

Universidad Nacional del Altiplano

FACULTAD DE INGENIERÍA MECÁNICA ELÉCTRICA,
ELECTRÓNICA Y SISTEMAS

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS



TESIS

“MODELO DE IMPLEMENTACIÓN DE REDES VIRTUALES VLAN Y
PRIORIZACIÓN DEL ANCHO DE BANDA PARA LA RED DE ÁREA LOCAL
DEL PROYECTO ESPECIAL LAGO TITICACA – SEDE CENTRAL PUNO -
2016”

PRESENTADO POR:
JORGE LUIS FARAH MIRAVAL

PARA OPTAR EL TÍTULO PROFESIONAL DE: INGENIERO DE SISTEMAS

Puno – Perú

2016

Universidad Nacional del Altiplano

FACULTAD DE INGENIERÍA MECÁNICA ELÉCTRICA, ELECTRÓNICA Y SISTEMAS

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

"MODELO DE IMPLEMENTACIÓN DE REDES VIRTUALES VLAN Y PRIORIZACIÓN DEL ANCHO DE BANDA PARA LA RED DE ÁREA LOCAL DEL PROYECTO ESPECIAL LAGO TITICACA – SEDE CENTRAL PUNO - 2016"

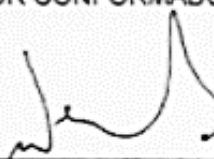
**TESIS PRESENTADA POR:
JORGE LUIS FARAH MIRAVAL**

PARA OPTAR EL TÍTULO PROFESIONAL DE: INGENIERO DE SISTEMAS

APROBADA POR EL JURADO REVISOR CONFORMADO POR:

PRESIDENTE

:



M.Sc. WILLIAM EUSEBIO ARCAYA COAQUIRA

PRIMER MIEMBRO

:


M.Sc. EDGAR HOLGUIN HOLGUIN

SEGUNDO MIEMBRO

:


Ing. ADOLFO CARLOS JIMENEZ CHURA

DIRECTOR DE TESIS

:


M.Sc. CARLOS BORIS SOSA MAYDANA

Puno – Perú

2016

Área: Informática

Tema: Comunicación de datos

AGRADECIMIENTOS

A mi familia, por el constante apoyo y motivación para culminar el trabajo de investigación.

Al director de tesis: M.Sc. Ing. Carlos Boris Sosa Maydana, y a los jurados M.Sc. William Eusebio Arcaya Coaquira, M.Sc. Edgar Holguin Holguin e Ing. Adolfo Carlos Jiménez Chura, por su valiosa orientación para la elaboración de la investigación.

Al personal administrativo del Proyecto Especial Lago Titicaca – sede central Puno, por la disposición y facilidades para la obtención de información.

A Evelyne Luz Atayupanqui Sayritupa por el apoyo, ánimo y consejos durante todo el proceso de investigación.

DEDICATORIA

A mis queridos padres Juana y Alberto, por el esfuerzo, sacrificio y dedicación puestos en mi educación, por el ejemplo, cariño y constante aliento para salir siempre adelante.

INDICE

ÍNDICE DE FIGURAS	7
ÍNDICE DE TABLAS	9
RESUMEN	11
ABSTRACT	12
INTRODUCCIÓN	13
CAPÍTULO I	15
PLANTEAMIENTO DEL PROBLEMA DE INVESTIGACIÓN	15
1.1. Descripción del problema	16
1.2. Justificación del problema	16
1.3. Objetivos de la investigación	17
CAPÍTULO II	18
MARCO TEÓRICO	18
2.1. Antecedentes de investigación	19
2.2. Sustento teórico	20
2.3. Glosario de términos básicos	44
2.4. Hipótesis de la investigación	47
2.5. Operacionalización de variables	47
CAPÍTULO III	49
DISEÑO METODOLÓGICO DE LA INVESTIGACIÓN	49
3.1. Tipo y Diseño de investigación	50
3.1.1. Tipo de investigación	50
3.1.2. Diseño de investigación	50
3.2. Población y muestra de investigación	50
3.3. Ubicación y descripción de la población	51

3.4.	Técnicas e instrumentos para recolectar información	51
3.5.	Técnicas para el procesamiento y análisis de datos	51
3.6.	Plan de tratamiento de los datos	51
CAPÍTULO IV		53
ANÁLISIS E INTERPRETACIÓN DE RESULTADOS DE LA INVESTIGACIÓN		53
4.1.	Análisis del rendimiento de la red actual	54
4.1.1.	Análisis de metas y restricciones	54
4.1.1.1.	Análisis de metas técnicas y compensaciones	58
4.1.1.1.1.	Escalabilidad	58
4.1.1.1.2.	Disponibilidad	61
4.1.1.1.3.	Utilización óptima	66
4.1.1.1.4.	Latencia	70
4.1.1.1.5.	Seguridad	71
4.1.1.2.	Identificar la red existente	75
4.1.1.2.1.	Infraestructura de red	75
4.1.1.2.2.	Direccionamiento	80
4.1.1.2.3.	Salud de la red	81
4.1.1.2.4.	Disponibilidad	85
4.2.	Diseño del modelo	89
4.2.1.	Diseño lógico propuesto	89
4.2.1.1.	Topología de red	89
4.2.1.2.	Direccionamiento	93
4.2.1.3.	Estructura del modelo	94
4.2.1.4.	VLAN	97

4.2.1.5.	Direccionamiento	98
4.2.1.6.	Seguridad	100
4.2.1.7.	Calidad de Servicio QoS	101
4.2.2.	Diseño Físico	101
4.2.2.2.	Cableado LAN	101
4.2.2.3.	Dispositivos	102
4.2.2.4.	Configuración de equipos	103
4.3.	Simular y evaluar el modelo	103
CONCLUSIONES		108
SUGERENCIAS		110
BIBLIOGRAFÍA		111
ANEXOS		113
ANEXO 1: REPORTE DE PROGRAMA PING		114
ANEXO 2: CONFIGURACIÓN DE SWITCHES Y ROUTER		117
ANEXO 3: PANEL FOTOGRÁFICO		141

ÍNDICE DE FIGURAS

Figura 1: Capas del modelo OSI	24
Figura 2: Iconos de los dispositivos de red	32
Figura 3: Orden de transmisión de mensajes DHCP	34
Figura 4: Modelo jerárquico de Cisco	38
Figura 5: Topología de red virtual VLAN	43
Figura 6: Organigrama del PELT	55
Figura 7: Disponibilidad	62
Figura 8: Sobreutilización de enlaces	64
Figura 9: Utilización del ancho de banda	67
Figura 10: Frecuencias del promedio del ancho de banda	68
Figura 11: Estadística de jerarquía de protocolos	69
Figura 12: Frecuencias del promedio de uso del Protocolo ARP	69
Figura 13: Frecuencias del promedio de latencia máxima	71
Figura 14: Topología LAN actual – Routers y Switches	78
Figura 15: Topología LAN actual Switches y PCs	79
Figura 16: Ancho de banda Switch primer piso – Edificio A	81
Figura 17: Ancho de banda Switch segundo piso – Edificio A	82
Figura 18: Ancho de banda Switch tercer piso – Edificio A	82
Figura 19: Ancho de banda Switch cuarto piso – Edificio A	83

Figura 20: Ancho de banda Switch quinto piso – Edificio A	83
Figura 21: Ancho de banda Switch primer piso – Edificio B	84
Figura 22: Ancho de banda Switch segundo piso – Edificio B	84
Figura 23: Ancho de banda Switch tercer piso – Edificio B	85
Figura 24: Topología de modelo – Switches y Router	91
Figura 25: Topología de modelo – Switches y usuarios	92
Figura 26: Frecuencias del promedio de latencia máxima – Modelo	105
Figura 27: Prueba T – Promedios de latencia máxima	106

ÍNDICE DE TABLAS

Tabla 1: Operacionalización de variables	48
Tabla 2: Comparación de indicadores	52
Tabla 3: Aplicaciones	57
Tabla 4: Histórico y proyección de usuarios	59
Tabla 5: Interfaces o puertos de red disponibles	60
Tabla 6: Direcciones IP – Red actual	60
Tabla 7: Disponibilidad de red	61
Tabla 8: Disponibilidad de aplicaciones	63
Tabla 9: Costo por estar fuera de servicio	64
Tabla 10: Ancho de banda contratado	66
Tabla 11: Activos de red – Hardware	72
Tabla 12: Activos de red - Software	73
Tabla 13: Activos de red – Data	73
Tabla 14: Activos de red – Amenazas de seguridad	73
Tabla 15: Requerimientos de seguridad	74
Tabla 16: Comunidad de usuarios y switches – Edificio A	76
Tabla 17: Comunidad de usuarios y switches – Edificio B	77
Tabla 18: Comunidad de usuarios y switches – Área libre	77
Tabla 19: Direccionamiento de red	86

Tabla 20: Dispositivos de red operativos	87
Tabla 21: Número de usuarios por comunidad	88
Tabla 22: Direccionamiento IP – Modelo	94
Tabla 23: Comunidad de usuarios	95
Tabla 24: Comunidad de usuarios – VLANs – Dirección IP	97
Tabla 25: Equipos de red - Modelo	103
Tabla 26: Comparación de red actual y modelo	107

RESUMEN

La presente investigación titulada “MODELO DE IMPLEMENTACIÓN DE REDES VIRTUALES VLAN Y PRIORIZACIÓN DE ANCHO DE BANDA PARA LA RED DE ÁREA LOCAL DEL PROYECTO ESPECIAL LAGO TITICACA – SEDE CENTRAL PUNO -2016” tuvo por objetivo general diseñar un modelo para para mejorar el rendimiento de la red de área local del Proyecto Especial Lago Titicaca – sede central Puno -2016. Esto debido a que la red actual es plana en su diseño, no existen subredes o redes virtuales VLAN, su expansión resulta difícil de planificar e implementar, no cuenta con enlace redundantes para garantizar la disponibilidad de rutas, tampoco existen configuraciones de calidad de servicio, el throughput de los equipos de red en algunos casos reduce el ancho de banda hasta el 10%. Es así que se determinó rediseñar la red utilizando la metodología “Top-Down Network Design” de Cisco Press y Priscilla Oppenheimer, mediante la cual se identificó los requerimientos actuales y futuros. Finalmente se comprobó las mejoras asociadas al uso del modelo.

Palabras clave: Rendimiento de red, escalabilidad, disponibilidad, seguridad

ABSTRACT

The present research entitled "MODEL OF IMPLEMENTATION OF VLAN NETWORKS AND BANDWIDTH PRIORIZATION FOR THE LOCAL AREA NETWORK OF THE LATIC TITICACA SPECIAL PROJECT - PUNO CENTRAL HEADQUARTER -2016" had the general objective of designing a model to improve the performance of the Local area network of the Lake Titicaca Special Project - Puno headquarters -2016. This is because the current network is flat in its design, there are no subnets or virtual networks VLAN, its expansion is difficult to plan and implement, no redundant link to ensure the availability of routes, there are no configurations of quality of service, The throughput of the network equipment in some cases reduces the bandwidth up to 10%. It was thus determined to redesign the network using the "Top-Down Network Design" methodology ofiscopress and Priscilla Oppenheimer, which identified the current and future requirements. Finally, the improvements associated with the use of the model were verified.

Keywords: Red performance, scalability, availability, security

INTRODUCCIÓN

La utilización de las tecnologías de información y comunicación (en adelante TIC) por parte de la administración pública está aumentando notablemente, ya que es innegable el impulso que da al incremento de la eficiencia en la prestación de servicios públicos, mejora la participación de las personas en el acceso a la información pública y en las decisiones de gobierno, fortalece el proceso de descentralización e insta una administración moderna orientada a la prestación de servicios en línea, para que esto se logre, las TIC deben estar correctamente implementadas y configuradas, de otra manera generarían nuevos problemas, como pérdidas de información en la red, lentitud en el acceso a páginas web del estado, inaccesibilidad a las cuentas de correo electrónico, sistemas de información, impresoras, recursos compartidos, y otros.

Particularmente sobre las tecnologías de comunicación, es indispensable que la arquitectura de red de área local (LAN) de las entidades públicas, cumplan con las características básicas de toda red: tolerancia a fallas, escalabilidad, calidad de servicio y seguridad, las cuales garantizan el flujo dinámico de información y de esta manera la correcta utilización de toda la plataforma de las TIC.

El Proyecto Especial Binacional Lago Titicaca es un órgano desconcentrado de ejecución, dependiente del Ministerio de Agricultura, cuya sede central se encuentra ubicada actualmente en el Jirón Deustua N° 822 de la ciudad de Puno, posee una red de área local plana en su diseño, con ausencia de

estándares de calidad en gestión de tráfico de red, políticas de seguridad inexistentes y desaprovechamiento de la performance de los equipos y medios de comunicación, ocasionando latencia en horas pico, degradando la transferencia de información y perjudicando las labores de las áreas dependientes del uso de internet. La presente investigación diseñó un modelo de implementación de redes virtuales VLAN y priorización del ancho de banda que mejorar el rendimiento de la red.

Esta tesis se encuentra constituida por cuatro capítulos:

CAPÍTULO I: Contiene la descripción, justificación del problema, y los objetivos de la investigación.

CAPÍTULO II: Presenta los antecedentes de la investigación, sustento teórico, glosario de términos, hipótesis de la investigación y la operacionalización de variables.

CAPÍTULO III: Detalla el tipo, diseño y muestra de la investigación, también la ubicación y descripción de la población, técnicas e instrumentos para recolectar información, y para el procesamiento y análisis de datos, asimismo el plan y tratamiento de los datos.

CAPÍTULO IV: Desarrolla el análisis e interpretación de resultados de la investigación.

CAPÍTULO V: Finalmente se presentan las conclusiones y sugerencias arribadas de la investigación, además de los anexos que detallan la configuración de los equipos de red.

CAPÍTULO I

PLANTEAMIENTO DEL PROBLEMA DE

INVESTIGACIÓN

1.1. Descripción del problema

Actualmente las redes de datos de las entidades públicas tienen una mayor carga de tráfico debido al uso de sistemas integrados como ERP, base de datos, voz y video, es así que la red del Proyecto Especial Lago Titicaca, en su sede central Puno, presenta varios problemas como latencia, fallas de conexión, ausencia de mecanismos de control del uso del ancho de banda, pérdida de información, y otros. Son más de cuatro años sin lograr una solución que cumpla los requerimientos de los usuarios, y permita el normal desarrollo de sus funciones, de seguir así, continuarán los retrasos y hasta incumplimiento de los objetivos institucionales.

1.2. Justificación del problema

La mayoría o todos los trabajadores que laboran en el Proyecto Especial Lago Titicaca sede central Puno, usan las tecnologías de información y comunicación para realizar sus labores diarias, es de vital importancia que los sistemas de información y específicamente la red que los conecta y comunica con internet funcione correctamente, sin fallas, sin retrasos y garantizando la seguridad de la información que por ella fluye.

Más aun, para lograr la eficiencia en la gestión pública, es necesario que los equipos, medios, y software de comunicaciones estén correctamente configurados respecto a la necesidad de la entidad, para que los funcionarios puedan laborar de la mejor manera, siendo respaldados por una red de datos confiable y rápida.

El presente trabajo se justifica por la importancia de contar con una red que garantice el intercambio de información sin retraso alguno y de forma segura, de tal manera que coadyuve al logro de objetivos institucionales.

1.3. Objetivos de la investigación

1.3.1. Objetivo general

Diseñar un modelo de implementación de redes virtuales VLAN y priorización del ancho de banda para mejorar el rendimiento de la red de área local del Proyecto Especial Lago Titicaca - sede central Puno.

1.3.2. Objetivos específicos

- Analizar el rendimiento de la red de área local del Proyecto Especial Lago Titicaca sede central Puno- 2016.
- Diseñar un modelo de implementación de redes virtuales VLAN y priorización del ancho de banda.
- Simular y evaluar el rendimiento del modelo de implementación de redes virtuales VLAN y priorización del ancho de banda.

CAPÍTULO II

MARCO TEÓRICO

2.1. Antecedentes de investigación

Se consideraron como antecedentes los siguientes trabajos de investigación:

- **Título:** Diseño de red LAN utilizando el protocolo MPLS para la transmisión de voz, dato y video en la EPIS – UNA – Puno 2011.

Autor: Yeny Betzabe Calcina Tuni

Año: 2013

Universidad: Universidad Nacional del Altiplano

Objetivo general: Elaborar un diseño de red LAN utilizando el protocolo MPLS para la transmisión de voz, video y datos de la EPIS – UNA – Puno.

Conclusión principal: Con el nuevo diseño de red LAN se logró transmitir eficientemente voz, datos en MPLS optimizando la calidad de servicio para el usuario de la EPIS – UNA –Puno 2011.

- **Título:** Propuesta de segmentación con redes virtuales y priorización del ancho de banda con QoS para la mejora del rendimiento y seguridad de la red LAN en la empresa editora El Comercio planta norte.

Autor: Julio Edgar Molina Ruiz

Año: 2012

Universidad: Universidad Católica Santo Toribio de Mogrovejo - Chiclayo

Conclusión principal: Se implementó y configuró la red para soportar el promedio de crecimiento de usuarios sin afectar el rendimiento de la red, la tasa de transferencia está operando dentro de los rangos esperados, la configuración del Firewall Cisco solucionó la pérdida de información.

- **Título:** Modelo de implementación jerárquico de la red de datos IP de la Universidad Católica de Santa María utilizando la metodología Top Down y el estándar IEEE 802.3ae, IEEE 802.3an y IEEE 802.3ab.

Autor: Cesar Huanayque Vilca

Año: 2013

Universidad: Universidad Católica de Santa María - Arequipa

Objetivo general: Diseñar e implementar un modelo de implantación jerárquico para la red de datos IP de la UCSM utilizando la metodología Top Down y el estándar IEEE 802.3ae, IEEE 802.3an y IEEE 802.3ab.

Conclusión principal: Se logró implementar la red basada en un modelo jerárquico de acuerdo al diseño propuesto obteniendo los tres niveles de red: Core, distribución y acceso permitiendo que la red sea confiable y segura.

2.2. Sustento teórico

2.2.1. Modelo:

(Definicion.de, 2016) Un modelo es un arquetipo o punto de referencia para imitarlo o reproducirlo que se toma como pauta a seguir, otros usos de la palabra refieren a la representación en pequeño de alguna cosa. Los modelos enfocan ciertas partes importantes de un sistema (por lo menos, aquella que le interesan a un tipo de modelo específico), restándole importancia a otras.

(Seiffe, 2013) Un modelo es un esquema teórico de un sistema o realidad compleja que se elabora para facilitar su comprensión y estudio. Cada una de las modalidades, tipos o categorías que existen de algo. En ingeniería se le llaman modelos a representación gráfica o esquemática de una realidad, sirve para organizar y comunicar de forma clara los elementos que involucran un todo. La ciencia moderna ofrece una colección creciente de métodos, técnicas y teorías acerca de diversos tipos de modelos.

2.2.2. Modelo OSI

(Wikipedia, 2016) El modelo de interconexión de sistemas abiertos (ISO/IEC 7498-1), más conocido como “modelo OSI”, (en inglés, Open System Interconnection) es un modelo de referencia para los protocolos de la red de arquitectura en capas, creado en el año 1980 por la Organización Internacional de Normalización (ISO, International Organization for Standardization). Se ha publicado desde 1983 por la Unión Internacional de Telecomunicaciones (UIT) y, desde 1984, la Organización Internacional de Normalización (ISO) también lo publicó con estándar. Su desarrollo comenzó en 1977.

Fue desarrollado en 1980 por la ISO, una federación global de organizaciones que representa aproximadamente a 130 países. El núcleo de este estándar es el modelo de referencia OSI, una normativa formada por siete capas que define las diferentes fases por las que deben pasar los datos para viajar de un dispositivo a otro sobre una red de comunicaciones.

Siguiendo el esquema de este modelo se crearon numerosos protocolos. El advenimiento de protocolos más flexibles donde las capas no están tan desmarcadas y la correspondencia con los niveles no era tan clara puso a este esquema en un segundo plano. Sin embargo se usa en la enseñanza como una manera de mostrar cómo puede estructurarse una "pila" de protocolos de comunicaciones.

El modelo especifica el protocolo que debe usarse en cada capa, y suele hablarse de modelo de referencia ya que se usa como una gran herramienta para la enseñanza de comunicación de redes.

Se trata de una normativa estandarizada útil debido a la existencia de muchas tecnologías, fabricantes y compañías dentro del mundo de las comunicaciones, y al estar en continua expansión, se tuvo que crear un método para que todos pudieran entenderse de algún modo, incluso cuando las tecnologías no coincidieran. De este modo, no importa la localización geográfica o el lenguaje utilizado. Todo el mundo debe atenerse a unas normas mínimas para poder comunicarse entre sí.

Esto es sobre todo importante cuando hablamos de la red de redes, es decir, Internet.

(Atelin & Dordoigne, 2006) Un aspecto importante en la apertura de las redes fue la instauración de un modelo de referencia, el modelo OSI. Este define un modelo de red en siete capas, presentes en cada estación que desee conectarse. Cada capa dispone de funcionalidades que le son propias y presentan servicios a las capas inmediatamente adyacentes. Aunque el modelo OSI se utiliza muy poco, sirve de referencia para definir el nivel de funcionamiento de un componente de red. Aunque hoy en día y de manera paradójica, el TCP/IP se utiliza de manera generalizada, e incluso cuando se habla de este protocolo se le asocia con las capas de modelo OSI.

2.2.3. Criterios de diseño

(Tolosa, 2014)

- Se creará una nueva capa siempre que se precise un nuevo grado de abstracción.
- Capa tendrá un número bien definido de funciones propias.
- La frontera de las capas será tal que se minimice el flujo de información a través de la interfaz.
- Número de capas: Balance para no reunir en un nivel funcionalidades distinta (+) y que el resultado final sea manejable en la práctica (-).

2.2.4. Ventajas

(Tolosa, 2014)

- Divide la comunicación de red en partes más pequeñas y sencillas.
- Normaliza los componentes de red para permitir el desarrollo y el soporte de los productos de diferentes fabricantes.
- Permite que hardware y software de red diferente se comuniquen entre sí.
- Impide que los cambios en una capa puedan afectar las demás capas.
- Se simplifica el aprendizaje por la división de funciones.

2.2.5. Capas del modelo OSI

(Microsoft, 2013)

El modelo de interconexión de sistemas abiertos (OSI) tiene siete capas. Este artículo las describe y explica sus funciones, empezando por la más baja en la jerarquía (la física) y siguiendo hacia la más alta (la aplicación). Las capas se apilan de esta forma:



Figura 1: Capas del modelo OSI
Fuente: Organización Internacional de Normalización (ISO)
Elaboración: Propia

2.2.5.1. Capa física

La función de la capa física de OSI es la de codificar en señales los dígitos binarios que representan las tramas de la capa de Enlace de datos, además de transmitir y recibir estas señales a través de los medios físicos (alambres de cobre, fibra óptica o medio inalámbrico) que conectan los dispositivos de la red. Proporciona los medios de transporte para los bits que conforman la trama de la capa de Enlace de datos a través de los medios de red. Esta capa acepta una trama completa desde la capa de Enlace de datos y lo codifica como una secuencia de señales que se transmiten en los medios locales. Un dispositivo final o un dispositivo intermedio reciben los bits codificados que componen una trama.

El envío de tramas a través de medios de transmisión requiere los siguientes elementos de la capa física:

- Medios físicos y conectores asociados.
- Una representación de los bits en los medios.
- Codificación de los datos y de la información de control.
- Sistema de circuitos del receptor y transmisor en los dispositivos de red.

2.2.5.2. Capa de enlace de datos

La capa de vínculo de datos ofrece una transferencia sin errores de tramas de datos desde un nodo a otro a través de la capa física, permitiendo a las capas por encima asumir virtualmente la transmisión sin errores a través del vínculo. Para ello, la capa de vínculo de datos proporciona:

- Establecimiento y finalización de vínculos: establece y finaliza el vínculo lógico entre dos nodos.
- Control del tráfico de tramas: indica al nodo de transmisión que "dé marcha atrás" cuando no haya ningún búfer de trama disponible.
- Secuenciación de tramas: transmite y recibe tramas secuencialmente.
- Confirmación de trama: proporciona/espera confirmaciones de trama. Detecta errores y se recupera de ellos cuando se producen en la capa física mediante la retransmisión de tramas no confirmadas y el control de la recepción de tramas duplicadas.
- Delimitación de trama: crea y reconoce los límites de la trama.
- Comprobación de errores de trama: comprueba la integridad de las tramas recibidas.
- Administración de acceso al medio: determina si el nodo "tiene derecho" a utilizar el medio físico.

2.2.5.3. Capa de red

La capa de red o capa 3 de OSI provee servicios para intercambiar secciones de datos individuales a través de la red entre dispositivos finales identificados.

Para realizar este transporte, se utilizan cuatro procesos básicos:

Direccionamiento:

La capa de red debe proveer un mecanismo para direccionar estos dispositivos finales, si las secciones individuales de datos deben dirigirse a un dispositivo final, este debe tener una dirección única.

Encapsulación:

La capa de red debe proveer encapsulación, la capa 3 recibe la PDU de la capa 4 y agrega un encabezado o etiqueta de capa 3 para crear la PDU de capa 3. Cuando crea este paquete el encabezado debe contener entre otra información, la dirección del host destino.

Enrutamiento:

La capa de red debe proveer los servicios para dirigir los paquetes a su destino, cada paquete debe ser guiado a través de la red para que llegue a su destino final.

Desencapsulamiento:

Finalmente, el paquete llega a su destino y es procesado en la capa 3, se examina la dirección de destino para verificar que el paquete fue direccionado correctamente, luego el paquete es desencapsulado por la capa de red y se envía a la capa de transporte.

2.2.5.4. Capa de transporte

La capa de transporte garantiza que los mensajes se entregan sin errores, en secuencia y sin pérdidas o duplicaciones. Libera a los protocolos de capas superiores de cualquier cuestión relacionada con la transferencia de datos entre ellos y sus pares.

El tamaño y la complejidad de un protocolo de transporte dependen del tipo de servicio que pueda obtener de la capa de transporte.

Para tener una capa de transporte confiable con una capacidad de circuito virtual, se requiere una mínima capa de transporte. Si la capa de red no es confiable o solo admite datagramas, el protocolo de transporte debería incluir detección y recuperación de errores extensivos.

La capa de transporte proporciona:

- Segmentación de mensajes: acepta un mensaje de la capa (de sesión) que tiene por encima, lo divide en unidades más pequeñas (si no es aún lo suficientemente pequeño) y transmite las unidades más pequeñas a la capa de red. La capa de transporte en la estación de destino vuelve a ensamblar el mensaje.
- Confirmación de mensaje: proporciona una entrega de mensajes confiable de extremo a extremo con confirmaciones.
- Control del tráfico de mensajes: indica a la estación de transmisión que "dé marcha atrás" cuando no haya ningún búfer de mensaje disponible.
- Multiplexación de sesión: multiplexa varias secuencias de mensajes, o sesiones, en un vínculo lógico y realiza un seguimiento de qué mensajes pertenecen a qué sesiones (consulte la capa de sesiones).

Normalmente, la capa de transporte puede aceptar mensajes relativamente grandes, pero existen estrictas limitaciones de tamaño para los mensajes impuestas por la capa de red (o inferior). Como

consecuencia, la capa de transporte debe dividir los mensajes en unidades más pequeñas, o tramas, anteponiendo un encabezado a cada una de ellas.

Así pues, la información del encabezado de la capa de transporte debe incluir información de control, como marcadores de inicio y fin de mensajes, para permitir a la capa de transporte del otro extremo reconocer los límites del mensaje. Además, si las capas inferiores no mantienen la secuencia, el encabezado de transporte debe contener información de secuencias para permitir a la capa de transporte en el extremo receptor recolocar las piezas en el orden correcto antes de enviar el mensaje recibido a la capa superior.

Capas de un extremo a otro

A diferencia de las capas inferiores de "subred" cuyo protocolo se encuentra entre nodos inmediatamente adyacentes, la capa de transporte y las capas superiores son verdaderas capas de "origen a destino" o de un extremo a otro, y no les atañen los detalles de la instalación de comunicaciones subyacente. El software de capa de transporte (y el software superior) en la estación de origen lleva una conversación con software similar en la estación de destino utilizando encabezados de mensajes y mensajes de control.

2.2.5.5. Capa de sesión

La capa de sesión permite el establecimiento de sesiones entre procesos que se ejecutan en diferentes estaciones. Proporciona:

- Establecimiento, mantenimiento y finalización de sesiones: permite que dos procesos de aplicación en diferentes equipos establezcan, utilicen y finalicen una conexión, que se denomina sesión.
- Soporte de sesión: realiza las funciones que permiten a estos procesos comunicarse a través de una red, ejecutando la seguridad, el reconocimiento de nombres, el registro, etc.

2.2.5.6. Capa de presentación

La capa de presentación da formato a los datos que deberán presentarse en la capa de aplicación. Se puede decir que es el traductor de la red. Esta capa puede traducir datos de un formato utilizado por la capa de la aplicación a un formato común en la estación emisora y, a continuación, traducir el formato común a un formato conocido por la capa de la aplicación en la estación receptora.

La capa de presentación proporciona:

- Conversión de código de caracteres: por ejemplo, de ASCII a EBCDIC.
- Conversión de datos: orden de bits, CR-CR/LF, punto flotante entre enteros, etc.
- Compresión de datos: reduce el número de bits que es necesario transmitir en la red.
- Cifrado de datos: cifra los datos por motivos de seguridad. Por ejemplo, cifrado de contraseñas.

2.2.5.7. Capa de aplicación

El nivel de aplicación actúa como ventana para los usuarios y los procesos de aplicaciones para tener acceso a servicios de red. Esta capa contiene varias funciones que se utilizan con frecuencia:

- Uso compartido de recursos y redirección de dispositivos
- Acceso a archivos remotos
- Acceso a la impresora remota
- Comunicación entre procesos
- Administración de la red
- Servicios de directorio
- Mensajería electrónica (como correo)
- Terminales virtuales de red.

2.2.6. Dispositivos de red

(Stallings, 2000) Señala que existen dos clasificaciones, la primera clasificación son los dispositivos de usuario final, como por ejemplo computadoras, impresoras, scanners y otros dispositivos que provean servicios directamente al usuario.

Estos dispositivos son conectados físicamente a la red usando una Network Interface Card (NIC) que tiene su propio código o dirección MAC. La segunda clasificación son los dispositivos de red.

Los dispositivos de red proveen la comunicación entre dispositivos de usuario final. Como por ejemplo:









Dispositivos de red	
Repetidor 	Puente 
Hub 10BASE-T 	Switch de grupo de trabajo 
Hub 100BASE-T 	Router 
Hub 	Nube de red 

Figura 2: Iconos de los dispositivos de red
Fuente: Cisco CCNA EXPLORATION 4.0

2.2.7. Repetidores:

Un repetidor es un dispositivo de red que se utiliza para regenerar la señal tanto analógicas como digitales que se distorsionan a causa de pérdidas en la transmisión producidas por la atenuación, este dispositivo trabaja a nivel de capa física del modelo OSI tiene dos puertos y permite extender la red, un repetidor no toma decisiones inteligentes acerca del envío de paquetes como lo hace un router o puente.

2.2.8. Hubs:

Permiten que la red trate un grupo de hosts como si fuera una sola unidad. Esto sucede de manera pasiva, sin interferir en la transmisión de datos. Los hubs activos no sólo concentran hosts, sino que además regeneran señales, estos dispositivos trabajan física y tienen más puertos que un repetidor.

2.2.9. Puentes:

Convierten los formatos de transmisión de datos de la red además de realizar la administración básica de la transmisión de datos. Los puentes, tal como su nombre lo indica, proporcionan las conexiones entre LAN. Los puentes no sólo conectan las LAN, sino que además verifican los datos para determinar si les corresponde o no cruzar el puente. Esto aumenta la eficiencia de cada parte de la red. Trabajan a nivel de la capa de enlace de datos del modelo OSI, segmentan la red por puertos y son dispositivos pasivos.

2.2.10. Switch:

Agregan inteligencia a la administración de transferencia de datos. No sólo son capaces de determinar si los datos deben permanecer o no en una LAN, sino que pueden transferir los datos únicamente a la conexión que necesita esos datos. Otra diferencia entre un puente y un switch es que un switch no convierte formatos de transmisión de datos, trabajan en la capa de enlace de datos tienen más interfaces.

2.2.11. Routers:

Los routers pueden regenerar señales, concentrar múltiples conexiones, convertir formatos de transmisión de datos, y manejar transferencias de datos. También pueden conectarse a una WAN, lo que les permite conectar LAN que se encuentran separadas por grandes distancias. Ninguno de los demás dispositivos puede proporcionar este tipo de conexión. Trabajan en la capa de red del modelo OSI segmentan la red por puerto a nivel de capa 2 y 3.

2.2.12. Protocolo de configuración de hosts dinámico – DHCP

El DHCP (Protocolo de Configuración de Hosts Dinámico) se basa en el RFC 2131, y trabaja en modo cliente –servidor. El protocolo de configuración de hosts dinámico, habilita a los clientes DHCP, obtener sus configuraciones desde un servidor DHCP, considerando que la opción de configuración de mayor importancia, es la dirección IP asignada al cliente.

El DHCP no se utiliza para la configuración de los switches, routers o servidores. Estos hosts necesitan tener direcciones estáticas.

DHCP usa el UDP como protocolo de transporte. El cliente envía mensajes al servidor sobre el puerto 67, mientras que el servidor envía mensajes al cliente sobre el puerto 68. Los clientes DHCP arriendan la información del servidor por un periodo definido administrativamente. Y cuando el arrendamiento expira, el cliente debe pedir otra dirección, aunque generalmente se le reasigna la misma.

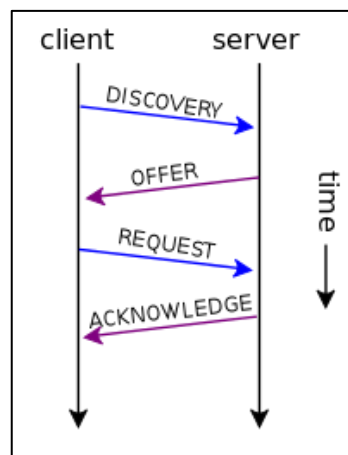


Figura 3: Orden de transmisión de mensajes DHCP

Fuente: es.wikipedia.org

2.2.13. ETHERNET

(Cisco, 2008) En la página oficial de CISCO (2008) podemos encontrar que originalmente Ethernet fue desarrollado como prueba de redes de cable coaxial por la compañía Xerox en la década de 1970, operaba con una velocidad de transmisión de 3Mbps y utilizaba como protocolo de acceso al medio CSMA/CD.

Rápidamente el proyecto fue un éxito y la atención temprana que causó, condujo al desarrollo en la década de los 80 de la versión de Ethernet a 10 Mbps Ver. 1.0 donde se sumaron al desarrollo las empresas DEC e Intel.

Otras tecnologías y protocolos han sido promocionados como probables sustitutos de Ethernet pero esta se ha pronunciado en el mercado y ha sobrevivido como la principal tecnología de LAN (hoy día aproximadamente el 85 % de las LAN de todo el mundo están basadas en Ethernet) porque su protocolo tiene las siguientes características:

- a) Es fácil de comprender, aplicar, administrar y mantener.
- b) Tiene bajo costo en las implementaciones de red.
- c) Proporciona amplia flexibilidad topológica para la instalación de red
- d) Garantiza completa interconexión y operación de normas de productos, independientemente del fabricante.

2.2.14. Dominio de colisión

Las redes LAN Ethernet usan el esquema de acceso al medio CSMA/CD, el cual determina que dispositivo puede transmitir datos en una red compartida.

(Herrera Perez, 2003) Menciona que si más de un dispositivo quiere transmitir en el mismo lapso de tiempo, ocurrirá una colisión.

(Mejía Mesa, 2005) Afirma que ambas transacciones colisionadas se dañan y los dispositivos tendrán que intentar retransmitir los datos más tarde utilizando el algoritmo de retroceso exponencial binario. Esta problemática no es agradable a los usuarios de la red los cuales requieren cumplir con su objetivo en el menor tiempo posible.

(Íñigo Griera, y otros, 2009) Comentan que hay dos soluciones posibles para resolver en la red el problema que se genera al tener un gran dominio de colisiones y son las siguientes:

- a) Cambiar el estándar utilizado por uno de mayor velocidad.
- b) Segmentar el dominio de colisiones de manera que el número de terminales pertenecientes al dominio de colisiones sea menor.

Esta posible solución usa puentes transparentes para que solo se transmitan las tramas de capa 2 al segmento de red donde se encuentra la dirección.

2.2.15. Dominio de broadcast

(Oppenheimer, 2004) Comenta que aparte del problema de las colisiones (puede resolverse en la capa 2), existe otro problema potencial con las redes no jerárquicas y es el dominio de broadcast.

(Mejía Mesa, 2005) Define la técnica broadcast como la consistencia en enviar simultáneamente por la red un mismo mensaje a múltiples estaciones

(Caprile, 2009) Los broadcast a diferencia de las colisiones merecen un tratamiento especial, debido a que tienen que ser repetidos por los routers para que trasciendan la red y puedan llegar a destinos más lejanos, pero sin ocasionar el problema clásico de los puentes conocidos como broadcast storm (tormenta de broadcast) en donde un simple broadcast en una red con caminos paralelos es repetido una y otra vez pues cada puente debe de repetir el que genera su puente vecino. El problema generado por una tormenta de broadcast es el saturar o dejar sin operar los equipos activos de red.

2.2.16. Modelo jerárquico CISCO

(Luis R, 2008) La jerarquía tiene muchos beneficios en el diseño de las redes y nos ayuda a hacerlas más predecibles. En sí, definimos funciones dentro de cada capa, ya que las redes grandes pueden ser extremadamente complejas e incluir múltiples protocolos y tecnologías; así, el modelo nos ayuda a tener un modelo fácilmente entendible de una red y por tanto a decidir una manera apropiada de aplicar una configuración.

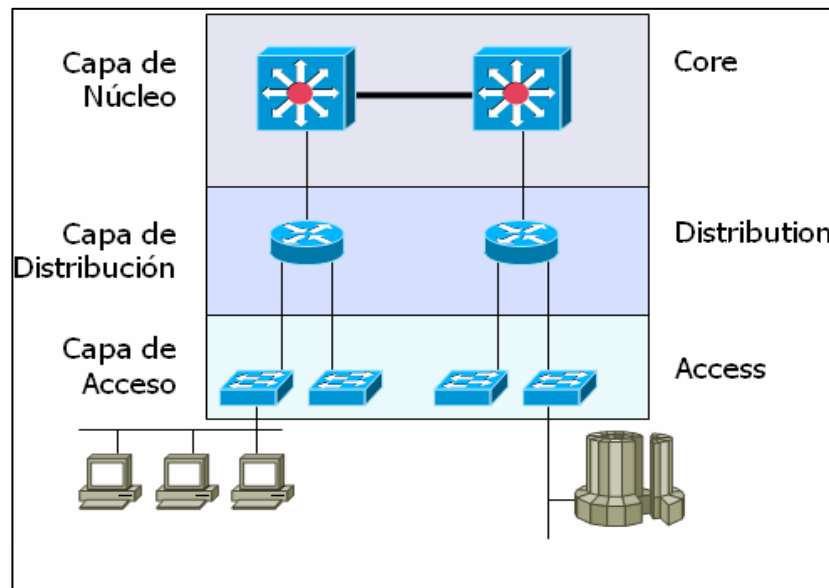


Figura 4: Modelo jerárquico de Cisco

Fuente: ipref.wordpress.com

Entre las ventajas que tenemos de separar las redes en 3 niveles tenemos que es más fácil diseñar, implementar, mantener y escalar la red, además de que la hace más confiable, con una mejor relación costo/beneficio. Cada capa tiene funciones específicas asignadas y no se refiere necesariamente a una separación física, sino lógica; así que podemos tener distintos dispositivos en una sola capa o un dispositivo haciendo las funciones de más de una de las capas.

(Flores, 2008) Cisco recomienda el uso del modelo de tres capas a la hora de diseñar nuestras redes.

2.2.16.1. Capa de acceso

La capa de acceso de la red es el punto en el que cada usuario se conecta a la red. Ésta es la razón por la cual la capa de acceso se denomina a veces capa de puesto de trabajo, capa de escritorio o de usuario. Los usuarios así como los recursos a los que estos necesitan acceder con más frecuencia, están disponibles a nivel

local. El tráfico hacia y desde recursos locales está confinado entre los recursos, switches y usuarios finales.

En la capa de acceso podemos encontrar múltiples grupos de usuarios con sus correspondientes recursos. En muchas redes no es posible proporcionar a los usuarios un acceso local a todos los servicios, como archivos de bases de datos, almacenamiento centralizado o acceso telefónico al Web. En estos casos, el tráfico de usuarios que demandan estos servicios se desvía a la siguiente capa del modelo: la capa de distribución.

2.2.16.2. Capa de distribución

La capa de distribución representa el punto medio entre la capa de acceso y los servicios principales de la red. La función primordial de esta capa es realizar funciones tales como enrutamiento, filtrado y acceso a WAN.

En un entorno de campus, la capa de distribución abarca una gran diversidad de funciones, entre las que figuran las siguientes:

- Servir como punto de concentración para acceder a los dispositivos de capa de acceso.
- Enrutar el tráfico para proporcionar acceso a los departamentos o grupos de trabajo.
- Segmentar la red en múltiples dominios de difusión / multidifusión.

- Traducir los diálogos entre diferentes tipos de medios, como Token Ring y Ethernet.
- Proporcionar servicios de seguridad y filtrado.

La capa de distribución puede resumirse como la capa que proporciona una conectividad basada en una determinada política, dado que determina cuándo y cómo los paquete pueden acceder a los servicios principales de la red. La capa de distribución determina la forma más rápida para que la petición de un usuario (como un acceso al servidor de archivos) pueda ser remitida al servidor. Una vez que la capa de distribución ha elegido la ruta, envía la petición a la capa de núcleo. La capa de núcleo podrá entonces transportar la petición al servicio apropiado.

2.2.16.3. Capa de núcleo

La capa del núcleo, principal o Core se encarga de desviar el tráfico lo más rápidamente posible hacia los servicios apropiados. Normalmente, el tráfico transportado se dirige o proviene de servicios comunes a todos los usuarios.

Estos servicios se conocen como servicios globales o corporativos. Algunos de tales servicios pueden ser e-mail, el acceso a Internet o la videoconferencia.

Analice el siguiente caso práctico: **Un usuario necesita acceder a un servicio corporativo:**

- a) La petición se procesa al nivel de la capa de distribución.

- b) El dispositivo de la capa de distribución envía la petición del usuario al núcleo.
- c) Este se limita a proporcionar un transporte rápido hasta el servicio corporativo solicitado.
- d) El dispositivo de la capa de distribución se encarga de proporcionar un acceso controlado a la capa de núcleo.

2.2.16.4. Beneficios del modelo jerárquico

(Valentine & Whitaker, 2008) Encuentran que el modelo de tres capas tiene importantes ventajas que se explican brevemente enseguida:

- a) Escalabilidad:** Cuando se requiere agregar usuarios, si se quiere poner un dispositivo adicional en alguna capa, al no tener que reemplazar toda la capa distribución y de acceso, al mismo tiempo. Es fácil agregar funcionalidad extendida a una capa a la vez, según sea necesario o a todos a la vez.
- b) Ahorro de costos:** Ya que los dispositivos de la capa de acceso son mucho más económicos que los dispositivos de distribución o núcleo; se puede mejorar una sola capa sin tener que actualizar las tres capas a la vez, e incurrir en gastos altos innecesarios.
- c) Fácil solución de problemas:** Si un componente de una capa falla, no afecta el funcionamiento total del sistema. Es muy fácil encontrar el problema si falla un dispositivo y solo afecta a su capa.

2.2.17. Redes de área local virtuales (VLAN)

(Wikipedia , 2016) Una VLAN, acrónimo de virtual LAN (red de área local virtual), es un método para crear redes lógicas independientes dentro de una misma red física.¹ Varias VLAN pueden coexistir en un único conmutador físico o en una única red física. Son útiles para reducir el tamaño del dominio de difusión y ayudan en la administración de la red, separando segmentos lógicos de una red de área local (los departamentos de una empresa, por ejemplo) que no deberían intercambiar datos usando la red local (aunque podrían hacerlo a través de un enrutador o un conmutador de capa 3 y 4).

Una VLAN consiste en dos o más redes de computadoras que se comportan como si estuviesen conectados al mismo PCI, aunque se encuentren físicamente conectados a diferentes segmentos de una red de área local (LAN). Los administradores de red configuran las VLAN mediante software en lugar de hardware, lo que las hace extremadamente fuertes.

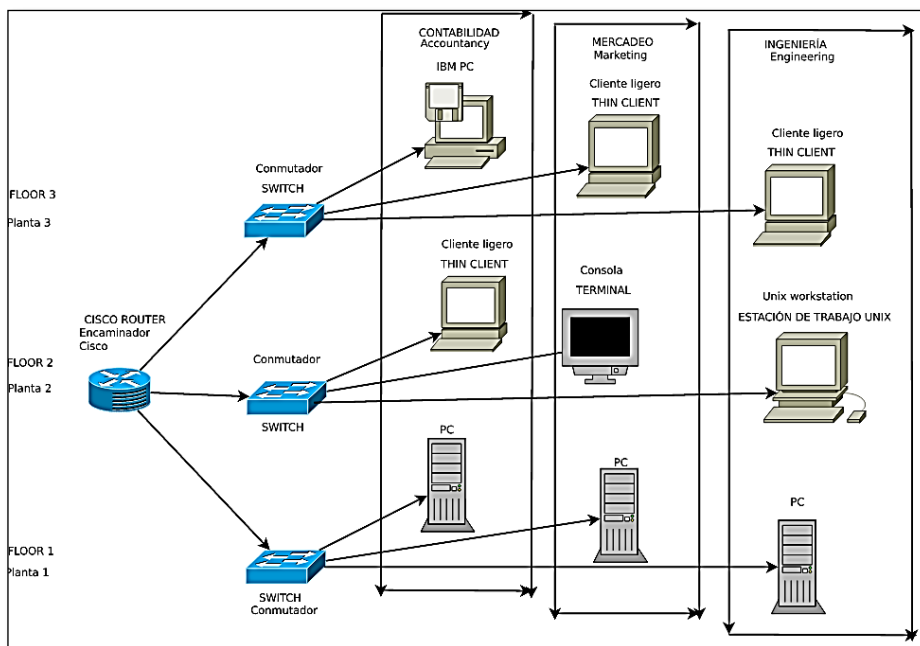


Figura 5: Topología de red virtual VLAN

Fuente: es.wikipedia.org

2.2.18. Clasificación

(Wikipedia , 2016) Aunque las más habituales son las VLAN basadas en puertos (nivel 1), las redes de área local virtuales se pueden clasificar en cuatro tipos según el nivel de la jerarquía OSI en el que operen:

VLAN de nivel 1 (Por puerto):

También conocida como “port switching”. Se especifica qué puertos del switch pertenecen a la VLAN, los miembros de dicha VLAN son los que se conecten a esos puertos. No permite la movilidad de los usuarios, habría que reconfigurar las VLAN si el usuario se mueve físicamente. Es la más común y la que se explica en profundidad en este artículo.

VLAN de nivel 2 (Por direcciones MAC):

Se asignan hosts a una VLAN en función de su dirección MAC. Tiene la ventaja de que no hay que reconfigurar el dispositivo de conmutación si el usuario cambia su localización, es decir, se conecta a otro puerto de ese u otro dispositivo. El principal inconveniente es que si hay cientos de usuarios habría que asignar los miembros uno a uno.

VLAN de nivel 2 (Por tipo de protocolo):

La VLAN queda determinada por el contenido del campo tipo de protocolo de la trama MAC. Por ejemplo, se asociaría VLAN 1 al protocolo IPv4, VLAN 2 al protocolo IPv6, VLAN 3 a AppleTalk, VLAN 4 a IPX.

VLAN de nivel 3 (Por direcciones de subred - subred virtual):

La cabecera de nivel 3 se utiliza para mapear la VLAN a la que pertenece. En este tipo de VLAN son los paquetes, y no las estaciones, quienes pertenecen a la VLAN. Estaciones con múltiples protocolos de red (nivel 3) estarán en múltiples VLAN.

VLAN de niveles superiores:

Se crea una VLAN para cada aplicación: FTP, flujos multimedia, correo electrónico... La pertenencia a una VLAN puede basarse en una combinación de factores como puertos, direcciones MAC, subred, hora del día, forma de acceso, condiciones de seguridad del equipo.

2.3. Glosario de términos básicos

- **PDU o Protocol Data Unit**

Por sus siglas en inglés, significa Unidad de datos del protocolo, es la forma que adopta una sección de datos en cualquier capa del modelo OSI.

- **Arquitectura de red**

Es el diseño de una red de comunicaciones, el marco para la especificación de los componentes físicos de una red y de su organización funcional y configuración, sus procedimientos y principios operacionales, así como los formatos de los datos utilizados en su funcionamiento.

- **Subnetting**

Es dividir una red, en sub-redes más pequeñas para que estas redes puedan funcionar mejor.

- **Medios de red**

Son el soporte físico o inalámbrico que se utiliza para la transmisión de información en las redes.

- **Dirección IP**

Dirección que se utiliza para identificar un equipo o dispositivo en una red.

- **Ethernet**

Protocolo de red estándar de IEEE que especifica la forma en que se colocan los datos y se recuperan de un medio de transmisión común.

- **FTP (Protocolo de transferencia de archivos)**

Protocolo estándar de envío de archivos entre equipos a través de redes TCP/IP e Internet.

- **Red troncal**

Parte de una red que conecta la mayoría de los sistemas y los une en red, así como controla la mayoría de datos

- **Rendimiento**

Cantidad de datos que se han movido correctamente de un nodo a otro en un periodo de tiempo determinado.

- **Routing**

El proceso de mover un paquete de datos de fuente a destino, normalmente se usa un "Router".

- **Servidor**

Cualquier equipo cuya función en una red sea proporcionar acceso al usuario a archivos, impresión, comunicaciones y otros servicios.

- **Ancho de banda**

Relación de velocidad para la transmisión de datos medidos en Kbps (kilo comunicación para transportar datos).

- **Internet**

Red de redes con base en TCP/IP y acceso público mundial.

- **IP**

Es el protocolo de envío de paquetes donde el paquete tiene una dirección destino, y éste se envía sin acuse de recibo.

2.4. Hipótesis de la investigación

El modelo de implementación de redes virtuales VLAN y priorización del ancho de banda, mejora el rendimiento de la red de área local del Proyecto Especial Lago Titicaca - Sede central Puno – 2016.

2.5. Operacionalización de variables

Tabla 1: Operacionalización de variables

Variables	Dimensiones	Indicadores	Escala
<p>Independiente (Red de área local)</p> <p>Y</p> <p>Dependiente (Modelo de implementación de redes virtuales VLAN y priorización de ancho de banda).</p>	<p>Rendimiento de red: Escalabilidad, calidad de servicio, disponibilidad y seguridad</p>	Ancho de banda	Bits por segundo
		Throughput	Bits por segundo
		Latencia	Micro segundos
		Segmentos de red	Número de subredes
		VLANs	Número de VLANs implementadas.
		Fallas en la red	Número de fallas en la red
		Diámetro de red	Número de dispositivos que cruza un paquete
		Interfaces de red disponibles	Número de interfaces disponibles
		Direcciones IP disponibles	Número de direcciones IP disponibles
		Diseño de red	Existe / No existe
		Identificación de tipos de paquetes	Existe / No existe
		Priorización del ancho de banda	Existe / No existe
		Enlaces redundantes	Número de enlaces redundantes
		Listas de control de acceso	Existe / No existe
Resguardo de equipos y medios de red	Si / No		

Elaboración: Propia

CAPÍTULO III

DISEÑO METODOLÓGICO DE LA

INVESTIGACIÓN

3.1. Tipo y Diseño de investigación

3.1.1. Tipo de investigación

De acuerdo a la hipótesis y objetivos, es descriptiva, ya que se recogió información de las características y propiedades de la variable independiente.

Por su propósito también es una investigación de tipo aplicada, ya que el modelo resuelve el problema de rendimiento de la red de área local actual.

3.1.2. Diseño de investigación

Acorde al criterio expuesto Hernández (2010), el diseño es no experimental longitudinal de tendencia porque se analizaron cambios a través del tiempo a la misma población; también es sistemático y empírico, debido que la variable independiente ya sucedió y no fue manipulada.

3.2. Población y muestra de investigación

Población:

Usuarios con acceso a la red de área local del Proyecto Especial Lago Titicaca – Puno – 2016, los cuales se cuantifican en un total de 162.

Muestra:

La muestra no probabilística son todos los usuarios con acceso a la red de área local del Proyecto Especial Lago Titicaca –sede central Puno – 2016.

3.3. Ubicación y descripción de la población

La sede central del Proyecto Especial Lago Titicaca se encuentra ubicada en la ciudad de Puno, exactamente en el Jirón Deustua N° 822.

3.4. Técnicas e instrumentos para recolectar información

Técnicas:

Las técnicas utilizadas fueron:

- Observación
- Análisis

Instrumentos:

Para obtener información detallada, objetiva y confiable, se utilizaron los siguientes instrumentos electrónicos o programas:

- PRTG Network Monitor
- Wireshark
- Iperf
- Packet Tracer 7.0
- PSPP

3.5. Técnicas para el procesamiento y análisis de datos

Los datos obtenidos fueron procesados y analizados según la metodología Top-Down Network Design Third Edition de Priscilla Oppenheimer y Cisco, instrumentos electrónicos, y también mediante análisis estadístico descriptivo.

3.6. Plan de tratamiento de los datos

Los datos se procesaron de forma cualitativa, mediante gráficos, tablas, hojas de cálculo y en forma estadística, se utilizó la “prueba t”.

Para la comparación entre los indicadores de la red actual y los proyectados mediante el modelo, se utilizará la siguiente tabla:

Tabla 2: Comparación de indicadores

Indicador	Red actual	Modelo	Diferencia
Ancho de banda de los equipos.			
Throughput			
Promedio de latencia máximo			
Segmentos de red			
VLANs			
Número de fallas en la red			
Número de dispositivos que cruza un paquete			
Interfaces o puertos de red disponibles			
Direcciones IP disponibles			
Diseño de red			
Identificación de tipos de paquetes			
Priorización del ancho de banda			
Enlaces redundantes			
Listas de control de acceso			
Resguardo de equipos y medios de red			

Elaboración: Propia

CAPÍTULO IV

**ANÁLISIS E INTERPRETACIÓN DE
RESULTADOS DE LA INVESTIGACIÓN**

4.1. Análisis del rendimiento de la red actual

El análisis se realizó de acuerdo a Cisco Systems y Oppenheimer, (2011). Top-Down Network Design. 3a ed. United State of America: Cisco Press.

4.1.1. Análisis de metas y restricciones

El Proyecto Especial Lago Titicaca (PELT) es Unidad Ejecutora del Ministerio de Agricultura y Riego tiene como objetivo central “Lograr el aprovechamiento sostenible de los recursos hídricos y naturales en la cuenca del lago Titicaca del sistema endorreico Titicaca – Desaguadero – Poopó – Salar de Coipasa (TDPS) lado peruano”.

La estructura orgánica es la siguiente:

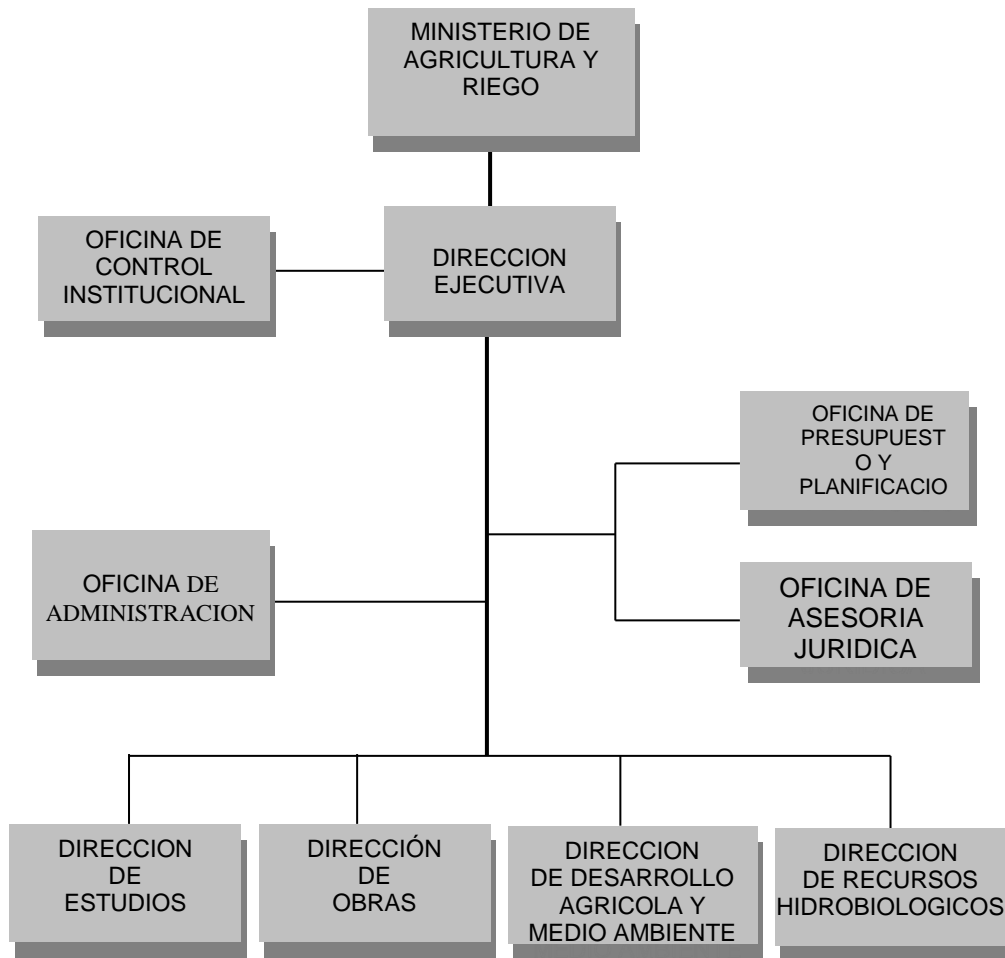


Figura 6: Organigrama del PELT
Fuente: Plan Operativo Institucional 2016 - PELT

La sede central de la entidad se encuentra ubicada en la ciudad de Puno, específicamente en el Jirón Deustua N° 822.

Las metas del diseño de red son:

- Minimizar los problemas de conexión.
- Elevar la productividad de los usuarios de las TIC para coadyuvar al logro de objetivos de la entidad.
- Gestionar el uso eficiente de las TIC.
- Proteger la información.

Metas técnicas:

- Rediseño del direccionamiento IP.
- Proveer seguridad a los usuarios que acceden a la red.
- Proveer una red Enterprise disponible al 92%.
- Proveer seguridad para proteger conexiones a internet y la red interna.
- Proveer una red escalable y que soporte un futuro uso de aplicaciones de voz y multimedia (red convergente).
- Priorizar el tráfico de red

Ámbito

El proyecto comprende el análisis y entendimiento de la arquitectura y rendimiento de la red de la sede central del PELT, que comprende las siguientes direcciones u oficinas:

- Dirección de Estudios.
- Dirección de Obras.
- Dirección Ejecutiva
- Dirección de Desarrollo Agrícola y Medio Ambiente
- Dirección de Recursos Hidrobiológicos
- Oficina de Presupuesto y Planificación
- Oficina de Administración
- Oficina de Contabilidad
- Oficina de Abastecimientos
- Oficina de Asesoría Legal
- Oficina de Imagen Institucional

- Oficina de Personal
- Oficina de Tesorería
- Oficina de Gestión Documentaria
- Órgano de Control Institucional
- Oficina de Informática
- Oficina de Patrimonio

Es preciso mencionar que la Dirección de Recursos Hidrobiológicos se encuentra ubicada en la sub-sede Chucuito, no obstante en la sede central cuenta con una pequeña oficina para realizar trámites administrativos.

Identificación de aplicaciones de la red

Tabla 3: Aplicaciones

Nombre de la aplicación	Tipo de aplicación	Aplicación nueva (si o no)	Critica	Comentarios
Newton	File server	No	No	
Clarisa	File server	No	No	
Melisa	File server	No	No	
Sistema de Gestión Documentaria (SGD)	Web		Si	
SIAF	ERP	No	Si	
SIGA	ERP	No	Si	
Control de Asistencia	File server	No	Si	Solamente están conectadas dos PCs.
SEACE	Web	No	Si	

Elaboración: Propia

Política y políticas

La mayoría de los usuarios están acostumbrados a usar el servicio de internet con fines propios de estudio, distracción, etc. Es probable que no acepten las restricciones que se plantean, por lo que el apoyo de la dirección ejecutiva es esencial.

Así mismo, es preciso mencionar que la implementación del modelo no elimina puesto de trabajo alguno.

Restricciones de presupuesto y personal

Debido que el proyecto simulará el modelo, no existe gasto en equipos, licencias, medios de comunicación, servicios de mantenimiento, u otros, pero la finalidad es que a mediano plazo se implemente el modelo propuesto.

Referente al personal, de acuerdo a lo observado durante el periodo de recolección de información, en la entidad no labora personal capacitado para la administración de la red, por lo que se sugiere outsourcing.

4.1.1.1. Análisis de metas técnicas y compensaciones

4.1.1.1.1. Escalabilidad

Plan de expansión

Tabla 4: Histórico y proyección de usuarios

Año	Usuarios	Teléfonos VoIP (posibles usuarios)	Total
2011	85	-	85
2012	99	-	99
2013	105	-	102
2014	120	-	120
2015	135	-	135
2016	162	52	214
2017	167	53	220
2018	172	54	226
2019	177	55	232
2020	182	56	238
2021	187	57	244

Elaboración: Propia

De acuerdo al Plan Operativo Informático del año 2016, la entidad no programó adquisición de servidores.

Expandir acceso a la data

Según el Plan Operativo Informático 2016:

- No existen planes para expandir la red.
- Se planificaron tres actividades que reflejan problemas en la red: Mejoramiento del servicio de internet, realizar un diagnóstico del estado del cableado, y realizar mantenimiento preventivo y correctivo de cableado incluyendo el reemplazo de equipos de red si es necesario.

Interfaces o puertos de red disponibles

Referente a las interfaces o puertos de red disponibles de los diez (10) switches, se tiene:

Tabla 5: Interfaces o puertos de red disponibles

Switches en funcionamiento	10
Puertos disponibles de los 10 switches	224
Puertos utilizados por usuarios	162
Puertos que deberían estar disponibles	62
Puertos disponibles	32
Puertos ocupados (desconocimiento los dispositivos que conecta)	30

Elaboración: Propia

Direcciones IP disponibles

Debido al diseño plano se tiene:

Tabla 6: Direcciones IP – Red actual

Número máximo de subredes	0
Número máximo de direcciones IP disponibles	254
Número de direcciones IP utilizadas	162
Número de direcciones IP disponibles	92

Elaboración: Propia

Es importante mencionar que la Oficina de Tecnologías de Información no tiene registro de cuales direcciones están disponibles, ya que el direccionamiento fue realizado aleatoriamente, es decir, no cuenta con plan de expansión.

4.1.1.1.2. Disponibilidad

Recuperación ante desastres

La entidad no cuenta con un plan para sostener la continuidad de sus funciones o labores en caso de desastres naturales, los sistemas de tipo “file server” no cuentan con backups que se ubiquen fuera del alcance del desastre, excepto por en el caso del Sistema de Gestión Documentaria, actualmente se está implementando un servidor local que enviará información diariamente al servidor central ubicado en el Ministerio de Agricultura - Lima. En el modelo se tomó en cuenta el resguardo de la data de configuración de cada dispositivo de conexión, y con la nueva infraestructura de red, será posible crear y mantener actualizados backups de todos los sistemas utilizados.

Requerimientos de disponibilidad

De acuerdo a las necesidades de la entidad, se tiene:

Tabla 7: Disponibilidad de red

Horas	Días	Meses	Años
24	7	12	10

Elaboración: Propia

Tolerancia de tiempo de inactividad

Definimos la disponibilidad mediante la siguiente fórmula:

$$\text{Porcentaje de disponibilidad} = \frac{MTBF}{MTBF + MTTR} * 100$$

Figura 7: Disponibilidad
Fuente: Top-down Network Design – Cisco Press & Priscilla
Oppenheimer

Donde:

MTBF: Tiempo promedio entre fallas.

MTTR: Tiempo promedio que toma reparar la falla (tiempo de inactividad).

Respecto a la red en general:

Del análisis y consultas realizadas a la dirección ejecutiva y personal de TI se tiene:

MTBF: 12

MTTR: 1

Entonces:

Disponibilidad = $(12 / 13) * 100 = 92.3\%$

Número de fallas

La Oficina de Tecnologías de Información no registra las fallas que ocurren en la red, de la consulta realizada menciona que aproximadamente suceden 2 fallas al mes.

Respecto a las aplicaciones:

Tabla 8: Disponibilidad de aplicaciones

Nombre de la aplicación	Tipo de aplicación	Aplicación nueva (Si o No)	Criticidad	MTBF aceptable	Disponibilidad
Newton	File server	No	No	8	88.9%
Clarisa	File server	No	No	8	88.9%
Melisa	File server	No	No	8	88.9%
Sistema de Gestión Documentaria (SGD)	Web	No	Si	12	92.3%
SIAF	ERP	No	Si	12	92.3%
SIGA	ERP	No	Si	12	92.3%
Control de Asistencia	File server	No	Si	12	92.3%
SEACE	Web	No	Si	12	92.3%

Elaboración: Propia

Cabe mencionar que existe la posibilidad de ocurrencia de fallas externas que exceden el alcance de este trabajo de investigación:

- Cortes de energía eléctrica.
- Latencia o disminución del ancho de banda por problemas en la red de la empresa proveedora del servicio de internet.

El costo de estar fuera de servicio

Se tiene:

Tabla 9: Costo por estar fuera de servicio

Nombre de la aplicación	Tipo de aplicación	Costo por estar fuera de servicio
Newton	File server	Medio
Clarisa	File server	Medio
Melisa	File server	Medio
Sistema de Gestión Documentaria (SGD)	Web	Alto
SIAF	ERP	Alto
SIGA	ERP	Alto
Control de Asistencia	File server	Alto
SEACE	Web	Alto

Elaboración: Propia

Enlaces redundantes

La red no cuenta con enlaces redundantes, es más se identifica sobreutilización de dos enlaces (denominados cuellos de botella), los cuales se muestran señalados de color rojo en la siguiente figura:

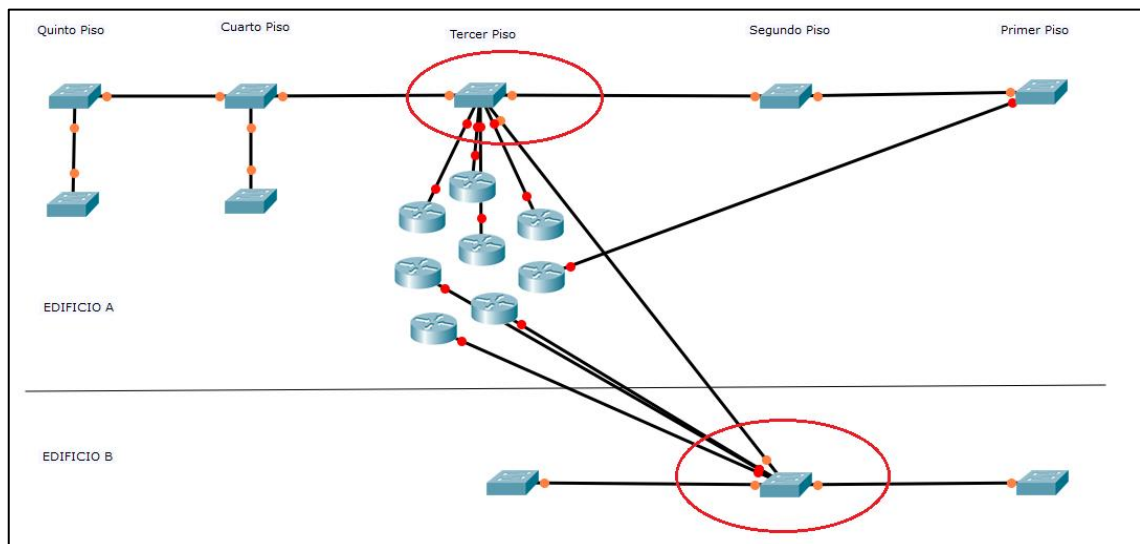


Figura 8: Sobreutilización de enlaces
Fuente: Cisco Packet Tracer
Elaboración: Propia

En la figura 4.2, se puede apreciar que el máximo diámetro de red es seis (6).

Rendimiento de la red

El Director Ejecutivo indica “Tiene que trabajar sin quejas de los usuarios”, el encargado de la Oficina de TI no especifica cual es la performance de la red.

Para el establecer las metas de performance se tomó en cuenta los siguientes factores:

Ancho de banda (bps)

Actualmente la entidad contrata ocho (08) paquetes o planes de internet, de acuerdo al siguiente detalle:

Tabla 10: Ancho de banda contratado

Ítem	Plan de internet contratado	Ancho de banda
1	Dúo Fijo (LíneaPremium Plana 79 y Movistar Internet – Cat Residencial 20Mbps)	De 20 Mbps a 8Mbps (Garantiza el 40%)
2	Dúo Fijo (LíneaPremium Plana 79 y Movistar Internet – Cat Residencial 20Mbps)	De 20 Mbps a 8Mbps (Garantiza el 40%)
3	Dúo Fijo (LíneaPremium Plana 79 y Movistar Internet – Cat Comercial 20Mbps)	De 20 Mbps a 8Mbps (Garantiza el 40%)
4	Dúo Fijo (LíneaPremium Plana 79 y Movistar Internet – Cat Comercial 20Mbps)	De 20 Mbps a 8Mbps (Garantiza el 40%)
5	Dúo Fijo (LíneaPremium Plana+Multide y Speedy Uno 10Mbps)	De 10 Mbps a 4 Mbps (Garantiza el 40%)
6	Dúo Fijo (LíneaPremium Plana+Multide y Speedy Uno 10Mbps)	De 10 Mbps a 4 Mbps (Garantiza el 40%)
7	Dúo Fijo (LíneaPremium Plana+Multide y Speedy Uno 10Mbps)	De 10 Mbps a 4 Mbps (Garantiza el 40%)
8	Movistar Speedy Avanzado 3Mbps	3Mbps (Garantiza el 100%)

Fuente: Oficina de TI - PELT
Elaboración: Propia

Los equipos de red (switches y routers) y el medio de conexión (cable de red) soportan 10Mbps y 100Mbps.

4.1.1.1.3. Utilización óptima

De la información obtenida por la herramienta Wireshark se tiene:

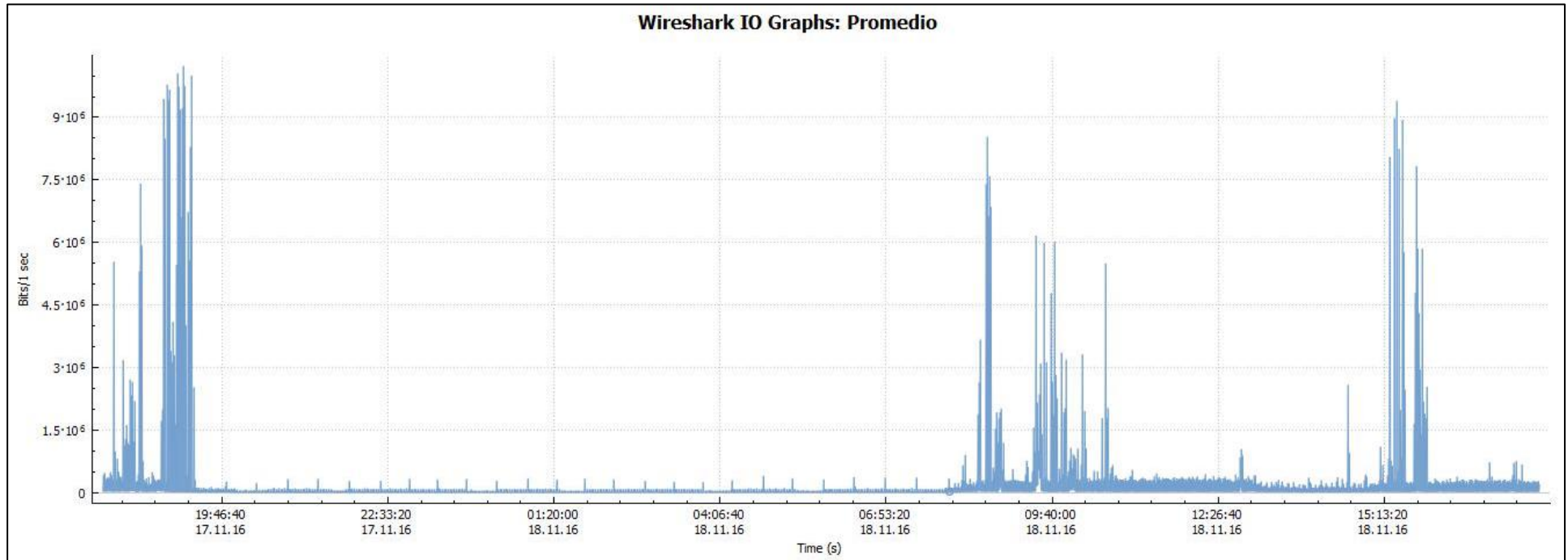


Figura 9: Utilización del ancho de banda
Fuente: Reporte Gráfico de Wireshark
Elaboración: Propia

Donde:

AnchodeBandaPromedio					
<i>Etiqueta de Valor</i>	<i>Valor</i>	<i>Frecuencia</i>	<i>Porcentaje</i>	<i>Porcentaje Válido</i>	<i>Porcentaje Acumulado</i>
	3.90	1	5.00	5.00	5.00
	4.00	1	5.00	5.00	10.00
	4.01	1	5.00	5.00	15.00
	4.07	1	5.00	5.00	20.00
	4.08	2	10.00	10.00	30.00
	4.09	3	15.00	15.00	45.00
	4.10	2	10.00	10.00	55.00
	4.12	1	5.00	5.00	60.00
	4.13	1	5.00	5.00	65.00
	4.15	1	5.00	5.00	70.00
	4.20	1	5.00	5.00	75.00
	4.21	1	5.00	5.00	80.00
	4.22	1	5.00	5.00	85.00
	4.30	1	5.00	5.00	90.00
	4.50	1	5.00	5.00	95.00
	4.70	1	5.00	5.00	100.00
<i>Total</i>		20	100.0	100.0	

AnchodeBandaPromedio		
<i>N</i>	<i>Válido</i>	20
	<i>Perdidos</i>	0
<i>Media</i>		4.16
<i>Desv Std</i>		.18
<i>Mínimo</i>		3.90
<i>Máximo</i>		4.70

Figura 10: Frecuencias del promedio del ancho de banda

Fuente: Tabla generada en PSPP

Elaboración: Propia

Interpretación

El promedio de uso del ancho de banda en veinte (20) días es de 4.16 Mbps, el mismo que varía ligeramente a 0.18 Mbps, el mínimo ancho de banda promedio utilizado fue de 3.90 Mbps y el máximo de 4.7 Mbps, estos resultados demuestran que no existe una utilización óptima del ancho de banda contratado, ya que se cuenta con varios servicios que garantizan un mínimo de 8 Mbps y un máximo de 20 Mbps, por lo tanto, que de acuerdo a los datos obtenidos, solamente es necesario un (01) “Dúo Fijo (LíneaPremium Plana 79 y Movistar Internet – Cat Residencial 20Mbps”.

Del análisis a la información obtenida por Wireshark se tiene:

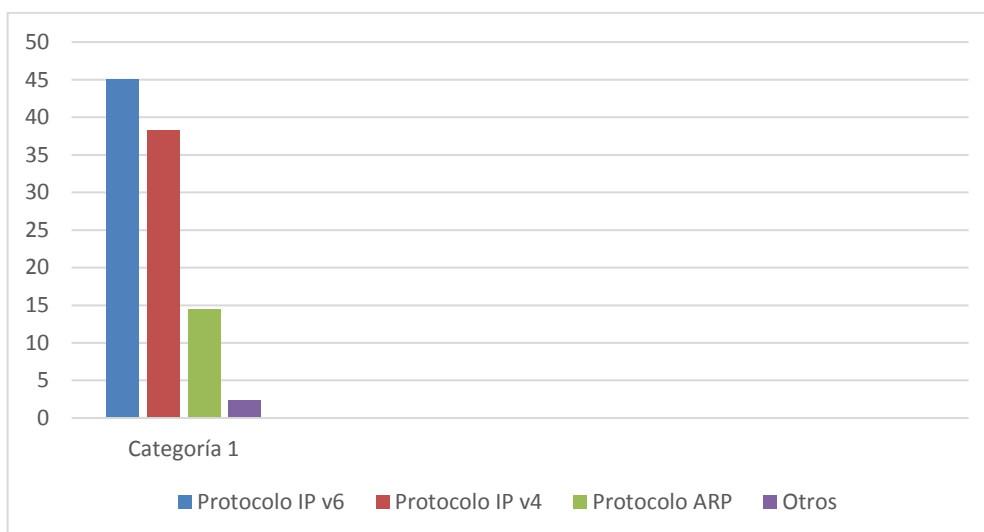


Figura 11: Estadística de jerarquía de protocolos
Fuente: Reporte de Wireshark
Elaboración: Propia

UsoDeProtocoloARP					
Etiqueta de Valor	Valor	Frecuencia	Porcentaje	Porcentaje Válido	Porcentaje Acumulado
	12.00	1	5.00	5.00	5.00
	12.90	1	5.00	5.00	10.00
	12.96	1	5.00	5.00	15.00
	13.00	2	10.00	10.00	25.00
	13.20	1	5.00	5.00	30.00
	13.50	1	5.00	5.00	35.00
	13.59	1	5.00	5.00	40.00
	13.75	1	5.00	5.00	45.00
	13.80	1	5.00	5.00	50.00
	13.85	1	5.00	5.00	55.00
	13.90	1	5.00	5.00	60.00
	13.95	1	5.00	5.00	65.00
	14.00	1	5.00	5.00	70.00
	14.10	1	5.00	5.00	75.00
	14.25	1	5.00	5.00	80.00
	14.30	1	5.00	5.00	85.00
	14.32	1	5.00	5.00	90.00
	14.50	1	5.00	5.00	95.00
	14.80	1	5.00	5.00	100.00
	Total	20	100.0	100.0	

UsoDeProtocoloARP		
N	Válido	20
	Perdidos	0
Media		13.68
Desv Std		.67
Mínimo		12.00
Máximo		14.80

Figura 12: Frecuencias del promedio de uso del Protocolo ARP
Fuente: Tabla generada en PSPP
Elaboración: Propia

Interpretación:

En veinte (20) días el promedio del porcentaje de uso del protocolo ARP es de 13.68%, con una variabilidad de 0.67%, valor mínimo de 12.00% y máximo de 14.80%, es decir, el protocolo ARP (Address Resolution Protocol) que es responsable de encontrar la dirección MAC (Media Access Control) usa un promedio del 13.68% o al menos el 12% y en otros casos 14.8% del tráfico de red, lo cual disminuye la capacidad de tráfico útil en la red, esto debido a la ausencia de mecanismos de control de dominios broadcast.

4.1.1.1.4. Latencia

Es el indicador más significativo y por motivos prácticos se realizó la medición mediante el programa PING, para hacer ping a toda la red se utilizó el siguiente código para MS-DOS:

@echo off

for /L %%a in (1,1,254) do ping -n 1 -w 350 192.168.1.%%a |

findstr /i Respuesta

Pause

En el anexo 1 se puede observar reporte ejemplo del programa PING, los resultados del análisis estadístico son:

LatenciaMáxima					
<i>Etiqueta de Valor</i>	<i>Valor</i>	<i>Frecuencia</i>	<i>Porcentaje</i>	<i>Porcentaje Válido</i>	<i>Porcentaje Acumulado</i>
	12.00	1	5.00	5.00	5.00
	25.00	1	5.00	5.00	10.00
	64.00	1	5.00	5.00	15.00
	75.00	1	5.00	5.00	20.00
	79.00	1	5.00	5.00	25.00
	89.00	1	5.00	5.00	30.00
	125.00	1	5.00	5.00	35.00
	128.00	1	5.00	5.00	40.00
	301.00	1	5.00	5.00	45.00
	350.00	1	5.00	5.00	50.00
	377.00	1	5.00	5.00	55.00
	398.00	1	5.00	5.00	60.00
	462.00	1	5.00	5.00	65.00
	464.00	1	5.00	5.00	70.00
	542.00	1	5.00	5.00	75.00
	548.00	1	5.00	5.00	80.00
	621.00	1	5.00	5.00	85.00
	639.00	1	5.00	5.00	90.00
	640.00	1	5.00	5.00	95.00
	644.00	1	5.00	5.00	100.00
<i>Total</i>		20	100.0	100.0	

LatenciaMáxima		
<i>N</i>	<i>Válido</i>	20
	<i>Perdidos</i>	0
<i>Media</i>		329.15
<i>Desv Std</i>		234.48
<i>Mínimo</i>		12.00
<i>Máximo</i>		644.00

Figura 13: Frecuencias del promedio de latencia máxima
Fuente: Tabla generada en PSPP
Elaboración: Propia

Interpretación:

En veinte (20) días, el promedio de latencia máxima en la red es de 329.15ms, el cual puede variar tremendamente hasta en 234.48ms, hasta un mínimo de 12ms y máximo de 644ms, lo cual indica que la transmisión de datos en la red LAN usualmente presenta latencia, pero esta puede variar en gran medida, no existen mecanismos que disminuyan la latencia.

4.1.1.1.5. Seguridad

Identificación de activos de la red

Hardware:

Tabla 11: Activos de red – Hardware

Activo	Cantidad	Costo total
Rack de pared para soporte de equipos de comunicación	1	S/. 3,712.00
Switch de 24 puertos 3COM	1	S/. 2,263.00
Switch baseline 24 puertos 3COM	1	S/. 2,648.41
Tester Kit electrónico de cables	1	S/. 845.00
Gabinete rack metálico con puertas de vidrio	4	S/. 3,120.00
Switch de 24 puertos 3COM	3	S/. 2,091.00
Switch de 8 puertos 3COM	1	S/. 1,044.00
Switch de 24 puertos 3COM	1	S/. 1,044.00
Central telefónica SAMSUNG	1	S/. 23,483.94
Sistema de alimentación ininterrumpida UPS – APC	1	S/. 624.00
Central telefónica para tres líneas	1	S/. 1,852.55
Tarjeta de expansión de líneas y ocho anexos	1	S/. 1,172.50
Tarjeta de expansión de tres líneas y ocho anexos	1	S/. 1,373.50
Teléfonos análogos	51	S/. 3,246.15
Gabinetes rack FAMETAL	3	S/. 550.50
Sistema de alimentación ininterrumpida UPS 2000	1	S/. 999.00
Modem externo DSL V.35	1	S/. 1,500.00
Switch de 24 puertos T “Autonegociable”	1	S/. 1,571.00
Sistema de alimentación ininterrumpida UPS	1	S/. 1,585.00
Switch de 24 puertos	2	S/. 2,690.00
Cable tester	1	S/. 483.00
Gabinete Rack MTS	1	S/. 550.00
Switch CISCO 2960 de 48 puertos	1	S/. 3,734.00
Central telefónica SAMSUNG OS7070	2	S/. 26,526.75
Access Point	2	S/. 210.00
Extractor de aire	2	S/. 358.00
Sistema de alimentación ininterrumpida UPS – Marca APC	3	S/. 984.00
Router de cuatro puertos	1	S/. 90.00
Modem-router de cuatro puertos	1	S/. 110.00
Switch de 24 puertos SATRA	1	S/. 264.00
TOTAL	93	S/. 90,725.30

Fuente: Oficina de Patrimonio - PELT
Elaboración: Propia

Software:

Tabla 12: Activos de red - Software

Activo	Cantidad	Costo total
Licencia de antivirus ESET CORPORATIVO	38	S/. 3,800.00
Sistema de Control de Asistencia	1	Desconocido
TOTAL	39	S/. 3,800.00

Fuente: Oficina de Patrimonio - PELT
Elaboración: Propia

Data:

Tabla 13: Activos de red – Data

Activo	Cantidad	Costo total
BD de bienes patrimoniales	1	Desconocido
BD de asistencia	1	Desconocido
BD SIAF	1	Desconocido
TOTAL	4	Desconocido

Elaboración: propia

Riesgos de seguridad

A continuación se señalan las amenazas a la red:

Tabla 14: Activos de red – Amenazas de seguridad

Ítem	Amenazas	Probabilidad
1	Infiltración de usuarios no autorizados en la red	Muy alta
2	Alteración, robo de información	Muy alta
3	Uso no autorizado a software y/o hardware	Muy alta
4	Uso indebido del ancho de banda	Muy alta
5	Acceso no autorizado a configuración de equipos informáticos	Alta
6	Manipulación no autorizada de los equipos de red	Media
7	No tomar ninguna acción de seguridad	Muy alta
8	No evaluar los riesgos continuamente.	Alta

Elaboración: Propia

Por lo tanto se plantean los siguientes requerimientos de seguridad:

Tabla 15: Requerimientos de seguridad

Ítem	Requerimientos de seguridad	Atención a riesgo
1	Autenticación de usuarios, mediante la implementación de políticas de seguridad en las capas 2 y 3	1, 2, 3, 5, 7
2	Segmentación de la red en comunidades de usuarios	2, 3, 5, 7
3	Implementación de Calidad de Servicio	4, 7
4	Implementación de listas de control de acceso	1, 3, 5
5	Ubicación segura de todos los equipos de red	6, 7

Elaboración: Propia

4.1.1.2. Identificar la red existente

La red es plana, no existen subredes o redes virtuales VLAN, su expansión resulta difícil de planificar e implementar, no cuenta con enlaces redundantes para garantizar la disponibilidad de rutas, no existe configuraciones de calidad de servicio, el throughput de los equipos de red es en algunos casos hasta el 10% del ancho de banda, no cuenta con políticas de seguridad, la implementación de nuevos switches significan mayor latencia y degradación del throughput.

4.1.1.2.1. Infraestructura de red

- La red está compuesta por switches de ocho (08) y veinticuatro (24) puertos Fast Ethernet ubicados en cada piso de los dos edificios.
- No cuenta con servidor proxy
- Existe solamente un dominio de broadcast lo cual afecta directamente al rendimiento de la red.

A continuación se muestra el detalle de comunidades de usuarios distribuidos en dos edificios:

Edificio A:

Tabla 16: Comunidad de usuarios y switches – Edificio A

Piso	Comunidad de usuarios /Oficinas	Número de switches
Primero	Oficina de Administración, Oficina de Abastecimientos, Oficina de Gestión Documentaria.	1
Segundo	Oficina de Contabilidad, Oficina de Personal, Oficina de Tesorería.	1
Tercero	Dirección Ejecutiva, Oficina de Presupuesto y Planificación, Data Center.	1
Cuarto	Oficina de Asesoría Legal, Dirección de Obras.	2
Quinto	Dirección de Estudios, Dirección de Obras, Oficina de Imagen Institucional.	2

Elaboración: Propia

Edificio B:

Tabla 17: Comunidad de usuarios y switches – Edificio B

Piso	Comunidad de Usuarios / Oficinas	Número de switches
Primero	Dirección de Desarrollo Agrícola y Medio Ambiente.	1
Segundo	Oficina de Imagen Institucional, Dirección de Obras, Oficina de Tecnologías de Información.	1
Tercero	Órgano de Control Interno, Dirección de Desarrollo Agrícola y Medio Ambiente, Oficina de Patrimonio.	1

Elaboración: Propia

Otros:

Tabla 18: Comunidad de usuarios y switches – Área libre

Piso	Comunidad de Usuarios / Oficinas	Número de switches
Primero	Auditorio	0
Primero	Dirección de Recursos Hidrobiológicos	0

Elaboración: Propia

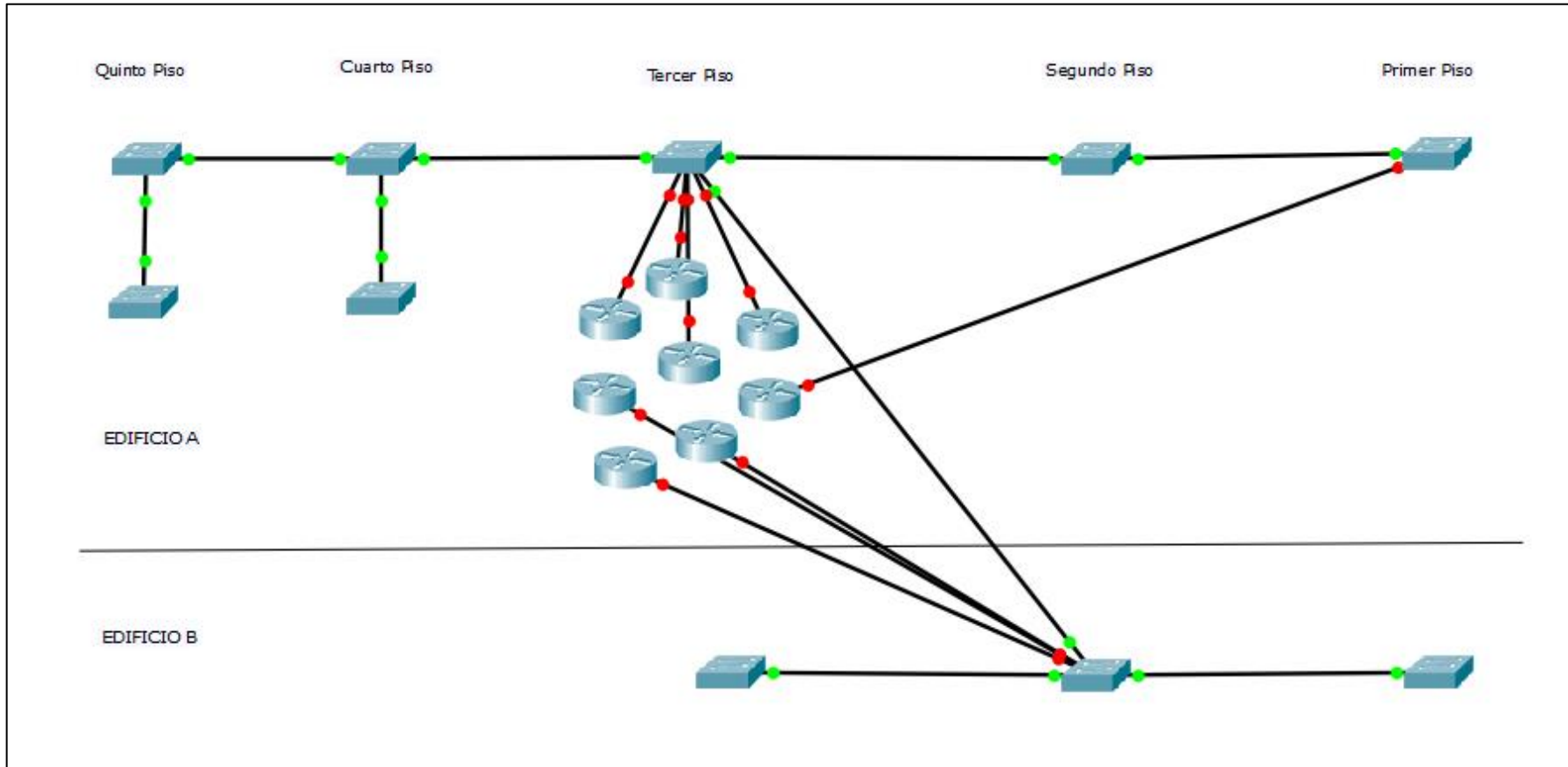


Figura 14: Topología LAN actual – Routers y Switches
Fuente: Cisco Packet Tracer
Elaboración: Propia

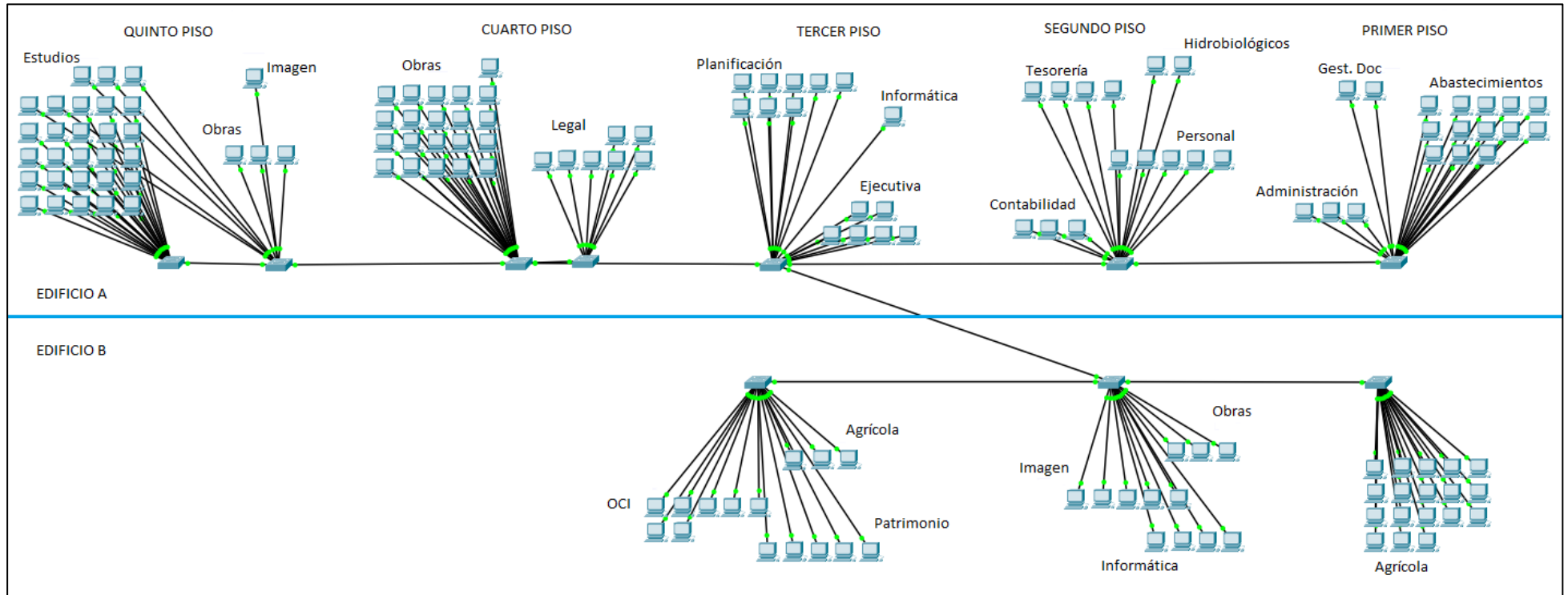


Figura 15: Topología LAN actual Switches y PCs
 Fuente: Cisco Packet Tracer
 Elaboración: Propia

4.1.1.2.2. Direccionamiento

El direccionamiento en toda la red es estático. Es preciso mencionar que no existen conexiones inalámbricas.

Nombramiento

La asignación de nombres a los dispositivos no tiene patrón definido, a continuación se presentan ejemplos:

- **Routers:**
 - 192.168.1.1
 - 192.168.1.2
 - 192.168.1.3
 - 192.168.1.4
 - 192.168.1.5
 - 192.168.1.6
 - 192.168.1.7
 - 192.168.1.8
- **Switches:**
 - Valor por defecto
- **Host:**
 - MARGARITA-PC
 - UPERPELT
 - 192.168.1.46
 - OBRAS1
 - Ventanilaa-PC
- **Servidores:**
 - De archivos: WindowServer

Protocolos:

Capa 1

- UTP categoría 5e
- UTP Categoría 6

Capa 2

- ARP
- Ethernet
- Fast Ethernet
- **Capa 3**
- Ruteo estático

Capa 4

- TCP/UDP

4.1.1.2.3. Salud de la red

Performance o rendimiento

Switches

- Edificio A – Primer piso

Ancho de banda: 100 Mbps

Throughput promedio: 94.557 Mbps

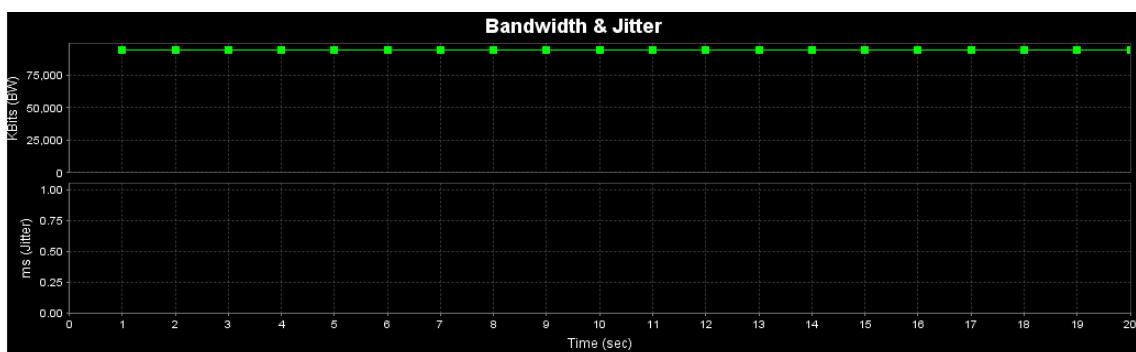


Figura 16: Ancho de banda Switch primer piso – Edificio A

Fuente: Reporte generado en Iperf

Elaboración: Propia

- Edificio A – Segundo piso

Ancho de banda: 100 Mbps

Throughput promedio: 94.381 Mbps

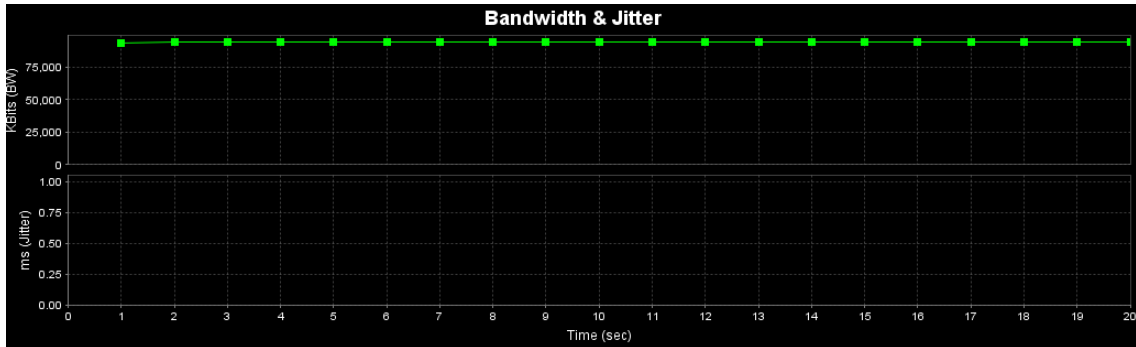


Figura 17: Ancho de banda Switch segundo piso – Edificio A

Fuente: Reporte generado en Iperf

Elaboración: Propia

- Edificio A – Tercer piso

Ancho de banda: 100 Mbps

Throughput promedio: 94.500 Mbps

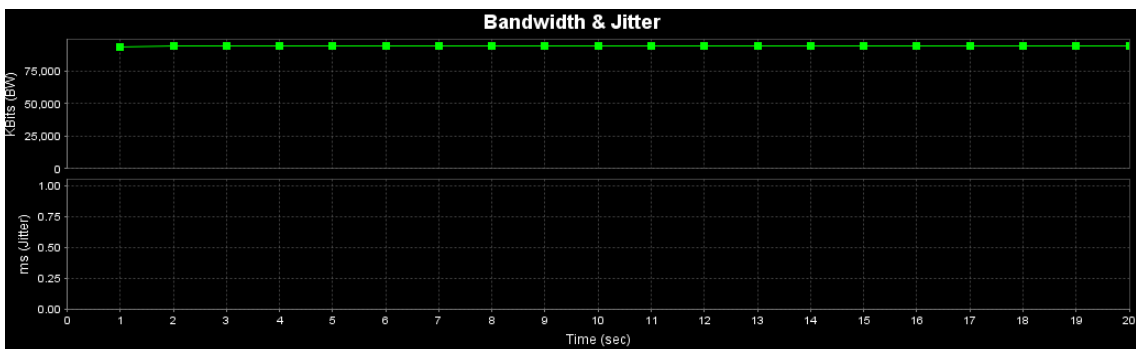


Figura 18: Ancho de banda Switch tercer piso – Edificio A

Fuente: Reporte generado en Iperf

Elaboración: Propia

- Edificio A – Cuarto piso

Ancho de banda: 100 Mbps

Throughput promedio: 94.481 Mbps

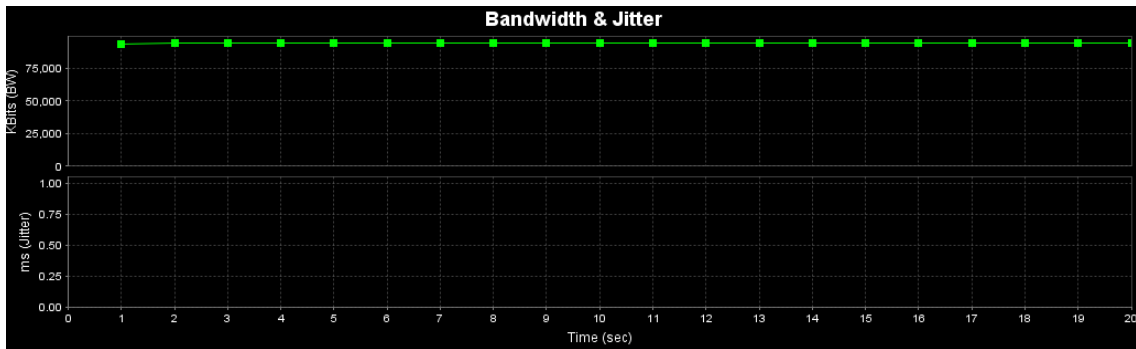


Figura 19: Ancho de banda Switch cuarto piso – Edificio A
 Fuente: Reporte generado en Iperf
 Elaboración: Propia

- Edificio A – Cuarto piso
- Ancho de banda: 100 Mbps
- Throughput promedio: 94.747 Mbps

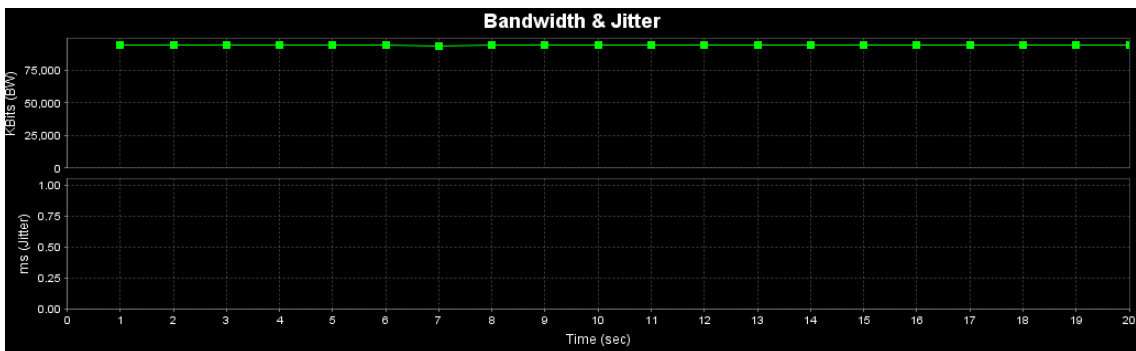


Figura 20: Ancho de banda Switch quinto piso – Edificio A
 Fuente: Reporte generado en Iperf
 Elaboración: Propia

- Edificio B – Primer piso
- Ancho de banda: 100 Mbps
- Throughput promedio: 94.548 Mbps

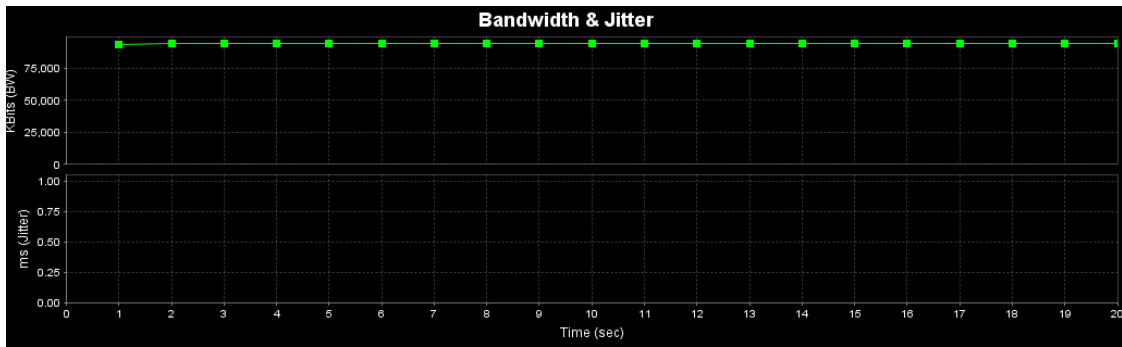


Figura 21: Ancho de banda Switch primer piso – Edificio B
Fuente: Reporte generado en Iperf
Elaboración: Propia

- Edificio A – Segundo piso

Ancho de banda: 100 Mbps

Throughput promedio: 7.582 Mbps

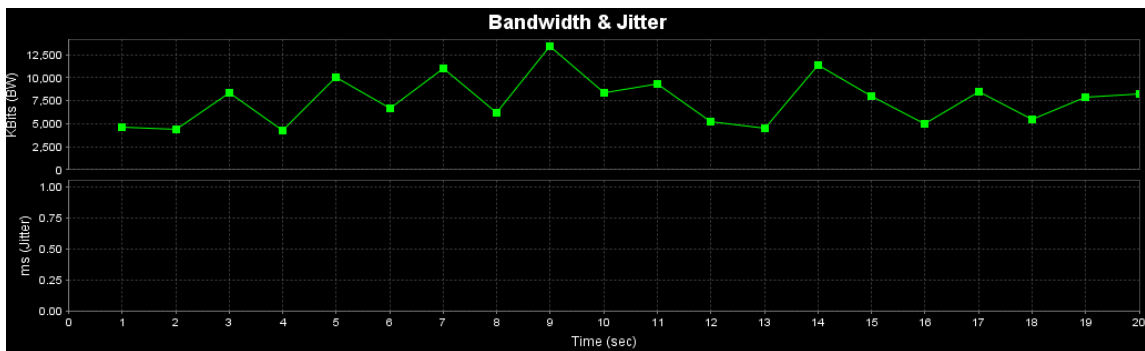


Figura 22: Ancho de banda Switch segundo piso – Edificio B
Fuente: Reporte generado en Iperf
Elaboración: Propia

- Edificio A – Tercer piso

Ancho de banda: 100 Mbps

Throughput promedio: 94.420 Mbps

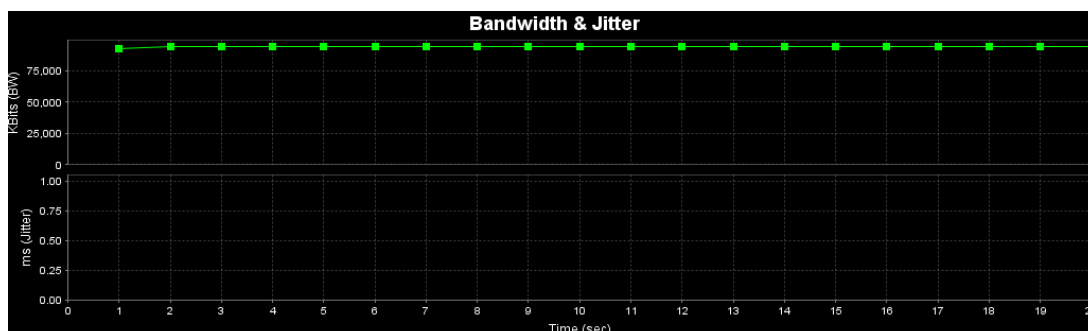


Figura 23: Ancho de banda Switch tercer piso – Edificio B
Fuente: Reporte generado en Iperf
Elaboración: Propia

4.1.1.2.4. Disponibilidad

No existe registro de fallas o errores de la red, sin embargo durante los periodos de recolección de información, ocurrieron dos fallas en la red, la medida tomada por el encargado de la oficina de TI fue reiniciar los switches, no se analizó la causa del error, pero solucionó el problema.

Diseño lógico

- La red es plana, no presenta redes virtuales o VLANs.
- El direccionamiento es estático en la red 192.168.1.0, las primeras ocho (08) direcciones se asignaron a los routers, las demás se asignaron de manera aleatoria a PCs, laptops, impresoras, todos poseen la máscara 255.255.255.0 tal como muestra la tabla siguiente:

Tabla 19: Direccionamiento de red

Estado	Equipo	Dirección IP	Máscara
Reservado	Modem	192.168.1.1	255.255.255.0
Reservado	Modem	192.168.1.2	255.255.255.0
Reservado	Modem	192.168.1.3	255.255.255.0
Reservado	Modem	192.168.1.4	255.255.255.0
Reservado	Modem	192.168.1.5	255.255.255.0
Reservado	Modem	192.168.1.6	255.255.255.0
Reservado	Modem	192.168.1.7	255.255.255.0
Reservado	Laptop	192.168.1.8	255.255.255.0
Desconocido	-	192.168.1.9	255.255.255.0
Activado	-	192.168.1.10	255.255.255.0
Desconocido	-	192.168.1.11	255.255.255.0
Activado	-	192.168.1.12	255.255.255.0
Activado	-	192.168.1.13	255.255.255.0
Activado	-	192.168.1.14	255.255.255.0

Elaboración: Propia

Diseño Físico

Topología

Estrella extendida

Dispositivos

Dispositivos de red

Los dispositivos de red que funcionan actualmente son:

Tabla 20: Dispositivos de red operativos

Ítem	Equipo	Marca	Número de puertos	Administrable	Ubicación
1	Switch	3COM	24	Si	Primer piso edificio B
2	Switch	3COM	24	Si	Segundo piso edificio B
3	Switch	3COM	24	Si	Tercer piso edificio B
4	Switch	3COM	24	Si	Primer piso Edificio A
5	Switch	3COM	24	Si	Segundo piso edificio A
6	Switch	CISCO	48	Si	Tercer Piso Edificio A
7	Switch	3COM	24	Si	Cuarto piso edificio A
8	Switch	3COM	8	No	Cuarto piso edificio A
9	Switch	3COM	24	Si	Quinto piso edificio A
10	Switch	SATRA	24	Si	Quinto piso Edificio A

Elaboración: Propia

Host o usuarios:

Tabla 21: Número de usuarios por comunidad

Ítem	Dirección / Oficina	Usuarios
1	Dirección de Estudios	28
2	Dirección de Obras	27
3	Dirección Ejecutiva	6
4	Dirección de Desarrollo Agrícola y Medio Ambiente	21
5	Dirección de Recursos Hidrobiológicos	2
6	OPP	8
7	Administración	3
8	Contabilidad	3
9	Abastecimientos	13
10	Asesoría Legal	7
11	OCI	6
12	Personal	5
13	Tesorería	4
14	Gestión Documentaria	2
15	Órgano de Control Interno	7
16	Oficina de Informática	5
17	Patrimonio	5
18	Usuarios temporales	10
	Total	162

Elaboración: Propia

Nuevamente se precisa, que la Oficina de Tecnologías de Información no cuenta con registro de usuarios y comunidades de usuarios.

Tecnologías LAN

Las tecnologías LAN que se encuentran funcionando:

- Fast Ethernet 100Mbps
- Ethernet 10Mbps

Cableado

El cableado Backbone y vertical es:

- Cobre: UTP categorías 5e y 6
- Marca: NEXXT
- Distancia máxima: 50m
- Conector: RJ45
- Los switches y routers también se conectan por el cable mencionado.

4.2. Diseño del modelo

4.2.1. Diseño lógico propuesto

4.2.1.1. Topología de red

Diseño jerárquico

De acuerdo a la metodología del “Diseño de redes Top-Down” se plantean las siguientes áreas

- Data center A: Donde se ubicarán el router, switches del edificio A, y los servidores.
- Data center B: Donde se ubicarán los switches del edificio B

- LAN: cuenta con el cableado y dispositivos finales de toda la red.

Por el tamaño de la entidad, la arquitectura de red jerárquica con modelo de núcleo colapsado, es decir, las capas de distribución y núcleo se combinan.

A continuación se muestra la topología del modelo propuesto:

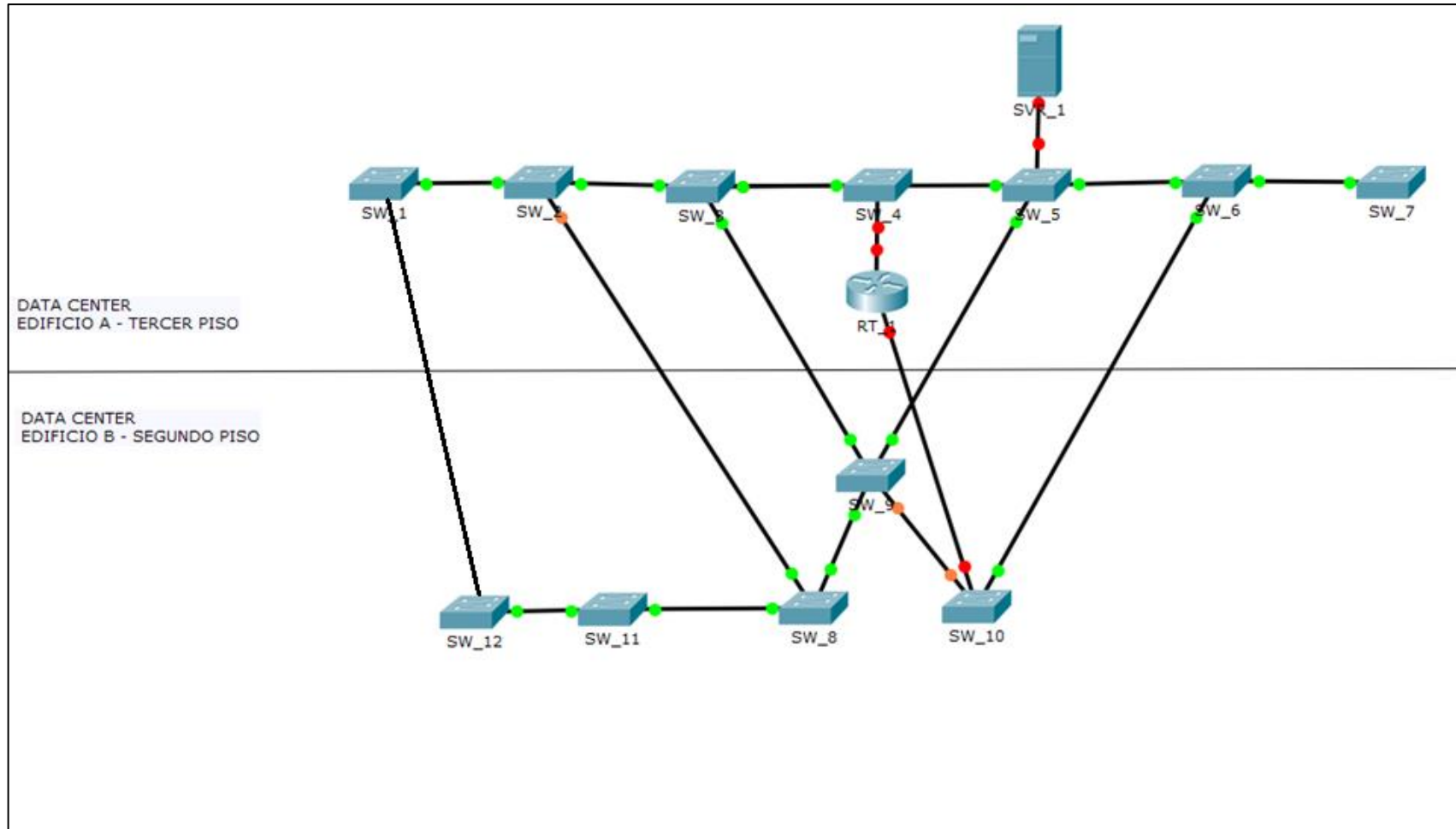


Figura 24: Topología de modelo – Switches y Router
 Fuente: Cisco Packet Tracer
 Elaboración: Propia

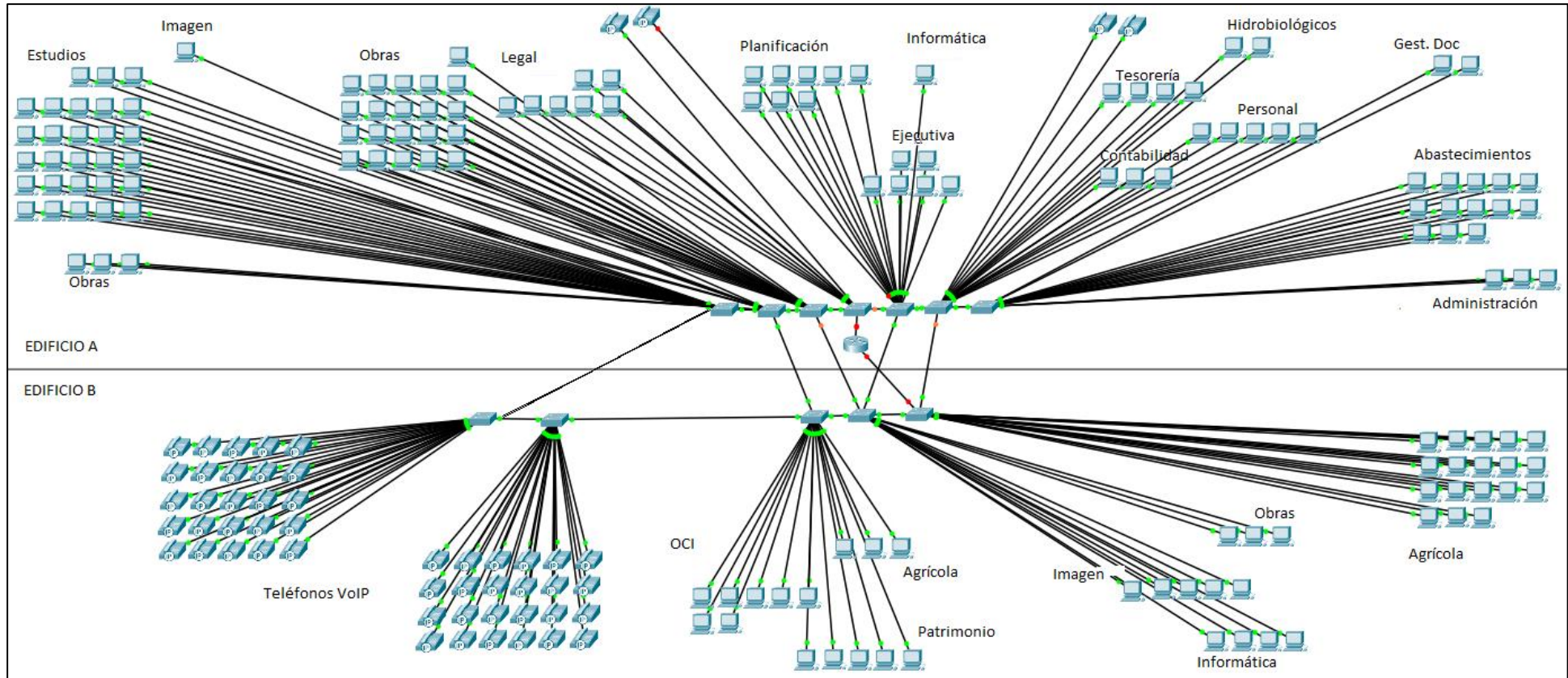


Figura 25: Topología de modelo – Switches y usuarios
 Fuente: Cisco Packet Tracer
 Elaboración: Propia

4.2.1.2. Direccionamiento

Para el direccionamiento, segmentación y creación de VLANs se considerarán las comunidades de usuarios es decir cada Oficina o Dirección:

- Dirección de Estudios.
- Dirección de Obras.
- Dirección Ejecutiva
- Dirección de Desarrollo Agrícola y Medio Ambiente
- Dirección de Recursos Hidrobiológicos
- Oficina de Presupuesto y Planificación
- Oficina de Administración
- Oficina de Contabilidad
- Oficina de Abastecimientos
- Oficina de Asesoría Legal
- Oficina de Imagen Institucional
- Oficina de Personal
- Oficina de Tesorería
- Oficina de Gestión Documentaria
- Órgano de Control Institucional
- Oficina de Informática
- Oficina de Patrimonio

4.2.1.3. Estructura del modelo

De acuerdo al documento RFC 1918 que especifica las “Mejores prácticas actuales” para el direccionamiento, se utilizará el bloque de direcciones privadas clase C y se realizará el subneteo en concordancia con las necesidades de la entidad:

Red a utilizar: 192.168.0.0

Tabla 22: Direccionamiento IP – Modelo

192	168	0	0
Bloque 1	Bloque 2	Bloque 3	Bloque 4

Elaboración: Propia

Bloque 1 y 2: Prefijo de red clase C

- Único valor 192.168.

Bloque 3: Identificador de comunidad de usuarios

Número máximo de comunidades: 256

Las comunidades son:

- 1: Dirección de Estudios
- 2: Dirección de Obras
- 3: Dirección Ejecutiva
- 4: Dirección de Desarrollo Agrícola y Medio Ambiente
- 5: Dirección de Recursos Hidrobiológicos
- 6: Presupuesto y Planificación
- 7: Administración
- 8: Contabilidad

- 9: Abastecimientos
- 10: Asesoría Legal
- 11: Imagen Institucional
- 12: Personal
- 13: Tesorería
- 14: Gestión Documentaria
- 15: Órgano de Control Interno
- 16: Informática
- 17: Patrimonio
- 18: Usuarios temporales
- 19: Servidores
- 20: Datacenter

Bloque 4: Identificador de host

- Número máximo de bits para host: 8
- Número máximo de host: 254

Máscara de red: Número variable según la cantidad de host necesarios.

Detalle de segmentos:

La cantidad de usuarios en cada comunidad es:

Tabla 23: Comunidad de usuarios

Subred	Dirección / Oficina	Usuarios
1	Dirección de Estudios	28
2	Dirección de Obras	27
3	Dirección Ejecutiva	6
4	Dirección de Desarrollo Agrícola y Medio Ambiente	21
5	DRH	2
6	OPP	8
7	Administración	3
8	Contabilidad	3
9	Abastecimientos	13
10	Asesoría Legal	7
11	Imagen Institucional	6
12	Personal	5
13	Tesorería	4
14	Gestión Documentaria	2
15	Órgano de Control Interno	7
16	Informática	5
17	Patrimonio	5
18	Usuarios temporales	10
19	Servidores	4
20	Datacenter	11
21	Teléfonos	52
	Total	214

Elaboración propia

4.2.1.4. VLAN

Se asignó una VLAN de rango normal por cada subred.

A continuación se detalla las comunidades de usuarios, número de usuarios, VLANs y dirección de red.

Tabla 24: Comunidad de usuarios – VLANs – Dirección IP

Ítem	Oficina o Dirección	Us	Max Us	Nombre de VLAN	ID de VLAN	Dirección de red
1	Dirección de Estudios	28	62	ADM_DES	2	192.168.1.0/26
2	Dirección de Obras	27	62	ADM_DO	3	192.168.2.0/26
3	Dirección Ejecutiva	6	14	ADM_DE	4	192.168.3.0/28
4	Dirección de Desarrollo Agrícola y Medio Ambiente	21	30	ADM_DDAYMA	5	192.168.4.0/27
5	Dirección de Recursos Hidrobiológicos	2	6	ADM_DRH	6	192.168.5.0/29
6	Oficina de Presupuesto y Planificación	8	14	ADM_OPP	7	192.168.6.0/28
7	Administración	3	14	ADM_ADM	8	192.168.7.0/28
8	Contabilidad	3	14	ADM_CONT	9	192.168.8.0/28

9	Abastecimien tos	13	30	ADM_ABAST	10	192.168.9.0/27
10	Asesoría Legal	7	14	ADM_LEGAL	11	192.168.10.0/28
11	Oficina de Imagen Institucional	6	14	ADM_IMAG	12	192.168.11.0/28
12	Personal	5	14	ADM_PER	13	192.168.12.0/28
13	Tesorería	4	14	ADM_TES	14	192.168.13.0/28
14	Gestión Documentari a	2	6	ADM_GD	15	192.168.14.0/29
15	Órgano de Control Interno	7	14	ADM_OCI	16	192.168.15.0/28
16	Oficina de Informática	5	14	ADM_TI	17	192.168.16.0/28
17	Patrimonio	5	14	ADM_PAT	18	192.168.17.0/28
18	Usuarios temporales	10	30	ADM_TMP	19	192.168.18.0/27
19	Servidores	4	14	MGMT_SERV	20	192.168.19.0/28
20	Datacenter	11	30	MGMT_DATA	21	192.168.20.0/27
21	Teléfonos	52	52	ADM_VOIP	22	192.168.21.0

Elaboración: Propia

4.2.1.5. Direccionamiento

Estático: Se realizó direccionamiento estático, debido al control necesario los primeros meses de puesta en marcha y mientras se implementa el servidor DHCP.

Nombramiento:

Modelo de VLAN

Los nombres de las VLANs son referencias de acuerdo a su función principal y el nombre de la dirección u oficina:

Función

- ADM: Administrativa
- MGMT: Administración

Nombre de la dirección u oficina

- DE: Dirección Ejecutiva
- DO: Dirección de Obras
- TES: Tesorería
- DATA: Datacenter

Nombre de VLAN: ADM_DE, MGMT_DATA

Modelo de dispositivo de red

Se dispuso asignar un nombre de acuerdo al tipo de dispositivo, edificio en el que se ubica y número correlativo.

- SW: Switch
- RT: Router

Nombre de dispositivo: SW_A_1, SW_B_1

Modelo de servidores

Se nombraron con el prefijo SVR y número correlativo:

Nombre de servidor: SVR_1

Protocolos:

Switching

- **Etiquetado de tramas**
 - IEEE 802.1q
- **Prevención de loops**
 - IEEE 802.1w
- **Seguridad**
 - Implementación de ACL por VLAN
- **Calidad de servicio**
 - IEEE 802.1p

4.2.1.6. Seguridad

Políticas

Se implementaron políticas de seguridad de la siguiente manera:

- **Capa 2:**
 - ACL: Filtrado de paquetes a través de filtro de MAC Address mediante VLAN.
 - MAC Address: Solamente una dirección MAC se puede conectar a un dispositivo, de lo contrario el puerto afectado se apagará y se dispara un evento logs.
- **Capa 3:**
 - ACL: Filtrado de paquetes determinado por dirección de IP origen y destino.

4.2.1.7. Calidad de Servicio QoS

Mediante la configuración de Voice VLAN, se configura la preferencia al tráfico de voz y no al de datos.

4.2.2. Diseño Físico

4.2.2.1. Diseño

Topología: Árbol

Jerárquico: Se delimitan claramente las capas Core-Distribución y Acceso.

Redundancia:

Se implementaron 4 enlaces redundantes, con lo cual el diámetro de red máximo es: 5

Seguridad:

- Ambos data centers se encuentran protegidos en ambientes aislados.
- Los gabinetes de los dispositivos de red también están protegidos en gabinetes bajo llave.

Mantenimiento:

- Físico: Cada tres meses se realizará limpieza de los data centers, dispositivos de red.
- Lógico: Se instalarán las actualizaciones de software de todos los equipos de red.

4.2.2.2. Cableado LAN

Tipo de cables

Tanto en las capas Core-Distribución y Acceso se utilizará el medio de conexión de cobre:

- Cable UTP categoría 6
- Distancia máxima: 90 metros
- Conectores: RJ45

4.2.2.3. Dispositivos

Tecnología

LAN

- Fast Ethernet BaseT
- Gigabit Ethernet BaseT

Características

A continuación se detallan las características de los equipos de red:

Equipo Core – Distribución: Router 2911

- Interfaces: Tres (03) puertos Gigabit full dúplex con conector RJ45, dos puertos de consola RJ45 y mini USB, Un puerto serial.
- Memoria RAM 512 MB ampliable a 2GB
- Memoria Flash de 256 MB ampliable a 4 GB
- Tasa de reenvío 31 Gbps

Equipos de Acceso: Cisco Catalyst 2960-X Series

- Interfaces: Veinticuatro (24) puertos FastEthernet PoE, Dos (02) puertos Gigabit, ambos de conectores RJ45 y full dúplex.
- Memoria RAM 512 MB
- Memoria Flash de 128MB
- Tasa de reenvío de 106 Gbps

A continuación se muestra tabla con lista de equipos implementados:

Tabla 25: Equipos de red - Modelo

Capa	Equipo	Cantidad	Adm	Puertos
Core - Distribución	Router CISCO 2911	1	Si	3
Acceso	Switch CISCO Catalyst 2960-X series	10	Si	26

Elaboración: Propia

4.2.2.4. Configuración de equipos

La configuración de los equipos de red se realizó mediante la interface de línea de comando de Cisco, la cual se puede ver detalladamente en el anexo 2.

4.3. Simular y evaluar el modelo

4.3.1. Simulación y evaluación

Utilizando el instrumento electrónico Packet Tracer de Cisco, se simuló el modelo, logrando obtener los siguientes datos:

Escalabilidad

Debido a que el diseño se basa en un modelo jerárquico de núcleo colapsado, en el cual la capa de distribución y núcleo se combinan, la escalabilidad se puede implementar fácilmente, sin afectar el rendimiento de la red.

Plan de expansión

De acuerdo a los datos obtenidos en el análisis, se proyectó el crecimiento a 244 usuarios para el año 2021, el modelo abastece a 270 usuarios, cantidad que cubre la proyección.

Así mismo, se registraron las direcciones IP de cada usuario y también se consideró el crecimiento en cada comunidad de usuarios, tal como se puede apreciar en la tabla 24.

Direccionamiento

Se crearon veintiún (21) sub redes para cada comunidad de usuarios. Ver tabla 24.

Disponibilidad

Tomando en cuenta los requerimientos de disponibilidad y costo de fuera de servicio, se eliminó la sobreutilización de dos enlaces y se agregaron cinco (05) enlaces redundantes. Con lo cual se obtiene un máximo diámetro de red igual a cinco (05).

Ancho de banda

- Los dispositivos de red soportan 100 y 1000 Mbps, lo cual es 10 y 100 veces más rápido que la red actual.
- Se redujo el tráfico de red respecto al protocolo ARP, mediante la segmentación en redes para cada comunidad de usuarios.

Latencia

Packet Tracer limita las funcionalidades del programa ping, pero se logró disminuir la latencia en cualquier segmento de red a un promedio de 3.3 ms, una latencia máxima de 11ms y mínima de 1ms, con una variabilidad pequeña de 2.74ms, esto quiere decir que la latencia disminuye a casi el 1% de lo registrado en la red actual, tal como muestra la siguiente figura:

LatenciaMáximaModelo					
<i>Etiqueta de Valor</i>	<i>Valor</i>	<i>Frecuencia</i>	<i>Porcentaje</i>	<i>Porcentaje Válido</i>	<i>Porcentaje Acumulado</i>
	1.00	7	35.00	35.00	35.00
	2.00	3	15.00	15.00	50.00
	3.00	1	5.00	5.00	55.00
	4.00	5	25.00	25.00	80.00
	5.00	2	10.00	10.00	90.00
	9.00	1	5.00	5.00	95.00
	11.00	1	5.00	5.00	100.00
<i>Total</i>		20	100.0	100.0	

LatenciaMáximaModelo		
<i>N</i>	<i>Válido</i>	20
	<i>Perdidos</i>	0
<i>Media</i>		3.30
<i>Desv Std</i>		2.74
<i>Mínimo</i>		1.00
<i>Máximo</i>		11.00

Figura 26: Frecuencias del promedio de latencia máxima – Modelo

Fuente: Tabla generada en PSPP

Elaboración: Propia

Para evaluar estadísticamente al indicador más importante se utilizó la “prueba t”, tal como sigue:

Hipótesis nula: La latencia del modelo es la misma a la de la red actual.

Hipótesis alterna: La latencia en el modelo disminuye significativamente.

De la comparación de medias para muestras emparejadas se tiene:

Estadísticas de muestras emparejadas					
		Media	N	Desviación Estándar	Err.Est.Medía
Pareja 1	LatenciaMáxima	329.15	20	234.48	52.43
	LatenciaMáximaModelo	3.30	20	2.74	.61

Correlaciones de muestras emparejadas				
		N	Correlación	Sign.
Pareja 1	LatenciaMáxima & LatenciaMáximaModelo	20	-.11	.643

Prueba de muestras emparejadas									
		Diferencias emparejadas					t	df	Sign. (2-colas)
		Media	Desviación Estándar	Error Est. Media	Intervalo de confianza 95% de la Diferencia				
					Inferior	Superior			
Pareja 1	LatenciaMáxima - LatenciaMáximaModelo	325.85	234.79	52.50	215.96	435.74	6.21	19	.000

Figura 27: Prueba T – Promedios de latencia máxima
Fuente: Tabla generada en PSPP
Elaboración: Propia

Interpretación:

El promedio de latencia máxima en el modelo es de 3.30 ms y en la red actual es 329.15 ms, lo cual indica una reducción importante.

La prueba t indica que existe diferencias significativas entre los promedios de latencia máxima ($t= 6.21$, grados de libertad = 19), por lo tanto, se rechaza la hipótesis nula con un grado de confianza del 99.9% ($sign < 0.001$), ya que la latencia se reduce significativamente en el modelo propuesto.

Seguridad

- Como se observa en la figura 24, los equipos de red son resguardados en dos Data Centers ubicados en el tercer piso del edificio A y el segundo piso del Edificio B.
- Se segmentó la red en veintiún (21) sub redes de acuerdo a la comunidad de usuarios.
- Se implementaron listas de control de acceso.

- Se atendieron todos los requerimientos de información, con lo cual se minimiza el riesgo de seguridad.

En la tabla siguiente se visualizan las diferencias entre la red actual y el modelo:

Tabla 26: Comparación de red actual y modelo

Indicador	Red actual	Modelo	Diferencia
Ancho de banda de los equipos.	10 – 100 Mbps	100 – 1000 Mbps	90 – 900 Mbps
Throughput	7.5 – 94.7 Mbps	98 – 996 Mbps	90.5 – 901.3 Mbps
Promedio de latencia máximo	329.15 ms	3.30 ms	325.85 ms
Segmentos de red	1	21	20
VLANs	0	21	21
Número de fallas en la red (por mes)	2	0	2
Número de dispositivos que cruza un paquete (Diámetro de red)	6	5	1
Interfaces o puertos de red disponibles	32	56	24
Direcciones IP disponibles	92	59182	59090
Diseño de red	No existe	Si existe	Si existe
Identificación de tipos de paquetes	No existe	Si existe	Si existe
Priorización del ancho de banda	No existe	Si existe	Si existe
Enlaces redundantes	0	5	5
Listas de control de acceso	No existen	Si existen	Si existen
Resguardo de equipos y medios de red	Si	No	Si

Fuente: Elaboración propia

CONCLUSIONES

PRIMERA

Se diseñó un modelo jerárquico que proyecta mejorar el rendimiento de red, mediante la implementación de políticas de seguridad, mecanismos y configuración de equipos que dan como resultado una red escalable, disponible y segura.

SEGUNDA

El rendimiento de la red de área local del Proyecto Especial Lago Titicaca, sede central Puno – 2016, se ve reducido a más del 10% debido a la incorrecta configuración de equipos, no existe una administración eficiente de interfaces de red, direccionamiento IP y ancho de banda contratado, se sobre utilizan enlaces de red, se sobrecarga la red con tráfico innecesario del protocolo ARP, el promedio de latencia es de 329.15ms y existen ocho (08) riesgos de seguridad no atendidos.

TERCERA

Se diseñó un modelo que soporta la transmisión de voz y datos, cuenta con redes virtuales VLAN, priorización del ancho de banda, políticas de seguridad, mapeo de usuarios y direcciones IP, segmentación de redes, cubre la proyección de usuarios de los próximos cinco (05) años, minimiza los riesgos de seguridad y utiliza eficazmente el ancho de banda.

CUARTA

Se simuló el modelo utilizando la aplicación PacketTracer, en el cual se configuraron los equipos de red y las PC, se aumentó el ancho de banda de los equipos hasta en 900Mbps, se agregaron cinco (05) enlaces redundantes, se priorizó el ancho de banda, así mismo se aumentó la capacidad de direcciones IP en 59090, se redujeron los riesgos de seguridad y mediante la “prueba t”, se demostró la disminución significativa del promedio de latencia máximo, con un grado de confiabilidad del 99.9%.

SUGERENCIAS

PRIMERA

Implementar el modelo siguiendo detalladamente los pasos indicados, con el objetivo de mejorar el rendimiento y coadyuvar al logro de los objetivos institucionales.

SEGUNDA

Se sugiere considerar el modelo antes de realizar gastos en compra de equipos o contratación de servicios relacionados a la red de datos.

TERCERA

Una vez implementado el modelo, se sugiere a la nueva administración de la entidad, gestionar el enlace con la red del Ministerio de Agricultura y Riego, para hacer mejor uso de la aplicación de Gestión Documentaria e innovar con la comunicación rápida y segura vía video conferencias.

CUARTA

A los nuevos investigadores se sugiere utilizar herramientas que permitan analizar el tráfico de red de manera individual, es decir el que genera cada usuario de la red de datos, esto para sustentar cambios en la configuración base.

BIBLIOGRAFÍA

- Atelin , P., & Dordoigne, J. (2006). *Redes informáticas: conceptos fundamentales : normas, arquitectura, modelo OSI, TCP/IP, Ethernet, Wi-Fi...* Ediciones ENI.
- Barceló Ordinas, J. M., & Peig Olivé, E. (s.f.). *Redes de área local - Topologías y políticas de control de acceso al medio*. UOC.
- Caprile, S. (2009). *Equisbí: Desarrollo de aplicaciones con comunicación remota basadas en módulos ZigBee y 802.15.4*. Buenos Aires: Gran Aldea.
- Cisco. (2008). *Internetworking Technology Handbook*. Recuperado el 01 de junio de 2016, de http://www.cisco.com/en/US/docs/internetworking/technology/handbook/ito_doc.html
- Definicion.de*. (2016). Recuperado el 20 de mayo de 2016, de <http://definicion.de/modelo/>
- Flores, G. (07 de octubre de 2008). *Redes Web.com*. Recuperado el 31 de mayo de 2016, de <http://gehovani.blogspot.pe/2008/10/modelo-de-3-capas-de-modelo-jerrquico.html>
- Herrera Perez, E. (2003). *Tecnologías y redes de transmisión de datos*. Mexico: Limusa/Noriega.
- Íñigo Griera, J., Barceló Ordinas, J. M., Cerdà Alabern, L., Peig Olivé, E., Abella i Fuentes, J., & Corral i Torruella, G. (2009). *Estructuras de redes de computadores*. Barcelona: UOC.
- Luis R. (28 de noviembre de 2008). *IP reference*. Recuperado el 31 de mayo de 2016, de <https://ipref.wordpress.com/2008/11/28/modelo-jerarquico-de-red/>
- Mejía Mesa, A. (2005). *Guía práctica para manejar y reparar el computador*. Medellín: Panamericana Formas e Impresos.
- Microsoft*. (29 de noviembre de 2013). Recuperado el 25 de mayo de 2016, de <https://support.microsoft.com/es-es/kb/103884>
- Oppenheimer, P. (2004). *Top-down network design*. Indianápolis: Cisco Press.
- Seiffe, S. (15 de abril de 2013). *Introducción a la Ingeniería*. Recuperado el 20 de mayo de 2016, de <https://introaingenieria.wordpress.com/2013/04/15/modelos/>
- Stallings, W. (2000). *Comunicacion y redes de computadoras*. Mexico: Editorial Pearson Education.

Tolosa, G. (2014). *Protocolos y Modelos OSI*. Recuperado el 25 de mayo de 2016, de <http://www.tyr.unlu.edu.ar/TYR-publica/02-Protocolos-y-OSI.pdf>

Valentine, M., & Whitaker, A. (2008). *CCNA Exam Cram (Exam 640-802)*. Pearson IT Certification.

Wikipedia . (28 de mayo de 2016). Recuperado el 02 de junio de 2016, de VLAN: <https://es.wikipedia.org/wiki/VLAN>

Wikipedia. (17 de mayo de 2016). Recuperado el 25 de mayo de 2016, de https://es.wikipedia.org/wiki/Modelo_OSI#cite_note-OSI-1

Cisco Systems y Oppenheimer, (2011). *Top-Down Network Design*. 3a ed. United State of America: Cisco Press

ANEXOS

ANEXO 1: REPORTE DE PROGRAMA PING

Respuesta desde 192.168.1.2: bytes=32 tiempo<1m TTL=64
Respuesta desde 192.168.1.3: bytes=32 tiempo=1ms TTL=64
Respuesta desde 192.168.1.4: bytes=32 tiempo=2ms TTL=128
Respuesta desde 192.168.1.5: bytes=32 tiempo<1m TTL=64
Respuesta desde 192.168.1.6: bytes=32 tiempo=1ms TTL=64
Respuesta desde 192.168.1.7: bytes=32 tiempo<1m TTL=64
Respuesta desde 192.168.1.12: bytes=32 tiempo<1m TTL=64
Respuesta desde 192.168.1.13: bytes=32 tiempo=1ms TTL=128
Respuesta desde 192.168.1.14: bytes=32 tiempo<1m TTL=128
Respuesta desde 192.168.1.15: bytes=32 tiempo<1m TTL=128
Respuesta desde 192.168.1.16: bytes=32 tiempo<1m TTL=128
Respuesta desde 192.168.1.18: bytes=32 tiempo<1m TTL=128
Respuesta desde 192.168.1.20: bytes=32 tiempo<1m TTL=128
Respuesta desde 192.168.1.21: bytes=32 tiempo=1ms TTL=128
Respuesta desde 192.168.1.22: bytes=32 tiempo=2ms TTL=128
Respuesta desde 192.168.1.24: bytes=32 tiempo<1m TTL=128
Respuesta desde 192.168.1.26: bytes=32 tiempo<100m TTL=64
Respuesta desde 192.168.1.29: bytes=32 tiempo=1ms TTL=128
Respuesta desde 192.168.1.30: bytes=32 tiempo=3ms TTL=128
Respuesta desde 192.168.1.34: bytes=32 tiempo<5m TTL=128
Respuesta desde 192.168.1.38: bytes=32 tiempo=2ms TTL=255
Respuesta desde 192.168.1.40: bytes=32 tiempo=6ms TTL=128
Respuesta desde 192.168.1.43: bytes=32 tiempo<6m TTL=255
Respuesta desde 192.168.1.51: bytes=32 tiempo=4ms TTL=128
Respuesta desde 192.168.1.53: bytes=32 tiempo=8ms TTL=128
Respuesta desde 192.168.1.54: bytes=32 tiempo=8ms TTL=128
Respuesta desde 192.168.1.55: bytes=32 tiempo=8ms TTL=128
Respuesta desde 192.168.1.58: bytes=32 tiempo<8m TTL=128
Respuesta desde 192.168.1.63: bytes=32 tiempo<8m TTL=128
Respuesta desde 192.168.1.64: bytes=32 tiempo=6ms TTL=128
Respuesta desde 192.168.1.65: bytes=32 tiempo<6m TTL=128
Respuesta desde 192.168.1.66: bytes=32 tiempo=5ms TTL=128
Respuesta desde 192.168.1.67: bytes=32 tiempo=13ms TTL=128
Respuesta desde 192.168.1.70: bytes=32 tiempo<250m TTL=64
Respuesta desde 192.168.1.71: bytes=32 tiempo=31ms TTL=128
Respuesta desde 192.168.1.73: bytes=32 tiempo<378m TTL=64
Respuesta desde 192.168.1.77: bytes=32 tiempo<1m TTL=128
Respuesta desde 192.168.1.84: bytes=32 tiempo=142ms TTL=64
Respuesta desde 192.168.1.85: bytes=32 tiempo<300m TTL=64
Respuesta desde 192.168.1.87: bytes=32 tiempo<350m TTL=64
Respuesta desde 192.168.1.88: bytes=32 tiempo=298ms TTL=64
Respuesta desde 192.168.1.89: bytes=32 tiempo=1ms TTL=128
Respuesta desde 192.168.1.90: bytes=32 tiempo=1ms TTL=64
Respuesta desde 192.168.1.92: bytes=32 tiempo=250ms TTL=64
Respuesta desde 192.168.1.94: bytes=32 tiempo<1m TTL=128
Respuesta desde 192.168.1.95: bytes=32 tiempo<1m TTL=128
Respuesta desde 192.168.1.98: bytes=32 tiempo<1m TTL=64
Respuesta desde 192.168.1.100: bytes=32 tiempo=1ms TTL=128
Respuesta desde 192.168.1.101: bytes=32 tiempo<1m TTL=64
Respuesta desde 192.168.1.102: bytes=32 tiempo<1m TTL=128
Respuesta desde 192.168.1.103: bytes=32 tiempo<1m TTL=128
Respuesta desde 192.168.1.104: bytes=32 tiempo<1m TTL=128
Respuesta desde 192.168.1.105: bytes=32 tiempo<1m TTL=255
Respuesta desde 192.168.1.107: bytes=32 tiempo<1m TTL=128
Respuesta desde 192.168.1.108: bytes=321 tiempo<1m TTL=64
Respuesta desde 192.168.1.110: bytes=243 tiempo<177ms TTL=64
Respuesta desde 192.168.1.111: bytes=312 tiempo=2ms TTL=64
Respuesta desde 192.168.1.112: bytes=372 tiempo<1m TTL=64

Respuesta desde 192.168.1.114: bytes=311 tiempo=1ms TTL=64
Respuesta desde 192.168.1.116: bytes=233 tiempo=1ms TTL=64
Respuesta desde 192.168.1.117: bytes=230 tiempo=1ms TTL=64
Respuesta desde 192.168.1.121: bytes=201 tiempo<1m TTL=64
Respuesta desde 192.168.1.123: bytes=329 tiempo<1m TTL=64
Respuesta desde 192.168.1.124: bytes=300 tiempo=1ms TTL=64
Respuesta desde 192.168.1.125: bytes=32 tiempo=1ms TTL=128
Respuesta desde 192.168.1.126: bytes=32 tiempo=3ms TTL=128
Respuesta desde 192.168.1.128: bytes=32 tiempo<1m TTL=128
Respuesta desde 192.168.1.129: bytes=32 tiempo=3ms TTL=128
Respuesta desde 192.168.1.130: bytes=32 tiempo=1ms TTL=128
Respuesta desde 192.168.1.135: bytes=32 tiempo=1ms TTL=128
Respuesta desde 192.168.1.137: bytes=32 tiempo=1ms TTL=128
Respuesta desde 192.168.1.140: bytes=32 tiempo=253ms TTL=128
Respuesta desde 192.168.1.141: bytes=32 tiempo<1m TTL=255
Respuesta desde 192.168.1.143: bytes=32 tiempo=10ms TTL=128
Respuesta desde 192.168.1.148: bytes=32 tiempo=2ms TTL=128
Respuesta desde 192.168.1.151: bytes=32 tiempo=1ms TTL=128
Respuesta desde 192.168.1.153: bytes=32 tiempo<1m TTL=128
Respuesta desde 192.168.1.154: bytes=32 tiempo=1ms TTL=128
Respuesta desde 192.168.1.156: bytes=32 tiempo<1m TTL=128
Respuesta desde 192.168.1.157: bytes=32 tiempo<1m TTL=128
Respuesta desde 192.168.1.163: bytes=32 tiempo=195ms TTL=64
Respuesta desde 192.168.1.165: bytes=32 tiempo<255ms TTL=64
Respuesta desde 192.168.1.167: bytes=32 tiempo<288ms TTL=64
Respuesta desde 192.168.1.169: bytes=32 tiempo<325ms TTL=64
Respuesta desde 192.168.1.172: bytes=32 tiempo=522 TTL=64
Respuesta desde 192.168.1.175: bytes=32 tiempo<644m TTL=64
Respuesta desde 192.168.1.179: bytes=32 tiempo=2ms TTL=53
Respuesta desde 192.168.1.182: bytes=32 tiempo=1ms TTL=128
Respuesta desde 192.168.1.183: bytes=32 tiempo=1ms TTL=128
Respuesta desde 192.168.1.184: bytes=32 tiempo=6ms TTL=128
Respuesta desde 192.168.1.187: bytes=32 tiempo=1ms TTL=128
Respuesta desde 192.168.1.189: bytes=32 tiempo=1ms TTL=128
Respuesta desde 192.168.1.192: bytes=32 tiempo=1ms TTL=64
Respuesta desde 192.168.1.193: bytes=32 tiempo=1ms TTL=128
Respuesta desde 192.168.1.194: bytes=32 tiempo<1m TTL=128
Respuesta desde 192.168.1.195: bytes=32 tiempo<199ms TTL=64
Respuesta desde 192.168.1.197: bytes=32 tiempo=173ms TTL=64
Respuesta desde 192.168.1.199: bytes=32 tiempo=2ms TTL=128
Respuesta desde 192.168.1.200: bytes=32 tiempo<1m TTL=128
Respuesta desde 192.168.1.201: bytes=32 tiempo=6ms TTL=128
Respuesta desde 192.168.1.202: bytes=32 tiempo<1m TTL=128
Respuesta desde 192.168.1.204: bytes=32 tiempo<1m TTL=128
Respuesta desde 192.168.1.206: bytes=32 tiempo=5ms TTL=128
Respuesta desde 192.168.1.207: bytes=32 tiempo<1m TTL=128
Respuesta desde 192.168.1.211: bytes=32 tiempo=1ms TTL=128
Respuesta desde 192.168.1.212: bytes=32 tiempo=1ms TTL=128
Respuesta desde 192.168.1.213: bytes=32 tiempo<1m TTL=128
Respuesta desde 192.168.1.214: bytes=32 tiempo<1m TTL=128
Respuesta desde 192.168.1.216: bytes=32 tiempo<1m TTL=128
Respuesta desde 192.168.1.217: bytes=32 tiempo<1m TTL=128
Respuesta desde 192.168.1.219: bytes=32 tiempo<1m TTL=128
Respuesta desde 192.168.1.220: bytes=32 tiempo<387ms TTL=64
Respuesta desde 192.168.1.222: bytes=32 tiempo<400ms TTL=64
Respuesta desde 192.168.1.223: bytes=32 tiempo=455ms TTL=64
Respuesta desde 192.168.1.227: bytes=32 tiempo=199ms TTL=64
Respuesta desde 192.168.1.228: bytes=32 tiempo=269ms TTL=64
Respuesta desde 192.168.1.236: bytes=32 tiempo=354ms TTL=64
Respuesta desde 192.168.1.238: bytes=32 tiempo=395ms TTL=64

Respuesta desde 192.168.1.243: bytes=32 tiempo<478m TTL=64
Respuesta desde 192.168.1.251: bytes=32 tiempo<101m TTL=64
Respuesta desde 192.168.1.253: bytes=32 tiempo=171ms TTL=64
Respuesta desde 192.168.1.254: bytes=32 tiempo=188ms TTL=64

ANEXO 2: CONFIGURACIÓN DE SWITCHES Y ROUTER

SW_1:

```
Enable
Configure terminal
Interface fastEthernet 0/1
Switchport mode Access
Switchport Access vlan 2
End
Configure terminal
Interface fastEthernet 0/2
Switchport mode Access
Switchport Access vlan 2
End
Configure terminal
Interface fastEthernet 0/3
Switchport mode Access
Switchport Access vlan 2
End
Configure terminal
Interface fastEthernet 0/4
Switchport mode Access
Switchport Access vlan 2
end
Configure terminal
Interface fastEthernet 0/5
Switchport mode Access
Switchport Access vlan 2
end
Configure terminal
Interface fastEthernet 0/6
Switchport mode Access
Switchport Access vlan 2
end
Configure terminal
Interface fastEthernet 0/7
Switchport mode Access
Switchport Access vlan 2
end
Configure terminal
Interface fastEthernet 0/8
Switchport mode Access
Switchport Access vlan 2
end
Configure terminal
Interface fastEthernet 0/9
Switchport mode Access
Switchport Access vlan 2
end
```

```
Configure terminal
Interface fastEthernet 0/10
Switchport mode Access
Switchport Access vlan 2
end
Configure terminal
Interface fastEthernet 0/11
Switchport mode Access
Switchport Access vlan 2
end
Configure terminal
Interface fastEthernet 0/12
Switchport mode Access
Switchport Access vlan 2
end
Configure terminal
Interface fastEthernet 0/13
Switchport mode Access
Switchport Access vlan 2
end
Configure terminal
Interface fastEthernet 0/14
Switchport mode Access
Switchport Access vlan 2
end
Configure terminal
Interface fastEthernet 0/15
Switchport mode Access
Switchport Access vlan 2
end
Configure terminal
Interface fastEthernet 0/16
Switchport mode Access
Switchport Access vlan 2
End
Configure terminal
Interface fastEthernet 0/17
Switchport mode Access
Switchport Access vlan 2
end
Configure terminal
Interface fastEthernet 0/18
Switchport mode Access
Switchport Access vlan 2
end

Configure terminal
Interface fastEthernet 0/19
Switchport mode Access
Switchport Access vlan 2
```

```
end
Configure terminal
Interface fastEthernet 0/20
Switchport mode Access
Switchport Access vlan 2
end
Configure terminal
Interface fastEthernet 0/21
Switchport mode Access
Switchport Access vlan 2
end
Configure terminal
Interface fastEthernet 0/22
Switchport mode Access
Switchport Access vlan 2
end
Configure terminal
Interface fastEthernet 0/23
Switchport mode Access
Switchport Access vlan 2
end
Configure terminal
Interface fastEthernet 0/24
Switchport mode Access
Switchport Access vlan 2
End
Configure terminal
Interface gigabit 0/1
Switchport mode Trunk
Switchport trunk native vlan 99
end
```

SW_2:

```
Enable
Configure terminal
Interface fastEthernet 0/1
Switchport mode Access
Switchport Access vlan 2
End
Configure terminal
Interface fastEthernet 0/2
Switchport mode Access
Switchport Access vlan 2
End
Configure terminal
Interface fastEthernet 0/3
Switchport mode Access
Switchport Access vlan 2
End
```



```
Configure terminal
Interface fastEthernet 0/4
Switchport mode Access
Switchport Access vlan 3
end
Configure terminal
Interface fastEthernet 0/5
Switchport mode Access
Switchport Access vlan 3
end
Configure terminal
Interface fastEthernet 0/6
Switchport mode Access
Switchport Access vlan 3
end
Configure terminal
Interface fastEthernet 0/7
Switchport mode Access
Switchport Access vlan 12
end
Configure terminal
Interface gigabit 0/1
Switchport mode Trunk
Switchport trunk native vlan 99
End
Configure terminal
Interface gigabit 0/2
Switchport mode Trunk
Switchport trunk native vlan 99
end
```

SW_3:

```
Enable
Configure terminal
Interface fastEthernet 0/1
Switchport mode Access
Switchport Access vlan 3
End
Configure terminal
Interface fastEthernet 0/2
Switchport mode Access
Switchport Access vlan 3
End
Configure terminal
Interface fastEthernet 0/3
Switchport mode Access
Switchport Access vlan 2
End
```

```
Configure terminal
Interface fastEthernet 0/4
Switchport mode Access
Switchport Access vlan 3
end
Configure terminal
Interface fastEthernet 0/5
Switchport mode Access
Switchport Access vlan 3
end
Configure terminal
Interface fastEthernet 0/6
Switchport mode Access
Switchport Access vlan 3
end
Configure terminal
Interface fastEthernet 0/7
Switchport mode Access
Switchport Access vlan 3
end
Configure terminal
Interface fastEthernet 0/8
Switchport mode Access
Switchport Access vlan 3
end
Configure terminal
Interface fastEthernet 0/9
Switchport mode Access
Switchport Access vlan 3
end
Configure terminal
Interface fastEthernet 0/10
Switchport mode Access
Switchport Access vlan 3
end
Configure terminal
Interface fastEthernet 0/11
Switchport mode Access
Switchport Access vlan 3
end
Configure terminal
Interface fastEthernet 0/12
Switchport mode Access
Switchport Access vlan 3
end
Configure terminal
Interface fastEthernet 0/13
Switchport mode Access
Switchport Access vlan 3
end
```

```
Configure terminal
Interface fastEthernet 0/14
Switchport mode Access
Switchport Access vlan 3
end
Configure terminal
Interface fastEthernet 0/15
Switchport mode Access
Switchport Access vlan 3
end
Configure terminal
Interface fastEthernet 0/16
Switchport mode Access
Switchport Access vlan 3
End
Configure terminal
Interface fastEthernet 0/17
Switchport mode Access
Switchport Access vlan 3
end
Configure terminal
Interface fastEthernet 0/18
Switchport mode Access
Switchport Access vlan 3
end
Configure terminal
Interface fastEthernet 0/19
Switchport mode Access
Switchport Access vlan 3
end
Configure terminal
Interface fastEthernet 0/20
Switchport mode Access
Switchport Access vlan 3
end
Configure terminal
Interface fastEthernet 0/21
Switchport mode Access
Switchport Access vlan 3
end
Configure terminal
Interface gigabit 0/1
Switchport mode Trunk
Switchport trunk native vlan 99
End
Configure terminal
Interface gigabit 0/2
Switchport mode Trunk
Switchport trunk native vlan 99
End
```

SW_4:

```
Enable
Configure terminal
Interface fastEthernet 0/1
Switchport mode Access
Switchport Access vlan 11
End
Configure terminal
Interface fastEthernet 0/2
Switchport mode Access
Switchport Access vlan 11
End
Configure terminal
Interface fastEthernet 0/3
Switchport mode Access
Switchport Access vlan 11
End
Configure terminal
Interface fastEthernet 0/4
Switchport mode Access
Switchport Access vlan 11
end
Configure terminal
Interface fastEthernet 0/5
Switchport mode Access
Switchport Access vlan 11
end
Configure terminal
Interface fastEthernet 0/6
Switchport mode Access
Switchport Access vlan 11
end
Configure terminal
Interface fastEthernet 0/7
Switchport mode Access
Switchport Access vlan 11
end
Configure terminal
Interface gigabit 0/1
Switchport mode Trunk
Switchport trunk native vlan 99
End
Configure terminal
Interface gigabit 0/2
Switchport mode Trunk
Switchport trunk native vlan 99
End
```

SW_5:

```
Enable
Configure terminal
Interface fastEthernet 0/1
Switchport mode Access
Switchport Access vlan 7
End
Configure terminal
Interface fastEthernet 0/2
Switchport mode Access
Switchport Access vlan 7
End
Configure terminal
Interface fastEthernet 0/3
Switchport mode Access
Switchport Access vlan 7
End
Configure terminal
Interface fastEthernet 0/4
Switchport mode Access
Switchport Access vlan 7
end
Configure terminal
Interface fastEthernet 0/5
Switchport mode Access
Switchport Access vlan 7
end
Configure terminal
Interface fastEthernet 0/6
Switchport mode Access
Switchport Access vlan 7
end
Configure terminal
Interface fastEthernet 0/7
Switchport mode Access
Switchport Access vlan 7
end
Configure terminal
Interface fastEthernet 0/8
Switchport mode Access
Switchport Access vlan 7
end
Configure terminal
Interface fastEthernet 0/9
Switchport mode Access
Switchport Access vlan 4
end
Configure terminal
Interface fastEthernet 0/10
```

```
Switport mode Access
Switchport Access vlan 4
end
Configure terminal
Interface fastEthernet 0/11
Switport mode Access
Switchport Access vlan 4
end
Configure terminal
Interface fastEthernet 0/12
Switport mode Access
Switchport Access vlan 4
end
Configure terminal
Interface fastEthernet 0/13
Switport mode Access
Switchport Access vlan 4
end
Configure terminal
Interface fastEthernet 0/14
Switport mode Access
Switchport Access vlan 4
end
Configure terminal
Interface fastEthernet 0/15
Switport mode Access
Switchport Access vlan 17
end
Configure terminal
Interface gigabit 0/1
Switport mode Trunk
Switchport trunk native vlan 99
End
Configure terminal
Interface gigabit 0/2
Switport mode Trunk
Switchport trunk native vlan 99
End
```

SW_6:

```
Enable
Configure terminal
Interface fastEthernet 0/1
Switport mode Access
Switchport Access vlan 14
End
Configure terminal
Interface fastEthernet 0/2
Switport mode Access
```

```
Switchport Access vlan 14
End
Configure terminal
Interface fastEthernet 0/3
Switchport mode Access
Switchport Access vlan 14
End
Configure terminal
Interface fastEthernet 0/4
Switchport mode Access
Switchport Access vlan 14
end
Configure terminal
Interface fastEthernet 0/5
Switchport mode Access
Switchport Access vlan 9
end
Configure terminal
Interface fastEthernet 0/6
Switchport mode Access
Switchport Access vlan 9
end
Configure terminal
Interface fastEthernet 0/7
Switchport mode Access
Switchport Access vlan 9
end
Configure terminal
Interface fastEthernet 0/8
Switchport mode Access
Switchport Access vlan 13
end
Configure terminal
Interface fastEthernet 0/9
Switchport mode Access
Switchport Access vlan 13
end
Configure terminal
Interface fastEthernet 0/10
Switchport mode Access
Switchport Access vlan 13
end
Configure terminal
Interface fastEthernet 0/11
Switchport mode Access
Switchport Access vlan 13
end
Configure terminal
Interface fastEthernet 0/12
Switchport mode Access
```

```
Switchport Access vlan 13
end
Configure terminal
Interface gigabit 0/1
Switchport mode Trunk
Switchport trunk native vlan 99
End
Configure terminal
Interface gigabit 0/2
Switchport mode Trunk
Switchport trunk native vlan 99
End
```

SW_7:

```
Enable
Configure terminal
Interface fastEthernet 0/1
Switchport mode Access
Switchport Access vlan 15
End
Configure terminal
Interface fastEthernet 0/2
Switchport mode Access
Switchport Access vlan 15
End
Configure terminal
Interface fastEthernet 0/3
Switchport mode Access
Switchport Access vlan 10
End
Configure terminal
Interface fastEthernet 0/4
Switchport mode Access
Switchport Access vlan 10
end
Configure terminal
Interface fastEthernet 0/5
Switchport mode Access
Switchport Access vlan 10
end
Configure terminal
Interface fastEthernet 0/6
Switchport mode Access
Switchport Access vlan 10
end
Configure terminal
Interface fastEthernet 0/7
Switchport mode Access
Switchport Access vlan 10
```



```
end
Configure terminal
Interface fastEthernet 0/8
Switchport mode Access
Switchport Access vlan 10
end
Configure terminal
Interface fastEthernet 0/9
Switchport mode Access
Switchport Access vlan 10
end
Configure terminal
Interface fastEthernet 0/10
Switchport mode Access
Switchport Access vlan 10
end
Configure terminal
Interface fastEthernet 0/11
Switchport mode Access
Switchport Access vlan 10
end
Configure terminal
Interface fastEthernet 0/12
Switchport mode Access
Switchport Access vlan 10
end
Configure terminal
Interface fastEthernet 0/13
Switchport mode Access
Switchport Access vlan 10
end
Configure terminal
Interface fastEthernet 0/14
Switchport mode Access
Switchport Access vlan 10
end
Configure terminal
Interface fastEthernet 0/15
Switchport mode Access
Switchport Access vlan 10
end
Configure terminal
Interface fastEthernet 0/16
Switchport mode Access
Switchport Access vlan 8
end
Configure terminal
Interface fastEthernet 0/17
Switchport mode Access
Switchport Access vlan 8
```

```
End
Configure terminal
Interface fastEthernet 0/18
Switchport mode Access
Switchport Access vlan 8
end
Configure terminal
Interface gigabit 0/1
Switchport mode Trunk
Switchport trunk native vlan 99
End
Configure terminal
Interface gigabit 0/2
Switchport mode Trunk
Switchport trunk native vlan 99
End
```

SW_8:

```
Enable
Configure terminal
Interface fastEthernet 0/1
Switchport mode Access
Switchport Access vlan 16
End
Configure terminal
Interface fastEthernet 0/2
Switchport mode Access
Switchport Access vlan 16
End
Configure terminal
Interface fastEthernet 0/3
Switchport mode Access
Switchport Access vlan 16
End
Configure terminal
Interface fastEthernet 0/4
Switchport mode Access
Switchport Access vlan 16
end
Configure terminal
Interface fastEthernet 0/5
Switchport mode Access
Switchport Access vlan 16
end
Configure terminal
Interface fastEthernet 0/6
Switchport mode Access
Switchport Access vlan 16
end
```

```
Configure terminal
Interface fastEthernet 0/7
Switchport mode Access
Switchport Access vlan 16
end
Configure terminal
Interface fastEthernet 0/8
Switchport mode Access
Switchport Access vlan 18
end
Configure terminal
Interface fastEthernet 0/9
Switchport mode Access
Switchport Access vlan 18
end
Configure terminal
Interface fastEthernet 0/10
Switchport mode Access
Switchport Access vlan 18
end
Configure terminal
Interface fastEthernet 0/11
Switchport mode Access
Switchport Access vlan 18
end
Configure terminal
Interface fastEthernet 0/12
Switchport mode Access
Switchport Access vlan 18
end
Configure terminal
Interface fastEthernet 0/13
Switchport mode Access
Switchport Access vlan 5
end
Configure terminal
Interface fastEthernet 0/14
Switchport mode Access
Switchport Access vlan 5
end
Configure terminal
Interface fastEthernet 0/15
Switchport mode Access
Switchport Access vlan 5
end
Configure terminal
Interface gigabit 0/1
Switchport mode Trunk
Switchport trunk native vlan 99
End
```

```
Configure terminal
Interface gigabit 0/2
Switchport mode Trunk
Switchport trunk native vlan 99
End
```

SW_9:

```
Enable
Configure terminal
Interface fastEthernet 0/1
Switchport mode Access
Switchport Access vlan 12
End
Configure terminal
Interface fastEthernet 0/2
Switchport mode Access
Switchport Access vlan 12
End
Configure terminal
Interface fastEthernet 0/3
Switchport mode Access
Switchport Access vlan 12
End
Configure terminal
Interface fastEthernet 0/4
Switchport mode Access
Switchport Access vlan 12
end
Configure terminal
Interface fastEthernet 0/5
Switchport mode Access
Switchport Access vlan 12
end
Configure terminal
Interface fastEthernet 0/6
Switchport mode Access
Switchport Access vlan 17
end
Configure terminal
Interface fastEthernet 0/7
Switchport mode Access
Switchport Access vlan 17
end
Configure terminal
Interface fastEthernet 0/8
Switchport mode Access
Switchport Access vlan 17
end
```

```
Configure terminal
Interface fastEthernet 0/9
Switchport mode Access
Switchport Access vlan 17
end
Configure terminal
Interface fastEthernet 0/10
Switchport mode Access
Switchport Access vlan 3
end
Configure terminal
Interface fastEthernet 0/11
Switchport mode Access
Switchport Access vlan 3
end
Configure terminal
Interface fastEthernet 0/12
Switchport mode Access
Switchport Access vlan 3
end
Configure terminal
Interface gigabit 0/1
Switchport mode Trunk
Switchport trunk native vlan 99
End
Configure terminal
Interface gigabit 0/2
Switchport mode Trunk
Switchport trunk native vlan 99
End
```

SW_10:

```
Enable
Configure terminal
Interface fastEthernet 0/1
Switchport mode Access
Switchport Access vlan 5
End
Configure terminal
Interface fastEthernet 0/2
Switchport mode Access
Switchport Access vlan 5
End
Configure terminal
Interface fastEthernet 0/3
Switchport mode Access
Switchport Access vlan 5
End
```

```
Configure terminal
Interface fastEthernet 0/4
Switchport mode Access
Switchport Access vlan 5
end
Configure terminal
Interface fastEthernet 0/5
Switchport mode Access
Switchport Access vlan 5
end
Configure terminal
Interface fastEthernet 0/6
Switchport mode Access
Switchport Access vlan 5
end
Configure terminal
Interface fastEthernet 0/7
Switchport mode Access
Switchport Access vlan 5
end
Configure terminal
Interface fastEthernet 0/8
Switchport mode Access
Switchport Access vlan 5
end
Configure terminal
Interface fastEthernet 0/9
Switchport mode Access
Switchport Access vlan 5
end
Configure terminal
Interface fastEthernet 0/10
Switchport mode Access
Switchport Access vlan 5
end
Configure terminal
Interface fastEthernet 0/11
Switchport mode Access
Switchport Access vlan 5
end
Configure terminal
Interface fastEthernet 0/12
Switchport mode Access
Switchport Access vlan 5
end
Configure terminal
Interface fastEthernet 0/13
Switchport mode Access
Switchport Access vlan 5
end
```

```
Configure terminal
Interface fastEthernet 0/14
Switchport mode Access
Switchport Access vlan 5
end
Configure terminal
Interface fastEthernet 0/15
Switchport mode Access
Switchport Access vlan 5
end
Configure terminal
Interface fastEthernet 0/16
Switchport mode Access
Switchport Access vlan 5
end
Configure terminal
Interface fastEthernet 0/17
Switchport mode Access
Switchport Access vlan 5
End
Configure terminal
Interface fastEthernet 0/18
Switchport mode Access
Switchport Access vlan 5
end
Configure terminal
Interface gigabit 0/1
Switchport mode Trunk
Switchport trunk native vlan 99
End
Configure terminal
Interface gigabit 0/2
Switchport mode Trunk
Switchport trunk native vlan 99
End
```

SW_11:

```
Configure terminal
Interface fastEthernet 0/1
Switchport mode trunk
Switchport voice vlan 22
Spanning port
End
Configure terminal
Interface fastEthernet 0/2
Switchport mode trunk
Switchport voice vlan 22
Spanning port
```

```
end
Configure terminal
Interface fastEthernet 0/3
Switchport mode trunk
Switchport voice vlan 22
Spanning port
end
Configure terminal
Interface fastEthernet 0/4
Switchport mode trunk
Switchport voice vlan 22
Spanning port
end
Configure terminal
Interface fastEthernet 0/5
Switchport mode trunk
Switchport voice vlan 22
Spanning port
end
Configure terminal
Interface fastEthernet 0/6
Switchport mode trunk
Switchport voice vlan 22
Spanning port
end
Configure terminal
Interface fastEthernet 0/7
Switchport mode trunk
Switchport voice vlan 22
Spanning port
end
Configure terminal
Interface fastEthernet 0/8
Switchport mode trunk
Switchport voice vlan 22
Spanning port
end
Configure terminal
Interface fastEthernet 0/9
Switchport mode trunk
Switchport voice vlan 22
Spanning port
end
Configure terminal
Interface fastEthernet 0/10
Switchport mode trunk
Switchport voice vlan 22
Spanning port
end
Configure terminal
```



```
Interface fastEthernet 0/11
Switchport mode trunk
Switchport voice vlan 22
Spanning port
end
Configure terminal
Interface fastEthernet 0/12
Switchport mode trunk
Switchport voice vlan 22
Spanning port
end
Configure terminal
Interface fastEthernet 0/13
Switchport mode trunk
Switchport voice vlan 22
Spanning port
end
Configure terminal
Interface fastEthernet 0/14
Switchport mode trunk
Switchport voice vlan 22
Spanning port
end
Configure terminal
Interface fastEthernet 0/15
Switchport mode trunk
Switchport voice vlan 22
Spanning port
end
Configure terminal
Interface fastEthernet 0/16
Switchport mode trunk
Switchport voice vlan 22
Spanning port
end
Configure terminal
Interface fastEthernet 0/17
Switchport mode trunk
Switchport voice vlan 22
Spanning port
end
Configure terminal
Interface fastEthernet 0/18
Switchport mode trunk
Switchport voice vlan 22
Spanning port
end
Configure terminal
Interface fastEthernet 0/19
Switchport mode trunk
```

```
Switchport voice vlan 22
Spanning port
end
Configure terminal
Interface fastEthernet 0/20
Switchport mode trunk
Switchport voice vlan 22
Spanning port
end
Configure terminal
Interface fastEthernet 0/21
Switchport mode trunk
Switchport voice vlan 22
Spanning port
end
Configure terminal
Interface fastEthernet 0/22
Switchport mode trunk
Switchport voice vlan 22
Spanning port
end
Configure terminal
Interface fastEthernet 0/23
Switchport mode trunk
Switchport voice vlan 22
Spanning port
end
Configure terminal
Interface fastEthernet 0/24
Switchport mode trunk
Switchport voice vlan 22
Spanning port
end
```

SW_12:

```
Configure terminal
Interface fastEthernet 0/1
Switchport mode trunk
Switchport voice vlan 22
Spanning port
End
Configure terminal
Interface fastEthernet 0/2
Switchport mode trunk
Switchport voice vlan 22
Spanning port
end
Configure terminal
Interface fastEthernet 0/3
```

```
Switchport mode trunk
Switchport voice vlan 22
Spanning port
end
Configure terminal
Interface fastEthernet 0/4
Switchport mode trunk
Switchport voice vlan 22
Spanning port
end
Configure terminal
Interface fastEthernet 0/5
Switchport mode trunk
Switchport voice vlan 22
Spanning port
end
Configure terminal
Interface fastEthernet 0/6
Switchport mode trunk
Switchport voice vlan 22
Spanning port
end
Configure terminal
Interface fastEthernet 0/7
Switchport mode trunk
Switchport voice vlan 22
Spanning port
end
Configure terminal
Interface fastEthernet 0/8
Switchport mode trunk
Switchport voice vlan 22
Spanning port
end
Configure terminal
Interface fastEthernet 0/9
Switchport mode trunk
Switchport voice vlan 22
Spanning port
end
Configure terminal
Interface fastEthernet 0/10
Switchport mode trunk
Switchport voice vlan 22
Spanning port
end
Configure terminal
Interface fastEthernet 0/11
Switchport mode trunk
Switchport voice vlan 22
```

```
Spanning port
end
Configure terminal
Interface fastEthernet 0/12
Switchport mode trunk
Switchport voice vlan 22
Spanning port
end
Configure terminal
Interface fastEthernet 0/13
Switchport mode trunk
Switchport voice vlan 22
Spanning port
end
Configure terminal
Interface fastEthernet 0/14
Switchport mode trunk
Switchport voice vlan 22
Spanning port
end
Configure terminal
Interface fastEthernet 0/15
Switchport mode trunk
Switchport voice vlan 22
Spanning port
end
Configure terminal
Interface fastEthernet 0/16
Switchport mode trunk
Switchport voice vlan 22
Spanning port
end
Configure terminal
Interface fastEthernet 0/17
Switchport mode trunk
Switchport voice vlan 22
Spanning port
end
Configure terminal
Interface fastEthernet 0/18
Switchport mode trunk
Switchport voice vlan 22
Spanning port
end
Configure terminal
Interface fastEthernet 0/19
Switchport mode trunk
Switchport voice vlan 22
Spanning port
end
```

```
Configure terminal
Interface fastEthernet 0/20
Switchport mode trunk
Switchport voice vlan 22
Spanning port
end
Configure terminal
Interface fastEthernet 0/21
Switchport mode trunk
Switchport voice vlan 22
Spanning port
end
Configure terminal
Interface fastEthernet 0/22
Switchport mode trunk
Switchport voice vlan 22
Spanning port
end
Configure terminal
Interface fastEthernet 0/23
Switchport mode trunk
Switchport voice vlan 22
Spanning port
end
Configure terminal
Interface fastEthernet 0/24
Switchport mode trunk
Switchport voice vlan 22
Spanning port
end
```

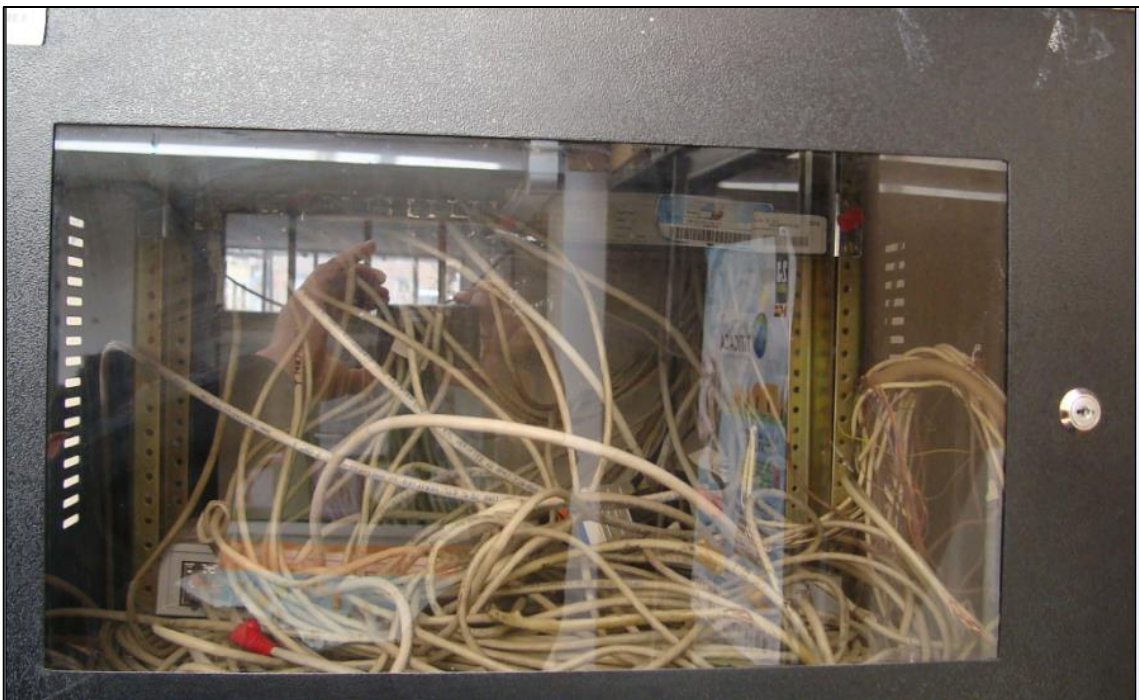
RT_1:

```
Hostname RT_1
enable secret
username ADM secret PASS1
aaa new-model
radius-server host 192.168.19.1
radius-server key PASS2
aaa authentication login USUARIOS
login authentication default
tacacs-server host 192.168.19.1
tacacs-server key PASS3
```

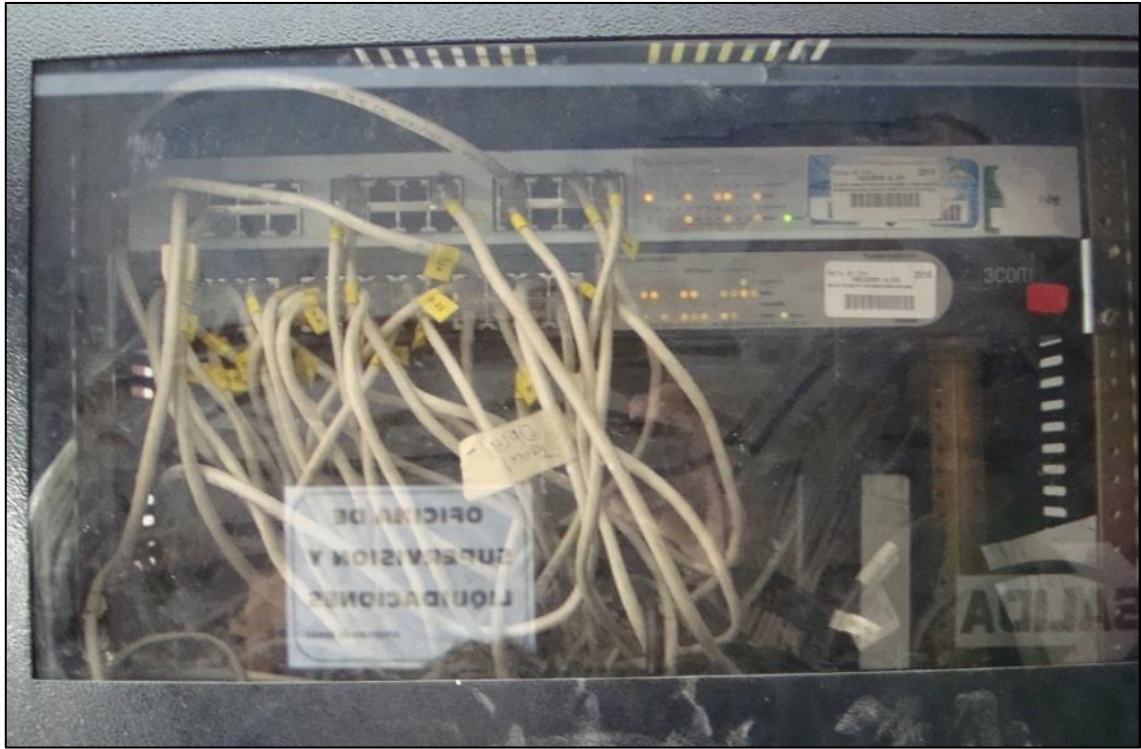
ANEXO 3: PANEL FOTOGRÁFICO



Rack del quinto piso - Edificio A



Switches del quinto piso - Edificio A



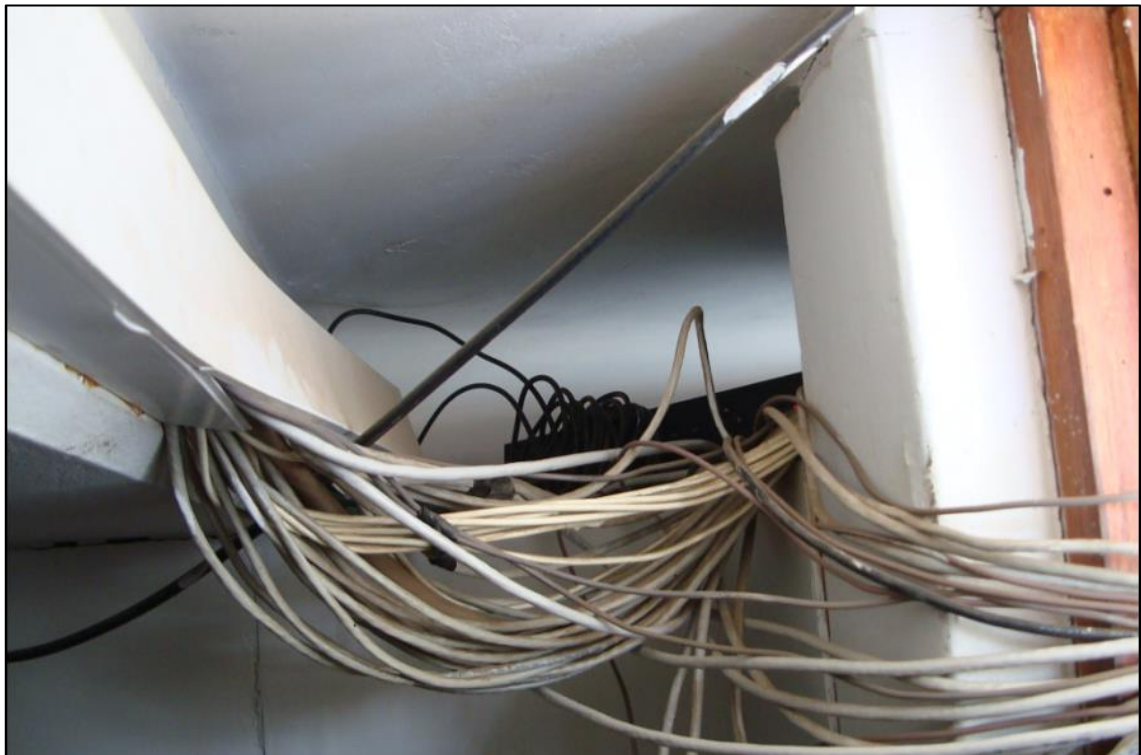
Rack y switch del cuarto piso - Edificio A



Cables expuestos – Edificio A



Cables expuestos en el tercer piso - Edificio A



Cables y equipos expuestos en el tercer piso – Edificio A



Cables expuestos en el tercer piso – Edificio B



Cables expuestos al exterior del edificio A



Ventana con vidrio facturado – Data Center – Tercer Piso Edificio A



Cables expuestos en el segundo piso – Edificio A