Nanotechnology Perceptions
ISSN 1660-6795
www.nano-ntp.com

Analysis of the Impact of Loops or Flapping in VoIP Quality of Service

Rossina I. Gonzales-Calienes[1], Rafael Bustamante-Alvarez[1], Wilbert Chavez-Irazabal[1], Martin M. Soto-Cordova[1,2]

[1]Universidad Nacional Mayor de San Marcos
[2]Escuela de Educación Superior Cibertec
Email: rgonzalesc1@unmsm.edu.pe

Quality of Service (QoS) in a data network is a key factor in the provision of services, especially when they are real-time and interactive. In particular, loops or flapping in a data network can cause a number of problems related to QoS degradation, including network instability, broadcast storms, routing database inconsistency, packet duplication, slow convergence. They can also have a significant impact on real-time traffic such as Voice over IP (VoIP) communications, as VoIP is sensitive to latency, packet loss and inconsistency in quality of service. It should be noted that specific effects of VoIP loops or flapping can be identified such as call quality degradation, call interruptions, inconsistency in quality of service. In this paper, we present a method for detecting loops or flapping in a data network, an analysis of loops or flapping is performed focusing on a real campus network. Additionally, their effects on the quality of service of VoIP traffic are analysed and guidelines for solving the problem are provided.

Keywords: Quality of Service, Network Loops, MAC Flapping, Spanning Tree Protocol, VoIP.

1. Introduction

In today's interconnected world, VoIP has emerged as a cornerstone of modern communication systems, offering cost-effective and flexible solutions for voice transmission over data networks. With the increasing adoption of VoIP technology in various sectors including education, business, and healthcare, ensuring QoS has become paramount. However, the robustness of VoIP services can be compromised by network anomalies such as loops or flapping, which can severely impact QoS metrics such as latency, jitter, and packet loss [1].

Traffic measurements was used in [2, 3] to identify the issues involved in voice service over a tier-1 IP backbone network. It was found that link failures may be followed by long periods of routing instability, during which packets can be dropped because forwarded along invalid paths.

The stability and formation of the symmetric loop network by using of the cost-benefit method

is analysed in [4, 5]. It interprets the formation mechanism of loop networks with network effects principle. The loop networks may be formed and keep stable if the connect cost is larger than its benefits because of network effects [6, 7, 8].

The link-flapping effect in a network generates IP link failures causing data loss, thus affecting the services running over the network. For this reason, [9] proposes the use of SDN (Software Defined Networking) capabilities as an alternative to reduce this effect, and [10] reviews some schemes that enable link failure recovery and highlights technical aspects to be considered in the SDN architecture.

This paper presents a comprehensive research into the impact of loops or flapping on VoIP QoS within the campus data network of Universidad Nacional Mayor de San Marcos as a case study of a traditional network that occurs in many similar environments.. By examining the specific challenges faced by educational institutions in ensuring reliable VoIP communication, this study aims to shed light on effective mitigation strategies and provide valuable insights for network administrators and policymakers. Thus, this paper analyse the university campus network during a flapping or loops event and its impact on the network quality of service, specifically on the VoIP service.

This paper is organized as follows: Section I corresponds to the introduction where the VoIP issues are described. The fundamentals on analysed VoIP QoS components over campus networks are shown in section II. Section III covers the procedure followed in the research, and Section IV shows the results obtained. Finally, the conclusion of the work carried out is indicated.

2. Background

A. The University Campus Network

Typically, a technical office attached to the university is responsible for planning, managing and maintaining the operability of the university's telecommunications infrastructure and IT services. It also establishes the necessary internal policies and regulations for IT and telecommunications development. Services of high importance are usually Internet and VoIP-based telephony services. Specifically, the case study of a university campus network is the so-called UNMSM Telematic Network shown in Fig. 1.

The logical star topology of the network consists of single-mode fibre optic links, spanning the entire University Campus. The network structure operates on three hierarchical levels:

- Core Layer: It guarantees connectivity between the different layers and segments of the network through a high-speed backbone and redundancy. It consists of high performance, high availability and low latency Core Switches. There are two Cisco WS-6509E switches as Core Nodes located in the network management centre building and the university headquarters building. These are connected to the distribution nodes and the external university sites. Through these nodes, communication services are provided to all users (Internet access, VoIP, PSTN, e-mail, and access to the computer systems developed by the university, such as: the Single Registration Information System, the General Secretariat Information System, the Documentary Processing Information System and the Integrating

System for financial administration named Quipucamayoc System, among others).

- Distribution Layer: This aggregates traffic from multiple access devices and applies network policies such as traffic filtering, routing between VLANs and load balancing. This layer is made up of six Cisco WS-3750X Switches, which interconnect with one of the 10Gbps Core Switches. These are located in the faculties of: Chemistry, Industrial Engineering, Economics, Electronic Engineering, Dentistry and EPG.

- Access Layer: It provides connectivity to devices such as computers, IP phones, printers and wireless access points. It is composed of Access Switches offering PoE (Power over Ethernet), port security, VLANs for network segmentation and QoS. There is at least one Access Node per Faculty, mostly Cisco WS-2960 Switches connected at 1Gbps to the Distribution Switches. However, to provide connectivity to more workstations there are also unmanaged hubs and switches, which represent 35% of the access devices.

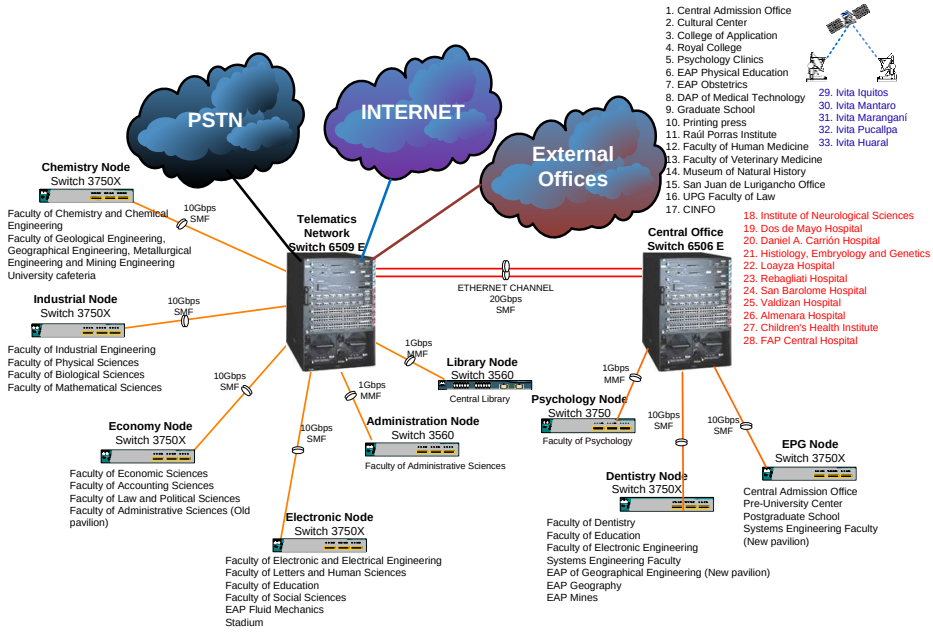


Figure 1. UNMSM Telematic Network Topology

B. VoIP Service

The VoIP platform consists of a cluster composed of two Cisco CUCM (Cisco Unified Communications Manager) servers in version 9.1.2, called Publisher and Subscriber. The Publisher server functions as the main server of the CUCM cluster, hosting the database that contains the configurations of all the devices, such as IP phones, gateways, user profiles, among others. It is responsible for the administration and management of the cluster, although it does not participate directly in the processing of telephone calls.

On the other hand, the Subscriber server receives a replica of the Publisher's database, allowing it to distribute the workload by handling call management and provision of communication services autonomously. All terminals are registered on both servers. However, configuration

changes (such as adding users, configuring telephones and setting call policies) are made exclusively on the Publisher. Subsequently, these changes are automatically synchronised with the Subscriber.

In the event of Publisher failure, the Subscriber server acts as a backup, handling calls with the previously replicated database. This configuration guarantees both redundancy and scalability of the system, ensuring continuous operation.

C. Impact of Looping or Flapping on VoIP

In the data communications within campus networks, ensuring seamless VoIP services is paramount for efficient and effective communication among students, faculty, and staff. However, the presence of network anomalies, such as loops or flapping, can disrupt the smooth transmission of voice data, consequently impacting VoIP QoS metrics.

Loops in network infrastructure occur when there is a redundancy in the network topology, causing packets to circulate endlessly between interconnected switches or routers. This results in excessive traffic and can lead to congestion, latency, and packet loss, ultimately degrading the QoS for VoIP applications. Loops may arise due to misconfigurations, equipment failures, or inadvertent network changes, posing significant challenges for network administrators.

Flapping, on the other hand, refers to the rapid and frequent changes in the operational state of network interfaces or links. This instability can stem from hardware malfunctions, software bugs, or environmental factors such as electromagnetic interference. Flapping interfaces disrupt the orderly flow of data packets, causing jitter and packet loss, which directly impact the clarity and reliability of VoIP calls.

The impact of loops or flapping on VoIP QoS in campus networks is multifaceted and can manifest in several ways:

- Latency: Loops or flapping introduce delays in packet delivery, increasing latency in VoIP communications. This delay results in noticeable lags between the transmission and reception of voice data, affecting the real-time nature of voice conversations.

- Jitter: Variability in packet arrival times, induced by loops or flapping, leads to jitter in VoIP streams. Excessive jitter disrupts the smooth playback of voice data, causing choppy or distorted audio during calls.

- Packet Loss: Loops or flapping can cause packets to be dropped or discarded, resulting in packet loss in VoIP transmissions. Even minor packet loss can significantly degrade call quality, leading to gaps or interruptions in audio playback.

- Call Setup Failures: Instability in network links due to flapping can disrupt the establishment of VoIP calls, leading to call setup failures or dropped calls. This impacts user experience and productivity, particularly in scenarios where reliable communication is critical.

D. Looping or Flapping of the MAC level in the Campus Network

When the switches detect that a network device is reachable through two ports and therefore send the frame through both ports, then the loop originates. Thus, when the frame arrives at the next switch, the next switch sends the frame again on the ports that allow the equipment to be reached. This results in a situation of exponential growth in the number of frames,

congesting the network and causing ongoing communications to fail. In addition, the processor consumption of the Switch Core is increased to 100%. In practice, this is caused when the user connects two ports of a switch via a UTP cable, who probably did not notice the error. Another cause is the failure of a computer or device on the network. This problem causes a degradation of the quality of service on the network, which impacts the VoIP service. The immediate solution is to locate the switch where the loop occurs.

Spanning Tree Protocol-STP is the solution to control a logical loop at Layer 2 in managed switches. However, when using unmanaged hubs or switches that do not support STP, loops are a very common cause of network failures. An unmanaged switch only registers the source MAC address and corresponding ports in an internal MAC table and then forwards according to the destination MAC address. Its main purpose is to provide basic communication between devices in a small local network, without advanced features such as STP, VLAN or QoS. As a result, all devices are part of the same broadcast domain.

Distribution switches and access switches, which are installed as headends in campus network buildings, protect the network from loops with the RSTP-Rapid Spanning Tree Protocol, but when hubs or unmanaged switches, which do not support STP, are connected, they do not protect the network from loops. In areas such as college and university offices, it is common to see unmanaged switches installed, usually accompanied by poor cabling. However, unmanaged switches do not protect against loops. Such equipment cannot detect network loops or disable redundant ports as a STP-managed switch would. This increases the risk of broadcast storms and degradation of network performance due to traffic saturation. Because unlike the Layer 3 IP protocol, which discards packets when the TTL field reaches 0, Layer 2 lacks a mechanism to stop broadcast storms.

Unmanaged switches do not participate in the STP process. This means that they do not send and process BPDUs (Bridge Protocol Data Units) messages, which are essential to correctly detect redundant topologies or loops in the network. In a network that includes unmanaged switches, topology changes (such as the addition or removal of a link) can result in longer convergence times and temporary network instability while STP attempts to resolve the new topology. Unmanaged switches also do not support STP enhancements such as RSTP and Multiple Spanning Tree Protocol (MSTP), which require specific features and configurations, limiting the network's ability to benefit from faster convergence times and more efficient topology management.

Implementing commands such as BPDU Guard or Loop Guard on manageable switches for loop prevention does not fully mitigate the adverse effects on the network when loops originate on segments containing hubs or unmanageable switches. This problem is shown in Fig. 2, where the network topology presents two loops due to improper connections on unmanaged switches.

Even if the spanning-tree portfast edge and spanning-tree bpduguard enable commands have been set up on the GigabitEthernet0/3 ports of the manageable switches called Switch01 y Switch03, saturation occurs in the Swicth03 processor and connectivity between the PCs is lost; as shown in Figure 3.

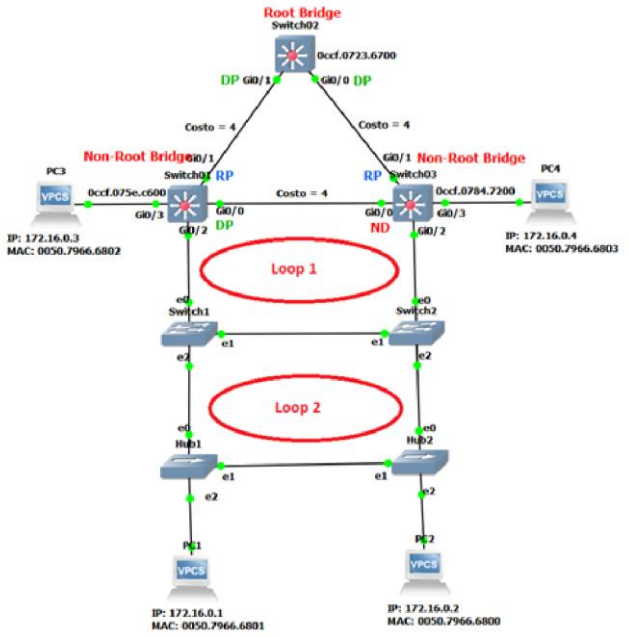


Figure 2. Effect of MAC flapping in a network of managed and unmanaged switches

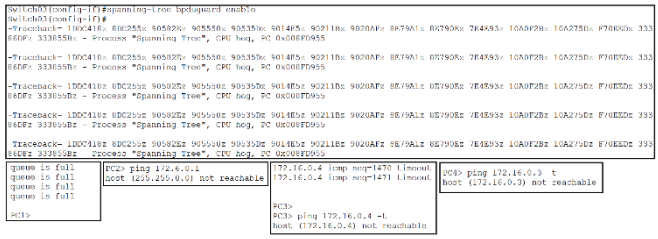


Figure 3. Loss of connectivity in a network affected by MAC flapping

3. Methodology

An analysis of the quality of service of VoIP in a campus network when it is affected by the presence of loops or flapping that have been generated by improper connections and faulty equipment. This analysis was carried out on the QoS parameters, in order to guarantee the communication and availability of the network. For this purpose, these are collected through traffic readings using the Wireshark software on the UNMSM Telematic Network's Switch Core. Likewise, the line commands executed on the Switch Core during the presence of flapping are used to verify the percentage of processor consumption and the frequency of MAC flapping log messages. The importance of this study lies in the early detection of faults that occur in the network and allow its timely solution in order that end users receive a good service, ensuring the availability and control of the QoS parameters.

The flowchart of the methodological process is shown in Fig. 4, where the steps to detect loops in a network of managed and unmanaged switches are described:

- Incident reporting: Through the technical support office of the UNMSM Telematic Network, users report deficiencies in the VoIP and Internet services.

- MAC flapping test: This is done on the Core and Distribution switches, using the commands as show logging | include MACFLAP (to detect if there is MAC address flapping in the network); and show process cpu history (to show the peaks in processor usage). When correlating the peaks with the event log records, if they coincide in time, it can be stated that the cause of the network degradation is due to MAC flapping.

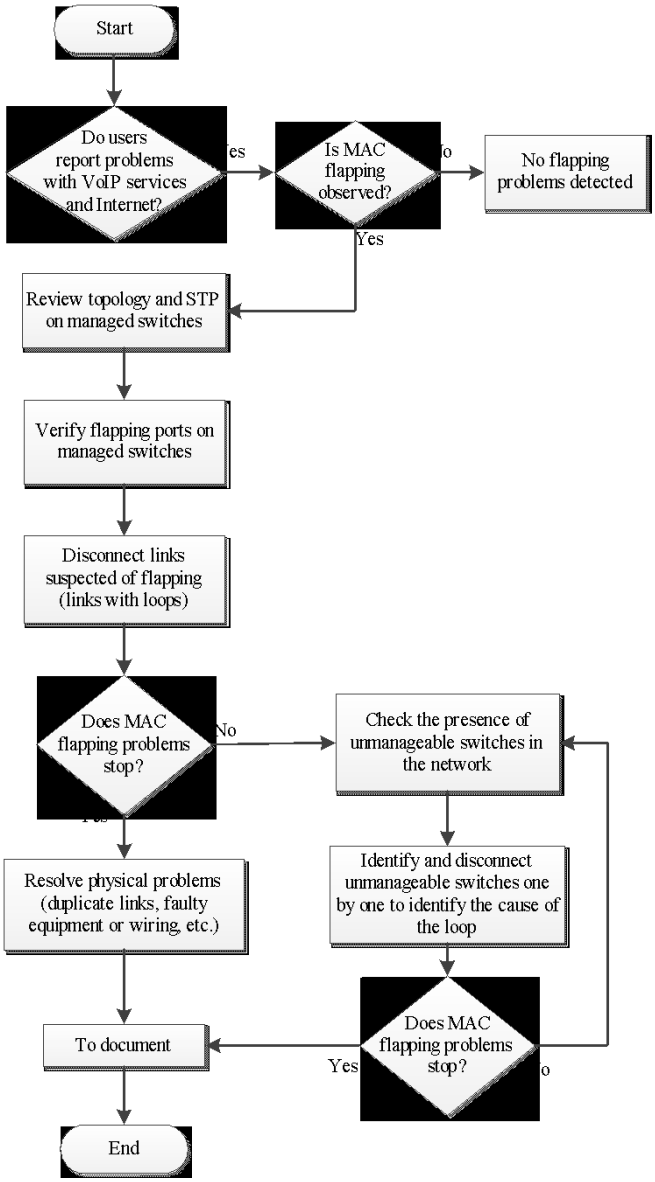


Figure 4. Flow chart of the methodology

- Review of the network topology and STP on managed switches: This consists of validating how the switches are connected in the network. It is checked with the show spanning-tree command. In case the Core Switch is the Root Bridge, it is necessary to know which ports are designated and which are blocked on the switches.

- Verification of event logs: Proceed to review the logs on the manageable switches to identify the affected ports. Execute the show mac-address table command (to check on which ports the same MAC is learned).

- Disconnection of suspicious links: The shutdown command is executed on the switch ports where the suspicious links are generated in order to identify the origin of the loop.

- Disconnection of unmanaged switches involved: If the MAC flapping problem persists, disable one by one the links to the unmanaged switches discarding the possible loop cause.

- Physical troubleshooting: This involves manually checking and disconnecting links that generate loops in network devices, disabling improper connections, switches or faulty cabling.

- Documentation and recovery procedures: This is the elaboration of detailed documentation on the network configuration, changes made to the physical cabling; updating of topology charts and procedures executed in the network restoration; for reference in future similar incidents.

An analysis is carried out by monitoring the Switch Core to check the degradation of the VoIP quality of service, taking as a reference the QoS parameters in Table I. Thus, the packet loss must be less than 1%, the delay less than 150ms and the jitter below 30ms. On these standardised values, it depends that telephone calls are heard clearly, free of echo, without clipping, i.e. with an acceptable QoS [11].

Table I. Parameters determining QoS in VoIP

Variables	Indicators	Ranges	Quantification
Presence of loops or flapping (Independent)	Jitter	0ms ≤ Jitter < 10ms	Excellent
		10ms ≤ Jitter < 20ms	Very Good
		20ms ≤ Jitter < 30ms	Good
		30ms ≤ Jitter < 40ms	Fair
		Jitter ≥ 40ms	Poor
	Delay	0ms≤ Delay < 50ms	Excellent
		50ms ≤ Delay < 100ms	Very Good
		100ms ≤ Delay < 150ms	Good
		150ms ≤ Delay < 200ms	Fair
		Delay ≥ 200ms	Poor
	Packet Loss	PL < 1%	Excellent
		PL > 1%	Poor
Quality of Service (Dependent)	QoS	Q = 5	Excellent
		Q = 4	Very Good
		Q = 3	Good
		Q = 2	Fair
		Q = 1	Poor

4. Results and Discussions

A. VoIP QoS measurements in the presence of MAC flapping

In the following, we present the captures made before a MAC flapping event due to improper connections in loops or loops in the network. It led to a consumption of 100% of the processor of the Switch Core, and the general collapse of the network affecting the VoIP services and Internet access of the campus network called Telematic Network UNMSM; as shown in Figures 5 and 6 respectively.

Fig. 5 shows the log messages with their respective event codes, whose specific meanings are related to network and MAC address management. In addition, the messages indicate the date and time when the events occur. The event code `%MAC_MOVE-4-NOTIF:` indicates that it is a warning notification message (severity level 4) that is related to the movement of MAC addresses in the network. For example, it indicates that the MAC address 000c.2935.6088 is flapping between ports Gi3/2 and Gi4/40 in VLAN 2. MAC flapping means that the MAC address is appearing on different ports of a switch within a short period of time, which can cause network instability.

```
Dec  7 14:59:36.081: %MAC_MOVE-4-NOTIF: Host 001a.6d10.b0e3 in vlan 2 is flapping between port Gi4/40 and port Po1
Dec  7 14:59:36.081: %L2_MMC-4-MMC_MAX: Maximum limit for MAC move counters exceeded for vlan 2
Dec  7 14:59:36.081: %MAC_MOVE-4-NOTIF: Host 000c.2955.124d in vlan 2 is flapping between port Gi3/1 and port Gi4/40
Dec  7 14:59:36.081: %L2_MMC-4-MMC_MAX: Maximum limit for MAC move counters exceeded for vlan 2
Dec  7 14:59:36.081: %MAC_MOVE-4-NOTIF: Host 78da.6eb4.bd70 in vlan 2 is flapping between port Gi3/5 and port Gi4/40
Dec  7 14:59:36.081: %L2_MMC-4-MMC_MAX: Maximum limit for MAC move counters exceeded for vlan 2
Dec  7 14:59:36.085: %MAC_MOVE-4-NOTIF: Host 000c.2935.6088 in vlan 2 is flapping between port Gi3/2 and port Gi4/40
Dec  7 14:59:36.085: %L2_MMC-4-MMC_MAX: Maximum limit for MAC move counters exceeded for vlan 2
Dec  7 14:59:36.085: %MAC_MOVE-4-NOTIF: Host 000c.2935.6088 in vlan 2 is flapping between port Gi3/2 and port Gi4/40
Dec  7 14:59:36.085: %L2_MMC-4-MMC_MAX: Maximum limit for MAC move counters exceeded for vlan 2
Dec  7 14:59:36.085: %MAC_MOVE-4-NOTIF: Host 000c.2935.6088 in vlan 2 is flapping between port Gi3/2 and port Gi4/40
Dec  7 14:59:36.085: %L2_MMC-4-MMC_MAX: Maximum limit for MAC move counters exceeded for vlan 2
Dec  7 14:59:36.085: %MAC_MOVE-4-NOTIF: Host 001a.6d10.b0e3 in vlan 2 is flapping between port Gi4/40 and port Po1
Dec  7 14:59:36.085: %L2_MMC-4-MMC_MAX: Maximum limit for MAC move counters exceeded for vlan 2
Dec  7 14:59:36.085: %MAC_MOVE-4-NOTIF: Host 78da.6eb4.bd70 in vlan 2 is flapping between port Gi3/5 and port Gi4/40
Dec  7 14:59:36.085: %L2_MMC-4-MMC_MAX: Maximum limit for MAC move counters exceeded for vlan 2
Dec  7 14:59:36.085: %MAC_MOVE-4-NOTIF: Host 78da.6eb4.bd70 in vlan 2 is flapping between port Gi3/5 and port Gi4/40
Dec  7 14:59:36.085: %L2_MMC-4-MMC_MAX: Maximum limit for MAC move counters exceeded for vlan 2
Dec  7 14:59:36.085: %MAC_MOVE-4-NOTIF: Host 78da.6eb4.bd70 in vlan 2 is flapping between port Gi3/5 and port Gi4/40
Dec  7 14:59:36.085: %L2_MMC-4-MMC_MAX: Maximum limit for MAC move counters exceeded for vlan 2
Dec  7 14:59:36.085: %MAC_MOVE-4-NOTIF: Host 0008.2fb9.1d98 in vlan 2 is flapping between port Gi4/40 and port Po1
Dec  7 14:59:36.085: %L2_MMC-4-MMC_MAX: Maximum limit for MAC move counters exceeded for vlan 2
Dec  7 14:59:36.085: %MAC_MOVE-4-NOTIF: Host 000c.2935.6088 in vlan 2 is flapping between port Gi3/2 and port Gi4/40
Dec  7 14:59:36.085: %L2_MMC-4-MMC_MAX: Maximum limit for MAC move counters exceeded for vlan 2
Dec  7 14:59:36.085: %MAC_MOVE-4-NOTIF: Host 000c.2935.6088 in vlan 2 is flapping between port Gi3/2 and port Gi4/40
Dec  7 14:59:36.085: %L2_MMC-4-MMC_MAX: Maximum limit for MAC move counters exceeded for vlan 2
Dec  7 14:59:36.085: %MAC_MOVE-4-NOTIF: Host 000c.2935.6088 in vlan 2 is flapping between port Gi3/2 and port Gi4/40
Dec  7 14:59:36.085: %L2_MMC-4-MMC_MAX: Maximum limit for MAC move counters exceeded for vlan 2
Dec  7 14:59:36.085: %MAC_MOVE-4-NOTIF: Host 000c.2935.6088 in vlan 2 is flapping between port Gi3/2 and port Gi4/40
Dec  7 14:59:36.089: %L2_MMC-4-MMC_MAX: Maximum limit for MAC move counters exceeded for vlan 2
Dec  7 14:59:36.089: %MAC_MOVE-4-NOTIF: Host 000c.2935.6088 in vlan 2 is flapping between port Gi3/2 and port Gi4/40
Dec  7 14:59:36.089: %L2_MMC-4-MMC_MAX: Maximum limit for MAC move counters exceeded for vlan 2
Dec  7 14:59:36.089: %MAC_MOVE-4-NOTIF: Host 000c.2935.6088 in vlan 2 is flapping between port Gi3/2 and port Gi4/40
Dec  7 14:59:36.089: %L2_MMC-4-MMC_MAX: Maximum limit for MAC move counters exceeded for vlan 2
Dec  7 14:59:36.089: %MAC_MOVE-4-NOTIF: Host d824.bdbb.ff3f in vlan 2 is flapping between port Te2/4 and port Gi4/40
Dec  7 14:59:36.089: %L2_MMC-4-MMC_MAX: Maximum limit for MAC move counters exceeded for vlan 2
Dec  7 14:59:36.089: %MAC_MOVE-4-NOTIF: Host 000c.2935.6088 in vlan 2 is flapping between port Gi3/2 and port Gi4/40
Dec  7 14:59:36.089: %L2_MMC-4-MMC_MAX: Maximum limit for MAC move counters exceeded for vlan 2
Dec  7 14:59:36.089: %MAC_MOVE-4-NOTIF: Host 000c.2935.6088 in vlan 2 is flapping between port Gi3/2 and port Gi4/40
Dec  7 14:59:36.089: %L2_MMC-4-MMC_MAX: Maximum limit for MAC move counters exceeded for vlan 2
Dec  7 14:59:36.089: %MAC_MOVE-4-NOTIF: Host 000c.2935.6088 in vlan 2 is flapping between port Gi3/2 and port Gi4/40
Dec  7 14:59:36.089: %L2_MMC-4-MMC_MAX: Maximum limit for MAC move counters exceeded for vlan 2
Dec  7 14:59:36.089: %MAC_MOVE-4-NOTIF: Host 78da.6eb4.bd70 in vlan 2 is flapping between port Gi3/5 and port Gi4/40
Dec  7 14:59:36.089: %L2_MMC-4-MMC_MAX: Maximum limit for MAC move counters exceeded for vlan 2
```

Figure 5. Log messages with presence of MAC flapping on VLAN 2

The event code `%L2_MMC-4-MMC_MAX:` indicates that the message is generated by an OSI model layer 2 function (Data Link Layer) and MMC is the abbreviation for "MAC Move Counter", related to the count of MAC address moves. The level 4 severity message indicates a warning for having reached or exceeded the maximum limit of MAC address moves "MMC_MAC:", this suggests that there is an abnormally high number of MAC moves on the network, which may be a symptom of a problem such as network loops or faulty devices.

Fig. 6 shows the CPU usage of the Cisco Core WS-6509E switch of the UNMSM Telematic Network for the last 60 seconds and 60 minutes, generated by executing the show process cpu history command.

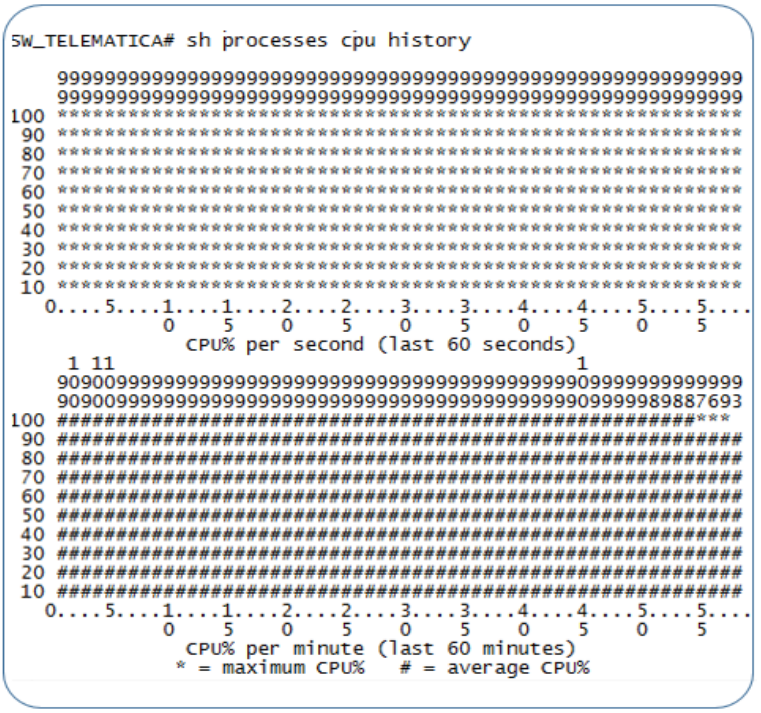


Figure 6. Switch Core CPU utilisation at 100% in MAC flapping event

The Y-axis (vertical) represents the percentage of processor usage, the X-axis (horizontal) represents the elapsed time in 5-second and minute marks respectively. The # symbol represents the average processor usage per minute and the * symbol represents the maximum processor usage per minute. The numbers at the top of the graph indicate the levels achieved by processor usage. Overall, the average CPU usage has been 99.8% for one hour (the last 60 minutes); this is shown by the concentration of # symbols in this part of the graph. The peaks where the maximum CPU usage has reached 100% are verified by the asterisks * that go to the top of the graph. These episodes of high CPU load are correlated in time with MAC flapping events and high traffic processing due to loops in the network, shown in Fig. 5.

Table II shows the values of packet loss and delay parameters with low or poor quantization values, resulting in an average QoS value of 1, which means Bad, and Figure 7 shows graphically the VoIP quality of service.

Table II. VoIP Q..oS in the presence of MAC flapping and 100% Switch Core CPU utilisation

Sample N°	Packet Loss (%)	Quantification of PL	Delay (ms)	Quantification of Delay	Jitter (ms)	Quantification of Jitter	QoS
1	0.8	Excellent	159.64	Fair	0.18	Excellent	2
2	0.9	Excellent	160.17	Fair	0.66	Excellent	2
3	1.2	Poor	160.69	Fair	0.69	Excellent	1
4	1.3	Poor	80.05	Very Good	0.35	Excellent	1
5	1.6	Poor	200.37	Poor	0.51	Excellent	1
6	1	Poor	400	Poor	0.02	Excellent	1
7	1	Poor	240.31	Poor	0.38	Excellent	1
8	0.9	Excellent	120.09	Good	0.53	Excellent	3
9	1.6	Poor	119.61	Good	0.58	Excellent	1
10	1.5	Poor	120.61	Good	0.2	Excellent	1
11	1.4	Poor	140.14	Good	1.02	Excellent	1
12	1.4	Poor	139.56	Good	0.30	Excellent	1
13	1.3	Poor	140.06	Good	0.67	Excellent	1
14	1.3	Poor	100.13	Good	0.63	Excellent	1
15	1.1	Poor	140.14	Good	1.02	Excellent	1
16	1	Poor	140.02	Good	0.46	Excellent	1
17	1	Poor	120.07	Good	0.18	Excellent	1
18	2.9	Poor	140.14	Good	0.21	Excellent	1
19	3.1	Poor	100.97	Good	0.16	Excellent	1
20	3.3	Poor	140.48	Good	0.65	Excellent	1
21	86.2	Poor	560.25	Poor	0.01	Excellent	1
22	97.1	Poor	3163.29	Poor	0.55	Excellent	1
23	97.1	Poor	2979.78	Poor	0.00	Excellent	1
24	97.8	Poor	2919.92	Poor	0.01	Excellent	1
25	99.3	Poor	1582.56	Poor	0.48	Excellent	1
26	99.5	Poor	1580	Poor	0.15	Excellent	1
Average VoIP QoS							**1**

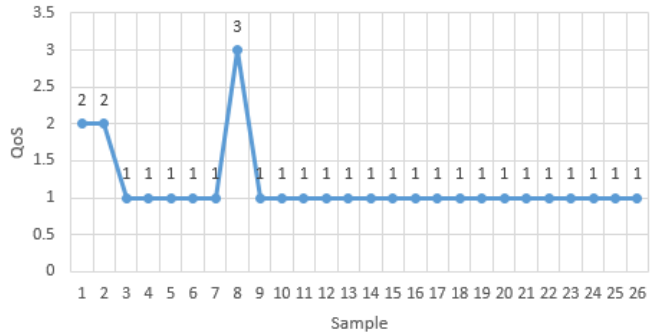


Figure 7. VoIP QoS with presence of MAC flapping

B. VoIP QoS measurements without the presence of MAC flapping

Fig. 8 shows the results with the absence of MAC flapping and the average CPU usage of the Switch Core per minute (#) is between 20% and 30%, indicating a relatively low load during the last hour. Although, there are maximum peaks reaching 88% (*), these are one-off, and do not significantly affect the overall average.

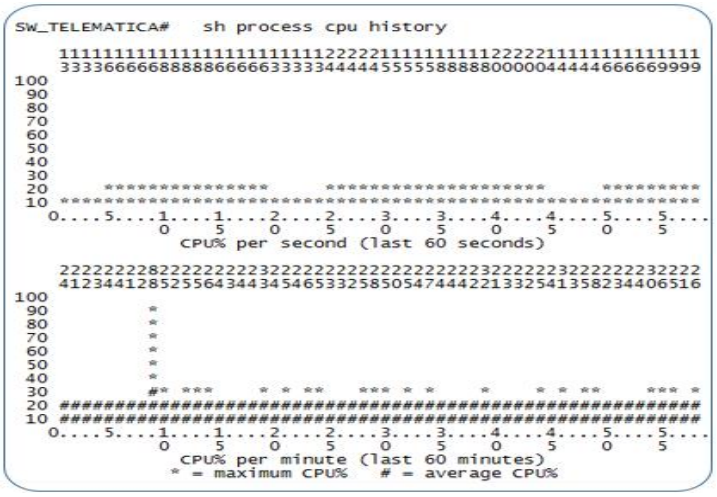


Figure 8. Switch Core CPU utilisation in the absence of MAC flapping

Table III shows the values of the packet loss and delay parameters with high or acceptable quantification values, resulting in an average QoS value of four, which means Very Good, and is shown graphically in Fig. 9.

Table III. VoIP QoS without MAC flapping and Switch Core CPU usage between 20% and 30%

Sample N°	Packet Loss (%)	Quantification of PL	Delay (ms)	Quantification of Delay	Jitter (ms)	Quantification of Jitter	QoS
1	0.8	Excellent	140.14	Good	0.44	Excellent	5
2	0.7	Excellent	140.22	Good	0.43	Excellent	3
3	0.7	Excellent	140.19	Good	0.18	Excellent	3
4	0.7	Excellent	100.04	Good	1.4	Excellent	3
5	0.6	Excellent	143.37	Good	0.4	Excellent	3
6	0.6	Excellent	140.68	Good	0.54	Excellent	3
7	0.6	Excellent	140.52	Good	0.82	Excellent	3
8	0.6	Excellent	140.22	Good	0.53	Excellent	3
9	0.6	Excellent	140.21	Good	0.52	Excellent	3
10	0.6	Excellent	140.01	Good	0.17	Excellent	3
11	0.6	Excellent	139.66	Good	0.19	Excellent	3
12	0.5	Excellent	140.38	Good	0.35	Excellent	3
13	0	Excellent	20.55	Good	0.21	Excellent	3
14	0.7	Excellent	0.13	Excellent	0.65	Excellent	5
15	0.4	Excellent	40.05	Excellent	0.17	Excellent	5
16	0.2	Excellent	40.02	Excellent	2.07	Excellent	5
17	0.1	Excellent	40.15	Excellent	0.38	Excellent	5
18	0	Excellent	40.15	Excellent	0.29	Excellent	5
19	0	Excellent	27.34	Excellent	0.40	Excellent	5
20	0	Excellent	25.42	Excellent	1.66	Excellent	5
21	0	Excellent	25.26	Excellent	2.19	Excellent	5
22	0	Excellent	25.19	Excellent	2.49	Excellent	5
23	0	Excellent	24.53	Excellent	2.32	Excellent	5
24	0	Excellent	24.43	Excellent	2.02	Excellent	5
25	0	Excellent	24.41	Excellent	2.28	Excellent	5
26	0	Excellent	21.6	Excellent	0.27	Excellent	5
27	0	Excellent	20.8	Excellent	0.17	Excellent	5
28	0	Excellent	20.68	Excellent	0.16	Excellent	5
29	0	Excellent	20.55	Excellent	0.17	Excellent	5
30	0	Excellent	0	Excellent	0	Excellent	5
31	0	Excellent	0	Excellent	0	Excellent	5
32	0	Excellent	0	Excellent	0	Excellent	5
33	0.4	Excellent	79.98	Very Good	0.12	Excellent	4
34	0.4	Excellent	60.46	Very Good	0.2	Excellent	4
35	0.3	Excellent	59.95	Very Good	0.57	Excellent	4
36	0.2	Excellent	80.19	Very Good	0.18	Excellent	4
37	0.2	Excellent	60.63	Very Good	1.63	Excellent	4
38	0.1	Excellent	80.15	Very Good	0.47	Excellent	4
Average VoIP QoS							**4**

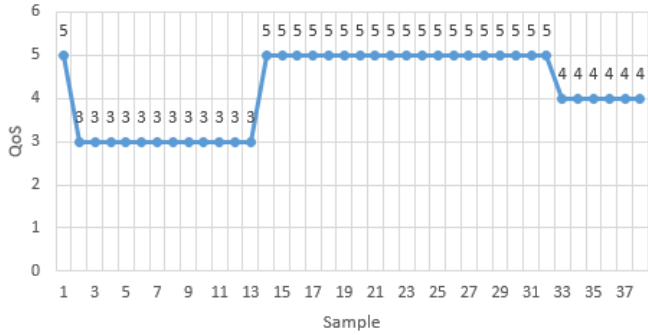


Figure 9. VoIP QoS in the absence of MAC flapping

C. Simulation of the UNMSM Telematic Network in GNS3

For testing purposes, simulations of various scenarios of interest are carried out [12]. Thus, the simulation of the UNMSM Telematic Network was carried out with the GNS3 software (Graphic Network Simulator-3) in a virtualised environment on VMware Workstation 16 Pro. Fig. 10 shows the network diagram considered for the test.

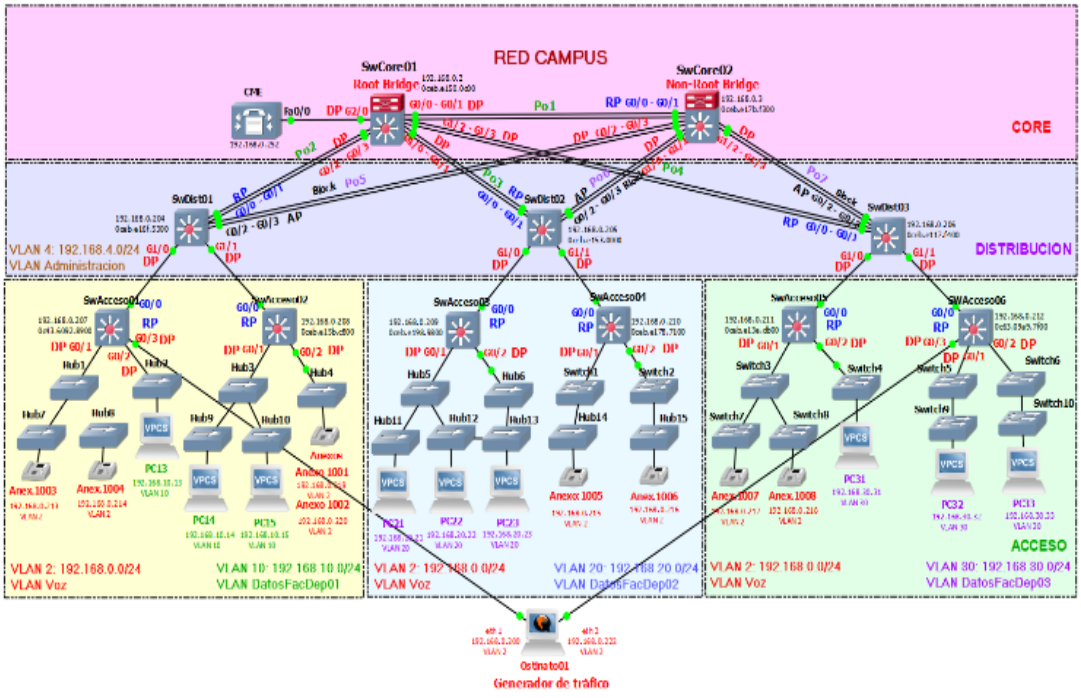


Figure 10. GNS3 Simulation of the UNMSM Telematic Network

To simulate the Core, Distribution and Access Switches we used the image vios_l2-adventerprisek9-m.03.2017.qcow2, with virtual disk format QEMU (Quick EMUlator), which corresponds to a Cisco Layer 2 virtual switch with advanced functionalities such as: VLANs, Trunking (802.1Q), STP, EtherChannel, QoS and ACLs; among others.

For the CME (Cisco Unified Communications Manager Express) we used the image c3725-adventerprisek9-mz.124-15.T14.image, which is a Dynamips emulation of the Cisco 3725 router, belonging to the 3700 series of modular routers, equipped to handle data, voice and video applications with QoS.

In the case of the Cisco IP Phone (CIPC 2.1.3.0), these were installed in virtual machines with Windows 98 operating system, configured in VirtualBox, to integrate with the GNS3 network topology.

Ostinato software is also used to generate and analyse network traffic, and to analyse the VoIP QoS in the simulation. For this purpose, the ostinatostd-1.3.0-1.qcow2 image was used in a QEMU VM preconfigured with Ostinato compatible with VMWare.

The simulation considers the main characteristics and functionalities of the UNMSM Campus network, which has VLANs (Virtual Local Area Networks) for the logical segmentation of the physical network into networks corresponding to the faculties and departments, providing improvements in terms of management, security, performance and scalability. Three Data VLANs are considered in the simulation: VLAN 10, 20 and 30; and VLAN 2 as Voice VLAN, which is applied to the entire Campus network, to prioritise VoIP traffic over other types of traffic, ensuring that voice calls have low latency and minimal packet loss. Also, VLAN 4 is configured as the native VLAN or Administrative VLAN. The switches are configured with Rapid Per-VLAN Spanning Tree Plus (Rapid PVST+), which is an enhanced version of the STP protocol that enables faster convergence, on a per-VLAN basis.

QoS for VoIP is implemented on all switches in the network. By classifying, marking and prioritising VoIP traffic, it can ensure that voice calls have low latency and minimal packet loss, providing an optimal user experience. It also considers the three hierarchical levels of network structure:

Core Layer: It consists of two Core Switches connected together by two 1Gbps backbone links configured in EtherChannel, to increase bandwidth. To provide high availability and redundancy, HSRP (Hot Standby Router Protocol) was configured between the layer 3 Core Switches to ensure that, in the event of failure of one of the switches, the other takes on the role of gateway, maintaining connectivity in the network. The SwCore01 switch is configured with a lower priority value, which sets a higher STP priority for the VLANs, causing it to be assigned as the Root Bridge of the network.

Distribution Layer: Consists of three Distribution Switches connected to each Core Switch by two 1Gbps EtherChannel backbone links, to guarantee network service availability and increase bandwidth. RSTP determines the forwarding ports and blocked ports on the switches, activating or deactivating EtherChannel links, building a topology free of logical loops. Each Distribution Switch in turn connects to two Access Switches via 1Gbps backbone links.

Access Layer: The Access Switches are connected to the Distribution Switches by 1Gbps trunk links and to the unmanaged switches and hubs by 1Gbps access links to extend the network points in each Faculty and Unit. Data and Voice VLAN access ports are configured with PortFast and BPDU Guard in order to optimise STP convergence time and protect the network against network loops caused by unauthorised devices. PortFast ensures that end devices can start sending and receiving traffic immediately, while BPDU Guard protects the network

topology from unwanted changes. Implementing these configurations improves both the efficiency and security of the campus network.

Finally, the Cisco 3725 router, configured as Cisco Unified Communications Manager Express, enables VoIP services on the campus network. The subinterface configuration allows traffic to be segmented into VLANs, and the CME configuration provides PBX services, including support for six IP phones and directory numbers or attachments. The configuration can handle up to 100 IP phones and 500 directory numbers, providing full VoIP functionality for a small to medium-sized organisation.

To measure the VoIP QoS, Wireshark captures were taken during the course of telephone calls between attachments, with and without the presence of loops, verifying the degradation of service due to MAC flapping. These tests were also replicated with Ostinato, the VoIP traffic generator, with and without the presence of loops in the network:

- Ostinato v1.3 software configuration for VoIP traffic generation in GNS3 network simulation.

The test encompasses the entire network, including all devices, connections and configurations that make up the test network. In the context of Ostinato, NUT (Network Under Test) is the complete simulated environment consisting of the switches, the CME router, the softphones, the workstations and any other devices involved in the test topology.

To verify, the QoS of the VoIP traffic generated by Ostinato v1.3 in a simulated network in GNS3, RTP or SIP traffic streams are created, and an appropriate QoS is assigned based on 802.1Q VLAN priority and/or IPv4 TOS/DSCP.

To configure the VoIP stream parameters in the Ethernet II and IPv4 header, the source addresses are considered to be those corresponding to the Ostinato eth1 (traffic generator) port and the destination addresses are considered to be those corresponding to the Ostinato eth2 (traffic receiver) port. The DSCP value is assigned with EF (Expedited Forwarding), in decimal 46, ECN (Explicit Congestion Notification) with ECT(0) and Priority in VLAN 2 (PCP) with value 5, recommended for VoIP traffic. In the UDP header, the destination port is set to 5060 (for SIP) or RTP port. In the payload, a pattern representing voice traffic is selected, such as a continuous 64 kbps transmission rate to simulate G.711 codec traffic. The configuration is shown in Fig. 11.

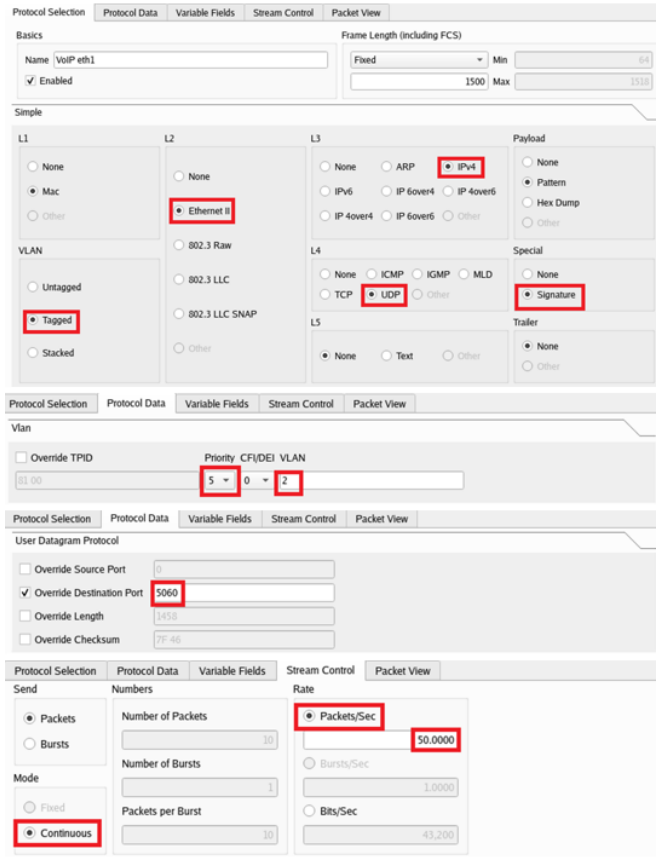
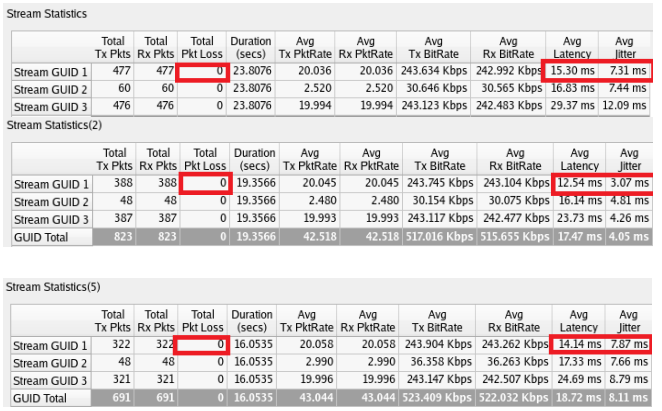


Figure 11. Editing VoIP stream protocols

For the test, it was necessary to generate multiple traffic flows with different QoS for each flow, in interlaced transmissions, so that the NUT can prioritise the flows with higher priority and discard (if necessary) those with lower priority. The traffic flows considered were VoIP, video and data, from which their respective statistics such as packet loss, latency and jitter were obtained.

- Testing for VoIP QoS measurement with Ostinato v1.3 traffic generator on a simulated network in GNS3, without loops.

Fig. 12 shows the results of packet loss, latency and jitter measurements for the three traffic flows injected into the network without loops. The GUID stream 1, 2 and 3 correspond to VOIP, video and data traffic flows respectively. It should be noted that in all cases the latency and jitter are lower for the VoIP traffic flow, as it has a higher priority than the video and data streams.



Stream Statistics

	Total Tx Pkts	Total Rx Pkts	Total Pkt Loss	Duration (secs)	Avg Tx PktRate	Avg Rx PktRate	Avg Tx BitRate	Avg Rx BitRate	Avg Latency	Avg Jitter
Stream GUID 1	477	477	0	23.8076	20.036	20.036	243.634 Kbps	242.992 Kbps	15.30 ms	7.31 ms
Stream GUID 2	60	60	0	23.8076	2.520	2.520	30.646 Kbps	30.565 Kbps	16.83 ms	7.44 ms
Stream GUID 3	476	476	0	23.8076	19.994	19.994	243.123 Kbps	242.483 Kbps	29.37 ms	12.09 ms

Stream Statistics(2)

	Total Tx Pkts	Total Rx Pkts	Total Pkt Loss	Duration (secs)	Avg Tx PktRate	Avg Rx PktRate	Avg Tx BitRate	Avg Rx BitRate	Avg Latency	Avg Jitter
Stream GUID 1	388	388	0	19.3566	20.045	20.045	243.745 Kbps	243.104 Kbps	12.54 ms	3.07 ms
Stream GUID 2	48	48	0	19.3566	2.480	2.480	30.154 Kbps	30.075 Kbps	16.14 ms	4.81 ms
Stream GUID 3	387	387	0	19.3566	19.993	19.993	243.117 Kbps	242.477 Kbps	23.73 ms	4.26 ms
GUID Total	823	823	0	19.3566	42.518	42.518	517.016 Kbps	515.655 Kbps	17.47 ms	4.05 ms

Stream Statistics(5)

	Total Tx Pkts	Total Rx Pkts	Total Pkt Loss	Duration (secs)	Avg Tx PktRate	Avg Rx PktRate	Avg Tx BitRate	Avg Rx BitRate	Avg Latency	Avg Jitter
Stream GUID 1	322	322	0	16.0535	20.058	20.058	243.904 Kbps	243.262 Kbps	14.14 ms	7.87 ms
Stream GUID 2	48	48	0	16.0535	2.990	2.990	36.358 Kbps	36.263 Kbps	17.33 ms	7.66 ms
Stream GUID 3	321	321	0	16.0535	19.996	19.996	243.147 Kbps	242.507 Kbps	24.69 ms	8.79 ms
GUID Total	691	691	0	16.0535	43.044	43.044	523.409 Kbps	522.032 Kbps	18.72 ms	8.11 ms

Figure 12. Stream statistics with QoS indicators for different traffic streams

Table IV shows the values of packet loss, latency and jitter indicators with high quantification values, giving an average QoS value of 5, which means Excellent, and is shown graphically in Fig. 13.

Table IV. VoIP QoS in simulated network on GNS3 without loops present.

Sample N°	Packet Loss (%)	Quantification of PL	Delay (ms)	Quantification of Delay	Jitter (ms)	Quantification of Jitter	QoS
1	0	Excellent	15.30	Excellent	0.44	Excellent	5
2	0	Excellent	12.54	Excellent	0.43	Excellent	5
3	0	Excellent	14.14	Excellent	0.18	Excellent	5
Average VoIP QoS							**5**

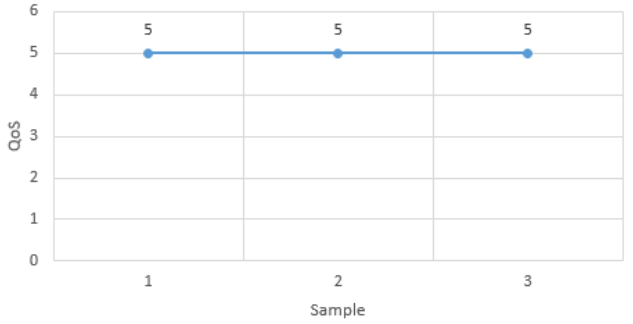


Figure 13. VoIP QoS in simulated network on GNS3 without loops

- Tests for VoIP QoS measurement with Ostinato v1.3 traffic generator, with the presence of two loops.

Fig. 14 shows the topology of the simulated network in GNS3 with two loops caused by improper connections on unmanageable equipment. As a result, SwCore02, SWDist01 and SWAccess02 become inoperative.

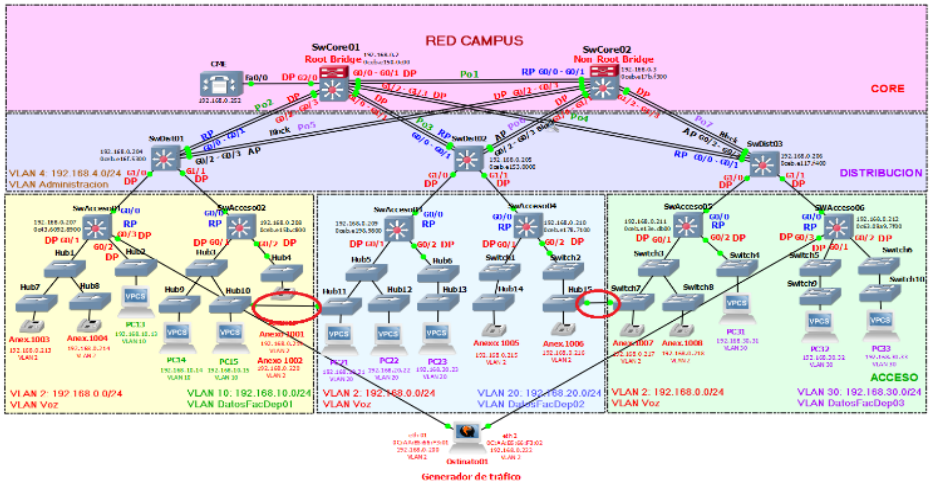


Figure 14. Network topology with presence of loops

Next, Fig. 15 presents the results of the packet loss, latency and jitter measurements of the three VoIP, video and data traffic flows (GUI 1, 2 and 3) injected in the network with presence of loops. The packet loss is total due to the collapse of SwCore02, SwDist01 and Access02.

Stream Statistics(31)

	Total Tx Pkts	Total Rx Pkts	Total Pkt Loss	Duration (secs)	Avg Tx PktRate	Avg Rx PktRate	Avg Tx BitRate	Avg Rx BitRate	Avg Latency	Avg Jitter
Stream GUID 1	304	0	304	92.9695	3.270	0.000	39.762 Kbps	0.000 bps	-	-
Stream GUID 2	228	0	228	92.9695	2.452	0.000	29.821 Kbps	0.000 bps	-	-
Stream GUID 3	1,860	0	1,860	92.9695	20.007	0.000	243.280 Kbps	0.000 bps	-	-
GUID Total	2,392	0	2,392	92.9695	25.729	0.000	312.863 Kbps	0.000 bps	-	-

Stream Statistics(32)

	Total Tx Pkts	Total Rx Pkts	Total Pkt Loss	Duration (secs)	Avg Tx PktRate	Avg Rx PktRate	Avg Tx BitRate	Avg Rx BitRate	Avg Latency	Avg Jitter
Stream GUID 4	136	0	136	25.1678	5.404	0.000	65.709 Kbps	0.000 bps	-	-
Stream GUID 5	38	0	38	25.1678	1.510	0.000	18.360 Kbps	0.000 bps	-	-
Stream GUID 6	37	0	37	25.1678	1.470	0.000	17.877 Kbps	0.000 bps	-	-
GUID Total	211	0	211	25.1678	8.384	0.000	101.946 Kbps	0.000 bps	-	-

Stream Statistics(33)

	Total Tx Pkts	Total Rx Pkts	Total Pkt Loss	Duration (secs)	Avg Tx PktRate	Avg Rx PktRate	Avg Tx BitRate	Avg Rx BitRate	Avg Latency	Avg Jitter
Stream GUID 1	144	0	144	43.1056	3.341	0.000	40.622 Kbps	0.000 bps	-	-
Stream GUID 2	108	0	108	43.1056	2.505	0.000	30.467 Kbps	0.000 bps	-	-
Stream GUID 3	863	0	863	43.1056	20.021	0.000	243.451 Kbps	0.000 bps	-	-
GUID Total	1,115	0	1,115	43.1056	25.867	0.000	314.539 Kbps	0.000 bps	-	-

Figure 15. Stream statistics with QoS indicators for different traffic flows in the presence of loops.

Table V shows the values of packet loss, latency and jitter indicators with low quantification values, since there is a packet loss of 100%, which gives an average QoS value of 1, meaning Bad, as shown in Figure 16.

Table V. QoS for VoIP service in simulated network with presence of loops

Sample N°	Packet Loss (%)	Quantification of PL	Delay (ms)	Quantification of Delay	Jitter (ms)	Quantification of Jitter	QoS
1	100	Poor	-		-		1
2	100	Poor	-		-		1
3	100	Poor	-		-		1
Average VoIP QoS							1

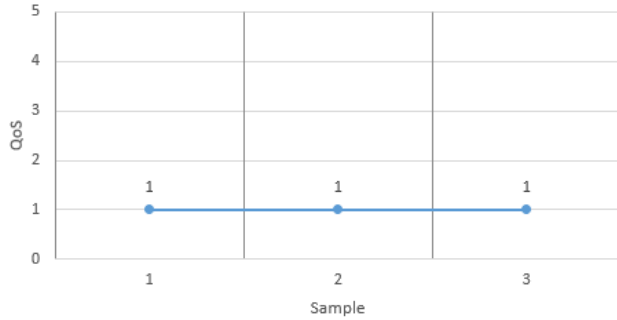


Figure 16. VoIP QoS in simulated network with loops

D. Proposal for improvement

To address the problem presented by the presence of loops in a campus network with traditional topology, which at the access layer level has a third of unmanageable equipment, it is proposed to rethink the Campus Network with VxLAN - EVPN technology, an effective solution to manage and protect workloads caused by massive applications in campus and data center environments.

Extensible Virtual Local Area Networks (VxLAN) allow the creation of a logical network overlay on top of an existing physical network. This overlay network is composed of VxLAN tunnels, each with a VNI (Virtual Network Identifier). In a VxLAN, the physical switches do not need to learn all the MAC addresses of the end devices. Instead, they only need to know the MAC addresses of the VTEs (VxLAN Tunnel Endpoints). This can reduce the load on physical switches and the frequency of MAC table updates, mitigating MAC flapping. In addition, VxLAN encapsulates Ethernet packets into UDP packets, transporting them across the physical network. This encapsulation can help isolate and contain the effects of MAC flapping within the VXLAN tunnel, preventing it from propagating to the underlying physical network.

5. Conclusion

It has been determined that flapping or loops caused by improper connections and faulty equipment have a significant influence on the degradation of VoIP Service quality in a campus network, specifically in the case of the UNMSM telematics network. Also, if packet loss, latency, jitter and excessive use of CPU resources of the Switch Core are indicators that are associated with the occurrence of flapping or loops. Indeed, the CPU consumption of the Switch Core reaches 100% when there are network problems such as flapping, and when there are no network problems the CPU consumption reaches 30% or 40% on average, which is an indicator of the presence of loops. The quantification of the parameters makes it possible to represent any sample and give an approximation of the QoS level, which benefits network administrators as they can keep this dependent variable monitored.

The results show the need for a software tool that provides early warning of the presence of flapping and calculates the QoS in real time, whose inputs are the readings of the QoS parameters, and whose output is the activation of a set of alarms when the QoS is affected.

Likewise, it is convenient to establish an adequate signalling policy in the network devices from computers, IP telephones, switches and other network devices, with the purpose of adequate connectivity and care of the equipment. Finally, it is necessary to consider the renewal of network devices at least every five years, in order to help the optimal functioning of the network.

References

1. C. Boutremans, G. Iannaccone, and C. Diot, “Impact of link failures on VoIP performance,” Proceedings of the 12th international workshop on Network and operating systems support for digital audio and video (NOSSDAV '02), pp. 63-71, May 12-14, 2002.
2. M. H. Miraz, M. A. Ganie, S. A. Molvi, M. Ali, and A. H. Hussein, “Simulation and Analysis of Quality of Service (QoS) Parameters of Voice over IP (VoIP) Traffic through Heterogeneous Networks,” International Journal of Advanced Computer Science and Applications (IJACSA), vol. 8, no. 7, pp. 242-248, 2017.
3. Q. A. Hidayaturrohman and B. A. Wardijono, “Implementation and Analysis Quality of Service Voice over IP on Wide Area Network,” Technical Report, Teknik Elektro, Fakultas Teknologi Industri, Universitas Gunadarma, 2014.
4. S. Dhanalakshmi, M. Sathiya, and R. Gowthami, “Investigating The Performance Of Voip Over Ethernet Lan in Campus Network,” International Journal of Recent Scientific Research, vol. 6, no. 6, pp. 4389-4394, 2015.
5. Z. Fan and L. X. Wu, "Network Effects and the Stability of Loop Networks," 2011 International Conference of Information Technology, Computer Engineering and Management Sciences, pp. 249-253, Nanjing, China, 2011.
6. K. Elmeleegy, A. L. Cox and T. S. E. Ng, "Understanding and Mitigating the Effects of Count to Infinity in Ethernet Networks," in IEEE/ACM Transactions on Networking, vol. 17, no. 1, pp. 186-199, Feb. 2009.
7. K. Elmeleegy, A. L. Cox and T. S. E. Ng, "On Count-to-Infinity Induced Forwarding Loops Ethernet Networks," Proceedings 25th IEEE International Conference on Computer Communications (INFOCOM), pp. 1-13, Barcelona, Spain, 2006.
8. M. Maier and J. Ullrich, “In the loop: A measurement study of persistent routing loops on the IPv4/IPv6 Internet,” Computer Networks, vol. 221, 109500, February 2023.
9. S. Mani and M. J. Nene, "Data Loss Prevention due to Link-flapping using Software Defined Networking," IEEE 6th International Conference for Convergence in Technology (I2CT), pp. 1-5, Maharashtra, India, 2021.
10. J. Ali, G. Lee, B. Roh, D. K. Ryu, and G. Park, “Software-Defined Networking Approaches for Link Failure Recovery: A Survey,” Sustainability, vol. 12, 4255, 2020.
11. R. C. Streijl, S. Winkler, and D. S. Hands, "Mean opinion score (MOS) revisited: methods and applications, limitations and alternatives," Multimedia Systems, vol. 22, no 2, pp. 213–227, March 2016.
12. Q. Liu, “Hardware-Free Network Internals Exploration: A Simulation-Based Approach for Online Computer Networking Course,” International Journal of Innovative Teaching and Learning in Higher Education, vol. 5, no. 1, pp. 1-16, 2024.