Research Article

Performance Evaluation of Triple Play Services Delivery with E2E QoS Provisioning

Nikolaos Zotos, Evangelos Pallis, and Anastasios Kourtis

NCSR Demokritos, Institute of Informatics & Telecommunications, Partiarxou Grigoriou & Neapolews,
Agia Paraskevi, Attiki, 15310 Athens, Italy

Correspondence should be addressed to Nikolaos Zotos, nzotos@iit.demokritos.gr

The creation and wide use of new high quality demanding services (VoIP, High Quality Video Streaming) and the delivery of them over already saturated core and access network infrastructures have created the necessity for E2E QoS provisioning. Network Providers use at their infrastructures several kinds of mechanisms and techniques for providing QoS. Most known and widely used technologies are MPLS and DiffServ. The IEEE 802.16-2004 standard (WiMAX) refers to a promising wireless broadband technology with enhanced QoS support algorithms. This document presents an experimental network infrastructure providing E2E QoS, using a combination of MPLS and DiffServ technologies in the core network and WiMAX technology as the wireless access medium for high priority services (VoIP, High Quality Video Streaming) transmission. The main scope is to map the traffic prioritization and classification attributes of the core network to the access network in a way which does not affect the E2E QoS provisioning. The performance evaluation will be done by introducing different kinds of traffic scenarios in a saturated and overloaded network environment. The evaluation will prove that this combination made feasible the E2E QoS provisioning while keeping the initial constrains as well as the services delivered over a wireless network.

1. Introduction

The increased use of the Internet and the creation of new high quality (bandwidth, loss, and delay sensitive) services (Internet telephony, High-quality video, and time critical data) have created an extremely large capacity problem to the core and access network infrastructures. In order to transfer such kinds of services, the networks should support high bandwidth, low-delay and low-jitter (Delay variation) transmission. In order to achieve a transmission keeping these constrains, the core networks should support service separation and service prioritization, in order to transfer different kinds of traffic with different behaviour aggregates. Such solutions are provided by the well-known Multiprotocol Label Switching mechanism and Differential Services protocol which are used for traffic engineering and QoS provisioning in the core networks. The promising WiMAX technology includes features that support QoS algorithms which could be used for the expansion of QoS constrains used by a wired QoS-enabled network to a wireless access network.

Despite the QoS perspective investigation regarding the MPLS, DiffServ technologies have been analysed in deep, and the performance of these technologies with the WiMAX technology fusion has been not tested yet. This document presents an experimental E2E network architecture and topology combining MPLS mechanism and DiffServ technology as a solution for enhanced QoS provisioning over core network infrastructures. Considering that the problem of inadequate service prioritisation still exists also inside the access network infrastructures, the paper describes how to use the WiMAX technology in order to provide the QoS guarantees keeping the same traffic behaviour until the end user. The main objective of this work is to test how the combination of MPLS traffic engineering mechanism and DiffServ technology with WiMAX technology helps to solve the network debility to transmit new high-priority services (internet telephony, video, time critical data) with an acceptable level of delay (according to the service characteristics), without distortion and with the predefined and guarantee quality of service until the end user. Another

important objective is to show how to configure such network in order to optimise its performance in sensitive (bandwidth, delay) data transmission. Therewithal, tests will be performed of how the access network environment can affect the network performance. The rest of the paper is organized as follows: in Section 2, a survey of MPLS, DiffServ, and WiMAX QoS approaches is provided as a way of solving the network congestion problem, providing service priority and an efficient way for service allocation. Section 3 presents the proposed experimental network architecture design and configuration. Section 4 describes the proposed evaluation scenarios, including different kind of services, passing through the network, with different quality and priority constrains. Mainly, in this section the experimental results of the applied scenarios are presented. Finally, in Section 5 the results are summarised and suggestions for future improvement and discussion are provided.

2. MPLS, DIFFSERV, and WiMAX QoS Perspective

2.1. QoS Definition. There are many QoS definitions and everyone can give a different definition for QoS. In this paper, the definition below is of the QoS perspective that is used to test and evaluate the performance of the experimental network infrastructure, in "high quality" services transmission. ITU-T (Recommendation E.800 [ITU-TE.800]) and ETSI [ETSI-ETR003] basically define Quality of Service (QoS) as "the collective effect of service performance which determines the degree of satisfaction of a user of the service" [1]. Mainly, QoS is the ability to differentiate between traffic types in order for the network to treat certain traffic flows differently from others and keep to acceptable level the service categorization and the overall network performance [1].

2.2. QoS Need Applications Overview. The applications that require a specific level of assurance from the network are the applications that need QoS, namely, applications which are sensitive in packet loss and delay. There is a big amount of applications that need a level of assurance but it is difficult to define a specific level for each one of them. For that reason, there exist several categories which called "QoS classes" in which the applications have been classified. The way that the application classification has been done related to the applications attributes. More specific, the attributes of applications which need quality assurance are

  (i) real-time, jitter sensitive, highly interactive,

  (ii) real-time, jitter sensitive, interactive,

  (iii) transaction data, highly interactive,

  (iv) transaction data, interactive,

  (v) low loss only (short transactions, bulk data, video streaming),

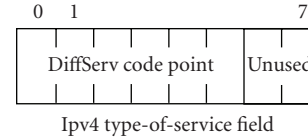 (vi) traditional applications of default IP networks.

FIGURE 1: TOS field [2].

2.3. DiffServ QoS Approach Overview. Differentiated Services are a computer networking architecture that specifies a simple, scalable, and coarse-grained mechanism for classifying, managing network traffic and providing quality of service (QoS) guarantees on modern IP networks.

The DiffServ architecture is based on a simple model. When traffic entering a network is classified and conditioned at the boundaries of the network, and assigned to different Behaviour Aggregates (BAs), with each BA being identified by a single DiffServ Code-Point (DSCP). Within the core of the network, packets are forwarded according to a Per-Hop Behaviour (PHB) associated with the DSCP [2]. The smallest autonomic unit of DiffServ is called a DiffServ domain, where services are assured by identical principles. A domain consists of two types of nodes: Boundary (or Edge) routers and Core routers. Core nodes only forward packets; they do no signalling. Each router packets traverse is called a "hop" Packets, classified at the edge of the network, and forwarded according to a specific PHB throughout the core of the network. Packets may be forwarded across multiple networks on their way from source to destination. Each one of those networks is called a DiffServ Domain. More specific, a DiffServ Domain is a set of routers implementing the same set of PHBs. The DiffServ PHB class selector offers three forwarding priorities:

(1) Expedited Forwarding (EF) characterized by a minimum configurable service rate, independent of the other aggregates within the router, and oriented to low-delay and low-loss services [1],

(2) Assured Forwarding (AF) group, recommended in [RFC 2597] for 4 independent classes (AF1, AF2, AF3, AF4) although a DiffServ domain can provide a different number of AF classes. Within each AF class, traffic differentiated into 3 "drop precedence" categories [1],

(3) Best Effort (BE), which does not provide any performance guarantee and does not define any QoS level.

2.4. MPLS QoS Approach Overview. Multiprotocol Label Switching (MPLS) as known in computer networking and telecommunications is a data-carrying mechanism which emulates some properties of a circuit-switched network over a packet-switched network. This mechanism lies between traditional definitions of Layer 2 (Data Link layer) and Layer 3 (Network layer) of the OSI Model and thus is often referred to as a "Layer 2.5" protocol. It was designed to provide a unified data-carrying service for both circuit-based clients and packet-switching clients. It can be used to carry many different kinds of traffic [3]. MPLS basic idea is to

TTL 8 bits	S 1 bit	EXP 3 bits	Label 20 bits

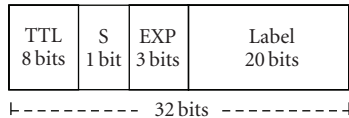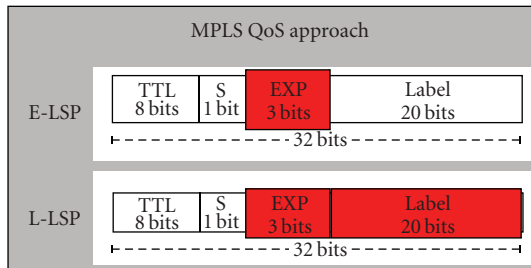├──────── 32 bits ────────┤

FIGURE 2: MPLS Header [4].

FIGURE 3: MPLS QoS-based Label distribution.

append a small fix length label before each packet in order to forward it inside the MPLS network. This label with some other attributes which also appended in front of the packets consists of the 32-bit length MPLS header. Figure 1 depicts the MPLS header and the use of each field. MPLS header entry contains four fields:

(i) a 20-bit label value,

(ii) a 3-bit field for QoS priority,

(iii) a 1-bit bottom of stack flag. If this is set, it signifies the current label is the last in the stack,

(iv) an 8-bit TTL (time to live) field.

MPLS has the capability to combine with DiffServ in order to enhance the QoS support inside the MPLS core network [5]. More specific there are two approaches of how LER [4] router can attach a label to packet in order to keep the predefined priorities: (a) the EXP-Inferred approach and (b) the Label-Inferred approach. Figure 2 shows how these two approaches work.

(i) **E-LSP**

Queue inferred EXP field
Drop priority inferred EXP field
8 Classes maximum (like IP TOS)

(ii) **L-LSP**

Queue inferred exclusively from label
(IP+ATM multi vc)
Drop priority inferred from EXP field
Combination will allow up to 64 classes
(DiffServ)

2.5. WiMAX QoS Approach Overview. WiMAX is defined as Worldwide Interoperability for Microwave Access by the WiMAX Forum, formed in April 2001 to promote conformance and interoperability of the standard IEEE 802.16. The

original WiMAX standard, IEEE 802.16, specifies WiMAX in the 10 to 66 GHz range. 802.16a, updated in 2004 to 802.16-2004, added support for the 2 to 11 GHz range, of which most parts are already unlicensed internationally and only very few still require domestic licenses. Most business interest will be in the 802.16-2004 standards, as opposed to licensed frequencies. 802.16-2004 is often called 802.16d, since that was the working party that developed the standard. It is also frequently referred to as "fixed WiMAX" since it has no support for mobility [6, 7]. 802.16e-2005 is an amendment to 802.16-2004 and is often referred to in shortened form as 802.16e [6–8]. It introduced support for mobility, among other things and is therefore also frequently called "mobile WiMAX". The WiMAX specification improves upon many of the limitations of the Wi-Fi standard by providing increased bandwidth and stronger encryption. It also aims to provide connectivity between network endpoints without direct line of sight in some circumstances.

WiMAX systems support a wide range of network services: IP Access, IP VPN, VOIP, PPPoE, tunneling and of course give the ability to operators to provide differentiated SLAs with committed QoS for each service profile. The 802.16 standard provides powerful tools in order to achieve different QoS constrains [8]. The QoS support on 802.16 networks is defined by providing four different scheduling services for different service classification. The four scheduling services defined in 802.16 are

(1) Unsolicited Grant Service (UGS),

(2) real-time Polling Service (rtPS),

(3) nonreal-time Polling Service (nrtPS),

(4) Best Effort (BE).

2.6. UGS Scheduling. The UGS is designed to support real-time service flow of fixed-size data packets on a fixed interval. In UGS, there is no bandwidth sharing of multiple connections and each connection (service flow) is allocated with a dedicated channel (time slot) [6]. An example for UGS scheduling is the VOIP service.

2.7. rtPS Scheduling. The rtPS scheduling is designed to support real-time data streams consisting of variable-sized data packets that are issued at periodic intervals [8]. This would be the case for MPEG (Moving Pictures Experts Group) video transmission for example, nrtPS Scheduling.

The nrtPS scheduling is designed to support delay-tolerant data streams consisting of variable-size data packets for which a minimum data rate is required. The standard considers that this would be the case for an FTP transmission for example [8].

2.8. BE Service. The BE service is designed to support data streams for which no minimum service guarantees are required and therefore may be handled on a best available basis. The packets fitted in BE service in network congestion state cannot be transmitted for a long period [8].

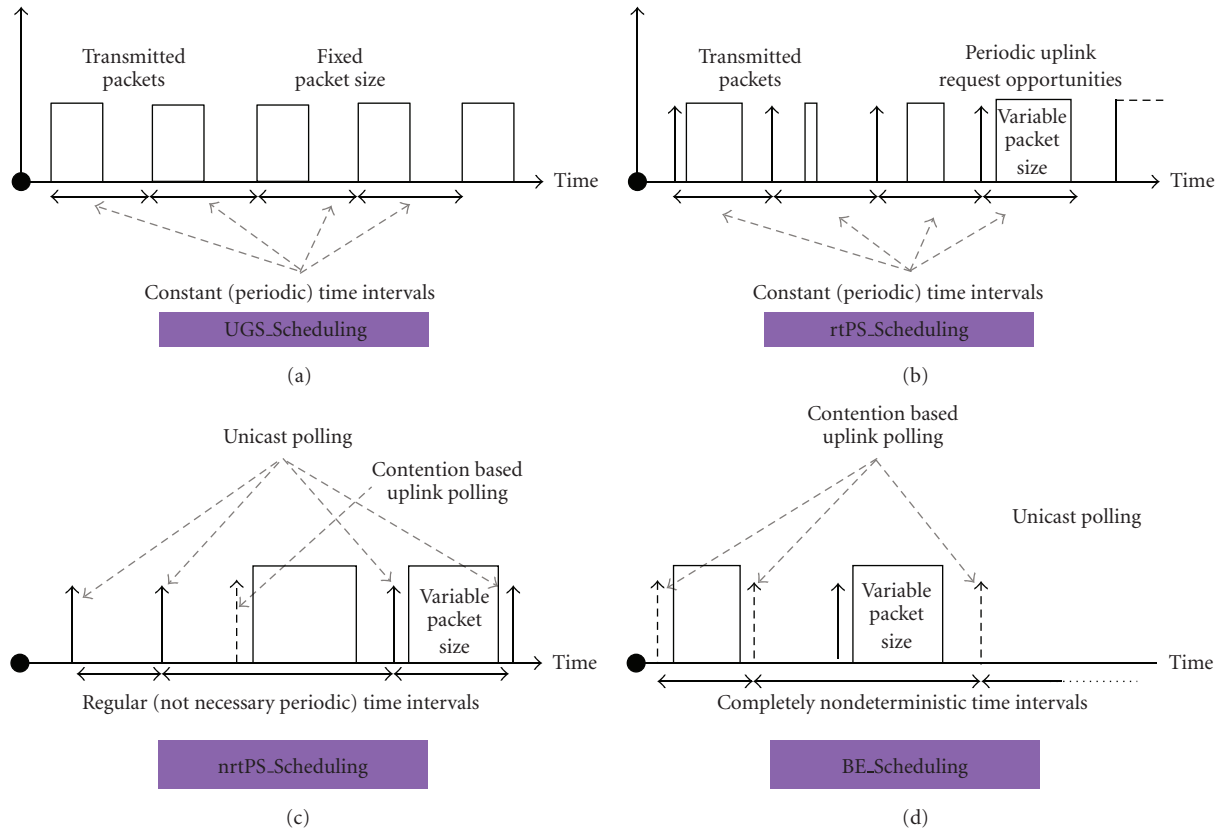The 802.16e also supports a fifth scheduling service called extended real-time Polling Service (ertPS) which is

FIGURE 4: WiMAX scheduling algorithms [6].

a scheduling mechanism combining the efficiency of both UGS and rtPS [8].

3. QoS Architecture and Configuration

As shown in Figure 5, the implemented MPLS-DiffServ-WiMAX network infrastructure consists of: (i) a Service Provider Network, (ii) an MPLS-DiffServ capable domain, and (iii) a WiMAX Access Network where End-Users reside.

Service Provider network contains an A/V content server, a VoIP server, and Internet access (HTTP, FTP, mail, etc.). Also for test purposes, a traffic generator has been installed and configured in service provider network.

At the Core network, the traffic coming from the service providers reaches the ingress LER (Label Edge Router). The ingress LER router is responsible for mangling, marking the incoming traffic, and separating it into different traffic trunks with different QoS requirements. Also, ingress LER is attended to attach a short length label to each incoming packet. The decision on what label should be chosen at the ingress LER is based on the marked DSCP field in the packet header and on a predetermined policy and current-state information. For the needs of the experiment, the labels are predefined for each service and allocated to each traffic trunk with a static way. At the core of the network, there are the Label Switch Routers (LSR 1, LSR 2) which check the labels of the incoming packets and change them in order to

keep the same QoS requirements as the initial traffic. After the packets are forwarded to the egress LER, the labels will be removed and the packets will be forwarded according to the original network-layer routing scheme to the access network.

The WiMAX technology is used as the Access medium for the end user/s. The selection of WiMAX technology has been done in order to support hard QoS guarantees in the access network in contrast to the lack of QoS provision in 802.11 wireless network environments. The WiMAX Base station has the responsibility to map the traffic based on DSCP field to WiMAX QoS classes.

3.1. Network QoS Configuration. As mentioned before, the whole network consists of three parts. The first part deals with the high-quality services (VoIP and Video) creation. For the voice service, a Linux OS- (Operating System) based VoIP (Asterisk PBX) server is installed and configured in Service Provider's premises. For Video service creation, an H-264 encoder has also been installed and configured. The encoder has the ability to encode in H-264 video format two video streams simultaneously. For time critical data and background traffic, a traffic generator (using MGEN software) has been installed, which generates the traffic and allocates it into different QoS classes (based on DSCP field).

The second part is the core network infrastructure which consists of 4 Linux OS- (Debian testing with 2.6.21 kernel) based routers. Linux OS has been chosen because of its

TABLE 1: Traffic classes by flow.

EF (DSCP-0x2e)	VoIP
AF11(DSCP-0x0a)	A/V Content
AF22, BE	Other internet services

TABLE 2: GRED queuing.

$$Q_{max} = \frac{0.01 * BS * L * BW}{8 \text{ bits/bytes} * 1000 \text{ ms/sec}} \quad (1)$$

$$Q_{min} = \frac{1}{2} * Q_{max} \quad (2)$$

$$B = \frac{2 * Q_{min} + Q_{max}}{3 * AvPkt} \quad (3)$$

$$Q_{limI} = 4 * Q_{max} \quad (4)$$

TABLE 3: Traffic class mapping.

CLASSES	DSCP	EXP
EF	0x2e	0x01
AF11	0x0a	0x02
AF12	0x0c	0x03
AF13	0x0e	0x04
AF21	0x12	0x05
AF22	0x14	0x06
AF23	0x16	0x07
BE	0x00	0x00

TABLE 4: Mapping with WiMAX traffic classes.

Service	Core network	Access network
VoIP	EF (DSCP-0x2e)	UGS Scheduling
A/V Content	AF11 (DSCP-0x0a)	rtPS Scheduling
High priority Services	AF22 (DSCP-0x14)	nrtPS Scheduling
Other internet services	BE	BE Scheduling

enhanced network implementation in contrast with other OS and because it is capable to support inside its kernel the MPLS and DiffServ technologies. The MPLS and DiffServ support in Linux achieved by installing the modules for each one technology separately inside Linux Kernel. The layered structure of the MPLS and DiffServ modules inside Linux kernel are shown in Figure 6. Based on this Linux kernel implementation and according to the architecture proposed in Figure 5, different packets are arriving from the SP and the traffic generator to the MPLS-DiffServ network.

The packets throughout the MPLS-DiffServ network are marked and assigned into different traffic classes by attaching to each class a different DSCP classifier value and by using HTB packet scheduler [9], at the Label Edge Router 1 (LER 1). The supported traffic classes are EF, AFxx, and BE. The following table shows the assignation of corresponding DSCP values to the services (VoIP, A/V, and Internet).

A Hierarchical Token Bucket (HTB) packet scheduler used for the DiffServ supported PHB. Specifically, a pFIFO queuing discipline is adopted for the EF class. Three GRED virtual queues with different drop precedence (2% for AF11, 4% for AF22) are implemented for the AFxx [9, 10]. The BE class served through a RED queuing discipline with 40% drop precedence. The maximum bandwidth allocated at the parent HTB class is 4 Mbps. The EF class guarantees 0.9 Mbit with maximum rate 1 Mbit for VoIP service. The AF11 provide 0.9 Mbit for video service. The AF22 provide 0.9 Mbit and the BE 0.9 Mbit. Figure 7 shows how the different flows classified and assigned to different traffic classes.

GRED queues were configured adjusting the following parameters:

(1) Q_{max}: maximum average queue size after which all packets get dropped, BS: percentage of the expected bandwidth share, L: maximum desired latency, BW: total network bandwidth,

(2) Q_{min}: minimum average queue length after which packets get dropped, AvPkt: average packet size,

(3) B: burst value in number of packets, and

(4) Q_{limit}: actual queue length which should never be exceeded.

Also, in LER 1 attached a short fixed length label to each incoming packet. The decision on what label to choose at the LER 1 based on the marked DSCP field in the packet header and on a predetermined policy and current-state information. One way of selecting labels is to aggregate different flows into trunks. A trunk is an aggregate of traffic flows that belongs to the same class, which means that all packets flowing in a trunk have the same MPLS header, including the 3-bit class of service field (currently experimental field or EXP), which it matched with a DSCP value.

Different trunks can be routed along the same LSP, the only thing that distinguishes flows in different trunks is the class of service field. The following table shows how the EXP field matches with the correspondence DSCP values.

At each Label Switch Router (LSR 1, LSR 2), the label on the incoming packet is used as index in a table that contains the outgoing interface and a new label that is to replace the incoming label before it is transmitted to the next hop. Also the LSR routers take care of keeping the same PHB for each trunk. When a packet reaches the LER 2, the label will be removed and the packet will be forwarded to the access network.

At the access network, the WiMAX BS (Base Station) is configured to receive each service and map its predefined policy with core network similar one in order to keep the same quality until it reaches the end user. Table 4 shows the WiMAX scheduling services mapped with the different support traffic classes of the core network.

The way in which this allocation has been done is that the WiMAX base station takes into account the DiffServ traffic classes attributes, and comparing these attributes with the WiMAX scheduling algorithms characteristics (as reported in Section 2), it maps the corresponding traffic (based on DSCP field) to the WiMAX appropriate scheduling algorithm.
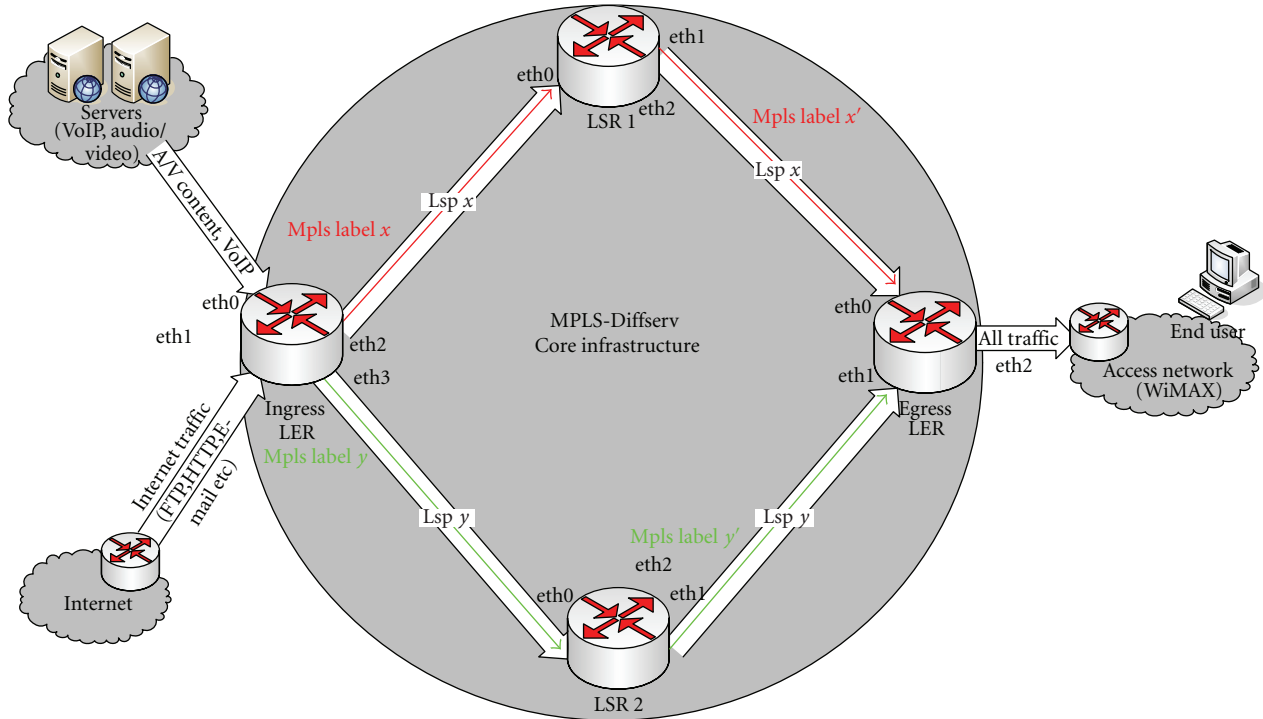
LER: label edge router
LSR: label switch router
LSP: label switch path

FIGURE 5: MPLS-DiffServ-WiMAX experimental infrastructure.

4. Evaluation Scenario

4.1. Building the Experiments Environment. The level of quality that the proposed architecture assures in high priority services transmission is evaluated by the creation of different traffic scenarios. These scenarios contain different kinds of high priority services (internet telephony, video, time critical data, and background traffic) with different priorities and quality constrains, passing through the network. The scenarios also consist of video on demand and audio transmission at the maximum threshold of the network bandwidth in order to test how efficient MPLS, DiffServ, and WiMAX QoS mechanisms could be combined to each other.

Initially, all services transmitted together at the network maximum threshold which is 4 Mbps (1 Mbps for each service). Secondly, the network load increased gradually and finally all services (internet telephony, video, and time critical data) transmitted simultaneously with bulk traffic until network load exceeded the network capacity upper threshold for 25% (5 Mbits load). Afterwards, the tests extended at the access network comprising the service flows forwarding to the end user with service prioritization, mapping the service classification inside the Core network with the same classification inside the Access network. The table below shows a more analytical view of the initial test scenario.

The evaluation of the experimental infrastructure is performed in 4 stages:

(1) high quality services creation,

(2) core network without QoS support,

(3) QoS provisioning over MPLS-DiffServ (2 LSP's),

(4) QoS provisioning over MPLS-DiffServ-WiMAX.

4.2. Service Generation. At the service generation part as mentioned above, VoIP server transmits 5 streams of the VoIP service marked as EF. The transmitted packet size is 214 bytes which is a very small packet size and it is difficult to protect it against packet loss. The source transmission rate becomes 1 Mbps (5 ∗ 200 kbps per stream).

The high quality video streaming generated from a real-time video H-264 server/encoder. The transmitted packet size varies and depends on each evaluation scenario. The class which this service is allocated is AF11. The source transmission rate sets at 1 Mbps.

The time critical data and the background traffic generated from a traffic generator (MGEN [11]) and the rate sets at 1 Mbps per service. The classes which these services are allocated are AF22 and BE, respectively.

4.3. Core Network without QoS Support. The 1st stage of the evaluation consists of the core network without any QoS support. The 4 flows entering the network unmarked and routed inside the core network according to the default routing scheme. The measurement server generates 3 flows of 3 Mbps (1 Mbps each), and 1 flow of 1 Mbps reaches the network from the VoIP server. The traffic from VoIP
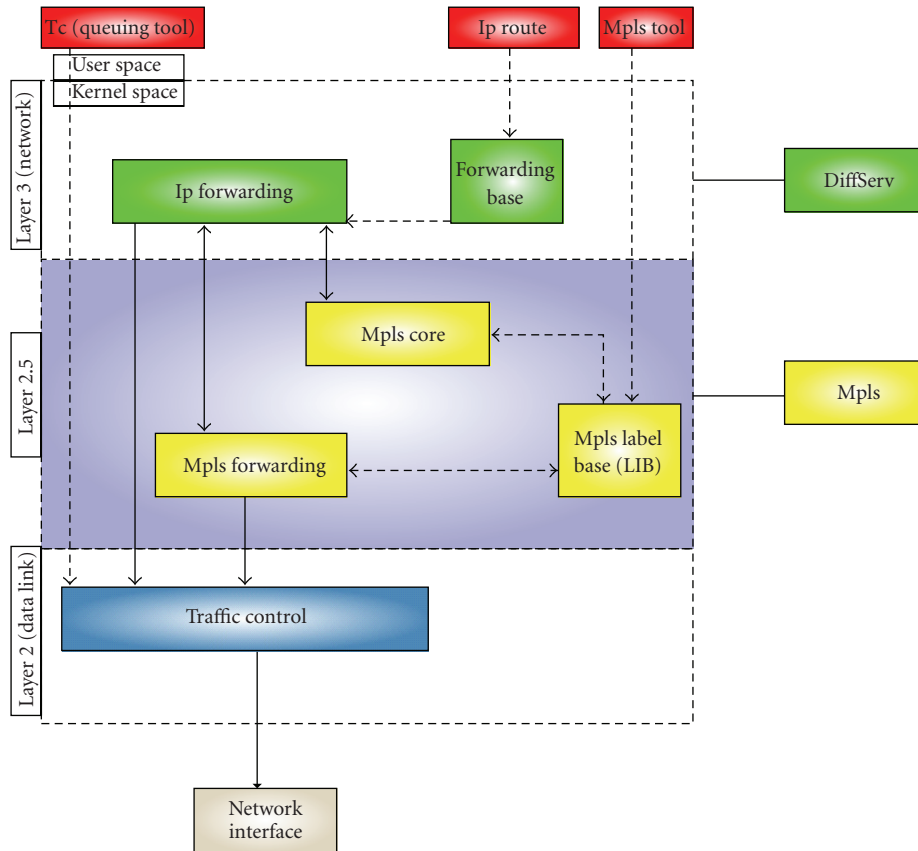
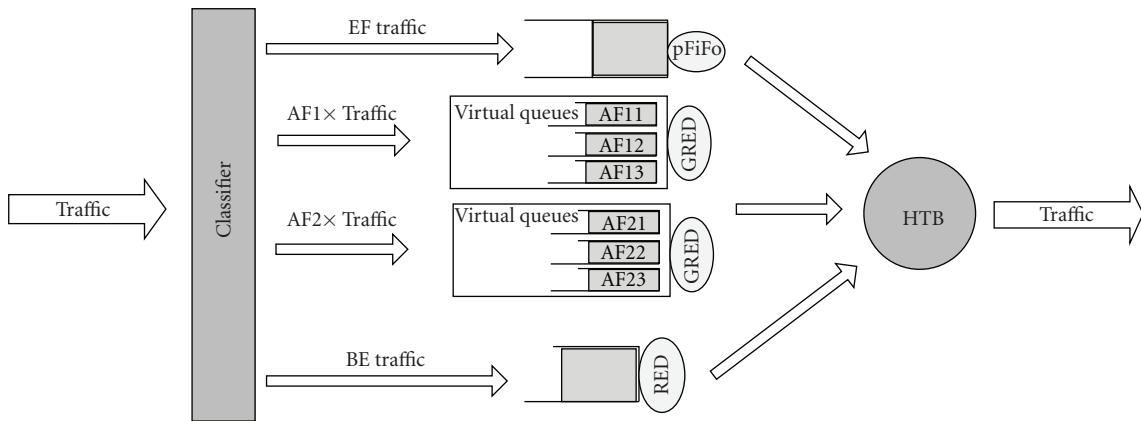Figure 6: MPLS and DiffServ modules inside Linux Kernel.

Figure 7: HTB packet scheduler and DiffServ supported classes [10].

Table 5: Initial test scenario.

Traffic class and packet size	Periodic traffic type							Poisson traffic type
	EF (214 Bytes fixed)	AF11	AF22	BE	EF	AF11	AF22	BE
512	1Mbit Traffic per class							
768	make the total ingress traffic of the network							
1024	reach the upper capacity threshold which is 4 Mbits.							
1312	The BE class increase its traffic from 1 Mbps up to 2 Mbps.							
1472	The network load increases from 4 Mbps up to 5 Mbps but the network capacity still 4 Mbps							

server and from the H-264 encoder reaches the network via passing through the measurement server first. This happens because the measurement server needs to collect all data in order to produce the results for the one-way delay, data loss, and the jitter (delay variation). The network capacity at this phase is limited to 4 Mbps (by applying a filter at ingress LER) in order to realize how this can affect the 4 flows. The measurement server is going to increase gradually the bulk data flow (BE class) up to 2 Mbits. The network setup is shown in Figure 5.

4.4. QoS Provisioning over MPLS-DiffServ. During the second phase, the core network is configured again adapting the MPLS DiffServ QoS mechanism support. The four flows entering the network are marked (EF, AF11, AF22, BE) and allocated into two LSP's according to the DSCP and EXP field mapping. The EF (exp-0x01) and AF11 (exp–0x02) traffic classes are forwarded inside the same LSP (LSP1) in which label 10000 is assigned. In the second LSP (LSP2), the AF22 (exp-0x05) and BE (exp-0x0) traffic classes are forwarded marked with the label 20000. The measurement server generates three flows of 3 Mbps (1 Mbps each), and one1 flow of 1 Mbps is reaching the network from the VoIP server. The traffic from VoIP server and from the real time H-264 encoder reaches the network passing through the measurement server in the first place. This is happening because the measurement server needs to collect all data in order to produce the results for the one-way delay, data loss, and the jitter (delay variation). The network capacity at this phase is limited to 4 Mbits in order to be cleared out; how this can affect the four flows and how it could be compared to the previous setup results. The measurement server is going to increase gradually the bulk data flow (BE) up to 2 Mbits. Figure 8 shows the network setup.

4.5. QoS Provisioning over MPLS-DiffServ-WiMAX. The final step is to expand the same scenario into the WiMAX access network. Egress LER connects with the WiMAX BU (Base Unit) which is configured in order to keep the same quality constrains as the core network. The WiMAX access network capacity is limited up to 4 Mbps and maps each traffic class with the corresponding WiMAX classes. The EF mapped as UGS class, the AF11 as rtBS, the AF22 as nrtBS, and the BE as BE. The four flows are forwarded to the WiMAX SU (Subscriber Unit) and to the end user via the measurement server which collects data in order to provide the measurement results. The figure below shows the setup of the entire experiment and the role of each network entity.

5. Experimental Results

At this Section, the experimental results for each scenario are presented analytically and they will be discussed in order to introduce how the network changes can affect its performance. For each network, setup will be the graphs of average one way delay; jitter and packet loss will be included. The values that all graphs will show are the mean values of all used packet sizes (512, 768, 1024, 1312, and 1472). It is

TABLE 6: IP QoS classes and objective performance-metric upper limits (U-Unspecified) [1].

QoS Class	Characteristics	IPTD	IPDV	IPLR	IPER
0	Real time, jitter sensitive, highly interactive	100 ms	50 ms	1×10^{-3}	1×10^{-4}
1	Real time, jitter sensitive, interactive	400 ms	50 ms	1×10^{-3}	1×10^{-4}
2	Transaction data, highly interactive	100 ms	U	1×10^{-3}	1×10^{-4}
3	Transaction data, interactive	400 ms	U	1×10^{-3}	1×10^{-4}
4	Low loss only (short transactions, bulk data, video streaming)	1 s	U	1×10^{-3}	1×10^{-4}
5	Traditional applications of default IP networks	U	U	U	U

very important to mention that the packet size for EF flow is constant at 214 bytes during the whole experiment in order to take measurements which correspond better to the real applications. The network was tested at a 100% of network capacity traffic load (4 Mbps–1 Mbps per flow), with 112.5% traffic load (4.5 Mbps–3 flows of 1 Mbps and 1.5 Mbps BE) and finally 125% (5 Mbps–3 flows of 1 Mbps and 2 Mbps BE). The next paragraph refers to the QoS metrics which the experimental results depended on.

5.1. QoS Metrics. The QoS metrics mostly used [ITU-T-Y.1540] in an IP-based environment are as follows:

  (i) IPLR-IP Packet Loss Ratio,

 (ii) IPTD-IP Packet Transfer Delay,

(iii) IPDV-IP Packet Delay Variation (Jitter),

 (iv) IPER-IP Packet Error Ratio.

The following table shows the upper bound of the acceptable values for each QoS class for each one of these metrics [1].

5.2. Core Network without QoS Support Experimental Results. At the first scenario, the analysis focused on the core network without QoS support. It is very important to understand how the network corresponds to any network change in order to state the metrics for the next experiment stages. After finishing the first stage of the experiment, the results, regarding the average one way delay and average packet loss ratio, are shown in the following figures.

Figure 11 shows the average one way delay for the four flows including all different traffic loads. The average delay values are very low, less than 1 msec. This seems to be very logical when considered that no queues have been installed but only the filter which limits the network capacity at 4 Mbps and just drops the packets which exceed this capacity. Figure 12 shows the average packet loss ratio. Observing Figure 11, it is clearly shown that when the traffic flows have a
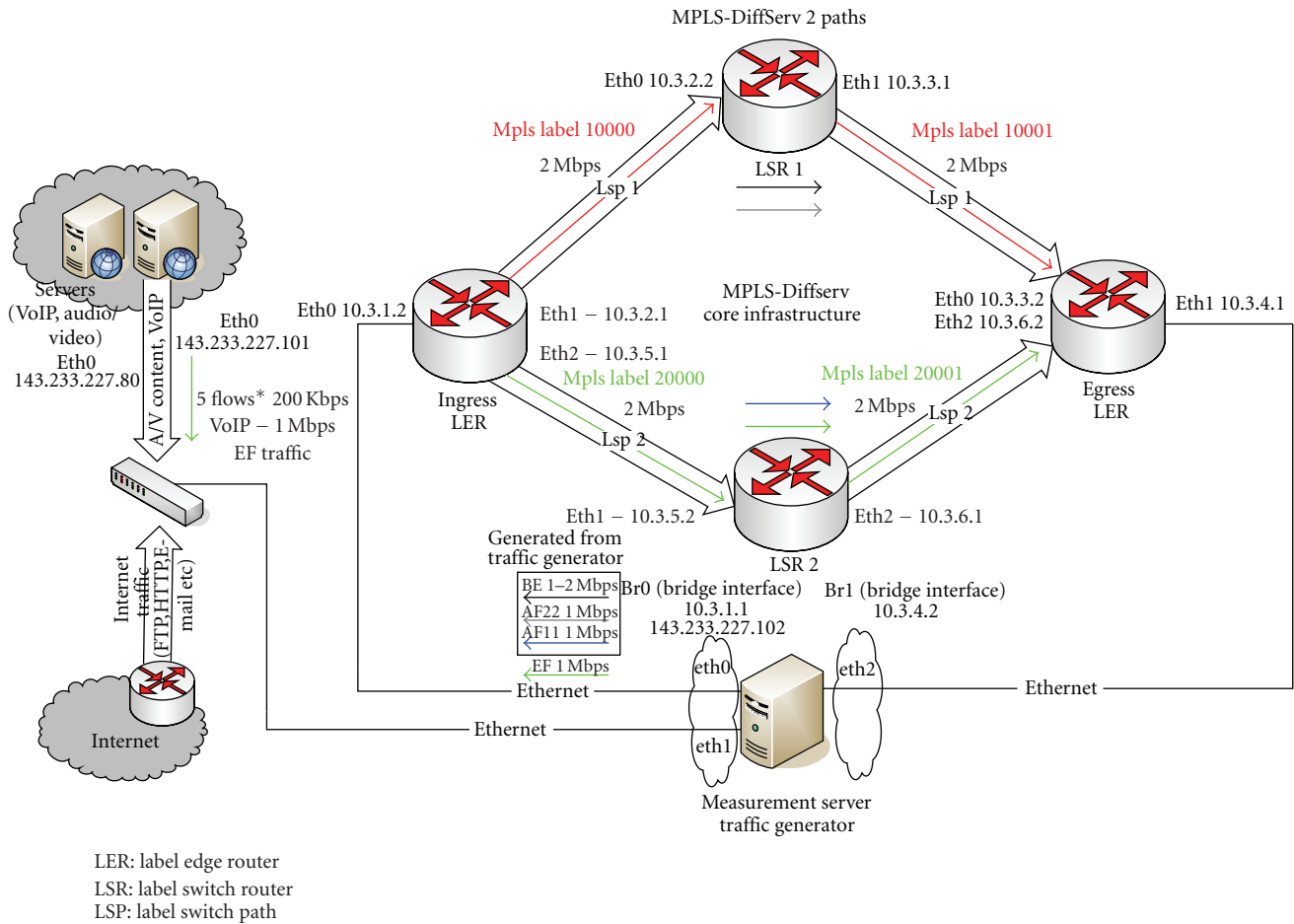
FIGURE 8: Core network with MPLS-DiffServ QoS enabled 2 paths.

PERIODIC transmission type, the packet loss can be detected in BE traffic only (bulk internet data). This is happening because the flows are separately transmitted and separately captured and the filter drops the packets inside the flow which exceeds the network capacity load (even when the flows carry the data unmarked).

It is ideal that data are created and they travel through core networks. In the real world systems, the way that a data transmission can occur is like POISSON transmission. That means that data have not a constant bit rate, but as the transmission continues there is a deviation between a minimum rate and a maximum rate. The most important observation from Figures 4–6 is that in POISSON transmission type even though that the increased traffic comes from BE class there is a high percentage of packet loss in AF11 and AF22 traffic classes (high quality video streaming, high priority internet service). That causes video transmission interruption and content distortion in a way that it is infeasible for the user to see it. The average packet loss percentage for EF class (Internet telephony-VoIP service) is lower than AF11 class, but by an average percentage of 2.636% for traffic load 112.5% (POISSON) and a 3.322% for traffic load 125% (POISSON), it is enough to distort the voice traffic (acceptable value 0.1% and in some special conditions until

1%). So it is imperative to add QoS support in order to protect the transmitted data.

Figure 13 above shows the average delay variation which has no special meaning to discuss because the values in all different circumstances are too low to affect the data transmission.

5.3. Core Network with QoS Support—2 LSP's—Experimental Results. The MPLS traffic engineering capabilities are introduced to the network by separating the traffic classes into two different LSP's with different routes inside the core network. The 1st LSP comprised of the EF and AF11 traffic classes in order to protect the most sensitive data from the BE class rate increase. The AF22 and BE traffic class comprised the 2nd LSP which also has a different route from the 1st LSP. Figure 14 below depicts the average one-way delay.

Regarding Figure 14, the most important observation is that the one-way delay of AF11 class decreased for approximately 10% from previous set up for traffic scenarios. The same decrease observed also for AF22 traffic class. The approximately 100 msec average one way delay decrease is the result of the different LSPs that the traffic classes are assigned. Data inside LSP 1 travels through the network in a different route from LSP 2 and the delay of EF and AF11 traffic classes
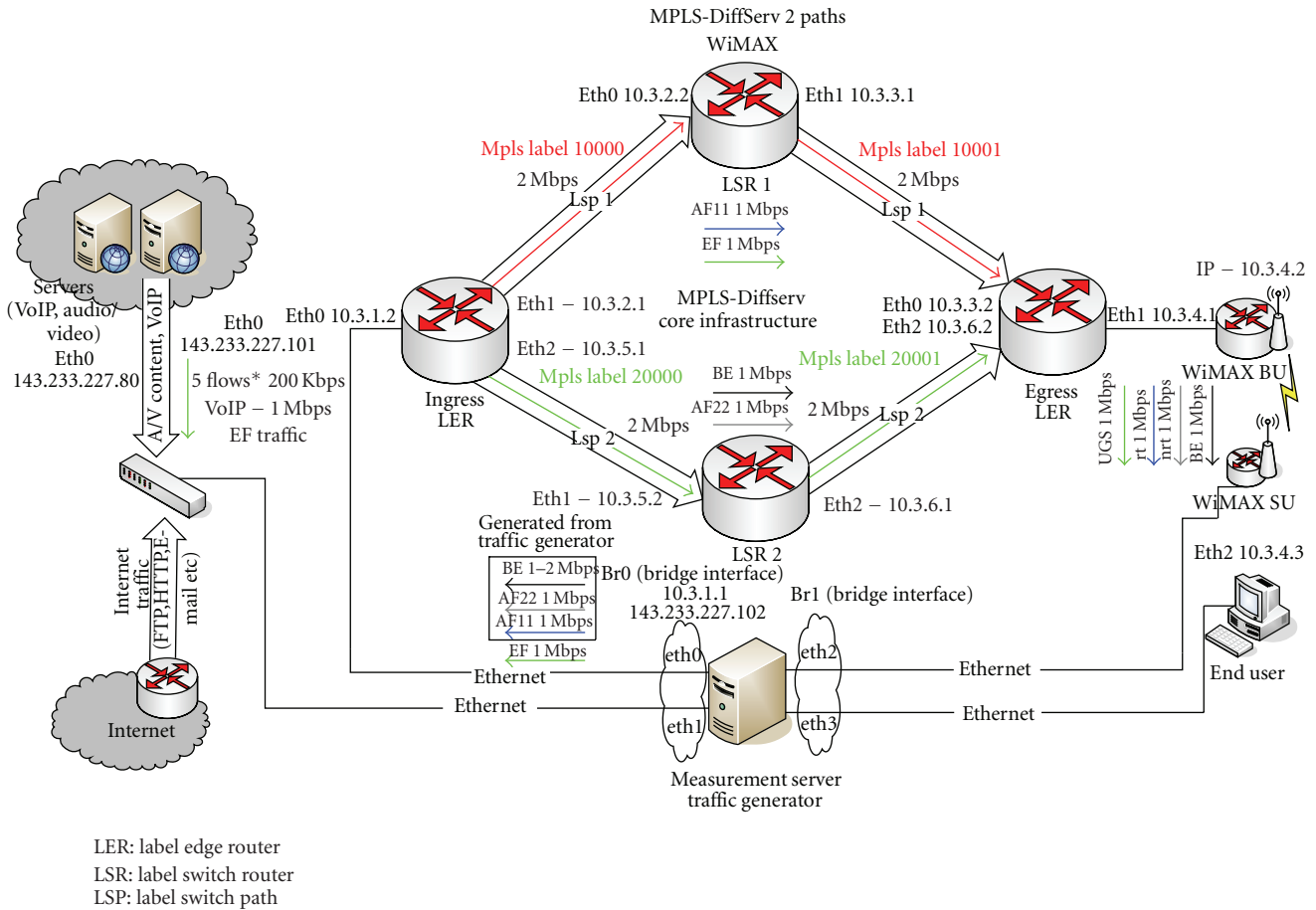
FIGURE 9: Core network with MPLS-DiffServ QoS enabled 2 paths with WiMAX access network.
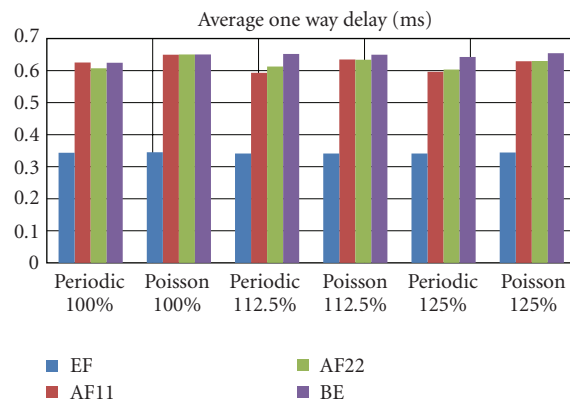

FIGURE 10: Average one way Delay graph.

affected only each other. Whereas the LSP 1 route is limited to 2 Mbps, the EF and AF11 traffic classes affect each other and the result is the increase of EF traffic delay for about 2% which is still an acceptable value for voice transmission. The delay of AF11 traffic decreases as much as to increase the quality of the data transmission. The fact that the AF22 is the class with the highest priority inside LSP 2 is the cause of the average delay decrease for this class.

Observing Figure 15, it is easy to understand that the results regarding the packet loss are the same as the previous setup for the EF and BE traffic with small differences. The AF11 and AF22 classes have a decrease packet loss ratio about 0.5% because when the BE rate increases this affect less the AF11 than before because of the different LSP and different route that the classes follow. AF22 has decreased packet loss because in the second LSP is the
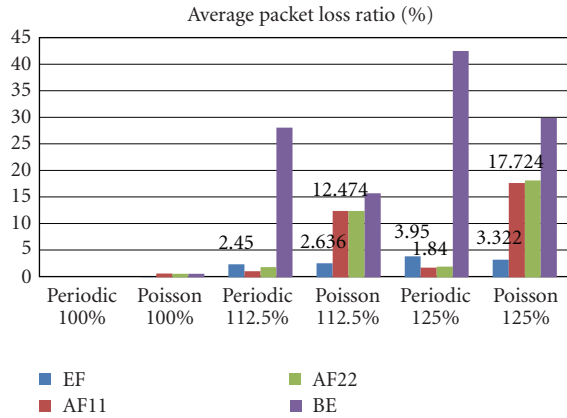
FIGURE 11: Average packet loss ratio.
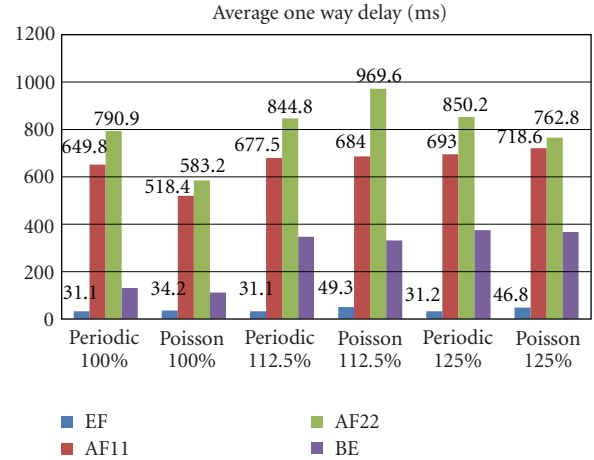
FIGURE 13: Average one way Delay graph.
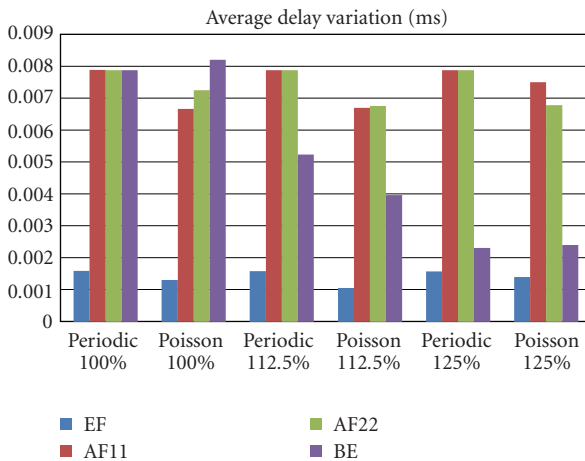
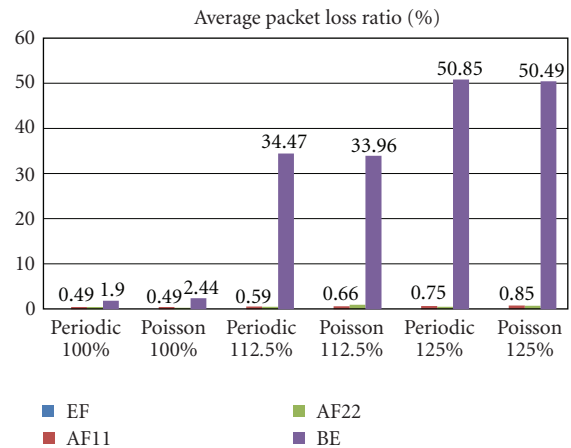FIGURE 12: Average delay variation.

FIGURE 14: Average packet loss ratio.

traffic with the highest priority. Also the 95% of the whole average loss ratio are detected in BE class which is the class causing the network to exceed the capacity for about the 12.5% and 25%, respectively. Also, the average packet loss ratio between different traffic loads increased but with a rate of 0.1% every 12.5% traffic load increase. That means that the network will respond successfully in difficult congestion circumstances protecting the loss sensitive flows. Figure 16 below depicts the average delay variation which is still very small as at the initial stage for all the different traffic scenarios. That means that the packets are transmitted and received with constant ratio which does not affect the network performance and the service initial quality.

5.4. Core Network with QoS Support in 2LSP's and WiMAX Access Network. Completing the evaluation of the core network, it is shown that the provided level of quality was as high as to protect the services from distortion and transmission failure. The average one-way delay of the whole Core and Access networks infrastructure (including all traffic scenarios) are shown below in Figure 17.

Regarding the average one way delay, the WiMAX entity affects the delay by increasing it for about 10% (including all traffic scenarios) comparing with the results in the setup without WiMAX network (previous paragraph). Taking into account that it is a wireless technology, the delay increase is the physical cause for the network. Also this change lets the average one way delay values inside the acceptable limits that the initial data transmitted without distortion. The results are similar to the MPLS-DiffServ with the single-path network setup which means that the addition of a new LSP to the network helped to keep the delay in the acceptable limits. The EF class which is very sensitive (because it carries the voice service) exceeds the acceptable threshold of 50 msec for 12 msec (62 msec) in the case of the 125% traffic load which may cause a delay for the voice service. The delay would be understandable from human ear but in such an affordable level. Comparing with the results in Figure 15, the loss ratio for the EF traffic is 0.1% so the quality is still in high level.

For the AF11 class of service, the delay in whole range of data increases about 10% also, and loss ratio is about 1% for all traffic scenarios; the result is that the level of providing
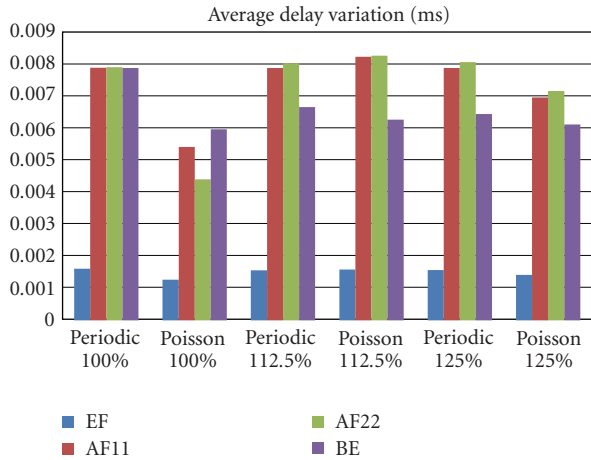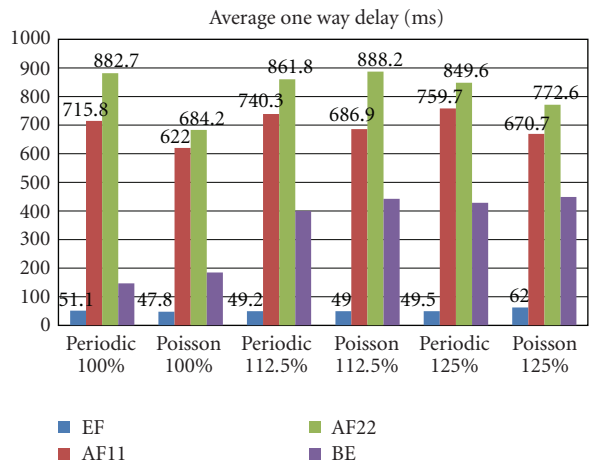
FIGURE 15: Average delay variation.

FIGURE 17: Average packet loss ratio.

FIGURE 16: Average one way Delay graph.

FIGURE 18: Average Delay variation.

quality is high considering the wireless medium and the high traffic load. The same results are for AF22 class which stays also inside the acceptable levels of quality. Below, Figure 19 shows the average delay variation for the whole experimental infrastructure. The values for all traffic scenarios are very low to affect the quality level and also the network performance.

5.5. Core versus E2E (Average Delay and Loss). Summarizing the experimental results will prove that overall E2E QoS provisioning succeeds even after the addition of the WiMAX access network.

(i) Loss

The figures below depict the difference and the average loss percentage addition; that WiMAX QoS enabled access network adds to the existing loss percentage of the core network.

As shown from the Figures 20 and 21, the level of loss percentage addition does not affect the E2E QoS provision. The services reach the end-user keeping the initial constrains even the traffic load exceeds the network capacity 25%.
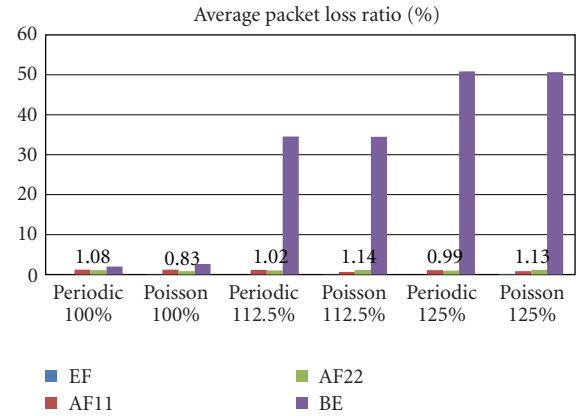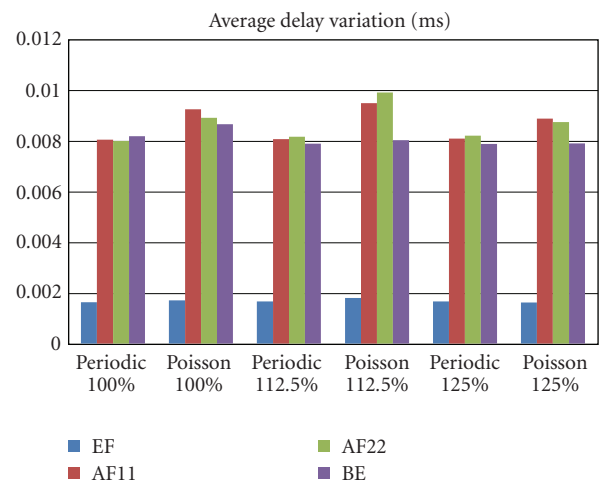
(ii) Delay

The figures below depict the difference and the average delay (ms) addition; that WiMAX QoS enabled access network appends to the existing delay percentage of the core network.

As shown from the above delay comparison figures, the level of delay addition does not affect the E2E QoS provision. The services reach the end-user keeping the initial constrains; even the traffic load increases 25% higher than the network capacity.

6. Conclusions

Completing the evaluation of the core network, it is shown that the MPLS-DiffServ combination regarding the QoS provisioning (in delay and loss sensitive services) improved the core network performance. The provided level of quality was high enough to protect the transmitted services from distortion and transmission failure. The network responds impeccably to the dramatical change of network traffic load which initially was on saturation until the traffic load reaches the 125% of the configured network capacity.
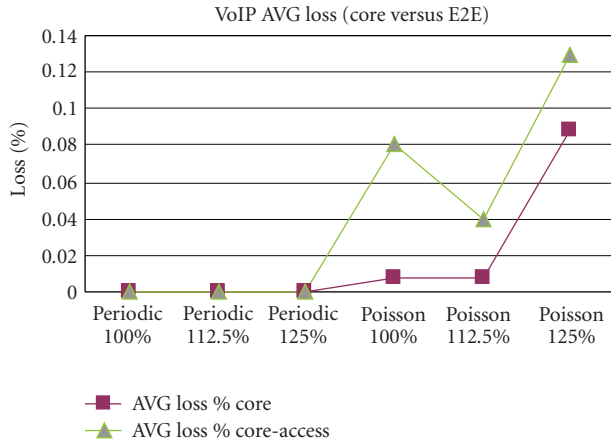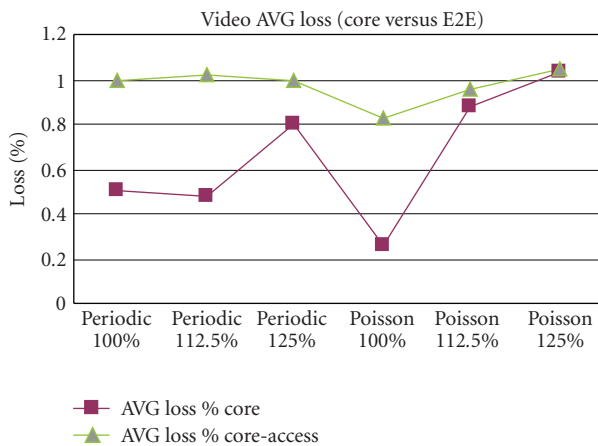
FIGURE 19: VoIP loss percentage AS addition.

FIGURE 20: Video loss percentage AS addition.

FIGURE 21: VoIP delay (ms) AS addition.

FIGURE 22: VoIP delay (ms) AS addition.

The DiffServ architecture provided the expected quality guarantees by classifying the services into different BA's (Behavior Aggregates).

The delay inside core network was increasing and remaining in acceptable levels for a high quality services transmission, but the most important aspect is that the packet loss was decreasing dramatically giving to the voice service and to video streaming service a level of quality familiar with the initial. The MPLS traffic engineering capabilities are shown by the addition of a second LSP to the core network which decreased more than the average one way delay, improving the network performance and the QoS provisioning over the core infrastructure.

The expansion of the same QoS requirements into the access network using WiMAX technology has been tested successfully, providing results that prove the QoS provisioning over a wireless technology keeping the initial QoS constrains for sensitive services as VoIP and high quality video streaming. The average one way delay after the WiMAX addition was similar with delay average of the core network with a single LSP. This fact is shown as follows.
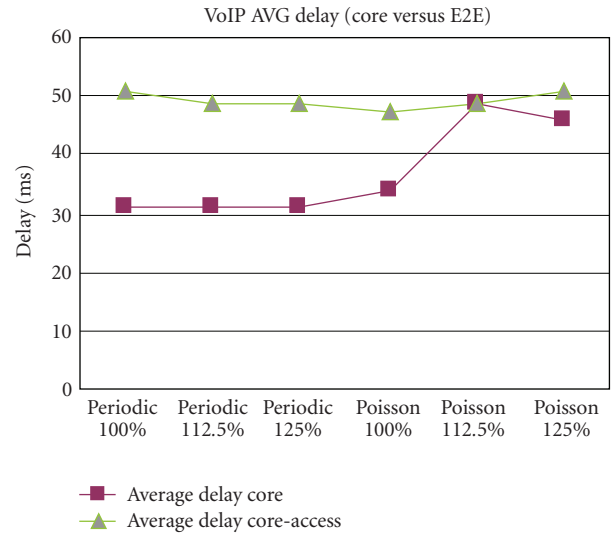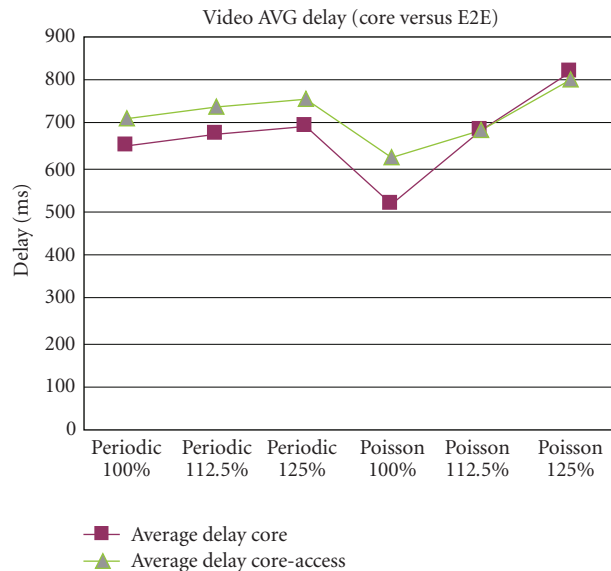
(1) The integration of the WiMAX as Access medium and the Core network infrastructure show that the QoS provisioning inside wireless network is feasible even when the transmitted services are high quality services (VoIP, H-264 Video).

(2) The evaluation of the infrastructure with the different proposed test scenarios shows that the MPLS-DiffServ-combined mechanism provides QoS to core network with low-packet loss ratio and with an acceptable level of one way delay when the MPLS traffic engineering capabilities have been used.

(3) The WiMAX as access network technology successfully provides QoS guarantees to loss- and delay-sensitive services and affects the core network

performance only by adding a small ratio of loss and an acceptable level of delay (for wireless networks).

(4) The Network Operators and Service Providers have another perspective of how a similar network can be attached in their premises (and with which type of format in their services) in order to provide triple play services with QoS guarantees.

Acknowledgment

References

[1] M. Marchese, *QoS over Heterogeneous Networks*, John Wiley & Sons, New York, NY, USA, 2007.

[2] Z. Wang, *Internet QoS: Architectures and Mechanisms for Quality of Service*, Morgan Kaufmann, San Francisco, Calif, USA, 2001.

[3] B. S. Davie and Y. Rekhter, *MPLS: Technology and Applications*, Morgan Kaufmann, San Francisco, Calif, USA, 2000.

[4] I. Minei and J. Lucek, *MPLS-Enabled Applications: Emerging Developments and New Technologies*, John Wiley & Sons, New York, NY, USA, 2005.

[5] IETF RFC 3270, L. Wu, B. Davie, and S. Davari, "Multi-protocol Label Switching (MPLS) Support of Differential Services," May 2002, http://www.ietf.org/rfc/rfc3270.txt.

[6] L. Nuaymi, *WiMAX Technology for Broadband Wireless Access*, John Wiley & Sons, New York, NY, USA, 2007.

[7] N. Zotos, G. Xilouris, E. Pallis, and A. Kourtis, "An MPLS-DiffServ experimental core network infrastructure for E2E QoS content delivery," in *Proceedings of the 6th IEEE/ACS International Conference on Computer Systems and Applications (AICCSA '08)*, pp. 947–951, Doha, Qatar, April 2008.

[8] D. Sweeney, *WiMAX Operator's Manual: Building 802.16 Wireless Networks*, Apress, New York, NY, USA, 2006.

[9] G. Xilouris, T. Pliakas, and A. Kourtis, "Enthrone experimental infrastructure for E2E QoS provisioning," in *Proceedings of the 18th Annual IEEE International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC '07)*, pp. 1–6, Greece, Athens, September 2007.

[10] D. Miras, et al., *A Survey of Network QoS Needs of Advanced Internet Applications*, Internet2 QoS Working Group, November 2002.

[11] MGEN: Multi-Generator, http://cs.itd.nrl.navy.mil/work/mgen/.