A Network and Data Link Layer QoS Model to Improve Traffic Performance

Jesús Arturo Pérez, Victor Hugo Zárate, Christian Cabrera

Department of Electronics
ITESM - Campus Cuernavaca.
Temixco, Morelos, 62589 México
{ jesus.arturo.perez, vzarate, a00375730 }@itesm.mx

Abstract. Currently, there are a lot of e-learning and collaborative platforms to support distance and collaborative learning, however, all of them were designed just like an application without considering the network infrastructure below. Under these circumstances when the platform is installed and runs in a campus, sometimes it has very poor performance. This paper presents a network and data link layer infrastructure design that classifies and prioritizes the voice and video traffic in order to improve the performance and QoS of the collaborative systems applications. This infrastructure has been designed taking in consideration a typical network of a university campus, so that in this way it can be implemented in any campus. After making the design we have made some tests in a laboratory network demonstrating that our design improves 70-130% the performance of these real time collaborative systems which transmit voice and video.

1. Introduction

There are many e-learning applications that support collaborative work; however, this does not imply that they are neither effective nor functional. The mayor issues in those applications are focused in the synchronous collaboration [1] because of the problem of managing the information that flows across the network and the mechanism to ensure the quality of the service [2].

Applications, like “Synergeia” [3], “Synergo” [4] and “Blackboard” [5] do not provide efficient tools to communicate across the internet in a synchronous manner. The problem in this case is the lack of control and management in the underlying protocols to achieve the demanded Quality of Service (QoS). This problem forces the software programmers to only provide tools that do not exhaust the bandwidth of the communication (like chats or shared blackboards).

All the analyzed collaborative systems work properly when they use a chat or an off-line communication like e-mail. However, the performance and success of real time voice and video is conditioned to the performance of the network below. In many cases modern networks are fast enough to support these applications [6], but the lack of a proper configuration in routers and switches make the applications suffer from performance issues.

Because synchronous communication is the most difficult to implement [7], we need to provide a designed framework to manage the data flow in order to guarantee the QoS independently of the data type.

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 [8]. The data packets may arrive at their destination at slightly varying times, and possibly out of order. In order to keep the "real time" impression, the packets must arrive on time and in time to be re-ordered for delivery through the videoconferencing terminal.

An efficient solution for solving the previously mentioned issues involves the use of policies to identify, mark and prioritize traffic in order to preserve the required bandwidth and latency that the application demands. After satisfying these requirements, the packet loss and jitter levels should be kept to a minimum so the end user experience receives the best available quality. These considerations apply to delay sensitive traffic, such as voice over IP [9].

In this work we are considering that the network of the Autonomous System (AS) where the designed infrastructure is going to be implemented has enough bandwidth for voice and video traffic. We will focus on creating a configuration to minimize the packet loss, latency and jitter for videoconference traffic.

3. General model for traffic prioritization

Traffic should always follow a prioritization scheme in order to guarantee specific bandwidth requirements from real time communications. This scheme can be represented in the form of a general model which applies to all applications with special conditions (such as maximum delay) to be met. This model is represented in Figure 1.

After receiving the traffic through the incoming interface, the first step would be to mark the incoming frames/packets according to our needs. This should be done using a different traffic class for every kind of traffic with different needs. A common practice is to classify voice and video in its own class, away from any other type.

Next, the traffic should be ready to be classified according to our own requirements. Delay sensitive data should receive a special treatment to avoid delay at all costs. Any other data should be considered as delay tolerant and further processed 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 allows traffic to skip directly to the output interface, reducing its processing time. By specifying a reasonable amount of the total bandwidth, we will be guaranteeing the required resources for this traffic type.

The rest of the classes must go through WRED congestion avoidance mechanisms and queuing (see figure 1). This process would divide the remaining bandwidth according to the policies configured for each data class.

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

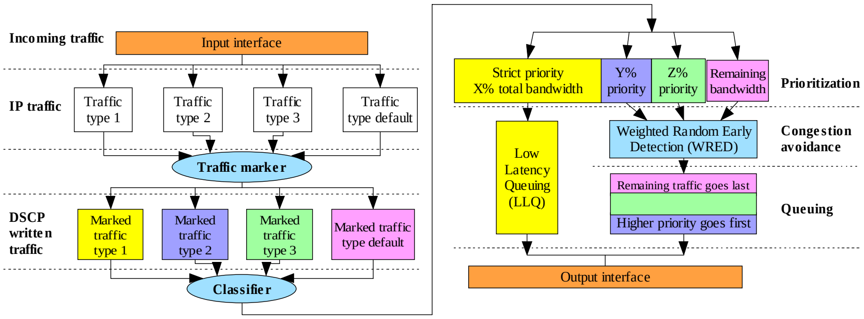

Fig 1. General model for prioritizing network traffic

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

To improve the performance of the network at layer 2, we need to configure the operation mode and traffic prioritization of the switches at the data link layer.

3.1.1 Switch mode Operation. How a frame is switched from the 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 is called *cut-through* and results in the lowest latency through the switch. No error checking is available, but considering the application, it is more important to transfer frames faster than to lose some frames.

3.1.2 Traffic Prioritization with 802.1p. If VLANs are used inside our network and traffic is sent among users of the same VLAN, the traffic will never go past layer 2. 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 VLAN tag has two parts: VLAN ID (12-bit) and Prioritization (3-bit). The prioritization field was not defined in the 802.1Q, but is defined in 802.1p.

VLAN frame tagging is an approach that has been specifically developed for switched communications and gives the possibility of using the prioritization field.

The 802.1p standard also offers provisions to filter multicast traffic to ensure it does not proliferate over layer 2-switched networks. The 802.1p header includes a three-bit field for prioritization, which allows packets to be grouped into various traffic classes. It can also be defined as best-effort QoS (Quality of Service) or CoS (Class of Service) at Layer 2 and can be implemented in network adapters and switches without involving any reservation setup. 802.1p traffic is simply classified and sent to the destination; no bandwidth reservations are established.

IEEE 802.1p establishes eight levels of priority. The highest priority is seven, which might go to network-critical traffic like Open Shortest Path First (OSPF) table updates. Values five and six may be used for delay-sensitive applications such as interactive video and voice. Data classes four through one range from controlled-load applications such as streaming multimedia and business-critical traffic - carrying SAP data, for instance - down to "loss eligible" traffic. The zero value is used as a best-effort default, invoked automatically when no other value has been set.

Using the described datagram fields will create a faster infrastructure in the data link layer. This is sometimes described as "layer 2 quality of service".

3.2 Improving network layer

When willing to provide QoS for traffic that will flow outside our LAN, we need to specify layer 3 priorities to obtain the desired latency and bandwidth.

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 [10]. To achieve this, we use the Differentiated Services Codepoint (DSCP) or the IP Precedence field in the packet header. These values provide the necessary marking as suggested by the first step of our general model (Figure 1) for layer 3 traffic.

DSCP is composed by the first six bits in the ToS byte, while the IP Precedence 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. We suggest deciding at which layer to mark after considering the following:

- 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 and use CoS to mark frames to allow layer 2 devices to provide the QoS requirements of frames at the data link layer.

A mapping between layer two CoS and layer three QoS (DSCP) is possible, as presented by Ubik [11] However, since we are just trying to improve QoS inside our Autonomous System, we will only propose tools associated with the network edge.

After completing the marking stage, classification will be needed to create different classes of traffic with different priorities.

3.2.1 Low bandwidth WAN circuits. If any low speed connections exist in the network, and a high portion of the traffic is RTP, the most proper protocol to use is the Compressed Real Time Transport Protocol (cRTP) which reduces the consumed bandwidth by compressing the IP/RTP/UDP headers.

With cRTP the required bandwidth for a G729A VoIP call is reduced to approximately 50%. In this way, it is possible to double the amount of simultaneous calls in one link. cRTP is not required to ensure good voice quality, but rather a feature that reduces bandwidth consumption. cRTP must be configured on both ends of the link.

By default with G.729, two 10-ms speech samples are put into one frame [12]. This creates a packet every 20 ms, so a VoIP packet can be transmitted every 20 ms.

Blocking directly affects the delay budget, so it is always desirable to keep the blocking delay at 80 percent of your total voice packet size. So in our case we have a 20 ms seconds packet so the maximum blocking delay must be 16 ms. Now, we need to determinate the exact packet fragmentation size for the links we could have in our collaborative environment with the following algorithm:

```
WAN bandwidth x blocking delay = fragment size in bits
```

The low bandwidth circuits that we could support are a dial up 56Kbps link or ADSL 256Kbps link, so applying the last algorithm we have:

```
Fragment size Dial-up link = 56Kbps x 16 ms = 896 bits
per second = 112 bytes per second.

Fragment size ADSL link = 256Kbps x 16 ms = 4096 bits
per second = 512 bytes per second
```

As we can see, in the low bandwidth WAN link is it necessary to fragment the packets to 128 or 64 bytes for the dial up connection and to 512 bytes to the ADSL connection.

In order to fragment the packets we can use FRF.12 if we have a frame-relay interface, if we have interfaces that can run PPP, MCML is recommended otherwise we should use IP MTU, even though this last tool can cause many problems since the receiving station's overall performance is affected. MCML PPP still requires fragments to be classified by IP Precedence, and to be queued by WFQ.

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.

3.2.2 Low latency queuing and congestion avoidance techniques. Low latency queuing (LLQ) was designed for realtime applications. It brings strict Priority Queuing (PQ) to Class Based Weighted Fair Queuing (CBWFQ). Strict PQ allows delay-sensitive data to be sent directly through the outgoing interface [13] 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. LLQ provides strict priority queuing for CBWFQ, reducing jitter in voice conversations.

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.

We propose (see figure 1) to include a congestion avoidance technique for remaining traffic, Weighted Random Early Detection (WRED) with CBWFQ. WRED selectively drops packets according to its importance (packets of lower priority are dropped more than the ones from high priority).

4. Experiments and Results

The aim of this section is to show the performance improvement that a real AS LAN will have after the above described 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, routers and switches will be configured with the proposed model. We will compare results to determine the level of performance improvement obtained with the proposed design.

The proposed network topology that represent an AS 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 edge routers will be connected through their Fast Ethernet interface with a Catalyst 2900 series switch. Each of these switches connects to one more switch by using its Gigabit Ethernet trunk interfaces. Finally, the hubs and hosts are connected into these, just as it is pointed out in Figure 2. For each tested scenario we will measure the packet loss, delay and jitter, while testing the data link and network layer.

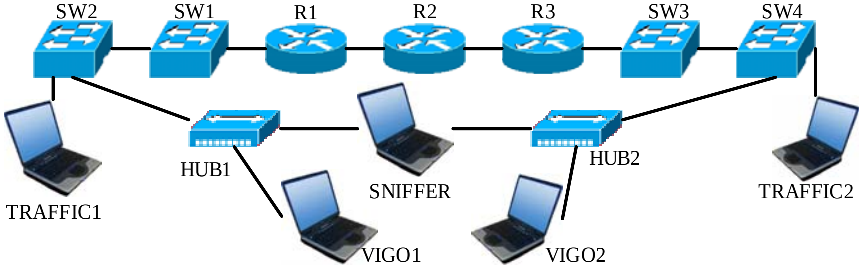

Figure 2. Scenario network topology

The routers were configured following a single area OSPF scheme. 802.1q was used on the Fast Ethernet interfaces to support the VLAN tagging of the switches

The used IP addresses were as follows:

R1 Fa0.0:	192.168.3.1	**R1 S0**:	192.168.1.1
R2 S1:	192.168.1.2	**R2 S0**:	192.168.2.1
R3 Fa0.0:	192.168.4.1	**R3 S1**:	192.168.2.2
Traffic1:	192.168.3.20	**Traffic2**:	192.168.4.20
Sniff NIC1:	192.168.3.10	**Sniff NIC2**:	192.168.4.10
Vigo1:	192.168.3.15	**Vigo2**:	192.168.4.15

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

By recreating a videoconference enabled scenario while also simulating normal network traffic, our testing environment comes very close in terms of reality and thus gives us a much better perception of what would the QoS performance benefit be when applied into a real world case, such as an university campus.

4.1 Endpoints inside the same network – layer 2 priority

The first and simplest scenario describes the typical switched 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 at the Fa0/1 of each of the switches, while also using a traffic generator laptop plugged into the Fa0/2 port of each switch. Both a Vigo videoconference laptop and the sniffer laptop were connected to each of the hubs. The two sniffer cards were inside the same laptop, and each card was connected to a different hub.

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

The tests ran in our simulated network showed up some slight improvements after applying QoS at layer 2. The improvements 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 100/1000 Ethernet interfaces. This points out that our attention should be focused into improving layer 3 prioritization which covers our network full AS.

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 used network topology can be observed at Figure 2. The sniffer has two cards, each one is connected to a different network.

For this scheme, there are 2 types of router configurations that should be noted. We will refer to them as the edge and the middle routers, being the edge routers the ones that are directly connected 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 used for the edge routers were as follows:

```
Router(config)#class-map match-any VOICE-VIDEO
Router(config-cmap)# match protocol rtp audio
Router(config-cmap)# match protocol rtp video
```

The creation of the VOICE-VIDEO class identifies the RTP traffic commonly used in videoconference.

```
Router(config-cmap)# class-map match-any HTTP-FTP
Router(config-cmap)# match protocol ftp
Router(config-cmap)# match protocol http
```

The HTTP-FTP class identifies the traffic we will be using as a 2nd priority. In our tests, our injected traffic is of this kind, so we provide a specific class for it to ensure the router responds as we request.

```
Router(config)# policy-map MARKING
Router(config-pmap)# class VOICE-VIDEO
Router(config-pmap-c)# set dscp af41
```

The MARKING policy is specific of the edge routers. Once in the middle routers, traffic has already been marked so there's no need to do this again.

```
Router(config)# policy-map VOICE-VIDEO
Router(config-pmap)# class VOICE-VIDEO
Router(config-pmap-c)# priority percent 50
Router(config-pmap-c)# class HTTP-FTP
Router(config-pmap-c)# bandwidth remaining percent 70
Router(config-pmap-c)# class class-default
Router(config-pmap-c)# bandwidth remaining percent 30
Router(config-pmap-c)# random-detect
```

The VOICE-VIDEO policy gives special treatment to each traffic class specified previously. We define a strict 50% traffic priority to all the data matched by our VOICE-VIDEO class. From the remaining bandwidth we chose to give 70% (35% from the total absolute bandwidth) for HTTP and FTP traffic, while giving the rest of the bandwidth to any other kind of traffic not previously defined.

For each of the edge routers, we applied our policies VOICE-VIDEO and MARKING to the corresponding interfaces. For R1:

```
R1(config)# interface s0/0
R1(config-if)# service-policy output VOICE-VIDEO
R1(config-if)# interface fa0/0
R1(config-if)# service-policy input MARKING
```

The configurations for the middle router differ from the edge ones, so it doesn't require any marking because R1 and R3 (the edge routers) are doing all the marking themselves. The extra configuration required for the middle router R2 to work was:

```
R2(config)# class-map match-any VOICE-VIDEO
R2(config-cmap)# match ip dscp af41
```

The edge routers MARKING policy already set the dscp to af41, so the middle routers can trust this value and only compare the incoming packets against this.

The only difference between the middle and edge routers is the MARKING policy. The VOICE-VIDEO policy remains the same, so the only missing thing is to apply the policy to an interface.

```
R2(config)# interface s0/0
R2(config-if)#service-policy output VOICE-VIDEO
R2(config-if)#interface s0/1
R2(config-if)#service-policy output VOICE-VIDEO
```

Finally, we apply the policy to our serial interfaces. In contrast to the edge routers, the same service policy needs to be applied to both serial interfaces. Since we don't process nor do any marking from incoming traffic, we do only need to specify the prioritization for the data already marked.

The edge router marks the header and the middle routers are dedicated to give a preferential or deferential treatment to the marked packets with a given DSCP field [14]. 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 table shows the differences when applying the commands shown above:

Table 1. Experiment results

	Total packets	**Average delay (ms)**	**Jitter (ms)**
Voice (No QoS)	686	27.910	60.870
Voice (QoS)	705	12.036	60.401
Benefit (%)		**131.88**	**.776**
Video (No QoS)	2328	31.209	18.610
Video (QoS)	2399	17.671	17.940
Benefit (%)		**76.61**	**3.60**

During the tests there were no lost packets at all and, as shown, there is a remarkable improvement in both voice and video (131.88% and 76.61% respectively) after applying the QoS settings. We should 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 bigger.

5. Conclusions

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

Even though we prioritize the voice and video traffic in our experiments, this model can be applied to any kind of traffic required in collaborative systems.

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 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 are required since we can not control the traffic coming from other sources. We must follow the proposed model in order to prioritize the outgoing/incoming traffic to assure that the most important data keeps flowing smoothly without congestions. Inside an AS, this paper provides the required steps to enable QoS in both incoming and outgoing traffic.

The obtained results show the type of improvement which will be obtained in the target AS where these settings are applied (up to 131%). This AS refers to the final network where our collaborative system could be connected, enhancing the quality of their communications while allowing for total control of the traffic flowing through it.

By using a scenario recreating real traffic with the use of TCP, UDP and ICMP traffic, our tests come close to reality, demonstrating that our general model can be successfully applied into a real world scenario while obtaining similar benefits.

With this model, we can guarantee an optimal performance inside the AS, translating into a direct benefit to the network where the collaborative systems are set down.

6. References

[1] Guzdial, M., Hmelo, C., Hubscher, R., Newstetter, W., Puntambekar, S., Shabo, A., Turns, J., & Kolodner, J. (1997). Integrating and guiding collaboration: Lessons learned in computer-supported collaboration learning research at Georgia Tech. Proceedings of Computer-Support for Collaborative Learning (CSCL '97), Toronto, Ontario, 91-100

[2] A. Campbell, G. Coulson and D. Hutchison, "A Quality of Service Architecture", Computer Communication Review, Vol.1, No.2, April 1994, pp. 6-27

[3] ECOLE. "Synergeia". Internet Web Site. http://www.ecolenet.nl/best/synergeia.htm. Consultation date: October 2004.

[4] Patras, U. "Synergo". Internet Web Site. http://www.ee.upatras.gr/hci/synergo/. Consultation date: October 2004.

[5] Blackboard, I. "Blackboard Portal System". Internet Web Site. http://www.blackboard.com. Consultation date: October 2004.

[6] S. Chen, K. Nahrstedt, An overview of quality-of-service routing for the next generation high-speed networks: problems and solutions, IEEE Network, Special Issue on Transmission and Distribution of Digital Video, November/December 1998

[7] Avouris, N.; Margaritis, M.; Komis, V. "Real-Time Peer Collaboration In Open And Distance Learning". Proceedings: 6th Hellenic European Conference On Computer Mathematics & Its Applications. Athenas. September 2003.

[8] I. Miloucheva, A. Nassri, A. Anzaloni, "Automated analysis of network QoS parameters for Voice over IP applications", 2nd International Workshop on Inter-Domain Performance and Simulation (IPS 2004), 22-23 March 2004, Budapest, Hungary.

[9] S. Vegesna, "IP Quality of Service", Cisco Press, 2001. ISBN 1-57870-116-3.

[10] L. Burgstahler et al, "Beyond Technology: The Missing Pieces for QoS Success", Proceedings of the ACM SIGCOMM 2003 Workshops, Aug 2003, pp: 121-130.

[11] Seven Ubik, Josef Vojtech. QoS in Layer 2 Networks with Cisco Catalyst 3350. CESNET Technical Report 3/2003.

[12] M.J. Karam, F.A. Tobagi, Analysis of the Delay and Jitter of Voice Traffic Over the Internet, IEEE INFOCOM 2001

[13] Fayaz, A., McClellan, S., Manpreet, S. and Sannedhi K. End-to-end Testing of IP QoS Mechanisms. IEEE Transactions on Mobile Computing 0018-9162/02 IEEE pp 80-86.

[14] Fineberg, V., "A practical architecture for implementing end-to-end QoS in an IP network", IEEE Communications Magazine, Vol. 40 , Issue: 1, Jan.2002, pp.122– 130.