Journal of King Saud University – Computer and Information Sciences (2013) 25, 89–98

King Saud University

Journal of King Saud University – Computer and Information Sciences

www.ksu.edu.sa
www.sciencedirect.com

ORIGINAL ARTICLE

Efficient priority schemes for the provision of end-to-end quality of service for multimedia traffic over MPLS VPN networks

Nasser-Eddine Rikli [a,*], **Saad Almogari** [b,1]

[a] *Department of Computer Engineering, King Saud University, Riyadh, Saudi Arabia*
[b] *National Information Center, Ministry of Interior, Riyadh, Saudi Arabia*

Received 17 March 2012; revised 3 July 2012; accepted 27 August 2012
Available online 5 September 2012

KEYWORDS

Virtual private networks;
Quality of service;
Multimedia;
MPLS;
Queueing mechanisms

Abstract In this paper, a VPN network simulation model will be built using the MPLS protocol and based on an existing network. Various queueing policies will be implemented to evaluate the provision of the end-to-end QoS requirements for various traffic types. Input traffic based on real data was used. After a thorough analysis of the policies, the merits and shortcomings of each policy are determined and recommendations are given along with future research directions.

1. Introduction

Virtual Private Network (VPN) has served as a cost effective and efficient means to let users on physically separated networks appear to their remote users as existing on a single network. The complexity of the protocols involved and the high bandwidth required are by themselves quite a formidable challenge. If security issues and Quality-of-Service (QoS) requirements are added, then this challenge will increase by many folds.

Provision of some QoS requirements over Virtual Private Networks (VPN), which is the focus of our study, will require surmounting many challenges. Getting a flexible and scalable QoS support in such networks is of primordial importance, and is usually achieved through setting access and service policies (Saika et al., 2011; Tran Cong et al., 2010; Dhaini et al., 2010; Jialei and Yuanping, 2010; Rahimi et al., 2009; El Hachimi et al., 2008). It is imperative that any VPN service provider offers to his customers different Classes of Service (CoS) per VPN that may satisfy their needs (Luyuan et al., 2005). Furthermore, depending on the customer choice and selection, the CoS that a particular application would get within one VPN could be different from the CoS that exactly the same application would get within another VPN. Thus, the set of policies to support QoS should allow the decision to be made on a per-VPN basis.

VPN networks have been implemented through two major models that may be used to provide customers' QoS requirements: the *pipe* model and the *hose* model (Duffield, 2002). In the former, a customer is supplied with certain QoS guarantees for the traffic from one Customer Edge (CE) router to another. While in the latter, to be considered in our study, a customer is

* Corresponding author.
E-mail addresses: rikli@ksu.edu.sa (N.-E. Rikli), smogri@nic.org.sa (S. Almogari).

[1] Eng. Saad contributed to this research while working towards his MS degree in the Department of Computer Engineering at King Saud University.

Peer review under responsibility of King Saud University.

Production and hosting by Elsevier

1319-1578 © 2012 King Saud University. Production and hosting by Elsevier B.V. All rights reserved.
http://dx.doi.org/10.1016/j.jksuci.2012.08.001

supplied with certain guarantees for the traffic that the customer's CE router sends to and receives from other CE routers.

Due to the great interest shown by both the end users and the service providers, the research community has been actively contributing to the development and integration of new techniques and protocols for the private network virtualization. For instance, a programmable framework was proposed in Kumar et al. (2004) for CoS Based Resource Allocation (CBRA) in Multi-Protocol Label Switching (MPLS) tunneled VPNs, where the resources were partitioned in a way that facilitates the creation of multiple VPNs on a demand basis. Also, the QoS over an IP VPN network, which included the provision of QoS guarantees both at the network level and at the node level, was presented from a service provider point of view in Zeng and Ansari (2003). In Girish et al. (2003), a CoS classification with associated QoS parameter set for VPNs over an IP WAN was presented, various scenarios were studied, and it was determined that by policing the aggregate arrival rates of each class from each VPN access interface into the IP network, the appropriate QoS can be guaranteed for each CoS.

The main goal of this paper is to build a simulation model for a large existing VPN network and to study its performance under various queueing mechanisms and for various types of traffic with different QoS requirements. It is believed that a mapping between the traffic types and the queueing mechanisms will be established in a way that will optimize the sought QoS requirements.

The rest of the paper is organized as follows. In Section 2, the architecture of the network to be studied will be presented. Then, in Section 3 the traffic models and traces to be used in the simulation will be described. In Section 4, the queueing models to be used in the various routers will be introduced. The results will be presented in Section 5, along with some network specific data. Finally, in Section 6 conclusions will be summarized.

2. Network architecture model

Although this study may be easily extended to any similar VPN architecture, the results upon which our conclusions and recommendations will be based are derived from a simulation model of an existing network. The VPN service provider (VPN-SP) has a network that consists of nine sites distributed according to their geographic location and covering the whole country. However, the network to be considered consists of four sites that are related to the VPN of one customer, with one main site situated at the company headquarters and three remote sites. The general network architecture under study is shown in Fig. 1. The network topology of the VPN-SP related to our study consists of:

(1) *Provider routers* (P): there are a total of six P routers. Three routers are located at the main site, and one router is located at each of three remote areas. Each P router at a remote area is connected to a separate P router at the main area.
(2) *Provider Edge router* (PE): there is one PE router located at each of the three remote areas.

The customer, to be considered in this study and as shown in Fig. 1, has a main site, denoted by *Area A*, and three separate remote sites, denoted by *Area B*, *Area C*, and *Area D*. The remote sites are linked to the main site in *Area A* through the VPN-SP using P routers. The P routers at each remote site are connected to the user network through a sequence of PE routers followed by a CE router. All customers hook to the VPN network through the CE router. Note that *Area B* has two CE routers, while *Area C* and *Area D* have only one. Each site may have a configuration similar to the one shown in Fig. 2. All users are connected through a 100 Mbps Ethernet switch to the CE router (this model is to be used in the simulation).

The VPN services are assumed to be provided through a *hose* model, and most traffic is assumed to pass through the routers at the main area. The routing protocol used between a CE router and a PE router is the Border Gateway Protocol (BGP) (Rekhter et al., 2006). At the PE router, each site connects its customers through an interface that marks all outgoing traffic with a unique VPN label to mark its traffic between PE routers. Routing table information is exchanged between PE routers using Multi-protocol BGP (MP-BGP) (Bates

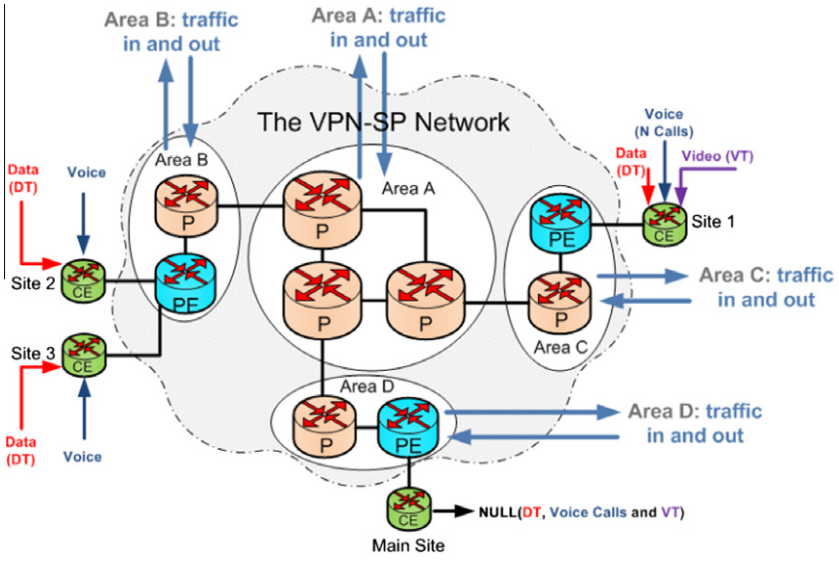

Figure 1 Network architecture and traffic input locations and types.

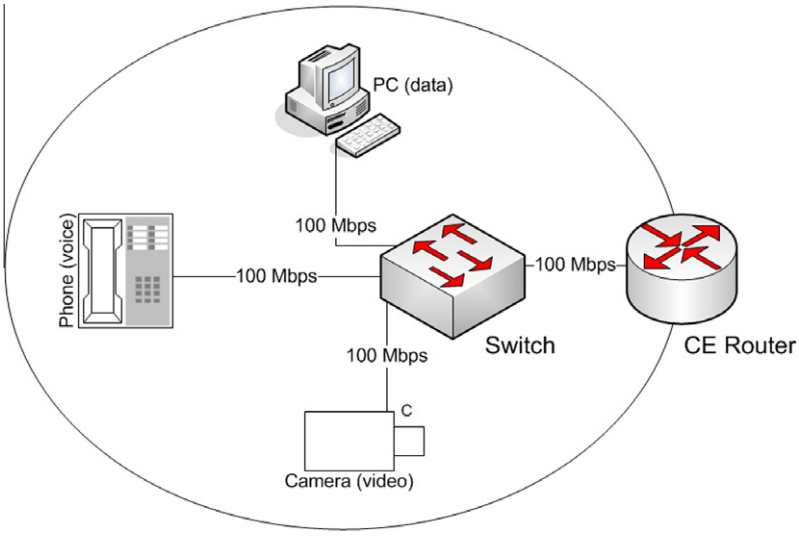

Figure 2 Typical site architecture model.

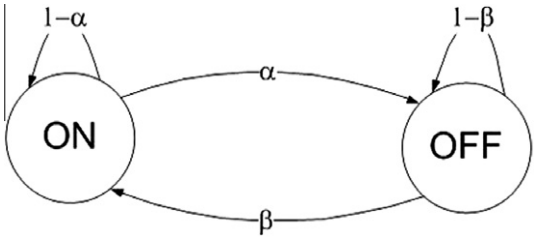

Figure 3 ON–OFF voice source model.

et al., 2007). The VPN-SP uses Multi-protocol Label Switching (MPLS) over Open Short Path First (OSPF) network.

3. Traffic models

3.1. Types

The VPN-SP network is assumed to carry various types of traffic generated by the customers attached to the four company sites. Three types of traffic aggregated at the CE routers will be considered: voice traffic, video traffic, and data traffic.

Voice traffic is assumed to be generated through sources using a G.729 coder. The corresponding aggregate traffic was modeled by an ON–OFF source with exponential durations, as shown in Fig. 3. During the ON period, packets of fixed size are generated at fixed time intervals, while during the OFF period no packets are generated (Hassan et al., 2006). The parameters α and β represent the inverse of the average periods spent in the ON and OFF periods, respectively.

The two other types of traffic, i.e., MPEG-4 video (Coding of Moving Pictures and Audio, 2002) and data, were captured into trace files from the real traffic flows at the various locations of the actual VPN-SP network using a packet sniffer tool (Wireshark).

For video traffic, a laptop with Ethereal software installed on it, was connected to a port on a remote site switch, and configured to send all generated traffic through this switch. Then, the video traffic was sniffed (or captured) for 10 min and stored into an ASCII file. Since the trace file has to satisfy NS-2 requirements, a Perl script was designed to convert it into a special binary format. In a manner very similar to video, a data trace was generated by capturing the Ethereal data traffic for 60 min, which was also converted into a binary format.

These files were used as input at their corresponding locations to simulate real traffic from site-to-site of the chosen customer (or inside the VPN-SP network when coming from other customers).

3.2. Load distribution

Fig. 1 illustrates the traffic direction over the various sites. This traffic is composed of two main categories: internal traffic and external traffic.

3.2.1. Internal traffic

It consists of three types: voice, video, and data that originate from sites 1, 2, and 3. All these types of traffic are directed to the main site. No traffic is assumed to be generated from the main site. While site 1 generates all three types of traffic, sites 2 and 3 generate only voice and data types.

3.2.2. External traffic

Any traffic other than the traffic coming from the considered customer VPN is assumed *External*. Each of the four Areas (A, B, C, and D) is assumed to both receive external traffic input to the network and deliver output traffic leaving the network. It is assumed that all external flows include the three types of traffic.

3.3. QoS requirements

The QoS traffic requirements, shown in Table 1 (Understanding Delay in Packet Voice Networks, 2008; VoIP: An In-Depth Analysis, 2006), were chosen to satisfy both generic requirements of the types of traffic carried over the network, and the capabilities of the equipment existing on the premises. It is worthwhile to note that in our requirements setting, voice and video traffic were considered to be sensitive to delay and

Table 1 Traffic requirements.

Criteria	Voice	Video	Data
Packet delay (msecs)	200	250	–
Jitter (msecs)	40	40	–
Packet loss[a] (%)	5	10	–
Packets resent (%)	–	–	10

[a] Here, packet loss includes both the number of dropped packets and delayed packets.

jitter delay. The traffic was allowed to have packets that were not conforming to the preset limits to be dropped, but no retransmissions were allowed (since this will be useless as the delay limits at the destination will be surpassed). Nevertheless, a threshold was put to this packet dropping that was not allowed to be surpassed.

Data traffic, on the other hand, was assumed to be insensitive to packet delay and jitter delay; it was allowed to have retransmissions to get the erroneous packets corrected, but still with a limit bound not surpassing 10 retransmissions.

4. Queueing models

4.1. Policies

The queueing disciplines implemented in the routers were designed to serve traffic streams in accordance with their QoS requirements. In this regard, various queueing policies have been suggested and implemented to come up with a selection that will fulfill disparate traffic requirements. In this study, we have considered four different types of policies representing different categories.

If no queueing policy were implemented, then the traffic streams will join a common queue and will be served in a First-in-First-Out (FIFO) manner, as shown in Fig. 4. All three types of traffic will be treated equally, and a data packet may be dropped if the queue is full. This may happen while video and voice packets, arriving earlier, were in the queue. Of course, video and voice traffic may tolerate packet loss more than data packets. It is also ironic that these packets, which caused this data packet drop, may be discarded at their destination if they arrive with a delay exceeding their maximum delay limit. Such situations may be avoided or minimized by implementing an appropriate queueing policy.

4.1.1. Fair queueing (FQ)

The basic policy in FQ is to divide the traffic into separate flows, as in our case, which is based on the traffic types: video, voice, and data; this is shown in Fig. 5. Each flow will join a separate FIFO queue. The queues are then served through a round-robin scheduling, with each queue sending one byte at every round.

4.1.2. Priority queueing (PQ)

In a manner similar to FQ, the packets are classified into three separate FIFO queues, as shown in Fig. 6. In this case, however, the queues are not served in a round-robin fashion but according to a predefined priority scheme. In our case, the voice queue is served with priority one (the highest), the video queue is served with priority two, and the data queue with priority three (the lowest). Packets are then served within each queue in FIFO manner, and if a newly arriving packet finds the queue full, it will be dropped.

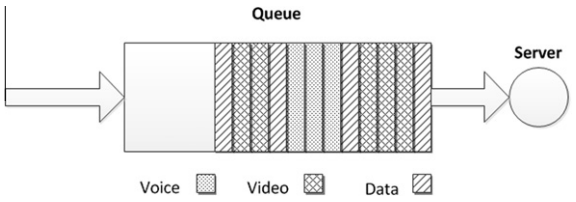

Figure 4 Queue without priority policy.

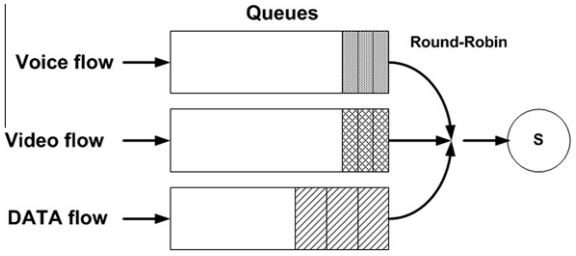

Figure 5 Fair queueing policy.

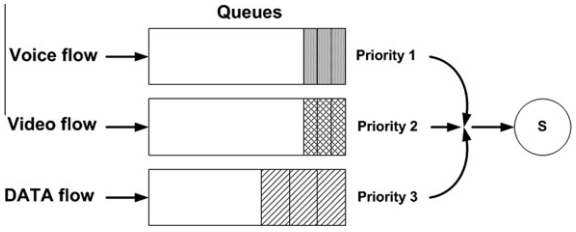

Figure 6 Priority queueing policy.

4.1.3. Custom queueing (CQ)

CQ is similar to PQ since they both support a certain classification option. However, CQ scheduling is completely different than PQ. In CQ, a round-robin service is used as in FQ, but with each queue allowed to forward a different number of bytes (not packets) depending on its priority. The queues may be thought as being served in a weighted round-robin scheme. The available bandwidth is distributed among the queues in a fixed weighted manner, and tail dropping is still used with each individual queue.

Fig. 7 shows two CQ schemes. In the first scheme, Fig. 7a, weights were distributed as follows: 10% for voice, 20% for video and 70% for data. In the second scheme, Fig. 7b, the weight distribution is changed to 20% for voice, 30% for video and 50% for data.

4.1.4. Low-latency queueing (LLQ)

The LLQ is a combination of PQ and CQ policies (Low latency queueing). The first queue has the highest priority, and is still served first as in PQ. Only if the first queue is empty, the second and third queues will be served based on a fixed partition, such as 30% for the second queue and 70% for

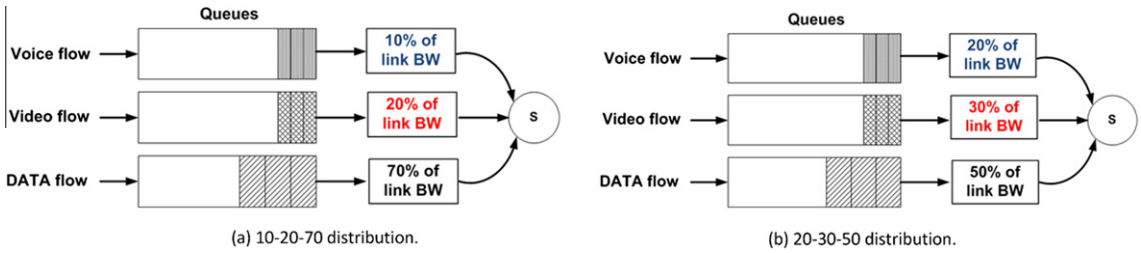

Figure 7 Customized priority policy.

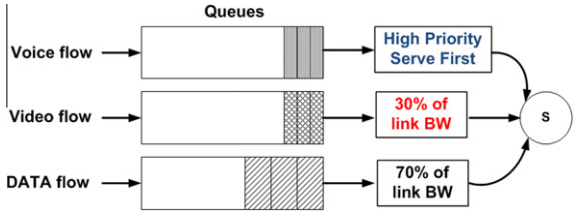

Figure 8 Low latency queueing policy.

the third queue, similar to CQ. In this study, the first queue was assigned to voice flow, the second to video flow, and the third to data flow, as shown in Fig. 8.

4.2. Characteristics

Fig. 9 shows the location of the ports of each router where the proposed queueing mechanisms will be implemented. Each P router in area A has three ports, while each P router in the remaining areas, B, C, and D, has two ports. Also, the PE routers in areas C and D have two ports each, while the PE router in area B has three ports. Finally, all CE routers have a single port.

Each router port is served with buffers with the number of flows for each queue. Various sizes have been used depending on the policy to be implemented.

5. Results

To investigate various aspects of the effects of the queueing policy on the performance of the considered network, two sets of experiments have been designed. In the first set, the effects of the number of input sources will be studied followed by the effects of the bandwidth of the "last mile" link between the PE and CE routers at the main site. Furthermore, five experiments will be run, within each set, to evaluate the network performance under the various proposed queueing policies.

The simulation experiments were conducted using the NS2 simulation tool, and ran for one hour of the simulation time. All router queues were assumed to have finite buffer sizes and had a total size of 512 KBytes (KB) with 128 KB for the first and second queues, while 256 KB for the third queue.

The default router capacities were 1 Gbps for the core P routers, 10 Mbps for the P routers at the three remote areas, 1 Gbps for the PE routers, and 1 Mbps for all CE routers except the one at the main site, which had 2 Mbps. Note that this last link capacity will be varied in the second set of experiments, and its effects will be studied.

The default number of sources, assumed in our study, was based on typical network conditions for the considered customer. They were three voice sources representing the internal traffic from the customer network (one at each remote site) and 10 voice sources representing the external traffic. The video sources were one from remote site 1 and 4 from the

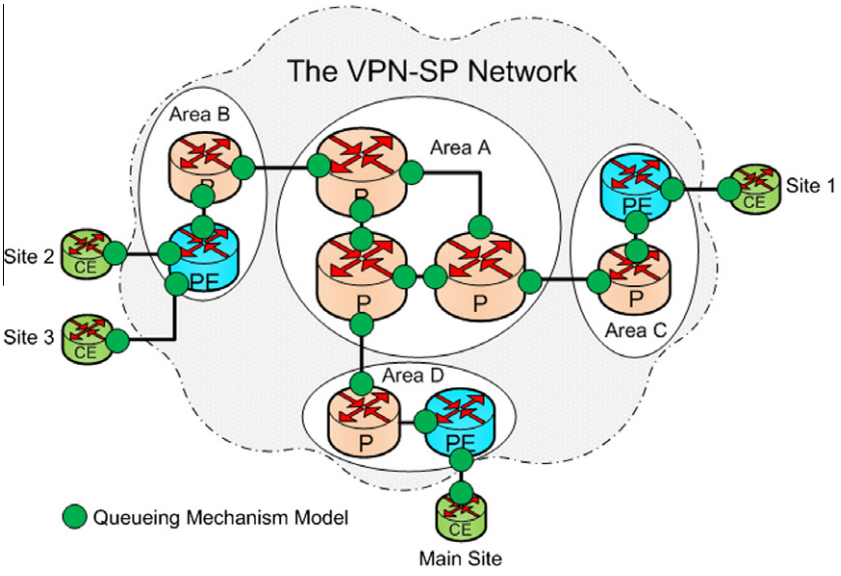

Figure 9 Points of implementation of the queueing mechanisms.

external traffic. The internal data sources were three from each remote site and five external data sources.

5.1. Effects of the number of channel calls

In the first set of experiments, the effects of the voice traffic on the VPN-SP's network was studied by increasing the number of voice calls, initiated from site 1 and going to the main site, from 1 to 7 channel calls. The same experiment was repeated using the proposed five queueing policies. The main focus will be on the traffic flowing from site 1 to the main site, including voice, video, and data.

5.1.1. Effects on voice traffic

Fig. 10 shows the percentage of voice packets with delay exceeding the maximum limit of 200 ms. The results obtained when using the PQ and LLQ mechanisms were the best and were very similar. This is due to the fact that with these mechanisms, voice was given the highest priority, and thus received a privileged service.

The CQ 20-30-50 mechanism was able to handle up to four voice calls by keeping the dropping rate less than 5%, as set in Table 1. In the case of the CQ 10-20-70 policy, the network barely handled one call. However, in both cases, the results were worse than the ones achieved with PQ and LLQ due to the fact that only a fraction of the voice traffic was served with the highest priority. This is confirmed by remarking that the 20% scheme had a performance advantage over the 10% scheme since it had a higher share of its traffic privileged.

Lastly, the FQ mechanism was not able to handle even one call, since there was no priority mechanism implemented. Also, we noticed that the performance trend was almost constant with PQ and LLQ mechanisms, since voice was given the highest priority. With all other mechanisms, it deteriorated rapidly after a certain number of calls, because there was not enough priority provided.

5.1.2. Effects on video traffic

In the next experiment, as the voice traffic was increased, its effect on the dropping rate of video traffic, exceeding 250 ms, was recorded in Fig. 11. The performance of video traffic was kept very close to the required bound with the best performance achieved through the CQ 20-30-50 and FQ mechanisms, with a slight advantage of the latter over the former. In the case of the LLQ and PQ mechanisms, the video traffic performance was kept acceptable up to four voice calls, and deteriorated very quickly afterwards. Lastly, for the CQ 10-20-70 mechanism, although the performance was kept almost constant, it was very far from the required limit.

These results were in accordance with the fact that video traffic has the second priority in the LLQ and PQ mechanisms. Thus video traffic performance was the best when the first priority traffic (i.e., voice) was comparatively low (< 5 sources). As the first priority traffic was increased, all lower priority traffic suffered. In the case of the other mechanisms, the share of the video traffic was not affected by the increase in voice traffic.

Furthermore, it was noticed also that the CQ mechanisms had better performance than the FQ mechanism, since they used some form of priority service for video. Additionally, the 30% CQ case performed better than the 20% one, although the voice share was also decreased from 20% to 10%. Also, the performance of FQ was the worst in all cases, although prior to 4 voice calls, it was similar to the performance of the other mechanisms.

5.1.3. Effects on data traffic

Fig. 12 shows the retransmission rate of data traffic as the voice traffic was increased. The best performance was achieved through the CQ 10-20-70, CQ 20-30-50, and FQ; the former was the best and the latter was the worst. In the three cases, the results were kept almost constant, in accordance with a non-prioritized mechanism or partially prioritized ones. Here also, the mechanism that allowed 70% of the data traffic to

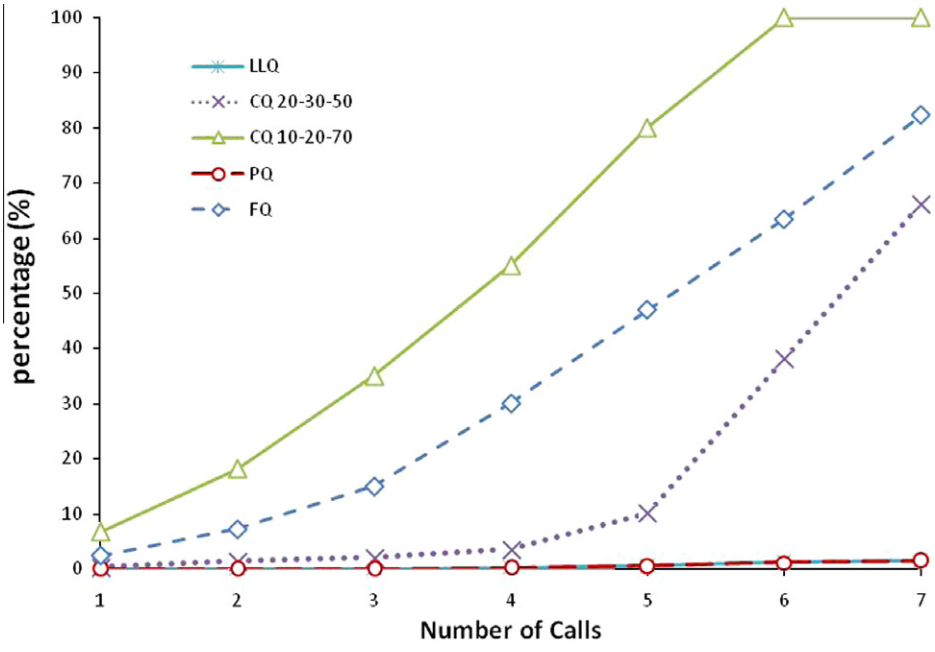

Figure 10 Percentage of voice packets with delay over 200 ms.

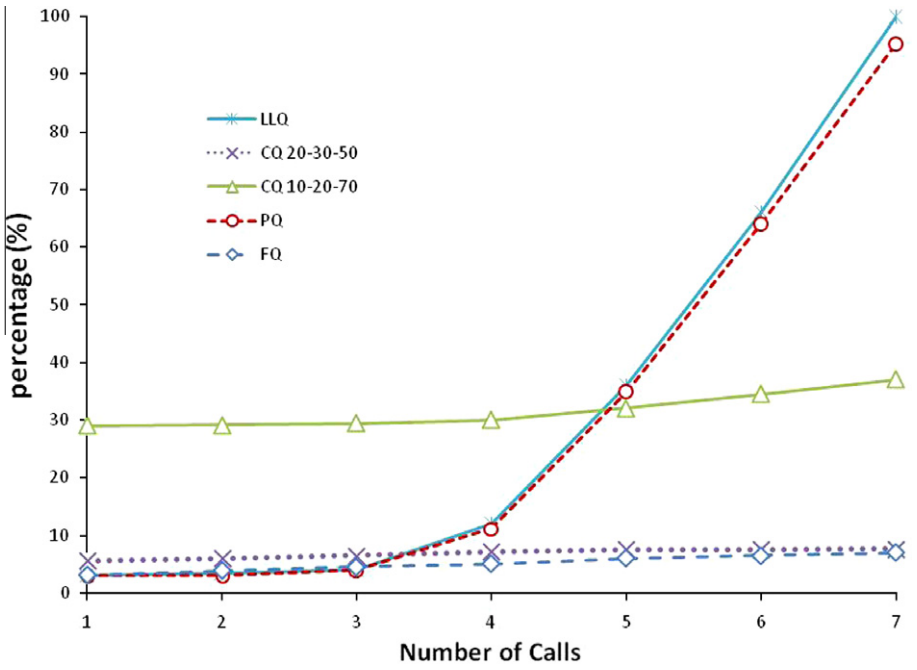

Figure 11 Percentage of video packets with delay over 250 ms.

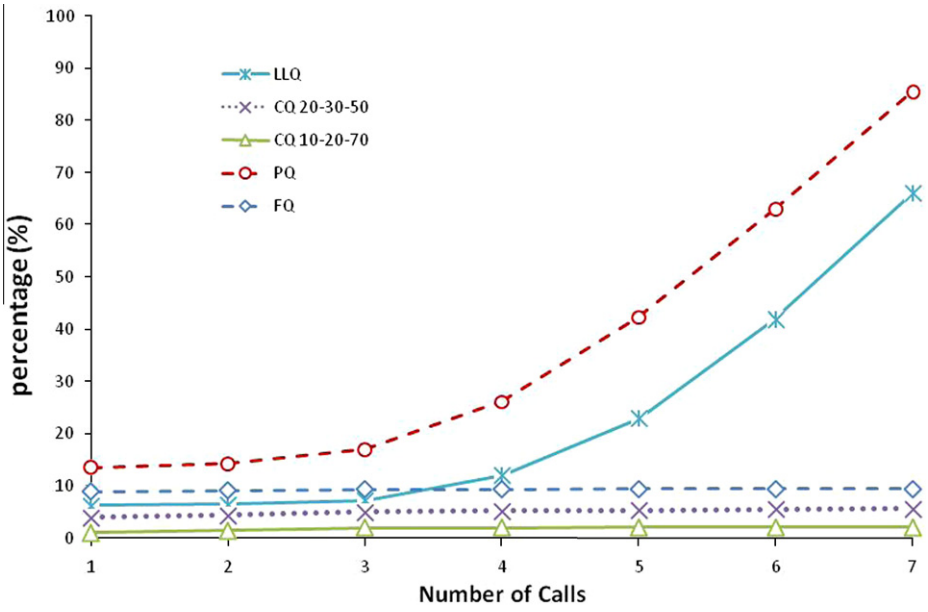

Figure 12 Percentage of data packets being resent.

be served as a third priority performed better than the one allowing only 50%.

In the case of LLQ and PQ mechanisms, the performance was kept constant up to three calls, and then increased rapidly for both of them. However, with the difference that in the case of LLQ the performance was acceptable before the three calls knee, while that of PQ was unacceptable in all cases. This trend was similar to the video traffic case results, but with a much larger gap in favor of LLQ.

5.2. Effects of last-mile bandwidth

In the second part of the experiment, we wanted to study the effects of the last-mile bandwidth. It is the channel capacity of the link connecting the CE router to the PE router at the main site; it is expected to be the bottleneck for the customer's traffic behavior in the VPN-SP's network.

Its effects will be studied by increasing the capacity of the link from 128 Kbps to 8 Mbps. Here also, the five different

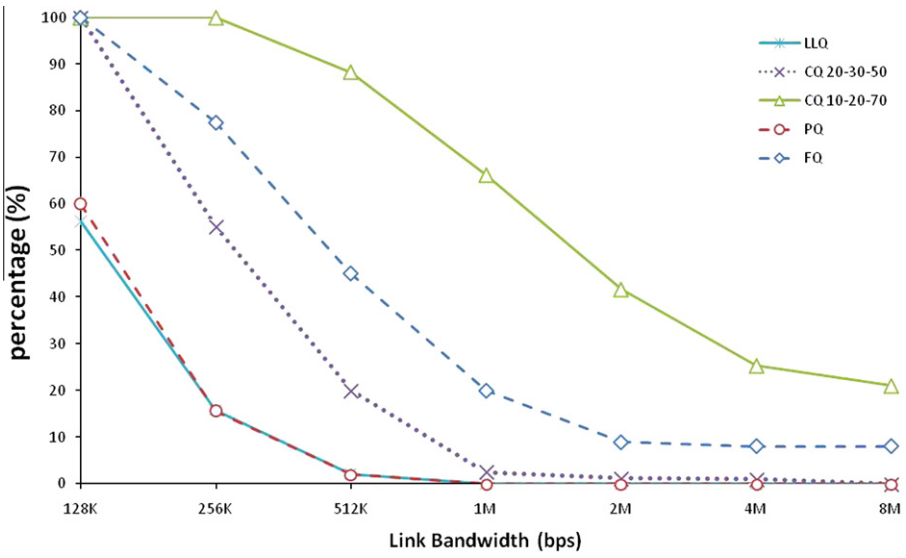

Figure 13 Percentage of voice packets with delay over 200 ms.

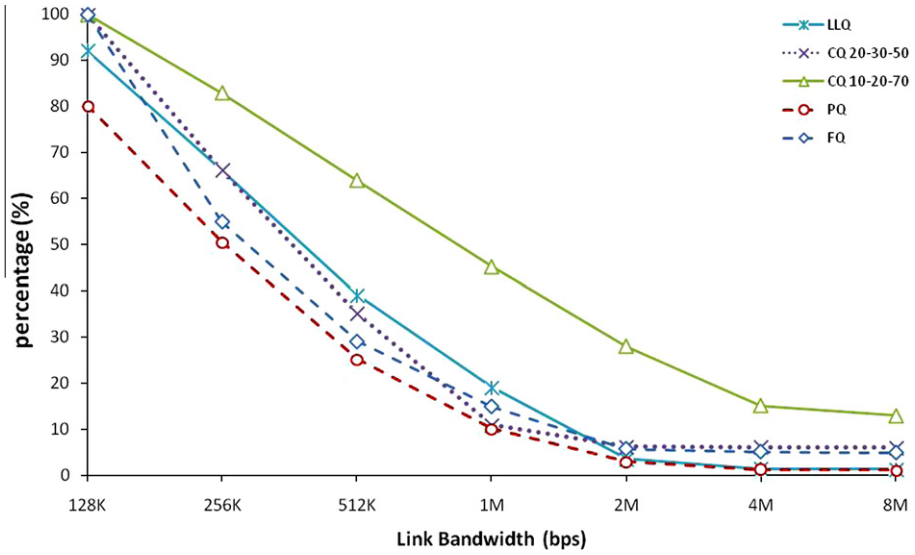

Figure 14 Percentage of video packets with delay over 250 ms.

queueing mechanisms will be tested, and the performance of the voice, video, and data traffic from site 1 to the main site will be monitored.

5.2.1. Effects on voice traffic

Fig. 13 shows the dropping rate for the voice traffic that exceeded a 200 ms delay as a function of the last-mile bandwidth and for the various queueing mechanisms. In all cases the dropping rate decreases as more bandwidth was made available at the bottleneck link. The same relative performances were obtained as in Fig. 9.

The LLQ and PQ mechanisms achieved acceptable performance for bandwidths larger than 512 Kbps, the CQ 20-30-50 mechanism required at least 1 Mbps, while FQ and CQ 10-20-70 failed for all bandwidths.

5.2.2. Effects on video traffic

Fig. 14 shows the dropping rate for the video traffic as a function of the last-mile bandwidth. The CQ 10-20-70 mechanism had a poor performance for all bandwidth values, while the remaining mechanisms had very close performance, with a bandwidth requirement of at least 2 Mbps. The PQ mechanism achieved the best performance for all bandwidths.

5.2.3. Effects on data traffic

Fig. 15 shows the retransmission rate of data traffic as a function of the last-mile bandwidth. The minimum required bandwidths for acceptable data traffic performance were summarized in Table 2. The two CQ mechanisms achieved the best performance, with a noticeable advantage of CQ 10-20-70, which had a larger fraction reserved for data (70%); this was true for all bandwidth values.

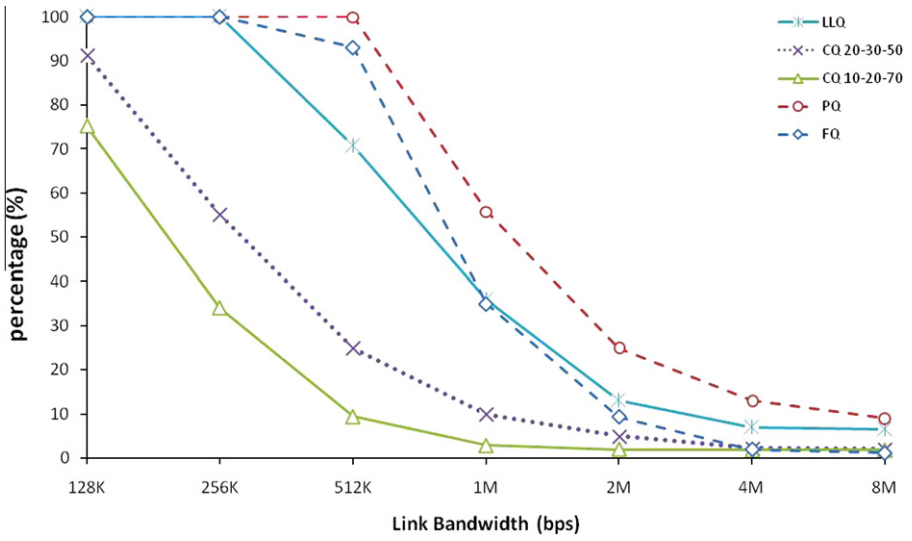

Figure 15 Percentage of data packets being resent.

Table 2 Minimum bandwidth for acceptable data packets resent.

Mechanism	PQ	FQ	LLQ	CQ20-30-50	CQ10-20-70
BW_{min} (Mbps)	8	4	4	1	0.512

The PQ mechanism, which gives data traffic the least priority, achieved the worst performance. With high bandwidths, the FQ mechanism reaches the same level of performance as the CQ mechanisms.

6. Conclusion

In this paper, we have considered a large VPN-SP network providing service to a customer with four remote sites. A simulation model was built with real traffic input. Various queueing policies were suggested and tested with the QoS performance of the various traffic streams being observed. The four queuing mechanisms considered were FQ, PQ, CQ (two versions), and LLQ. Criteria for acceptable performance were set for each carried traffic type which was assumed to be carried over the network.

As a result, an estimation of the impact of a new voice call on the performance of the other traffic types being carried over the network was quantified. Consequently, it was possible to determine the limitation on the number of calls in each customer's sites. As a general rule, it may be concluded that the priority-based schemes PQ and LLQ may be used when the number of high priority voice sources is low. When the number of high-priority sources increases, it becomes necessary to use the other schemes, as a sort of starvation happening to the other low-priority sources. The CQ schemes may also be a viable alternative for a larger number of voice sources, but there has to be a balance between the weight assigned to the class of the traffic and the number of carried sources: as the number of sources increases the corresponding weight has also to increase.

Finally, we varied the bandwidth of the last-mile link located at the customer's main site, given that it was considered as the main bottleneck to the traffic being carried. Consequently, it was possible to advise the service provider whether or not to increase the bandwidth of the last-mile link at the main site if the need for accepting more customers of certain type may arise. This is a second alternative for achieving the QoS requirements for the high priority traffic if the corresponding number of sources increase and the priority scheme cannot add any improvements.

To conclude, as the number of high priority traffic sources increases, it is possible to achieve its required QoS either by requiring more bandwidth at the main site, or by changing the priority scheme at the switching routers in favor of the priority traffic.

References

Bates, T., Chandra, R., Katz, D., Rekhter, Y., 2007. Multiprotocol extensions for BGP-4. RFC 4760, IETF, January 2007, at <http://www.ietf.org/rfc/rfc4760.txt>.

Coding of Moving Pictures and Audio: Overview of the MPEG-4 Standard. ISO/IEC JTC1/SC29/WG11-N4668, March 2002, at <http://mpeg.chiariglione.org/standards/mpeg-4/mpeg-4.htm>.

Dhaini, A.R., Pin-Han, H., Xiaohong, J., 2010. Performance analysis of QoS-aware layer-2 VPNs over fiber-wireless (FiWi) networks. In: IEEE Global Telecommunications Conference (GLOBECOM 2010). December 2010, pp. 1–6.

Duffield, N.G. et al., 2002. Resource management with hoses: point-to-cloud services for virtual private networks. IEEE/ACM Transactions on Networking 10 (5), 679–692.

El Hachimi, M., Breton, M.-A., Bennani, M., Efficient QoS implementation for MPLS VPN. In: International Conference on Advanced Information Networking and Applications. March 2008, pp. 259–263.

Girish, M., Yu, J., Soon, T., 2003. A QoS specification proposal for IP virtual private networks. In: IEEE Workshop on IP Operations and Management. October 2003, pp. 85–90.

Hassan, H., Garcia, J.M., Bockstal, C., 2006. Aggregate traffic models for VoIP applications. In: IEEE International Conference on Digital, Telecommunications. August 2006, p. 70.

Jialei, W., Yuanping, Z., 2010. A layered MPLS network architecture. In: 6th International Conference on Wireless Communications Networking and Mobile Computing (WiCOM). September 2010, pp. 1–4.

Kumar, P., Dhanakoti, N., Gopalan, S., Sridhar, V., 2004. CoS based resource allocation (CBRA) in VPNs over MPLS. In: IEEE Workshop on IP Operations and Management. pp. 140–145.

Low latency Queueing. Cisco IOS Release 12.0(7)T, at <http://www.cisco.com/en/US/docs/ios/12_0t/12_0t7/feature/guide/pqcbwfq.pdf>.

Luyuan, F., Bita, N., Le Roux, J.-L., Miles, J., 2005. Interprovider IP-MPLS services: requirements, implementations, and challenges. Ieee Communications Magazine 43 (6), 119–128.

Rahimi, M., Hashim, H., Rahman, R.A., 2009. Implementation of quality of service (QoS) in multi protocol label switching (MPLS) networks. In: 5th International Colloquium on Signal Processing and Its Applications. March 2009, pp. 98–103.

Rekhter, Y., Li, T., Hares, S., 2006. A border gateway protocol 4 (BGP-4). RFC 4271, IETF, January 2006, at <http://www.ietf.org/rfc/rfc4271>.

Saika, A., El Kouch, R., Bellafkih, M., Raouyane, B., 2011. Functioning and management of MPLS/QOS in the IMS architecture. In: International Conference on Multimedia Computing and Systems (ICMCS). April 2011, pp. 1–9.

Tran Cong, H., Le Quoc, C., Tran Thi Thuy, M., 2010. A study on any transport over MPLS (AToM). In: The 12th International Conference on Advanced Communication Technology (ICACT). February 2010, pp. 64–70.

Understanding Delay in Packet Voice Networks. Cisco Press, July 2008, at <http://www.cisco.com/application/pdf/paws/5125/delay-details.pdf>.

VoIP: An In-Depth Analysis, 2006. In: Bhatia, M., Davidson, J., Kalidindi, S., Mukherjee, S., Peters, J. (Eds.), Chapter in Voice over IP Fundamentals. Cisco Press.

Zeng, J., Ansari, N., 2003. Toward IP virtual private network quality of service. A service provider perspective. IEEE Communications Magazine 41 (4), 113–119.