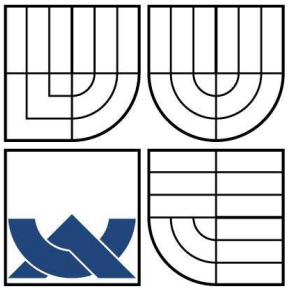
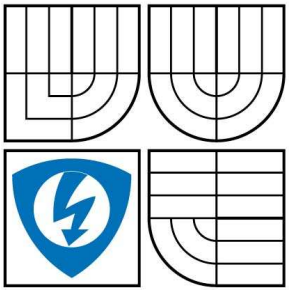


VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY



FAKULTA ELEKTROTECHNIKY A KOMUNIKACNÍCH TECHNOLOGIÍ
ÚSTAV TELEKOMUNIKACÍ

FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION
DEPARTMENT OF TELECOMMUNICATIONS

ZAJIŠTĚNÍ KVALITY SLUŽEB QOS V BEZDRÁTOVÝCH SÍTÍCH 802.11

QUALITY OF SERVICES IN WIRELESS NETWORKS 802.11

BAKALÁŘSKÁ PRÁCE
BACHELOR'S THESIS

AUTOR PRÁCE — TOMÁŠ KOPEČEK
AUTHOR

VEDOUCÍ PRÁCE — ING. JOSEF VYORAL
SUPERVISOR

BRNO 2007

ORIGINÁLNÍ ZADÁNÍ

LICENČNÍ SMLOUVA
POSKYTOVANÁ K VÝKONU PRÁVA UŽÍT ŠKOLNÍ DÍLO

uzavřená mezi smluvními stranami:

1. Pan/paní

Jméno a příjmení: Tomáš Kopeček

Bytem: Kaunicova 1075, Jaroměřice n./Rok, 67551

Narozen/a (datum a místo): 5. 3. 1985, Třebíč

(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:

.....

(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:	
Vedoucí/ školitel VŠKP:	
Ústav:	
Datum obhajoby VŠKP:	

VŠKP odevzdal autor nabyvateli v*:

□ tištěné formě – počet exemplářů ……..

□ elektronické formě – počet exemplářů ……..

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 pořizovaní 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.

---

* hodící se zaškrtněte

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 tísni a za nápadně nevýhodných podmínek.
4. Licenční smlouva nabývá platnosti a účinnosti dnem jejího podpisu oběma smluvními stranami.

V Brně dne: …….

…….. ……

Nabyvatel Autor

ANOTACE

Tato bakalářská práce podává ucelený přehled o bezdrátových sítích typu 802.11, známých pod označením Wi-Fi. Obsahuje tři hlavní části, z nichž první dvě jsou teoretické poznatky. V první části se práce týká problematiky zabezpečení těchto sítí a v druhé pak problematiky kolem zajištění kvality služeb, QoS. Třetí, praktická část, se zaměřuje na ověření správné funkce standardu 802.11e, který zajišťuje v sítích 802.11 podporu kvality služeb. Protože došlo v posledních letech k obrovskému zvýšení poptávky po multimediálních službách, je tato podpora v bezdrátových sítích nezbytná.

ABSTRACT

This bachelor's thesis reports an integrated view of wireless networks of standard 802.11, known as Wi-Fi. It contains three main parts, the first two of them are theoretical knowledge. The first part of work have to do with the security issue of WLAN, the second part refers to security issue of quality of services (QoS). The aim of the third, practical part is to verify the right functions of standard 802.11e, which ensures the support of quality of services in networks 802.11. Because of huge expansion of multimedia services demand, is this support in wireless networks necessary.

PROHLÁŠENÍ

Prohlašuji, že svou bakalářskou práci na téma " Zajištění kvality služeb QoS v bezdrátových sítích 802.11" jsem vypracoval samostatně pod vedením vedoucího bakalářské práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou všechny citovány v práci a uvedeny v seznamu literatury na konci práce.

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

V Brně dne …… ……..……..

Podpis

PODĚKOVÁNÍ

Děkuji vedoucímu bakalářské práce Ing. Josefu Vyoralovi za účinnou metodickou, pedagogickou a odbornou pomoc a další cenné rady při zpracování mé bakalářské práce.

SEZNAM ZKRATEK

AC	Access Category – kategorie přístupu
ACK	Acknowledge – potvrzení o přijetí
AES	Advanced Encryption Standard - způsob šifrování
AIFS	Arbitration Interframe Space - intervalu čekání v QoS
AP	Access Point – přístupový bod
CFP	Contention Free Period –interval, nedochází k soupeření o přístup
CP	Contention Period – interval, použitá funkce DCF
CW	Conection Windows – okno soutěžení
DCF	Distributed Coordination Function – distribuovaná koordinační fc
DIFS	Distributed Interframe Space -
DSSS	Direkt Sequence Spread Spektrum
EAP	Extensible Authentication Protocol
EDCA	Ehanced Distributed Channel Access
EDCF	Enhanced Distributed Coordination Function
FEC	Forvard Error Correction
FHSS	Frequency Hopping Spread Spektrum
FTP	File Transfer Protokol
HCCA	HCF Controlled Channel Access
HCF	Hybrid Coordination Function
IEEE	Institute of Electrical and Electronics Engineers
IP	Internet Protokol
ISM	Industrial Scientific and Medical
LAN	Local Area Network
MAC	Media Access Control
MIC	Message Integrity Check
OFDM	Orthogonal Frequency Division Multiplex
PCF	Point Coordination Function
PIFS	Point Coordination Function Interframe Space
QoS	Quality of Service
RADIUS	Remote Authentication Dial-In User Service
SIFS	Short Interframe Space
SSID	Service Set Identifier
TKIP	Temporal Key Integrity Protocol
VoIP	Voice over Internet Protokol
WEP	Wired Equivalent Privacy
Wi-Fi	Wireless Fidelity
WLAN	Wireless Local Area Network
WPA	Wi-Fi Protected Access

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

OBSAH

1 ÚVOD

Bezdrátové technologie jsou v dnešní době jedním z nejperspektivnějších odvětví informačních technologií. Právě toto bylo jedním z důvodů, proč jsem si zvolil za téma bakalářské práce tuto problematiku. Moje práce se zaměřuje na nejrozšířenější technologii z bezdrátových komunikací a to na standard IEEE 802.11, zvaný též Wi-Fi, vyvíjeného pracovní skupinou č. 11 v rámci schvalovací komise IEEE (Institute of Electrical and Electronics Engineers). V jednotlivých kapitolách je zde rozebrána problematika týkající se zabezpečení WiFi sítí a dále pak problematika zajištění kvality a služeb QoS (Quality of services), která je zahrnuta v novém standardu 802.11e.

V posledních několika letech došlo k velkému rozmachu multimediálních služeb, které však kladou na bezdrátovou komunikační síť nemalé nároky, protože vyžadují přenos v reálném čase. Jedná se především o IP telefonii, kterou známe pod označením VoIP, dále pak přenos videa a dalších interaktivních služeb. Tyto služby vyžadují úpravu stávajících sítí v podpoře zajištění kvality a služeb.

Výsledkem této bakalářské práce by mělo být porovnání bezdrátových sítí typu 802.11 bez podpory QoS a s implementovanou podporou 802.11e, což je doplňující standard zajišťující kvalitu služeb. Práce by měla objasnit, zda tento nový standard plní správně svoji funkci a zda je díky němu dosaženo požadované úrovně kvality služeb. Těchto výsledků chci dosáhnou pomocí simulačního nástroje programu Opnet Modeler, ve kterém nasimuluji sítě obou typů a následně je pomocí vygenerovaných statistik porovnám. Současně by práce měla ukázat, jak budou ve stávajících Wi-Fi sítích spolupracovat stanice bez podpory QoS a s ní.

2 BEZDRÁTOVÉ SÍTĚ WLAN

O výhodách využití bezdrátových lokálních sítí (Wireless Local Area Network, WLAN) k rozšíření stávajících sítí LAN i jejich plnohodnotné náhradě není třeba příliš hovořit. Jejich donedávna malé rozšíření souviselo s pomalou standardizací, nižšími přenosovými rychlostmi a také dražšími zařízeními. Ale normalizace i trh dnes vypadají jinak a zejména poslední dva roky jsou svědkem jejich výrazného nástupu, jak v podnikovém nebo domácím prostředí, tak na veřejných místech.

Rádiové vysílání, kterým je dnes řešena většina komerčně nasazovaných sítí, je náchylné na rušení, a to všemi prostředky, které mohou na příslušných kmitočtech pracovat (např. i mikrovlnné trouby - to se týká zejména bezlicenčního pásma 2,4GHz). Optické bezdrátové sítě či sítě založené na infračerveném záření zase nesnesou překážky mezi vysílačem a anténou přijímače. Dosah související s kvalitou přenosu pak omezuje jejich velikost i počet systémů, které se v rámci daného prostoru mohou nacházet, aby nedocházelo k nežádoucímu rušení. Zajištění bezpečnosti bezdrátové komunikace je při rádiovém vysílání jedním z nejobtížnějších problémů, podobně jako roaming a směrování mezi různými sítěmi. To však již je záležitostí vyšších vrstev, nikoli nejnižších dvou, jež definují normy IEEE 802.

2.1 Historie a vznik Wi-Fi

Hlavní odlišností bezdrátových Wi-Fi sítí od jiných druhů bezdrátových sítí jako jsou např. GSM, CDMA atd. je v používaném frekvenčním pásmu, od něhož se také odvíjí dostupnost běžným uživatelům. Většina ostatních bezdrátových sítí (tedy ne Wi-Fi) jsou tzv. licencované sítě, což znamená, že každá taková síť má svoji přidělenou frekvenci a pásmo, na kterou musí mít provozovatel licenci

vydávanou regulačními orgány. Na dané frekvenci smí vysílat jen ten, kdo si zaplatil licenci. Kromě těchto licencovaných pásem existuje ale i pásmo veřejné – tzv. pásmo ISM (Industrial Scientific and Medical). ISM pásmo využívají kromě vědeckých, průmyslových a lékařských organizací také např. mikrovlnné trouby a bezdrátové telefony (typu DECT, avšak ne mobilní). Pásmo ISM je vymezeno na frekvenci 2,4GHz v Evropě regulační organizací ETSI a v USA organizací FCC. Toto pásmo neuniklo pozornosti ani výrobcům bezdrátových sítí. Zpočátku však každý výrobce vyráběl vlastní technologie. Tyto proprietární technologie většinou nebyly kompatibilní s ostatními bezdrátovými sítěmi, proto vznikl v červnu 1997 společný standard pro bezdrátové sítě v pásmu ISM. Tento standard vytvořený institutem IEEE (Institute of Electrical and Electronic Engineers) je znám pod označením 802.11 a podporuje datové přenosy v oboru infračerveného záření a dva typy rádiových přenosů v nelicencovaném frekvenčním pásu 2,4GHz s maximální komunikační rychlostí 2Mb/s. Prvním je Frequency Hopping Spread Spektrum (FHSS) a druhým Direkt Sequence Spread Spektrum (DSSS). Ačkoliv šlo o standard, tak stále nebylo možné v některých případech provozovat a kombinovat zařízení od různých výrobců. Nekompatibilita výrobků vzbuzovala nedůvěru uživatelů a snižovala zájem o sítě 802.11. Proto vznikla certifikační společnost WECA, která testuje kompatibilitu jednotlivých zařízení standardu 802.11 a výrobkům vyhovujícím všem požadavkům uděluje logo Wi-Fi, které je na Obr. 2.1. Tato zkratka znamená Wireless Fidelity (zde je patrná analogie s označením Hi-Fi, používaným u audio a video techniky). Wi-Fi technologie dosáhla takového úspěchu, že se sama společnost WECA přejmenovala roku 2003 na Wi-Fi. V dnešní době, pokud mluvíme o Wi-Fi sítích, máme na mysli především sítě standardu 802.11 a jeho dalších variant.

Obr. 2.1: Ochranná známka WiFi

2.2 Další vývoj standardu 802.11

Hned po vzniku standardu 802.11 bylo jasné, že v porovnání s klasickými sítěmi bude potřeba bezdrátové sítě zrychlit a rozšířit jejich funkce, protože např. již zmíněná rychlost 2Mb/s se ukázala jako nedostačující. S postupem doby byly tedy definovány následující standardy:

- 802.11a - byl schválen v roce 1999 a na rozdíl od IEEE 802.11 pracuje v pásmu 5GHz s výrazně vyšší přenosovou rychlostí - 54Mbit/s. Pro její dosažení se poprvé v paketových komunikacích používá ortogonální multiplex s kmitočtovým dělením (Orthogonal Frequency Division Multiplex, OFDM), který se dosud používal pouze v systémech jako DAB (Digital Audio Broadcasting) nebo DVB (Digital Video Broadcasting) určených pro distribuci digitálního zvuku a videa. Výhoda IEEE 802.11a oproti původnímu standardu není pouze ve vyšší rychlosti, ale také v použitém kmitočtu, protože kmitočtové pásmo 5GHz je méně vytížené než pásmo 2,4GHz a také dovoluje využití více kanálů bez vzájemného rušení (IEEE 802.11a nabízí až osm vzájemně nezávislých a nepřekrývajících se kanálů).
- 802.11b - tento doplněk vznikl v roce 1999 a poskytuje vyšší přenosové rychlosti v pásmu 2,4GHz, a to až 11Mbit/s. Pro jejich dosažení využívá

nový způsob kódování, tzv. doplňkové kódové klíčování (Complementary Code Keying, CCK) s použitím DSSS (Direct Sequence Spread Spectrum) na fyzické vrstvě. Doplněk specifikuje, že podle momentálního rušení prostředí se dynamicky mění rychlost: 11Mbit/s, 5,5Mbit/s, 2Mbit/s či 1Mbit/s.

- 802.11c - jde o standard definující procedury pro síťové mosty (bridge). Je využíván hlavně přístupovými body.
- 802.11d - upravuje IEEE 802.11b pro jiné kmitočty s cílem umožnit nasazení těchto sítí v místech, kde pásmo 2,4GHz není dostupné. Doplněk byl schválen v roce 2001.
- 802.11e - doplňuje podporu pro kvalitu služeb (Quality of Service, QoS) pro zajištění přenosu hovorového signálu, obrazu apod. Standard 802.11e doplňuje sítě definované IEEE 802.11a/b/g a nahrazuje stávající metody pro přístup k médiu: DCF (Distributed Coordination Function) a PCF (Point Coordination Function). Nově použité přístupové metody jsou: EDCF (Enhanced DCF) a HCF (Hybrid Coordination Function). Doplněk navíc zajišťuje zpětnou kompatibilitu se zařízeními, které nejsou podporou pro QoS vybaveny.
- 802.11f – přináší Inter Access Point Protocol (IAPP). Předchozí specifikace 802.11 nezahrnují standardizaci komunikace mezi jednotlivými access pointy (přístupovými body) pro zajištění roamingu (tzn. přechodu uživatele od jednoho access pointu k druhému).
- 802.11g - doplněk IEEE 802.11g je obdobou IEEE 802.11a s tím rozdílem, že je specifikován pro pásmo 2,4GHz, stejně jako IEEE 802.11b. Pro dosažení vyšší rychlosti, až do 54Mbit/s, se používá na fyzické vrstvě OFDM, a navíc se používá DSSS pro zpětnou kompatibilitu s IEEE 802.11b. Pro modulaci se používá podle hodnoty odstupu signálu od šumu QPSK, BPSK, 16-QAM či 64-QAM. Podporované rychlosti v závislosti na modulaci jsou následující:

54Mbit/s (64-QAM), 48, 36 a 24Mbit/s (16-QAM), 18 a 12Mbit/s (QPSK), 9 a 6Mbit/s (BPSK). Další rychlosti jsou stejné jako u 802.11b: 11Mbit/s (CCK), 5,5Mbit/s (CCK), 2Mbit/s (DQPSK) a 1Mbit/s (DBPSK). Doplněk byl schválen v roce 2003.

- 802.11h - změny v řízení přístupu k spektru 5GHz pásma tak, aby bylo možno tyto sítě využívat mimo budovy.
- 802.11i - doplňuje lepší zabezpečení sítí 802.11. Místo WEP (Wired Equivalent Privacy) používá nový způsob šifrování AES (Advanced Encryption Standard). Doplněk byl schválen v roce 2004.
- 802.11j – rozpracovaný standard týkající se alokací nových frekvenčních rozsahů pro multimediální služby bezdrátových sítí (hlavně v Japonsku).
- 802.11k – jedná se o pokračování předešlého standardu 802.11j.

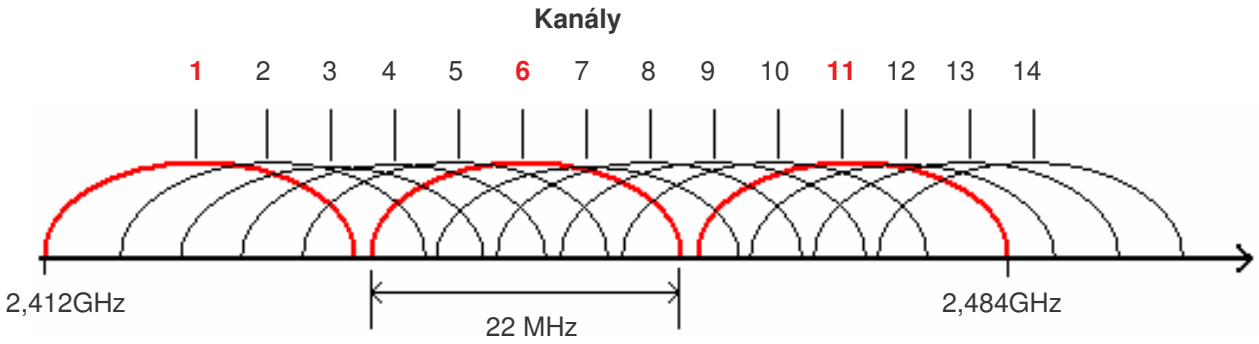
2.3 Frekvenční spektrum a Wi-Fi technologie

Ve Wi-Fi sítích se používají následující tři režimy přenosu dat v rozprostřeném spektru:

- DSSS (Direct Sequence Spread Spectrum) - každý jednotlivý bit určený k přenosu je nejprve nahrazen určitou početnější sekvencí bitů
- OFDM (Orthogonal Frequency Division Multiplexing) - signál je vysílán na více nezávislých frekvencích, což zvyšuje odolnost vůči interferenci
- FHSS (Frequency Hopping Spread Spectrum) - princip této metody spočívá v přeskakování mezi několika frekvencemi při přenosu bitu nebo bitů

2.3.1 DSSS – používaná standardem 802.11b

Technika přímo rozprostřeného spektra (Direct Sequence Spread Spektrum, DSSS) předpokládá, že každý jednotlivý bit, určený k přenosu, je nejprve nahrazen určitou sekvencí bitů, a skutečně přenášena (modulována na nosný signál) je pak až tato sekvence bitů. DSSS dělí pásmo (2,412GHz - 2,484GHz) na 14 kanálů viz Obr. 2.2. Šířka jednoho kanálu je 22Mhz, ale rozdíl mezi frekvencemi je pouze 5Mhz, tzn. že vedle sebe ležící kanály se překrývají. Pouze 3 se nepřekrývají vůbec (kanály 1, 6 a 11). Vysílač komunikuje s přijímačem na jednom předem zvoleném kanále (frekvenci). Pásmo 2,4Ghz však není ve všech zemích stejné, a tak je v různých zemích povoleno vyžívat pouze některé kanály (např. v ČR je možno využít kanály 1 - 13).



Obr. 2.2: Kanály při použití DSSS

Standard 802.11 pro přenosové rychlosti 1Mb/s a 2Mb/s počítá s tím, že každý bit je nahrazen 11-bitovou sekvencí bitů (tzv. Barterovým kódem), označovanou také jako tzv. chip. Jde o umělé zavedení redundance (nadbytečnosti), podobné tomu, které se při datových přenosech někdy používá pro zajištění větší spolehlivosti přenosů. Zde je ale důvod pro zavedení takovéto redundance jiný - signál je zde rozprostřen do větší části spektra, je méně citlivý vůči rušení (což opět zvyšuje spolehlivost přenosu), a ostatním uživatelům se jeví jako náhodný šum (k tomu je zapotřebí, aby příslušná sekvence bitů, neboli chip, byla volena alespoň

pseudonáhodně). Systém modulace je závislý na použité přenosové rychlosti. Technologie DSSS umožňuje přenosy rychlostmi 1/2/5,5 a 11Mb/s. Pro rychlost 1Mb/s je signál modulován na nosnou frekvenci pomocí BPSK (Binary Phase Shift Keying). Pro rychlost 2Mb/s se používá čtyřstavová fázová modulace QPSK (Quaternary Phase Shift Keying). Rychlosti 11Mb/s a 5,5Mb/s (definované v 802.11b) používají modulace CCK (Complimentary Code Keying) vyvinuté firmami Lucent Technologies a Harris Semiconductor. Kromě kódování CCK nabízí standard 802.11b alternativně kódování PBCC (Packet Binary Convolutional Coding), které poskytuje za cenu složitějšího dekodéru, poněkud lepší výsledky.

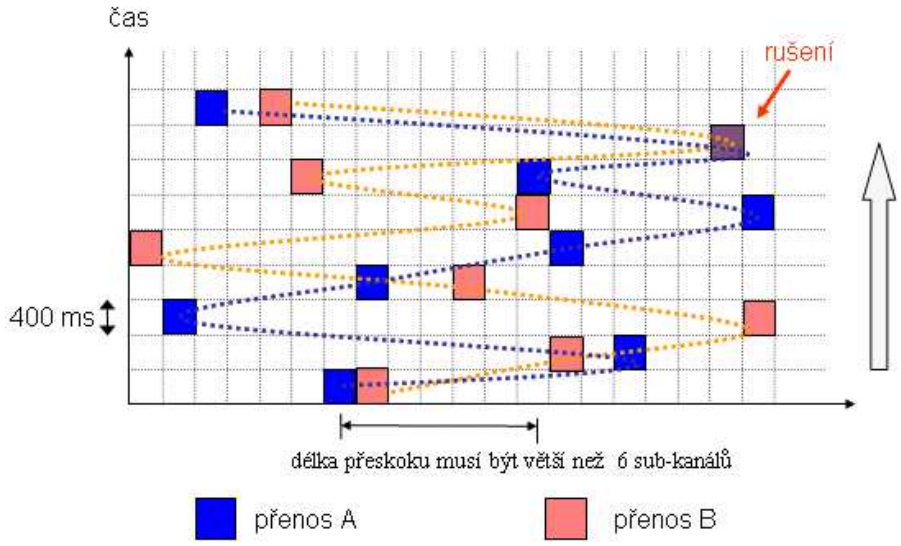
2.3.2 OFDM – používaná standardem 802.11g a 802.11a

Nový standard 802.11g přinesl technologii ortogonálního frekvenčního multiplexu (Orthogonal Frequency Division Multiplexing, OFDM) i do pásma 2,4GHz (původně jej vyžíval standard. 802.11a v pásmu 5GHz). Maximální rychlost byla zvýšena až na 54Mb/s. Princip je takový, že tu část frekvenčního spektra, kterou má tato technika k dispozici, rozděluje na menší části (sub-kanály), po kterých přenáší samostatné nosné signály (sub-nosné). Na každý takovýto (sub) nosný signál pak mohou být samostatně namodulována konkrétní data, čímž vzniká nezávislý přenosový kanál. Lze si tedy představit, že "celková" data, určená k přenosu, jsou průběžně rozkládána do jednotlivých dílčích přenosových kanálů, přičemž toto rozdělování může být adaptivní a sledovat to, jaké jsou v daném okamžiku přenosové schopnosti daného dílčího kanálu (jak se v něm projevuje eventuální rušení atd.) - momentálně nejméně zarušené dílčí kanály mohou být využívány intenzivněji (s vyšší přenosovou rychlostí) než ty dílčí kanály, které právě vykazují zhoršené přenosové vlastnosti. Základní přenosovou rychlostí 802.11g při kódování FEC (Forvard Error Correction) a při modulaci BPSK, je

6Mb/s. Použití alternativního kódování FEC s vyšší efektivitou při modulaci BPSK poskytuje 9Mb/s. Vyšších rychlostí dosahují režimy, opírající se o čtyřstavovou QPSK (12 a 18Mb/s), o šestnáctistavovou 16-QAM (24 a 36Mb/s) a o čtyřiašedesátistavovou 64-QAM (48 a 54Mb/s). Obdobná technika frekvenčního multiplexu je využívána např. u technologie ADSL. Ve všech případech umožňuje maximalizovat využití přenosových schopností daného média i v situaci, když část přenosového spektra má různé vlastnosti a tyto se v čase mění.

2.3.3 FHSS

Princip této techniky je takový, že nosný signál s namodulovanými daty je vysílán na určité frekvenci (resp. v úzkém frekvenčním pásmu, sub-kanálu, v případě 802.11 o šířce 1MHz) jen po velmi krátkou dobu (t<400ms), a poté "přeskočí" a pokračuje na jiné frekvenci podle předem známého schématu, viz. Obr. 2.3. Dostupné pásmo (zhruba 83,5Mhz) je rozděleno na 79 kanálů o šířce 1Mhz, zbylé pásmo slouží jako "ochranné" proti interferencím ze sousedních frekvenčních pásem. Přenosová rychlost je definována ve dvou úrovních, zaručená je 1Mb/s a při dobrých přenosových podmínkách je možné přejít na 2Mb/s. Výhodou je možnost existence více nerušících se sítí vedle sebe (prakticky až 15 na rozdíl od tří u DSSS). Nevýhodou je menší odolnost proti rušení a malá přenosová rychlost. Dnes se již prakticky nepoužívá.



Obr. 2.3: Ukázka FHSS přenosu

3 ZABEZPEČENÍ

Data se v bezdrátových sítích vysílají všesměrově, a tak není těžké je odposlechnout. Pokud se tedy najdou uživatelé, kteří šifrování vypnou, lze jednoduše získat jejich hesla k emailům, ftp serverům apod. Navíc při pasivním odposlechu je téměř nemožné vás odhalit.

Základní bezpečnostní mechanismy pro Wi-Fi sítě nejsou příliš dobré. Protože kryptografické zabezpečení WEP není standardem 802.11 přímo vyžadováno a v prvních zařízeních nebylo často vůbec implementováno, bylo hojně využíváno a stále je i filtrovaní počítačů podle MAC adres a skrývání SSID přístupového bodu. Žádný z těchto mechanismů bohužel nezajistí dostatečnou bezpečnost.

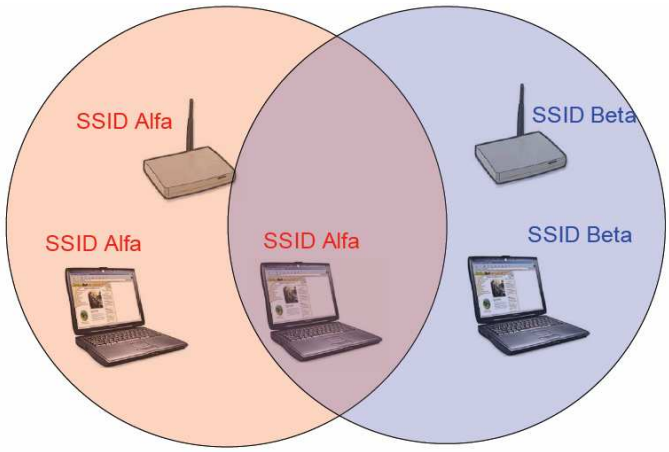
3.1 Základní bezpečnostní infrastruktura 802.11

- Oddělení logických bezdrátových sítí (Service Set Identifier) - SSID
- Autentizace přidružení zařízení k AP (Open Authentication, Shared Key Authentication)
- Šifrování komunikace (Wired Equivalent Privacy) - WEP
- Autorizace wireless karty (MAC Address Authentication)

3.1.1 Zablokování vysílání SSID

Zablokování vysílání SSID sice porušuje standard, ale je nejjednodušším zabezpečením bezdrátové sítě pomocí jejího zdánlivého skrytí. Klienti síť nezobrazí v seznamu dostupných bezdrátových sítí, protože nepřijímají broadcasty s SSID. Takové oddělení sítí je vidět na Obr. 3.4. Bohužel při připojování klienta k přípojnému bodu je SSID přenášen v otevřené podobě a lze

ho tak snadno zachytit. Při zachytávání SSID při asociaci klienta s přípojným bodem se používá i provokací, kdy útočník do bezdrátové sítě vysílá rámce, které přinutí klienty, aby se znovu asociovali.



Obr. 3.4: Oddělení sítí pomocí SSID

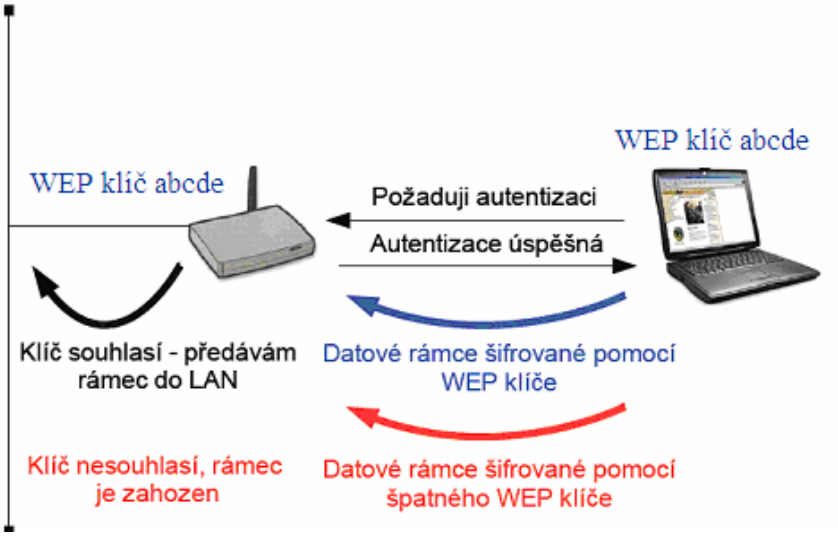
3.1.2 Autentizace

Standard 802.11 specifikuje dva možné způsoby autentizace (ověření „totožnosti“ uživatele) na linkové vrstvě:

- Open-system autentizace
- Shared key autentizace

3.1.2.1 Open-system autentizace

Tento typ autentizace, který je vidět na Obr. 3.5, je jako jediný vyžadovaný ve standardu 802.11 pro všechny zařízení. Bohužel však nepředstavuje téměř žádnou úroveň zabezpečení. Klient je totiž autentizován pouze na základě informací jím zaslaných, které nejsou ověřovány. To znamená, že Access Point vždy autentizuje každého klienta.

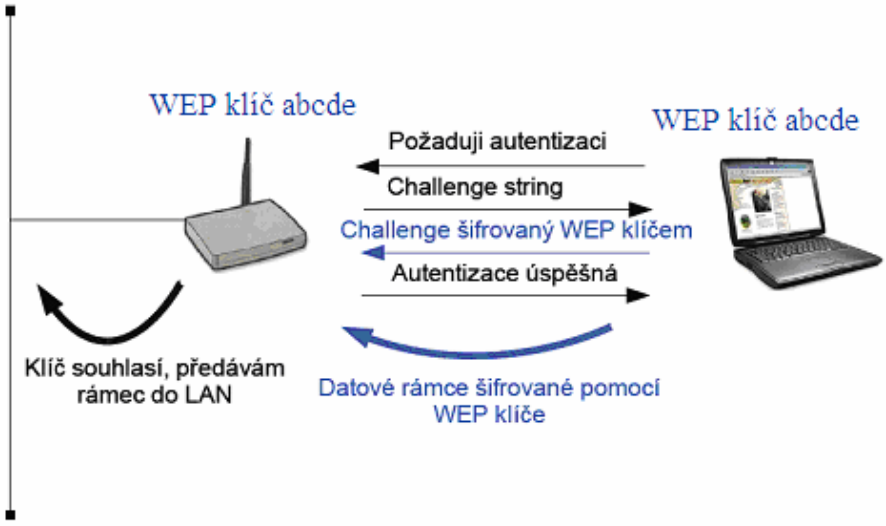


Obr. 3.5: Ukázka autentizace pomocí open-systém

3.1.2.2 Shared key autentizace

Autentizace pomocí sdíleného klíče, viz. Obr. 3.6, je ve standardu vyžadována pro všechna zařízení, která podporují WEP. Zatímco u open-system autentizace pouze klient odeslal žádost „Authentication request" a AP mu ihned odpověděl zprávou „Authentication succes", zde je proces poněkud komplikovanější. Klient, který se chce připojit k síti, nejprve vyšle žádost o autentizaci „Authentication request". Přístupový bod mu odpoví náhodně vygenerovaným textem „Authentication challenge", nebo též challenge text. Klient tento text zašifruje algoritmem RC4 (stejným způsobem jako při použití WEPu) a pošle jej zpět „authentication response". AP si tento text dešifruje a zkontroluje, zda souhlasí s vyslaným. Pokud ano, data od klienta jsou dále propouštěna do sítě a klient je informován o úspěšném přihlášení. Bohužel však tento typ autentizace přináší řadu bezpečnostních rizik. Tím, že posílá jeden text (náhodné číslo, challenge text) nejprve jako volný text, a nazpět již zašifrované, může tak útočník odposlouchávající přenos získat hodnotné informace – dvojici nezašifrovaného

a zašifrovaného textu, ze kterého již pak jednoduchým způsobem získá použitý klíč (díky slabinám algoritmu RC4).



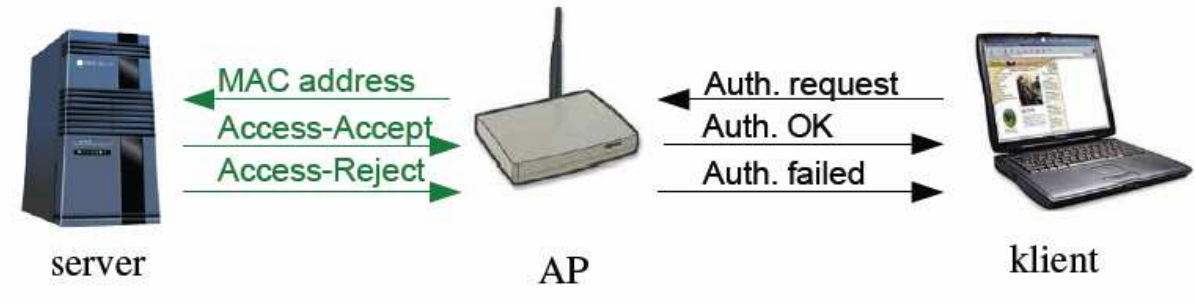
Obr. 3.6: Ukázka autentizace pomocí shared key

3.1.3 Filtrování pomocí MAC adres

Některé přístupové body umožňují omezit přístup do sítě podle MAC adres, jak je předvedeno na Obr. 3.7. MAC (Media Access Control) adresa je celosvětově jednoznačný identifikátor většiny síťového zařízení, který používá mnoho síťových protokolů druhé vrstvy. MAC adresa má délku 48bitů a nejčastěji se zapisuje jako šestice dvou hexadecimálních čísel, tedy ve tvaru xx:xx:xx:xx:xx:xx. První tři dvojice určují výrobce zařízení. MAC adresa příjemce a odesílatele je součástí každého ethernetového rámce. Ke zjištění MAC adresy cílového počítače z jeho IP adresy se používá protokol ARP.

Filtrování MAC adres přináší totiž několik problémů - mezi ty základní patří distribuce seznamu MAC adres a možnost falšovat MAC adresu. Každý přístupový bod si totiž musí udržovat vlastní databázi povolených MAC adres. Ve chvíli, kdy spravujeme několik přístupových bodů ke kterým se nepřipojuje více

jak několik desítek klientů, je toto možné dělat standardní cestou - a to přes webové konfigurační rozhraní AP (některé AP ani jinou možnost nepodporují), kde se přidávají/ubírají jednotlivé MAC adresy. V případě větší sítě by se však toto stalo noční můrou správce sítě. Některé AP tuto možnost řeší uploadem seznamu pomocí TFTP (Trivial FTP), avšak ten sám není nijak zabezpečený. MAC adresa bývá obvykle uložena v nějaké flash paměti zařízení. V dnešní době je tato paměť přepisovatelná, tzn. že se dá MAC adresa změnit. Útočník tak může zkusit nastavit náhodnou MAC adresu, a doufat že se „trefí" do povoleného rozsahu, nebo může odposlouchávat komunikaci na síti a odchytit si jednu z povolených MAC adres, kterou později použije.



Obr. 3.7: Ukázka autentizace pomocí filtrování MAC adres

3.1.4 WEP

Protokol WEP (Wired Equivalent Privacy) pracuje jako volitelný doplněk k 802.11 pro řízení přístupu k síti a zabezpečení přenášených dat. WEP funguje na symetrickém principu, kdy se pro šifrování a dešifrování používá stejný algoritmus i totožný statický klíč. Klíč je stejný pro všechny uživatele dané sítě (sdílený klíč) a klienti jej využívají spolu se svou adresou MAC pro autentizaci vůči přístupovému bodu. Ve skutečnosti se tedy ověřuje totožnost síťové karty, nikoli samotného uživatele. Autentizace ve WEP pracuje pouze jednostranně, nikoli vzájemně. Šifrování přenášených dat se provádí 64-bitovým klíčem, který je

složen z uživatelského klíče a dynamicky se měnícího inicializačního vektoru IV (Initialization Vector) o délce 24 bitů. IV se posílá v otevřené formě a mění se s každým paketem, takže výsledná šifra je jedinečná pro každý jednotlivý paket. WEP používá šifrovací algoritmus RC4. Existuje i silnější zabezpečení ve formě 128-bitového šifrováni (sdílený klíč má délku 104 bitů, inicializační vektor poté 24 bitů).

Hlavní problémy WEPu spočívají především ve statických klíčích (nijak neřeší automatickou distribuci nových klíčů, a tak si ho v případě změny musí každý uživatel sám ručně znovu nastavit), a ve slabém inicializačním vektoru (posílá se "vzduchem" nezakódovaný a ještě se jeho kombinace poměrně "brzy" vyčerpají - jedná se "pouze" o 2^{24} možností). Bezpečnost sítě s WEP je možno narušit snadno odposlechem. K získání WEP klíče stačí odchytat pouze několik set tisíc paketů a pomoci volně dostupných nástrojů (Airsnort, WEPcrack ,Kismet) je to již otázka několika málo minut, než útočník získá klíč.

3.2 Skutečné zabezpečení bezdrátových sítí Wi-Fi

- Autentizace pomocí standardu 802.1x a dynamické (per-session) WEP klíče
- WPA:
- Per Packet Keying
- Message Integrity Check (MIC)
- Broadcast key rotation
- Standard 802.11i

3.2.1 802.1x a dynamické WEP klíče

802.1x (Port-Based Network Access Control, 2001) je obecný bezpečnostní rámec pro všechny typy LAN, zahrnující autentizaci uživatelů, integritu zpráv (šifrováním) a distribuci klíčů. Standard 802.1x má za cíl blokovat přístup k segmentu lokální sítě pro neoprávněné uživatele. Je založený na protokolu EAP (Extensible Authentication Protocol, RFC 2284). Ověřování provádí přístupový bod na základě výzvy klienta pomocí externího autentizačního systému (např. Kerberos, nebo RADIUS - Remote Authentication Dial-In User Service).

Obecný postup autentizace podle 802.1x:

1) přístupový server k síti (Network Access Server - NAS), tj. switch nebo bezdrátový přístupový bod, vyšle klientovi na základě detekce jeho přítomnosti zprávu „Eap requestid".

2) Klient odpoví zprávou „Eap response-id", která obsahuje identifikační údaje uživatele. Přístupový server zapouzdří celou zprávu „Eap response-id" do paketu „Radius access request" a vyšle ji serveru RADIUS.

3) Server RADIUS odpoví zprávou obsahujícím povolení/zákaz přístupu pro daného klienta do sítě „Radius access accept/deny", která v sobě obsahuje informaci „Eap success/failure", jíž přístupový server přepošle klientovi.

4) v případě povolení „Success" je příslušný port přístupu do sítě (přes nějž autentizační komunikace probíhala) otevřen pro data daného uživatele, který je na základě úspěšného výše popsaného procesu považován za autentizovaného. 802.1x používá k šifrování dat v další komunikaci pro každou autentizovanou stanici dynamické klíče. Tyto klíče jsou známy pouze dané stanici, mají omezenou životnost a využívají se k šifrování rámců na daném portu, dokud se stanice

neodhlásí nebo neodpojí. Dynamické klíče 802.1x omezují možnosti útočníků. Už se ovšem prokázalo, že ani 802.1x není dostatečně odolný vůči některým typům útoků (session hacking , man-in-the-middle attack).

3.2.2 WPA

WPA (Wi-Fi Protected Access) vytvořila Wi-Fi Aliance, jež vlastní práva na značku Wi-Fi a certifikuje zařízení, která ji nesou. WPA je navrženo pro použití s autentizačním serverem IEEE 802.1x, který distribuuje jednotlivým uživatelům rozdílné klíče. Lze jej však použít i v režimu s „předsdíleným heslem“ (pre-shared key, PSK), kdy všichni uživatelé používají stejné přístupové heslo. WPA vychází ze 3. pracovního návrhu IEEE 802.11i.

Wi-Fi Aliance vytvořila WPA s cílem umožnit zavedení bezpečných produktů pro bezdrátové sítě vycházejících ze standardů ještě před dokončením prací na IEEE 802.11i. Data jsou zašifrována pomocí proudové šifrovací metody RC4 se 128bitovým klíčem a 48bitovým inicializačním vektorem (IV). Zásadní vylepšení oproti WEP zabezpečení spočívá v použití TKIP (Temporal Key Integrity Protocol), což je protokol dynamicky měnící klíče pomocí těchto mechanismů:

- PPK (per-packet key hashing) - umožňuje změnu klíče pro každý paket. Tím je odstraněna slabina standardní definice WEP, jež pracuje se statickým klíčem, který se během spojení nemění.
- MIC (Message Integrity Check) - jedná se o „digitální podpis“ nesený v každém paketu. Je to 32bitová hodnota stanovená z náhodné hodnoty, záhlaví rámce, datového obsahu a sekvenčního čísla. Tímto je odstraněna možnost útoku nazývaného "man-in-the-middle", tedy takového útoku, kdy útočník zachytává pakety od vysílajícího, modifikuje je a posílá příjemci.

- Rotace broadcastových klíčů (Broadcast key rotation) - PPK zajišťuje změnu klíčů pro unicastovou komunikaci. Protože je 802.11 založen (jako všechny 802.x sítě) na broadcastovém mechanismu, je nutné zajistit změnu i klíčů používaných pro broadcasty a multicasty.

3.2.3 Standard 802.11i

Autentizaci a zabezpečení v sítích Wi-Fi komplexně řeší až nový standard 802.11i. Problém autentizace je vyřešen zakomponováním standardu 802.1x. Zabezpečení dat se děje pomocí protokolu TKIP (Tempoval Integrity Protocol). Ten vylepšuje WEP o dynamickou změnu klíčů kontrolu integrity přenášených zpráv (MIC – Message Integrity Check). K protokolu TKIP, který může pracovat s minimálními požadavky na softwarový upgrade na stávajících zařízeních s hardwarem pro WEP, se přidal nový protokol CCMP (Counter-mode-CBC-MAC Protocol)(CBC - Cipher Block Chaining, MAC - Message Authentication Code), zaručující silnější šifrování díky využití AES (Advanced Encryption Standard) právě v režimu CCM (kombinuje režim CTR, Counter Mode, pro utajení a CBCMAC pro autentizaci a integritu). K vlastnímu šifrování se používá algoritmus AES (Advanced Encryption Standard). Velikost šifrovacího klíče AES může být zvolena jako 128,192 nebo 256 bitů, a samozřejmě platí, že čím delší klíč, tím více poskytuje bezpečnosti ale zároveň potřebuje tím vyšší výpočetní výkon. V protokolu TKIP nahradí AES starý a nevyhovující algoritmus RC-4. Zatímco dříve stačilo útočníkovi odposlechnout dostatečný objem zpráv, aby mohl zlomit klíč WEP, a jedinou obranou bylo manuálně klíče včas změnit, než k tomu dojde, s 802.11i se mění šifrovací klíče automaticky.

4 QOS VE WI-FI

Obrovskou nevýhodou Wi-Fi sítí je fakt, že nemají v základním standardu 802.11 žádnou podporu upřednostňování služeb a řízení propustnosti pro určené protokoly. Ačkoliv to nejdříve nevypadalo na důležité opomenutí, spolu s tím, jak se Wi-Fi technologie stala nejenom psaným, ale i faktickým standardem pro bezdrátové připojení, vyvstala otázka priorizace určitého provozu v síti a to hlavně v souvislosti s multimédii. Ve Wi-Fi najednou začala citelně chybět obdoba služby QoS, Quality of Service, jak ji známe z jiných typů sítí.

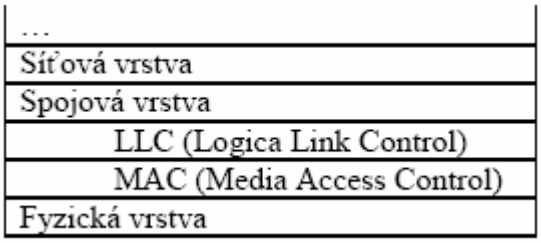
4.1 Základní problém

Základním problémem každého přístupového bodu je skutečnost, že se snaží rozdělovat přenosové pásmo, které má k dispozici, podle svého vlastního algoritmu, neexistuje žádné ustanovení, jak se má přístupový bod v případě zatížení více klienty chovat. Obvyklé chování je z pohledu uživatele poměrně chaotické. Přístupový bod přidělí prvnímu klientu veškeré své zdroje a pokud se připojují další klienti, snaží se vyhovět i jim. Fakt, že dopředu nejsme schopni říci, podle jakého principu se bude přístupový bod klienty snažit obsloužit, způsobuje nepříjemnosti pro aplikace, které jsou na co nejvyrovnanější charakteristiku datového přenosu háklivé – především tedy pro multimediální aplikace, jako je streamované video, hudba nebo internetová telefonie. Výsledkem je v zatížené Wi-Fi síti nerovnoměrný datový přenos, což má za následek přerušování přehrávaného videa nebo hudby, případně výpadky v telefonním hovoru prováděném z Wi-Fi telefonů. A bohužel tento problém je reálný už v sítích o dvou a více uživatelích Wi-Fi připojení. Pro koncové uživatele to znamená špatnou zkušenost s produktem, pro výrobce zase nemožnost prodávat něco,

s čím by zákazníci byli spokojeni. Poptávka po multimediálních produktech využívajících Wi-Fi je ale značná a bylo třeba usilovně hledat řešení.

4.2 Standard 802.11e

IEEE 802.11e byl odsouhlasen ke konci roku 2005 jako standard definující množinu rozšíření pro zajištění kvality služeb (Quality of Service, QoS) pro síťové komunikace na bázi bezdrátového spojení. Existence takového standardu je nesmírně důležitá pro aplikace citlivé na zpoždění dodání nebo ztráty požadovaných dat. Standard 802.11e rozšiřuje možnosti MAC (Media Access Control) vrstvy v původní definici standardu 802.11. Jak je vidět na Obr. 4.8, MAC je nižší podvrstva spojové vrstvy v modelu ISO OSI, která přímo sousedí s fyzickou vrstvou a poskytuje služby a funkce specifické pro dané přenosové médium.



Obr. 4.8: Model ISO OSI

4.3 Řízení přístupu k médiu

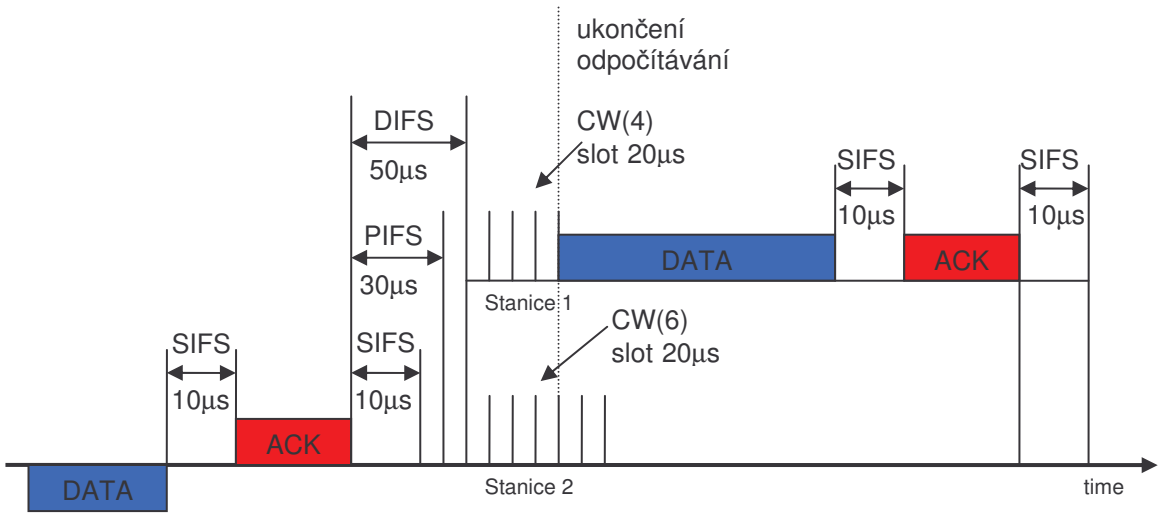
Bezdrátové sítě standardu 802.11 využívají náhodnou přístupovou metodu vícenásobného přístupu s detekcí nosné (Collision Detection Multiple Access, CDMA). U technologie Wi-Fi se přístupová metoda označuje jako koordinační

funkce. Pro standardy 802.11a/b/g jsou určeny dva typy základních koordinačních funkcí - distribuované a centralizované:

- Distribuovaná koordinační funkce (Distributed Coordination Function, DCF)
- Centralizovaná koordinační funkce (Point Coordiantion Fuction, PCF)

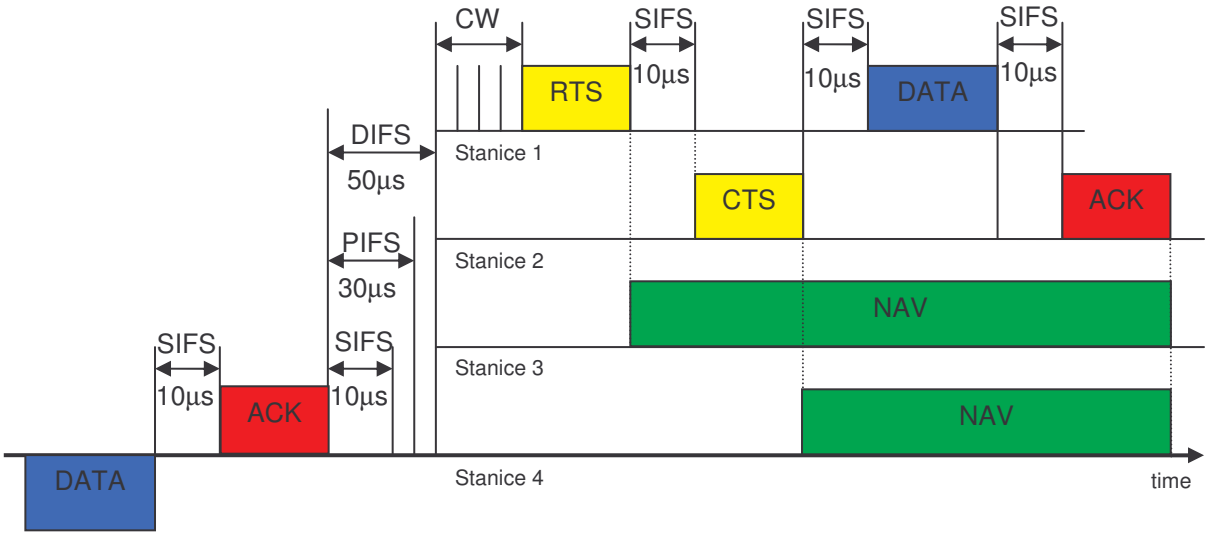
4.3.1 Distribuovaná koordinační funkce (DCF)

Jedná se o základní přístupovou metodu, kterou implementují všechny stanice. V režimu DCF stanice hlídá stav přenosového média. Je-li po uplynutí definovaného časového úseku DIFS (Distributed Interframe Space) médium volné, vyšle stanice paket. V opačném případě odloží přenos a nadále monitoruje médium. V okamžiku kdy dojde k uvolnění média, stanice vyčká po dobu definovanou jako DIFS + Trandom, kde Trandom je náhodný časový interval(probíhá tzv. soutěžení – Conection Windows, CW), jak je vidět na Obr. 4.9. Po uplynutí této doby se opět snaží vyslat paket. Detekce volného média se provádí měřením signálu na anténě (je definována prahová hodnota, od které je médium považováno za volné). Detekce kolizí v případech, kdy dvě stanice začnou vysílat současně, se řeší potvrzováním pomocí ACK (resp. výpadkem potvrzení) přijetí dat a příslušná stanice se tak okamžitě dozví o chybě v přenosu. Pokud totiž odesílatel po odeslání paketu neobdrží po definovaném intervalu SIFS (Short Interframe Space) potvrzení o přijetí ACK, vyhodnotí tento stav jako kolizi. Aby stanice nemusela čekat zbytečně dlouho na potvrzení, rámec ACK je zařazen mezi rámce, které mají nejvyšší prioritu. Znamená to, že uzel, který chce poslat rámec ACK, musí čekat nejkratší čekací interval SIFS a pak může zahájit vysílání.



Obr. 4.9: Přenos pomocí DCF pro standard 802.11g

V případech, kdy se vysílající stanice navzájem „nevidí“ (vidí pouze na přístupový bod - AP), musí AP řešit mnohem více kolizí, protože okolní stanice si myslí, že jsou v prostoru samy. Proto umožňuje většina stanic zapnout mód RTS/CTS (Request To Send / Clear To Send), ve kterém stanice zahajuje vysílání požadavkem (paket RTS) a pokud je médium volné, dostává stanice potvrzení od AP (paket CTS), že může po stanovenou dobu vysílat. Ostatní stanice v okolí si na základě intervalu uvedeného v paketu CTS upraví tzv. alokační vektor (NAV, Network Allocation Vector), což je interval, ve kterém se stanice nesnaží o přístup k médiu. Využití RTS/CTS má ale velmi negativní dopad na celkovou propustnost systému (propustnost může klesnout až na 20 % deklarované kapacity). Princip metody DCF (s použitím módu RTS/CTS) ukazuje Obr. 4.10.



Obr. 4.10: Princip metody DCF pomocí rámců RTS/CTS pro 802.11g

Z pohledu poskytování služeb QoS je metoda DCF nevýhodná zejména z následujících důvodů:

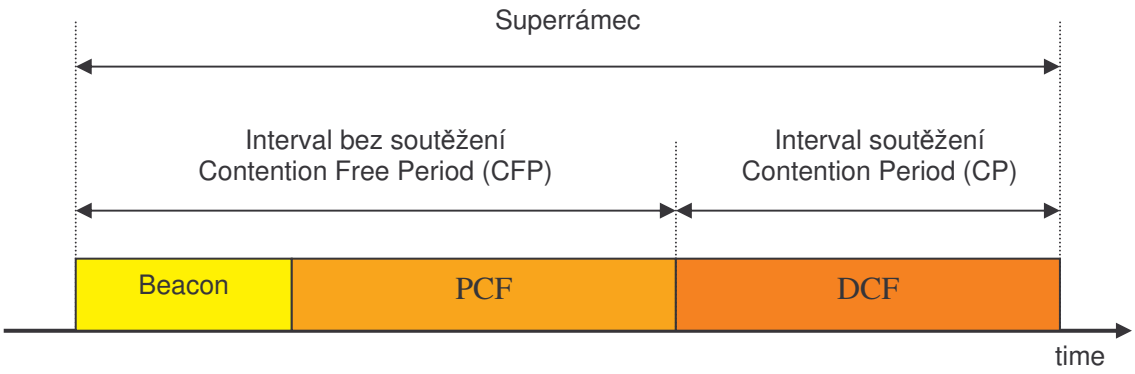
- U většího počtu stanic prudce stoupá pravděpodobnost kolizí a jejich řešením klesá celková přenosová šířka pásma
- Neexistuje žádný systém nastavení priorit přenosů

4.3.2 Centralizovaná koordinační funkce (PCF)

Jedná se o funkci, kterou norma 802.11 definuje jako dodatečnou a mezi stávajícími zařízeními není moc podporována. Využití nachází v případech, kdy jsou stanice připojovány do sítě skrz přístupový bod (AP). AP v tomto režimu funguje jako arbitr (rozhodčí) a centrálně přiděluje přenosové médium registrovaným žadatelům.

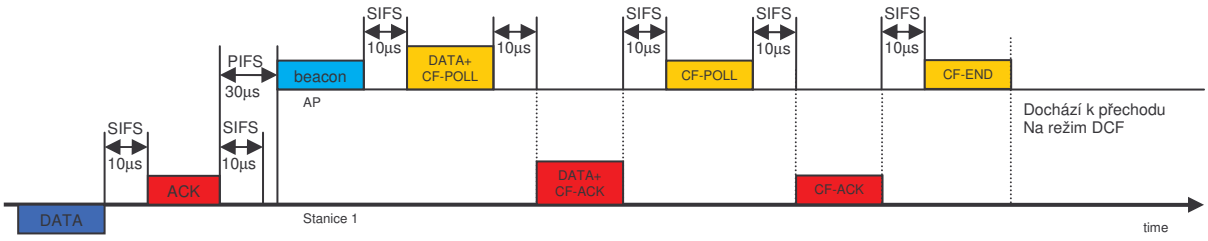
V režimu PCF je přenos dat synchronizován pomocí super-rámců (Super Frame nebo též Contetion Free Repetition Interval). Tento rámec (Obr. 4.11) je rozdělen na dva menší intervaly:

- Contention Free Period (CFP) – interval kdy nedochází k soupeření o přístup k médiu. Přístup určuje arbitr (AP).
- Contention Period (CP) – v tomto intervalu je pro přístup k přenosovému médiu využita klasická DCF metoda



Obr. 4.11: Superrámec

Časový průběh komunikace založené na PCF je vidět na Obr. 4.12. Před zahájením intervalu bez soutěžení přístupový bod místo čekací doby DIFS čeká pouze PIFS, tj. může získat přístup ke sdílenému médiu dříve, než stanice čekající na odeslání datového rámce. Interval CFP je pak zahájen vysíláním rámce beacon. Během CFP přístupový bod dotazuje zaregistrovanou stanici 1 pomocí rámce CF-POLL. Na obrázku je také vidět, že přístupový bod už má data pro stanici 1, která mu je odešle v kombinovaném rámci Data + CF-POLL. Dotázaná stanice zašle přístupovému bodu data spolu s potvrzením v kombinovaném rámci Data + CF-ACK. V následujícím kroku už přístupový bod nemá data k zaslání, takže pošle pouze dotaz v rámci CF-POLL. Ani dotázaná stanice nemá data k odeslání a proto pouze potvrdí dotaz rámcem CF-ACK. Přístupový bod tak může ukončit interval bez soutěžní, což provede vysláním rámce CF-END. Po ukončení CFP je zahájen interval CP, během kterého jednotlivé stanice soutěží o přístup využitím mechanismu DCF.



Obr. 4.12: Časový průběh komunikace založené využívající PCF pro 802.11g

Jak je vidět, mechanismus PCF není příliš propracovaný. Není schopný prioritně rozlišit různé datové toky či třídy provozu. Časování je dále výrazně ovlivněno délkou přenášených datových rámců a proto může přenos dlouhého rámce zablokovat přenos pro další stanice. Navíc, trvání přenosu rámců v následujícím režimu DCF je také nepředvídatelné, což způsobí, že rámce beacon nejsou generovány ve zcela pravidelných intervalech. To vše může mít nepříznivý vliv na kvalitu služeb vyžadující striktní časování. Navíc, podle standardu IEEE implementace PFC je pouze volitelná a proto většina síťových prvků tuto funkci ani nenabízí.

4.4 Mezirámcové mezery

Jedná se o název pro čekací doby, které jsou povinné před zahájením pokusu o vyslání každého nového rámce. Délka této čekací doby ovlivňuje to, s jakou pravděpodobností získá stanice přístup médiu. Čekací doba může tedy zajistit prioritní řízení přístupu. Koordinační funkce DCF a PCF používají tři typy mezirámcových mezer:

- Krátká mezirámcová mezera - SIFS (Short Interframe Space)
- Mezirámcová mezera centralizované koordinační funkce - PIFS (Point Coordination Function Interframe Space)

- Mezirámcová mezera distribuované koordinační funkce - DIFS (Distributed Coordination Function Interframe Space)

Konkrétní velikosti mezirámcových mezer a čekacího intervalu slot time jsou uvedeny v Tab. 4.1.

Technologie	SIFS	PIFS	DIFS	slot time	CW_{min}	CW_{max}
802.11a	16μs	25μs	34μs	9μs	15	1023
802.11b	10μs	30μs	50μs	20μs	31	1023
802.11g	10μs	30μs	50μs	20μs	15	1023

Tab. 4.1: Velikosti mezirámcových mezer

4.5 Rozšíření MAC podle 802.11e

Standard 802.11e rozšiřuje původní metody DCF a PCF a zavádí tak dvě nové přístupové metody (koordinační funkce):

- rozšířená distribuovaná koordinační funkce EDCF - (Enhanced Distributed Coordination Function)
- hybridní koordinační funkce HCF - (Hybrid Coordination Function)

U obou nových metod standard 802.11e definuje třídy provozu (Traffic classes). Lze tak rozlišovat možnost zatížení přenosového kanálu na základě typu použití (typu aplikace). Např. emailová služba může mít přiřazenu nižší třídu priority než třeba VoWIP (Voice over Wireless IP), u kterého požadujeme minimální výpadky a zpoždění, tudíž bude mít přiřazenu prioritu vyšší. Tyto mechanismy byly navíc navrženy tak, aby přístupový bod nebo bezdrátová stanice s podporou 802.11e mohly spolupracovat i se staršími komponenty, které tyto pokročilé mechanismy nemají. Standard 802.11e definuje další sadu služeb označenou jako základní sada služeb s podporou kvality služeb (QoS supporting BSS, QBSS). QBSS se skládá z tzv. hybridního koordinátoru (Hybrid Coordinator, HC), kterým je většinou

přístupový bod s podporou 802.11e. Stanice podporující mechanismy 802.11e jsou označovány jako QSTA podle anglického názvu „QoS station“.

Tento nový standard je nadstavbou (rozšířením) základního mechanismu řízení přístupu pomocí DCF a PCF a tyto mechanismy jsou i v tomto standardu zachovány. Nedochází ani ke změně významu intervalů bez soutěžení CFP a se soutěžením CP. Nové koordinační funkce pracují nadále v těchto intervalech a to tak, že EDCF může pracovat pouze během CP. Funkce HCF pracuje v obou režimech, přičemž během CP pro svou funkci využívá metodu EDCF. Na základě těchto nových koordinačních funkcí byl definován rozšířený distribuovaný přístup ke kanálu (Ehanced Distributed Channel Access, EDCA) a přístup ke kanálu řízený pomocí HCF (HCF Controlled Channel Access, HCCA).

4.6 Rozšířený distribuovaný přístup ke kanálu EDCA

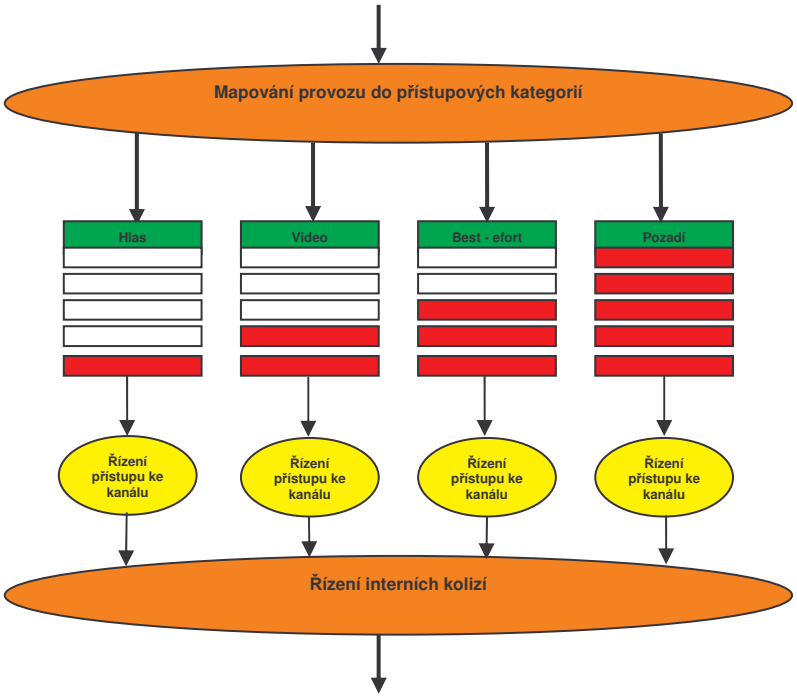
Podpora QoS u EDCA je zajištěna na základě kategorií přístupu (Access Category, AC). Každá stanice může mít až 4 kategorie přístupu a provoz může rozdělit až do osmy prioritních úrovní. Prioritní úrovně pak budou odpovídat kategoriím přístupu, přičemž jedné kategorii může odpovídat i více prioritních úrovní. Prioritní úrovně používané ve standardu 802.11e jsou identické s prioritami definovanými ve standardu IEEE 802.1D, což zajišťuje vhodnou spolupráci s mechanismy řízení přístupu v pevných lokáních sítích. Osm prioritních úrovní dle 802.1D a jejich předpokládané využití je uvedeno v Tab. 4.2. Z tabulky je zřejmé, že v současnosti nejčastější způsob přenosu, tj. „best-effort“, s úrovní priority 0 má vyšší prioritu, než prioritní úrovně 1 a 2. Přenos „excellent-effort“ představuje provoz s charakterem „best-effort“ ale pouze od specifické skupiny důležitých uživatelů, resp. stanic. Tak např. je možné zvýhodnit běžný provoz generovaný vedoucími organizace. Řízená zátěž odpovídá provozu, který splňuje

určitá, předem stanovená, kritéria. Tab. 4.2 dále obsahuje čtyři definované kategorie přístupu značeny jako AC_BK (přenos v pozadí), AC_BE (přenos typy best-effort), AC_VI (přenos videa) a AC_VO (přenos hlasu). Z tabulky je jasná i provázanost kategorií přístupu a prioritních úrovní. Je také vidět, že předpokládané využití dostupných prioritních úrovní v sítích WLAN se mírně liší od využití předpokládaného v pevných sítích.

	Prioritní úroveň dle 802.1D	Předpokládané využití (dle 802.1D)	Kategorie přístupu	Předpokládané využití dle 802.11e
Nejnižší	1	přenos na pozadí	AC_BK (0)	přenos na pozadí
	2	nedefinované	AC_BK (0)	přenos na pozadí
	0	best-effort (výchozí)	AC_BE (1)	best-effort
	3	excellent-effort	AC_BE (1)	best-effort
	4	řízená zátěž	AC_VI (2)	video
	5	video(zpoždění do 100ms)	AC_VI (2)	video
	6	hlas(zpoždění do 10ms)	AC_VO (3)	hlas
Nejvyšší	7	správa sítě	AC_VO (3)	hlas

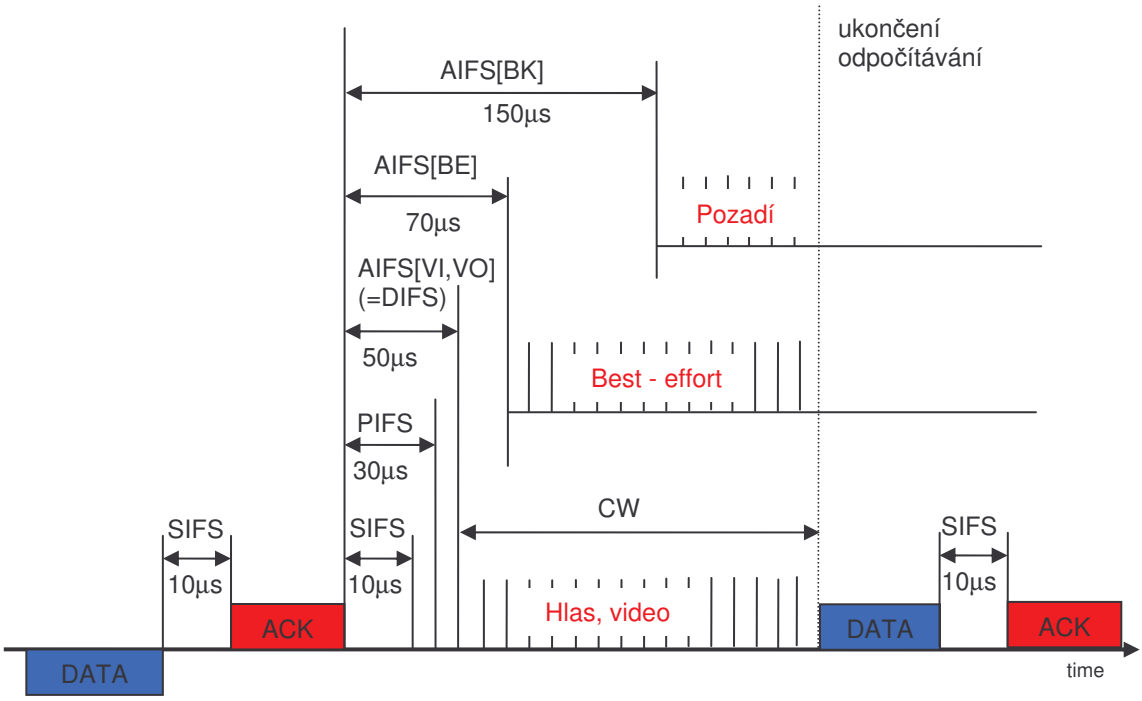
Tab. 4.2: Přehled kategorií a prioritních úrovní přístupu v QoS

Každá stanice může mít až čtyři kategorie provozu na podporu osmi úrovní priority jak ukazuje Obr. 4.13. Tab. 4.3 naznačuje mapování priorit na kategorie přístupu, odpovídající jedné ze čtyř vysílacích front, které jsou odbavovány právě podle své priority.



Obr. 4.13: Referenční realizace mechanismu EDCA

Rámce z jednotlivých kategorií přístupu soutěží o tzv. příležitost přenosu (Transmission Oportunity, TXOP). Jedná se o časový interval ve kterém bude možné přenést rámec, jehož trvání je předem časově omezeno, což eliminuje synchronizační problémy způsobené neznámou délkou rámce. Informaci o maximální povolené délce EDCA-TXOP získají stanice z rámce „beacon“ vysílaného přístupovým bodem daného QBSS. Pro kategorie přístupu AC_VI a AC_VO je stanovená doba, po kterou mohou využívat médium, tzn. přenášet rámce s tím, že přenos musí být ukončen vč. potvrzení do uvedené délky TXOP. Nulová maximální délka TXOP označuje, že daná kategorie přístupu může v rámci získaného TXOP odeslat pouze jeden rámec viz Tab. 4.4. Vysílací stanice, 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 (Arbitration Interframe Space, AIFS).



Obr. 4.14: Soutěžení o přístup v rámci mechanismu EDCA pro 802.11g

Pro každou kategorii musí samozřejmě platit, že AIFS[AC] ≥ DIFS. Kromě mezirámcové mezery pro každou kategorii přístupu je možné nastavit samostatné hodnoty pro parametry CW_{min}[AC], CW_{max}[AC] a AIFS[AC]. Pro nastavení velikosti okna soutěžení CW platí logická podmínka, že pro přístupovou kategorii s vyšší prioritou je třeba nastavit kratší okno soutěžení, aby pravděpodobnost získání přístupu byla větší. CW brání kolizím paketů stejné kategorie. Zdvojnásobuje svou délku po každé nastalé kolizi a po úspěšném přenosu se zase vrací na minimální hodnotu. Přístup k médiu se tak stává řízeně neférový - provoz s vyšší prioritou je upřednostněn na úkor provozu s prioritou nižší.

Kategorie	AIFSN	CW (Contention Window)		Min. doba čekání	Max. doba čekání
		CW_{min}	CW_{max}		
hlas (7,6)	2	$(CW_{min}+1)/4-1$	$(CW_{min}+1)/2-1$	2 - 5	9
		3	7		
video (5,4)	2	$(CW_{min}+1)/2-1$	CW_{min}	2 - 9	17
		7	15		
best effort (0,3)	3	CW_{min}	CW_{max}	3 - 18	1026
		15	1023		
pozadí (2,1)	7	CW_{min}	CW_{max}	7 - 22	1030
		15	1023		

Tab. 4.3: Doba čekání na vysílání (v time slotech) u jednotlivých kategorií, zde ukázka využití v 802.11g

Parametr AIFSN udává délku AIFS vzhledem k mezirámcové mezeře SIFS v čekacích intervalech slot time. Např. hodnota AIFSN = 2 označuje, že AIFS = SIFS + 2 * slot time, viz Tab. 4.1.

Kategorie přístupu	802.11 (DSSS), 802.11b (HR/DSSS)	802.11b (HR/DSSS), 802.11g (OFDM)
hlas (7,6)	3,264ms	1,504ms
video (5,4)	6,016ms	3,008ms
best effort (0,3)	0	0
pozadí (2,1)	0	0

Tab. 4.4: Maximální délka intervalu TXOP

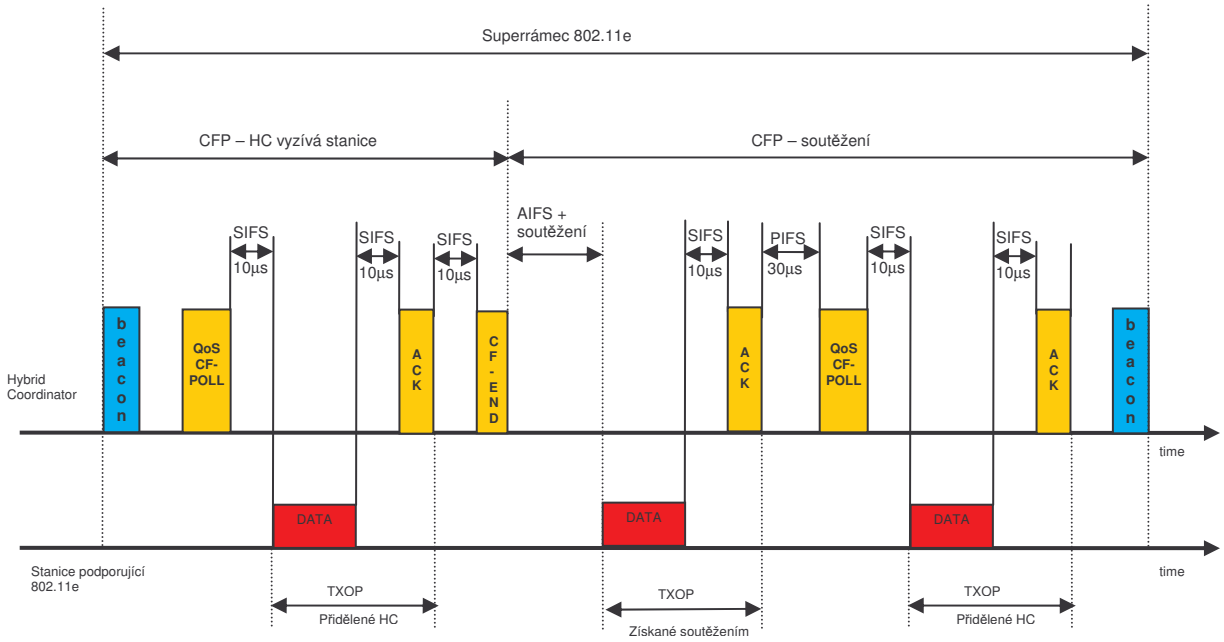
4.7 Přístup ke kanálu řízený pomocí HCCA

802.11e nabízí volitelně také centralizovaný protokol HCF (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 (HCF Controlled Channel Access). Podobně jako u původní funkce PCF řídí i v rámci HCCA přístup ke kanálu přístupový bod, který plní funkci hybridního koordinátoru (Hybrid Coordinator, HC) pomocí výzev jednotlivým

stanicím. Hlavní funkcí HC je přidělování příležitostí přenosu TXOP kategoriím přístupu v bezdrátových stanicích QSTA a v přístupovém bodě QAP. QoS se bere v potaz při plánování vysílacích dob, kdy některý provoz dostává k dispozici větší část kanálu. HCCA s dobře nastavenými parametry QoS může zajistit efektivnější využití přenosového kanálu zejména u WLAN primárně používaných pro přenos hlasu či videa, protože eliminuje „ztrátové“ doby čekání.

Oproti EDCA, kde je přístup k médiu řízen na základě prioritních úrovní, HCCA může zaručit absolutní garanci doby přenosu či zpoždění. Je to řešeno vyšší prioritou HCCA a možností pracovat jak během intervalu bez soutěžení CFP, ta i během intervalu soutěžení CP. Ke správné funkci mechanismu HCCA už nestačí jednoduchá registrace stanic u koordinátora. Stanice musí konkrétně specifikovat svoje požadavky na síťové prostředky, které jsou pak vyhodnoceny HC a schváleny příp. odmítnuty, pokud HC požadavky nemůže zaručit. Na základě takto sjednaných parametrů pak HC přiděluje stanicím TXOP o dostačující délce a počtu. Přidělení TXOP kategorii přístupu v konkrétní stanici je zajištěno zasláním rámce QoS CF - POLL. Tento rámec je vygenerován vždy na začátku intervalu bez soutěžení CFP a podle potřeby HC může tento rámec generovat i během intervalu soutěžení. HC pomocí rámce QoS CF - POLL může vyzvat současně i více stanic (kategorií přístupu) k odeslání svých dat s tím, že pro každou kategorii specifikuje, kdy má zahájit vysílání. Na základě informací z rámce QoS CF - POLL si ostatní stanice nastaví vektor alokace sítě NAV, který udává jak dlouho musí čekat na uvolnění média. Interval CFP musí být ukončen rámcem CF - END. Jak už bylo uvedeno, HCF může pracovat i během intervalu soutěžení. Tehdy, po ukončení přenosu a uplynutí PIFS HC může získat přístup k médiu. Zasláním rámce QoS CF - POLL pak vyzve příslušné kategorie přístupu k odeslání svých dat. Rámec QoS CF - POLL obsahuje TXOP, která uvnitř CP vymezuje interval, kdy mohou vyzvané kategorie přenést svoje data bez soutěžení. V standardu 802.11e je tento interval označen jako interval s řízeným

přístupem (Controlled Access Phase - CAP). Středně dlouhá mezirámcová mezera PIFS zajišťuje, že rámec QoS CF - POLL bude vyslán dříve, než by některá ze soutěžících stanic mohla zahájit přenos. Trvání CAP je dáno délkou TXOP uvedené v rámci QoS CF - POLL. Příklad časového průběhu popsaných mechanismů je uveden na Obr. 4.15.



Obr. 4.15: Superrámec podle standardu 802.11e

5 PRAKTICKÁ IMPLEMENTACE 802.11E

5.1 Opnet Modeler

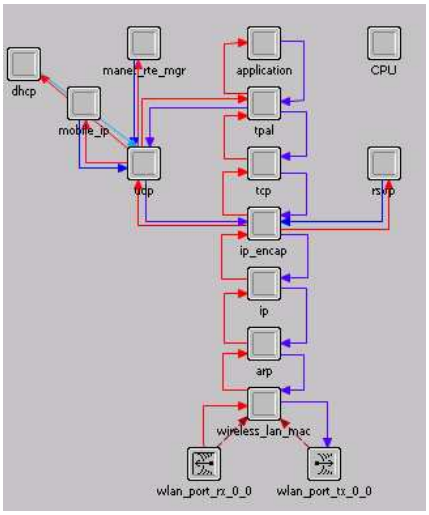
Jedná se o jeden z nejpoužívanějších simulačních programů, který je určen pro návrh a studování komunikačních sítí, zařízení, protokolů a aplikací. Tímto programem lze simulovat nejrůznější sítě, které se tvoří použitím rozsáhlé knihovny komponent (stanice, servery, propojovací prvky atd.), až po možnosti naprogramovat vlastní síťové protokoly, formáty přenášených dat i způsob jejich zpracování. Opnet Modeler (OM) je produktem firmy OPNET Technologies z USA a poprvé se na trhu objevil v roce 1987. Je to efektivní a velmi výkonný nástroj, jeden měsíc reálného provozu sítě lze nasimulovat za několik hodin (rychlost simulace závisí na výkonu PC). V současné době je na trhu již ve verzi 14.5. Tento nástroj je používán vedoucími firmami v oblasti vývoje síťových technologií.

Hlavní předností OM je široká možnost tvorby nejrůznějších charakteristik z dané simulace, jeho efektivnost a výkonnost, což ho předurčuje všude tam, kde je třeba ověřit chování prvku sítě v různých extrémních podmínkách (např. chování routeru při vysoké zátěži apod.) nehledě na to, že v praxi není možné vždy sledovat všechny vlastnosti sítě, které nás zajímají. OM je hierarchicky a objektově orientován, grafické prostředí ukazuje reálné rozložení jednotlivých síťových komponent. Výsledky statistik je možné vygenerovat a získaná data uložit do tabulek.

5.2 Struktura programu

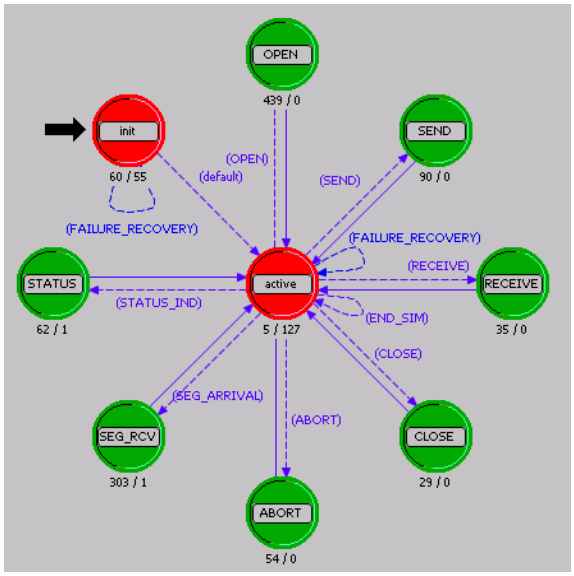
Opnet Modeler obsahuje velké množství editorů sloužících pro vytvoření modelů sítí a k nastavení jejich nejrůznějších vlastností. Pro návrh sítě se nejčastěji používají tři základní editory, mezi které patří:

- Project Editor (editor projektu) - jedná se o základní grafické prostředí programu. Zde se zobrazuje aktuální topologie sítě vytvořeného projektu, viz Obr. 5.18. Jsou zde také zobrazeny jednotlivé uzly sítě a způsoby komunikace mezi nimy. Pro vytvoření sítě se využívají jednotlivé objekty prvků sítě v nabídce Object Palette přetažením prvku z nabídky do pracovního prostoru. Předdefinované síťové prvky jsou uloženy v knihovnách OM a jsou tématicky rozděleny do určitých skupin jako např. Internet, WLAN, Ethernet, ATM a další.
- Node Editor (editor uzlu) – tento editor představuje rozhraní nižší úrovně než Projekt Editor. Je zde zobrazena architektura síťového zařízení nebo systému a jeho vzájemné vztahy mezi funkčními modely a volanými funkcemi.



Obr. 5.16: Node Editor pro Wireless work station

- Process Editor (editor procesu) – jedná se o rozhraní nejnižší úrovně. Definuje jednotlivé procesy uzlu v jazyce C/C++. Je zde tedy možnost zadání a změny jednotlivých proměnných a statistik.



Obr. 5.17: Process Editor pro TCP u Wireless work station

5.3 Kvalita přenosu hlasu u VoIP

Pro přenos hovoru v počítačových sítích je dnes nejrozšířenější technologie VoIP (Voice over IP). Její základy byly vytvořeny v polovině devadesátých let a nejznámějšími komunikačními protokoly jsou H.323, SIP (Session Initiation Protocol) a MGCP (Media Gateway kontrol Protocol).

Kvalitu hovoru můžeme rozdělit do tří základních kategorií:

- Kvalita poslechu hodnocená uživatelem, která je závislá především na použitém kódování.
- Kvalita konverzace, kde se posuzuje schopnost vést rozhovor. Zde se uplatňují vlivy jako je echo a zpoždění.
- Kvalita přenosu, která je vztažena ke schopnosti sítě přenášet hlas.

V IP sítích je hlas přenášen v paketech RTP (Real Time Protocol). Tento protokol je založen na datagramové službě (nespojově orientovaná a nespolehlivý přenos), což ovšem neznamená, že hovor uskutečněný přes IP síť nemůže být kvalitní. Absolutní stanovení kvality hlasové služby není uskutečnitelné, jelikož každý jedinec vnímá kvalitu jinak. VoIP přináší z hlediska kvality hovoru používání různých metod kódování, které mají odlišnou hodnotu parametru MOS (Mean Opinion Score). MOS je stanoven subjektivní metodou hodnocení a může dosáhnout maximálně hodnoty 5. V Tab 5.5 jsou uvedeny používané standardy kódování, názvy algoritmů, náročnosti na zpracování vyjádřené parametrem MIPS (Million Instructions Per Second, počet miliónů instrukcí za sekundu), přenosové rychlosti kodeků a jejich kvalita ohodnocená parametrem MOS dle ACR (Absolute Category Rating). Nejpoužívanějším kodekem je jednoznačně pulsní kódová modulace PCM dle standardu ITU-T G.711. Druhým nejrozšířenějším kodekem je ITU-T G.729 s kódově buzenou lineární predikcí CS - ACELP (Conjugate Structure Algebraic Code Excited Linear Prediction), který má obdobný MOS jako G.711, menší přenosovou rychlost a vyšší nároky na procesorový výkon. Kódování a dekódování je většinou zajišťováno na signálových procesorech DSP (Digital Signal Processing).

Standard	Algoritmus	MIPS	Přenosová rychlost [kb/s]	MOS [ACR]
G.711	PCM	0	64	4,1
G.726	ADPCM	1	32	3,85
G.728	LD-CELP	30	16	3,61
GSM	RPE-LTP	10	13	3,5
G.729	CS-ACELP	20	8	3,92
G.723.1	MP-MLQ	16	6,3	3,9
G.723.1	ACELP	20	5,3	3,65

Tab. 5.5: Kodeky používané pro hlas

Z přehledu v tabulce to vypadá, že G.729 bude oproti G.711 osmkrát úspornější na šířku pásma v IP sítích. Pro vytvoření paketů a započtení jejich hlaviček si G.729 nárokuje v síti Ethernet zhruba 35 kb/s a G.711 až 90 kb/s. U kodeku G.729 se musí počítat se zpožděním 10 ms pro každý rámec a dalších 5 ms tvoří dopředné zpoždění. A protože se většinou do jednoho RTP paketu vkládají dva rámce, tak musíme počítat se zpožděním 25 ms při kódování. Před dekódováním jsou přicházející pakety shromažďovány v mezipaměti, kde se vyrovnává proměnné zpoždění vznikající při přenosu IP sítí, toto zpoždění se označuje jako jitter, velikost mezipaměti je v násobcích časových velikostí přijímaných rámců.

Vliv na kvalitu hovoru a zpoždění mezi odesílatelem a příjemcem je popsán v doporučení ITU-T G.114. Toto zpoždění by se mělo pohybovat do 150 ms, pokud překročí 300 ms, tak degradace kvality hovoru roste exponenciálně s narůstajícím zpožděním. Na kvalitu hovoru může mít zásadní vliv jitter, kterému se dá zabránit použitím nástrojů QoS, označováním hlasových paketů, jejich upřednostňováním ve frontách a fragmentací dlouhých paketů nebo rezervací zdrojů s využitím rezervačního protokolu. Zdroje musí být rezervovány na celé trase, aby byla garantována maximální doba doručení, tím pádem se jedná o rezervaci pásma. Při rychlostech nad 1 Mb/s se jitter u VoIP téměř neuplatňuje a je tedy možné, že širokopásmová připojení tento problém zcela odstraní.

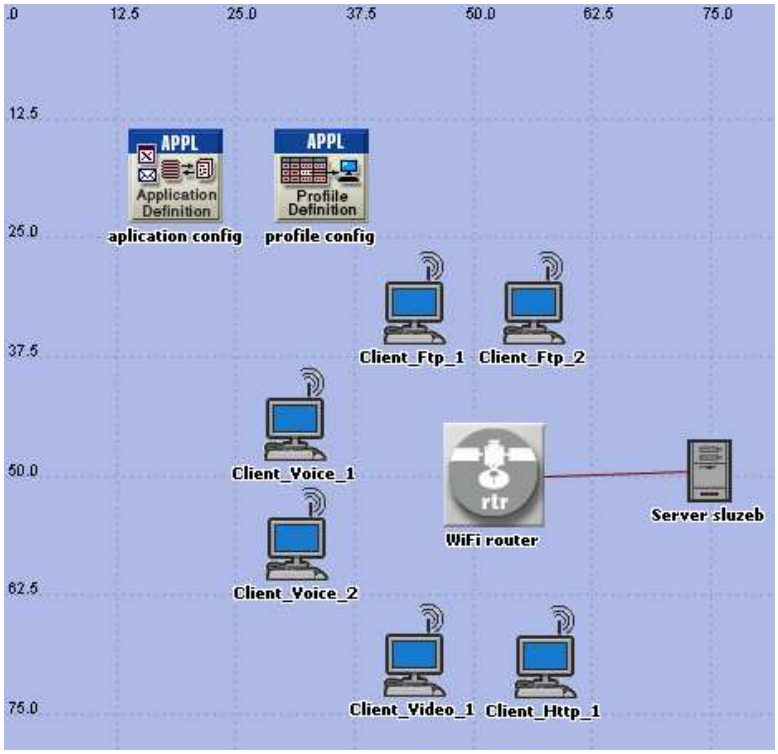
S použitím VoIP je potřebné věnovat pozornost i ztrátovosti paketů, jelikož ztrátovost má u kodeků s predikčními metodami přímo destruktivní účinek na kvalitu hovoru. Ztráty okolo 3% u G.729 pocítí uživatel snížením hodnoty MOS o 0,5 a dostává se na úroveň kvality GSM kodeku používaného v mobilních sítích. V případě, že se jedná o ojedinělé ztráty, tak se může kvalita udržet použitím algoritmu maskování ztracených paketů PLC (Packet Loss Concealment), v případě shluku po sobě se vyskytujících ztrát efektivita algoritmu PLC klesá.

Kvalita hlasu	Dobrá	Vyhovující	Nevyhovující
Zpoždění	0-150ms	150-300ms	nad 300ms
Jitter	0-20ms	20-50ms	nad 50ms
Ztrátovost	0-0.5%	0.5-1.5%	nad 1.5%

Tab. 5.6: Kvalita hovoru v závislosti na parametrech sítě

5.4 Vlastnosti modelované sítě

V Opnet Modeler jsem vytvořil dvě topologicky identické sítě pomocí funkce SCENARIO, viz Obr. 5.18. Obě navržené sítě obsahují server služeb, WLAN router a klientské Wi-Fi stanice. Server služeb je z WLAN routerem spojen přes rozhranní ethernet standardu 100BaseT. Klientské stanice komunikují s routerem pomocí standardu 802.11b s maximální rychlostí 11Mb/s.



Obr. 5.18: Navržená modelovaná síť

Sítě jsou vytvořeny ve scénáři OFFICE, tzn. na maximální ploše 100x100m. Scénář obsahuje mimo síťové komponenty, které tvoří vlastní síť, ještě dva prvky:

- Application Config – zde jsem nadefinoval aplikace a jejich konfigurace, které jsou využívány v síťovém modelu na jednotlivých stanicích nebo serveru:

  1) Ftp
  2) Http
  3) Voice
  4) Video

- Profile Config – zde jsem nastavil profily k příslušným aplikacím (čas startu, využití jednotlivých služeb atd.)

U sítě s podporou QoS jsem dále v rámci přístupové metody EDCA (Ehanced Distributed Channel Access) u jednotlivých aplikací nadefinoval třídy provozu a rozdělil je do prioritních úrovní:

- Http - Background– AC_BG(0) - prioritní úroveň 1
- Ftp - Best Effort – AC_BE(1) - prioritní úroveň 0
- Video – Video – AC_VI(2) - prioritní úroveň 4 (Streaming Mul.)
- Voice - Voice – AC_VO(3) - prioritní úroveň 6 (Interactive Voice)

Ve scénáři se sítí s podporou QoS jsem dále na všech klientských stanicích a WLAN routeru zapnul v jejich konfiguraci podporu QoS, tzn. mechanismus EDCA a jejich hodnoty jsem nechal nastaveny podle výchozího nastavení standardu 802.11e. Tyto hodnoty čekacích intervalů a oken soutěžení jsou uvedeny v teoretické části, viz Tab. 4.3.

Ve scénáři se sítí bez podpory QoS je podpora EDCA vypnuta a komunikace mezi klientskou stanicí a WLAN routerem probíhá pomocí základního přístupového mechanismu DCF viz Tab. 4.1. To znamená, že se datový tok nerozděluje do tříd provozu a proto nemohou být jednotlivé stanice mezi sebou upřednostňovány.

Síťové služby (aplikace), které využívají jednotlivé stanice jsem zvolil záměrně z důvodu, že jsou nejčastěji využívané jak v domácím tak i v pracovním prostředí jako jsou kanceláře a firemní sítě.

5.5 Výsledky simulace

Obě nadefinované sítě, jejichž nastavení a struktura je popsána v předcházející kapitole jsem simuloval v délce 10 minut reálného provozu a vygenerované hodnoty jsem zpracoval do grafů.

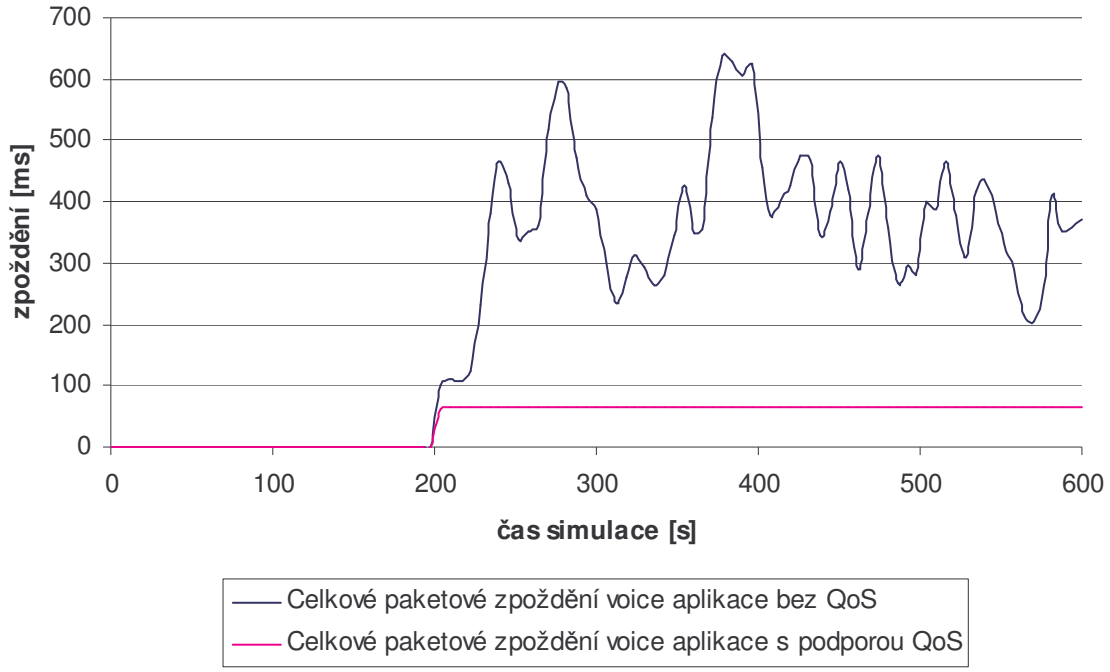
Protože QoS v bezdrátových sítích zajišťuje především správnou funkci multimediálních služeb, zaměřil jsem se na statistiky provozu, ve kterých budou jasné důkazy o správné funkci 802.11e. Mezi charakteristiky, které jsem sledoval, patří packet delay variation (zpoždění přenosu paketů v síti), end to end delay (celkové zpoždění paketů včetně dalších úprav signálu), throughput (prostupnost sítě) a data dropped (zahazování paketů díky přetečení paměti).

5.5.1 Celkové paketové zpoždění

Toto celkové zpoždění v sobě zahrnuje zpoždění paketů určité aplikace a zpoždění díky přenosu přes síť. Například u hlasu dochází ke kompresi a dekompresi, dále k šifrování a zabezpečení přenášené informace atd. Tyto hodnoty jsem naměřil u stanice Client_Voice_1. Téměř shodné hodnoty jsem naměřil i na druhé stanici využívající službu voice.

Jak je vidět z Obr. 5.19, zpoždění paketů u voice aplikace je v síti bez podpory QoS v rozmezí 250 – 650 ms a toto zpoždění je velice kolísavé, což by mělo za následek výpadky hovoru a tyto hodnoty jsou již pro VoIP nevyhovující. V síti s podporou QoS je zpoždění konstantí a to cca 80 ms. Podle Tab. 5.6 je kvalita hovoru dobrá do

zpoždění 150 ms, to tedy znamená, že využitím QoS jsme dosáhli požadované kvality služby.

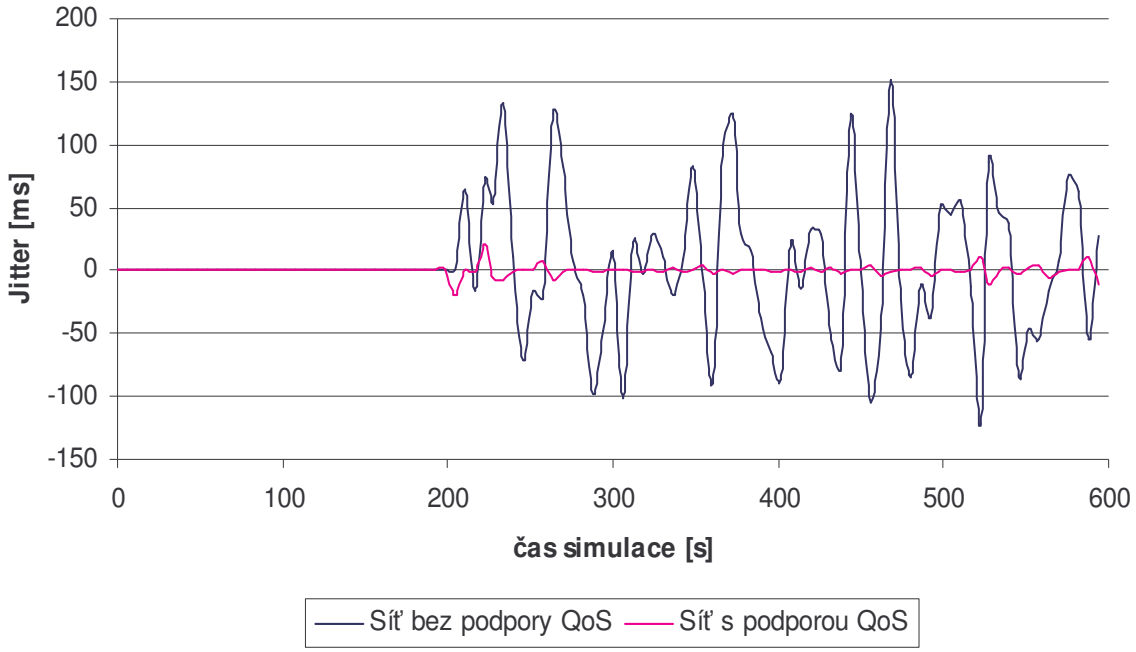


Obr. 5.19: Celkové paketové zpoždění v síti pro voice aplikaci

5.5.2 Jitter v bezdrátové síti

Jitter, neboli kolísání zpoždění v síti jsem měřil opět na klientské stanici Client_Voice_1. Podobných hodnot bylo opět dosahováno i na druhé stanici využívající voice aplikaci.

Z následujícího obrázku je opět jasně vidět rozdíl mezi oběma typy sítí. V síti bez podpory QoS se kolísání zpoždění pohybuje v rozmezí 30 – 130 ms, což by opět znamenalo nevyhovující podmínky pro přenos hlasu. Naopak výborných hodnot bylo dosaženo v síti s podporou QoS, kde jsem naměřil hodnoty v rozmezí 0 – 18 ms. Takovéto hodnoty kolísání zpoždění již nebrání kvalitnímu přenosu hlasu po IP síti.

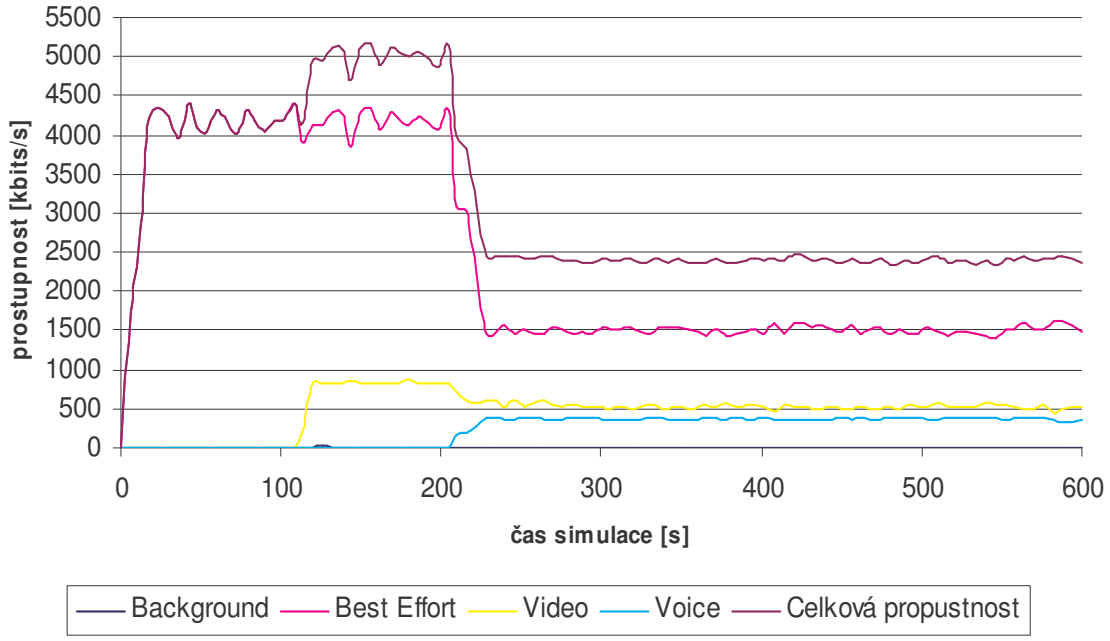


Obr. 5.20: Jitter v síti pro voice aplikaci

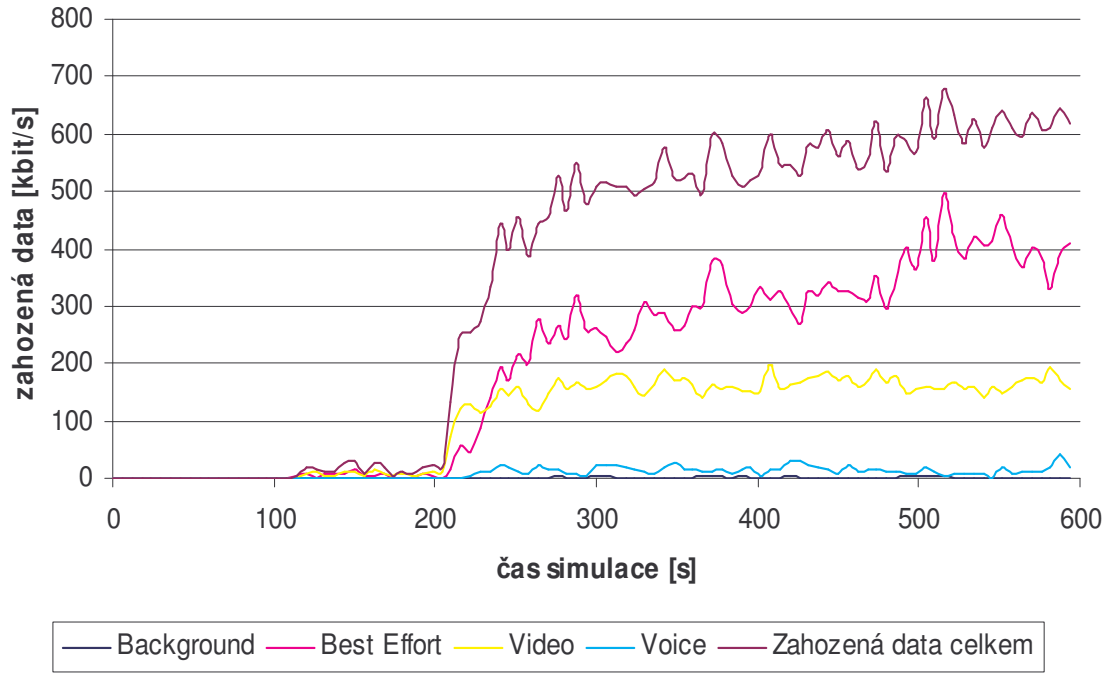
5.5.3 Prostupnost bezdrátové sítě

Jak je vidět z následujících dvou obrázků, síť byla velice zatížena. V Profile config jsem pro jednotlivé aplikace nastavil různé časy jejich startu z toho důvodu, abych mohl sledovat co se dělo s prostupností sítě, když nabíhaly další přenosy. Přenos typu Best-effort pro Ftp začíná již v počátku simulace, dále se k němu v čase 100 s přidává přenos kategorie Video a nakonec v čase 200 s se spouští aplikace kategorie Voice. Z obrázků je vidět, že prostupnost sítě byla v čase od 0 s do 100 s rychlostí cca 4500 kb/s. Tato vysoká propustnost sítě je způsobená tím, že WLAN router obsluhoval pouze 2 stanice s Ftp přenosem. V čase 100 s začíná o přenos dat soutěžit další stanice s daty kategorie Video. Zde je již vidět, že začíná docházet k mírnému zahazování paketů WLAN routeru, ale propustnost nadále mírně vzroste na hodnotu 5000 kb/s. V čase 200 s se přidávají další stanice s daty kategorie Voice, které mají nejvyšší prioritu a tím i největší šanci přenášet svá data. Zde je velmi dobře vidět náhlé poklesnutí celkové propustnosti sítě.

Dochází zde k tomu, že data od stanic s aplikací Voice jsou upřednostněna před ostatními a stanice tak může bez problémů vysílat svá data, zatímco ostatní stanice zatím soutěží o další přístup k médiu. Dále je na Obr. 5.22 dobře viditelný nárůst zahozených paketů, který je největší u kategorie Best-effort.



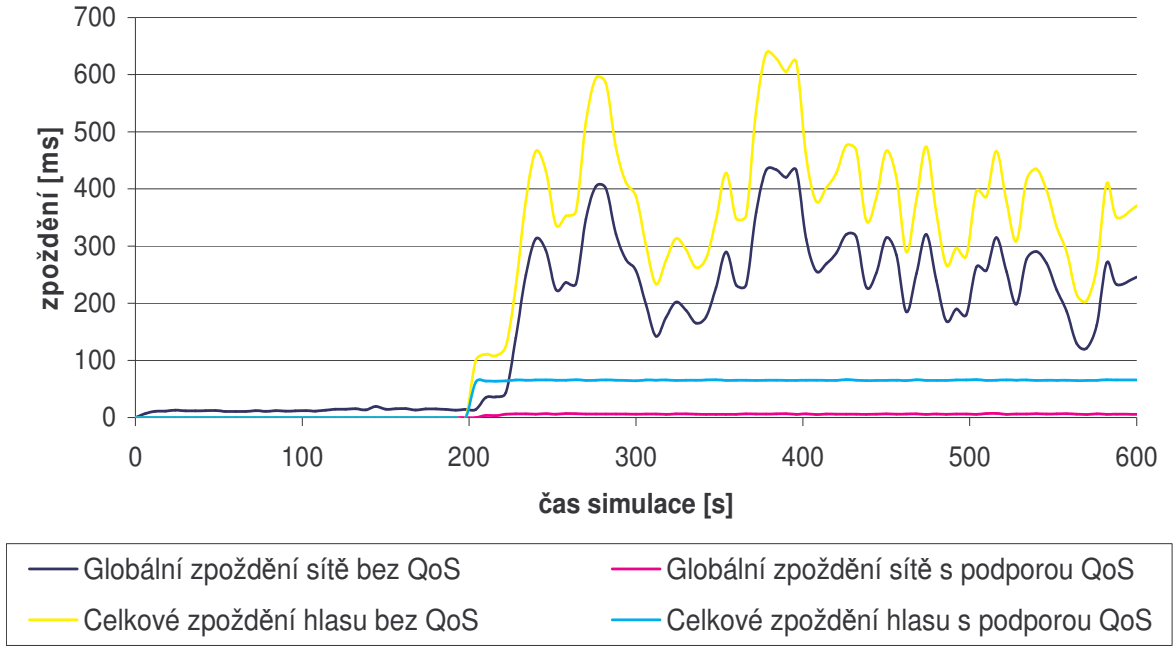
Obr. 5.21: Prostupnost sítě s podporou QoS podle tříd provozu



Obr. 5.22: Zahozená data způsobená přetečením paměti podle tříd

5.5.4 Porovnání globálního a celkového zpoždění

Při porovnání těchto dvou charakteristik je vidět, že celkové paketové zpoždění aplikace je větší než globální zpoždění sítě.



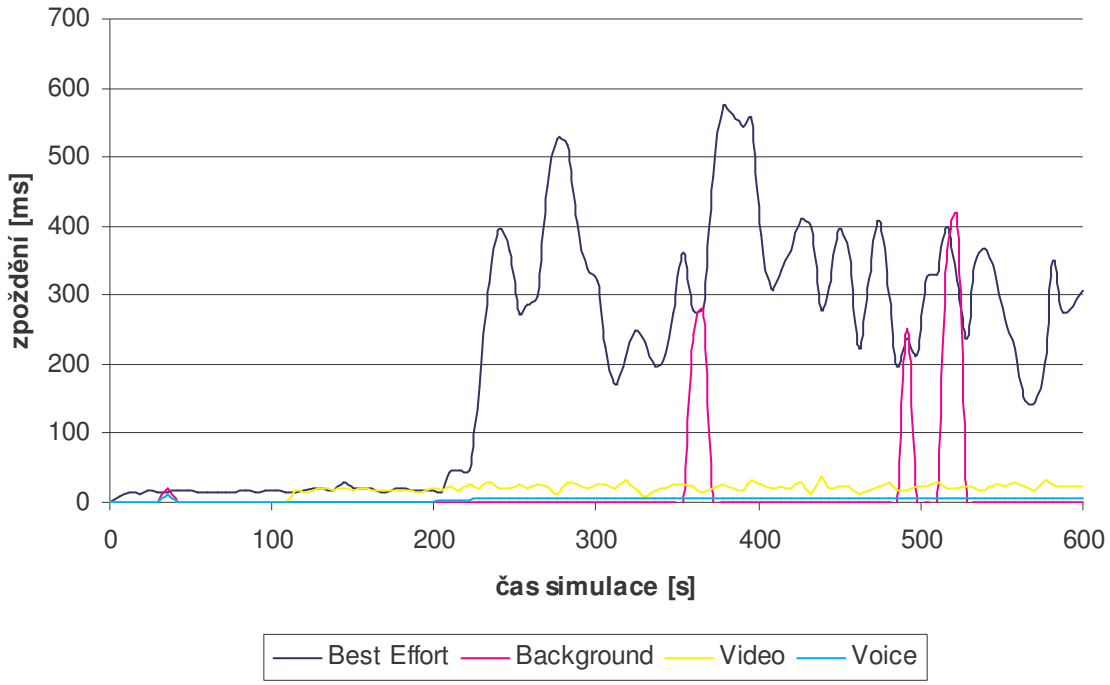
Obr. 5.23: Globální zpoždění sítě a celkové paketové zpoždění voice aplikace

Celkové paketové zpoždění hlasu je, jak již bylo uvedeno výše, způsobeno nejen zpožděním přenosu v síti, ale dalšími úpravami dat. Mezi ně patří komprese a dekomprese, dále šifrování a zabezpečení přenášené informace atd.

Z obrázku je také patrné, že celkové paketové zpoždění hlasu v síti s podporou Qos má konstantní zpoždění, což je pro přenos hlasu velice důležité. Přenos paketů hlasu v síti bez podpory QoS je značně kolísavý a proto nevyhovující.

5.5.5 Porovnání zpoždění kategorií v síti s QoS

Z Obr. 5.24 je patrné, že k velkému kolísání zpoždění dochází pouze u kategorií provozu Best-effort a Background. Hodnoty zpoždění se pohybují v rozmezí 200 - 600 ms. U kategorie Video došlo k velice nepatrnému zvýšení zpoždění a u třídy provozu Voice k navýšení zpoždění nedošlo vůbec.



Obr. 5.24: Zpoždění datového toku v síti s podporou QoS podle tříd provozu

Co se týče kolísání zpoždění paketů u kategorie provozu Video s prioritou 4, je vidět, že k mírnému kolísání dochází. Toto kolísání je v rozmezí 20 – 50 ms. Kdybychom chtěli porovnat celkové paketové zpoždění kategorie Video s globálním zpoždění sítě, došli bychom k velice podobnému grafu, jako je Obr. 5.23 s voice klientem.

U kategorie provozu Voice s prioritou 6 je kolísání zpoždění minimální a to v rozsahu 5 – 15 ms.

5.6 Kooperace starších zařízení s novými

Právě s příchodem nových zařízení, které v sobě mají implementován mechanismus pro podporu QoS (tzn. např. EDCA) vyvstává otázka, zda budou tyto stanice, které jsou označovány jako QSTA (QoS stations), spolupracovat se staršími, již používanými stanicemi.

Pro simulaci této situace jsem použil stávající síť s podporou QoS a u klientské stanice Client_Voice_1 jsem zrušil podporu EDCA a ponechal výchozí nastavení přístupové metody pomocí DCF. Tímto způsobem jsem vlastně vytvořil síť, kde mezi sebou komunikují dva voice klienti, přičemž jeden má zapnutou podporu QoS a druhý ne.

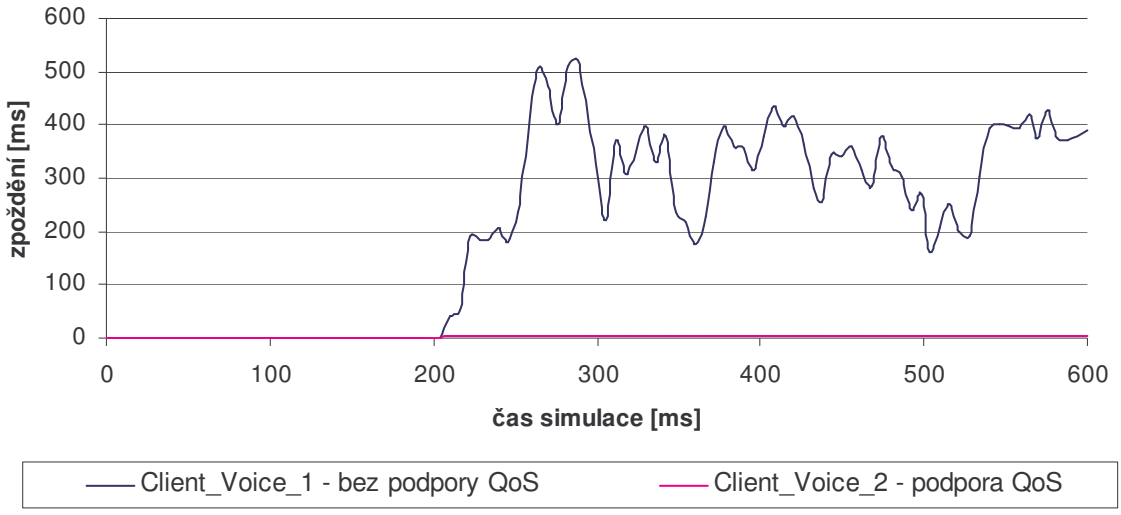
Mechanismus EDCA je vytvořen tak, aby QSTA plnily svoji funkci i v síti se stanicemi, které tento mechanismus nepodporují. Je toho dosaženo tím, že nejkratší čekací interval AIFS u mechanismu EDCA, po kterém mohou stanice začít soutěžit o přístup k médiu je roven čekacímu intervalu DIFS u základního mechanismu DCF. To tedy vlastně znamená, že všechny stanice (s podporou QoS i bez ní) mohou začít soutěžit o přístup k médiu současně. Rozdíl nastává až v okamžiku generování náhodně dlouhé čekací doby z okna soutěžení CW, která je dána podle kategorie provozu viz Tab. 5.7, kde jsou hodnoty vypočítány pro 802.11b, protože síť tohoto standardu používáme v simulaci.

Metoda	Čekací interval	AIFSN	Čekání [µs]	CW_{min}	CW_{max}
DCF	DIFS	-	50	31	1023
EDCA	AIFS (VO)	2	50	7	15
	AIFS (VI)	2	50	15	31
	AIFS (BE)	3	70	31	1023
	AIFS (BC)	7	150	31	1023

Tab. 5.7: Čekací intervaly přístupových metod u standardu 802.11b

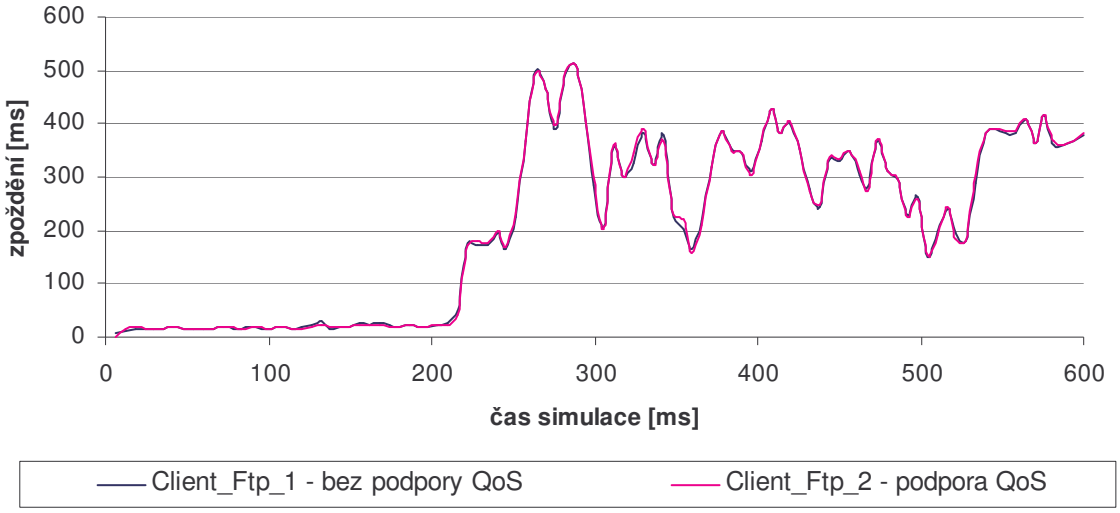
Z tabulky je poznat, že data kategorie Voice a Video jsou upřednostněna díky kratšímu oknu soutěžení (CW) oproti datům od stanice s přístupovou metodou DCF. Naopak data kategorie Background jsou znevýhodněna díky delšímu čekacímu intervalu před soutěžením. Hodnoty kategorie Best-effort se nejvíce blíží časům mechanismu DCF, to tedy znamená, že datový provoz stanic bez podpory QoS se řadí přibližně do kategorie Best-effort.

Následující dva grafy dokazují správnou kooperaci stanic obou typů. Na Obr. 5.25 je zobrazeno zpoždění přenosu u VoIP mezi klienty Client_Voice_1 a Client_Voice_2. Client_Voice_1 pracuje pomocí klasické metody DCF a Client_Voice_2 využívá mechanismu EDCA kategorie Voice.



Obr. 5.25: Kooperace stanic voice klientů

Obr. 5.26 ukazuje vzájemnou kooperaci stanic Client_Ftp_1 a Client_Ftp_2. Client_Ftp_1 pracuje podle mechanismu DCF a Client_Ftp_2 pomocí EDCA s kategorií Best-effort. Zpoždění obou přenosů je shodné, což dokazuje, že provoz stanice bez podpory QoS je řazen do kategorie Best-effort.



Obr. 5.26: Kooperace stanic ftp klientů

6 ZÁVĚR

Tato bakalářská práce se skládá ze tří hlavních částí. V první z nich nalezneme shrnutí problematiky zabezpečení bezdrátových sítí Wi-Fi. Tímto tématem se zabývá spousta knižních publikací a bylo o ní již mnoho napsáno. Proto v mé práci nalezneme pouze shrnutí dosavadních používaných technik a jejich objasnění. Jednotlivé metody zabezpečení jsem v práci seřadil podle jejich stupně bezpečnosti, tzn. od těch nejjednodušších až po ty nejdokonalejší, které se využívají v moderních komunikačních sítích.

Druhá část práce se týká zajištění kvality služeb (QoS) v bezdrátových sítích standardu 802.11. Protože je tento požadavek na zajištění kvality služeb poměrně novinkou a většina hardwarového zařízení jej ještě ani nepodporuje, měl jsem značný problém s hledáním materiálů pro zpracování a nastudování technologie jako takové. Po překonání těchto problémů se mi ale podařilo vytvořit přehled o doplňku 802.11e, který se právě týká zajištění QoS. Nalezneme zde základní funkční mechanizmy pomocí kterých se této služby dosahuje.

V poslední části bakalářské práce jsem se zabýval praktickým ověřením získaných poznatků z předchozích dvou teoretických částí. K tomuto mi sloužil simulační nástroj Opnet Modeler. V tomto programu jsme vytvořit funkční model reálné sítě, kterou můžeme nalézt na mnoha místech kolem nás. Musím říci, že tento nástroj je velice dobrým pomocníkem při návrhu a odstraňování nedostatků sítí. Pro zkušeného uživatele zde není problém vytvořit a simulovat síť podle vlastních požadavků během krátké doby.

Pro tuto práci, ve které bylo mým úkolem ověřit vlastnosti bezdrátové sítě 802.11 s podporou standardu 802.11e, jsem vytvořil dvě identické sítě. Rozdíl mezi nimi je v tom, že jedna z nich obsahuje zařízení s podporou standardu 802.11e a druhá

nikoli. V síti s podporou QoS, tzn. s podporovaným mechanismem EDCA, jsem rozdělil provoz do čtyřech kategorií provozu a každému z nich přidělil určitý stupeň priority.

Tyto dvě sítě jsem simuloval pro 10 minut reálného provozu a zjištěné charakteristiky zaznamenal do grafů. Jednotlivé průběhy (zpoždění paketů, prostupnost sítě atd.) jsem potom porovnal pro obě sítě a došel k závěru, že nový standard 802.11e plní svoji funkci zcela správně a dle očekávání z teoretických poznatků. Mechanismus pro zajištění QoS funguje velmi efektivně a je schopen zajistit správnou funkci pro multimediální služby, především pro IP telefonii a přenos videa.

Uživatelé, kteří si do své stávající sítě, která obsahuje síťové prvky bez podpory QoS, přidají nové zařízení s implementovanou podporou QoS, se nemusí obávat toho, že by nové zařízení neplnilo svoji funkci. Díky dobře navrženému mechanismu, který zajišťuje kvalitu služeb, je dosaženo správné kooperace starších zařízení s novými.

Standard 802.11e je tedy dobrým řešením, jak zajistit požadovanou kvalitu služeb v bezdrátových sítích WLAN typu 802.11. Tento standard přinese uživatelům zpříjemnění multimediálních služeb, po kterých je v dnešní době stále větší poptávka.

SEZNAM LITERATURY A POUŽITÝCH ZDROJŮ

[1] VELTE, Toby, VELTE, Anthony. *Síťové Technologie Cisco : Velký průvodce*. Libor Pácl; David Krásenský. Brno : Computer Press, 1993. 759 s. ISBN 80-7226-857-0.

[2] SHELLY, Brisbin. *Wi-Fi : Postavte si svou vlastní wi-fi síť a mnoho dalšího*. RNDr. Petr Zavadil. Praha : Neocortex, spol s.r.o, 2003. 248 s. ISBN 80-86330-13-3.

[3] KÖHRE, Thomas. *Stavíme si bezdrátovou síť Wi-Fi*. Jindřich Jonák; Marek Šiller. Brno : Computer Press, 2004. 295 s. ISBN 80-251-0391-9.

[4] BARKEN, Lee. *Jak zabezpečit bezdrátovou síť*. Jiří Matoušek; Jiří Veselský. Brno : Computer Press, 2004. 175 s. ISBN 80-251-0346-3.

[5] MOLNÁR, Karol. *Řízení kvality služeb v bezdrátových sítích*. [s.l.], 2007. 36 s. Skripta.

[6] WEBER, Filip. *Svět sítí : technologie* [online]. 2007 [cit. 2007-11-14]. Dostupný z WWW: <www.svetsiti.cz>.

[7] PUŽMANOVÁ, Rita. *Lupa : Server o českém internetu* [online]. 2004 [cit. 2004 -09-02]. Dostupný z WWW: <www.lupa.cz>. ISSN 1213-0702.

[8] *Wi-Fi Alliance* [online]. 2007 [cit. 2007-11-15]. Dostupný z WWW: <www.wi-fi.org>.

[9] OLEXA, R., G. *Implementing 802.11, 802.16 and 802.20 Wireless Networks*. Elsevier, Burlington, USA. ISBN:0-7506-7808-9.

[10] PRASAD, A.; PRASAD, N. *802.11 Wlans And Ip Networking, Security, QoS and mobility*. Boston-London, 2005, ISBN-13: 978-1580537896.