Journal of Information Assurance and Security.
ISSN 1554-1010 Volume 6 (2011) pp. 379–388
© MIR Labs, www.mirlabs.net/jias/index.html

A Methodology to Build VPN IP MPLS with Performance and Quality of Service

Adao Boava[1] and Yuzo Iano[2]

[1]Federal University of Fronteira Sul,
Av Dom João Hoffmann 313, Brasil
adao@uffs.edu.br

[2]State University Of Campinas,
Av. Albert Einsten, 400, Brazil
yuzo@decom.fee.unicamp.br

***Abstract*: This article presents a methodology to build a VPN (Virtual Private Network) IP (Internet Protocol) MPLS (Multi-Protocol Label Switching) system to supply network resources in an IP MPLS domain. The methodology is composed of seven stages of a proposed model to build the VPN IP MPLS system. The article emphasizes stage 7 of the proposed methodology, which describes the evaluation of the quality of service (QoS) and presents the results of QoS evaluation based on the VPN IP MPLS technology. The study utilizes a test environment that was developed to validate this stage 7 of the proposed methodology for VPN IP MPLS systems with end-to-end QoS. Tests aimed at data generation (bandwidth, delay, jitter and loss) concerning the service quality were implemented for the performance analysis of the proposed methodology, which is important because the future Networks New Generation (NGN) systems are expected to perform with a known target of delay, loss and jitter. The data-capture test was conducted using CE (Customer Edge) devices and PE (Provider Edge) routers for performance analysis, and the applications were classified according to their DiffServ architecture. Four applications, i.e., Data (BE), Voice (EF), Mission Critical (AF11) and Business Support (AF31) were utilized to raise the QoS parameters.**

***Keywords*: Class Of Service, VPN IP MPLS, DiffServ, Quality of Service and Data.**

I. Introduction

Over the last few years, an increase has been observed in the demand for data communication services capable of integrating multiple types of media such as data, voice and image with quality of service (QoS) [1, 2].

A growing interest has been detected in the use of distributed multimedia applications (e.g., videoconference, digital television, telemedicine and IP Telephony) in private IP networks. These applications are characterized by the use of several types of media, which impose varying QoS requirements on the communication system. Some examples of QoS attributes are maximum delay variation, transmission rate, loss rate and availability. However, despite their best-effort service model, traditional IP VPNs recently begin to show signs of exhaustion. A consequence of using Best Effort model is that all traffic is handled uniformly without any differentiation or prioritization of packets. Therefore, a method is required for building a VPN IP MPLS system that emphasizes QoS, which is the aim of this article.

For the methodology presented in this manuscript, we consider that the CORE of the service provider contains an MPLS [2] with the VPN IP MPLS functionality [3, 4]. The methodology is based on the necessity for receiving differentiated treatment by certain applications in accordance with their specific requirements, which is not possible in the conventional model of the IP network. For this reason, considerable research has been performed to develop service architectures to integrate VPN MPLS [4] technologies to offer new services with scalability and QoS. However, there are several challenges related to the VPN project based on MPLS technology with end-to-end QoS. This article presents a methodology composed of seven stages that outline the necessary steps for the development of a VPN IP MPLS system that can meet the user's application requirements.

This manuscript is organized as follows: Section 2 provides a brief introduction to the main characteristics of the VPN IP MPLS technology; Section 3 presents the proposed methodology; Section 4 presents the main QoS architecture and finally, section 5 presents the implementation of stage 7 of the proposed methodology, which consists of the QoS evaluation.

II. Main Characteristics of the VPN IP MPLS technology

A. VPN IP MPLS – RFC 2574

MPLS VPN in RFC-2547[4, 5, 6] defines a mechanism through which service providers provide VPN services to their clients using their backbones. RFC-2547bis is also known as BGP-MPLS VPN because the BGP protocol is used to distribute VPN routing information and MPLS is used to establish virtual circuits and for traffic routing.

B. RFC components

In the context of RFC 2547bis, a VPN is a collection of rules for the control of connectivity among a set of networks. A service provider connects the client's network through one or more ports, associating each port with a VPN routing table. In RFC 2574, the VPN routing table is called the VPN Routing and Forwarding (VRF) table. Figure 1 illustrates the fundamental blocks of the BGP/MPLS VPN, which are described below:

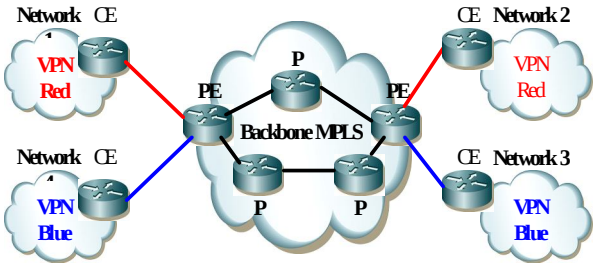

Figure 1. Components of RFC

PE Routers: PE routers exchange routing information with CE routers through static routing, RIPv2, OSPF or eBGP

Provider (P) Routers: P routers are located in the provider's network and do not exchange information directly with the CE devices.

CE Devices: CE devices provide customer access to the service provider network. Typically, a CE device is an IP router that directly establishes a connection with the PE router.

VPN Routing and Forwarding (VRF) Table: The VRF table is a routing and forwarding table for each VPN inside a PE router. A private VRF is only accessible through interfaces that are a part of the corresponding VPN.

III. Proposed methodology for the construction of VPN IP MPLS with QoS

For the methodology presented in the figure 2, we will consider a network core that works with MPLS to form the VPN IP MPLS. The following stages compose the methodology:

Stage 1 [8]: This stage specifies the applications and identifies the requirements of the main applications and the QoS parameters.

Stage 2 [7]: This stage maps and divides applications into the following service classes: Data Best Effort, Data Mission Critical (AF11), Data Management (AF3), Data Business Support (AF31), Data Not Critical (AF1) and Voice (EF).

Stage 3 [5]: This stage selects the VPN MPLS access technology from the following options: Frame Relay, ATM, ADSL, UMTS and Metroethernet.

Stage 4: This stage selects the CE type from two options - with QoS or without QoS.

Stage 5 [5]: This stage configures the VPN IP MPLS as follows: (a) it defines the configurations of the Virtual Routers (VRF), router identifiers (user VPN identifier), route import and export policies (RT) and PE-CE links, (b) it associates the CE interface previously defined in the VRFs and (c) it configures the Multiprotocol BGP.

Stage 6 [9, 10]: This stage performs the Isolation and Connectivity Test between the VPN IP MPLS systems.

Stage 7 [11]: This stage performs the QoS Test of the VPN IP MPLS system.

The objective of Stage 1 is to identify the main applications and requirements that are currently found in the corporative environment. Stage 2 suggests the mapping of the application into 6 classes based on the requirements identified in stage 1. Stage 3 presents a new feature in relation to the traditional VPNs - the implementation of VPN MPLS with xDSL and mobile access. Stage 4 evaluates the requirements of the most important parameters of CE/CPE that may reach the service class parameters. Stage 5 presents topics on VPN configuration, which is one of the most important parts of the VPN MPLS project because a configuration error may allow unauthorized VPN access to a specific user of a different VPN. Stage 6 is responsible for the connectivity and isolation of the VPN. Stage 7 evaluates the performance of the VPN in prioritizing the packages and offering service levels in accordance with the classification performed in stage 2. The evaluation will be performed using public domain software called Iperf in a specially designed environment. This article focuses on stage 7 of the method.

Figure 2 below shows the flowchart of the proposed methodology.

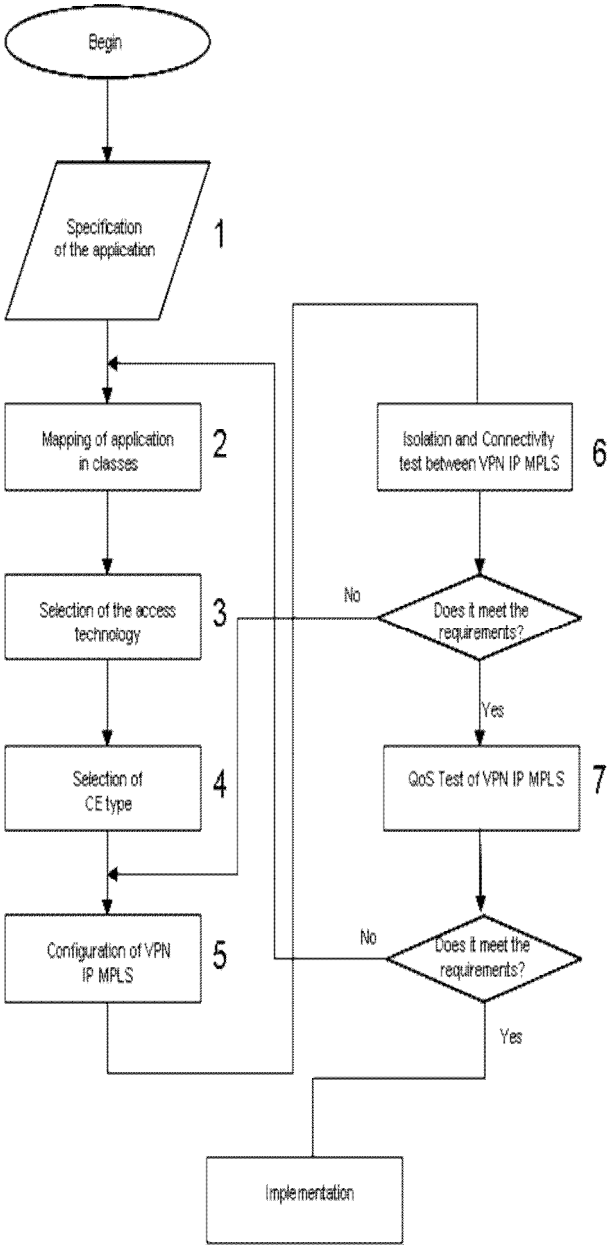

Figure 2. Proposed Methodology

IV. QUALITY OF SERVICE (QOS)

The QoS model adopted for the VPN MPLS performance analysis is based on DiffServ/MPLS. IP packet DSCP classification and marking is conducted through CEs, and the marking of MPLS packet EXP is performed using the PEs involved. From these markings, the classification is performed in queues for each router on the IP network. Each queue is associated with a CoS(class of service) that defines the priority characteristics for transmission (WFQ, WRR), queue size (buffer) and flow control policies (WRED). Table 1 below presents the QoS mechanisms for each MPLS network element involved in the performance analysis described in this manuscript.

Method	CPE/CE	PE
Classification	TCP/UDP/IP	DSCP (IP)
Marking	ACL → DSCP	DSCP → EXP
Voice Queuing	LLQ	Strict Priority
Queuing Serving	CB → WFQ	WRR
Rate Limiting	WRED	TCP /WRED
ATM CoS	VBR-nrt	UBR

Table 1 – QoS Mechanisms

Among the currently available alternatives for offering QoS to MPLS VPN, the following two architectures are used predominantly:

- Integrated Services – IntServ [12, 13]
- Differentiated Services - DiffServ [7, 14]

The IntServ architecture presents problems of scalability because it is limited to small and medium sized networks. DiffServ, on the other hand, has proven to be highly scalable because most of the work is performed on the edge, which eliminates the need of maintaining a state of microflow in the core (as for the IntServ architecture). The random characteristic of flow arrival in different service classes requires the use of a technique to supply the QoS. The main techniques for such supply are the following: (a) resource provision in excess and (b) dynamic provision. The advantage of provision in excess is its ease of implementation due to its use of the existing infrastructure, which increases the transmission rate and the storage capacity in the communicating devices. The characteristic of this technique is the absence of different service classes during normal operation and the use of the common resource and QoS by every flow. The primary disadvantage, however, is the high cost of service due to the maintenance of a channel of communication with a capacity that is greater than the demand.

Dynamic provision consists of using communication channels that are compatible with the demand and executing reconfiguration mechanisms that offer the desired QoS to certain flows. This results in better use of the network's capacity with the provision of a higher QoS, keeping the infrastructure's dimensions in line with the demand. Thus, dynamic provision can potentially offer QoS at a lower cost. The disadvantage of this mechanism is that it demands alteration of the network's devices and introduces additional complexity into the system.

Owing to the dynamic provision's mechanism complexity and the excess bandwidth in the backbone, most operating companies have oversized their resources to obtain the desired QoS. This procedure, however, leads to significantly high costs due to the wasted capacity during the majority of the operating time (i.e., the provision is based on the peak) as

well as for the need to accurately plan growth because telecommunication infrastructure development requires an estimation of future traffic, which is often inaccurate.

With the arrival of xDSL broadband access networks, the operating companies' backbones are experiencing difficulties in maintaining the service standards for their clients using overprovisioning only. Additionally, the need to offer services at lower costs and competitive prices is forcing the operating companies to implement dynamic provisioning.

The use of dynamic provisioning mechanisms is not sufficient to guarantee QoS throughout the VPN; provisioning control and management must be executed over the entire VPN domain, i.e., over the entire set of devices of the company and the clients' (CE to CE).

DiffServ is an architectural proposition for offering QoS resources throughout the set of devices without the issue of scalability. In this case, data flows are aggregated in service classes with a specific QoS pattern. With a limited number of classes, the need for computational resources in routers is reduced by the lower number of states that require treatment.

The use of dynamic provision with DiffServ is recommended in backbones where the operating company wishes to provide its customers with BGP/MPLS VPN solutions with different service classes. In the next section, we discuss some DiffServ architecture-based tests of the VPN with QoS.

Service class identification is performed using a mark in the DiffServ field which is a former TOS (Type of Service) field in the IP header. The DS field contains a value known as the codepoint, which is associated with each service class. The treatment of a certain service class depends on a set of rules applied, which includes methods of classification, scheduling and queue treatment. This set of rules is called PHB – Per Hop Behavior. A network operator that offers DiffServ already has an SLA contract with the user and must follow QoS parameters such as delay, delay jitter and discard for the user traffic that crosses the VPN.

- DiffServ Architecture [13,15]

To avoid the problem of scalability in IntServ architecture (in which core routers cannot treat a large amount of flow), the DiffServ architecture was divided into two types of routers based on their position in the domain: (a) edge and (b) core. Edge routers are located at the domain's boundaries and perform the function of communicating with the routers of other backbone providers or customers. Core routers are located at the network's core and do not maintain any contact with other companies' backbones or with customers. Traffic and quantity of data flow are higher at the core routers due to the aggregation of traffic from several edge routers. Figure 3 shows a schematic of the architecture of a DiffServ domain.

In DiffServ architecture, edge routers perform all of the complex tasks related to classification, marking, shaping and policing. Due to these routers treating a smaller quantity of flow, the functions, which are otherwise computationally intense, can be performed without a loss in scalability.

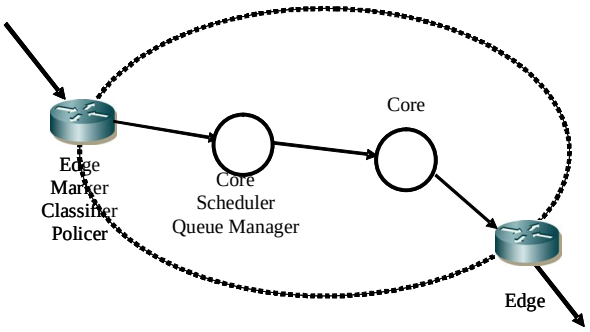

Figure 3. DiffServ Architecture

V. Quality of Service Test (CE and PE)

A. Test Methodology

For QoS tests in CE and PE, the following four scenarios were used (Table 1):

Scenario 1: EF and BE Data, with the sum of bandwidth generated (30 + 120) for each class being lower than the access speed (256 kbit/s).

Scenario 2: Voice (EF) and Best Effort (BE) Data, with the sum of bandwidth generated for each class (30 + 300) exceeding the access speed (256 kbit/s).

Scenario 3: Voice (EF), Best Effort (BE) Data, Mission Critical (AF11) and Business Support (AF31), with the sum of bandwidth (30 + 50 + 30 + 20) being lower than the access speed (256 kbit/s).

Scenario 4: Voice (EF), Best Effort (BE) Data, Mission Critical (AF11) and Business Support (AF31), with the sum of bandwidth (30 + 50 + 30 + 200) exceeding the access speed (256 kbit/s).

The QoS tests are performed at the CE because in the MPLS VPN systems offered currently by the main providers, packets are classified using CE and not PE (as in the traditional MPLS VPN).

Test Purpose: To evaluate the behavior of QoS parameters for the service classes of Voice (EF), Mission Critical (AF11), Business Support (AF31) and Best Effort (BE) Data, implemented in CE with traffic demand being higher than the nominal bandwidth. In other words, the test must demonstrate the following: (a) Packets classified as EF are prioritized over AF and BE, (b) AF11 is prioritized over AF31 and BE and (c) AF31 is prioritized over BE.

For these tests the following components are used:

Traffic Generator - This specific type of test uses Iperf [16],

which is installed in the generating and receiving machines.

Capture Units – The Capture Units are the monitors of 2 computers in which the traffic report is generated and the log files are captured.

B. QoS Test in CE

To validate stage 7 of the proposed methodology, the test environment was put together as shown in Figure 4. In this topology, the PE of the city A and the PE of the city B formed the MPLS[17] network of the VPN IP MPLS service providers of the national provider. The Euclidian distance between the A and B sites is 1018 miles.

Test Setup

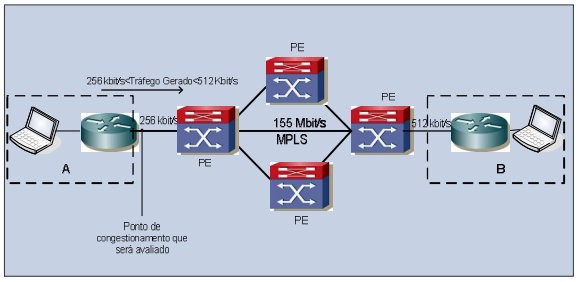

Figure 4. Topology for Test in CE

Scenario	Service Class	Configured bandwidth (Kbps)	Generated traffic (Kbps)	Packet size (bytes)
1	Voice (EF)	54	30	60
	Mission Critical (AF11)	-	-	-
	Business support (AF31)	-	-	-
	Data (BE)	138	120	500
				1200
2	Voice (EF)	54	30	60
	Mission Critical (AF11)	-	-	-
	Business support (AF31)	-	-	-
	Data (BE)	138	300	500
				1200
3	Voice (EF)	54	30	60
	Mission Critical (AF11)	68	50	500
				1200
	Business support (AF31)	43	30	500
				1200
	Data (BE)	27	20	500
				1200
4	Voice (EF)	54	30	200
	Mission Critical (AF11)	68	50	500
				1200
	Business support (AF31)	43	30	500
				1200
	Data (BE)	27	200	500

Table 2 - QoS test parameters in CE

Procedure:

Traffic flows are generated for each service class according to Table 2. In this table, the configured bandwidth refers to CE, and the generated traffic, packet sizes, protocol and port are Iperf (generator) input parameters.

Data to be registered: QoS parameters including bandwidth, delay, packet loss and jitter.

The procedure for capturing Voice class Data in scenario 1 is shown as an example. Although the same procedures were performed for the remaining scenarios and classes, only the graphics were plotted.

Example: Configure Iperf server for UDP flow in the computer in site/city B.

Receiver: Iperf –s –u – p5001 – b54k

Configure Iperf client for UDP flow in the computer in site A Generator: Iperf –c10.200.0.2 –u –p5001 –b54k.

C. Results of tests

Scenario 1: For this scenario, the measured values for the jitter parameters, bandwidth and RTT are presented in the figure 5 and 6. The voice packet utilized measured 60 bytes in size and the date packet varied between 500 bytes and 1200 bytes (shown in Table 2). Figure 5 presents the jitter results for a Data class sized 500 bytes, and Figure 6 presents the bandwidth results for a Data class sized 1200 bytes. The measured RTT was 173 ms for packets sized 500 bytes and 199 ms for the 1200-byte packet.

QoS Test (CE) in scenario 1

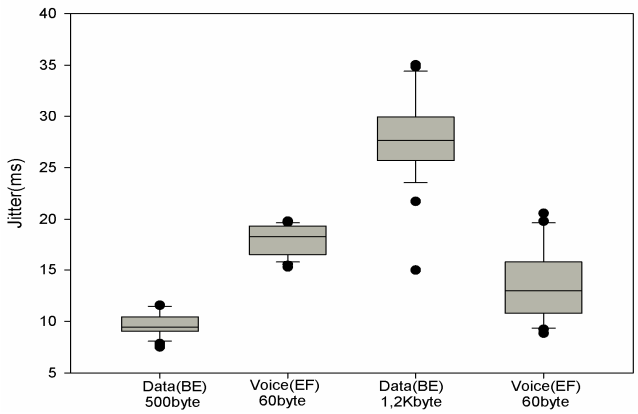

Figure 5. Jitter result for data packet sizes of 500/1200 bytes and packet voice of 60 bytes (scenario 1 - CE)

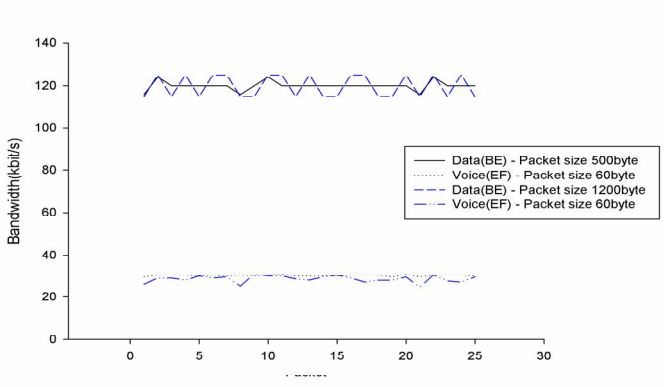

Figure 6. Bandwidth result for data packet sizes of 500/1200 bytes and packet voice of 60 bytes (scenario 1 - CE)

The result of scenario 1 above shows that the values of bandwidth, delay, jitter and packet loss were maintained at

regular levels, i.e., the applications' performance was not damaged in the case of 'no congestion'. 'No congestion' is a condition in which the sum of the traffic generated (i.e., 30 + 120) by applications is lower than the speed of access (256 kbit/s). The values of packet losses are not presented in this scenario because no packet losses were observed.

Scenario 2: For this scenario, we consider four applications (according to Table 2). The QoS parameters will be evaluated using data packet sizes ranging from 500 bytes to 1200 bytes and under conditions of access congestion.

QoS Test (CE) in scenario 2

Figure 7 presents jitter results in a 'congestion' environment with varying sizes for the data packets. We verified that jitter for Voice class was maintained at acceptable levels and showed negligible variation, but the values of jitter for Data classes showed a significant increase of jitter, mainly as a consequence of the higher priority of the EF class over the BE class.

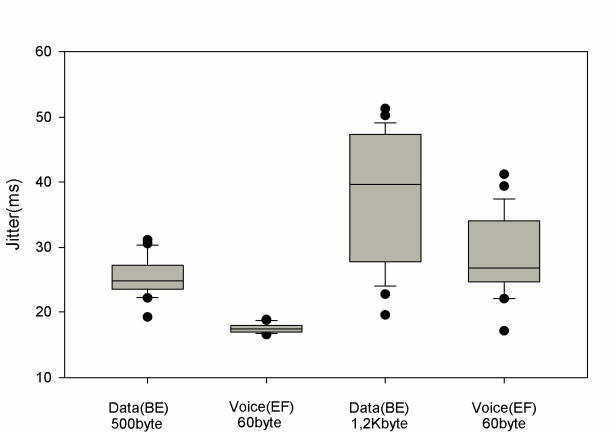

Figure 7. Jitter result for data packet sizes of 500/1200 bytes and packet voice of 60 bytes (scenario 2 - CE)

Figure 8 presents values for loss packets in the 'congestion' situation with a variation in data packet size. The Voice class exhibited a lower packet loss due to its greater priority towards data.

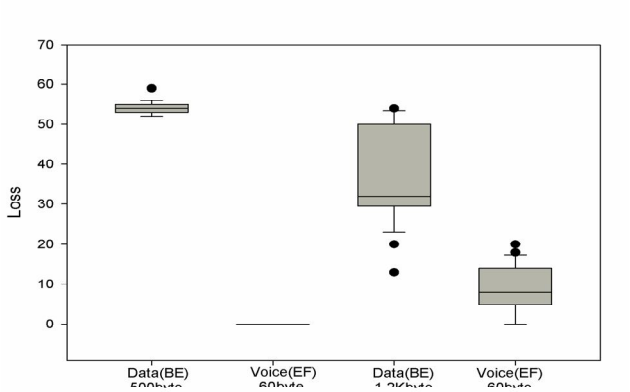

Figure 8. Loss result for data packet sizes of 500/1200 bytes and a packet voice of 60 bytes (scenario 2 - CE)

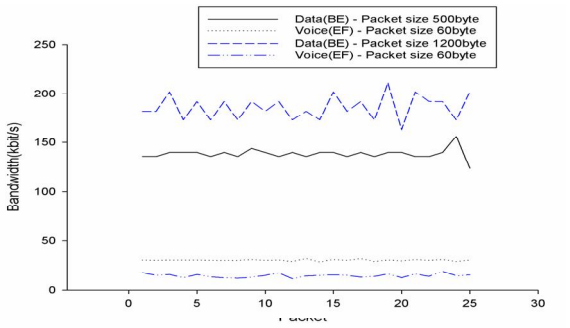

Figure 9. Bandwidth result for data packet sizes of 500/1200 bytes and a packet voice of 60 bytes (scenario 2 - CE)

The results of scenario 2 indicate that for the 500-byte data packets, the values of bandwidth, delay, jitter and packet loss were maintained at acceptable levels for the Voice (EF) and Data classes even in the 'congestion' situation. The 'congestion' situation is one in which the traffic generated by applications (30 + 300) exceeds the access speed (256 kbit/s).

For 1200-byte data packets, we noted a decrease in the bandwidth rate, the occurrence of packet loss and an increase in jitter for the Voice class. This is a consequence of the amount of time for which the voice packets (small; 60 bytes) must wait in queue while the data packets (large; 1200 bytes) are transmitted. The use of LFI (Link Fragmentation and Interleaving) mechanisms in accesses is strongly recommended to keep jitter values at levels that do not damage the quality of voice communication. A fine adjustment should be made on the voice queue size in CE and PE to reduce packet loss[18].

1) RTT evaluation for all four scenarios

For the RTT evaluation, measurements were obtained using data packet sizes of 500 bytes and 1200 bytes as shown in Table 3.

Scenario/Packet Size	RTT (ms) - 500 byte	RTT (ms) - 1200 byte
Scenario 1 (without congestion)	173	199
Scenario 3 (without	181	207

congestion)		
Scenario 2 (with congestion)	340	405
Secanrio 4 (with congestion)	365	700

Table 3 – RTT vs Packet size

If the objective is to manage the delays for the traffic, the first step in finding the solution is to determine which applications on the network can support the delay and the variation in the delay (i.e., jitter). The solution to enable better control of the delay is to isolate the applications that do not support certain types of delay. This is possible through the identification of certain sets of applications, the isolation of these applications from other types of traffic treated within a dedicated queue and the controlling of the delay quantity through the queuing of the specific applications.

The fragmentation of packets diminished the standard deviation of the packets handled by the output queues, resulting in a decrease in the average packet queuing time. Figure 10 shows that in the no congestion situations (i.e., scenarios 1 and 3) the increase in data packet size maintained a linear relationship with RTT for data packet sizes of 500 bytes and 1200 bytes. In the 'congestion' scenarios (i.e., scenarios 2 and 4), the increase in packet size provoked a large increase in the RTT, which compromised some of the applications.

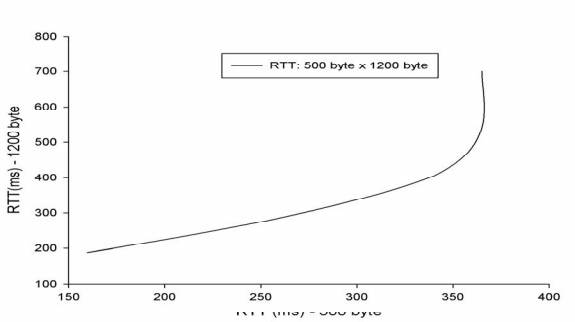

Figure 10. RTT: 500 vs 1200 bytes

D. QoS Test in PE

QoS Test: Evaluation of QoS in the Aggregator (PE)
Purpose: To evaluate the behavior of QoS parameters for service classes Voice (EF), Mission Critical (AF11), Business Support (AF31) and Best Effort (BE), implemented in the PE aggregator in the presence of traffic demand that exceeds the nominal bandwidth. In other words, the test must demonstrate the following: (a) Packets classified as EF are prioritized over AF and BE, (b) AF11 is prioritized over AF31 and BE and (c) AF31 is prioritized over BE.

Procedure: Traffic flows are generated for each service class according to Table 4. Each test is executed with packet sizes ranging from 500 to 1200 bytes for the following service classes: Mission Critical (AF11), Business Support (AF31) and Best Effort (BE) Data. Voice class size is fixed at 60 bytes.

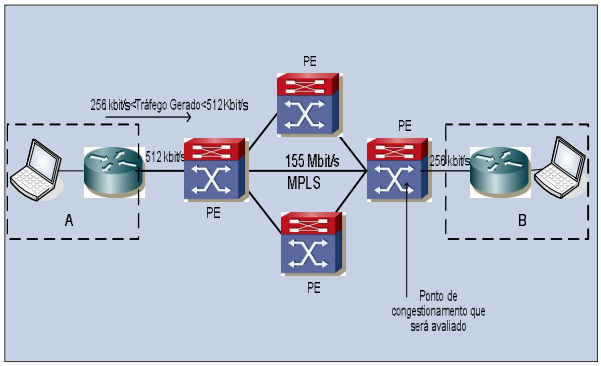

Figure 11. Topology for test in PE

Scenario	Service Class	Configured bandwidth (Kbps)	Generated traffic (Kbps)	Packet size (bytes)
1	Voice (EF)	34	30	60
	Mission Critical (AF11)	-	-	-
	Business support (AF31)	-	-	-
	Data (BE)	350	150	500 1200
2	Voice (EF)	34	30	60
	Mission Critical (AF11)	-	-	-
	Business support (AF31)	-	-	-
	Data (BE)	350	300	500 1200
3	Voice (EF)	34	30	60
	Mission Critical (AF11)	80	40	500 1200
	Business support (AF31)	80	40	500 1200
	Data (BE)	190	80	500 1200
4	Voice (EF)	34	30	60
	Mission Critical (AF11)	80	40	500 1200
	Business support (AF31)	80	40	500 1200
	Data (BE)	170	300	500

Table 4 - QoS tests parameters in PE

Data to be registered: QoS parameters including bandwidth, delay, packet loss and jitter.

Scenario 1: Figure 12 shows the jitter values measured at PE for data packet sizes of 500 and 1200 bytes. The Voice and Data classes were configured for a bandwidth of 34 Kbit/s and 350 Kbit/s, respectively. The traffic generated by the Voice and Data classes for data collection at the PE in a no congestion situation was 30 Kbit/s and 150 Kbit/s, respectively. The increase in data packet size from 500 to 1200 bytes provoked an increase in jitter for the Voice class but maintained acceptable levels of voice quality.

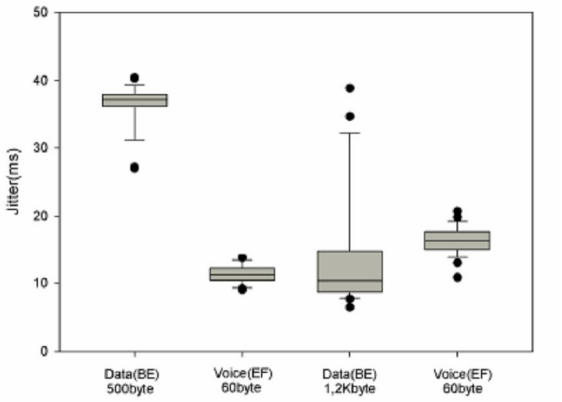

Figure 12. Jitter result for data packet sizes of 500/1200 bytes and packet voice of 60 bytes (scenario 1 - PE)

The values of bandwidth, jitter, delay and packet loss were maintained at regular levels for the 'no congestion' situation. No packet loss was observed in this scenario. RTT was maintained at acceptable levels for several packet sizes.

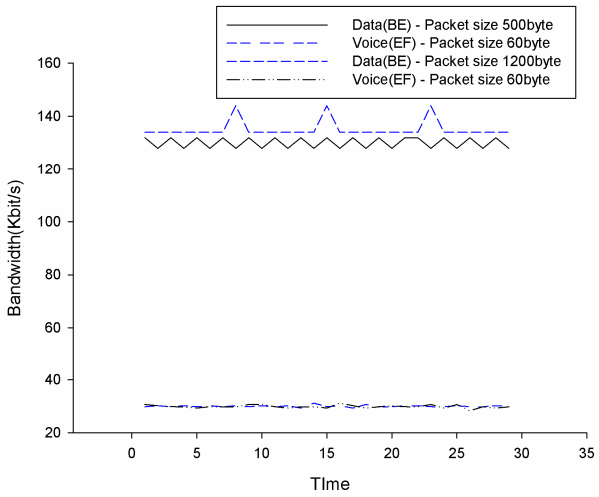

Figure 13. Bandwidth result for data packet sizes of 500/1200 bytes and packet voice of 60 bytes (scenario 1 - PE)

Scenario 2
QoS Test (PE) in scenario 2

Figure 14 shows a congestion scenario at PE for the Data and Voice classes. The increase in packet size provoked a significant increase in the jitter for the Data class. The increase was not significant for the Voice class due to its priority over the Data class. The average value of jitter of 20 ms is sufficient for an acceptable quality of voice transmission.

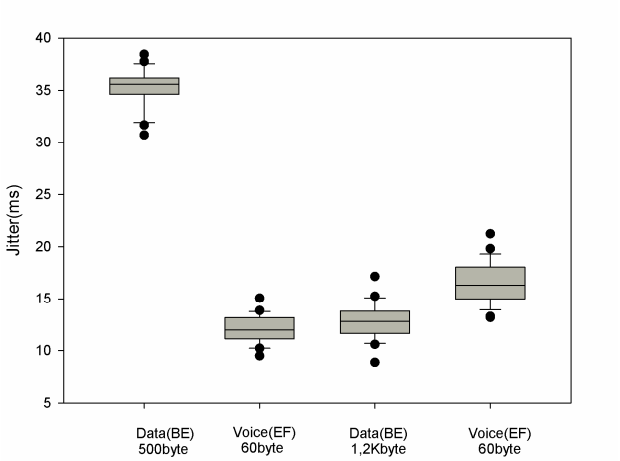

Figure 14. Jitter result for data packet sizes of 500/1200 bytes and a packet voice of 60 bytes (scenario 2 - PE)

Figure 15 shows the packet loss for the Data and Voice classes for 500-byte and 1200-byte data packets in the congestion scenario. The loss of packets was less sensitive for the Data class than for the voice class, justifying the adopted QoS mechanism.

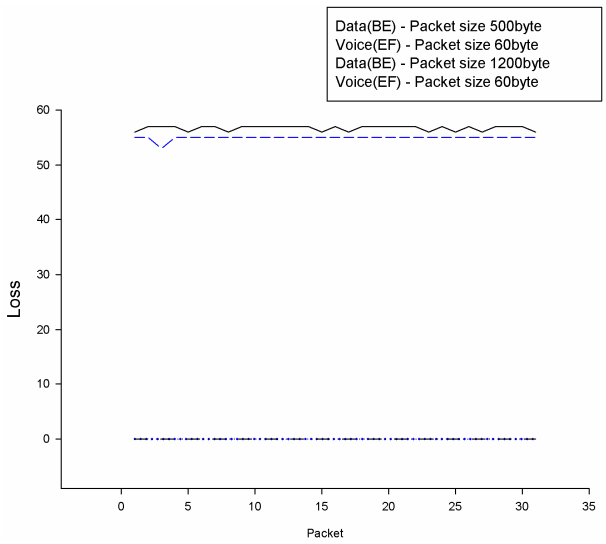

Figure 15. Packet loss results for data packet sizes of 500/1200 bytes and packet voice of 60 bytes (scenario 2 - PE)

Scenario 3: QoS Test (PE) in scenario 3.

For this scenario (i.e., without congestion), jitter was evaluated only for a posterior comparison with scenario 4 jitter (i.e., with congestion). The loss of packets, bandwidth and delay maintained acceptable values. The increase in packet size for applications BE, AF31 and AF11 for the no congestion scenario (scenario 3) provoked an increase in the data dispersion and in the standard deviation for the jitter, but the average values remained acceptable for each application.

The values of bandwidth, delay, jitter (Figure 16) and packet loss were maintained at regular levels. No packet loss was observed for the four classes in this scenario.

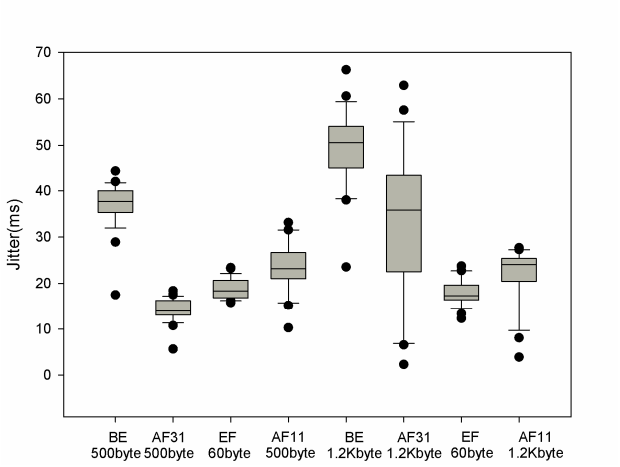

Figure 16. Jitter result for BE, AF31, AF11 packet sizes of 500/1200 bytes and packet of voice 60 bytes (scenario 3 - PE)

QoS Test (PE) in scenario 4

For scenario 4, we observed the prioritization of EF over the remaining packets. For the voice application (EF), the average value and dispersion remained identical; however, variations in packet size were observed for applications BE, AF31 and AF11. Satisfactory performance of a voice application requires a low jitter value, and therefore, the QoS strategy worked adequately. Figure 17 shows the results for the jitter in scenario 4(table 4).

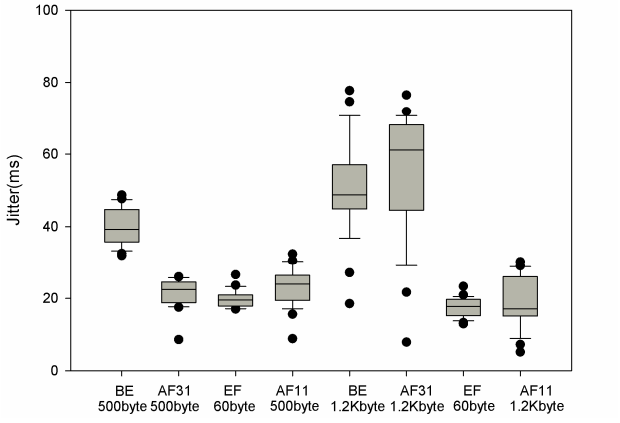

Figure 17. Jitter result for BE, AF31, AF11 packet sizes of 500/1200 bytes and packet voice of 60 bytes (scenario 4 - PE)

For 500-byte data packets, the occurrence of a small packet loss was observed in the mission critical class. For the Voice and business support classes, the values of bandwidth, delay, jitter and packet loss maintained regular levels.

VI. Conclusion

In this article, we have presented a method for building a VPN MPLS system focused on QoS (stage 7 of the method). A testing environment was implemented to evaluate the performance of stage 7. The assembly and verification of the results was performed using software that is completely free (Iperf). The service quality test evaluated four scenarios to investigate whether both CE and PE prioritized packets based on their classification in situations of access congestion.

The results demonstrated that the QoS mechanisms analyzed exhibited satisfactory performance in all four scenarios. Some precautions must be exercised for Voice class (EF) transmission with regard to data packet sizes in the network.

To prevent the article from becoming excessively long, we placed an emphasis on the tests, considering that previous steps such as VPN configurations were already completed.

References

[1] Vegesna, S. “IP Quality of Service”, Cisco Press 2001
[2] Monique Morrow, Azhar Sayeed. “MPLS and Next-Generation Networks: Foundations for NGN and Enterprise Virtualization”,2006.
[3] A White Paper by NetScreen Technologies, Inc. - Deploying Scalable, Secure, DynamicVirtual Private Networks, May 2003
[4] Semeria, Chuck. – “RFC 2547bis: BGP/MPLS VPN Hierarchical and Recursive Applications”, 2001
[5] I. Pepelnjak, J. Guichard, J. Apcar. “MPLS and VPN Architectures – Volume II” Cisco Press 2003
[6] Guichard, Jim and I, Pepelnjak MPLS and VPN Architectures: A Practical Guide to Understanding, Designing and Deploying MPLS and MPLS-Enabled VPNs Cisco Press 2000.
[7] RCF 2983, “Differentiated Services and Tunnels”, http://www.ietf.org/rfc/rfc2983.txt
[8] Joseph Ghetie**, “**Fixed-Mobile Wireless Networks Convergence”, Cambridge University Press 2008
[9] Ina Minei, Julian Lucek, MPLS-Enabled Applications, John Wiley & Sons Ltd, 2005
[10] A White Paper by NetScreen Technologies, Inc. - Deploying Scalable, Secure, DynamicVirtual Private Networks, May 2003
[11] Leinen, Leinen, S., Przybylski, M, Reijs, V. & Trocha, S., “Testing of Traffic Measurement Tools”,TF-NGN Deliverable D9.4, September 2001
[12] R. Braden, et al., RFC 2205, “Resource ReServation Protocol (RSVP) – Version 1, Functional Specification, “September 1997
[13] Magalhães, M. F.; Cardozo, E. (1999). Quality of Service in Internet. Technical Report, UNICAMP/FEEC/DCA, Campinas, SP.
[14] E. Osborne, A. Simba, “Engenharia de Tráfego com MPLS” Cisco Press 2003
[15] S.Blake, et. Al., RFC 2475, “Na Architecture for Differentiated Services,”December 1998.

[16] http://sourceforge.net/projects/iperf/ developed by NLANR/DAST
[17] Luc De Ghein/Cisco Press, MPLS Fundamentals,2007
[18] Zhuo (Frank) Xu/Alcatel –Lucent, Designing and Implementing IP/MPLS-Based Ethernet Layer 2 VPN Services,2010.

Author Biographies

Adao Boava received his B.S. degree in Electrical Engineering in 1991 from Federal University of Santa Catarina (UFSC), Florianopolis-SC, Brazil. He received his M.S. degree from the State University of Campinas, and M.B.A. from Foundation Getulio Vargas (FGV), São Paulo, Brazil. Currently, he is working towards his Ph.D. degree in Telecommunications at the State University of Campinas (Unicamp), São Paulo, Brazil. He is a professor at Federal University of Fronteira Sul (UFFS), Santa Catarina, Brazil. He has worked in Brasil Telecom for 16 years with product development MPLS.

Yuzo Iano received his PhD. in electrical engineering in 1986. Currently he is an Associate Professor in Electrical Engineering at Unicamp (State University of Campinas, Brazil). He also works at the Visual Communication Laboratory in the same University and is responsible for digital signal processing (sound and image) projects. His research interests include video and audio coding, digital video and audio compression and digital signal transmission. He is a member of IEEE.