REVISTA MEXICANA DE INGENIERÍA BIOMÉDICA
SOMIB

ARTÍCULO DE INVESTIGACIÓN ORIGINAL

Vol. XXVIII, Núm. 2
Diciembre 2007
pp 62 - 69

A network and data link layer design to improve QoS for voice and video in telesurgery

Jesús Arturo Pérez Díaz,*
Víctor Hugo Zárate,*
Christian Cabrera Roselló*

* Department of Electronics, ITESM - Campus Cuernavaca. Temixco, Morelos, 62589 México.

Correspondencia:
Jesús Arturo Pérez Díaz
jesus.arturo.perez@itesm.mx

Artículo recibido: 26/Abril/2006
Artículo aceptado: 25/septiembre/2007

ABSTRACT

The feasibility and practicability of performing telesurgery depend not only on the ability to overcome the barriers of surgery, but also on the ability to transmit data rapidly and securely. Telecommunications designers for telesurgery have focused in the transoceanic WAN links. However, if the WAN link is good enough but the Autonomous System (AS) Network to which the destination hospital belongs doesn't have the proper configuration; applications running on top could have a very poor performance. This paper presents a network and data link layer infrastructure design that classifies and prioritizes voice and video traffic in order to improve the performance and QoS of telesurgery applications. This infrastructure has been designed taking into consideration a typical AS network, like the one at which end hospitals could connect. In this way, this model can be implemented in any hospital or autonomous system. After implementing it, we ran some tests inside a network laboratory which demonstrated an improvement greater than 75% in any kind of traffic transmission. This rate is enough to perform telesurgery and any real time application that uses voice and video.

Key Words: Telesurgery, QoS, VoIP and videoconference.

RESUMEN

La factibilidad y practicidad de realizar una telecirugía depende no sólo de la habilidad de superar las barreras de la cirugía, sino también de la habilidad de transmitir datos rápidamente y de forma segura. Los diseñadores de telecomunicaciones para telecirugías se han enfocado en los enlaces WAN transoceánicos. Sin embargo, aunque el enlace WAN sea bueno pero la red del Sistema Autónomo a la cual pertenece el hospital destino no tiene las configuraciones apropiadas, entonces las aplicaciones que se ejecuten por encima podrían tener un desempeño muy pobre. Este artículo presenta un diseño de una infraestructura de cada red y de enlace de datos que clasifica y prioriza el tráfico de voz y video con el fin de mejorar el desempeño y la QoS de las aplicaciones de telecirugía. Esta infraestructura ha sido diseñada tomando en consideración una red típica de un Sistema Autónomo, como a la que los hospitales podrían estar conectados. De esta manera, este modelo puede ser implementado en cualquier hospital o Sistema Autónomo. Después de implementarlo, corrimos algunas pruebas en una red de laboratorio las cuales demostraron una mejora superior al 75% en cualquier tipo de transmisión de tráfico. Este porcentaje es suficiente para ejecutar una telecirugía y cualquier aplicación en tiempo real que use voz y video.

Palabras clave: Telecirugía, QoS, VoIP y videoconferencia.

1. INTRODUCTION

The telesurgery, or surgery at distance, is a technique which allows surgeons to robotically operate on a patient while being at a considerable distance. Telesurgery has been made possible by extraordinary advances in the fields of robotics and telecommunications and has the potential to revolutionize healthcare delivery in the near future[1]. In February 2001, an unprecedented feat was performed: the "Operation Lindbergh", which became the first telesurgery in the world. The success of the operation as well as the technological infrastructure set in place highlighted major developments in the field of telemedicine, particularly in telesurgery.

One of the most important and limiting factors in telesurgery is the delay while transferring data from the surgeon to the robot. Preliminary studies estimate the maximum time delay compatible with safe performance of surgical manipulations at about 300 ms[2]. During the first telesurgery, this delay was reduced to less than 200 milliseconds. Switch speed data transfer was made possible by a high-speed data transmission system linking the equipment with a transatlantic high bandwidth fiber-optic service running at 10 Mbits per second[3]. The France Telecom deployment was successful at five levels, the surgeon's actions via robot and data transmissions, voice using VoIP, the surgeon's eyes, using the endoscopic camera and the video monitor, a videoconference to coordinate the two rooms and continuous control data exchanged between two PCs at each end[4]. These different kinds of traffic required different kinds of QoS and treatment. Another important consideration is that all the considerations to improve the traffic's QoS had been applied to the transatlantic links, without considering the WANs links inside the AS to which hospitals belong.

Once the transatlantic communications become more popular and cheaper, the improvement of the WAN links which connect hospitals will be required in order to deploy more than one telesurgery at the same time. In this paper, we propose a model to improve the voice, video or any specific traffic needed to deploy a telesurgery. We focus on a network and data link layer design which prioritizes any kind of traffic, allowing us to provide the proper and specific QoS level to any of the five levels demanded in a telesurgery like the one that was described in the paragraph above.

In our tests, we considered videoconference traffic which is the most demanded traffic used in the telesurgery.

2. VIDEO AND VOICE REQUIREMENTS

The audio/video information within a videoconference is segmented into chunks by the application, encoded and compressed, put into a series of data packets and sent over the network to the remote end at basically constant intervals. The data packets may arrive at their destination at slightly varying times, possibly out of order and some of them can be lost. To keep the "real time" impression of an interactive videoconference, the packets must arrive, on time and in time to be re-ordered for delivery through the videoconferencing terminal.

Before showing how to improve the performance of the networks of an autonomous system it is important to involve the five fundamentals network problems for videoconferencing and for the transmission of voice over IP (VoIP)[5].

1. **Bandwidth** is the fundamental requirement that there be enough space in a network path for all of the packets to get through unimpeded. This bandwidth need is symmetric-each end will transmit and receive this amount of traffic.
2. **Packet loss** is the amount of packets that does not arrive correctly to their destination. This is due to insufficient bandwidth or transmission errors. The packet loss percentage must always be below 1% for voice and 2% for video.
3. **Latency** is the time delay between an event occurring on one site and the remote end seeing it. Latency is introduced both by the encoding/decoding process, and hence depends on the equipment used, and also by the time it takes packets to traverse the network. A disruption in the image can cause a bad playing in the destination, but a disruption in the voice is more important since it makes the transmission not under-

standable, so it is considered that the biggest latency allowed in the voice transmission to keep a good quality is around 150 ms.

4. **Jitter** is the time variation among each packet that is received at the destination. Sometimes, this result in packets arriving in a different order than the transmitted one, which gives uneven and unpredictable quality within a videoconference, increasing the latency even further. Jitter should always be below 50 ms.
5. **Policies** are introduced by things like firewalls and network address translation (NAT) devices that are generally used to try to hide or protect network elements from the wider Internet.

Some other aspects must be considered if the traffic is encrypted[6], but in this work we are considering that the network of the autonomous system where the designed infrastructure is going to be implemented has enough bandwidth for voice and video traffic and no firewalls. We will focus on creating a configuration to minimize the packet loss, latency and jitter for videoconference traffic.

3. AN EFFICIENT NETWORK AND DATA LINK LAYER

In order to maintain the high standards that modern applications and telesurgery require, traffic should always follow a prioritization scheme in order to guarantee specific bandwidth requirements from real time communications, such as voice and video. This scheme can be represented in the form of a general model which applies to all applications which require special conditions (such as maximum delay) to be met. This general model is represented in Figure 1.

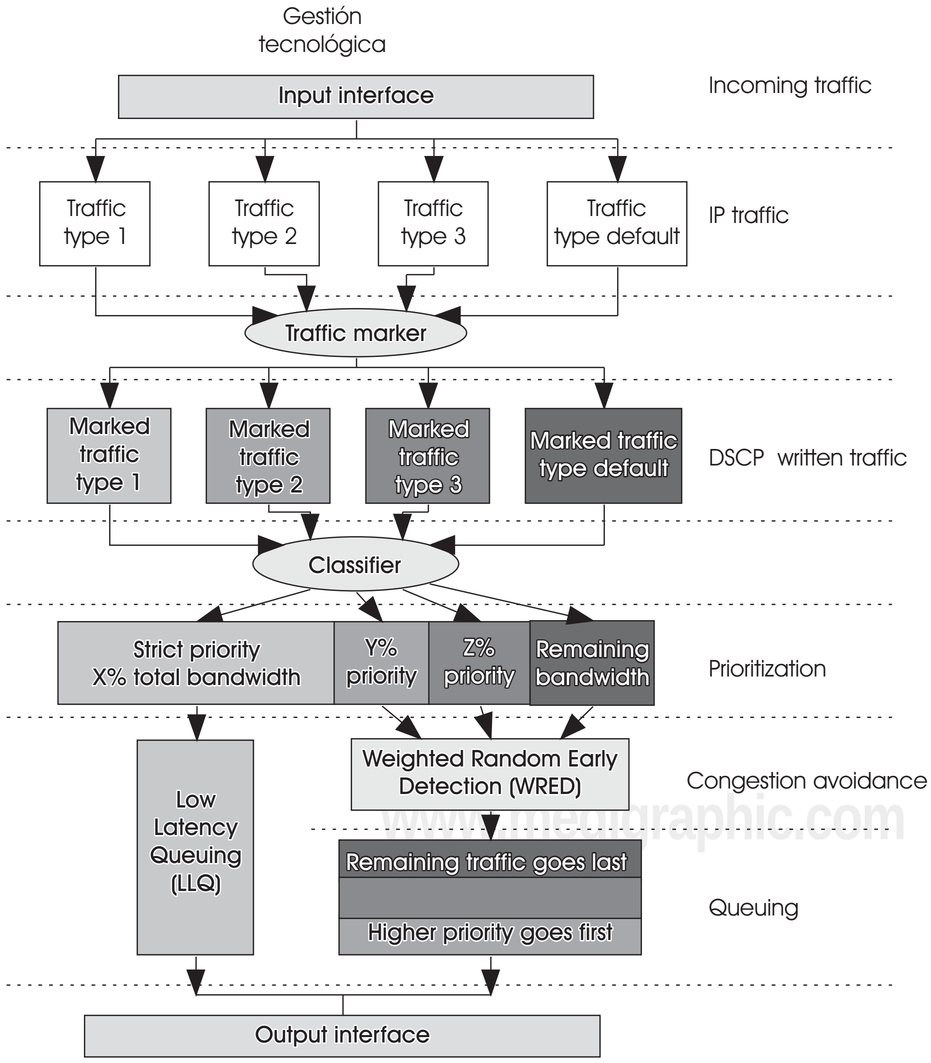

Figure 1. General model for prioritizing network traffic.

After receiving the IP traffic, the first step would be to mark the incoming frames/packets according to our needs. This marking should be done in the way of traffic *classes*. A different class should be specified for every kind of traffic which should be treated in different way. A common practice is to classify the voice and video traffic in its own class, away from any other type that might cause delays in the processing of the real time data.

After traffic has been marked, it is ready to be classified according to our own requirements. Since voice and video are the most delay sensitive type of data, they should receive a special treatment in order to avoid delay at all costs. Any other type would be considered as delay tolerant and so, it would be subject of further processing in order to provide the bandwidth only to those applications that do really need it.

The most important traffic class should receive a *strict priority* using Low Latency Queuing (LLQ). LLQ provides to the traffic the ability to skip directly to the output interface without having to deal with any congestion avoidance, reducing its time to go out from the router. By also specifying a reasonable amount of the total bandwidth, we will be guaranteeing that this type of traffic always has the resources it needs for proper functioning.

As it is shown in the general model, the rest of the traffic classes must go through WRED congestion avoidance mechanisms and queuing. This process would divide the remaining bandwidth according to the specific policies configured for each data class.

Once all conditions are met and all the policies are applied, the now marked and prioritized is sent through the router's outgoing interface to its destination.

Now that we have shown the general model, we will describe in detail what we propose to improve the performance in each layer of our model.

3.1 IMPROVING DATA LINK LAYER

A shared LAN (using hubs) divides the bandwidth between all the available users, so on average we get much less of the nominal bandwidth, plus increasing the risk of packet loss and jitter due to collisions, while a switched network allows full duplex transmission by using microsegmentation. This totally avoids collisions and provides the highest possible available bandwidth for each of the devices connected to the switch. As additional enhancements, switches open up the possibility of using VLANs for increasing security and reducing broadcast domains, while also allowing the use of trunk interfaces for extending the availability of ports for other medical devices.

In order to improve the performance in the switched network, at layer two, we need to configure in the switches their switch mode operation and traffic prioritization with 802.1p.

3.1.1 SWITCH MODE OPERATION

The way a frame is switched from its source port to its destination is a trade off between latency and reliability. A switch can start to transfer the frame as soon as the destination MAC address is received. This switching method is called cut-through and results in the lowest latency through the switch. However, no error checking is available, but considering the type of application, it is more important to transfer frames faster than to lose some frames. So the switch network infrastructure must support cut-through mode instead of store and forward (or fragment-free modes). The switch cut-through command must be entered for each of the switch's port where cut-through mode should be used.

3.1.2 TRAFFIC PRIORITIZATION WITH 802.1P.

If VLANs are used inside the campus and the traffic is sent among users belonging to the same VLAN, then the traffic will never go through any router interface, meaning there will be no need to prioritize the traffic with layer 3 policies. For this reason we need to add layer 2 priorities to our designed infrastructure.

The IEEE 802.1p is an extension of the IEEE 802.1q (VLANs tagging) standard. The 802.1q standard specifies a tag that appends to an Ethernet MAC frame. This tag has two parts: the VLAN ID (12-bit) and Prioritization (3-bit). The prioritization field was neither defined nor used in the 802.1q VLAN standard, so 802.1p defines this prioritization field.

The 802.1p header also includes a three-bit field for prioritization, which allows packets to be grouped into various traffic classes. 802.1p traffic is simply classified and sent to the destination; no bandwidth reservations are established.

IEEE 802.1p establishes eight levels of priority, being 7 the highest priority and 0 the best-effort (lowest) priority available. The zero value is used as a best-effort default, invoked automatically when no other value has been set. These eight levels provide the marking that should be used according to the general model (Figure 1) when layer 2 QoS is required.

However, hardware must support this feature in order to work.

3.2 IMPROVING NETWORK LAYER

When we are willing to provide QoS for traffic that will flow outside of our own LAN, there is the need to specify priorities at layer 3 in order to obtain the desired latency and bandwidth for specific delay sensitive data.

QoS refers to both class of service (CoS) and type of service (ToS). The basic goal of these is to guarantee specific bandwidth and latency for a particular application[7]. To achieve this, we use the Differentiated Services Codepoint (DSCP) field in the packet header to indicate the desired service. This value provides the necessary marking as suggested by the first step of our general model (Figure 1) when dealing with layer 3 traffic.

DSCP redefines the older IPv4 ToS octet and IPv6 traffic class octet. It is composed by the first six bits in the ToS byte, while the IP Precedence value is created with the first three bits in the ToS value. The IP Precedence value is actually part of the IP DSCP value, so both values can not be set simultaneously. If both values are set simultaneously, the DSCP value overwrites the IP precedence one.

The marking of traffic at layers 2 or 3 is crucial to providing QoS within a network, and the decision of whether to mark traffic at any or both of these layers is not trivial. We suggest deciding after the following considerations are made:

- Layer 2 marking can be performed for non IP traffic. This is the only option available for non "IP aware" switches.
- Layer 3 marking will carry the QoS information end-to-end.

We propose to use both DSCP to mark packets through the routed links of the network and also mark the frames using CoS to allow layer 2 devices to provide the QoS requirements of packet at the data link layer.

It is important to mention that a mapping between layer two QoS (CoS) and layer three QoS (DSCP) is possible, as it is presented by Ubik[8]. However, since in this paper we are just trying to improve the QoS inside our Autonomous System, we will only propose tools associated with the network edge.

After marking the packages classification will be needed in order to create different classes of traffic with different priority.

For RTP traffic prioritizing at layer 3 over normal bandwidth WAN circuits, our general model proposes the use of Low Latency Queuing (LLQ) to give absolute priority to voice and video traffic over any other traffic over an interface.

LLQ was designed for being used in realtime applications, such as a videoconference. It brings strict Priority Queuing (PQ) to CBWFQ. Strict PQ allows delay-sensitive data such as voice to be sent directly through the outgoing interface before packets in other queues are sent (as shown in Figure 1). Without LLQ, CBWFQ provides WFQ based on defined classes with no strict priority queue available for real-time traffic. For CBWFQ, all packets are serviced fairly based on weight and no class of packets may be granted strict priority. This scheme poses problems for voice traffic that is largely delay intolerant, especially delay variation. For voice traffic, variations in delay introduce irregularities of transmission becoming evident as a jitter in the heard conversation. LLQ provides strict priority queuing for CBWFQ, reducing jitter in voice conversations.

To configure LLQ priority to a class within a policy map, we need to define a class to match the desired traffic. After this, a policy must be created to specify the allowed bandwidth for each class. As an example:

```
R1(config)# class-map match-any VoiceTraffic
R1(config-cmap)# match protocol rtp audio
R1(config-cmap)# match protocol rtp video

R1(config)#policy-map StrictPriority
R1(config-pmap)#class VoiceTraffic
R1(config-pmap-c)#strict priority 128
R1(config-pmap-c)#class class-default
R1(config-pmap-c)#fair-queue
```

This would create a class named VoiceTraffic which matches any rtp audio or video packet. Then, the policy would give it a 128kbits bandwidth while also setting the fair-queue as queuing scheme for any other kind of traffic.

When LLQ is not possible to configure, CBWFQ is the best solution, since we can create a specific class and then assign a specific bandwidth that will be enough to guarantee the QoS of the voice traffic. In the following configuration we assign 50% of the bandwidth for the traffic matched by the VoiceTraffic class.

```
Router(config)#policy-map priorityCBWFQ
Router(config-pmap)#class class-default
Router(config-pmap-c)#random-detect
Router(config-pmap-c)#class VoiceTraffic
Router(config-pmap-c)#priority percent 50
```

It is important to show that we also propose (see figure 1) to include a congestion avoidance technique for the rest of the traffic, Weighted Random Early Detection (WRED) with CBWFQ. With the *random-detect* command we activate WRED, the net result being that the highest priority and lowest bandwidth traffic is preserved, since it starts to drop less important packets once that the net starts to be congested. WRED allows the link to be used more efficiently by selectively dropping packets according to its importance (more packets of lower priority are dropped more than the ones from high priority).

Following the designed rules that we have previously explained in our WAN Links, creating and prioritizing specific classes will have an important performance improvement.

4. EXPERIMENTS AND TESTS

The aim of this section is to show the performance improvement that an Autonomous System LAN will have after these procedures are followed.

First, we will deploy a network infrastructure using a default configuration (without any kind of priority neither for voice nor video traffic). After that, we will configure the routers with the design model that we proposed in the previous section. We will compare results to determine the level of performance improvement obtained with the proposed network design.

The proposed network topology for system consists on 3 Catalyst 2600 series routers connected through their serial interfaces configured at a 2 Mb/s link speed (simulating an E1 connection). Each of the two edge routers is connected through their fast ethernet interface with a Catalyst 2900 series switch. These switches connect through 2 more switches by using their gigabit ethernet trunk interfaces. Finally, the corresponding hubs and hosts are connected into these, just as it is pointed out in Figure 2.

For each tested scenario we will measure the packets loss, delay and jitter. Some scenarios will measure layer 2 configurations, while some other will test the layer 2 and layer 3 ones.

Used IP Addresses:

R1 Fa0.0 : 192.168.3.1	Trafico1 : 192.168.3.20
R1 S0 : 192.168.1.1	Traffic 2 : 192.168.4.20
R2 S1 : 192.168.1.2	Sniffer NIC1 : 192.168.3.10
R2 S0 : 192.168.2.1	Sniffer NIC2 : 192.168.4.10.
R3 Fa0.0 : 192.168.4.1	Vigo 1 : 192.168.3.15
R3 S1 : 192.168.2.2	Vigo 2 : 192.168.4.15

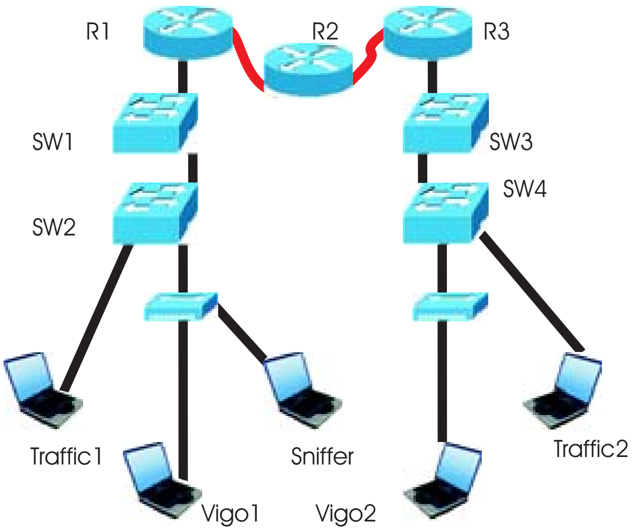

Figure 2. Scenario network topology.

We will use Vigo videoconference equipment in each end point of the network, while having some other clients generating traffic from protocols like ftp, http, etc. Some other computers will use special software to flood the network with random packets in order to simulate a real scenario. The test for each scenario consists on keeping a videoconference open between two end points of the network while traffic is also being transmitted. We will perform the test of each scenario with and without voice priority configurations so that we can measure the improvement percentage.

4.1 ENDPOINTS INSIDE THE SAME NETWORK – LAYER 2 PRIORITY

The first and simplest scenario describes the typical LAN created only by switches. In our simulation, 2 Cisco Catalyst 2950 switches were connected through their Gigabit Ethernet trunk interfaces. For testing, one 3Com 10/100 hub was connected to the Fa0/0 of each of the switches, while also using a traffic generator laptop plugged into the Fa0/1 port of each switch. Both a Vigo videoconference laptop and a 2 NIC sniffer were connected to each of the hubs.

A videoconference was established between the 2 Vigo enabled laptops while also injecting traffic from the laptops connected through the Fa0/1 port. All traffic between switches will be exchanged through the Gb Ethernet trunk interfaces.

The tests ran in our simulated network showed up some slight improvements after applying QoS settings. The results were small due to the fact that our layer 2 equipment is able to switch great amounts of data in a very short time, thanks to its fast Ethernet and gigabit Ethernet interfaces. This points out that our attention should be focused into improving the layer 3 prioritization.

4.2 ENDPOINTS IN DIFFERENT NETWORKS – LAYER 3 PRIORITY

In this scenario, the end points are located in different networks, so the traffic will have to go through the router's serial interfaces. In this way we will just evaluate the layer 3 priority. The proposed network topology can be observed at Figure 2.

For this scheme, there are 2 types of router configurations that should be noted. We will refer to them as the *edge routers* and the *middle routers*, being the edge routers the ones that are in direct connection to the switches and the middle routers the ones that only use their serial links to communicate the rest of the routers between themselves.

The configuration steps used were as follows:

EDGE ROUTERS

1. Create a class to identify all the RTP traffic from the voice and video kind
2. Create all the other classes required to identify the rest of the traffic, such as HTTP, FTP, etc.
3. Create a marking policy which sets the IP DSCP value of the voice and video class.
4. Create a prioritization policy defining the amount of bandwidth to be provided to each of the classes.
5. Apply the marking policy to the incoming traffic from the fast Ethernet interface being used.
6. Apply the prioritization policy to the outgoing traffic from the Serial interface connecting to the next router, applying also WRED a congestion avoidance technique.

MIDDLE ROUTERS

1. Create a class to identify the RTP traffic from its IP DSCP value.
2. Create all the other classes required to identify the rest of the traffic, such as HTTP, FTP, etc.
3. Create a prioritization policy defining the amount of bandwidth to be provided to each of the classes. This policy has to match the one created in the edge routers.
4. Apply the prioritization policy to the outgoing traffic from both serial interfaces, applying also WRED a congestion avoidance technique.

By following the previous steps, we will be successfully marking and prioritizing our traffic through all of our routers. It is important to note that the policies must remain equal through all routers to maintain consistency.

After applying this configuration, the sniffer laptop was set to capture and measure the time differences for a 1-way throughput. The following chart shows the differences when applying the commands shown above:

	Total packets	Average delay (ms)	Jitter (ms)
Voice (No QoS)	686	27.910	60.870
Voice (QoS)	705	12.036	60.401
Benefit (%)		131.880	0.776
Video (No QoS)	2328	31.209	18.610
Video (QoS)	2399	17.671	17.940
Benefit (%)		76.610	3.60

During the tests there were no lost packets at all and, as shown, there is a noticeable improvement in both voice and video (131.88% and 76.61%) after applying the QoS settings. However, let's keep in mind that these results were obtained on a simulated network where lots of traffic was being injected into the fast ethernet interfaces to flow through the serial link, thus forcing the router to apply the prioritization. Under higher data load, the benefits margin would have been even better.

CONCLUSIONS

In this paper we proposed a general guide for enabling QoS inside an autonomous system composed by many routers in order to provide a more suitable environment for real time traffic used in telesurgery. The two created scenarios for simulation of layer 2 and layer 3 infrastructures showed benefits from the implementation of QoS in their policies.

Even though we prioritize the voice and video traffic in our experiments, we can prioritize any kind of the 5 traffic levels required in a telesurgery, in order to prioritize first, the robot manipulation traffic for example.

After running the tests, it's easy to notice the difference between a network with QoS enabled and one without it. The video in both edges appears smoother and the audio is not chopped, no matter what the load in the routers is, as long as the specified priority in the policy maps is enough to handle the resources a video conference demand.

When talking about the urgency to implement QoS at layer 2, we do know that this is not so relevant to keep a good quality conference, since layer 2 only involves devices directly attached into our own switched network, thus providing a connection which depends only on our local hardware, usually fast Ethernet devices. Having a Fast Ethernet switched network provides enough bandwidth for all the devices connected to it, so QoS is not so important as long as the link speed remains constant.

However, when dealing with layer 3, many considerations have to be made since we can not control the traffic coming from other sources. Against this, we must follow the propose model in order to prioritize the outgoing/incoming traffic to be sure that the most important data keeps flowing smoothly without congestions. Inside an autonomous system(AS), this article provides the required steps to enable QoS in both incoming and outgoing traffic.

The obtained results are a clear sign of the type of improvement which will be obtained in the target AS where these settings are applied. This AS refers to the final network where one or more hospitals could be connected, enhancing the quality of their communications while allowing for total control of the traffic flowing through it.

With this general configuration model, we can guarantee an optimal performance inside the AS, translating into a direct benefit to the network where the hospital could be connected.

REFERENCES

1. Holt D, Zaidi A, Abramson J. Telesurgery: Advances and Trends. University of Toronto medical journal. Canada.
2. Marescaux J, Rubino F. Telesurgery: Trend including robot assisted technology. Report of European Institute of Telesurgery (EITS). France.
3. Rassweiler J, Binder J, Frede T. Robotic and Telesurgery: will they change our future? Current opinion in Urology. 2001
4. WeBSurg's World Virtual University. Operation Lindbergh: the surgical act crosses the Atlantic. New York – Strasbourg. 2001.
5. Vegesna S. IP Quality of Service, Cisco Press, 2001. ISBN 1-57870-116-3.
6. Pérez DJA, Zárate VH, Montes ACG. Quality of Service analysis of IPSec VPNs for voice and video traffic. IEEE Computer Society and IEEE Xplore Site. Proceedings of the Advanced International Conference on Telecommunication. February 2006. Guadaloupe, France. ISBN: 0-7695-2522-9
7. Burgstahler L et al. Beyond Technology: The Missing Pieces for QoS Success. Proceedings of the ACM SIGCOMM 2003 Workshops, Aug 2003: 121-130.
8. Ubik S, Vojtech J. QoS in Layer 2 Networks with Cisco Catalyst 3350. CESNET Technical Report 3/2003.