NETWORK PERFORMANCE EVALUATION WITH REAL TIME APPLICATION ENSURING QUALITY OF SERVICE WITH NS2

Luis Fernando Espinosa Moreno[1]

[1]Student of Electronic Engineering, Faculty of Engineering, Universidad Distrital Francisco José de Caldas, Bogotá, Colombia
lfespinosam@correo.udistrital.edu.co

ABSTRACT

The quality of service is a need in recent computer network developments. The present paper evaluates some characteristics in a proposed network topology such as dropped packets and bandwidth use, using two traffic sources, firstly a VoIP source over an UDP agent, then a CBR traffic source over an UDP agent as well as the previous one. Two possible configurations are proposed, implementing both of them in the Network Simulator, and implementing in one of them differentiated services to compare the results. Statistics results are shown, in both cases showing the accumulative dropped packet number and the throughput in the link, obtaining a reducer number of dropped packets in the stage with differentiated services, and an improvement in the bandwidth use.

KEYWORDS

Quality of Service, DiffServ, Computer Network, VoIP

1. INTRODUCTION

In past decades, the IP Protocol was limited to offer as service model the provided known as "best effort" [1]. Recently, the new applications requirements make the service model offered not enough to ensure the properly network operation [2]. Some applications such as voice over IP, television signal transmission, i.e., require some guarantees to have a correct performance in transmission.

Network Quality of Service is evaluated through 4 parameter measurements: Bandwidths, end-to-end delay, jitter and lost packets amount. For communication systems that implement voice over IP or video streaming to work properly, the bandwidth must be as large as possible while the delay, jitter and packet loss should be minimized.

To ensure service quality have arisen several alternatives [3], currently being used extensions to existing protocols and architecture known as Differentiated Services, DiffServ, and Integrated Services, IntServ. The differentiated services architecture packages have special treatment depending on traffic, reflected in a code that is assigned to your packages which network devices known to prioritize or degrade. For Integrated Services architectures, the network parameters are explicitly managed to ensure quality of service; the pillars of this architecture are resource reservation and admission control.

DOI : 10.5121/ijngn.2012.4301

For analysis networks behavior, network simulators are used often, with the aim of generate statistical results which report network events. A commonly used tool in research is The Network Simulator, also known as NS, a discrete events simulator intended for network research [4]. It offers wide support for a variety of network protocols, as well as applications and services. It is also capable of carry out developments which involve Quality of Service, due to the fact it can obtain a set of data about parameters related to the network, furthermore, this simulator is suitable for analyzing and evaluating architectures as well as differentiated services.

This paper is organized as follows: Section II gives a brief review on quality of service in IP networks, as well as the architecture characteristics that are deployed in differentiated services and integrated services, in addition it introduces some basic notions about NS. Section III describes the setting which is going to be implemented to perform quality of service measurements with and without differentiated services. Section IV presents the setting implementation in NS2, describing used parameter for each simulation. Section V provides simulation results, also their analysis. Finally, conclusions are shown in Section VI.

2. PRELIMINARIES

2.1. IP Networks Quality of Service

IP is limited specifically to provide the functions necessary to send a packet of bits from a source to a destination through a system of interconnected networks. There are no mechanisms to increase the reliability of data between the extremes, flow control, sequencing, or other services that are normally found in other protocols host-to-host. However it can take advantage of the services of its supporting networks to provide various types of quality of service (QoS) [3].

The QoS specifies whether a network guarantees a certain level of performance in handling packages. In the initial stage of the IP protocol, it was only provided a service class called “best effort” related to the effort made by the network to carry the packet to its destination, which in this case is an attempt to do this effort in the best way. It does not take into account the type of traffic that can be flowing through the network, nor are notifications about the packets delivered successfully send.

This scheme of operation was not efficient enough to handle new types of traffic such as VoIP and online gaming. These types of applications are susceptible to delays and require special treatment if you ensure optimal arrival thereof. The standards and applications have adapted best to tackle the problems of the lack of QoS in the IP protocol, e.g. using connection-oriented technologies like TCP, but equally, there was no preferential treatment for certain traffic types. An alternative to ensure preferential treatment to certain types of traffic has been the implementation of extensions to the Internet architecture and protocols known as integrated services and differentiated services.

2.2. DiffServ

In this architecture, packets are classified and marked to receive special treatment in terms of ships in each jump. Sophisticated classification, marking, and packaging operations policy need only be implemented at the edges of the network or in the host [5].

Differentiated services are intended to provide a framework and building blocks to allow discrimination of Internet services. The DiffServ approach is to accelerate the architecture implementation by separating it into two main components. This implementation is guided by the original design of the Internet, where it was decided to separate the transmission and routing components. In analogy, the Differentiated Services architecture contains two main components: one well understood is the behavior of the transmission path, and the other component is more complex and still emerging background and policy allocation component that configures the parameters used in the transmission path [6].

2.2.1. Packets marking

In IPv4 protocol packets have a byte called “Type of Service Octet”, *TOS octet*. Before the implementation of DiffServ that field was not used. Now this field is known as “Differentiated Services Field”, *DSCP*, used to tell the router the treatment that must be given to each packet. This treatment is called per-hop behavior, or *PHB*. The PHB present in devices such as routers and hosts is configured according to a standard for certain performance characteristics. For example, the following standards are commonly used:

- Default Behavior [6]: The DCSP value is zero, so the scheme is “best effort”.
- Class Selector Behavior (CS PHB) [7]: It has seven different behaviors, depending on the 6-bit DSCP field.
- Expedited Forwarding Behavior (EF PHB) [8]: The DSCP value is 101110. In this case the throughput is configurable.
- Assured Forwarding Behavior (AF PHB) [9]: It has three different behaviors: AF1, AF2 and AF3; when there is a change in behavior, the probability that the packets are discarded changes.

2.2.2. Edge nodes and internal nodes

The edge nodes are in charge of organizing the packages for different classes. Also check to see if it meets the service level agreements, discarding packets that do not comply. Internal nodes only retransmit packets based on the class defined in the header.

2.2.3. Guarantee of services

DiffServ ensures resources through the use of combined providing with prioritization. There is not a reservation policy flows and neither an absolute guarantee of bandwidth or delay bounds for individual flows. Service levels are achieved by allocating resources to relay classes and controlling the amount of traffic these.

2.2.4. Service Level Agreements *SLA*

Services are defined between the customer and the service provider with an SLA [6]. This consists of several parts, such as a TCA (Traffic Conditioning Agreement), availability, security, monitoring, auditing, among others. The TCA specifies operating parameters for traffic profiles and police controls, and may include performance metrics such as delay and priorities.

2.3. Integrated Services

The integrated service model includes two types of services for real-time traffic: guaranteed and predictive. It integrates these services with links shared control, and also it is designed to work with multicast and unicast. Considerations must be taken to understand this architecture [11].

The first assumption is that the resources (e.g. bandwidth) must be explicitly managed in order to satisfy the needs of the application. This implies that the “resource reservation” and the “admission control” are the pillars of the service. The other consideration is to use the Internet as a common infrastructure to support both types of traffic, real-time communication and what is not. It has the view that there should be a unique model for Internet services.

2.3.1. Framework

To implement this model, a framework is proposed. This consists of four components, which are [11]:

- Packet scheduler: Handles the sending of packets using various types of queues or other mechanisms, such as timers.
- Classifier: The purpose of this component is to control traffic. Each incoming packet should be linked to a class; all packets of the same class are treated as equal in the packet scheduler.
- Admission Control: Implements the decision algorithm that a host or router uses to determine whether a new flow QoS can be guaranteed without impacting other flows.
- Reservations Configuration Protocol: It is a need to create and maintain the status of a specific flow between the host and the routers through the flow path. The most known protocol is RSVP.

3. PERFORMANCE EVALUATION SETTING

A network with the topology shown in Figure 1 was evaluated with NS2, to observe the metrics that characterize the quality of service, running under a real time application, which in this case corresponds to an application which handles voice over IP (VoIP).

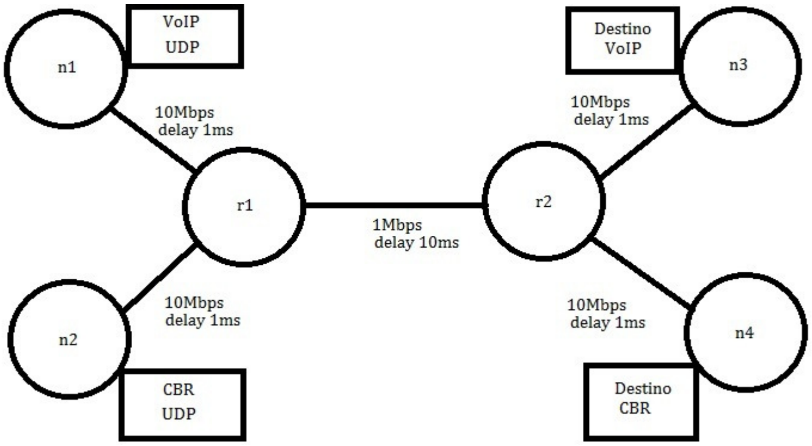

Figure 1. Network topology deployed.

Two traffic types were generated, one of which was owed to offer quality of service, since it was a real-time application, hence delay sensitive. The other type of traffic generated was a CBR traffic source. This type of traffic occupies much of the bandwidth of the channel, and contributes to the production of a bottleneck"" in the channel between the routers R1 and R2. These types of traffic will be analyzed in more detail in the next section.

There were carried out two different simulations. The first did not offer quality of service, in the second simulation was guaranteed QoS by implementing differentiated services, such as end nodes using two routers which manage the framework upon this architecture was developed.

4. NS2 SIMULATION

NS2 provides substantial support for TCP simulation, routing and multicast protocols over wired networks as well as wireless (local and satellite). Written in C + +, its user interface presents a Tcl language interpreter object oriented called OTcl. In the simulation, as time goes on, events are happening as they are executed by the event planner.

4.1. VoIP

This service consists of using the infrastructure deployed for the transmission of data to send voice, using the IP protocol. The basic tasks that must perform a VoIP system are digitization of voice, packaging of voice and routing packets [12].

This type of service is not integrated with the NS2, but was developed a module that allows the simulation of a VoIP service to perform simulations. The patch is called Ns2voip, and was developed and is maintained by the group of computer networks of the Department of Information Engineering, University of Pisa, Italy [13].

This module models a transmitter, "sender" and a destination, "receiver" separately. The user speech activity is modeled as a series of frame bursts that contain voice, and silence moments. To model the operation of the traffic generated by a conversation, several data structures are generated, and are listed below [14]:

- *VoipFrame*: Includes the main characteristics of the speech frames, for example the size of the packets and the sequence numbers.
- *VoipPayload*: A collection of VoipFrame. It is the container, which is linked with the application.
- *VoipSource*: It is in charge of generating agent packages.
- *VoipAgreggate*: Used to create aggregates to generate multiple frames in the payload.
- *VoipHeader*: Get the payload and adds the headers RTP/UDP/IP, plus compressive support.

4.2. CBR Traffic

CBR traffic is meant for traffic with constant bit rate. In this type of agent can be configured the packet size and interval time between each packet. This agent is going to be used as traffic generator not susceptible to delays, and it will be in charge of congestion and take care of the channel shared by the two traffic sources, in order to obtain a bottleneck in the channel and generate tail package removal and delays delivery thereof. This traffic is also connected to a UDP agent.

4.3. QoS not guaranteed simulation

To implement this scenario, it is first built the topology defining the following parameters in the script created in NS2:

```
$ns duplex-link $n1 $r1 10Mb 2ms DropTail
$ns duplex-link $n2 $r1 10Mb 2ms DropTail
$ns duplex-link $n3 $r2 10Mb 2ms DropTail
$ns duplex-link $n4 $r2 10Mb 2ms DropTail
$ns duplex-link $r1 $r2 1Mb 10ms DropTail
```

As noted, DropTail queues are used. With this, packets are removed which make the queue exceeds the maximum size. The events generated by the simulation are as follows:

```
$ns at 0.0 "record"
$ns at 0.2 "$source start"
$ns at 0.5 "$cbr0 start"
$ns at 4.5 "$cbr0 stop"
$ns at 4.8 "$source stop"
$ns at 5.0 "finish"
```

The function call "record" is responsible for gathering statistics. The sources of traffic (VoIP, CBR) start at 0.2s and 0.5s, and they end in 4.5s and 4.8s respectively.

3.4. QoS guaranteed simulation

To provide preferences in dealing with the transmission of packets, the DiffServ architecture is implemented in the channel between the routers r1 and r2. For the simulation, the DiffServ NS2 module is used, which can support four traffic classes, where each of them has three priorities to choose which packets are dropped, allowing differential treatment of traffic from each class. The packages in one traffic class are put into the corresponding physical RED type queue, which contains three virtual queues (one for each priority packets dropped) [15].

The module has three main components:

- Policy: Policy is specified by network administrator about the level of service a class of traffic that is received on the network.
- Edge router: mark packets with a "Code Point", CP, according to the specified policy.
- Core router: examines CP and transmits this.

A DiffServ queue (class dsREDQueue) derived from the base class of the queue, takes place in the DiffServ module to provide basic functionality in DiffServ routers. DsREDQueue class comprises four physical queues RED type, each having three virtual queues.

A. Policy

The Policy class defines the policies used by edge-routers to mark packets arriving. A policy is established between the source and destination nodes. Six different policy models are defined:

- Time Sliding Window with 2 Color Marking(TSW2CMPolicer)
- Time Sliding Window with 3 Color Marking(TSW3CMPolicer)
- Token Bucket (tokenBucketPolicer)
- Single Rate Three Color Marker (srTCMPolicer)
- Two Rate Three Color Marker (trTCMPolicer)
- NullPolicer

B. Configuration

First, set the canal linking r1 to r2 with a RED queue:

```
$ns simplex-link $r1 $r2 1Mb
10ms dsRED/edge
```

Following parameters were configured to implement a service that gives priority to packets that are VoIP, assigning a policy model Token Bucket creating two virtual queues. The Token Bucket for VoIP traffic has the ID number 10, and the 11 virtual queue and CBR traffic identifier is the number 20 and its virtual queue is the queue 21.

5. Results

5.1. First scenario

When performing the script simulation is obtained 138 lost packets for CBR traffic and VoIP traffic had a loss of 58, as shown in Figure 2. It is observed as the number of lost packets for both traffics are not far apart, presenting a high amount in the case of VoIP, this being undesirable because in this kind of traffic the integrity of data sent should be ensured, since with this amount of discarded data communication between aggregates will not run properly. This result shows the problems derived from the "best effort" IP model applied to real time applications, where no QoS in ensured.

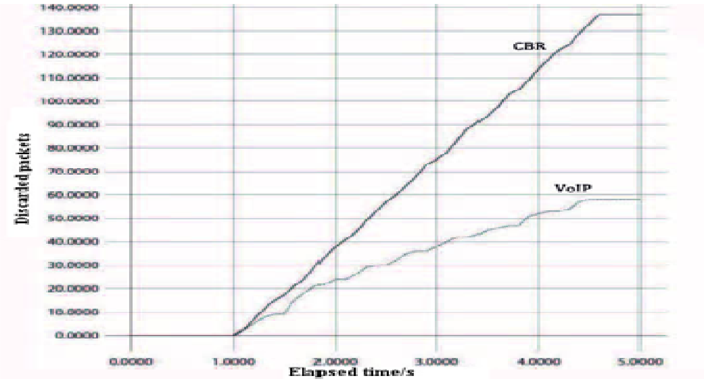

Figure 2. Lost packets for each traffic

The use of the channel bandwidth is not efficient, as the CBR traffic is always consuming almost everything of it, leaving little for the required for VoIP traffic. Although the latter consumes less bandwidth, this should be reserved, as it can create delays and packet losses if given the same treatment as other applications. This situation is seen in Figure 3.

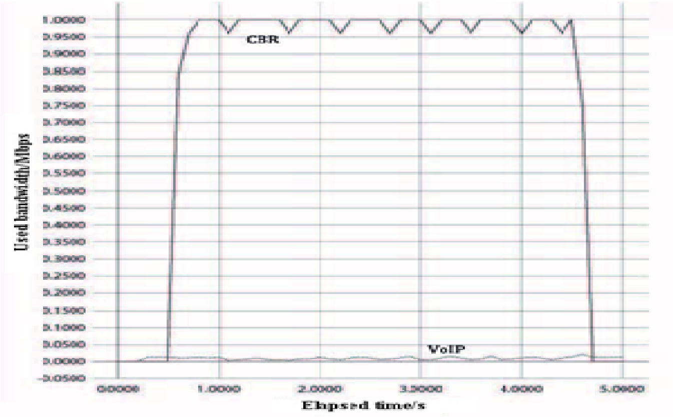

Figure 3. Channel bandwidth used by the two applications.

Is observed how the CBR traffic uses a bandwidth of between 1Mbps and 0.95Mbps, so this saturates the channel sending this information, which in the case of this simulation, has no relevance to the traffic which is susceptible to delays, where should be insured an amount of bandwidth of the channel to avoid improperly transmission of such applications.

5.2. Second scenario

When performing the simulation script implementing differentiated services, Table 1 is obtained, indicating packet loss statistics for each traffic type.

Table 1. Number of packets lost for each type of traffic.

Traffic	CP	Total Package	Transmitted	ldrops	edrops
All	All	1383	1228	96	59
VoIP	10	240	239	1	0
CBR	20	219	212	7	0
CBR	21	924	777	88	59

Where "CP" means the Code Point, "Total Package" refers to the total number of packets sent by both traffic sources, "Transmitted" refers to packages that were sent to each destination successfully, "ldrops" is refers to packets that are discarded due to overload in the channel, and "edrops" packets are discarded at an early stage by the RED algorithm [15]. It is observed as the number of lost packets for traffic with better treatment, in this case VoIP, dropped to almost zero, as shown in Table 1. Consequently there was a slight increase in losses CBR traffic. For the latter, two queues were used, according to the definition of the type of queue used, which generated a virtual queue with CP equal to 21, which had the largest number of packets discarded due in equal proportion to the RED algorithm and those due to channel saturation. Although in the case of CBR increased the number of lost packets, this results in a more privileged treatment for the other traffic. A graph was generated showing the number of packets lost at each moment in the simulation; it is shown in Figure 4.

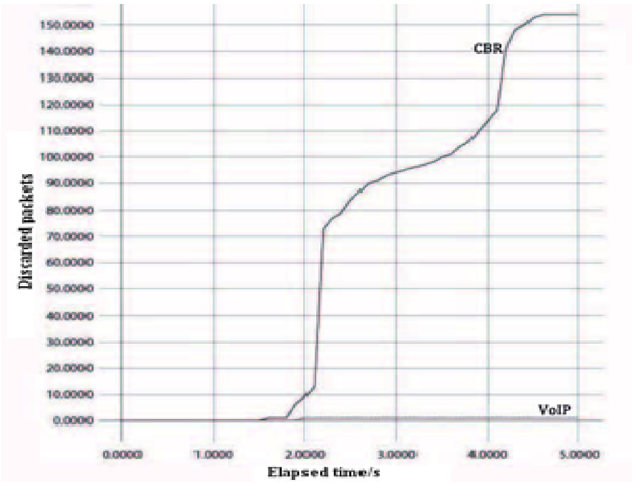

Figure 4.Lost packets for each traffic type.

This gave a total amount of lost packets for CBR packets of 155, whereas only oneVoIP packet is discarded. These data are consistent with those obtained in Table 1, adding discarded packets in two modes (ldrops, edrops) for each of the traffic sources.

The bandwidth in this case is assigned with privileges for VoIP traffic, so when it is necessary the bandwidth consumed by the CBR traffic falls considerably, as seen in figure 5, the instant of time

2.2s where the bandwidth used by CBR traffic drops to 0.65Mbps, so that the whole VoIP packet could be delivered. So it was possible to simulate a condition where the bandwidth for certain types of traffic with higher priority is guaranteed, being this one of the conditions necessary to guarantee QoS.

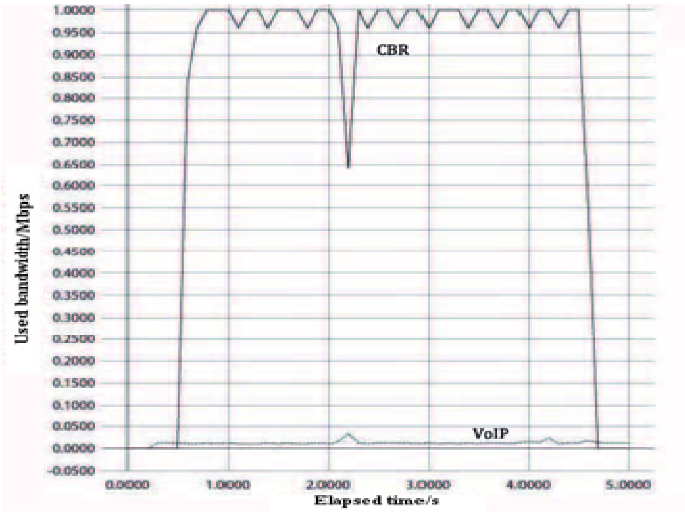

Figure 5. Channel bandwidth used by the two applications.

6. CONCLUSIONS

Two simulation scenarios were developed using NS2 scripts, and there were generated graphs showing the channel usage and the number of lost packets for each traffic type. The scenario which does not exhibit quality of service presented a not proportionated bandwidth, responding only to the type of queue used, in this case, DropTrail. Also the number of packets lost was similar in both types of traffic, flow regardless. In the second scenario was implemented a differentiated services scheme, hoping to improve the quality of service parameters. This gave a reduction of the number of packets discarded and a distribution of bandwidth further favoring higher priority traffic, VoIP, increasing this to provide smaller delays and smaller amount of lost packets.

REFERENCES

[1] U. de Jaén. (2012, June) Calidad de servicio en redes ip. Trasparencias. [Online]. Available: http://www4.ujaen.es/jccuevas/data/AATTAA2/Transparencias/Tema%201%20Calidad%20de%20servicio%20en 20redes%20IP.pdf

[2] E. B. Kelly. (2012, June) Quality of service in internet protocol networks. [Online]. Available: http://wainhouse.com/files/papers/wr-qos-in-ip-networks.pdf

[3] J. Postel. (2012, June) Internet Protocol. RFC 791 (Standard). Internet Engineering Task Force. Updated by RFC 1349. [Online]. Available: http://www.ietf.org/rfc/rfc791.txt

[4] (2012, June) The network simulator. [Online]. Available: http://www.isi.edu/nsnam/ns/

[5] S. R. Adrián Delfino. (2012, June) Diffserv: Servicios diferenciados. [Online]. Available: http://iie.fing.edu.uy/ense/asign/perfredes/trabajos/trabajos_2003/diffserv/Trabajo%20Final.pdf

[6] K. Nichols, S. Blake, F. Baker, and D. Black. (2012, June) Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers. RFC 2474 (Proposed Standard). Internet Engineering Task Force. Updated by RFCs 3168, 3260. [Online]. Available: http://www.ietf.org/rfc/rfc2474.txt

[7] J. Babiarz, K. Chan, and F. Baker. (2012, June) Configuration Guidelines for DiffServ Service Classes. RFC 4594 (Informational). Internet Engineering Task Force. Updated by RFC 5865. [Online]. Available: http://www.ietf.org/rfc/rfc4594.txt

[8] B. Davie, A. Charny, J. Bennet, K. Benson, J. L. Boudec, W. Courtney, S. Davari, V. Firoiu, and D. Stiliadis. (2012, June) An Expedited Forwarding PHB (Per-Hop Behavior). RFC 3246 (Proposed Standard). Internet Engineering Task Force. [Online]. Available: http://www.ietf.org/rfc/rfc3246.txt

[9] J. Heinanen, F. Baker, W. Weiss, and J. Wroclawski. (2012, June) Assured Forwarding PHB Group. RFC 2597 (Proposed Standard). Internet Engineering Task Force. Updated by RFC 3260. [Online]. Available: http://www.ietf.org/rfc/rfc2597.txt

[10] J. J. Padilla. (2012, June) Calidad de servicio en internet: Servicios diferenciados. [Online]. Available: http://jpadilla.docentes.upbbga.edu.co/QoS/DiffServ1%20Introduccion.pdf

[11] R. Braden, D. Clark, and S. Shenker. (2012, June) IntegratedServices in the Internet Architecture: an Overview. RFC 1633(Informational). Internet Engineering Task Force [Online]. Available: http://www.ietf.org/rfc/rfc1633.txt

[12] E. Pietrosemoli. (2012, June) Voip. Escuela Latinoamericanade Redes. Mérida, Venezuela. [Online]. Available:http://www.eslared.org.ve/articulos/ermanno/voip.pdf

[13] (2012, June) Ns2voip. Computer Networking Group of the Dipartimentodi Ingegneria dell'Informazione of the University of Pisa. Italy. [Online].Available: http://cng1.iet.unipi.it/wiki/index.php/Ns2voip

[14] A. Bacioccola. (2012, June) User-level performanceevaluation of voip using ns-2. [Online]. Available:http://cng1.iet.unipi.it/archive/ns2voip/bacioccola07user.pdf

[15] K. Fall. (2012, June) The ns manual. The VINT Project. [Online].Available: http://www.isi.edu/nsnam/ns/doc/ns_doc.pdf

Authors

Luis Fernando Espinosa Moreno, Student of Electronic Engineering, Faculty of Engineering Universidad Distrital Francisco José de Caldas. Bogotá D.C., Colombia.