



VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

BRNO UNIVERSITY OF TECHNOLOGY



FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH  
TECHNOLOGIÍ

ÚSTAV TELEKOMUNIKACÍ

FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION  
DEPARTMENT OF TELECOMMUNICATIONS

## REALIZACE ZAJIŠTĚNÍ KVALITY SLUŽEB V BEZDRÁTOVÉ SÍTI

QUALITY OF SERVICE ASSURANCE INTRODUCTION IN WIRELESS NETWORK

BAKALÁŘSKÁ PRÁCE

BACHELOR'S THESIS

AUTOR PRÁCE

AUTHOR

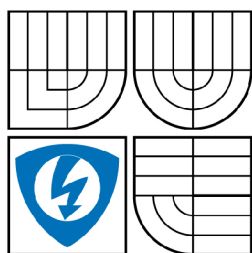
MARTIN BRANČ

VEDOUCÍ PRÁCE

SUPERVISOR

Ing. JIŘÍ HOŠEK

BRNO 2009



VYSOKÉ UČENÍ  
TECHNICKÉ V BRNĚ

Fakulta elektrotechniky  
a komunikačních technologií

Ústav telekomunikací

# Bakalářská práce

bakalářský studijní obor  
**Teleinformatika**

**Student:** Martin Branč

**ID:** 78049

**Ročník:** 3

**Akademický rok:** 2008/2009

## NÁZEV TÉMATU:

**Realizace zajištění kvality služeb v bezdrátové síti**

## POKYNY PRO VYPRACOVÁNÍ:

Seznamte se s možnostmi zajištění kvality služeb (QoS) v bezdrátových sítích. Podrobně prostudujte a popište standard 802.11e. Vytvořte bezdrátovou lokální síť, v které nakonfigurujete mechanismus pro zajištění kvality služeb v dané síti. Pomocí nástroje IxChariot vygenerujte ve vytvořené bezdrátové síti provoz skládající se z několika typů síťových služeb a následně proveďte podrobnou analýzu hlavních síťových QoS statistik. Výsledky analýzy uveďte formou grafů a tabulek. Závěrem zhodnoťte význam QoS mechanismů v bezdrátových sítích.

## DOPORUČENÁ LITERATURA:

[1] DOOLEY, K., BROWN, I.: Cisco IOS Cookbook. Sebastopol: O'Reilly Media, 2006, ISBN: 978-0596527228.

[2] GAST, M.: 802.11 Wireless Networks: The Definitive Guide, Second Edition. Sebastopol: O'Reilly Media, 2005, ISBN: 978-0596100520.

[3] PRASAD, N., PRASAD, A.: 802.11 WLANs and IP Networking: Security, QoS, and Mobility. London: Artech House Publishers, 2005, ISBN: 1580537898.

**Termín zadání:** 9.2.2009

**Termín odevzdání:** 2.6.2009

**Vedoucí práce:** Ing. Jiří Hošek

**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.

## **Anotace**

Tato bakalářská práce podává kompletní přehled o bezdrátových sítích 802.11. Popisuje základní standardy a jejich doplňky. Práce je rozdělena na čtyři kapitoly. Dvě teoretické a dvě praktické. Teoretická část obsahuje ucelený přehled o všech standardech, historii bezdrátových sítí a technologii. Dále je zde rozebrána podpora kvality služeb v bezdrátových sítích a podrobněji standard 802.11e. V praktické části je popsána konfigurace sítě, na které probíhalo měření. Poslední částí je již implementace podpory pro kvalitu služeb, měření programem IxChariot, vyhodnocování výsledků a rozdílů v provozu při zapnuté a vypnuté podpoře pro kvalitu služeb.

## **The Abstract**

This bachelor's thesis gives a complete overview of wireless networks 802.11. It describes the basic standards and their drafts. This thesis is divided into four chapters (sections), from which two are theoretical and two practical. The theoretical part contains a comprehensive overview of all standards, the history of wireless networks and technology. Further the support of quality of service in wireless networks is here analysed and in more detail standard 802.11e. In the practical part there is the network configuration described, at which the measurement was taken. The last part is already the implementation of support for quality of service, programme IxChariot measurement, evaluation of the results and differences between network traffic with and without support for quality of service.

## **Klíčová slova**

Kvalita služeb, bezdrátové sítě, Wi-fi, 802.11e, WLAN, QoS

## **Keywords**

Quality of Service, wireless networks, Wi-fi, 802.11e, WLAN, QoS

## **Bibliografická citace**

BRANČ, M. *Realizace zajištění kvality služeb v bezdrátové síti*. Brno: Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, 2009. 53s.  
Vedoucí bakalářské práce Ing. Jiří Hošek.



## **Prohlášení**

Prohlašuji, že svou bakalářskou práci na téma "Realizace zajištění kvality služeb v bezdrátové síti" jsem vypracoval samostatně pod vedením vedoucího bakalářské práce s použitím odborné literatury a dalších informačních zdrojů, které jsou všechny citovány v práci a uvedeny v seznamu literatury na konci práce.

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

V Brně dne .....

.....

Podpis

## **Poděkování**

Děkuji Ing. Jiřímu Hoškovi za vedení bakalářské práce. Také bych také rád poděkoval mé rodině, za jejich podporu, kterou mi poskytovali po celou dobu mého studia.

V Brně dne .....

.....

Podpis

## Obsah

1. Úvod.....	10
2. Bezdrátové sítě.....	11
2.1 Historie bezdrátových sítí .....	12
2.2 Standardy 802.11 a jejich doplňky .....	13
2.3 Architektura a konfigurace sítí .....	14
2.4 Technologie přenosu dat.....	17
2.4.1 DSSS .....	17
2.4.2 FHSS .....	18
2.4.3 OFDM.....	18
2.4.4 UWB .....	19
3. Kvalita služeb ve WLAN.....	20
3.1 Parametry kvality služeb.....	20
3.2.1 MOS .....	21
3.3 Doplňěk 802.11e.....	24
3.3.1 Podvrstva MAC .....	24
3.4 Řízení přístupu k médiu.....	25
3.4.1 DCF.....	25
3.4.2 PCF .....	26
3.5 Rozšířené přístupové metody podle 802.11e.....	27
3.5.1 EDCA.....	28
3.5.2 HCCA .....	30
4. Návrh bezdrátové sítě .....	31
5. Implementace QoS a diagnostika sítě.....	33
5.1 Wireless Multimedia - WMM.....	33
5.2 Zapnutí podpory QoS.....	35
5.3 IxChariot .....	39
5.3.1 Definování služeb .....	40
5.3.2 Nastavení toků .....	41
5.3.3 Vlastní měření.....	43
6. Závěr .....	49
Použitá literatura.....	50
Seznam použitých zkratk .....	52

## Seznam obrázků

Obr.2.1: Základní prvky bezdrátové sítě. ....	14
Obr.2.2: Buňka BSS, režim infrastruktury. ....	15
Obr.2.3: Nezávislá buňka IBSS, režim Ad Hoc. ....	16
Obr.2.4: Bezdrátová síť ESS složená z více BSS buňek. ....	16
Obr.2.5: Seznam dostupných bezdrátových sítí.....	17
Obr.2.7: Přenos pomocí FHSS.....	18
Obr.3.1: Spokojenost uživatelů v závislosti na MOS a R-factor ..... 22	22
Obr.3.2: Závislost MOS na R-factoru a jejich maxima. ....	23
Obr.3.3: Závislost MOS na zpoždění u různých typů kodeků.....	23
Obr.3.5: Metoda DCF včetně RTS/CTS paketů. ....	26
Obr.3.7: Základní sada služeb podporujících QoS. ....	28
Obr.3.8: Superrámec podle 802.11e. ....	30
Obr. 4.1: LAN/WAN/WLAN router Cisco 871W.....	31
Obr. 4.2: Architektura vytvořené bezdrátové sítě.....	32
Obr.5.2: Nastavení WiFi Multimedia s defaultními hodnotami. ....	34
Obr.5.3: Kopírování IOS z paměti flash. ....	35
Obr.5.4: Nastavování class-map. ....	36
Obr.5.5: Přiřazení class-map do policy-mapy. ....	37
Obr.5.6: Zobrazení nastavené policy-mapy. ....	38
Obr.5.7: Nastavení policy-mapy na bezdrátové rozhraní. ....	38
Obr.5.8: Nastavení policy-mapy pro WAN rozhraní.....	39
Obr.5.9: Přiřazení policy-mapy na výstup WAN rozhraní. ....	39
Obr.5.10: Nastavení služby VoIP v programu IxChariot. ....	40
Obr.5.11: Nastavení služeb v programu IxChariot. ....	41
Obr.5.13: Nastavení kritických dat. ....	42
Obr.5.16: Jitter u komunikace bez QoS.....	44
Obr.5.17: MOS bez QoS.....	44
Obr.5.18: Propustnost sítě u toku videa bez QoS. ....	45
Obr.5.19: Propustnost sítě u oboustranné hlas.komunikace bez QoS. ....	45
Obr.5.20: Zpoždění hlasu a videa s QoS. ....	46
Obr.5.21: Jitter u komunikace s QoS.....	46
Obr.5.22: MOS při komunikaci s QoS od 1. stanice ke 2.....	47
Obr.5.23: Propustnost sítě u toku videa s QoS. ....	47
Obr.5.24: Propustnost sítě u toku hlasu oběma směry s QoS.....	48

## Seznam tabulek

Tab.3.1: Velikost mezirámcových mezer .....	27
Tab.3.2: Spojitost prioritních úrovní s kategoriemi přístupu.....	28
Tab.3.3: Parametry kategorií přístupu. ....	29
Tab.5.1: Pole Diffserv.....	36
Tab.5.2: Služby, prioritní úrovně a jejich rozdělení. ....	37
Tab.5.3: Shrnutí změřených parametrů.....	48

## 1. Úvod

Lokální bezdrátové sítě (*WLAN - Wireless Local Area Network*) jsou rozšířením lokálních sítí LAN (*Local Area Network*) nikoli však jejich náhradou. Výhodou je snadná instalace na hůře dostupných místech, ve starých budovách, kde je problém s pokládáním kabeláže atd. V poslední době jsou stále více využívány, ať již v podnicích, domácnostech nebo na veřejně dostupných místech. Toto rozšíření a masové používání bezdrátových sítí souvisí především s jejich neustále se snižující pořizovací cenou a také s tím, že jsou velmi efektivním technickým řešením. Dále je tomu díky stále se zvyšující kvalitě bezdrátových technologií, které umožňují podporu řady multimediálních služeb. Mezi nejatraktivnější patří tzv. IP telefonie (*VoIP – Voice over IP, resp. VoWLAN, někdy označováno i jako VoWiFi*) a přenos videa (videokonference, streamované vysílání atd.).

Výše uvedené je důvodem pro zpracování bakalářské práce právě na toto téma. Jedná se o velmi zajímavé odvětví komunikačních technologií, nabízející širokou škálu uplatnění i různých druhů řešení. Seznámení s problematikou bezdrátových sítí bylo zajímavé již v rámci výuky, kde byla vysvětlena podstata a základy, společně s praktickými laboratorními cvičeními. Ta byla inspirací pro stavbu domácí bezdrátové sítě a využití nabytých dovedností, které jsou uplatňovány i při tvorbě laboratorní bezdrátové sítě pro tuto bakalářskou práci. Ta se podrobněji zabývá historickým vývojem bezdrátových sítí a velmi podstatnou problematikou, kterou je zajištění kvality služeb v bezdrátových sítích. Dané téma nabývá v dnešní době na významu, jelikož využitelnost bezdrátových sítí a jejich množství se za poslední dobu velmi rozrostla. Tato bakalářská práce podrobněji rozebírá mechanismy pro zajištění kvality služeb a doplněk IEEE 802.11e. V rámci praktické části této práce je sestavena laboratorní síť, kde je dle možností použitých směrovačů implementována podpora pro zajištění kvality služeb. Na této síti je mezi dvěma koncovými stanicemi programem IxChariot generován provoz videa v reálném čase, obousměrná hlasová komunikace a FTP. Měření je prováděno s vypnutou a následně zapnutou podporou pro kvalitu služeb. Výsledné grafy jsou porovnány a je zhodnocena funkčnost podpory kvality služeb.

## 2. Bezdrátové sítě

Pojem bezdrátové sítě zahrnuje veškeré sítě, které nejsou propojeny kabely. Hlavní rozdíl oproti lokálním sítím je zde ovšem v mobilitě. Ve WiFi sítích je koncovému zařízení umožněna určitá mobilita, avšak pouze v okruhu signálu přístupového bodu (*AP – Access Point*), kdy samozřejmě úměrně vzdálenosti od AP klesá i přenosová rychlost. Naproti tomu např. v mobilních sítích je možný volný pohyb po signálem pokryté oblasti a nehraje roli počet vysílačů, přes které „procházíme“. S používáním bezdrátových sítí je ale spojeno i pár problémů. Bezdrátové sítě jsou citlivé na rušení. K němu může dojít všemi zařízeními, které pracují na daném kmitočtu (mikrovlnné trouby, bezdrátové myši aj.). Značnou pozornost je třeba věnovat také zabezpečení a zajištění kvality služeb (*QoS – Quality of Service*). [17]

Bezdrátové sítě lze rozdělit podle různých druhů pohledu:

- a) Dle šířky pásma na:**
  - úzkopásmové** - s teoretickou propustností sítě do 2Mb/s
  - širokopásmové** - s teoretickou propustností sítě nad 2Mb/s
- b) Dle mobility na:**
  - mobilní** - umožňují pohyb uživatele jak v rámci jedné bezdrátové sítě, tak i v dalších sítích
  - fixní** - pohyb je umožněn pouze v rámci jedné sítě, tzv. pevné bezdrátové připojení
- c) Dle typu signálu:**
  - rádiové sítě** - mají dosah řádově stovek metrů, jsou nejběžnější, používají se pro domácí a podnikové sítě
  - infračervené sítě** - mají malý dosah, signál neprochází překážkami
  - optické bezdrátové sítě** – s dosahem až stovek metrů, vysokou kapacitou přenosu, vhodné využití mezi budovami s přímou viditelností. [17]

## 2.1 Historie bezdrátových sítí

Roku 1990 zahájil výbor standardizační komise IEEE (*Institute of Electrical and Electronics Engineers*) vývoj standardů bezdrátových sítí. Celkem se dělí na tři podvýbory, který má každý na starosti různé druhy sítí.

- **IEEE 802.11** - Bezdrátové lokální síť (*WLAN - Wireless Local Area Network*)
- **IEEE 802.15** - Bezdrátové osobní síť (*WPAN - Wireless Personal Area Network*)
- **IEEE 802.16** - Bezdrátové metropolitní síť (*WMAN - Wireless Metropolitan Area Network*)

O sedm let později, tedy roku 1997 byla v červnu schválena norma IEEE 802.11, vyvinutá podskupinou 11. Základním nedostatkem standardu 802.11 byla nízká přenosová rychlost (1 - 2 Mbit/s). Proto byl zahájen vývoj nového standardu 802.11a, který byl nakonec schválen roku 1999. Nicméně jeho vývoj byl časově náročnější než standardu 802.11b, který začal být sice vyvíjen o něco později, ale byl schválen dříve téhož roku. Standard 802.11a totiž pracuje v licenčním pásmu 5 GHz, s teoretickou rychlostí až 54 Mbit/s. Standard 802.11b (označován jako Wi-Fi – *Wireless Fidelity*), který v kmitočtovém pásmu 2,4 GHz dosahuje rychlosti až 11 Mbit/s. Bohužel rozdílné kmitočty obou standardů znemožňují vzájemnou komunikaci. Roku 2003 byl proto zaveden standard 802.11g, který je rozšířením 802.11b. Pracuje ve stejném bezlicenčním pásmu 2,4 GHz s maximální rychlostí totožnou se standardem 802.11a, tedy 54 Mbit/s. a je zpětně slučitelný s Wi-Fi (802.11b). [16]

**Organizace IEEE** - „IEEE (*Institute of Electrical and Electronics Engineers*) je mezinárodně uznaná organizace sdružující elektroinženýry (v současnosti je jich kolem čtvrt milionu ze 150 zemí světa). Členství v IEEE je individuální, otevřené všem dobrovolníkům. Kromě vzdělávací a publikační činnosti vytváří IEEE důležité technické normy (*IEEE Standards Association, IEEE-SA*). Ve svém portfoliu má přes 870 schválených norem a přes 400 ve vývoji. Asi nejznámější normy IEEE se týkají oblasti komunikačních sítí: výbor IEEE 802 normalizoval prakticky všechny lokální a metropolitní sítě (*LAN a MAN*), jako 802.3 (normalizovaný Ethernet), 802.5



(normalizovaný Token Ring). Výjimkou je pouze FDDI (*Fiber Distributed Data Interface*) a Fibre Channel, které spadají do působnosti ANSI (*American National Standards Institute*).“[16]

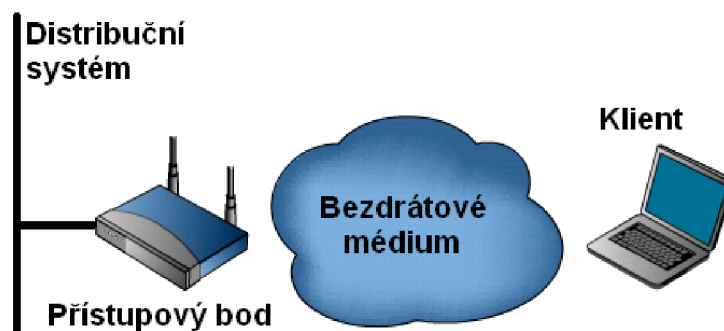
## 2.2 Standardy 802.11 a jejich doplňky

- IEEE 802.11 (1997) - zahrnuje přenosové technologie DSSS (*Direct Sequence Spread Spectrum*), FHSS (*Frequency Hopping Spread Spectrum*) a infračervený přenos. Obě technologie pracují s přenosovou rychlostí 1 - 2 Mbit/s v kmitočtovém pásmu 2,4 - 2,4835 GHz. [11]
- IEEE 802.11a (1999) - oproti původnímu standardu pracuje v licenčním pásmu 5 GHz, které není tolik využíváno a umožňuje využití až 8 nezávislých kanálů bez vzájemné interference. 802.11a pracuje také s mnohonásobně vyšší přenosovou rychlostí (až 54 Mbit/s). Pro dosažení této rychlosti používá OFDM (*Orthogonal Frequency Division Multiplex*). [11]
- IEEE 802.11b (1999) - standard označován také jako Wi-Fi (*Wireless Fidelity*) vznikl o chvíli dříve než 802.11a. Nabízí celkem 4 podporované rychlosti 1 Mbit/s, 2 Mbit/s, 5,5 Mbit/s a 11 Mbit/s. Pro dosažení této rychlosti používá na fyzické vrstvě metodu DSSS (*Direct Sequence Spread Spectrum*) s tzv. doplňkovým klíčováním CCK (*Complementary Code Keying*). Aktuální přenosová rychlost se specifikuje v závislosti na chybovosti a rušení v daném prostředí. Reálná rychlost je ovšem nižší, protože 30 - 40% kapacity je potřebné pro řízení protokolu MAC. Dosah sítě je okolo 100m v závislosti na prostředí. Důležité je také zachování bezlicenčního pásma 2,4 - 2,4835 GHz, díky kterému je zajištěna kompatibilita mezi systémy 802.11. [17]
- IEEE 802.11e (2005) doplněk standardů 802.11a/b/g pro zajištění kvality služeb (QoS - Quality of Service) v bezdrátových sítích WLAN. Rozšiřuje DCF (*Distributed Coordination Function*) a PCF (*Point Coordination Function*) novými přístupovými metodami EDCF (*Enhanced DCF*) a HCF (*Hybrid Coordination Function*). A je také zpětně kompatibilní i se zařízeními, která QoS nepodporovala. [15]

- IEEE 802.11g (2003) - „Higher Speed Physical Layer Extension to IEEE 802.11b“ využívá bezlicenčního kmitočtu 2,4GHz stejně jako Wi-Fi, ale dosahuje maximální rychlosti až 54Mbit/s. Je zpětně slučitelná s 802.11b, což umožňuje vzájemnou spolupráci klientů využívajících oba standardy. Oproti 802.11b využívá pro docílení vyšší rychlosti (stejně jako 802.11a) ortogonálního multiplexu s kmitočtovým dělením (*OFDM - Orthogonal Frequency Division Multiplex*). Výkonnost sítě s 802.11g závisí na tom, jací klienti se nacházejí v síti. Pokud síť obsahuje i klienty využívající standard 802.11b může dojít k problému s komunikací, protože nerozumí komunikaci s OFDM. Pak je tedy pro komunikaci v síti využívána metoda DSSS, která má ovšem menší přenosovou rychlost. Z toho tedy vyplývá, že vyšší propustnost bude mít síť složená čistě z klientů využívajících standard 802.11g (reálně okolo 25 Mbit/s) oproti kombinované síti, kdy propustnost klesá až o dvě třetiny (reálně okolo 8 Mbit/s). [16]

### 2.3 Architektura a konfigurace sítí

Mezi hlavní prvky sítě patří klient, médium, přístupový bod a distribuční systém jak zobrazuje obrázek 2.1.

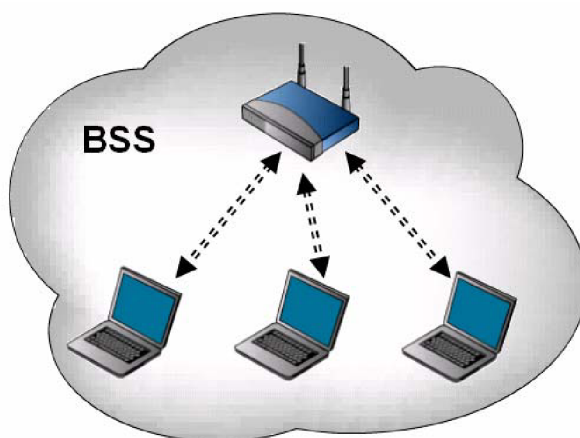


Obr.2.1: Základní prvky bezdrátové sítě. [12]

- **Klient** je jakékoli koncové zařízení, ať už fixní nebo mobilní - PC, notebook, PDA, bezdrátová tiskárna aj.

- **Bezdrátové médium** jsou v sítích 802.11 rádiové vlny o frekvenci 2,4 GHz, 3,7GHz (viz 802.11y) a 5GHz.
- **Přístupový bod (Access Point - AP)** je zařízení umožňující přístup bezdrátovým klientům do sítě. Přístupový bod má vždy nejméně dvě rozhraní. Jedním se připojuje do distribučního systému a druhým zprostředkovává spojení s danými bezdrátovými klienty. Moderní přístupové body v sobě sdružují i funkce bezdrátových směrovačů usnadňujících správu např. domácí bezdrátové sítě.
- **Distribuční systém (Distribution system - DS)** si lze představit jako páteřní síť realizovanou např. metalickou lokální sítí. Zajišťuje přenos dat s dalšími sítěmi.

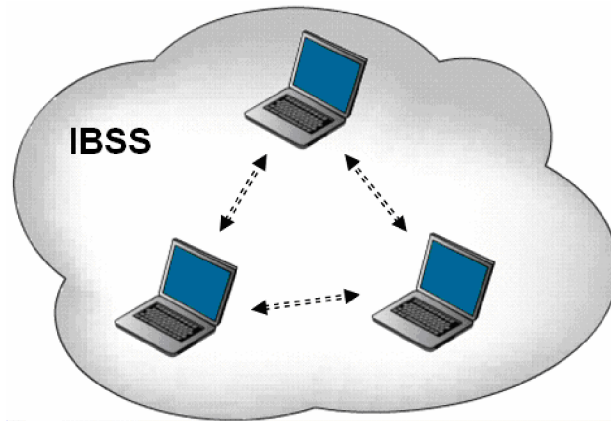
Základní jednotkou v bezdrátových sítích 802.11 je buňka. Ta zahrnuje jeden přístupový bod a množinu stanic s ním spojených v režimu infrastruktury. Buňka se také označuje jako „základní sada služeb“ (*Basic Service Set - BSS*) viz obr.2.2. Identifikátorem buňky BSS je **BSSID (BSS Identifier)**. Ten nabývá hodnotu MAC adresy daného přístupového bodu. [13]



Obr.2.2: Buňka BSS, režim infrastruktury. [13]

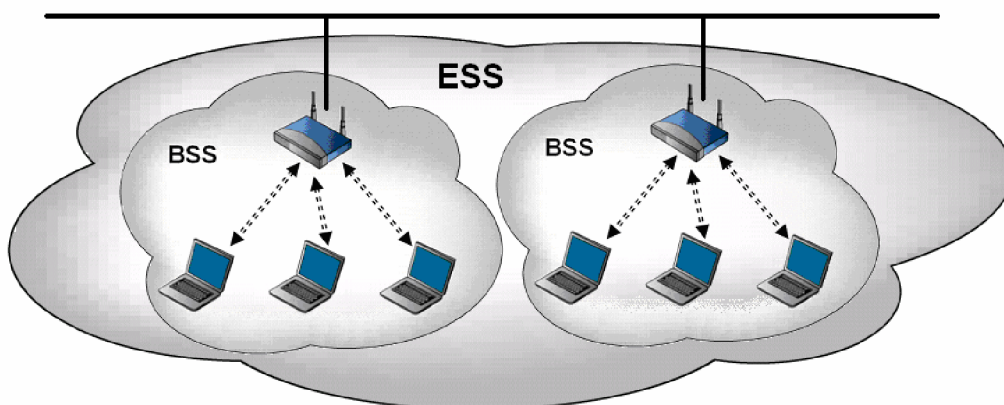
Existuje také spojení klientů mezi sebou, které ke komunikaci nepotřebuje přístupový bod. Takzvaná nezávislá buňka (*Independent Basic Service Set - IBSS*), kdy spolu dané stanice komunikují v režimu Ad Hoc. Tato buňka nemá spojení s vnějším světem a

slouží čistě jen k výměně informací mezi klienty (viz obr.2.3). Toto spojení je vhodné pouze pro krátkodobé výměny informací. Tuto konfiguraci lze využít např. při komunikaci notebooku s PDA. [17]

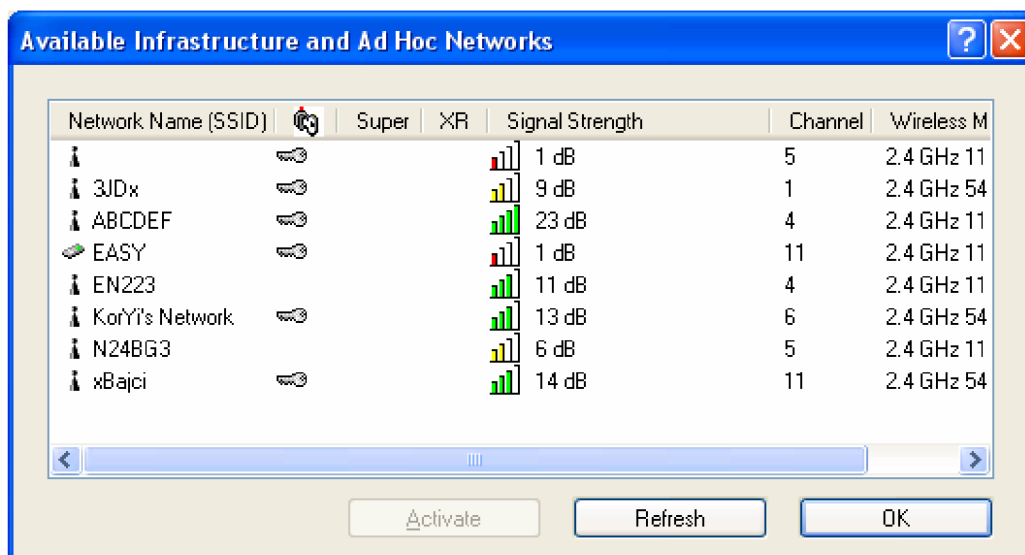


Obr.2.3: Nezávislá buňka IBSS, režim Ad Hoc. [13]

Vlastní bezdrátová síť vzniká spojením přístupových bodů buněk BSS v pracovním režimu infrastruktury. Takovému celku se říká soubor rozšířených služeb (*Extended Service Set - ESS*) viz obr.2.4. Identifikátor této sítě je SSID (ESS Identifier). Pod tímto označením lze pak danou bezdrátovou síť najít v seznamu dostupných připojení. Viz obrázek 2.5., kde je patrné, že první nalezená síť má skryté SSID, dále je vidět, který kanál daná síť využívá, jaká je síla signálu, použité frekvenční pásmo (ze kterého lze odvodit i využívaný standard) a také, zda je síť chráněna nějakým klíčem či nikoli. [13]



Obr.2.4: Bezdrátová síť ESS složená z více BSS buňek. [12]



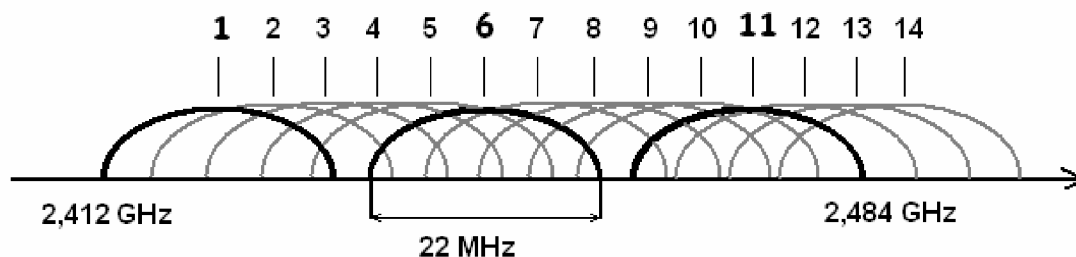
Obr.2.5: Seznam dostupných bezdrátových sítí.

## 2.4 Technologie přenosu dat

V současných bezdrátových sítích jsou využívány různé režimy pro přenos dat v rozprostřeném spektru na fyzické vrstvě.

### 2.4.1 DSSS

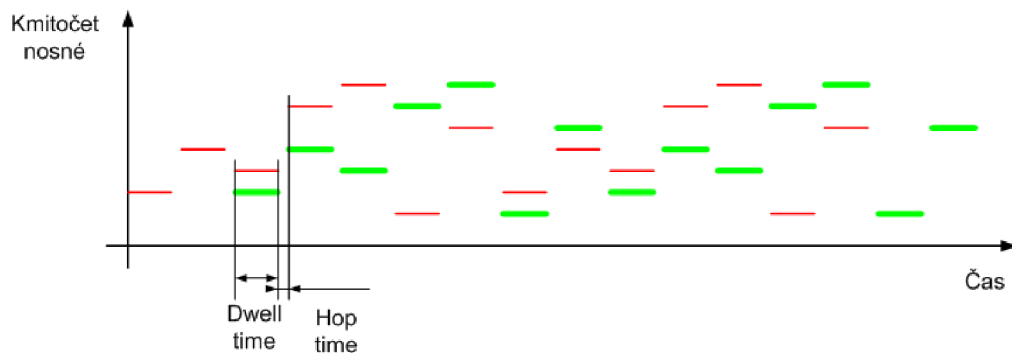
Neboli rádiový přenos v přímo rozprostřeném spektru (*Direct Sequence Spread Spectrum Radio - DSSS*). Vysílač přeměňuje tok dat na symboly, kdy každý ze symbolů zastupuje jeden nebo více bitů. Tento tok symbolů se jednotlivě moduluje pseudonáhodnou sekvencí a až potom se přenáší. DSSS dělí pásmo své působnosti 2,412GHz - 2,484GHz na 14 kanálů, vzdálených od sebe 5MHz. Pro každý kanál je potřeba 22MHz, což vede k částečnému překrývání kanálů. Pouze tři z nich se nepřekrývají (a to první, šestý a jedenáctý, viz obrázek 2.6). V každé zemi je povoleno používat jen určité kanály. U nás například smíme používat kanály 1-13. Tuto technologii využívá standard 802.11b. [7]



Obr.2.6: Rozdělení kmitočtového pásma u DSSS. [7]

### 2.4.2 FHSS

Jedná se o rádiový přenos v rozprostřeném spektru s přeskokováním mezi kmitočty (*Frequency Hopping Spread Spectrum - FHSS*). Vysílá se jeden nebo více datových paketů po určitém kmitočtu (pásma se dělí na 79 podkanálů každý po 1MHz) a pak komunikace pokračuje na dalším kmitočtu a vysílá dál. Systém přeskokování frekvencí ovšem není náhodný, jde o pseudonáhodné pořadí které předem zná pouze vysílač a přijímač. Rušení se minimalizuje krátkou vysílací dobou na daném kmitočtu (*dwell time*). Vysílá se po dobu 100-200ms, což snižuje pravděpodobnost kolize. Doba potřebná k přeladění na další kmitočet je 200-300 $\mu$ s (*hop time*). Výhodou je možnost existence množství sítí bez vzájemného rušení, ovšem kvůli nízkým přenosovým rychlostem se dnes již téměř nepoužívá. Na obr.2.7 je zobrazen přenos dat současně dvěma různými zařízeními. [11]



Obr.2.7: Přenos pomocí FHSS. [11]

### 2.4.3 OFDM

V moderních verzích bezdrátových sítí se pro dosažení vyšší rychlosti používá ortogonální multiplex s kmitočtovým dělením (*Orthogonal Frequency Division Multiplex*), jedna z přenosových metod MCM (*MultiCarrier Modulation*), kdy se data k vysílání nejprve rozdělí do několika paralelních toků bitů o mnohem nižší bitové rychlosti. Každý z toků se používá pro modulaci jiné nosné. Kanály jsou velmi blízko u sebe, ale nepřekrývají se, díky čemuž nehrozí vzájemné rušení. Zatímco tradiční kmitočtový multiplex dělí kmitočtové pásmo do N nepřekrývajících se subkanálů vzájemně oddělených ochranným kmitočtovým pásmem (guard), OFDM používá překrývající se subkanály, takže kmitočtové pásmo se využívá účinněji. Přísně vzato není OFDM modulační metoda, ale metoda pro generování a modulaci více nosných

současně, každé s malou částí datového toku. Jako konkrétní modulaci lze pak použít jakýkoli typ digitální modulace včetně QPSK, 16-QAM či 64-QAM. Způsobem paralelního vysílání se OFDM účinně brání zkreslení při přenosu signálu různými cestami, protože každý přenášený symbol trvá na dílčí nosné délce, takže se prakticky vyloučí nepříznivý dopad zpoždění signálu delší cestou. Navíc se používá více úzkopásmových nosných a jejich vzájemné rušení ovlivní jen velmi malou část signálu. OFDM se používá v bezdrátových systémech všude, kde je potřeba docílit vysoké propustnosti a přitom podmínky na kanálu mohou být ztíženy. OFDM se uplatňuje například ve WLAN typu 802.11a/g nebo WiMAX podle 802.16, protože nepodléhá útlumu signálu právě ve venkovním prostředí.[16]

#### **2.4.4 UWB**

Širokopásmové komunikační sítě (Ultra WideBand - UWB) jsou zatím málo známou bezdrátovou technologií, ovšem s velkým potenciálem. Lze ji použít pro přenosy velkých objemů dat po širokém spektru kmitočtů s nízkým výkonem na krátkou vzdálenost. UWB se už dlouho využívá pro vojenské účely, především jako radarová technologie. UWB se posazením ve spektru odlišuje od úzkopásmových komunikací, které jsou dnes běžné, ale také od širokopásmových. Rozdíl je v přenosové rychlosti, kde UWB dosahuje až stovek Mb/s a také z mnohořádkově nižší energetické spotřeby, než je tomu u sítí 802.11b. Vysoká propustnost je vhodná pro aplikace s velkými požadavky na šířku pásma i podporu kvality služeb (videokonference aj.) Dalším kladem sítí s technologií UWB je fakt, že je prakticky nemožné je odposlouchávat (signály vypadají jako slabý šum). Díky tomu se ani přístroje v UWB sítích neruší s dalšími zařízeními elektromagnetického spektra. Historie UWB začala ve čtyřicátých letech dvacátého století v souvislosti s radary. V sedmdesátých letech se armáda zaměřila i na využití pro komunikační účely. Na rozdíl od většiny moderních rádiových technologií pulsní signály nemodulují nosnou o pevném kmitočtu. Rozprostřené spektrum u IEEE 802.11 vlastně dociluje uměle toho, co UWB provádí ze své podstaty. Rozkládá signál v rámci velmi širokého spektra tak, aby výkon v každém pásmu byl pod hranicí možného vzájemného rušení. [16]

### 3. Kvalita služeb ve WLAN

Velikou nevýhodou bezdrátových sítí podle 802.11 je fakt, že v základních standardech není zahrnuta podpora kvality služeb. Dříve se to nezdálo být velkým problémem, nicméně s masovým používáním Wi-Fi sítí a se zkvalitňující se škálou služeb a programů využívajících těchto sítí začala citelně chybět nějaká podpora pro zajištění kvality služeb, jaká je již běžně implementována v lokálních sítích. Dalo by se tedy říci nějakého upřednostnění přístupu k médiu multimediálním aplikacím.

Přístupové body se snaží zacházet se všemi svými klienty stejně a rovnoměrně jim rozdělovat přenosové pásmo, které mají k dispozici. U bezdrátových sítí hraje velkou roli na kapacitě signálu útlum, šum i rušení, což pro většinu aplikací nenáročných na stabilitu není tolik podstatné. Problém vyvstává, pokud v nerovnoměrně zatížené síti chce některý klient využívat aplikace, které potřebují stabilní tok dat s minimálním zpožděním (jako je třeba přehrávání videa a hudby v reálném čase, nebo internetová telefonie). Bude totiž docházet k výpadkům spojení, video či hudba se nebude přehrávat spojitě a klient bude nespokojen se službou.

#### 3.1 Parametry kvality služeb

Kvalitu služeb ovlivňuje několik parametrů, přičemž každá ze služeb je citlivá na jiný z nich. Například na populární službu VoIP má negativní vliv zpoždění paketů, na přehrávání videa zase ztráta paketů. Mezi parametry nejvíce ovlivňující komunikaci patří:

- **Ztráta paketů** - může mít různé příčiny, většinou je na vině zahlcená, nebo přetížená síť, kdy některé routery nestíhají preposílat přicházející pakety a jejich vyrovnávací paměti přetečou. Pak další příchozí pakety musí být zahozeny. V případě aplikací, které neprobíhají v reálném čase to není až tak citelné, ovšem u aplikací, které probíhají v reálném čase to je problém, jelikož pozdější doručení paketů už narušuje komunikaci. Například u přenosu hlasu při „telefonování“ přes internet, může být komunikace nestabilní. Dokonce může docházet ke krátkým výpadkům, případně může



být komunikace nepříjemně rušena. Celkový počet ztracených paketů by neměl přesáhnout jedno procento. V případě videa (např. videokonference) to může být i o něco vyšší procento, jelikož video je méně citlivé na ztrátu paketů než hlas. Při streamování videa již zpoždění paketů hraje nejmenší roli, protože se data před přehráváním tzv. buffrují, čili ukládají do dočasné paměti. [9]

- **Zpoždění** - je doba od vyslání paketu vysílajícím klientem po přijetí příjemcem. Doba, po kterou putují data z jednoho konce sítě na druhý se nazývá **propagační zpoždění**. Doba spojená digitalizací hlasového signálu a jeho kódováním hlasovými kodeky se nazývá **paketizační zpoždění** (čím větší má použitý kodek kompresi, tím větší je i doba paketizačního zpoždění). Zpoždění má největší dopad na hlasové služby. Ovšem neovlivňuje kvalitu přenášeného hlasu. Při vyšších hodnotách zpoždění by se mohli oba uživatelé navzájem přerušovat těmito zpožděnými pakety. Při streamování videa zpoždění paketů hraje menší roli, protože se data před přehráváním tzv. buffrují, čili ukládají do dočasné paměti a až následně přehrávají. [9]
- **Jitter** (proměnlivost zpoždění) - protože pakety nemusí vždy přicházet se stejným zpožděním. To může být způsobeno proměnlivou čekací dobou v uzlech, případně zahlcením sítě. Pro odstranění těchto vlivů je třeba nějaká dočasná paměť (jitter buffer), pro uložení paketů na tak dlouhou dobu, než jsou přeneseny pomalejší pakety, mnohdy mimo pořadí, aby pak mohly být předány ve správném pořadí. Zdržení paketu ve vyrovnávací paměti samozřejmě přidává tzv. **jitter zpoždění**, které se používá pro odstranění kolísání zpoždění každého paketu procházejícího sítí. [9]

### 3.2.1 MOS

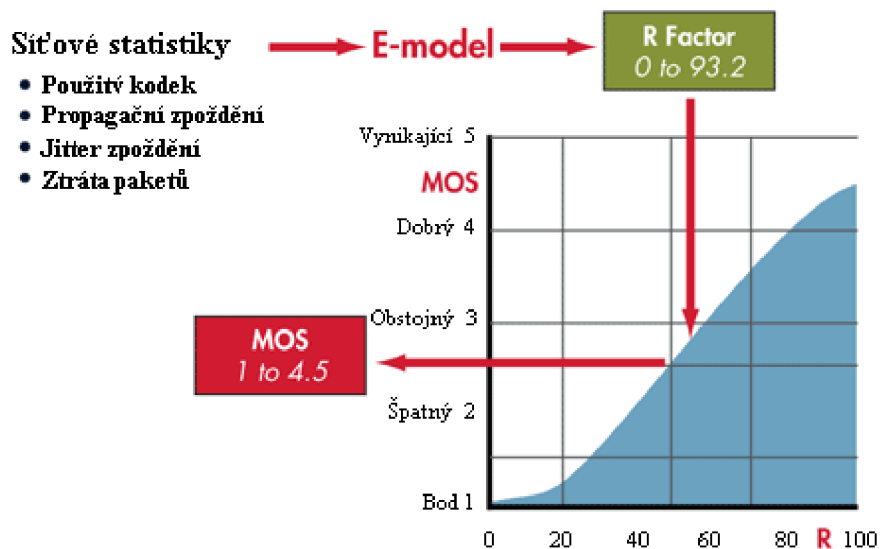
Vnímání kvality telefonního hovoru je vždy subjektivní. Hlavním měřítkem pro objektivní hodnocení kvality hlasu je MOS (Mean Opinion Score), který je popsán

standardem ITU P.800. Ten mimo jiné také popisuje, jak lidé reagují na telefonní hovory s různým zpožděním a různou ztrátovostí paketů, jak hodnotí daný telefonní hovor a jak moc jsou se službou spokojeni. Z obrázku 3.1 vyplývá, že při hodnotách MOS pod 4.0 jsou již někteří uživatelé nespokojeni, a proto by ve správně nastavené síti hodnota MOS neměla klesnout pod tuto úroveň, aby byla zajištěna maximální spokojenost uživatelů. [9]



Obr.3.1: Spokojenost uživatelů v závislosti na MOS a R-factoru. [9]

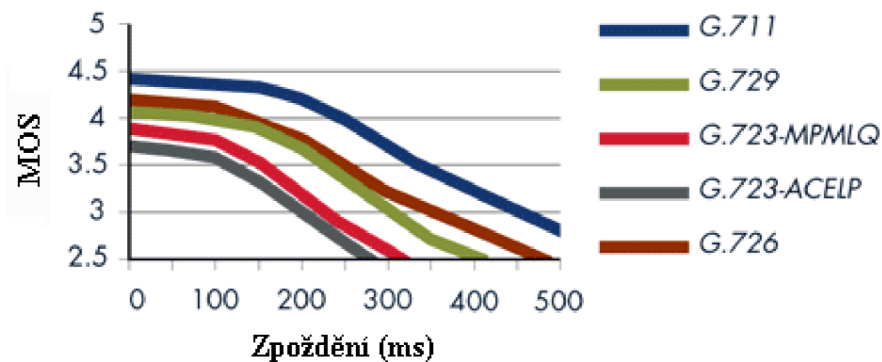
Byly vypracovány různé standardy pro výpočet MOSu. Mezi nimi i dnes nejvíce používaný The E-model (ITU G.107). Výstupem tohoto standardu je číslo nazývané R-factor. Při výpočtu R-factoru se bere ohled na použitý kodek a s ním spojené paketizační zpoždění, na propagační zpoždění, na jitter zpoždění a na ztrátovost paketů. Teoretický rozsah MOS je od 5 do 1. Hodnotu MOS lze přímo vypočítat z hodnoty R-factoru. Praktická maximální hodnota R-factoru je 93,2 a tedy odpovídající maximální hodnota MOS je asi 4,5. Na obrázku 3.2 je zachycena jejich vzájemná závislost. [9]



Obr.3.2: Závislost MOS na R-factoru a jejich maxima. [9]

Celkové zpoždění přenosu hlasových paketů, stejně jako hodnota MOS je ovlivněno výběrem kodeku. Obrázek 3.3 níže znázorňuje závislost MOS na zpoždění, při provozu bez ztráty paketů.

#### Teoretické hodnoty MOS různých kodeků



Obr.3.3: Závislost MOS na zpoždění u různých typů kodeků. [9]

Kodek G.711 má při přenosu nejlepší kvalitu hlasu, protože je bez komprese. Proto představuje i nejmenší paketizační poždění. Je ze všech kodeků nejméně citlivý na ztrátu paketů. Další kodeky již využívají kompresi. Ta snižuje kvalitu hlasu, srozumitelnost a činí hovor velmi citlivý na ztrátovost paketů.

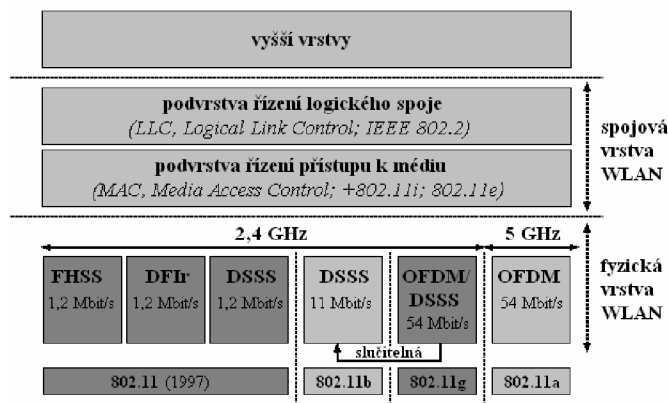
### 3.3 Doplněk 802.11e

Slouží pro zajištění podpory pro kvalitu služeb (Quality of Service - QoS), které by zohledňovalo potřebu multimediálních služeb na stabilní spojení s minimálním zpožděním nebo ztrátou dat. Proto byl roku 2005 odsouhlasen doplněk 802.11e který měl do dosavadních sítí 802.11 zavést podporu QoS.

#### 3.3.1 Podvrstva MAC

Sítě WLAN jsou tzv. sdílené sítě, kdy komunikace v obou směrech běží na jednom daném kmitočtu a v určitém čase může probíhat vždy jen jedna relace. Sítě WLAN pracují na principu časového duplexu (*Time Division Duplex - TDD*).

V případě bezdrátových sítí definuje standard IEEE 802 rozdělení spojové vrstvy na dvě podvrstvy (viz obr.3.4). Vyšší z nich se označuje jako podvrstva řízení logického spoje - **LLC** (*Logical Link Control*). Podvrstva LLC vykonává služby nezávisle na dané fyzické implementaci sítě. Je sdílená všemi technologiemi definovanými standardem IEEE 802. Má na starosti vytvořit a rušit spojení, řídit tok dat, kontrolovat případné chyby a hlavně adresovat na úrovni spojové vrstvy. Podvrstva LLC je většinou implementována softwarově. Druhá z nich se označuje jako podvrstva řízení přístupu k médiu - **MAC** (*Media Access Control*). MAC obstarává funkce spojové vrstvy spojené s danou síťovou technologií. Zajišťuje přenos dat fyzické vrstvě, řídí přístup k médiu, asociaci stanice k WLAN, autentizaci, utajení dat a kontroluje správnost přenášených paketů. Podvrstva MAC úzce spolupracuje s fyzickou vrstvou, proto by měla být schopná vykonávat funkce tak rychle, jak se může měnit tok dat na médiu. Bývá realizována hardwarově přímo na síťové kartě. [17]



Obr.3.4: Vrstvová architektura 802.11. [17]

### 3.4 Řízení přístupu k médiu

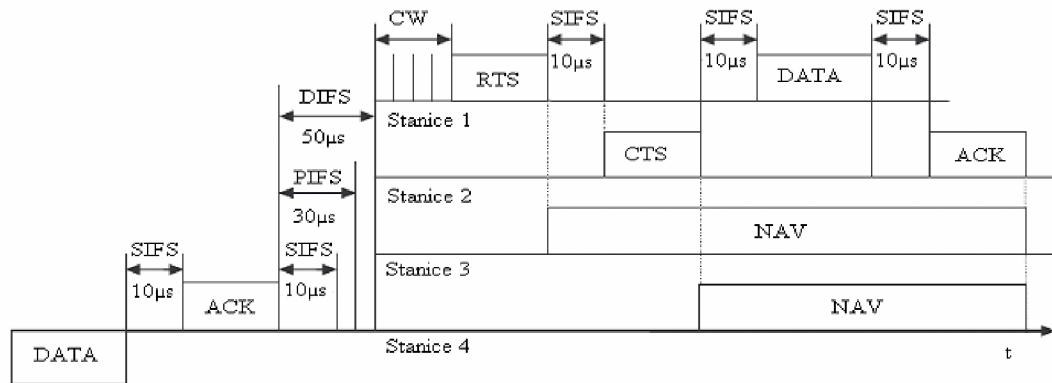
Jako protokol řízení přístupu k médiu využívá mnohonásobného přístupu s detekcí nosné a vyvarováním se kolizí CSMA/CA (*Carrier Sense Multiple Access/Collision Avoidance*). Princip je podobný jako u LAN a jeho přístupu pomocí CSMA/CD (*Collision Detection*). V případě CSMA/CA si stanice volí náhodně dlouhý čekací interval, který je násobkem nastaveného časového úseku a „soutěží“ o médium. V případě že chce stanice vysílat a médium je obsazeno, zachytí rádiový signál vysílající stanice a odloží své vysílání. Výjimkou v pořadí vysílání jsou rámce s nejvyšší prioritou, které jsou odesílány přednostně. V případě bezdrátové sítě nelze detekovat kolizi, proto se používá systém potvrzování. Vždy se potvrdí příjem uživatelských dat zaslanych na určitou MAC adresu. [17]

Základní standard 802.11 používá dvě funkce přístupu k médiu. Ani jedna z nich však není vhodná pro zajištění kvality služeb.

#### 3.4.1 DCF

Distribuovaná koordinační funkce (*Distributed Coordination Function*) zajišťuje koordinaci přístupu k médiu, ovšem nepodporuje žádné úrovně (priority) pro přístup. Jako přístupovou metodu používá CSMA/CA. Pro zabránění kolizím využívá dvě techniky. Vložení mezer mezi vysílací rámce (*IFS - InterFrame Space*) a odložení vysílání (*backoff*). Interval *DIFS (DCF IFS)* je povinná doba, kterou musí stanice počkat ve chvíli, kdy zjistí že je médium volné, než začne vysílat. Pokud by v tomto intervalu začala vysílat jiná stanice, musí své vysílání odložit. Doba, pro odložení vysílání je volena jako časový interval od nuly po tzv. okno sváru (*CW - Contention Window*). Stále by ovšem mohlo dojít ke kolizi, kdyby dvě stanice začaly vysílat ve stejný čas. Z tohoto důvodu je potřeba systém potvrzování. Když vysílač neobdrží po určité definované době (*SIFS - Short InterFrame Space*), která je kratší než *DIFS*, potvrzovací paket *ACK*, předpokládá, že došlo ke kolizi a opakuje vysílání. Pro předejití kolizím je možné zapnout ještě volitelný protokol *RTS/CTS (Request To Send/Clear To Send)*. Stanice začíná komunikaci vysláním rámce *RTS* s žádostí o vysílání. Pokud dostane odpověď v podobě *CTS*, může po určitou dobu vysílat. Ostatní stanice si podle intervalu, po který bude stanice vysílat nastaví svůj alokační vektor

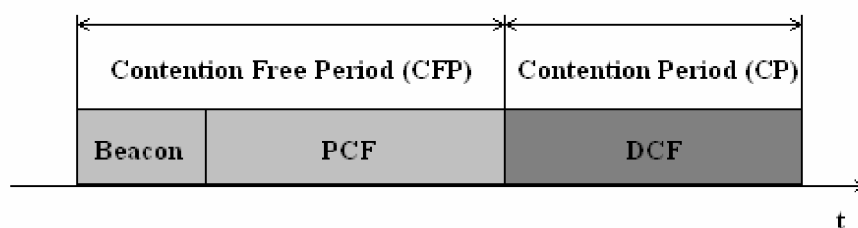
NAV (Network Allocation Vector) a po danou dobu se nesnaží vysílat, protože ví, že médium je již využíváno. Po přijetí dat je odeslán potvrzovací rámeček ACK (Acknowledge). Komunikace pomocí DCF je zobrazena na obrázku 3.5. Zapnutím tohoto protokolu klesá reálná využitelná rychlost bezdrátové sítě až na 20%, vzhledem k velkému množství zasílaných řídicích paketů. [16]



Obr.3.5: Metoda DCF včetně RTS/CTS paketů. [18]

### 3.4.2 PCF

Centralizovaná koordinační funkce (*Point Coordination Function*), není v dnešní době moc využívána, nedá se například použít v Ad Hoc sítích, pouze v sítích v režimu infrastruktury. Zde pak přístupový bod funguje jako centralizovaný koordinátor, který přiděluje médium klientům. Periodicky vysílá rámce *beacon*, obsahující informace pro identifikaci a řízení. Vzniklá časová perioda, včetně beacon rámce se nazývá superrámec (*SuperFrame*) viz obr. 3.6. Ta se dá rozdělit na dvě části. Doba bez soupeření (*CFP - Contention-Free Period*) a doba soupeření o médium (*CP - Contention Period*). V případě doby bez soutěžení se využívá koordinační funkce PCF, při době soutěžení o médium funkce DCF. Během doby bez soupeření se koordinátor ptá klientů, co mají k odeslání. Zde je využita další mezirámcová mezera PIFS (*Point Coordination Function Interframe Space*) viz tab.3.1.



Obr.3.6: Superrámec.[11]

Mechanismus PCF není celkově moc výhodný, nelze totiž nastavit třídy provozu, časovou synchronizaci vzhledem k různé délce přenášených rámců, kdy dlouhý rámec může nepříznivě ovlivnit výkon sítě, případně ji dočasně zablokovat. V závislosti na proměnlivé délce přenášených rámců také není pravidelně vysílán rámec beacon, což samozřejmě ovlivní služby, citlivé na časování. Z toho tedy vyplývá, že se tato přenosová funkce příliš nehodí pro multimediální služby. [17]

Tab.3.1: Velikost mezirámcových mezer. [12]

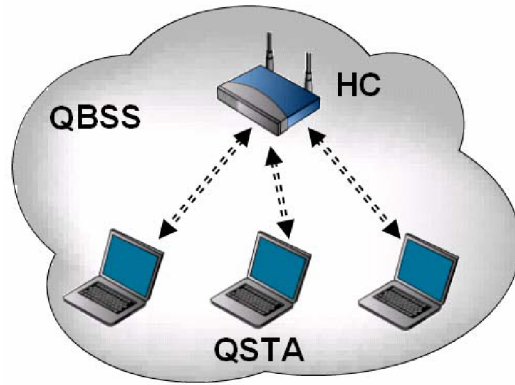
Standard	SIFS	PIFS	DIFS	slot	CW <sub>min</sub>	CW <sub>max</sub>
802.11a	16μs	25μs	34μs	9μs	15	1023
802.11b	10μs	30μs	50μs	20μs	31	1023
802.11g	10μs	30μs	50μs	20μs	15	1023

### 3.5 Rozšířené přístupové metody podle 802.11e

Protože původní přístupové funkce nebyly schopny poskytnout podporu kvality služeb a upřednostňování určitých aplikací, zavedl doplněk 802.11e dvě další koordinační funkce.

- EDCF (*Enhanced Distributed Coordination Function*) na základě které je zaveden nový rozšířený distribuovaný přístup k médiu EDCA (*Enhanced Distributed Channel Access*).
- HCF (*Hybrid Coordination Function*), která řídí přístup ke kanálu HCCA (*HCF Controlled Channel Access*).

U obou z nich jsou definované třídy provozu podle doplňku 802.11e. Díky tomu je možné přidělovat přenosové médium podle typu aplikace. Například hlas bude mít vyšší prioritu, před například nahráváním internetových stránek, ftp a dalšími. Celý systém navíc funguje tak, že při implementaci služeb podle tohoto doplňku je možné komunikovat i se zařízeními, které podporu kvality služeb nemají. Doplněk zavádí i novou sadu služeb, podporující kvalitu služeb QBSS (*QoS supporting Basic Service Set*) viz obr.3.7, s tím rozdílem, že přístupovému bodu se říká HC (*Hybrid Coordinator*) a stanicím QSTA (*QoS supporting Station*) [12]



Obr.3.7: Základní sada služeb podporujících QoS. [13]

### 3.5.1 EDCA

Definuje přístupové kategorie AC (*Access Category*) pro podporu priorit na stanicích. Každá stanice může mít až čtyři kategorie přístupu pro podporu až osmi uživatelských prioritních úrovní UP (*User Priorities*). Jedna nebo více prioritních úrovní je přiděleno k jedné kategorii přístupu. Jejich přehled je zobrazen v tabulce 3.2 níže. Prioritní úrovně a jejich využití je popisováno standardem 802.1D.

Tab.3.2: Spojitost prioritních úrovní s kategoriemi přístupu. [14]

	Prioritní úroveň (UP) (802.1D)	Kategorie přístupu (AC)	Předpokládané využití (802.11e)
Nejnižší	1	AC_BK (0)	přenos na pozadí
	2	AC_BK (0)	přenos na pozadí
	0	AC_BE (0)	best-effort
	3	AC_VI (1)	video probe
	4	AC_VI (2)	video
	5	AC_VI (2)	video
Nejvyšší	6	AC_VO (3)	hlas
	7	AC_VO (3)	hlas

V tabulce jsou vidět čtyři různé kategorie přístupu. AC\_BK pro přenos na pozadí, AC\_BE pro přenos best-effort, AC\_VI pro přenos videa a AC\_VO pro přenos hlasu.



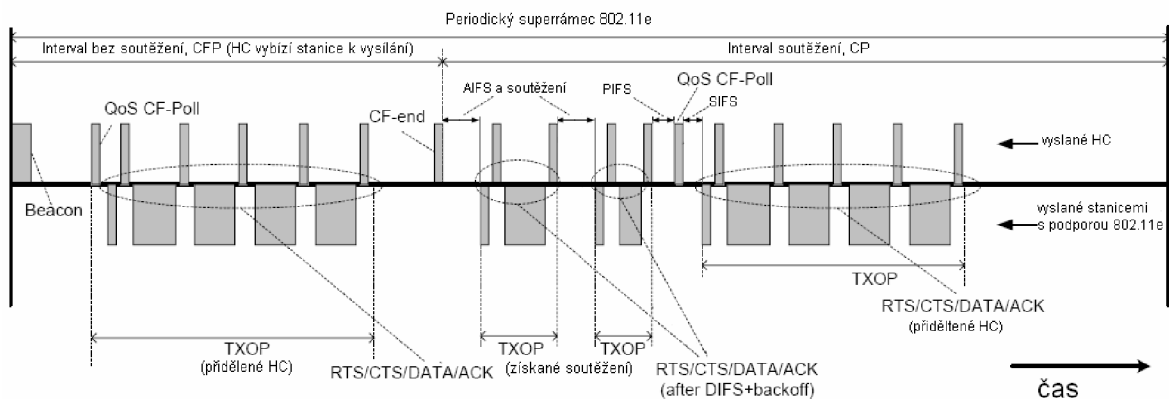
Dále je patrné, že přenos typu best-effort má i s nižší prioritní úrovní (UP\_0) vyšší prioritu přenosu než přenos na pozadí (UP\_1 a UP\_2). U EDCA rámce jednotlivých kategorií soutěží o příležitost k přenosu TXOP (Transmission Opportunity). Jedná se o časový úsek, kdy je možné přenášet. Velikost TXOP je pevně daný interval, aby nedocházelo k problémům se synchronizací. Informace o délce TXOP jsou obsaženy v každém beacon rámci. Pro správnou funkčnost byla zavedena další mezirámcová mezera AIFS (Arbitration Interframe Space). Velikost AIFS mezery je pro každou AC kategorii jiná. Tuto mezeru, stejně jako  $CW_{min}$ ,  $CW_{max}$  a AF lze nastavit podle potřeby. Samozřejmým předpokladem je, že okno sváru se bude zmenšovat úměrně rostoucí prioritě, aby aplikace z dané prioritní úrovně měla větší šanci k získání přístupu. Pokud má aplikace připravena data k odeslání, může je teoreticky ihned odeslat. Musí být ovšem prázdné fronty a volné přenosové médium. Pokud médium není volné, je datový rámec dané aplikace vložen do fronty odpovídající kategorie přístupu. Po uvolnění média se čeká po dobu stanovenou AIFS. Pak dochází k soutěžení o médium. Pokud by získala přístup k mediu více než jedna aplikace z dané přístupové kategorie, je TXOP přidělen kategorii s vyšší prioritou. Ostatní aplikace vyhodnotí situaci jako kolizi a čekají na uvolnění média. Kategorie přístupu AC\_BK a AC\_BE v případě přidělení média mohou přenést pouze jeden rámec. Naproti tomu AC\_VI a AC\_VO mohou přenášet spojitě po celou dobu trvání intervalu TXOP. Viz. tabulka 3.3. [6]

Tab.3.3: Parametry kategorií přístupu. [12]

AC	Předpokládané využití	CW	AIFS	TXOP limit (802.11b)	TXOP limit (802.11a/g)
Pozadí	datové soubory	0-15	7	0	0
Best effort	interaktivní aplikace, necitlivé na zpoždění	0-15	3	0	0
Video	video toky	0-7	2	6,016ms	3,008ms
Hlas	VoIP s nejvyšší kvalitou a minimálním zpožděním	0-3	2	3,264ms	1,504ms

### 3.5.2 HCCA

Přístup k médiu podle HCCA vychází původně z PCF, ale je propracovanější s ohledem na podporu kvality služeb. Centralizovanost opět zajišťuje hybridní koordinátor HC, většinou tedy přístupový bod - QAP (Quality of service supporting Acces Point). Hlavní rozdíl mezi EDCA a HCCA je ten, že HCCA garantuje dobu přenosu nebo zpoždění, zatímco u EDCA jsou priority relativní a ne vždy striktní. HCCA pracuje jak během doby bez soutěžení, tak i soutěžení. Tentokrát už ale nestačí pouhá registrace u koordinátora, stanice musí vždy specifikovat své požadavky na síť, které předloží HC ke schválení, případně odmítnutí, pokud by je nemohl zaručit. HC pak přiděluje TXOP stanicím. Přidělení TXOP se děje zasláním rámce QoS CF POLL. Ten je generován na začátku intervalu bez soutěžení. Ovšem HC jej může generovat prakticky kdykoli. Lze přidělit TXOP jedné kategorii přístupů, nebo i více najednou, kdy musí HC podrobně informovat, kdy může daná kategorie začít vysílat. Ostatní stanice si na tu dobu nastavují svůj NAV vektor, aby věděly, jak dlouho bude ještě médium obsazené. Interval CF POLL se ukončuje rámcem CF-END. Pokud HC potřebuje, může získat přístup k médiu i v intervalu soutěžení. Zasláním rámce QoS CF POLL informuje stanice, kdy mohou odeslat svá data bez soutěžení. Tento interval se nazývá CAP (Controlled Access Phase). Jeho trvání je dáno délkou TXOP uvedenou v zasláném rámcí QoS CF POLL. Příklad komunikace je vidět na obrázku 3.8, kde je zobrazeno, co se děje v jednom superrámci podle doplňku 802.11e. [12]



Obr.3.8: Superrámec podle 802.11e. [10]

#### 4. Návrh bezdrátové sítě

Podle zadání bakalářské práce byla vytvořena v laboratoři PA-249 bezdrátová síť. Na této síti byly v rámci této práce implementovány technologie pro zajištění podpory pro kvalitu služeb a následné simulace. Měření a vyhodnocování bylo prováděno programem IxChariot. Aktuální konfigurace sítě sestává ze dvou routerů Cisco 871W (viz obr.4.1). Obsahují tři rozhraní: čtyři 10/100 Mb/s porty pro Ethernet (LAN), jeden 10/100 Mb/s port pro WAN a bezdrátové rozhraní WLAN, podporující standardy 802.11b/g. Jejich konfigurace je možná buď přes velmi webovou java aplikaci, nebo přímo přes konzoli.

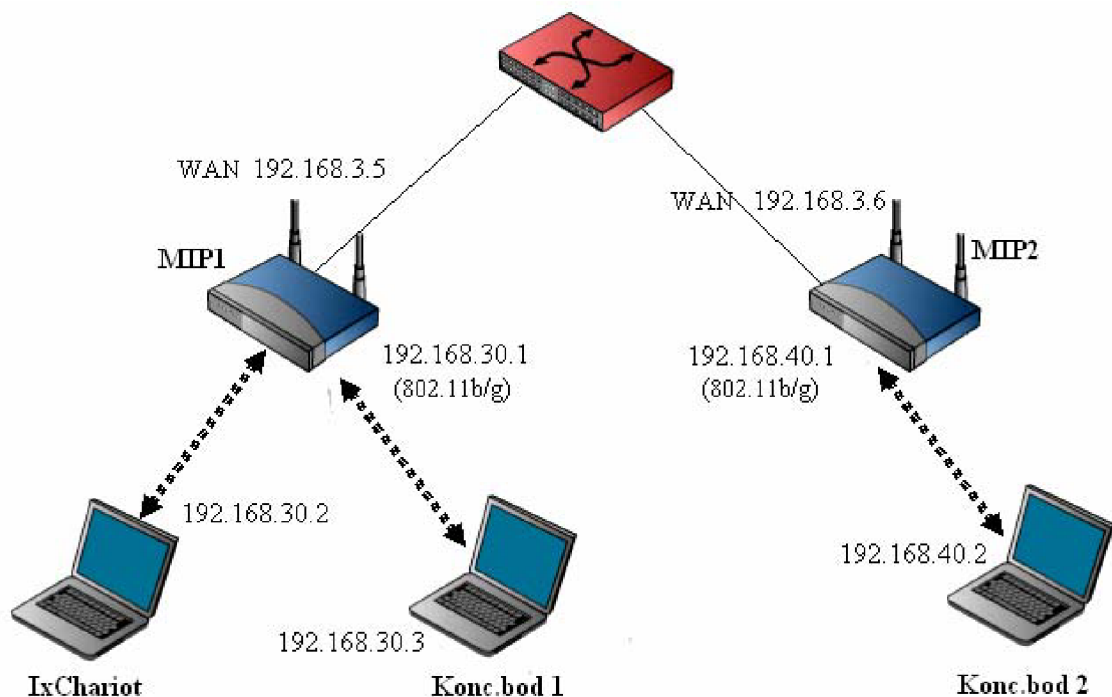


Obr. 4.1: LAN/WAN/WLAN router Cisco 871W.

Tyto routery zde vystupují jako dva přístupové body, které reprezentují každý jednu bezdrátovou síť s vlastním identifikátorem sítě SSID. Názvy sítí byly prozatím ponechány jako původně nastavené MIP1 a MIP2, a to vzhledem k tomu, že jde o pomůcky do výuky. Tyto dva přístupové body jsou spolu propojeny přes přepínač přes WAN rozhraní ethernetovými kabely. Přístupový bod MIP1 má na rozhraní WAN nastavenou IP adresu 192.168.3.5/24, MIP2 má IP adresu rozhraní WAN 192.168.3.6/24. Jak je vidět na obrázku 4.2, přístupový bod MIP1 má pro rádiové rozhraní WLAN nastavenou síť 192.168.30.1/24, přístupový bod MIP2 má pro WLAN nastavenou síť 192.168.40.1/24. Na obou přístupových bodech je zapnut DHCP server a nastaven rozsah přidělovatelných IP adres. Ten je omezen na 4 klienty v každé síti (tedy

v případě MIP1 je rozsah 192.168.30.2 - 192.168.30.5), protože více klientů zde zapotřebí nebylo. Obdobně je tomu u MIP2. U přístupových bodů je nastavena i adresa rozhraní LAN. Pro přístupový bod MIP1 je to 192.168.10.1/24, pro přístupový bod MIP2 192.168.20.1/24. U obou přístupových bodů bylo ještě třeba staticky nastavit směrovací tabulku na hodnotu WAN rozhraní druhého ze směrovačů, aby bylo jasné, kam mají data přes WAN rozhraní posílat.

K přístupovému bodu MIP1 byly bezdrátově připojeni dva klienti. Jedním z nich byl i notebook, obsahující program IxChariot. K přístupovému bodu MIP2 byl připojen pouze jeden notebook. Množství klientů zde není až tak podstatné, protože program IxChariot umí simulovat veškerý provoz v síti. Aby měření probíhalo co možná nejrealněji, notebook s IxChariotem pouze generoval data v síti, ale nebyl koncovým bodem. Vzhledem k tomu, že měření je opravdu náročné na procesor i paměť, by tím mohla být naměřená data negativně ovlivněna.



Obr. 4.2: Architektura vytvořené bezdrátové sítě.

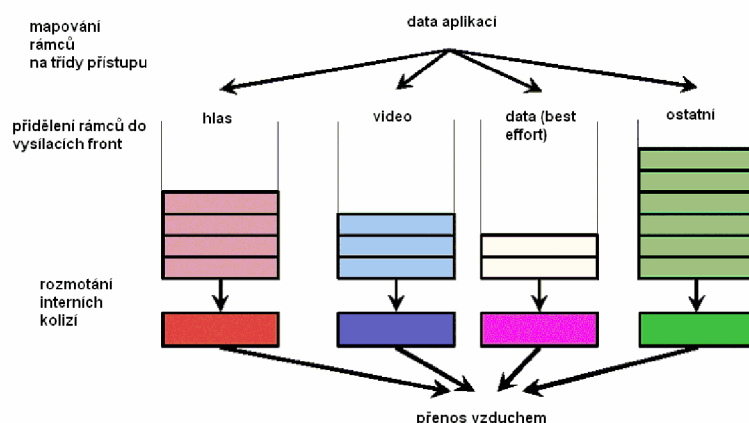
## 5. Implementace QoS a diagnostika sítě

Původním záměrem pro nastavení podpory pro kvalitu služeb bylo využití java aplikace SDM (Secure Device Manager) vytvořené přímo firmou Cisco pro snazší konfiguraci zařízení této řady. Původní verze SDM 2.4 ovšem tuto konfiguraci neumožňovala. Proto bylo třeba aktualizovat SDM na verzi 2.5, která již konfiguraci a podrobné nastavování kvality služeb umožňuje konfigurovat.

Po nainstalování a opětovném přihlášení do webové aplikace bylo třeba spustit sekundární aplikaci - pro konfiguraci bezdrátového připojení. Zde již byla v záložce služeb i možnost konfigurace kvality služeb. Po otevření záložky QoS se objevilo okno, kde bylo možno zaškrtnout použití WMM (Wireless Multimedia).

### 5.1 Wireless Multimedia - WMM

Je dočasné řešení pro podporu QoS vytvořené WiFi Aliancí. Původně WME (Wireless Multimedia Extensions). WMM podporuje pouze některé prvky 802.11e, jako označování rámců podle priorit a odpovídající 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 odlišení služeb po protokolu IP (mechanismus Differentiated Services) a rozděluje provoz do čtyř úrovní priorit (viz obrázek 5.1): nejvyšší prioritu má hlas, pak video, následuje best effort a vše ostatní. Tyto úrovně priorit se shodují s označením priorit podle 802.1d používaným v pevných LAN.[16]



Obr.5.1: Rozdělení provozu sítě do prioritních front. [16]

V současné době se pracuje na novém programu certifikace WMM-SA (WMM Scheduled Access), který už bude odvozen od schválené normy 802.11e.

- Při zapnutí WMM přidává přístupový bod třídu služby do hlavičky každého paketu.
- Každá přístupová třída má své sekvenční číslo. To umožňuje výše prioritovaným paketům přerušit vysílání níže prioritovaným paketům bez přetečení bufferu na straně příjemce.
- Pro přístupové třídy, které mají vysokou prioritu, jsou vysílače schopny vyslat skupinu čekajících paketů i v okamžiku, kdy je odloženo vysílání (backoff), dle nastavené doby - TXOP limitu, tedy doby, kdy mají příležitost k vysílání. To zvyšuje prostupnost sítě, protože pakety nemusí čekat až získají přístup, ale mohou být odesílány okamžitě, jeden po druhém. [1]

Při nastavování WMM je možno změnit přednastavené hodnoty pro jednotlivé přístupové kategorie dle potřeb správce sítě, viz obr.5.2. Vše lze samozřejmě nastavovat i přes příkazový řádek konzole (tzv. CLI - command line). Například zapnutí wmm se provádí v konfiguraci bezdrátového rozhraní zadáním příkazu: *dot11 qos mode wmm*

Enable WiFi Multimedia(WMM)

Access Category Definition					
Access Category		Background (CoS 1-2)	Best Effort (CoS 0,3)	Video (CoS 4-5)	Voice (CoS 6-7)
Min Contention Window (2 <sup>x</sup> -1; x can be 0-10)	Local	4	4	3	2
	Cell	4	4	3	2
Max Contention Window (2 <sup>x</sup> -1; x can be 0-10)	Local	10	6	4	3
	Cell	10	10	4	3
Fixed Slot Time (0-20)	Local	7	3	1	1
	Cell	7	3	2	2
Transmit Opportunity (0-65535 μS)	Local	0	0	3008	1504
	Cell	0	0	3008	1504

Obr.5.2: Nastavení WiFi Multimedia s defaultními hodnotami.

Protože SDM 2.5 je univerzální nástroj pro konfiguraci velkého množství typů Cisco směrovačů, ne všechny funkce musí být jednotlivými směrovači podporovány. WMM na směrovačích Cisco W871 není podporováno. Router nerozumí daným příkazům. Proto byl stáhnut nejnovější IOS (Internetwork Operating System), tedy operační systém routeru. Kvůli malé kapacitě flash paměti ve směrovačích bylo nutno nejdříve zálohovat a smazat stávající IOS, stejně jako SDM. Přístupové body jsou vybaveny USB porty, ale použitý flashdisk nebyl podporován. Jediným řešením byla komunikace pomocí Trivial FTP server (TFTP) od firmy SolarWinds. Jedná se o zjednodušený FTP server, který umožňuje bezdrátovou komunikaci s přístupovým bodem. Po vypsání obsahu paměti flash pomocí příkazu *show flash* již bylo možno zahájit kopírování.

```
copy flash: tftp:  
Source filename []? c870-advipservicesk9-mz.124-6.T7.bin  
Address or name of remote host []? 192.168.40.2  
Destination filename []?c870-advipservicesk9-mz.124-6.T7.bin
```

Obr.5.3: Kopírování IOS z paměti flash.

Ani s nejnovějším IOSem použité routery Cisco W871 nepodporovaly příkazy pro zapnutí mechanismu WMM. Proto bylo třeba nastavit podporu pro kvalitu služeb ručně, s použitím class-map a service-policy.

## 5.2 Zapnutí podpory QoS

Příkaz *class-map* – slouží k určení pravidel, dle kterých se budou vybírat pakety. Hledisek pro výběr paketů je mnoho. Lze vybrat podle access-listu, protokolu, hodnot DCSP, precedence, adres, příslušného VLANu a dalších. Lze nadefinovat i více pravidel, která musí paket splňovat. Jako rozlišovací hledisko byla zvolena hodnota DSCP, protože ji lze snadno nastavit u definice jednotlivých služeb v programu IxChariot.

Bylo třeba, aby se pakety žádaných služeb třídily do class-map dle hodnot DSCP (Differentiated Services Code Point) namísto třeba dle užitého protokolu. Jinak by

nebylo možné nastavit vyšší prioritu pro přenos hlasu než video, protože obě služby využívají protokol RTP (Real-time Transport Protocol), který je přenášen pomocí protokolu UDP (User Datagram Protocol).

DSCP - je šest nejdůležitějších bitů z hlavičky paketu v poli Diffserv, další dva se nazývají ECN (Explicit Congestion Notification) viz tab.5.1. Hodnota DSCP je zpětně slučitelná s IP Precedence (kterou tvoří první tři bity).

Tab.5.1: Pole Diffserv.

DS5	DS4	DS3	DS2	DS1	DS0	ECN	ECN
-----	-----	-----	-----	-----	-----	-----	-----

```

MIP2(config)#class-map match-all voice
MIP2(config-cmap)#match ip dscp ef
MIP2(config-cmap)#exit
MIP2(config)#class-map match-all video
MIP2(config-cmap)#match ip dscp af41
MIP2(config-cmap)#exit
MIP2(config)#class-map match-all priority_traffic
MIP2(config-cmap)#match ip dscp af31
MIP2(config-cmap)#exit

```

Obr.5.4: Nastavování class-map.

Příkaz **policy-map** – se používá pro definování pravidel QoS. Nejprve se zadá class-map, která nám dle nastavených parametrů vybírá pakety, na které se má aplikovat mechanismus pro zajištění QoS. Pro účel této bakalářské práce potřebujeme použít policy-mapu na bezdrátové rozhraní. Proto použijeme příkaz **set cos** pro nastavení jednotlivých tříd služeb nadeřinovaným class-mapám. Vzájemná spojitost mezi DSCP a COS je znázorněna v tabulce 5.2.



Tab.5.2: Služby, prioritní úrovně a jejich rozdělení. [4]

Typ provozu	IP DSCP	CoS	IEEE 802.11e	Poznámky
Řízení sítě	-	7	-	Reservováno pro řízení sítě
Mezisíťové řízení	48	6	7 (AC_VO)	IP routovací protokoly
Hlas	46 (EF)	5	6 (AC_VO)	Express Forwarding (EF)
Video	34 (AF41)	4	5 (AC_VI)	Třída 4
Priority data	26 (AF31)	3	4 (AC_VI)	Třída 3
Best Effort	0 (BE)	0	3 (AC_BE) 0 (AC_BE)	Best Effort
Pozadí	18 (AF21)	2	2 (AC_BK)	Třída 2
Pozadí	10 (AF11)	1	1 (AC_BK)	Třída 1

Do policy-mapy je třeba přiřadit všechny class-mapy s nastavenými rozlišovacími mechanismy pro jednotlivé pakety, na které chceme na daném rozhraní aplikovat QoS. (viz. obr.5.5)

```

MIP2(config)#policy-map WMM
MIP2(config-pmap)#class voice
MIP2(config-pmap-c)#set cos 5
MIP2(config-pmap-c)#exit
MIP2(config-pmap)#class video
MIP2(config-pmap-c)#set cos 4
MIP2(config-pmap-c)#exit
MIP2(config-pmap)#class priority_traffic
MIP2(config-pmap-c)#set cos 3
MIP2(config-pmap-c)#exit
MIP2(config-pmap)#exit

```

Obr.5.5: Přiřazení class-map do policy-mapy.

Příkazem *sh policy-map* - zobrazíme nastavené policy-mapy pro kontrolu, zda je vše správně nastaveno. (viz. obr.5.6)

```
MIP2#sh policy-map
Policy Map WMM
Class voice
set cos 5
Class video
set cos 4
Class priority_traffic
set cos 3
```

Obr.5.6: Zobrazení nastavené policy-mapy.

Příkaz *service-policy* – použitím tohoto příkazu lze přiřadit policy-mapu na zvolené rozhraní. Lze přiřadit jednu na vstup a jednu na výstup daného rozhraní. Nastavení kvality služeb je u obou přístupových bodů stejné. (viz. obr.5.7)

```
MIP2(config)#int dot11Radio 0
MIP2(config-if)#service-policy output WMM
MIP2(config-if)#exit
```

Obr.5.7: Nastavení policy-mapy na bezdrátové rozhraní.

Pro zajištění co možná nejvyšší kvality služeb bylo zapotřebí vytvořit alespoň základní nastavení QoS i na rozhraní WAN. Nastavíme pro každou z definovaných tříd provozu rezervovanou část linky. Pro video to je 20% v prioritní frontě, kde jsou data odesílána ihned. Pro hlas je to tentokrát 15% v prioritní frontě. Je to proto, že video toky mají neporovnatelně větší kapacitu (v řádech Mb/s) než hlasové toky (2x 64kb/s). Pro kritická data je rezervována 30% šířka pásma a pro ostatní provoz zbytek. (viz. obr.5.8)

Tuto policy-mapu je třeba, obdobně jako u bezdrátového rozhraní, přiřadit na rozhraní FastEthernet 4, tedy WAN. Zde ji stačí přiřadit pouze na výstup, směrem k druhému routeru. (viz. obr.5.9)

```
MIP2(config)#policy-map WAN
MIP2(config-pmap)#class voice
MIP2(config-pmap-c)#priority percent 15
MIP2(config-pmap-c)#exit
MIP2(config-pmap)#class video
MIP2(config-pmap-c)#priority percent 20
MIP2(config-pmap-c)#exit
MIP2(config-pmap)#class priority_traffic
MIP2(config-pmap-c)#bandwidth percent 30
MIP2(config-pmap-c)#exit
MIP2(config-pmap)#class class_default
MIP2(config-pmap-c)#fair-queue
MIP2(config-pmap-c)#exit
```

Obr.5.8: Nastavení policy-mapy pro WAN rozhraní.

```
MIP2(config)#int FastEthernet 4
MIP2(config-if)#service-policy output WAN
MIP2(config-if)#exit
```

Obr.5.9: Přřazení policy-mapy na výstup WAN rozhraní.

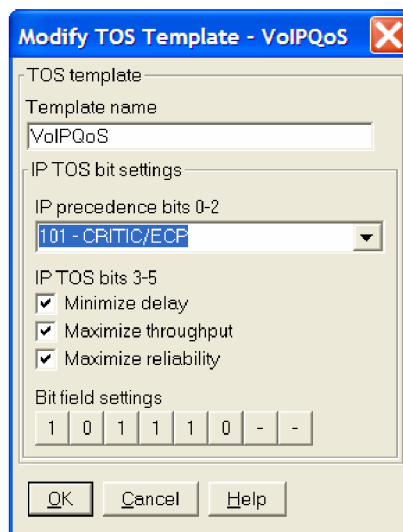
### 5.3 IxChariot

Program Ixchariot od společnosti Ixia, která je leaderem v testování výkonnosti sítí, je velice výkonným nástrojem, pro diagnostiku a simulování provozu v počítačových sítích. V rámci této bakalářské práce bylo využito především simulace provozu FTP serveru, obousměrné hlasové komunikace a videa v reálném čase.

### 5.3.1 Definování služeb

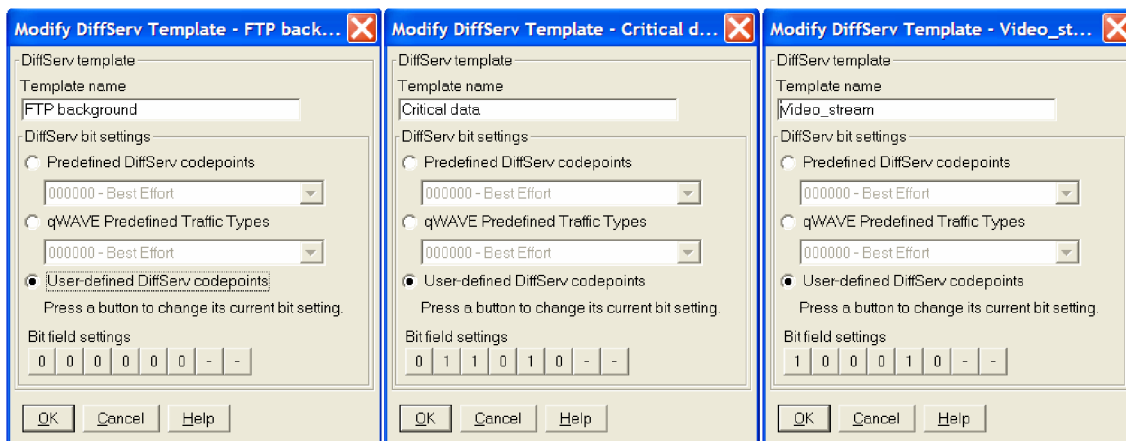
Nejprve bylo třeba nadefinovat si v programu jednotlivé služby dle doporučení RFC 2597 a RFC 2598 (Viz obrázky 5.10 a 5.11) [3].

Pro hlasové pakety se používá hodnota DSCP ef - Expedited Forwarding, která má nejnižší ztrátovost, nejnižší zpoždění i nejnižší jitter. Hodnota DSCP v binární podobě je 101110, v desítkové 46.



Obr.5.10: Nastavení služby VoIP v programu IxChariot.

Pro pakety video služeb je třeba také vysoká priorita, proto se používá čtvrtá třída s nejmenším možným zahazováním paketů. Použijeme DSCP AF41, v binární podobě je 100010, v desítkové soustavě 34. Pro kritická data, jako jsou přístupy k databázím a další je třeba také vyšší priority přenosu, než pro standardní data přenášená metodou Best effort. Proto jsem pro nadefinovanou třídu priority\_traffic použil třetí třídu, DSCP AF31, binárně 011010, desítkově odpovídající hodnotě 26. Pro zbývající provoz v síti je defaultně nastavena provozní třída default\_class, s metodou přenosu Best effort, DSCP default, binárně 000000.

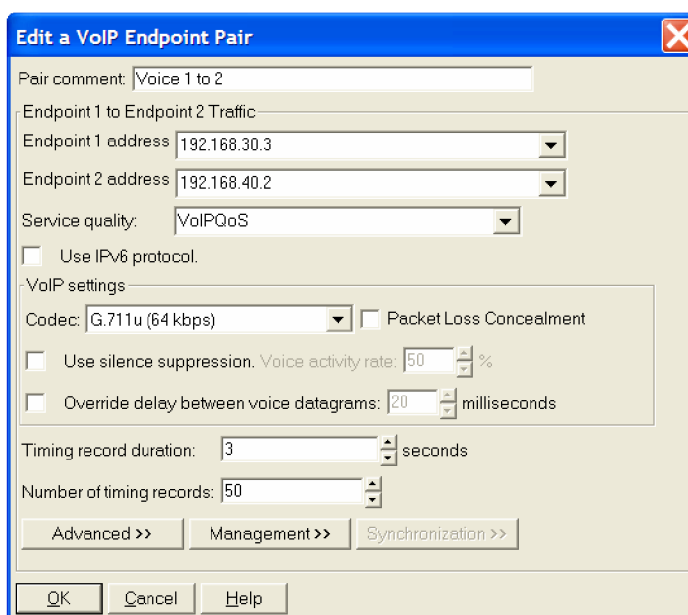


Obr.5.11: Nastavení služeb v programu IxChariot.

### 5.3.2 Nastavení toků

Nyní již stačí v IxChariotu nadefinovat koncové stanice, mezi kterými se bude měřit, nastavit typ simulovaného toku a nadefinovanou třídu služby. Aby mohlo měření probíhat, je nutno na obě koncové stanice nainstalovat program Endpoint Library. Ten je ke stažení na oficiálních stránkách IxChariotu v sekci download.

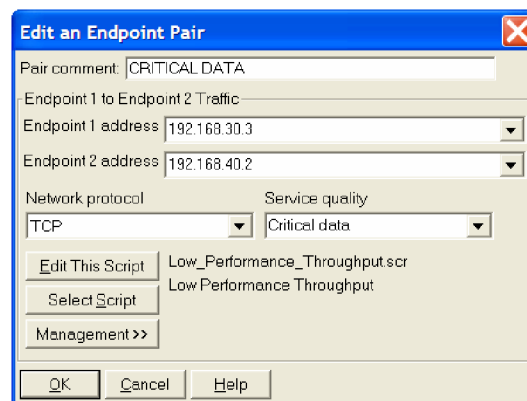
Nastavíme první hlasový pár, ve směru z první stanice do druhé, doplníme IP adresy jednotlivých stanic, vybereme nastavenou kvalitu služby a kodek, který bude použit pro hlas (viz. obr.5.12). Záměrně byl použit kodek G.711, protože má nejlepší kvalitu hlasu a nejmenší paketizační zpoždění.



Obr.5.12: Nastavení hlasového páru.

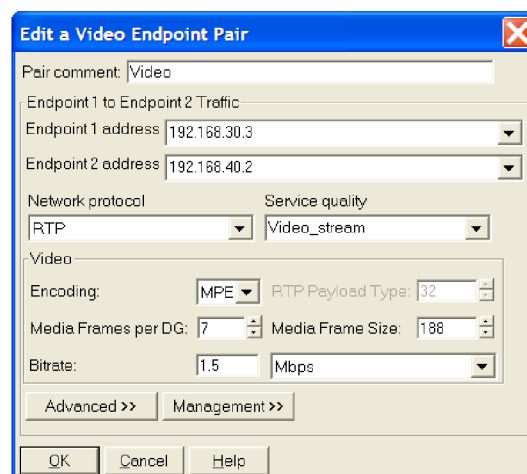
Obdobně se nastaví druhý hlasový pár, směrem od druhé stanice k první, protože telefonní hovor vždy probíhá oběma směry.

Dále byl nastaven TCP tok, představující kritická data (viz. obr.5.13). Je třeba zadat IP adresy obou koncových stanic, vybrat nastavenou kvalitu služby a vybrat z přednastavených scriptů pro simulaci TCP provozu na síti. Lze vybrat vysoké, střední a nižší zatížení sítě. V případě kritických dat jsem zvolil střední zatížení, protože v kombinaci s dalším TCP tokem, představujícím FTP již docházelo k zahlcení sítě, IxChariot zobrazoval varovná hlášení a měření neprobíhalo správně. Obdobné je nastavení simulovaného toku FTP. Zde byl ovšem zvolen script s vysokým zatížením sítě, protože při slabě zatížené síti nebyl tolik patrný rozdíl při zapnutí QoS.



Obr.5.13: Nastavení kritických dat.

Ještě bylo nutno nakonfigurovat simulaci videa v reálném čase. Po vyplnění adres koncových stanic je ještě třeba zvolit bitrate daného video toku a použité kódování.

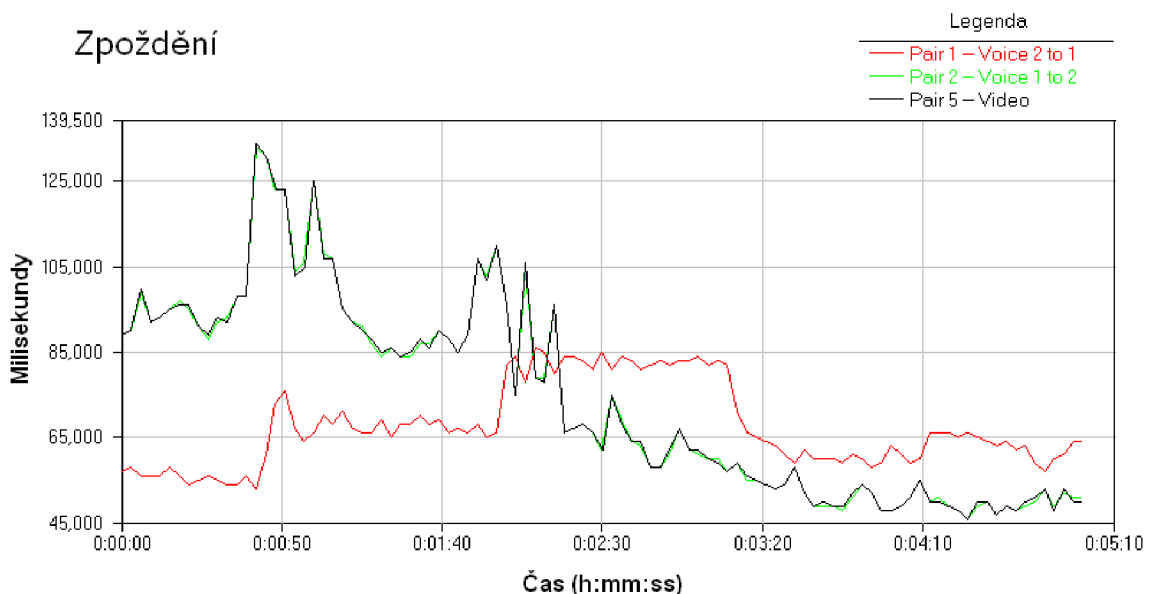


Obr.5.14: Nastavení videa v reálném čase.

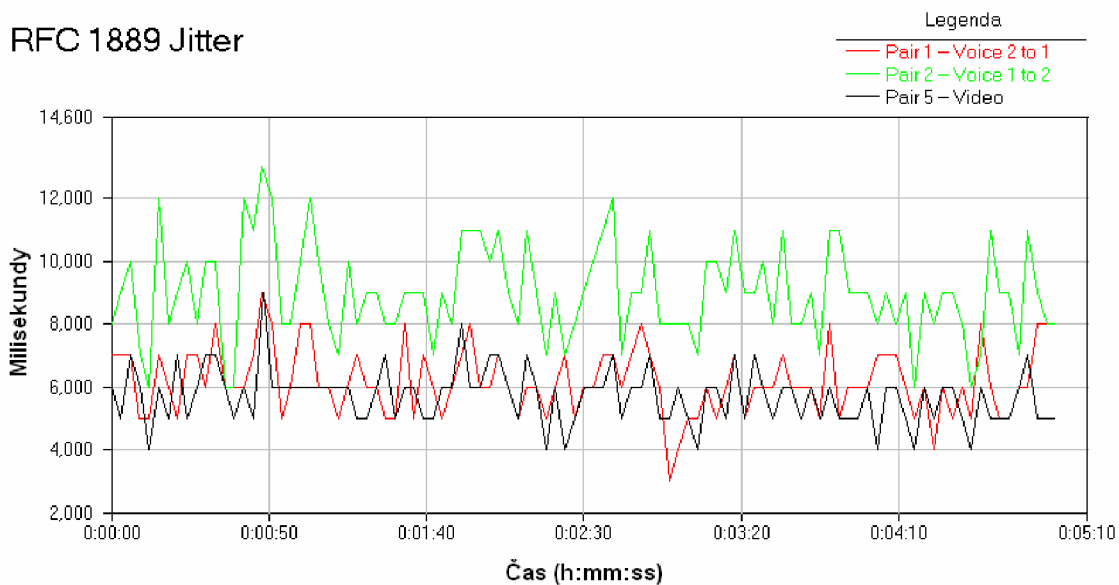
### 5.3.3 Vlastní měření

Po spuštění simulace se asi půl minuty inicializovali obě koncové stanice a pak již začalo probíhat vlastní měření, pěti minutového provozu v síti. Samozřejmě celá první série měření probíhala ještě dříve, než byla zapnuta podpora pro kvalitu služeb. Všechny simulované služby směřovali od první stanice ke druhé, vyjma hlasu, v grafech značeného jako Voice 2 to 1, který šel v opačném směru.

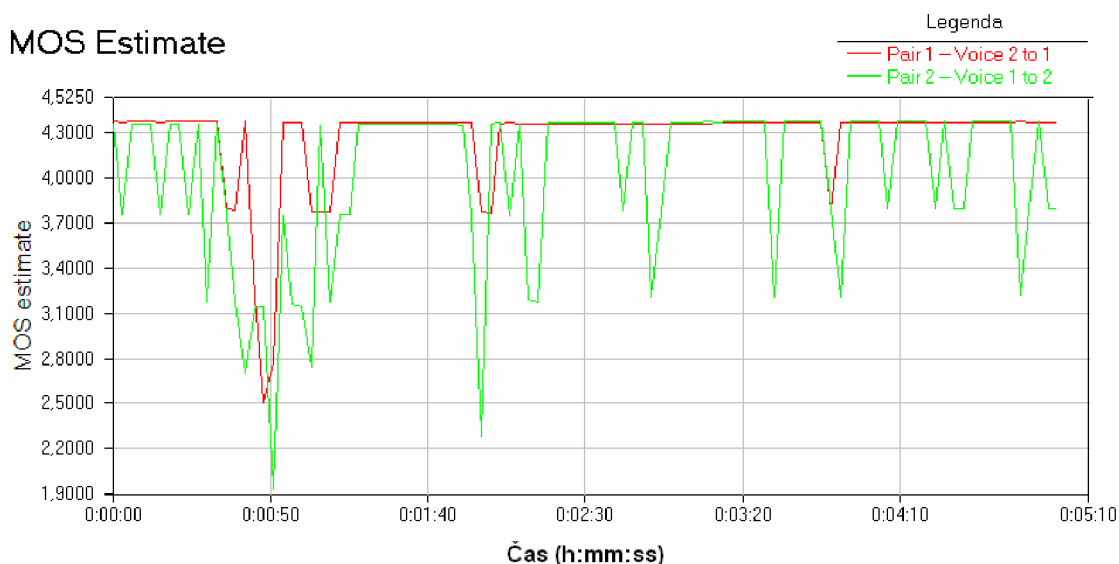
Jak je vidět na obrázku 5.15, bez zajištění kvality služeb je zpoždění relativně velké. Tok videa je kopírován hlasovým tokem stejného směru, protože oba využívají pro přenos protokolu UDP na transportní vrstvě. Zpoždění po určitém čase začíná klesat, protože UDP spojení „ovládne“ linku. Komunikace s použitím protokolu TCP je spolehlivá služba - je použito potvrzení o přijetí dat, v případě ztráty se vyžaduje jejich opětovné odeslání, což má za následek větší režii. Oproti tomu UDP je služba nespolehlivá, data se při ztrátě již znovu neposílají, jedná se o komunikaci s menší provozní režii. Na obrázku 5.16 je zobrazen jitter dané komunikace bez zapnuté podpory QoS. Jak je na něm patrné, je zde rozdíl zpoždění mezi přijatými pakety i 4ms. Níže na obrázku 5.17 je zobrazen MOS. Je zde patrné, že hlas, šířící se od první koncové stanice k druhé, bude pro uživatele vnímán velice negativně, hlas opačného směru až na jeden větší výpadek bude vnímán relativně obstojně. Je tomu proto, že ve směru od první stanice k druhé je protokol UDP využit ještě i k přenosu videa v reálném čase.



Obr.5.15: Zpoždění hlasu a videa bez QoS



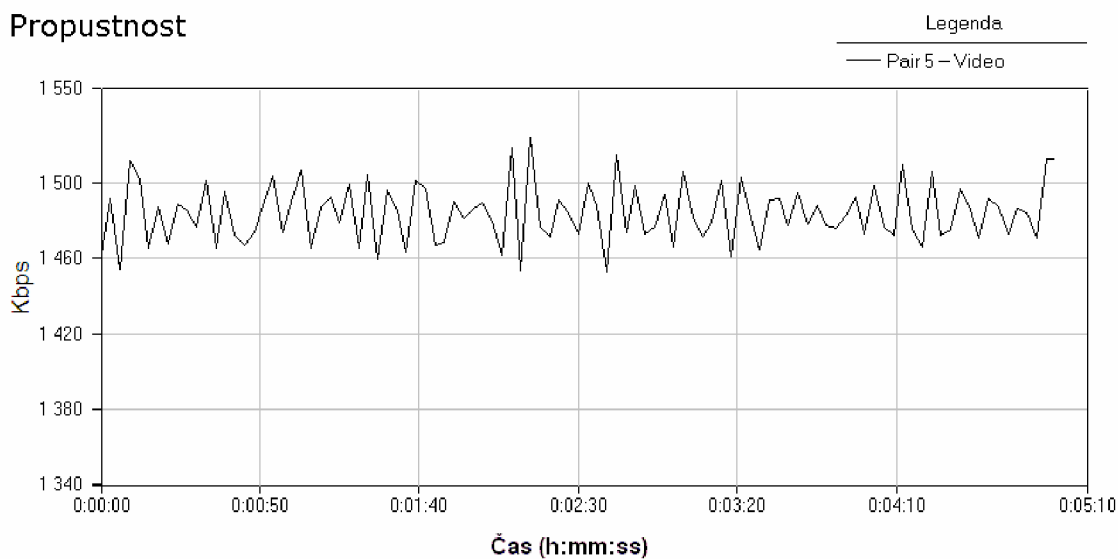
Obr.5.16: Jitter u komunikace bez QoS.



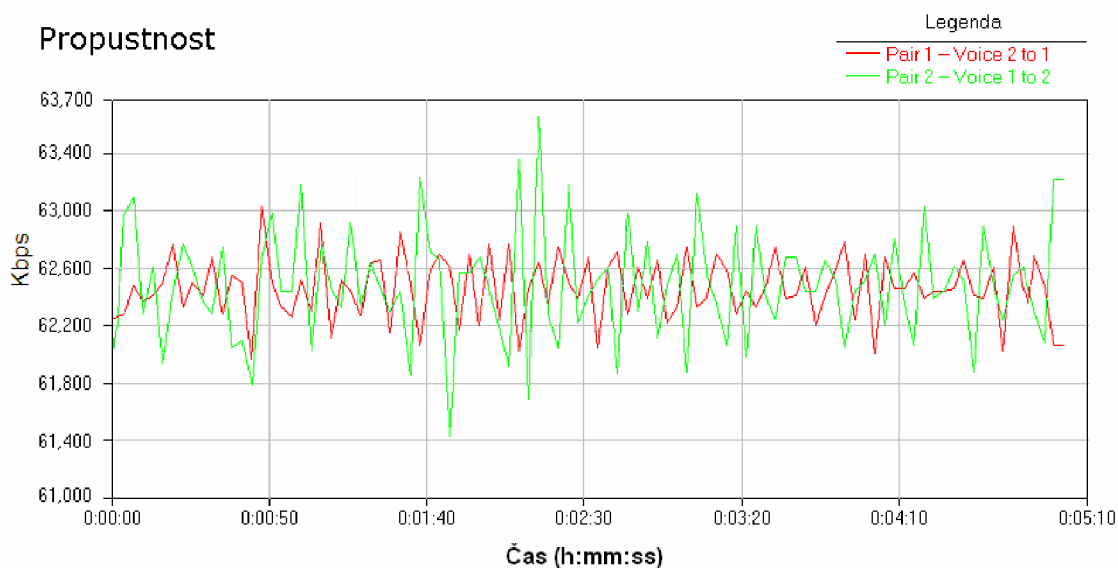
Obr.5.17: MOS bez QoS.

Na obrázcích 5.18 a 5.19 je zobrazena propustnost videa a hlasu bez QoS. Je zde vidět, že signál má relativně velký rozkmit. Pro srovnání je na obrázcích 5.23 a 5.24 zobrazena propustnost videa a hlasu se zapnutým QoS. Jak je vidět, signál je již ustálenější a má pouze malý rozkmit.





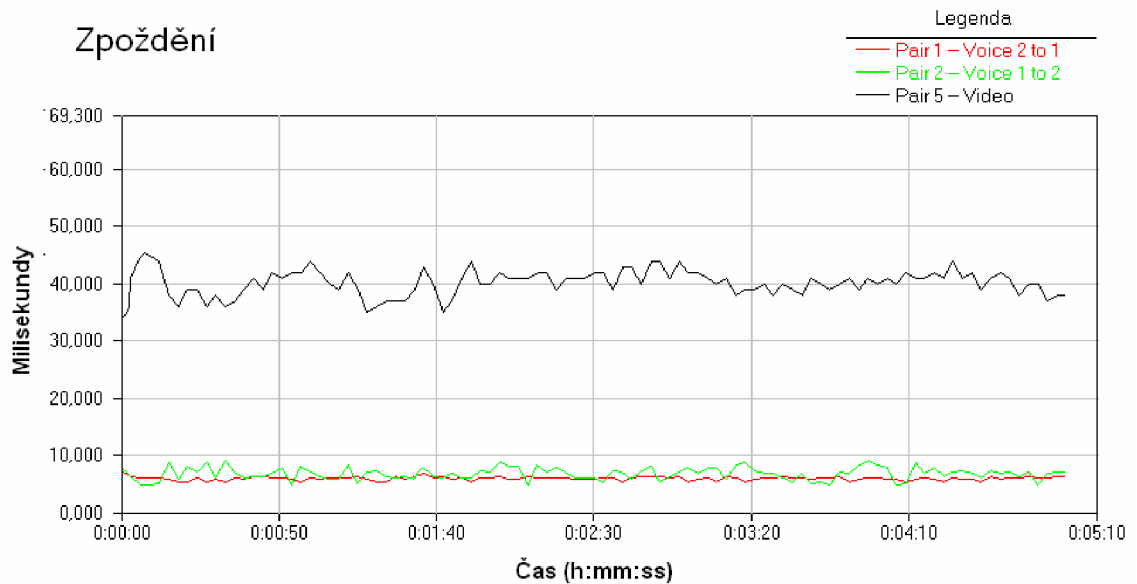
Obr.5.18: Propustnost sítě u toku videa bez QoS.



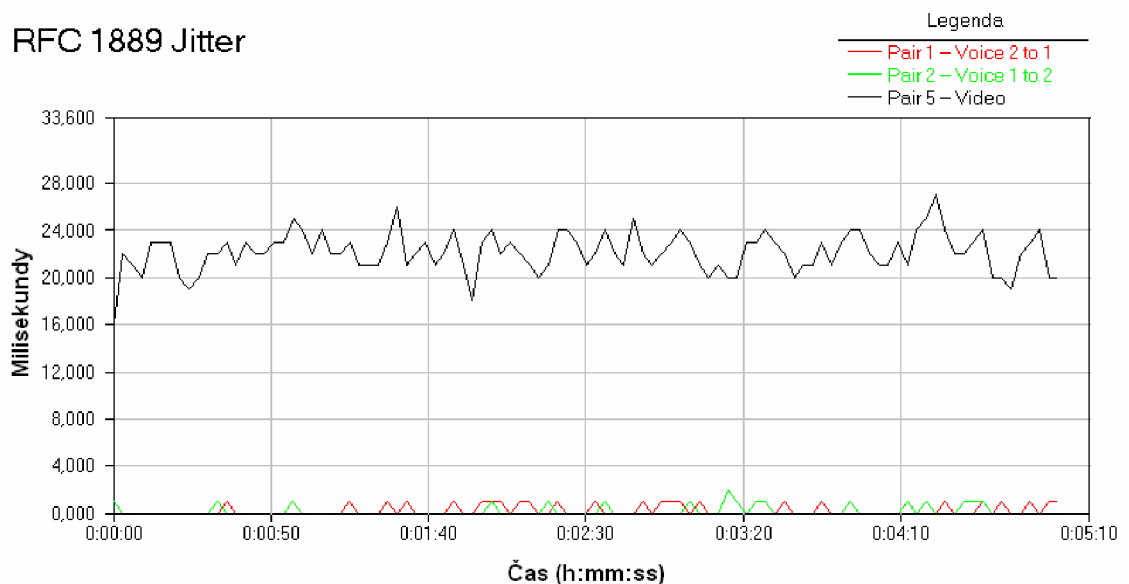
Obr.5.19: Propustnost sítě u oboustranné hlas.komunikace bez QoS.

Druhá série měření proběhla až po kompletním nastavení a zapnutí QoS. Jak je vidět na obr.5.20, zpoždění u videa kleslo zhruba na hodnotu 40ms, zpoždění obou toků hlasů se drží celou dobu přenosu pod 10ms. Kvalita hovoru dle vnímání uživatele je vynikající, bez jediného zakolísání (viz obr.5.22). V případě hovoru z druhé stanice do první vyšly

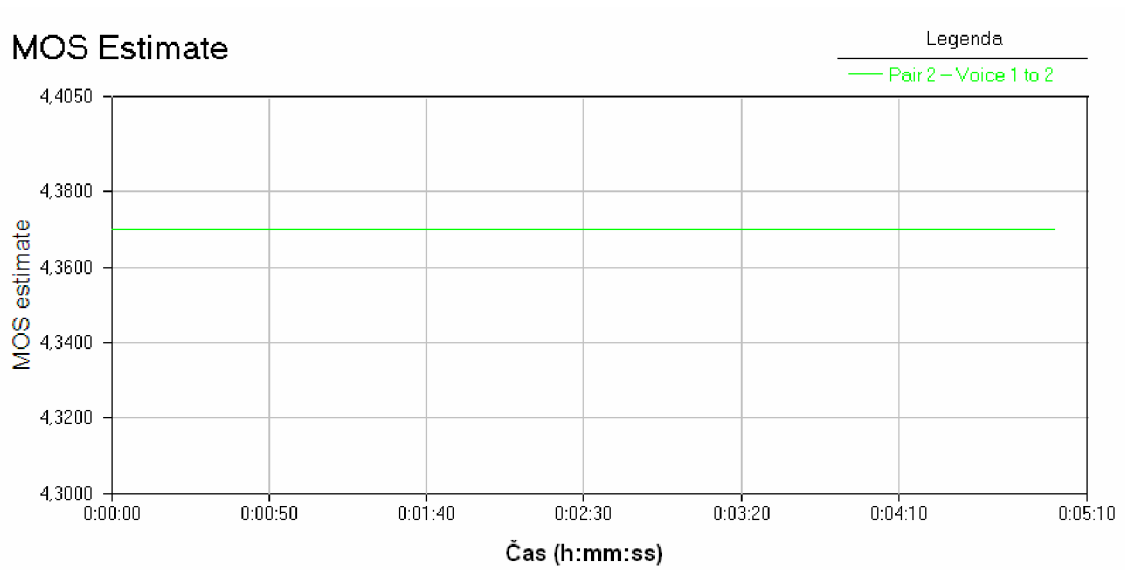
stejné hodnoty MOS jako při hovoru z první do druhé, grafy se shodovaly a obě přímky se překrývaly. Rovněž propustnost sítě pro video i hlas je rovněž podstatně stálější, téměř konstantní. Díky definici tříd provozu nejsou ani TCP toky ovlivněny UDP toky, které jim bez QoS „brali“ kapacitu linky.



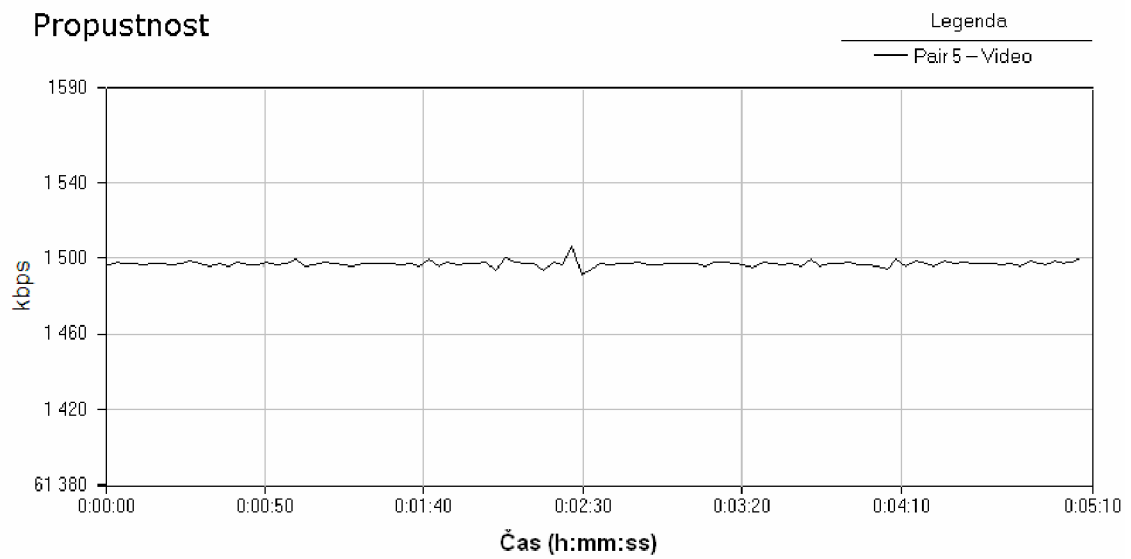
Obr.5.20: Zpoždění hlasu a videa s QoS.



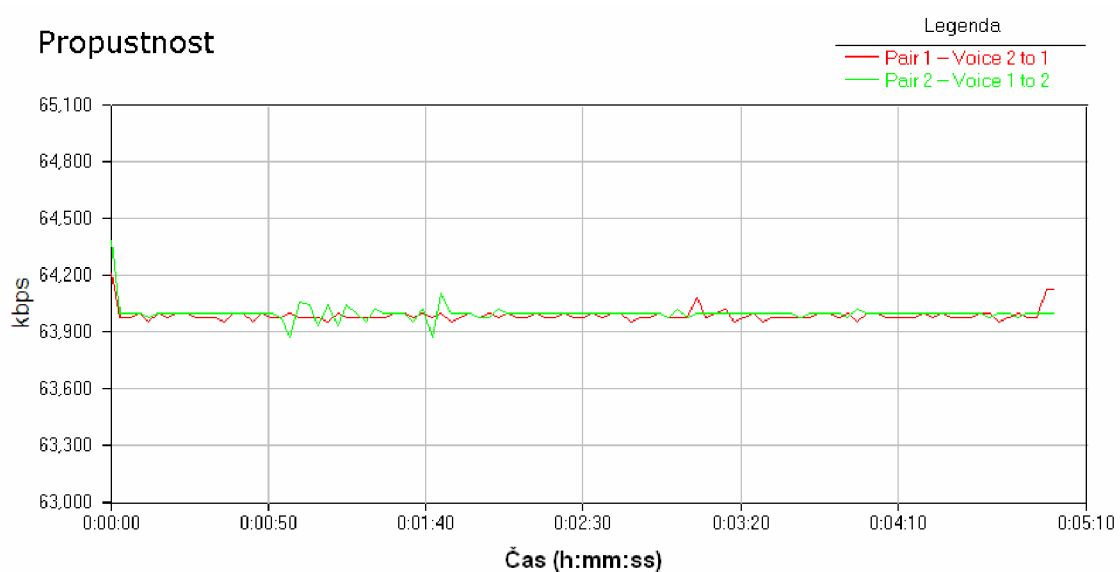
Obr.5.21: Jitter u komunikace s QoS.



Obr.5.22: MOS při komunikaci s QoS od 1. stanice ke 2.



Obr.5.23: Propustnost sítě u toku videa s QoS.



Obr.5.24: Propustnost sítě u toku hlasu oběma směry s QoS.

Shrnutí naměřených hodnot hlavních parametrů ovlivňujících multimediální služby v reálném čase je zobrazeno v tabulce 5.3.

Tab.5.3: Shrnutí změřených parametrů

	Maximální zpoždění (ms)		Minimální MOS	
	Bez QoS	S QoS	Bez QoS	S QoS
Hlas 1. k 2.	133	9	1,9	4,370
Hlas 2. k 1.	85	7	2,5	4,370
Video 1. k 2.	133	45	-	-

## 6. Závěr

Tato bakalářská práce shrnuje problematiku bezdrátových sítí a popis standardů 802.11. Hlouběji popisuje doplněk 802.11e a mechanismy, používané pro zajištění kvality služeb v bezdrátových sítích. Dále se zabývá parametry ovlivňujícími kvalitu služeb, přístupovými a koordinačními funkcemi.

Pro zpracování praktické části bakalářské práce bylo nezbytné seznámit se s možnostmi programu IxChariot, nastavením jednotlivých služeb a jejich následné simulace reálného provozu v síti a jeho vyhodnocování. Současně bylo třeba nastavit na aktivních prvcích dané sítě mechanismus pro podporu kvality služeb. Následně byla simulována a zaznamenávána komunikace mezi koncovými stanicemi dané sítě. Nejdříve bez zapnuté podpory kvality služeb a následně již s plně nastavenou podporou. Při porovnání obou situací byly zjištěny podstatné rozdíly. Bez zapnuté podpory pro kvalitu služeb docházelo k relativně velkému zpoždění u aplikací pracujících v reálném čase, která by v reálné síti měla za následek nižší kvalitu poskytovaných služeb a nespokojenost uživatelů s jejich používáním. Naopak při zapnuté podpoře pro kvalitu služeb tato zpoždění dosahovala minimálních hodnot. Díky tomu je umožněno plné využití těchto aplikací a maximální spokojenost uživatelů.

Vzhledem k tomu, že se jedná o laboratorní síť menších rozměrů, změřené hodnoty bez zapnuté podpory QoS nejsou kritické a služby by obstojně fungovaly. Nebyla by však zaručena jejich plná kvalita, proto bych doporučoval podporu pro kvalitu služeb ponechat zapnutou i v obdobně velkých bezdrátových sítích.

## Použitá literatura

- [1] Cisco Systems, Inc.. *Cisco Router and Security Device Manager 2.5 User's Guide* [online]. 2007 [cit. 2009-05-13]. Dostupný z WWW:  
<[http://www.cisco.com/en/US/docs/routers/access/cisco\\_router\\_and\\_security\\_device\\_manager/25/software/user/guide/SDM25ug.pdf](http://www.cisco.com/en/US/docs/routers/access/cisco_router_and_security_device_manager/25/software/user/guide/SDM25ug.pdf)>.
- [2] Cisco Systems, Inc.. *Configuring QoS on an Access Point* [online]. 1992-2009 [cit. 2009-05-13]. Dostupný z WWW:  
<<http://www.cisco.com/en/US/docs/routers/access/1800/wireless/configuration/guide/s37qos.html>>.
- [3] Cisco Systems, Inc.. *Implementing Quality of Service Policies with DSCP* [online]. 2008 [cit. 2009-05-16]. Dostupný z WWW:  
<[http://www.cisco.com/en/US/tech/tk543/tk757/technologies\\_tech\\_note09186a00800949f2.shtml](http://www.cisco.com/en/US/tech/tk543/tk757/technologies_tech_note09186a00800949f2.shtml)>.
- [4] Cisco Systems, Inc.. *QoS on Wireless LAN Controllers and Lightweight APs Configuration Example* [online]. 2008 [cit. 2009-05-14]. Dostupný z WWW:  
<[http://www.cisco.com/en/US/tech/tk722/tk809/technologies\\_configuration\\_example09186a00807e9717.shtml](http://www.cisco.com/en/US/tech/tk722/tk809/technologies_configuration_example09186a00807e9717.shtml)>.
- [5] DOOLEY, Kevin., BROWN, Ian. *Cisco IOS Cookbook*. Sebastopol: O'Reilly Media, 2006, ISBN 978-0596527228.
- [6] GAST, Mathew. *802.11 Wireless Networks: The Definitive Guide, Second Edition*. Sebastopol: O'Reilly Media, 2005, ISBN 978-0596100520.
- [7] HELD, Gilbert. *Ethernet Networks: Design, Implementation, Operation, Management*. [s.l.] : [s.n.], 2003. 610 s. ISBN 978-0-470-8.
- [8] HORSKÝ, Radek, *Bezdrátové Wi-Fi v rekordním čase*. Praha: Grada Publishing 2006, ISBN 80-247-1790-5.

- [9] Ixia. *Assessing VoIP Call Quality Using the E-model* [online]. c2009 [cit. 2009-05-12]. Dostupný z WWW: <[http://www.ixiacom.com/library/white\\_papers/display?skey=voip\\_quality](http://www.ixiacom.com/library/white_papers/display?skey=voip_quality)>.
- [10] MANGOLD, Stefan, et al. *IEEE 802.11e Wireless LAN for Quality of Service*. [s.l.] : [s.n.], [2006]. 8 s.
- [11] MOLNÁR, Karol. *Bezdrátové síťové technologie*, 2004. 21 s, Skripta.
- [12] MOLNÁR, Karol. *Zajištění kvality služeb v bezdrátových a mobilních sítích*. 2007. 36 s, Skripta.
- [13] PETERKA, Jiří. *Archiv článků a přednášek* [online]. 2006. Dostupný z WWW: <<http://www.earchiv.cz>>.
- [14] PRASAD, Neeli, PRASAD, Anand. *802.11 WLANs and IP Networking: Security, QoS, and Mobility*. London: Artech House Publishers, 2005, ISBN: 1580537898.
- [15] *Přehled doplňků standardu IEEE 802.11* [online]. 30. 12. 2005 [cit. 2009-01-10]. Dostupný z WWW: <<http://access.feld.cvut.cz/view.php?cisloclanku=2005113002>>.
- [16] PUŽMANOVÁ, Rita. *Lupa: server o českém internetu* [online]. 2002-2006. Dostupný z WWW: <[www.lupa.cz](http://www.lupa.cz)>.
- [17] PUŽMANOVÁ, Rita. *Moderní komunikační sítě od A do Z*. 2. aktualiz. vyd. Brno : Computer Press a.s., 2006, ISBN 80-251-1278-0.
- [18] WEIHUA XI, Helen, et al. *Modeling and Simulation of MAC for QoS in IEEE 802.11e Using OPNET Modeler.*, Bristol: University of Bristol, 2004. 6 s.
- [19] *Wikipedia, the free encyclopedia* [online]. 2001- [cit. 2008-11-04]. Dostupný z WWW: <<http://en.wikipedia.org>>.

## Seznam použitých zkratek

<b>AC</b>	Access Category
<b>ACK</b>	Acknowledge
<b>AIFS</b>	Arbitration Interframe Space
<b>ANSI</b>	American National Standards Institute
<b>AP</b>	Access Point
<b>BSS</b>	Basic Service Set
<b>BSSID</b>	BSS Identifier
<b>CAP</b>	Controlled Access Phase
<b>CCK</b>	Complementary Code Keying
<b>CFP</b>	Contention-Free Period
<b>CLI</b>	Command Line
<b>CoS</b>	Class of Service
<b>CP</b>	Contention Period
<b>CSMA/CA</b>	Carrier Sense Multiple Access/Collision Avoidance
<b>CSMA/CD</b>	Carrier Sense Multiple Access/Collision Detection
<b>CTS</b>	Clear to send
<b>CW</b>	Contention Window
<b>DCF</b>	Distributed Coordination Function
<b>DIFS</b>	DCF InterFrame Space
<b>DS</b>	Distribution system
<b>DSCP</b>	Differentiated Services Code Point
<b>DSRC</b>	Dedicated Short Range Communications
<b>DSSS</b>	Direct Sequence Spread Spectrum
<b>EAS</b>	Advanced Encryption Standard
<b>ECN</b>	Explicit Congestion Notification
<b>EDCA</b>	Enhanced Distributed Channel Access
<b>EDCF</b>	Enhanced Distributed Coordination Function
<b>ESS</b>	Extended Service Set
<b>EWC</b>	Enhanced Wireless Consortium
<b>FDDI</b>	Fiber Distributed Data Interface
<b>FHSS</b>	Frequency Hopping Spread Spectrum
<b>FSS</b>	Fixed Satellite Service
<b>HC</b>	Hybrid Coordinator
<b>HCCA</b>	HCF Controlled Channel Access
<b>HCF</b>	Hybrid Coordination Function
<b>IAPP</b>	Inter - Access Point Protocol
<b>IBSS</b>	Independent Basic Service Set
<b>IEEE</b>	Institute of Electrical and Electronics Engineers
<b>IEEE-SA</b>	IEEE Standards Association
<b>IFS</b>	InterFrame Space
<b>IOS</b>	Internetwork Operating System
<b>ITU-T</b>	International Telecommunications Union - Telecommunications Standardization Sector
<b>LAN</b>	Local Area Network
<b>LLC</b>	Logical Link Control
<b>MAC</b>	Media Access Control



<b>MCM</b>	MultiCarrier Modulation
<b>MIMO</b>	Multiple Input Multiple Output
<b>MOS</b>	Mean Opinion Score
<b>NAV</b>	Network Allocation Vector
<b>OFDM</b>	Orthogonal Frequency Division Multiplex
<b>PCF</b>	Point Coordination Function
<b>PIFS</b>	Point Coordination Function Interframe Space
<b>QAP</b>	Quality of service supporting Acces Point
<b>QBSS</b>	QoS supporting Basic Service Set
<b>QoS</b>	Quality of Service
<b>QSTA</b>	QoS supporting Station
<b>RRM</b>	Radio Resource Measurement
<b>RTP</b>	Real-time Transport Protocol
<b>RTS</b>	Request To Send
<b>SDM</b>	Secure Device Manager
<b>SIFS</b>	Short InterFrame Space
<b>SSID</b>	ESS Identifier
<b>STP</b>	Spanning Tree Protocol
<b>TDD</b>	Time Division Duplex
<b>TXOP</b>	Transmission Oportunity
<b>UDP</b>	User Datagram Protocol
<b>UP</b>	User Priorities
<b>UWB</b>	Ultra WideBand
<b>VoIP</b>	Voice over IP
<b>WAVE</b>	Wireless Access for the Vehicular Environment
<b>WEP</b>	Wireless Encryption Privacy
<b>Wi - Fi</b>	Wireless Fidelity
<b>WLAN</b>	Wireless Local Area Network
<b>WMAN</b>	Wireless Metropolitan Area Network
<b>WME</b>	Wireless Media Extension
<b>WMM</b>	Wireless Multi Media
<b>WMM-SA</b>	Wireless Multi Media Scheduled Access
<b>WPAN</b>	Wireless Personal Area Network
<b>WPP</b>	Wireless Performance Prediction