potvrdil předpoklad, když se zvyšující se zátěží nesnižovala kvalita hovotu, a to ani u jedno kodeku.

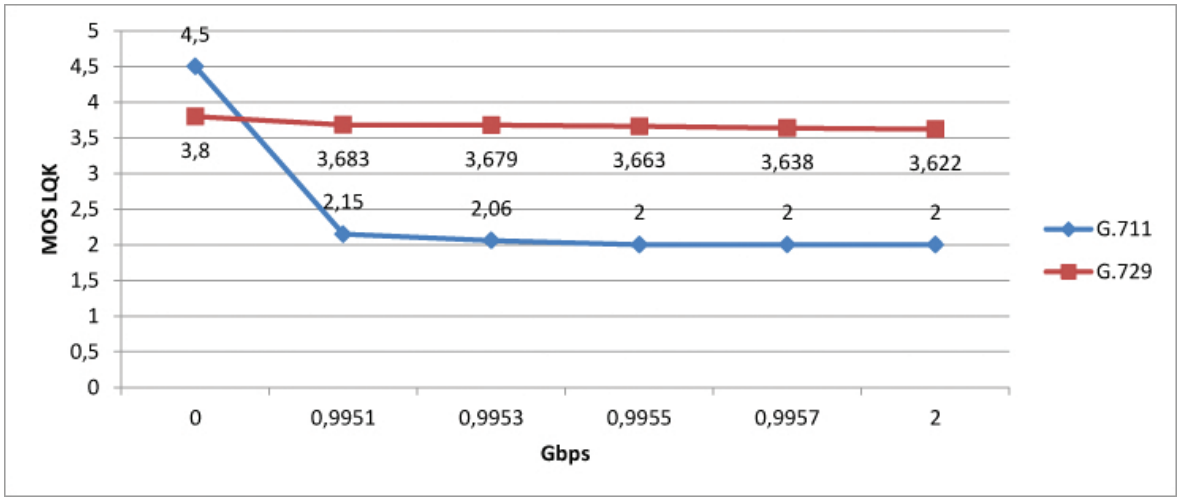
Pro další test bylo použito nastavení, při kterém se snížila šířka pásma na minimum a to jen ve frontě pro VoIP. To znamená, že zůstal zapnutý mód share v konfiguraci **srr-queue bandwidth share** 1 255 255 255 a mód byl vypnutý **srr-queue bandwidth shape** 0 0 0 0.

Tímto testem jsem dostali nejnižší šířku pásma a plánovač se osvědčil, když ve výsledku kvalita hlasu nebyla ani u jednoho kodeku ovlivněna a tudíž měla maximální hodnoty.

Posledním testem bylo nastavení šířky pásma takové, aby se projevilo, který kodek je náročnější na šířku pásma. Je známo, že čím vyšší hodnota váhy, tím nižší šířka pásma je. Zvolilo se experimentálně nastavení fronty následně **srr-queue bandwidth shape** 2830 0 0 0 a **srr-queue bandwidth share** 25 25 25 25.

Na obrázku 4.9 můžeme vidět, že kodek G.729 je méně náročnější na šířku pásma než kodek G.711, který je při tomto nastavení nepoužitelný. Ověřily se tím i uváděné informace v dokumentacích.

Velikost bufferu Další vlastností, kterou lze na testovaném přepínači vyzkoušet je nastavení různých velikostí bufferů. Buffery tvoří v rámci fronty velmi důležitý prvek. Na jejich velikosti závisí parametry jako je zpoždění, jitter a nebo předčasné zahazování paketů. V případě příliš malé fronty hrozí právě rychlé zahazování paketů, a je to způsobeno malým množstvím alokovaných bufferů. Naopak velká fronta bude zhoršovat parametry zpoždění a jitteru.



Obr. 4.9 Test šířky pásma SRR

Na ověření, jak opravdu funguje nastavení byly použity dva testy. V prvním testu se rezervovalo pro prioritní frontu podstatné množství bufferu. To se provede příkazy **mls qos queue-ser output** 1 **buffers** 70 3 17 10, ještě je pořeba určit prioritní frontu, to se provede příkazem **priority-queue out**. V prvním případě jsme rezervovali 70 procent bufferů pro prioritní frontu. V druhém případě se na to šlo opačně, prioritní frontě bylo přiřazeno pouze 1 procento bufferů **mls qos queue-ser output** 1 **buffers** 1 27 12 60.

Výsledek testu v obou případech dopadl tak, že hodnota kvality hlasu MOS byla po celé zatížení na plných hodnotách. Pro kodek G.729 to bylo 3,7 a pro kodek G.711 to bylo 4,5. Důvodem tohoto výsledku pravděpodobně bude to, že se používal pouze jeden hlasový přenos a tudíž nemohlo k výraznému výkyvu dojít.

5 ZHODNOCENÍ VÝSLEDKŮ

Problematika kvality služeb a IP telefonie je velmi rozsáhlé téma. Mnohdy je složité se v tématu kvalitně orientovat, a to zvláště v kontextu velmi rychlého vývoje v oblasti síťových technologií. Přesto ale bylo zjištěno, že kvalita služeb skýtá rozsáhlé možnosti k nastavení sítě tak, aby pracovala podle představ designera. Přesto zde nebylo popsáno vše, co je možné o kvalitě služeb napsat. Byla použita jen malá část problematiky a to jen tolik, aby bylo možné porozumět oblasti nastavování QoS na použitých zařízeních v kombinaci s VoIP.

5.1 Zhodnocení výsledků zapojení na směrovačích

Nastavování QoS na směrovačích Cisco je velmi jednoduché a intuitivní. Je kvalitně popsána dokumentace ke směrovačů, ze kterých lze čerpat dostatek informací pro správné pochopení a nastavení. Byly řešeny konkrétní nastavení pro řazení do front na směrovači Cisco Catalyst 2801. Těmito nastaveními byly techniky FIFO, WFQ, CBWFQ a LLQ. Žádná z použitých technik se nikterak výrazně nevychýlila od očekávaného chování, naopak vše fungovalo hladce a bezchybně. Je důležité nezapomínat na to, aby data náchylná na čas doručení byly umísťovány do prioritní fronty, v opačném případě je možné, že kvalita přenosu dat náchylných na čas doručení nebude uspokojivý. S tím také souvisí, aby zařízení byla dostatečně dimenzována a s ohledem na typ přenosu a umístění zařízení. Předejde se tak pozdějším problémům se zahlcením.

Směrovače umožňují nastavení technik, které předcházení zahlcení sítě. Jsou jimi RED a WRED, ale pracují s pakety typu TCP, kdežto IP telefonie pracuje s pakety typu UDP. Proto nebyly tyto techniky do testování zařazeny.

Také bylo vynechána automatická konfigurace, to z toho důvodu, že se velmi podobá nastavením LLQ a CBWFQ. Všechna nastavení je možné si prohlédnout v příloze.

5.2 Zhodnocení výsledků zapojení na přepínačích

Tak jako na směrovačích, tak také na přepínačích je konfigurace intuitivní, ale o něco komplikovanější. Některé příkazy obsahují veliké množství proměnných a není problém se v konfiguraci ztratit a nebo něco přehlédnout. Zde proto oceníme možnost automatické konfigurace (autoQoS), která disponuje velmi obstojnými výsledky. Vše ale funguje tak jak se od toho očekává a velice svižně. Pro testování byly zvoleny přepínače Cisco Catalyst 2960S, které disponují gigabitovými linkami. To mělo svůj vliv i na měření, která nebyla tolik průkazná při vedení pouze jediného hlasového hovoru. Šířka pásma, které hlasové kodeky potřebují pro přenos se pohybuje v řádech kilobitů

za sekundu. Přesto bylo možné ověřit chování přepínačů v dostatečné míře. K testování byly zvoleny techniky automatického nastavení QoS, vliv velikosti bufferu a SRR. Opět i zde platí, nezapomínat na nastavení časově citlivých dat do prioritní fronty.

ZÁVĚR

Tato práce se zaměřila na možnosti kvality služeb u přepínačů a směrovačů společnosti Cisco v kombinaci s VoIP. Cílem bylo ověřit získané informace na konkrétních zařízeních a jaký vliv mají různá nastavení na IP telefonii.

V teoretické části byly popsány základní pojmy kvality služeb, které mají přímý vliv na kvalitu přenosu hlasu. Dále byly představeny techniky, které zařízení používají pro práci s frontami. V projektové části byly získané informace otestovány na zařízeních společnosti Cisco. Zkoumán byl vliv jednotlivých nastavení na průběh hlasového hovoru. Použity byly dvě schémata zapojení, jedno schéma dělilo síť na dvě části oddělené sériovou linkou, která tvořila úzké hrdlo a druhé schéma bylo zapojení s dvěma přepínači a jedním směrovačem do jedné sítě. Výsledky byly uspokojivé a dá se říci, že odpovídaly předpokladům.

Během práce nedošlo k žádným výraznějším obtížím, které by nebylo možné uspokojivě vyřešit. Touto prací jsem si rozšířil své znalosti z oblasti síťových technologií právě o část kvality služeb a IP telefonii. Dříve jsem neměl možnost se k této problematice blíže dostat a tudíž byla diplomová práce velmi podnětná a zajímavá.

ZÁVĚR V ANGLIČTINĚ

This thesis has focused on the possibility of quality of services on Cisco switches and routers combined with VoIP. The goal was to verify the information on specific devices and what impact they have different settings for voice over IP.

In the theoretical part was described the basic concepts of quality of services that have a direct impact on the quality of voice transmission. Furthermore, techniques were introduced that use the device to work with queues. The project part was the information tested on Cisco equipment. We examined the influence of individual settings on the progress of a voice call. Used were two diagrams, one diagram network divided into two parts separated of serial interface, which formed a narrow neck and a second scheme was wired with two switches and one router in a network. The results were satisfactory and we can say that corresponded to expectations.

During the work, there were no significant problems which could not be satisfactorily resolved. This work, I expanded my knowledge of networking technologies just part of the quality of service and voice over IP. Previously, I was not able to get closer to this issue and therefore thesis was very inspiring and interesting.

SEZNAM POUŽITÉ LITERATURY

[1] WALLACE, Kevin. *Cisco VoIP: autorizovaný výukový průvodce.* Vyd. 1. Brno: Computer Press, 2009, 527 s. Samostudium. ISBN 978-80-251-2228-0.

[2] HUCABY, Dave, Steve MCQUERRY, Andrew WHITAKER a Dave HUCABY. *Cisco router configuration handbook.* 2nd ed. Indianapolis, IN: Cisco Press, c2010, xxii, 641 p. ISBN 1587141167.

[3] MCQUERRY, Steve, David JANSEN a Dave HUCABY. *Cisco LAN switching configuration handbook.* 1st print. Indianapolis: Cisco Press, c2009, xx, 333 s. ISBN 9781587056109.

[4] ODOM, Wendell, Rus HEALY a Naren MEHTA. *Směrování a přepínání sítí: autorizovaný výukový průvodce.* Vyd. 1. Brno: Computer Press, 2009, 879 s. Samostudium. ISBN 978-80-251-2520-5.

[5] LAMMLE, Todd. *CCNA: výukový průvodce přípravou na zkoušku 640-802.* Vyd. 1. Brno: Computer Press, 2010, 928 s. ISBN 978-80-251-2359-1.

[6] ODOM, Wendell a Michael J CAVANAUGH. *Cisco DQOS exam certification guide: IP telephony self-study.* Indianapolis, IN: Cisco Press, c2004, xxxvi, 900 p. ISBN 1587200589.

[7] FROEHLICH, Andrew. *CCNA voice: study guide.* 1st ed. Indianapolis, Ind.: Wiley Technology, c2010, xli, 602 p.

[8] HUCABY, Dave. *CCNP SWITCH 642-813 official certification guide.* Indianapolis, Ind.: CISCO Press, c2010, xxvii, 460 s. Official certification guide series. ISBN 9781587202438.

[9] *Cisco IOS Quality of Service Solutions Configuration Guide* [online]. 2009. 12.2SR. Cisco Systems. [cit. 2015-05-10]. Dostupné z: `http://www.cisco.com/c/en/us/td/docs/ios/qos/configuration/guide/12_2sr/qos_12_2sr_book.pdf`

[10] *Implementing Cisco Quality of Service: Student Guide.* 2006. Version 2.2. 698 s. CISCO SYSTEMS. [cit. 2015-05-10].

[11] *Quality of Service for Voice over IP.* 2001. Www.cisco.com [online]. [cit. 2015-05-12]. Dostupné z: `http://www.cisco.com/c/en/us/td/docs/ios/solutions_docs/qos_solutions/QoSVoIP/QoSVoIP.html`

[12] *Cisco Unified IP Phone 7942G.* Www.cisco.com [online]. [cit. 2015-05-12]. Dostupné z: http://www.cisco.com/c/en/us/products/collateral/collaboration-endpoints/unified-ip-phone-7942g/product_data_sheet0900aecd8069bb68.html

[13] *Cisco Unified IP Phone 7962G and 7942G Administration Guide for Cisco Unified Communications Manager 6.0* . Www.cisco.com [online]. [cit. 2015-05-12]. Dostupné z: http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cuipph/7962g_7942g/6_0/english/administration/guide/7962G-Admin-Book-Wrapper.pdf

[14] *Catalyst 2960 and 2960-S Switches Software Configuration Guide.* Www.cisco.com [online]. Release 15.0(1)SE. [cit. 2015-05-12]. Dostupné z: http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst2960/software/release/15-0_1_se/configuration/guide/scg2960.pdf

[15] *Cisco IOS Voice, Video, and Fax Configuration Guide.* Www.cisco.com [online]. Release 12.2. [cit. 2015-05-12]. Dostupné z: http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst2960/software/release/15-0_1_se/configuration/guide/scg2960.pdf

[16] WALLACE, Kevin. *CCNP TSHOOT 642-832 official certification guide.* Indianapolis, IN: Cisco Press, c2010, xxvii, 508 s. Official certification guide series. ISBN 9781587058448.

[17] GOUGH, Clare. *Cisco CCNP routing exam certification guide.* Indianapolis, IN: Cisco, c2001, xxiv, 826 p. ISBN 1587200015.

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

QoS	Quality of Service
VIP	Versatile Interface Processors
OSI	Referrční Model ISO/OSI
CIR	Committed Information Rate
DTE	Data Terminal Equipment
VC	Virtual Circuit
CAC	Call Admission Control
VoIP	Voice over IP
IP	Internet Protocol
FIFO	First In First Out
BER	Bit Error Rate
RED	Random Early Detection
TCP	Transmission Control Protocol
RTP	Real-time Transport Protocol
FRTS	Frame Relax Traffic Shaping
CoS	Class of Service
WFQ	Weighted Fair Queueing
DWFQ	Distributed Weighted Fair Queueing
CBWFQ	Class-Based Weighted Fair Queueing
DCBWFQ	Distributed Class-Based Weighted Fair Queueing
ATM	Asynchronous Transfer Mode
WAN	Wide Area Network
LLQ	Low Latency Queuing
UDP	User Datagram Protocol
MLP	Multiling PPP
PPP	Point to Poing Protocol
RSVP	Resource Reservation Protocol
DE	Discard Eligibility
LAN	Local Area Network
VLAN	Virtual LAN
TOS	Type Of Service
ISL	Inter-Switch Link
IPP	IP Precedence
DSCP	Differentiated Services Code Point
DS	Differentiated Services
ECN	Explicit Congestion Notification
PQ	Priority Queuing

RR	Round Robin
WRR	Weighted Round Robin
DRR	Deficit Round Robin
CQ	Custom Queuing
FTP	File Transfer Protocol
ACL	Access Control List
MQC	Modular QoS CLI
WRED	Weighted Random Early Detection
MPD	Mark Probability Denominator
MOS	Mean Opinion Score
PSQM	Perceptual Speech Quality Measurement
PESQ	Perceptual Evaluation of Speech Quality
SNMP	Simple Network Management Protocol
PAMS	Perceptual Analysis Measurement System
VAD	Voice Activity Detection
FXS	The Foreign Exchange Station
FXO	Foreign Exchange Office
PC	Personal Computer
CUCME	Cisco Unified Communications Manager Express
CVTQ	Cisco Voice Transmission Quality
SRR	Shaped Round Robin

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM PŘÍLOH

PŘÍLOHA P I. ZÁKLADNÍ KONFIGURACE PŘI TESTOVÁNÍ NA SMĚROVAČÍCH

1.1 Směrovač R1

```
version 12.4
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname R1
!
ip dhcp excluded-address 192.168.30.1 192.168.30.10
!
ip dhcp pool IP_Phones
 network 192.168.30.0 255.255.255.0
 default-router 192.168.30.1
 option 150 ip 192.168.30.1
!
ip cef
no ipv6 cef
!
spanning-tree mode pvst
!
class-map match-any voip
 match dscp ef
 match ip precedence 5
 match precedence 5
 match ip dscp ef
!
interface FastEthernet0/0
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface FastEthernet0/1
 ip address 192.168.2.1 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet0/1.20
 encapsulation dot1Q 20
 ip address 192.168.20.1 255.255.255.0
!
interface FastEthernet0/1.30
 encapsulation dot1Q 30
 ip address 192.168.30.1 255.255.255.0
!
interface Serial0/1/0
 ip address 192.168.1.1 255.255.255.0
 clock rate 2000000
!
interface Serial0/1/1
 no ip address
 clock rate 2000000
!
interface Vlan1
 no ip address
 shutdown
!
router rip
!
ip classless
ip route 192.168.31.0 255.255.255.0 192.168.1.2
ip route 192.168.21.0 255.255.255.0 192.168.1.2
ip route 0.0.0.0 0.0.0.0 192.168.1.2
!
ip flow-export version 9
!
telephony-service
 max-ephones 5
```

```
 max-dn 5
 ip source-address 192.168.30.1 port 2000
!
ephone-dn 1
 number 2001
!
ephone-dn 2
 number 2002
!
ephone 1
 device-security-mode none
 mac-address A418.7528.465B
 button 1:1
!
ephone 2
 device-security-mode none
 mac-address 0CD9.9690.9D5E
 button 1:2
!
line con 0
!
line aux 0
!
line vty 0 4
 login
!
end
```

1.2 Směrovač R2

```
version 12.4
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname R2
!
ip dhcp excluded-address 192.168.31.1 192.168.31.10
!
ip dhcp pool IP_Phones
 network 192.168.31.0 255.255.255.0
 default-router 192.168.31.1
 option 150 ip 192.168.30.1
!
ip cef
no ipv6 cef
!
spanning-tree mode pvst
!
interface FastEthernet0/0
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface FastEthernet0/1
 ip address 192.168.3.1 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet0/1.20
 encapsulation dot1Q 20
 ip address 192.168.21.1 255.255.255.0
!
interface FastEthernet0/1.21
 no ip address
!
interface FastEthernet0/1.30
 encapsulation dot1Q 30
 ip address 192.168.31.1 255.255.255.0
!
interface Serial0/1/0
 ip address 192.168.1.2 255.255.255.0
!
interface Serial0/1/1
```

```
 no ip address
 clock rate 2000000
 shutdown
!
interface Vlan1
 no ip address
 shutdown
!
ip classless
ip route 0.0.0.0 0.0.0.0 192.168.1.1
ip route 192.168.30.0 255.255.255.0 192.168.1.1
ip route 192.168.20.0 255.255.255.0 192.168.1.1
!
ip flow-export version 9
!
line con 0
!
line aux 0
!
line vty 0 4
 login
!
end
```

1.3 Přepínač S1

```
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname S1
!
spanning-tree mode pvst
!
interface GigabitEthernet1/0/1
 switchport mode trunk
!
interface GigabitEthernet1/0/2
 switchport access vlan 20
!
interface GigabitEthernet1/0/3
 switchport voice vlan 30
!
interface GigabitEthernet1/0/4
 switchport access vlan 20
!
interface GigabitEthernet1/0/5
!
interface GigabitEthernet1/0/6
!
interface GigabitEthernet1/0/7
!
interface GigabitEthernet1/0/8
!
interface GigabitEthernet1/0/9
!
interface GigabitEthernet1/0/10
!
interface GigabitEthernet1/0/11
!
interface GigabitEthernet1/0/12
!
interface GigabitEthernet1/0/13
!
interface GigabitEthernet1/0/14
!
interface GigabitEthernet1/0/15
!
interface GigabitEthernet1/0/16
!
interface GigabitEthernet1/0/17
!
interface GigabitEthernet1/0/18
```

```
!
interface GigabitEthernet1/0/19
!
interface GigabitEthernet1/0/20
!
interface GigabitEthernet1/0/21
!
interface GigabitEthernet1/0/22
!
interface GigabitEthernet1/0/23
!
interface GigabitEthernet1/0/24
!
interface GigabitEthernet1/0/25
!
interface GigabitEthernet1/0/26
!
interface TenGigabitEthernet1/0/1
!
interface TenGigabitEthernet1/0/2
!
interface Vlan1
 no ip address
 shutdown
!
line con 0
!
line vty 0 4
 login
line vty 5 15
 login
!
end
```

1.4 Přepínač S2

```
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname S2
!
spanning-tree mode pvst
!
interface GigabitEthernet1/0/1
 switchport mode trunk
!
interface GigabitEthernet1/0/2
 switchport access vlan 20
!
interface GigabitEthernet1/0/3
 switchport voice vlan 30
!
interface GigabitEthernet1/0/4
 switchport access vlan 20
!
interface GigabitEthernet1/0/5
!
interface GigabitEthernet1/0/6
!
interface GigabitEthernet1/0/7
!
interface GigabitEthernet1/0/8
!
interface GigabitEthernet1/0/9
!
interface GigabitEthernet1/0/10
!
interface GigabitEthernet1/0/11
!
interface GigabitEthernet1/0/12
!
interface GigabitEthernet1/0/13
```

```
!
interface GigabitEthernet1/0/14
!
interface GigabitEthernet1/0/15
!
interface GigabitEthernet1/0/16
!
interface GigabitEthernet1/0/17
!
interface GigabitEthernet1/0/18
!
interface GigabitEthernet1/0/19
!
interface GigabitEthernet1/0/20
!
interface GigabitEthernet1/0/21
!
interface GigabitEthernet1/0/22
!
interface GigabitEthernet1/0/23
!
interface GigabitEthernet1/0/24
!
interface GigabitEthernet1/0/25
!
interface GigabitEthernet1/0/26
!
interface TenGigabitEthernet1/0/1
!
interface TenGigabitEthernet1/0/2
!
interface Vlan1
 no ip address
 shutdown
!
line con 0
!
line vty 0 4
 login
line vty 5 15
 login
!
end
```

2.1 Směrovač R1

```
version 12.4
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname R1
!
ip dhcp excluded-address 192.168.30.1 192.168.30.10
!
ip dhcp pool IP_Phones
 network 192.168.30.0 255.255.255.0
 default-router 192.168.30.1
 option 150 ip 192.168.30.1
!
ip cef
no ipv6 cef
!
spanning-tree mode pvst
!
class-map match-any voip
 match dscp ef
 match ip precedence 5
 match precedence 5
 match ip dscp ef
!
!
interface FastEthernet0/1
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface FastEthernet0/1.10
 encapsulation dot1Q 10
 ip address 192.168.10.1 255.255.255.0
!
interface Serial0/1/0
 no ip address
 clock rate 2000000
!
interface Serial0/1/1
 no ip address
 clock rate 2000000
!
interface Vlan1
 no ip address
 shutdown
!
ip flow-export version 9
!
telephony-service
 max-ephones 5
 max-dn 5
 ip source-address 192.168.30.1 port 2000
!
ephone-dn 1
 number 2001
!
ephone-dn 2
 number 2002
!
ephone 1
 device-security-mode none
 mac-address A418.7528.465B
 button 1:1
!
ephone 2
 device-security-mode none
 mac-address 0CD9.9690.9D5E
 button 1:2
!
```

```
line con 0
!
line aux 0
!
line vty 0 4
 login
!
end
```

2.2 Přepínač S1

```
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname S1
!
spanning-tree mode pvst
!
mls qos map cos-dscp 0 8 16 24 32 46 48 56
!
vlan internal allocation policy ascending
!
interface GigabitEthernet1/0/1
 switchport mode  encapsulation dot1q
!
interface GigabitEthernet1/0/2
 switchport access vlan 20
!
interface GigabitEthernet1/0/3
 switchport voice vlan 30
!
interface GigabitEthernet1/0/4
 switchport access vlan 20
!
interface GigabitEthernet1/0/5
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface GigabitEthernet1/0/6
!
interface GigabitEthernet1/0/7
!
interface GigabitEthernet1/0/8
!
interface GigabitEthernet1/0/9
!
interface GigabitEthernet1/0/10
!
interface GigabitEthernet1/0/11
!
interface GigabitEthernet1/0/12
!
interface GigabitEthernet1/0/13
!
interface GigabitEthernet1/0/14
!
interface GigabitEthernet1/0/15
!
interface GigabitEthernet1/0/16
!
interface GigabitEthernet1/0/17
!
interface GigabitEthernet1/0/18
!
interface GigabitEthernet1/0/19
!
interface GigabitEthernet1/0/20
!
interface GigabitEthernet1/0/21
!
interface GigabitEthernet1/0/22
```

```
!
interface GigabitEthernet1/0/23
!
interface GigabitEthernet1/0/24
!
interface GigabitEthernet1/0/25
!
interface GigabitEthernet1/0/26
!
interface TenGigabitEthernet1/0/1
!
interface TenGigabitEthernet1/0/2
!
interface Vlan1
 no ip address
 shutdown
!
line con 0
!
line vty 0 4
 login
line vty 5 15
 login
!
end
```

2.3 Přepínač S2

```
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname S2
!
spanning-tree mode pvst
!
interface GigabitEthernet1/0/1
!
interface GigabitEthernet1/0/2
 switchport access vlan 20
!
interface GigabitEthernet1/0/3
 switchport voice vlan 30
!
interface GigabitEthernet1/0/4
 switchport access vlan 20
!
interface GigabitEthernet1/0/5
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface GigabitEthernet1/0/6
!
interface GigabitEthernet1/0/7
!
interface GigabitEthernet1/0/8
!
interface GigabitEthernet1/0/9
!
interface GigabitEthernet1/0/10
!
interface GigabitEthernet1/0/11
!
interface GigabitEthernet1/0/12
!
interface GigabitEthernet1/0/13
!
interface GigabitEthernet1/0/14
!
interface GigabitEthernet1/0/15
!
interface GigabitEthernet1/0/16
```

```
!
interface GigabitEthernet1/0/17
!
interface GigabitEthernet1/0/18
!
interface GigabitEthernet1/0/19
!
interface GigabitEthernet1/0/20
!
interface GigabitEthernet1/0/21
!
interface GigabitEthernet1/0/22
!
interface GigabitEthernet1/0/23
!
interface GigabitEthernet1/0/24
!
interface GigabitEthernet1/0/25
!
interface GigabitEthernet1/0/26
!
interface TenGigabitEthernet1/0/1
!
interface TenGigabitEthernet1/0/2
!
interface Vlan1
 no ip address
 shutdown
!
line con 0
!
line vty 0 4
 login
line vty 5 15
 login
!
end
```

3.1 Auto QoS

```
 class-map match-any AutoQoS-VoIP-RTP-Trust
  match ip dscp ef
 class-map match-any AutoQoS-VoIP-Control-Trust
  match ip dscp cs3
  match ip dscp af31
!
policy-map AutoQoS-Policy-Trust
class AutoQoS-VoIP-RTP-Trust
 priority percent 70
class AutoQoS-VoIP-Control-Trust
 bandwidth percent 5
class class-default
 fair-queue
!
interface Serial0/1/0
 bandwidth 2000
 ip address 192.168.1.1 255.255.255.0
 auto qos voip trust
 clock rate 2000000
```

3.2 CBWFQ

```
class-map match-any voip
 match dscp ef
 match ip precedence 5
 match precedence 5
 match ip dscp ef
!
policy-map voip_map
 class voip
  bandwidth 250
 class class-default
  bandwidth 500
!
interface Serial0/1/0
 bandwidth 2000
 ip address 192.168.1.1 255.255.255.0
 clock rate 2000000
!
service-policy output voip_map
```

4.1 Auto QoS

```
mls qos map policed-dscp 24 26 46 to 0
!
mls qos map cos-dscp 0 8 16 24 32 46 48 56
!
no mls qos srr-queue input bandwidth 90 10
no mls qos srr-queue input threshold 1 8 16
no mls qos srr-queue input threshold 2 34 66
no mls qos srr-queue input buffers 67 33
no mls qos srr-queue input cos-map queue 1 threshold 2 1
no mls qos srr-queue input cos-map queue 1 threshold 3 0
no mls qos srr-queue input cos-map queue 2 threshold 1 2
no mls qos srr-queue input cos-map queue 2 threshold 2 4 6 7
no mls qos srr-queue input cos-map queue 2 threshold 3 3 5
no mls qos srr-queue input dscp-map queue 1 threshold 2 9 10 11 12 13 14 15
no mls qos srr-queue input dscp-map queue 1 threshold 3 0 1 2 3 4 5 6 7
no mls qos srr-queue input dscp-map queue 1 threshold 3 32
no mls qos srr-queue input dscp-map queue 2 threshold 1 16 17 18 19 20 21 22 23
no mls qos srr-queue input dscp-map queue 2 threshold 2 33 34 35 36 37 38 39 48
no mls qos srr-queue input dscp-map queue 2 threshold 2 49 50 51 52 53 54 55 56
no mls qos srr-queue input dscp-map queue 2 threshold 2 57 58 59 60 61 62 63
no mls qos srr-queue input dscp-map queue 2 threshold 3 24 25 26 27 28 29 30 31
no mls qos srr-queue input dscp-map queue 2 threshold 3 40 41 42 43 44 45 46 47
!
mls qos srr-queue output cos-map queue 1 threshold 3 5
mls qos srr-queue output cos-map queue 2 threshold 3 3 6 7
mls qos srr-queue output cos-map queue 3 threshold 3 2 4
mls qos srr-queue output cos-map queue 4 threshold 2 1
mls qos srr-queue output cos-map queue 4 threshold 3 0
!
mls qos srr-queue output dscp-map queue 1 threshold 3 40 41 42 43 44 45 46 47
mls qos srr-queue output dscp-map queue 2 threshold 3 24 25 26 27 28 29 30 31
mls qos srr-queue output dscp-map queue 2 threshold 3 48 49 50 51 52 53 54 55
mls qos srr-queue output dscp-map queue 2 threshold 3 56 57 58 59 60 61 62 63
mls qos srr-queue output dscp-map queue 3 threshold 3 16 17 18 19 20 21 22 23
mls qos srr-queue output dscp-map queue 3 threshold 3 32 33 34 35 36 37 38 39
mls qos srr-queue output dscp-map queue 4 threshold 1 8
mls qos srr-queue output dscp-map queue 4 threshold 2 9 10 11 12 13 14 15
mls qos srr-queue output dscp-map queue 4 threshold 3 0 1 2 3 4 5 6 7
!
mls qos queue-set output 1 threshold 1 138 138 92 138
mls qos queue-set output 1 threshold 2 138 138 92 400
mls qos queue-set output 1 threshold 3 36 77 100 318
mls qos queue-set output 1 threshold 4 20 50 67 400
!
mls qos queue-set output 2 threshold 1 149 149 100 149
mls qos queue-set output 2 threshold 2 118 118 100 235
mls qos queue-set output 2 threshold 3 41 68 100 272
mls qos queue-set output 2 threshold 4 42 72 100 242
!
mls qos queue-set output 1 buffers 10 10 26 54
mls qos queue-set output 2 buffers 16 6 17 61
mls qos
!
class-map match-all AutoQoS-VoIP-RTP-Trust
 match ip dscp ef
class-map match-all AutoQoS-VoIP-Control-Trust
 match ip dscp cs3 af31
!
policy-map AutoQoS-Police-CiscoPhone
class AutoQoS-VoIP-RTP-Trust
 set dscp ef
 police 320000 8000 exceed-action policed-dscp-transmit
class AutoQoS-VoIP-Control-Trust
 set dscp cs3
 police 32000 8000 exceed-action policed-dscp-transmit
!
```

```
interface GigabitEthernet1/0/3
srr-queue bandwidth share 10 10 60 20
  priority-queue out
mls qos trust device cisco-phone
mls qos trust cos
auto qos voip cisco-phone
  service-policy input AutoQoS-Police-CiscoPhone
!
interface GigabitEthernet1/0/5
srr-queue bandwidth share 10 10 60 20
 priority-queue out
mls qos trust cos
auto qos voip trust
```

4.2 SRR

```
mls qos queue-set output 1 buffers 10 10 20 60
!
mls qos queue-set output 1 buffers 10 10 26 54
mls qos queue-set output 2 buffers 16 6 17 61
!
interface GigabitEthernet1/0/3
mls qos trust device cisco-phone
mls qos trust cos
!
interface GigabitEthernet1/0/5
mls qos trust cos
 srr-queue bandwidth shape 2830 0 0 0
 srr-queue bandwidth share 25 25 25 25
 queue-set 1
 no priority-queue out
```

4.3 Test bufferů

```
mls qos queue-set output 1 buffers 70 3 17 10
!
mls qos queue-set output 1 threshold 1 100 100 100 100
mls qos queue-set output 1 threshold 4 100 100 100 100
!
interface GigabitEthernet1/0/3
mls qos trust device cisco-phhone
mls qos trust cos
!
interface GigabitEthernet1/0/5
mls qos trust cos
srr-queue bandwidth shape 4 4 4 4
queue-set 1
priority-queue out
```