Universidade de Aveiro

2009

Departamento de Electrónica, Telecomunicações e Informática

Cláudia Sofia Rodrigues Sequeira

Avaliação do Desempenho de Novos Serviços em Redes IP

Universidade de Aveiro

2009

Departamento de Electrónica, Telecomunicações e Informática

Cláudia Sofia Rodrigues Sequeira

Avaliação do Desempenho de Novos Serviços em Redes IP

Dissertação apresentada à Universidade de Aveiro para cumprimento dos requisitos necessários à obtenção do grau de Mestre em ~~(designação do mestrado)~~ Engenharia Electrónica, realizada sob a orientação científica do Professora Dra. Susana Sargento, Professora auxiliar do Departamento de Electrónica, Telecomunicações e Informática da Universidade de Aveiro e do Professor Dr. António Nogueira, Professor auxiliar do Departamento de Electrónica, Telecomunicações e Informática da Universidade de Aveiro.

Dedico este trabalho a:

Jorge, Glória, David, Suzie, Diana, Filipe, Inês, Jorge, Hugo e Nuno.

o júri

Presidente	Prof. Dr. Atílio Manuel Silva Gameiro, Professor associado do Departamento de Electrónica, Telecomunicações e Informática da Universidade de Aveiro.
Orientador	Prof. Dra. Susana Isabel Barreto de Miranda Sargento, Professora auxiliar do Departamento de Electrónica, Telecomunicações e Informática da Universidade de Aveiro.
Co-orientador	Prof. Dr. António Manuel Duarte Nogueira, Professor auxiliar do Departamento de Electrónica, Telecomunicações e Informática da Universidade de Aveiro.
Arguente	Prof. Dr. Manuel Alberto Pereira Ricardo, Professor associado do Departamento de Eng. Electrotécnica e de Computadores da Faculdade de Engenharia da Universidade do Porto.

Agradecimentos

Este trabalho não teria sido possível sem a contribuição de algumas pessoas, as quais quero aqui deixar os mais sinceros agradecimentos.

Primeiramente, gostaria agradecer a Professora Susana Sargento, pela disponibilidade que sempre demonstrou mas também pelo apoio e motivação que sempre incutiu.

Ao meu co-orientador Miguel Almeida, por me ter instruído ao longo de todo este trabalho, pela paciência e apoio.

Ao Filipe Santos, pelas úteis sugestões e por todas as interessantes discussões.

Aos meus amigos André Cardote e André Reis, por todos os conhecimentos partilhados, mas acima de tudo pela amizade.

Ao Instituto de Telecomunicações de Aveiro por me ter oferecido todo o apoio e condições necessárias para o correcto desenvolvimento do meu trabalho.

A Nokia Siemens Networks, que me ofereceu as condições necessárias, um especial agradecimento ao Rafael Sarro, João Monteiro e Rui Leal que muitas vezes suportaram as minhas actividades.

Aos meus Pais, Irmãos e sobrinhos por todo o carinho, apoio e compreensão.

palavras-chave QoS, IPTV, VoIP, monitorização,desempenho, medidas, requisitos.

resumo

Os benefícios económicos de fornecer múltiplos serviços numa única rede têm despertado grande interesse na introdução dos serviços VoIP e IPTV na internet. No entanto, estes serviços possuem requisitos rigorosos de qualidade de serviço, que a internet não está preparada para fornecer.

Esta dissertação possui dois objectivos principais:

O primeiro consiste em testar o comportamento dos serviços de IPTV e VoIP nas tecnologias IP existentes como Ethernet, IEEE 802.11 e ADSL quando expostas a diferentes condições de carga. Pretende-se também identificar os efeitos nos serviços de VoIP e IPTV de outros serviços como FTP, correio electrónico e HTTP. Foi utilizado OpNet um simulador de redes bastante popular ao no ambiente académico. Os resultados das simulações fornecem orientações importantes sobre a capacidade máxima de cada tecnologia tendo em conta os requisitos de qualidade de serviço; por outro lado identificam os serviços mais destrutivos para IPTV e VoIP.

O segundo objectivo é a implementação de um modelo que permite a monitorização dos serviços de VoIP e IPTV, analisa os indicadores de desempenho reunidos e grava esses indicadores numa base de dados. Todo este processo será efectuado em tempo real com o objectivo de manter a base de dados actualizada.

Os resultados disponibilizados por esta estrutura permitem uma melhor gestão da rede, os prestadores de serviços podem ter informações actualizadas sobre o desempenho dos seus serviços, consequentemente é possível identificar uma falha ou uma tendência futura.

keywords QoS, IPTV, VoIP, monitoring, performance, measurements, requirements.

abstract

The economical benefits of providing multiple services over a single network infrastructure have spawned great interest in the introduction of new services, such VoIP and IPTV, in the Internet. However, these services have stringent Quality of Service requirements that the Internet was not designed to meet. This dissertation has two main objectives:

The first objective is to test the behavior of IPTV and VoIP services in the existing IP network technologies such as Ethernet, IEEE 802.11 and ADSL when exposed to different load conditions; and identify the effects of other services such as FTP, Email and HTTP in VoIP and IPTV demands. In our work we use OpNet, a popular network simulator in the academic environment. The simulation results provide important guidelines about the maximum capacity of each technology keeping in mind QoS requirements; on the other hand, they enable identification of the most damaging services for VoIP and IPTV.

The second objective is the implementation of a framework that allows monitoring VoIP and IPTV services, analyzing the collected performance measurements, and storing them in a database; all these processes will be performed in real time in order to keep the database up to date.

The results available by this framework allow a better network management, the service providers can have current information about their services performance, and consequently it is possible to identify a failure or a future trend.

Content

List of Figures

List of Tables

Acronyms and Symbols

ADSL	Asymmetric Digital Subscriber Line
AP	Access Point
ARPANet	Advanced Research Projects Agency Network
ATM	Asynchronous Transfer Mode
BSS	Basic Service Set
CDR	Call Detail Records
CMIP	Common Management Information Protocol
CMOT	CMIP over TCP/IP
CODEC	Compressor/Decompressor
CSMA/CA	Carrier Sense Multiple Access, Collision Avoidance
CSMA/CD	Carrier Sense Multiple Access, Collision Detection
CSV	Comma Separated Values
CTS	Clear to Send
DFC	Distributed Coordination Functions
DSL	Digital Subscriber Line
DSLAM	Digital Subscriber Line Access Multiplexer
EMS	Element Management System
ETL	Extract, Transform, Load
GOP	Group of Pictures
IEEE	Institute of Electrical and Electronics Engineers
IMS	International Microwave Symposium
IP	Internet Protocol
ITU	International Telecommunication Union
LAN	Local Area Network
MAC	Media Access Control
MF	Mediation Function
MGCP	Media Gateway Control Protocol
MIB	Management Information Base

MODEM	Modulator demodulator
MPEG	Moving Picture Experts Group
NEF	Network Element Function
NSN	Nokia Siemens Networks
NTSC	National Television System Committee
OMeS	Open Measurement Standard
OSF	Operations Systems Function
PFC	Point Co-ordination Function
PGM	Probe Gap Model
PLC	Packet Loss Concealment
PRM	Probe Rate Model
PSTN	Public Switched Telephone Network
QAF	Q Adaptor Function
QoE	Quality of Experience
QoS	Quality of Service
RFC	Request For Comments
RR	Receiver Report
RTCP	RTP Control Protocol
RTP	Real-time Transport Protocol
RTS	Request to Send
RTT	Round Trip Time
SDK	Software Development Kit
SDTV	Standard-Definition Television
SIP	Session Initiation Protocol
SLA	Service Level Agreement
SLM	Service Level Management
SNMP	Simple Network Management Protocol
SR	Sender Report
SSH	Secure Shell
TCP	Transmission Control Protocol

TMN	Telecommunications Management Network
UDP	User Datagram Protocol
VC	Videoconferencing
VLC	Video LAN Client
VoD	Video on Demand
WLAN	Wireless LAN
WSF	Workstation Function
WWW	World Wide Web
XML	Extensible Markup Language

1 Introduction

1.1 Motivation

Born in the mid-1960s, at the time of the Cold War, ARPANET was created by USA Department of Defense that desired a reliable network that could survive to a nuclear war. The main purpose of creating the Internet was to guarantee that information arrives to the final destiny; however, a single level of service quality was provided, the best-effort model, where all packets are treated in the same way.

The adventure of new applications, such as video over internet, internet telephony and videoconferencing, with completely different requirements from the original data transported over internet, require differentiation of the traffic providing different levels of services for the different applications, in order to guarantee a minimum of quality of service (QoS) for each service. To ensure QoS, it is essential to be aware of the requirements of each service. In multimedia applications, which have been the focus of the market in the last years, the most relevant QoS metrics are the end-to-end delay, jitter and packet loss rate.

The increasing amount of traffic produced in the internet and the variety of technologies and applications available, which have different characteristics and different quality of service requirements, require the control of internet performance. In order to manage the internet, it is essential to have a precise knowledge of the behavior of each network element and each service. Nevertheless, for a successful and precise network management, it is also crucial to be aware of the current state of the network.

As aforementioned, the actual internet is composed by a complex group of technologies and services. It is particularly important to have an accurate understanding of the performance of each service over the different technologies; also, the information about the impact of the multiple services coexisting in the same network represents an essential point in network knowledge. This information is fundamental in the management of the network, allowing it to take better decisions in the planning of the network or in the recovery of any undesirable situation.

To ensure that the services are delivered with the quality expected by the costumers, it is necessary to have mechanisms which aim to know the actual state of the internet, performing end-to-end monitoring in real-time. The collection of the performance measurements, such as end-to-end delay, jitter and packet loss is an important task; however, to be aware about the network performance is not sufficient: these values must be stored and analyzed in order to allow the readjustment of the system taking into account its actual condition.

1.2 Objectives

This thesis deals with the problems associated with providing end-to-end QoS for three main services, VoIP, Videoconferencing and IPTV. Two different studies will be presented.

In the first study, the OpNet simulator will be used with the objective of testing VoIP and IPTV services over different access technologies (Ethernet, ADSL and IEEE802.11), varying the network conditions. VoIP and IPTV services will be also evaluated when interacting with other connection-oriented services such as HTTP, Email and FTP.

In the second part, it will be implemented a solution that allows real-time monitoring of IPTV, Videoconferencing and VoIP service, analysis of performance measurement collected and storage of the values in a database. All of these processes will be performed in real time, maintaining the database up to date.

The following activities will be developed:

- Study of VoIP behavior over Ethernet, ADSL and IEEE802.11 varying the network conditions.
- Study of the impact of HTTP, Email and FTP in the VoIP service.
- Study of Video behavior over Ethernet, ADSL and IEEE802.11 varying the network conditions.
- Study of the impact of HTTP, Email and FTP in the Video service.
- Development of a framework to monitor VoIP and IPTV traffic, analyzing the data and storing the performance measurements in a database, in real-time.

1.3 Organization

- Chapter 2 – Related Work: provides an overview of the access technologies Ethernet, ADSL and IEEE802.11. It will present some techniques of network monitoring and some of the most important mechanisms for network management: TMN, SNMP and CMIP. This chapter will also describe the main characteristics of some of the services available in the internet giving a special attention to Voice, Videoconferencing and Video service. Finally, an overview will be given of mechanisms used when managing multimedia services.

- Chapter 3 – Matching the evaluation of the network performance with the Quality of Service: the work in this chapter matches the evaluation of the network performance with quality of service: it characterizes all the scenarios created in OpNet simulator, with the objective of testing the VoIP and IPTV services. OpNet simulation results and their respective analysis are also presented in this chapter.

- Chapter 4 – Architecture Overview: Describes all the steps in the framework creation, the modules used during the implementation and the final architecture of the process.

- Chapter 5 – Conclusions and Future Work: Presents the main conclusions of the execution of this work, also presenting some possibilities of future activities related with this thesis.

1.4 Contributions

The main objective of this thesis is the study of multimedia services and network performance; we keep our attention focused on the most attractive services to the market, VoIP, Videoconferencing and IPTV. The performed work results in a set of contributions.

This thesis contributes with information about the behavior of IPTV and VoIP services over the more utilized access technologies at the present time (Ethernet, ADSL, and IEEE 802.11). One of the interesting contributions of this study is the identification of the maximum capacity of each technology, varying the load condition of the network.

Other important contribution is the identification of the most intrusive service for VoIP and IPTV services; keeping in mind some of the most widely used services, FTP, Email and HTTP services have been tested interacting with IPTV and VoIP.

The last contribution of our work is the development of a framework that has as main functions: monitoring the IPTV, VoIP and videoconferencing services, collecting important performance indicators; and storing the gathered values in a database, keeping it updated.

2 Related Work

This chapter presents information which is important to understand the work performed in the rest of the document. Section 2.1 presents some of the access technologies considered, which include Ethernet, IEEE802.11 and ADSL. Section 2.2 provides information about some of the services presently available in the internet, giving particular emphasis on VoIP and IPTV services that are the main targets of this study; moreover, it also gives an overview of other oriented services such as FTP, HTTP and Email. Section 2.3 is divided into three subsections: 2.3.1 provides information about the different performance monitoring types, indicating some of the existent solutions; section 2.3.2 introduces the network management mechanisms: TMN, SNMP and CMIP; and section 2.3.3 also provides information about mechanisms to perform network monitoring and management, however in a way that is more oriented towards the analysis of multimedia services. For that purpose, RTP/RTCP monitoring, CDR, SLA and data management methods are addressed.

2.1 Access Technologies

This sections aims at introducing and describing a set of technologies which, at the present time, are widely used as access technologies: Ethernet, IEEE802.11 and DSL. The knowledge of the main characteristics of these technologies allows a better understanding of their behavior in various situations and scenarios.

2.1.1 Ethernet

Ethernet was commonly used as a networking technology in LANs (Local Area Networks), however the high bit rates supported for the most recent standards lead Ethernet to become a valid solution for network backbone as well. Ethernet has various standards associated but the most relevant standard is IEEE 802.3.

All nodes in an IEEE 802.3 LAN share the medium, and only one can communicate at a given time. To control the access to the medium, Carries Sense Multiple Access Collision Detection (CSMA/CD) is used. When a station wants to transmit, it monitors the medium. If the cable is busy, the station waits until for the idle condition to send data; otherwise it transmits immediately. If two or more stations start to transmit at the same time when the medium was idle a collision occur, thus each node must listens the bus at the same time that it is transmitting. When a collision occurs all the stations must

wait a random period in of time before attempt another transmission, with objective to avoid further collisions. A minimum frame size of 64 bytes is required to ensure that the collision is detectable before next frame is sent.

Ethernet is a best-effort technology that does not supply any QoS guarantee, in [1] a detailed analisis of Ethernet technology is performed, being pointed as a reasonable solution for real-time applications. In very congested environments the number of collisions increases and more packets are lost; this situation is particularly relevant for scenarios with VoIP traffic. However the high data rates supported by the last standards of this technology and lower price associated, allow the over-provisioning of the access network, in order to guarantee a high quality for real-time applications.

2.1.2 XDSL

DSL services are point-to-point public network access technologies that allow multiple forms of data, voice, video and data to be carried over twisted-pair copper wires on the local loop, between the service provider and the costumer. A costumer´s site must have a DSL (digital subscriber line) modem and a splitter that is responsible for separating voice and data transmissions.

The major advantage of high-speed DSL services is that it uses ordinary copper telephone lines, which are already broadly installed. This is a very cost-effective solution because the current infrastructures do not need to be updated in order to provide DSL services.

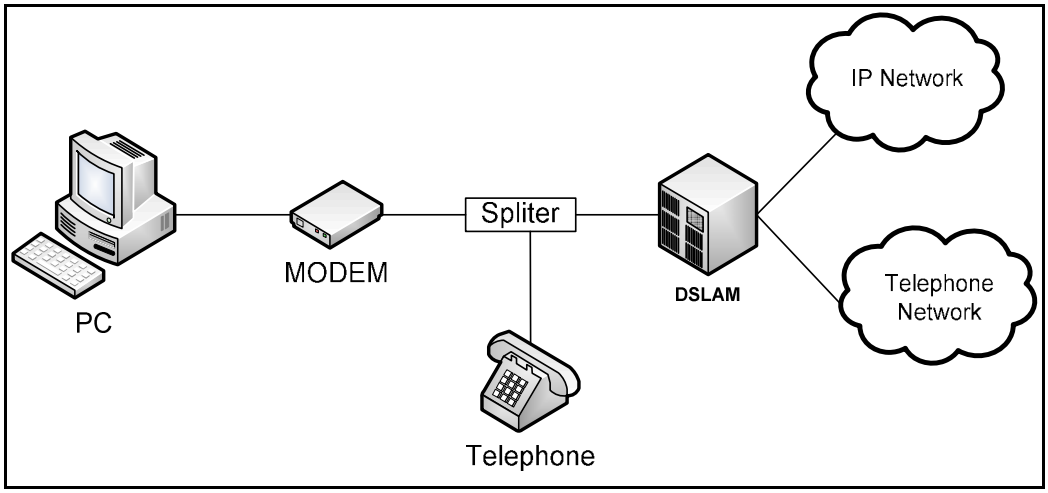

Figure 1 - ADSL architecture

ADSL stands for Asymmetric Digital Subscriber Line and it is the most popular version of consumer-ready DSL (Digital Subscriber Line). The ADSL provides a faster data transmission over copper telephone lines than a conventional voice band modem because it uses frequencies that are not used by a voice telephone call. It is possible for a single telephone connection to be used for both ADSL service and voice calls at the same time by applying a splitter.

A DSLAM, Digital Subscriber Line Access Multiplexer is a network device located near the costumer's location that allows phone lines to make faster connection to the internet by connecting multiple costumer DSL's to a high-speed Internet backbone line using multiplexing techniques. Here another frequency splitter separates the voice band signal for the conventional phone network.

The costumers' connection to the DSLAM is made through ADSL modems, which are connected to the PSTN network via typical unshielded twisted pair telephone lines.

As the name says, ADSL is asymmetric because the volume of data flow is bigger in one direction than in the other. It is a service for consumers to connect to the Internet in a relatively passive mode, using the higher speed direction for the downlink.

Various ADSL standards have been defined; the first standard approved in 1998 supports 8 Mbps in Downstream and 1Mbps in Upstream, in 2002 a new standard had emerged ADSL2 supporting 12 Mbps in Downstream and 1Mbps in Upstream, the last approved standard was ADSL2+, supporting 24Mbps in Downstream and 1Mbps in Upstream. Annexes J and M shift the upstream/downstream frequency in order to improve upstream rates; reaching values up to 3.5 Mbps.

Some studies performed such [2] that points out ADSL as an ideal solution for video services such: video on-demand (VoD) and IPTV, for these type of service more information is downloaded than sent in upstream, the upstream connection it is only used to control the service.

2.1.3 IEEE 802.11

IEEE 802.11 is a standard that specifies the characteristics of Wireless Local Area Network (WLANs), often used at home, enterprises and public access areas due to their low cost, simplicity, acceptable data rates.

Various protocols regarding this technology have been deployed, being the most popular, at the present time: 802.11a, 802.11b, and 802.11g. However news protocols such 802.11n are emerging.

While IEEE 802.11b devices provide up to 11Mbps and operate in the 2.4GHz IMS (International Microwave Symposium) bands, IEEE 802.11a promise higher rates (54Mbps) but operate in the 5GHz U-NII (Unlicensed National Information Infrastructure) bands. IEEE 802.11g also support 54Mbps, however operates in the IMS band, and as a result, it is compatible with 802.11b.

The Medium Access control (MAC) layer defines two main modes: Distributed Coordination Functions (DFC) and Point Co-ordination Function (PCF). The PCF mode was developed with the objective to support quality of service for multimedia traffic; however some previous studies [3] indicate that PFC does not provides an significant improvement in the performance relatively to DCF.

DFC is the most extensively utilized protocol is set by default, operates using the carrier sense multi access method with colision avoidence (CSMA/CA), mobile nodes must sense if the medium is idle before transmiting, however when a collision occurs, a retransmition is performed. A wireless frame can suffer severan transmission attempts before sucess.

After an unsucessful transmition, indicated by a lack of acknowledgement, a random backoff algorith is applied to define a time which must be waited before trying another retransmition. This backoff time increases exponnentially which each unsucesseful transmition. The wireless frame will be droped if severel number of transmitions occur without success.

In addiction to the MAC modes, the IEEE 802.11 standard also specifies two management modes called: Infrastructured mode and Ad Hoc mode. The infrastrutured mode requires one acess point (AP), each comunication between mobile nodes must be transmited trough AP, while the Ad hoc allows direct comunications between mobile nodes.

The 802.11 protocols provide best-effort services, packets are carried without any guarantee, these networks were originally designed to carrier simple data, however with the demand of multimedia applications in the last years, are growing the interest in use WLANs to support them.

2.2 Multimedia Contents Characteristics

Multimedia applications such as IPTV, VoD, VoIP and Videoconferencing, have seen an impressive increase in terms of popularity in the last years. These applications have specific traffic characteristics and QoS requirements that are different from typical data oriented applications. Delay, jitter and packet losses are important metrics for real-time traffic. Real-time applications have severe End to End time transmission requirements. Real-time applications are characterized by timers and all information received after the timer expires is considered as harmful and is dropped, this definition does not means that all real-time applications use the same time boundary.

2.2.1 Voice/Conferencing

Voice over Internet Protocol (VoIP) and videoconferencing (VC) are characterized by a high economic viability and the possibility of a single network capable of transporting different types of data became these services very attractive.

The ITU-T H.323 recommendation [4] is the most extensively deployed VoIP/VC protocol. H.323 specifies how multimedia traffic is carried over packet networks and also covers the end systems, attached to the packet oriented networks communicate with telephones attached to the circuit-switched telephone networks.

However this protocol is not considered to be sufficiently robust when it regards the interaction with PSTN networks, it is pointed as excessively complex protocol. By this reason other protocols have been deployed, such as Media Gateway Control Protocol (MGCP) and Session Initiation Protocol (SIP).

SIP protocol has been referenced as a solution; is a lightweight protocol that allows calls between users within the IP network, but also allows communication with PSTN telephones. This protocol provides mechanisms for call management, such adding new media streams, changing encoding during the call, inviting new participators and call transfer procedures.

Voice and Videoconferencing services utilize Real-time Transport Protocol (RTP), over a User Datagram Protocol (UDP). The RTP header helps the receiver to determine; when a packet was expected, if the packet was in order, and if the packet has been received too late. This information is

very important to the receiver since allows to determine how it must adjust its own settings to mask delay, jitter, and packet loss.

2.2.1.1 Voice traffic

When generating telephony traffic, the sound must be compressed in order to utilize less bandwidth. There is a wide range of CODECs (compress/de-compress) to compress voice. ITU-T's G.711, G729 and G723 represent some of the most used speech CODECs at the present time. After the speech compression, the samples are grouped in packets, each packet contains a minimum of 1 voice frame and each voice frame contains a minimum of 10 milliseconds of audio. Each voice packet is encapsulated with RTP, UDP and IP headers.

Consequently, voice stream is composed by packets with fixed size that are generated at a fixed rate. Such rates can vary depending on the CODEC used and the packetization rate (default of 50 packets per seconds).

Real-time voice traffic has rigorous QoS requirements, essentially time requirements, ITU G.114 recommendation [5] has defined the threshold as:

- ≤ 150 ms of one-way latency from mouth to ear.
- ≤ 30 ms jitter
- ≤ 1 percent packet loss

Packet loss causes voice clipping and skips. Packet loss concealment (PLC) is a mechanism utilized to minimize these effects. The choice of PLC method depends on the type of CODEC; for example G.711 replay the last received sample, increasing the attenuation at each repeat.

Latency can cause voice quality degradation, which represents one of the most relevant issues in VoIP performance, specified by ITU standard G.114 state that 150 ms, end-to-end (from mouth to ear) delay ensures QoE for telephony applications. When end-to-end delay is exceedingly long, the interaction is lost.

Jitter buffers are used to eliminate asynchronous packet arrivals, allowing the receiver reorganize the packets producing a synchronous stream. The main purpose of jitter buffers is to define the equilibrium between interrupting a call with an excessive packet delay, or drop out-of-order packets.

If the jitter buffer is extremely large or too small, it imposes limitations on the characteristics of the network. A jitter buffer set too large, it will increase the end-to-end delay. On the other hand, if it is too small, underflows or overflows can happens. In an underflow, the buffer is empty when the CODEC needs to playout a sample. Overflow occurs when a new out-of order packet arrives however the jitter buffer is already full and consequently this packet cannot be enqueued being dropped. An ITU G.114 recommendation points out a value 30ms as a reasonable threshold for jitter.

2.2.1.2 Videoconferencing

Videoconferencing merges VoIP and video streaming. Most of the existing conferencing platforms use a central serving unit which assembles all the data from the multiple users and then re-distributes all of the information amongst them, but more efficient solutions using multicast protocols are gaining popularity.

A Videoconferencing session is composed by two bidirectional streams (voice and video) streams, the voice stream with the characteristics explained above regarding the VoIP service; however the video traffic pattern is completely different from the voice service. Video packets have variable size and this variability depends on the nature of the video content being encoded.

Since videoconferencing combines both services (video and voice) it has the same loss, delay, and jitter requirements as VoIP service, however in videoconferencing, voice and video streams must be synchronized, this characteristic also identified as “lip-sync” is one of the biggest concerns of videoconferencing service.

The bandwidth required by this service can be calculated summing the individual bandwidth consumed by each flow and consequently is depends on the voice and video CODEC used.

2.2.2 Video

Video services over internet have experienced a massive demand last years; it is pointed as one of the services that presents higher economic viability, consequently various video-based services are emerging in the IP network.

At the present time the majority of the video-based services available in the internet are videos available to download and videos available to playout without storing (streaming). However these types of video service must be distinguished from true entertainment-grade video, also referred as IPTV; this type of service is commonly displayed in large screens and the services are delivery in real-time.

Services such VoD (video on demand) and IPTV impose a weighty bandwidth challenges to the service providers, since they are dedicated to millions of customers with periods of peak demands.

As a response to these challenges, source coding technologies have been deployed with the objective to aggressively increase the compression rate reducing the bandwidth required, the most popular CODECs to this service is MPEG (Moving Picture Experts Group).

MPEG compresses video in three types of frames, I frames (intrapicture), P frames (predicted frames), and B frames (bidirectional frames).

I frames, also referred as reference frames, each of these frames is pictures coded using JPEG, I frames are considered self-contained do not depending from other frames. However P frames are dependent from the previous I frame, and B frames are dependent from previous and successive I or P frames. As a result of inter-dependency between the frames it is necessary to have I frames appearing at the output stream periodically. A single loss of this type of frames can represent a visible degradation in the playback of the video. P frames depends from the previous I frame, to be possible the decompression at the receiver, I frames must arrive earlier. B frames depends from the preceding and successive I or P as a result both of these frames must previous arrive at the receiver to become the decompression possible.

Each video is composed by a succession of groups of pictures (GOP), each GOP is composed by a sequence of I frames followed by P frames or B frames, the number of frames can vary between 12 in

standard-definition television (SDTV) and 30-fps National Television System Committee (NTSC), thus in this worst case an I-frame is sent every half second. As a result of the interdependency of the packets and the rate at which the frames are sent a single packet loss can lead up to one second of video degradation, studies defined that for acceptable video quality of experience no more than one visible degradation can occurs in two hours of video playback. Consequently video service has rigorous quality of service requirements for packet loss, 10^{-6} maximum loss is considered a threshold by the service providers.

Based on all aforementioned information, the thresholds for streaming video were evaluated by ITU-T [5] as:

- Four to Five seconds of latency acceptable.
- Packet loss ≤ 10^{-6}
- Delay and jitter: insensitive.

With the adventure of video-based services, it is expected that household bandwidth requirements considerably increase, even with powerfully codec mechanisms being developed.

2.3 Other user oriented Applications

2.3.1 FTP (File Transfer Protocol)

FTP [6] is amongst the oldest application protocols still widely used in the internet. It allows a copy of a file to be transferred between an arbitrary pair of machines and includes a mechanism that allows files to have ownership and access restriction. This correlation is very important, because it hides the details of the individual computers systems.

FTP establishes two autonomous connection types between user and server; a control connection and a data connection. The control connection is a logical TCP session established when a FTP session is formed, used to exchange commands and replies that allow the control of the transmission. Data connection is a full duplex connection over which data is transferred, in a specific mode type; the transmitted data can be fraction of a file, a complete file or group of files.

FTP is a non-real time applications, and thus time requirements are more flexible. Nevertheless this application still an interactive applications assume some relationship between source and destinations while the application service is active.

2.3.2 HTTP

Hypertext transfer protocol (HTTP) is an application-level protocol, one of the most used protocols on the internet; each time that we select to access some page in the internet HTTP is running over TCP. The standard HTTP1.0 was involved in considerable debate and experience, however never generate a formal specification, RFC 1945 [7] only presents the common usage of HTTP. In 1999 an HTTP1.1 protocol [8] was specified by IETF, addressing the most complex requisites of this protocol.

HTTP is a stateless protocol consequently has the advantage that servers do not need to preserve information about users between the requests; it allows the rapid World-Wide Web (WWW) pages over various distributed servers. HTTP is also a request/response protocol, the client (end-user) initiates a request (establishes a TCP connection to a server and sends a request). The server sends back a status line and a message of its own. This message contains the requested information, an error message or some other information, once the transaction is completed then terminates the connection.

Like FTP, HTTP application is an interactive non real-time application, so some timing relationship between user and server must be ensured but not with high requirements.

2.3.3 Email

Electronic mail was originally designed to allow the peoples to communicate each other. The E-mail software transmits a copy of the message to each recipient. When the user finishes composing the outgoing message, the mail interface puts the message in a queue. The mail system contains a mail transfer program that handles the details of sending a message. When that software contacts a server on a remote machine, it establishes a TCP connection over which it communicates. Once the connection is in place, both programs follow the Simple Mail Transfer Protocol (SMNP), allowing the sender to identify itself to specify a recipient, and to transfer an e-mail message.

E-mail is an asynchronous non-real time application and therefore relatively insensitive to time, assuming either non time relationship between the source and destination.

2.4 Network Performance Management Solutions

2.4.1 Network Monitoring

Since we can only manage what we can measure, performance measurements have become crucial in controlling network performance. The conventional monitoring schemes to measure network performance can be divided into three main types: active, passive and hybrid.

Each monitoring type has different characteristics, restricting the type of the information that is possible gathered and its applicability.

2.4.1.1 Active measurement

Active measurement is used with the purpose of operating, supporting, and testing the internet performance. The measurements are performed by sending probe packets and monitoring them. By actively analyzing the packets we can collect network information such as: available bandwidth, delay and loss. Probe-packets are streamed into the network and used to determine the network performance; this means that we assume that network performance is the same as the values obtained by evaluating the probe-packets.

This mechanism allows relatively accurate measurements however presents some troubles such as scalability and periodicity. Scalability, since that probe-packets stream increases the traffic in the network affecting its performance, on the other hand the performance measurements obtained by the active packets its different from the real values without of influence of active stream. Periodicity, since the probe-packets are sent periodically, the performance measures generally differ from the actual performance that user experiences. Moreover, since different traffic profiles behave in different ways, so at the best, when using different applications it becomes difficult to evaluate the individual performance of all applications.

Some solutions have been developed in the last years, based in active measurement, one of the most interesting is STING presented in [9]. It allows the measuring of packet losses in both directions, analyzing the TCP flows.

This solution presents some limitations. STING only allows acceptable performance measures in a reasonably large scale of time, since this mechanism is based in ACK parity, and when this information is not transmitted a large timeout must be waited. Another limitation of this tool is related with large TCP packets. TCP receivers usually have small buffers when this buffer are completely full a new TCP connection is created, consequently the buffer can become full with only five or six TCP packets; this packets do not carrier enough information to accurate analysis of the connection.

The Network Radar [10] tool can perform a network tomography based on TCP packets changes during the three-way handshake. SYN probe-packets are sent to different receivers and the delay is calculated using the variation between the sending time and the time at which the TCP SYN-ACKs are received by the sender. Performing this procedure as often as number of path that we pretend analyze; this tool creates a network tomography with end-to-end delay of each path. However in real situations the packets belonging to some flow can travel through different paths, consequently the unidirectional analysis of network performance become crucial.

In [11], a commercial solution named Saturne is presented. This tool evaluates the one-way delay and the packet loss in the network, taking into account some quality of service mechanisms. Saturne measures the performance of the network, analyzing the different packets in their class of service, becoming possible to identify the exact moment when some service level agreement (SLA) is violated.

Available bandwidth is an extremely important performance measurement and its estimation is very useful in the networks management, allowing QoS verification and route selection, consequently many tools have been implemented with ability to estimate it.

The existent solutions allowing to measure the available bandwidth can be divided in two groups: probe gap model (PGM) or probe rate model (PRM).

PGM is based in a mathematical relationship between the inter-arrival (also referred as *dispersion*) of probing packets at the ingress and egress of the measured path. Using this technique PGM tools such as *Delphi* [12]or *Spruce [13]* estimate the end-to-end available bandwidth.

The probe rate model (PRM), sends probe packets at a fixed rate and if probe-traffic is sent at lower rate than the available bandwidth along the path, then the arrival rate of active-traffic at the receiver

is the same than their sending rate. In contrast, if the active-probe traffic is sent at a higher rate than the available bandwidth, the probe traffic will be delayed, consequently, the probes' rate at the receiver is the same than bottleneck rate. Consequently available bandwidth can be measured finding the matching point. Using in this technique a tool is worthy of mention: *pathChirp [14]*, which estimates the available bandwidth.

2.4.1.2 Passive measurement

This technique has the advantage that non additional traffic is introduced into the network; as a result the network performance and the values gathered are not affected. Passive monitoring specifies two main types: two-point monitoring and one-point monitoring.

Two-point monitoring uses two monitors, each of this monitor is located at one of the ends, this device analyze the packets data and derive performance metrics such delay and loss, making a comparison with the data gathered in the other monitoring device. One-point monitoring can be performed based on TCP acknowledgements mechanism or RTP (Real Time Protocol).

When a TCP-sink receives a packet from a TCP-source, an acknowledgement is transmitted. By analyzing a packet-acknowledgment pair it is possible to measure round trip delays and packet losses. This method is similar to the method used by the active measurement Network radar tool, however at this point the packets analyzed are not produced by monitoring system. Instead the real traffic traveling through the network is analyzed.

Using the RTP/RTCP (protocols frequently used for real-time applications such VoIP or Video-Streaming), round trip delay, delay variation and packet loss can be evaluated analyzing some fields from the RTP packet header such Time-stamp and Sequence-number or analyzing the data statistics provided by RTCP protocol.

Tstat [15], represent an example of a solution that performs both TCP and RTP/RTCP analysis. It is a very interesting tool that observes passively the traffic on a network link. Tstat gives a set of performance measurements based in analysis of TCP or RTP/RTCP flows and the statistics collected are available to user of these flows.

The large collection of statistics provided by this tool, make it very attractive. Metrics such as: number of duplicate packets, number of lost packets, number of late packets, jitter, RTT, bitrates and others are provided by this solution. This tool will be used in this study to gather important metrics of real-time applications (IPTV and VoIP).

2.4.1.3 Hybrid Measurement

There are situations where passive and active measurements methods can be used cooperatively, this situation allows us to take advantages of both mechanisms. Hybrid measurement does not provide any specification and can be applied to any combination of active and passive measurements. An example is the CoMPACT monitor extensively described in [16], which estimates the quality of service and network performance via a scalable and lightweight method, measuring the traffic volume as passive monitor and measuring the network performance as active monitor.

2.4.2 Network Management Mechanisms

The Telecommunications management network (TMN) [17] model describes the basic operating and management functions to be used between networks components and network management systems. Key elements of the TMN concept are the CMIP [18] and SNMP [19] protocols. TMN provides a consistent and efficient management of complex telecommunications Networks.

TMN has been defined for the first time in 1985, the first recommendation was called M.30, however this recommendation has been revised and the last version, M.3010, date from 1996. TMN provides the resources to transfer and process information associated to the management of telecommunications networks. TMN provides five functional areas: performance management, fault management, configuration management, accounting management and security management.

The TMN functional architecture is based on five function blocks that support the management functions: Data Communication Function, Operations Systems Function, Network Element Function, Workstation Function and Q Adaptor Function.

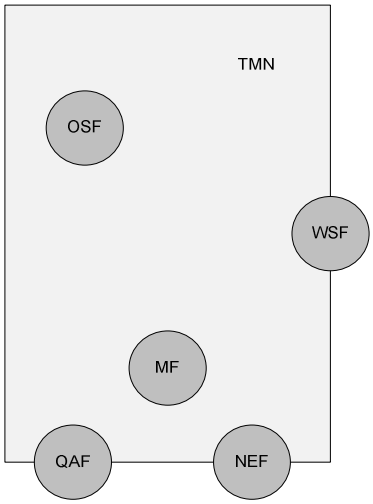

Figure 2 - TMN function blocks

The Data Communication Function (DCF) is utilized to transport information between function blocks. The Operations Systems Function (OSF) block starts management process and receives notifications. It processes the information associated to the telecommunications management for the purpose of monitoring and controlling. OSF communicates with NEF via Q3 interface. The Q3 interface is used when management information must be transferred via a management protocol such CMIP or SNMP.

The Network Element Function (NEF) block provides two main functions, telecommunications and support functions. Telecommunications functions manage and support the transfers of information between the users of the telecommunication network. Support, allows the NEF block to works in an agent role. Transfers and transmission systems are examples of network elements (NEF)

The Workstation Function (WSF) block provides the means to interpret TMN information for the human user, and vice versa. The WSF includes support for interacting with a human user translating information; consequently in Figure 2 this function block is shown on the TMN boundary.

Mediation Function (MF) block acts on data exchange between an OSF and NEF or between OSF and QAF, to guarantee that the information exchanged match the expectations of the function blocks attached to the MF.

The Q Adaptor Function (QAF) block is used to connect a TMN to non-TMN units. QAF is the responsible to translate the information between these entities; once more this block is depicted in the boundary of the TMN.

There are currently two major network management protocols both can be used by TMN system: the simple network management protocol (SNMP) and the common management information protocol (CMIP), CMIP includes its derivation over TCP/IP (CMOT). These network management protocols provide mechanism for retrieving, charging, and transport of the network management data across the network.

SNMP has been pointed as a basis for many management systems; it provides interfaces to read information and to write configurations in network devices. The SNMP agents and stations use a request/reply protocol to communicate. This protocol supports standard messages (Get-Request, Get Response, Get-Next-Request, Set-Request and Trap). The SNMP station uses Get-Request to solicit information from the network node, a SNMP agent which responds with a Get-Response message. Information that might be exchange includes: the name of the system, how long the system has been running and the number of the network interfaces on the system.

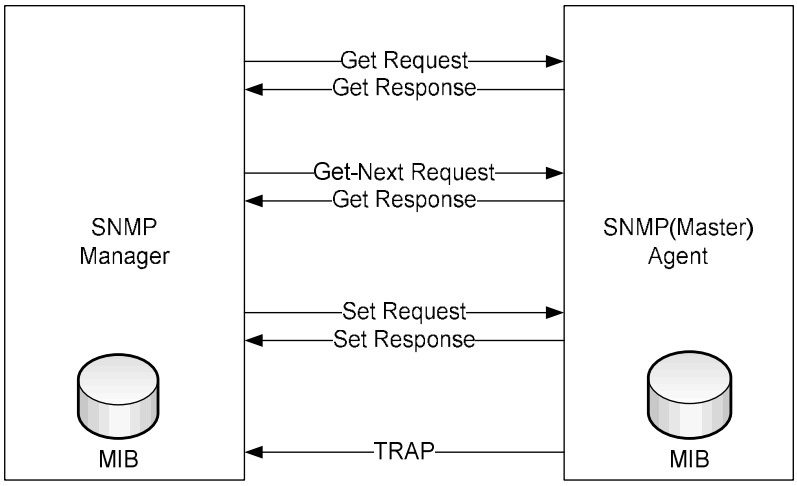

Figure 3 - SNMP architecture.

Get-Request and Get-Next-Request used in conjunction obtain a table of objects, for example if we intend to know the number of interfaces of some station, first it is sent a Get-Request for the first interface for the additional interfaces Get-Next-Request messages are used.

Set-Request allows remote configuration of parameters on a device such: name of the device, setting an interface administratively down or change the address of the interfaces.

SNMP-Trap is an unsolicited message sent by SNMP agents to the manager. These messages inform about the occurrence of a specific event, for example SNMP Trap messages, can be used to inform that some link is down or that that the agent is reinitializing itself. The parameters that are accessible via SNMP are grouped into management information bases, MIBs.

CMIP intends to provide a complete network management protocol over many, diverse network machines and computer architectures. CMIP mode of operation is significantly different from the SNMP, since SNMP was designed for simplicity and ease of implementation. CMIP provides the same functions as SNMP, however presents more functionalities allowing more operations.

CMIP only defines how to decipher the information in the packet and does not state what should be done with the information requested, thus the CMIP standard does not limit the functionality of the network management system. Any relevant information can be requested from the managed object and this information can be interpreted in any manner.

2.4.3 Multimedia Services' Management

2.4.3.1 RTP/RTCP monitoring

The Real-time Transport Protocol [20] offers end-to-end transport services for real-time data, including audio and video, over the internet. It can be used for video on-demand or interactive services such VoIP. This protocol is accompanied by the RTP control protocol (RTCP), which is used to exchange QoS information between the source and destination. RTP/RTCP does not provide resources reservations neither ensure quality-of-service, however provide important functions to do it.

RTP provides end-to-end information for real-time data, such as a sequence number, payload type identification, sequence number and timestamp. Since packets travel through the internet, they may arrive at random time in a random order and some packets can also be lost or late, the information provided by RTP header may be used by the receiver to reorganize the packets, recover from some lost and analyzing the RTP header receiver creates the RTCP reports.

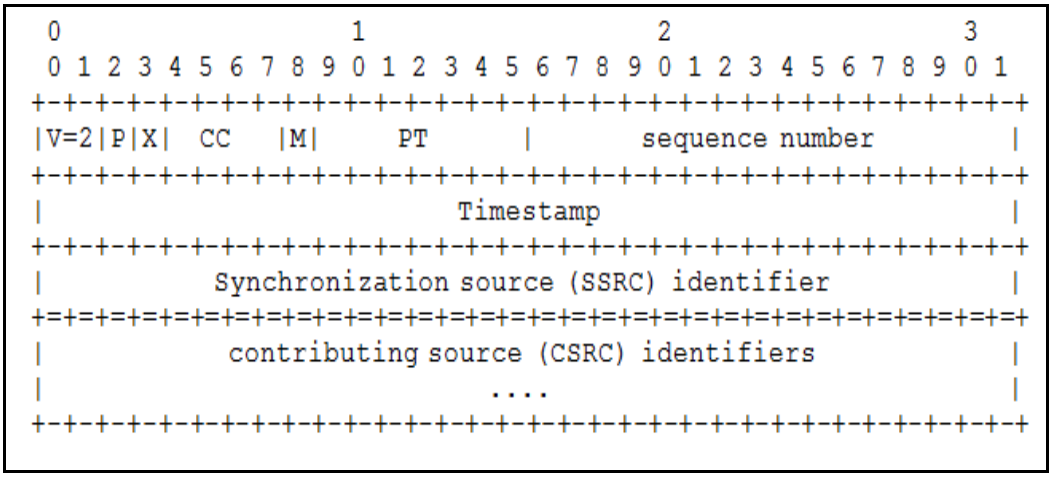

Figure 4 - RTP packet format

RTP typically runs over UDP which is very useful for real-time interactive services such VoIP, since retransmissions are not usually recommended. However RTP may be used with other transport protocols such TCP; which can represent a good solution for video streaming or VoD services, once that are less sensitive to the delay and consequently retransmissions can be useful.

RTCP, as a primary function, offers feedback on the quality of data distribution; the feedback function is based on the periodic transmission of control messages such, Receiver Report (RR) and Sender Reports (SR). These reports are sent out at regular intervals by every participant. To assure scalability, RTCP can be grouped and transmitted in a single packet of underlying protocol, this functionality is enable by the length field in the RTCP packet header.

The sender and receiver reports are very similar; the difference between them is that sender reports add 20-bytes of sender information. Typically receiver reports are used; the Sender Report is only used if no packet is sent since the last RTCP report. Each report is composed of several fields with statistics about RTP received data, such packet lost and delay.

2.4.3.1 Call Detailed Records

Call detailed Records (CDR) [21]are a collection of data that contains call information, including call date and time, call length, calling party, called party, type of the call and supplementary service input. These are the basic information that are mandatory in a CDR and allow functionalities such as billing

services. However a CDR may contain a huge amount of optional information (e.g. call failures, denial of a service, reaching a quality threshold, change of observed service quality). This additional information allows fraud investigation, quality of service analysis and network traffic management. If the service providers know the customers behavior they can make better decisions managing the network performance.

There are three ways to transfer CDR records: the first is a real-time transfer of a single CDR, the second method, where a near-to-real-time transfer occurs after several CDRs being grouped into a single Blocked Generation Log and subsequently sent via Event Forwarding Discriminator (EFD) and the third and last one CDR records are stored in File Generating Log and when this log are requested is sent via FTP.

When CDRs are very complete and detailed they can play a major role in the analysis of call problems, and at the same time suit as a good input for data mining processes. They are very used for trend analysis and higher level service fault management, but can also give input on call problems occurring with certain device types.

2.4.3.2 SLA Threshold

Service level agreement (SLA) is a contract between service providers and customer or between two service providers and defines several quality of service thresholds that the service providers must respect. When some of these thresholds are violated a penalty is imposed to the service provider in order to ensure credibility.

SLA can be a contract between internet providers and customers and thus define performance parameters of a network service, including values for metrics such as the available bandwidth and burst tolerance, or can be a contract between the third-party service provider and its costumers defining levels such delay and packet loss.

In order to be possible to identify the moment when an SLA is violated the network must be monitored. Some solutions have been developed in order to perform this function from which IBM Cognos[22] and Tivoli Service Level advisor [23] can be underlined.

SLA monitoring solutions perform some common task; analyzing automatically and periodically the service levels agreement or evaluating the values collected with the purpose of predicting future violations. When a violation trend occurs, it is saved in a SLM (service level management) database and an alert is sent to allow the service manager to recover the situation, this alert can be sent via Email or SNMP. After the measurement data are collected and analyzed, reports are created providing useful information to how have access to the SLA monitoring tool. This information can be displayed hourly, daily or weekly, depending to the customer's requirements.

2.5 Summary

This chapter dealt with three main sections: the analysis of access technologies, detailing of multimedia services and network management methods.

Regarding the access technologies' topic, some of the most widely used access technologies at the present time were shown: Ethernet, IEEE802.11 and ADSL. We explain some of the most important characteristics of each of these technologies.

Dealing with the multimedia analysis subject, more emphasis was included on VoIP, Videoconferencing and IPTV, addressing the traffic characteristics and the requirements of each service. Moreover, other user oriented services have been mentioned including Email, FTP and HTTP, indicating some of the most relevant features of these services.

In the network management section the main architectures of monitoring system (active, passive and hybrid) were introduced. Also some of the existent solutions at the present time were shown. The existents network management mechanisms such TMN, SNMP and CMIP were also mentioned, as well as the multimedia services' management techniques, addressing topics of particular interest to this thesis such as RTP/RTCP monitoring, data management and SLA thresholds.

3 Matching the evaluation of the network performance with the Quality of Service

VoIP and IPTV services are characterized by high economic viability and are considered very attractive given the possibility of mixing voice and data into one network. When implementing a VoIP or Video solution, it is necessary to take into account that, at the present time, IP networks are best-effort oriented, since they were not designed to deal with real-time applications.

It became necessary to study the behavior of these services over different types of IP networks, as well as their performance when submitted to different network conditions.

Keeping in mind the goal of this thesis, an evaluation of the different access technologies such as ADSL, Ethernet and IEEE 802.11 will be shown. These technologies will be tested under different network conditions (different values of background traffic will reproduce different values of load in the network). VoIP and IPTV services will be also tested under the influence of the other oriented services such as HTTP, Email and FTP, in order to find the most harmful service for these real-time applications.

OpNet 10.0 [24] was the simulator selected to perform our study. This network simulator has gained popularity over the last years.

This chapter is divided into 6 main subsections; section 3.1 presents the main characteristics of the VoIP service and how it was implemented; subsequently, this service is tested over different technologies and varying the network conditions. This section also presents the simulation results and analyzes them. Section 3.2 introduces the characteristics of VoIP, HTTP, Email and FTP, which are subsequently tested and analyzed to evaluate the impact of the HTTP, Email and FTP services in the VoIP service. Section 3.3 and 3.4 repeats the process of 3.1 and 3.2, respectively; however, at this time the target of this study was the IPTV service as a replacement for the VoIP one. Section 3.5 analyzes the impact of the voice service in the video service and vice versa, presenting the results and analyzing them. Section 3.6 exposes the main conclusions of this chapter.

3.1 Voice Behavior Vs Network Conditions

3.1.1 Objective

In this section we aim to determine the maximum number of calls that each of the considered access networks can support, while keeping quality of service VoIP requirements. This study aims at identifying the maximum capacity of the various access networks in different load conditions, but also at characterizing the behavior of VoIP for each technology.

The simulation results such as the difference between sent and received packets, end-to-end delay and jitter were monitored, in order to find the precise moment when some of these bounds are surpassed. This can be done by adding calls one by one to the network while monitoring the thresholds or bounds of VoIP service.

The access technologies selected to our studies are some of the most widely used technologies at the moment (Ethernet, ADSL and IEEE802.11); each technology has been tested under different network load conditions (1, 2, 4 and 6Mbps).

3.1.2 VoIP Configuration

VoIP application settings

One way to model the VoIP traffic in OpNet is to use the predefined voice application, which can be defined and configured using the Application Definition object. In this case the basic configurations are already defined but some flexibility is given to the user to change its attributes. Some important parameters are the “Encoder Scheme”, which was set to G.711, and the Voice Frames per Packet, which was set with value 1. This means that only one voice frame will be sent per voice packet. The configuration of Application Definition is presented in Figure 5.

Silence Length (seconds)	default
Talk Spurt Length (seconds)	default
Symbolic Destination Name	Voice Destination
Encoder Scheme	G.711
Voice Frames per Packet	1
Type of Service	Interactive Voice (6)
RSVP Parameters	None
Traffic Mix (%)	All Discrete

Figure 5 – Voice traffic characteristics, testing VoIP over different technologies.

For G.711 the required bandwidth for a single VoIP call, one direction, is 64Kbps. G.711 codec samples 10ms of voice per packet. Since the service was not configured to use silence suppression 100 packets need to be transmitted per second. Each packet contains 80 voice samples in order to give 8000 samples per second.

VoIP Profile Settings

After defining and configuring the VoIP application, it is required to configure the way in which the workstations will implement this application. The profiles can be defined and configured using the Profile Definition object. The configuration of this object is shown in Figure 6; the first VoIP call is generated 200 seconds after the start of the simulation. The repeatability of the VoIP application is set to be "*Unlimited"* with an inter-repetition time of 20 seconds, thus three new calls will be generated every 20 seconds.

⊟ Applications	(...)
├ rows	1
⊟ row 0	
├ Name	VoIP
├ Start Time Offset (seconds)	No Offset
├ Duration (seconds)	End of Profile
⊟ Repeatability	(...)
├ Inter-repetition Time (sec...	constant (20)
├ Number of Repetitions	Unlimited
└ Repetition Pattern	Concurrent
├ Operation Mode	Simultaneous
├ Start Time (seconds)	constant (200)
├ Duration (seconds)	End of Simulation
⊞ Repeatability	Once at Start Time

Figure 6 - Voice traffic profile, testing VoIP over different technologies.

The main objective of this profile is the generation of a common profile for all technologies, in order to subsequently make a comparison between their performances.

Since the call generation starts 200 seconds after the start of simulation and the number of calls is incremented by three, every twenty seconds, the number of calls produced is:

$$n_{calls} = 3\left(1 + \frac{t_{final}(s) - 200}{20}\right) \quad (1)$$

3.1.3 Scenario 1 – VoIP over Ethernet

3.1.3.1 Description

Network description

This scenario uses the Ethernet access technology. The topology of the network was configured according to Figure 7. Two routers (R1 and R2) are connected by a third router (RCore), which represents the network core. R1 is connected with two more switches (F1 and F2) and R2 is connected with one switch (F3).

Each Access switch (F1, F2 and F3) is connected with three workstations. Some of them are responsible for voice traffic production (F1ST1, F2ST1 and F3ST1) and the others (F1ST2, F2ST2 and F3ST2) are the destinations of the calls. The rest of the stations are considered to be the source of background traffic.

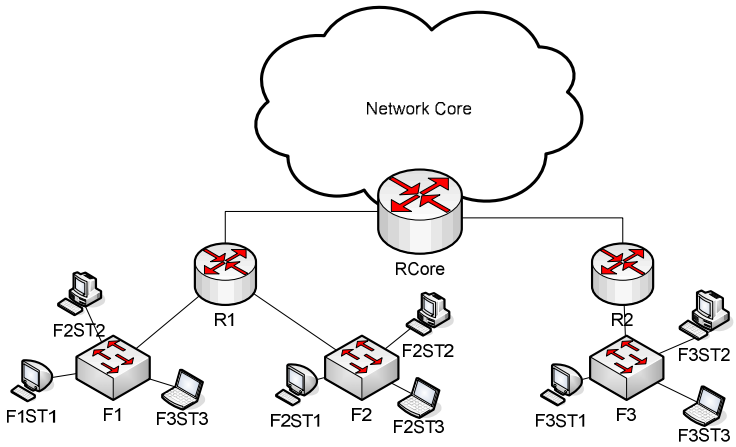

Figure 7 – VoIP over Ethernet, network topology.

The routers were deployed using the ethernet4_slip8_gtwy model, the switches use the Ethernet_16switch OpNet model, and all links used are Ethernet with 10 Mbps of bidirectional capacity. All devices are set by default. Links that connect the RCore to the routers (R1 and R2), and links that connect these routers to the access switches are configured with background traffic (1 Mbps, 2Mbps, 4Mbps and 6 Mbps). Four simulations have been performed in order to evaluate the effect of these different load conditions. The addresses and routes were configured automatically.

Traffic analysis

Each voice packet coded with G.711 is sent in one Ethernet frame. For every packet of size 80 bytes, headers of additional protocol layers are added. These headers include RTP + UDP + IP + Ethernet with preambles of sizes of 12, 8, 20, and 26 bytes, respectively. Therefore, a total of 146 bytes, or 1168 bits, needs to be transmitted 100 times per second, or 11.68kbps, in one direction. For both directions, the required bandwidth for a single call is 200 pps or 233 kbps for a symmetric flow.

Ethernet is a technology with more capacity than the other access technologies addressed in this study, so in order to perform the simulations in a reasonable period of time a different profile was created with intention to determine the maximum number of calls supported. In this new profile the calls are added at different rate —every two seconds three new calls are added. As a result, the maximum number of calls supported will be evaluated by:

$$n_{calls} = 3\left(1 + \frac{t_{final}(s) - 200}{2}\right) \qquad (2)$$

3.1.3.2 Results

This section presents the results collected while testing VoIP over Ethernet. The most relevant results are the difference between packets sent and received (packet loss) and end-to-end delay. In order to identify the cause of the service degradation, the link utilization was also depicted as shown in Figure 7. Table 1 performs a synopsis of the results collected in the various load conditions.

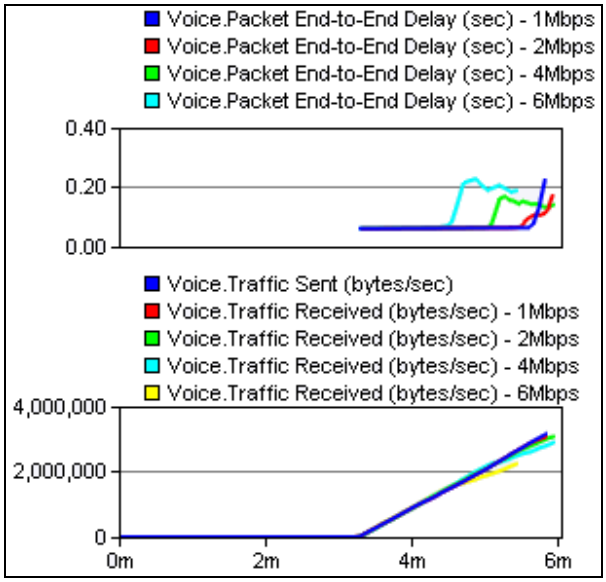

Figure 8 – Voice traffic behavior over Ethernet: end-to-end delay and packet loss.

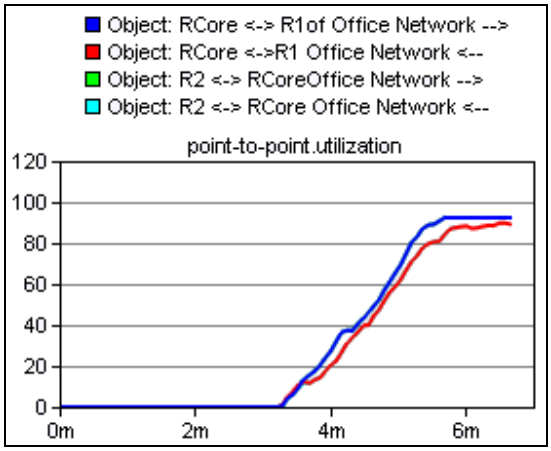

Figure 9 – Links utilization, testing VoIP over Ethernet: (R1<->RCore) and (R2<->RCore).

	Delay	**Loss**	**Calls**
1Mbps	5min42sec	5min 45sec	216
2Mbps	5min 34sec	5min 36sec	204
4Mbps	5min 7sec	5min 8sec	164
6Mbps	4min 34 sec	4min 35sec	114

Table 1 - Moment when the thresholds are met and number of calls supported, testing VoIP over Ethernet.

3.1.3.3 Discussion

With 1 Mbit of background traffic, Figure 8 shows that, after 5 minutes and 45 seconds of simulation, the packet loss reaches the threshold. The difference between voice traffic sent and received provides us the percentage of packets that is lost applying (3).

$$PacketLoss_{Max} = \frac{R_{b,sent} - R_{b,received}}{R_{b,sent}} \approx 1\% \qquad (3)$$

When the network is congested, the jitter and end-to-end delays have a sharp increase. The packet loss threshold is met after 5 minutes and 45 seconds from the simulation's start; however, end-to-end delay comes before surpassing the threshold 5 minutes and 42 seconds after the start of simulation. Therefore, the maximum number of calls supported by this network can be calculated by (2) replacing $t_{final}(s)$ by the moment when of the threshold match in seconds:

$$n_{calls} = 3\left(1 + \frac{342 - 200}{2}\right) = 216 \qquad (4)$$

Degradation of network performance is a consequence of the link saturation. The packets are being saved in the workstations buffers and consequently the delay will increase sharply until the buffer is saturated. These buffers are really large, and for that reason end-to-end delay can reach excessively high values before stabilizing.

The same analysis was performed for other scenarios (2, 4 and 6Mbps); the results are illustrated in Table 1. It is important to notice that jitter results were not considered in this analysis since the limit value was never reached during the simulation.

As well as for 1Mbps, the maximum number of calls supported has been calculated by (2), using the time when end-to-end delay threshold was met as $t_{final}(s)$, since this requirement was in all simulations the first threshold to be reached.

This study has evidenced Ethernet as a good solution for VoIP traffic, since a high amount of calls are supported with ensured quality of service. Even in high load traffic conditions (60% of background traffic), 114 calls were simultaneously supported (the links were set to 10Mbps).

The fact that the links are full-duplex represents a clear benefit, since VoIP traffic is bidirectional. However, as is depicted in Figure 9, the links never reach 100% of utilization. In a VoIP environment the packets generated are very small, consequently an elevated amount of VoIP packets is produced which poses a problem to the Ethernet links that begin to discard packets even before saturation is reached. Due to this fact, the Ethernet links must be over provisioned.

3.1.4 Scenario 2 – VoIP over IEEE802.11b/g

3.1.4.1 Description

IEEE802.11 represents a popular solution for home access redistribution of connectivity, but elevates even further the challenges of delay and loss reduction, which are critical for VoIP services.

The degradation of speech quality caused by packet delay and packet loss still imposes some of the critical barriers of the VoIP system in a wireless environment. Furthermore, apart from these limitations, WLANs will need to support a large number of concurrent VoIP communications since VoIP is spreading rapidly, especially in public spaces. These motivations led to the study of the maximum capacity of IEEE 802.11b/g networks in the VoIP support.

Network Description

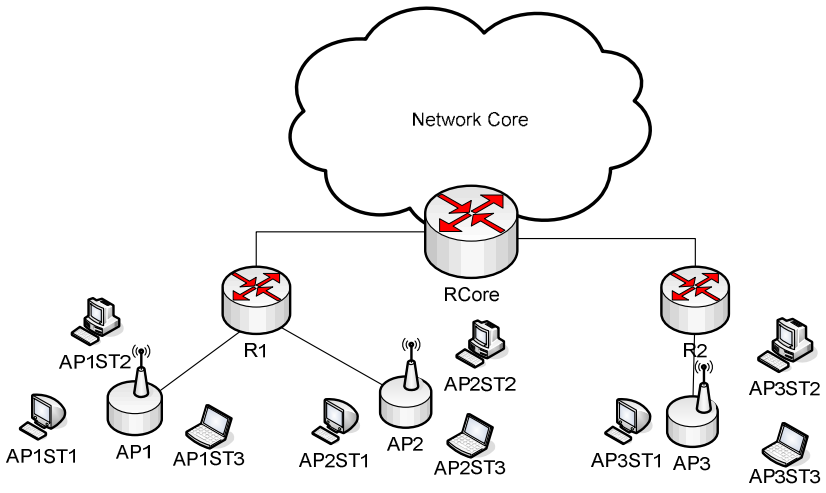

Figure 10 – VoIP over IEEE 802.11, network topology.

The access network is composed by three basic service set (BSS), each with one access points (AP1, AP2 and AP3); the workstations are mobile nodes and communicate with each other and with nodes outside their LAN through the Access Point (AP).

The wired network is Ethernet-base and has two routers (R1 and R2) connected by a router (RCore), R1 is also connected with two access points (AP1 and AP2), and R2 is connected with only one access point AP3. The links were configured with 10Mbps full-duplex.

Each access point (AP1, AP2 and AP3) is connected with three mobile nodes. AP1ST1, AP2ST1 and AP3ST1 are responsible for call generation, while AP1ST2, AP2ST2 and AP3ST2 are the call destinations, similarly to the Ethernet scenario.

Two scenarios have been created by IEEE802.11 study. In the first one, access points and workstations has been configured with protocol 802.11b (data rate 11Mbps), and in the second one with 802.11g (data rate 54Mbps).

Traffic analysis

As aforementioned, every voice packet has 80 bytes; additional headers must be included RTP + UDP + IP + IEEE802.11 with preamble of sizes 12, 8, 20 and 34 bytes, respectively. Therefore, a total of 154 bytes, or 1232 bits, needs to be transmitted 100 times per second, or 123,2kbps, in one direction. For both directions, the required bandwidth for a single call is 200 pps or 246,4 Kbps for a symmetric flow. To all of this we must add the IEEE 802.11 MAC layer overhead, caused by the signaling implied in the usage of Request to Send (RTS), Clear to Send (CTS) and acknowledgement (ACK) messages.

3.1.4.1 Results IEEE 802.11b

This section presents the results collected in VoIP over IEEE 802.11b scenario. Figure 11 depicts the packet loss and end-to-end delay; Figure 12 depicts the causes of the Voice service degradation. Table 2 summarizes the results collected in the various network conditions and indicates the maximum capacity of this network.

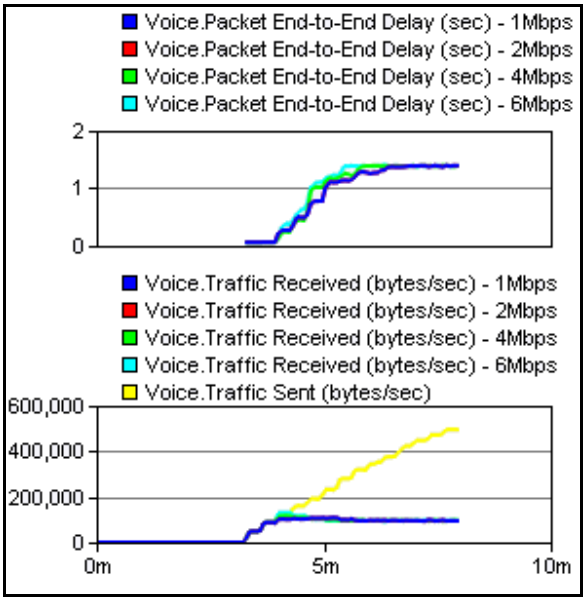

Figure 11 - Voice behavior over IEEE802.11b: End-to-end delay and packets loss.

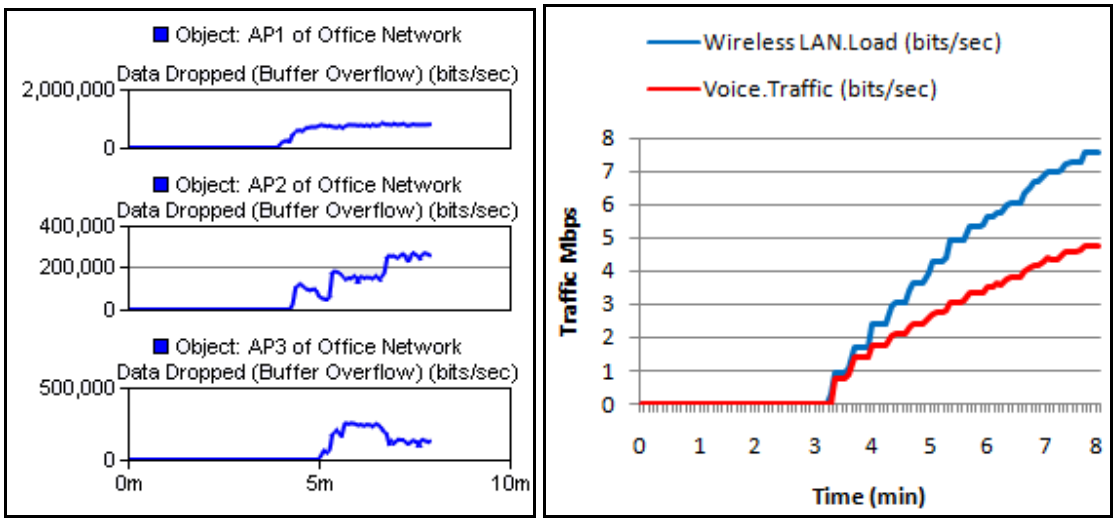

Figure 12 – Causes of saturation, testing VoIP over 802.11b: a) Traffic dropped by each access point; b) difference between traffic Voice and wireless traffic.

	Delay	**Loss**	**Nº calls**
1 Mbps	4min 15 sec	4min 0sec	9
2 Mbps	4min 16 sec	3min 59sec	9
4Mbps	4min 16sec	4min 4sec	9
6 Mbps	4min 5 sec	4min 4sec	9

Table 2 Moment of the thresholds match and number of calls supported, testing VoIP over IEEE802.11b.

3.1.4.2 Discussion IEEE802.11b

Analyzing Figure 11, it is evident that the VoIP service did not experience the changes in load conditions (1, 2, 4 and 6Mbps). The performance of VoIP service is not influenced by changes in the load conditions at the network's core; the voice degradation is the result of the behavior of the access network (IEEE802.11b). Figure 12 indicates that the main reason for the low performance of access network is the amount of traffic dropped by the access points. This effect is a consequence of the small size of the voice packets. Each packet has an elevated MAC layer overhead associated: for each voice packet sent, messages such as ACK, RTS and CTS are transmitted.

Table 2 shows that packet loss was the first threshold to be surpassed in all simulations, approximately four minutes after the simulation starts; the small differences between the results collected do not have a considerable influence of the load conditions, the values have some fluctuation since different simulations produce small differences between the results.

The maximum number of calls that this network can generate before corrupting the VoIP traffic can be calculated by (1), replacing $t_{final}(s)$ by the moment (in seconds) when the limit of packet loss was met,

$$3\left(1+\frac{237-200}{20}\right)\approx 9 \qquad (5)$$

The result of nine calls in our network must be interpreted as 3 calls generated by each access point.

In [25], a detailed analysis of the number of VoIP connection that can be supported by IEEE 802.11b network with a single access point using G711 codec is presented. In this paper, the maximum number of calls supported without a considerable damage in the quality of voice service is of six calls, however in their topology the calls were destined to outside of the wireless network. These results match with our experimental findings since our calls are received within our wireless network; 9 calls are generated and 9 calls are received in the 3 access points, as a result $\left(\frac{9+9}{3}\right)\approx 6$ VoIP flows by access point.

IEEE 802.11b does not represent a high quality solution as an access technology for VoIP services, since only six VoIP flows per access switch can be supported. These values are clearly insufficient to support an enterprise or a public domain; however, in a domestic environment this result can be considered acceptable.

3.1.4.3 Results IEEE 802.11g

This section presents the same results as those in the previous scenario, but while testing IEEE802.11g. Figure 13 depicts packet loss and end-to-end delay; Figure 14 depicts the causes of Voice degradation. Table 3 presents the moments when the thresholds are reached and the maximum capacity of this network.

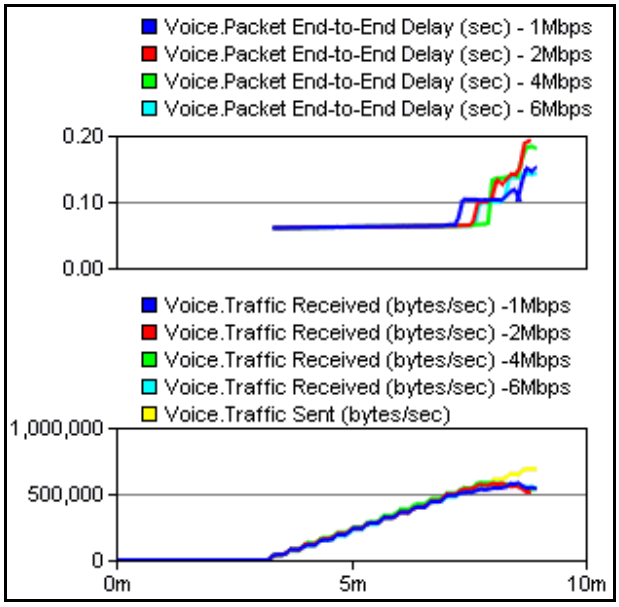

Figure 13 - Voice behavior over IEEE802.11g: End-to-end delay and packets loss.

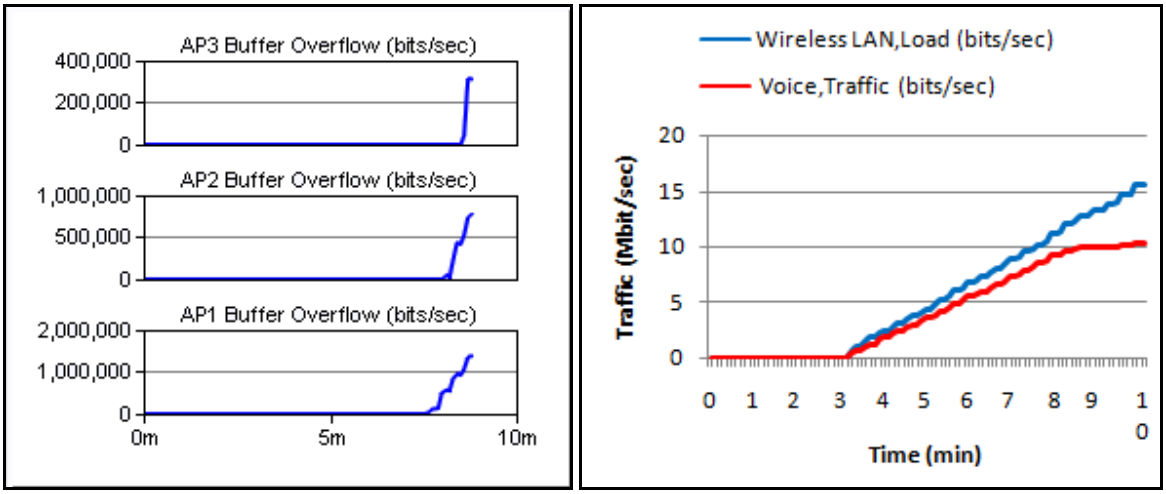

Figure 14 – Causes of saturation testing VoIP over IEEE80211g: a) Traffic dropped by each access point; b) Difference between traffic Voice and wireless traffic.

	Delay	Loss	Maximum Nº Calls
1Mbps	8min 41 sec	7min 40sec	42
2Mbps	8min 38 sec	7min 37 sec	42
4Mbps	8min 58 sec	7min 58 sec	44
6Mbps	8min 55 sec	7 min 54 sec	44

Table 3 - Moment of the thresholds match and number of calls supported, testing VoIP over IEEE802.11g

3.1.4.4 Discussion IEEE802.11g

IEEE802.11g produced a considerable improvement on WLAN performance when compared with the protocol IEEE802.11b, nevertheless the access network remains the cause of the VoIP degradation.

Figure 14 shows that after 7 minutes and 40 seconds from the simulation starts, the WiFi network starts to drop some packets and consequently the VoIP service is damaged. Jitter and end-to-end delay increase; however, jitter never surpasses the limit, (similarly to the previous scenario) and therefore the jitter results were omitted. The number of calls supported is calculated replacing in the expression (1) $t_{final}(s)$ by the moment when the first thresholds (packet loss) was met.

The analysis for the various load conditions has been performed. In all of these cases the wireless network starts to drop packets in between 7 minutes and 40 seconds and 8 minutes after the simulation starts. Packet losses are, in all simulations, the first requirement to be crossed. As in the previous scenario, the load conditions have no influence, since for all simulations the maximum number of calls supported remains almost unaltered and the links in the wired network were healthy. The performance of wireless network is the cause of network saturation and consequent VoIP degradation. The number of calls supported with 1, 2, 4 and 6 Mbps of additional load in the network was 42, 42, 44 and 44 respectively.

The improvement in performance when comparing with 802.11b is notorious; however, the IEEE 802.11g technology does not present the best characteristics for VoIP service, since voice is transmitted in small packets and for each packet additional MAC layer overhead is produced. Consequently, the high bandwidth available in this technology is mostly wasted.

Using IEEE802.11g, approximately 40 calls are supported in simultaneous. This result can be considered satisfactory and acceptable in a large range of situations such as public environments or enterprises.

3.1.5 Scenario 3 – VoIP over ADSL

3.1.5.1 Description

Network analysis

This network is composed by 3 digital subscriber line access multiplexer (DSLAM), which deliver high-speed data transmission over existing copper telephone lines. The DSLAM separates the voice-frequency signals from the high-speed data traffic. Moreover, it controls and routes digital subscriber line (xDSL) traffic between the subscriber's end-user equipment (router, modem or network interface card) and the network service provider's network. The network tested is depicted in Figure 15, where each DSLAM is connected to a DSL router/modem that has 3 workstations connected to it.

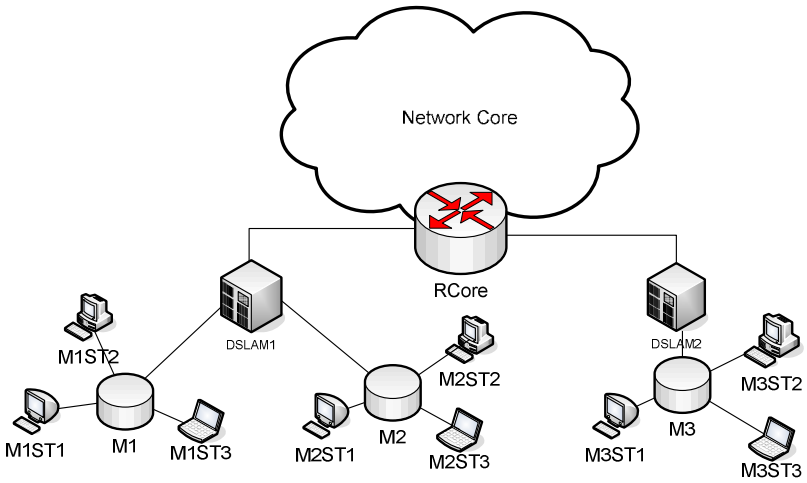

Figure 15 – VoIP over ADSL2, network topology.

ADSL supports different data rates in the upstream and downstream directions. In OpNet, simplex links were used to model such asymmetric data rates, and were manually configured. The data rates set represent ADSL2, which extends the capacity of basic ADSL, with data rates of 12 Mbit/s downstream and 3.5 Mbit/s upstream. Since VoIP is a symmetric application (same needs of up and down link) the uplink will represent the limitative factor in this network due to its lesser capacity.

Traffic Analysis

The Ethernet frames sent out by the workstations are inserted into ATM cells, therefore an additional overhead is added. Each ATM cell has its own header, and its own overhead. ATM cells are 53 bytes long; the header represents 5 bytes and the payload 48 bytes.

Each Ethernet voice packet has 146 bytes, which means that each voice packet generates 4 ATM cells and consequently an additional overhead of 66 bytes is had for each voice packet.

3.1.5.1 Results

This subsection presents the results collected in a scenario of VoIP over ADSL; Figure 16 depicts the voice performance indicators (packet loss and end-to-end delay), Figure 17 shows the utilization of the links that connect the RCore to each DSLAM, identifying the causes of the VoIP degradation. In Table 4, it is presented the summary of the results collected identifying the moment when the

thresholds were reached for the various load conditions. This table also includes information on the maximum number of calls supported simultaneously by this network.

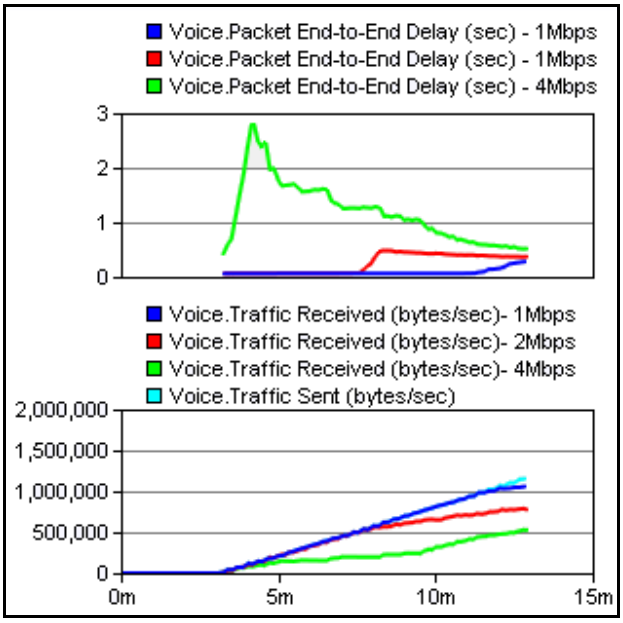

Figure 16 – Voice behavior over ADSL: End-to-end delay and packets loss.

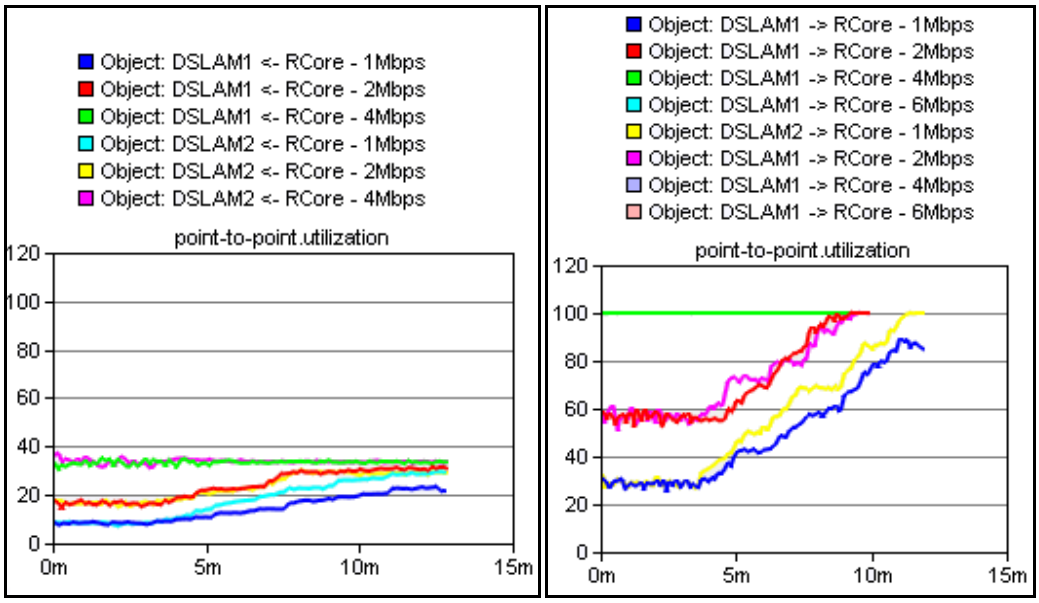

Figure 17 – Links utilization, testing VoIP over ADSL2: a) DSLAM1<->RCore; b) DSLAM2 <->RCore.

	Delay	Loss	Maximum Nº Calls
1Mbps	12min 48sec	11min 38sec	77
2Mbps	7min 59sec	7 min 40sec	42
4Mbps	-	-	0
6Mbps	-	-	0

Table 4 Moment of the thresholds match and number of calls supported, testing VoIP over ADSL.

3.1.5.2 Discussion

In this scenario, the network's conditions have influence in the performance of VoIP service. With 1Mbps of background load, packet loss was the first threshold reached (12 minutes and 38 seconds from the simulation's start), consequently the maximum number of calls supported is 77. Increasing the network load to 2Mbps, the first QoS bound is reached after 7 min and 40 sec; as a result, 42 calls were made ensuring quality of service. The VoIP damage is due to the upstream links which have only 3,5Mbps available, reaching the previous saturation.

The first requirement to surpass the limit was in both cases the packet loss; therefore, the time of its occurrence has been used to calculate the maximum number of calls that the network can support. As we can see in Table 4, with 1Mbps of load in the network, the number of calls supported is 77; changing the load in the network to 2 Mbps, the number of supported calls decreases to 42.

For 4Mbps and 6Mbps, the upstream links are completely saturated from the beginning of the simulation, as seen in Figure 17 b). Consequently, the performance of the network is seriously affected. Loss, jitter and end-to-end delay have inacceptable values during all of simulation, so the VoIP requirements cannot be guaranteed and no call can be performed with guaranteed quality of service.

ADSL can be considered a high-quality solution with low upstream load, since that the number of calls supported is considerably high and no additional installations are required, since ADSL uses the copper wire network already installed.

However, for special cases as enterprises that normally require higher upstream, this technology is seriously affected and its utilization unfeasible. Voice service represents a bidirectional flow, which requires the same bandwidth on the up and down links. This fact is not compatible with the ADSL technology.

3.1.6 Scenario 4 – Optimum voice packet size over IEEE802.11b networks.

3.1.6.1 Description

With the objective of improving the results obtained using the IEEE 802.11b technology, an additional scenario has been created. The network topology remains the same as in 3.1.4, but a change has been introduced in the voice application model. The number of voice frames per packet is configured with different values in order to achieve the optimum packet size for WLANs, as described below. Changing in the OpNet simulator the parameter "Voice Frames per Packet" from 1 to 10 gradually increases the size of the packets produced, and consequently less packets are required, thus decreasing the MAC layer overhead and the packet loss on an IEEE802.11b link.

Silence Length (seconds)	default
Talk Spurt Length (seconds)	default
Symbolic Destination Name	Voice Destination
Encoder Scheme	G.711
Voice Frames per Packet	10
Type of Service	Interactive Voice (6)
RSVP Parameters	None
Traffic Mix (%)	All Discrete

Figure 18 - Voice traffic characteristics, changing the parameter "*Voice frames per packets*".

3.1.6.1 Results

This section presents the results collected in the scenario: Optimum voice packet size over IEEE802.11b networks. Table 5 presents the moment when the thresholds were reached when varying the voice packets' size, and the maximum number of calls supported by the network.

	Delay	Loss	Nº Calls
1 Frame/packet	4min 15 sec	4min 0sec	9
2 Frame/packet	5min36sec	4min 37sec	15
3 Frame/packet	5min 48 sec	5 min 55sec	26
4 Frame/packet	6min 15 sec	6 min 16sec	29
5 Frame/packet	6min 50sec	6min 54sec	34
6 Frame/packet	-	7min 30sec	-
7 Frame/packet	-	8min 0sec	-
8 Frame/packet	-	8min42sec	-
9 Frame/packet	-	9min42sec	-
10 Frame/packet	-	9min50sec	-

Table 5 - Moment of the thresholds match and maximum number of calls supported, searching for the optimum voice packet size.

3.1.6.2 Discussion

Increasing the number of voice frames per packet, less packets need to be generated, thus decreasing the MAC overhead and consequently the packet loss; on the other hand, larger packets increase the end-to-end delay. The conjunction of these facts makes it possible to find the ideal packet size for this type of network.

Analyzing Table 5, the gradual improvement of the IEEE802.11b technology is obvious, reaching its maximum performance with 5 voice frames per packet. A total of 34 calls were supported, and this progress occurs because the MAC layer is less crowded. However combining 5 voice frames in a single packet means that each packet contains 50ms of conversations, and a single loss represents more damage of the VoIP service. Consequently, packet losses can represent a higher risk.

With packets containing more than 5 frames, the end-to-end delay is always superior to 150 ms, the threshold to ensure quality of service in VoIP traffic, so any call can be performed with QoS guarantees.

This scenario aims to conclude that, in wireless environments, small packets reduce the network performance, since the packets are easily lost. On the other hand, with too large packets, the end-to-end delay reaches excessively high values. In a network with these characteristics and using the G.711 codec an ideal value of 5 voice frames should be transmitted in each packet.

3.1.7 Comparison between the different technologies

This subsection aims to compare the technologies tested above in order to identify which technology represents a better solution to the VoIP service, and which technology must be avoided due to its low performance.

3.1.7.1 Results

In order to compare the technologies aforementioned (Ethernet, IEEE802.11b/g and ADSL2), the maximum number of calls supported by each of these technologies is used. The results are depicted in the Table 6 and Figure 19.

Mbps	Ethernet	IEEE802.11b	IEEE802.11g	ADSL2
1	216	9	42	77
2	204	9	42	42
4	164	9	44	0
6	114	9	44	0

Table 6 - Number of calls supported by the different technologies.

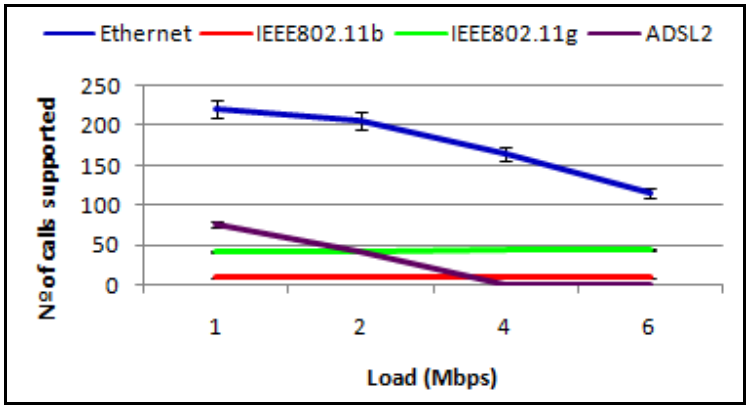

Figure 19 – VoIP performance over different technologies.

3.1.7.2 Discussion

Analyzing Table 6 and Figure 19, it is evident that Ethernet represents the most robust technology. Comparing its performance with the others technologies studied (IEEE802.11 and ADSL), Ethernet is clearly superior.

ADSL is the second best technology, but only with low upstream load. Higher rates of load turn into the worst solution, with zero calls supported if keeping the quality of service requirements. The selection of this technology to supply the VoIP service must be carefully taken, since VoIP produces a bidirectional flow and this technology is asymmetric; consequently, this technology must be only chosen for environment with low upload.

Using WiFi (IEEE802.11b and IEEE802.11g), the number of calls supported by the network is constant for the different load conditions; the wireless network is the responsible for the degradation of network performance. Using 802.11g, the number of calls supported is sufficient to support a small enterprise, nevertheless using 802.11b, the values are lower and applicable for a domestic environment.

3.2 Impact of other services on VoIP

3.2.1 Objective

As aforementioned, Internet works with the philosophy of best-effort. In this sense, the bandwidth is typically shared with all users and all services without distinction. Flows achieve the best possible way to reach the destination. When there is congestion, packets are discarded without distinction.

Keeping in mind the objective of studying the impact of other user oriented services (FTP, HTTP, and Email) on the VoIP service, the following network was created and the VoIP service was introduced among the simultaneous usage of other services. In order to detect which services introduce a more damaging performance penalty in the VoIP service, we evaluated their individual contributions on independent basis, by matching the performance of VoIP in the presence of another single service.

3.2.2 Network description

In this scenario, the damaging effect of FTP, Http and Email services on the VoIP service performance will be evaluated. We use 2 services per simulation: VoIP and other (Http or Email or FTP). The traffic produced by these services is grown gradually. Monitoring simulation results such as packet loss, end-to-end delay and jitter allows identification of the effect of each of these services on VoIP.

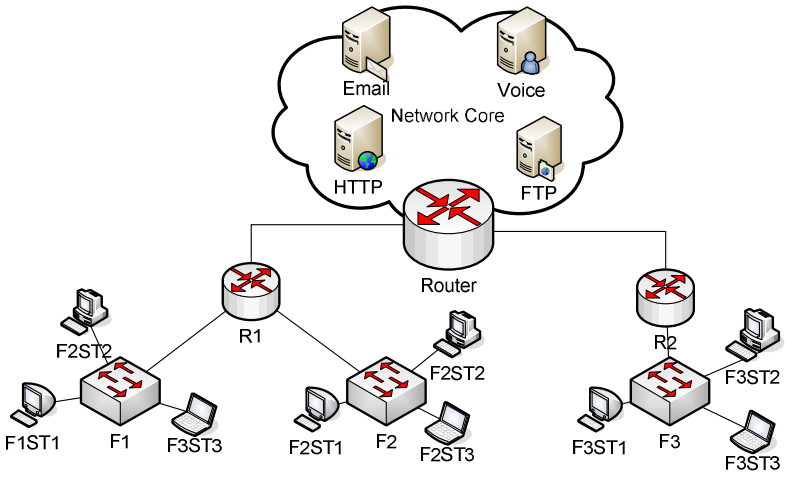

Figure 20 – Influence of other service on VoIP, network topology.

This network is similar to the network used in the scenario 3.1.3 (VoIP over Ethernet); the access and distribution network remains the same. The only difference appears on the network's core, four servers were introduced with intent of producing the services. Each service has a dedicated server (HTTP Server, FTP Server, Email Server and Voice Server), and the traffic produced by these servers has as destination all of the workstations in the network.

3.2.3 VoIP Traffic

VoIP Profile Settings

The voice application model was configured with the same characteristics as in 3.1, however reconfiguration was required. The Profile Definition object was configured to generate the first VoIP call after 70 (60 start time + 10 offset) seconds from the simulation's start, and the repeatability of the VoIP application was set to be *Unlimited* with an inter-repetition time of 2.(2) seconds. The inter-repetition time was calculated intending for each workstation to receive a call each 20 seconds (20/9≈2.2222), since the server it is the responsible for making all calls.

Profile Name	VoIP_Server_Profile
Applications	(...)
rows	1
row 0	
Name	VoIP Server
Start Time Offset (seconds)	constant (10)
Duration (seconds)	End of Profile
Repeatability	(...)
Inter-repetition Time (sec...	constant (2.222)
Number of Repetitions	Unlimited
Repetition Pattern	Concurrent
Operation Mode	Simultaneous
Start Time (seconds)	constant (60)
Duration (seconds)	End of Simulation

Figure 21 - Voice profile configuration, testing the influence of other services on VoIP.

Taking into account the profile defined above, the maximum number of calls in this network can be achieved by:

$$n_{calls} = 9\left(1 + \frac{t_{final}(s) - 70}{20}\right) \quad (6)$$

3.2.4 Services Settings

Profile settings

All further services (FTP, Email and HTTP) were configured with a single profile common to all these services; with this situation we intend that all workstations invoke all services with same frequency.
The services were configured to start their activity 70 seconds after the simulations start, inter-repetition time was set exponential (2), which means that the next application of the current service will start according with the following pattern: exponential distribution with 2 seconds average, Figure 22 depicts FTP profile, however the other services were set with the same configuration.

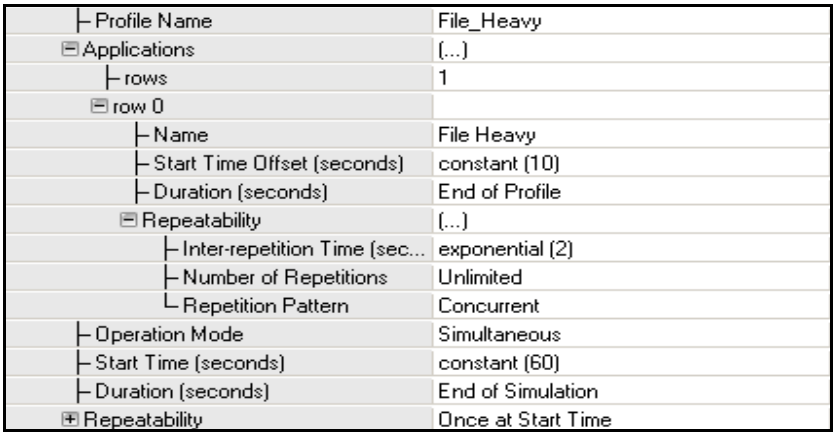

Figure 22 – FTP service, profile configuration.

Applications settings

As aforementioned, the different services have the same profile, consequently services are invoked with same frequency. However each application produces a different amount of traffic per each time that is applied. Analyzing the applications characteristics, the traffic produced was estimated for each service, and the results of our analysis can be found in the following table.

Service	Traffic produced (bytes)	Inter-repetition time (sec)	Traffic produced after 60 min	Traffic produced after 6 min
Ftp	50 000	360	500 000	50 000
Email	12 000	180	240 000	24 000
Http	7 250	6	4 350 000	435 000

Table 7 Evaluation of traffic produce by each service.

The data depicted in the Table 7 help us to understand the amount of traffic generated by each application and the impact that each one will have on VoIP service. It is obvious that for each time that the Http service is invoked, a higher amount of traffic is generated, followed by FTP and finally Email.

3.2.5 Results

This section presents the results collected in the scenario: Impact of other services on VoIP. Figure 23 presents the difference between traffic sent and traffic received of each of the services tested; Figure 24 shows the end-to-end delay and packet loss for the various simulations (VoIP + Email, VoIP + HTTP and VoIP + FTP). Table 8 does a synopsis of the most interesting results collected, identifying the moments when the thresholds were reached. Utilizing the moment when the first threshold was surpassed as $t_{final}(s)$ in (6) the maximum number of calls supported was calculated for the different groups of services.

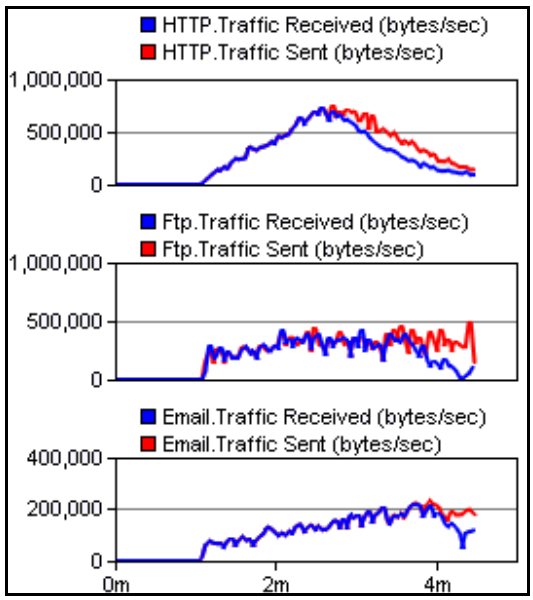

Figure 23 – Effects on TCP services: Voice Vs HTTP, Voice vs. Email, Voice vs. FTP.

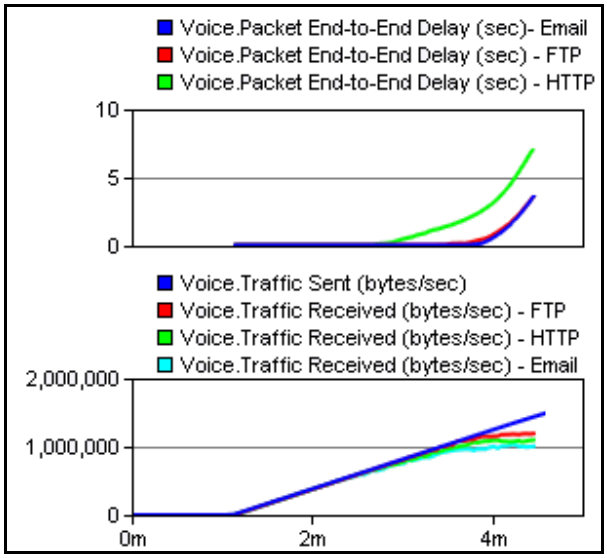

Figure 24 - Voice behavior testing the influence of other services: End-to-end delay and packets loss.

	Delay	Loss	Call
Email + VoIP	3min 35 sec	3min 49sec	75
FTP + VoIP	3min 31sec	3min 45sec	73
HTTP + VoIP	2 min 44 sec	2min 50sec	51

Table 8 Moment of the thresholds match and number of calls supported, testing the influence of other services in VoIP.

3.2.6 Discussion

Observing Figure 23 it becomes perceptible that, after the network congestion, all services (FTP, Http and Email) experience a notorious decrease on the amount of sent data. This fact is most evidenced in the HTTP service because this service presents a sharper traffic growth; however, this behavior is experienced by all services. This effect is a consequence of the transport protocol used - TCP, which is a reliable protocol that ensures that the servers send packets to the clients and wait for an ACK before sending more data, and if the ACK is not received within a stipulated time period, the packet must be retransmitted. On the other hand, voice service is run over UDP, an unreliable protocol, and as a result all traffic is sent regardless of its delivery success.

When comparing the effects of the three services in the VoIP service, it is obvious that Http is the most intrusive. This is easily understood from analyzing the application behaviors shown in Table 7; Http service produces the highest amount of traffic.

The maximum number of calls supported can be calculated by (6). Considering VoIP and HTTP simultaneously in the network, end-to-end delay was the first threshold reached at 2 minutes and 44 seconds after the start of simulation. As a result, 51 calls can be made with ensured quality of service.

Ftp and Email services have an identical amount of traffic produced; as a consequence, they have a similar effect in the voice service. However, Ftp is a little more invasive, the end-to-end delay was the first threshold met at 3 minutes and 31 seconds, and consequently the maximum number of calls that can be supported is 73. Regarding the Email service, the first threshold was met after 3 minutes and 35 seconds, consequently the maximum number of calls that can be supported is 75.

3.3 Video Behavior Vs Network Conditions

3.3.1 Objective

Delivering quality TV over IP networks is far more difficult than delivering data or even voice. And as the Multimedia Research Group [26] points out, people who spend thousands of dollars on high-definition home-theater systems will not tolerate poor video quality. Consumers will replace their cable and satellite systems only if they believe that IPTV can provide as good or better quality, and they will switch back if IPTV fails to live up to expectations.

Consequently, it is necessary to study the behavior of the Video service in different types of IP networks, as well as subjected to different network conditions. Keeping in mind our goal, we will evaluate three different access technologies: Ethernet, IEEE802.11 and ADLS2+ varying the load conditions in the network's core.

The target of this study, however, does not focus on the analysis of high definition video, but rather a type of video application which is more of a mobile-oriented service. Regardless of the fact that fixed networks are also being used, the objective is to allow such a service to be delivered in heterogeneous access technologies and see the performance penalty contributions of each type of networks to better evaluate the quality of delivery in such specific use cases and scenarios.

3.3.2 Video Configuration

One way to model the Video traffic in OPNET is using traffic flows, IP_traffic_flow model, and configuring it in order to represent the desired video service. Each of these demands represents one video flow; in order to simulate the unidirectional video service, one of these flows must be created between the Video server and each workstation.

Video traffic flow represents video compressed with MPEG4/H.264 that can achieve higher compression rates. IP_traffic_flow was configured with the following characteristics: average packet size is set to 2000 Bytes, traffic (bits/s) was set to 4853Kbps, and another important parameter that was configured was "*type of service"* that was changed to Streaming Multimedia.

Video flows have different start-times. In each access device (switch, modem/router or access point), one user starts to receive the video flow 70 seconds after from the simulation starts; after that, every 20 seconds a new user starts to receive another video flow with the same characteristics.

Keeping in mind our objective, the Video service was tested in different load conditions, introducing 30, 40, 50 and 60Mbps of background traffic in the core and distribution network.

3.3.3 Scenario 1 – Video over Ethernet

3.3.3.1 Network Description

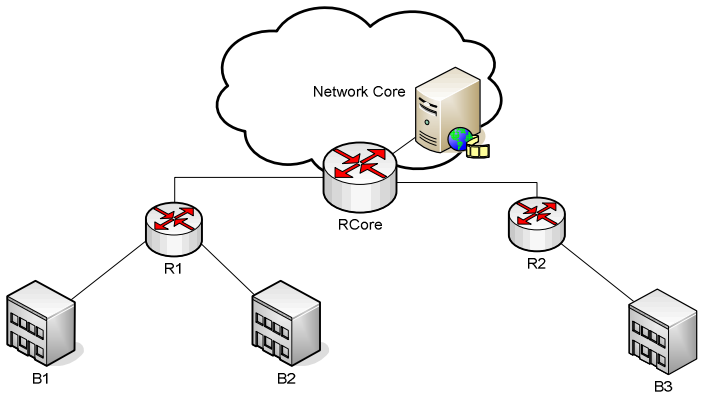

Figure 25 - Video over Ethernet, network topology.

This network topology is fairly different from the topologies used in VoIP service, has various workstations connected to each access switch, represented in the Figure 25 by buildings (B1, B2 and B3).

The capacity of distribution and core links was increased to 100Mbps; nevertheless the access links remain with only 10Mbps of capacity. The video server allocated in the core network is also connected to the RCore router using a 100Mbps connection.

3.3.3.2 Results

This section presents the results collected studying IPTV service over Ethernet. Figure 26 depicts the difference between traffic sent and traffic received; Figure 27 and Figure 28 depict the core and distribution links utilization: these links represent the most utilized links in the network. Table 8 represents the maximum number of video flows supported by the network. In order to better understand values presented in Table 8, since that in this network R1 reaches saturation before R2, Table 10 and Table 11 identify the cause and moment of the network saturation.

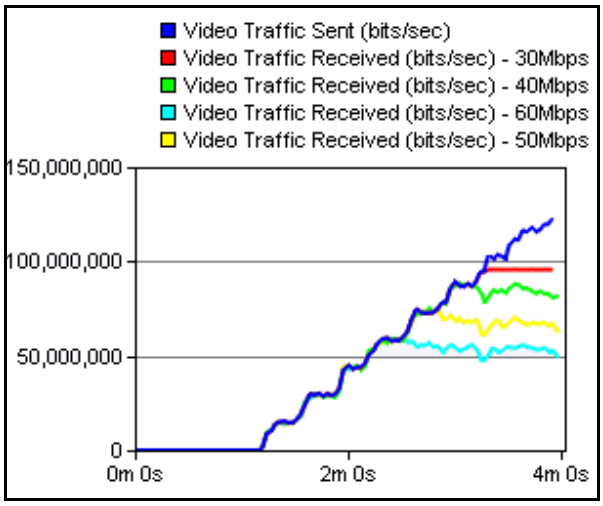

Figure 26 - Video traffic sent vs. video traffic received (packet loss), testing video over Ethernet.

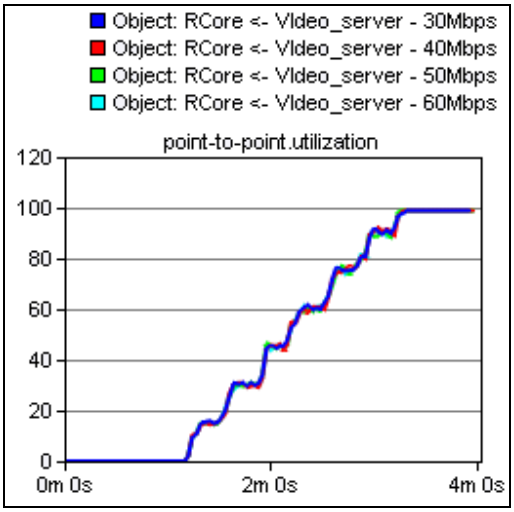

Figure 27 Core link utilization, testing video over Ethernet: RCore <- Video Server.

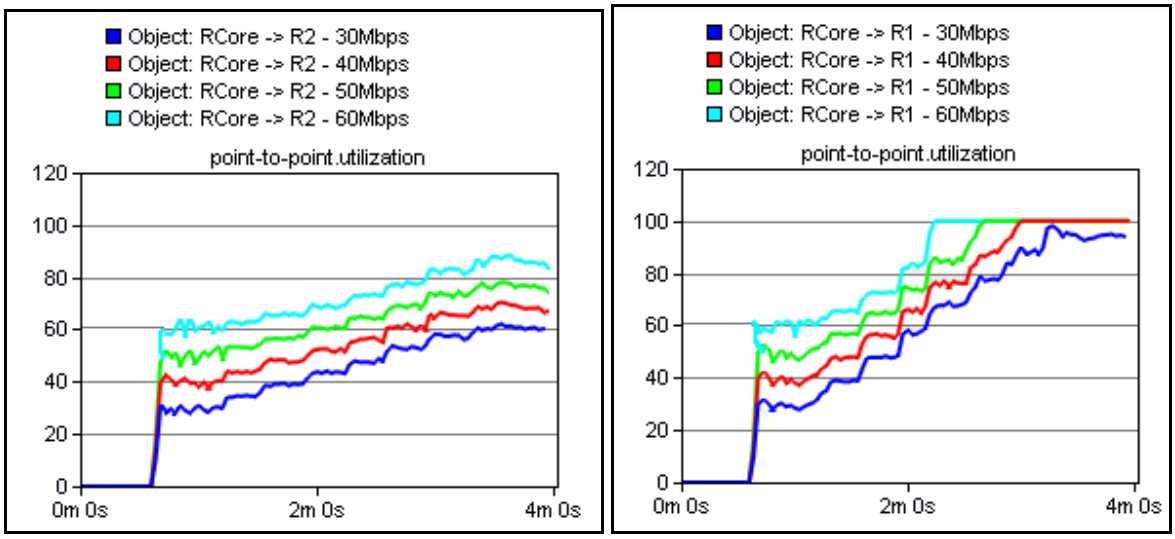

Figure 28 - Links utilization, testing video over Ethernet: a) RCore <->R1; b) RCore <->R2.

	30Mbps	40Mbps	50Mbps	60Mbps
Video flows B1	6	5	4	3
Video flows B2	6	5	4	3
Video flows B3	6	6	6	6
Video flows (Total)	18	16	14	12

Table 9- Number of video flows supported varying the load conditions in the network, testing video over Ethernet.

	30Mbps	40Mbps	50Mbps	60Mbps
Packet losses, B1	3min10sec	2min55sec	2min 30sec	2min14sec
Packet losses, B2	3 min 10sec	2min 55sec	2min 30sec	2min14sec
Packet losses, B3	3min 15 sec	3min 12sec	3min 14sec	3min 12sec

Table 10 - Moment when the threshold (packet loss) was met, testing video over Ethernet.

	30Mbps	40Mbps	50Mbps	60Mbps
Video server <-> RCore	3min18sec	3min17sec	3min18sec	3min17sec
R1<-> RCore	-	3min2sec	2min45sec	2min 18sec
R2<->RCore	-	-	-	-

Table 11 - Cause and moment of the network saturation, testing video over Ethernet.

3.3.3.3 Discussion

Video service is less sensitive to end-to-end delay and jitter. Since it is not interactive video the effects of delay and jitter can be destroyed if using a small buffer; consequently, these effects were not taken into account.

Based on Table 9, we can understand that with a low load in the network's core (30Mbps), this network can support 18 workstations receiving video flows. Figure 28 shows that, after 3 minutes and 10 seconds, some packets are discarded compromising the performance of the video service. The cause for the video service degradation is the saturation of the link that connects the Video Server to RCore. As a result, each building (B1, B2 and B3) supports a maximum of 6 video flows.

Increasing the load in the core and distribution network to 40Mbps, the number of video flows supported by this network is reduced to 16; the main cause of the earlier voice degradation is the link that connects R1 to the RCore, reaching the saturation 3 minutes and 2 seconds after the start of simulation. The link between Video Server and RCore reaches the saturation later as we can see in Table 11.

The saturation of the link between R1 and RCore only affects the performance of the flows directed to B1 and B2, limiting to 5 the maximum of video flows supported by each of these buildings. B3 remains with 6 flows supported, because its performance remains constrained by the link that connects the video server to the RCore.

With 50 and 60 Mbps of load on the core and distribution network, the causes of the saturation are the same as in the case abovementioned (40Mbps); however, the congestion occurs earlier and consequently, at each time that the load is increased, the number of video flows supported by B1 and B2 decreases but in B3 remains at 6. As a result, with 50 Mbps of load, the total of video flows supported is 14 and with 60 Mbps it decreases to 12.

3.3.4 Scenario 2 – Video over IEEE 802.11g

3.3.4.1 Network Description

This network is similar to the previous scenario (Video over Ethernet); the distribution and core of the network have the same characteristics. Nevertheless, network access is different, composed by 3 wireless access points (AP1, AP2 and AP3), each access point has also various workstations connected to it, the workstations are mobile nodes and communicate with each other and with nodes outside their LAN through their Access Point (AP). Data rate supported by these nodes is 54Mbits (IEEE802.11g).

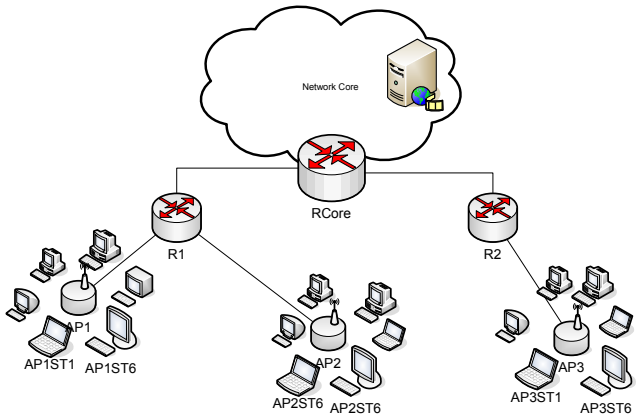

Figure 29 – Video over IEEE802.11g, network topology.

As has been mentioned above, a video packet has an average size of 2000 bytes, additional wireless headers must be include IEEE 802.11 with preamble of 34bytes, the effect of these headers is almost

insignificant, since they represent only 1.7% of the video traffic, however the MAC layer overhead must be taken into account.

3.3.4.2 Results

This section presents the results collected to IPTV over IEEE802.11g scenario. Figure 30 presents Video traffic sent and video traffic received and Figure 31 depicts the cause of the network saturation. Table 12 performs the summary of the results collected in the various load conditions.

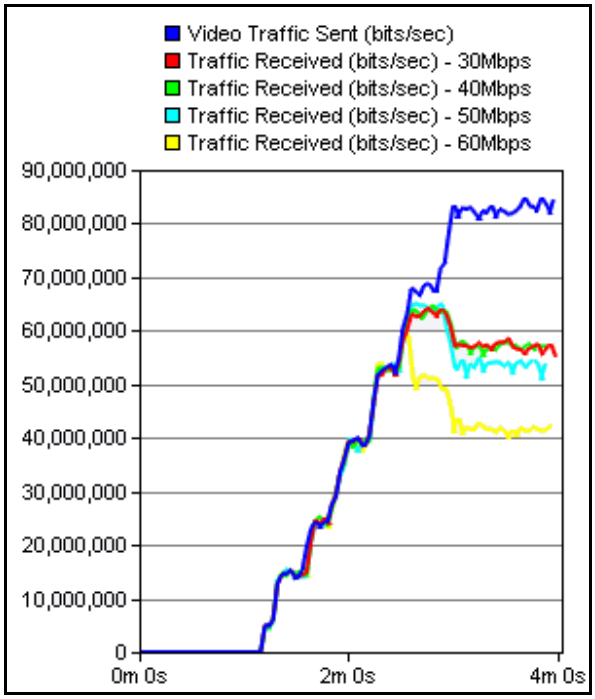

Figure 30 - Video traffic sent vs. video traffic received (packet loss), testing video over IEEE802.11g.

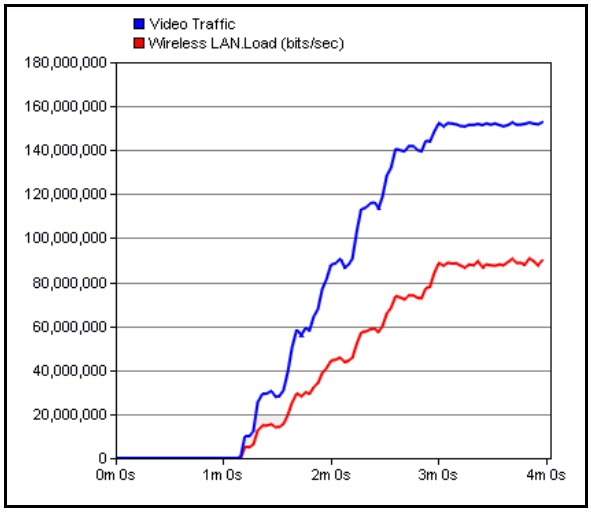

Figure 31 - Causes of saturation: Difference between traffic Voice and IEEE802.11g traffic.

	30 Mbps	**40 Mbps**	**50 Mbps**	**60 Mbps**
Packet losses (sec)	2min37sec	2min34sec	2min31sec	2min36
Video flows supported	12	12	12	10

Table 12 Moment of the threshold match and maximum number of video flows supported over 802.11g technology.

3.3.4.3 Discussion

Figure 30 reveals that approximately after 2minutes and 35 seconds from the simulation's start, video traffic is damaged, a total of 12 video flows got generated as a result by each access point. These results are common for 3 scenarios simulated (30, 40 and 50 Mbps); this shows that the changes in network conditions do not influence the network's performance.

The cause for video service degradation is, in all these scenarios, the wireless network, that, approximately after 2 minutes and 35 seconds, starts to discard some packets. The saturation occurs in the access network, consequently the different load conditions in core and distribution network have no effect in the video service performance. Figure 31 depicts the cause of the access network saturation; the amount of wireless traffic produced in the whole access network reached approximately 150 Mbps (50Mbps per access point) that matches with the data rates supported by IEEE802.11g. The MAC layer overhead adds to the video traffic represents the cause of the amount of wireless traffic produced.

With 60 Mbps of load in the core and distribution network, at the same time that access network reaches the saturation, the link that connects the RCore to the R1 also reached the saturation point, reducing the efficiency of the network and as a result the number of video flows supported by this network is reduced to 10 video flows. Each AP connected to the R1 only supports 3 video flows, but the AP connected to the R2 still supports 4 video flows.

3.3.5 Scenario 3 – Video over ADSL

3.3.5.1 Network Description

This network is composed by 2 digital subscriber line access multiplexer (DSLAM) delivering video flows; DSLAM1 is responsible for performing the data delivery for 2 buildings (B1 and B2) however DSLAM2 is only connected with one building (B3). Each user has DSL modems responsible for modulation and demodulations of ATM traffic.

As aforementioned, ADSL supports different data rates in the upstream and downstream directions, the data rates were manually configured and represent the ADSL2+ technology, with data rates of 24 Mbit/s downstream and 3.5 Mbit/s upstream. Since Video is also an asymmetric application, ADSL seems to present a good solution for this service.

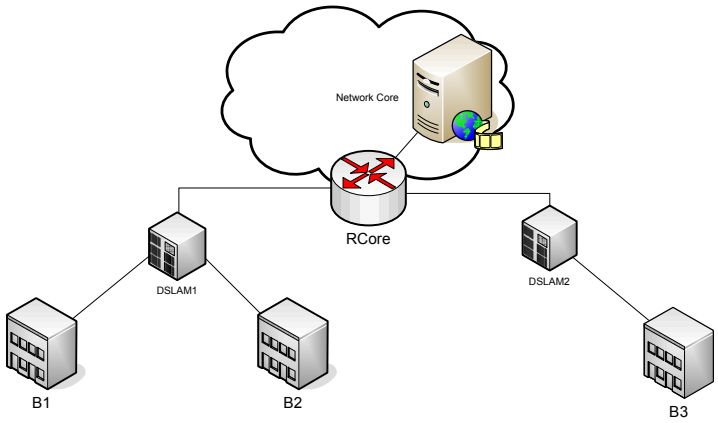

Figure 32 - Video over ADSL2+, network topology.

The transmission of video over ATM cells introduces additional overhead. Video packets have a medium size of 2000Bytes, each ATM cell supports a maximum of 48 bytes in the payload, consequently each video packet produces 42 ATM cells, which introduce an overhead of 210 bytes

per video packet. This value represents 10% of the traffic produced and will consequently introduce a perceptible effect.

3.3.5.2 Results

This section presents the results collected while testing IPTV over ADSL2+ technology. Figure 33 presents the difference between traffic sent and traffic received, Figure 34 and Figure 35 depict the link usage, keeping attention in the links that connect the DSLAM and Video server to the RCore. Table 13 presents the number of video flows supported by each access switch and the total of video flows supported by this network.

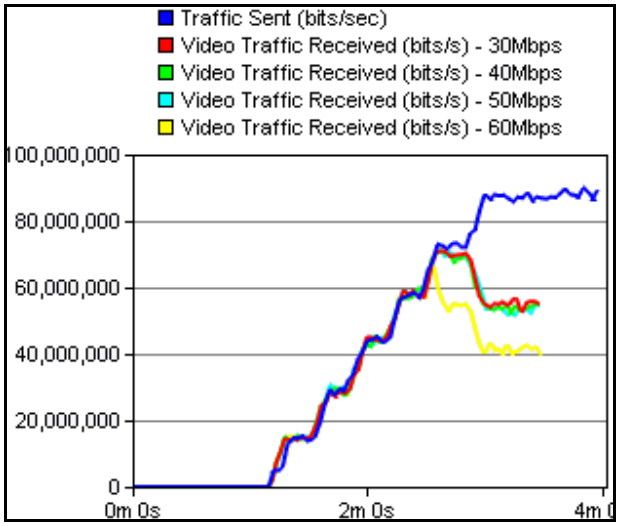

Figure 33 - Video traffic sent vs. video traffic received (packet loss), testing video over ADSL2+.

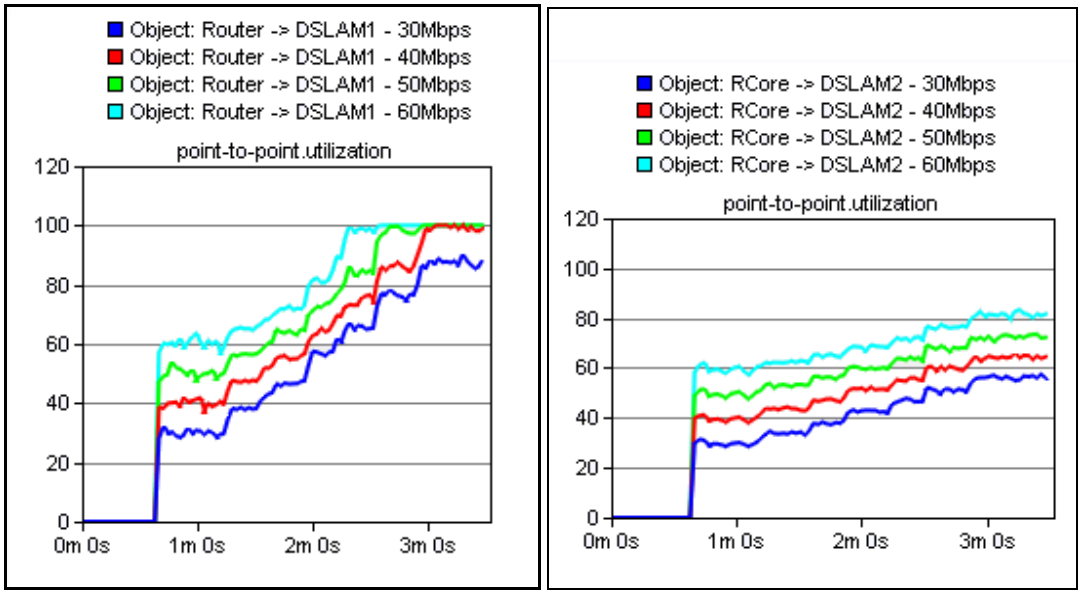

Figure 34 – Links utilization, testing video over ADSL2+: a) RCore -> DSLAM1; b) RCore -> DSLAM2.

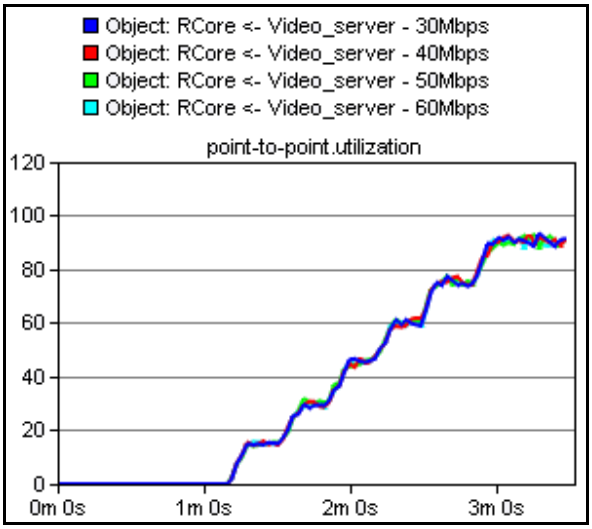

Figure 35 - Link utilization, testing video over ADSL2+: RCore -> Video Server.

Load in core	Num of video flows B1	Num of video flows B2	Num of video flows B3	Total
30MBps	4	4	4	12
40MBps	4	4	4	12
50MBps	4	4	4	12
60MBps	3	3	4	10

Table 13 -Video performance over ADSL technology.

3.3.5.3 Discussion

The network's core and distribution conditions only have influence in the performance of the Video service when the background load introduced is superior to 60Mbps.

In the first three scenarios (30, 40 and 50Mbps) of load in the core and distribution network, those responsible for the network saturation are the distribution links that connect each access router to the respective DSLAM. For this reason, the background load introduced in the core has no effect in the Video Service performance. The number of video flows supported guaranteeing quality of service is conditioned by the DSL links. Using ADSL2+ (24Mbps downlink), the maximum number of videos flows supported by each of this links is four.

With 60Mbps of background, the link that connects RCore to DSLAM1 also reaches saturation, reducing the number of videos supported in the DSLAM 1 to six, 3 flows per each access switch (B1 and B2). The number of video flows supported in B3 remains four; the cause of video degradation is the saturation of the link that connects this building to the DSLAM.

The packet losses were, in all scenarios, the main reason for the video service degradation. As has been mentioned before, this service is very sensitive to losses due to essential frames.

3.3.6 Comparison between different technologies

3.3.6.1 Results

This section aims to compare the performance of the various technologies for which the video service was tested. The maximum capacity of each network was used to determine which technology represents the best and the worst solution to the video service.

	30 Mbps	**40 Mbps**	**50 Mbps**	**60Mbps**
Ethernet	18	16	14	12
IEEE802.11g	12	12	12	10
ADSL	12	12	12	10

Table 14 – Comparison between the different technologies.

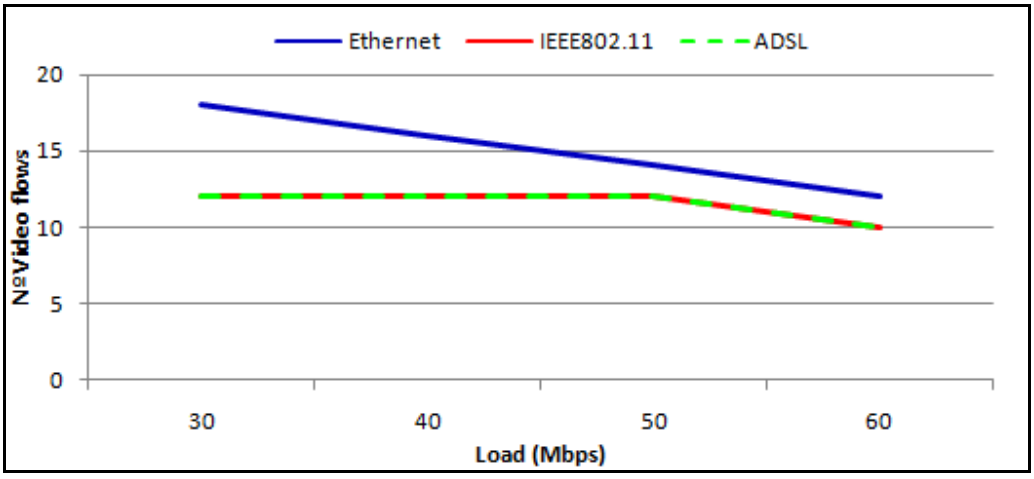

Figure 36 – Video performance over different technologies.

3.3.6.2 Discussion

By analyzing the Table 14, it is evident that Ethernet represents, once more, the most robust technology, when comparing its performance with the other technologies studied, IEEE802.11 and ADSL.

WiFi (IEEE802.11g) and ADSL had similar performance: 12 Video flows supported with 30, 40 and 50 Mbps of load in the core of the network. The number of video flows supported is constant because the cause of the Video degradation is the access network for both technologies.

Increasing the load in the network to 60Mbps, these technologies reduce their performance supporting a maximum of 10 Video flows, 3 video flows in B1 and B2 and 4 video flows in B3. In this case, the reason of the network saturation is a mix of access and core saturation.

ADSL services are supported on copper telephone wires already installed and the number of video flows supported is satisfactory. Consequently, this technology can be considered the most advantageous solution for video services delivery, presenting higher economical viability to the service providers. The asymmetry of the links does not represent any trouble. Since video service is a unidirectional application, all upstream is free to the other applications.

3.4 Impact of other services on Video delivery Behavior

3.4.1 Network Description

The network topology is very similar to the utilized in 3.3.3 video over Ethernet scenario; however, in the network core, additional servers were introduced; the objective of these news servers is the production of Http, Email and Ftp traffic. The network topology of the current scenario is depicted in Figure 37.

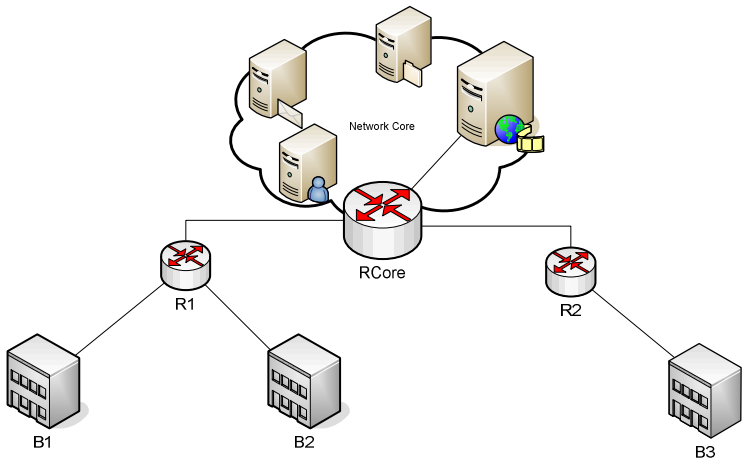

Figure 37 - Influence of other services on video, network topology.

Ftp, Email and HTTP applications were configured using the “application configuration” object with the same characteristics as in 3.2 (Impact of other services on VoIP), since the objective is the same, evoke all services at the same frequency, consequently FTP, Email and HTTP services were configured to be evoked by the workstations with distribution exponential and average 2 seconds.

The main objective of this study is the identification of a service that introduces the most damaging performance penalty in the Video service. Each service is evaluated in an independent basis, first we evaluate the impact of HTTP service, followed by the analysis of FTP services and, at last, Email service.

3.4.2 Results

This section presents the results collected in the scenario: Impact of other services in IPTV. Figure 38 depicts difference between Video traffic sent and Video traffic received, identifying the moments

when the thresholds were reached. Table 15 indicates the number of video flows supported by each access switch as well as the total number of video flows supported by the network.

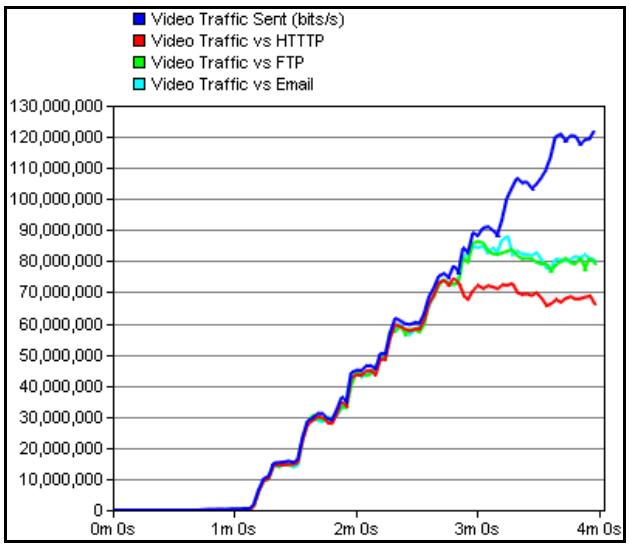

Figure 38 - Video traffic sent vs. video traffic received (packet loss), testing the influence of other services on video.

	40Mbps (Video)	40Mbps (Video +Http)	40Mbps (Video +Ftp)	40Mbps (video+ Email)
Video flows B1	5	3	4	4
Video flows B2	5	3	4	4
Video flows B3	6	6	6	6
Total video flows	16	12	14	14

Table 15 - Influence of other services in the performance of video service.

3.4.3 Discussion

Comparing the effects of the services (Http, FTP and Email) in the video stream, it is noticeable that Http represents the most destructive service; this is a consequence of the amount of traffic produced by this service which is clearly superior to the amount of traffic produced by the other services. The number of video flows supported in the presence of this service decrease to 12. This means that the HTTP services reduce the number of video flows supported in a total of 4 when compared with a scenario with Video service only. These results can be analyzed in Table 15.

FTP and Email services have less impact in Video service, since the amount of traffic produce by these applications is lower. The number of Video flows supported by this network in the presence of these services decreased to 14 and, as a result, 2 flows are avoided for the presence of FTP or Email service.

For users connected to B1 and B2, the reason of video degradation is the saturation of the link that connects R1 to the RCore. Users connected to B3 receive damaged video as a consequence of the saturation of the link that connects the video server to the RCore.

3.5 Impact of video on voice and voice in video

3.5.1 Description

The objective of this simulation was to evaluate the impact of voice in video service and video on voice. The same network was used as in the study of video performance over Ethernet; however, a new service was introduced in the core. The objective of this new server is the generation of VoIP service, each service Video and VoIP is generated in an independent server.

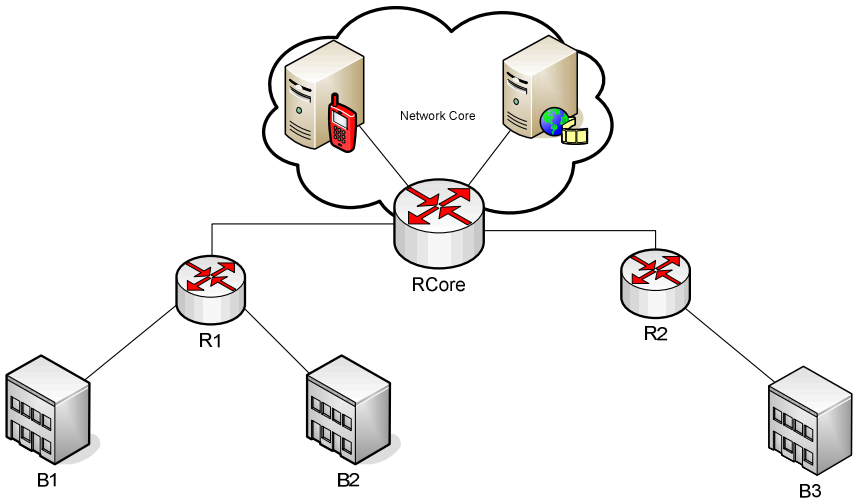

Figure 39 –VoIP and Video, network topology.

Keeping in mind our goal, 6 different scenarios were generated. The first scenario has only one video flow per access switch (B1, B2 and B3), and voice calls are generated at a fixed rate until the network saturates. On the second scenario, 2 video flows are generated per building and VoIP calls are

incremented until network saturation point is reached; the subsequent scenarios follow the same philosophy, the number of video flows per access switch was incremented one by one at each new scenario. For all these scenarios were calculated the maximum of voice calls that can be incremented without surpassing the video and VoIP thresholds independently.

The voice application object was configured to start the generation of calls 100 seconds after the start of simulation, and 2 new calls are incremented every two seconds, consequently the number of calls produced can be calculated by:

$$n_{calls} = 2\left(1 + \frac{t_{final}(s) - 100}{2}\right) \qquad (7)$$

3.5.2 Results

The following tables represent the values collected for all scenarios studying impact of voice in video and vice versa. Table 16 depicts the moment when the most relevant thresholds were reached; Table 17 has information about the maximum capacity of this network in both situations: maintaining the VoIP requirements or maintaining the Video requirements. Figure 40 compares the performance of both services.

Scenario	Voice Packet losses	Voice End-to-end delay	Video Packet losses
1 video flow per access switch	5min 32 sec	5min31sec	5min15sec
2 video flow per access switch	5min 25 sec	5min 17sec	5min 12sec
3 video flow per access switch	5min15sec	5min 14 sec	5min 10sec
4 video flow per access switch	5min8sec	5min6sec	5min 57sec
5 video flow per access switch	4min 20sec	4min 50sec	3min20sec
6 video flow per access switch	3min 4sec	4min 48sec	-

Table 16 - Moment when the requirements where reach for voice and video services.

Nº of Scenario	Total number of video flows	Nº of calls without damaged Voice	Nº of calls without damaged Video	Cause
1 video flow per access switch	3	245	228	Router saturation
2video flow per access switch	6	230	225	Router saturation
3 video flow per access switch	9	227	223	Router saturation
4 video flow per access switch	12	158	209	Router saturation
5 video flow per access switch	15	170	107	Router and links saturation
6 video flow per access switch	18	90	-	Router and links saturation

Table 17 – Maximum calls supported in each scenario: without damage voice, without damage video.

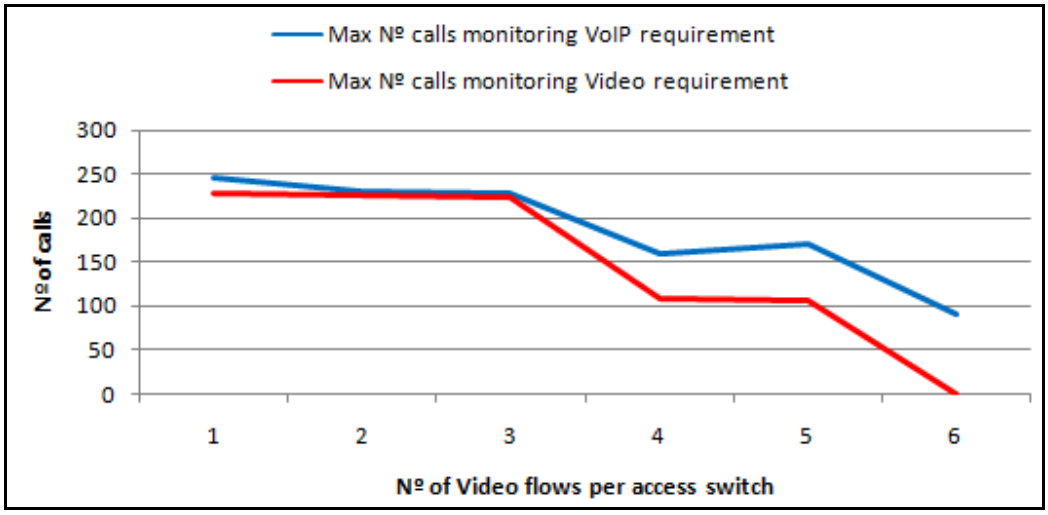

Figure 40 - Video vs. Voice performance.

3.5.3 Discussion

In all scenarios, the video service was the first service to be degraded, its thresholds were the first to be reached. Consequently, the maximum number of calls supported by this network is determined by (7) using the moment when packet loss occurs in video service as $t_{final}(s)$.

In the first scenario (only one video flow per access switch), the number of calls supported is very high: 243. Increasing the number of video flows, this value will be gradually reduced until the minimum of 88 calls, with 6 video flows per access switch.

We can conclude that the video service is more sensitive than VoIP service, since the damaging effects of both services working simultaneously are earlier experienced in this application. The high instability of Video service is a result of the presence of I-frames and consequent intolerance to packet loss.

However, the provisioning of both services simultaneously over Ethernet, represents a high-quality solution since, even in the eventuality of 6 flows being distributed by each building, the number of calls supported with ensured quality is very high (88); this can be considered an acceptable performance in a large range of situations.

3.6 Conclusions

During this study we address two main multimedia services, VoIP and IPTV. Each of these services has been tested over various technologies such as Ethernet, IEEE802.11 and ADSL; and each technology was tested in different load conditions. The second purpose of this study was to verify the impact of some services such FTP, Http and Email in our multimedia demands. Keeping in mind our goals, we performed extensive simulations using OpNet.

VoIP service has exhibited better performance over Ethernet with a maximum of 223 calls supported, followed by IEEE802.11g and finally IEEE802.11b and ADSL. Analyzing which of these technologies is the most inefficient for VoIP service, 802.11b has a low but constant performance for the different loads; ADSL has a good performance with low load in the core, but when the load increases, no calls are supported — the low upstream of this technology represents a difficulty to bidirectional applications such VoIP. Consequently the choice of IEEE802.11b or ADSL must take into account the

characteristics of the network where the services will be supplied. For example in a small enterprise that normally needs elevated upload the choice of ADSL can represents a mistake.

The most problematic requirement for each technology was also identified; in fact, over Ethernet, end-to-end delay was in all simulations the first threshold being met. On the other hand, in wireless and ADSL technologies, the first requirement to surpass the limit was in all cases the packet losses.

Similarly to VoIP, Video service also presents its best performance over Ethernet technology, with a maximum of 18 video flows supported by the network (low load in the core). Increasing the load in the core to the maximum of 60 Mbps, the number of flows that can be supplied is of 12. ADSL2+ and IEEE802.11g have a similar performance: with 30, 40 and 50 Mbps the number of video flows supported was 12; this number is not influenced by the load in the network core since the saturation occurs in the access network. However with load superior or equal to 60 Mbps the load conditions have influence in the network performance, and video service suffers an additional damage, consequently only 10 Video flows are supported. ADSL has the advantage of being able to be deployed over existing cables, which makes it much cheaper than installing a new infrastructure.

It is important to notice that video service is more sensitive than voice service with regards to packet losses, since a few packet losses in video can lead to catastrophic damages in video quality. On the other hand, VoIP is very sensitive to the delay, since it is an interactive service.

After the analysis of the VoIP and Video services over various technologies, our attention was oriented to the impact of other user-oriented services such FTP, HTTP and Email in our multimedia services (VoIP and Video).

The influence of other services operating simultaneously with VoIP introduced a considerable degradation of VoIP service. In the worst case, Http coexisting with VoIP, the network performance was reduced to half of the previous one. With the other addressed services (FTP and Email), the degradation was not so sharp; nevertheless, the number of calls supported decreased from 79 to 62 and 70, respectively.

For the Video service, the effects of introducing other services also had a relevant impact. Http remains the most intrusive service reducing the number of video flows supported by the network

from 16 to 12. The effects of FTP and Email service were also noted, the packets were discarded earlier than in the scenario containing only Video service. However, this effect was less destructive and as a result 14 video flows are still being supported by the network.

Testing simultaneous Video and Voice services, the earlier degradation of the video service proves that this service is the most sensitive. However, the results of both services working simultaneously over Ethernet technology is advantageous, allowing better utilization of the link's capacity.

4 Framework for IPTV and VoIP Monitoring

4.1 Introduction

With the increasing consumers demands, the service providers and third party service providers are forced to monitor the network, in order to ensure that their services are delivered with acceptable quality, and according with the agreement performed with the costumer. During this phase of the study, VoIP, Videoconferencing and IPTV services will be the target of our attention.

The data resulting from the network monitoring are very important and useful for network management. However this must be tracked and managed. A listing with all this information should be kept up to date, in a location when everyone involved in the process can access them. Some recommendations have been deployed with intend of managing these data.

Local storage versus archival store locally the data used for event and trend analysis since these data must be access easily and quickly. The data that is not used for these purposes must be stored in archive in a different location.

Selective copying data; when the data gathered is being used to event notification and trend analysis, all iteration of the data are copied to a database separated geographically. A trade off of this recommendation is that some data can be lost during the copy process.

Data migration: when the data is collected for trend analysis. Data can be stored locally and then downloaded to an archive when the traffic is expected to be low (e.g. at night).

Metadata: often referred as “data about other data” is supplementary information about the gathered data, such as time stamps, units, data types and any other useful information. A data archival system should provide this additional information to the gathered data.

In this chapter will be develop a framework that perform various steps in the management of multimedia services. The process starts with end-to-end monitoring of VoIP, Videoconferencing and IPTV services; the second step is the analysis of the performance measurements collected; finally, the values considered interesting for the analysis of the services are stored in a database. All this process

occurs automatically and in real-time, at the same time that performance measurements are collected, are analyzed and automatically sent to the database, which is updated every 15 minutes

To perform this process, several software packages were used: Open EMS Suite[27], Tshark[28] and Tstat [15]. Open EMS suite is Nokia Siemens Networks software that provides the fundamental capabilities of an element management system (EMS), the framework for management of telecommunication network elements; Open EMS Suite offers a number of features around adaptations, including runtime deployment, tool support, life cycle management, extensibility, and versioning. Tshark is a freeware packet sniffer that allows to capture the packets in wired networks. Tstat is a freeware passive monitor developed by *Politecnico di Torino*; this tool allows the network monitoring based on TCP and RTP/RTCP protocols.

The developed framework provides important capabilities for the network management, allowing the third-party service providers to have a precise awareness of the present state of their services performance. The information provided can be used to identify trends of failure; identifying these circumstances, it is possible to manage the network in order to recover and avoid the failure. Also in the case of failure, it is possible to give a better and quicker response to the problem.

This chapter is divided in various subsections: In 4.2 it is presented the main tasks performed during the framework development. Subsection 4.3 deeply explains the implementation of the various models necessaries. In 4.4 it is presented the two scenarios where it is possible to use this framework, and subsection 4.5 presents the results obtained and its subsequent analysis. In 4.6 it is pointed some of the problems encountered during the process, and finally, in 4.7 it is presented the main conclusions.

4.2 Framework Development

Before starting the traffic management process, it is necessary to develop the framework. This framework is a set of tools and software working together with objective to monitor VoIP, IPTV and Videoconferencing traffic. Consequently, it was necessary to perform several tasks that we following explain.

The first task was the selection of the tools that we would be using during the process. This implies a deep study of freeware monitoring tools available and the capabilities of each of them in order to identify and match each tool to the required characteristics. Then, it was necessary to identify the performance measurements and information that would be possible to collect.

The second main task was characterized by the specification of the architecture of our framework taking in to account the tools selected and consequently the implementation of the models that would be necessary to support our framework (Script model, Awk model and Noke2eKOALA model). These models were implemented by us; its implementation will be deeply explained in the section 4.3.

Subsequently, it was necessary the development of an adaptation mechanism. Adaptations are metadata that either describes how data in Open EMS Suite is represented or how it is manipulated during runtime usage. In our specific case, since the objective is to collect performance measurements from the network and store them in a database, the adaptation is the responsible to create a structure in the database that allows identifying and storing the performance measurements.

After the development of the adaptation, is was necessary to perform its deployment in an Open Suit EMS server: we use a south mediation interface for getting or setting data in the Open EMS Suite database.

After the deployment of the adaptation, we can start the performance measurements collection, and store them in the database. Figure 41 depicts the flow of the process.

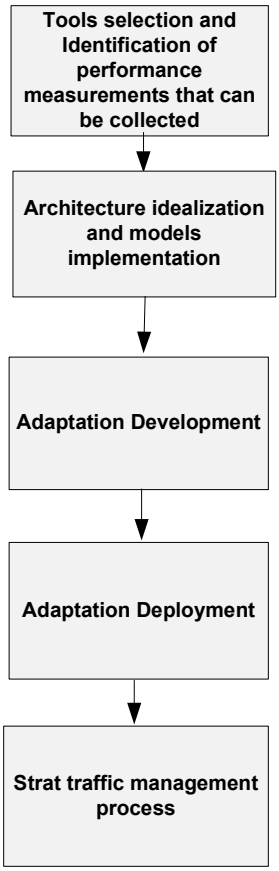

Figure 41 - Identification of the main task before traffic management.

4.3 Models

This section aims to present information about some of the fundamental models created during the framework development process: data model, OMeS model, adaptation Model (.pmb), Noke2eKOALA model and script model.

Data model presents all the performance measurements collected for the different types of traffic, in both scenarios. In OMeS model subsection, it is briefly described the process of OMeS construction and presented the final structure of the file, supporting all performance measurements in the format acceptable to Open EMS Suite. In adaptation model section, it is described the process of creating a .pmb (performance measurement basis) using Adaptation Software Development Kit (SDK) [29]. This represents the most important task in the adaptation development. Noke2eKoala subsection

introduces the main objective of this model and briefly describes the construction's process. Finally in the script model section, which is only used in the second scenario, we describe step by step all the tasks performed by the script.

4.3.1 Data model

The following model represents the structure of the performance measurements monitored and being the basis for the subsequent process. All the values collected are end-to-end performance measurements, so each service analyzed appears as a dependency of E2E. For each type of service, VoIP, IPTV and Videoconferencing, it is collected a group of performance measurements, such as delay, jitter, packet loss and others. A special analysis was performed for Skype, due to its high economics viability and popularity.

E2E

- **Voice**
  - Delay (ms)
  - Jitter Average (ms)
  - Jitter Max (ms)
  - Jitter Min (ms)
  - Packets Transferred (Units)
  - Packets Lost (Units)
  - Transferred Payload (Bytes)
  - Average Speed (bps)
- **Video (videoconferencing)**
  - Delay (ms)

- ↳ Jitter Average (ms)
- ↳ Jitter Max (ms)
- ↳ Jitter Min (ms)
- ↳ Packets Transferred (Units)
- ↳ Packets Lost (Units)
- ↳ Transferred Payload (Bytes)
- ↳ Average Speed (bps)

↳ **Video Streaming**

- ↳ Delay (ms)
- ↳ Jitter Average (ms)
- ↳ Jitter Max (ms)
- ↳ Jitter Min (ms)
- ↳ Packets Transferred (Units)
- ↳ Packets Lost (Units)
- ↳ Transferred Payload (Bytes)
- ↳ Average Speed (bps)

↳ **Skype**

- ↳ N Calls
- ↳ Total Data C->S (bytes)

- ↳ Total Data S->C
- ↳ Total Packets C->S
- ↳ Total Packets S->C
- ↳ Total bps C->S
- ↳ Total bps S->C
- ↳ Total Pps C->S
- ↳ Total Pps S->C
- ↳ Data C->S per Call
- ↳ Data S->C per Call
- ↳ Packets C->S per Call
- ↳ Packets S->C per Call
- ↳ Bps S->C per Call
- ↳ Pps C->S per Call
- ↳ Pps S->C per Call

4.3.2 OMES Model

The OMeS Model (Open Measurement Standard) is the file where the collected performance measurements are grouped; this file has specific characteristics and structure that allows the performance measurements to be supported by Open EMS suite and subsequently to be loaded in the database.

In our framework, the OMeS files can be created in two different ways, can be created using noke2eKOALA, a software that converts CSV files into OMeS. Another way is to use the script model developed in the framework of this Thesis, that will be explained in the section 4.3.5.

During OMeS creation process, it is necessary to pay special attention to the header creation, since the header contains the information that allows the file to be accepted by Open EMS Suite. Some of these essential fields are: accurate data and time, identification of the adaptation and interval of the data collection (in our case it was set with the default value, 15 minutes).

After the header construction, it is necessary to create the MeasurementType. This field indicates at which type of traffic the performance measurements are referring to; in our case, it was configured to VOICE, VIDEO, VC and SKYPE.

The last point in the OMeS construction is the allocation of the performance measurements collected to each MeasurementType. The performance measurements must be created one by one, and are introduced in the OMeS with the following formatting:

<PerformanceMeasurement> pm Value <PerformanceMeasurement>, in Figure 42, it is depicted the structure of an OMeS file.

```
<OMeS adapId="noke2e" adapRelease="E2E1.0" version="2.3">
    <PMSetup startTime="2009-05-28 T11:58:50+00:00" interval="15">
        <PMMOResult>
            <MO dimension="network_element">
                <DN>PLMN-1/E2E-noke2eE2E1_1</DN>
            </MO>
            <PMTarget measurementType="VOICE">
                <VoiceDelay> 30.642 </VoiceDelay>
                <VoiceJiter> 0.000000 </VoiceJiter>
                ...
            </PMTarget>
        </PMMOResult>
        <PMMOResult>
            <MO dimension="network_element">
                <DN>PLMN-1/E2E-noke2eE2E1_1</DN>
            </MO>
            <PMTarget measurementType="VIDEOSTREAM">
                <VideoStreamDelay> 5.012430 </VideoStreamDelay>
                <VideoStreamJiter> 6.855470 </VideoStreamJiter>
                ...
            </PMTarget>
        </PMMOResult>
        <PMMOResult>
            <MO dimension="network_element">
                <DN>PLMN-1/E2E-noke2eE2E1_1</DN>
            </MO>
            <PMTarget measurementType="VIDEOVC">
                <VideoVCDelay> 0.000000 </VideoVCDelay>
                <VideoVCJiter> 0.000000 </VideoVCJiter>
                ...
            </PMTarget>
        </PMMOResult>
    </PMSetup>
</OMeS>
```

Figure 42 - OMeS structure

4.3.3 Adaptation Model (.pmb)

Performance measurement basis (.pmb) model is the responsible by the creation of a structure in a database that allows the reception of the performance measurements. The model creates the fields in the database that will receive the results collected.

This model represents only one of the models utilized during the development of our adaptation. The adaptation development is a complex task since it is necessary the creation of various models, each of these models add a new capability to the adaptation. We opt to only explain the creation of .pmb file

that represents the most important step during the adaptation conception, in view of the fact that that we aim to use the adaptation to create a database structure to receive the gathered values.

The .pmb file was developed using Adaptation Software Development Kit (SDK), a Nokia Siemens Network software with graphical environment.

For this development, first it was necessary to identify the measurement types and the ID (identification) of each measurement. Measurement types were configured in concordance with OMeS file with parameters: VOICE, VIDEO, VC and SKYPE. After this point, it was necessary to specify the default measurement period as fifteen minutes according with OMeS file. Finally, we configure all performance indicators such delay, jitter and packet loss. Each performance indicator is associated with one measurement type and with the correspondent units. Figure 43 shows few parts of the SDK output (.pmb file).

```
<?xml version="1.0" encoding="ASCII"?>
<com.nokia.oss.pm.pmb:PMBasicAdaptation xmi:version="2.0"
  <Adaptation href="noke2e.common#/"/>
  <MeasurementType id="voice" presentation="VOICE"
  description="Voice Service Info. (VOICE)"
  defaultMeasurementPeriod="FifteenMinutes">
    <annotations>
      <elements name="aliasName" value="VOICE"/>
      <type href="../core/core.common#//nameInMeasFile"/>
    </annotations>
    <annotations>
    <MeasuredIndicator id="voice0001" presentation="Voice Delay"
    description="Voice Delay ms">
    <MeasuredIndicator id="voice0002" presentation="Voice Jiter "
    description="VoiceJiterAvg_ms">
    (...)
    <MeasuredTarget>
  </MeasurementType>
  <MeasurementType id="video" presentation="VIDEO"
  description="Video Service Info. (VIDEO)"
  defaultMeasurementPeriod="FifteenMinutes">
```

Figure 43 - Few parts of the application structure

4.3.4 Noke2eKoala Model

Noke2eKoala model is a metadata that allows the Open EMS Suit system to convert CSV files in OMeS files. This model will only be used in Scenario 1 explained in the subsection 4.4.1. In this scenario, the performance measurements will be collected using the OpNet simulator.

This XML file needs to be manually implemented and then supplied to the Open EMS Suit software. Noke2eKola allows the Open EMS Suit to support the CSV files exported by OpNet, converting them to the OMeS files. After this conversion, the performance indicators extracted by OpNet are ready to be loaded in the database.

During the implementation of Noke2eKOALA, it is necessary to have a previously knowledge of the CSV architecture, in order to correctly convert the file.

Each CSV file contains only one measurement type (VOICE or VIDEO), and each column of the CSV file represents one performance measurement. The name of the CSV file identifies the measurement type, and the first line of the CSV file identifies each performance measurement. Taking into account this information, we can start the implementation.

The first step in the implementation is the identification of the adaptation and the release to which this converter will be utilized, that is represented by the first block of the Figure 44. Following, it is necessary to associate to the measurement type (CSV file's name) the name of the measurement type in the OMeS file: this procedure is represented by the second block; additionally, at this point we must provide information about the period of data collection. Aforementioned, each column in the CSV file represents one performance measurement; consequently these fields will generate a performance indicator in OMes file. Information about the measurement units must be also provided in this Step that is represented by the third block in the Figure 44 that must be repeated for various performance measurements collected.

Figure 44 depicts the code responsible to convert the Voice measurements. However, a similar structure was implemented to IPTV service. It is important to notice that Figure 44 does not represent the real structure of the implementation, but it is just a synopsis of some of the most important steps.

After the implementation, this file is included to the Open EMS Suit, becoming this software capable to convert the CSV files to OMeS and subsequently load them in the database.

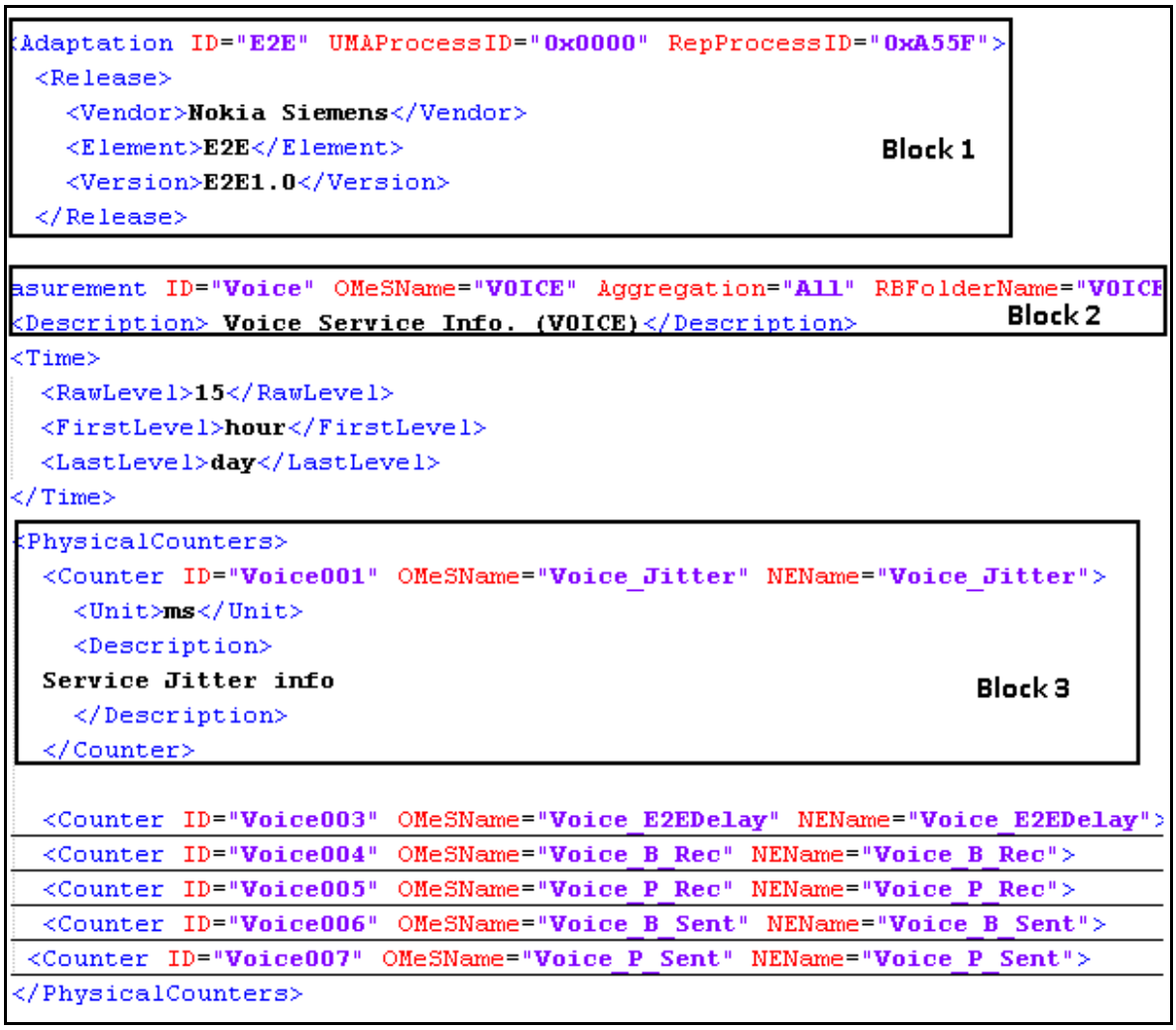

Figure 44- Noke2eKoala Structure.

4.3.5 Script Model

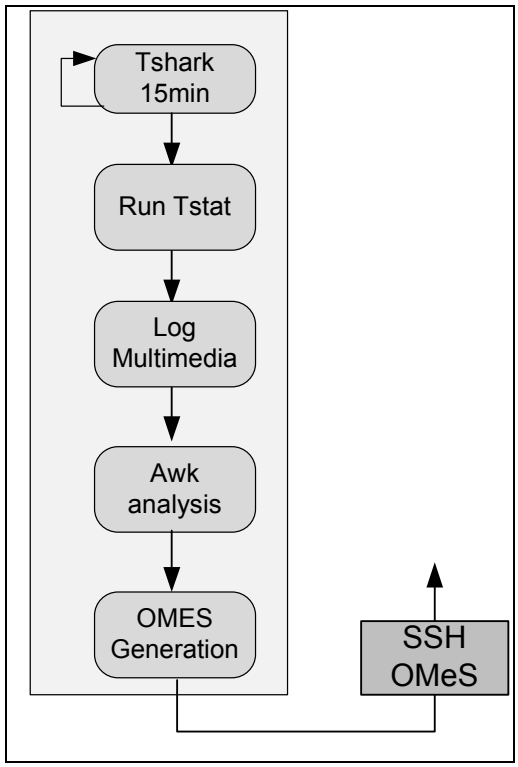

Figure 45 - Script model

The script model was only used in the second scenario. This script has as principal objective to provide all the framework process autonomous. Therefore, when we opt to gather data and send it to the database, we only need to run this script and all management process runs a successive times until reach the limit stipulated in the script (this value can be also set to infinite).

Figure 45 represents the structure of the script model. To better understand this model, we will describe the script functionalities step by step:

First step is the utilization of Tshark sniffer to capture the traffic during 15 minutes. Immediately after this capture stops, another capture starts, with the objective to analyze the maximum number of packets.

The packets captured by Tshark are piped to Tstat. These captured packets are then analyzed by Tstat and the output is saved in a Log Multimedia, Tstat returns some important metrics such as jitter, delay and packet loss. This is the second step.

In the third step, the output of the Tstat is analyzed selecting the interesting information. Some of the fields returned by Tstat are directly used in the OMeS generation.

In order to gather the largest number of measurements possible, in the fourth step the Tstat output was once more analyzed evoking an AWK file. This step has as objective to produce more performance measurements about the traffic such as bitrates, in addition to the information directly provided by Tstat.

The fifth step is the generation of OMeS with the structure referred above in the section 4.3.2. It is important take into account the header fields that must be accurately treated, then each performance measurement collected is independently inserted in the OMeS

The last step is characterized by sending the OMeS files via SSH (Secure shell) to the Open EMS Suite database.

4.4 Management Process Description

This section presents two different scenarios in which it is possible to use the developed framework, collecting the service performance indicators and send them to a database, keeping the database updated. In the subsection 4.4.1 Scenario 1, the performance indicators used in the process are OpNet results; on the other hand, in the subsection 4.4.2 Scenario 2, the data is extracted in real-time from the NSN network.

4.4.1 Scenario 1

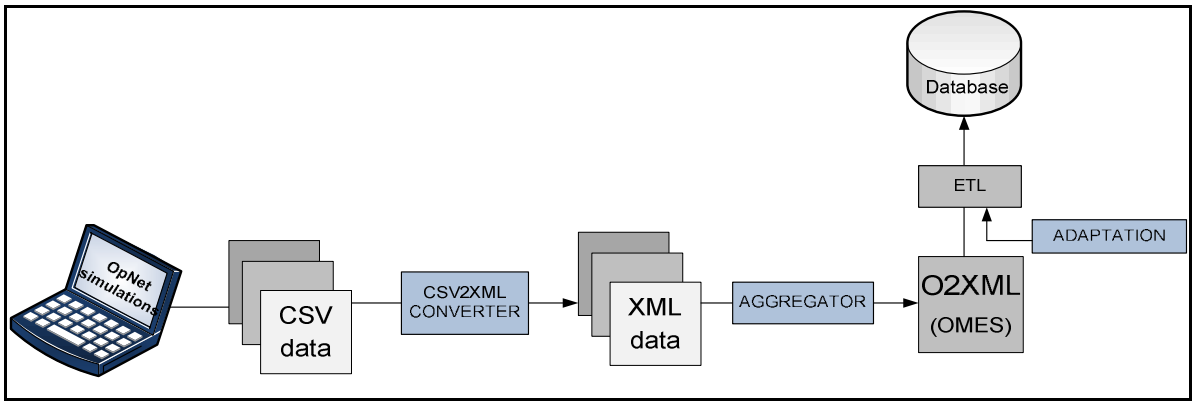

Figure 46 – Process description, data gathered via OpNet

As has been referred above, before starting the process of data collection we must prepare the database and the Open EMS Suit. It is necessary the creation of an adaptation: using SDK we develop the .pmb file as we explained above in the section 4.3.3. The .pmb is the responsible to create a model in the database for the reception of the performance measurements contained in O2XML files (OMeS). After the adaptation creation and deployment we prepare the Open Suit EMS server to receive the CSV files and convert them into OMeS through the Noke2eKOALA.

After the preparation of the database and Open EMS Suit, we start to collect the performance measurements using OpNet simulator. At the same time this simulation is running, the performance measurements are being periodically exported via CSV files, aforementioned each CSV file contains only one measurement type.

After this step, the CSV files are converted into XML files; each CSV file is automatically converted in an OMeS file allowing to be supported by Open EMS Suite.

Furthermore, to be possible to load the data in the database, the XML files must be aggregated in only one O2XML file. O2XML is a result of the aggregation of the OMeS; it is also an OMeS but containing all performance measurements. Since the adaptation has been previously created and deployed, we are ready now to the next step, the Extraction, Transformation, and Load.

ETL (Extraction, Transformation, and Load) defines the process of obtaining the data and converting it into useful, compatible and accurate data. Extraction is the operation of obtain the data from the

source systems, in our case it represents the acquiring of OMES file. Transformation is more than only converting data formats: in this step the data is analyzed, and the one that is not in conformance is rejected. Load corresponds to the final phase where the gathered and transformed data is included into the database.

4.4.2 Scenario 2

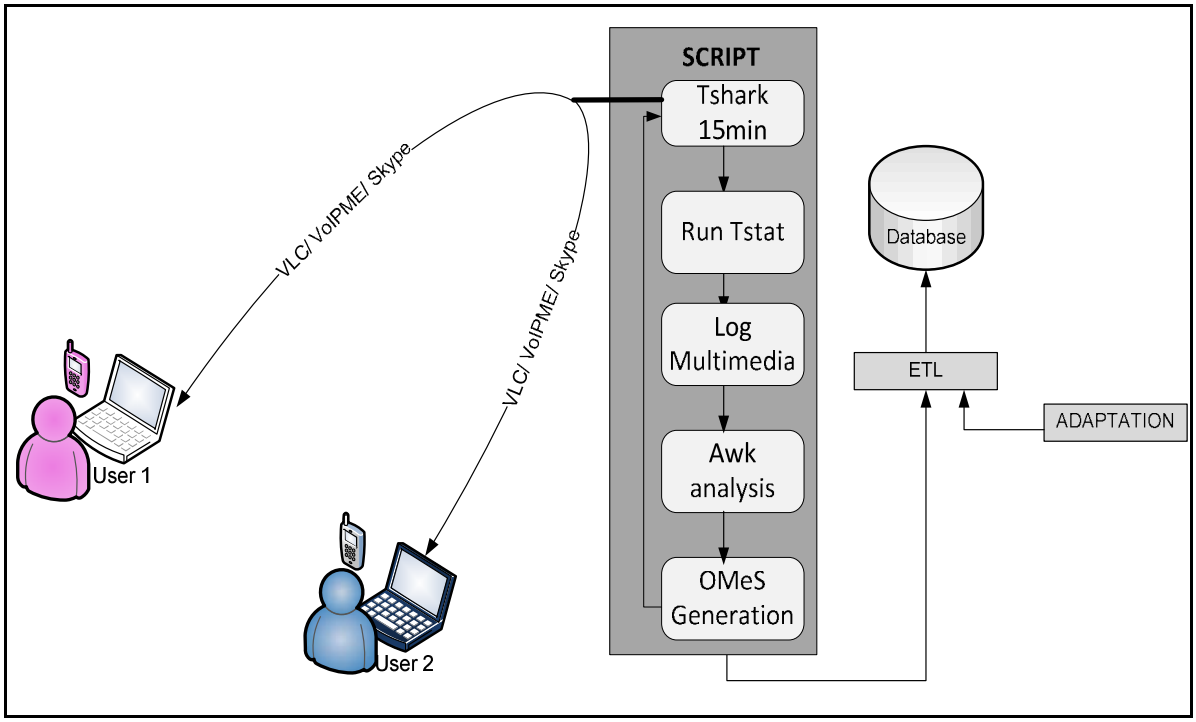

Figure 47 - Script description

The second scenario is very different from the previous one, since in this scenario the data is not collected using OpNet; the data is gathered in real-time monitoring a NSN network. Maintaining our focus in real-time multimedia applications, IPTV, Videoconferencing and VoIP services were the target.

Considering that the database is ready to receive the performance measurements, the first step in this module is characterized by the traffic generation.

With objective to produce the video-stream traffic, we used Video LAN Client (VLC) media player [30]. This tool supports transmission modes, unicast and multicast. We have configured VLC to stream video service over Real Time Protocol encapsulated MPEG-TS packets in a peer-to-peer architecture.

For VoIP traffic generation, we have used Nokia VoIP ME [31] with the default configuration. In this sense, both types of traffic were analyzed, voice and videoconferencing. Since Skype represents one of the most popular tools for internet telephony and videoconferencing, this tool was also particularly analyzed; however, due to the NSN restrictions, the results of videoconferencing and Skype analysis cannot be stored in the database; consequently, these results were omitted in the subsection 4.5.

After the traffic generation, it was necessary to capture and analyze the traffic. With this propose, Tshark and Tstat were the selected tools. Tshark was the responsible to capture the traffic and Tstat to analyze it, providing the several performance measurements. Some of the performance measurements available by Tstat were directly used for the creation of OMES files; however, in order to gather other interesting metrics, such as bit rates the output of Tstat has been once more analyzed using an AWK file, and the values resulting from this analysis are also added to the OMes file.

After this point (after the data is gathered), the process is similar to the Scenario 1, where the next step is the storage of the performance measurements collected through the ETL process.

In order to provide this process interactive and autonomous, a script was created. The main structure of the script is depicted in the Figure 45 and has been deeper discussed in the section 4.3.5; this script starts with the collection of the data using Tshark and finishes with the sending of data to database via SSH.

After this step, the performance measurements are loaded in the database and can be consulted and managed by who has interest, and utilized to better manage the network.

4.5 Results

This section presents the results of the operation of the developed framework. The subsection 4.5.1 presents the database output, resulting from the analysis of IPTV and VoIP services; subsection 4.5.2 presents some charts depicting the IPTV and VoIP performance.

4.5.1 Database output

Table 18 and Table 19 represent the database output; the results have been collect using the framework with the same architecture as in 4.4.2 (Scenario 2), so the results were collected in real-time using the NSN network. IPTV and VoIP service were analyzed. The metrics collected include end-to-end delay, jitter and information about the amount of traffic transferred.

IPTV:

Data – Time	Duration (min)	E2E Delay (ms)	Jitter average (ms)	Jitter Max (ms)	Jitter Min (ms)	Packets Transferred (Units)	Packets Lost (Units)	Bytes Transferred (Units)	Speed rate (bps)
06-16-2009 10:03:25	15,00	4,81	1,25	38,52	0,01	170.400	10	224.236.530	2.190.000
06-16-2009 10:18:28	15,00	6,77	1,02	55,26	0,45	121.275	70	159.588.030	1.554.650
06-16-2009 10:33:32	15,00	6,59	0,81	41,86	0,42	124.732	8	164.138.100	1.598.440
06-16-2009 10:48:33	15,00	6,82	0,79	39,68	0,36	120.420	5	158.462.850	1.542.960
06-16-2009 11:03:38	15,00	6,62	1,05	71,41	0,48	124.020	1	163.200.450	1.589.290
06-16-2009 11:18:41	15,00	6,84	5,13	38,55	0,38	120.150	78	158.107.530	1.540.040
06-16-2009 11:33:48	15,00	7,77	0,85	44,66	0,39	106.020	22	139.512.450	1.354.890
06-16-2009 11:48:49	15,00	7,46	1,34	58,70	0,38	110.055	7	144.822.510	1.411.630
06-16-2009 12:03:53	15,00	6,11	12,25	45,00	0,44	134.227	1	176.633.520	1.723.030

Table 18 - Video performance measurements stored in database

VoIP:

Time – Data	Duration	E2E Delay (ms)	Jitter avg (ms)	Jitter Max (ms)	Jitter Min (ms)	Packets Transferred (Units)	Packets Lost (Units)	Bytes Transferred	Speed Rate (bps)
06-16-2009 11:48:49	15,00	32,38	0,69	553,25	0,22	25.268	78	1.263.000	12.304
06-16-2009 12:03:53	15,00	30,00	1,25	38,52	0,01	27.323	9	1.365.750	13.333
06-16-2009 12:18:58	15,00	30,01	1,02	55,26	0,45	27.383	11	1.368.750	13.330
06-16-2009 12:33:36	15,00	30,00	0,81	41,86	0,42	27.278	94	1.363.500	13.278
06-16-2009 12:48:28	15,00	30,00	0,79	39,68	0,36	27.390	8	1.369.125	13.333
06-16-2009 13:03:20	15,00	30,00	1,05	71,41	0,48	27.323	18	1.365.750	13.303
06-16-2009 13:18:12	15,00	30,00	5,13	38,55	0,38	27.368	11	1.368.000	13.329
06-16-2009 13:33:05	15,00	30,00	0,85	44,66	0,39	27.465	5	1.372.875	13.335
06-16-2009 13:48:26	15,00	30,00	1,34	58,70	0,38	27.360	0	1.367.625	13.334
06-16-2009 14:03:18	15,00	30,00	12,25	45,00	0,44	27.323	12	1.365.750	13.327
06-16-2009 14:18:10	15,00	30,00	1,49	45,32	0,42	27.330	16	1.366.125	13.312

Table 19 - Voice performance measurements stored in database

4.5.2 VoIP and Video Performance

The following charts show the most relevant performance measurements available in the tables above, end-to-end delay, jitter, packets loss and packets transferred.

IPTV:

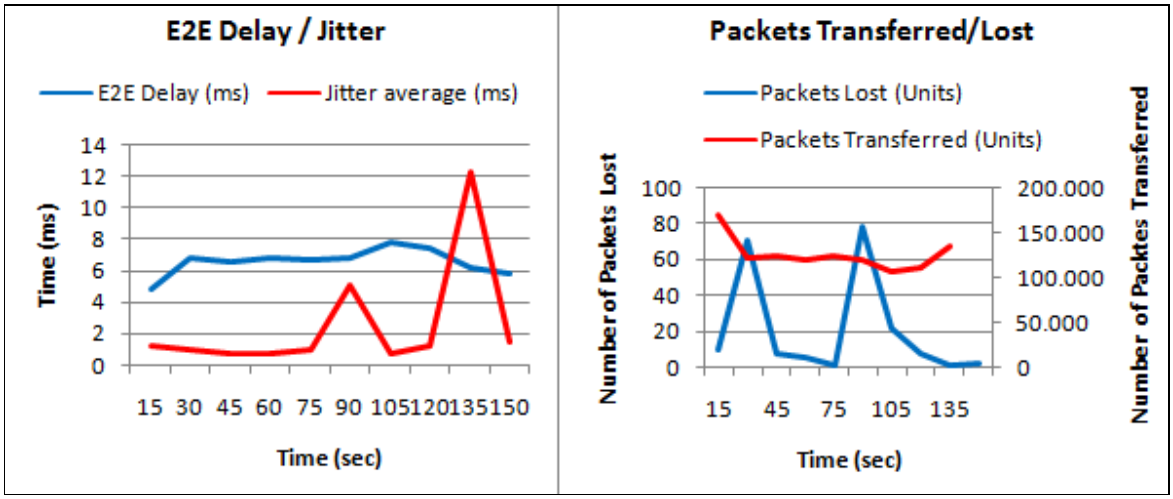

Figure 48 - IPTV performance measurements stores in database: a) Packets lost b) E2E delay and jitter

VoIP:

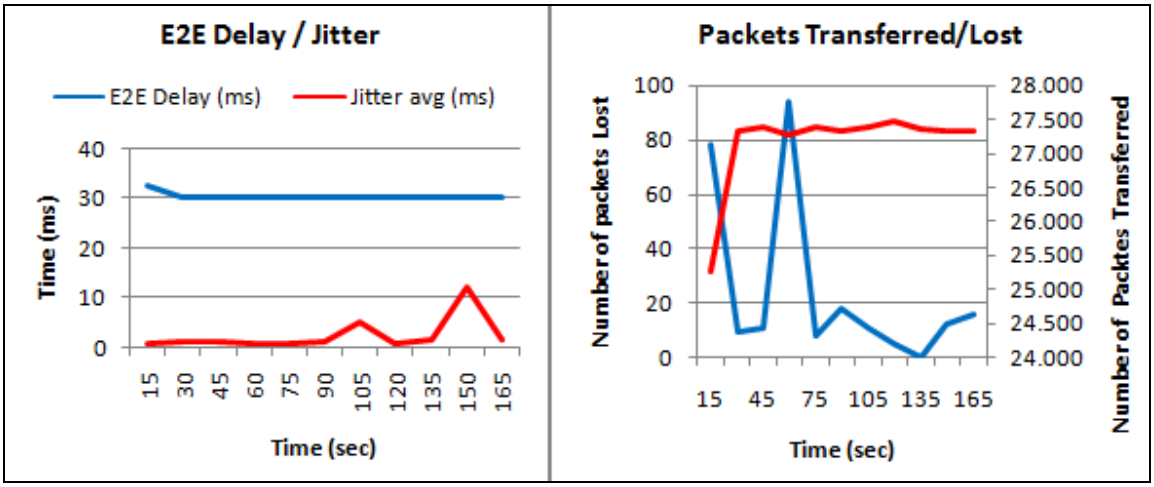

Figure 49 - VoIP performance measurements stores in database: a) E2E delay and jitter b) Packets transferred vs. lost

Analyzing the results depicted in Figure 48 and Figure 49, we can conclude that the performance measurement values agree with the expected values, consequently they can be considered valid values.

Analyzing Figure 48b) we can verify that IPTV traffic is delivered at variable rate with values approximately 120.000 during 15 minutes, that results in approximately 130 packets per second. These results represent acceptable values since high quality video is being streamed, and consequently a large amount of information must be transferred. The values of jitter and end-to-end delay were confirmed using the *ping* command that returned values similar to the exposed in the table. The speed rate and the amount of information transferred also match with the expected values, representing values presently used in the video transmission.

Analyzing Figure 49 b), VoIP traffic as opposed to the IPTV service, is transmitted at fixed rate, approximately 25.000 packets during 15 minutes that results in approximately 30 packets per second in each way. This value is in accordance with the packetization rates actually utilized, for example, by G728 speech CODEC with 30 ms of voice per packet. End-to-end delay and jitter represent credible values, taking into account that the traffic was originated and received inside the Nokia Siemens network; end-to-end delay and jitter has also been confirmed using ping command. The bit rate and the amount of traffic transferred are also in accordance with our expectations, since to the original VoIP traffic additional network overhead is added by the lower layers.

The validation of the performance measurements allows to realize that our framework is working in accordance to the expected.

Analyzing the field “Data – Time” in the Table 18 and Table 19, we can see that some performance measurements were collected at the same time. This situation occurs because the developed framework allows the analysis of the various types of traffic (VoIP, IPTV, Videoconferencing and Skype) at the same time; in the database it is created a structure for each type of traffic, similar to the tables presented in section 4.5.1, and the performance measurements are allocated in the respective structure according with their measurement type.

4.6 Existent Problems

End-to-end monitoring is far from to be a trivial procedure for real-time multimedia applications. Some of the existent solutions become completely unusable when confronted with some problems such as clock synchronization. Although we used the Tshark to perform RTP traffic analysis, non-synchronized clocks completely invalidate the performance measurements collected.

Another problem encountered was the fact that this framework has been tested in Nokia Siemens Network in order to become possible the utilization of Open EMS Suit software. This network presents some characteristics that limited our study. For example, it is not possible to use Videoconferencing Service: although our framework is implemented to support this service, it was not possible to test it.

4.7 Conclusions

The main objective of this framework for both scenarios is the constantly actualization of a database with VoIP, Videoconferencing and IPTV metrics, executing all the process since the collection of performance measurements, analyzing the values gathered and loading the values in the database. All processes occur in real time, keeping the database updated.

After the development of the framework, two scenarios have been implemented. Although they have the same objective, the process is relatively different.

In the first scenario the data is not collected in a real network: the performance measurements are a result of OpNet simulation. In this scenario we have kept our attention in VoIP, Videoconferencing and IPTV traffic. However, since OpNet is a very complete simulator, we can easily collect metrics relative to another user oriented services.

In the second scenario the performance measurements are being collected through the analysis of real traffic in a real network. Tshark and Tstat are the tools used to gather and analyze the traffic, respectively. both programs (Tshark and Tstat) working together represent our passive monitor, that each 15 minutes calculate the performance indicators, later loaded in the database via SSH.

This framework can be very interesting for third-party service providers, since it enables the full awareness of their services performance. Through the analysis of the performance indicator in the database, service providers can manage their services. In case of failure or SLA violation, the service providers can for example reconfigure routes in order to recover from this situation, or even analyzing the database through the time can identify future trends and recover the situation even before the failure or violation occurs.

5 Conclusions and Future Work

5.1 Conclusions

In this thesis we evaluated different services in different technologies. We also performed a framework for data collection and analyzes in real time.

The first step was the performance of the VoIP service over different technologies, Ethernet, IEEE802.11b/g and ADSL2. For each technology, different load settings have been simulated in order to recognize the behavior of VoIP service under different network conditions. Ethernet was the most robust technology. However, this technology presents a trade off, since it must be overprovisioned in order to ensure that links never reach limits excessively high of utilization. With utilization over 90%, Ethernet links start to discard voice packets.

VoIP service has also been studied operating simultaneously with other services (HTTP, FTP and Email). VoIP service has been tested with each service independently, evaluating the performance of VoIP in the presence of another single service. Consequently, three different simulations have been performed, evaluation VoIP and HTTP, VoIP and FTP and finally testing VoIP in simultaneous use with Email. HTTP was the most intrusive services, since the amount of traffic produced by a single utilization is superior than the traffic created by the other services.

In this thesis IPTV service was targeted to the same analysis as VoIP service. IPTV has also been tested for different access networks, varying the load conditions of these networks. The technologies remain the same; however, in some situations the standards has been changed taken into account the amount of traffic produce by IPTV service. In this sense, Ethernet, IEEE802.11g and ADSL2+ were the technologies selected. Again, the Ethernet has revealed the most robust technology in the access network. Ethernet does not present the same drawback as in VoIP service since links only start to discard packets when the utilization reaches 100% or it is really near to that. ADSL technology also represents a high quality solution for video service; However, the amount of traffic supported is lower - the fact that this technology uses the telephone cooper wires already installed combined with higher download capacity, can increase the viability of this technology.

Testing the impact of HTTP, FTP and Email in the IPTV service, HTTP services was again the most destructive service. Again, the HTTP service produces larger amount of traffic, resulting in the most intrusive service.

This thesis also presented a developed framework that allows passive monitoring of the VoIP, IPTV and Videoconferencing traffic in real time, collecting important performance indicators such as, delay, jitter, packet loss and packet rate. These performance indicators are continuously sent to a database in order to keep it updated, allowing to consult this database and make use of the available data, for example, for network management purposes.

A framework with these characteristics presents high viability. The current huge demand of the IPTV, VoIP and Videoconferencing services combined with the increasing demands of the costumers, require a platform that allows the third-party service providers to support solutions that allow full control of its traffic in order to guarantee the quality of service that their customers expect.

5.2 Future Work

As future work, we include the following:

- Use a simulator to test the IPTV, VoIP and Videoconferencing services over the emerging technologies such LTE, WiMAX and GPON.

- To make a more exhaustive study of IPTV service considering the HD stream, testing the impact of a stream HD in the core and access network.

- Test the performance of the developed framework, in different networks with improvement of the complexity.

- As has been abovementioned, one of the problems encountered during elaboration of this thesis was that existent monitoring tools for real time applications are not very efficient, so the improvement of a monitoring tool already existent can be very useful, for example, to improve Tstat to perform SIP analysis.

- Development of monitoring tools close to the costumer as possible, providing collection of QoE metrics for IPTV and VoIP services. Metrics such as MOS and R-factors can be the target.

- Development of an algorithm that, through the analysis of the performance measurements saved in the database, allows the identification of trends of failure. In the situation of identification of failure trends, the algorithm must advise the service provider in order to allow the recovery of the situation.

- Development of a mechanism that, comparing the E2E performance values saved in the database, constructs a network map with the metrics available in the network.

References

[1] Dolejs O.; Hanzalek Z., *Simulation of Ethernet for Real-Time Applications*, in *2003 IEEE International Conference on Industrial Technology,*. 2003. p. 1018 - 1021.

[2] Veeneman D.; Olshansky R., *ADSL for Video and Data Services*, in *IEEE International Conference on Communications*. 1995: Seattle, WA, USA. p. 837 - 841.

[3] Bianchi, G., *Performance analysis of the IEEE 802.11 distributed coordination function*, in *IEEE Journal on Selected Areas in Communications,*. 2000. p. 535-547

[4] ITU-T, *ITU-T Recommendation H.323*, in *Packet-based multimedia communications systems*. 2006.

[5] ITU-T. *ITU-T Recommendation G.114*. One-way transmission time 2003 [cited January 2009,]; Available from: http://www1.cs.columbia.edu/~andreaf/new/documents/other/T-REC-G.114-200305.pdf.

[6] Internet Engineering Task Force. *File Transfer Protocol (FTP)*. 1985 [cited January 2009]; Available from: http://www.ietf.org/rfc/rfc959.txt.

[7] Internet Engineering Task Force, N.W.G. *RFC 1945, Hypertext Transfer Protocol -- HTTP/1.0*. 1996 [cited May 2009]; Available from: http://tools.ietf.org/html/rfc1945.

[8] Internet Engineering Task Force, N.W.G. *RFC 2616, Hypertext Transfer Protocol -- HTTP/1.1*. 1999 [cited September 2009]; Available from: http://www.ietf.org/rfc/rfc2616.txt.

[9] Savage, S. *STING: a TCP-Based Network*. University of Washington, Seattle [cited May 2009]; Available from: http://cseweb.ucsd.edu/~savage/papers/Usits99.pdf.

[10] Yolanda Tsang, M.Y., Paul Barford, Robert Nowak. . *Network Radar: Tomography from Round Trip TimeMeasurements*. [cited May 2009]; Available from: http://www.imconf.net/imc-2004/papers/p175-tsang.pdf.

[11] Joel Corral, G.e.T., Laurent Toutain. *End-to-end active measurement architecture in IP*. [cited May 2009]; Available from: http://moat.nlanr.net/PAM2003/PAM2003papers/3776.pdf.

[12] V. J. Ribeiro, M.C., R. H. Riedi, S. Sarvotham, . *Multifractal cross traffic estimation*. [cited 2009 May]; Available from: http://www-dsp.rice.edu/publications/pub/itc00_cross_traffic.ps.

[13] Jacob Strauss, D.K., Frans Kaashoek, *A Measurement Study of Available Bandwidth Estimation*: MIT Computer Science and Artificial Intelligence Laboratory.

[14] Vinay J. Ribeiro, R.H.R., R. G. Baraniuk, J. Navratil, L. Cottrell. *pathChirp: Efficien Available Bandwidth Estimation for Network Paths*. [cited 2009 May]; Available from: http://www.nlanr.net/PAM2003/PAM2003papers/3824.pdf.

[15] Torino, T.N.G.-P.d. *Tstat TCP STatistic and Analysis Tool*. 2002 [cited 2009 January]; Available from: http://www.tlc-networks.polito.it/mellia/papers/Tstat_network.pdf.

[16] Masaki Aida, N.M.a.K.I. *Approaches, A Scalable and Lightweight QoS Monitoring Technique Combining Passive and Active*. 2003 [cited January 2009]; Available from: http://www.comsoc.org/confs/ieee-infocom/2003/papers/04_01.PDF.

[17] ITU-T. *ITU-T Recommendation M.3010*. Telecommunications management network 1996 [cited October 2008]; Available from: http://eu.sabotage.org/www/ITU/M/M3010e.pdf.

[18] Internet Engineering Task Force. *RFC 1189 - Common Management Information Services and Protocols for the Internet (CMOT and CMIP)*. 1990 [cited; Available from: http://www.faqs.org/rfcs/rfc1189.html.

[19] Internet Engineering Task Force. *RFC 1157, A Simple Network Management Protocol (SNMP)*. May 1990 [cited; Available from: http://www.ietf.org/rfc/rfc1157.txt.

[20] Internet Engineering Task Force, N.W.G. *RFC1889, RTP: A Transport Protocol for Real-Time Applications*. 1996 [cited November 2008]; Available from: http://www.ietf.org/rfc/rfc1889.

[21] ITU-T. *Specification of TMN applications at the Q3 interface: Call detail recording*. 1998 [cited October 2009]; Available from: http://eu.sabotage.org/www/ITU/M/M3010e.pdf.

[22] IBM. *Cognos, Technote Search Readme* 2009 [cited January 2009]; Available from: http://www-01.ibm.com/support/docview.wss?rs=3442&context=SS9RTN&context=SSWGNW&dc =D600&uid=swg21373237&loc=en_US&cs=UTF-8&lang=en.

[23] Corporation, I. *IBM Tivoli Monitoring*. 2006 [cited May 2009]; Available from: ftp://ftp.software.ibm.com/software/tivoli/products/monitor/TivoliMonitoring61_GC28-8379-01.pdf.

[24] Marc A. Cohen, C.C., Alain J. Cohen, CTO & President. *OPNET Technologies, Inc*. 1986 [cited September 2009]; Available from: www.opnet.com.

[25] S. Grag; M.Kappes; M.Many, *Can I add a VoIP call ?*, in *IEEE International Conference on Communications,*. 2003. p. 779 - 783.

[26] Multimedia, R.G. *IP TV Home Networking Strategies.* 2006 [cited October 2008]; Available from: www.mrgco.com/TOC_IPTV_HN06.html.

[27] Nokia, S.N., *Open EMS Suite, Rel. OES 2.0, Open EMS Suite Developer's* 2008(2-0).

[28] Combs, G. *Tshark - Dump and analyze network traffic*. 1998 [cited January 2009]; Available from: http://www.wireshark.org/docs/man-pages/tshark.html.

[29] Nokia, S. *The Open EMS Suite Software Development Kit*. [cited January 2009]; Available from: http://www.nokiasiemensnetworks.com/global/Portfolio/Solutions/OSS+Middleware/Insights/The_Open_EMS_Suite_Software_Development_Kit.htm?languagecode=e.

[30] LAN, V. *VLC media player*. 2009 [cited May 2009]; Available from: http://www.videolan.org/.

[31] Nokia Business Infrastructure Environment Creation and Support, *VoIP ME*.

[32] Tanenbaun, A.S., *Computer Networks*. Third Edition ed. 1996: Pretice hall.

[33] Clark, M.P., *Network and Telecommunications, Desing and operation* Second Edition ed. 1998: WIlEY.

[34] Davie, L.L.-P.a.B.S., *Computer Networks A system approach* ed. C. David, MIT. 2003: Morgan Kaufmenn Publisher.