



**UNIVERSIDAD POLITÉCNICA SALESIANA
SEDE QUITO**

CARRERA DE TELECOMUNICACIONES

**DISEÑO DE UNA ARQUITECTURA SPINE LEAF PARA LA RED DEL
DATA CENTER DEL CAMPUS SUR BLOQUE D DE LA UNIVERSIDAD
POLITÉCNICA SALESIANA.**

**Trabajo de titulación previo a la obtención del
Título de Ingeniero en Telecomunicaciones**

**AUTORES: JOHN MICHAEL AGUILAR AGUIRRE
HENRY DAVID ATI GRANJA**

DIRECTORA: VERÓNICA EMMA SORIA MALDONADO

**Quito – Ecuador
2023**

CERTIFICADO DE RESPONSABILIDAD Y AUTORÍA DEL TRABAJO DE TITULACIÓN

Nosotros, John Michael Aguilar Aguirre y Henry David Ati Granja, con documento de identificación N° 1104470941 y N° 1727087189 manifestamos que:

Somos los autores y responsables del presente trabajo; y, autorizamos a que sin fines de lucro la Universidad Politécnica Salesiana pueda usar, difundir, reproducir o publicar de manera total o parcial el presente trabajo de titulación.

Quito, 01 de Agosto del año 2023.

Atentamente,



John Michael Aguilar Aguirre

1104470941



Henry David Ati Granja

1727087189

**CERTIFICADO DE CESIÓN DE DERECHOS
DE AUTOR DEL TRABAJO DE TITULACIÓN
A LA UNIVERSIDAD POLITÉCNICA
SALESIANA.**

Nosotros, John Michael Aguilar Aguirre y Henry David Ati Granja, con documento de identificación N° 1104470941 y N° 1727087189, expresamos nuestra voluntad y por medio del presente documento cedemos a la Universidad Politécnica Salesiana la titularidad sobre los derechos patrimoniales en virtud de que somos los autor del Proyecto Técnico: "Diseño de una arquitectura Spine Leaf para la red del data center del campus sur bloque D de la universidad politécnica salesiana", el cual ha sido desarrollado para optar por el título de: Ingeniero en Telecomunicaciones, en la Universidad Politécnica Salesiana, quedando la Universidad facultada para ejercer plenamente los derechos cedidos anteriormente.

En aplicación a lo determinado en la Ley de Propiedad Intelectual, en mi condición de autor nos reservamos los derechos morales de la obra antes citada. En concordancia, suscribimos este documento en el momento que hacemos la entrega del trabajo final en formato impreso y digital a la Biblioteca de la Universidad Politécnica Salesiana.

Quito, 01 de Agosto del año 2023.

Atentamente,



John Michael Aguilar Aguirre

1104470941



Henry David Ati Granja

1727087189

CERTIFICADO DE DIRECCIÓN DEL TRABAJO DE TITULACIÓN

Yo, Verónica Emma Soria Maldonado con documento de identificación N°0000000000, docente de la Universidad Politécnica Salesiana , declaro que bajo mi tutoría fue desarrollado el trabajo de titulación: ” DISEÑO DE UNA ARQUITECTURA SPINE LEAF PARA LA RED DEL DATA CENTER DEL CAMPUS SUR BLOQUE D DE LA UNIVERSIDAD POLITÉCNICA SALESIANA.”, realizado por John Michael Aguilar Aguirre y Henry David Ati Granja, con documento de identificación N° 1104470941 y N° 1727087189, obteniendo como resultado final el trabajo de titulación bajo la opción Proyecto Técnico que cumple con todos los requisitos determinados por la Universidad Politécnica Salesiana.

Quito, 01 de Agosto del año 2023.

Atentamente,



Ing. Verónica Emma Soria Maldonado, MSc

1715185961

DEDICATORIA

El presente trabajo está dedicado a mi familia, a mi hermana que desde el cielo me ha brindado su protección y bendición para llegar a alcanzar mis metas; y también está dedicado a mis padres y mi hermano que han sido un apoyo incondicional frente a las adversidades que se han presentado en mi vida; sin cada uno de ellos esto no hubiera sido posible.

HENRY ATI.

Este trabajo va dedicado especialmente a mis abuelitos que son mis padres, ya que ellos siempre me guiaron, me dieron siempre su bendición y sus consejos para lograr alcanzar mis metas, a mi mamá y a mis hermanas que también estuvieron conmigo en el transcurso de mi carrera, a toda mi familia que siempre me apoyó y nunca me dejaron solo, ya que sin su apoyo no hubiese llegado tan lejos.

JOHN AGUILAR.

AGRADECIMIENTO

Quiero agradecer a Dios, por brindarme la salud y ser mi guía para poder llegar a cumplir mis metas. Agradezco también a mis padres, por su esfuerzo diario para que yo pueda tener educación una de calidad y por todo el sacrificio que han hecho por mí. Quiero también agradecer a mi hermano por su apoyo incondicional en los momentos difíciles que se han presentado en mi vida y también por los sacrificios que él ha realizado para que yo pueda llegar a cumplir este objetivo tan importante en mi vida.

Quiero también agradecer de forma muy especial a la Ingeniera Verónica Soria, por su ayuda y apoyo para llevar a cabo el presente proyecto; finalmente agradezco a la noble institución, la Universidad Politécnica Salesiana y con ello a cada uno de los profesores que tuve durante mi vida académica por los conocimientos brindados en este tiempo. Finalmente agradezco a mi compañero de tesis John por amistad y ayuda en este proyecto.

HENRY ATI.

AGRADECIMIENTO

Quiero agradecer primeramente a Dios y a la Virgencita por darme la salud, vida y la sabiduría para salir adelante, por guiarme, ser mi apoyo y fortaleza en aquellos momentos de dificultad y debilidad.

Agradecer a mis abuelitos Santos Aguirre y María Castillo que son mis padres y ser siempre los principales promotores de mis sueños, ya que siempre me brindan su apoyo incondicional para lograr cumplir todas mis metas y objetivos personales y académicos, ellos son los que con su cariño me han inspirado siempre a perseguir mis metas y nunca dejarlas frente a las adversidades de la vida.

Agradecer a mi mamá Daysi que me apoyó en el transcurso de mi carrera y que nunca me abandonó a igual que mis hermanas Adriana y Ani.

A mi tíos José Páez y Fanny Aguirre que me abrieron sus puertas, ayudarme en todo momento con sus consejos, sabiduría para culminar mi objetivo ya que siempre están conmigo en las buenas y en las malas, a mi primo Efrén Pardo que es un pilar fundamental para mi carrera y que siempre me ha apoyado. A toda mi familia que siempre está conmigo incondicionalmente y que siempre estuvieron conmigo y que nunca me dejaron solo para poder culminar mi carrera.

Agradecer a mi jefe Ricardo Zapata que, desde cuando entré a trabajar me apoyó con flexibilidad en el trabajo para poder desarrollar y culminar con los objetivos propuestos.

Quiero también agradecer de una manera muy especial a la Ingeniera Verónica Soria, por su ayuda y apoyo para desarrollar a cabo el presente proyecto, también agradecer a la Universidad Politécnica Salesiana a toda la facultad de ingeniería en Telecomunicaciones, a los ingenieros quienes con sus enseñanzas y sus valiosos conocimientos lograron que pueda ir creciendo día a día como un profesional, mis sinceros agradecimientos a cada uno por su dedicación, paciencia, apoyo incondicional y amistad.

A todos mis compañeros y amigos, a Henry Ati que siempre estuvimos en las buenas y malas desde el comienzo hasta el final.

JOHN AGUILAR.

ÍNDICE DE CONTENIDO

Tabla de contenido

CERTIFICADO DE RESPONSABILIDAD Y AUTORÍA DEL TRABAJO DE TITULACIÓN.....	i
CERTIFICADO DE CESIÓN DE DERECHOS DE AUTOR DEL TRABAJO DE TITULACIÓN A LA UNIVERSIDAD POLITÉCNICA SALESIANA.	ii
CERTIFICADO DE DIRECCIÓN DEL TRABAJO DE TITULACIÓN	iii
DEDICATORIA.....	iv
AGRADECIMIENTO	v
AGRADECIMIENTO	vi
ÍNDICE DE CONTENIDO.....	vii
ÍNDICE DE FIGURAS	xii
RESUMEN	15
ABSTRACT.....	16
CAPÍTULO 1	17
1.1 PROBLEMA DE ESTUDIO.....	17
1.2 OBJETIVOS	18
1.3 JUSTIFICACIÓN	19
1.4 METODOLOGÍA	20
1.4.1 Paradigma de Investigación.	20
1.4.2 Tipo de Investigación.	20
1.4.3 Alcance.....	20

1.4.4 Unidad de Análisis.....	20
1.5 DISEÑO DE LA INVESTIGACIÓN.....	20
1.5.1 Enfoque cuantitativo y cualitativo.....	20
1.5.2 Experimental.....	20
1.6 MARCO CONCEPTUAL.....	21
1.7 DATA CENTER.....	21
<i>1.7.1 Continuidad de negocio.....</i>	<i>21</i>
<i>1.7.2 Velocidad de respuesta.....</i>	<i>21</i>
<i>1.7.3 Seguridad de la información.....</i>	<i>21</i>
<i>1.7.4 Alta capacidad de almacenamiento.....</i>	<i>22</i>
<i>1.7.5 Simplicidad.....</i>	<i>22</i>
<i>1.7.6 Escalabilidad.....</i>	<i>22</i>
<i>1.7.8 Flexibilidad.....</i>	<i>22</i>
<i>1.7.9 Eficiencia y confiabilidad.....</i>	<i>22</i>
1.8 REQUISITOS DE UN CENTRO DE DATOS.....	22
<i>1.8.1 Suministros de energía.....</i>	<i>22</i>
<i>1.8.2 Refrigeración.....</i>	<i>22</i>
<i>1.8.3 Seguridad física y virtual.....</i>	<i>23</i>
1.9 TIPOS DE CENTROS DE DATOS.....	23
1.10. CENTRO DE DATOS TRADICIONAL.....	23
1.11 CENTRO DE DATOS MODULAR.....	23

1.12	CENTRO DE DATOS EN LA NUBE.....	24
1.13	TIPOS DE SERVICIOS OFERTADOS POR CENTROS DE DATOS EN NUBE.	25
<i>1.13.1</i>	<i>Software como un servicio (SaaS).....</i>	<i>25</i>
<i>1.13.2</i>	<i>Plataforma como un servicio (PaaS).....</i>	<i>25</i>
<i>1.13.3</i>	<i>Infraestructura como un servicio (IaaS).....</i>	<i>25</i>
1.14	TIPOS DE ARQUITECTURAS PARA UN CENTRO DE DATOS.....	25
1.15	ARQUITECTURA TRADICIONAL	25
1.16	ARQUITECTURA SPINE AND LEAF	26
1.17	CERTIFICACIONES DE CENTRO DE DATOS (TIERS)	27
1.17.1	TIER I	27
1.17.2	TIER II.....	27
1.17.3	TIER III.....	28
1.17.4	TIER IV	28
1.18	REDES SAN	28
1.19	PROTOCOLOS USADOS EN LA REDES SAN	29
1.20	PING	29
1.21	COMO USAR EL COMANDO DE PING	30
<i>1.21.1</i>	<i>BYTES.....</i>	<i>30</i>
<i>1.21.2</i>	<i>TIEMPO.....</i>	<i>30</i>
<i>1.21.3</i>	<i>TTL.....</i>	<i>30</i>
<i>1.21.4</i>	<i>PAQUETES.....</i>	<i>31</i>

1.21.5	TIEMPO DE RESPUESTA EN MS	31
1.22	USO DEL PING PARA COMPROBAR UNA RED	31
1.23	PING DIVULGADA LOCAL DIRIGIDA.....	31
1.24	HACIA EL ENRUTADOR.....	31
1.25	INUNDACIÓN DE PING CIEGO.....	31
1.26	PING FLOOD	31
SITUACIÓN ACTUAL.....		33
CAPÍTULO 2		33
2.1	RED ACTUAL DEL DATA CENTER DEL BLOQUE D.....	33
2.2	SISTEMAS DE TEMPERATURA.....	37
2.3	SISTEMA DE ENERGÍA.....	38
2.4	ANÁLISIS DE LA RED CON AYUDA DEL SOFTWARE WIRE SHARK.....	38
2.5	Datos generales de la captura de tráfico.....	38
2.6	Transmisión de paquetes por puntos finales	39
2.7	Protocolo de mayor uso.....	40
2.8	Transmisión de paquetes por tiempo.	42
CAPÍTULO 3		43
3.1.	DISEÑO E INFRAESTRUCTURA DE LA NUEVA RED.....	43
3.2.	Diseño de la nueva topología.	43
3.3.	Equipos usados en la implementación.	45
3.4.	Configuración de los equipos (switch capa 3) serie 3650.....	45

3.5. Servidor de llamadas BigAnt Messenger	48
3.6. Servidor de Juego (Counter Strike).....	52
3.7. Creación de máquinas virtuales mediante TightVNC Viewer.	53
3.8. Generación de ping extendido con carga de bytes	56
CAPÍTULO 4	58
4.1 RESULTADOS	58
4.2 CAPTURA SPINE 1	58
4.3 TRANSMISIÓN DE PAQUETES POR TIEMPO.	59
4.4 Spine 2.....	60
4.5 PROTOCOLO DE MAYOR USO.....	60
4.6 TRANSMISIÓN DE PAQUETES POR TIEMPO	61
4.7. PARÁMETROS DE RENDIMIENTO CON LA NUEVA ARQUITECTURA.	63
CAPÍTULO 5	65
5.1. CONCLUSIONES	65
5.2. RECOMENDACIONES	66
6. BIBLIOGRAFÍA	67
CAPÍTULO 7	69
ANEXOS.....	69
7.1. ANEXO #1: VLAN TRUNK PROTOCOL	69
7.2 ANEXO #2: DATASHEET DEL SWITCH CISCO NEXUS	70
7.3 ANEXO #3: DATASHEET DEL SWITCH CISCO 3650	70

ÍNDICE DE FIGURAS

GRÁFICO 1: DISTRIBUCIÓN DE LA ARQUITECTURA TRADICIONAL DE UN DATA CENTER “ARQUITECTURA DEL CENTRO DE DATOS, DATA CENTER - BLOG DE DATA CENTER, CLOUD.” RECUPERADO DE: HTTPS://WWW.ARUBANETWORKS.COM/FAQ/WHAT-IS-SPINE-LEAF-ARCHITECTURE/ (ACCESSED MAR. 04, 2023).....	26
GRÁFICO 2: DISTRIBUCIÓN DE LA ARQUITECTURA SPINE LEAF DE UN CENTRO DE DATOS “ARQUITECTURA DEL CENTRO DE DATOS, DATA CENTER - BLOG DE DATA CENTER, CLOUD.” RECUPERADO DE: HTTPS://WWW.ARUBANETWORKS.COM/FAQ/WHAT-IS-SPINE-LEAF-ARCHITECTURE/ (ACCESSED MAR. 04, 2023)	27
GRÁFICO 3: CAPTURA DE CÓMO REALIZAR UN PING A LA PÁGINA DE GOOGLE. RECUPERADO DE UNA CAPTURA DE JOHN Y HENRY	30
GRÁFICO 4: ESTRUCTURA ACTUAL DEL DATA CENTER (TRADICIONAL) UBICADA EN EL SEGUNDO PISO DEL BLOQUE D DE LA UPS. ELABORADO POR EL DEPARTAMENTO DEL DATA CENTER.....	34
GRÁFICO 5: DIAGRAMA DE RED DEL DATA CENTER EXTENDIDO (TRADICIONAL) UBICADA EN EL SEGUNDO PISO DEL BLOQUE D DE LA UPS. ELABORADO POR EL DEPARTAMENTO DEL DATA CENTER.....	34
GRÁFICO 6: INFORMACIÓN DETALLADA DEL PROCESAMIENTO DEL DATA CENTER: ELABORADO POR PERSONAL DEL DATA CENTER.	35
GRÁFICO 7: INFORMACIÓN DETALLADA DEL ALMACENAMIENTO DEL CENTRO DE DATOS: ELABORADO POR PERSONAL DEL DATA CENTER.	36
GRÁFICO 8: CAPTURA DE PANTALLA DE LOS SENSORES DEL DATA CENTER. RECUPERADA DEL SOFTWARE DE SENSORES DEL DATA CENTER BLOQUE D UPS SUR.....	37
GRÁFICO 9: LECTURA DEL PANEL DE ENERGÍA ELÉCTRICA TOMADA DEL DATA CENTER. DATO TOMADO POR JOHN Y HENRY DEL PANEL ELÉCTRICO.	38
GRÁFICO 10: CAPTURA DE PANTALLA DE WIRESHARK CON LOS DATOS GENERALES DE LA CAPTURA. RECUPERADO DEL SOFTWARE WIRESHARK	39
GRÁFICO 11: CAPTURA DE PANTALLA DE LOS DATOS POR PUNTOS FINALES DE LA RED. RECUPERADO DEL SOFTWARE WIRESHARK	40
GRÁFICO 12: CAPTURA DE PANTALLA DE WIRESHARK CON LOS DATOS POR PROTOCOLO DE LA RED. RECUPERADO DEL SOFTWARE WIRESHARK	40
GRÁFICO 13: PORCENTAJE DE PAQUETES GENERADOS POR PROTOCOLO EN UDP. REALIZADO POR JOHN Y HENRY	41
GRÁFICO 14: PORCENTAJE DE PAQUETES GENERADOS POR PROTOCOLO EN TCP. REALIZADO POR JOHN Y HENRY	41
GRÁFICO 15: CAPTURA DE PANTALLA DE WIRESHARK CON LA TRANSMISIÓN DE PAQUETES POR TIEMPO.	

RECUPERADO DEL SOFTWARE WIRESHARK	42
GRÁFICO 16: DISEÑO DE LA NUEVA ARQUITECTURA SPINE AND LEAF. ELABORADO POR JOHN Y HENRY	44
GRÁFICO 17: DISEÑO DE LA RED EN EL SOFTWARE PACKET TRACER. ELABORADO POR JOHN Y HENRY	46
GRÁFICO 18: RED IMPLEMENTADA CON LOS EQUIPOS DEL LABORATORIO DE LA UPS. TOMADA POR JOHN Y HENRY.....	47
GRÁFICO 19: CAPTURA DE LA PÁGINA OFICIAL DEL PROGRAMA BIGANT. CAPTURA DE JOHN Y HENRY. RECUPERADA DEL SITIO OFICIAL DEL SOFTWARE [23].....	48
GRÁFICO 20: CAPTURA DE CONFIGURACIONES DEL PROTOCOLO DE INTERNET VERSIÓN 4 (TCP/IPV4). CAPTURA DE JOHN Y HENRY.....	49
GRÁFICO 21: CAPTURA DE LA APP DE BIGANT CONSOLE. CAPTURA DE JOHN Y HENRY.....	49
GRÁFICO 22: CAPTURA DE VERIFICACIÓN DE IP EN EL SERVIDOR DE BIGANT. CAPTURA DE JOHN Y HENRY.....	49
GRÁFICO 23: CREACIÓN DE LOS USUARIOS EN LA VENTANA DE BIGANT CONSOLE. CAPTURA DE JOHN Y HENRY.....	50
GRÁFICO 24: VERIFICACIÓN DE LOS USUARIOS CREADOS. CAPTURA DE JOHN Y HENRY.....	50
GRÁFICO 25: CAPTURA DE LA APP DE BIGANT MESSENGER (CLIENTE). CAPTURA DE JOHN Y HENRY	51
GRÁFICO 26: ACCESO A LA APP CON CREDENCIALES CREADAS EN EL SERVIDOR. CAPTURA DE JOHN Y HENRY	51
GRÁFICO 27: VIDEOLLAMADA ENTRE EL PC DE JOHN Y HENRY. CAPTURA DE JOHN Y HENRY	51
GRÁFICO 28: CAPTURA DE CHAT, LLAMADA Y TRANSFERENCIA DE DATOS MEDIANTE EL BIGANT. CAPTURA DE JOHN Y HENRY.....	52
GRÁFICO 29: ARCHIVOS DE DESCARGA DEL SERVIDOR DE JUEGO. CAPTURA DE JOHN Y HENRY	52
GRÁFICO 30: EJECUCIÓN DEL SERVIDOR DEL JUEGO COUNTER. CAPTURA DE JOHN Y HENRY	52
GRÁFICO 31: CREACIÓN DE LAS PARTIDAS DENTRO DE LA MISMA VLAN. CAPTURA DE JOHN Y HENRY	53
GRÁFICO 32: FOTO DEL JUEGO IMPLEMENTADO. TOMADA POR JOHN Y HENRY.....	53
GRÁFICO 33: CAPTURA DEL SITIO OFICIAL Y DOCUMENTOS A DESCARGAR PARA LA IMPLEMENTACIÓN. CAPTURA DE JOHN Y HENRY.....	54
GRÁFICO 34: CAPTURA DE LA PANTALLA PRINCIPAL DE LA APP. CAPTURA DE JOHN Y HENRY.....	54
GRÁFICO 35: CONEXIÓN HACIA LA MÁQUINA PRINCIPAL DE SERVIDORES DE VIRTUALIZACIÓN. CAPTURA DE JOHN Y HENRY.....	54
GRÁFICO 36: SERVIDOR CON MOVIE PARA REPRODUCIR Y GENERAR TRÁFICO HACIA LOS SPINE. CAPTURA DE JOHN Y HENRY.....	55

GRÁFICO 37: SELECCIÓN DE ARCHIVOS PARA TRANSFERIR A OTRO DESTINO MEDIANTE TIGHTVNC. CAPTURA DE JOHN Y HENRY.....	55
GRÁFICO 38: TRASFERENCIA DE DOCUMENTOS HACIA OTRO DESTINO PARA LA CREACIÓN DE TRÁFICO. CAPTURA DE JOHN Y HENRY.....	56
GRÁFICO 39: EJEMPLO DE PING CARGADO DE BYTES HACIA LOS SPINE. CAPTURA DE JOHN Y HENRY.	57
GRÁFICO 40: INTERVALO DE TIEMPO DEL SPINE 1: CAPTURADO DEL TRÁFICO DEL SPINE 1 POR JOHN Y HENRY	58
GRÁFICO 41: INFORMACIÓN TRANSMITIDA DEL SPINE 1: CAPTURADO DEL TRÁFICO DEL SPINE 1 POR JOHN Y HENRY.....	58
GRÁFICO 42: GRÁFICA DEL SPINE 1: CAPTURADO DEL TRÁFICO DEL SPINE 1 Y DE WIRESHARK, POR JOHN Y HENRY.....	59
GRÁFICO 43: INFORMACIÓN TRANSMITIDA DEL SPINE 2: CAPTURADO DEL TRÁFICO DEL SPINE 2 POR JOHN Y HENRY.....	60
GRÁFICO 44: CAPTURA DE PANTALLA DE WIRESHARK CON LOS DATOS POR PROTOCOLO DE LA RED DEL SPINE 1. RECUPERADO DEL SOFTWARE WIRESHARK POR JOHN Y HENRY.....	60
GRÁFICO 45: GRÁFICA DEL SPINE 2: CAPTURADO DEL TRÁFICO DEL SPINE 2 Y DE WIRESHARK, POR JOHN Y HENRY.....	61
GRÁFICO 46: ZOOM DEL PICO DE LA GRÁFICA DEL SPINE 2: CAPTURADO DEL TRÁFICO DEL SPINE 2 Y DE WIRESHARK, POR JOHN Y HENRY	62
GRÁFICO 47: ANCHO DE BANDA DE LA RED DE LOS DOS SPINE CON LA HERRAMIENTA IPERF-3: CAPTURADO POR JOHN Y HENRY	63
GRÁFICO 48: CAPTURA DEL PING CARGADO DESDE LA MÁQUINA DE SERVIDORES HACIA LA RED EXTERNA: CAPTURADA POR JOHN Y HENRY	64

RESUMEN

El centro de datos de la Universidad Politécnica Salesiana campus sur, boque D, es muy importante porque tiene varias funciones, la principal es brindar recursos de tecnología para ayudar, a los estudiantes de la UPS de las sedes Quito, Guayaquil y Cuenca, con máquinas virtuales. El data center que se tiene en el bloque D implementa un modelo tradicional el cual presenta cuellos de botella, esto debido a que genera mucho tráfico de datos. En el presente proyecto se propone una arquitectura de red con el modelo Spine and Leaf con la certificación TIER II, con el fin de eliminar los cuellos de botella. La idea del diseño surge de una visita a la empresa CNT donde se conoció por primera vez este tipo de infraestructura de red en un centro de datos. Luego de la visita al centro de datos del bloque D del campus sur de la UPS y con la entrevista a los encargados del mismo, manifestaron que efectivamente la red presenta problemas, si bien por el momento se logra satisfacer las necesidades, con la arquitectura actual no se tiene ya una capacidad de crecimiento en cuestión de recursos disponibles para los estudiantes.

Se pretende que el modelo Spine and Leaf mejore la situación actual de la red y permita que los recursos actuales sean utilizados de una mejor manera y con este modelo se permita tener un crecimiento en cuanto a recursos de virtualización y storage para brindar un mejor servicio a los alumnos y en general usuarios que requieran de servicios de este centro de datos.

Palabras claves. – Arquitectura, Centro de Datos, Rendimiento, Spine and Leaf.

ABSTRACT

The data center of the Universidad Politécnica Salesiana south campus, block D, is very important because it has several functions, the main one is to provide technology resources to help UPS students from Quito, Guayaquil and Cuenca, with virtual machines. The data center in block D implements a traditional model which presents bottlenecks because it generates a lot of data traffic. This project proposes a network architecture with the Spine and Leaf model with TIER II certification, in order to eliminate bottlenecks. The idea of the design arises from a visit to the company CNT where this type of network infrastructure in a data center was known for the first time. After the visit to the data center in block D of the UPS south campus and the interview with the people in charge of it, they stated that indeed the network presents problems, although for the moment it is able to meet the needs, with the current architecture there is no longer a capacity for growth in terms of resources available for students. The Spine and Leaf model is intended to improve the current situation of the network and allow the current resources to be used in a better way and with this model it is possible to have a growth in terms of virtualization and storage resources to provide a better service to students and users in general who require services from this data center.

Keywords. – Architecture, Data center, Performance, Spine and Leaf.

CAPÍTULO 1

1.1 PROBLEMA DE ESTUDIO

El Data Center del bloque D del Campus Sur de la UPS, fue creado para brindar servicio a todas las carreras de la Universidad, de la sede Quito, Guayaquil y Cuenca, cuando estas lo requieran, tanto para fines académicos como de investigación, actualmente para cumplir con este objetivo trabaja con máquinas y servidores virtuales.

Originalmente la red del Data Center fue diseñada utilizando una arquitectura tradicional, esta arquitectura tradicional consta de tres capas; la primera que es el núcleo que está encargado de transportar los mensajes a los distintos servidores del centro de datos; la segunda capa es la de agregación, que se encarga de brindar redundancia para garantizar que no existan caídas del data center; y finalmente se tiene la capa de acceso que se encarga de brindar conexión a usuarios finales.

A pesar de que la arquitectura tradicional se la considera como moderna, esta no favorece a la escalabilidad de la red tanto en infraestructura como en servicios y tecnología tales como computación en la nube, IoT, virtualización. Además de que puede generar pérdidas de información, también puede existir deficiencias de aparatos informáticos como de comunicación entre todas las carreras universitarias.

Para cumplir con el objetivo fundamental del Data Center, de una manera eficiente se requiere plantear el uso de una arquitectura que resuelva los problemas mencionados anteriormente, como lo es la arquitectura Spine and Leaf, que consta de 2 capas en forma de hoja en la cual cada switch de acceso se conecta directamente con el servidor, Spine and Leaf no necesita del protocolo STP debido a que usa enrutamiento por varias rutas ya que tiene protocolo ECPM que ayuda a balancear el tráfico que existe en estas rutas y a su vez evita los bucles de red.

1.2 OBJETIVOS

1.2.1 OBJETIVO GENERAL

Diseñar una arquitectura Spine Leaf con certificación de TIER II para la red del Data Center del Campus Sur bloque D de la Universidad Politécnica Salesiana.

1.2.2 OBJETIVOS ESPECÍFICOS

- Recopilar información de la actual infraestructura del Data Center Bloque D.
- Desarrollar el modelo Spine Leaf para el Data Center.
- Simular la arquitectura propuesta del Data Center mediante software.

1.3 JUSTIFICACIÓN

De acuerdo con la tasa de crecimiento que tiene el Data Center, la arquitectura actual que presenta (arquitectura tradicional) no tendrá beneficios de rendimiento y, por el contrario, actualmente se presentan los problemas conocidos como cuellos de botella.

Una arquitectura Spine-Leaf mejora la escalabilidad, rendimiento y fiabilidad puesto que esta arquitectura ayuda a integrar la virtualización y disminuye los cuellos de botella; además tiene una mejora ya que su modelo basado en la redundancia ayuda a que la red no sufra caídas por cortes en el núcleo.

Con el nuevo diseño de la arquitectura Spine-Leaf para el Data Center del Bloque D del campus Sur de la Universidad Politécnica Salesiana se podrá realizar una migración de tecnología de convergencia o Hiperconvergencia a la industria 4.0, esto depende también del presupuesto que las autoridades asignen si en un futuro desean utilizar el diseño que se propone, dado que los equipos de alto rendimiento ya se encuentran en operación estos ayudarán a eliminar el problema de los cuellos de botella y a mejorar el rendimiento de operación y trabajo.

1.4 METODOLOGÍA

1.4.1 Paradigma de Investigación.

EL paradigma de la investigación es interpretativo; puesto que los resultados que se tengan de la investigación serán producto de una interpretación del comportamiento de las variables que rigen el funcionamiento del data center con la nueva arquitectura propuesta [1]

1.4.2 Tipo de Investigación.

El tipo de investigación que se llevará a cabo es la investigación científica experimental, ya que el estudio para la nueva arquitectura se basará primero en resultados obtenidos de investigación de otros data center con la arquitectura Spine and Leaf y en segundo lugar de los resultados obtenidos de simulaciones realizadas en software y la comparación con los datos que actualmente genere el data center del bloque D de la UPS campus sur; de esta manera mostrar que efectivamente se tiene una mejora con una migración de arquitectura[1]

1.4.3 Alcance.

El presente proyecto corresponde a una investigación de tipo descriptivo; ya que los resultados obtenidos se pretenden mostrar a los encargados del data center y así mostrar que la nueva arquitectura presenta una mejor calidad de servicio y el comportamiento que tendría el mismo una vez implementado la nueva arquitectura propuesta para los usuarios [1]

Cabe mencionar que el proyecto solamente constará de diseñar la arquitectura más no de presentarla en producción ya que serán las mismas autoridades de la Universidad Politécnica Salesiana quienes decidan llevar a cabo o no la migración de arquitectura; es decir el diseño se lo presentará solamente en simulación [1].

1.4.4 Unidad de Análisis.

El data center del Bloque D de la Universidad Politécnica Salesiana.

1.5 DISEÑO DE LA INVESTIGACIÓN

1.5.1 Enfoque cuantitativo y cualitativo.

Para realizar el diseño de la arquitectura Spine Leaf, se recolecta información sobre la situación actual del Data Center, además, se realiza un estudio previo de las condiciones que se tiene para implementar la nueva arquitectura. Una vez realizado todo el proceso se continua con la simulación de la arquitectura Spine Leaf y se analizará los cambios obtenidos dentro del Data Center [1].

1.5.2 Experimental.

Se pretende realizar una comparación entre los datos actuales con los nuevos datos al momento de realizar la simulación con el modelo Spine Leaf .

1.6 MARCO CONCEPTUAL

1.7 DATA CENTER

Un Centro de Procesamiento de Datos en la actualidad es de suma importancia para las grandes empresas, puesto que permite dar un paso en la transformación digital, además de buscar una mejora en la productividad. De manera global un Data Center se lo puede conocer como un espacio físico, que puede ir desde el tamaño de una oficina hasta grandes edificios, donde se encuentran alojados equipos electrónicos cuya función primordial es salvaguardar los datos en ambientes controlados, de manera que la información se encuentre disponible en cualquier momento que la empresa lo requiera [2].

Un Data Center permite gestionar los recursos necesarios para el procesamiento de datos de una determinada empresa que cuenta con servidores, firewalls, routers, sistemas y controladores de entrega de aplicaciones, switches, equipos de red, almacenamiento y demás recursos necesarios que se requieren para tener una red de información que cumple con el carácter de disponibilidad lo que indica que debe estar en operación durante las 24 horas y en cualquier día del año [3].

Los lugares que ocupan los centros de datos pueden ser del tamaño de una oficina hasta del tamaño de un edificio de varios metros cuadrados de espacio, los cuales albergan muchos equipos electrónicos, informáticos, mecánicos, racks, fibra óptica entre otros [3]. Los Data Center son el foco en donde se realizan las operaciones que incluyen los servicios que se utiliza normalmente como son las redes sociales, mensajería, navegadores web, servicios de facturación, investigación médica, etc., todo lo que se genera en estos servicios en línea es guardado en estos data center, los datos obtenidos son analizados y procesados por algoritmos de comportamiento [3].

Implementar un centro de datos como segmento clave para la transformación digital o como recurso para robustecer actividades, trae consigo grandes beneficios a la empresa, los mismos que se detallan a continuación:

1.7.1 Continuidad de negocio.

Los data center deben garantizar que los recursos, información y procesos siempre tienen que estar disponibles de manera correcta, sin importar los sucesos que puedan interferir [3].

1.7.2 Velocidad de respuesta.

Los data center deben tener una respuesta rápida a la información, contar con tecnología óptima de conectividad desde el punto de los servidores, contar con fibra óptica y gestión de enlaces a través de soluciones SD-WAN (red de área amplia definida por software) [4], que garantiza la disponibilidad de los sistemas más esenciales para el negocio [3].

1.7.3 Seguridad de la información.

Los data center cuentan con altos estándares de seguridad de información, también cuenta con personas capacitadas y calificadas para impedir el robo, filtraciones o pérdidas de información [3].

1.7.4 Alta capacidad de almacenamiento.

Los centros de datos ofrecen un almacenamiento de una cantidad muy elevada de información, debido a la infraestructura de los proveedores [3].

1.7.5 Simplicidad.

Contratar un distribuidor que ofrezca los servicios de centros de datos, el cual permite a las empresas desarrollar mejor sus actividades y reducir el proceso de almacenamiento de información [3].

1.7.6 Escalabilidad

Las empresas deben proyectarse a su crecimiento e ir escalando sus capacidades de acuerdo como lo necesiten, pueden solicitar un incremento de almacenamiento o infraestructura de forma casi inmediata, además se puede solicitar almacenamiento en nube solo pagando el espacio a emplear sin límite predeterminado [3].

1.7.8 Flexibilidad.

Cuando los data center tienen una disponibilidad alta, estos permiten que las empresas usen su información cuando más lo requieran, también se puede usar vía remota [3].

1.7.9 Eficiencia y confiabilidad.

Los data center de mayor nivel tiene una disponibilidad de 99.995%, lo cual garantiza que los datos corporativos estarán disponibles cuando lo necesiten con una mayor velocidad de descarga o desglose de aplicaciones [3].

Originalmente la red del Data Center consta de tres capas; la primera que es el núcleo que está encargado transportar los mensajes a los distintos servidores del centro de datos; la segunda capa es la de agregación, que se encarga de brindar redundancia para garantizar que no existan caídas del data center; y finalmente se tiene la capa de acceso que se encarga de brindar conexión a usuarios finales [5].

1.8 REQUISITOS DE UN CENTRO DE DATOS

Como ya se ha mencionado un centro de datos ofrece una variedad de servicios relacionados con tecnologías de información, y por lo tanto tiene un elevado costo de puesta en operación; paralelamente se tienen sistemas que ayudan al funcionamiento del centro de datos [6].

1.8.1 Suministros de energía.

Los centros de datos requieren de una gran cantidad de energía para su correcto funcionamiento, es por eso por lo que la fuente de energía debe estar respaldada con sistemas secundarios que puedan ponerse en funcionamiento de forma inmediata en caso de que la fuente principal de energía sufra un desperfecto o no se encuentre disponible [6].

1.8.2 Refrigeración.

Al tener varios equipos en funcionamiento y un elevado consumo de energía, los centros de datos generan calor y este debe ser contrarrestado con un sistema de refrigeración. Al tener dispositivos electrónicos el agua no se puede utilizar en caso de un incendio, en su lugar se utilizan sustitutos

químicos que protegen los equipos y contrarrestan el fuego [6].

1.8.3 Seguridad física y virtual.

Al tener un sinfín de datos, la seguridad es lo primordial en un centro de datos, ya que una vulneración a este sitio implicaría una filtración de información de miles de usuarios o de empresas, esto conllevaría incluso hasta la banca rota de una empresa. Es por este motivo que un centro de datos debe estar protegido frente a robos con medidas de seguridad primero físicas, como son: seguridad de guardianía, video vigilancia, acceso restringido; y segundo con seguridad virtual como: software de monitoreo, seguridad de la red, credenciales de acceso virtual [6].

Los sistemas presentados anteriormente aseguran un óptimo funcionamiento del centro de datos, la distribución de cada uno de estos sistemas dependerá del tamaño del centro de datos, ya que existen centros de datos pequeños que únicamente cuenta con un solo rack en un armario y por otro lado existen centros de datos de tamaños de edificios enteros en donde cada uno de los sistemas debe ser diseñado para abarcar todo el centro de datos [6].

1.9. TIPOS DE CENTROS DE DATOS

1.10. CENTRO DE DATOS TRADICIONAL

Un centro de datos tradicional ocupa un espacio físico y consta de varios servidores, los cuales se encuentran distribuidos en varios racks, para el correcto funcionamiento de cada uno de los servidores, la red del centro de datos requiere de protocolos de redundancia de red, de tal manera que se garantice que el servidor se encuentre operativo de forma ininterrumpida [7].

Cada servidor que se encuentra en el centro de datos se lo implementa de manera independiente al resto de servidores. Los centros de datos requieren distintos sistemas operativos, como LINUX o WINDOWS para su operación, monitoreo y mantenimiento. Al poner en producción esta infraestructura además de los sistemas operativos ya mencionados, se requiere de personal capacitado para la operación de distintos sistemas que funcionan de forma complementaria para la correcta operación del centro de datos, como son los sistemas de energía eléctrico, temperatura, etc. [7].

1.11 CENTRO DE DATOS MODULAR.

Un centro de datos modular tiene una característica y ventaja particular, la cual es que, a diferencia de un centro de datos tradicional, el centro de datos modular se lo puede definir como un centro de datos portátil que, como su nombre lo indica, puede ser trasladado de un lugar a otro, estos ya cuentan con sistemas propios de alimentación, de energía y refrigeramiento, usualmente son trasladados en contenedores y son transportados bajo una estricta seguridad [8].

Este tipo de centros de datos presenta ventajas [8] como son:

- Una mayor accesibilidad para los clientes de acuerdo con los requerimientos.

- A medida que el proyecto aumente sus necesidades, el centro de datos puede seguir creciendo, por lo que facilita la escalabilidad del data center.
- Pueden ser pre fabricables, por lo que sus componentes son más económicas.
- El tiempo de puesta en marcha es menor en comparación a un estático.
- Es una solución ideal para zonas en las que se tiene riesgos de desastres naturales, ya que no se ven afectados por el daño de una infraestructura física de un edificio.

En estos centros de datos se deben implementar los mismos mecanismos de seguridad y de monitoreo que en los centros de datos estáticos. Con respecto a la seguridad física del centro de datos modular, los containers cuentan con una estructura sándwich de tres placas de acero, con el fin de incrementar el grosor de las compuertas y paredes laterales, además cuentan con sistemas de aislamientos, los cuales consisten en revestimientos de placas de acero, se coloca un blindaje adicional que cumple la función de soporte del peso de los equipos que componen el centro de datos [8].

Este tipo de centros de datos se los ha puesto en funcionamiento como una fase de prueba en varias zonas de Asia como Japón, donde su infraestructura ha sido diseñada para soportar terremotos de hasta siete grados[8].

1.12 CENTRO DE DATOS EN LA NUBE

En la actualidad los servicios que ofrece la nube en TI (tecnologías de la Información) se encuentran en constante crecimiento, es tal que ahora se puede llegar a crear todo un centro de datos únicamente con servicio de nube. Un centro de datos en nube garantiza una mayor seguridad y facilidad de acceso a la información y además presenta soluciones integrales que ofrecen una mayor eficiencia de datos y aplicaciones para los usuarios [9].

Para una arquitectura de nube el primer requisito del centro de datos será personal capacitado en cloud computing para la administración y monitoreo del tráfico de datos que se gestione, la arquitectura que se gestiona con este tipo de centro de datos está orientada a servicios SOA (Service Oriented Architecture, o servicios web) [9].

Este tipo de centros de datos se caracteriza principalmente por virtualizar recursos, esto a su vez tiene beneficios de disminución de costos de operación, una administración simplificada, ya que el monitoreo puede aumentar o disminuir recursos para cada sistema. A su vez permite una consolidación de servidores que consiste en la distribución de cargas de trabajo en distintos servidores, esto se lo puede realizar de dos formas [9]:

- Destinar varias cargas de varios servidores a un solo servidor de alta capacidad [9].
- Con ayuda de sistemas operativos combinar las cargas de trabajo [9].

Todo esto permite realizar la virtualización de servidores [9].

1.13 TIPOS DE SERVICIOS OFERTADOS POR CENTROS DE DATOS EN NUBE.

1.13.1 Software como un servicio (SaaS).

Es la capa más alta de la nube, la aplicación consiste en una sola instancia de software que corre en la infraestructura del proveedor y da servicio a múltiples organizaciones [9].

1.13.2 Plataforma como un servicio (PaaS).

Conocida como la capa intermedia de la nube, ofrece un entorno de desarrollo o de empaquetamiento de servicios, los servicios son especializados a cualquier área en particular [9].

1.13.3 Infraestructura como un servicio (IaaS).

La capa inferior de la nube ofrece servicios únicamente de almacenamiento [9].

1.14 TIPOS DE ARQUITECTURAS PARA UN CENTRO DE DATOS

1.15 ARQUITECTURA TRADICIONAL

Surgió en la década de 1990 cuando distintas empresas buscaron el almacenamiento digital de su información; la arquitectura tradicional se presenta con varios servidores distribuidos en distintos racks, la distribución de cada servidor depende la aplicación que tiene cada uno; además se requiere de un nivel alto de redundancia para la administración de distintos procesos críticos que se pueden presentar, es por eso que uno de los protocolos más usados con este tipo de arquitecturas es el STP [10], (Spanning Tree Protocol), el cual permite solucionar problemas manteniendo en funcionamiento la red, aun cuando el problema sea tan crítico como la caída de un switch [10].

1. Las redes de centros de datos se basaban en un modelo de tres niveles: Los conmutadores de acceso se conectan a los servidores [11].
2. Los dispositivos de agregación o distribución proporcionan conexiones redundantes para acceder a los conmutadores de acceso [11].
3. Los switches centrales proporcionan un transporte rápido entre los dispositivos de agregación, normalmente conectados en un par redundante para una alta disponibilidad [11].

En el año del 2005 fue aprobado el estándar TIA-942 por ANSI-TIA (American National Standards Institute- Telecommunications Industry Association), el cual facilita una guía de recomendaciones y directrices para el montaje de un Data Center (centro de datos) mostrando su nivel de fiabilidad en operación del nivel de disponibilidad [12].

Cuando se diseña los centros de Datos al pie de las normas se obtiene ventajas [12] como se describen a continuación:

- Nomenclatura estándar,

- Puesto en marcha a prueba de averías,
- Incremento de protección ante los agentes externos,
- Fiabilidad a largo plazo, aumento de capacidad de expansión y escalabilidad.

Un centro de Datos tiene una verificación de fiabilidad que viene indicado por uno de los cuatro niveles conocidos como TIER. Cuando se tiene un mayor TIER y una gran disponibilidad se tendrá un costo alto de construcción y mantenimiento [12].

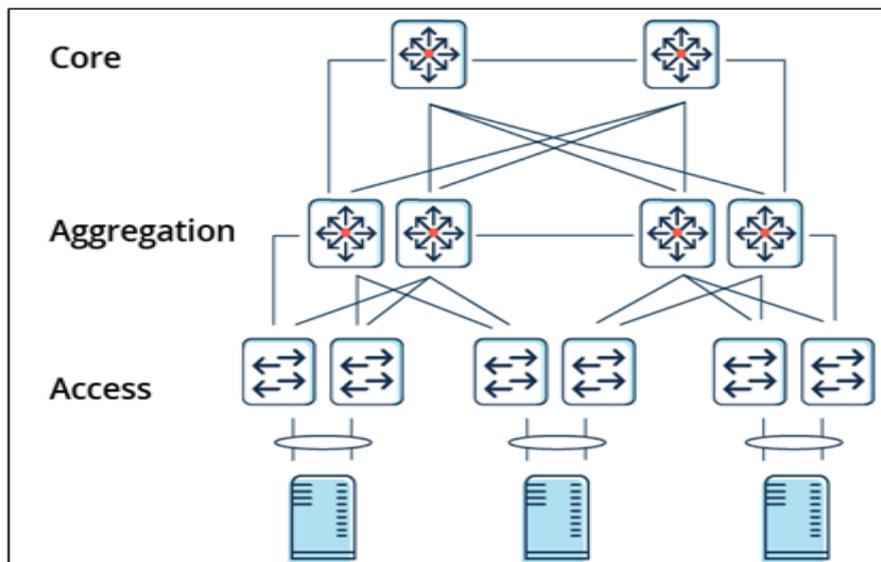


Gráfico 1: Distribución de la arquitectura tradicional de un data center “Arquitectura del centro de datos, data center - Blog de data center, cloud.” Recuperado de: <https://www.arubanetworks.com/faq/what-is-spine-leaf-architecture/> (accessed Mar. 04, 2023).

1.16 ARQUITECTURA SPINE AND LEAF

La arquitectura Spine and Leaf consiste en dos capas de conmutación; las cuales se orientan tanto en sentido vertical como horizontal, es por eso por lo que se considera como columna y hoja porque nacen ramificaciones de la columna principal de la arquitectura, que permiten tener una comunicación eficaz entre los servidores del centro de datos [11]. En sí la arquitectura presenta los switches de acceso que agregan tráfico a los servidores que están directamente conectados a la topología y no requiere de tanta redundancia en su diseño; cabe recalcar que todos los switches de la topología tienen intercomunicación [11].

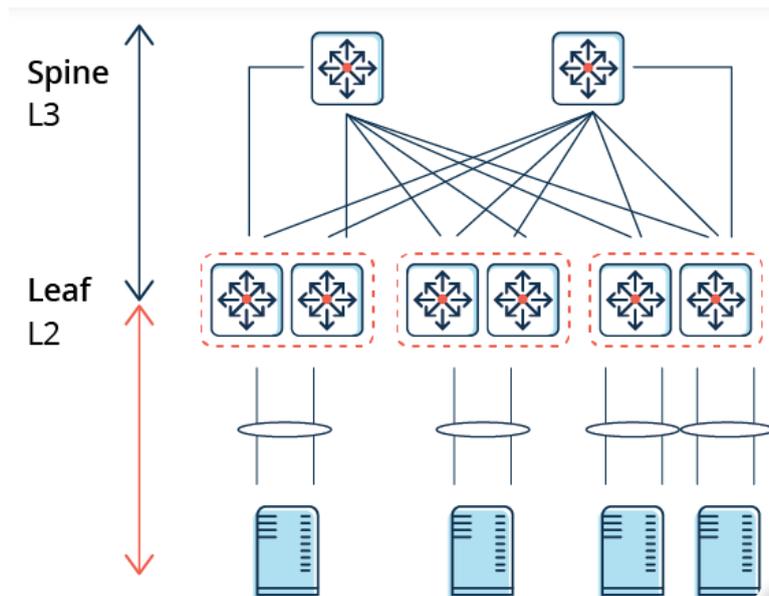


Gráfico 2: Distribución de la arquitectura Spine Leaf de un CENTRO DE DATOS “Arquitectura del centro de datos, data center - Blog de data center, cloud.” Recuperado de: <https://www.arubanetworks.com/faq/what-is-spine-leaf-architecture/> (accessed Mar. 04, 2023)

1.17 CERTIFICACIONES DE CENTRO DE DATOS (TIERS)

1.17.1 TIER I

El nivel 1 o conocido como básico, indica que es delicado a las paralizaciones ya sean planificadas o no, también no cuenta con componentes redundantes y tiene un solo flujo de corriente como aire acondicionado, no exige pisos elevados, por lo tanto, se tiene una disponibilidad (99,671%), porcentaje de parada (0,33) y tiempo anual de parada en horas (28,82), para lograr una implementación con el nivel 1 se tiene un tiempo determinado de 3 meses aproximadamente y al momento de realizar un mantenimiento preventivo se debe cerrar en su totalidad [12].

1.17.2 TIER II

El nivel 2 o conocido como componentes redundantes, indica que es menos delicado a las paralizaciones, cuenta con un componente redundante y tiene un solo flujo de corriente como aire acondicionado, exige pisos elevados, UPS y generador, por ende, se tiene una disponibilidad (99,741%), porcentaje de parada (0,25) y tiempo anual de parada en horas (22,68), para lograr una implementación con el nivel 2 se tiene un tiempo determinado de 3 a 6 meses aproximadamente al momento de realizar un mantenimiento preventivo de la estructura o de alimentación se debe realizar un cierre de procesamiento [12].

1.17.3 TIER III

En el nivel 3 o también distinguido como mantenimiento concurrente se prevé un tiempo estimado de 15 a 20 meses para lograr una implementación del centro de datos, se tiene mantenimientos planificados de tal manera que el funcionamiento no se vea afectado, tiene varios ingresos de energía como al igual de refrigeración que llega por un solo acceso activo y tiene componentes redundantes N+1, debido a ellos, se tiene una disponibilidad (99,982%), porcentaje de parada (0,02) y tiempo anual de parada en horas (1,57) [12].

1.17.4 TIER IV

Para el nivel 4 o llamado también como Tolerante a errores, se tiene que al momento de existir un interrupción planificada no afectará el funcionamiento y tendrá la posibilidad de existir un caso aislado sin perjuicios críticos, tiene varias entradas de energía como de refrigeración, consta de componentes redundantes $(2(N+1))-2$ UPS que tiene cada uno de ellos (N+1) redundancia, por ende, se tiene una disponibilidad (100%), porcentaje de parada (0,01) y tiempo anual de parada en minutos (52,56) [12].

Para cumplir con la implementación del nivel 4 se tiene un tiempo específico de 15 a 20 meses [12].

1.18 REDES SAN

Las redes SAN (red de área de almacenamiento) son independientes de alta velocidad que se encarga de conectar y suministrar depósitos compartidos de almacenamientos a varios servidores. Independientemente cada servidor puede ingresar al almacenamiento compartido como una unidad conectada directo al servidor. Las redes SAN se implementan mediante cable, adaptadores de bus del host y los conmutadores SAN que son conectados a la matriz de almacenamiento y del servidor. Los conmutadores y los sistemas de almacenamiento deben estar conectados. Una SAN es una red equipos de almacenamiento donde se puede ingresar varios servidores u computadores donde proporcionas un almacenamiento compartido[13].

Componen arquitecturas de redes de almacenamiento más semejante como las que utilizan las empresas para que sus aplicaciones sean más distinguidos, logren un alto rendimiento y tengan baja latencia. Las redes SAN no dejan de crecer porque aprovechan el almacenamiento all-flash [14], para lograr un mayor rendimiento, latencia baja constante y reducir el costo comparado con el de los discos giratorios [15]

Cuando se almacena los datos mediante un almacenamiento compartido centralizado, las redes SAN admiten a las organizaciones usar métodos y herramientas iguales en cuestión de seguridad, protección de datos y la recuperación ante catástrofes [15].

El almacenamiento SAN se fundamenta en bloques y se aprovecha una arquitectura de alta velocidad que conecta a los servidores con los discos lógicos (LUN). Una LUN es una diversidad de bloques que

proveen de un conjunto de almacenamiento compartido, la cual se presenta al servidor como un disco lógico. El servidor particiona y proporciona formato a estos bloques frecuentemente con un sistema de archivos, para que puedan ser almacenados en la LNU al igual que los discos locales. Son diseñados para eliminar únicos puntos de error, otorgando una gran disponibilidad y resiliencia, tal que una SAN cuando está bien diseñada resiste fácilmente algunos errores de componentes o dispositivos. Estos constituyen dos tercios del almacenamiento total en la red [15].

A continuación, se puede detallar varios casos donde se pueden utilizar redes SAN [15]:

- BD de Oracle, las cuales son importantes para el negocio donde se requiere un nivel elevado de rendimiento y disponibilidad.
- BD de Microsoft SQL Server, se almacenan los datos más importantes de una empresa, se requiere un nivel elevado de rendimiento y disponibilidad.
- Grandes implementaciones de virtualización VMware o Microsoft Hyper-V. – estos entornos se incrementan a miles de máquinas virtuales con una gran variedad de SO con diferentes requerimientos de rendimiento.
- Grandes estructuras de puesto de trabajo virtual (VDI).- Las VDI pueden alcanzar decenas de miles de puestos de trabajos virtuales, donde se puede centralizar estos puestos para poder gestionar con mejor facilidad la seguridad de datos.
- SAP u otros grandes entorno ERP o CRM.- las redes SAN son perfectas para las cargas de trabajo con recursos empresariales de planificación y recursos de los clientes.

1.19 PROTOCOLOS USADOS EN LA REDES SAN

- Protocolo Fibre Channel (FCP).- Se utiliza en un total de 70 o el 80% en el mercado de SAN [15].
- Interfaz de sistemas para equipos pequeños de internet (iSCSI).- Se utiliza de un 10 o un 15 % en el mercado de SAN [15].
- Fibre Chanel sobre Ethernet (FCoE).- supone menos de 5% del mercado de SAN [15].
- Memoria no volátil exprés a través de Fibre Channel (FC-NVMe).- es un protocolo que sirve para acceder al almacenamiento flash mediante un bus PCI Express (PCIe) [15].

1.20 PING

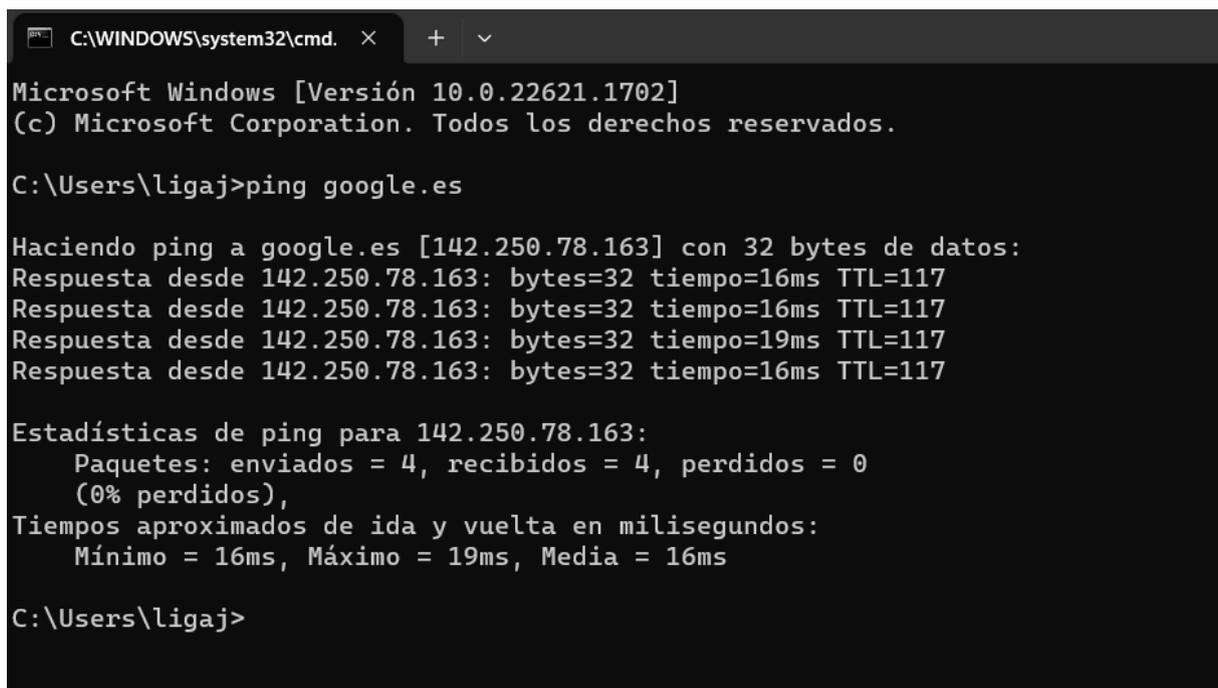
Es un comando que permite verificar si se tiene acceso o comprobar si se llega al destino de forma correcta o al contrario sino se tiene acceso, cuando se ejecuta la solicitud de ping, envía un mensaje ICMP Echo Request al host de destino y si se tiene respuesta en el destino le contesta con un mensaje ICMP Echo Reply. Esta respuesta se calcula el tiempo mínimo, medio y máximo de respuesta. Si no se tiene acceso se recibe un mensaje de host inaccesible, la red no se encuentra en la ruta al host [16].

No necesariamente se debe tener acceso o respuesta del destino, debido a que, si el destino se encuentra tiene un firewall que impide la llegada de ICMP Echo Request no podrá responder a la solicitud de

petición. Ocurre al igual que si el equipo tiene bloqueada la salida ICMP Echo Reply. En ocasiones se tiene que se envíe la petición de ping correctamente y llegue sin problemas, pero no se obtiene respuesta ya que se encuentra bloqueado la entrada de ping (ICMP Echo Request) no los Reply [16].

1.21 COMO USAR EL COMANDO DE PING

1. Abrir la consola "símbolo de sistema"
2. Escribir el comando ping seguido de un espacio y la IP del destino o sitio web que se desea consultar.
3. Se puede observar en la siguiente imagen.



```
C:\WINDOWS\system32\cmd. x + v
Microsoft Windows [Versión 10.0.22621.1702]
(c) Microsoft Corporation. Todos los derechos reservados.

C:\Users\ligaj>ping google.es

Haciendo ping a google.es [142.250.78.163] con 32 bytes de datos:
Respuesta desde 142.250.78.163: bytes=32 tiempo=16ms TTL=117
Respuesta desde 142.250.78.163: bytes=32 tiempo=16ms TTL=117
Respuesta desde 142.250.78.163: bytes=32 tiempo=19ms TTL=117
Respuesta desde 142.250.78.163: bytes=32 tiempo=16ms TTL=117

Estadísticas de ping para 142.250.78.163:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 16ms, Máximo = 19ms, Media = 16ms

C:\Users\ligaj>
```

Gráfico 3: Captura de cómo realizar un ping a la página de Google. Recuperado de una captura de John y Henry

En la figura anterior se puede observar cómo se tiene respuesta a la página de google.es, se puede tener la siguiente información acerca de la respuesta [16]

1.21.1 BYTES

Tamaño de paquetes enviados [16].

1.21.2 TIEMPO

Tiempo que tarda en enviar y recibir al host de destino [16].

1.21.3 TTL

Tiempo de vida, en cada salto descuenta uno hasta llegar al host de destino. Lo realiza para que el paquete no recorra la red infinitamente y se pueda desechar llegando el momento.

1.21.4 PAQUETES

Cantidad de paquetes enviados y recibidos [16].

1.21.5 TIEMPO DE RESPUESTA EN MS

Muestra cuanto se tardó en completar las cuatro (4) peticiones que se ha solicitado [16].

1.22 USO DEL PING PARA COMPROBAR UNA RED

El ping normalmente se usa para probar la conectividad de dos ordenadores que permite medir el tiempo de ida y retorno de solicitud eco ICMP, sin embargo, para realizar una prueba de red se utilizan una mayor carga de paquetes de datos o bytes [17].

Para poder realizar una comprobación con inundación de ping se debe conocer la ip de destino o su objetivo. Las verificaciones se pueden dividir en tres (3) según su objetivo y como resolver su dirección IP [18]:

1.23 PING DIVULGADA LOCAL DIRIGIDA

Este ping se dirige a un solo computador que se encuentra en una red local. Este ataque se necesita tener acceso físico para obtener su dirección IP. El ataque éxito será que la computadora atacada sea eliminada [18].

1.24 HACIA EL ENRUTADOR

Cuando se ataca directamente a los enrutadores interrumpe las comunicaciones entre los ordenadores conectados en la misma red. Se debe conocer la IP interna del enrutador local para que el ataque sea exitoso, si este finaliza todas las máquinas conectadas en la misma red serían eliminadas [18].

1.25 INUNDACIÓN DE PING CIEGO

Utiliza programas externos para descifrar la dirección IP del ordenador o enrutador de destino antes de comenzar el ataque [18].

1.26 PING FLOOD

El ping flood tiene como objetivo saturar el sistema de llegada de todas las solicitudes arbitrarias mediante un número excesivo de bytes ICMP hasta que se encuentre saturado o colapsado, no se debe confundir con ping de la muerte (ping of death), este no permite el acceso al sistema de destino directamente, sin sobrecargar de datos [19]–[21].

La carga utiliza un longitud máxima de protocolo IP al igual que la capacidad de la fragmentación de los datagramas de la IP. La longitud de un datagrama máximo es 64K (65535 bytes) adicional se incluye la cabecera del paquete que son 20 bytes. En los sistemas actuales ya tienen una protección para no permitir enviar paquetes superiores a 65500 Bytes [20], [21].

Existe una serie de comandos para el protocolo ICMP que se puede usar [16], [18]:

- 2 El comando -n.- especifica el número de veces que va a enviar una solicitud.
- 3 El comando -l.- se utiliza para especificar la cantidad de datos a enviar o carga en bytes por cada paquete.
- 4 El comando -t.- conocido como ping extendido o hasta que se agote el tiempo de espera del host.
- 5 Es importante recordar que la computadora donde se va a realizar el ataque debe tener una mayor cantidad de ancho de banda que la víctima.
- 6 El comando -a.-Resuelve direcciones en nombres host.
- 7 El comando -f.- Establece la marca de no fragmentar en paquetes, únicamente funciona con IPV4.
- 8 El comando -i.- Sirve para determinar el tiempo de vida del ping. Se debe ingresar -i, un espacio y el tiempo de vida que se desea.
- 9 El comando -r.- Sirve para determinar el número de saltos que se desea que realice la petición.
- 10 El comando -s.- Registra el tiempo de saltos máximos que se tiene en la petición.
- 11 El comando -j.- Sirve para enseñar a la petición cual será el destino no estricto de la solicitud de ping hacia el host.
- 12 El comando -k.- Indica a la solicitud cual es el origen estricto para la solicitud hacia el host.
- 13 El comando -W.-Sirve para enseñar el tiempo de espera en ms máximo para cada respuesta antes de que se del fallo de conexión.
- 14 El comando -R.- Sirve para usar un encabezamiento de enrutamiento y probar la ruta inversa. Únicamente funciona con IPV6.
- 15 El comando -S.- Indica a la petición del ping que dirección de origen usar para realizar dicha petición.
- 16 El comando -c.- Sirve para el enrutamiento e identifica el comportamiento.
- 17 El comando -p.- No sirve para realizar ping a los servidores virtualizados con Hyper-V.
- 18 El comando -4.- Sirve únicamente para forzar el uso de IPV4
- 19 El comando -6.- Sirve únicamente para forzar el uso de IPV6.

SITUACIÓN ACTUAL

CAPÍTULO 2

2.1 RED ACTUAL DEL DATA CENTER DEL BLOQUE D

La red del centro de datos actual brinda servicio de máquinas virtuales a las sedes de Quito, Cuenca y Guayaquil de la universidad Politécnica Salesiana. Se trabaja con fibra óptica que llega desde el quinto piso del bloque A, desde el switch Core se tiene doble salida de fibra óptica, mediante doble transceiver por redundancia, el primer punto de FO conecta al rack de los laboratorios del bloque D (Laboratorios de Networking) y el otro punto llega hacia los laboratorios del bloque C (laboratorio de investigación). En el centro de datos se emplea una arquitectura jerárquica de núcleo colapsado, donde el switch core (o switch de núcleo), es un switch Cisco 9300 de 48 puertos; desde este switch se tienen reflejos hacia los switches de distribución que a su vez conectan con los switches de acceso tanto del rack del centro de datos como de los distintos laboratorios del bloque D y C de la UPS, además en cada switch se gestionan las distintas VLAN de telefonía, cámaras, biométricos y de laboratorios. Adicionalmente, se tiene una vlan interna la que otorga el departamento de TI la cual se encarga de administrar las tres (3) capas importantes antes mencionados (core, distribución y acceso). Como se muestra en las gráficas 4 y 5 se tiene el switch organizador patch panel y siempre se organiza de la siguiente manera:

Para el rack de servidores se tiene un switch SAN que se comunica mediante fibra canal con el switch core, es en este punto donde se generan cuellos de botella, motivo por el cual únicamente se está transmitiendo a 1Gbit y no se puede aprovechar las características del switch, que puede transmitir a una velocidad de 5Gbit. Se conectan también con los switches de administración mediante cable UTP categoría 6. Los switches de acceso y los de distribución se conectan mediante cable UTP categoría 6. El centro de datos posee comunicación con el bloque C a través de fibra óptica monomodo, por presupuesto tienen conexión de 1 Gbit/s ya que no se tienen SFP para poder comunicarse a 10 Gbit/s y se emerge por medio de transceiver. La vlan de servidores se mantiene separadas por motivo de seguridad. El centro de datos al momento cuenta con certificación TIA-942, no se ha podido obtener la certificación TIER II debido a que no cuenta con todos los ventiladores en el sistema de temperatura, en la arquitectura no se tiene implementada el protocolo STP.

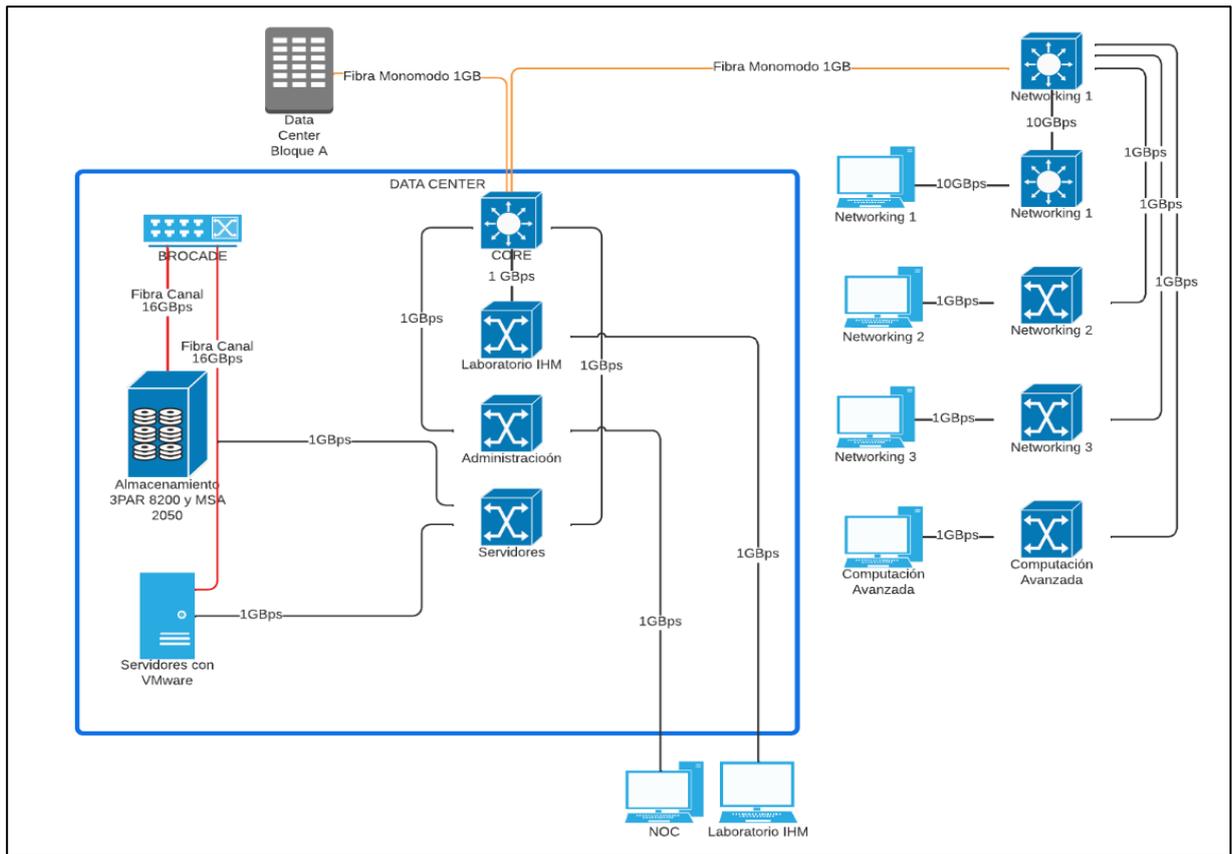


Gráfico 4: Estructura actual del data Center (tradicional) ubicada en el segundo piso del bloque D de la UPS. Elaborado por El departamento del Data Center

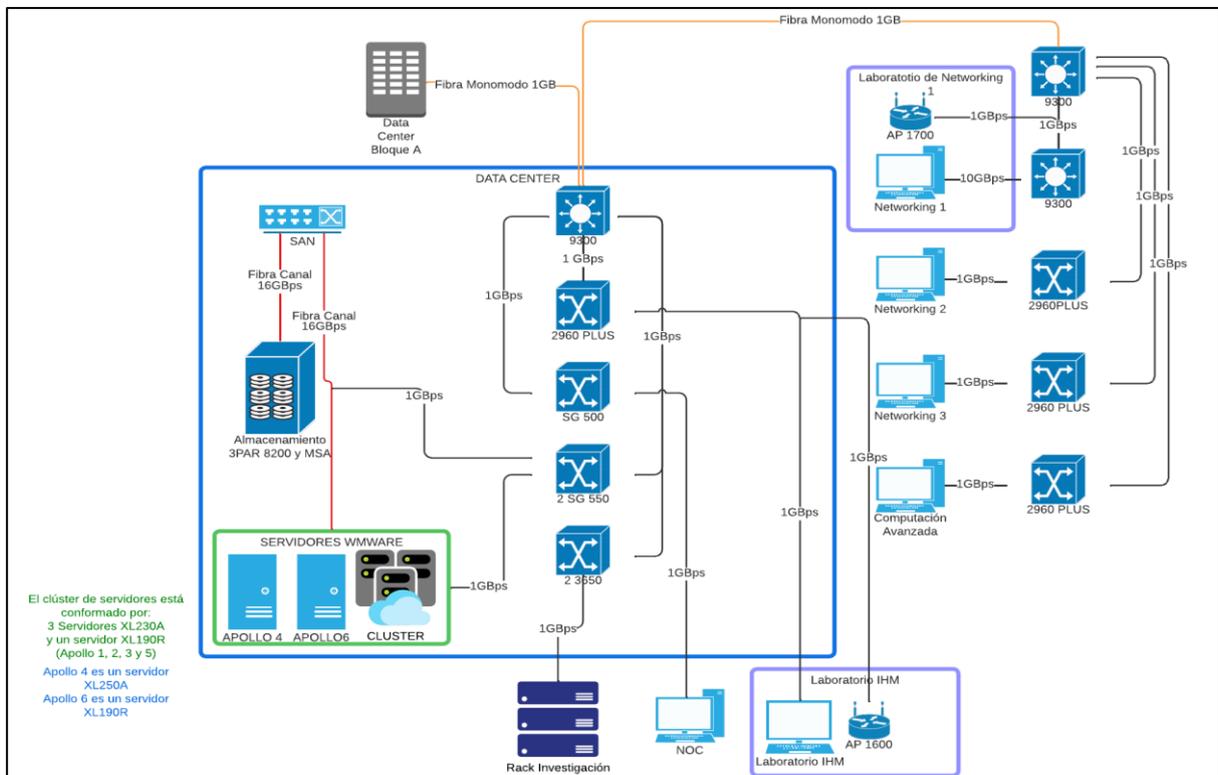


Gráfico 5: Diagrama de red del data Center extendido (tradicional) ubicada en el segundo piso del bloque D de la UPS. Elaborado por El departamento del Data Center

Se tiene seis (6) servidores en total de la marca HPE, la infraestructura consta de 3T en RAM (procesamiento) y 120 TB en storage (almacenamiento), la forma de comunicación entre los servidores se realiza a través de una red SAN a 16 Gbit/s; en un clúster se tiene 2 servidores Apolo y los otros dos (2) servidores (.24 y .6) están fuera del clúster ya que poseen una tarjeta de video y trabajan de manera independiente, teóricamente los servidores se comunican a 10 Gbit/s con los switch de agregación y ya con el switch de Core es a 1 Gbit/s. Se puede observar en el gráfico cinco (5) como se encuentran dividido el procesamiento. En el gráfico seis (6) se puede observar cómo se encuentra distribuido el almacenamiento del data center actual.

De acuerdo al gráfico 4 y 5 y con las visitas realizadas al centro de datos, el switch SAN es el encargado de gestionar toda la comunicación en todo el chasis de los servidores con una velocidad de 16Gbps, se conecta mediante fibra canal. Luego de los switchs SAN se conecta por cable categoría siete (7) al switch de administración y se comunican a 10Gbps. Luego, de los switchs de administración para comunicarse con el Core, este se comunica a 1Gbps. La máxima capacidad para salir en los switchs de administración es de 5Gbps, lo que ocasiona un cuello de botella.

Todo lo que se refiere a conexión horizontal se conecta mediante cable categoría 6a que trabaja a 1Gbps, únicamente se utiliza cable categoría 7 por la velocidad entre los dos rack.



Gráfico 6: Información detallada del procesamiento del data center: Elaborado por personal del Data Center.

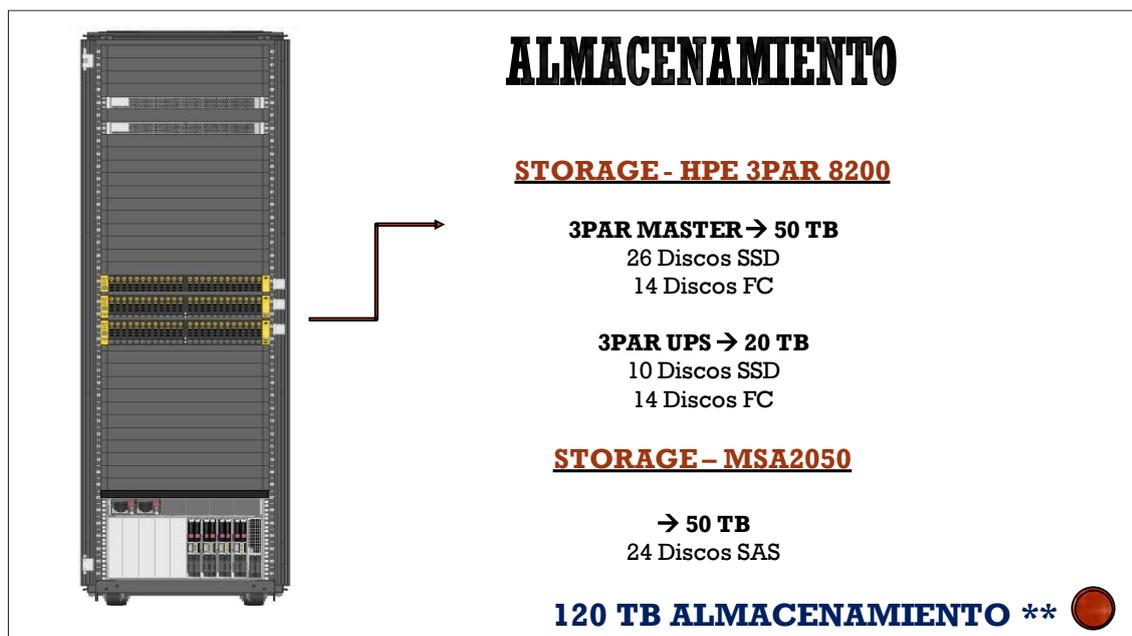


Gráfico 7: Información detallada del almacenamiento del centro de datos: Elaborado por Personal del Data center.

Toda la red del centro de datos se encuentra trabajando con las siguientes marcas de equipos:

- Conectividad: Cisco
- Procesamiento: HPE
- Almacenamiento: HPE

Los 4 servidores se encuentran clusterizados, el sistema operativo es ESXI [22], que sirve para virtualizar con VMware. El servidor (.6) tiene una tarjeta gráfica Envidia V100 que puede funcionar en modo grid [23], es decir 16 Gb dedicados. La otra tarjeta es de la marca Envidia k80 alojada en el servidor .24, la característica de la tarjeta es que solo se puede usar dos máquinas virtuales porque dispone de dos ranuras la tarjeta de video k80.

De momento se tienen aproximadamente 250 máquinas virtuales, las que se encuentran en el clúster y en los otros servidores; los protocolos de conexión se encarga el departamento de TI y los encargados del centro de datos; es decir todo el networking se encarga TI; el tráfico local que más se genera se tiene entre servidores, el nivel de procesamiento depende de la situación actual en que se encuentre. La arquitectura no presenta redundancia entre switch a nivel de distribución.

No se tenía en cuenta el nivel de crecimiento que iba a tener, por el cual se tendría que realizar muchos Subneteos para poder soportar todas las máquinas virtuales, ya que solo se asignó un (/24). Se puede tener una solución volviendo a reconfigurar con la ayuda de un /16, con las nuevas direcciones de las máquinas virtuales. Se tiene problemas de ruteo, es decir, se tiene ruteo de entrada, pero no de salida, no existe un forward bastante sólido al momento de realizar un ruteo. El centro de datos también ofrece servicios de almacenamiento, para esto se encuentra configurado de tal forma que se asignen en los discos de estado sólido y cuando estos se saturan, se brinda apoyo con los discos mecánicos.

Se tiene dos criterios de virtualización:

- Ha(alta disponibilidad se aplica a nivel de host, si se cae una salta el otro),
- ft (full tolerant a nivel de máquina virtual, trata de ser como un clon, se gasta más recursos porque se entrega una copia en tiempo real de la máquina virtual, por ende, genera más tráfico.).

A nivel de procesamiento no se cuenta con proveedores, debido a que balancea automáticamente, existe a veces problemas en red, porque se ingresa por escritorio remoto, la Universidad no permite realizar la conexión por vpn. Se gestiona el tráfico de manera virtual, el mayor tráfico se gestiona entre el clúster y el rack de comunicaciones.

2.2 SISTEMAS DE TEMPERATURA

El mecanismo de enfriamiento es por Gas. La tubería de agua se encarga de humidificar los rangos de operaciones mínimo al 30% de humedad, bajo eso se procede a un apagado del data center. Se trabaja a 19° casi estable a un 50%. Los parámetros que se consideran más importantes son flujo, nivel, humedad y punto de rocío, temperatura.

Se debe tener en cuenta que lo más importante es el punto de rocío, porque, indica cuando va a existir condensación, por problemas del otro aire acondicionado, impide que se tenga certificación TIER II porque es el único que no se está redundando.

La temperatura cuando excede, el flujo de aire se mide a 30 cm de la baldosa perforada ya que consta de sistema de pasillo frio y caliente. EL nivel de sonido, indica la condición de los ventiladores. Se tiene sensores de incendio bajo el piso y sobre el techo. Los sensores de vibración y presencia se encuentran bajo el piso más por control de seguridad.

El sistema de incendio cuenta con Ecaro 25, que es un sistema automatizado en su totalidad en estos incidentes.

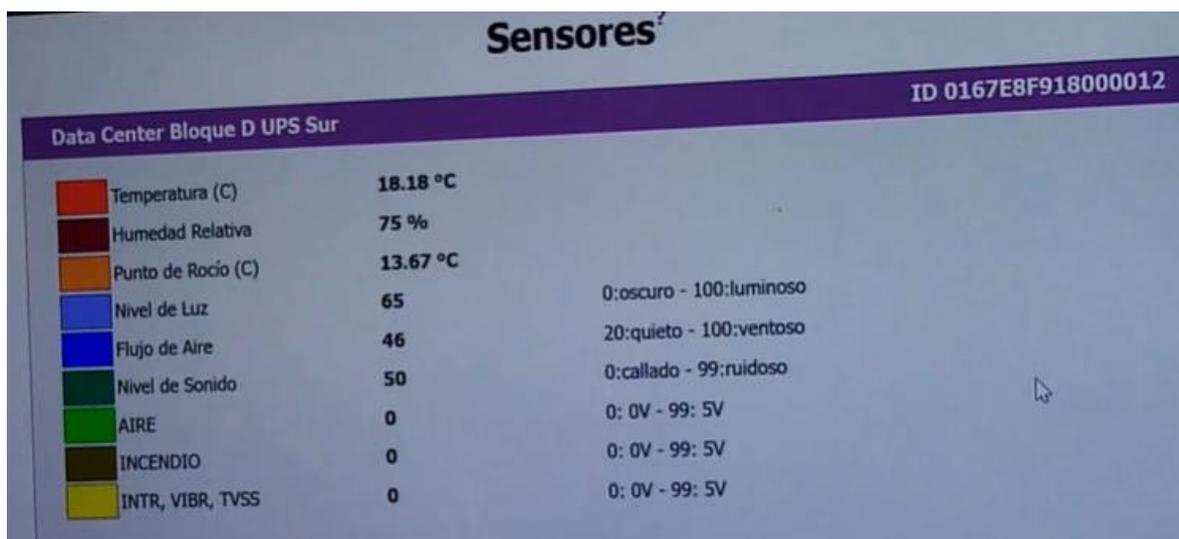


Gráfico 8: Captura de pantalla de los sensores del data center. Recuperada del software de sensores del Data Center Bloque D UPS Sur

2.3 SISTEMA DE ENERGÍA

Se encuentra energizado a 240 V. La reconexión de energía se realiza manualmente. Se tienen dos generadores propios de la universidad, si existe un fallo total de energía se tienen un tiempo de 20 minutos para poder realizar un apagado controlado.

Cuenta con dos líneas de red eléctrica de acuerdo con los estándares, de los dos generadores se distribuyen a los UPS, cuenta con N+1. El funcionamiento de la red depende también de la red propia de la universidad, ya que no se tiene un ISP propio para el centro de datos.



Gráfico 9: Lectura del panel de energía eléctrica tomada del data center. Dato tomado por John y Henry del panel eléctrico.

La única falla o caída de servidores se puede ocasionar cuando se pierda la energía, las fuentes de energía si son redundantes; si se produce una caída por pérdida de energía, no se tiene acceso a los servidores del centro de datos, pero se mantiene en gestión; se tienen supresores de pico para proteger los equipos que funcionan en complemento al para rayos que se tiene en la puerta principal del centro de datos. Los equipos se encuentran protegidos con tres mallas, de alta tensión, de alta frecuencia y media tensión, que se encuentran conectados a las mallas de la parte posterior separados de chispa.

2.4 ANÁLISIS DE LA RED CON AYUDA DEL SOFTWARE WIRE SHARK

Para el análisis de la situación actual del tráfico generado y recibido en la red operante en el centro de datos que se realiza el estudio, con ayuda del software Wireshark se puso en análisis durante 24 horas para determinar los paquetes que pasan a través del switch core del centro de datos; los resultados obtenidos se presentan a continuación.

2.5 Datos generales de la captura de tráfico.

Por el switch Core atraviesa todo el tráfico de la red, ya que es justamente este switch el que realiza la comunicación entre los servidores del centro de datos y las solicitudes de los usuarios. Por este motivo

se solicitó acceso al tráfico actual del centro de datos y para esto los encargados facilitaron un acceso remoto a una máquina que está conectada a este switch; los datos generales son:

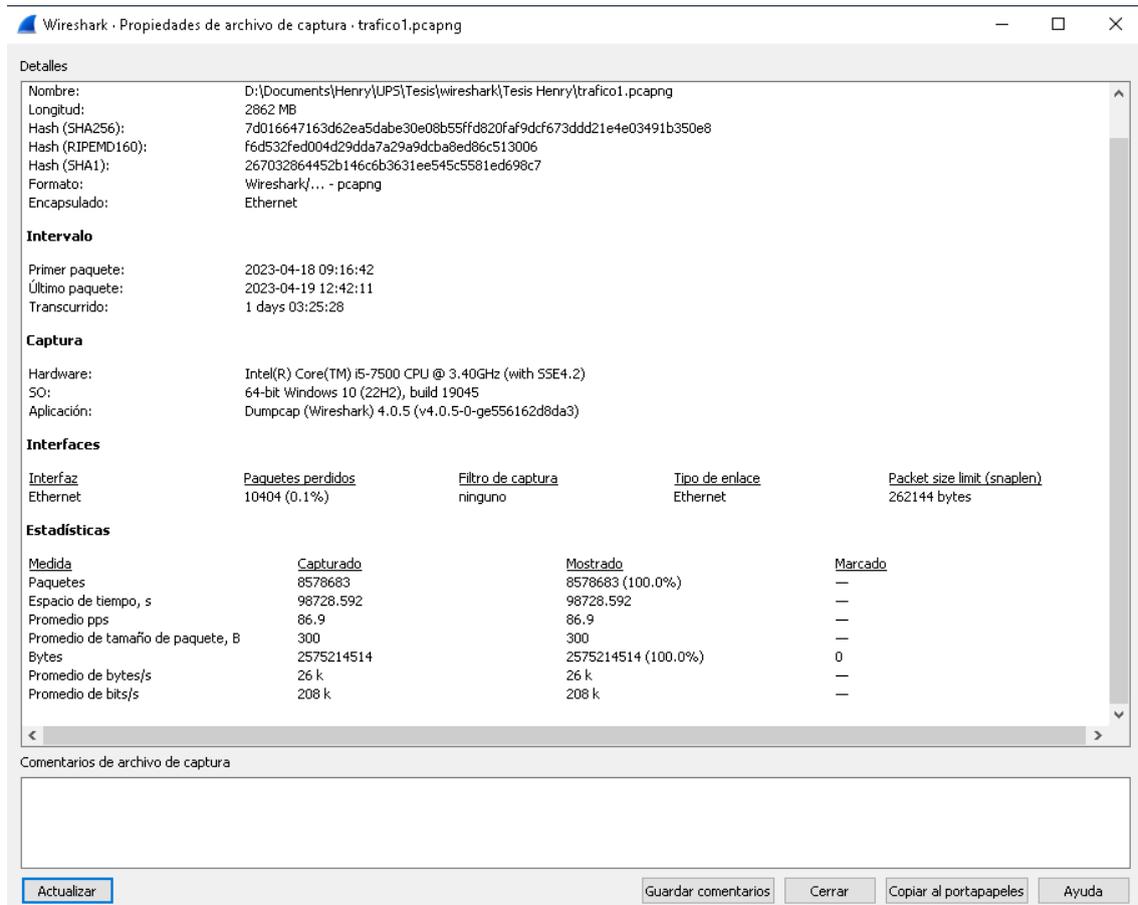


Gráfico 10: Captura de pantalla de Wireshark con los datos generales de la captura. Recuperado del software Wireshark

Como se muestra en el gráfico 10, el tiempo de captura de tráfico fue de 27 horas con 25 minutos y 28 segundos, donde se observa que por el switch Core circularon 8'578.683 paquetes de datos, cada uno de estos paquetes en promedio tienen un tamaño de 300 bytes.

Una de las ventajas de este software es que entrega datos de manera estadística, por este motivo no se requiere de un estudio estadístico extra con los datos ya generados por el software, como por ejemplo la gráfica diez (10) indica que en promedio se tiene una tasa de transferencia de 208 kbps; lo que corresponde a un promedio de 26 k bytes/s.

2.6 Transmisión de paquetes por puntos finales

Con ayuda de las herramientas de Wireshark se obtiene la información de paquetes enviados por cada uno de los puntos finales de la red; los datos obtenidos son los siguientes:

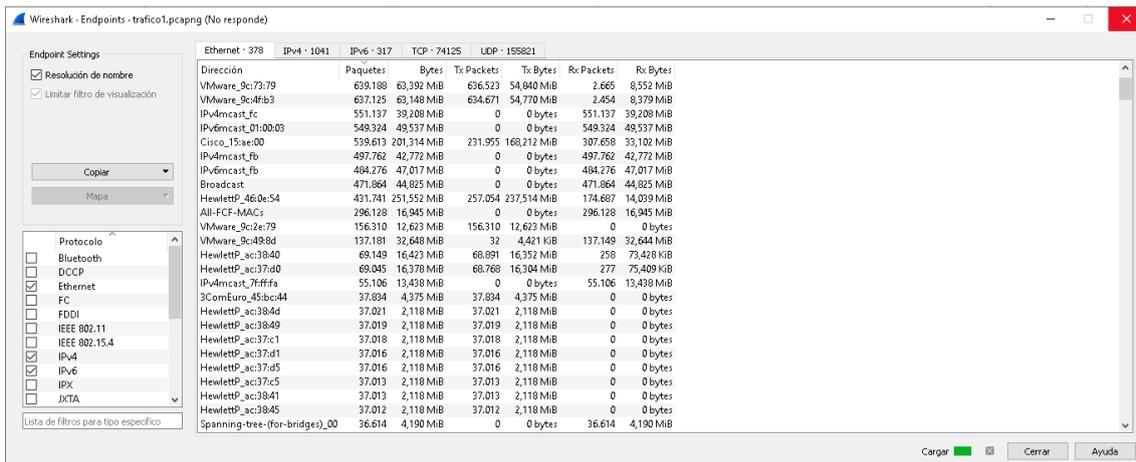


Gráfico 11: Captura de pantalla de los datos por puntos finales de la red. Recuperado del software Wireshark

Como se puede observar en los datos del gráfico once (11), los puntos que mayores paquetes generaron en la red son los correspondientes a VMware, lo que es lógico ya que con las licencias de VMware están asociados los servidores de virtualización, es decir durante todo el tiempo de captura existieron solicitudes para acceder a cada una de las máquinas virtuales del servidor.

2.7 Protocolo de mayor uso

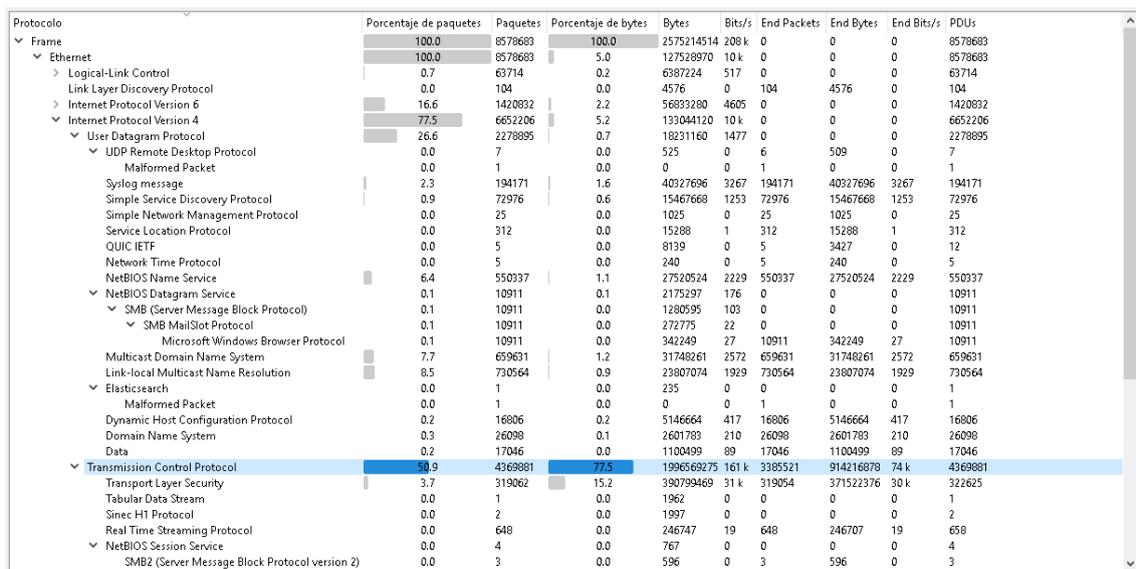


Gráfico 12: Captura de pantalla de Wireshark con los datos por protocolo de la red. Recuperado del software Wireshark

Todo el monitoreo se realizó con el puerto ethernet por ese motivo el 100 % de protocolos están dentro de la trama ethernet. Dentro de ethernet el protocolo de mayor uso es protocolo de internet versión 4; como se observa en el gráfico doce (12).

Dentro del protocolo IPV4, el protocolo con mayor uso es TCP (Transmission Control Protocol), seguido por el protocolo UDP (User Datagram Protocol); es decir el mayor consumo de recursos se da en la capa de transporte del modelo de red, justo para gestionar las capas aplicación y de red.

En el protocolo UDP se encuentran protocolos como los mensajes Syslog [24], los cuales representan

194.171 paquetes de los 8.578.683, lo que representa el 2,2% del total de paquetes enviados. UDP también cuenta con el protocolo SSDP (Simple Service Discovery Protocol), el cual es un protocolo que permite la interconexión entre dispositivos finales, este protocolo representa el 0,9% de paquetes transitados a través de la red.

EL último protocolo que se encuentra en UDP es el NET BIOS Name Service, este protocolo permite el acceso a los servicios que ofrece la red; se encuentran asociados 550.337 paquetes lo que representan el 6.4 % de paquetes.

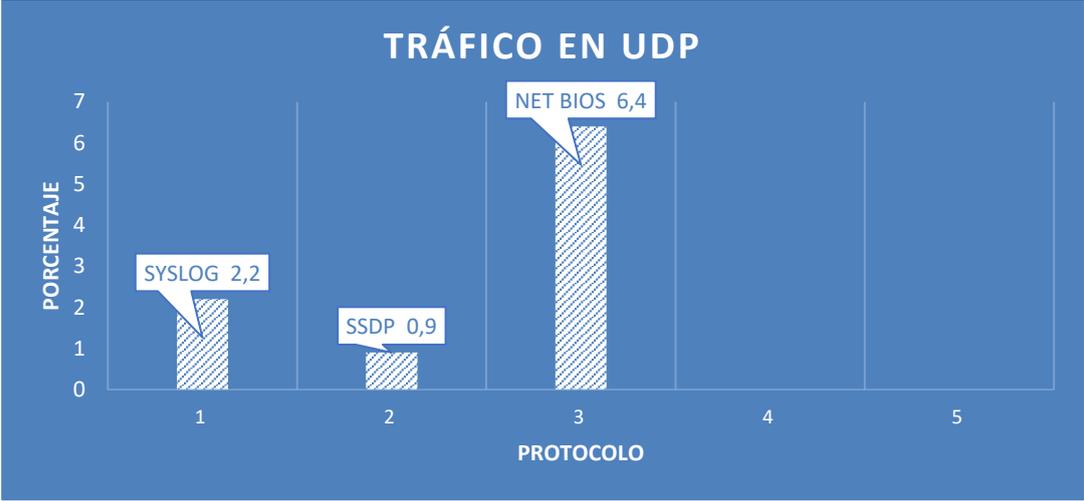


Gráfico 13: Porcentaje de paquetes generados por protocolo en UDP. Realizado por John y Henry

En conjuntos con el protocolo TCP, intervienen otros protocolos los cuales se especifican a continuación:

- El protocolo que mayor cantidad de paquetes genera es el HTTP (Hipertext Transfer Protocol), que representan el 7.6% del total de paquetes circulantes por la red.
- El protocolo TCP es orientado a establecer conexión entre dispositivos, por este motivo un protocolo que existe dentro de TCP es el protocolo de seguridad que genera el 3.7 % de paquetes.

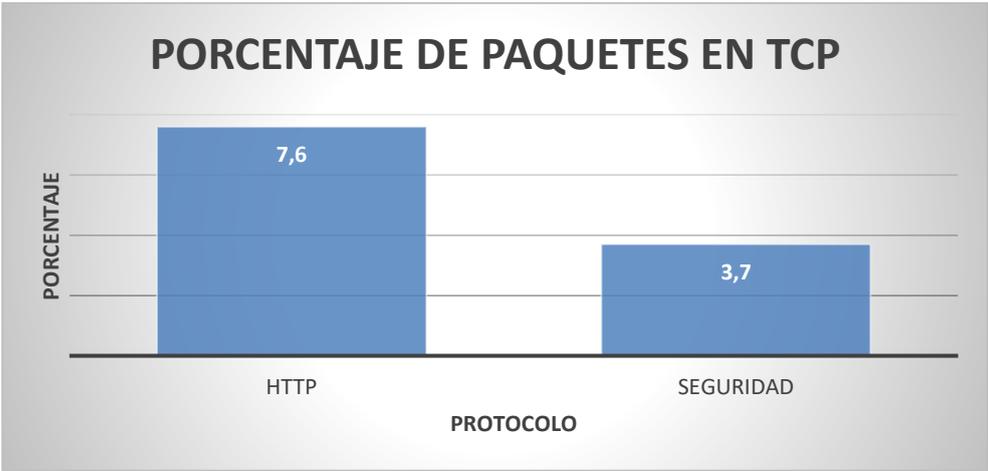


Gráfico 14: Porcentaje de paquetes generados por protocolo en TCP. Realizado por John y Henry

2.8 Transmisión de paquetes por tiempo.

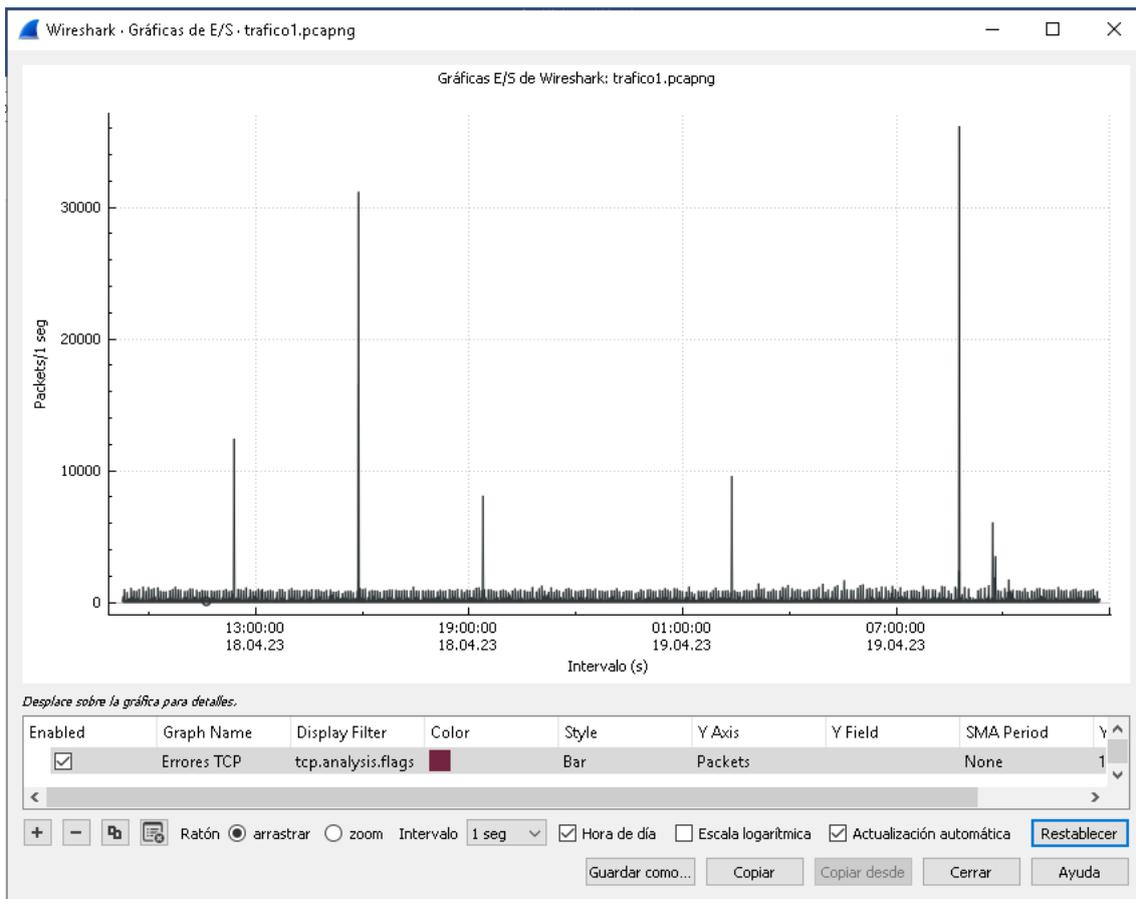


Gráfico 15: Captura de pantalla de Wireshark con la transmisión de paquetes por tiempo. Recuperado del software Wireshark

En el gráfico quince (15) se observa la transmisión de paquetes durante todo el periodo de tiempo en que se ejecutó y capturó el tráfico el Wireshark, donde se puede observar que a las 15:53 de la tarde del martes 19 de abril se tuvo un primer pico de transferencia de paquetes con un promedio de 31.176 de paquetes por segundo equivalente al 0.36% del total transmitido.

El pico más alto de transferencia en el periodo en el que se capturó el tráfico fue el miércoles 19 de abril a las 8:45 de la mañana con un promedio de 36.168 paquetes por segundo equivalente al 0.42% del total transmitido.

Como se puede observar en el gráfico trece (13) el protocolo de UDP de mayor uso es de NET BIOS con un porcentaje de 6.4%, el cual permite acceder a los servicios que ofrece la red implementada, por otro lado, el protocolo TCP (Transmission Control Protocol), de mayor uso es de HTTP (HiperText Transfer Protocol) con un porcentaje de 7.6% del total de los paquetes que circulan por la red actual. Todo los protocolos con respecto a seguridad, firewall no se encuentran reflejados en la captura del tráfico de la red del data center del bloque D debido a que estos protocolos se los maneja en el principal que se encuentra en el bloque A.

CAPÍTULO 3

3.1. DISEÑO E INFRAESTRUCTURA DE LA NUEVA RED

Una vez que se estudió el modelo actual del Centro de Datos del Bloque D de la Universidad Politécnica Salesiana, se propondrá un nuevo diseño con la arquitectura Spine and Leaf para el centro de datos del bloque D. Este diseño se enfoca en mejorar y reducir los cuellos de botella que presenta actualmente y con el adicional que este modelo de arquitectura tiene una gran ventaja, la cual es que tiene un mayor crecimiento en cuanto a la implementación de nuevos recursos para la presentación de máquinas virtuales. El modelo Spine and Leaf consta de dos capas: Spine y Leaf, se considera como columna y hoja y para su crecimiento lo que se debe realizar es agregar un switch en la capa Leaf para colocar un nuevo rack dependiendo de las necesidades que se requieran.

Al momento de realizar la simulación con el programa GNS3, al cargar las imágenes de los nuevos equipos para realizar el modelo Spine and Leaf se presentó el inconveniente que deja de funcionar el programa debido a la insuficiencia de memoria RAM, ya que las imágenes del switch CISCO NEXUS demandan de mucha RAM y solo al momento que se cargan no permite continuar. Se trabajó en Linux y Windows obteniendo el mismo resultado. Se pretendía utilizar el switch CISCO NEXUS debido a que presenta mejores características para su utilización en un centro de datos, por lo que se podría obtener mejores resultados en el desempeño de red, se puede evidenciar las especificaciones del switch en el anexo dos (2). Debido a esto se optó por realizar una simulación con equipos reales en el laboratorio Networking 3 del Bloque D de la Universidad Politécnica Salesiana prestado por los encargados del Data Center y del mismo Bloque. Se realizó la implementación de la red con la modelo de arquitectura Spine and Leaf; para la simulación del tráfico que genera la red, tomando en cuenta lo presentado en el capítulo 22, se procedió a realizar una emulación de máquinas virtuales, llamadas, para el caso de la vlan de telefonía, transferencias de datos entre vlan, ping extendido con carga de bytes, un servidor de juegos, etc., para poder generar la mayor cantidad de tráfico y poder simular el funcionamiento del Data center con el nuevo modelo.

3.2. Diseño de la nueva topología.

La red propuesta con la arquitectura Spine and Leaf, que se muestra en el gráfico 16, consta de dos switches en la capa Spine, los cuales se conectaran con el centro de datos del Bloque A del campus sur de la UPS. Para la capa de Leaf se ha mantenido los 7 switches, uno por cada departamento. La conexión física entre switches se realizó con cable UTP, esto para tener una conexión física similar a la actual. Para la distribución del enrutamiento inter-VLAN se configuró el protocolo VTP donde el switch Spine-1 se lo configuró como servidor del protocolo y el resto de switches únicamente como clientes, de esta forma todas la VLAN's creadas en el switch servidor serán aprendidas por los switches cliente. Este modelo permite dirigir el tráfico de la red por cada switch Spine y no quedará saturado como sucede actualmente en el switch core.

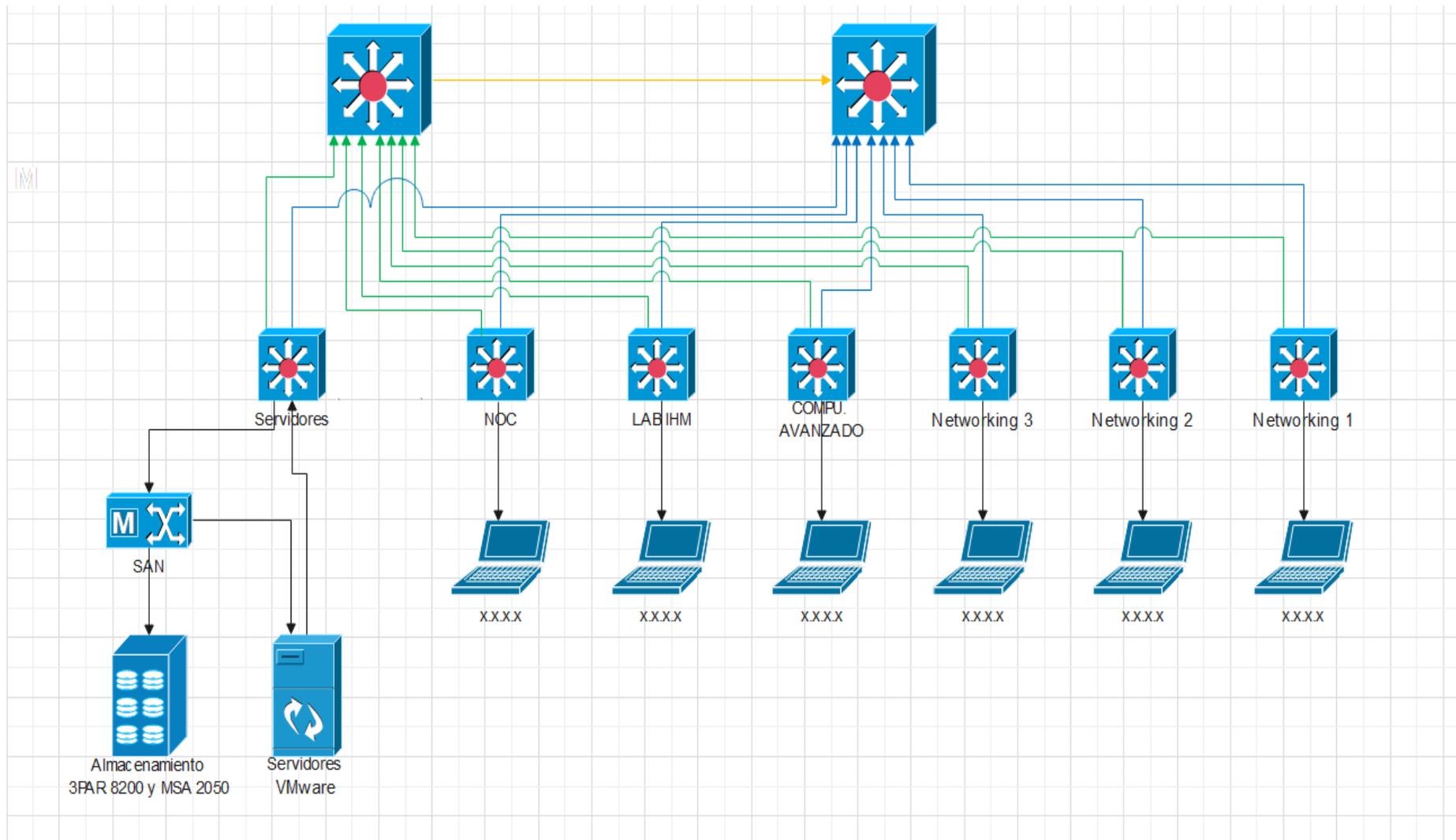


Gráfico 16: Diseño de la nueva arquitectura Spine and Leaf. Elaborado por John y Henry

La simulación de la red se realizó con equipos disponibles en los laboratorios de la UPS, además se optó por realizar todas las conexiones con cable UTP debido a que en la arquitectura actual no se cuenta con SFP's para realizar conexiones con fibra, motivo por el cual se realizaron las conexiones solo con este medio. No se ha puesto las IP por privacidad de la red interna.

3.3. Equipos usados en la implementación.

- Switch capa 3 de la marca cisco 3650
- Cable utp categoría 7
- Computadoras del laboratorio Networking 3

Se utilizó el switch capa 3 CISCO 3650 debido a que la infraestructura de la red actual tiene estos dispositivos en su diseño, y se pretende mostrar que utilizando los mismos conmutadores se obtendrán mejores resultados con la nueva infraestructura. Se puede evidenciar las características del switch en el anexo tres (3).

3.4. Configuración de los equipos (switch capa 3) serie 3650

La configuración de cada switch consta en principio de la configuración básica, es decir se coloca el hostname a cada switch, la contraseña de acceso a los equipos, a todos los equipos se les colocó de contraseña "tele" y la configuración de las líneas vty desde la 0 hasta la 15 para establecer un acceso mediante telnet a cada uno de los equipos.

Para la configuración de las VLAN en cada uno de los switches, se utilizó el protocolo Vlan Trunk Protocol (VTP), el cual permite establecer a un switch como un servidor VTP y al resto como cliente VTP; de esta forma cada switch cliente conocerá las VLAN configuradas en el switch servidor. Como en el modelo original del centro de datos, los switches no cuentan con ninguna configuración adicional, el modelo presentado en este proyecto tampoco se han agregado configuraciones extra a las mencionadas. Para conocer más sobre el protocolo VTP se recomienda leer en el anexo #1, donde podrá encontrar más información, así como los comandos de activación del protocolo en cada switch.

Previo a realizar la implementación en los equipos físicos se realizó una simulación a modo de prueba en el software Packet Tracer ya que el préstamo de los equipos fue por tiempo limitado y para evitar demoras en las configuraciones de cada uno de los equipos; una vez ya con las configuraciones que se implementó en los equipos del software, se procedió a cargar cada uno de los equipos para proceder con las pruebas necesarias en la red.

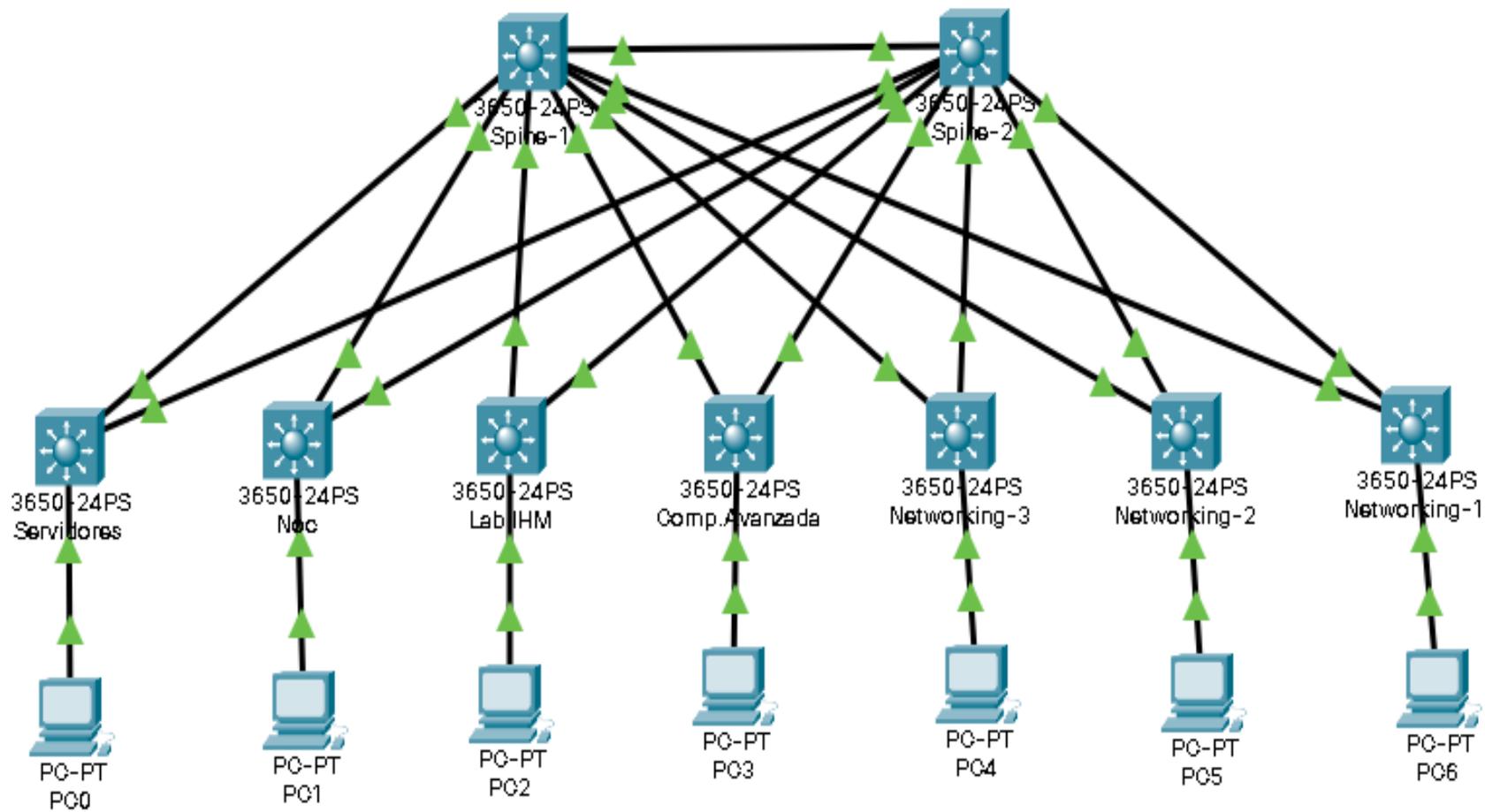


Gráfico 17: Diseño de la red en el software Packet Tracer. Elaborado por John y Henry

La red implementada físicamente, se presenta en el gráfico 18:

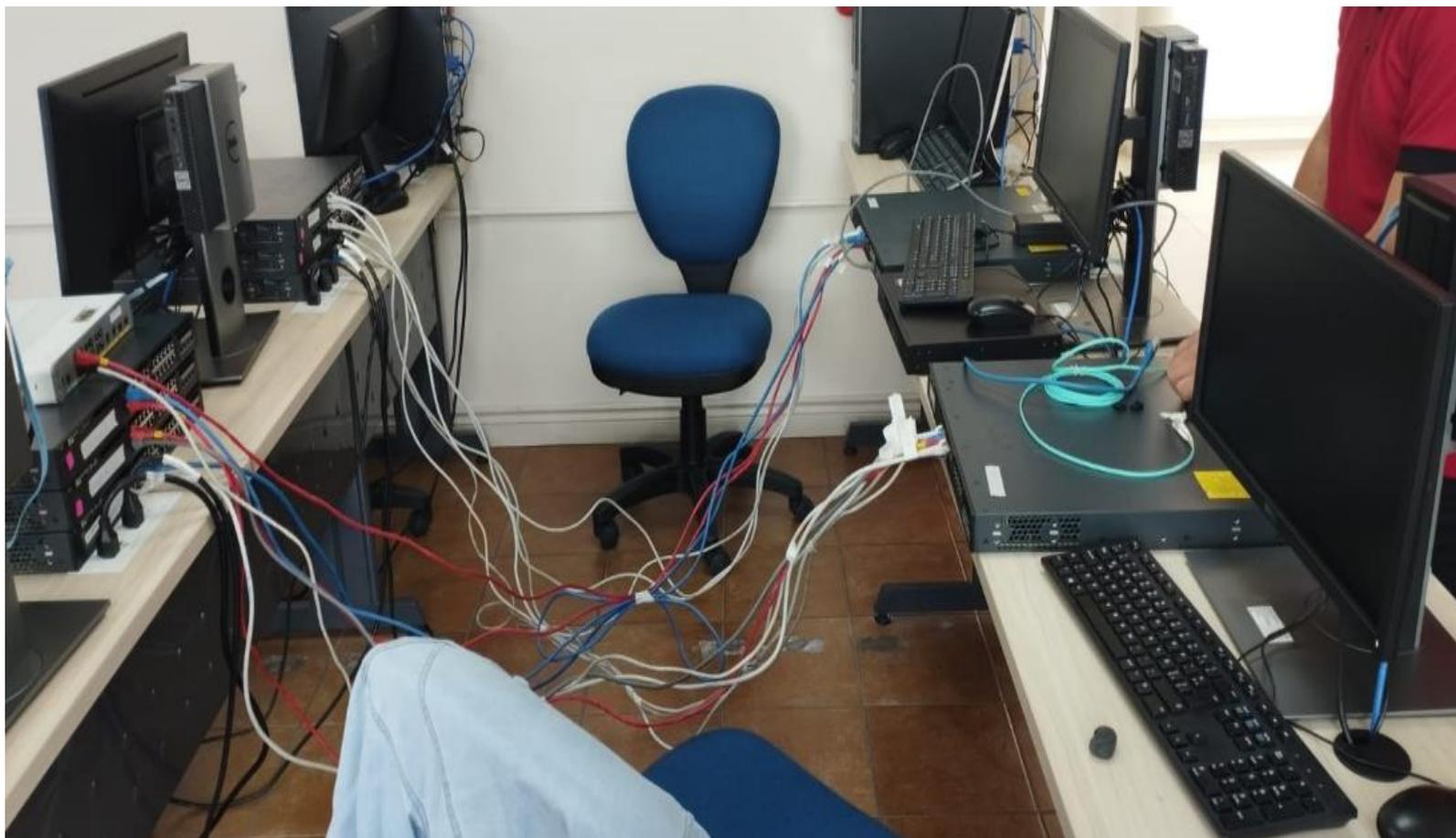


Gráfico 18: Red implementada con los equipos del laboratorio de la UPS. Tomada por John y Henry

Como cada departamento cuenta con telefonía, en cada switch se destinó un número de puertos para la vlan de telefonía y para simular la gestión de llamadas entre departamentos se utilizó el software BigAnt Messenger, que se detalla en el siguiente punto su funcionamiento y configuración.

Para simular una virtualización, en el switch de servidores se destinó una computadora y con ayuda del software TightVNC Viewer, que se detalla más adelante su configuración y funcionamiento, se realizó un acceso a un escritorio de forma remota desde las máquinas externas de la red hacia el computador del switch de servidores, con la conexión remota establecida se realizaron actividades como transferencia de un video con el uso del mismo software.

3.5. Servidor de llamadas BigAnt Messenger

3.5.1 Primero se debe descargar los archivos (server y cliente) de la página oficial de BigAnt www.bigantsoft.com/, se tiene dos versiones, una licenciada y otra de prueba, para la implementación se utilizó la de prueba.

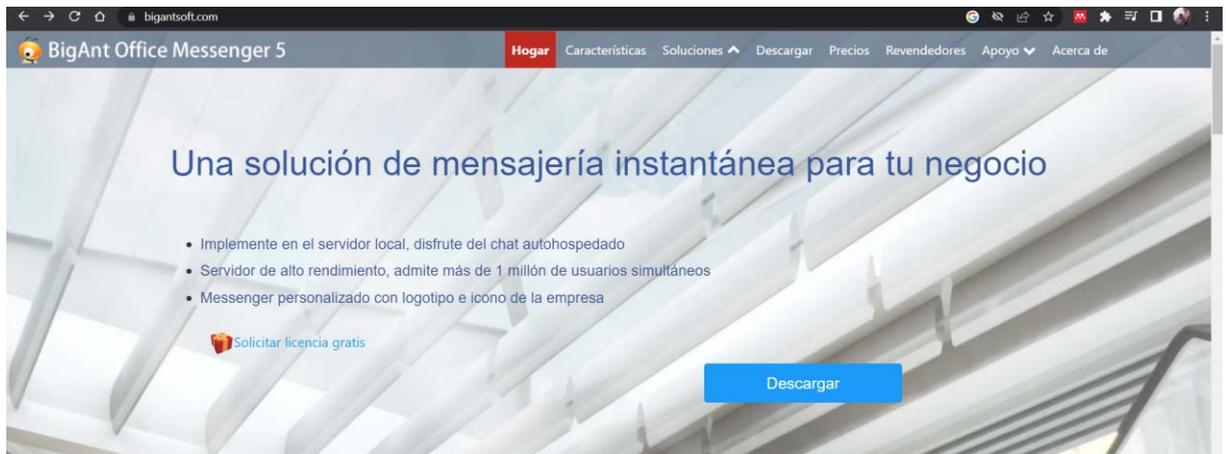


Gráfico 19: Captura de la página oficial del programa BigAnt. Captura de John y Henry. Recuperada del sitio oficial del software [25]

3.5.2 Descomprimir el documento .rar donde se encuentra almacenado el servidor y el cliente.

3.5.3 En el servidor y todas las computadoras que van a simular el papel de telefonía se configura la misma IP de esta vlan llamada “Telefonía”, por privacidad de las IP internas manejadas en el data center no se muestra la configuraciones de los computadores, se detalla en el grafico () la configuración del protocolo ipv4 de dos PC asegurando que se encuentren en la misma dirección de red.

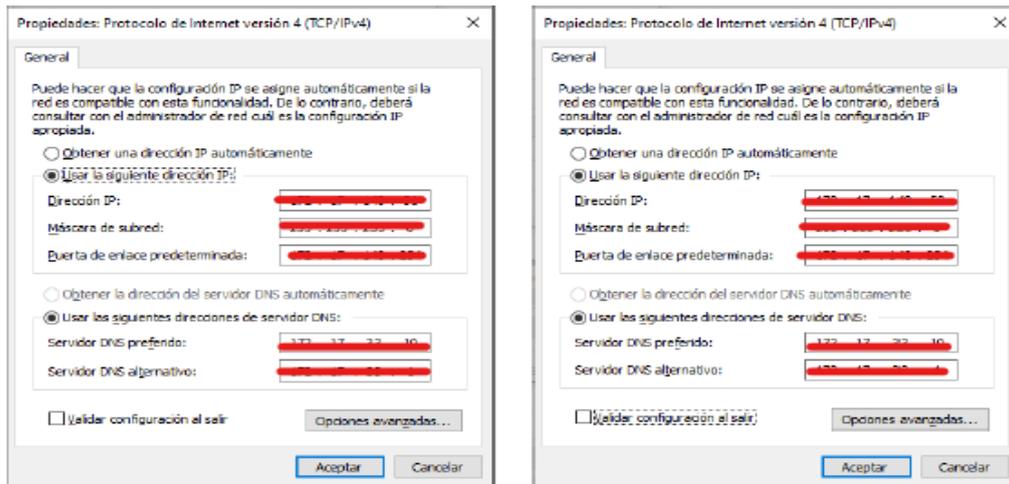


Gráfico 20: Captura de configuraciones del protocolo de Internet versión 4 (TCP/IPv4). Captura de John y Henry.

- 3.5.4 En un computador ejecutar y abrir el servidor de chat y video nombrado como BigAnt Console, como muestra la siguiente imagen.

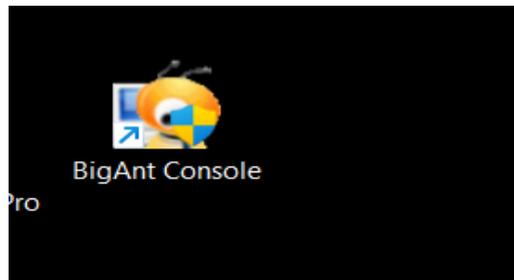


Gráfico 21: Captura de la app de BigAnt Console. Captura de John y Henry.

- 3.5.5 Dentro de la aplicación de BigAnt Console, presionar el botón IP (resaltado con color amarillo), para verificar la Ip que se encuentre configurada como estáticamente en la dirección de red, luego se debe cerrar la ventana ya cuando se encuentre verificado el mismo segmento de red.

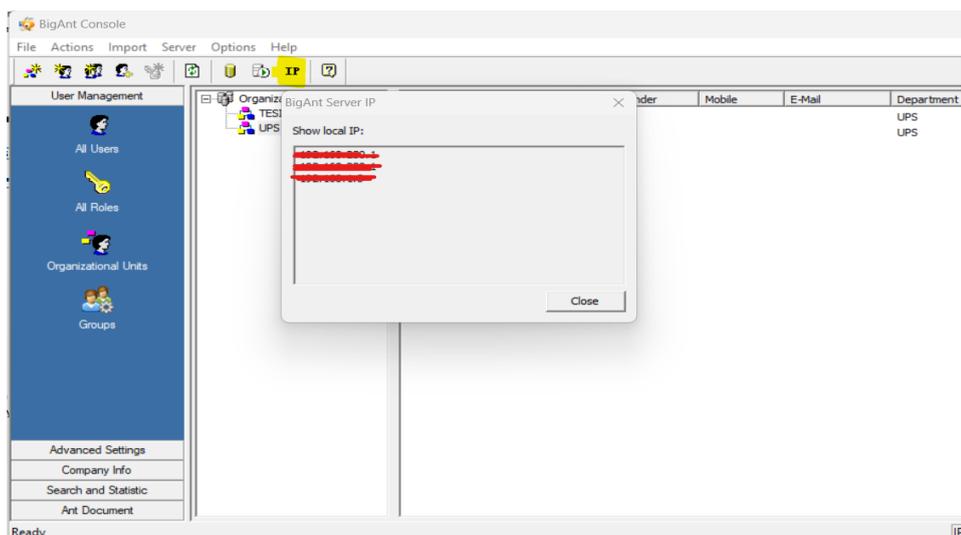


Gráfico 22: Captura de verificación de IP en el servidor de BigAnt. Captura de John y Henry.

- 3.5.6 Para la creación de los usuarios, en la ventana del Console presione el botón *create new user* y se debe agregar los usuarios que se encuentren dentro de la *vlan*, se debe configurar un nombre y una contraseña, luego se presiona el botón *acceptar* y se repite el paso para los usuarios que desea crear, guiarse de la figura veinte y tres (23).

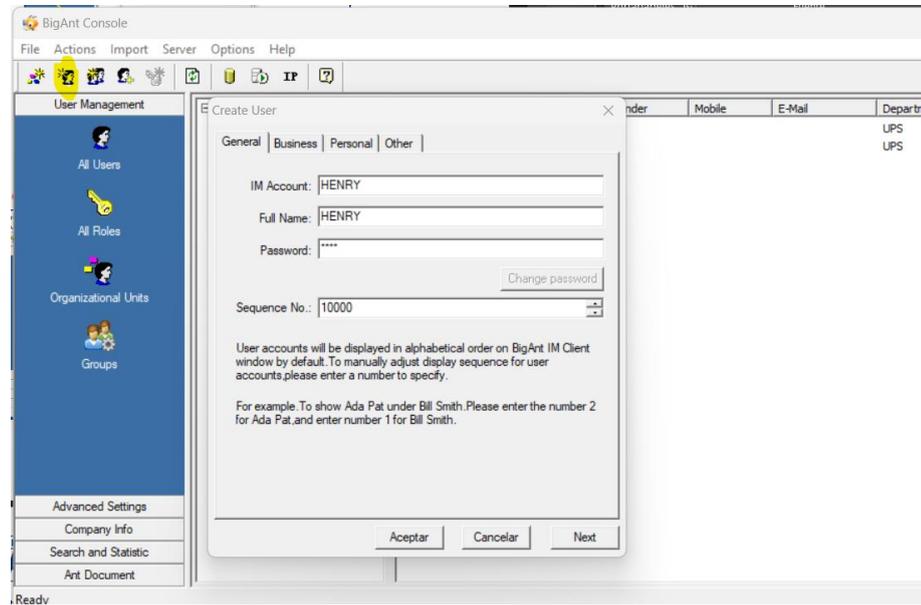


Gráfico 23: Creación de los usuarios en la ventana de BigAnt Console. Captura de John y Henry.

- 3.5.7 Para verificar la creación de los usuarios, presionar *all user* en la pantalla principal, como se muestra en la siguiente figura.

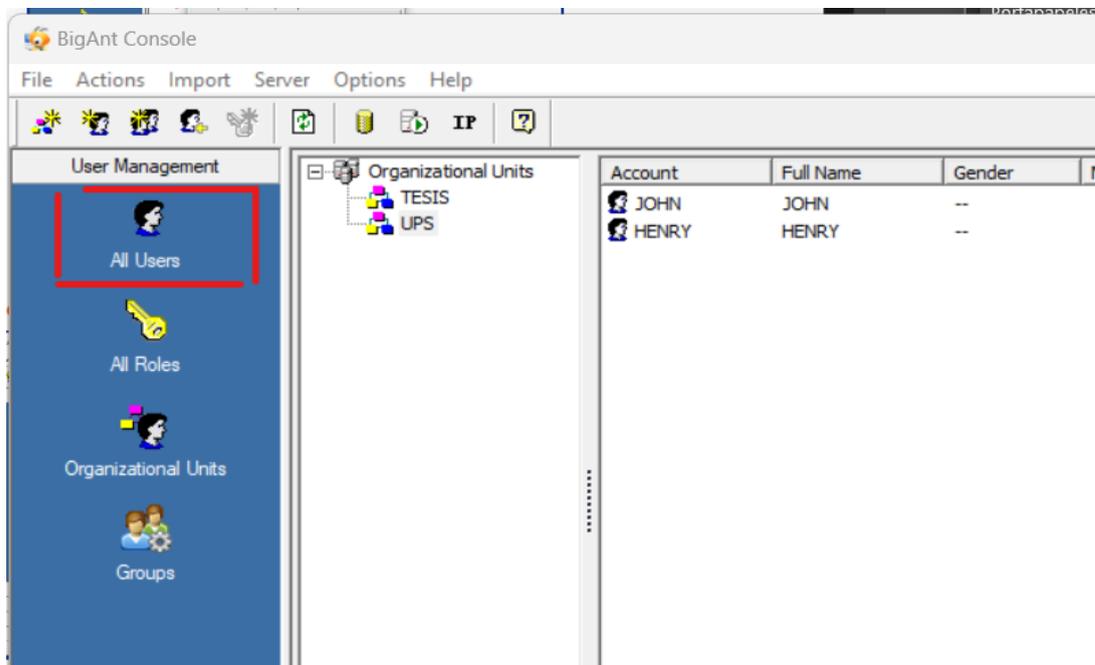


Gráfico 24: Verificación de los usuarios creados. Captura de John y Henry.

- 3.5.8 Una vez creado el servidor, se ejecuta y se abre el cliente en otras computadoras conectadas en la misma *vlan*, se debe configurar la misma dirección de red en las computadoras cliente.

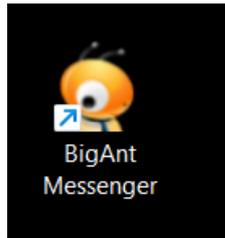


Gráfico 25: Captura de la app de BigAnt Messenger (cliente). Captura de John y Henry

3.5.9 Se va a desplegar la configuración de la IP del servidor que se configuró anteriormente, iniciar sesión con los usuarios y contraseñas creadas.

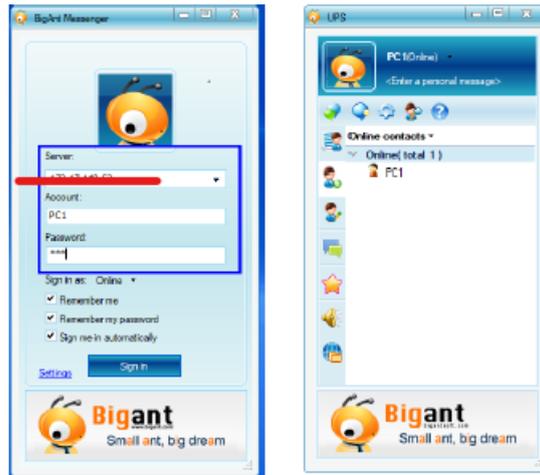


Gráfico 26: Acceso a la app con credenciales creadas en el servidor. Captura de John y Henry

3.5.10 Una vez que se inició se puede visualizar a todos los usuarios conectados y se puede interactuar con los usuarios conectados, llamadas, videollamadas, transferencia de archivos, etc.



Gráfico 27: Videollamada entre el pc de John y Henry. Captura de John y Henry

De esta manera se realizó la simulación de telefonía, transferencia de archivos, con esta simulación se genera tráfico y se evidencia en los Spine principales.

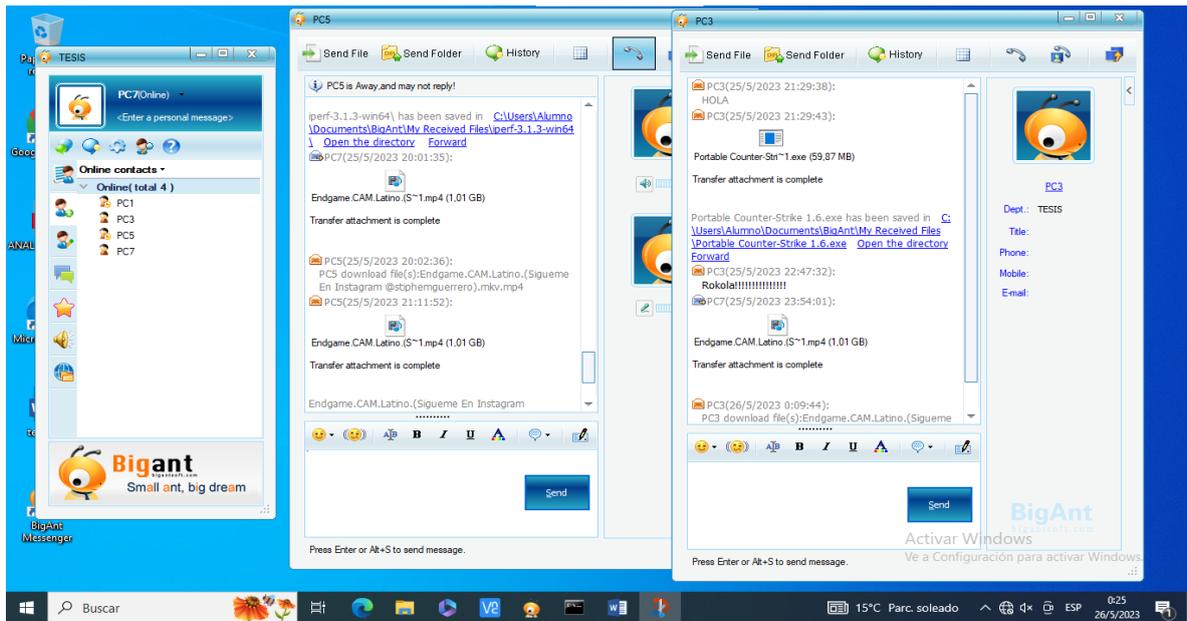


Gráfico 28: Captura de chat, llamada y transferencia de datos mediante el BigAnt. Captura de John y Henry.

3.6. Servidor de Juego (Counter Strike)

3.6.1 Primero se debe descargar el archivo del juego de la página oficial, para la simulación se descargó un portable.

COUNTER STRIKE 1.6	31/5/2017 20:38	Aplicación	233.025 KB
CSFull ByErasmusProducciones	21/3/2020 21:01	Archivo WinRAR	271.253 KB
TRADUCCION AL ESPAÑOL (COUNTER_S...	27/2/2011 13:47	Aplicación	38.407 KB

Gráfico 29: Archivos de descarga del servidor de juego. Captura de John y Henry

3.6.2 Luego se ejecuta y en una máquina principal como servidor, para la creación del servidor se debe ingresar el código que solicita el juego para poder crear las partidas.



Gráfico 30: Ejecución del servidor del juego counter. Captura de John y Henry

3.6.3 Una vez ingresado el CD Key se crea la partida dentro de la misma vlan para que los otros

jugadores cliente se puedan conectar y poder estar en la misma partida.

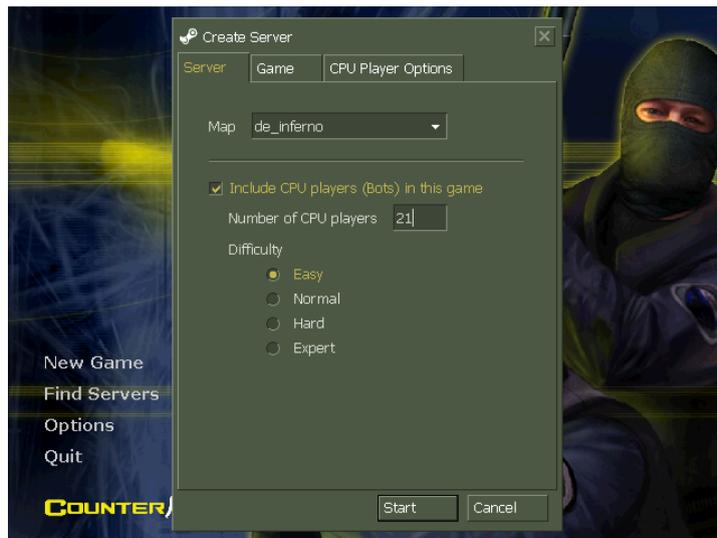


Gráfico 31: Creación de las partidas dentro de la misma Vlan. Captura de John y Henry

- 3.6.4 Las otras computadoras que se encuentran en la misma vlan, igual se debe ejecutar el portable, para conectarse al servidor creado en la vlan, este se reflejará ya creado en la página principal del juego. Por privacidad de las IP's no se muestra la creación de la partida en la vlan.
- 3.6.5 Una vez que se ha seleccionado la LAN del servidor, se direcciona directo a la recreación y se podrá jugar en la misma partida, esto ayudará a generar más tráfico simulando la nueva red y verificar el desempeño de los Spine.



Gráfico 32: Foto del juego implementado. Tomada por John y Henry.

3.7. Creación de máquinas virtuales mediante TightVNC Viewer.

- 3.6.1 Primero se debe descargar el archivo del TightVNC de la página oficial de TightVNC, se debe descargar de acuerdo con su computador.



Gráfico 33: Captura del sitio oficial y documentos a descargar para la implementación. Captura de John y Henry

3.6.2 Se ejecuta el archivo y se desplegará una ventana como la siguiente figura treinta y cuatro (34), se debe colocar la IP asignada a su máquina virtual, esta se relaciona a la vlan de servidores, donde se encuentra las máquinas virtuales que oferta la universidad.

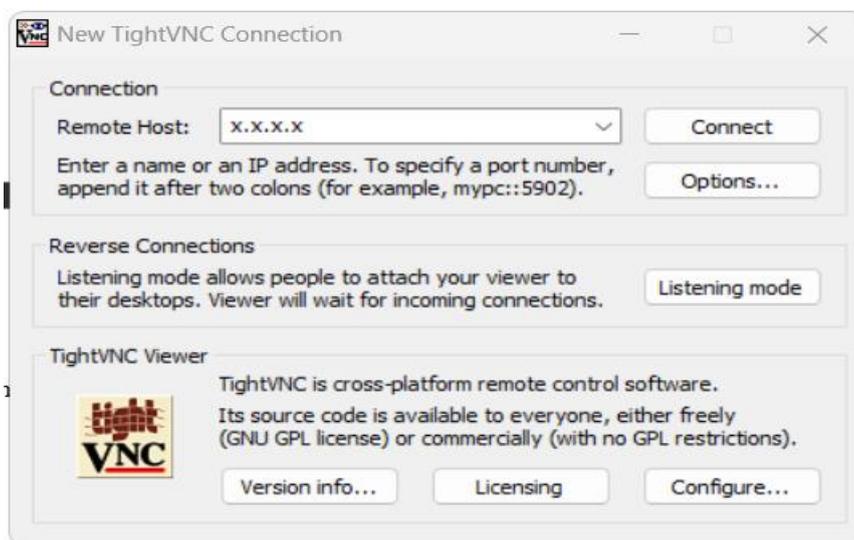


Gráfico 34: Captura de la pantalla principal de la app. Captura de John y Henry

3.6.3 Para la simulación de estas máquina virtuales se conectó a la principal donde se encuentra en la vlan de servidores.

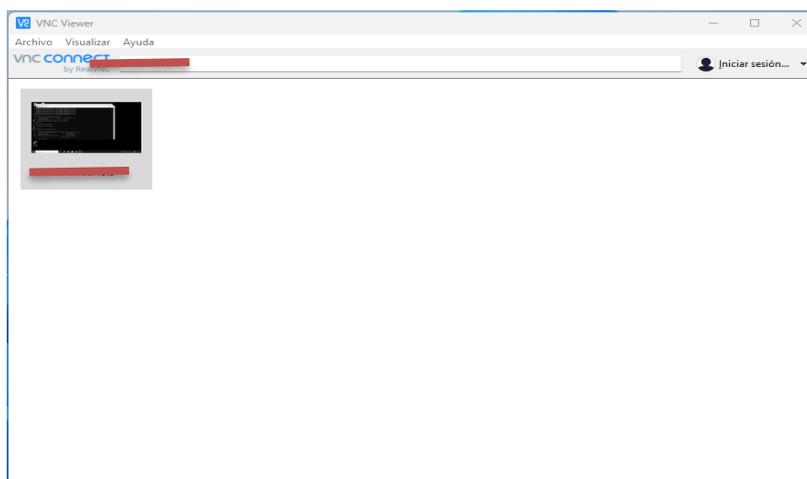


Gráfico 35: Conexión hacia la máquina principal de servidores de virtualización. Captura de John y Henry

3.6.4 En el servidor principal se puso a reproducir una película el cual ayudará a generar más tráfico y verificar el desempeño de los Spine.

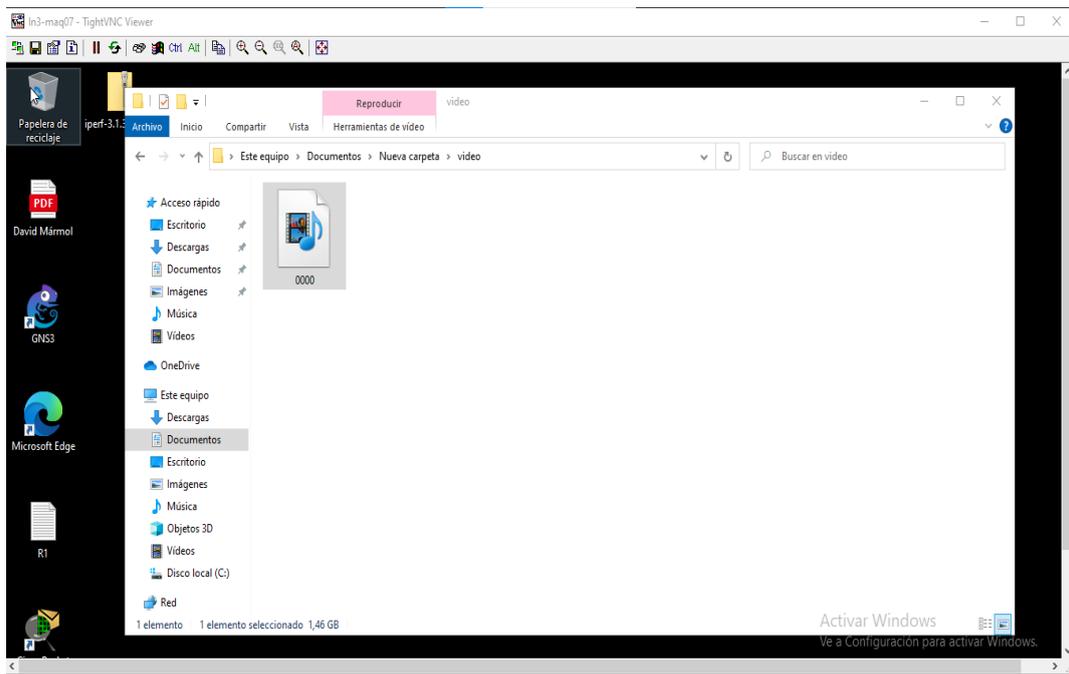


Gráfico 36: Servidor con movie para reproducir y generar tráfico hacia los Spine. Captura de John y Henry.

3.6.5 Adicional, el programa TightVNC sirve como gestor de transmisor y receptor de documentos, archivos, etc., para ello se copia un documento pesado de la maquina principal a la simulación de la máquina virtual. Se debe escoger el documento a copiar y seleccionar donde se va a alojar en el momento que se copie.

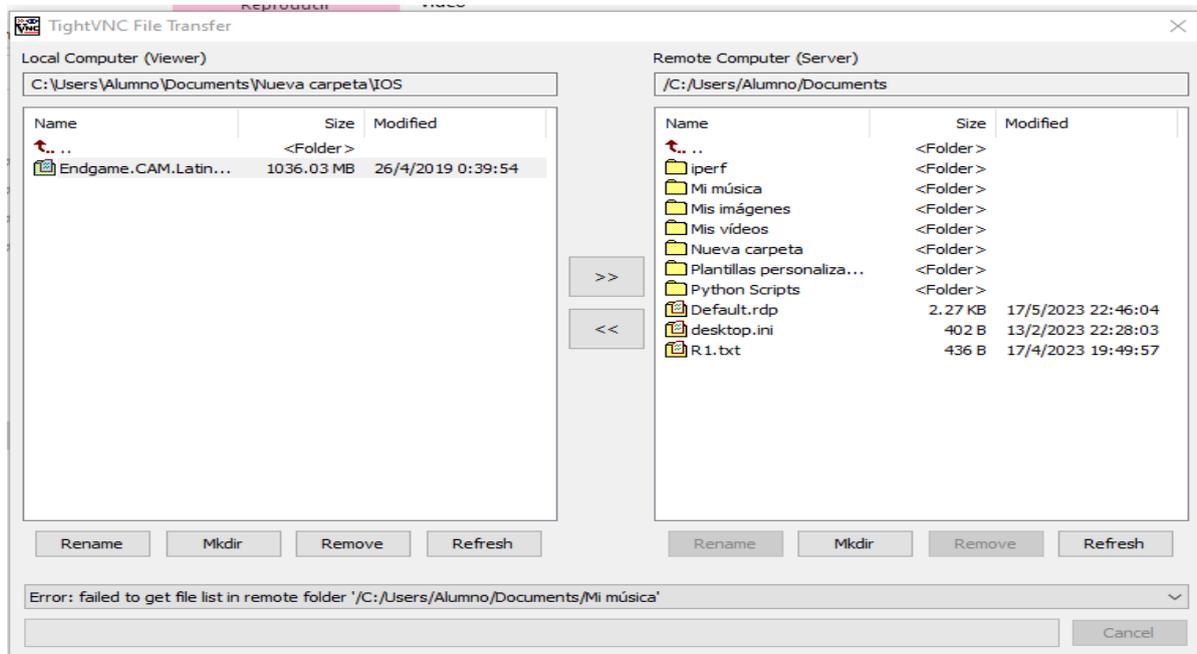


Gráfico 37: Selección de archivos para transferir a otro destino mediante TightVNC. Captura de John y Henry

3.6.6 Una vez realizado el paso 3.6.5. se selecciona los símbolos de mayor para realizar la copia, como se muestra en la siguiente imagen

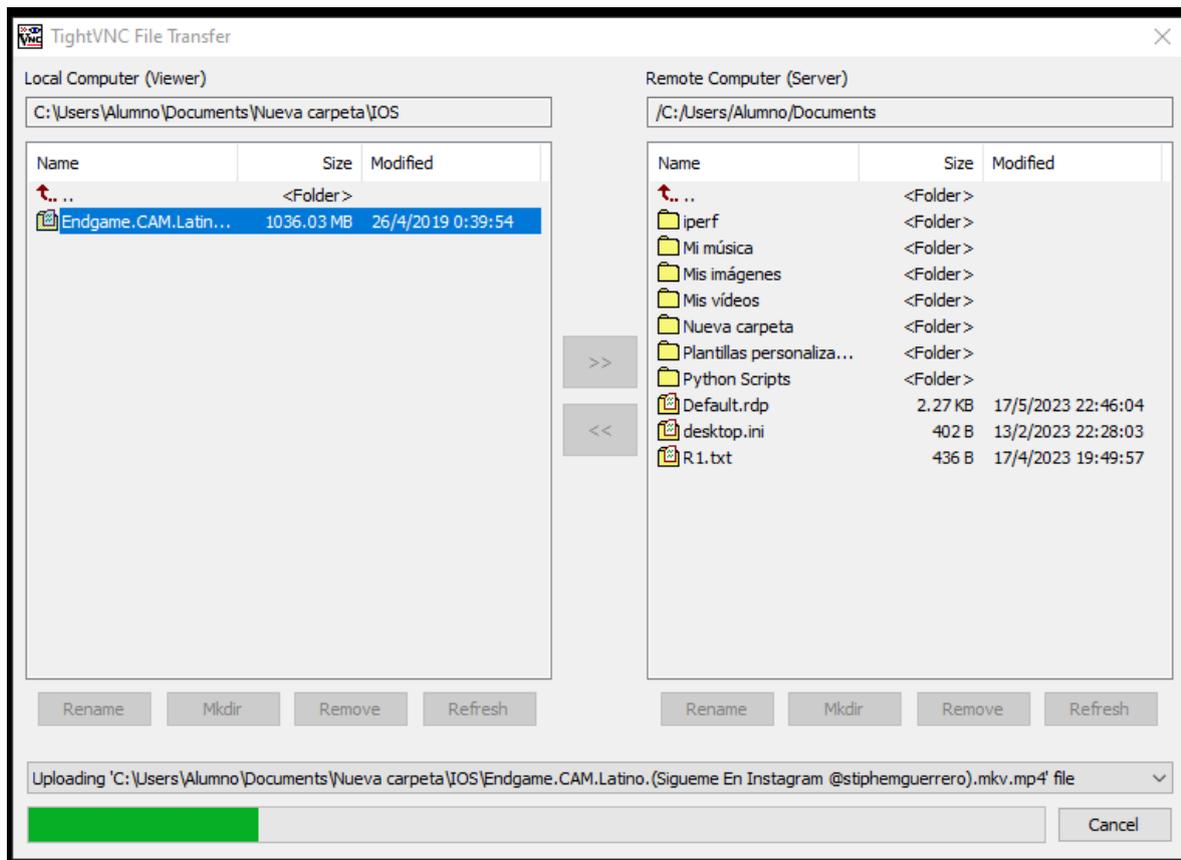


Gráfico 38: Tránsito de documentos hacia otro destino para la creación de tráfico. Captura de John y Henry

3.8. Generación de ping extendido con carga de bytes

Para la creación del ping extendido cargado de bytes, se realizó el ataque desde los computadores conectados en los diferentes switches, a continuación, se detalla cómo realizar la carga de bytes:

- 3.8.1. Abrir la consola "símbolo de sistema"
- 3.8.2. Escribir el comando ping -t seguido de un espacio y la IP del destino (spine 1, spine 2 o máquinas) que se desea llegar, seguido un espacio y el comando -l, no olvide especificar el tamaño de bytes para enviar.
- 3.8.3. Se puede observar en la siguiente imagen.

```
C:\WINDOWS\system32\cmd. x + v - □ x
Respuesta desde : bytes=17000 tiempo=6ms TTL=254
Respuesta desde : bytes=17000 tiempo=5ms TTL=254
Respuesta desde : bytes=17000 tiempo=8ms TTL=254
Respuesta desde : bytes=17000 tiempo=9ms TTL=254
Respuesta desde : bytes=17000 tiempo=9ms TTL=254
Respuesta desde : bytes=17000 tiempo=4ms TTL=254
Respuesta desde : bytes=17000 tiempo=5ms TTL=254
Respuesta desde : bytes=17000 tiempo=6ms TTL=254
Respuesta desde : bytes=17000 tiempo=5ms TTL=254

Estadísticas de ping para .....
Paquetes: enviados = 20306, recibidos = 20306, perdidos = 0
(0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
Mínimo = 4ms, Máximo = 72ms, Media = 6ms
Control-C
^C
C:\Users\ligaj>

C:\WINDOWS\system32\cmd. x + v - □ x
Respuesta desde : bytes=17000 tiempo=11ms TTL=254
Respuesta desde : bytes=17000 tiempo=6ms TTL=254
Respuesta desde : bytes=17000 tiempo=13ms TTL=254
Respuesta desde : bytes=17000 tiempo=5ms TTL=254
Respuesta desde : bytes=17000 tiempo=5ms TTL=254
Respuesta desde : bytes=17000 tiempo=6ms TTL=254
Respuesta desde : bytes=17000 tiempo=6ms TTL=254
Respuesta desde : bytes=17000 tiempo=6ms TTL=254
Respuesta desde : bytes=17000 tiempo=5ms TTL=254

Estadísticas de ping para .....
Paquetes: enviados = 20280, recibidos = 20280, perdidos = 0
(0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
Mínimo = 4ms, Máximo = 76ms, Media = 6ms
Control-C
^C
C:\Users\ligaj>
```

Gráfico 39: Ejemplo de ping cargado de bytes hacia los Spine. Captura de John y Henry.

CAPÍTULO 4

4.1 RESULTADOS

Como se observó en el diseño de la nueva arquitectura de red, se tienen dos switches que permiten salir a la red principal de la UPS, por lo que en la implementación de la red se colocó dos computadoras conectadas a los switches Spine, con el objetivo de poder realizar una captura del tráfico que estuvo generando en la red implementada. De manera similar a lo que se presenta en el capítulo 2 en la sección del análisis de la red actual, con ayuda del software WireShark, se realizó la captura durante 5 horas, 48 minutos con 17 segundos para lograr con el objetivo de superar los 8 millones de paquetes transmitidos durante la captura de la red actual, los resultados de las capturas de cada switch se las presentan a continuación.

Intervalo	
Primer paquete:	2023-05-25 11:32:01
Último paquete:	2023-05-25 17:20:18
Transcurrido:	05:48:17

Gráfico 40: Intervalo de tiempo del Spine 1: Capturado del tráfico del Spine 1 por John y Henry

4.2 CAPTURA SPINE 1

En este apartado se realiza un análisis del tráfico capturado por el switch spine-1, Se debe recordar que en cada switch Spine fue conectada una computadora que simularon ser redes externas desde las cuales se realizó una interacción con la red interna. En primer lugar, se presentan los datos generales de la captura, donde se evidencia el número de paquetes se transmitió por el switch spine-1.

The screenshot shows the Wireshark 'Properties of capture file' window for 'SPINE1.pcapng'. It is divided into several sections:

- Detalles:** Shows hashes (SHA256, RIFEMD160, SHA1) and format (Wireshark/... - pcapng).
- Intervalo:** Shows the capture period from 2023-05-25 11:32:01 to 2023-05-25 17:20:18, lasting 05:48:17.
- Captura:** Lists hardware (Intel(R) Core(TM) i7-8700T CPU @ 2.40GHz), OS (64-bit Windows 10), and application (Dumpcap).
- Interfaces:** A table showing the capture interface (Ethernet) with 0 lost packets, no filter, Ethernet link type, and a 262144 byte packet size limit.
- Estadísticas:** A table comparing captured vs. displayed data. All captured data (4113859 packets, 5823858580 bytes) is shown.

Medida	Capturado	Mostrado	Marcado
Paquetes	4113859	4113859 (100.0%)	—
Espacio de tiempo, s	20897.122	20897.122	—
Promedio pps	196.9	196.9	—
Promedio de tamaño de paquete, B	1416	1416	—
Bytes	5823858580	5823858580 (100.0%)	0
Promedio de bytes/s	278 k	278 k	—
Promedio de bits/s	2229 k	2229 k	—

Gráfico 41: Información transmitida del Spine 1: Capturado del tráfico del Spine 1 por John y Henry

Como se ve en la gráfica cuarenta y uno (41), durante todo el proceso de captura no existieron pérdidas de paquetes, a pesar de que en la máquina conectada a este switch se realizó una conexión con escritorio remoto hacia la máquina conectada en el switch de servidores y se realizaron actividades como: transferencia de archivos, que incluyó una película de 1 GB y se realizó una transmisión de video en vivo, en este punto fue fácil identificar que la red estaba funcionando de forma correcta, porque el video en el escritorio remoto no sufrió retardos en comparación al video que se pudo observar en la máquina del switch de servidores.

4.3 TRANSMISIÓN DE PAQUETES POR TIEMPO.

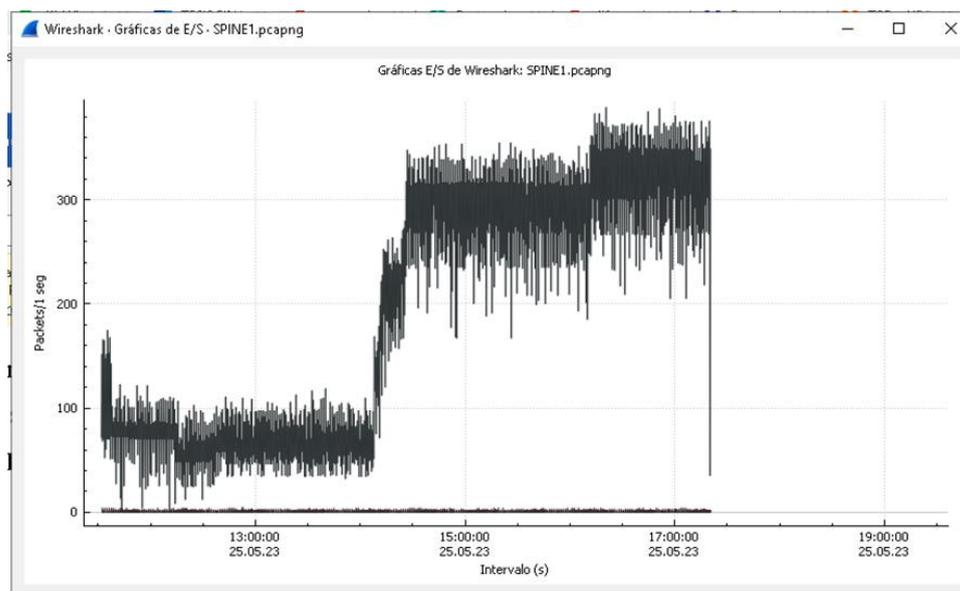


Gráfico 42: Gráfica del Spine 1: Capturado del tráfico del Spine 1 y de WireShark, por John y Henry

Para el análisis del funcionamiento de la red se inició estableciendo los servicios de telefonía en cada una de las VLAN que se configuró en los switches; también se levantó el servidor del juego de video para tener el tráfico inter-VLAN. Como el objetivo de este modelo de arquitectura de red es brindar una conexión al centro de datos al rack de virtualización, desde las máquinas configuradas externamente a las VLAN existentes se realizó una transmisión de video en vivo durante todo el proceso de captura de tráfico, esto con ayuda del software de escritorio remoto Tight VNC.

Como la red permaneció sin ninguna pérdida durante este proceso, para ver el rendimiento de la red, se procedió a realizar actividades como incrementar el número de máquinas conectadas a los servicios de telefonía y videojuegos. En este punto de la experimentación con la red se realizó el levantamiento de una videollamada sin retirar ni el servicio de videojuego y tampoco la transmisión de video desde la máquina del switch de servidores hacia las máquinas externas, de este manera se logró gestionar un mayor número de paquetes por segundo y se pudo comprobar que la red pertenece estable y no se tiene pérdidas de paquetes, aún con una alta solicitud de transferencia de datos.

4.4 Spine 2

Por el Spine 2 también atraviesa todo el tráfico de la red, ya que es justamente este switch el que realiza la comunicación entre los servidores del centro de datos y las solicitudes de los usuarios. Los datos generales son:

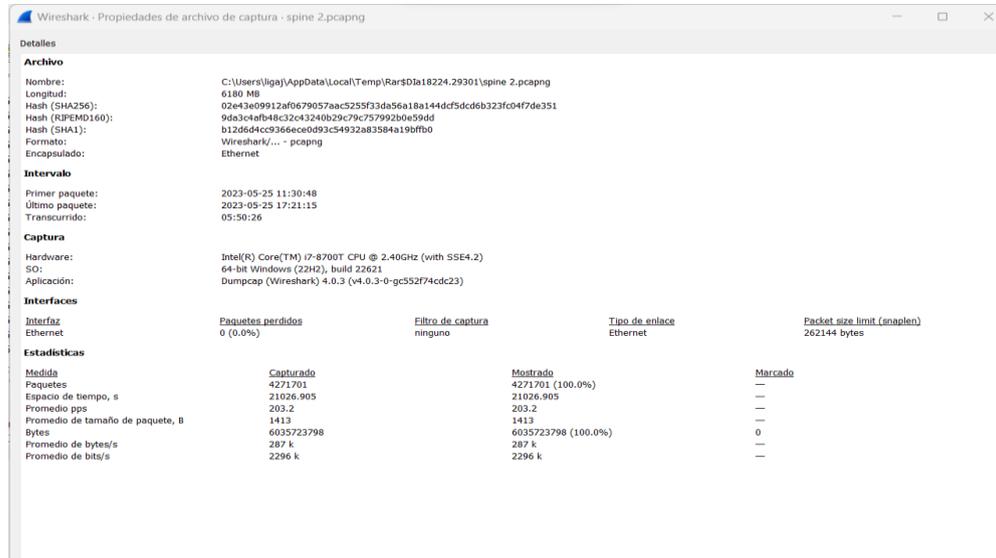


Gráfico 43: Información transmitida del Spine 2: Capturado del tráfico del Spine 2 por John y Henry

En el gráfico cuarenta y tres (43) se puede observar el tiempo de transmisión y una cantidad de 4271701 de paquetes enviados durante las 5 horas 50 minutos 26 segundos, cada paquete transmitido tiene un tamaño promedio de 1413 byte. Se verifica el promedio de bytes que circulan 287Kbytes/s, también se tiene un promedio de bit de un total de 2296kbits/s

4.5 PROTOCOLO DE MAYOR USO

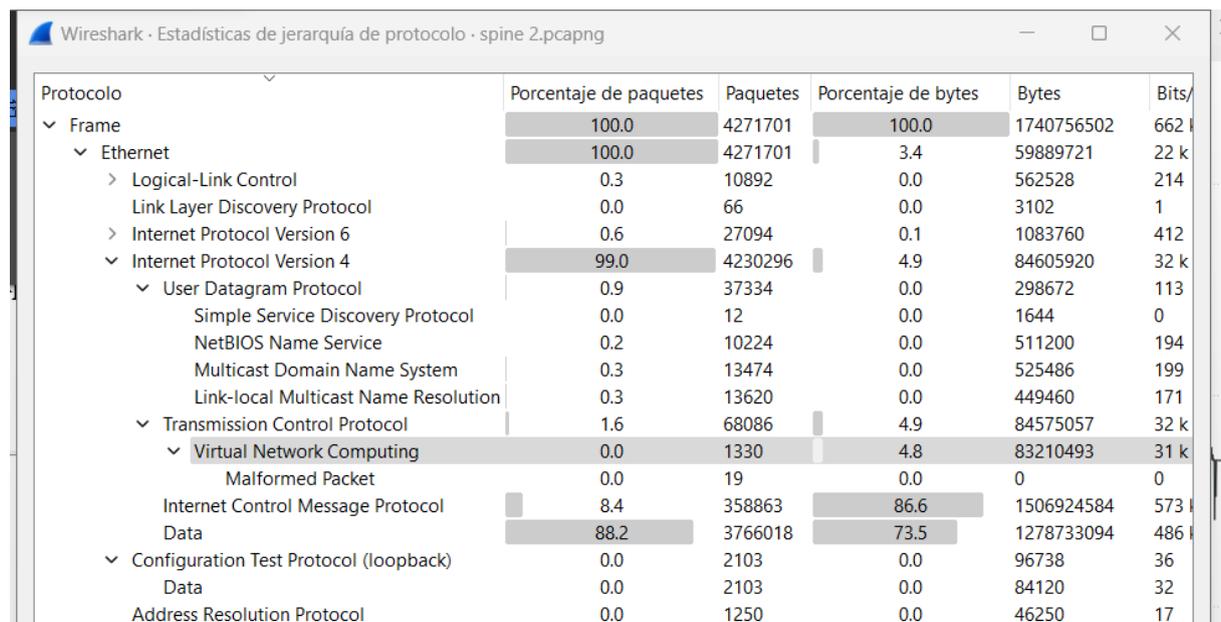


Gráfico 44: Captura de pantalla de Wireshark con los datos por protocolo de la red del Spine 1. Recuperado del software Wireshark por John y Henry

Todo el monitoreo se realizó con el puerto ethernet por ese motivo el 100 % de protocolos están dentro de la trama ethernet. Dentro de ethernet el protocolo de mayor uso es protocolo de internet versión 4; como se observa en el gráfico cuarenta y cuatro (44) Dentro del protocolo IPV4, el protocolo con mayor uso es TCP (Transmission Control Protocol) dentro de ellos se tiene a la transmisión de datos (DATA) con 88.2% enviando un total de paquetes de 3.766.018 además se tiene el protocolo ICMP (Internet Control Message Protocol) que tiene un porcentaje de 8.4% con un total de paquetes de 358.862 , seguido por el protocolo UDP (User Datagram Protocol); es decir el consumo de recursos se da en la capa de transporte del modelo de red con un 0.9%.

En el protocolo UDP también cuenta con el protocolo SSDP (Simple Service Discovery Protocol), el cual es un protocolo que permite la interconexión entre dispositivos finales, este protocolo representa el 0,0% de paquetes transitados a través de la red. es el NET BIOS Name Service, este protocolo permite el acceso a los servicios que ofrece la red; se encuentran asociados 10224 paquetes lo que representan el 0.2 % de paquetes. Se encuentran protocolos como los mensajes de Multicast domain Name System [26], los cuales representan 13474 paquetes de los 4.271.701, lo que representa el 0.3% del total de paquetes enviados. UDP también cuenta con el protocolo Link-local Multicast Name Resolution [27], el cual es un protocolo que todos los host de ipv4 como ipv6 hagan la resolución de nombres para host dentro del mismo enlace local, este protocolo representa el 0,3% de paquetes transitados a través de la red.

4.6 TRANSMISIÓN DE PAQUETES POR TIEMPO

Se obtiene la siguiente información de los paquetes enviados durante el tiempo de simulación de tráfico de la red; los datos obtenidos son los siguientes:

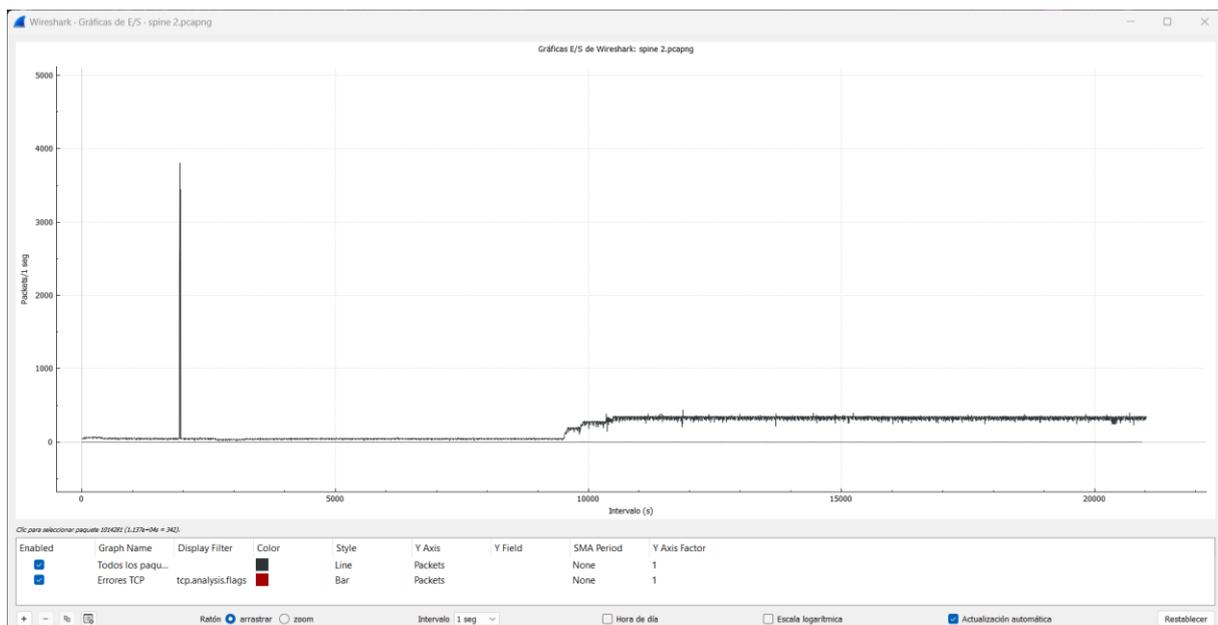


Gráfico 45: Gráfica del Spine 2: Capturado del tráfico del Spine 2 y de WireShark, por John y Henry

Para analizar el desempeño de la red, primero se establecieron los servicios de telefonía en la VLAN configurada en cada switch; también se creó un servidor de videojuegos para manejar el tráfico entre vlan. Dado que el modelo de arquitectura de red tenía como objetivo proporcionar un centro de datos a una conexión de rack virtualizado, desde equipos configurados de forma remota hasta VLAN existentes, la transmisión de un película de video en vivo mediante el software de escritorio remoto Tight VNC se realizó durante la captura de tráfico.

Dado que nada se perdió en la red al momento de realizar todos los procesos anteriores, se realizaron acciones como incrementar la cantidad de dispositivos conectados a los servicios de telefonía y videojuegos para probar el rendimiento de la red. En este punto de la transmisión de paquetes hacia la red, se realiza una videollamada sin dejar de lado el servicio de videojuegos o la transferencia de video desde la máquina de conmutación del servidor a la máquina remota.

De esta forma, puede administrar varios paquetes a la vez y puede comprobar que la red es estable y no hay pérdidas de paquetes incluso cuando hay una alta demanda de transferencia de datos.

En el gráfico cuarenta y seis (46) se observa la transmisión de paquetes durante todo el periodo de tiempo en que se ejecutó y capturó el tráfico el Wireshark, donde se puede observar que a las 12:02 de la tarde del martes 25 de mayo se tuvo un primer pico de transferencia de paquetes con un promedio de 3808 paquetes por segundo siendo este el pico más alto de transferencia en el periodo en el que se capturó el tráfico.

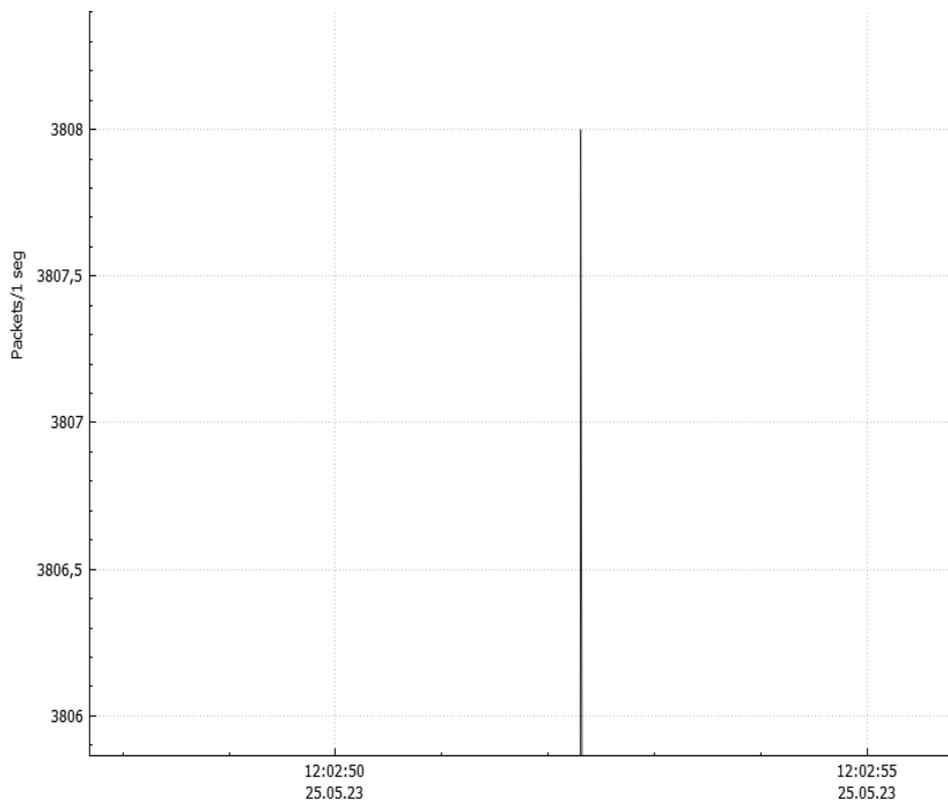


Gráfico 46: Zoom del pico de la gráfica del Spine 2: Capturado del tráfico del Spine 2 y de WireShark, por John y Henry

4.7. PARÁMETROS DE RENDIMIENTO CON LA NUEVA ARQUITECTURA.

Para realizar esta medición, se utilizó el software IPERF-3, el cual es justamente desarrollado para realizar mediciones de velocidad de transferencia en redes de área local. Una gran ventaja que presenta IPERF-3 es que en la prueba realizada entre los puntos brinda velocidades y descarga, además el ancho de banda con el que se está trabajando y finalmente la pérdida de paquetes que se registra durante la medición. IPERF-3 es la herramienta más utilizada para obtener el rendimiento de una red; para realizar las mediciones esta herramienta toma los flujos de datos tanto en TCP, que mide la carga útil, como en UDP, que sirve para proporcionar información sobre la pérdida de paquetes.

El procedimiento para realizar la medición de la red es sencillo, se instala el software en las máquinas que intervengan en la medición; para esto se instaló en las dos máquinas externas y se la estableció como servidores, ya que fueron los puntos hacia donde se requería la medición.

Luego se estableció una máquina interna como cliente, para la medición únicamente se requiere establecer tanto el servidor como el cliente desde la consola del CMD, y se realiza la medición como se muestra a continuación:

```
C:\Windows\system32\cmd.exe
Microsoft Windows [Versión 10.0.19045.2965]
(c) Microsoft Corporation. Todos los derechos reservados.

C:\Users\Alumno>cd C:\Users\Alumno\Documents\iperf\iperf-3.1.3-win64\iperf-3.1.3-win64
C:\Users\Alumno\Documents\iperf\iperf-3.1.3-win64\iperf-3.1.3-win64>iperf3 -c 192.168.25.5
Connecting to host 192.168.25.5, port 5201
[ 4] local 192.168.35.15 port 62005 connected to 192.168.25.5 port 5201
[ ID] Interval      Transfer    Bandwidth
[ 4] 0.00-1.00 sec  105 MBytes  880 Mbits/sec
[ 4] 1.00-2.00 sec  112 MBytes  937 Mbits/sec
[ 4] 2.00-3.00 sec  112 MBytes  938 Mbits/sec
[ 4] 3.00-4.00 sec  112 MBytes  940 Mbits/sec
[ 4] 4.00-5.00 sec  112 MBytes  939 Mbits/sec
[ 4] 5.00-6.00 sec  112 MBytes  939 Mbits/sec
[ 4] 6.00-7.00 sec  112 MBytes  939 Mbits/sec
[ 4] 7.00-8.00 sec  112 MBytes  939 Mbits/sec
[ 4] 8.00-9.00 sec  112 MBytes  940 Mbits/sec
[ 4] 9.00-10.00 sec 112 MBytes  939 Mbits/sec
-----
[ ID] Interval      Transfer    Bandwidth
[ 4] 0.00-10.00 sec 1.09 GBytes  933 Mbits/sec      sender
[ 4] 0.00-10.00 sec 1.09 GBytes  933 Mbits/sec      receiver

iperf Done.
C:\Users\Alumno\Documents\iperf\iperf-3.1.3-win64\iperf-3.1.3-win64>
```

```
C:\Windows\system32\cmd.exe
Microsoft Windows [Versión 10.0.19045.2965]
(c) Microsoft Corporation. Todos los derechos reservados.

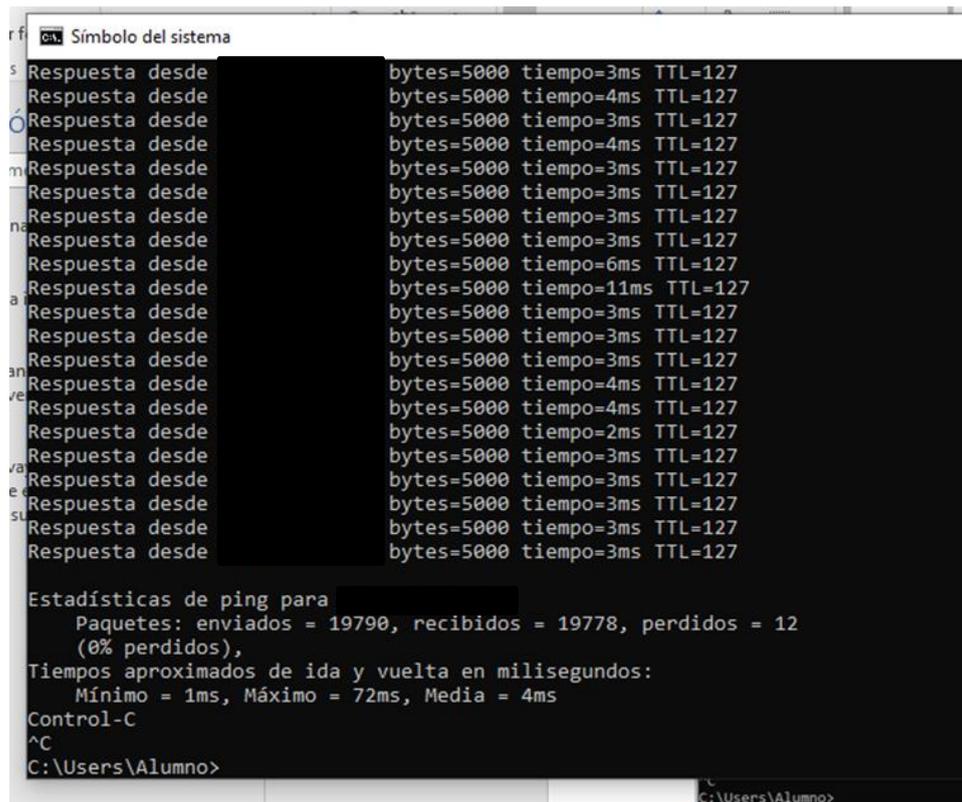
C:\Users\Alumno>cd C:\Users\Alumno\Documents\iperf\iperf-3.1.3-win64\iperf-3.1.3-win64
C:\Users\Alumno\Documents\iperf\iperf-3.1.3-win64\iperf-3.1.3-win64>iperf3 -c 172.178.6.253
Connecting to host 172.178.6.253, port 5201
[ 4] local 192.168.35.15 port 56155 connected to 172.178.6.253 port 5201
[ ID] Interval      Transfer    Bandwidth
[ 4] 0.00-1.00 sec  112 MBytes  935 Mbits/sec
[ 4] 1.00-2.00 sec  111 MBytes  934 Mbits/sec
[ 4] 2.00-3.00 sec  112 MBytes  937 Mbits/sec
[ 4] 3.00-4.00 sec  112 MBytes  936 Mbits/sec
[ 4] 4.00-5.00 sec  105 MBytes  878 Mbits/sec
[ 4] 5.00-6.00 sec  111 MBytes  933 Mbits/sec
[ 4] 6.00-7.00 sec  111 MBytes  929 Mbits/sec
[ 4] 7.00-8.00 sec  111 MBytes  921 Mbits/sec
[ 4] 8.00-9.00 sec  112 MBytes  935 Mbits/sec
[ 4] 9.00-10.00 sec 104 MBytes  874 Mbits/sec
-----
[ ID] Interval      Transfer    Bandwidth
[ 4] 0.00-10.00 sec 1.07 GBytes  922 Mbits/sec      sender
[ 4] 0.00-10.00 sec 1.07 GBytes  922 Mbits/sec      receiver

iperf Done.
C:\Users\Alumno\Documents\iperf\iperf-3.1.3-win64\iperf-3.1.3-win64>
```

Gráfico 47: Ancho de banda de la red de los dos Spine con la herramienta IPERF-3: Capturado por John y Henry

El ancho de banda de una red se lo define como la máxima capacidad de transferencia de datos en una unidad de tiempo; con la herramienta IPERF-3 en las gráficas cuarenta y siete (47) se logró determinar que el ancho de banda de la red es de 922 Mbits/s, es decir la red será saturada cuando se realicen transmisiones con una tasa de transferencia de (922) bits en 1 segundo.

La latencia de una red es por definición el tiempo que tarda un ping en obtener respuesta de un servidor, es decir si se tiene un tiempo de ping alto, la red no será estable; por lo tanto, es necesario que la red obtenga un tiempo de ping bastante bajo, recomendado en el rango de los 40 y 60 ms [28], [29]. Para el caso de la red diseñada se obtuvieron los siguientes resultados:



```
 Símbolo del sistema
Respuesta desde bytes=5000 tiempo=3ms TTL=127
Respuesta desde bytes=5000 tiempo=4ms TTL=127
Respuesta desde bytes=5000 tiempo=3ms TTL=127
Respuesta desde bytes=5000 tiempo=4ms TTL=127
Respuesta desde bytes=5000 tiempo=3ms TTL=127
Respuesta desde bytes=5000 tiempo=6ms TTL=127
Respuesta desde bytes=5000 tiempo=11ms TTL=127
Respuesta desde bytes=5000 tiempo=3ms TTL=127
Respuesta desde bytes=5000 tiempo=3ms TTL=127
Respuesta desde bytes=5000 tiempo=3ms TTL=127
Respuesta desde bytes=5000 tiempo=4ms TTL=127
Respuesta desde bytes=5000 tiempo=4ms TTL=127
Respuesta desde bytes=5000 tiempo=2ms TTL=127
Respuesta desde bytes=5000 tiempo=3ms TTL=127

Estadísticas de ping para
Paquetes: enviados = 19790, recibidos = 19778, perdidos = 12
(0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
Mínimo = 1ms, Máximo = 72ms, Media = 4ms
Control-C
^C
C:\Users\Alumno>
```

Gráfico 48: Captura del ping cargado desde la máquina de servidores hacia la red externa: Capturada por John y Henry

Como se observa en la gráfica cuarenta y ocho (48), el tiempo de respuesta ping obtenida desde la máquina de servidores hacia la máquina externa de red fue de: mínimo 1 ms y máximo 72 ms (milisegundos), esta captura de respuesta fue tomada cuando al final del tiempo de captura, es decir cuando se tuvo una gran cantidad de tráfico generado en la red.

CAPÍTULO 5

5.1. CONCLUSIONES

- Con la implementación de la arquitectura de red Spine and Leaf, el centro de datos de la Universidad Politécnica Salesiana, del campus sur, del bloque D, obtiene un mayor crecimiento en cuanto se refiere a la prestación de servicios a los usuarios que lo requieran de las distintas sedes de la UPS; ya que con esta nueva arquitectura de red, el centro de datos puede ofrecer un sistema de conexión a las máquinas virtuales más seguro con una futura implementación de un servicio de una red privada virtual (VPN), ya que con las nuevas condiciones de la red esto ya sería posible.
- La red propuesta elimina el problema principal de la red actual, es decir los cuellos de botella en la red, debido a que el tráfico que ingresa y sale por la red ya no depende de un solo switch como se encuentra actualmente sino, que se gestiona con dos switches en la capa de spine. Si bien esto no afectó a brindar los servicios de virtualización de máquinas, si es un problema grave en el crecimiento del centro de datos, por tal motivo se requería una arquitectura que ayude a tener una óptima utilización de los recursos con los que se cuenta en la UPS; por este motivo la arquitectura Spine and Leaf si brinda la característica de crecimiento y como se mostró en el presente documento, el crecimiento de la red esta dado únicamente con la adición de switches en las capas de Spine y Leaf.
- Con el prototipo de la arquitectura Spine and Leaf, se evidencia una mejora en el rendimiento de la red superior al 50%, ya que, con la red actual en la captura de tráfico en 27 horas de captura, la red gestionó alrededor de 8 millones de paquetes; y con la implementación del prototipo de la nueva arquitectura de red en tan solo 5 horas ya se pudo gestionar los mismos 8 millones de paquetes; motivo suficiente como para tener en consideración una futura implementación real en el centro de datos.
- La Universidad Politécnica Salesiana puede dar un salto tecnológico, a nivel de instituciones, sin precedentes en el país; ya que con el diseño propuesto en el presente proyecto la UPS puede llegar a brindar ya no solo servicios de virtualización, sino que, con una inversión económica adicional, se pueden llegar a implementar servicios de tecnología 4.0, como por ejemplo los servicios de inteligencia artificial o servicios de almacenamiento en nube.

5.2. RECOMENDACIONES

- En un determinado caso que se decida realizar la implementación de la red con la arquitectura propuesta, se recomienda que se realice con los dispositivos CISCO NEXUS de la serie 7000 en adelante, ya que son dispositivos con mejores características que el switch cisco 3650, por lo tanto, el rendimiento de la red será aún mejor puesto que estos dispositivos son diseñados justamente para este tipo de infraestructura, así se pueden implementar nuevos servicios y optimizar la utilidad del centro de datos.
- Puesto que de momento el centro de datos es tipo TIER II no certificado, debido al problema con el sistema de aire acondicionado, se recomienda que cuando se implemente la nueva arquitectura de red, se realice la inversión necesaria para implementar el ventilador faltante y de este modo tener la certificación TIER II.
- Para un mejor aprovechamiento de los recursos, se recomienda realizar la conexión de la red con el bloque C (Laboratorio de Sistemas Embebidos) mediante fibra óptica, para esto se requiera realizar la inversión económica necesaria para colocar los transceiver SFP; al realizar las conexiones con fibra óptica se tendrá una mejor transferencia de paquetes de datos debido a que la fibra óptica posee una mayor velocidad de transferencia que el cable UTP.
- Se recomienda realizar un estudio de factibilidad de implementación de un servicio de VPN para la accesibilidad a las máquinas virtuales, esto con el fin de tener una conexión más segura para cada uno de los usuarios y para el servidor.

6. BIBLIOGRAFÍA

- [1] “METODOLOGÍA de la investigación.”
- [2] P. Facultad, D. E. Sistemas, Y. Telecomunicaciones, and L. A. Upse, “UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA "EL DESARROLLO DE ESTÁNDARES Y PROCEDIMIENTOS PARA LA CREACIÓN DE UN DATA Previa a la obtención del Título de”.
- [3] “¿Qué es un Data Center y cuál es su importancia?” <https://www.optical.pe/blog/que-es-un-data-center-y-cual-es-su-importancia/> (accessed Mar. 04, 2023).
- [4] “¿Qué es SD-WAN? Funcionamientos y beneficios.” https://www.optical.pe/blog/sd-wan-conoces-las-redes-controladas-por-software/#Que_es_SD-WAN (accessed Mar. 04, 2023).
- [5] “Arquitectura Leaf Spine vs Arquitectura Tradicional | Blogs La Salle | Campus Barcelona.” <https://blogs.salleurl.edu/es/arquitectura-leaf-spine-vs-arquitectura-tradicional> (accessed Mar. 04, 2023).
- [6] “¿Qué es un centro de datos? | Glosario de VMware | LATAM.” <https://www.vmware.com/latam/topics/glossary/content/data-center.html> (accessed Mar. 05, 2023).
- [7] “Arquitectura del centro de datos, data center - Blog de data center, cloud.” <https://blog.hostdime.com.co/arquitectura-del-centro-de-datos-data-center/> (accessed Mar. 05, 2023).
- [8] “Todo lo que necesitas saber sobre el data center modular | GESAB.” <https://gesab.com/noticias/data-centers-modulares/> (accessed Mar. 05, 2023).
- [9] “Tema 9-Centros de datos computacion en nube y organizacion fisica”.
- [10] “¿Qué es STP y Para que Sirve STP? - CCNA Desde Cero.” <https://ccnadesdecero.com/curso/stp/> (accessed Mar. 04, 2023).
- [11] “¿Qué es la arquitectura Spine-Leaf y cómo funciona? | Aruba.” <https://www.arubanetworks.com/faq/what-is-spine-leaf-architecture/> (accessed Mar. 04, 2023).
- [12] “Data Center: El Estándar TIA 942 | Grupo COFITEL.” <https://www.c3comunicaciones.es/data-center-el-estandar-tia-942/> (accessed Mar. 04, 2023).
- [13] “¿Qué es la red de área de almacenamiento (SAN)? | Glosario de VMware | ES.” <https://www.vmware.com/es/topics/glossary/content/storage-area-network-san.html> (accessed May 06, 2023).
- [14] “¿Qué es el almacenamiento flash? | NetApp.” <https://www.netapp.com/es/data-storage/what-is-flash-storage/> (accessed May 06, 2023).
- [15] “¿Qué es una red de área de almacenamiento? | NetApp.” <https://www.netapp.com/es/data-storage/what-is-san-storage-area-network/> (accessed May 06, 2023).
- [16] “Qué es el ping y para qué sirve: Conoce cómo funciona el ping en detalle.” <https://www.redeszone.net/tutoriales/internet/que-es-comando-ping/> (accessed Jun. 06, 2023).
- [17] “What is a Ping Flood | ICMP Flood | DDoS Attack Glossary | Imperva.” <https://www.imperva.com/learn/ddos/ping-icmp-flood/> (accessed Jul. 05, 2023).
- [18] “(1) New Messages!” <https://www.imperva.com/learn/ddos/ping-icmp-flood/> (accessed Jun. 06, 2023).
- [19] “Ping flood: los peligros del ataque de denegación de servicio - IONOS.” <https://www.ionos.es/digitalguide/servidores/seguridad/ataque-ping-flood/> (accessed Jun. 06, 2023).
- [20] “Ping flood - Wikipedia, la enciclopedia libre.” https://es.wikipedia.org/wiki/Ping_flood (accessed Jun. 06, 2023).
- [21] “Ping flood,” *IONOS Digitalguide*, Accessed: Jun. 06, 2023. [Online]. Available: <https://www.ionos.mx/digitalguide/servidores/seguridad/ataque-ping-flood/>
- [22] “VMware vSphere - Documentación de IBM.” <https://www.ibm.com/docs/es/license-metric-tool?topic=connections-vmware-vsphere> (accessed May 06, 2023).
- [23] “Agregar una vGPU NVIDIA GRID a una máquina virtual.” https://docs.vmware.com/es/VMware-vSphere/6.7/com.vmware.vsphere.vm_admin.doc/GUID-

- C597DC2A-FE28-4243-8F40-9F8061C7A663.html (accessed Jun. 20, 2023).
- [24] “8.1.1.3 Formato de los mensajes de syslog.”
<https://www.sapalomera.cat/moodlecf/RS/4/course/module8/8.1.1.3/8.1.1.3.html> (accessed May 06, 2023).
 - [25] “BigAnt Office Messenger, Office Messaging For Business.” <https://www.bigantsoft.com/> (accessed Jun. 08, 2023).
 - [26] “mDNS: ¿Cómo funciona el DNS de multidifusión? -IONOS.”
<https://www.ionos.com/digitalguide/server/know-how/multicast-dns/> (accessed Jun. 19, 2023).
 - [27] “IPv6 - Principios e implementación - El protocolo de resolución local LLMNR (Link Local Multicast Name Resolution) | Ediciones ENI.” <https://www.ediciones-eni.com/open/mediabook.aspx?idR=16235b5c43d41e08b8842836d739ba71> (accessed Jun. 19, 2023).
 - [28] “¿Qué es la latencia? - Explicación de la latencia de red - AWS.”
<https://aws.amazon.com/es/what-is/latency/> (accessed Jul. 06, 2023).
 - [29] “¿Cómo medir la latencia?” <https://www.kio.tech/blog/data-center/c%C3%B3mo-medir-la-latencia> (accessed Jul. 06, 2023).
 - [30] “Aprende Redes.com » Vlan Trunking Protocol (VTP).”
<https://aprenderedes.com/2019/12/vlan-trunking-protocol-vtp/> (accessed Jun. 11, 2023).
 - [31] “VTP, VLAN Trunking Protocol - Eduardo Collado.”
<https://www.eduardocollado.com/2018/04/02/pocast-142-vtp-vlan-trunking-protocol/> (accessed Jun. 11, 2023).
 - [32] “Cómo Comprender VLAN Trunk Protocol (VTP) Contenido”.
 - [33] “Cómo Comprender VLAN Trunk Protocol (VTP) Contenido”.

CAPÍTULO 7

ANEXOS

7.1. ANEXO #1: VLAN TRUNK PROTOCOL

La configuración de las distintas Vlan de una red en términos generales es sencilla, sin embargo, ya en una red grande resulta en un proceso bastante demorado el configurar cada una de las VLAN en cada switch de la red. Para realizar esa configuración de una manera más eficiente y rápido, CISCO desarrollo un protocolo que permite que todos los switches de una red aprendan de forma automática todas las VLAN que se requieran implementar en la red que se esté trabajando.

VTP es un protocolo a nivel de capa 2 que permite establecer una la configuración de VLAN a través de la red conmutada; el administrador de la red está en la capacidad de configurar los switches para que trabajen en una de las 3 versiones que se presenta este protocolo; el aspecto más importante de este protocolo es que los puertos de conexión entre cada uno de los switches debe estar en modo troncal, ya que de esta forma se podrá establecer una comunicación entre el switch servidor y los switches cliente [30], [31].

7.1.1 Modo servidor.

Para establecer un switch de la red como servidor VTP, lo primero que se debe realizar es establecer un dominio VTP en el switch con el comando “*vtp domain xxxx*”, con este dominio el resto de switches reconocerán el nombre con el cual se accederá a las VLAN que se gestionen en la red. En segundo lugar, se establece al switch como servidor VTP con el comando “*vtp mode server*”, de esta forma este switch será el encargado de informará al resto de switches todas las VLAN que se configuren para la red.

Para la configuración de las VLAN se debe realizar en el switch que se estableció como modo servidor, pues en el resto de switches con un “*show vlan brief*”, se podrá observar todas las Vlan aprendidas con ayuda del protocolo VTP [32]

7.1.2 Modo cliente.

Ya establecido un switch como modo servidor, lo que se debe realizar es al resto de switches establecerlos como modo servidor; para esto se ingresa el dominio VTP que se estableció en el switch servidor con el comando “*vtp domain xxxx*”, de este modo el switch sabe que bajo ese único dominio se gestionaran las VLAN, y en segundo lugar establecerlo en modo cliente con el comando “*vtp mode client*”.

Ya con esta configuración se puede realizar una inspección de la VLAN aprendidas con

el comando “*show vtp status*”, donde se muestran el estado del protocolo, así como las VLAN que se están compartiendo gracias al protocolo VTP [33].

Como se puede notar la configuración del protocolo VTP es bastante sencillo y se obtiene un gran ahorro de tiempo al realizar la configuración de todas las VLAN requeridas en la red conmutada.

7.2 ANEXO #2: DATASHEET DEL SWITCH CISCO NEXUS

7.3 ANEXO #3: DATASHEET DEL SWITCH CISCO 3650