Universidade de Aveiro Departamento de Electrónica, Telecomunicações e Informática

2009

João Carlos Cruz Borges

Análise Experimental da Qualidade de Serviço do WiMAX e Wi-Fi em Malha

Experimental Analysis of WiMAX and Meshed Wi-Fi Quality of Service

Versão Final

Universidade de Aveiro
2009
Departamento de Electrónica, Telecomunicações e Informática

João Carlos Cruz Borges

Análise Experimental da Qualidade de Serviço do WiMAX e Wi-Fi em Malha

Experimental Analysis of WiMAX and Meshed Wi-Fi Quality of Service

Dissertação apresentada à Universidade de Aveiro para cumprimento dos requisitos necessários à obtenção do grau de Mestre em Engenharia Electrónica e de Telecomunicações (Mestrado Integrado), realizada sob a orientação científica do Prof. Dr. Amaro de Sousa, Professor auxiliar do Departamento de Electrónica, Telecomunicações e Informática da Universidade de Aveiro.

o júri

presidente

Prof. Doutor Rui Andrade Aguiar

Professor Associado do Departamento de Electrónica, Telecomunicações e Informática da Universidade de Aveiro

vogais

Prof. Doutor Amaro Fernandes de Sousa

Professor auxiliar do Departamento de Electrónica, Telecomunicações e Informática da Universidade de Aveiro

Prof. Doutor Carlos Manuel da Silva Rabadão

Professor Adjunto do Departamento de Engenharia Informática da Escola Superior de Tecnologia e Gestão do Instituto Politécnico de Leiria

agradecimentos

Apresento os meus agradecimentos ao Professor Doutor Amaro de Sousa que sempre se mostrou disponível para me ajudar.

Agradeço a todos os meus colegas de laboratório pelas ajudas, sugestões e explicações tão amavelmente prestadas e aos meus amigos pela sua tolerância e simpatia.

Finalmente, agradeço à minha família, que como ninguém, me apoiou pacientemente em todos os desafios e dificuldades que enfrentei.

palavras-chave

Redes sem Fios, Qualidade de Serviço, WiMAX, Wi-Fi em Malha

resumo

A indústria das telecomunicações tem sofrido uma evolução enorme nos últimos anos. Tanto em termos de comunicações sem fios, como em termos de ligações de banda larga, assistiu-se a uma adesão massiva por parte do mercado, o que se traduziu num crescimento enorme, já que a tecnologia tem que estar um passo à frente da procura, de forma a suprir as carências dos consumidores. Assim, a evolução persegue um objectivo claro: possibilidade de possuir conectividade de banda larga em qualquer lugar e instante. Neste contexto, aparecem as tecnologias WiMAX (Worldwide Interoperability for Microwave Access) e WI-FI em Malha como possibilidades para atingir este fim.

O tema desta dissertação incide no estudo das tecnologias de WiMAX e WI-FI em Malha, mais concretamente no estudo da Qualidade de Serviço (QoS) providenciada pelas normas IEEE 802.16 e IEEE 802.11s para serviços de VoIP e VoD.

Esta tese apresenta a arquitectura desenvolvida para a correcta integração de QoS para serviços em tempo real no acesso à banda larga sem fios de próxima geração. De seguida, apresenta testes efectuados com os equipamentos disponíveis de WiMAX e WI-FI em Malha, de forma a mostrar o correcto comportamento da atribuição extremo-a-extremo de QoS nos cenários escolhidos com serviços em tempo real, bem como os efeitos da mobilidade na tecnologia WI-FI em Malha.

keywords Wireless Networks, Quality of Service, WiMAX, Mesh Wi-Fi

abstract

The telecommunication industry has suffered a massive evolution throughout past years. In terms of wireless communications, as well as broadband connections, we've seen a massive adoption by the market, which conducted into an enormous growth, since the technology must always be one step ahead of the demand, in order to be to fulfill the needs of the consumers. Therefore, the evolution pursues one clear goal: the possibility to establish a broadband connection anywhere and anytime. In this context, the WiMAX (Worldwide Interoperability for Microwave Access) and Meshed WI-FI technologies appear as possibilities to reach this goal.

The subject of this thesis is the study of both the WiMAX and Meshed WI-FI technologies, and more concretely the study of the QoS provided by the IEEE802.16 and IEEE 802.11s standards to VoIP and VoD services.

This thesis presents the architecture developed to provide the correct integration of QoS for real-media traffic in next generation broadband wireless access. It presents tests carried out with the available WiMAX and Meshed WI-FI equipments, to show the correct behavior in the attribution of end-to-end QoS in selected scenarios with real-time services, as well as mobility effects on WI-FI Wireless Mesh technology.

Table of Contents

Index of Figures

Index of Tables

Acronyms

AC	Access Category
ACK	Acknowledgement
AIFS	Arbitration IFS
AIFSN	Arbitration IFS Number
AODV	Ad-Hoc On-Demand Distance Vector
AP	Access Point
BS	Base Station
BE	Best Effort
BSS	Basic Service Set
BWA	Broadband Wireless Access
CAP	Controlled Access Phase
CCA	Clear Channel Assessment
CCC	Common Control Channel
CCF	Common Channel Framework
CCK	Complementary Code Keying
CCW	Channel Coordination Window
CF	Contention-Free
CFB	Contention Free Burst
CFP	Contention-Free Period
CID	Connection Identifier
CP	Contention Period
CPS	Common Part Sublayer
CPE	Customer Premises Equipment
CRC	Cyclic Redundancy Check
CS	Convergence Sublayer
CSMA/CA	Carrier Sense Multiple Access with Collision Avoidance
CTS	Clear to Send
DBPSK	Differential Binary Phase Shift Keying
DCF	Distribution Coordination Function
DFS	Dynamic Frequency Selection
DHCP	Dynamic Host Configuration Protocol
DIFS	Distributed Coordination Function Inter Frame Space
DLP	Direct Link Protocol
DQPSK	Differential Quadrature Phase Shift Keying
DS	Distribution System
DSL	Direct Subscriber Line
DSSS	Direct Sequence Spread Spectrum
DTIM	Delivery Traffic Indication Map
EDCA	Enhanced Distributed Channel Access
ESS	Extended Service Set
FDD	Frequency Division Duplex
FHSS	Frequency Hopping Spread Spectrum

GHM	Generic MAC Header
HC	Hybrid Coordinator
HCCA	HCF-Controlled Channel Access
HCF	Hybrid Coordination Function
HWMP	Hybrid Wireless Mesh Protocol
IAPP	Inter Access Point Protocol
IBSS	Independent Basic Service Set
ICI	Inter Carrier Interference
IFS	Inter Frame Spacing
IR	Infrared
ISI	Inter Symbol Interference
ISM	Industrial Scientific and Medical
JTG	Jugi's Traffic Generator
LAN	Local Area Network
MAC	Medium Access Control
MAF	Mesh Access Fraction
MAP	Mesh AP
MCM	Multicarrier Modulation
MDA	Mesh Deterministic Access
MDAOP	Mesh Deterministic Access Opportunity
MP	Mesh Point
MPDU	MAC Protocol Data Unit
MPP	Mesh Portal
MSDU	MAC Service Data Unit
MTU	Maximum Transmission Unit
NAV	Network Allocation Vector
NLOS	Non Line of sight
nrTPS	Non-Real-Time Polling Services
OFDM	Orthogonal Frequency Division Multiplexing
OFDMA	Orthogonal Frequency Division Multiple Access
PC	Point Coordinators
PCF	Point Coordination Function
PCI	Peripheral Component Interconnect
PDU	Packet Data Unit
PHY	Physical
PHS	Payload Header Suppression
PIFS	Point Coordination Function Inter Frame Space
PIR	Packet Identification Rules
PN	Pseudorandom Number
PTP	Precision Time Protocol

PTPd	Precision Time Protocol daemon
QAM	Quadrature Amplitude Modulation
QAP	QoS-Enhanced AP
QBSS	QoS-Supporting BSS
QoS	Quality of Service
QoS	Quality of Service
QPSK	Quadrature Phase Shift Keying
QSTA	QoS-Enhanced STA
RA-OLSR	Radio Aware-Optimized Link State Routing
RREP	Route Response
RREQ	Route Request
rTPS	Real-Time Polling Service
RTS	Request to Send
SAP	Service Access Point
SC	Single Carrier
SF	Service Flow
SIFS	Short Inter Frame Spacing
SSID	Service Set Identifier
STA	Station
SS	Subscriber Station
TBTT	Target Beacon Transmission Time
TDD	Time Division Duplex
TID	Traffic Identifier
TOS	Type of Service
TS	Traffic Stream
TSF	Timing Synchronization Function
TXOP	Transmission Opportunity
UCG	Unified Channel Graph
UDP	User Datagram Protocol
UGS	Unsolicited Grant Service
UP	User Priority
VoD	Video-on-Demand
WAN	Wide Area Network
WDS	Wireless Distribution System
WEP	Wired Equivalent Privacy
Wi-Fi	Wireless Fidelity
WiMAX	Worldwide Interoperability for Microwave Access
WLAN	Wireless Local Area Network
WM	Wireless Medium
WMAN	Wireless Metropolitan Area Network
WMN	Wireless MESH Networks

1. Introduction

This chapter offers a global vision of the work developed in this thesis. We start by presenting a brief motivation for the wireless technologies and, then, we proceed describing the objectives of this work and structure of this thesis.

1.1. Motivation

As the number of Internet users, with a need to be "connected" at anytime and anywhere, keeps growing, one of the main concerns in Telecommunications has become the delivery of "last-mile" broadband wireless access as an alternative to Cable and DSL (Digital Subscriber Line) to these users. Broadband Wireless Access (BWA) is a high data rate Wireless Metropolitan Area Network (WMAN) with the objective of providing broadband access services in a wireless context, offering users, both residential and commercial, increased benefits and convenience. The BWA not only provides fast Web surfing and quick file downloads but also enables multimedia applications, such as real-time audio (VOIP) and video-on-demand (VoD) streaming, multimedia conferencing and interactive gaming.

As multimedia services are becoming more and more important, new broadband access technologies emerge to address the specific requirements of such services. To this purpose, there exist several traditional first mile solutions, using either cables or fibers, and a novel family of Broadband Wireless Access (BWA) technologies. Among BWA technologies, the IEEE 802.16 standard is one of the possible alternatives for the provision of Internet-based broadband services in wide area networks. The IEEE 802.16 group was formed in 1998 to develop an air-interface standard for wireless broadband. The resulting standard is a technology that enables the delivery of last mile wireless broadband access and provides fixed, nomadic, portable and, eventually, mobile wireless broadband connectivity. Having, in a typical cell radius deployment of 3 to 10 kilometers, a capacity to deliver up to 40 Mbps, per channel, for fixed and portable applications, the IEEE 802.16 (commonly called Worldwide Interoperability for Microwave Access - WiMAX) is a technology for metropolitan access. The key advantage of the IEEE 802.16 standard is to ensure large area coverage and inexpensive equipment at the subscriber side. Modern requirements to wireless connectivity include mandatory QoS guarantees for a wide set of real-time applications: this is the case of the ever growing trend of VoIP calls and VoD services.

In the recent years the deployment of Wireless MESH Networks (WMNs) has been looked upon as an upcoming and promising step towards the goal of ubiquitous broadband wireless access. WMNs are interesting not only in the context of small community networks and neighborhood networks, but also in the area of enterprise-wide networks or wireless backbone. In order to achieve these goals, QoS is a critical issue. Network providers, who look at WMNs as a cheap alternative to expand their existing wireless network infrastructure, without incurring exorbitant deployment costs, also look at WMNs as a viable alternative. In such networks, the providers wish to support the integrated services they already offer on their traditional wireless platforms. These applications such as voice and video over IP need to be provided with carrier-grade QoS support.

1.2. Objectives

The main objective of this work is to characterize the QoS provided by different broadband wireless access technologies on VoIP and VoD services. We analyze both WiMAX and WI-FI (on a mesh configuration) and test the different QoS mechanisms provided by each technology in managing VoIP and VoD services. We use off-the-shelf equipments and generate VoIP and VoD traffic through our network, with multiple competing TCP flows, and measure the capacity of our equipments to handle a multitude of traffic on real user scenarios. To complete this objective, a deep study of both technologies and QoS mechanisms was conducted, as well as a familiarization with the equipments and their configuration.

1.3. Organization of the Thesis

The presented thesis is organized as follows:

- Chapter 2 presents an overview of the IEEE 802.16 standard, including the Medium Access Control (MAC) and Physical (PHY) layers. It includes an explanation of the QoS mechanisms inherited, a comparison between the fixed and mobile IEEE 802.16 standards, and the main characteristics of the equipment used in this work.
- Chapter 3 provides an overview of Wireless Local Area Networks (WLANs) with emphasis on the IEEE 802.11 standard, including the Medium Access Control (MAC) and Physical (PHY) layers. It includes an explanation of possible architectures and the QoS mechanisms inherited and optimized on IEEE 802.11 standard.
- Chapter 4 provides an overview of Wireless Mesh Networks (WMNs), including the Medium Access Control (MAC) optimization for mesh configuration. It includes a comparison between MESH and AD-HOC networks, an explanation on routing and QoS mechanisms, and the main characteristics of the equipment used in this work.
- Chapter 5 describes the experiments conducted with real-time traffic (VoIP and VoD) under a fixed WiMAX topology and evaluates the QoS performance of the equipment used on the testing scenarios.
- Chapter 6 describes the experiments conducted with real-time traffic (VoIP and VoD) under an IEEE 802.11 Wireless Mesh Network and evaluates the characteristics of the network, a handover scenario and the QoS performance of the equipment used on the testing scenarios.
- Chapter 7 provides the final conclusions of this work as well as the possible direction for future work.

2. IEEE 802.16

WiMAX is based on the IEEE 802.16 standard and has two variants: IEEE.16-2004 (also known as 802.16d), which defines a fixed wireless access WMAN technology, and IEEE 802.16e-2005, which is an amendment of 802.16-2004, including mobility and fast handover. Its architecture is defined by the WiMAX Forum.

These standards define WiMAX as a layer 1 (Physical - PHY) and layer 2 (Medium Access Control - MAC) technology (Figure 1). It includes Non Line of Sight (NLOS) applications on the 2GHz-11GHz band, using Orthogonal Frequency Division Multiplexing (OFDM), and has support for Orthogonal Frequency Division Multiple Access (OFDMA).

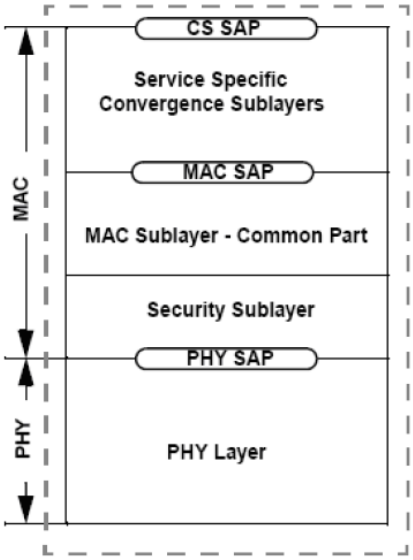

Figure 1 - 802.16-2004 layers (PHY and MAC)

Using a system profile based on the IEEE 802.16-2004 OFDM physical layer with a Point-to-Multipoint (PMP) or Mesh MAC layer, and possibility for Time Division Duplexing (TDD) or Frequency Division Duplexing (FDD), WiMAX uses more efficiently the frequency, allowing better QoS and security for the various services provided.

2.1. Network Architecture and Deployment Topology:

An IEEE 802.16 network consists of fixed infrastructural sites. In fact, an IEEE 802.16 network resembles a cellular phone network. Each cell consists of a Base Station (BS) and one or more Subscriber Station (SS), depending on the implementation of the topology. The BS provides either Point-to-Point (PTP) or Point-to-Multipoint (PMP) services in order to serve multiple SSs. BSs provide connectivity to core networks. The SS can be a roof mounted or wall mounted Customer

Premises Equipment (CPE) or a standalone hand held device like Mobile phone, personal digital assistant (PDA) or Peripheral Component Interconnect (PCI) card for PC or Laptop. In case of an outside CPE, the users inside the building are connected to a conventional network like Ethernet Local Area Network (IEEE 802.3 for LAN) or Wireless LAN (IEEE 802.11b/g for WAN) which have access to the CPE. A group of cells can be grouped together to form a network, where BSs are connected through a core network, as shown in Figure 2. The IEEE 802.16 network also support mesh topology, where SSs are able to communicate among themselves without the need of a BS [29].

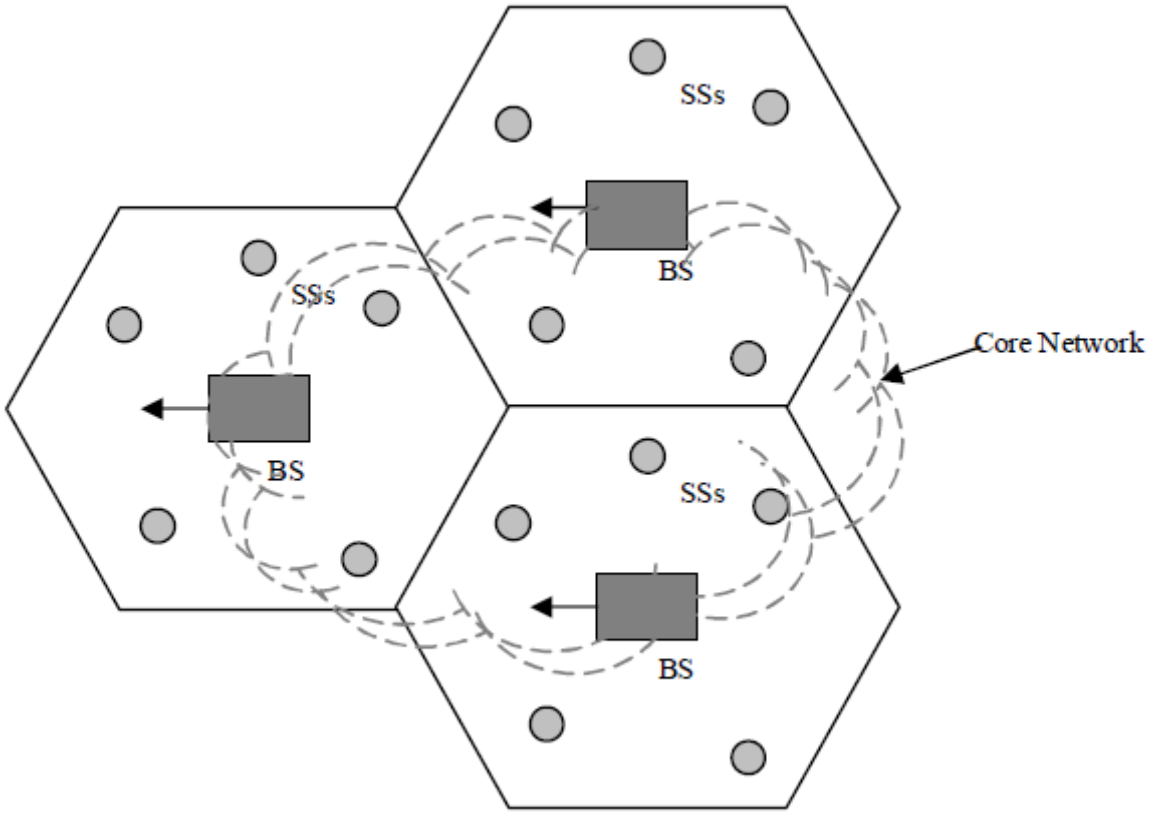

Figure 2 - A typical IEEE 802.16 Network

BSs typically employ one or more wide beam antennas that may be partitioned into several smaller sectors, where all sectors sum to complete 360 degree coverage. CPEs typically employ highly directional antennas that are pointed towards the BS. Depending on the need, IEEE 802.16 network can be deployed in different forms.

2.2. IEEE 802.16-2004 PHY Layer

The PHY Layer is responsible for establishing the physical connection between the source and destination for uplink and downlink, defining the type of signal used, modulation, demodulation, bit transmission, etc.

WiMAX physical layer is based on Orthogonal Frequency Division Multiplexing (OFDM). OFDM is based on multicarrier modulation, which is based on the principle of transmitting simultaneously many narrow-band orthogonal frequencies by dividing a given high-bit-rate data stream into several parallel lower bit-rate streams and modulating each stream (using Quadrature Amplitude Modulation – QAM, or Quadrature Phase Shift Keying - QPSK) on separate carriers. Since the subcarriers are orthogonal to each other the Inter Symbol interference (ISI) is eliminated. Also, having a smaller frequency bandwidth for each channel allows for a better resistance to multipath propagation.

Four physical interfaces are defined, by the IEEE 802.16 standard, along the frequency band 2-66GHz, using TDD and FDD (half-duplex and full-duplex). We can divide them into two different frequency bands:

- **10-66 GHz** licensed frequency band, requiring line of sight (LOS) due to the short wave length. In this band we find: **WirelessMAN-SC** (Single Carrier) – provides a physical layer with a single carrier air interface.
- **2-11 GHz** licensed frequency band, not requiring LOS due to the higher wave length. In this band we find: **WirelessMAN-SCa** (Single Carrier a) – provides a physical layer with a single carrier air interface; **WirelessMAN-OFDM** – provides a physical layer with multiple-carrier air interface, using Orthogonal Frequency Division Multiplexing (OFDM) with 256 carriers; **WirelessMAN-OFDMA** – provides a physical layer with multiple-carrier air interface, using Orthogonal Frequency Division Multiple Access (OFDMA) with 2048 carriers.

Thus, OFDM is the preferred transmission scheme to enable high-speed data and multimedia application services.

2.2.1. OFDM

The idea of OFDM comes from Multicarrier Modulation (MCM) transmission technique. The principle of MCM describes the division of input bit stream into several parallel bit streams and then they are used to modulate several sub carriers. Each subcarrier is separated by a guard band to ensure that they do not overlap with each other. In the receiver side, bandpass filters are used to separate the spectrum of individual subcarriers. OFDM is a special form of spectrally efficient MCM technique, which employs densely spaced orthogonal subcarriers and overlapping spectrums. The use of bandpass filters is not required in OFDM because of the orthogonality nature of the subcarriers. Hence, the available bandwidth is used very efficiently without causing the Inter Carrier Interference (ICI) (is possible to recover the individual subcarrier despite their overlapping spectrum provided that the orthogonality is ensured). The orthogonality is achieved by performing Fast Fourier Transform (FFT) on the input stream. Because of the combination of multiple low data rate subcarriers, OFDM provides a composite high data rate with long symbol duration. Depending on the channel coherence time, this reduces or completely eliminates the risk of Inter Symbol Interference (ISI), which is a common phenomenon in multipath channel environment with short symbol duration. The use of Cyclic Prefix (CP) in OFDM symbol can reduce the effect of ISI even more [30], but it also introduces a loss in SNR and data rate.

A simplified OFDM process block is depicted in Figure 3.

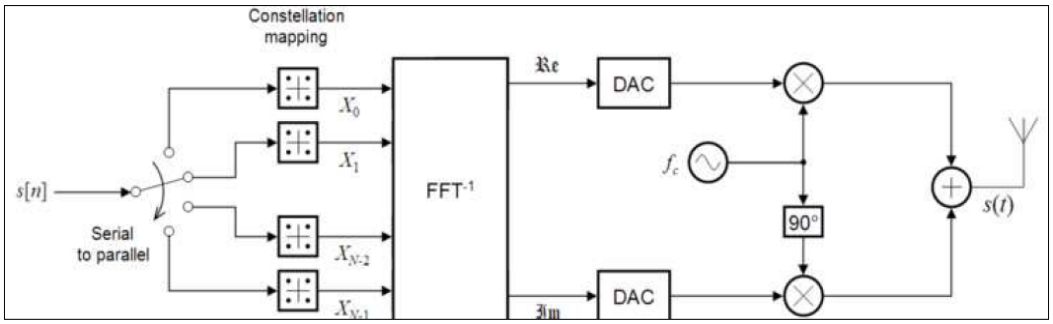

Figure 3 - Basic OFDM Transmitter

2.2.2. TDD and FDD Duplex Schemes

One of the key elements of any radio communications system is the way in which radio communications are maintained in both directions. Terms including simplex, duplex, Frequency Division Duplex (FDD) and Time Division Duplex (TDD) are all methods that can be used.

For cellular systems, it is required to send data in both directions simultaneously, and this places a number of constraints on the schemes that may be used to control the transmission flow. As it is such a key element of the system, it is necessary to decide which scheme is to be used. As a result the duplex scheme to be used forms a very basic part of the overall specification for the cellular (or any radio communications system) that is to be used.

The WiMAX, 802.16 standard offers two forms of duplex transmission to separate the uplink and downlink messages: WiMAX TDD (time division duplex) and WiMAX FDD (frequency division duplex). Each method offers its own advantages and disadvantages.

2.2.2.1. Transmission control schemes

There are a variety of different ways of controlling the passage of information between two transmitters:

- **Simplex:** it can only occur in one direction. One example of this may be a broadcast system.
- **Half duplex:** This is a duplex scheme whereby communication is possible in two directions, but communication is only possible in one direction at a time. If one side is transmitting, the other side must wait until the first stops before transmitting. This form of communication is used for walkie-talkies, CB, etc.
- **Full duplex:** Full duplex, which is sometimes referred to simply as duplex, is a scheme whereby transmissions may be sent in both directions simultaneously. However it is still necessary for the transmissions to be separated in some way to enable the receivers to receive signals at the same time as transmissions are being made. There are two ways of

achieving this. One is to use frequency separation (frequency division duplex, FDD) and the other is to use time separation (time division duplex, TDD).

2.2.2.2. Frequency Division Duplex

Frequency Division Duplex (FDD) uses the idea that the transmission and reception of signals are achieved simultaneously using two different frequencies. Using FDD it is possible to transmit and receive signals simultaneously as the receiver is not tuned to the same frequency as the transmitter as shown in Figure 4.

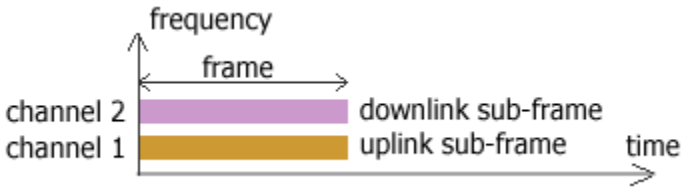

Figure 4 - Frequency Division Duplex

For the FDD scheme to operate satisfactorily, the channel separation between the transmission and reception frequencies must be enough to enable the receiver not to be affected by the transmitter signal. This is known as the guard band.

Receiver blocking is an important issue with FDD schemes, and often highly selective filters may be required. The use of an FDD system enables true simultaneous transmission and reception of signals. However two channels are required and this may not always use the available spectrum efficiently.

The spectrum used for FDD systems is allocated by the regulatory authorities. As there is a frequency separation between the uplink and downlink directions, it is not normally possible to reallocate spectrum to change the balance between the capacity of the uplink and downlink directions if there are changing capacity requirements for each direction.

2.2.2.3. Time Division Duplex

The other system uses only a single frequency and it shares the channel between transmission and reception, spacing them apart by multiplexing the two signals on a time basis, as depicted in Figure 5. Time Division Duplex (TDD) is used with data transmissions (data, digitized voice, etc…), transmitting a short burst of data in each direction. As the transmission periods are relatively short, no time delay is noticed on voice transmissions resulting from the time delays introduced by using TDD.

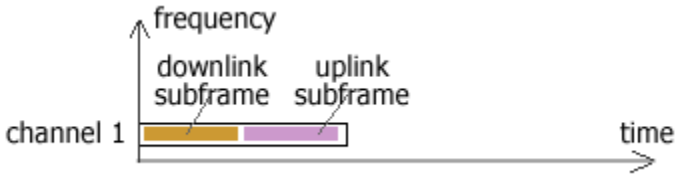

Figure 5 - Time Division Duplex

While FDD transmissions require a guard band between the transmitter and receiver frequencies, TDD schemes require a guard time interval between transmission and reception. This must be enough to allow the signals travelling from the remote transmitter to arrive before a transmission is started. Although this delay is relatively short, when changing between transmission and reception many times a second, even a small guard time can reduce the efficiency of the system as a percentage of the time must be used for the guard interval. For systems communicating over short distances, e.g. up to a one and half kilometer or so the guard interval is normally small and acceptable but for greater distances it may become an issue.

As a result, TDD is not normally suitable for use over long distances as the guard time interval increases and the channel efficiency decreases

It is often found that traffic in both directions is not balanced. Typically there is more data travelling in the downlink direction of a cellular telecommunications system, which means that, ideally, the capacity should be greater in the downlink direction. Using a TDD system, it is possible to change the capacity in either direction relatively easily by changing the number of time slots allocated to each direction. Often this is dynamically configurable so it can be altered to match the demand.

A further aspect to be noted with TDD transmissions is latency. As data may not be able to be routed immediately onto a transmission as a result of the time multiplexing between transmit and receive, there will be a small delay between the data being generated and it being actually transmitted. Typically this may be a few milliseconds depending upon the frame times which might be negligible for some applications but might be significant for others, namely for VoIP service.

2.3. IEEE 802.16-2004 MAC Layer

The primary task of the WiMAX MAC layer is to provide an interface between the higher transport layers (IP, ATM) and the physical layer. It can be divided into three sublayers: Service Specific Convergence Sublayer (CS) provides the interface with the higher transport layers through a CS service access point (SAP); Medium Access Control Common Part Sublayer (MAC CPS) resides in the middle of the MAC layer and is responsible for the bandwidth allocation and data transport of the MAC layer; Security Sublayer follows MAC CPS. The MAC layer supports both PMP and Mesh.

2.3.1. Service Specific Convergence Sublayer

The Service Specific Convergence Sublayer (CS) is responsible for the convergence of ATM and packet services, such as TDM Voice, Ethernet, IP, and any unknown future protocol.

The CS takes Packet Data Units (PDUs) from the upper layer (MAC Service Data Units - MSDUs), through the Service Access Point (SAP) and organizes them into MAC Protocol Data Units (MPDUs), which are sent across multiple frames. Each MAC frame is prefixed with a Generic MAC Header (GMH) containing a Connection Identifier (CID), which serves as a temporary address for data transmissions over the particular link and is a basic function of the QoS management mechanisms. The CS also delivers the PDUs to the appropriate MAC SAP and receives PDUs from the peer entity. An optional function is the Payload Header Suppression (PHS), a process to suppress the repetitive parts of the payload headers; this is the case of some RTP/UDP/IPv6 packets (RTP – Real-Time Protocol, UDP – User Datagram Protocol).

In order to provide unidirectional transport of packets on the uplink or downlink, the MAC layer uses a Service Flow (SF). A SF is a MAC transport service characterized by a set of QoS parameters (such as traffic priority, tolerated jitter, latency and throughput) and identified by a service flow identifier (SFID). As a packet, taken from the upper layers through the SAP, is being delivered on the connection defined by its CID, the SF characteristics of the connection provide the QoS for that packet. This principle can be seen in Figure 6, downlink from a Base Station (BS) and uplink from a Subscriber Station (SS).

Thus, IEEE 802.16 MAC is connection oriented.

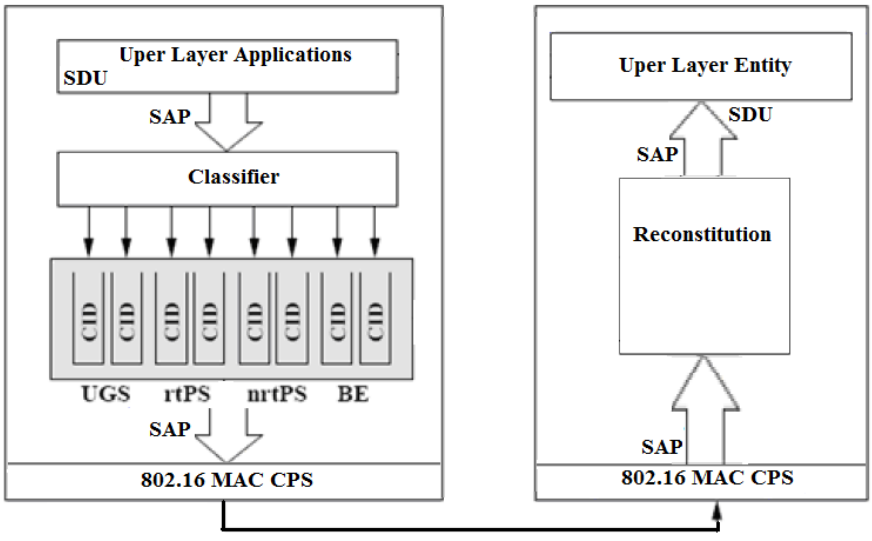

Figure 6 - Classification and CID Mapping

2.3.2. Medium Access Control Common Part Sublayer

Residing in the middle of the MAC layer, the Medium Access Control Common Part Sublayer (MAC CPS) represents the core of the MAC protocol and is responsible for:

- Bandwidth allocation
- QoS and Traffic parameters association
- Connection establishment
- Transport and routing of packets to the appropriate CS
- Maintenance of the connection between two sides (BS and SS)

To support a wide variety of applications, the 802.16-2004 standard defines a set of management and transfer messages that are exchanged between the SS and the BS before and during the establishment of the connection. When the connection is realized, the transfer messages can be exchanged to allow the data transmission. As the MAC CPS receives data from the various CSs, through the SAP, with specific CID, the QoS is taken into account for the transmission and scheduling of data over the PHY layer. Hence, the 802.16-2004 standard defines four scheduling services that should be supported by the base station and subscriber station MAC scheduler for data transport over a connection:

- **Real-Time Polling Services (rtPS)** – aimed for real-time service flows, such as MPEG video.
- **Non-Real-Time Polling Services (nrtPS)** – aimed for delay-tolerant data streams, such as an FTP.
- **Best-Effort (BE) service** – aimed to support data streams, such as Web browsing.
- **Unsolicited Grant Services (UGS)** – aimed to support fixed-sized data packets at a *constant bit rate* (CBR), such as T1/E1 emulation and VoIP without silence suppression.

2.4. IEEE 802.16 Hardware – Proxim Wireless Tsunami MP.16 3500

The IEEE 802.16 equipment (Proxim Wireless Tsunami MP.16 3500) used in this work is compliant with the IEEE 802.16-2004 standard. It is composed by an indoor terminal (IDU) and outdoor transceiver (ODU) with internal antenna. Both the BS and SS have a WiMAX Forum Certification. The antennas used for the tests were mounted on the roof of our premises.

The MP.16 3500 features:

- Operation on the frequency of 3.4-3.6 GHz and maximum channel size of 7 MHz, allowing up to 25 Mbps data rate. The MP.16 3500 system uses time division duplex (TDD) to transmit and supports coding rates of 1/2, 2/3, and 3/4, OFDM modulation, 256 FFT points; BPSK, QPSK, 16-QAM, 64-QAM.
- BS: Database to support up to 256 Service Flow Classes, 512 Packet Identification Rules, and 64 SS Classes; 16 Service Flows per SS Class.

- Asymmetric Bandwidth Control: Uplink and Downlink CIR Control “committed information rate" per service flow; Uplink and Downlink MIR Control "maximum information rate" per service flow.
- Scheduling: Best Effort, Universal Grant Services, Traffic is scheduled per service flow, enabling min/max bandwidth, priority, jitter and latency control for voice, video and data
- Management Interface: Telnet/CLI, HTTP, TFTP; SNMP v1, v2 (MIBII, Proxim MIBs, Bridge MIB, 802.16 MIB, Etherlike MIB)

3. IEEE 802.11

A Wireless Local Area Network (Wireless LAN) is a wireless communication system that allows computers and workstations to communicate data with each other using radio waves as the transmission medium.

Although WLANs can be independent they are more typically an extension to a conventional wired network. They can allow users to access and share data, applications, internet access or other network resources in the same way as wired networks. Currently, Wireless LAN technology is significantly slower than wired LAN. Wireless LANs have a nominal data transfer rate of between 11 and 54 Megabits per second (Mbps) compared to most wired LANs in schools which operate at 100Mbps or 1000Mbps.

Wireless LANs are typically used with wireless enabled mobile devices such as notebook computers, PDAs and Tablet PCs. This allows users to take advantage of the flexibility, convenience and portability that WLANs can provide. Wireless networking is also appearing on other devices such as mobile phones, digital cameras, handheld games consoles and other consumer electronics.

There are several benefits in using WLANs [1], such as:
. Mobility - WLANs enhance the possibility to access real time information on the move, allowing the user to stay connected at all times while he moves within the coverage area.
. Short-Term Usage - Short-term connectivity allows users to deploy capabilities to connect to the network on an as needed basis, without concerning with wired solutions that can be expensive.
. Speed of Deployment - WLANs enable quick connectivity to the network, allowing for an easy forming and disbanding of work groups.
. Difficult Wiring Environment - Many situations do not enable the easy installation of wires, such as installation on historic or very old buildings, across a busy street, or on a disaster scenario where fast connectivity in the field is needed to gather data and coordinate relief efforts.
. Scalability - Wireless LAN systems can be configured in a variety of topologies to meet the needs of specific applications and installations.

The IEEE 802.11 protocol is a network access technology for providing connectivity between wireless stations and wired networking infrastructures. 802.11 WLAN is commonly referred to as “Wi-Fi” (Wireless Fidelity). To help ensure Wi-Fi products perform correctly and are interoperable with each other, the Wi-Fi Alliance was created in 1999.

By deploying the IEEE 802.11 protocol and associated technologies, mobile users are enabled to move between various locations within the coverage area, such as meeting rooms, hallways, lobbies, cafeterias, classrooms, and so forth, and still have access to networked data. Also, beyond the corporate workplace, Internet access is enabled and even corporate sites can be made available through public wireless “hot spot” networks (airports, restaurants, rail stations, and common areas throughout cities can be configured to provide this service).

3.1. 802.11 Architecture

The 802.11 logical architecture contains several main components [1][4]: Station (STA), Wireless Access Point (AP), Independent Basic Service Set (IBSS), Basic Service Set (BSS), Distribution System (DS), and Extended Service Set (ESS). Some of the components of the 802.11 logical architecture map directly to hardware devices, such as STAs and wireless APs. The wireless STA contains an adapter card, PC Card, or an embedded device to provide wireless connectivity. The wireless AP functions as a bridge between the wireless STAs and the existing network backbone for network access.

- An IBSS is a wireless network, consisting of at least two STAs, used where no access to a DS is available. An IBSS is also sometimes referred to as an ad hoc wireless network.
- A BSS is a wireless network, consisting of a single wireless AP supporting one or multiple wireless clients. A BSS is also sometimes referred to as an infrastructure wireless network. All STAs in a BSS communicate through the AP. The AP provides connectivity to the wired LAN and provides bridging functionality when one STA initiates communication to another STA or a node on the DS.
- An ESS is a set of two or more wireless APs connected to the same wired network that defines a single logical network segment bounded by a router (also known as a *subnet*).
- The APs of multiple BSSs are interconnected by the DS. This allows for mobility, because STAs can move from one BSS to another BSS. APs can be interconnected with or without wires; however, most of the time they are connected with wires. The DS is the logical component used to interconnect BSSs. The DS provides distribution services to allow for the roaming of STAs between BSSs.

Figure 7 shows the 802.11 architecture:

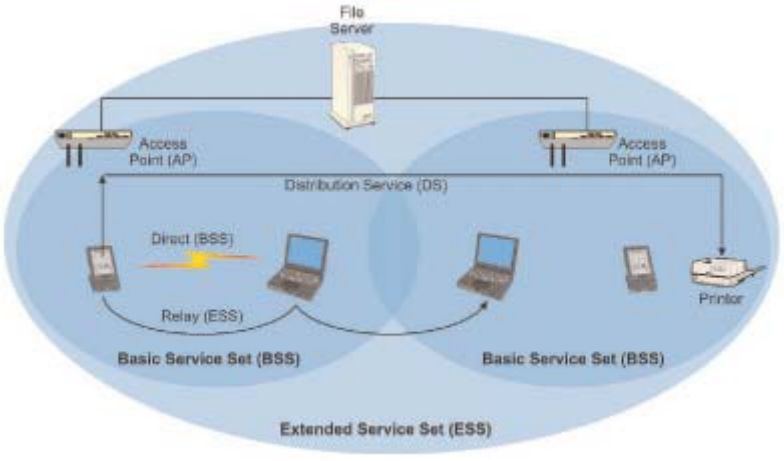

Figure 7 – IEEE 802.11 WLAN Architecture

3.2. IEEE 802.11 MAC Layer

The IEEE 802.11 standard [2] specifies a common Medium Access Control (MAC) Layer, which provides a variety of functions that support the operation of 802.11-based wireless LANs. In general, the MAC Layer manages and maintains communications between 802.11 stations (radio network cards and access points) by coordinating access to a shared radio channel and utilizing protocols that enhance communications over a wireless medium.

The IEEE 802.11 MAC Layer uses an 802.11 Physical (PHY) Layer, such as 802.11a, 802.11b or 802.11g, to perform the tasks of carrier sensing, transmission, and receiving of 802.11 frames.

The IEEE 802.11 MAC Layer defines two medium access coordination functions, the mandatory Distributed Coordination Function (DCF) and the optional Point Coordination Function (PCF).

3.2.1. Distributed Coordination Function

The basic 802.11 MAC protocol is referred to as the Distributed Coordination Function (DCF) and is based on the Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) protocol.

There are two kinds of DCF in the standard: the basic mandatory CSMA/CA and the optional Request to Send/Clear to Send (RTS/CTS) scheme.

3.2.1.1. DCF CSMA/CA

In the DCF based on CSMA/CA, the Station (STA) must sense the medium before initializing a packet transmission, only transmitting if the medium is free [1][3][6][7].

Two carrier sensing mechanisms are possible:

- PHY carrier sensing analyses the medium and detects the presence of other transmitting STA.
- Virtual carrier sensing can be used by an STA that sends a MAC Protocol Data Unit (MPDU) to all other STAs in the same Basic Service Set (BSS) with information on how long the channel will be reserved for transmitting its frame. With this information, the STAs in the BSS can adjust their Network Allocation Vector (NAV) to indicate this duration.

The priority access to the wireless medium is controlled trough the use of mandatory time intervals between the transmissions of frames, known as Inter Frame Space (IFS). The three IFS intervals, depicted in Figure 8, specified in the protocol are: Short IFS (SIFS), Point Coordination Function IFS (PIFS) and Distributed Coordination Function IFS (DIFS).

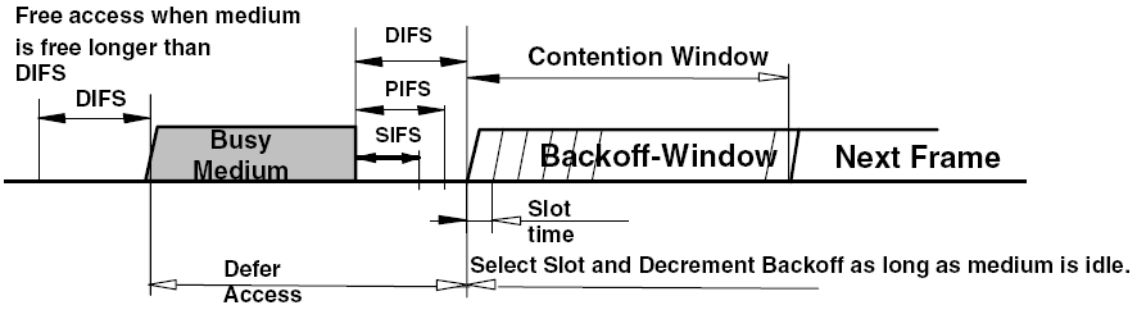

Figure 8 - IEEE 802.11 Inter Frame Spacing (IFS)

As depicted in Figure 9**,** if the wireless medium is free for a DIFS period the STA transmits its frames. Otherwise, if the STA senses the channel to be busy, the transmission is delayed for a DIFS period and the STA computes a random backoff timer selected from the Contention Window (CW): backoff_time = rand [0, CW] * slot_time. The CW_{min} < CW < CW_{max} and the slot_time depends on the PHY Layer type. Each time the medium becomes idle the backoff timer is decremented and as soon as it expires the STA is allowed to transmit.

In order to notify the sender that the frame as been successfully received, the receiver sends an Acknowledgement (ACK) packet after a SIFS period. If no ACK is received the STA assumes that a collision as occurred and reenters the backoff process. To reduce the possibility of new collisions, after each unsuccessful transmission the CW_{min} is doubled until it reaches the CW_{max} value. If the value surpasses the CW_{max} then the packet is discarded.

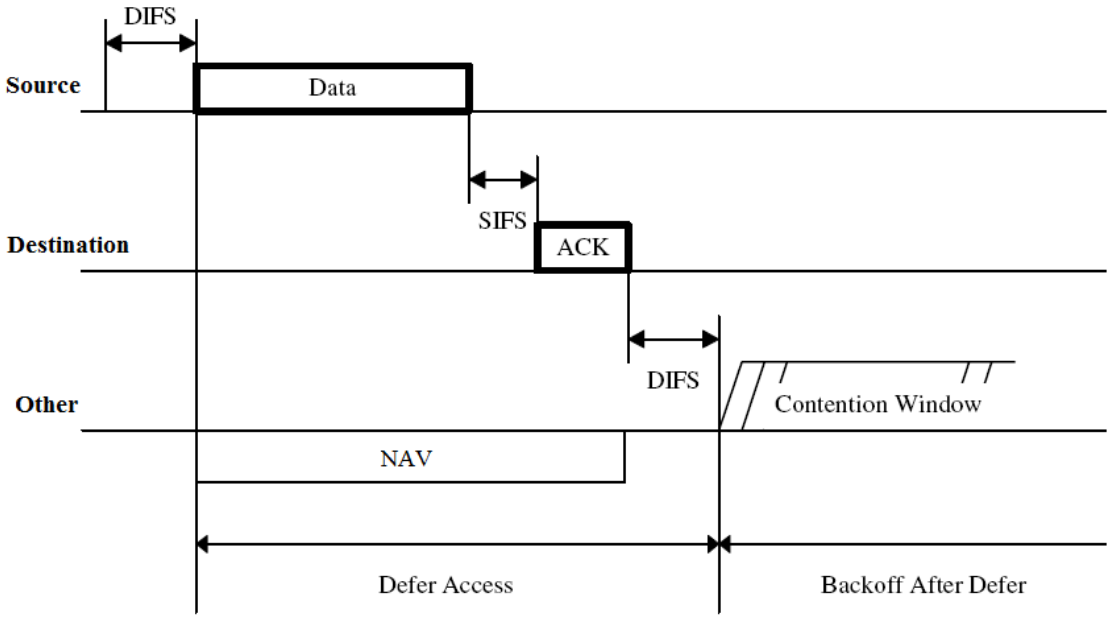

Figure 9 - DCF CSMA/CA

3.2.1.2. DCF RTS/CTS

The optional DCF based on RTS/CTS is used to avoid problems from hidden terminals. Hidden terminals are STAs that the receiver can detect but that are hidden from other senders, occurring collisions at the receiver between packets from different senders [1][3][6][7].

As depicted in Figure 10, the STA sends a RTS, after sensing the medium free for a DIFS period, to the receiver before sending the frame. The receiver answers with CTS, after the medium is idle for a SIFS period.

All STAs that hear the RTS, CTS or both can update their NAV and will start transmitting only when their NAV timers reach zero. Since the RTS frame has 20 bytes and the CTS frame has 14 bytes, they are much smaller than a data frame that can go up to 2346 bytes, allowing for less likely collision, thus improving the performance of basic DCF scheme. Any hidden terminal can now delay their transmission to avoid collisions.

Receiving the CTS after a SIFS period, the STA transmits its frame just like in basic DCF.

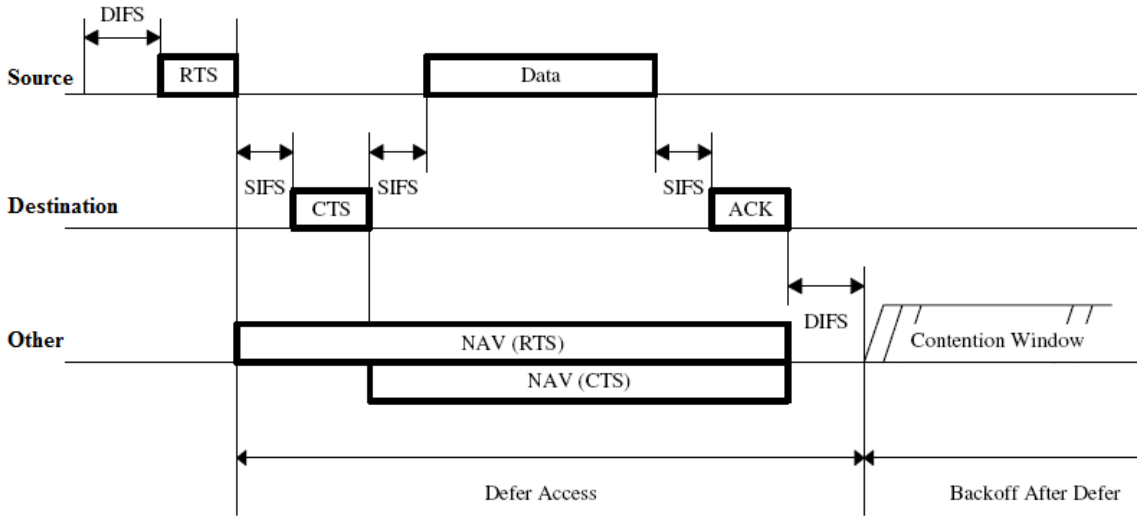

Figure 10 - DCF RTS/CTS

3.2.2. Point Coordination Function

The Point Coordination Function (PCF) provides contention-free (CF) services. Special stations called Point Coordinators (PC) are used to ensure that the medium is provided without contention. The PC resides in Access Points (AP), so the PCF is restricted to infrastructure networks. To gain priority over standard contention-based services, the PCF allows stations to transmit frames after a shorter interval [1][3][6][7].

The PC divides the access time into periodic intervals named beacon intervals that have a Contention-Free Period (CFP) (PCF mode) and a Contention Period (CP) (DCF mode), as depicted on Figure 11. During the CFP, the PC maintains a list of the registered STAs and polls each STA according to its list. The polled STA has permission to transmit its frame.

After listening to the medium for a PIFS period the PC begins the CFP by sending a Beacon signal containing the next Target Beacon Transmission Time (TBTT) and broadcasts it to all the other STA in the BSS. Beacon frames are used to maintain the synchronization of the local timers in the stations and to deliver protocol-related parameters. Since the PIFS is smaller than DIFS, no STA can start sending data in the DCF mode before the PC. Then all STA set their NAV value to the $CFP_{maxduration}$.

When it is time for an STA to transmit, the PC polls the STA and it can piggyback the data frames to the STA together with the CF-Poll. After a SIFS interval the STA sends back a data frame (if is the case) piggybacked with an ACK. When the PC polls the next STA in its list, not only it piggybacks the data frame with the CF-Poll but also with the previous ACK. If the polled STA does not answer to the PC after a PIFS period it is removed from the polling list and another STA is polled. The removed STA can be polled again at the beginning of the next CFP. At any time the PC can terminate the CFP by sending a PCF-End packet.

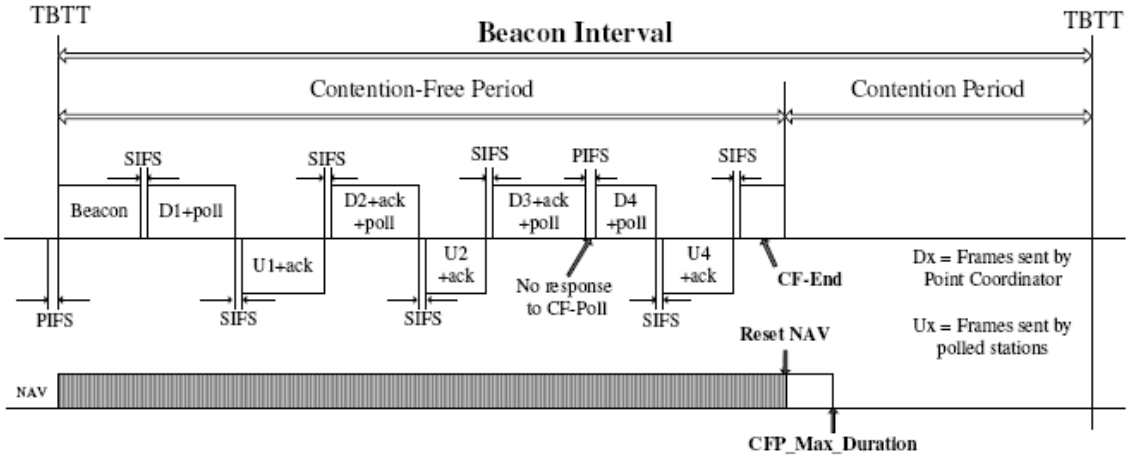

Figure 11 - PCF and DCF cycles

3.2.3. Fragmentation

In order to diminish the error probability due to signal weakness or noise, larger frames can be fragmented into smaller frames. The IEEE 802.11 standard mandates that all receivers have fragmentation support by reassembling the frames but leaves as optional in the senders [1].

Large MAC Protocol Data Units (MPDUs) and MAC Service Data Units (MSDUs) are compared to the Fragmentation_Threshold. If MPDU exceeds that value the MSDU is broken into multiple fragments. The resulting MPDUs are transmitted sequentially and the channel is not released until

the complete MSDU has been transmitted successfully. Each fragment is sent SIFS seconds after receiving an ACK from the previous fragment, as depicted in Figure 12. When the ACK is not received the source STA stops the transmission and frees the channel.

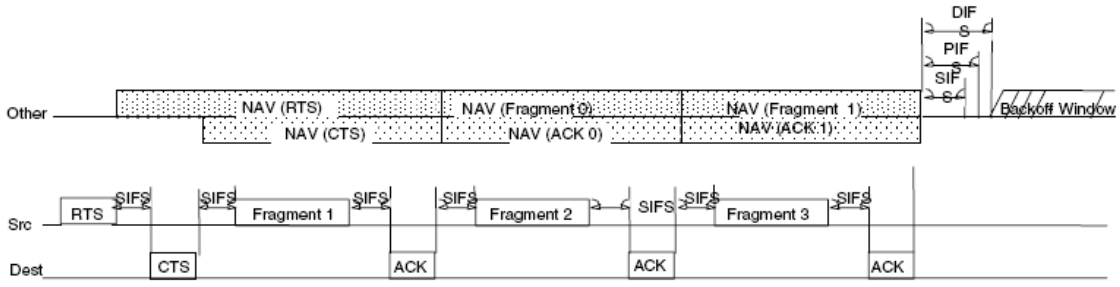

Figure 12 - Transmission of fragmented MPDU

3.2.4. Scanning, Authentication and Association

When activated the STA must perform 3 steps before being able to use the network to communicate with other hosts: scanning, authentication and association.

In the scanning step, the 802.11 standard defines both passive and active scanning [1][3][6][7]. Passive scanning is mandatory where each STA scans individual channels to find the best AP signal. Periodically, AP broadcast a beacon containing information about the AP, including Service Set Identifier (SSID), supported data rates, etc. The STA can use this information along with the signal strength to compare access points and decide upon which one to use. Optional active scanning is similar, except that the STA initiates the process by broadcasting a probe frame and all APs within range respond with a probe response.

Authentication is the process of proving identity, and the 802.11 standard specifies two forms: Open system authentication and shared key authentication [1][3][6][7]. Open system authentication is mandatory. The STA first sends an authentication request frame to the AP that replies with an authentication response frame containing approval or disapproval of authentication. Shared key authentication is an optional process that bases authentication on whether the authenticating device has the correct Wired Equivalent Privacy (WEP) key. The STA starts by sending an authentication request frame to the AP. The AP then places a challenge text into the frame body of a response frame and sends it to the STA. The STA uses its WEP key to encrypt the challenge text and then sends it back to the AP in another authentication frame. The AP decrypts the challenge text and compares it to the initial text. If the text is equivalent, then the AP assumes that the radio NIC has the correct key. The AP finishes the sequence by sending an authentication frame to the radio NIC with the approval or disapproval.

Once authenticated, the STA must associate with the AP before sending data frames [1]. The STA initiates the association by sending an association request frame containing elements such as SSID and supported data rates. The AP responds by sending an association response frame containing an association ID along with other information regarding the access point. Once the STA and AP complete the association process, they can send data frames to each other.

3.2.5. Roaming

The IEEE 802.11 standard [2] also allows for the STA to roam between different AP without loss of connectivity to the backbone, either in the same or different channel. When a STA moves from one AP to another, a Re-Association to the "new" AP is executed to assure that the STA maintains connection to the network. In this way the "new" AP will know about the arrival of the STA. The "old" AP (from where the STA roamed from) needs to be informed about this event, so that it will not send traffic to the STA. The "old" AP can be informed in two different ways:

- Passive - The STA initiates traffic that is received by the "old" AP on a different port (the Ethernet port for instance), than where the "old" AP expected it (i.e. the wireless port). As a result the "old" AP will update its bridge tables.
- Active - The "new" AP will inform the "old" AP that the STA has reassociated.

3.2.6. Power Management

The optional power save mode enables the STA to preserve battery power when there is no need to send data [1]. With power save mode on, the STA indicates its desire to enter into the "sleep" state to the AP. The access point takes note of each STA wishing to enter in the power save mode, and buffers packets corresponding to the sleeping station.

In order to still receive data frames, the sleeping STA must wake up periodically to receive regular beacon transmissions coming from the AP. After receiving the frames, the STA can go back to sleep.

3.3. IEEE 802.11 PHY Layer

The IEEE 802.11 standard [2] initially defined three Physical (PHY) Layer implementations: Frequency Hopping Spread Spectrum (FHSS), Direct Sequence Spread Spectrum (DSSS) an Infrared (IR) [7], offering a data rate between 1 and 2 Mbps. All three PHY layers included the provision of Clear Channel Assessment (CCA) used by the MAC layer to indicate if the medium is idle.

3.3.1. DSSS in IEEE 802.11

DSS in IEEE 802.11 uses Differential Binary Phase Shift Keying (DBPSK) and Differential Quadrature Phase Shift Keying (DQPSK) modulation for 1 and 2 Mbps data rates [1][8].

The carrier frequency in an IEEE 802.11 DSS transmitter is spread by an 11-b Barker code. The chipping rate is 11 MHz for a 1 Mbps data rate and 22 MHz for a 2 Mbps data rate. As depicted in Figure 13, the main lobe spacing is twice the chip rate and each side lobe is the chip rate. The spreading of the data is achieved by modulating the data with a Pseudorandom Number (PN) sequence of binary values called a PN code.

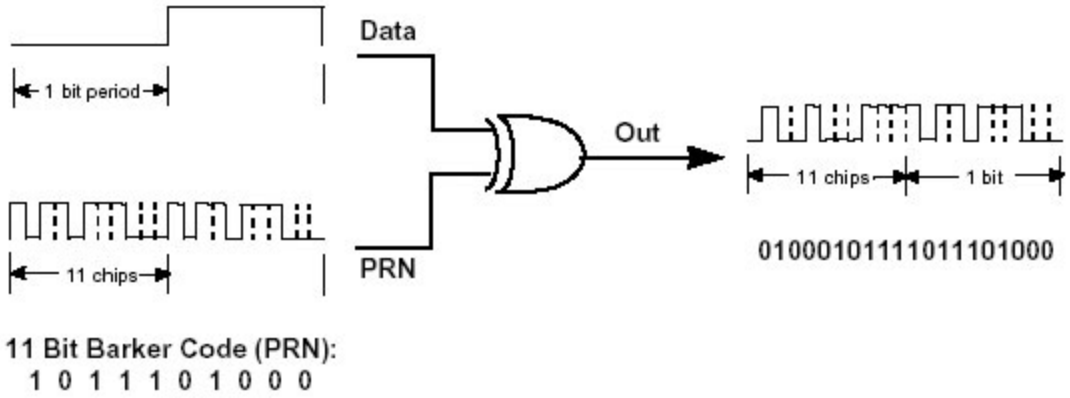

Figure 13 - DSSS Spreading

The DSSS receiver will filter the side lobes, down-convert the main lobe spectral component to baseband and use a copy of the PN code on a correlator circuit to recover the transmitted signal.

3.3.2. IEEE 802.11b

The IEEE 802.11b standard [9] is the most popular and widely implemented of the 802.11 family standards, for reasons including its early availability and the price of supported products [1][4][5].

802.11b is a physical layer standard that specifies operation in the 2.4 GHz industrial, scientific, and medical (ISM) unlicensed frequency band, using the direct-sequence spread spectrum (DSSS) modulation technique.

The number of channels the 2.4 GHz spectrum provides varies in different countries according to local regulatory restrictions. In most of European countries there are 13 available channels, as depicted in Figure 14. The channels overlap one another, since the centers of adjacent channels are separated by only 5 MHz. As a result, only three of the channels in the 2.4 GHz band are non-overlapping. Devices that use overlapping channels within range of each other will tend to interfere with one another's operation. Interference problems are avoided only by configuring adjacent Access Points (AP) to operate on non-overlapping channels. Interference that can affect

802.11b devices include microwave ovens, cordless phones, Bluetooth devices, wireless headsets, garage door openers, and other appliances – all of which use the same limited 2.4 GHz range.

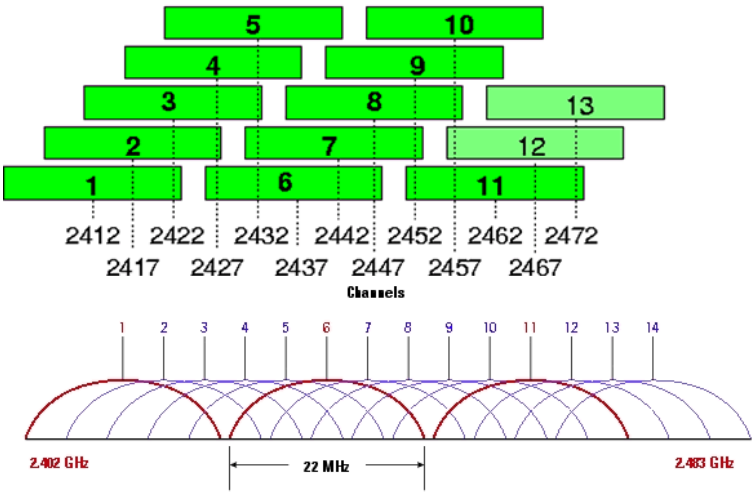

Figure 14 - IEEE 802.11b Channel Assignment for Europe

The 802.11b standard defines a maximum data rate of 11 Mbps using a Complementary Code Keying (CCK) on the DSSS, which provides a realistic maximum usable throughput of about 4-6 Mbps under normal conditions.

3.3.3. IEEE 802.11g

The IEEE 802.11g standard [9] is a direct extension of 802.11b that extends the maximum data rate (signaling speed) to 54 Mbps, making it possible to serve up to five times as many users [1][4][5].

The higher signaling speed is made possible by using a more efficient means of transmission called Orthogonal Frequency Division Multiplexing (OFDM). OFDM breaks a wide-frequency channel into several sub-channels and transmits the data in parallel. 802.11g provides a realistic maximum throughput of about 20 Mbps in normal conditions. The 802.11g standard can scale back to support data rates of 48, 36, 24, 18, 12, and 9 Mbps.

Because 802.11g operates at the same frequency - 2.4 GHz - as 802.11b, devices are subject to the same limitations: only three non-overlapping channels and interference from unlicensed, non-protocol equipment.

On the positive side, using the same 2.4 GHz frequency means that 802.11g devices are backward-compatible with 802.11b access points and other devices that enterprises may already have. However, different modulation techniques prevent 802.11b and 802.11g devices from coordinating with one another to prevent collisions when using the same shared frequency. Thus the presence of an 802.11b station within range of an 802.11g AP forces the AP to invoke a

Request to Send/Clear to Send (RTS/CTS) protection mechanism. This protected mode prevents simultaneous transmission by devices using 802.11g and 802.11b (which would result in collisions and retransmissions), but it significantly reduces the throughput of the overall wireless network. In protected mode, the access point drops down to 802.11b speeds to alert the 802.11b station that an 802.11g transmission is taking control of the media. To serve the 802.11b station, the access point must use DSSS modulation (rather than OFDM), and is thus limited to the lower data rates. Running in protected mode is required by standards whenever an 802.11b station is present.

3.3.4. IEEE 802.11a

The IEEE 802.11a standard [10] provides the same 54 Mbps maximum data rate as 802.11g [1][4][5]. But unlike 802.11b and 802.11g, the 802.11a standard operates in the 5 GHz ISM band. This means that 802.11a devices are not subject to interference that affects 802.11g and 802.11b devices, but they are still subject to interference from other products designed to use this 5 GHz ISM band.

The 5 GHz band allocates up to 19 non-overlapping channels depending on local regulations. The higher data rate, coupled with more non-overlapping channels, enables greater density deployments (more access points within a given area) to accommodate more users and provide greater capacity.

With its high throughput and lower range, 802.11a is ideally suited for provisioning connectivity to densely populated user environments such as computer labs, classrooms, large conference rooms, airports or convention centers.

Because 802.11a operates in the 5 GHz band, its signal range is somewhat more limited than that of 802.11b/g, which operates at 2.4 GHz. The shorter wavelength radio signals have more difficulty crossing walls and other obstructions. As a result, more access points are typically required to cover a given area.

Without backward compatibility for the installed base of predominately 2.4 GHz-based wireless clients, 802.11a, by itself, never gained mass adoption in the business or home wireless networks. With the overall rapid industry growth of wireless and the technology advances that followed, today most mobile devices such as notebooks support both 802.11b/g and 802.11a.

3.4. Quality of Service: IEEE 802.11e

Both DCF and PCF mechanisms treat data flows the same way, i.e., all data flows have the same access priority to the medium since the legacy 802.11 MAC protocol has no way to differentiate them.

In order to support traffic differentiation for services with requirements in bandwidth, delay, jitter and packet loss, such as voice and video, IEEE 802.11e [11] introduces three main enhancements: Hybrid Coordination Function (HFC), Direct Link Protocol (DLP) and block acknowledgment [3][6].

3.4.1. Hybrid Coordination Function

The Hybrid Coordination Function (HCF) combines both DCF and PCF with enhanced QoS mechanisms to enable QoS data transfers in both CP and CFP, using a uniform set of frame exchange sequences. HCF uses two mechanisms: a contention-based channel access method, called Enhanced Distributed Channel Access (EDCA), and a controlled channel access, called HCF-Controlled Channel Access (HCCA).

3.4.1.1. Enhanced Distributed Channel Access

The Enhanced Distributed Channel Access (EDCA) provides differentiated and distributed access to the Wireless Medium (WM) for QoS-Enhanced Stations (QSTAs). The EDCA defines for each QSTA four Access Categories (ACs) that support eight User Priorities (UPs), as defined in IEEE 802.1D [**12**], as seen in Table 1. One or more UP are assigned per AC, as depicted in Figure 15.

Priority	User Priority (UP - Same as 802.1D UP)	802.1D Designation	802.11e Access Category (AC)	Service Type
Lowest	1	Background (BK)	0	Background
	2	-	0	Background
	0	Best Effort (BE)	1	Best Effort
	3	Excellent Effort (EE)	1	Best Effort
	4	Controlled Load (CL)	2	Video
	5	VI (Video < 100ms latency and jitter)	2	Video
	6	VO (Voice < 10ms latency and jitter)	3	Voice
Highest	7	Network Control	3	Voice

Table 1 - Mapping between IEEE 802.1D and AC

Each AC is an enhanced variation of the DCF and contends for Transmission Opportunity (TXOP), which is a time interval giving the right to a particular QSTA to transmit its data to the WM. The TXOP can be obtained by the QSTA in two ways: by winning a successful EDCA contention (EDCA-TXOP) or by receiving a QoS CF-poll frame from the QAP (polled-TXOP). The duration of the TXOP is limited to a value given by $TXOP_{limit}$, allowing control of the maximum time a QSTA allocates the medium for MPDU delivery.

In the event that two or more backoff timers from parallel AC reach zero at the same time, a scheduler inside the QSTA will avoid collisions by guarantying EDCA-TXOP to the highest priority AC. In the case of a collision the colliding ACs enter a backoff process and double their CW sizes.

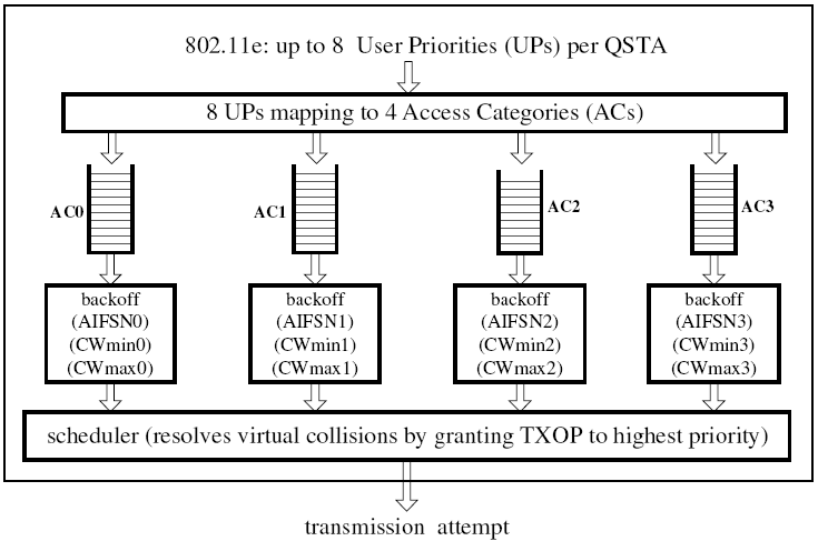

Figure 15 - EDCA proposed by IEEE 802.11e

In order to support service differentiation, the EDCA introduces two methods to prioritize medium access: the use of an Arbitration IFS (AIFS) and allocating different CW sizes for different AC. Figure 16shows the time frame of the EDCA scheme.

Instead of DIFS, a new kind of IFS is used in the EDCA, the Arbitration IFS (AIFS), determined by:

$$AIFS\ [AC] = AIFSN\ [AC] * SlotTime + SIFS,$$

where the default value of the Arbitration IFS Number (AIFSN) is defined as either 1, for high priority, or 2, for low priority [11]. When AIFSN = 1, high priority AC queues have AIFS value equal to PIFS, while when AIFSN = 2, low priority AC queues have AIFS value equal to DIFS. This way, when the medium is idle for longer than AIFS [AC] + SlotTime a packet that arrives at an empty AC queue is immediately transmitted.

By allocating different CW sizes for different AC, short CW are assigned to high priority AC and long CW are assigned to low priority AC, ensuring that that high priority AC can transmit packets ahead of low priority AC.

Data frames are now delivered through multiple backoff instances within the one QSTA, each with the parameter of the Traffic Stream (TS). The backoff interval is now a random number drawn by the interval [1, CW [AC] + 1] [1].

In order to improve throughput, when as QSTA gains an EDCA-TXOP it can send multiple packets without contending for the medium again, as long as the total access time does not exceed $TXOP_{limit}$, following the completion of a frame exchange sequence, such as an ACK frame. A SIFS interval is used between packet bursts to ensure that no other QSTA interrupts the burst since if a collision occurs the bursting is terminated. The $TXOP_{limit}$ duration values are advertised by the QAP in the EDCA Parameter Set Information Element in Beacon frames. A $TXOP_{limit}$ value of 0 indicates

that a single MPDU may be transmitted for each TXOP. This is also referred to as Contention Free Burst (CFB).

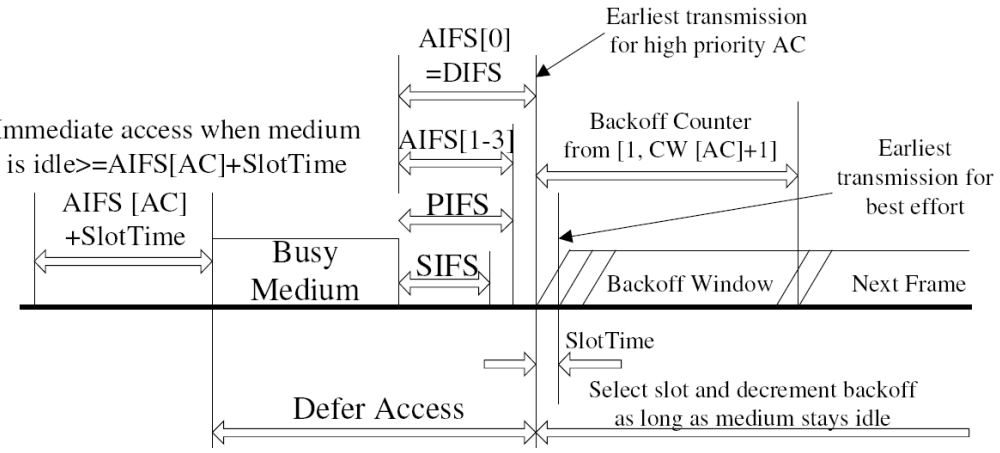

Figure 16 - EDCA IFS Channel Access

3.4.1.2. HCF-Controlled Channel Access

The HCF-Controlled Channel Access (HCCA) mechanism is designed for the parameterized QoS support by combining the advantages of PCF and DCF. HCCA uses a QoS-aware centralized coordinator, called a Hybrid Coordinator (HC), collocated in the QSTA of the QoS-Supporting BSS (QBSS), using its higher priority access to the WM to initiate frame exchange sequences and to allocate TXOPs to itself and other QSTAs.

During the Contention Period (CP) a new Contention Free Period (CFP) is introduced during which frames are transmitted using HCCA mechanism, called Controlled Access Phase (CAP). As depicted in Figure 17, during CP, each TXOP begins either when the medium is determined to be available under the EDCA rules, i.e., after AIFS + backoff time, or when the station receives a special poll frame, the QoS CF-Poll, from the HC, starting the CAP. The QoS CF-Poll from the HC can be sent after a PIFS idle period without any backoff, allowing the HC to issue polled TXOPs in the CP using its prioritized medium access. During the CFP, the starting time and maximum duration of each TXOP is specified by the HC, again using the QoS CF-Poll frames. Stations will not attempt to get medium access on its own during the CFP, so only the HC can grant TXOPs by sending QoS CF-Poll frames. The CFP ends after the time announced in the beacon frame or by a CF-End frame from the HC.

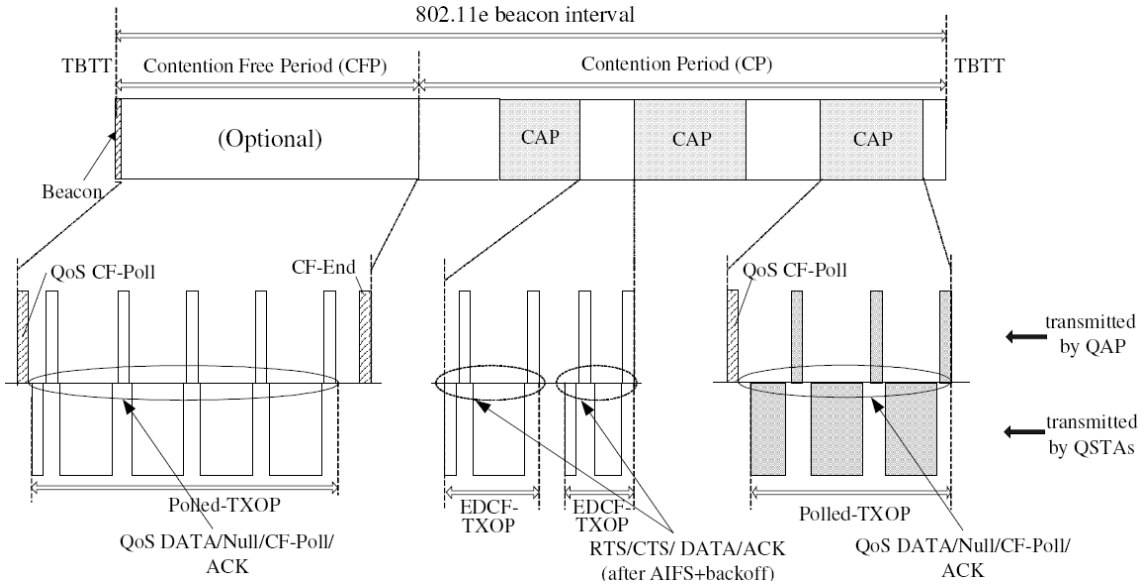

Figure 17 - IEEE 802.11e Beacon Interval

In HCCA mechanism the HC polls stations for MSDU Delivery. For this, the HC requires information that has to be updated by the polled stations from time to time. Thus, QoS guarantee is based on the Traffic Specification (TSPEC) negotiation between the QAP and the QSTAs, that include mean data rate, nominal frame size, maximum service delay, delay bound, etc.... Based on these TSPECs parameters, the QAP scheduler computes the duration of polled-TXOP for each QSTA. The scheduler on each QSTA then allocates the TXOP for different Traffic Streams (TS) according to the priority order. When TS is set up, the QAP attempts to provide QoS by allocating the required bandwidth to the TS during a CFP or a CP after a PIFS idle time. All other STAs use the $TXOP_{limit}$ plus a SlotTime to set their NAVs until the end of the controlled contention period. For fast collision resolution, the HC acknowledges the reception of request by generating a control frame with a feedback field so that the requesting stations can detect collisions during controlled contention.

3.4.1.3. Priority Parameters in MAC Service Primitives

As a frame arrives at the MAC layer it is tagged with a Traffic Identifier (TID) with a priority value relative to its QoS requirement between 0 and 15 [1].

When the priority parameter and the TID field value ranges from 0 to 7 the User Priority (UP) is given directly and mapped into four Access Categories (AC) queues using EDCA access rule.

When the priority parameter and the TID field ranges from 8 to 15 the UP is given indirectly through the Traffic Specifications (TSPECs) and mapped into 8 Traffic Streams (TS) using the HCCA rule. This way, outgoing MSDUs with priority values between 8 and 15 are handled by MAC entities at QSTAs in accordance with the UP value determined from EDCA rule as well as other parameter values in the selected TSPEC, allowing for a coordination of QoS priorities between IEEE 802.11e frames and Virtual LAN [15] (VLAN) frames, or with Differentiated Services [16] (DiffServ) policies [14].

3.4.2. Direct Link Protocol and Block Acknowledgement

In the legacy IEEE 802.11 standard [2] in order for an STA to communicate with another within the BSS all frames had to go through the AP, which can significantly increase the bandwidth consumption. With the implementation of the Direct Link Protocol (DLP), any QSTA can communicate directly with another QSTA within a QBSS without communicating through the QAP.

The optional Block Acknowledgment allows a QSTA to deliver and transmit a consecutive number of MSDUs as a block during one TXOP without individual ACK frames, improving the throughput efficiency of the protocol.

4. Wireless Mesh Networks

Wireless Mesh Networks (WMN) are multihop networks of wirelessly connected devices (nodes) such as access points, computers and router platforms, dynamically self-organized and self configured. The wireless nodes are typically stationary, but the clients can be mobile. A mesh network can provide multihop communication paths between wireless clients, serving as a community network or as a broadband access network for the Internet.

WMN are considered cost-effective alternatives to WLANs, as there is no need to deploy any wired infrastructure to support a mesh network. This is particularly attractive in developing countries and rural communities, where large-scale deployment of wired broadband infrastructure is not affordable. With the low cost of 802.11-based hardware platforms, wireless mesh networking is becoming an important technology with several industry players developing 802.11-based mesh networking platforms and services.

A Wireless Mesh Network (WMN) can be seen as a special type of wireless AD-HOC network [17][22]. Wireless ad-hoc networks are mainly networks without infrastructure, with high mobility and constant topology change, while WMNs have a relative static network configuration with most relay nodes fixed, having lower mobility than ad-hoc. Due to the static topology of WMNs, they offer better energy storage, removing the energy constraint from wireless ad-hoc networks.

Although wireless ad-hoc networks are very similar to WMNs, the protocols and architectures designed for wireless ad-hoc networks perform very poorly when applied in WMNs.

WMNs can operate in both single-radio and multi-radio topologies. On Single-Radio Wireless Mesh Networks (SR-WMNs), both access to the medium from STA and communication between Mesh AP (MAP) is done in the same shared channel. On a Multi-Radio Wireless Mesh Network (MR-WMN) different channels are used improving capacity, scalability, reliability, robustness, and architectural flexibility.

A WMN can be designed in three different architectures [19]:

. Client WMNs – the network is formed by client machines that are both hosts and routers, coordinating among themselves to provide routing, network configuration and service provisioning.

. Infrastructure/Backbone WMNs – the network has multiple hierarchical levels in which the client nodes are in the lowest level and they can communicate with the WMN backbone through MAP, which are responsible to maintain the backbone network.

. Hybrid WMNs – the WMN can use other networks for communication such as the Internet, Wi-Fi, WiMAX, cellular and sensor networks.

4.1. IEEE 802.11 WMN

The IEEE 802.11s standard [20] was created to extend the IEEE 802.11 architecture and protocol for providing the functionality of an Extended Service Set (ESS) Mesh (i.e., access points capable of establishing wireless links among each other to enable automatic topology learning and dynamic path configuration), by creating an IEEE 802.11 wireless distribution system that supports both broadcast/multicast and unicast delivery at the MAC layer using radio-aware metrics over self-configuring multihop topologies.

The IEEE 802.11s standard defines a mesh network as two or more nodes that are connected via IEEE 802.11 links that communicate through mesh services and comprise an IEEE 802.11-based Wireless Distribution System (WDS) [18][21]. Any node that supports the mesh services of control, management, and operation of the mesh is a Mesh Point (MP). If the node additionally supports access to client stations (STAs) or non-mesh nodes, it is called a Mesh Access Point (MAP). A Mesh Portal (MPP) is an MP that has a non-802.11 connection to the Internet and serves as an entry point for MAC Service Data Units (MSDUs) to enter or exit the mesh, as depicted in Figure 18. A mesh network can have one operating channel or multiple operating channels. A Unified Channel Graph (UCG) is a set of nodes that are interconnected on the same channel within a mesh network.

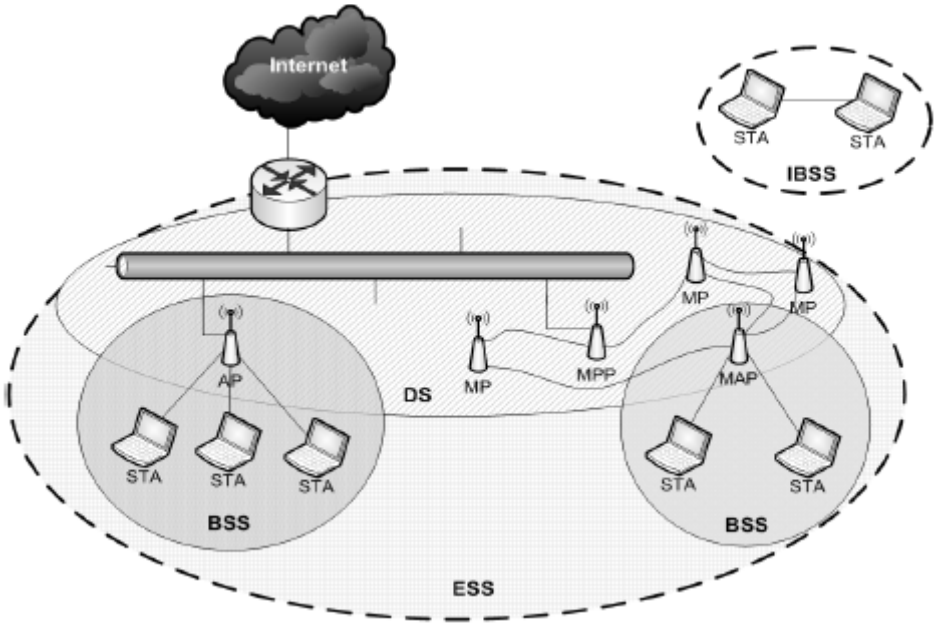

Figure 18 - IEEE 802.11s Architecture

4.1.1. Backhaul Channel Selection [18]

After initialization, a node uses the Simple Channel Unification Protocol where the MP performs active or passive scanning of the neighbors. If no neighboring MPs are found, the MP can establish

itself as the initiator of a mesh network by adopting a mesh ID from one of its profiles and selecting a channel precedence value based upon the boot time of the mesh point plus a random number. If two disjoint mesh networks are discovered (i.e., they are on different channels), the channel is chosen according to the highest precedence value. If the mesh is in the 5 GHz band, the mesh is required to conform to the regulatory requirements of the Dynamic Frequency Selection (DFS) and radar avoidance.

4.1.2. Interworking

Mesh Portals (MPP) bridge the wireless and wired networks by sending a MPP announcement information element in management frames [21]. MPPs function as if on a single loop-free logical layer 2 and interconnected layer 3 for both the internal mesh and the external LAN segments. For layer 2, the MPPs use the IEEE 802.1D bridging standard, and at layer 3, routing must be performed in a similar fashion to IP gateway routers.

4.1.3. Topology Formation and Discovery

Mesh Points (MPs) that are not yet members of the WMN must first perform neighbor discovery to connect to the network. A node scans neighboring nodes for beacons which contain at least one matching profile, consisting of a mesh ID, path selection protocol identifier, and link metric identifier. The purpose of the local link-state discovery procedure is to identify the r (current bit rate) and e_{pt} (packet error rate at current bit rate) to determine the most efficient available routes [18]. If the beacon contains a mesh capacity element that contains a nonzero peer link value (r and e_{pt}) then the link can be established through a secure protocol.

4.1.4. Routing in the MAC Layer [18][21]

Mesh traffic is predominantly forwarded to and from wired line gateway nodes forming a logical tree structure. The mandatory Hybrid Wireless Mesh Protocol (HWMP) within the IEEE 802.11s standard [20] uses an on-demand routing protocol to address mobility and hierarchical routing to exploit this tree-like logical structure. The on-demand routing protocol is based upon Ad Hoc On-Demand Distance Vector routing (AODV) which uses a simple hop count routing metric [24]. The draft standard also defines an optional Radio Aware-Optimized Link State Routing (RA-OLSR) that uses multipoint relays, a subset of nodes that flood a radio aware link metric, thereby, reducing control overhead of the routing protocol.

4.1.4.1. Hybrid Wireless Mesh Protocol

Hybrid Wireless Mesh Protocol (HWMP) is the mandatory routing protocol of the IEEE 802.11s draft standard, used to provide both on-demand routing for predominantly mobile topologies and proactive tree-based routing for predominantly fixed infrastructure networks. The hybrid protocol is used in the case that an MP does not have an on-demand route to another MP and sends the first packet to the root. Subsequent packets can be sent along a shorter path that is found directly.

4.1.4.1.1. Tree-Based Routing in HWMP

When a Mesh Portal (MPP) exists within the WMN and is optionally configured as a root node, the network can use proactive, distance vector routing through the root to find and maintain routes. The root announcement is broadcast by the root MPP with a sequence number assigned to each broadcast round. Each node updates the metric as the announcements are received and rebroadcasted. The MP chooses the best parent and caches other potential parents. Periodic Route Requests (RREQs) are sent to parents to maintain the path to the root. If the connection to the parent is lost (3 consecutive RREQs), the MP will notify its children, find a new parent, and send a gratuitous Route Response (RREP) to the root, which all intermediate nodes use to update their next-hop information about the source.

4.1.4.1.2. On-Demand Routing in HWMP

With the on-demand routing protocol, the network is not required to use routes through the root node (or even have a root node). IEEE 802.11s MPs use a RREQ and RREP mechanism to discover link metric information from source to destination. To maintain the route, nodes send periodic RREQs during a refresh-round, which is the time between two different RREQs transmitted at the same source. Sequence numbers are used per refresh-round to ensure loop-free operation.

When a MP receives a RREQ it creates a route to the source or updates its current route if the RREQ contains a greater sequence number, or the sequence number is the same as the current route and the RREQ offers a better metric than the current route. If a new route is created or an existing route modified, the RREQ is also forwarded.

Intermediate MPs create a route to the destination on receiving the RREP, and also forward the RREP toward the source. When the source receives the RREP, it creates a route to the destination. If the destination receives further RREQs with a better metric, then the destination updates its route to the source to the new route and also sends a fresh RREP to the source along the updated route. Thus a bidirectional, best metric end-to-end route is established between the source and destination.

4.1.4.2. Radio-Aware Optimized Link-State Routing Protocol

The Radio-Aware Optimized Link-State Routing (RA-OLSR) protocol is a proactive link state routing protocol based on the original OLSR [25] protocol, with several extensions included. RA-OLSR enables the discovery and maintenance of optimal routes based on a predefined metric, as long as the MPs have mechanisms to determine the metric cost of a link to each of its neighbors, choosing the path with less cost. In order to propagate the metric information between MPs, a metric field is used in RA-OLSR control messages. In disseminating topology information over the network, RA-OLSR adopts the following approaches in order to reduce the related control overhead: it uses only a subset of MPs in the network, called multipoint relays (MPRs), in flooding process, and It can control (and thereby reduce) the message exchange frequencies by using periodic control message transmissions.

The Airtime Link Metric is used to calculate the cost of each airtime link within the mesh network in order to choose the best link, and is defined to be the amount of channel resources consumed by transmitting the frame over a particular link. The airtime cost C_a is defined in terms of the modulation rate r and bit error rate e_{pt} for a test frame of size B_t,

$$C_a = \left(O_{ca} + O_p + \frac{B_t}{r}\right) \times \left(\frac{1}{1 - e_{pt}}\right)$$

where the channel access overhead O_{ca}, protocol overhead O_p, and Bt are defined constants for each 802.11 modulation type, given in Table 2.

Parameter	802.11a	802.11b	Description
O_{ca}	75 µs	335 µs	Channel access overhead
O_p	110 µs	364 µs	Protocol overhead
B_t	8224	8224	Number of bits in test frame

Table 2 - Airtime Link Contants

This way, the routing algorithm computes the initial routes for each node pair given a set of node pairs and the expected traffic load between each node pair. The radio channel assignment algorithm assigns a radio channel to each interface such that the available bandwidth at each virtual link is no less than its expected load. The new channel assignment is fed back to the routing algorithm to reach more informed routing decisions.

4.2. IEEE 802.11s MAC Layer

The basic operation of IEEE 802.11s MAC is the Enhanced Distributed Channel Access (EDCA). Due to multihop forwarding, flows of equivalent throughput but differing hop count from the gateway consume different amounts of network resources according to the distance from the portal node. The prioritization mechanism of EDCA does not work well for mesh networks in a multihop mesh environment, thus several enhancements were made to the 802.11 MAC.

4.2.1. Beaconing and Synchronization

In this optional feature of the IEEE 802.11s draft standard, beaconing or probing procedures similar to the original Timing Synchronization Function (TSF) of the original IEEE 802.11 standard [2] are used for synchronizing and unsynchronizing MPs.

Synchronization is an optional feature for MPs. With synchronization, each MP updates its timers with a time stamp and offset information received in beacons and probe responses from other MPs, thereby maintaining a common Mesh TSF time. The self time stamp from the perspective of the receiving MP is in terms of the received time stamp plus received offset minus the receiver offset. Otherwise, synchronizing MPs may choose to update their offsets instead of the timers. The

new self offset value is updated when the received time stamp plus received offset is greater than the self time stamp plus the self offset. Some MPs, however, choose to be unsynchronized if communicating with the other MPs do not need synchronization.

MPs implementing mesh beaconing may adjust their TSF timers, using the Mesh Beacon Collision Avoidance Protocol, to reduce the chances of transmitting beacons at the same time as their neighbors.

4.2.2. Multichannel MAC Operation

The IEEE 802.11s draft standard implements a Common Channel Framework (CCF) that enables the operation of both single and multi-radio devices in a multichannel environment. Using a multichannel MAC, where transmissions can take place simultaneously on orthogonal channels, the aggregate throughput can be increased considerably. This is a dynamic channel allocation scheme.

As depicted in Figure 19, the destination channel information (channel n) is exchanged using the RTX and CTX frames, followed by data transmission on the same channel. While the data frame is being transmitted, another transmission can be initiated on a parallel channel m.

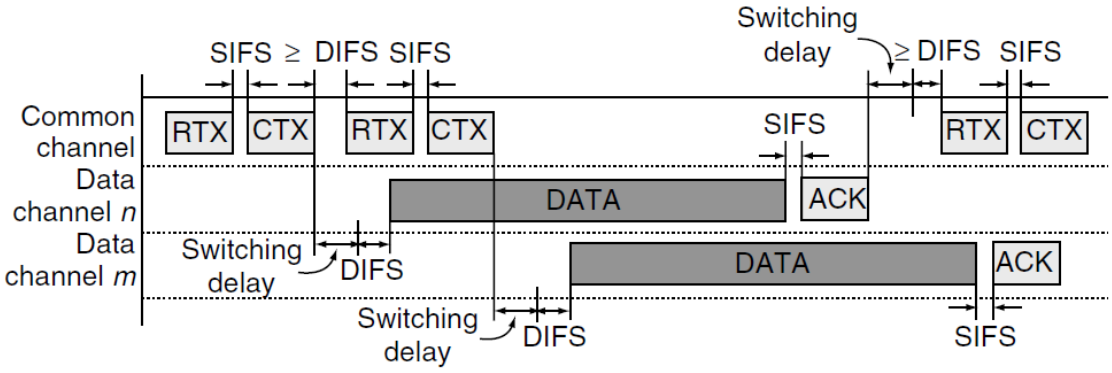

Figure 19 - Common Channel Framework

A Channel Coordination Window (CCW) is available in CCF to enable arbitrary MPs to establish communication with each other by tuning to the common channel at the start of CCW. CCW is repeated with a period P and has duration of a fraction of P. A channel coordination mechanism is used with the help of a Common Control Channel (CCC).

4.2.3. Mesh Deterministic Access

The Mesh Deterministic Access (MDA) mechanism allows supporting MPs to access the channel during a certain period, called Mesh Deterministic Access Opportunity (MDAOP), with lower contention than otherwise in selected times. MDA sets up MDAOPs in mesh neighborhoods in which a number of MDA-supporting MPs are set not to initiate any transmission sequences when

there's a possibility of interference between their transmissions. During that time period, synchronized MPs that set up the state for the use of these time periods are allowed to access the channel.

A map of neighborhood MDAOP times is build into a mesh Delivery Traffic Indication Map (DTIM) prior to transmitting the MDAOP request message, which includes the MDAOP neighborhood times and neighbor MDAOP interfering times of all neighbor peer Mesh Points (MPs). MPs that set up MDAOPs access the medium by using the MDA access parameters CWMin, CWMax, and AIFSN within these periods.

The MP that intends to be the transmitter in a new MDAOP set builds a map of neighborhood MDAOP times in the Mesh DTIM interval after hearing advertisements from all of its neighbors that have MDA active. The transmitter then chooses the MDAOP starting point and duration in the Mesh DTIM interval that does not overlap with either its neighborhood MDAOP times or the neighbor MDAOP interfering times of the intended receiver. The transmitter then verifies that the new MDAOP set will not cause the Mesh Access Fraction (MAF) limit to be crossed for any of its neighbors and, if the MAF is not crossed, it transmits an MDAOP setup request Information Element (IE) to the intended receiver with the chosen MDAOP location and duration. The receiver of the MDAOP setup request IE checks to see if the proposed MDAOP times have any overlap with its neighborhood MDAOP times or if it will cause the MAF limit to be crossed for any of its neighbors. If suitable, the receiver accepts the setup. After successful setup, both the MDAOP owner (the transmitter) and the receiver advertise the MDAOP set times in the transmit-receive (TX-RX) times report field of the MDAOP advertisement IE.

After the MDAOP is set up, the MDAOP owner uses CSMA/CA and backoff to obtain a TXOP using the MDA-CWmin, MDA-CWmax, and MDA-IFSN parameters. The range of values of the parameters is identical to those used in EDCA. Except the MDAOP owner, all other MPs should not initiate transmissions during the TXOP initiated in the MDAOP.

4.2.4. Intra-Mesh Congestion Control

Neither 802.11 DCF nor 802.11e EDCA provides any QoS over a multihop WLAN network. Each MP contends for the channel independently, without any regard for what is happening in the upstream or downstream nodes. One of the consequences is that a sender with backlogged traffic may rapidly inject many packets into the network, which would result in local congestion of nodes downstream, thereby deteriorating QoS of downstream nodes.

To effectively control or avoid congestion in the network, each mesh node monitors its local/neighborhood congestion condition so that, when necessary, it can notify the neighborhood/upstream nodes of congestion by transmitting a broadcast ''neighborhood congestion announcement'' and/or a unicast ''congestion control request.'' The standard does not mandate how to monitor and detect the congestion situation and it is up to the implementers to decide what scheme should be used. Two different monitoring and congestion detection mechanisms are provided as example implementations by the standard:

- Monitor the backpressure of the network, which is the difference between the aggregate receive and transmit rates. When the backpressure builds up significantly at the local node, the node informs its previous hop nodes or neighbors so that the recipient nodes can decrease their transmission rate according to a local rate control mechanism. Upon receiving either congestion control request or neighborhood congestion announcement message, the receiving node needs to reduce its effective MAC transmission rate, accordingly, by locally rate limiting its traffic.
- The other suggested method for congestion detection is based on queue size. If the queue size is above a predefined upper threshold, the node informs its previous hop neighbors by sending unicast signaling messages ‘‘congestion control request messages’’ to each of its upstream nodes, so that the upstream nodes can decrease their transmission rate to it according to a local rate control mechanism.

4.3. IEEE 802.11s Hardware – Proxim’s Orinoco AP 4000-MR

The IEEE 802.11s equipment (Proxim Wireless Orinoco AP-4000MR) used in this work is compliant with the IEEE 802.11 standard and was acquired from Proxim Wireless for deployment of a fixed Wireless Mesh Network for both indoor and outdoor usage. It is comprised of three terminals in which the configuration dictates the Portal to the backbone. The antennas used for our tests were placed inside the Instituto de Telecomunicações building.

The Orinoco AP-4000MR features:

- ORiNOCO Mesh Creation Protocol (OMCP) enables mesh backhaul and Wi-Fi coverage on one radio, while the second radio is used exclusively for Wi-Fi coverage
- Industry-leading throughput with 802.11b/g and 802.11a simultaneous operation
- Robust RADIUS accounting and authorization interface enables detailed subscriber usage tracking
- WMM/802.11e draft Quality of Service (QoS) support on access and enhanced QoS on mesh backhaul for triple play applications
- Wi-Fi certified to interoperate with any Wi-Fi certified client access product
- Self-forming and self-healing ORiNOCO Mesh Creation Protocol automatically routes traffic through the best path as mesh access points are added or removed from the network

5. IEEE 802.16 for Real-Time IP Services: VoIP and VoD

The aim of the work reported in this chapter is the experimental investigation of WiMAX performance and its evaluation on a fixed WiMAX testbed acting as a VoIP and VoD streaming backhaul in Point-to-Point scenarios. The evaluation is conducted comparing network configurations with and without Quality of Service (QoS).

We employ multiple competing traffic sources over a point-to-point WiMAX topology and measure the capacity of our WiMAX equipment to handle a multitude of VoIP and VoD flows on both upstream and downstream, while handling multiple competing TCP flows.

We use Jugi's Traffic Generator (JTG) [29] to generate our UDP packets from VoIP and VoD emulated streams, IPERF [30] to generate multiple bi-directional TCP flows and a software-only implementation of the IEEE 1588 Precision Time Protocol (PTP) [31].

Section 5.1 describes the used methodology in our experiments. Section 5.2 describes the obtained performance measurements and their evaluation for VoIP and VoD services without QoS. Section 5.3 addresses the QoS case. Section 5.4 provides a final conclusion to the chapter.

5.1. Used Methodology

In order to conduct the experiments the work was divided into several phases, including the testbed configuration, clock synchronization and traffic generation.

5.1.1. Testbed Configuration

Our testbed is comprised of one PROXIM MP.16 3500 Base Station (BS) [28], one PROXIM MP.16 3500 Subscriber Station (SS) [28] and two computers, one connected to the BS (PC1) and the other to the SS (PC2). The two computers are used to act as traffic sources, generating and receiving both background TCP and emulated VoIP and VoD flows. Besides being connected through the WiMAX system, the two computers are also connected via their Ethernet cards through an Ethernet Hub for clock synchronization purposes.

The WiMAX BS and SS were installed on the roof of Instituto de Telecomunicações with a distance of 15 m from each other under line-of-sight (LOS) conditions. Given the distance between BS and SS, the equipments adapted the modulation scheme of 64 QAM (FEC: ¾) for both Uplink (UL) and Downlink (DL). They operate in the 3.5 GHz frequency band, with a 3.5 MHz channel bandwidth, and the transmission control scheme is TDD. Using a transmission power of 10 dBm, we measured a best value of Received Signal Strength Indicator (RSSI) at the SS of -15.7 dBm and a best value of Signal-to-Noise Ration (SNR) of 30.3 dB. All tests were performed with the WiMAX antennas on the outside where conditions were not ideal, due to weather and neighbor equipment

interference, allowing for a more realistic testing scenario. For this reason, it was not always possible to have the best RSSI and SNR values and, many times, we had to wait for conditions close to the previous described values to conduct the experiments.

The network was configured with Class C 192.168.10.0 IP addresses for the WiMAX system, and with Class A 10.240.2.0 IP addresses for the clock synchronization system (Figure 20 presents our experimental WiMAX testbed). The WiMAX BS and SS were set to a Download/Upload ratio of 50%/50%.

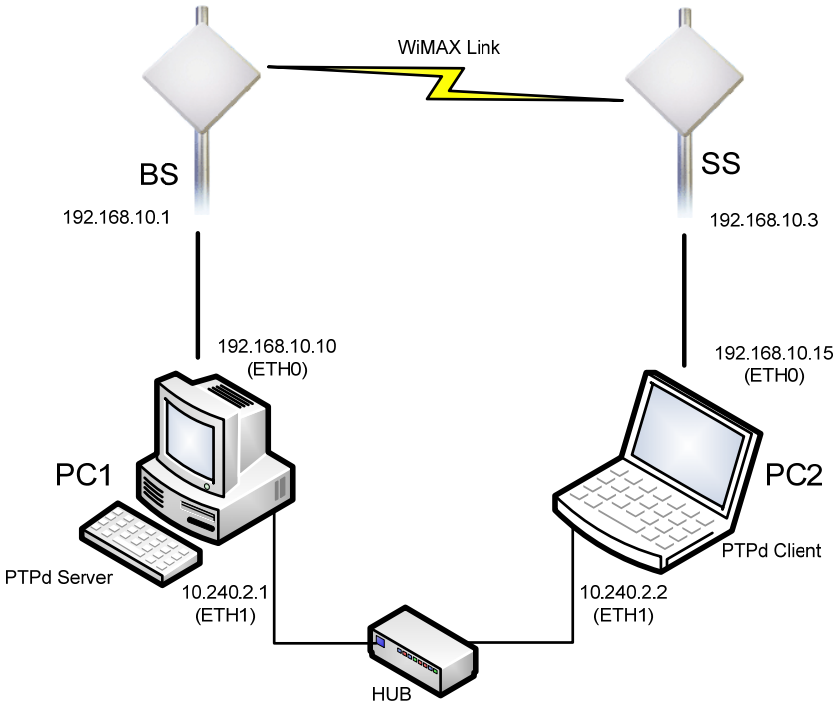

Figure 20 - WiMAX Testbed

5.1.2. Synchronizing with PTP

For high-precision one way delay measurements, accurate clock synchronization is necessary, taking care of both absolute time and clock drift at different hosts in the network. So, we decided to use the IEEE 1588 Precision Time Protocol (PTP) [31] to ensure clock LAN synchronization between the two computers. The PTP provides a means by which networked computer systems can agree on a master clock reference time, and a means by which slave clocks can estimate their offset from master clock time. PTP implementations typically have a clock servo that uses a series of time offset estimates to coordinate the local slave clock with the reference master clock time, a process referred to as clock discipline.

The PTP daemon (PTPd) [5] implements the Precision Time Protocol (PTP) as defined by the IEEE 1588 standard. PTPd was developed to provide very precise time coordination of LAN connected computers (PTPd is able to coordinate the clocks within tens of microseconds).

5.1.3. Measuring the maximum WiMAX link capacity

Before proceeding with any measurements and to define the amount of VoIP/VoD flows the network can sustain for our scenarios, we conducted baseline experiments using Iperf to determine the maximum throughput that can be obtained on the WiMAX link. We saturated the fixed WiMAX link with various different UDP sources with higher and higher bandwidth and obtained 4.68 Mbps on downlink and 4.62 Mbps on uplink.

5.1.4. Traffic Generation

To emulate our VoIP and VoD UDP traffic we have used JTG [2], an open source, simple and configurable network traffic generator. JTG does not include pre-build traffic models. However, traffic models can be easily defined with custom-made scripts. JTG allows us to generate different traffic patterns by setting transmission rates, packet sizes, by providing trace files for replaying traffic or defining arbitrary traffic patterns.

To emulate our TCP background traffic we have used IPERF [3]. It is a commonly used network testing tool that can create TCP data streams and measure the throughput of a network that is carrying them. Iperf allows the user to set various parameters that can be used for testing a network, or alternately for optimizing or tuning a network. Iperf uses a client-server model and can measure the throughput between the two ends, either unidirectionally or bi-directionally.

- **Emulating VoIP using JTG**

To evaluate WiMAX performance for VoIP services under network congestion, we generate 10 synthetic VoIP flows with source/sink pairs in the domain of both SS and BS. To model each VoIP flow, we have used the characteristics of Speex [34], an open source audio codec specially designed for VoIP applications over packet switching networks. We emulate 10 VoIP flows each with a 12.8 kbps based codec using JTG. For each flow, JTG generates 50 packets/s with a codec payload of 32 bytes, thus leading to an effective application bitrate of 17.6 Kbps (including RTP headers). At the IP level (after adding a total of 28 bytes of UDP and IP headers), each JTG instance generates 28.8 Kbps of total emulated Speex CBR traffic into the network.

- **Capturing and emulating VoD streaming traffic using JTG**

In order to emulate a set of video streams, we got access to 20 minutes of live video transmission captured from a music video TV channel and created a packet trace with Wireshark [35]. The captured stream was coded in H.264/AVC format (also known as MPEG-4) [36], with a bitrate of 512 Kbps (360x288, 25 f/s), and the accompanying audio stream was encoded in MPEG-1 Audio Layer II (also known as MP2) [37], with a bitrate of 192 Kbps, emphasizing audio quality over video

quality. The video was streamed with the use of VLC Media Player [33] and collected at the receiver side using Wireshark, recording very low delay and delay variance, with no RSTP [38] message exchange and no RTP [39] packet loss.

To study in a straightforward manner the performance of VoIP and VoD A/V over a congested fixed WiMAX link, two trace files were created based on the Wireshark trace: one for video and one for audio. The captured video stream has a Variable Bit Rate (VBR) with packets varying up to 1492 bytes. The captured audio stream has a Constant Bit Rate (CBR) with the total packet size fixed at 634 bytes (including RTP/UDP/IP/MAC headers).

Based on the trace files, we generate simultaneous video and audio streams using JTG [29].

5.1.5. Configuring QoS parameters

QoS configuration is needed only on Proxim's MP.16 3500 Base Station (BS) [40]. When a Subscriber Station (SS) enters the network an SS Class is associated with the SS, which contains all QoS specifications for that SS. Each SS Class can be assigned with multiple Service Flows (SF) which are managed by Packet Identification Rules (PIR).

The traffic's QoS treatment is done by SFs which specify the four QoS scheduling mechanism for uplink and downlink traffic and their parameters:

. Unsolicited Grant Services (UGS): maximum sustained data rate, maximum latency, and tolerable jitter.

. Real-Time Polling Services (rTPS): maximum sustained data rate, minimum reserved data rate, and maximum latency.

. Non-Real-Time Polling Services (nrTPS): maximum sustained data rate, minimum reserved traffic rate, and traffic priority.

. Best Effort (BE) Services: maximum sustained data rate and traffic priority.

The PIRs determine which packets are mapped to which service flow. A priority is used when assigning a PIR to a SF during SS Class creation, which is used to filter traffic, with higher priority PIRs being served first. The classification can be done by: IP Type of service (TOS), Ethernet Type, Ethernet Priority, VLAN ID, Source IP Address, Destination IP Address, IP Protocol, Source MAC Address and Destination MAC Address.

Given the available bandwidth on both uplink and downlink, we generate 10 VoIP and 5 VoD flows.

- **Configuring QoS parameters for VoIP**

We have created a PIR for VoIP QoS uplink and downlink traffic with two classifiers: Destination IP Port as 3000-3999, and IP protocol as 17 (UDP). We have also created a PIR for BE uplink and downlink traffic with no classifiers.

In order to configure our VoIP Service Flow (SF), we must first calculate the amount of "on wire" traffic of each VoIP flow. Thus, we have:

(12 bytes RTP Header) + (36 bytes RTP payload) + (28 bytes UDP/IP) + (18 bytes MAC Headers) = 90 bytes/packet

(90 bytes/packet) x (8 bit/byte) x (50 packet/second) = 36 Kpbs per VoIP flow

We have created two SFs for uplink and downlink traffic with UGS and BE scheduling type. We have defined in the UGS scheduling, a maximum sustained data rate of 360 Kbps (which can accommodate 10 VoIP flows), a maximum latency of 100 ms, and a tolerable jitter of 25 ms.

Now we have to create the SS class by selecting the SFs to be used and associating the PIRs to the respective SF. After the PIRs are associated with a SF, we classify SF priority by assigning a priority to the PIRs. The values range from 0-7.

- **Configuring QoS parameters for VoD**

We have created two PIRs for VoD QoS uplink and downlink traffic, one for audio and one for video. Audio has two classifiers: Destination IP Port as 4000-4999, and IP protocol as 17 (UDP). Video has two classifiers: Destination IP Port as 5000-5999, and IP protocol as 17 (UDP).

In order to configure our VoD Service Flow (SF), we must first calculate the amount of "on wire" traffic of each VoD flow. Thus, we have:

Video: (1492 bytes/packet) x (8 bit/packet) x (55 packets/second) = 646.48 Kbps

Audio: (634 bytes/packet) x (8 bit/packet) x (40 packets/second) = 202.88 Kbps

Total amount of "on wire" traffic: 849.36 Kbps

We then created a SF for uplink and downlink traffic for both audio and video with rTPS scheduling type. We defined for a maximum sustained data rate of 4250 Kbps (which can accommodate 5 VoD flows), minimum reserved data rate of 4250 Kbps, and maximum latency of 25 ms.

We created the SS class as before, but giving higher priority to audio over video.

- **Configuring QoS parameters for VoIP and VoD**

We have created a SS class with all three SFs (UGS, rTPS and BE) giving higher priority to VoIP than all other traffic, and higher priority for audio over video.

5.1.6. Steps of each experiment

For each conducted test, we have followed a set of steps which are described below:

- **Configure the targeted QoS strategy on WiMAX system**

We enter the BS configuration page and assign to the SS a pre-defined SS Class based on the experiment to conduct. After rebooting, the SS associates with the BS and receives the configured SS Class.

- **Starting PTPd**

We run the shell scripts using PTPd for both for server and client, and wait for 10 minutes to ensure clock synchronization before starting the tests.

- **Emulating traffic with IPERF**

After clock synchronization, we generate multiple bi-directional TCP flows and wait for 60 seconds to ensure the full utilization of the WiMAX link with background traffic.

- **Emulating traffic with JTG**

In order to test VoIP backhauling inside the WiMAX fixed wireless link, we generate 10 simultaneous unidirectional VoIP flows, yielding an application throughput of 360 Kbps. To test VoD backhauling capability, we generate 5 simultaneous unidirectional VoD flows (5 audio plus 5 video), yielding an application throughput of 4.25 Mbps. To test VoIP and VoD backhauling capability, we generate 10 simultaneous unidirectional VoIP flows and 5 simultaneous unidirectional VoD flows, yielding an application throughput of 4.61 Mbps. This is roughly the total available capacity of the uplink and almost all of the downlink. In this scenario, competing TCP flows have little available bandwidth. In all experiments, VoIP and/or VoD flows are generated with duration of 60 seconds.

5.2. VoIP and VoD services over WiMAX without QoS

In the first set of tests, the aim is to analyze the network performance of VoIP and VoD flows with competing background TCP flows when no QoS mechanism is configured on the WiMAX system. Given that our WiMAX system is a Time Division Duplex (TDD) scheme, we have conducted these tests only in the downlink direction since the results are expected to be close in the uplink direction with increased delay, but with no relevance to our intention to show that the non-QoS implementation is the worst scenario. Note that Packet Delay Variation is the same as Jitter. PC1 is the computer connected to the BS and PC2 is the computer connected to the SS. The presented results for VoIP are the resulting average of the 10 VoIP flows and the presented results for VoD are the resulting average of the 5 VoD flows.

5.2.1. VoIP over WiMAX without QoS

This section presents our measurements for VoIP traffic under a non-QoS WiMAX link. We run a shell script on PC2 that uses JTG to wait for incoming traffic, and another on PC1 that uses JTG to generate 10 simultaneous VoIP flows on the downlink direction to PC2. We measured One Way Delay, Packet Delay Variation (PDV) and Packet Loss for 10 simultaneous VoIP flows under a growing number of TCP flows ranging from none to 40. Each experiment was conducted as explained in section 5.1.6.

- **Average Delay**

Looking at Figure 21, we can easily see that, as the number of TCP flows grow, one way delay increases exponentially. There is a major increase on delay as we pass from one TCP flow to two TCP flows of around 60ms, after which the increase becomes linear. VoIP delay passes the maximum tolerable value of 150ms [49] after 30 TCP flows.

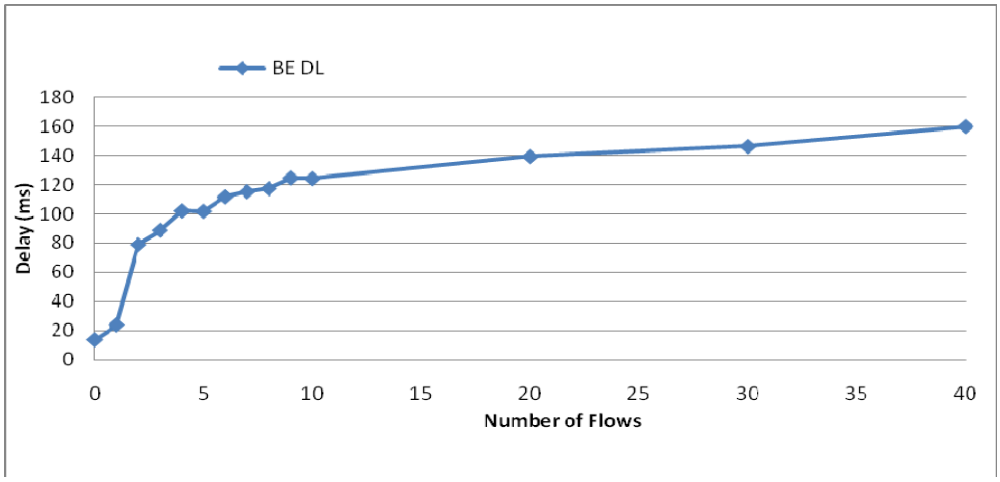

Figure 21 – One Way Delay BE DL

- **Packet Delay Variation**

Figure 22 shows packet delay variation where we can see that, after a major increase from no TCP flows to two TCP flows of 10ms, its value reaches a maximum of 13ms slightly decreases to 11ms.

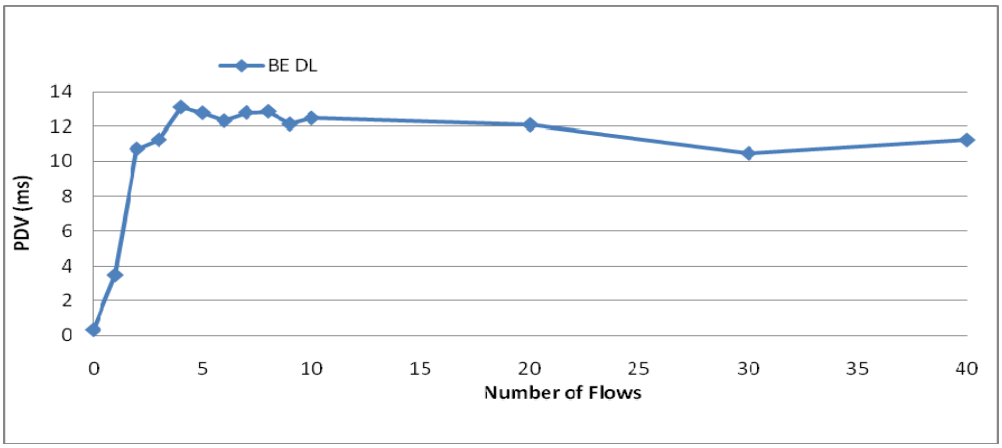

Figure 22 - PDV BE DL

- **Packet Loss**

The results depicted in Figure 23, show that an increase of TCP flows leads to tremendous packet losses with an exponential growth. Packet loss achieves a maximum of around 11% when the network is saturated with 40 TCP flows. VoIP packet loss passes the maximum tolerable value of 1% [52] after 2 TCP flows.

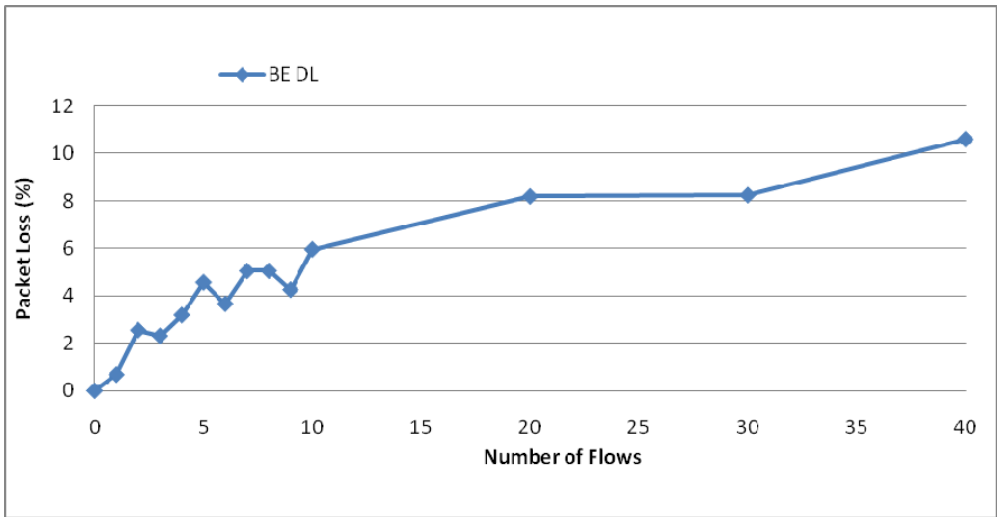

Figure 23 – Packet Loss BE DL

5.2.2. VoD over WiMAX without QoS

This section presents our measurements for VoD traffic under a non-QoS WiMAX link. We run a shell script on PC2 that uses JTG to wait for incoming traffic, and another on PC1 that uses JTG to generate 5 simultaneous video and audio flows on the downlink direction to PC2. We measured One Way Delay, Packet Delay Variation (PDV) and Packet Loss for 5 simultaneous VoD flows under a growing number of TCP flows ranging from none to 40. Once again, each experiment was conducted as explained in section 5.1.6.

- **One Way Delays**

The measured one way delay for audio and video are depicted in Figure 24 and Figure 25 respectively. We can see that even one TCP flow leads to a major increase of delay to almost 150ms. As the number of TCP flows grows so does the delay grows linearly. Delay for video is slightly larger than audio. Audio delay passes the maximum tolerable value of 150ms after 3 TCP flows and video after 20 TCP flows.

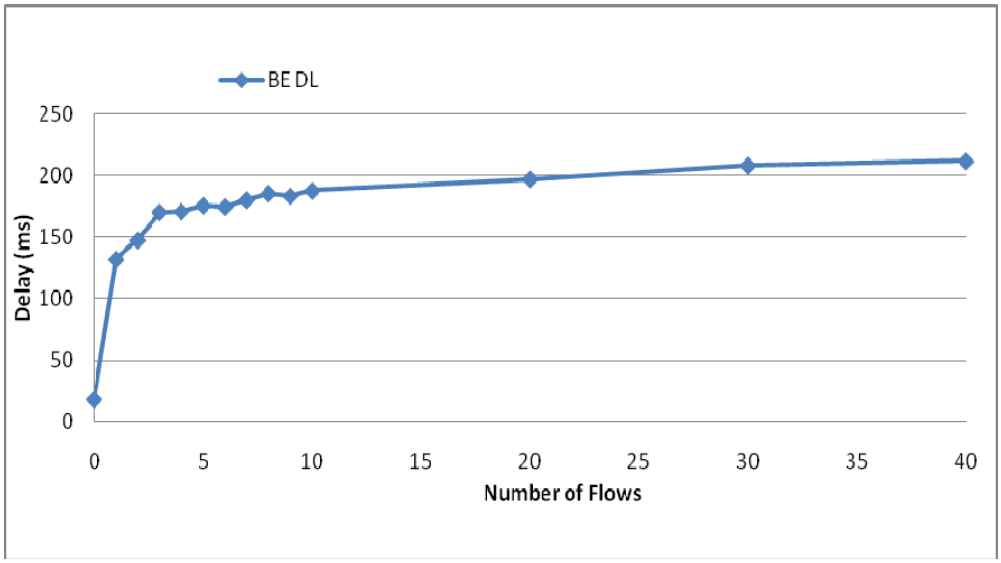

Figure 24 – One Way Delay Audio BE DL

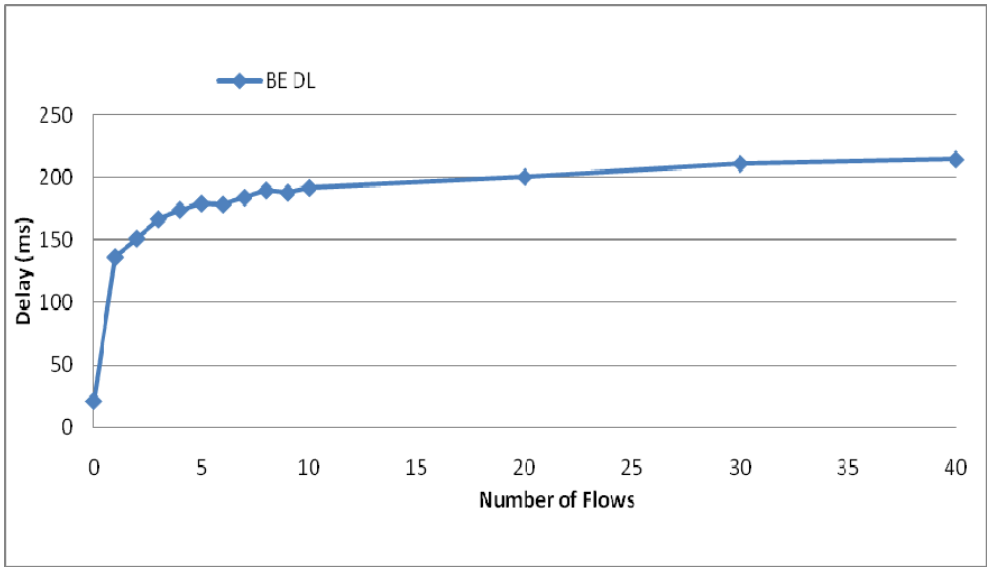

Figure 25 – One Way Delay Video BE DL

- **Packet Delay Variations**

Packet delay variations mesured for audio and video are depicted in Figure 26 and Figure 27 repectively. The results show that after an increase of 5ms on audio and 4ms on video from one TCP flow, the PDV value does not vary much and maintains relativelly constant. We can also see that PDV in video is smaller than audio.

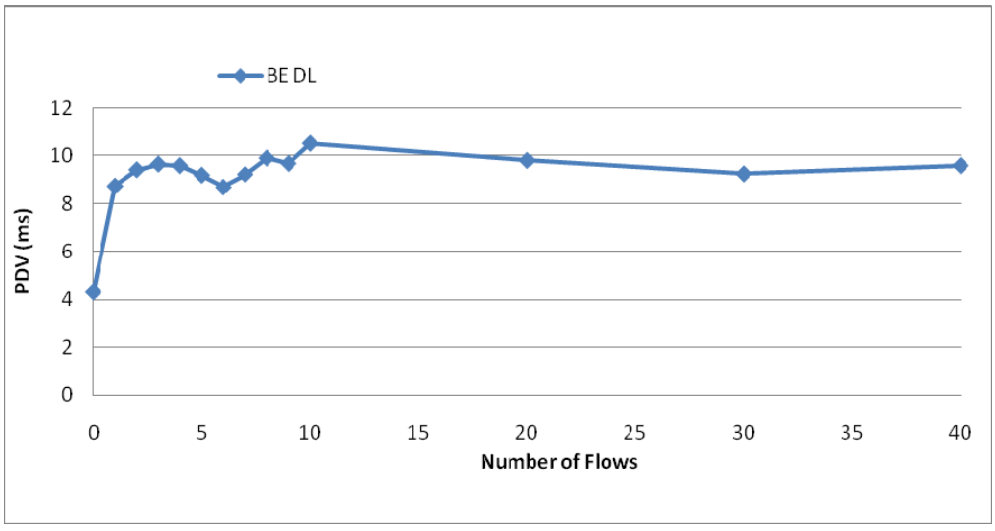

Figure 26 - PDV Audio BE DL

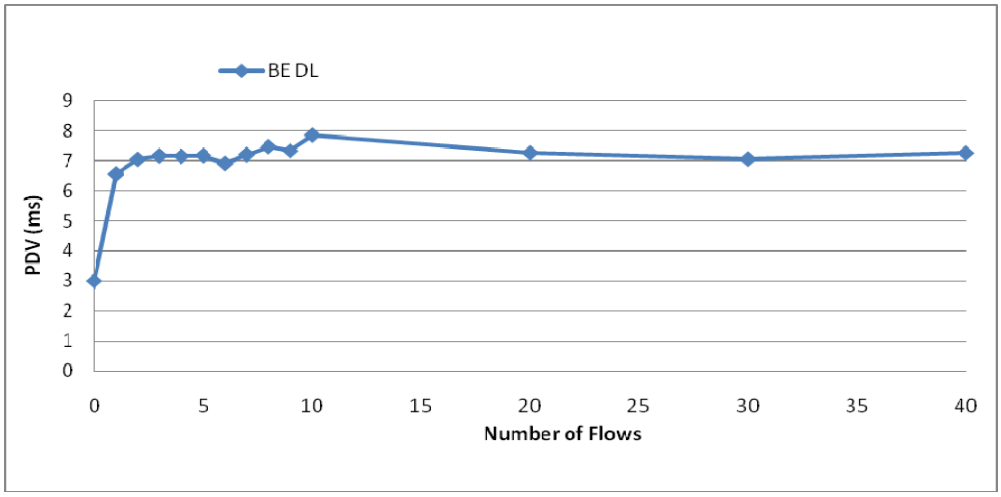

Figure 27 - PDV Video BE DL

- **Packet Losses**

As depicted in Figure 28 for audio and Figure 29 for video, packet loss increases linearly as more and more TCP flows congest the network. Packet loss achieves a maximum of around 17.5% for audio and 20% for video when the network is saturated with 40 TCP flows. Both audio and video packet loss pass the maximum tolerable value of 2% [50] after 1 TCP flow.

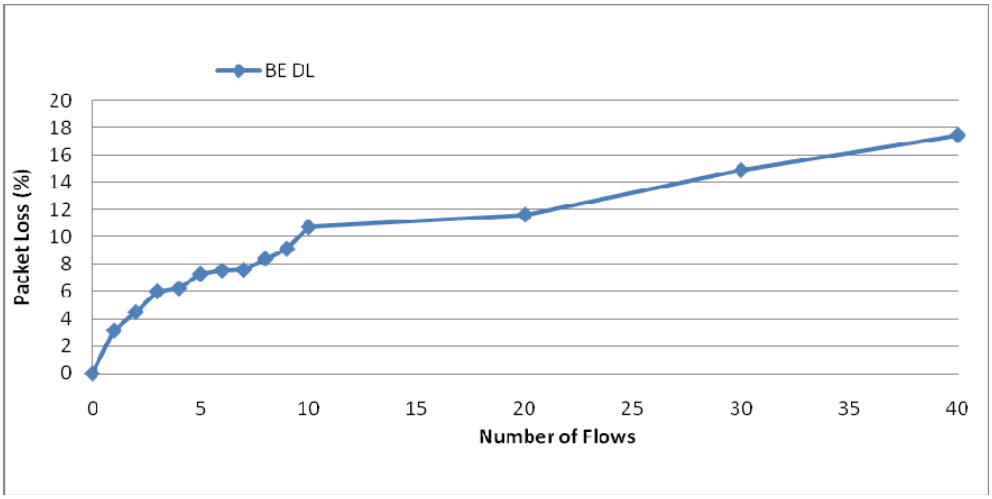

Figure 28 - Packet Loss Audio BE DL

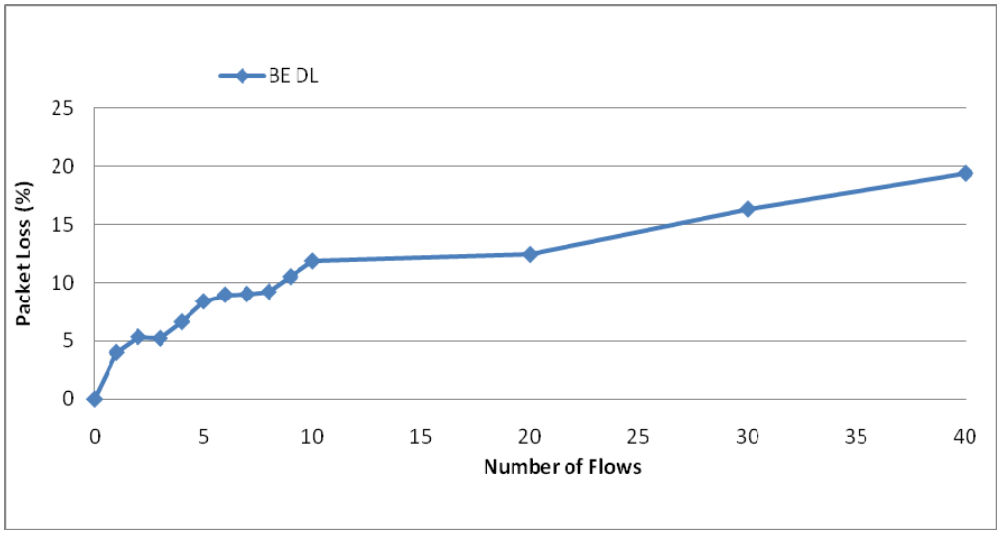

Figure 29 - Packet Loss Video BE DL

5.2.3. Observations

Given that we are testing a Best Effort scenario, all traffic has the same priority. As the packets reach the Convergence Sublayer (CS), they all receive the same classification and are sent to the same Service Flow (SF) that acts as a bucket, were packets have to wait until they can go through. Smaller packets, such as VoIP, move rapidly in the medium, thus having a smaller delay, but as they wait for larger packets to be sent their PDV increases. Larger packets, such as video and audio, take longer to cross the medium, thus having a larger delay, and as smaller packets are rapidly sent they don't wait long, leading to a smaller PDV.

Comparing the results between VoIP, audio and video, we confirm that each flow has its own behavior due to the size of the packets of the flow. Video and audio flows have an increased delay and packet loss in comparison to VoIP, with video presenting worst results than audio. VoIP flows have the biggest packet delay variation, followed by video and finally by audio.

The differences seen between video and voice flows can be explained by the fact that audio is CBR and video is VBR. Although audio packets are smaller than normal video packets, many video packets are larger than the Maximum Transmitted Unit (MTU), being divided into one MTU packet and a smaller one. Thus, video has larger delay than audio but smaller PDV.

Although the PDV is within the tolerable values for both VoIP of 30ms [50] and VoD flows of 50ms [53], measured delay and packet loss pass the maximum tolerable values. With the obtained results we can conclude that a Best Effort scenario on a fixed WiMAX link cannot sustain either VoIP or VoD backhauling.

5.3. VoIP and VoD services over WiMAX with QoS

In this set of tests, the aim is to analyze the network performance of VoIP and VoD flows with competing background TCP flows when the QoS mechanism is configured on the WiMAX system. Thus, we define in our Proxim's BS an Unsolicited Grant Service (UGS) SS Class for VoIP testing, a Real-Time Polling Service (rTPS) SS Class for VoD testing, and a mixed UGS/rTPS SS Class for VoIP/VoD testing, as described in section 5.1.5. Note that Packet Delay Variation is the same as Jitter. PC1 is the computer connected to the BS and PC2 is the computer connected to the SS. The presented results for VoIP are the resulting average of the 10 VoIP flows and the presented results for VoD are the resulting average of the 5 VoD flows.

5.3.1. VoIP over WiMAX with QoS

This section presents our measurements for VoiP traffic under a QoS WiMAX link. We run a shell script on PC2 that uses JTG to wait for incoming traffic on ports 3000-3009, and another on PC1 that uses JTG to generate 10 simultaneous VoIP flows on the downlink direction to PC2 with destination ports 3000-3009. For the uplink direction we run the receiver on PC1 and the generator on PC2, with the same configuration as for downlink. We measured One Way Delay, Packet Delay Variation (PDV) and Packet Loss for 10 simultaneous VoIP flows under a growing number of TCP flows ranging from none to 40. Each experiment was conducted as explained in section 5.1.6.

- **One Way Delay (DL/UL)**

Figure 30 illustrates the measurements for one way delay on both downlink (DL) and uplink (UL). We can see on downlink that delay increases slightly but remains mostly constant on 20ms with very small variations, with another slight increase to 22ms at 30 TCP flows. Looking at uplink we can see that the delay value remains within 22 - 25ms with small variations, and has a peak of 27ms at 7 TCP flows. The uplink delay is slightly larger than downlink.

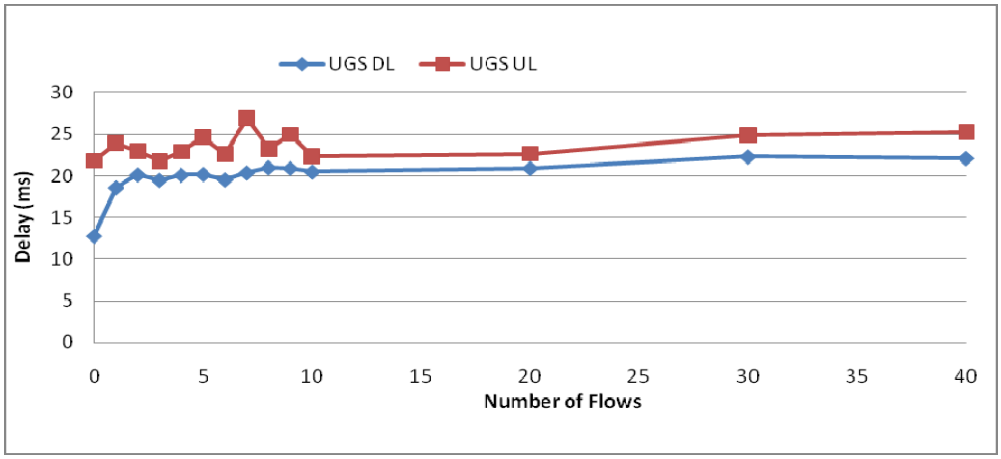

Figure 30 - One Delay VoIP UGS (DL/UL)

- **Packet Delay Variations (DL/UL)**

The packet delay variation for both downlink and uplink is depicted in Figure 31. Comparing both uplink and downlink we notice a very similar behavior and close values. Downlink PDV increases up until 7 TCP flows, equaling uplink and remains constant with a value around 4.2ms. Uplink PDV increases up until 10 TCP flows remaining constant with a value around 4.9ms.

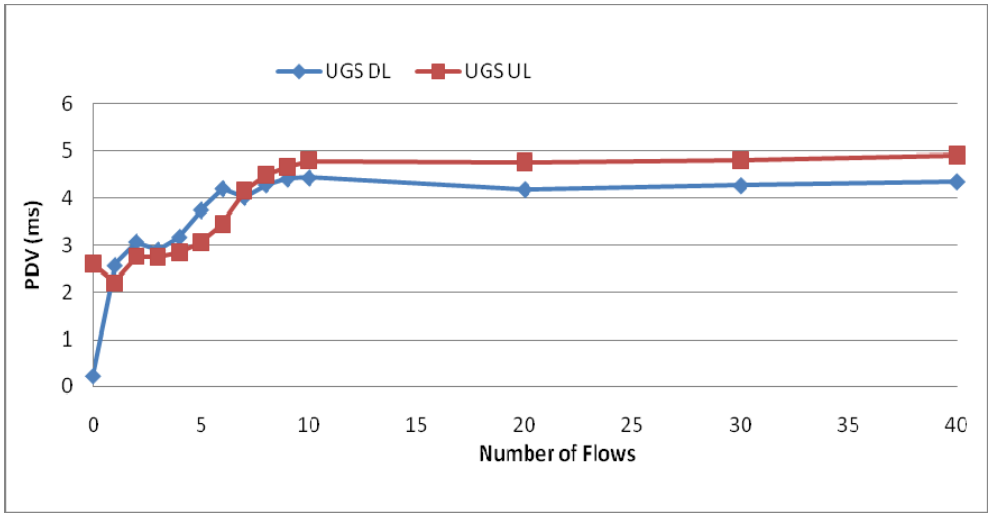

Figure 31 - PDV VoIP UGS (DL/UL)

- **Packet Loss (DL/UL)**

The results depicted in Figure 32 show that packet loss is very low in both downlink and uplink, with a maximum of 0.16% for downlink and 0.1% for uplink.

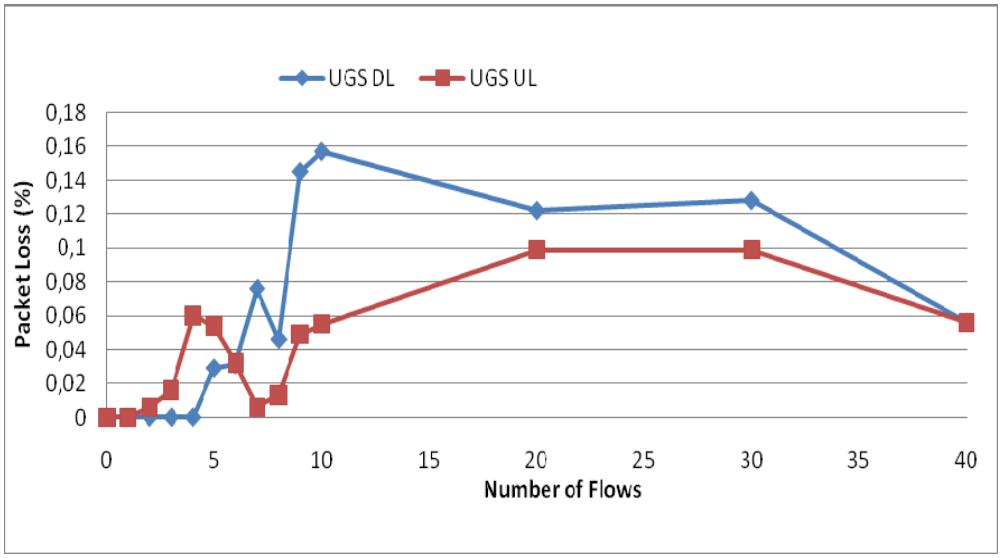

Figure 32 - Packet Loss VoIP UGS

5.3.2. VoD over WiMAX with QoS

This section presents our measurements for VoD traffic under a QoS WiMAX link. We run a shell script on PC2 that uses JTG to wait for incoming traffic on ports 4000-4004 and 5000-5004. Another script is run on PC1 that uses JTG to generate 5 simultaneous video and audio flows on the downlink direction to PC2 with destination ports 4000-4004 for audio and 5000-5004 to video. For the uplink direction we run the receiver on PC1 and the generator on PC2, with the same configuration as for downlink. We measured One Way Delay, Packet Delay Variation (PDV) and Packet Loss for 5 simultaneous VoIP flows under a growing number of TCP flows ranging from none to 40. Each experiment was conducted as explained in section 5.1.6.

- **One Way Delays (DL/UL)**

The measured one way delay for audio and video flows in both downlink (DL) and uplink (UL) is depicted in Figure 33 and FFigure 34 respectively. Comparing both results we realize that they have identical behavior, with a downlink delay half the uplink one. In downlink both audio and video delay remains constant around the value acquired for 1 TCP flow, with audio around 20ms and video around 22ms. In uplink both audio and video delay has small variations until 4 TCP flows, increasing 10ms until 6 TCP flows, and remaining constant with slight variations. Audio delay reaches the peak at 50ms and video delay at 52ms.

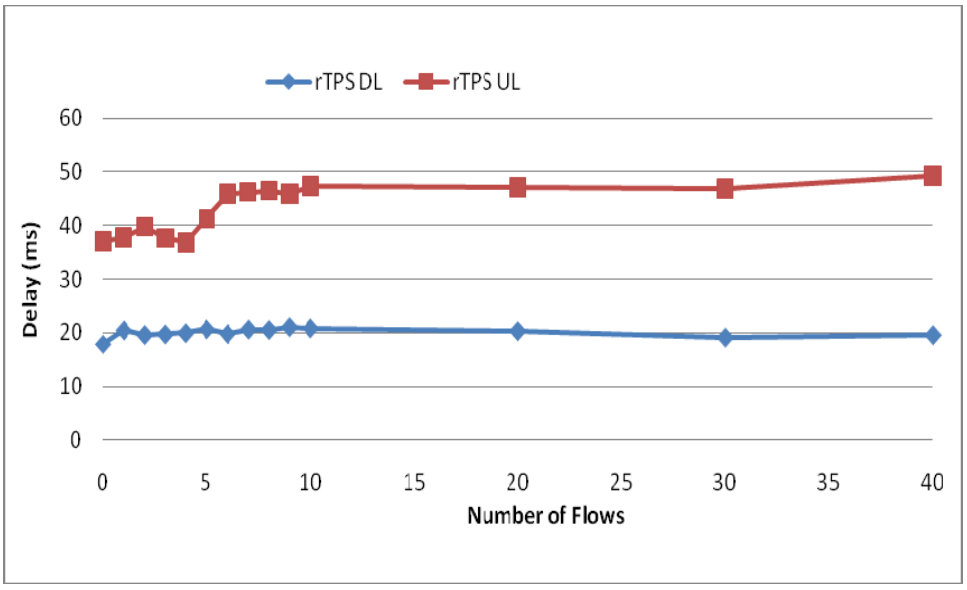

Figure 33 – One Way Delay Audio rTPS (DL/UL)

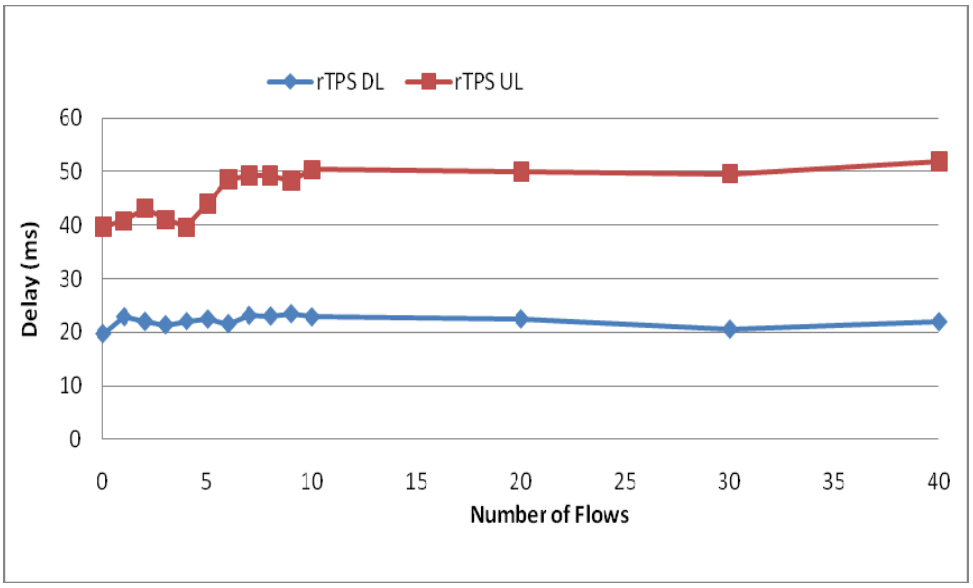

Figure 34 – One Way Delay Video rTPS (DL/UL)

- **Packet Delay Variations (DL/UL)**

Figure 35 for audio and Figure 36 for video illustrates the packet delay variation on both uplink and downlink. Just like for delay, both audio and video have identical behaviors with video having a larger PDV. From none to 40 TCP flows, uplink PDV for uplink remains with very small variation, with a value between 5 - 5.5 ms on audio and around 4ms on video. Downlink PDV, after a slight increase with one TCP flow, remains with very small variations around 5ms for audio and between 3.5 – 4ms, decreasing 1ms on both audio and video at 30 TCP flows.

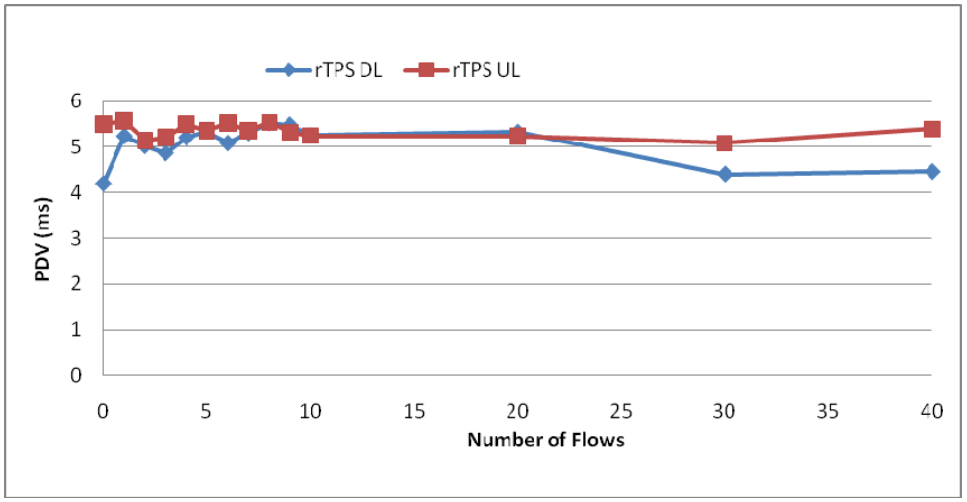

Figure 35 - PDV Audio rTPS (DL/UL)

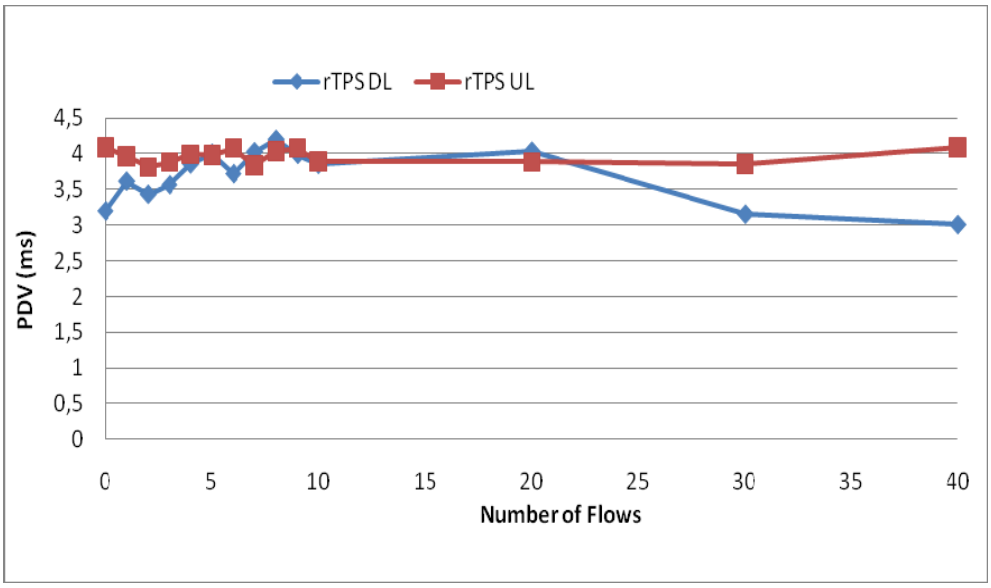

Figure 36 - PDV Video rTPS (DL/UL)

- **Packet Loss (DL/UL)**

Looking at Figure 37 and Figure 38, that depict packet loss for audio and video respectively for both downlink and uplink, we verify that packet loss on the downlink channel is practically none. The uplink channel presents very little packet loss with a peak of 0.1% for audio and 0.14% for video.

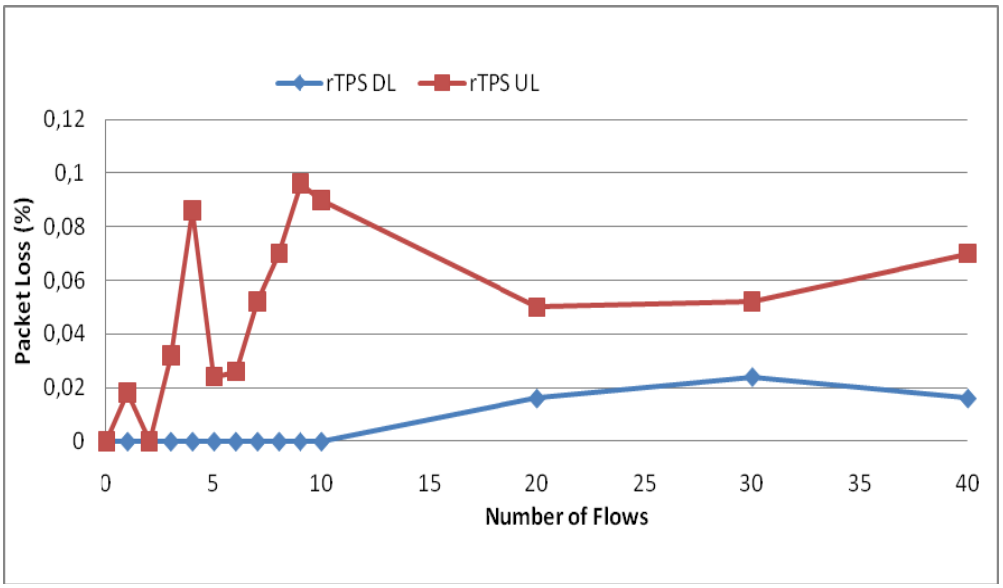

Figure 37 - Packet Loss Audio rTPS (DL/UL)

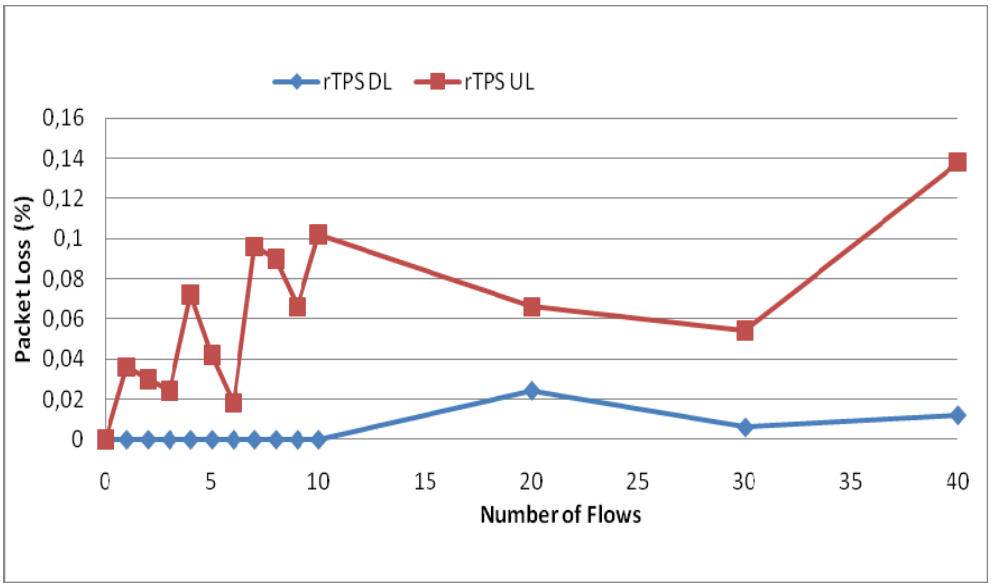

Figure 38 - Packet Loss Video rTPS (DL/UL)

5.3.3. VoIP and VoD over WiMAX with QoS

This section presents our measurements for VoIP/VoD traffic under a QoS WiMAX link. We run a shell script on PC2 that uses JTG to wait for incoming traffic on ports 3000-3009, 4000-4004 and 5000-5004. Another script is run on PC1 that uses JTG to generate 10 simultaneous VoIP flows and 5 simultaneous video and audio flows on the downlink direction to PC2 with destination ports 3000-3009 for VoIP, 4000-4004 for audio and 5000-5004 to video. For the uplink direction we run the receiver on PC1 and the generator on PC2, with the same configuration as for downlink. We measured One Way Delay, Packet Delay Variation (PDV) and Packet Loss for 5 simultaneous VoIP flows under a growing number of TCP flows ranging from none to 40. Each experiment was conducted as explained in section 5.1.6.

- **One Way Delays (DL/UL)**

Comparing one way delay measured values for VoIP (see Figure 39), audio (see Figure 40) and video (see Figure 41) we verify that VoIP is the one with less delay, followed by audio and video. VoIP uplink maintains a delay value between 18 - 22ms and downlink has small variations within 15 - 20ms.

Audio uplink maintains a delay value between 45 - 50ms and downlink has small variations around 25ms. Video uplink maintains a delay value between 45 - 50ms and downlink has small variations around 25ms. In both audio and video downlink delay is almost half the uplink.

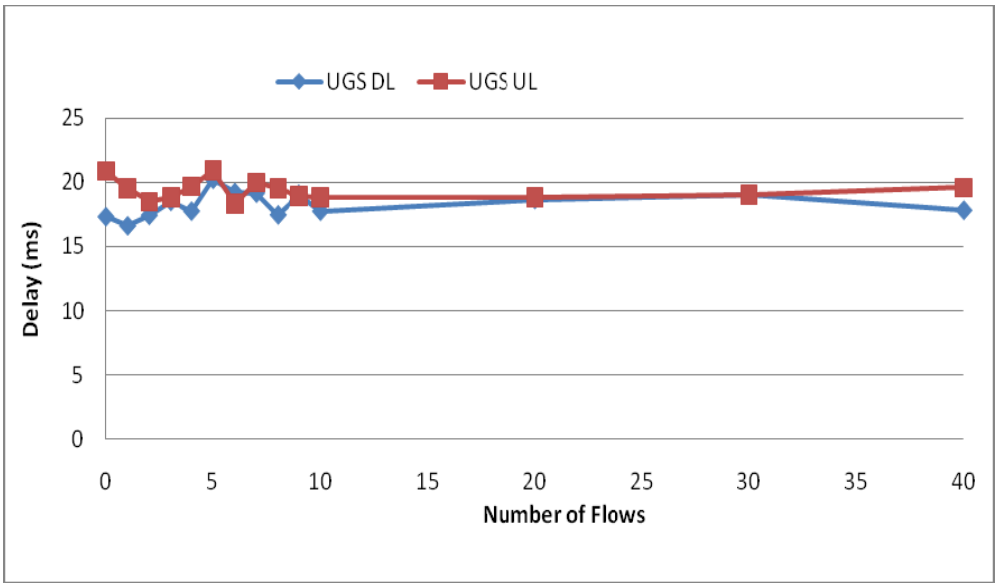

Figure 39 – One Way Delay VoIP

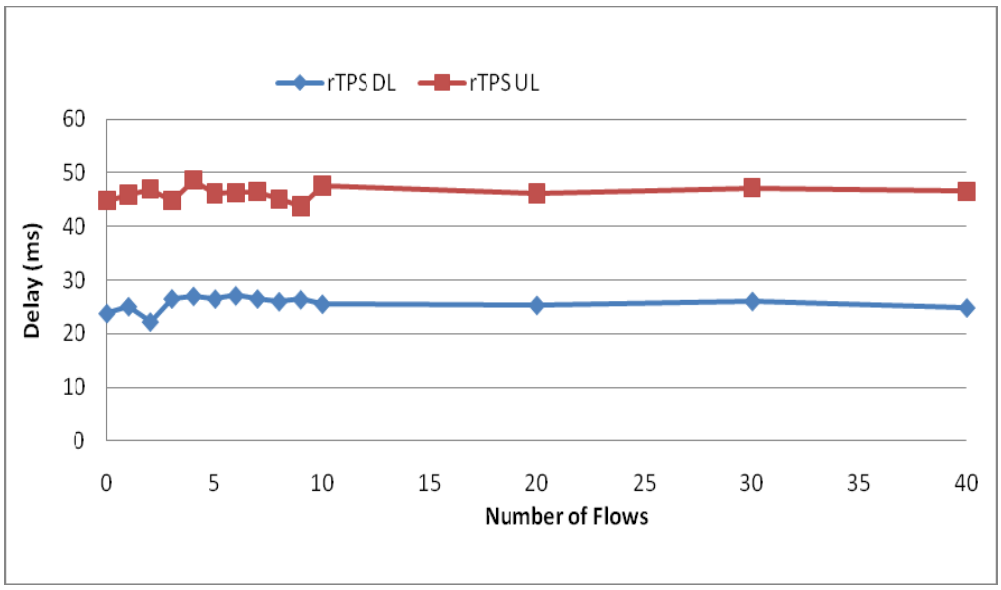

Figure 40 - Average Delay Audio

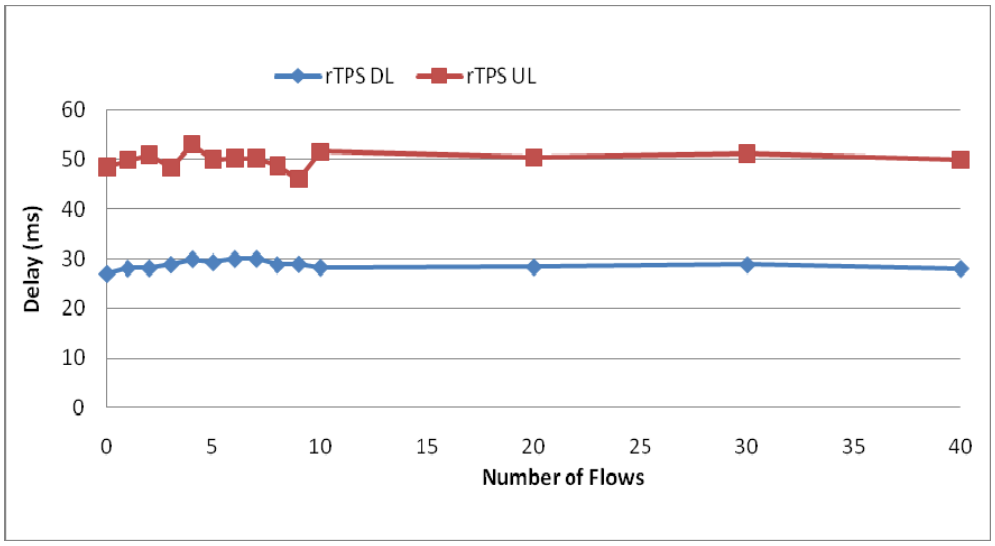

Figure 41 - Average Delay Video

- **Packet Delay Variations (DL/UL)**

Figure 42 depicts the packet delay variation on the VoIP flow. Looking at the measured results we can see variations on the PDV for both uplink and downlink. Uplink PDV value varies between 2 – 2.5ms until 20 TCP flows, with the value dropping to 1.3ms at 40 TCP flows, while downlink PDV value grows from 0.9ms to 3ms until 7 TCP flows, decreasing to 1.5ms at 40 TCP flows. Comparing VoIP to audio (see Figure 43) and video (see Figure 44we verify that VoIP's PDV is still much smaller than the rest, with audio PDV larger than video. Audio PDV values range from 5 – 6ms for downlink and remains around 7.5ms for uplink. Video PDV values range from 3 – 5ms for downlink and drops from 6 – 5ms for uplink.

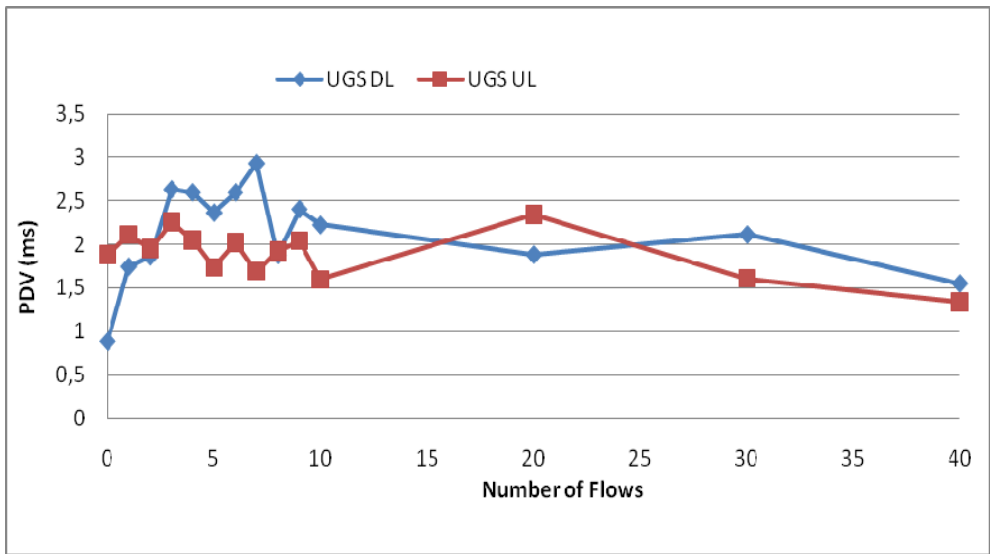

Figure 42 - PDV VoIP

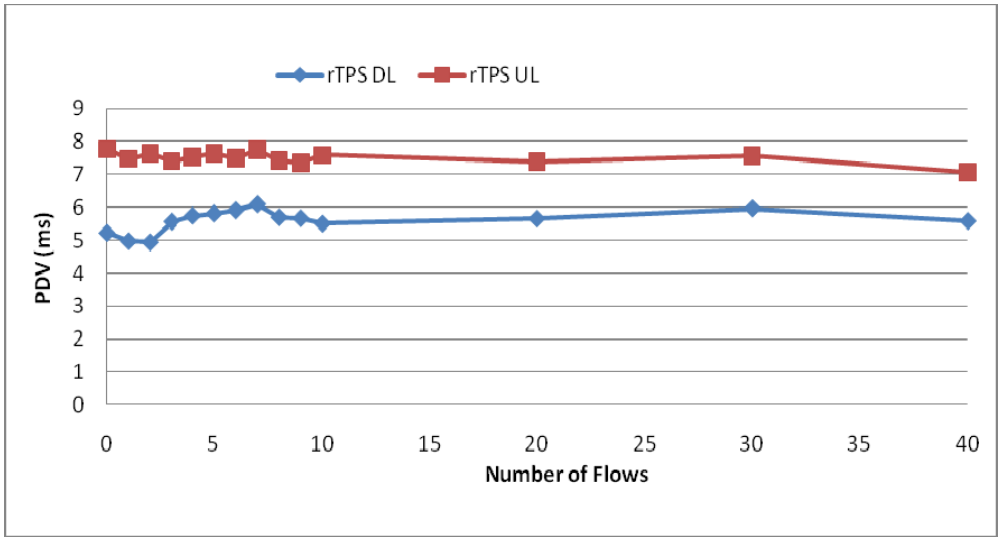

Figure 43 - PDV Audio

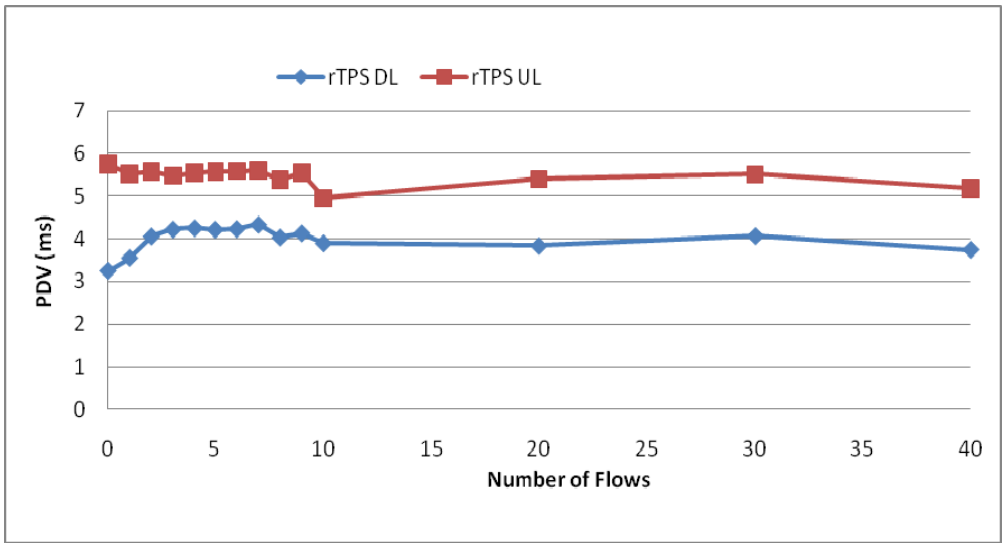

Figure 44 - PDV Video

- **Packet Loss (DL/UL)**

Packet loss for both downlink and uplink on VoIP, audio and video are depicted in Figure 45, Figure 46 and Figure 47 respectively. We verify that, although packet loss values are well below the tolerance value, there is some packet loss on all flows. Packet loss on VoIP reaches a peak at 4 TCP flows of 0.3% and uplink 0.1% ate 30 TCP flows. For audio and video packet loss increases in every increase of TCP flows, with peaks at 0.4% loss on downlink and 0.3% on uplink.

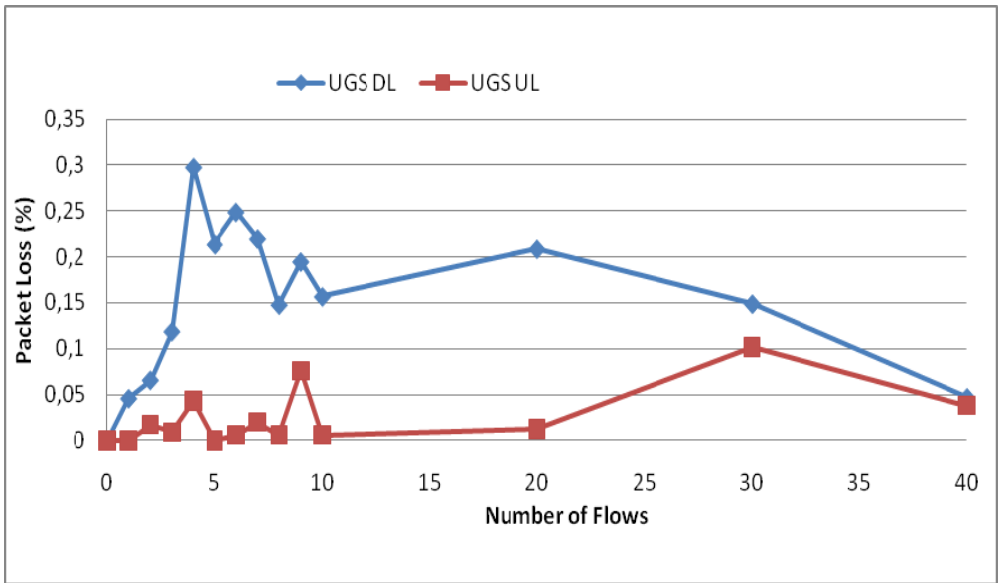

Figure 45 - Packet Loss VoIP

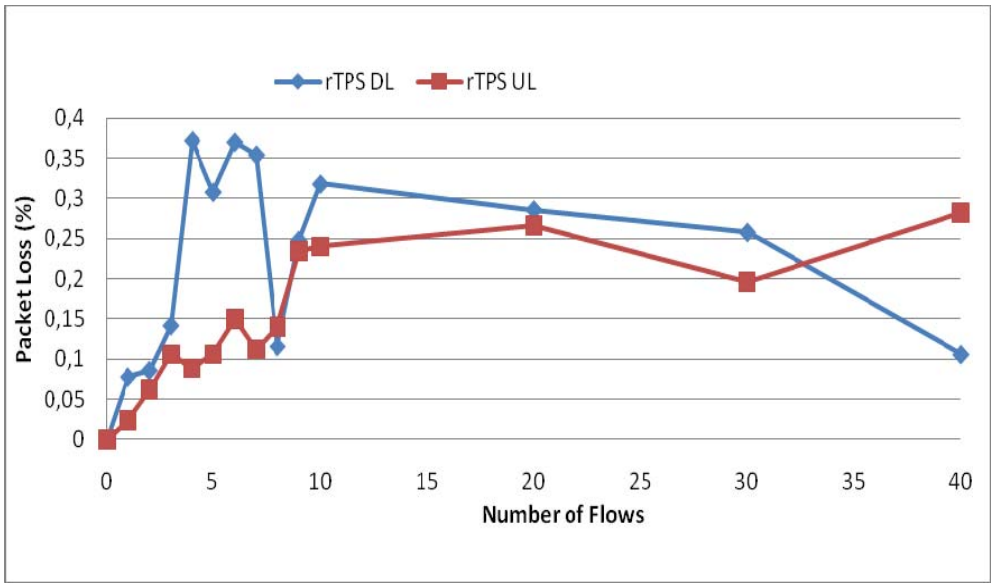

Figure 46 - Packet Loss Audio

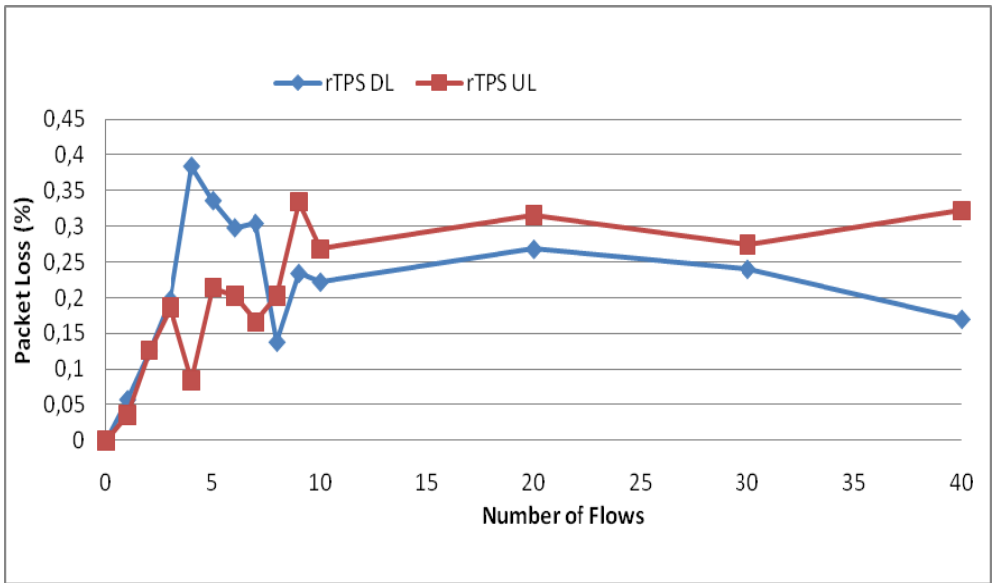

Figure 47 - Packet Loss Video

5.3.4. Observations

The results obtained from the measurements in all three scenarios allow us to conclude that the QoS reserve bandwidth and priority mechanisms were successfully implemented for all SS Classes, since QoS-flows crossed the medium with low delay and virtually zero packet loss. We also conclude that both one way delay and PDV are larger in uplink than on downlink due to the TDD scheme, as downlink frames are sent first than uplink ones, independently of being QoS or non-QoS frames.

Comparing VoIP results from the first and third scenarios, we verify that delay and PDV is smaller in the third scenario than in the first. If we compare VoD results from the second and third scenarios we come to verify the opposite. The differences seen can be explained by the bandwidth reserve and priority mechanism. In the first scenario the reserved bandwidth for VoIP UGS was 360 Kbps (7.8% of available bandwidth), in the second scenario the minimum reserved bandwidth was 4250 Kbps (92% of available bandwidth), and on the third scenario the combined reserved bandwidth was 4610 Kbps (99% of available bandwidth). Given that VoIP packets have higher priority than audio, audio than video, and video than all other, as the packets arrive at the bucket the QoS-packets are served first from highest to lowest priority. In the first scenario available bandwidth for TCP flows is 92.2%, allowing for large TCP packets to cross the medium, which increases delay and PDV, as explained in section 5.2.3. On the second scenario there is little available bandwidth for TCP flows, which means that as the number of TCP flows increases the size of the packets decreases, thus leading to a minimum occupation of the medium and allowing for low delay and PDV on VoD flows. On the third scenario we have two competing QoS-flows VoIP

and VoD. Since the available bandwidth for TCP flows is less than 1%, the medium is basically shared by VoIP and VoD flows. VoIP has higher priority than VoD, which means that as traffic arrives at the bucket, VoIP packets are served first than VoD packets, which increments VOD delay and PDV. Small VBR video packets, resulting from dividing a packet larger than MTU, occupy the medium for a small time, thus decreasing the delay and PDV of VoIP flows.

Given the differences between the results obtained from the three scenarios we can conclude that QoS for real-media achieves better results when less bandwidth is allowed for non-QoS services.

Since in all three scenarios the measured results of one way delay, PDV and packet loss are within the tolerable values for both uplink and downlink, we can conclude that with QoS a fixed WiMAX link can sustain VoIP, VoD or VoIP and VoD backhauling.

5.4. Experiments Conclusions

With these experiments we tried to understand the real performance of today's WiMAX equipments in supporting VoIP and VoD services. From the results obtained from section 5.2 we conclude that a Best-Effort scenario cannot support real-media streaming on a congested WiMAX link, with delay and packet loss above the tolerable values. From section 5.3 we can conclude that WiMAX allows us to provide QoS for different type of traffics through bandwidth allocation and traffic prioritization mechanisms, ensuring good performance for real-media traffic. We can conclude that a QoS scenario on a fixed WiMAX link can sustain real-media backhauling.

6. QoS analysis of IEEE 802.11 Wireless MESH Networks

The aim of the work reported in this chapter is the experimental investigation of IEEE 802.11 MESH Networks performance and its evaluation on a fixed WMN for VoIP and VoD services with and without QoS.

We employ multiple competing traffic sources at each cell and measure the capacity of our IEEE 802.11 Mesh equipment to handle bidirectional VoIP and VoD flows, while handling multiple competing TCP flows.

We use Jugi's Traffic Generator (JTG) [29] to generate our UDP packets from VoIP and VoD emulated streams, IPERF [30] to generate multiple bi-directional TCP flows and a software-only implementation of the IEEE 1588 Precision Time Protocol (PTP) [31].

Section 6.1 provides an overview on the used methodology to conduct the experiments. Section 6.2 describes the performance evaluation of IEEE WMNs. Section 6.3 addresses VoIP and VoD services on WMNs with or without QoS. Section 6.4 provides a final conclusion to the chapter.

6.1. Used Methodology

This section explains the testbed and the methodology used to evaluate the network performance and to qualify VoIP and VoD over IEEE 802.11 MESH Network.

6.1.1. Testbed Configuration

Our testbed was comprised of three Proxim's Orinoco AP-4000MR [28], four laptops and one computer. The Mesh Portal (MPP) was connected to the computer that served as a backbone to the entire network. Three notebooks (STA2, STA3 and STA4) are connected wirelessly to the Mesh Access Points (MAPs) and are used as traffic sources. The fourth laptop (STA1) is used to evaluate the performance of the WMN on all its three cells. The Backbone and STA1 are also connected via their Ethernet cards through an Ethernet Hub for clock synchronization purposes.

Before beginning to configure our testbed, we had first to conduct a site survey to determine the placement of the MAPs in order to provide adequate signal coverage to achieve roaming capability between MAPs. Moreover, we have to ensure that each MAP has a mutual coverage area with its neighbors, but also that the cells are spread far enough in order that each AP has its own privileged coverage area.

We downloaded and used a trial version of "WiFi Hopper" which is a WLAN utility that combines the features of a Network Discovery and Site Survey [56]. The trial had a 15 day limit and allowed us to use all its features during that period.

Given that for the MESH Link we can chose both IEEE 802.11a [10] or IEEE 802.11b/g [9] modulation schemes and that our testbed was indoors, we chose IEEE 802.11a for the MESH Link and IEEE 802.11b/g for WLAN access, since IEEE 802.11a has better throughput but shorter range. We chose a multi-radio configuration since on single-radio the channel used by the MESH Link is the same as the WLAN access, thus decreasing the signal quality and throughput performance due to co-channel interference and shared bandwidth between the MESH link and the WLAN access.

Using "WiFi Hopper" we measured the Received Signal Strength Indicator (RSSI) from the MESH Portal and stretched our network to the maximum coverage area possible (around -75dBm) placing in that position the second MESH AP (MESH AP1). Using the same process for the second AP, we realized that, given the building configuration, the third AP (MESH AP2) would have to be placed in a lower floor.

Realizing that the throughput given between the MESH APs was too low, which was expected since the signal had to cross an entire floor and the mutual coverage area between MESH AP1 and MESH AP2 was too small, we reduced the emitted power by 10dBm and placed all three MAP in the same floor. Using "WiFi Hopper" we were able to identify the appropriate architecture to ensure good throughput and small delay. Figure 48 depicts our final Mesh architecture. The Portal was placed inside the LAB and the other MAPs on the hall, with a distance of 15m between each one.

Figure 48 - Network Arquitecture

All tests were performed indoors with the presence of multiple foreign equipments operating on the 2.4GHz, which implied a lot of interference. Thus we turned to WiFi Hopper's network discovery tool and chose channel 44 for the MESH Link and channels 3 (MESH Portal), 8 (Mesh AP1) and 4 (MESH AP2) for WLAN access in order to minimize interference. The chosen Service Set Identifier (SSID) was "MeshNET" for 802.11a radio and "ProximBG" for 802.11b/g radio.

The network was configured with Class C 192.168.1.0 IP addresses for the wireless mesh system, and with Class A 10.240.2.0 IP addresses for the clock synchronization system.

Figure 49 illustrates our experimental WMN testbed.

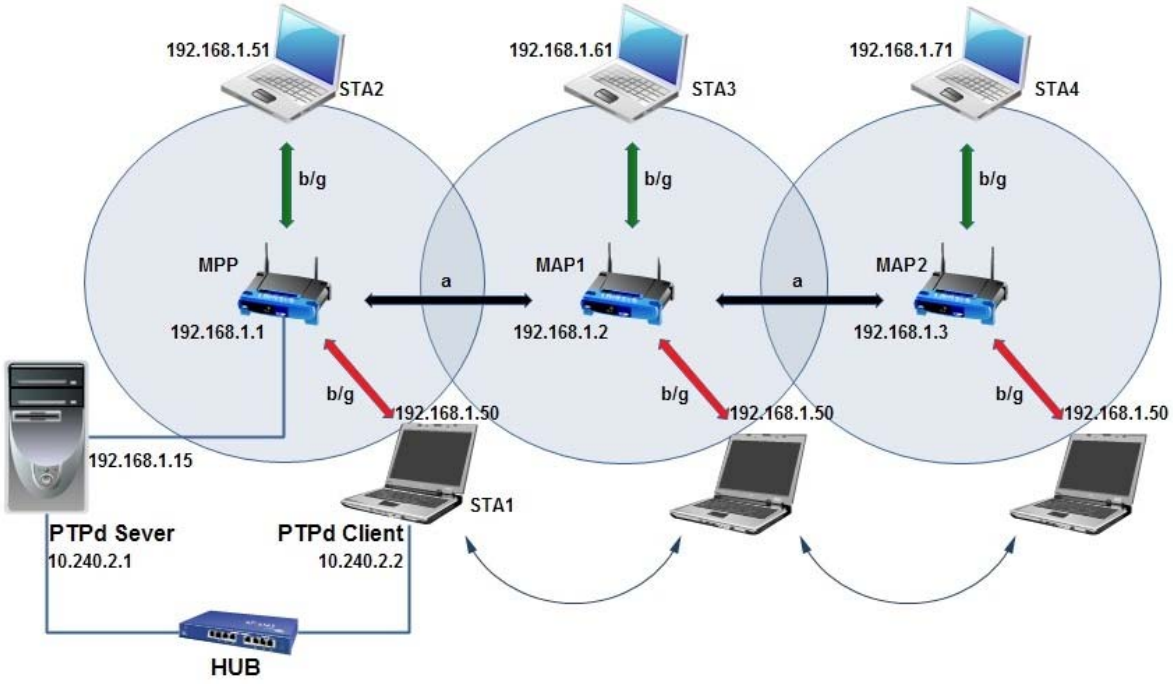

Figure 49 - IEEE 802.11 Mesh Testbed

6.1.2. Synchronization and Traffic Generation

For high-precision synchronization we used the IEEE 1588 Precision Time Protocol (PTP) [31], as described in section 5.1.2.

For traffic generation we used JTG [29] and IPERF [30]. Traffic emulation for VoIP and VoD services was as described in section 5.1.4.

6.1.3. Configuring QoS parameters

QoS configuration on Proxim's Orinoco AP4000-MR [28] has to be done in all MAP to ensure QoS coverage through the entire network. The AP supports Wi-Fi Multimedia (WMM), which is a solution for QoS functionality based on the IEEE 802.11e [11] specification, supporting Enhanced Distributed Channel Access (EDCA) for prioritized QoS services.

EDCA introduces four virtual Access Categories (AC) with different access parameters: Arbitrary Inter Frame Space Number (AIFSN), Contention Windows (CW) min, CWmax and Transmission Opportunity Limit (Tx OP Limit. These parameters are configured such that frames in the different AC access the wireless media with different priorities.

The priority of the frame determines which Access Category handles the frame. The priority of the frame outside the 802.11 link is the layer 2 (802.1p) priority or the layer 3 priority (the IP Precedence or DSCP value). These are mapped to an 802.1D priority/User Priority via a mapping table and this mapped priority is used to determine which Access Category handles the frame. Since we d not have VLANs in our network, we will not make use of this part of the configuration.

Unfortunately, for some reason unknown to us, we could not change QoS parameters either in the EDCA table, the priority mapping table or the QoS policy. Any change would cause the AP to classify all inbound traffic as Best Effort. This constraint limited our work since we were not allowed to relate effective QoS with different EDCA parameters [60] or with a collaborative QoS with DiffServ [58]. Still, enabling QoS feature with the default values allowed us to make our measurements properly.

The main areas for configuring the QoS feature are (note that the values presented are the default values):

- **Configuring EDCA Parameters**

Given our multi-radio topology, we must configure the EDCA parameters for both Radio A (the mesh link between MAPs) and Radio B (link between STA and MAP) for all Access Categories (AC). The EDCA parameters used are described in Table 3 and Table 4:

Access Category	CWmin	CWmax	AIFSN	Tx OP Limit
Best Effort	15	1023	3	0
Background	15	1023	7	0
Video	7	15	2	3008
Voice	3	7	2	1504

Table 3 - STA EDCA Parameters

Access Category	CWmin	CWmax	AIFSN	Tx OP Limit
Best Effort	15	63	3	0
Background	15	1023	7	0
Video	7	15	1	3008
Voice	3	7	1	1504

Table 4 - MAP EDCA Parameters

- **Configuring the QoS Priority Mapping Tables**

The EDCA supports eight User Priorities (UPs) as defined in IEEE 802.1D [12]. For each 802.1D priority a lower and upper value for DSCP is defined. There is a 1 to 1 mapping between each 802.D priority (0-7) and DSCP priority ranges and an index is associated with each created table. The IP DSCP mapping is described in Table 5:

IEEE 802.1D Priority	DSCP Lower Range	DSCP Upper Range
0	0	7
1	8	15
2	16	23
3	24	31
4	32	39
5	40	47
6	48	55
7	56	63

Table 5 - IEEE 802.1D to IP DSCP Priority Mapping Table

- **Configuring QoS Policies**

After configuring the EDCA and the priority mapping tables, we must now associate these parameters for all inbound and outbound traffic by creating a QoS Policy, which requires only the number of the index associated with the desired mapping table. The created QoS policy is then applied to the Service Set Identifier (SSID) of each radio and enabled on the QoS tab.

6.2. Evaluation of IEEE 802.11 WMN Characteristics

At this section the aim is to evaluate our network characteristics for the configured testbed. We measure RSSI values throughout the network coverage area, as well as bandwidth performance between MAPs and between different points in our network to the backbone by the Mesh link. The measurements were performed on 9 points in the network, which are depicted in Figure 50.

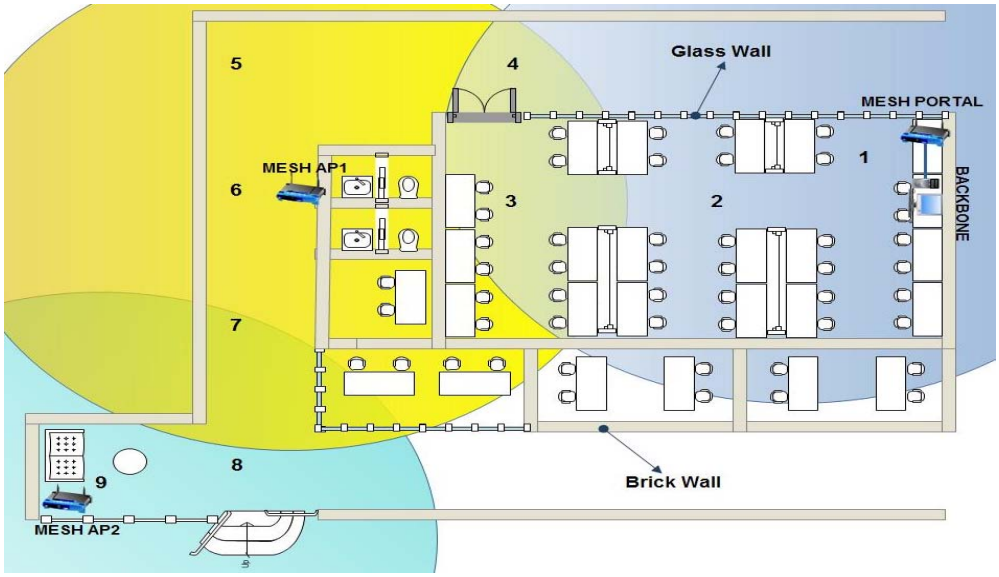

Figure 50 - Evaluation Points

6.2.1. Network Coverage

In order to ensure we had proper signal coverage throughout the network we measured the RSSI values on the 9 points of the network defined in the previous figure. Using "WiFi Hopper" we performed a scan for all available channels in our network and discovered the three MAP. We began capturing the RSSI values from all MAPs on point 1 for two minutes and paused for 30 seconds. After 30 seconds we continued capturing RRSI values on point 2. We repeated the process until point 9. Figure 51 depicts the measured RSSI values from the Mesh Portal (MPP), Figure 52 from the Mesh AP1 (MAP1) and Figure 53 from the Mesh AP2 (MAP2). The average RSSI measured values are described in Table 6.

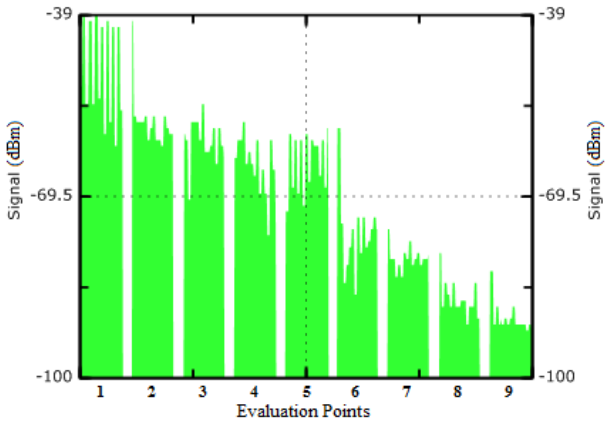

Figure 51 - RSSI Values MPP

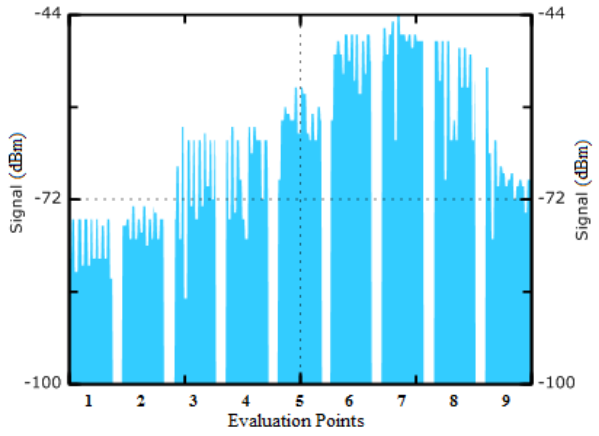

Figure 52 - RSSI Values MAP1

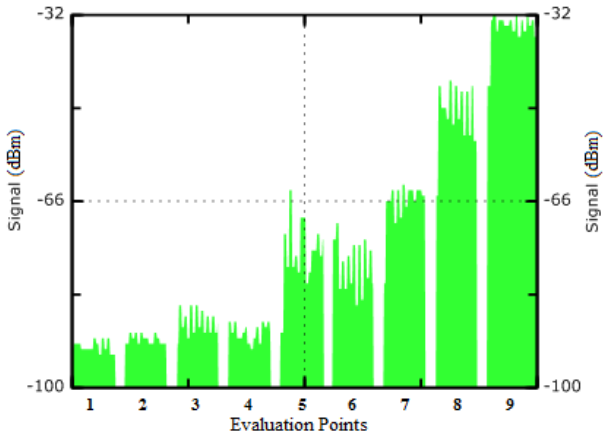

Figure 53 - RSSI Values MAP2

Points	MPP (dBm)	MAP1 (dBm)	MAP2 (dBm)
1	-46,9	-79,8	-92,4
2	-58,5	-76,3	-91,1
3	-60,4	-70,5	-88,4
4	-66,3	-68,3	-90,1
5	-67,1	-59,5	-75,8
6	-78,2	-50,3	-77,2
7	-80,2	-47,5	-66,1
8	-86,9	-56,5	-49,9
9	-90,9	-67,9	-33,7

Table 6 - Average RSSI Values

The obtained values allow us to verify that we have full coverage on our network designated area, as well as three 802.11 cells with common and independent areas for roaming testing. We can extrapolate from the results that handover will occur in Points 5 an 8.

6.2.2. Mesh Channel Throughput

Before proceeding with any more measurements, we conducted baseline experiments using Iperf to determine the maximum throughput that can be obtained on the Wi-Fi link, as well as the relation between the number of hops to the MPP and the available throughput.

We connected to each MAP a laptop via Ethernet and used Iperf to generate TCP and UDP traffic between them. We generated a single TCP flow to measure the maximum TCP link capacity. To measure the maximum UDP link capacity we used various different UDP sources with higher and higher bandwidth. Results of the measurements for both TCP and UDP between MPP and MAP2 are described in Table 7, between MAP2 and MAP3 in Table 8, and between MPP and MAP3 in Table 9.

	MPP -> MAP1			**MAP1 -> MPP**		
	MIN (Mbps)	**AVE (Mbps)**	**MAX (Mbps)**	**MIN (Mbps)**	**AVE (Mbps)**	**MAX (Mbps)**
TCP	18	18,3	18,7	16,6	17	17,6
UDP	22	22,4	22,6	22	22,1	22,2

Table 7 - Measured throughput between MPP and MAP1

	MAP1 -> MAP2			**MAP2 -> MAP1**		
	MIN (Mbps)	**AVE (Mbps)**	**MAX (Mbps)**	**MIN (Mbps)**	**AVE (Mbps)**	**MAX (Mbps)**
TCP	22	22,2	22,6	21,2	21,5	22,1
UDP	27,2	27,8	28,4	28	28,2	28,5

Table 8 - Measured throughput between MAP1 and MAP2

	MAP2 -> MPP			**MPP -> MAP2**		
	MIN (Mbps)	**AVE (Mbps)**	**MAX (Mbps)**	**MIN (Mbps)**	**AVE (Mbps)**	**MAX (Mbps)**
TCP	8,5	8,9	9,1	8,9	9,2	9,5
UDP	11,3	11,8	12,1	12,2	12,5	12,7

Table 9 - Measured throughput between MPP and MAP2

These obtained values are according to the expected. UDP throughput is larger than TCP throughput, since TCP packets are connection oriented and will perform a 3-way handshake while

UDP packets are connectionless. The available bandwidth between MAPs and the MPP decreases as the number of hops increases.

6.2.3. STA to Backbone Throughput

We connected wirelessly one STA to the mesh network and with Iperf measured throughput to the backbone, on the nine points described in section 6.2.1, for both TCP and UDP. Traffic generation was described in section 6.2.2.

Table 10 presents the results for TCP and Table 11 for UDP.

		BACKBONE TO MOBILE			MOBILE TO BACKBONE		
AP	**POINT**	**MIN (Mbps)**	**AVE (Mbps)**	**MAX (Mbps)**	**MIN (Mbps)**	**AVE (Mbps)**	**MAX (Mbps)**
1	**1**	22,4	22,5	22,6	21,1	22	22,3
	2	20,4	20,8	21,2	20,5	20,9	21,4
	3	21,8	22,1	22,3	20,7	21,3	22,2
	4	22	22,2	22,5	21	21,2	21,4
2	**5**	16,7	17,3	17,8	16	16,1	16,4
	6	17,7	17,9	18	15,7	16	16,4
	7	17,5	18	18,2	16,2	16,8	17,1
3	**8**	9,4	9,5	9,6	8,7	8,8	9,1
	9	9,5	9,6	9,8	8,8	9	9,4

Table 10 - Measured TCP Throughput

		BACKBONE TO MOBILE			MOBILE TO BACKBONE		
AP	**POINT**	**MIN (Mbps)**	**AVE (Mbps)**	**MAX (Mbps)**	**MIN (Mbps)**	**AVE (Mbps)**	**MAX (Mbps)**
1	**1**	27,9	28	28,1	25	25,5	26
	2	27,5	27,7	27,9	23,9	25	25,2
	3	27,7	28	28,2	25,6	26,1	26,4
	4	27,5	27,6	27,7	24	24,4	25
2	**5**	22,1	22,3	22,4	20,5	21,1	21,5
	6	22,5	22,5	23	21,1	21,5	21,6
	7	22,2	22,7	23,5	22	22,5	22,7
3	**8**	12,6	12,7	12,8	11,9	12,1	12,2
	9	12,6	12,8	12,9	12,2	12,4	12,6

Table 11 - Measured UDP Throughput

These values are according to the expected and in concordance with the measured values in the previous section. As a STA moves away from the MPP jumping to another MAP, the available bandwidth decreases with the number of hops.

6.2.4. Observations

Evaluating the characteristics of our network coverage we observe two possible roaming points and guarantee full coverage in the test area.

From the throughput results obtained between MAPs, we can observe that the best throughput performance is achieved between MAP1 and MAP2, which can be explained by the fact that between them there is less interference due to fewer obstacles. We measured an average of 27.8 Mbps UDP Downlink (DL) and 28.2 Mbps UDP Uplink (UL), and 22.2 Mbps TCP DL and 21.5 TCP UL.

Looking at the results from STA throughput test to the backbone, we observe that STAs near the MPP have better throughput performance than STAs far from the MPP on other nodes. We measured a maximum average throughput of 28 Mbps UDP DL and 26.1 Mbps UDP UL, and 22.5 Mbps TCP DL and 22 Mbps TCP UL. We observe that the available bandwidth for mesh links and STA access is not shared between the two radios. We can observe that throughput remains the same within the AP's coverage area, with very low variations on the average value. We can also observe that the farther the node, the smaller the throughput between it and MPP.

6.3. Roaming Between MAPs

In this section we will test roaming capabilities of our WMN and identify the effect of roaming on real-media to and from the STA.

To support the smooth handover of a roaming station, our equipment relays on an Inter Access Point Protocol (IAPP) designed by Proxim that ensures fast update of bridge tables, in order to avoid loose traffic that is directed to the station. IAPP carries information that is used by the MAPs to build a Basic Service Set Identifier (BSSID)-to-IP conversion table. The table is used by the "new" MAP to relate the BSSID to the IP address of the "old" MAP, which is used by the roaming station to identify its "old" MAP.

When a MAP starts up it broadcasts an IAPP "Announce Request", by sending this message to an IP Multicast Destination Address (224.0.1.76), asking other MAPs to make themselves known. Other MAPs already operational in the same network will respond with an IAPP "Announce Response". When all responses are received the "new" MAP issues an IAPP "Announce Response" to indicate its operational status. Each MAP sends two IAPP messages, one for each radio interface.

The above process can be seen on the captures done on the Backbone with Wireshark and depicted on Figure 54, Figure 55 and Figure 56. MAP3 enters the network in which MPP and MAP1 are already operational. Figure 54 and Figure 55 depict a capture of the IAPP “Announcement Requests” for Radio A and Radio B respectively.

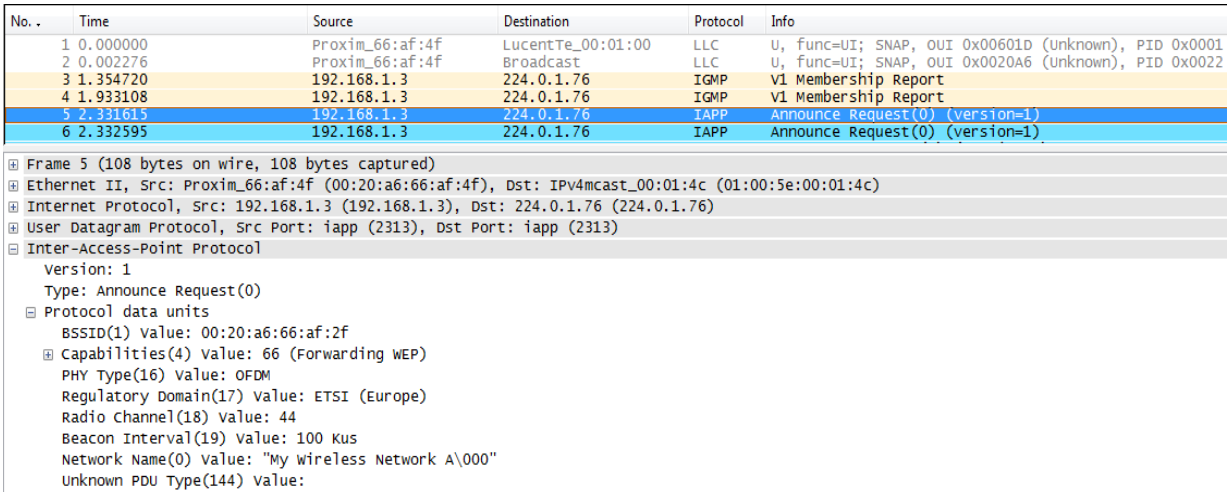

Figure 54 - IAPP Announce Request - Radio A

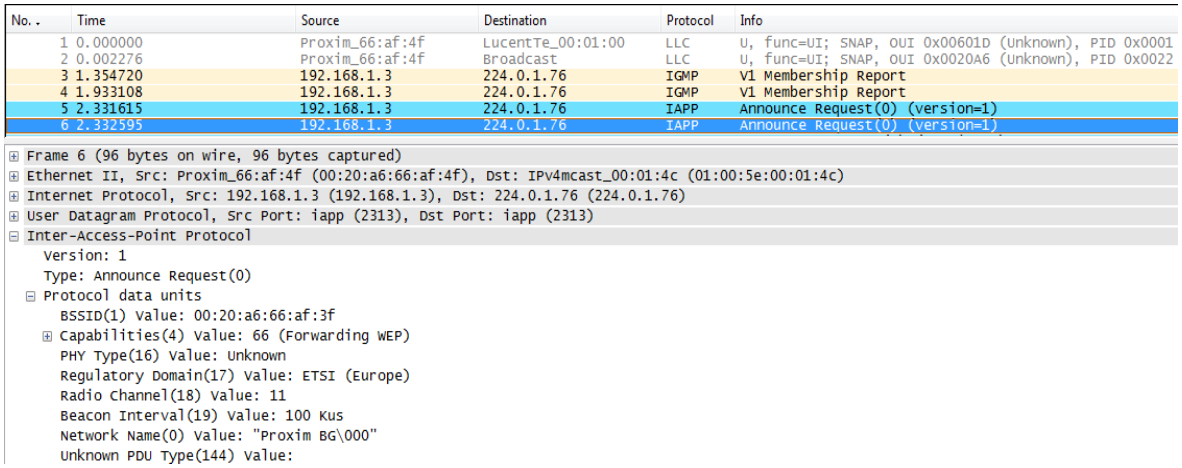

Figure 55 - IAPP Announce Request - Radio B

Figure 56 depicts a capture of the IAPP “Announce Responses” from MPP and MAP2 after the “Announce Request” from MAP3.

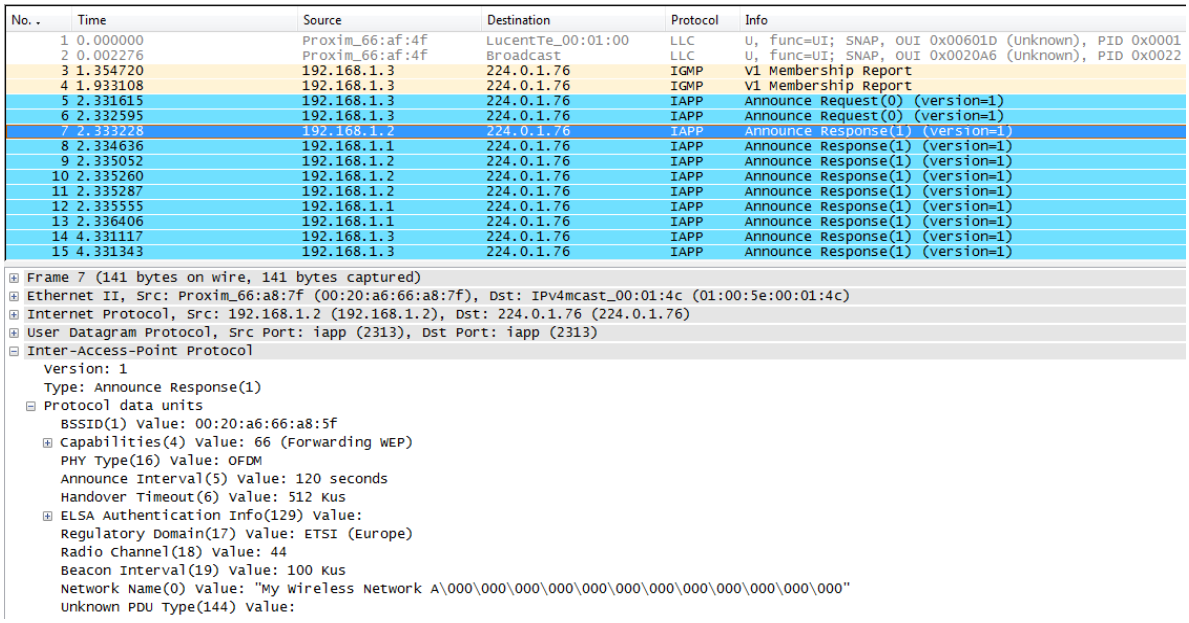

Figure 56 - IAPP Announce Responses

Now that all MAPs have their bridge tables updated with the identification of the other MAPs in the network. We can test the effects of roaming on real-media traffic directed to and from the STA. In order to evaluate the effects of roaming, we used a laptop running Windows XP operating system and changed roaming parameters to from medium (the STA will only roam if the RSSI from original AP is very low and much lower than the RSSI from another AP in the vicinity) to aggressive (the STA roams as soon as a better RSSI from other AP is achieved). This laptop was also running a virtual Ubuntu Linux operating system on the Windows background so that we could use JTG to emulate the real-media traffic. Virtualization was achieved through the use of VirtualBox [59], an open source desktop virtualization software. We had to use this topology as we could not configure roaming parameters in the wireless card on STA1 due to Linux kernel problems.

To ensure that all handover requests passed through the MPP we created a Dynamic Host Configuration Protocol (DHCP) server on MPP in order to simulate DHCP requests to the Backbone. After entering the network the STA received the IP Address 192.168.1.51.

We run two script files using JTG on both STA and Backbone generating a simultaneous bidirectional VoIP and VoD flow with duration of 360 seconds. We performed multiple handovers by roaming between MAPs, as depicted Figure 57.

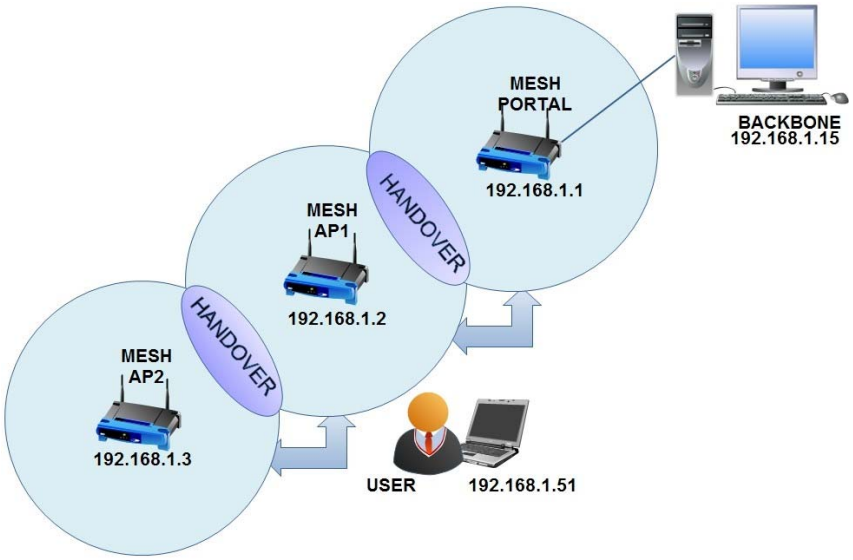

Figure 57 - Roaming in IEEE 802.11 WMN

Using Wireshark on the STA's Ubuntu virtual desktop we captured all traffic exchange between the STA and the Backbone. Unfortunately, aggressive roaming was not working properly on the used STA for these experiments, as the STA did not roam between the MPP and MAP1 when traveling from MPP to MAP2, but between MPP to MAP2. Thus, we used "Wi-Fi Hooper's" option to force roaming and manually roamed between MAPs as we reached the probable roaming points.

We performed a total of 20 handovers during the experiment and measured the delay between the DHCP request and DHCP acknowledgement for each one. The first handover capture is depicted in Figure 58 and Figure 59 with the capture of the DHCP Request and Acknowledgement, respectively.

```
   8519 36.400928   192.168.1.63          192.168.1.15          UDP      Source port: 58444  Destination port: commplex-link
   8520 36.408905   192.168.1.63          192.168.1.15          UDP      Source port: 49565  Destination port: 3001
   8521 36.410008   192.168.1.15          192.168.1.63          UDP      Source port: 33153  Destination port: newoak
   8522 36.411014   192.168.1.51          255.255.255.255       DHCP     DHCP Request  - Transaction ID 0x328b0a20
   8523 36.414641   192.168.1.1           192.168.1.51          DHCP     DHCP ACK      - Transaction ID 0x328b0a20
   8524 36.417299   192.168.1.63          192.168.1.15          UDP      Source port: 49851  Destination port: newoak
   8525 36.421009   192.168.1.15          192.168.1.63          UDP      Source port: 33151  Destination port: 3001
   8526 36.421322   192.168.1.63          192.168.1.15          UDP      Source port: 58444  Destination port: commplex-link
⊞ Frame 8522 (342 bytes on wire, 342 bytes captured)
⊞ Ethernet II, Src: IntelCor_10:cf:49 (00:1f:3b:10:cf:49), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
⊞ Internet Protocol, Src: 192.168.1.51 (192.168.1.51), Dst: 255.255.255.255 (255.255.255.255)
⊞ User Datagram Protocol, Src Port: bootpc (68), Dst Port: bootps (67)
⊟ Bootstrap Protocol
    Message type: Boot Request (1)
    Hardware type: Ethernet
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0x328b0a20
    Seconds elapsed: 0
  ⊞ Bootp flags: 0x0000 (Unicast)
    Client IP address: 192.168.1.51 (192.168.1.51)
    Your (client) IP address: 0.0.0.0 (0.0.0.0)
    Next server IP address: 0.0.0.0 (0.0.0.0)
    Relay agent IP address: 0.0.0.0 (0.0.0.0)
    Client MAC address: IntelCor_10:cf:49 (00:1f:3b:10:cf:49)
```

Figure 58 - DHCP Request

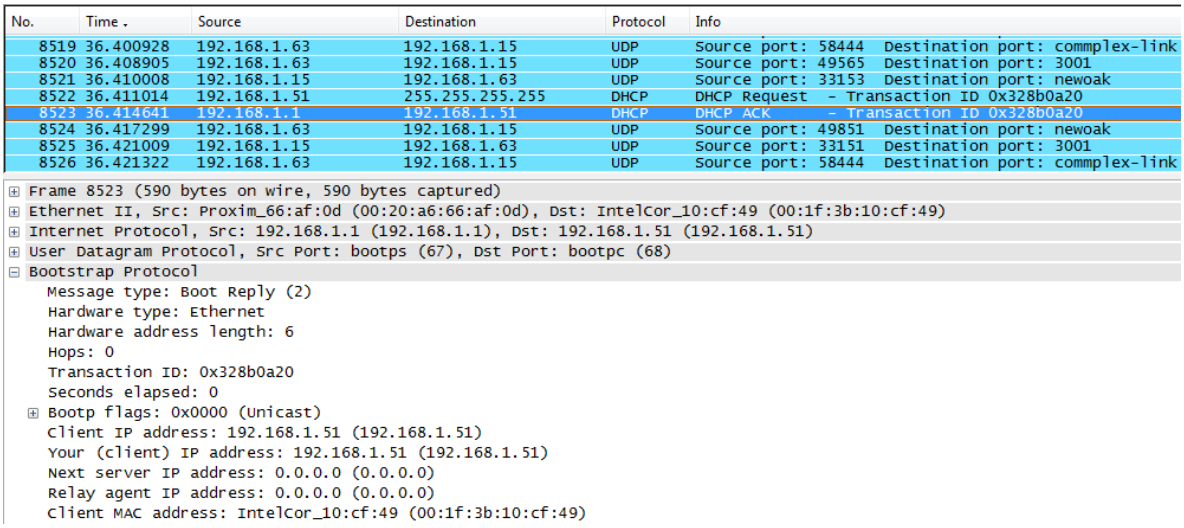

Figure 59 - DHCP Acknowledgement

Figure 60 depictes the delay of each handover. The results sequence from 1st to 12th relate to handover between MAP2-MPP-MAP2, ending at MPP. Result number 13 relates to a handover between MPP and MAP3 as we walked from the MPP to MP2 without forcing a handover. Remaining results relate to handover between MAP3-MAP2-MAP3, ending at MAP2.

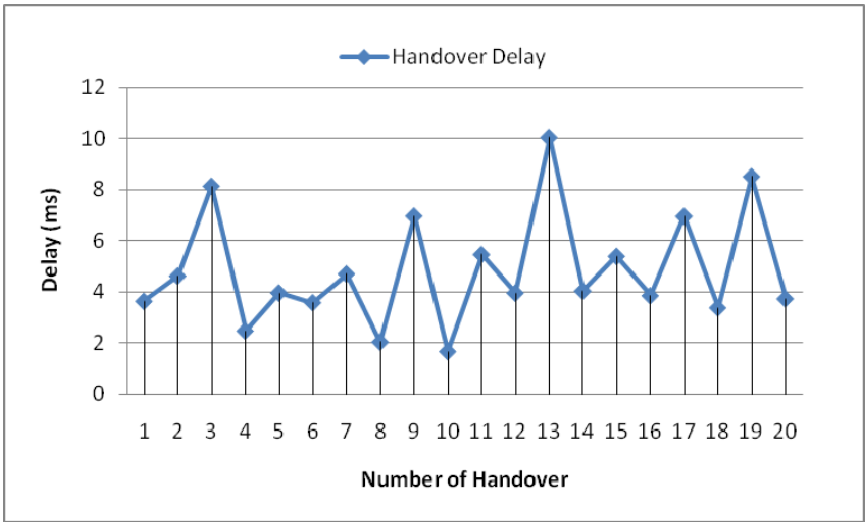

Figure 60 - Handover Delay

6.3.1. Observations

From the obtained results, we verify that the handover delay is more accentuated when roaming is performed to a MAP that is far away from the network DCHP server. Maximum delay was achieved when we roamed from MPP to MAP3. As for the impact on real-media streaming we observed no packet loss. Unfortunately we could not measure with JTG the delay and variation of each individual flow due to clock synchronization issues in VirtualBox between the host and the guest virtual machine. Still, the overall delay introduced by 20 handovers in a period of 360 seconds was 97.02 ms (achieved by adding all 20 handover delays) and the maximum delay achieved in one handover was 10.05 ms, we can conclude that roaming happens smoothly and does not present significant effects on real-media transmission.

6.4. VoIP and VoD services on WMNs

At this section, we describe the performance tests of our testbed by injecting simultaneously a bidirectional VoIP and VoD flows between STA1 and the Backbone. Traffic is generated to and from fixed spots in the cells with competing TCP flows on background, without any QoS and with QoS. The presented results for VoIP and VoD are individual. Each flow has duration of 60 seconds. The tests were performed in Points 3, 5 and 8 (see Figure 50). To perform the tests for VoIP and VoD services, we have followed the steps described as follows:

- **Starting PTPd**

First, we run the shell scripts using PTPd for both for server and client, and wait for 10 minutes to ensure clock synchronization before starting the tests.

- **Emulating traffic with IPERF**

After clock synchronization, we generate multiple bi-directional TCP flows from each STA to the backbone and wait for 60 seconds before generating real-time media to ensure we have saturated our WMN.

- **Emulating traffic with JTG**

In order to test VoIP and VoD capacity inside the WMN, we generate a bidirectional VoIP stream and a bidirectional VoD stream between our mobile STA (192.168.1.50) and the backbone PC, yielding an application throughput of 1.77 Mbps. This is only 7.1% of the total goodput of the STA-MPP link, 8.4% of the STA-MAP2-MPP link, and 15% of the STA-MAP3-MAP2-MPP. Still, this is the most likely scenario to the user. With multiple background TCP flows coming from all MAP to the backbone, we can congest the network enough to lose quality on the single user real-media transfer, so this is a viable scenario for our tests.

6.4.1. VoIP and VoD over non-QoS WMN without background TCP

This section presents our measurements for VoIP and VoD traffic under a non-QoS wireless mesh architecture without any background TCP traffic. We run a shell script on both Backbone and STA1 that uses JTG to wait for incoming traffic from each other and another script that uses JTG to generate a simultaneous bidirectional VoIP and VoD flow. The measured results for one way delay, packet delay variation (PDV) and packet loss are described in Table 12, for both uplink and downlink scenario.

			BACKBONE TO MOBILE			MOBILE TO BACKBONE		
AP	POINT	Data Flow	Delay (ms)	IPDV (ms)	Packet Loss (%)	Delay (ms)	IPDV (ms)	Packet Loss (%)
MPP	3	VoIP	2,13	1,64	0	2,29	1,47	0
		Video	2,51	1,57	0	2,61	1,5	0
		Audio	2,25	1,89	0	2,48	1,7	0
MAP2	5	VoIP	2,37	1,48	0	2,69	1,41	0
		Video	2,95	1,52	0	3,58	1,67	0
		Audio	2,57	1,7	0	3,23	1,67	0
MAP3	8	VoIP	2,12	1,35	0	2,62	1,48	0
		Video	2,89	1,4	0	2,88	1,22	0
		Audio	2,35	1,4	0	2,21	1,92	0

Table 12 - Results for VoIP and VoD over non-QoS WMN without TCP

From the measured results we conclude that without traffic differentiation and added background traffic, all traffic classes behave similarly, with values for delay and PDV very close to each other. As expected, no packets were loss.

6.4.2. VoIP and VoD over non-QoS WMN with background TCP

This section presents our measurements for VoIP and VoD traffic under a non-QoS wireless mesh architecture with background TCP traffic. After connecting wirelessly STA2 to MPP, STA3 to MAP2 and STA4 to MAP3 in the network, we use Iperf to generate 10 simultaneous bidirectional TCP flows from each of them to the Backbone in order to congest our network. We run a shell script on both Backbone and STA1 that uses JTG as described in section 6.4.1 for traffic generation. The measured results for one way delay, packet delay variation (PDV) and packet loss are described in Table 13, for both uplink and downlink scenario.

			BACKBONE TO MOBILE			MOBILE TO BACKBONE		
AP	POINT	Data Flow	Delay (ms)	IPDV (ms)	Packet Loss (%)	Delay (ms)	IPDV (ms)	Packet Loss (%)
MPP	3	VoIP	5,45	4,1	0,23	10,93	5,43	0
		Video	5,47	3,53	0,37	12,3	6,29	0
		Audio	5,24	4,05	0,18	11,78	6,48	0
MAP2	5	VoIP	149,21	5,64	0,3	162,91	6,72	2,03
		Video	150,71	5,82	4,78	162,93	6,91	2
		Audio	149,48	6,16	4,46	163,16	7,11	1,92
MAP3	8	VoIP	166,36	7,22	2,9	190,68	8,69	2,36
		Video	165,72	7,14	10,76	191,03	7,76	2,5
		Audio	165,89	8,17	10,6	191,2	9,3	2,41

Table 13 - Results for VoIP and VoD over non-QoS WMN with TCP

The presented results allow us to conclude that in a congested WMN the performance for real-media is very poor. After one hop from the MPP to MAP2 delay increases drastically and packet loss overflows the maximum tolerable values. We can also conclude that there is good performance within MPP coverage area as opposed to the others. This is due to the fact that in the coverage area of MPP an STA has a larger available bandwidth, which is only shared with 10 TCP flows, while an STA within the coverage area of MAP2 or MAP3 not only has to deal with smaller bandwidth but also with double competing TCP flows.

6.4.3. VoIP and VoD over QoS WMN with background TCP

This section presents our measurements for VoIP and VoD traffic under a QoS wireless mesh architecture with background TCP traffic. Before performing any measurements we must first enable QoS as described in section 6.1.3. We use Iperf to generate 10 simultaneous bidirectional TCP flows from each STA to the Backbone in order to congest our network, as described in section 6.4.2. To ensure that QoS is active for VoIP and VoD services, we change our JTG scripts and add an IP DSCP value to the flows. Given the chosen configuration in section 6.1.3, we have the following relation between the IP DSCP values and the four access categories described in Table 14:

IEEE 802.1D Priority	DSCP Lower Range	DSCP Upper Range	802.11e AC
0 (Best Effort)	0	7	Background
1 (Background)	8	15	Background
2 (-)	16	23	Best Effort
3 (Excellent Effort)	24	31	Best Effort
4 (Controlled Load)	32	39	Video
5 (Video < 100ms latency and jitter)	40	47	Video
6 (Voice < 10ms latency and jitter)	48	55	Voice
7 (Network Control)	56	63	Voice

Table 14 – 802.1D Priority to 802.11e AC

Thus, we chose for VoIP flows to have an IP DSCP value of 48 and Audio and Video flows to have an IP DSCP value 40.

We run a shell script on both Backbone and STA1 that uses JTG as described in section 6.4.1 for traffic generation. The measured results for one way delay, packet delay variation (PDV) and packet loss are described in Table 15, for both uplink and downlink scenario.

			BACKBONE TO MOBILE			MOBILE TO BACKBONE		
AP	POINT	Data Flow	Delay (ms)	IPDV (ms)	Packet Loss (%)	Delay (ms)	IPDV (ms)	Packet Loss (%)
MPP	3	VoIP	1,49	0,78	0	3,68	2,01	0
		Video	2,56	1,32	0	6,32	3,42	0
		Audio	1,86	0,79	0	4,29	2,28	0
MAP2	5	VoIP	4,92	3,44	0	5,35	3,19	0
		Video	6,9	4,31	0	8,24	5,96	0
		Audio	5,57	3,84	0	5,59	2,94	0
MAP3	8	VoIP	5	2,59	0	5,3	4,4	0
		Video	10,44	7,22	0	11,67	5,56	0
		Audio	5,61	3,32	0	6,47	5,67	0

Table 15 - Results for VoIP and VoD over QoS WMN with TCP

Looking at the obtained results we can conclude that the EDCA provides differentiated and distributed access to the wireless medium, with VoIP presenting the best results within the differentiated traffic, followed by audio and finally video. We can also conclude that as we go further away from the MPP delay values increase for all traffic, independent of their Access Categories (ACs), and that within the same AC smaller packets obtain better results than larger ones. Although the QoS defined parameters were the default ones, we can conclude that a congested QoS WMN can support real-media streaming without visual impact to the user.

6.4.4. Observations

Comparing the results from the three scenarios we can conclude that a QoS policy must be implemented in order to ensure good performance in real-media transmission. When the network is congested, traffic from a STA, which is connected far from the MPP, suffers an increase on delay related with the number of hops to the portal and concurrent TCP flows. VoIP is the service with best performance, not suffering much on performance as the STA moves away from the MPP. VoIP packets are the first to be sent to the medium and since they are small they can easily cross a congested medium with larger TCP packets. Within VoD service, video packets have the biggest delay and delay variation due to their size, while the smaller audio packets, with same priority as the video ones, do not have to wait so long and can cross the congested medium faster than video.

6.5. Experiments Conclusions

With these experiments, we tried to understand the real performance provided by today's IEEE 802.11 Mesh equipments. From the results obtained from section 6.2 we conclude that WMN provide good throughput on a multi-radio topology throughout the covered network area. From section 6.3, we conclude that handover occurs smoothly during roaming, without affecting real-media transmissions. From section 6.4, we conclude that WMN allows us to provide QoS for different traffics through a distributed and differentiated access scheme, ensuring good performance for real-media traffic. We can conclude that a QoS scenario on a WMN can sustain real-media backhauling.

7. Conclusions

The work presented in this thesis addresses the performance evaluation of next generation broadband wireless access technologies, WiMAX and Meshed Wi-Fi, in dealing with real-time media. In this section we provide a final conclusion to our work and address possible topics for future work.

7.1. Final Conclusion

In this thesis, we have conducted an experimental evaluation of real-time services, such as VoIP and VoD, over IEEE 802.16 in different modes of operation: as VoIP backhaul, VoD backhaul, and VoIP/VoD backhaul. Thus, with the three different modes of operation several tests with different characteristics were exploited, not only with Best Effort traffic, but also establishing different service classes for each traffic flow, in order to obtain the real capacities of Proxim Wireless equipment at resource allocation. We concluded that our Proxim Wireless equipment can sustain individual and combined VoIP and VoD backhauling during network congestion. In a congested QoS network with up to 40 bidirectional TCP flows, we emulated 10 VoIP and 5 VoD streams, acquiring adequate application-level throughput, with one way delay, packet variation and packet loss well below the proper bounds. Results also show that due to the TDD scheme, the uplink presents larger delay values than downlink, but still well within the tolerable ones. Best Effort results lead us to conclude that QoS is mandatory for real-media streaming in IEEE 802.16.

This thesis also evaluated the performance of an IEEE 802.11 Wireless Mesh Network (WMN) on both available resources and support of real-time services. Using “WiFi Hopper”, we were able to measure accurately the RSSI on the entire network performing throughput tests with Iperf on 9 measuring points representative of different network attached conditions. We concluded that on an indoor implementation the distance to the AP does not influence the available channel throughput, as results show very little variation. We also tested the effects of handover during real-time transmissions on a bidirectional VoIP and VoD flow while roaming within the network coverage area. We created a DHCP server on the Mesh Portal (MPP) in order to emulate an outside DHCP server as requests have to pass through MPP. Results show that the farther away we get from the MPP the larger is the delay introduced by the handover. Still the delay value does not affect the quality of the received stream with no visible packet losses. Finally we tested the capacity of our WMN to support real-media transmission by evaluating both a Best Effort and QoS scenarios. We concluded that inside the coverage area of the MPP the QoS does not necessarily need to be implemented, as delay and variation values are well within the tolerable ones, due to the larger available bandwidth and proximity to backhaul. As we move away from the MPP the delay, variation and packet loss measure show that only with a QoS implementation we have quality transmission on real-time media. Using the EDCA scheme, we concluded that IEEE 802.11 WMNs have good performance in real-media transmission between users and backhaul when QoS is implemented.

7.2. Future Work

After analyzing independently both WiMAX and Meshed Wi-Fi technologies through the evaluation of the performance of licensed equipments, we decided to analyze a WiMAX/Wi-Fi network topology with WiMAX as a backhaul to the Meshed Wi-Fi network. Unfortunately we were not able to perform such tests due to equipment malfunction. Every time we connected a switch, router or hub to our Meshed network through the MPP the mesh links broke and connectivity was lost within the network. The only way to resume correct operation was to reset the equipments and connect the MPP to a computer. We tried several different routing equipments with the same result. Another problem we had is reported in section 6.1.3 as we were not able to create QoS profiles with different CWs and AIFSN to analyze different implementations of the EDCA, or DSCP values to analyze a collaborative QoS with DiffServ. After contacting Proxim Wireless a new firmware was released that was supposed to correct these malfunctions. Unfortunately that was not the case. Thus, as the next step for future work, these combined tests should be conducted as soon as a new firmware release can correct these bugs.

8. REFERENCES

[1] Anand R. Prasad, and Neeli R. Prasad, “802.11 WLANs and IP Networking”, Artech House, London, 2005.

[2] “Wireless LAN medium access control (MAC) and physical layer (PHY) specifications”, IEEE Standard 802.11, 1999.

[3] Qiang Ni, et al. Journal of Wireless Communications and Mobile Computing, Wiley. 2004: Volume 4, Issue 5: pp.547-566.

[4] Matthew Gast, “802.11 Wireless Networks – The Definitive Guide”, O’Reilly, 2005.

[5] ”Tutorial 802.11ABG Demystified”, Xirrus, 2008.

[6] Stefan Mangold, Sunghyun Choi, Guido R. Hiertzm Ole Klein, and Bernhard Walke, “Analysis of IEEE 802.11e for QoS Support in Wireless LANs”, IEEE Wireless Communications, 2003.

[7] Marcelo G. Rubinstein, and José Ferreira de Rezende, “Qualidade de Serviço em Redes 802.11”, Universidade Estadual do Rio de Janeiro, 2007.

[8] URL: http://www.terabeam.com/solutions/whitepapers/tutorial_80211.php.

[9] “Wireless LAN medium access control (MAC) and physical layer (PHY) specifications: Higher Speed Physical Layer (PHY) extension in the 2.4GHz band”, IEEE Standard 802.11, 1999.

[10] “Wireless LAN medium access control (MAC) and physical layer (PHY) specifications: High-speed Physical Layer (PHY) in the 5GHz band”, IEEE Standard 802.11, 1999.

[11] “Wireless Medium Access Control (MAC) and physical layer (PHY) specifications: Medium Access Control (MAC) Enhancements for Quality of Service (QoS), IEEE 802.11e/D2.0, Nov. 2001.

[12] IEEE 802.1D-1998, Part3: Media Access Control (MAC) Bridges, ANSI/IEEE Std. 802.1D, 1998.

[13] Saurabh Sehrawat, and Revoti Prasad Bora, and Dheeraj Harihar, “Performance Analysis of QoS supported by Enhanced Distributed Channel Access (EDCA) mechanism in IEEE 802.11e”, International Journal of Computer Science, 2006.

[14] Seyong Park, and Kyungtae Kim, and Doug C. Kim, and Sunghyun Choi, and Sangjin Hong, “Collaborative QoS Architecture between DiffServ an 802.11e Wireless LAN”.

[15] IEEE 802.1Q-1998, “Virtual Bridge Local Area Networks, ANSI/IEEE Std. 802.1Q”, 1998 edition, 1998.

[16] RFC 2475, “An Architecture for Differentiated Services”, December 1998.

[17] C. Silva Ram Murphy, and B.S. Manoj, “Ad hoc Wireless Networks: Aerchitectures and Protocols”, Prentice Hall, New Jersey, May 2004

[18] Yan Zhang, and Jijun Luo, and Honglin Hu, “Wireless Mesh Networking: Architectures, Protocols and Standards”, Aucherbach Publications, 2007

[19] Ian F. Akylidiz, Weilin Wang, Xudong Wang, “Wireless mesh networks: a survey”, 15 March, 2005

[20] “Wireless Medium Access Control (MAC) and physical layer (PHY) specifications: Amendment: ESS Mesh Networking, IEEE 802.11s/D1.0, November 2006.

[21] Xudong Wang, and Azman O. Lim, “IEEE 802.11s wireless mesh networks: Framework and challenges”, Elsevier B.V., October 2007

[22] Raffaele Bruno, and Marco Conti, and Enrico Gregori, “Mesh Networks: Commodity Multihop Ad Hoc Networks”, IEEE Communications Magazine, March 2005

[23] “Mesh Technology Primer”, Position Paper, May 2005

[24] C. Perkins, and E. Belding-Royer, and S. Das, “Ad hoc on demand distance vector (AODV) routing,” IETF RFC 3561, July 2003

[25] T. Clausen and P. Jacquet, Optimized Link State Routing Protocol (OLSR), RFC 3626, IETF, October 2003.

[26] “Overview of Wireless Multimedia (WMM™) in Wireless LANs”, Technical Bulletin, Proxim, November 2004

[27] “Inter Access Point Protocol (IAPP)”, Technical Bulletin, Proxim, November 2002

[28]Proxim Wireless, URL: http://www.proxim.com

[29]J.Manner, Jugi’s Traffic Generator (JTG), URL:”http://hoslab.cs.helsinki.fi/savane/projects/jtg”

[30] IPERF, URL: http://dast.nlanr.net/Projects/Iperf/

[31] Precision clock synchronization protocol for networked measurement and control systems. International standard IEC 61588, 2004

[32] K. Correl, and N. Barendt, and M. Branicky, “Design considerations of the IEEE 1588 Precision Time Protocol”. Conference on IEEE 1588, 2005

[33] VLC Media Player, URL: http://www.videolan.org

[34] J. M. Valin, Speex: A Free Codec for Free Speech. URL: http://www.speex.org

[35] Wireshark, URL: www.wireshark.org/

[36] International Telecommunication Union, “Advanced video coding for generic audiovisual services”, ITU-T Recommendation H.264, 2005

[37] ISO/IEC, “Information technology - Coding of moving pictures and associated audio for digital storage media at up to about 1.5 Mbit/s – Part 3: Audio”, ISO/IEC 11172-3, 1993.

[38] H. Schulzrinne, A. Rao, and R. Lanphier,” Real Time Streaming Protocol (RTSP)”, RFC 2326, April 1998.

[39] H. Schulzrinne, S. Casner, R. Frederick, and V. Jacobson,” RTP: A Transport Protocol for Real-Time Applications”, RFC 3550, July 2003.

[40] Tsunami MP.16 3500 System User Guide V1.3, Proxim Wireless

[41] Kostas Pentikousis, and Esa Piri, and Jarno Pinola, and Ferk Fitzek, and Tuomas Nissilã, “Empirical Evaluation of VoiP Aggregation over a Fixed WiMAX Testbed”, Tridentcom, 2008

[42] Esa Piri, and Jarno Pinola, and Ferk Fitzek, and Kostas Pentikousis, “ROCH and Aggregated VoIP over Fixed WiMAX: An Empirical Evaluation”, Tridentcom, 2008

[43] Nicola Scalabrino, and Francesco De Pellegrini, and Roberto Riggio, and Andrea Maestrini, and Cristina Costa, and Imrich Chlamtac, “Measuring the Quality of VoIP Traffic on a WiMAX Testbed”, Create-net, 2005

[44] Nicola Scalabrino, and Francesco De Pellegrini, and Imrich Chlamtac, “Performance Evaluation of a WiMAX Testbed under VoIP Traffic”, Wintech’06, 2006

[45] Esa Piri, and Jarno Pinola, and Ferk Fitzek, and Kostas Pentikousis, “An Experimental Invesigation of VoIP and Video Streaming over Fixed WiMAX”, Tridentcom, 2008

[46] Edwin W.C. Peh, and Winston K.G. Seah, and Y.H Chew, and Y.Ge, “Experiemental Study of Voice over IP Services over Broadband Wireless Networks”, IEEE, 2008

[47] Emir Halepovic, and Qian Wu, and Carey Williamson, and Majid Ghaderi, “TCP over WiMAX: A Measurement Study”, IEEE, 2008

[48] Supriya Mahaeshwari, and Sridhar Iyer, and Kishna Paul, “An Efficient QoS Scheduling Architecture for IEEE 802.16 Wireless MANs”, International Mobile Computing Conference, Jan. 2006

[49] Colin Perkins, “RTP: Audio and Video for the Internet”, chapter 6, Addison-Wesley Professional, 2003

[50] Stephen R. Gulliver, and Gheorghita Ghinea, “THE PERCEPTUAL INFLUENCE OF MULTIMEDIA DELAY AND JITTER”, IEEE 2007

[51] Michael F. Finneran, “VoIP quality issues: Jitter, delay and echo”, EE-Times India, 2008

[52] URL: http://www.voip-info.org/wiki/view/QoS

[53] Emir Halepovic, and Majid Ghaderi, and Carey Williamson, “Multimedia Application Performance on a WiMAX Network”, University of Calgary, 2008

[54] IEEE 802.162004,” IEEE Standard for Local and Metropolitan Area Networks Part 16: Air Interface for Fixed Broadband Wireless Access Systems”, 1 October, 2004

[55] R.V. Nee & R. Prasad, *OFDM for Wireless Multimedia Communications*. Artech House Publishers, 2000.

[56] WiFi Hopper, URL: “http://www.wifihopper.com”

[57] Orinoco AP4000-MR User Guide, URL: “http://www.proxim.com”

[58] Seyong Park, and Kyungtae Kim, and Doug C. Kim, and Sunghyun Choi, and Sangjin Hong, “Collaborative QoS Architecture between DiffServ and 802.11 Wireless LAN”, Vehicular Technology Conference, 2003

[59] Orinoco Technical Bulletin, “Inter Access Point Protocol (IAPP)”, Proxim Wireless, 2001

[60] Hai Jiang, and Ping Wang, and Weihua Zhuang, “A Distributed Channel Access Scheme with Guaranteed Priority and Enhanced Fairness”, IEEE, 2007

[61] VirtualBox, URL: http://www.virtualbox.org