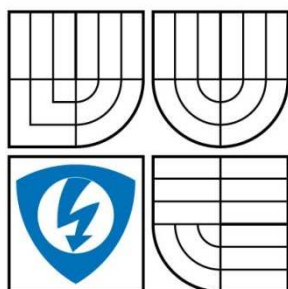


VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY



FAKULTA ELEKTROTECHNIKY A KOMUNIKACNÍCH
TECHNOLOGIÍ
ÚSTAV TELEKOMUNIKACÍ

FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION
DEPARTMENT OF TELECOMMUNICATIONS

MECHANISMY ZAJIŠTENÍ KVALITY SLUŽEB V PEVNÝCH, BEZDRÁTOVÝCH A MOBILNÍCH DATOVÝCH SÍTÍCH

MECHANISMS OF QOS ASSURANCE IN FIXED, WIRELESS AND MOBILE DATA NETWORKS

BAKALÁŘSKÁ PRÁCE
BACHELOR'S THESIS

AUTOR PRÁCE
AUTHOR

RADOVAN VÁCLAVEK

VEDOUCÍ PRÁCE
SUPERVISOR

ING. KAROL MOLNÁR PH.D

BRNO 2008

Bakalářská práce

bakalářský studijní obor
Teleinformatika

Student: Václavek Radovan
Ročník: 3

ID: 74560
Akademický rok: 2007/08

NÁZEV TÉMATU:

Mechanismy zajištění kvality služeb v pevných, bezdrátových a mobilních datových sítích

POKYNY PRO VYPRACOVÁNÍ:

Seznamte se s mechanismy zajištění kvality služeb, které se využívají na úrovni linkové vrstvy v technologiích pro pevné (Ethernet + 802.1Q, 802.1D), bezdrátové (802.11a/b/g + 802.11e) a WiMAX. Porovnejte jednotlivé mechanismy a identifikujte společné vlastnosti a odlišnosti mezi různými řešeními. Na základě získaných informací navrhnete konverzní procedury mezi vlastnostmi, které nejsou přímo dostupné u jiných technologií. Pokud možnost přímé automatické konverze neexistuje, specifikujte potřebné parametry, které je nutné znát k zajištění obdobného chování u cílového mechanismu QoS. Navržené konverzní mechanismy podrobně zdokumentujte.

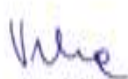
DOPORUČENÁ LITERATURA:

- [1] IEEE Computer Society, 802.1Q IEEE Standard for Local and metropolitan area network Virtual Bridged Local Area Networks, IEEE, New York, 2006
- [2] IEEE Computer Society, 802.11e IEEE Standard for Information technology- Telecommunications and information exchange between systems- Local and metropolitan area networks- Specific requirements 8: Medium Access Control (MAC) Quality of Service Enhancements, IEEE, New York 2005
- [3] 3GPP, 3GPP TS 23.107 3rd Generation Partnership Project, Technical Specification Group Services and System Aspects; Quality of Service (QoS) concept and architecture (Release 7), 3GPP, Valbonne, 2007

Termín zadání: 11.2.2008

Termín odevzdání: 4.6.2008

Vedoucí projektu: Ing. Karol Molnár, Ph.D.


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

UPOZORNĚNÍ:

Autor bakalářské práce nesmí při vytváření bakalářské práce porušit autorská práva třetích osob, zejména nesmí zasahovat nedovoleným způsobem do cizích autorských práv osobnostních a musí si být plně vědom následků porušení ustanovení § 11 a následujících autorského zákona č. 121/2000 Sb., včetně možných trestněprávních důsledků vyplývajících z ustanovení § 152 trestního zákona č. 140/1961 Sb.

LICENČNÍ SMLOUVA POSKYTOVANÁ K VÝKONU PRÁVA UŽÍT ŠKOLNÍ DÍLO

uzavřená mezi smluvními stranami:

1. Pan

Jméno a příjmení: Radovan Václavek

Bytem: Kamenná 3857, Zlín

Narozen/a (datum a místo): 7.2.1974 ve Zlíně

(dále jen „autor“)

a

2. Vysoké učení technické v Brně

Fakulta elektrotechniky a komunikačních technologií

se sídlem Údolní 244/53, 602 00, Brno

jejímž jménem jedná na základě písemného pověření děkanem fakulty:

prof. Ing. Kamil Vrba, CSc.

(dále jen „nabyvatel“)

Čl. 1 Specifikace školního díla

1. Předmětem této smlouvy je vysokoškolská kvalifikační práce (VŠKP):

- ☐ disertační práce
 - ☐ diplomová práce
 - ☐ bakalářská práce
 - ☐ jiná práce, jejíž druh je specifikován jako
- (dále jen VŠKP nebo dílo)

Název VŠKP: Mechanismy zajištění kvality služeb v pevných,
bezdrátových a mobilních datových sítích

Vedoucí/ školitel VŠKP: Ing. Karol Molnár, Ph.D.

Ústav: Ústav telekomunikací

Datum obhajoby VŠKP:

VŠKP odevzdal autor nabyvateli v*:

- ☐ tištěné formě – počet exemplářů 1
- ☐ elektronické formě – počet exemplářů 1

* hodící se zaškrtněte

2. Autor prohlašuje, že vytvořil samostatnou vlastní tvůrčí činností dílo shora popsané a specifikované. Autor dále prohlašuje, že při zpracovávání díla se sám nedostal do rozporu s autorským zákonem a předpisy souvisejícími a že je dílo dílem původním.
3. Dílo je chráněno jako dílo dle autorského zákona v platném znění.
4. Autor potvrzuje, že listinná a elektronická verze díla je identická.

Článek 2

Udělení licenčního oprávnění

1. Autor touto smlouvou poskytuje nabyvateli oprávnění (licenci) k výkonu práva uvedené dílo nevýdělečně užít, archivovat a zpřístupnit ke studijním, výukovým a výzkumným účelům včetně pořizování výpisů, opisů a rozmnoženin.
2. Licence je poskytována celosvětově, pro celou dobu trvání autorských a majetkových práv k dílu.
3. Autor souhlasí se zveřejněním díla v databázi přístupné v mezinárodní síti
 - ☐ ihned po uzavření této smlouvy
 - ☐ 1 rok po uzavření této smlouvy
 - ☐ 3 roky po uzavření této smlouvy
 - ☐ 5 let po uzavření této smlouvy
 - ☐ 10 let po uzavření této smlouvy(z důvodu utajení v něm obsažených informací)
4. Nevýdělečné zveřejňování díla nabyvatelem v souladu s ustanovením § 47b zákona č. 111/ 1998 Sb., v platném znění, nevyžaduje licenci a nabyvatel je k němu povinen a oprávněn ze zákona.

Článek 3

Závěrečná ustanovení

1. Smlouva je sepsána ve třech vyhotoveních s platností originálu, přičemž po jednom vyhotovení obdrží autor a nabyvatel, další vyhotovení je vloženo do VŠKP.
2. Vztahy mezi smluvními stranami vzniklé a neupravené touto smlouvou se řídí autorským zákonem, občanským zákoníkem, vysokoškolským zákonem, zákonem o archivnictví, v platném znění a popř. dalšími právními předpisy.
3. Licenční smlouva byla uzavřena na základě svobodné a pravé vůle smluvních stran, s plným porozuměním jejímu textu i důsledkům, nikoliv v tísní a za nápadně nevýhodných podmínek.
4. Licenční smlouva nabývá platnosti a účinnosti dnem jejího podpisu oběma smluvními stranami.

V Brně dne:

.....
Nabyvatel

.....
Autor

ABSTRAKT

Tato bakalářská práce se zabývá zmapováním technologií a základních parametrů sloužících k zabezpečení kvality služeb v pevných, bezdrátových a mobilních sítích. Zaměřil jsem se především na požadavky a klasifikace, které jsou pro jednotlivé typy sítí typické a to se zaměřením na linkovou vrstvu. V sítích Ethernetu jsem se zabýval postupným vývojem jednotlivých technologií včetně norem IEEE 802.1Q a na ni navazující IEEE 802.1p. Další části pak popisují danou problematiku v bezdrátových sítích, s pohledem na jiný druh prostředí a opět se snažím čerpat z daných standardů pro zabezpečení kvality služeb v normě 802.11e navazující na normu 802.11a/b/g. Další část je zaměřena na poslední generace mobilních sítí opět z pohledu typů a vývoje jednotlivých technologií. Zde pak čerpám z normalizačního projektu 3GPP a standardů organizace IEEE, které jsou na tuto problematiku zaměřeny. Další část je zaměřena na WiMAX technologie. V předposlední části pak srovnávám jednotlivé síťové technologie z pohledu zajištění QoS a navrhuji možné způsoby zabezpečení konverze mezi jednotlivými technologiemi. V závěru jsou shrnuty všechny uvedené technologie, možnosti jejich vzájemné konverze a další možný vývoj v dané oblasti

KLÍČOVÁ SLOVA

kvalita služeb, Instituce definující elektrické normy a standard, lokální síť, bezdrátová síť, mobilní síť, rámec, standardy, konverze

ABSTRACT

This bachelor's thesis deals with mapping technologies and base parameters used to guarantee the quality of systems in the local area networks, including wireless and mobile ones. I have focused mainly on requests and classifications, which are typical for the types of networks on link layer. In Ethernet I focused on the gradual trends in the fore mentioned technologies and IEEE 802.1Q and connected IEEE 802.1p standards included. The next part describes the quality of systems in wireless nets in different types of environments and again uses given standards for quality of systems guarantee in 802.11e and connected 802.11a/b/g standards. The next part focuses on the latest generations of mobile nets, looking at the types and trends of the latest technologies. Here I draw from standard project 3GPP, which describes the problems with these technological developments. The next part focuses on WiMAX technologies. In the penultimate part I compare each network technology from the view of QoS assuring and suggest possible methods of securing the conversion between each technology. The conclusion summarises all the technologies I have mentioned and the future trends including possible problems and challenges with these latest technologies.

KEYWORDS

Quality of Service, Institute of Electrical and Electronics Engineers, Local Area Network, Wireless Network, Mobile Network, Frame, Specifications, Conversion

PROHLÁŠENÍ

Prohlašuji, že svou bakalářskou práci na téma "Mechanismy zajištění kvality služeb v pevných, bezdrátových a mobilních datových sítích" jsem vypracoval samostatně pod vedením vedoucího semestrální práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou všechny citovány v práci a uvedeny v seznamu literatury na konci práce.

Jako autor uvedené bakalářské práce dále prohlašuji, že v souvislosti s vytvořením této semestrální práce jsem neporušil autorská práva třetích osob, zejména jsem nezasáhl nedovoleným způsobem do cizích autorských práv osobnostních a jsem si plně vědom následků porušení ustanovení § 11 a následujících autorského zákona č. 121/2000 Sb., včetně možných trestně právních důsledků vyplývajících z ustanovení § 152 trestního zákona č. 140/1961 Sb.

V Brně dne

.....
(podpis autora)

PODĚKOVÁNÍ

Děkuji vedoucímu bakalářské práce Ing.Karolu Molnárovi Ph.D, za trvalou podporu a celkovou pomoc při řešení a zpracování bakalářské práce.

V Brně dne

.....

(podpis autora)

SEZNAM POUŽITÝCH ZKRATEK

2G - síť 2. generace – 2nd generation

3G - síť 3. generace - 3rd generation

3GPP – partnerský projekt třetí generace - The 3rd Generation Partnership Project

AAA - autentizace, autorizace, přístup - Authentication, Authorization, Accounting

AIFS - mezirámcová mezera výběru - Arbitration Interframe Space

ATM - asynchronní mód přenosu - Asynchronous Transfer Mode

BCCH - širokopásmový řídicí kanál - Broadcast Control Channel

BLAN - přemostěná lokální síť - Bridged Local Area Network

BS – základnová stanice – Base Station

BWA - širokopásmový bezdrátový přístup - Broadband Wirelles Access

CBR - konstantní bitová rychlost - Constant Bit Rate

CCCH - společný řídicí kanál - Common Control Channel

CDMA2000 - vícenásobný přístup pomocí kódového dělení přenosových kanálů rok 2000 - Code Division Multiple Access year 2000

CFI - identifikátor kanonického formátu - Canonical Format Indicator

CID - identifikátor spojení - Connection IDentifier

CRNC - řídicí kontrolér rádiové přístupové sítě - Controlling RNC

CS - podvrstva konvergence - Convergence Sublayer

CSMA/CA - pravděpodobnostní protokol přístupu k médiu s předcházením kolizím - Carrier Sense Multiple Access with Collision Avoidance

CTCH - společný provozní kanál - Common Traffic Channel

CW - okno soutěžení - Contention Window

DCCH - podpůrný řídicí kanál - Dedicated Control Channel

DCF - funkce rozložené koordinace - Distributed Coordination Function

DiffServ - dynamické rozlišení úrovně služeb - Defferentiated Services

DIFS - rozložení mezirámcového prostoru - Distributed Inter Frame Space

DRNC - pomocný kontrolér rádiové přístupové sítě - Drift RNC

DSCP - rozlišovací bod kódu služby - Differentiated Services Code Point

DTCH - vyhrazený provozní kanál - Dedicated Traffic Channel

DWDM - multiplexace na základě dělení podle vlnové délky s vyšší hustotou - Dense Wavelength Division Multiplexing

EDCF - rozšířená distribuovaná koordinační funkce - Enhanced Distributed Coordination Function

EDGE - rozšířená data pro GSM evoluci - Enhanced Data For GSM Evolution

FCS - kontrolní součet rámce - Frame Check Sequence

FDD - frekvenční multiplex - Frequency Division Duplex
 FDDI - rozhraní pro distribuci dat vláknem - Fiber Distribute Data Interface
 GPRS - obecná paketová rádiová služba - General Packet Radio Service
 GSM - globální systém pro mobilní komunikaci - Global System for Mobile communications
 HA - síťový manažer - Home Agent
 HCCA - přístupová metoda ke kanálům řízená HCF - HCF Controlled Channal Access
 HCF - hybridní koordinační funkce - Hybrid Coordination Function
 HLR - domovský lokační registr - Home Location Register
 IEEE - Instituce definující elektrické normy a standard - Institute of Electrical and Electronics Engineers
 IFS - mezirámcový prostor - InterFrame Space
 IntServ - technologie rezervace pásma - Integrated Services
 ISO - mezinárodní organizace pro standardizaci - International Organization for Standardization
 ITU - mezinárodní telekomunikační konfederace - International Telecommunication Union
 LAN - místní síť – Local Area Network
 LLC Typ 2 - Řízení logického spoje typ 2 - Logical Link Control Type 2
 LOS - přímá viditelnost - Line of Sight
 LTE - standardy pro GSM 4.generace - Long Term Evolution
 NDP - protokol pro zjištění sousedních zařízení - Neighbor Discovery Protocol
 NLOS - nepřímá viditelnost - Non Line of Sight
 Node B - základnová stanice v systému UMTS - Node B
 MAC - metoda řízení přístupu - Media Access Control
 MBWA - mobilní širokopásmový bezdrátový přístup - Mobile Broadband Wireless Access
 MPLS - víceprotokolové přepojování okruhů na bázi návěští - Multi-Protocol Label Switching
 OSI - propojení otevřených systémů - Open Systems Interconnection
 PCF - funkce bodové koordinace - Point Coordination Function
 PCCH - pagingový řídicí kanál - Paging Control Channel
 QoS - kvalita služeb - Quality of Service
 RAM - paměť s libovolným (náhodným) přístupem - Random-Access Memory
 RB - rádiové nosiče - Radio Bearers
 RLC - řídicí rádiová vrstva - Radio Link Control
 RNC - kontrolér rádiové sítě - Radio Network Controler
 RSVP - rezervační protokol - Resource Reservation Protocol
 SDH - synchronní digitální hierarchie - Synchronous Digital Hierarchy

SDU - datová jednotka služby - Service Data Units

SFE - statické filtrační položky - Static Filtering Entries

SGSN - zařízení obsluhující GPRS provoz v GSM sítích - Serving GPRS Support Node

SID - identifikátor provozního toku - Traffic Stream Identifier

SIFS - krátkodobý rozestup mezi rámci - Short Inter-Frame Spacing

SLA - dohoda mezi společnostmi a zákazníky úrovně služeb - Service Level Agreement

SNAP - protokol přístupu k podsíti - SubNetwork Access Protocol

SRB - signalizační rádiové nosiče - Signalling Radio Bearers

SRNC - obsluhující kontrolér rádiové přístupové sítě - Serving RNC

SS - účastnická stanice - Subscriber Station

TCI - značková kontrolní informace - Tag Control Information

TDD - časový multiplex - Time Division Duplexing

TPID - značkový protokolový identifikátor - Tag Protocol Identifier

UE - uživatelské zařízení - User Equipment

UMTS - univerzální mobilní telekomunikační systém - Universal Mobile Telecommunication System

UTRAN - pozemní rádiová přístupová síť UMTS - UMTS Terrestrial Radio Access Network

VCI - identifikátor virtuálního kanálu - Virtual Channel Identifier

VLAN - virtuální síť - Virtual Local Area Network

VoIP - IP telefonie - Voice over IP

VPI - identifikátor virtuální cesty - Virtual Path Identifier

VTP - proprietární protokol pro distribuci VLAN konfiguračních informací - VLAN Trunking Protocol

WAN - rozlehlá síť - Wide Area Networks

WCDMA - širokopásmový vícenásobný přístup pomocí kódového dělení přenosových kanálů - Wideband Code Division Multiple Access

WiMAX - celosvětová součinnost pro mikrovlnný přístup - Worldwide Interoperability for Microwave Access

WLAN - bezdrátové lokální síť - Wireless Local Area Network

WMAN - bezdrátové metropolitní síť - Wireless Metropolitan Area Network

WME - rozšíření bezdrátových mechanismů o multimédia - Wireless Multimedia Extensions

WMM - bezdrátová multimédia - Wireless MultiMedia

WMM-SA - řízený přístup pro bezdrátová multimédia - WMM Scheduled Access

OBSAH

ÚVOD	15
1 KVALITA SLUŽEB V PEVNÝCH SÍTÍCH	16
1.1 Základní charakteristiky QoS.....	16
1.2 Jednotlivé prvky kvality služeb	17
1.2.1 Dostupnost služby.....	17
1.2.2 Ztráta rámce	18
1.2.3 Přerážení rámce.....	19
1.2.4 Duplikace rámce	19
1.2.5 Zpoždění přenosu rámce	19
1.2.6 Životnost rámce	19
1.2.7 Rámcová četnost chyb	20
1.2.8 Maximální velikost datové jednotky.....	20
1.2.9 Priorita rámce	20
1.2.10 Kapacita - propustnost	21
1.3 Řazení rámce do front	21
1.4 Druhy provozu	22
1.5 Základní rysy technologií zajištění kvality služeb.....	24
1.5.1 Standardy IEEE 802.1p	25
1.5.2 MPLS – Multi-Protocol Label Switching	26
1.5.3 ATM Asynchronous Transfer Mode.....	26
1.6 Možnosti řízení šířky pásma v LAN - implementace QoS v typické síti	27
1.6.1 Popis typické sítě	27
1.6.2 Řízení šířky pásma v LAN se zabezpečením QoS v praxi	27
1.6.3 Zajištění služeb po celé přenosové trase	28
2 KVALITA SLUŽEB V BEZDRÁTOVÝCH SÍTÍCH	29
2.1 Distributed Coordination Function (DCF).....	29
2.2 Point Coordination Function (PCF).....	30
2.3 Kvalita služby definovaná v 802.11e	30
3 KVALITA SLUŽEB V MOBILNÍCH SÍTÍCH	32
3.1 Technologie 2G, 2,5G a 2,7G	32
3.2 Technologie 3G	32
3.3 Třídy zabezpečující kvalitu služeb v sítích UMTS	33
3.3.1 Třída konverzační	33
3.3.2 Třída streamovací	34
3.3.3 Třída interaktivní	34
3.3.4 Třída služeb na pozadí	34
3.4 Definice kanálů v UMTS	34
3.4.1 Logické kanály v UMTS	35
3.5 Vývoj QoS v mobilních sítích třetí generace	35

4 KVALITA SLUŽEB V BEZDRÁTOVÝCH WiMAX SÍTÍCH	36
4.1 Technologie WiMAX	36
4.2 Vývoj standardů IEEE 802.16	36
4.3 Řízení provozu ve standardech IEEE 802.16	37
4.4 Kvalita služeb v IEEE 802.16	38
4.4.1 Unsolicited Grant Service	39
4.4.2 Real-Time Pooling Service.....	39
4.4.3 Enhanced Real-Time Pooling Service.....	39
4.4.4 Non Real-Time Pooling Service	39
4.4.5 Best -Effort	39
4.4 Další vlastnosti a možnosti WiMAXu	40
5 SROVNÁNÍ SÍŤOVÝCH TECHNOLOGIÍ Z POHLEDU QoS	40
6 KONVERGENCE MEZI SYSTÉMY	45
6 KONVERZNÍ PROCEDURY	47
7 ZÁVĚR	49
POUŽITÁ LITERATURA	52

SEZNAM OBRÁZKŮ

Obr. 1.1 Struktura hlaviček paketu a standardní hlavičky	25
---	-----------

SEZNAM TABULEK

Tab. 1.1 Zpoždění v mostu	20
Tab. 1.2 Doporučené priority pro mapování provozních tříd	22
Tab. 1.3 Typy provozů a mapování provozních tříd se zobrazením přidělení provozu	23
Tab. 1.4 Priority a mapování provozních tříd	24
Tab. 4.1 Přehled standardů systému WiMAX	37
Tab. 5.1 Kategorie a požadavky na obsluhu podle IEE802.11e	41
Tab. 5.2 Priority a požadavky na obsluhu podle WMW.....	44
Tab. 5.3 Celkové srovnání síťových technologií z pohledu QoS	44

ÚVOD

Zajištění kvality služeb – QoS (kvalita služeb - Quality of Service) je jedním ze současných hlavních trendů ve vývoji počítačových sítí. V této problematice se především řeší poskytování služeb s definovanou kvalitou v závislosti na požadovaném provozu sítě uživatele. V poslední době dochází především k rozvoji aplikací, u kterých je kvalita, z pohledu uživatele, závislá na časových charakteristikách komunikace a to jak přes běžnou počítačovou síť, bezdrátovou počítačovou síť tak i v nových sítích GSM třetí generace. Charakteristiky provozu v sítích se velmi rychle mění, jak v místních tak i v rozsáhlých sítích a vykazují značnou časovou závislost. To také vyžaduje od provozovatelů a poskytovatelů internetového připojení potřebu třídit provoz uvnitř těchto sítí a zároveň také hodnotit jejich absolutní a relativní význam.

V konečném důsledku pak podle něj můžou vytvořit žádané profily provozu na jednotlivých směrovačích. Jedním z hlavních požadavků na směrovače v datových sítích je schopnost určit daný tok aplikací, které požadují rozdílné zacházení v síti. Omezená kapacita tradiční architektury IP směrovačů (IP směrovač - IP router), vede k jednotnému způsobu zpracování přicházejících paketů, což se stává překážkou k zlepšení výkonu sítě. Je to způsobeno zvětšujícím se počtem aplikací, které potřebují záruku služeb od sítě, aby mohli správně fungovat. Existuje mnoho různých typů řešení a návrhů architektur, které zavádějí úroveň kvality služeb QoS a seřazují datové jednotky přicházejícího provozu podle daných priorit. Kvalita služeb v referenčním modelu počítačové sítě může být implementována v různých vrstvách.

S dalším rozmachem bezdrátových technologií a dynamicky se rozvíjejícím využíváním všech druhů datových provozů na nich, vyvstaly požadavky na zajištění QoS i v bezdrátových WLAN (bezdrátové lokální síť -Wireless Local Area Network) sítích. Bezdrátové rádiové sítě, ale znamenají navíc také specifické přenosové prostředí, které se musí adekvátně zohlednit. Bezdrátové spoje mají odlišné charakteristiky než pevné spoje. Ovlivňuje je jak útlum, tak i rušení signálu a samozřejmě i šum. Tyto parametry závisejí na místě a době vysílání a mohou pak následně vést k chybám a také v čase se měnící kapacitě kanálu. Okolní prostředí může způsobit značné ovlivnění kvality a síly rádiového signálu, a stejně tak může tyto parametry ovlivnit vzdálenost či vzájemné rušení. S tím také souvisí, jiné členění provozu na takové síti.

V neposlední řadě se problematika zajištění kvality služeb výrazně týká také sítí GSM (globální systém pro mobilní komunikaci - Global System for Mobile communications). To především v důsledku příchodu nových technologií podporujících přepínání paketů a širokopásmové služby. Stejně tak jako v LAN (místní síť – Local Area Network) nebo WLAN sítích i zde je třeba zajistit rozdílnou kvalitu služeb s ohledem na jednotlivé typy provozu a služeb. A to hlavně protože tyto sítě nejsou určeny jenom pro hlasové služby, ale také pro služby datové, jak je uživateli v poslední době výrazně vyžadováno a také využíváno.

V konečném důsledku pak nastává další problém, který přináší stále častěji aplikované propojení všech typů výše uvedených sítí. A samozřejmě přenos dat přes různá rozhraní, až ke koncovým adresátům, při zajištění požadované kvality služeb. V závěrečné části se pak pokusím popsat možnosti tohoto zajištění. Ať už jde o samotné propojení, rozpoznání, nebo zařazení jednotlivých typů úrovní kvality v těchto typech sítí, v závislosti na požadované kvalitě služeb.

1 KVALITA SLUŽEB V PEVNÝCH SÍTÍCH

V původních síťových technologiích navržených v 70. letech, bylo zacházeno se všemi datovými jednotkami stejně. Tento způsob zpracování datových jednotek se nazývá Best-Efford a pracuje na principu toho, že se snaží vyhovět žádosti datových jednotek o zajištění doručení na náležitý port, ovšem bez toho aby to jakkoliv garantoval. Z tohoto důvodu proto není možné určit jak přesný časový úsek pro zpracování datové jednotky tak ani samotné provedení přepojení datové jednotky.

Z výše uvedených vlastností vyplývá hodně omezení, které je třeba zohlednit. Technologie nemá možnost rozpoznat druhy datových toků, nezávisle na ostatních samostatně zpracovává každou datovou jednotku. Tím je dáno také to, že pokud je využíváno sdílených síťových prostředků také neumí diferencovat rozdílné datové toky. To že toto třídění není možné, může mít také za následek, že některé síťové spojení může vyčerpat všechny dostupné síťové prostředky a tím zablokovat všechny ostatní přenosy.

Jak je tedy zřejmé, ve chvíli kdy dojde k nedostatku síťových prostředků, ovlivní se tím všechny datové toky. To se ale může projevit velice různě na službě, která patří k danému datovému toku.

Například pokud půjde o IP telefonii - VoIP (IP telefonie - Voice over IP), videokonference a další interaktivní služby, které samozřejmě nebude až tak vadit ztráta paketu, jako tam kde půjde o přenášení datového souboru, kde ztráta paketu může způsobit znehodnocení celého souboru. A naopak pokud dojde datový soubor o něco později a rychlost při jeho stahování bude kolísat, nebude nám to vadit tak jako kdyby docházelo ke kolísání zpoždění například při VoIP.

Z toho také vyplývá, že Quality of Service nesouvisí pouze s tím, jakou má daná síť fyzickou rychlost, ale jak dokáže zajistit přenos jednotlivých toků dat podle charakteristik, které souvisí s SLA (dohoda mezi společností a zákazníky úrovní služeb - Service Level Agreement), tedy s dohodou o úrovni poskytovaných služeb.

1.1 Základní charakteristiky QoS:

Zpoždění (latency) – čas, který uplyne od odeslání zprávy zdrojovým uzlem po její přijetí na uzlu cílovém; zahrnuje zpoždění v přenosové trase a na zařízeních, které jsou její součástí. Existují aplikace, kterým zpoždění nevadí, ale jsou i aplikace na zpoždění náchylné.

Rozptyl zpoždění (jittering) – představuje variabilitu v doručování paketů cílovému uzlu (tedy ve zpoždění při přenosu). Stejně jako u zpoždění i zde lze nalézt typy aplikací, které nemají s rozptylem problém, a naopak i aplikace, u kterých problém působí.

Šířka pásma (bandwidth) – představuje kapacitu pro přenos dat, vyjadřuje se většinou v kilobitech za sekundu (kbit/s) nebo megabitech za sekundu (Mbit/s); pásmo představuje teoretickou maximální kapacitu spojení, s jeho zvyšováním může být za stejnou jednotku času přenesen větší objem dat; zpoždění s pásmem ne vždy přímo souvisí.

Ztráta paketů (packet loss) – je vyjadřována většinou procenty a představuje průměrnou ztrátu paketů za určité období.

Dostupnost (availability) – je vyjadřována většinou procenty a představuje průměrnou dostupnost služby za určité období.

Je tedy jasné, že technologie Best Effort byla pro současné požadavky sítí nevyhovující. Dnes vyžadujeme, aby při provozování různých služeb, byla síť schopná rozeznat, o jaké datové jednotky se jedná a ke které službě tyto jednotky patří. Od toho se pak odvíjí přímo i to jak s nimi bude v síti zacházeno.

V rámci sjednocení parametrů, které se týkají zajištění kvality služeb, bylo definováno několik základních prvků, které s touto službou přímo souvisí. IEEE (Institute definující elektrické normy a standard - Institute of Electrical and Electronics Engineers) standardy 802.1p jsou součástí IEEE standardů 802.1D. 802.1p standardy pokrývají provozní třídu a dynamické multicastové filtrování jako součást metody řízení přístupu – MAC (metoda řízení přístupu - Media Access Control) pro mosty (most – Bridge), které jsou známy jako IEEE standard 802.1D. IEEE standard 802.1Q je součástí IEEE standardu 802.1D, definující architekturu pro virtuální přemostění LAN a služby poskytované ve virtuálním přemostění LAN. Vyjádření QoS musí být pevně definována. Následující parametry jsou podstatné pro podmínky splnění QoS podle IEEE standardu 802.1p.

1.2 Jednotlivé parametry kvality služeb

Kvalita služeb je ovlivňována několika různými faktory. Mezi tyto důležité prvky ovlivňující kvalitu služby patří:

- a) dostupnost služby
- b) ztráta rámce
- c) přeřazení rámce
- d) opakování rámce
- e) zpoždění přenosu rámce
- f) životnost rámce
- g) rámcová četnost chyb
- h) maximální velikost datové jednotky služby
- i) priorita rámce
- j) kapacita přenosové cesty

1.2.1 Dostupnost služby

Dostupnost služby je měřena jako část celkového času, během kterého je služba MAC poskytována. Přemostění může zvýšit nebo snížit dostupnost služby.

Most (bridge) označuje v počítačové síti zařízení, které spojuje dvě části sítě na druhé (linkové) vrstvě referenčního modelu ISO/OSI (mezinárodní organizace pro standardizaci - International Organization for Standardization / propojení otevřených systémů - Open Systems Interconnection). Most je pro protokoly vyšších vrstev transparentní (neviditelný), odděluje provoz různých segmentů sítě a tím zmenšuje i zatížení sítě. Most odděluje provoz dvou segmentů sítě, tak že si ve své paměti RAM (paměť s libovolným (náhodným) přístupem - Random-Access Memory) sám sestaví tabulku MAC (fyzických) adres a portů, za kterými se dané adresy nacházejí. Leží-li příjemce ve stejném segmentu jako odesílatel, most rámce do jiných částí sítě neodešle. V opačném případě je odešle do příslušného segmentu v

nezměněném stavu (týká se pouze tzv. Unicast rámců, které jsou určeny jedinému příjemci). Všesměrové rámce (Multicast, Broadcast) jsou naopak propouštěny bez omezení.

Dostupnost služby může být zvýšena automatickým rekonfigurováním sítě, aby se vyhnula vadné části v datové cestě (např. opakovač, kabel nebo konektor). Dostupnost služby může být snížena selháním mostu nebo filtračních pravidel mostu.

Během rekonfigurace může most vyřadit určité rámce za účelem ochrany dalších aspektů služby MAC. Tím se ale snižuje dostupnost služeb pro koncové stanice, které tak z rekonfigurace nemají žádné výhody. Při přemístění koncové stanice je možné, že tato nebude schopná získat rámce od ostatních koncových stanic, dokud nebudou aktualizovány filtrační informace mostu. Tyto informace most používá pro lokalizaci zprávy. Pro optimalizaci funkčnosti služby, mohou být filtrační informace získané dynamicky během rekonfigurace změněny. Avšak filtrační informace, které jsou konfigurovány staticky, takto změněny být nemůžou. Most může odmítnout službu a vyřadit rámce, aby ochránil síť před přístupem neautorizovaných zařízení. Pro maximalizaci dostupnosti služby není žádná její ztráta nebo odklad přístupu způsoben mosty, kromě těchto příčin: následek selhání, přemístění nebo vložení síťové komponenty, přemístění konečné stanice, pokus o neautorizovaný přístup. Tyto důvody jsou výjimečnými stavy. Operace jakéhokoli dodatečného protokolu potřebného pro podporu kvality MAC služby je tak omezena konfigurací místní sítě BLAN (přemostěná lokální síť - Bridged Local Area Network) a je nezávislá na individuálních případech servisního zabezpečení.

1.2.2 Ztráta rámce

MAC služba nezajišťuje dodání SDU (datová jednotka služby - Service Data Units). Rámce přenášené pomocí zdrojové stanice dorazí s vysokou pravděpodobností neporušené do cílové stanice. Operace mostu způsobují minimální dodatečnou ztrátu rámce.

Přenesení rámce od zdrojové stanice do cílové stanice se nemusí podařit z následujících důvodů:

a) poškození rámce během přenosu nebo při příjmu z fyzické vrstvy

b) vyřazení rámce mostem protože:

1. Není možné přenést rámec za nějakou maximální dobu a je žádoucí vyřadit rámec pro ochranu maximální životnosti rámce – tedy aby nebyla překročena.
2. Není možné pokračovat ve skladování rámce, kvůli vyčerpání vnitřní vyrovnávací kapacity, protože rámce stále přichází, ve stále větším množství než je takové, které může být přeneseno.
3. Velikost datové jednotky přenesené pomocí rámce převyšuje možné maximum MAC procedur zapojených na LAN, do kterých má být rámec přenesen.
4. Změny ve fyzické topologii sítě vyžadují vyřazení rámce pro omezenou dobu, kvůli podpoře jiných stránek QoS.
5. Zařízení připojené k portu nemá oprávněný přístup do sítě.

6. konfigurace SFE (statické filtrační položky - Static Filtering Entries) v databázi filtrů, neumožňuje zasílání rámců do patřičné cílové adresy na specifických portech. Protože SFE souvisejí s konkrétními porty nebo kombinacemi portů, je možné, že nezdařená konfigurace SFE povede k neočekávanému vyřazení rámce během nebo následkem automatické opětovné konfigurace BLAN.

1.2.3 Přerazení rámce

MAC Služba (ISO/IEC 15802-1) dovoluje přerazení rámců s danou uživatelskou prioritou pro určitou kombinaci cílové a zdrojové adresy. Doručovací proces v mostech nepřerazuje ani neduplikuje rámce. Tam, kde jsou mosty schopné napojení individuální MAC tak, že znásobují cesty mezi jakoukoli zdrojovou a cílovou stanicí, je pak operační protokol vyžadován pro zajištění užití jediné cesty.

Přerazení a duplikace rámce se neděje během běžné operace. Když je malá pravděpodobnost duplikace či přerazení působící jako následek rekonfigurace, degradace vlastností MAC služby je nepatrná. Některé protokoly LAN, např. LLC Typ 2 (řízení logického spoje typ 2 - Logical Link Control Type 2) jsou obzvláště citlivé na přerazení či duplikaci rámce.

1.2.4 Duplikace rámce

MAC Služba (ISO/IEC 15802-1) povoluje zanedbatelnou úroveň duplikace rámců. Mosty neduplikují rámce uživatelských dat. Možnost duplikace rámce v BLAN může nastat v případě existence více cest mezi zdrojovými a cílovými stanicemi. Kde mohou mosty propojit individuální LAN pro poskytnutí násobných cest, operace protokolu je vyžadována pro zajištění užití jediné cesty.

1.2.5 Zpoždění přenosu rámce

Služba MAC vnáší variabilní zpoždění do přenosu rámce na média. Zpoždění přenosu rámce je definována jako uplynulý čas mezi odpovědí základního prvku a odpovídajícího základního prvku. Hodnoty uplynulého času jsou počítány pouze na SDU, které jsou úspěšně přeneseny.

Když je služba MAC poskytnuta v abstraktním rozhraní v koncové stanici, není možné přesně specifikovat zpoždění přenosu rámce. Avšak je možné měřit přístup médií, přenos a příjem rámce a přenosové zpoždění dosažené pomocným systémem. V tomto případě je to most. Minimální dodatečné přenosové zpoždění dosažené pomocí mostu je čas, potřebný na přijetí rámce, plus čas potřebný na přístup k médiu, na které se rámec přenesení. Rámec je přijat před přenosem, protože se musí spočítat FCS (kontrolní součet rámce - Frame Check Sequence) a v případě vzniklé chyby se musí rámec vyřadit.

1.2.6 Životnost rámce

Služba MAC určuje horní hranici povoleného zpoždění přenosu pro specifické případy komunikace. Tato maximální životnost rámce je potřebná pro zajištění správné operace protokolů vyšší úrovně. Když informace od MAC podvrstvy (podvrstva - sublayer) poskytnuté mostem obsahují již informace o zpoždění převyšující povolené, mosty tyto rámce vyřadí. Doporučené a maximální hodnoty jsou specifikovány v **Tab. 1-1**.

Tab. 1.1

Zpoždění v mostu

Parametr	Doporučená hodnota	Absolutní maximum
Maximální zpoždění v mostu	1,0 sekunda	4,0 sekundy

1.2.7 Rámcová četnost chyb

Služba MAC zaručuje velmi nízký počet skrytých chyb rámců. Skryté chyby nejsou detekovatelné zabezpečením FCS. Dvaatřicetibitový cyklický kontrolní kód, který se počítá ze všech polí s výjimkou preamble a FCS. Slouží ke kontrole správnosti dat - příjemce si jej vypočítá z obdrženého rámce a pokud výsledek nesouhlasí s hodnotou pole, rámec zahodí jako vadný.

1.2.8 Maximální velikost datové jednotky

Maximální velikost datové jednotky SDU, která může být podporována pomocí IEEE 802 LAN, závisí na MAC metodě a přístupných parametrech metody (rychlost, elektrické vlastnosti, atd.). Může být omezena vlastníkem LAN.

Maximální velikost SDU podporované mostem mezi dvěma LAN je menší, než ta, kterou podporuje LAN. Most se nepokouší o přenos rámce do LAN, která nepodporuje velikost SDU sdělené pomocí rámce.

1.2.9 Priorita rámce

Požadavky s vysokou prioritou mohou dostat přednost před požadavky se základní prioritou.

MAC podvrstva mapuje požadované priority na přístup, podporované přístupovou metodou individuálního média. Požadovaná priorita přenášených dat, může být přenesena na cílovou stanici s přeneseným rámcem s využitím mechanismů signalizujících prioritu, patřících do některých metod řízení přístupu média. Pokud nemohou všechny IEEE 802 LAN MAC signalizovat prioritu rámce, mosty nastaví prioritu na základě kombinace řídicích informací a konfiguračních informací nastavených mostu.

Hromadící se zpoždění může být řízeno pomocí priorit. Přístupové zpoždění může být řízeno pomocí priority v metodách řízení přístupu k médiu, které podporuje více než jednu přístupovou prioritu. Most mapuje prioritu v jedné nebo více třídách. Mosty, které podporují více jak jeden druh cesty, jsou schopny podpořit jednotlivé třídy provozu.

Schopnost signalizovat prioritu v IEEE 802 LAN umožňuje její přenesení s konečnou hodnotou přes BLAN. Toto spojené se shodným přístupem v mapování priority druhů cest a k přístupové prioritě umožňuje shodné užití informační priority podle možností mostů a MAC v cestě přenosu.

IEEE Std 802.1Q™ [3] definuje formát rámce a procedury, které mohou být použity pro přenesení priorit přes LAN. Užití IEEE 802.1Q formátu rámce umožňuje zachování

konečné signalizace priority bez ohledu na schopnosti individuálních LAN MAC typů signalizace priority.

Za normálních podmínek není priorita modifikována při přenosu přes příjmovou funkci mostu, avšak řízení sítě může kontrolovat, jak je priorita rozšiřována. Obnovená priorita je standardně identická s příchozí prioritou.

1.2.10 Kapacita - propustnost

Celková kapacita poskytovaná BLAN může být značně vyšší než ekvivalent samostatné LAN. Mosty mohou lokalizovat cestu v síti pomocí filtrujících rámců. Kapacita mezi konečnými stanicemi komunikujícími přes most může být snížena vyřazením rámce kvůli neschopnosti mostu přenosu v LAN do cílové stanice v požadované úrovni během delšího času.

1.3 Řazení rámce do front

Dopravní proces může poskytovat jeden nebo více přenosů a postavit tak rámce do fronty na každý port mostu. To poskytuje uskladnění ve frontě rámců, kde čekají na příležitost zařazení do těchto přenosů. Rámce budou přiděleny ke každé frontě podle jejich priorit.

Přenosový příkaz pro jednotlivý port přepínače:

- 1) unicast rámce (rámce se posílají jen na jeden počítač) s danou prioritou pro nějakou kombinaci cesty cílové a zdrojové adresy.
- 2) multicast rámce (rámce se posílají z jednoho zdroje skupině více koncových stanic) s danou prioritou cesty pro nějaké cílové adresy.

Rámce jsou přiděleny jejich jednotlivým paměťovým frontám podle jejich dřívějších uživatelských priorit podle tabulky provozních tříd (**tabulka 1.2**).

Standardní algoritmus vybrání rámce pro přenos: pro každý port, bude vybrán rámec podle třídy provozu podporované pro tento port. Rámec bude přenesený jen tehdy, jestliže se v systému nenachází žádný další rámec s vyšší prioritou.

Pro každou frontu platí, že pořadí, ve kterém jsou rámce přenesené, musí korespondovat se směrnicemi popsány v předchozí části.

Tab. 1.2.

Doporučené priority pro mapování provozních tříd.

		Množství dostupných provozních tříd							
		1	2	3	4	5	6	7	8
Priority	0	0	0	0	1	1	1	1	2
	1	0	0	0	0	0	0	0	0
	2	0	0	0	0	0	0	0	1
	3	0	0	0	1	1	2	2	3
	4	0	1	1	2	2	3	3	4
	5	0	1	1	2	3	4	4	5
	6	0	1	2	3	4	5	5	6
	7	0	1	2	3	4	5	6	7

1.4 Druhy provozu

Pro řízení provozu jsou velmi důležité jednotlivé druhy provozu. Různé typy provozu mají různé požadavky na přenos a také různé priority. Je tedy důležité daný provoz správně rozpoznat a zařadit do některé skupiny. Jednotlivé druhy provozu tedy rozlišujeme:

- a) řízení sítě - vysoké požadavky na dostupnost spojení, udržuje a podporuje síťovou infrastrukturu
- b) hlas - méně než 10 milisekund zpoždění
- c) video - méně než 100 milisekund zpoždění
- d) řízená zátěž - důležité pro některé aplikace
- e) excellent effort - best effort důležité pro vybranou skupinu uživatelů
- f) best effort - běžná LAN priorita
- g) aplikace na pozadí - hromadné přenosy, atd.

Tab. 1.3.

Typy provozů a mapování provozních tříd se zobrazením přidělení provozu k daným frontám

Počet front	Konkrétní fronta a k ní přidělený provoz	Typy provozu
1	1	a, b, c, d, e, f and g
2	1	a, b, c and d
	2	e, f and g
3	1	a and b
	2	c and d
	3	e, f and g
4	1	a and b
	2	c and d
	3	e and f
	4	g
5	1	a and b
	2	c
	3	d
	4	e and f
	5	g
6	1	a and b
	2	c
	3	d
	4	e
	5	f
	6	g
7	1	a
	2	b
	3	c
	4	d
	5	e
	6	f
	7	g

Tab. 1.4.

Priority a mapování provozních tříd

Priority	Typy provozu
1	aplikace na pozadí
2	náhradní provoz
0	běžný provoz
3	běžný provoz - důležitý pro uživatele
4	regulovaná zátěž
5	video
6	hlas
7	síťové řízení

1.5 Základní možnosti řešení zajištění kvality služeb

Lze definovat několik možností zajištění kvality služeb na jednotlivých úrovních v síti. Zaměříme-li se na standardy na úrovni vrstvy L2 tedy spojové (linkové) vrstvě, pak to mohou být tyto způsoby:

předimenzování linky – bývalo v minulosti a částečně je i dnes především v LAN prostředí nejpoužívanější metodou, jak zajistit všem aplikacím dostatečné pásmo. Ve WAN (rozlehlá síť - Wide Area Networks) prostředí jde o neefektivní a dokonce asi i nereálnou záležitost. Při stávajícím nárůstu používaných aplikací je veškeré předimenzování pouze dočasné.

rezervování síťových prostředků – je založeno na tom, že aplikace, která potřebuje určité prostředky, provede jejich rezervaci a po ukončení přenosu jej opět uvolní; typickým představitelem je technologie IntServ (integrované služby - Integrated Services) s protokolem RSVP (rezervační protokol - Resource Reservation Protocol).

využití prioritního systému – jsou dnes aplikovány několika metodami na různých úrovních komunikace, jde pouze o způsob definice, na základě jakých kritérií bude priorita provedena. Typickým představitelem metody jsou technologie DiffServ (dynamické rozlišení úrovně služeb - Differentiated Services), 802.1p a proprietární metody prioritního řízení provozu. Tento standard IEEE 802.1p pro zajištění kvality služeb na úrovni linkové vrstvy je jedním z hlavních , který se často využívá.

1.5.1 Standardy IEEE 802.1p

Jsou standardy pro zajištění priorit na úrovni linkové (spojové) vrstvy. Jsou definovány pro Ethernet, Token Ring (síťová technologi) a FDDI (rozhraní pro distribuci dat vláknem - Fiber Distribute Data Interface). Standard pro priority 802.1p je svázán se standardem pro virtuální síť VLAN (virtuální síť - Virtual Local Area Network) VTP (proprietární protokol pro distribuci VLAN konfiguračních informací - VLAN Trunking Protocol), což je L2 protokol (protokol na druhé vrstvě sítě), který slouží k přenášení informací o VLANech mezi switchi) 802.1Q.

Pokusím se tedy definovat možnosti a přínosy standardu IEEE 802.1p pro prostředí Ethernetu (totéž v podstatě platí i pro FDDI a Token Ring).

Standardy IEEE 802.1p/802.1Q používají stejnou strukturu hlavičky paketu, která do standardní hlavičky přidává několik bytů navíc, což jsou tedy v případě Ethernetu 4 byte. Znamená to, že může dojít k překročení dříve platné maximální velikosti rámce – neplatí tedy 1518, ale 1522, s čímž si ale nekompatibilní zařízení neporadí. Pokud by tedy bylo potřeba využívat priority, bylo by nutné nahradit všechna zařízení v síti (včetně síťových adaptérů) nebo zajistit IEEE 802.1p/802.1Q pouze v páteřních spojích, to ovšem L2 a L3 (L3 třetí vrstva sítě) aktivní prvky umí.

Políčka vyjadřující prioritu obsahují 3 bity, což představuje 8 úrovní priorit, nicméně v minulosti podporovala většina L2 přepínačů pouze dvě úrovně priorit rozdělené na 0 až 3 (bez priorit), 4 až 7 (s prioritou). Na obrázku 1.1 je struktura hlaviček paketu a standardní hlavičky:

Obr.1.1.

Struktura hlaviček paketu a standardní hlavičky

2 bajty	2 bajty
TPID	TCI

přídavná hlavička rámce v Ethernetu

8 bajtů	2 bajty
SNAP – encoder TPID	TCI

Token Ring a FDDI přídavné hlavičky

3 bity	1 bit	12 bitů
User priority	CFI	VID

značková kontrolní informace

Vysvětlení k obrázku: TPID - značkový protokolový identifikátor – Tag Protocol Identifier - má definovanou hodnotu 8100 (hex). Má-li tedy toto pole (EtherType) hodnotu 8100, rámec nese informace IEEE 802.1q/ 802.1p., TCI - značková kontrolní informace - Tag Control Information, SNAP - protokol přístupu k podsíti - SubNetwork Access Protocol, User priority – priority - umožňuje zakódování až osmi úrovní priority rámců (0 - 7, nula je přitom nejnížší prioritou) dle standardu 802.1p., CFI – identifikátor kanonického formátu - Canonical Format Indicator - bit indikuje, jestli jsou MAC adresy v kanonickém formátu, VDI - jednoznačně identifikuje VLAN, do které rámec přísluší

Další technologií pro zajištění kvality služeb, která částečně zasahuje do úrovně linkové vrstvy je standard MPLS (víceprotokolové přepojování okruhů na bázi návěští - Multi-Protocol Label Switching) původně navržený firmou Cisco Systems pod názvem Tag Switching.

1.5.2 MPLS – Multi-Protocol Label Switching

MPLS je moderní, obecně rozšířená technologie. Její výhodou by mělo být to, že je použitelná v rozdílných prostředích, které zahrnují např. ATM (asynchronní mód přenosu - Asynchronous Transfer Mode), Ethernet, Frame Relay, a Token Ring. MPLS kombinuje L2 přepínání se službami L3 při současném snížení složitosti a ceny provozu. MPLS není orientovaná pouze na protokol IP jako například Differentiated Services, ale je protokolově nezávislá (Multi-Protocol).

MPLS používá značkování rámců (dvacetibitovou značkou – label). Tato značka je přidávána na vstupním směrovači MPLS sítě a na výstupním směrovači je odebírána. Značka slouží pro zajištění rychlejšího průchodu paketů sítí, neboť pakety jsou značkovány na základě směrovacích informací. QoS je v MPLS zajištěno také prostřednictvím značky, do které jsou promítnuty podmínky na vstupním směrovači a to na základě vztahu MPLS-RSVP nebo MPLS-DiffServ. MPLS není přímo ovládáno aplikací, ale pouze prostřednictvím jiné QoS technologie, zajišťující QoS ještě před vstupem do MPLS sítě.

MPLS umožňuje také výhodnou integraci různých přenosových technologií na druhé vrstvě modelu ISO OSI, například Ethernet, SDH(synchronní digitální hierarchie - Synchronous Digital Hierarchy), DWDM (multiplexace na základě dělení podle vlnové délky s vyšší hustotou - Dense Wavelength Division Multiplexing) - a v neposlední řadě ATM, jež pro účely přenosu IP paketů můžeme zařadit do druhé vrstvy. Pokud daná technologie používá vlastní značky pevné délky (to je třeba případ identifikátorů VPI/VCI (identifikátor virtuální cesty/ identifikátor virtuálního kanálu - Virtual Path Identifier/Virtual Channel Identifier) v ATM), může MPLS používat právě tyto značky. Jinak se použije speciální zapouzdření a značka se zapíše do vnější hlavičky.

1.5.3 ATM - Asynchronous Transfer Mode

Pokud se bavíme o kvalitě služeb, je třeba zmínit i ATM. ATM technologie jako taková je na kvalitu služby připravená už v návrhu a má několik přenosových tříd, které definují kvalitu služby podle potřeb jednotlivých typů aplikací. Využívá dvě základní přenosové technologie – asynchronní multiplexování paketů a rychlé přepojování paketů. Kombinace těchto dvou technologií umožňuje pružné využití šířky pásma a podporuje rychlý přenos dat. Je to ale složitá technologie s vysokou cenou a malou efektivitou pro čistě datové implementace

1.6. Možnosti řízení šířky pásma v LAN - implementace QoS v typické síti

Z pohledu aplikací a uživatelů lze metodiku zajištění pásma aplikovat dvěma způsoby. Buď je aplikována na tok (flow) nebo na souhrn toků (aggregation).

Tok (flow) - je definován jako individuální, jednosměrný tok dat mezi dvěma aplikacemi. Je jednoznačně určen pěti parametry – transportním protokolem, zdrojovým portem, cílovým portem, zdrojovou adresou a cílovou adresou.

Souhrn toků (aggregation) - Jsou dva nebo více toků, se společnými vrstvami (v mezním případě může jít o jeden tok, ale s menším počtem určujících parametrů). Typicky jde o jeden nebo několik parametrů jako značka, priorita (L2/L3) nebo některá z dalších informací.

1.6.1 Popis typické sítě

Jednak se musíme zabývat tím, jak je síť rozlehlá. Obecně se skládá z centra, kde je soustředěno větší množství stanic a kde jsou umístěny primárně databázové, aplikační, centrální poštovní, centrální souborové a jiné servery. Na toto centrum pak navazují pobočky, kde mohou být sekundární servery, jako například souborové, tiskové a poštovní.

Z pohledu možností aktivních prvků využívaných v síti můžeme tedy použité zařízení rozdělit na:

- L1 prvky, které jsou z hlediska QoS transparentní jinak řečeno neovlivnitelné
- L2 prvky, které jsou schopné zajistit QoS na úrovni závislé na jejich typu (IEEE 802.1p, ATM);
- L3 prvky, které jsou schopné zajistit QoS v závislosti na typu aplikovaného protokolu (RSVP, DiffServ, proprietární implementace priorit).

Z výše uvedených informací je tedy zcela zřejmé, že pro zajištění e2e-QoS (neboli kvality služeb mezi dvěma koncovými uzly, tj. po celé přenosové trase (end-to-end) [6], je nutné zajistit dostatečnou kvalitu přenosu dat po celé trase. Čímž automaticky platí, že kvalita služby je dána nejslabší částí přenosové trasy.

1.6.2 Řízení šířky pásma v LAN se zabezpečením QoS v praxi:

To, jak vyřešit problematiku řízení šířky pásma v praxi, je možné provést několika způsoby:

a) Omezená či částečná aplikace QoS

V minulosti bylo nejobvyklejším a zároveň nejrozšířenějším způsobem předimenzování LAN části a trasování provozů ve WAN. Například využitím proprietárních priorit na směrovačích nebo použitím prvků typu Traffic Shaper, využívaných k řízení šířky pásma ve WAN sítích. Takováto řešení pak nekladou vysoké nároky na přizpůsobení síťových komponent a především pak na aplikace, které si potom nemusí umět vyžádat pásmo

ať už jeho rezervací nebo vyplněním příslušných položek L2 nebo L3 hlaviček. Kde L2 a L3 značí příslušnou vrstvu.

Taková metoda manuální aplikace priorit měla ovšem několik nevýhod, jimiž byly zejména: velká časová náročnost – především v případě většího množství podmínek jde o zdoluhavé plánování a vyplňování tabulek, dále to bylo riziko možnosti vnesení chyb – při větším množství podmínek šlo o poměrně náročné a jednotvárné vyplňování tabulek. A v neposlední řadě to byla také staticita řešení, což znamenalo, že při každé změně bylo nutné provést ruční rekonfiguraci. Na druhou stranu, tato metoda za určitých podmínek umožňuje i zachování L1 prvků (rozbočovačů).

b) Částečně automatizovaná nebo zcela automatizovaná aplikace QoS

Dnešní trendy již jednoznačně směřují k automatizaci těchto procesů. Částečná automatizace je zajišťována tak, že síťová zařízení podporují základní metody QoS a to především RSVP, DiffServ, IEEE 802.1p nebo MPLS a aplikace jsou schopné si o kvalitu služby vyžádat. Na rozdíl od předchozí metody již tedy už nedochází v takové míře k manuální konfiguraci prvků, což ovšem vyžaduje mnohem vyšší nároky kladené technologií na aplikační vrstvu a s tím úzce souvisí samotná připravenost jednotlivých komponent použitých v síti.

1.6.3 Zajištění kvality služeb po celé přenosové trase

Jestliže potřebujeme zajistit kvalitu služeb po celé délce přenosové trasy, což je garantovaná úroveň služeb mezi dvěma uzly, musí všechna použitá zařízení po cestě, a pokud je to možné, pak i oba koncové uzly schopnost podporovat technologii QoS.

V praxi to pak znamená že:

- a) Na pracovní stanici proces, který posílá data serveru, musí být schopen prostřednictvím RSVP buď rezervace pásma, nebo by měl být schopen označit rámce standardu IEEE 802.1p a pakety DiffServ. Možnost označení rámců na IEEE 802.1p neumožňují starší síťové adaptéry, schopnost rezervace pásma nebo nastavování DSCP (rozlišovací bod kódu služby - Differentiated Services Code Point) mělo v začátcích velmi málo aplikací.

Ve většině případů se tehdy nabízely dvě možnosti – změna technologie nebo ponechání těchto záležitostí na přístupovém prvku - přepínači mezi vrstvou L2 a vrstvou L1 – to ovšem vedlo na hybrid mezi částečnou automatizací a omezenou aplikací QoS manuální konfigurací prvků nebo na Policy Management - slouží pro definování a distribuci pravidel, koordinuje a řídí pravidla.

- b) Podpora IEEE 802.1p se očekává od přepínače. Pokud by ale stanice generovala rámce IEEE 802.1p a některý z prvků po cestě jim nerozuměl, dojde minimálně k takovým problémům, že rámce IEEE 802.1p/802.1Q jsou o 4 byte delší než standard a tím pádem mají i trochu jiný formát hlavičky.
- c) Ovšem jak jsem již zmínil výše, je tu i možnost že stanice, nebo aplikační proces neumí ani IEEE 802.1p ani DiffServ. Za tohoto předpokladu je pak možné na místě

přepínače mezi vrstvami L2 a L1 použít prvek, který přicházející data klasifikuje, značkuje a priority zajišťuje namísto aplikačního procesu koncové stanice.

- d) V další řadě se pak očekává podpora přepínače mezi vrstvami L3 a L1 technologií vyšších vrstev (RSVP, DiffServ), kdy by měl zároveň podporovat i IEEE 802.1p a může podporovat i funkci překladu mezi QoS funkcemi vyšších vrstev a IEEE 802.1p. Protože je to zařízení pracující na 3. vrstvě OSI, může podporovat i technologie MPLS a využívat tak případné možnosti WAN páteře.
- e) Server v tomto typu sítě by stejně jako stanice měl podporovat uvedené QoS funkce.

2 KVALITA SLUŽBY V BEZDRÁTOVÝCH SÍTÍCH

Norma, která specifikující podporu pro QoS v bezdrátových lokálních sítích má označení IEEE 802.11e [2] a funguje jako doplněk k původním normám 802.11a/b/g. Původní specifikace 802.11 protokolu pro přístup k médium (rádiovému kanálu) umožňuje dva režimy komunikace: DCF (funkce rozložené koordinace - Distributed Coordination Function) a PCF (funkce bodové koordinace - Point Coordination Function). Ani jeden z těchto režimů nerozlišuje mezi typy provozu, takže nemohou bez toho, aby byly rozšířeny, podporovat QoS.

Dnes obvykle používaný mechanismus DCF zajišťuje koordinaci přístupu k rádiovému kanálu, ale nepodporuje žádné priority přístupu. DCF je jednoduchý mechanismus vhodný pro asynchronní datové přenosy. Nepodporuje však požadavky na QoS a negarantuje zpoždění ani šířku pásma, pouze poskytuje službu best effort.

2.1 Distributed Coordination Function (DCF)

Režim DCF, fungující pro standardy 802.11 je navržený pro datové přenosy a je založený na metodě přístupu CSMA/CA (pravděpodobnostní protokol přístupu k médium s předcházením kolizím - Carrier Sense Multiple Access with Collision Avoidance). Stanice musí před vysláním nejprve naslouchat, zda nevysílá někdo jiný. Mechanismus pro obranu proti kolizím používá dvě techniky: vkládání mezery mezi vysílanými rámci IFS (mezirámcový prostor - InterFrame Space) a odklad vysílání (backoff). Interval DIFS (rozložení mezirámcového prostoru - Distributed Inter Frame Space DCF IFS) odpovídá době povinného čekání po zjištění volného vysílacího kanálu, než stanice může začít sama vysílat. Pokud v této době začne vysílat jiná stanice, musí se vysílání odložit.

Interval odkladu vysílání si každá stanice vybírá náhodně z intervalu mezi nulou a velikostí tzv. CW - okna soutěžení (okno soutěžení - Contention Window). Stále však může dojít ke kolizi. Pokud se o vysílací kanál uchází více stanic, je možné, že se požadavky stanic, které o sobě navzájem neví a pokusí se připojit ve stejný okamžik, opět odloží. Velikost okna soutěžení se při každé kolizi zdvojnásobuje (exponential backoff). Jakmile interval odkladu vyprchá a médium je volné, může stanice začít vysílat.

Příjemce nebo přístupový bod, po obdržení paketu čeká po dobu SIFS (krátkodobý rozestup mezi rámci - Short Inter-Frame Spacing, kratší než DIFS) a pak vyšle potvrzení přijetí paketu. Potvrzování je ve WLAN důležité, protože může dojít k chybě přenosu buď kvůli kolizi, nebo pro nedostatečnou kvalitu kanálu.

2.2 Point Coordination Function (PCF)

Režim PCF je určen pro synchronní datové přenosy, ale používá se jen zřídka (jedná se o volitelný mechanismus přístupu). Navíc ho lze využít pouze ve WLAN s infrastrukturou (tj. s přístupovým bodem), nikoli v ad-hoc sítích.

Režim PCF v 802.11 pracuje tak, že přístupové body WLAN periodicky vysílají rámce typu beacon, kterými sdělují stanicím v síti specifické parametry pro identifikaci a management. Mezi vysíláním těchto administrativních rámců dělí přístupový bod dobu na dvě části: doba bez boje o médium (contention-free) a doba, kdy probíhá boj o médium (contention).

Stanice s prioritními daty může na základě výzvy získat povolení ke garantovanému vysílání po dobu, kdy nemusí o médium s nikým jiným bojovat. PCF používá interval PIFS (PCF IFS) pro ohlášení intervalu bez kolizí pro stanice s prioritou vysílání. PIFS (30s pro 802.11b) je kratší než DIFS, ale delší než SIFS u režimu DCF.

2.3 Kvalita služby definovaná v 802.11e

Jak je z výše uvedených řešení zřejmé, přenosu po WLAN nedělal žádné rozdíly mezi probíhajícím typem provozu. Pro přenos citlivých dat (na zpoždění, kolísání zpoždění či ztrátu paketů) je samozřejmě potřeba jednotlivým typům paketů provozu zaručit požadované zacházení v síti při přenosu od zdrojové stanice k cíli. A právě tato norma má za úkol specifikovat řešení pro identifikaci jednotlivých tříd a zaručení kvality služby pro přenos hlasu, videa a dat po sítích WLAN [8].

Jestliže ale chceme, aby síť dokázala vyhovět požadavkům na různé typy provozu, pak musí systém být schopen provádět několik funkcí: přidělování síťových prostředků kdy jde obvykle o šířku pásma, mapování QoS typicky mezi informací o požadované QoS v IP datagramu na informace používané ve WLAN, řízení přístupu k médium kde jde především o to, zda je síť vůbec schopná danému požadavku vyhovět.

Poskytování síťových prostředků se řeší buď upřednostněním provozu, v distribuovaných metodách, nebo rezervací v centralizovaných metodách řízení přístupu. Upřednostnění je založeno na klasifikaci provozu na základě aplikace a přidělení prostředků podle třídy priority a podle dostupnosti prostředků a momentální poptávky. Rezervační mechanismy MAC jsou vhodné pro aplikace v reálném čase, protože minimalizují zpoždění při přístupu ke kanálu.

Jak jsem již uvedl výše, síť podle 802.11 jsou sítě sdílené, což tedy znamená, že všichni aktivní uživatelé, kteří jsou připojeni k jednomu přístupovému bodu, vysílají na stejném sdíleném kanále a žádné pakety nemají přednost před ostatními. To také znamená, že pokud dva uživatelé začnou vysílat současně, dojde ke kolizi. Této situaci se snažíme samozřejmě zabránit.

Druhý zmiňovaný mechanismus PCF se používá jen málokdy, umí podporovat toky dat citlivé na zpoždění, protože přístupový bod vyzývá stanice, zda mají data k odeslání. Pokud tyto data mají, získají od přístupového bodu dobu vyhrazenou k vysílání. Ale PCF stejně jako DCF nerozlišuje mezi typy provozu.

Nová specifikace IEEE 802.11e na podporu QoS rozšiřuje oba režimy přístupu k rádiovému kanálu, povinný DCF (rozšíření EDCF) i volitelný PCF (rozšíření HCF). Mimo to také zajišťuje zpětnou slučitelnost se zařízeními nevybavenými podporou pro QoS podle starších norem 802.11a/b/g.

EDCF - (pravděpodobnostní funkce rozložené koordinace - Enhanced Distributed Coordination Function) je pravděpodobnostní prioritní mechanismus pro alokaci šířky pásma na základě kategorií provozu. Každá stanice může mít až čtyři kategorie provozu na podporu osmi úrovní priority. Mapování priorit na kategorie přístupu, odpovídající jedné ze čtyř vysílacích front, které jsou odbavovány právě podle své priority. Vysílání stanic, které nepodporují QoS, se automaticky řadí do kategorie „best effort“. Každá stanice může vysílat, jakmile je médium volné, po intervalu čekání, který ovšem odpovídá dané kategorii provozu.

Doba čekání se prodlužuje se snižující se prioritou provozu, takže stanice s vysokou prioritou provozu bude čekat kratší dobu než stanice s daty pro provoz o nižší prioritě. Přístup k médiumu se tak stává řízený a to tak, že provoz s vyšší prioritou je upřednostněn na úkor provozu s prioritou nižší.

Doba čekání, která je pro každou přístupovou kategorii pevně nastavená a interval čekání ještě doplňuje náhodně dlouhé okno soutěžení CW, obojí v délce vyjádřené v násobku časových úseků (slots), která je 20 mikrosekund pro 802.11b a devět mikrosekund pro 802.11g. CW brání kolizím paketů stejné kategorie. Zdvojnásobuje svou délku po každé nastalé kolizi a po úspěšném přenosu se zase vrací na minimální hodnotu.

Další rozšíření, které 802.11e nabízí volitelně, je také centralizovaný protokol HCF (hybridní koordinační funkce - Hybrid Coordination Function), kdy si mobilní stanice vyžádá od přístupového bodu právo vysílat (přístup k rádiovému kanálu).

Vedle mechanismu QoS založeného na upřednostňování provozu nabízí IEEE 802.11e složitější rezervační mechanismus: HCCA (přístupová metoda ke kanálům řízená HCF - HCF Controlled Channal Access). Stejně tak jako u původní funkce PCF řídí i v rámci HCCA přístup ke kanálu přístupový bod za pomoci výzev k jednotlivým stanicím. QoS se bere v potaz při plánování vysílacích dob, kdy některý provoz dostává k dispozici větší část kanálu. AP přiděluje právo vysílat na základě osmi možných identifikátorů provozu SID (identifikátor provozního toku - Traffic Stream Identifier). HCCA s dobře nastavenými parametry QoS může zajistit efektivnější využití přenosového kanálu zejména u WLAN přednostně používaných pro přenos hlasu či videa, protože snižuje „ztrátové“ doby čekání.

3 KVALITA SLUŽBY V MOBILNÍCH SÍTÍCH

Oblast mobilních a bezdrátových sítí představuje nejperspektivnější směr vývoje telekomunikačních technologií. Spolu s vývojem přenosových technologií vzrůstá i zájem o služby poskytované těmito sítěmi. Stávající hlasové a omezené datové služby mobilních sítí budou brzy rozšířeny o mnohem propracovanější multimediální aplikace. Tomu nasvědčuje i technické vybavení nových koncových terminálů. Tyto nové aplikace budou mít však často odlišné požadavky na síť než současné služby.

3.1 Technologie 2G, 2,5G a 2,7G

Technologie 2G (sítě 2.generace – 2nd generation) používají ještě přepínání okruhů, ovšem nové technologie jsou už postavené na přepínání paketů a tím pádem podporují i přenos dat. Mezi druhou a třetí generací funguje i takzvaná přechodová generace 2,5G a 2,7G kam patří především technologie GPRS (obecná paketová rádiová služba - General Packet Radio Service) a EDGE (rozšířená data pro GSM evoluci - Enhanced Data For GSM Evolution).

Služba GPRS umožňuje najednou využívat až 8 GSM kanálů s výslednou kapacitou až 115 kbit/s ovšem pouze teoreticky. V praxi je přiděleno účastníku jen několik kanálů a navíc jsou také v jednom z kanálů přenášeny řídicí informace. GPRS je tedy jako paketová služba vhodná pro připojení k internetu, ačkoliv se ještě nejedná o širokopásmové připojení.

V GSM sítích je prioritně dávána přednost hlasovému provozu a v případě, že je všech osm časových úseků obsazeno hlasovými hovory musí uživatelé GPRS čekat až se nějaký časový úsek uvolní. V síti je ovšem možné vyhradit některé časové úseky jen pro GPRS takže jsou k dispozici vždy pro data a nelze je použít pro volání. Na každém kanálu může fungovat až osm vyhrazených datových úseků přičemž je možné nastavit jejich počet na každý kanál na každé základnové stanici zvlášť.

GPRS definuje požadavky na QoS pro každého uživatele v profilu QoS, který je uložený v domácím registru HLR (domovský lokační registr - Home Location Register) sítě. Uzel SGSN (zařízení obsluhující GPRS provoz v GSM sítích - Serving GPRS Support Node) je ten který se po celou dobu stará a zároveň je zodpovědný za dodržení tohoto profilu a to samozřejmě i v případě, že je uživatel mimo domácí síť. Tento QoS profil se skládá z několika indikátorů. Jsou to čtyři třídy priorit provozu, čtyři třídy zpoždění, pět tříd spolehlivosti, třídy maximální propustnosti, což je devět tříd od 8 do 2048 kbit/s, 19 tříd střední propustnosti od best-effort až po 111kbit/s.

3.2 Technologie 3G

Třetí generace mobilních 3G (sítě 3.generace - 3rd generation) sítí podporuje širokopásmové služby až do rychlosti 2Mbit. Do této kategorie spadá i technologie UMTS (univerzální mobilní telekomunikační systém - Universal Mobile Telecommunication System), která je součástí sady přijatých doporučení ITU-T (mezinárodní telekomunikační konfederace - International Telecommunication Union) kde jsou specifikovány technologie pro síť 3G. Na základě dohody byl založen normalizační projekt 3GPP (partnerský projekt třetí generace - The 3rd Generation Partnership Project) ve kterém se připravují specifikace pro UMTS. Právě

z tohoto projektu a ze specifikací 3GPP release 97 pro samotnou síť a release 99 pro rádiový přístup, vychází většina současných sítí 3G.

Technologie UMTS samozřejmě jako momentálně nejmodernější síť, která je navržena nejen pro hlasové, ale i pro datové služby podporuje kvalitu služeb QoS, tedy diferenciaci služeb sítě s ohledem na různé požadavky jednotlivých typů provozu.

Specifikace UMTS definuje čtyři třídy kvality služeb QoS, které se liší svojí citlivostí na zpoždění. Zároveň nesmíme zapomínat na omezení způsobené rádiovým rozhraním a tyto limity musíme respektovat. Z toho vyplývá, že nemůžeme očekávat ani navrhovat přesně takový mechanismus jaký byl v klasické kabelové síti, ale musíme očekávat jiné chyby, které se budou vyskytovat v závislosti na použitém rádiovém rozhraní. Je tedy jasné, že mechanismy zajišťující kvalitu služeb v buňkové síti, musí umět zabezpečit dostatečnou úroveň kvality služeb s rozumnými výsledky, s ohledem na prostředí, ve kterém pracují.

3.3 Třídy zabezpečující kvalitu služeb v sítích UMTS

Čtyři základní třídy zabezpečující kvalitu služeb v sítích UMTS jsou konverzační třída, streamovací třída, interaktivní třída a třída služeb na pozadí [1].

To, v čem se uvedené základní třídy liší, je především jejich různá citlivost na zpoždění. Nejméně citlivá na zpoždění je třída služeb na pozadí a naopak konverzační třída je na zpoždění nejvíce citlivá. K přenášení datových toků v reálném čase pak slouží především konverzační třída a streamovací třída, kde jsou ještě navíc kladeny vysoké nároky, z pohledu zpoždění, vzhledem k provádění videotelefonování, na konverzační třídu. Streamovací třída pak přenáší data pouze jedním směrem.

Pro využívání internetu, prohlížení webových stránek a jiné interaktivní aplikace je využívána interaktivní třída. Pro přijímání textových zpráv, stahování dat, přijímání e-mailů a další aplikace běžící na pozadí je využívána třída služeb na pozadí

Oddělením interaktivních aplikací od aplikací služeb na pozadí je dosaženo větší citlivosti na interaktivní aplikace. Tok v interaktivní třídě má větší prioritu než třída služeb na pozadí, a proto aplikace na pozadí využívají zdroj přenosu jen tehdy, když jej nepotřebují interaktivní aplikace. Toto má vysokou prioritu vzhledem k bezdrátovému prostředí, kde je šířka pásma proti kabelovým sítím nesrovnatelně menší.

3.3.1 Třída konverzační

Do této třídy patří jako typický představitel telefonní hovor. Vzhledem k rozšíření aplikací a stále většímu využití internetu a nových multimediálních aplikací sem dneska patří již také například VoIP tedy IP telefonie nebo videokonference. Z toho také vyplývají požadavky, které jsou kladeny na tento typ přenosů. Přenosy probíhají v reálném čase a jsou limitované lidským vnímáním, proto také je sledována především doba přenosu, která se musí pohybovat mezi 100 až 200 milisekundami, vzhledem ke konverzaci která zde probíhá. Od toho se také odvíjí maximální přípustné zpoždění, které je dáno, jak už jsem uvedl, lidským vnímáním. Limit akceptovatelného přenosového zpoždění je tedy velmi přísný. Selhání obsluhy nedostačující přenosovou rychlostí je pak vyhodnoceno jako nedostačující kvalita.

Požadavek přenosového zpoždění je proto významně nižší a mnohem přísnější, než zpoždění odbavení dotazu v interaktivní třídě.

3.3.2 Třída streamovací

V případě že uživatel sleduje například televizní přenos, video, případně poslouchá rádio v reálném čase, pak se využívá streamovací třída, která slouží právě pro jednosměrný provoz. Tato nová třída služeb vznikla vzhledem k stále vzrůstajícím požadavkům uživatelů a je více a více využívána v oblasti telekomunikačních a datových služeb. Je charakteristická tím, že časové vazby mezi informačními entitami (pakety) při přenosu musí být zachovány, přestože nemá žádné požadavky při malém přenosovém zpoždění. Kolísání zpoždění u koncového uživatele je limitováno zachováním časových vazeb mezi informačními entitami streamu. Protože vyrovnávání kolísání zpoždění provádí přijímač, největší tolerovaná hodnota bude dána vlastnostmi vyrovnávací funkce přijímací aplikace. V konečném důsledku pak přijatelné kolísání zpoždění je omezeno limity lidského vnímání.

3.3.3 Třída interaktivní

Tato třída se uplatňuje, když koncový uživatel ať už člověk nebo nějaký přístroj (počítač) vyžaduje data ze vzdáleného zařízení (server). Příkladem vyžádání dat člověkem od vzdáleného zařízení může být surfování na Internetu, správa databází, přístup k serveru, atd. Příkladem vyžádání dat přístrojů od vzdáleného zařízení je vyvolání zápisu měření, automatické databázové dotazy apod. Interaktivní přenos je klasickou datovou službou, s charakteristickým principem požadavek odpověď. Entita očekává zprávu (odpověď) v určitém čase. Zpoždění při vybavení dotazu je jednou z klíčových vlastností této třídy. Další důležitou vlastností je chybovost paketů, které budou přeneseny transparentně (s nízkou chybovostí).

3.3.4 Třída služeb na pozadí

Tato třída je využívána, když koncový uživatel, kterým je typicky počítač, posílá nebo přijímá data na pozadí. Příkladem jsou doručky emailů nebo SMS, stahování z databází nebo příjem záznamů měření. Přenos na pozadí je klasickou datovou službou, která je charakterizována tím, že neočekává doručení v daném čase, tj. nezáleží na čase doručení. Další důležitou vlastností je požadavek na nízkou chybovost paketů, které budou přeneseny transparentně.

3.4 Definice kanálů v systému UMTS

V systému UMTS jsou definovány různé typy kanálů pro přenos signálů mezi různými vrstvami podle modelu OSI. Fyzické kanály - Physical Channels - jsou používány pro vysílání datových signálů přes rádiové rozhraní. Jsou přesně definovány pomocí parametrů rádiových kanálů. Tyto parametry jsou kmitočet nosné, šířka pásma rádiového kanálu a použitý kódem. Transportní kanály - Transport Channels - jsou definovány na rozhraní mezi fyzickou vrstvou a vrstvou MAC. Používají se pro multiplexování signálů různých služeb a umožňují přenos s proměnnou bitovou rychlostí.

Z pohledu našeho zaměření nás zajímá vrstva spojová kde na rozhraní mezi vrstvami MAC a RLC (řídící rádiová vrstva - Radio Link Control), které jsou obě součástí spojové vrstvy, se používají logické kanály (logické kanály - Logical Channels). Existuje několik

různých typů logických kanálů, které jsou definovány podle typu přenášených dat (základní rozdělení: uživatelská a řídicí data). Ve směru k vyšší vrstvě RRC (Radio Ressource Control), jsou definovány rádiové nosiče RB (rádiové nosiče - Radio Bearers), které se dále dělí na signalizační rádiové nosiče SRB (signalizační rádiové nosiče - Signalling Radio Bearers), určené pro přenos signalizačních zpráv a uživatelské rádiové nosiče (uživatelské rádiové nosiče - User Plane Radio Bearers), pro přenos uživatelských signálů.

3.4.1 Logické kanály

Logické kanály, používané na rozhraní mezi vrstvami MAC a RLC, se obecně rozdělují na řídicí kanály (řídicí kanály - Control Channels) a provozní kanály (provozní kanály - Traffic Channels). Řídicí kanály se využívají pro přenos signalizace, provozní kanály se používají pro přenos uživatelských dat. Jednotlivé kanály mohou být vytvořeny buď pouze pro uplink nebo pouze pro downlink, případně mohou být vytvářeny pro oba směry přenosu současně (obousměrné řízení kanálů - Bi-directional Channels).

Řídicí kanály jsou BCCH (širokopásmový řídicí kanál - Broadcast Control Channel) – je vysílán pouze v downlinku a přenáší specifické řídicí informace o buňce, PCCH (pagingový řídicí kanál - Paging Control Channel) – je vysílán pouze v downlinku a obsahuje pagingové informace. DCCH (podpůrný řídicí kanál - Dedicated Control Channel) – je používán v obou směrech pro přenos řídicích informací k UE (uživatelské zařízení – User Equipment). Je vytvářen v případech, když UE provádí RRC připojení k síti, CCCH (společný řídicí kanál - Common Control Channel) – používá se pro oba směry přenosu a přenáší řídicí informace mezi sítí a UE. Účastnická zařízení jej využívají v případě, kdy není vytvořen kanál DCCH.

Provozní kanály jsou DTCH (vyhrazený provozní kanál - Dedicated Traffic Channel) – je kanál pro spojení point-to-point, vyhrazený pro jeden UE. Přenáší uživatelské informace a může být sestaven jak v uplinku, tak v downlinku. Není však kanálem obousměrným (obousměrný provozní kanál - Bi-directional Channel), protože může být sestaven pouze v jednom směru, CTCH (společný provozní kanál - Common Traffic Channel) – je kanál pro spojení point-to-multipoint, který je používán k přenosu specifických uživatelských informací pro všechny nebo pro vymezenou skupinu UE. Využívá se pouze v downlinku.

Všechny tyto funkce lze na úrovni linkové – spojové vrstvy využít k řízení provozu v systémech UMTS a tedy i efektivně využít k zabezpečení požadované kvality služby.

3.5 Vývoj QoS v mobilních sítích třetí generace

Z dalšího vývoje všech mobilních sítí je zřejmý odklon od čistě hovorových služeb k službám datovým. S tím samozřejmě souvisí i zcela jiný způsob posuzování kvality služeb poskytovaných konečným zákazníkům. Zároveň s rozšiřováním multimediálních aplikací musí být mobilní síť také schopná poskytovat přenosové cesty, které budou mít takové parametry, aby vyhověli požadavkům těchto nových služeb. Zaručení těchto přenosových parametrů v mobilních sítích je samozřejmě předmětem dalšího studia standardizačních komisí.

4 KVALITA SLUŽBY V BEZDRÁTOVÝCH WiMAX SÍTÍCH

4.1 Technologie WiMAX

Označení WiMAX (celosvětová součinnost pro mikrovlnný přístup - Worldwide Interoperability for Microwave Access) je vlastně pouze jaká si ochranná známka pro produkty vycházející ze specifikací standardů IEEE 802.16. Systém WiMAX se zásadně liší od systémů Wi-Fi a to už i především tím, že již v zárodku byl navrhovaný jako řešení pro metropolitní síť (MAN), přesněji bezdrátové metropolitní síť (WMAN) na rozdíl od Wi-Fi, která byla původně navrhována pro řešení lokálních sítí (LAN), přesněji bezdrátových lokálních sítí (WLAN). S tím souvisí také to, že technologie WiMAX není určena přímo pro koncové zákazníky, ale především pro operátory, kteří s ní dokážou obsloužit takzvanou poslední míli. Pomocí WiMAX tak můžou propojit jednak rozsáhlou přístupovou síť založenou na technologii Wi-Fi – hotspotů a vytvořit tak páteřní propojení (backhaul). Stejně tak může propojit síť poskytovatele připojení se zákaznickovou sítí, ať už bezdrátovou nebo klasickou, ale zároveň může propojit síť poskytovatele i s jediným koncovým bodem – samostatným počítačem zákazníka.

Z tohoto je jasné patrné, že už při návrhu parametrů tohoto typu sítí bylo myšleno na zajištění spolehlivosti, dostatečné kapacity a zajištění potřebné kvality služeb schopné zajistit kvalitní vysokorychlostní přístup BA (širokopásmový přístup - Broadband Access) na síť. Do této skupiny BWA (širokopásmový bezdrátový přístup - Broadband Wireless Access) také WiMAX patří.

Ze začátku vývoje se předpokládalo připojení pouze stacionárních stanic s rychlostí až 75Mbit/s, dnes ale s postupujícím vývojem se v této technologii rozvíjí podpora mobility a to až do 250km/h. Tím se tato technologie stává velmi významným konkurentem vyvíjejícím se standardům mobilních sítí 4. generace, známé v současnosti pod zkratkou LTE (standardy systémů GSM 4.generace - Long Term Evolution). Tyto technologie, již vylepšené o podporu HSDPA/HSUPA slibují přenosy pro koncové uživatele o rychlostech až 14,4Mbit/s pro pohybující stanice. Na rozdíl ale od WiMAX, ovšem nemůže zdaleka nabídnout stejnou rychlost pro stacionární stanice, což je u WiMAX až 75Mbit/s. To by mohlo hrát v budoucnu výrazně ve prospěch právě tohoto systému.

Aby to nebylo až tak jednoduché i pro WiMAX už roste konkurent, označovaný jako MBWA (mobilní širokopásmový bezdrátový přístup - Mobile Broadband Wireless Access), se standardy patřící do řady 802.20. Obě tyto řešení jsou si ale velmi blízká proto se zvažuje jejich začlenění do společné skupiny.

4.2 Vývoj standardů 802.16

Příprava standardů začala v roce 1999 v pracovní skupině označované jako IEEE 802.16 Working Group on Broadband Wireless Access Standard a první vytvořený standart touto skupinou se jmenoval IEEE802.16 WirelessMAN® Standard for Wireless Metropolitan Area –standard 802.16 pro bezdrátové metropolitní síť schválený v roce 2002. Předpokládal využití pásem od 10 až do 66GHz s rychlostmi od 32 do 134Mbit/s ovšem za předpokladu

přímé viditelnosti LOS (přímá viditelnost - Line of Sight). Tento standard se neprosadil a následoval další.

Jde o standard 802.16a – Fixed WiMAX z roku 2003 s revizí D z roku 2004. Tento standard již umožňoval využití frekvencí od 2 do 11GHz kde se již tolik neprojevují atmosférické vlivy a jsou více odolné. Tento posun také umožnil to, že již není potřeba přímá viditelnost a jde tedy o řešení označované jako NLOS (nepřímá viditelnost - Non Line of Sight). Zvětšil se také i teoretický dosah až na 50km. Ani tato revize ale neřešila podporu mobility – tedy pohyb základnových stanic a případné předávání mezi nimi.

Tuto problematiku začala řešit až standardy pod označením 802.16e. Přehled této standardizace a její vývoj je naznačen v tabulce 4.1. Jistou nevýhodou ovšem je snížení přenosových rychlostí, až na relativně “pouhých“ 15Mbit/s a snížení dosahu. Naopak zůstane zachována možnost NLOS – nebude nutnost přímé viditelnosti.

Tab 4.1.

Přehled standardů systému WiMAX

Standard / z roku	802.16 / 2001	802.16a-2003 /2003	802.16e / 2006 -2007
Frekvenční spektrum	10 – 66 GHz	2 – 11 GHz	< 6GHz
Nutnost LOS (Light On Sight) přímé viditelnosti	ANO	NE	NE
Poloměr buňky základnové stanice	2 – 5 km	7 – 10 km (max. 50 km)	2 – 5 km
Mobilita systému	NE	NE /částečně ANO	Nomadic / plně mobilní
Bitová rychlost	32 – 134 Mbit/s	až 75 Mbit/s	až 15 Mbit/s
	v kanálu šířky 28 MHz	v kanálu šířky 20 MHz	v kanálu šířky 5 MHz
Používaný typ modulace	QPSK, 16QAM, 64QAM	BPSK, QPSK, 16QAM, 64QAM (256QAM)	BPSK, QPSK, 16QAM, 64QAM (256QAM)
Používaná šířka kanálu	20, 25, 28 MHz	odstupňovaná	odstupňovaná
		od 1,25 MHz do 20 MHz	od 1,25 MHz do 20 MHz

4.3 Řízení provozu v IEEE 802.16

Zajištění kvality služeb ve WiMAX pevně souvisí s tím, jak tato technologie pracuje a je navržena. To znamená jakým způsobem je řízena komunikace mezi jednotlivými uzly (na úrovni podvrstvy MAC). Vše je zde řešeno centrálně, kdy existuje jedna centrální autorita, která plánuje a řídí veškerou komunikaci. Určuje, kdo a kdy může co přenášet, a sestavuje

nějaký "plán přenosů", podle kterého se pak uskutečňuje komunikace. Při plánování těchto přenosů se centrální autorita buďto přímo dotazuje jednotlivých uzlů, zda chtějí něco přenést (provádí tzv. polling), nebo jim dává šanci "přihlásit se o slovo". V případě WiMAXu je touto centrální autoritou základnová stanice, které řídí komunikaci se všemi stanicemi ve své buňce. Je zde tedy znatelný posun ke změně struktury sítě směrem k vyšší inteligenci základnové stanice. Základnová stanice s IP řadičem (IP Router) tvoří nový prvek sítě – Radio Router. Dále pak síťový manažer HA (síťový manažer - Home Agent) – řídí přenos dat v rámci jádra sítě. Další prvek v této síti Server AAA (autentizace, autorizace, přístup - Authentication, Authorization, Accounting) – má pak na starosti zpracování uživatelských dat podle nabízené služby

Tato situace umožňuje skvěle řešit řadu věcí, které mnohé jiné typy sítí neumožňují, nebo umožňují jen velmi obtížně. Je možné jakékoliv hospodaření se síťovými prostředky, ať už rozdělování kapacit mezi jednotlivé stanice nebo také průběžné změny během provozu. Zároveň tato řídicí základnová stanice rozhoduje, jak budou využívány dostupné frekvenční kanály.

U WiMAXu se jedná o dvě základní techniky využívání frekvenčního rozsahu a to TDD (časový multiplex - Time Division Duplexing) a FDD (frekvenční multiplex - Frequency Division Duplexing). Jde o způsob, jak se dostupné frekvence rozdělí buď v čase, nebo na užší frekvenční pásma a ty se jako dílčí části využijí pro komunikaci pro oba směry.

U TDD se použije dělení frekvenčního kanálu v čase na časové sloty sdružované do rámců. Každý rámec má určený počet slotů při čemž některé z nich jsou určeny pro komunikaci směrem ke koncové stanici (downstream), a jiné zase pro komunikaci od uživatele (upstream). O tom, kolik slotů v rámci má sloužit pro jeden směr a kolik pro druhý, určuje základnová stanice a může tyto počty dynamicky měnit. Tím sama určuje rozdělení dostupné kapacity mezi oba směry.

Podobně je tomu i při obousměrném rozdělení kapacity mezi jednotlivé uzly v případě techniky frekvenčního duplexu. I zde o tom rozhoduje základnová stanice, jako centrální autorita. Záleží na tom, kolik frekvenčních kanálů má základnová stanice (v rámci své buňky) k dispozici, a jakým způsobem rozděluje dostupnou kapacitu mezi jednotlivé koncové stanice. Jestli přidělí celý frekvenční kanál jednomu přenosu (k jedné koncové stanici), nebo jej rozdělí mezi více stanic. Standardy WiMAXu počítají i s tím, že kapacitu lze vyhradit buďto pro koncovou stanici jako takovou, nebo individuálně pro jednotlivá spojení, která vedou mezi základnovou stanicí a koncovou stanicí.

Způsob, jakým základnová stanice hospodaří s dostupnou přenosovou kapacitou a jakým ji rozděluje mezi jednotlivé koncové stanice či přenosy, závisí také na poskytované úrovni kvality služeb.

4.4 Kvalita služeb v IEEE 802.16.

Stejně jako jiné technologie i WiMAX řeší podporu jednotlivých typů komunikačních služeb provozovaných v síti s ohledem na jejich nároky a specifické potřeby. K tomu aby byla zajištěna potřebná kvalita pro různé typy, rozlišuje WiMAX pět základních tříd kvality služeb a to:

4.4.1 Unsolicited Grant Service (UGS)

V tomto režimu je pro každý jednotlivý přenos dopředu vyhrazen a následně garantován určitý objem prostředků (přenosové kapacity). Příslušná stanice se pak pravidelně "dostává ke slovu", aniž by o to musela základnovou stanicí znovu žádat. Hodí se například pro přenos nekomprimovaného obrazu a zvuku, kde zdroj dat generuje vždy stejný a dopředu odhadnutelný objem dat. U jiných technologií je tento režim označován jako CBR (konstantní bitová rychlost - Constant Bit Rate). V případě WiMAXu je označován jako UGC nejspíše proto, že stanice nemusí explicitně žádat o jednotlivé dílčí přenosy (proto: Unsolicited), a proto že požadované zdroje jsou garantovány (garantovaná služba - Grant Service). Služba poskytuje právo na vysílání s pevnou velikostí v periodických intervalech (to pomáhá eliminovat zpoždění a režii účastnické stanice).

4.4.2 Real-Time Polling Service (rtPS)

Tento režim je vhodný pro přenosy komprimovaného obrazu a zvuku. Velikost datového toku, který tyto přenosy generují, se mění v čase, a tak nemá smysl dopředu rezervovat a vyhradit určitou pevně danou kapacitu. Místo toho se základnová stanice pravidelně dotazuje jednotlivých koncových stanic, zda mají co k přenosu (provádí tzv. polling), musí to dělat velmi rychle, tak aby nedocházelo k většímu zpoždění (musí postupovat tzv. "v reálném čase" - real-time). U jiných technologií bývá tento režim označován jako rt-VBR (real-time Variable Bit Rate, ve smyslu: proměnná bitová rychlost).

4.4.3 Enhanced Real-Time Polling Service (ertPS)

Tento třetí režim se často neuvádí, je také určen pro datové přenosy typu VoIP ale s lepší garancí a aktivní detekcí probíhajícího provozu.

4.4.4 Non Real-Time Polling Service (nrtPS)

Tento čtvrtý režim je určen pro takové přenosy, jejichž datové toky se mění v čase - ale pro které není celkové zpoždění kritické. Proto "non real-time". Realizace tohoto režimu v rámci WiMAXu se od předchozího případu liší v četnosti a způsobu, jakým se základnová stanice dotazuje koncových stanic (jakým je realizován polling). Praktické využití je například pro přenosy velkých souborů apod. Stanice dostane právo k vysílání v intervalu menším než 1 sekunda.

4.4.5 Best Effort (BE)

V tomto posledním režimu nejsou koncové stanice poskytovány žádné garance toho, jak velká přenosová kapacita bude přidělena, ani to, kdy se "dostane ke slovu" a bude moci něco skutečně přenést. Základnová stanice se v tomto režimu sama nedotazuje koncové stanice (neprovádí tzv. polling), ale koncová stanice se sama musí přihlásit o slovo a prosadit se v soutěži s ostatními stanicemi, které komunikují ve stejném režimu.

4.5 Další vlastnosti a možnosti WiMAXu

Další vlastností WiMAXu je to, že na úrovni linkové vrstvy kterou se zabýváme, funguje spojovaně na rozdíl třeba od Ethernetu. Mezi základnovou stanicí a koncovou stanicí dojde tedy k navázání spojení a pak teprve následuje samotný přenos. Na rozdíl od Ethernetu, který ve svých základních verzích funguje nespojovaně. Tato vlastnost přináší řadu předností a to že se zařízení mohou dohodnout na požadované kvalitě služeb, z čehož pak zvolí vhodnou variantu (rtPS nebo nrtPS) nebo zda má rovnou vyčlenit určitou pevně danou kapacitu (UGS), nebo zda se má stanice přihlásit sama (BE).

S touto vlastností souvisí také zabezpečení, kdy WiMAX šifruje přenášená data (ne hlavičky) pomocí symetrického šifrování a pro distribuci klíčů využívá bezpečnější asymetrické kódování. Toto proběhne v rámci navazování spojení během procesu ověřování.

Poslední důležitou vlastností je pak samotná spolehlivost datového přenosu, kdy obvyklé opakování vysílání datových přenosů zde není efektivní, proto se obvykle u těchto datových přenosů využívá samoopravných kódů podobně jako u mobilních sítí. Jde o princip FEC (dopředné zabezpečení - Forward Error Control) pomocí rozšíření původní zprávy o přídatná data. Nejčastěji se zde používají Hammingovy samoopravné kódy.

5 SROVNÁNÍ SÍŤOVÝCH TECHNOLOGIÍ Z POHLEDU QoS A JEJICH KONVERZE

Srovnání jednotlivých síťových technologií z hlediska zajištění kvality služeb je vzhledem k jejich různosti poněkud problematické. Jednak to, že všechny technologie se neustále vyvíjejí a tím se mění jejich technické parametry a také především díky tomu, že pracují v různých prostředích na různých principech, pro které byly prioritně navrženy.

Jednotlivé technologie už od původních LAN sítí až po poslední nejmodernější technologií jako je například WiMAX jsou součástí standardizace IEEE 802.X. Přestože jednotlivé technologie musí splňovat tyto standardizace zastřešující organizace IEEE, která se snaží o zachování zpětné a vzájemné kompatibility jednotlivých systémů je jejich srovnání obtížné. Proto se zaměřím především na některé základní rysy jednotlivých technologií.

V první řadě bude zhodnoceno samotné rozdělení kvality služeb pro jednotlivé typy aplikací.

Pokud jde o LAN síť, původní technologie neměly žádné rozlišení priorit a všechny druhy provozu využívaly doručovací proces best-effort. V současnosti je v těchto sítích využíváno až osm typů priorit.

Podobně je tomu také u standardní WiFi sítě, tedy sítí podle standardu 802.11a/b/g/, které také neumí zabezpečit prioritu provozu. O všem i v bezdrátových technologiích již začíná fungovat nový standard 802.11e, který umí rozlišovat QoS kategorie přístupu. Standard IEEE 802.11e vylepšuje metody řízení přístupu DCF a PCF dvěma novými typy koordinačních funkcí EDCF (rozšířená distribuovaná koordinační funkce - Enhanced DCF Channel Access) a HCF (hybridní koordinační funkce - Hybrid Coordination Function).

HCF má dvě metody přístupu ke kanálu podobné původním metodám z 802.11 MAC. HCCA (přístupová metoda ke kanálům řízená HCF - Controlled Channel Access) a EDCA (vylepšená DCF přístupová metoda ke kanálům - Enhanced DCF Channel Access). Obě využívají kategorie přístupu (kategorie přístupu – Access Category) tj. třídy provozu TC (třídy provozu - Traffic Classes).

EDCF (rozšířená distribuovaná koordinační funkce - Enhanced Distributed Coordination Function) je mechanismus, který řídí přístup k médiu na základě kategorie přístupu. Standard 802.11e definuje čtyři kategorie přístupu a osm úrovní priority (CoS 0 až 7). V tabulce 5.1, je naznačeno mapování všech sedmi priorit a jím odpovídajících požadavků na obsluhu, které jsou odbavovány právě podle své priority. Provoz stanic, které nepodporují QoS, se automaticky řadí do kategorie „best effort“. Každá stanice může vysílat, hned jak je médium volné a po intervalu čekání, který ovšem odpovídá dané kategorii provozu.

Tab. 5.1.

Kategorie a požadavky na obsluhu podle standardů IEEE 802.11e

Kategorie	charakteristiky přenosu	AIFS	CW (Contention Window)	Celková doba čekání – násobek časového úseku (slot –time)
hlas (7;6)	VoIP s nejvyšší kvalitou - minimální zpoždění	2	0-3	2 - 5
video (5;4)	video toky, běžné i vysoké rozlišení	2	0-7	2 - 0
best effort (0;3)	interaktivní aplikace necitlivé na zpoždění	3	0-15	3 - 18
pozadí (2;1)	datové soubory	7	0-15	7 - 22

AIFS (mezirámcová mezera výběru - Arbitration Interframe Space). AIFS je doba, která se zkracuje se zvyšující se prioritou provozu. Což znamená, že stanice s větší prioritou provozu bude čekat menší dobu, než stanice s provozem s nižší prioritou. Provoz s vyšší prioritou je tak upřednostněn na úkor provozu s prioritou nižší. Doba AIFS je pro každou kategorii pevně daná respektive je nakonfigurovatelná správcem sítě. Interval čekání ještě doplňuje náhodně dlouhé okno soutěžení CW (okno soutěžení - Contention Window). Okno soutěžení, je doba soutěžení o samotný přístup k danému médiu tedy do sítě. Jak je naznačeno v tabulce 5.1. CW brání kolizím paketů stejné kategorie. Zdvojnásobuje svou délku po každé nastalé kolizi a po úspěšném přenosu se zase vrací na minimální hodnotu.

Jinak je tomu v systémech UMTS, kde v sítích třetí generace rozpoznává systém čtyři třídy provozu, kam musí případné datové toky zařadit. V UMTS si má uživatel možnost specifikovat svoje požadavky vůči síti a to vyžádáním si nosné služby (nosná služba - Bearer Service) se zvolenými parametry. Je zde možné nastavit v případě potřeby přednost zpracování například telefonních paketů před datovými. Systémové informace jsou distribuovány prostřednictvím Node B (základnová stanice v systému UMTS - Node B) podle přesného časového schématu generovaného v RNC (kontrolér rádiové sítě - Radio Network Controller). RNC přiděluje rádiové prostředky a zajišťuje řízení té části UTRAN (pozemní rádiová přístupová síť UMTS - UMTS Terrestrial Radio Access Network), která je pod jeho kontrolou a tím se mimo jiné také stará o přidělení dostatečných prostředků na základě požadavků QoS. RNC řídí všechny Node B, které jsou k němu připojeny. Z pohledu

přidělování rádiových prostředků se jeho funkce dělí podle způsobu připojení uživatelského zařízení UE (uživatelského zařízení - User Equipment) k UTRAN.

CRNC (řídící kontrolér rádiové přístupové sítě - Controlling RNC) obsluhuje (řídí) spojení k Node B. Existuje pouze jeden CRNC pro každý Node B. Hlavní funkce CRNC jsou:

- a) řízení systémových komponentů
- b) řízení provozu na používaných kanálech
- c) řízení zatížení v buňkách
- d) řízení přístupu a výběr kódu pro nová rádiová spojení v buňkách

SRNC (obsluhující kontrolér rádiové přístupové sítě - Serving RNC) obsluhuje (řídí) spojení k UE. Každý UE má jeden SRNC. Hlavní funkce SRNC jsou:

- a) vymezit prostředky na rozhraní Iu (přístupová rozhraní mezi subsystémy páteřní sítě - Iu) pro obsluhovaný UE
- b) řízení výkonu (tzv. vnější smyčka)
- c) rozhodování o provedení handoveru a použití makrodiverzity,
- d) mapování (přidělování) parametrů rádiových prostředků k parametrům transportních kanálů.

DRNC (pomocný kontrolér rádiové přístupové sítě - Drift RNC) spolupracuje se SRNC v případě spojení s využitím makrodiverzity. Jestliže spojení mezi UE a SRNC má diverzitní cestu přes jiný Node B připojený k jinému RNC, potom se takový RNC označuje pojem DRNC. Makrodiverzita je jedním z hlavních vlastností UMTS, kterým se odlišuje od systému GSM – stanice může být připojena k několika node B zároveň. Všechny tyto funkce mohou být využity pro zajištění požadované kvality přenosu.

Otázkou ovšem je, kam se bude QoS v těchto typech sítí rozvíjet jednak se rýsuje možnost využití technologie WiMAX pro mobilní datové a hovorové služby mobilních operátorů, nebo i nově vylepšené technologie Long Term Evolution a její technické a technologické možnosti.

Nejnovější je technologie WiMAX kde rozeznáváme pět typů datových toků podle přidělovaných priorit. Tato technologie, na rozdíl od Ethernetu funguje spojovaně, což ve výsledku výrazně ovlivňuje konečnou kvalitu přenosu. Navíc celá technologie WiMAX má už od počátečního návrhu zabudovanou podporu řízení kvality služeb, díky které lze na wimaxových spojích provozovat například IP telefonii nebo spolehlivě přenášet video v reálném čase, což u technologií na bázi norem IEEE 802.11a/b/g (Wi-Fi) nelze. Systém WiMAX podporuje protokoly IPv4, IPv6 apod. Koncepte systému WiMAX zcela odpovídá nové generaci struktury bezdrátových sítí pracující na bázi protokolu IPv6. Nový standard 802.16e, dokončený v roce 2006, specifikuje rádiové rozhraní pro mobilní metropolitní bezdrátové sítě MAN v pásmu 2 – 6 GHz. První varianta Wimaxu neumožňuje plnou mobilitu klienta za provozu pouze tzv. nomadic, tj. bez možnosti handoveru v aktivním stavu. V roce 2007 byla dokončena specifikace s plnou mobilitou, která nabízí obdobu celulárních sítí s mobilní IP adresou. Tu to variantu zvažují využít i stávající mobilní operátoři.

Z výše uvedených skutečností je tedy zřejmé, že pokud se týká nastavení priorit různých typů datových toků, nebude zcela jednoduché zařazení jednotlivých datových toků nebo služeb při přechodu mezi různými typy prostředí z hlediska nastavení priorit.

Další problémem v zajištění kvality služeb mezi jednotlivými technologiemi je délka a typy datových buněk případně označování priorit, které jednotlivé technologie používají a samozřejmě taky typy komunikace specifické pro dané prostředí.

Další možné dočasné řešení pro podporu QoS ve WiFi vytvořila aliance pod označením WMM (bezdrátová multimédia - Wireless MultiMedia), původně WME (rozšíření bezdrátových mechanismů o multimédia - Wireless Multimedia Extensions).

WMM podporuje pouze některé prvky 802.11e, jako označování rámců podle priorit a odpovídající řazení do front (označování rámců a řazení do front - priority tagging and queueing). WMM se neomezuje pouze na hlasové aplikace, ale zahrnuje všechny zvukové, obrazové i multimediální aplikace probíhající v reálném čase. Vychází z řešení podpory QoS pro mechanismus rozlišených služeb fungujícího ve spolupráci s protokolem IP (mechanismus diferencovaných služeb - Differentiated Services) a rozděluje provoz do čtyř úrovní priorit, jak je uvedeno v tabulce 5.2. Nejvyšší prioritu má hlas, pak video, následuje best effort a vše ostatní (např. tiskové úlohy, přenosy souborů). Tyto úrovně priorit se shodují s označením priorit podle 802.1d používaným v pevných LAN, takže podpora QoS může být jednotná.

WMM je dostačující pro nižší rychlosti, které vyhovují VoIP, zatímco plnohodnotné řešení podle 802.11e budou potřebovat náročnější aplikace vyžadující rezervovanou šířku pásma, typicky video streaming.

V roce 2005 se pracovalo na certifikaci WMM-SA [6] (řízený přístup pro bezdrátová multimédia - WMM Scheduled Access), který byl odvozen od schválené normy 802.11e. Standardy 802.11e kromě upřednostňování provozu citlivého na zpoždění, které je součástí WMM, podporuje také rezervaci šířky pásma (simuluje tradiční realizaci hlasové komunikace pomocí přepojování okruhů).

Následující tabulka 5.2 porovnává přístupové třídy, které podporuje WMM a převádí je na značky v rámci standardu 802.1d.

Tab. 5.2 Priority a požadavky na obsluhu podle WMM

Přístupová třída	Popis	Značka 802.1d
WMM hlasová priorita	nejvyšší priorita, nabídne více současných VoIP hovorů s nízkou latencí a dobrou kvalitou zvuku	7, 6
WMM video priorita	upřednostňuje video provoz před ostatním datovým provozem (mimo audio provozu). Jeden kanál 802.11g nebo 802.11 a/h umožní přenést 3 až 4 klasické televizní přenosy nebo jeden HD TV stream	5, 4
WMM normální	provoz z aplikací méně náročných na kolísání, zpoždění, ale citlivé na dlouhé prodlevy, jako například surfování po internetu	0, 3
WMM pozadí	provoz s nízkou prioritou, který není náchylný na zpoždění nebo proměnlivou velikost šířky přenosového pásma, jako je tisk nebo stahování souborů.	2, 1

Z výše uvedené tabulky je zřejmé že určité pokusy o začlenění různých typů QoS jednoznačně jsou. Nicméně je to problematické a pokud se máme věnovat právě linkové vrstvě, zde to jednoznačně záleží na použitých zařízeních. Ve chvíli kdy zařízení nepodporuje QoS jsou data zařazena do kategorie best-effort, což je ovšem zřejmé z popisů výše.

Tab. 5.3 Celkové srovnání síťových technologií z pohledu QoS

Technologie	Ethernet	WiFi	UMTS	WiMAX
podpora QoS v původních verzích	ne	ne	ano	ano
podpora QoS v nových verzích	ano / IEEE 802.1.p/Q	ano / IEEE 802.11e	ano	ano
počet rozlišovaných kategorií provozu	8	4	4	4(5)
mobilita systému	ne	ne	ano	ano
vícenásobný přístup		CSMA/CA	TDMA/CDMA	OFDMA/(S)OFDMA
maximální datový tok	10Gbit/s (podle druhu přenos. média)	14,4Mbit/s (HSDPA)	54Mbit/s (OFDM pro nepohybující se MS)	75Mbit/s (pro nepohybující se UE)
orientace spojení	paketově /spojově	paketově	paketově /spojově	spojově
mechanismy QoS	DiffServ, IntServ, MPLS, ATM	WDM	logické kanály sestavující spojení	řízeno přímo základnovými stanicemi

6 KONVERGENCE MEZI SYSTÉMY

Jak je naznačeno výše, některé typy přímé podpory kvality služeb podle rozlišení datových toků mezi WiMAX a IP jsou již obsaženy v navrhovaných standardech pro jednotlivé typy sítí. Tato podpora ovšem musí vycházet z vlastní konvergence jednotlivých systémů a jejich architektury. Toto také přímo souvisí se zajištěním kvality služeb. Další možností je mimo klasifikace datových toků také rezervace části síťových prostředků pro plánovaný provoz. Tato situace může nastat při přechodu z prostředí IP na WiMAX kdy sítě WiMAX jsou spojově orientovány. Norma IEEE 802.16 definuje pouze nejnižší dvě vrstvy síťové architektury. Přestože existují konvergenční podvrstvy, které jsou určeny na podporu vyšších protokolů, zejména IP pomocí které můžeme zabezpečit i požadovanou kvalitu přenosu, některé vlastnosti a potřeby IP nejsou zcela zohledněny. Proto se standardizacím přenosu IPv4 a IPv6 přes síť WiMAX věnuje také několik odborných skupin. [12]

Jejich záměrem je definovat problémy při uplatnění komunikace pomocí IP protokolu na síťové vrstvě přes infrastrukturu typu IEEE 802.16, které mohou nastat kvůli nedostatkům podvrstvy MAC pro přenos IPv4 nebo IPv6 datagramů.

Když se zaměříme právě na konvergenční podvrstvy, víme, že nejbližší k třetí, síťové, vrstvě má nejvyšší část MAC, tedy podvrstva konvergence CS (podvrstva konvergence - Convergence Sublayer), která je zodpovědná za přidělování přenosových služebních datových jednotek SDU přicházejících od aplikací vyšších vrstev ke správnému odchozímu transportnímu spojení. Norma 802.16 definuje dva typy konvergenční podvrstvy. Jednak je to vrstva paketová, která má tři specifické typy mapování a ATM s přímým mapováním. Standardizace se zaměřuje na dvě specifické části paketové konvergenční podvrstvy, a to IP a 802.3 Ethernet, které specifikují přenos a odpovídající zapouzdření paketů IP, tedy rámců Ethernetu po rádiovém spoji. Kromě IP a Ethernet CS ještě existuje třetí typ na podporu paketů se značkami 802.1 Q VLAN[12].

Konfiguraci IP přes 802.16 je složitá proto, že infrastruktura WiMAX poskytuje službu se spojením (služba se spojením - connection-oriented), navíc v dvoubodovém režimu komunikace (dvoubodová logická topologie na úrovni MAC, ovšem v rámci vícebodové fyzické topologie) mezi účastnickou stanicí SS (účastnická stanice - Subscriber Station) a základnovou stanicí BS. IP podsíť ovšem není běžně dvoubodová, ale zahrnuje topologicky síť více uzlů v určité oblasti se stejným prefixem IP adresy. IP adresy se dále nedělí, pouze jednotlivá rozhraní mají specifické IP adresy. Přitom IP CS i ethernetová CS očekávají jiné vlastnosti od vyšší vrstvy. A to především směrování IP, v případě Ethernetu pak přepojování na úrovni mostů. Charakteristiky spojové vrstvy pod IP se pak mohou měnit v závislosti na použité konvergenční podvrstvě [12].

Adresace na úrovni MAC není závislá na topologii, ale používá jedinečnou 48-bitovou adresu pro účastnické stanice. BS používá MAC adresy v případě Ethernet CS, ale jinak závisí na 48-bitovém identifikátoru. O jednotlivých MAC adresách se vzájemně stanice informují při připojení SS do sítě dané BS. Transportní spojení mezi základnovou a účastnickou stanicí se naváže prostřednictvím sekvence 3 signalizačních zpráv v rámci MAC. Ty jsou obvykle iniciovány ze strany základnové stanice. Teprve na základě úspěšného ustavení transportního spojení může následovat přenos uživatelských dat. Pro každý směr mezi SS a BS existuje samostatné, jednosměrné transportní spojení. A ke každému z těchto spojení přísluší sada parametrů včetně bezpečnostních šifer a parametrů potřebných právě pro

požadované zabezpečení kvality služby QoS. Dopředné transportní spojení (od BS směrem k SS) je svým charakterem skupinové, pokud je zpřístupněné základnovou stanicí více koncovým stanicím. Zpětné spojení od SS k BS je vždy individuální. IEEE 802.16 PDU sestává z obecného záhlaví MAC, několika volitelných podzáhlaví a datového obsahu. V záhlaví MAC pro 802.16 se neobjevují žádné adresy, ale pouze identifikátor příslušného spojení CID (identifikátor spojení - Connection IDentifier).

Konvergenční podvrstva má za úkol mapovat vyšší službu a vlastní spojovou službu se spojením, a to prostřednictvím klasifikace (přidělení odchozího transportního spojení dané SDU podle spravované tabulky klasifikátorů) a zapouzdření. Klasifikace pro Ethernet CS jsou následující: pakety přes 802.3Ethernet CS; IPv4 přes 802.3Ethernet CS; IPv6 přes 802.3 Ethernet CS; 802.3 Ethernet s kompresí záhlaví a 802.3 Ethernet s rozšířenou kompresí záhlaví podle příslušného protokolu. Prvně zmíněná paketová klasifikace ovšem nespecifikuje verzi IP, zatímco klasifikátory pro IP CS důsledně odlišují pakety IPv4 klasifikátor 1 a IPv6 klasifikátor 2. Implementace 802.16 může podporovat více typů CS, které spolu s klasifikací definují typ datového rozhraní pro vyšší vrstvy.

Podsít'ové modely umožněné například pomocí RFC 5154 nabízí IP jak pro IP CS, tak Ethernet CS. Z hlediska přístupu k adresaci vhodné pro 802.16 lze rozlišovat tři následující modely. Jako první je to model dvoubodového spoje, dále ethernetový model a model spoje se sdíleným prefixem IPv6. Pokud jde o model dvoubodového spoje, je každá zákaznická stanice na jiné podsíti, kterou sdílí pouze se základnovou stanicí, tedy přístupovým směrovačem. V takovém to případě by bylo vhodné využít přenosového protokolu PPP (Point-to-Point Protocol; RFC 1661), ale 802.16 nedefinuje konvergenční podvrstvu podporující tento protokol, a proto zapouzdření tímto protokolem není možné.

V případě ethernetového modelu všechny stanice pod jedním přístupovým směrovačem sídlí v jedné IP podsíti a to i v případě, když jsou připojeny k různým BS. Nastane-li tato situace, vyšší vrstvy očekávají stejnou funkčnost, která platí u Ethernetu. Což je podpora skupinového a všeobecného vysílání. Tady by bylo vhodné použít Ethernet CS, ale z principu to není možné. Standard 802.16 MAC nemůže podporovat skupinové vysílání, protože má charakter dvoubodového spoje. Proto se musí uplatnit mechanismus na podporu skupinového vysílání, i když časté vysílání skupině nebo dokonce všem stanicím by mělo být zamezeno, aby zbytečně nemusely stanice opouštět úsporné režimy spánku/klidu.

V modelu dvoubodového spoje existují problémy s podporou IPv4 a IPv6. Zjišťování fyzické MAC adresy cílové stanice při znalosti IP adresy cíle se u IPv4 klasicky provádí pomocí protokolu ARP (protokol pro získávání adres - Address Resolution Protocol). V rámci dvoubodového spoje není nutné zjišťovat adresu jediného možného cíle a v případě IP CS se ani v MAC rámci 802.16 adresa neuvádí. ARP je tak nadbytečný a ani ho v IP CS provést nelze. V případě IPv6 je mapování síťové a fyzické adresy funkcí IP vrstvy, k čemuž se využívá protokol zjišťování sousedních zařízení. Nelze tedy zablokovat tento protokol, aby bylo možné detekovat nedostupnost souseda[12].

Každá stanice potřebuje pro svou IP komunikaci znát adresy směrovače. Základnová stanice proto potřebuje pravidelně inzerovat směrovač se samostatným IP prefixem individuálním způsobem pro každou stanici. Přístupový směrovač je nejbližším následujícím skokem pro jakoukoli komunikaci po IP. Každá stanice musí mít svůj IP prefix, aby ji bylo možné lokalizovat v různých IP podsítích. Když se stanice přesune mezi základnovými

stanicemi v rámci téhož přístupového směrovače, ten musí redistribuovat stejný prefix podsítě, který stanice používala u předchozí základny.

V modelu typu ethernetového spoje musí odesílatel zjistit cílovou adresu, která slouží základnové stanici nebo mostu pro rozhodnutí, kam poslat ethernetový rámec po jeho rozbalení z rámce 802.16. Samotná cílová MAC adresa ale není potřeba pro přenos samotného rámce 802.16. Zjištění cílové adresy je třeba provést klasickou metodou – protokolem ARP nebo protokolem na zjištění sousedů NDP (protokol na zjištění sousedních zařízení - Neighbor Discovery Protocol). Příslušné zprávy je potřeba filtrovat, aby se stanice zbytečně „nebudily“. Stejně tak v případě inzerování adresy směrovače.

Stanice u ethernetového modelu sdílejí stejnou IP podsít' spolu s přístupovým směrovačem. To ale neznamená, že stanice spolu mohou přímo komunikovat s použitím MAC adres v rámci Ethernet CS. K tomu je třeba doplnit podporu pro přepojování přes komunikační mosty. Jak je z uvedených podrobností o konvergenci zřejmé realizace dvoubodového spoje má ještě mnoho otázek k vyřešení.

Momentálně probíhají dvě standardizace ke specifikaci IPv6 v sítích 802.16. Jednak je to RFC 5121 specifikující přenos datagramů IPv6 přes síť typu 802.16, s využitím IPv6 CS. V tomto případě se doporučuje přidělení jedinečného prefixu každé stanici s tím, že každá stanice má možnost používat více identifikátorů v rámci daného prefixu, včetně náhodně generovaných identifikátorů rozhraní. Vlastnosti a způsob práce IPv6 zůstává [12].

6 KONVERZNÍ PROCEDURY

Některé typy sítí a jejich řešení umožňují přímou a automatickou konverzi mezi sebou, jak je popsáno v dřívějších kapitolách. Jednotlivé systémy ale mají také své specifické možnosti zajištění kvality služeb, které nejsou přímo mezi jednotlivými systémy podporovány. V tomto případě je třeba navrhnout možný způsob řešení. Jednak lze využít automatických operací, které probíhají při předávání datových toků mezi zařízeními různých typů sítí. Jde o rozbalení paketu, kdy zařízení v síti zjišťuje informace z posílaných dat nutné k postoupení do dalšího doručovacího procesu. Tady je pak možné využít struktury, která nabízí různé možnosti signalizace úrovně priority doručovaných dat. Ostatně na tomto principu fungují popsané automatické konverze mezi datovými toky s určitou uživatelskou prioritou. Podmínkou ale je, aby zařízení, přes které tyto toky prochází, uměly mapovat tyto požadavky.

V případě ale, že je kvalita služby zabezpečována jiným způsobem, jako je například dojednání určitých přenosových prostředků pro daný přenos, bez ohledu na to zda přenášená data mají klasifikátory pro příslušný datový provoz, může nastat problém. Zde by bylo asi nejjednodušším řešením, aby dojednané parametry vyhrazených datových prostředků, umísťovaly do takových to dat, tekoucích přes tyto dohodnuté spojení nějaké identifikátory, aby při přestupu do jiného prostředí mohl tento systém, na základě těchto identifikátorů, vyhradit opět příslušné síťové prostředky, už ale s ohledem na svou vlastní infrastrukturu a okamžité možnosti. V podstatě by šlo o to, rozdělit provoz na základě několika bitových značek, umístěných v záhlaví podobně jako je tomu v případě přenosových tříd.

Zde se nabízí také přímé řešení a to u dostatečně vyspělých síťových zařízení. Pokud by šlo například o WiMAX, kdy by přicházející požadavek z Ethernetu specifikoval pouze

požadavek na vyhrazené spojení bod – bod s určitými parametry pro plánovaný přenos, mohla by základnová stanice tohoto systému rozhodnout o způsobu a velikosti přidělených prostředků pro koncového uživatele již na základě žádosti z Ethernetu a navíc může provoz podle skutečné situace ještě následně ovlivňovat a to při dodržení požadované kvality služeb. Tím se dosáhne mnohem lepšího využití síťových prostředků, při zachování požadované kvality přenosu. V následujícím textu se pokusím navrhnout způsob jakým toho dosáhnout.

V tomto případě by šlo o centralizované přidělování kanálů ve spojených WiMAX a WiFi sítích. WiMAX kontrolery a uzly by zajistili díky svým schopnostem prodloužení páteří pevné sítě směrem k uživateli. Navrhované centralizované přidělování kanálů ve WiMAX sítích by provedl kontroler (případně řídicí uzel). Podstatou je, aby pravidelně každá BS (základnová stanice - Base Station) nebo RS (rádiová stanice - Radio Station) poslala souhrn svého dopravního zatížení ke kontroleru nebo řídicímu uzlu, včetně provozu na všech vzájemných spojkách. Kontroler přidělí rádiové zdroje každé BS a RS ve dvou hladinách. V nejvyšší úrovni půjdou tyto informace o probíhajícím provozu, druhý kanál s vhodnou velikostí je přidělen zároveň více stanicím pro ostatní provoz.

Měřitelný OFDMA (SOFDMA), který je standardní součástí fyzické vrstvy ve WiMAX, připouští kanály o parametrech 1,25; 5; 10; nebo 20 MHz. V nižší úrovni se mezi BS a RS jednotlivě určuje počet subkanálů a časových úseků přidělených jednotlivým RS nebo pohyblivé stanice ve frekvenčních a časových oblastech, které jsou pro daný kanál a zařízení přípustné. Pro dosažení komunikace bez interferencí v mobilních a rádiových sítích, každý kontroler potřebuje znát a vyhodnotit interference uvnitř a vně oblasti, kterou řídí. Po vypočtení parametrů pro přidělování kanálů jsou výsledky kontrolem distribuovány k subsystémům základnových stanic BSS a rádiových stanic RSS pod které spadají a také o tomto pošlou zprávu ke kontrolerům sousedních oblastí.

Systém přidělování distribučních kanálů ve WiFi sítích by mohl fungovat asi takto. Protože WiFi sítě fungují v bezlicenčním pásmu, které je společné mnoha jiným bezdrátovým systémům a mnoha uživatelům, je zde reálné nebezpečí, že by interference mohla přijít jak zevnitř systému, tak i z dalších vnějších systémů. Je jasné, že v takových sítích musí fungovat nové standardy 802.11 MAC protokolů, aby systém přidělování kvality služeb vůbec fungoval. Jestliže je toto zaručeno, pak samotný distributivní přístup, ve kterém navzájem komunikují společné uzly, určují kanály pro své systémy založené na místní informaci a nastaví tak podmínky přístupu ke kanálu nejrychleji. Podobně jako přidělování kanálů v moderních mobilních sítích, navrhuji dvouúrovňový kanálový systém a použití určitého schématu, abychom mohli dosáhnout účinného řízení kanálů právě v sítích se standardy 802.11. Nejvyšší úroveň se bude zabývat rovnoměrným vyvážením QoS a zároveň bude mít povědomím o přidělování kanálů se zaměřením na minimalizaci využívané šířky pásma v jednotlivých kanálech. Dolní část systému, rozvrhne používání uvnitř stejného kanálu regulováním maximálního počtu jednotlivých spojení, které základnová stanice umožňuje provozovat v kanálu.

Hlavním úkolem vyváženého přidělování kanálů v sítích 802.11 by bylo, docílení rovnováhy mezi mnoha různými kanály napříč celou sítí. Toto může být mimo jiné také dosaženo minimalizováním rozdílů ve využívání kanálů uvnitř sítě. Odhad využívání kanálu by byl založen na dopravním zatížení, množství provozu v jednotlivých spojeních a poměru ztrát. Poměr ztrát je poměr neúspěšných k úspěšným přenosům u spojení, které jsou provozovány na stejném kanálu a jsou uvnitř interferenčního rozsahu daného kanálu. Dopravní zatížení spojení mezi jakýmkoliv dvěma uzly uvnitř komunikačního rozsahu, by

bylo měřeno ve směrovací vrstvě, včetně kontroly směrovacích dat a paketů kontroly topologie v optimálně probíhajícím směrování.

Provozy vznikající z transportní vrstvy měřením uzlu, a datový provoz ze sousedních uzlů, které potřebují být doručeny, by mohly být upřednostněny. Očekávaný odcházející provoz a poptávka po spojení by byly sledovány a případně vypočteny.

Vzhledem ke známému dopravnímu zatížení ve směrovačích, je očekávaný součet provozu na spojích základnových stanic v uzlech možné relativně jednoduše vypočítat. Další využití kanálu v sousedních uzlech, by bylo zvažováno na základě součtu provozů všech spojů nastavených na stejném kanálu, uvnitř jejich interferenčního rozsahu. Spoje uvnitř této oblasti, které jsou nastaveny ve stejném kanálu patřící ke stejnému kontroleru. Žádosti o určité hodnoty provozu mohou být opatřeny měřítkem určité šířky pásma a dovolili by tak přesné srovnání mezi spojeními proměnných kapacit.

Pomocí inteligentní heuristiky by bylo možné najít největší rozdíl ve snížení zatížení v místní oblasti. Zde by se pak mohl objevit problém s nalezením rozhraní a přidělením jeho kanálu a tím dosažení maximální změny. Pokud se to ale podaří, následně by se to projevilo jako změna napříč nastavením všech dostupných kanálů v lokální oblasti a tím i v centralizovaném řídicím uzlu.

Docházelo by k množství změn při využívání kanálů, až by byla dosažena rovnost, která by byla ideální změnou zatížení. Proto používání této nebo podobné metody, by zajistilo to, že každý uzel se pokusí vyrovnat využívání kanálu tím, že přeladí aktuální rozhraní na to, které je nejméně využíváno. Množství dopravního zatížení na jednotlivých spojích a v jednotlivých kanálech by se používáním tohoto způsobu přidělování snížilo. Došlo by tak k zajištění skutečného posunu v rozložení zatížení. Tím by se mohly optimálněji využít vzácné rádiové prostředky v místní oblasti.

Cílem tohoto kroku by bylo ovládat kanálové využití všech stanic sdílejících stejný kanál a to spravedlivým způsobem, založeném na jejich provozních požadavcích. Navrhují dvoufázový přístup k dosažení cíle kvalitní techniky provozu. V prvním kroku, by daná vstupní provozní matice vyřešila problém směrování a spojení s vhodnou šířkou pásma. Tento úkol by mohl být formulovaný jako lineární programovací problém. V dalším kroku by jsme pak přizpůsobili samotné toky, které jsou definovány v 802.11e, případně podobných standardech. Je jasné, že by tento způsob řízení přidělování kanálů byl určitým zatížením pro síťové uzly či základnové stanice, na které by tak byly kladeny vyšší inteligenční požadavky, ale efektivita využití rádiových kanálů by byla dotažena na maximum. Bohužel vzhledem ke složitosti systému jsem neměl možnost ověřit navrhovanou teorii.

7 ZÁVĚR

V této práci jsem se pokusil zmapovat problematiku zabezpečení kvality služeb v jednotlivých typech sítí. V úvodu jsem se nejprve obecně zabýval problematikou QoS z pohledu historického vývoje a nárůstu vlivu této problematiky do současných komunikačních technologií.

V další části jsem se pokusil podrobněji rozebrat strukturu a složení jak samotné kvality služeb a jejich tříd, či požadavků na nich plynoucích, tak především její strukturu a

řešení v Ethernetu. Zde jsem se pak zaměřil na řešení této problematiky na úrovni linkové vrstvy, ale také jsem se okrajově dotknul i jiných způsobů řešení, neboť se tato technologie často prolíná mezi jednotlivými vrstvami ISO-OSI. I to je jeden z důvodů velké složitosti popisované problematiky. Dalším aspektem je neustálý vývoj, jak technologií, tak především normalizačních standardů, které jsou neustále vyvíjeny. I těmito jsem se v rámci popisu vlastností QoS v LAN zabýval a zde jsem čerpal především ze schválených standardů pro technologii LAN IEEE 802.1Q a navazujících 802.1p, které definují požadavky na tyto služby v uvedeném prostředí a mají je sjednocovat. Částečně pak popisují možné způsoby zabezpečení QoS v praxi ať už zajištění přenosového pásma, nebo zabezpečení služby end-to-end, právě v závislosti na výše zmiňovaných standardech.

V druhé části se pak zabývám zajištěním kvality služeb v prostředí bezdrátových sítí. Opět se nejprve snažím mapovat vývoj od původních protokolů přístupu k médiu až po současné metody. Dále jsem se pak snažil popsat jednotlivé požadavky a technologie zabezpečení QoS v souvislosti s novými standardy pro toto prostředí, které vycházejí z původních standardů 802.11a/b/g a k nim navazující norma zabývající se přímo problematikou QoS pro toto prostředí 802.11e. Zde se pak věnuji jednotlivým mechanismům a jejich přístupům k médiu, právě v závislosti na požadované kvalitě služby pro jednotlivé typy datových přenosů. Stručně jsem se je pokusil charakterizovat a shrnout jejich základní parametry.

Ve třetí části se pak zabývám mobilními sítěmi. V této oblasti jde především o poslední generace mobilních sítí, které již umožňují paketový nebo širokopásmový přístup k datovým službám. Mapuji zde jejich vývoj právě s ohledem na možnosti zabezpečení kvality služeb, které se mění zároveň s jejich vývojem. Vycházím z normalizačního projektu 3GPP, který je na tuto problematiku zaměřen také. Odtud jsou odvozeny i jednotlivé třídy datových služeb definované pro toto prostředí.

Čtvrtá část je pak zaměřena na jednu z nejmodernějších technologií bezdrátového přenosu a tou je WiMAX. Zde popisují postupný vývoj jednotlivých standardů pro WiMAX a také samotnou technologii. Stejně jako jiné technologie rozeznává i WiMAX různé třídy provozu pro zajištění kvality služeb. Na rozdíl od jiných tato technologie je už navržena tak že funguje spojovaně, což je pro zajištění kvality služeb výhodou.

V páté kapitole se snažím porovnat jednotlivé typy zajištění kvality služeb ve všech technologiích a popisují, kde mají podobné vlastnosti. Zde se podrobně zabývám jednotlivými kategoriemi datových přenosů a jejich rozčlenění do různých tříd provozu v daného systému a prostředí. Zároveň jsou zde porovnány tyto kategorie v různých typech sítí a jejich vzájemnou konverzi při přestupu z jednoho prostředí do druhého.

V šesté části se zabývá konverzními procedurami mezi systémy. Pokouším se zde specifikovat určité vlastnosti a náměty na to jak zabezpečit přenositelnost nastavení požadované kvality služeb při přechodu z jednoho rozhraní do jiného. Navrhuji možnosti jak tyto požadavky zabezpečit případně zajistit přímo síťovými prostředky za pomoci využití inteligentních uzlů a kontrolerů rádiového provozu.

Je samozřejmé, že uvedená problematika nutně potřebuje vzájemnou kompatibilitu mezi jednotlivými druhy datových sítí a přenosů. Těmito projekty se již zabývají jednotlivé skupiny sdružené pod hlavičkami různých organizací, které se touto problematikou zabývají. Zde může jít například o projekt typu EuQoS který se snaží sjednotit tyto parametry v rámci

svého projektu pro celé spektrum komunikačních technologií, nebo například Flash OSDM (Fast Low Latency Access with Seamless Handoff, Orthogonal Frequency Division Multiplex), který se snaží sjednotit parametry Bluetooth. Samozřejmě hlavním hráčem na poli sjednocování a standardizace těchto systémů je organizace IEEE a jejich standardizační projekty, nebo na poli GSM pak organizace 3GPP, která se zabývá standardizacemi pro GSM systémy třetí a čtvrté generace. Je tedy zřejmé, že další vývoj v této problematice je nevyhnutelný a nejen to, je naopak velmi žádoucí.

LITERATURA

- [1] 3GPP, *3GPP TS 23.107 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Quality of Service (QoS) concept and architecture (Release 7)*, 3GPP, Valbonne, 2007., [cit. 17. 12. 2007]., Dostupné z URL: <<http://www.3gpp.org/ftp/Specs/>>.
- [2] IEEE Computer Society, *802.11e IEEE Standard for Information technology-Telecommunications and information exchange between systems- Local and metropolitan area networks- Specific requirements 8: Medium Access Control (MAC) Quality of Service Enhancements*, IEEE, New York 2005., [cit. 17. 12. 2007]., Dostupné z URL: <<http://standards.ieee.org/getieee802/portfolio.html>>.
- [3] IEEE Computer Society, *802.1Q IEEE Standard for Local and metropolitan area network Virtual Bridged Local Area Networks*, IEEE, New York, 2006., [cit. 17. 12. 2007]., Dostupné z URL: <<http://standards.ieee.org/getieee802/portfolio.html>>.
- [4] ISDN Server., *Síťový speciál: Jak na privátní podnikové sítě, Techniky QoS a jejich využití* [online]. Vydává: ACES, s.r.o., Copyright © 1997 - 2003, Dostupné z URL: <<http://www.isdn.cz/prilohy/vpn/art.php?id=2>>.
- [5] KABELOVÁ A., DOSTÁLEK L., *Velký průvodce protokoly TCP/IP a systémem DNS*, 2. aktualizované vydání, Praha: Computer Press, a.s. 2000. ISBN 70-7226-323-4
- [6] KLAŠKA L., *Základní parametry sítě (1), (2), (3)*, [online]. 2006, Publikováno: prosinec 2006, Copyright © 1999 - 2007 Svět sítí & Infinity, a.s., Dostupné z URL: <<http://www.svetsiti.cz/view.asp?rubrika=Tutorials&clanekID=326>>.
- [7] PETERKA J., *Protokol IP a kvalita služeb QoS*, [online]. 1999, Vyšlo v Softwarových novinách č. 10/99, Dostupné z URL: <<http://www.earchiv.cz/a912s200/a912s217.php3>>.
- [8] PUŽMANOVÁ R., *Moderní komunikační sítě od A do Z*, 2. aktualizované vydání, Brno: Computer Press, a.s. 2006., [cit. 17. 12. 2007]., ISBN 80-251-1278-0
- [9] PUŽMANOVÁ R., *TCP/IP v kostce*, Praha 2004: Computer Press, a.s. ISBN 80-7232-236-2,
- [10] Vonage.nmhoy, *What is Qos?* [online]. 2006, last revision April 2006. Dostupné z URL: < <http://vonage.nmhoy.net/qos.html> >.
- [11] Wikipedia, *the free encyclopedia, Quality of Service*, [online]. 2007, last revision August 2007. Dostupné z URL: < http://en.wikipedia.org/wiki/Quality_of_service>.
- [12] PUŽMANOVÁ R., *Problematika přenosu IP přes sítě WiMAX*, [online]. Publikováno: duben 2008, Copyright 2005 © WiMAX | Provozovatel ASPRA a.s. Dostupné z URL: < http://www.wimax.cz/index.php?option=com_content&task=view&id=214&Itemid=1>.