UNIVERSIDAD POLITÉCNICA SALESIANA

SEDE QUITO

CARRERA DE TELECOMUNICACIONES

REDISEÑO DE LA RED DE CAMPUS PARA LA EMPRESA ARTKOS BAJO LA METODOLOGÍA Y ARQUITECTURA CISCO SAFE.

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

AUTOR: Francys Josue Carrillo Chela

TUTOR: Juan Carlos Domínguez Ayala

Quito - Ecuador

2024

CERTIFICADO DE RESPONSABILIDAD Y AUTORÍA DEL TRABAJO DE TITULACIÓN

Yo, Francys Josue Carrillo Chela con documento de identificación N° 1727400101 manifiesto que:

Soy el autor y responsable del presente trabajo; y, autorizo a que sin fines de lucro la Universidad Politécnica Salesiana pueda usar, difundir, reproducir o publicar de manera total o parcial el presente trabajo de titulación.

Quito, 22 de febrero del año 2024

Atentamente,

Francys Josue Carrillo Chela
1727400101

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

Yo Francys Josue Carrillo Chela con documento de identificación No.1727400101 expreso mi voluntad y por medio del presente documento cedo a la Universidad Politécnica Salesiana la titularidad sobre los derechos patrimoniales en virtud de que soy autor del Proyecto Técnico: "Rediseño de la Red de Campus para la Empresa ARTKOS bajo la Metodología y Arquitectura Cisco SAFE", el cual ha sido desarrollado para optar por el título de Ingeniero en Telecomunicaciones, en la Universidad Politécnica Salesiana, quedando la Universidad facultada para ejercer plenamente los derechos cedidos anteriormente.

En concordancia con lo manifestado, suscribo este documento en el momento que hago (la entrega del trabajo final en formato digital a la Biblioteca de la Universidad Politécnica Salesiana

Quito, 22 de febrero del año 2024

Atentamente,

Francys Josue Carrillo Chela
1727400101

CERTIFICADO DE DIRECCIÓN DEL TRABAJO DE TITULACIÓN

Yo, Juan Carlos Domínguez Ayala con documento de identificación N° 1713195590 docente de la Universidad Politécnica Salesiana, declaro que bajo mi tutoría fue desarrollado el trabajo de titulación REDISEÑO DE LA RED DE CAMPUS PARA LA EMPRESA ARTKOS BAJO LA METODOLOGÍA Y ARQUITECTURA CISCO SAFE., realizado por Francys Josue Carrillo Chela con documento de identificación N° 1727400101, obteniendo como resultado final el trabajo de titulación bajo la opción: Proyecto Técnico que cumple con todos los requisitos determinados por la Universidad Politécnica Salesiana.

Quito, 22 de febrero del año 2024

Atentamente,

Ing. Juan Carlos Domínguez Ayala, MSc
1713195590

DEDICATORIA

Dedico el presente proyecto a mis padres, quienes siempre creyeron en mí: Angelito, por brindarme el apoyo para no decaer, por mantenerme persistente en mis metas, darme motivación cuando lo necesité, y enseñarme que, a pesar de las adversidades, siempre hay razones para levantarse y esforzarse más. A mi madre María, la persona que junto con mi padre más he admirado, quien me sentó sus principios y valores, que fue una inspiración de fuerza, trabajo, persistencia y alegría en todo momento. Y que aun con su pérdida sigue presente en mí y en mis acciones, te la dedico con todo mi amor, mi Marichui.

Francys Josue Carrillo

AGRADECIMIENTO

Mis sinceros agradecimientos a mis padres Ángel y María, quienes me brindaron su apoyo, cariño y enseñanzas. A mis hermanos, a cada uno de ellos: Melissa, Danilo, Mabel, Darío, Daniel y David. Quienes me enseñaron desde sus vivencias cómo persistir hasta conseguir mis metas, quienes me levantaron cuando no pude hacerlo solo, quienes me jalaron las orejas cuando fue necesario y me felicitaron cuando estaba en buen camino, ¡gracias!

A Andy, mi gran amigo, aquel con quien cuento cuando las cosas van mal, aquel que también está en los mejores momentos, el que en todo camino y jornada está siempre conmigo. A su familia, quienes me acogieron como un miembro más en su hogar, y que he llegado a estimar como un lazo familiar.

A los docentes de la Universidad Politécnica Salesiana que me permitieron seguir con este camino a pesar de las circunstancias suscitadas. Quienes me proporcionaron las herramientas, conocimientos y aptitudes para afrontar la vida profesional.

A mi tutor, Ing. Juan Carlos Domínguez, que incluso antes de tomar este proyecto ya me era tutor en cualquier consultoría académica. Y que ahora me ofreció sus conocimientos y experiencias para la realización de la presente.

Francys Josue Carrillo.

ÍNDICE GENERAL

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

RESUMEN

Artkos es una empresa consolidada en el campo de las Telecomunicaciones, ofreciendo una amplia gama de servicios. Con el paso de los años, la empresa ha experimentado un crecimiento notable, tanto en número de colaboradores como en infraestructura, con el objetivo de brindar un servicio de excelencia a sus clientes. Este crecimiento ha generado mayores necesidades tecnológicas, aumentando significativamente el flujo de datos en su red. Como resultado, los equipos, protocolos e infraestructura actuales se han vuelto ineficientes.

Para abordar esta situación, se propone rediseñar la red de campus de ARTKOS utilizando la metodología y arquitectura Cisco SAFE (Secure Architecture for Enterprise). El proyecto se ha iniciado con el levantamiento de una línea base, recopilando información detallada sobre hardware y software para identificar las vulnerabilidades presentes en la red actual.

Se está desarrollando una propuesta integral que fortalezca los aspectos críticos de la red. Se utilizará software especializado para simular esta propuesta y evaluar su rendimiento. Finalmente, se llevará a cabo un análisis de viabilidad económica de la propuesta, utilizando una variedad de instrumentos financieros.

Este rediseño cumple con las demandas de la empresa y también se alinea con los principios propuestos por Cisco SAFE, tales como escalabilidad, tolerancia a fallos y calidad de servicio. De esta manera, se abordarán las debilidades identificadas en la red actual.

Palabras Claves: Cisco SAFE**,** red de campus, escalabilidad, tolerancia a fallas, calidad de servicio.

ABSTRACT

ARTKOS is a well-established company in the field of Telecommunications, offering a wide range of services. Over the years, the company has experienced significant growth, both in the number of employees and in infrastructure, aiming to provide excellent service to its clients. This growth has generated increased technological needs, significantly raising the data flow within its network. As a result, the current equipment, protocols, and infrastructure have become inefficient.

To address this situation, it is proposed to redesign ARTKOS' campus network using the methodology and architecture of Cisco SAFE (Secure Architecture for Enterprise). The project has begun by establishing a baseline, gathering detailed information on hardware and software to identify vulnerabilities in the current network.

A comprehensive proposal is being developed to strengthen critical aspects of the network. Specialized software will be used to simulate this proposal and evaluate its performance. Finally, an economic feasibility analysis of the proposal will be carried out, employing various financial instruments.

This redesign meets the company's demands and also aligns with the principles proposed by Cisco SAFE, such as scalability, fault tolerance, and quality of service. This approach aims to address the weaknesses identified in the current network.

Keywords: Cisco SAFE, campus network, scalability, fault tolerance, quality of service

INTRODUCCIÓN

Actualmente, las redes empresariales necesitan cubrir las necesidades de comunicaciones de red para su infraestructura. Es de vital importancia mantenerse a la vanguardia en los protocolos y arquitecturas que existen para potenciar una red. Es por esto que se propone el rediseño de la red de campus de la empresa ARTKOS, todo esto detallado en la siguiente propuesta:

Capítulo 1: Se presentan los elementos propios de un proyecto técnico: planteamiento del problema, justificación del proyecto, objetivos y marco teórico

Capítulo 2: Se presenta línea base, estado actual de la red, equipos, cableado, direccionamiento, aplicaciones utilizadas y área Wifi.

Capítulo 3: Se presenta el rediseño, la simulación de la red, los equipos a utilizar y las mejoras para la red de ARTKOS.

Capítulo 4: Se presenta la simulación de la red, junto con los protocolos utilizados para la mejora de la misma.

Capítulo 5: Se presenta el estudio financiero para llevar a cabo la implementación de la red propuesta y su costo beneficio en la empresa.

Para concluir en base a los resultados obtenidos se presentan las conclusiones y recomendaciones junto con los aspectos técnicos del mismo.

Con esta propuesta se obtuvo una red con escalabilidad, calidad de servicio y tolerancia a fallas. Todo esto apegándose a las prácticas que refiere Cisco SAFE.

1. CAPÍTULO 1
ANTECEDENTES

En este capítulo, se examinará la presentación del problema, se desarrollará la justificación y se detallarán los objetivos.

1.1 Problema

Las vulnerabilidades en una red representan riesgos de secuestro o filtración de datos, así como interrupciones en los servicios, lo que supone un peligro tanto para la empresa como para sus clientes. En Ecuador, diversas instituciones estatales han experimentado filtraciones de datos y ataques a entidades bancarias debido a la falta de medidas preventivas adecuadas.

El crecimiento en la demanda de servicios de red en los últimos años ha resultado en un aumento de los ataques informáticos. En nuestro país, se ha detectado un 9% de estos ataques, ubicándonos en el quinto lugar en la región. Estos incidentes varían desde ataques de denegación de servicio hasta pérdidas económicas directas.

La seguridad de los datos es fundamental para el progreso de cualquier organización. Aunque ARTKOS cuenta con una infraestructura funcional de red de campus, no se considera completamente segura. Con la evolución de las tácticas de ciberataque, existe la posibilidad de que la arquitectura actual de la organización presente vulnerabilidades.

1.2 Delimitación del problema.

La organización no ha dado un mantenimiento, ni cambiado las metodologías y arquitecturas de su red, siendo así vulnerable. Cisco SAFE proporciona parámetros para diferentes módulos que podrían mejorar la seguridad de la red de la organización. El módulo Cisco SAFE Campus se centra en un modelo jerárquico de: acceso, distribución y núcleo. Para los cuales tienen diferentes metodologías para su protección, haciendo de la red escalable, con tolerancia a fallos y con calidad de servicio, por lo que la organización tendrá un mejor manejo de sus recursos y seguridad en la información.

Por dichas razones la presente se enfocará en definir la línea base de la organización para identificar los posibles fallos, así como la protección de los dispositivos de campus que

componen esta red, los cuales garanticen a la red de campus seguridad, además de brindar los servicios que se esperan de la misma.

1.3 Justificación

La organización ha descuidado el mantenimiento y la actualización de sus metodologías y arquitecturas de red, lo que la hace vulnerable. Cisco SAFE ofrece directrices para diversos módulos que podrían mejorar la seguridad de la red de la organización.

El módulo Cisco SAFE Campus se basa en un modelo jerárquico de acceso, distribución y núcleo. Proporciona metodologías específicas para proteger cada uno de estos componentes, lo que resulta en una red escalable, resistente a fallos y con alta calidad de servicio. Esto permitirá a la organización administrar mejor sus recursos y asegurar la información.

Por estas razones, este estudio se centrará en establecer la línea base de la organización para identificar posibles vulnerabilidades. Se enfocará en proteger los dispositivos de campus que conforman esta red, garantizando la seguridad de la red y proporcionando los servicios esperados

1.4 Objetivos

1.4.1 Objetivo General.

Rediseñar una red de campus para la organización ARTKOS basándose en la metodología y arquitectura Cisco SAFE

1.4.2 Objetivos Específicos.

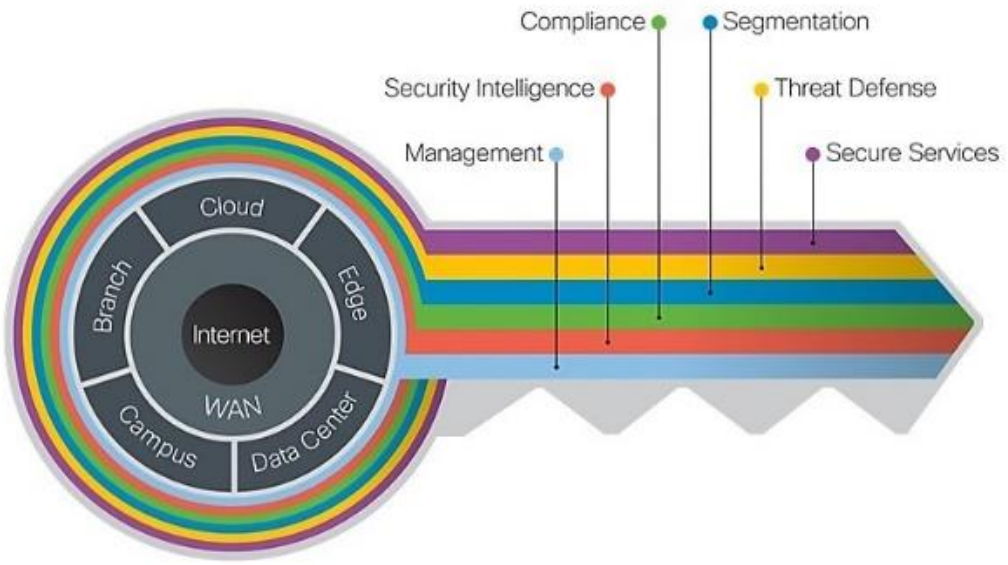
- Definir la línea base de la infraestructura de red de la organización ARTKOS para determinar las condiciones de seguridad de esta.
- Rediseñar la red de campus mediante el modelo Cisco SAFE con características de tolerancia a fallos, escalabilidad y QoS enfocados a la seguridad de esta.
- Simular el diseño de la red de campus con software para la comprobación de las nuevas propiedades de esta.
- Ponderar la factibilidad económica del proyecto para su rentabilidad y posible implementación

1.5 Marco Teórico

1.5.1 Modelo Cisco SAFE

Cisco SAFE (Secure Architecture For Everyone) es el cúmulo de información acerca de las mejores prácticas para el diseño e implementación de redes seguras, este tipo de arquitectura se enfoca en las amenazas esperadas y los medios para combatirlas. Así mismo dicha metodología incluye diseños ya probados, y aborda temas críticos en la seguridad de la red, documentando además como realizarlos (Cisco SAFE Reference Guide SAFE Overview Executive Summary, 2023) Este modelo separa la red en varios componentes: Cloud, Edge, Data Center, Campus y finalmente Branch. Para la presente se enfocará en el módulo Campus. Dentro del mismo se centrará en los puntos: Secure Services, Thread Defense, Segmentation, Compliance, Security Inteligence y Management.

Figura 1.1 Modelo CISCO SAFE



Arquitectura de Empresarial Cisco SAFE. Fuente: (Cisco SAFE Reference Guide SAFE Overview Executive Summary, 2023)

En la figura 1.1 se muestra el modelo Cisco SAFE, donde se muestran los puntos principales de la red y su división.

1.6 Diseño de red LAN

Las redes LAN son el conjunto de dispositivos interconectados que pueden compartir recurso o información, estas ocupan un lugar físico que puede ser pequeño como una habitación con tres dispositivos, o más amplio como un edificio en redes empresariales con miles de dispositivos (Leyva, 2021) Para el diseño de esta es necesario conocer los requerimientos de la entidad, usar métodos y protocolos que la satisfagan.

1.7 Metodología Top Down

Es una metodología que hace énfasis en una perspectiva general de la red como los objetivos de esta y requisitos del negocio, hasta ir a lo más específico como distribución de la red, protocolos, equipos y otros detalles técnicos, teniendo así una comprensión más amplia y estratégica de los requerimientos de la red. (Suarez, 2020)

1.8 Metodología PPDIOO

PPDIO son las siglas para: Preparar, planificar, diseñar, implementar, operar y optimizar. Siendo esta una metodología que determina el ciclo de vida de una red y sus servicios de manera continua. (Anthony Bruno, 2010)

1.8.1 Preparar

Establece el enfoque de la red, y proponer la arquitectura para la red, e identificar que las mejores soluciones tecnológicas que soporten a la red, así mismo un posible presupueste y los recursos necesarios para la misma. (Richard Froom, 2010)

1.8.2 Planificar

Identifica los requisitos iniciales de la red, las instalaciones, las necesidades de los usuarios. Evalúa la red existente, defines los protocolos, seguridad y topologías. Se adecua a los parámetros de alcance, costos y recursos establecidos. (Richard Froom, 2010)

1.8.3 Diseñar

Se elabora el diseño técnico de la red derivado de los requisitos iniciales de la misma, el mismo es detallado, y debe cumplir con los requerimientos planteados, en este caso QoS, escalabilidad y tolerancia a fallos. (Richard Froom, 2010)

1.8.4 Implementar

Se incorporan las componentes propuestas en la etapa anterior, este debe tener un enfoque de no interrumpir la red ni de crear algún punto de vulnerabilidad. Para este caso se configura la documentación con los diagramas establecidos en el diseño. (Richard Froom, 2010)

1.8.5 Operar

Implica mantener la red activa durante las actividades diarias, se verifica su funcionamiento en cuanto al control de los procesos y los cambios realizados. (Richard Froom, 2010)

1.8.6 Optimizar

Es una gestión proactiva de la red, se trata de identificar algún posible fallo que se pueda presentar a futuro y resolverlo. Esta puede dar lugar a un rediseño de la red si surge algún nuevo requerimiento o el rendimiento no cumple con las expectativas. (Richard Froom, 2010)

1.9 Modelo TCP/IP

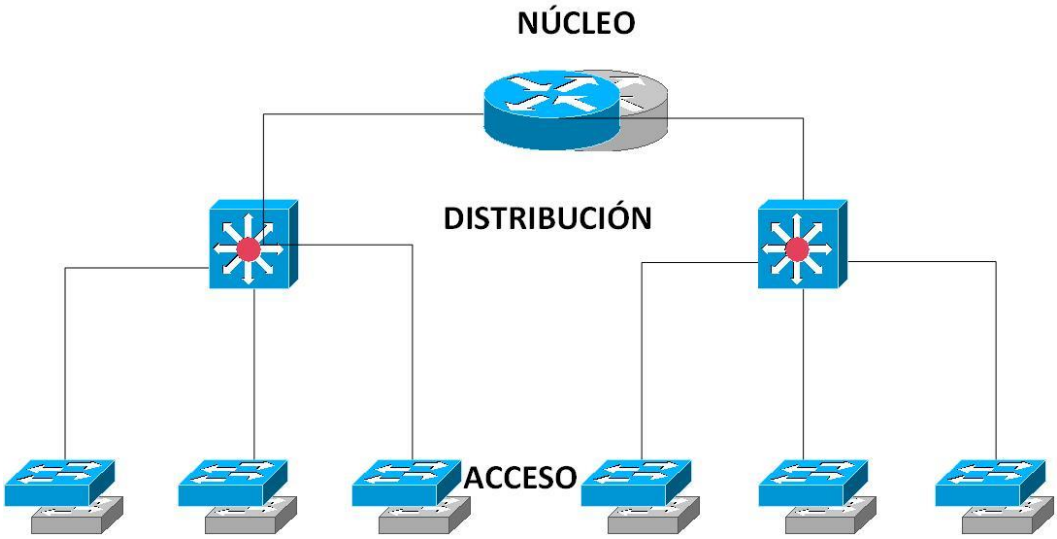
Es un conjunto de protocolos que permite la intercomunicación entre hosts, así como su intercambio de datos. Es un modelo estándar que a permitido el desarrollo de infraestructura moderna de redes. Este es altamente flexible y escalable. (Hernández, 2017)

1.10 Modelo jerárquico de la red

Es una topología de red que permite agrupar dispositivos con funciones precisas, estas las separan en tres niveles, con el fin de facilitar el diseño, mantenimiento e implementación (Patilla, 2021) Teniendo así escalabilidad. A nivel jerárquico LAN tiene tres capas:

- Capa de Acceso: Se encuentran los hosts finales de la red, donde se da su acceso a la red.
- Capa de Distribución: Permite unir las capas de acceso además de proporcionar un manejo del tráfico de la red, se gestiona la seguridad y se separa las áreas de la red.
- Capa de Núcleo: Permite la conectividad de las capas de distribución en las redes LAN, buscando minimizar el tiempo del procesamiento de datos.

Figura 1.2 Modelo Jerárquico



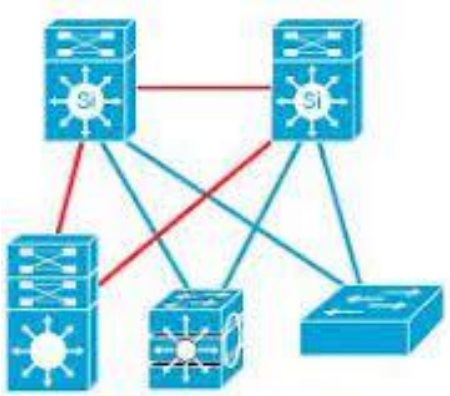
Modelo jerárquico: Núcleo, distribución y acceso. Elaborado por: Francys Carrillo

En la figura 1.2 se muestra el modelo jerárquico con: Acceso, distribución y núcleo. Esto con los componentes a usar en cada uno.

1.11 Modelo Núcleo Colapsado

Es un modelo que se usa en redes empresariales, este reduce costos al unir la capa de núcleo y distribución, simplificando sus funciones en un solo dispositivo de red. Este dispositivo es más robusto ya que tiene capacidades de conmutación, enrutamiento y gestión de tráfico. Este tipo de diseño suele ser más apropiado para redes medianas o pequeñas, por lo que se tomará este diseño para la presente, puesto que es una red mediana. Todo esto mostrado en la figura 1.3

Figura 1.3 Modelo Núcleo colapsado



Modelo de núcleo colapsado Acceso y Núcleo Colapsado: Tomado de: Cisco CCNA.

1.12 Calidad de servicio

Es la capacidad de una red para ofrecer un servicio de tráfico adecuado para la organización, teniendo en cuenta los requerimientos y basándose en: DSCP y el ancho de banda propuesto. (Ormachea Mejía, 2022)

Para voz y video Cisco recomienda para Delay valores menores a 150 ms, para Jitter valores menores a 30 ms y un ancho de banda superior a 100 KBPS, sin embargo, estos deben ser ajustados a las necesidades de la red. Todo esto permite controlar la congestión del ancho de banda, priorizar los tipos de conexiones, asignar el ancho de banda basándose en los perfiles de tráfico. (Mamani Bautista, 2019)

1.13 Escalabilidad

Es la capacidad de la red de adaptarse al crecimiento, como resultado de fusiones adquisiciones o separaciones, todo esto sin perjudicar a la red y manteniéndola disponible y administrable. (Lopes, 2018)

1.14 Tolerancia a fallas

Es la característica de la red que le permite continuar con sus operaciones sin ser interrumpida si es que algún elemento de la misma llega a fallar, teniendo así varias técnicas, como la redundancia de rutas, entre otros.

CAPÍTULO 2
LEVANTAMIENTO DE LA LINEA BASE Y PROPUESTA DEL REDISEÑO DE LA RED DE CAMPUS

2.1 Detalles de las áreas de la organización

ARTKOS es una empresa de TI que ofrece dar soluciones de comunicaciones, redes y conectividad orientadas al ámbito corporativo. La misma posee diferentes departamentos, cada uno con sus colaboradores, esta se detalla en la Tabla 2.1.

El edificio de ARTKOS posee cuatro pisos y un subsuelo, los cuartos de comunicaciones están presentes verticalmente en cada uno de ellos exceptuando el subsuelo, además, el Data Center se encuentra ubicado en el tercer piso.

Tabla 2.1 Áreas de ARTKOS

Departamentos	Empleados
Preventas	11
Financiero	10
Delivery Managment	3
Talento Humano	8
Tecnològicos	17
Administrativo	10
Legal	9
Seguridad	10
Gerencia	8
DATA CENTER	6
Total	92

Número de colaboradores de la organización por áreas. Fuente: ARTKOS

2.2 Infraestructura actual de la red

En el subsuelo se encuentran cuatro computadoras y tres teléfonos VOIP, estos se encuentran conectados al Rack del primer piso, estos para conectar a cuatro colaboradores del área de ventas.

En el primer piso se encuentran las áreas: Administrativos, legal y talento humano. En el presente piso se encuentra el Rack: RA001-AKROS. En el segundo piso se encuentra el RA002-Akros distribuyendo para el área de preventas, financiero y delivery management. Mientras que en el tercer piso se encuentra el RA003-Arktos, para los departamentos:

Tecnología y Seguridad. En el cuarto piso se encuentra el rack para gerencia RA004-Akros. Finalmente, en el quinto piso se encuentra el Data Center, este posee los equipos: Router de frontera servidores: DHCP, SFTP, SNMP, DNS, POP3. Un Firewall Palo Alto Network PA 220, y la salida a internet con un dispositivo otorgado por CNT para la salida a internet.

Tabla 2.2 Listado de equipos actuales

PISOS	Equipo	Modelo	Cantidad
Primer Piso	Switch Cisco	Catalyst 3560-48TS	1
	AP	Cisco Aironet 2800	2
Segundo Piso	Switch Cisco	Catalyst 3560-48TS	1
	AP	Cisco Aironet 2800	2
Tercer Piso	Switch Cisco	Catalyst 3560-48TS	1
	AP	Cisco Aironet 2800	2
Cuarto Piso	Switch Cisco	Catalyst 3560-24TS	1
	AP	Cisco Aironet 2800	2
Quinto Piso	Switch Cisco	Catalyst 3560-24TS	1
	Switch Cisco	Catalyst 3560-24TS	1
	Modem CNT		1
	Router Cisco	Cisco ISR 4321	2
	AP	Cisco Aironet 2800	2
Quinto Piso (Data center)	Servidor	DELL AIO	1
	Servidor	LENOVO	1
	Servidor	HP	1
	Servidor	DELL	1
	Servidor	HIKVISION	2
	UPS	APC Smart-UPS X 3000VA	1
	Firewall	Palo Alto Networks PA-220	1

Dispositivos utilizados actualmente por ARTKOS. Elaborador por: Francys Carrillo

Como se muestra en la tabla 2.2 hay equipos que ya tienen soporte de la fabricante, como Cisco 3560, su EoL (End of Life) a sido hasta marzo del 2023. Así mismo Cisco Airnet que su EoL fue en noviembre del 2023. En cuanto a Cisco ISR 4321 su EoL fue en noviembre del 2023. Sin embargo, el firewall Palo Alto PA 220 se mantiene con servicio del proveedor hasta el 2028.

2.3 Capa de acceso a la red

ARTKOS tiene una topología tipo estrella extendida, el enlace entra al ER donde se conecta al TR para distribuir los puntos de conexión a todo el edificio. Además, se tiene servidores en el ER de diferentes tipos.

Estos se distribuyen a través de cableado estructurado, con cable CAT 6A y se organizan con los diferentes PatchPannel usados en cada piso, al ser una topología estrella extendida cada uno de los switches en cada piso se conecta únicamente a un switch ubicado en el último piso. Esta posee en su Data center equipos de VOIP, y servidores DNS, DHCP, SFTP, SNMP, POP3. La topología se meustra en la figura 2.3

Figura 2.3 Estado actual de la organización ARTKOS

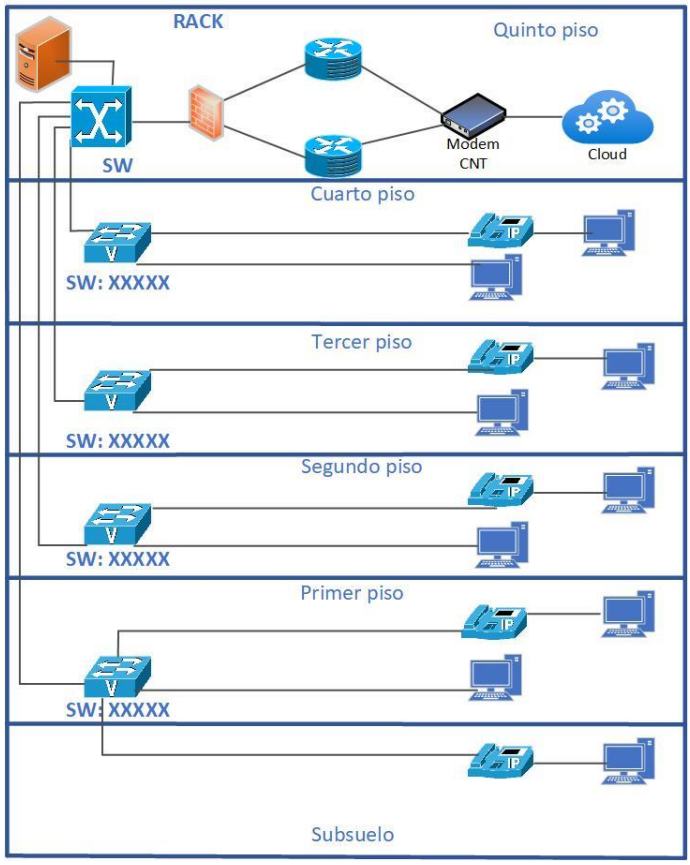


Diagrama lógico de “ARTKOS”. Elaborado por: Francys Carrillo

2.4 Cableado de red

ARTKOS tiene un enlace con CNT, este ISP provee una ONT HUAWEI a la cual llega una Fibra óptica de 6 hilos, ADSS de los cuales esta fusionado el hilo azul a la ONU, los demás llegan en reserva, esta fibra es monomodo.

La ONU se conecta a dos Routers Cisco, con el fin de tener redundancia en la red, en cuanto a las conexiones a los hosts finales, se las da a través de APs y switches Cisco distribuidos en cada piso, el inmueble cuenta con 135 puntos de red para las diferentes áreas, cabe recalcar que en el cableado horizontal las canaletas internas ya no poseen espacio para más cables de red.

Desde el data center se distribuye el Backbone hacia los Switches a través de canales del inmueble, para después en el techo de cada piso distribuirlas de manera horizontal a través de canaletas de aluminio, en cada rack de cada piso se encuentran los mencionados switches POE Catalyst 3560-48TS. En la Figura 2.4 Se muestra un diagrama de la distribución de los puertos de los dispositivos intermediarios de la red.

Figura 2.4 Distribución Física de los equipos

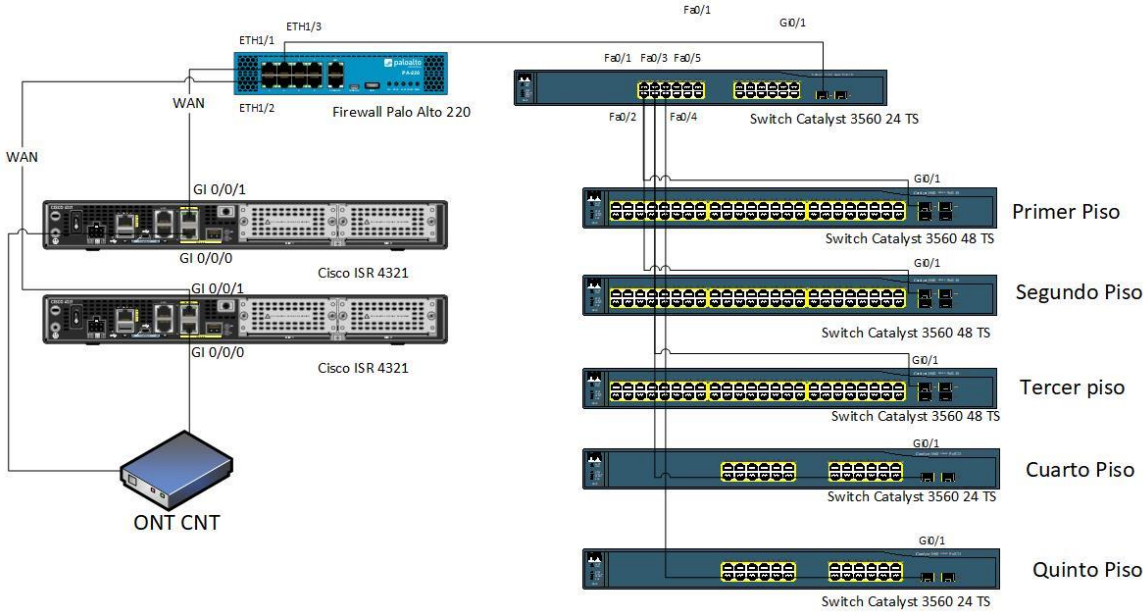
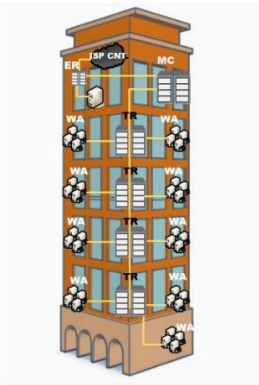


Diagrama físico de la red actual de la organización ARTKOS. Elaborador por: Francys Carrillo.

2.5 Diagrama físico de la red

Artkos cuenta con un cableado vertical como horizontal que se conecta a través del cableado estructurado dando a 120 puntos de conexión tipo ethernet. Esto mostrado en la figura 2.5

Figura 2.5 Sistema de cableado estructurado



Sistema de cableado estructurado actual de ARTKOS. Elaborado por: Francys Carrillo

2.6 Capa de enlace

2.6.1 Access Point

Para la red WLAN se utilizan diez APs del modelo Cisco Airnet 2800, teniendo dos por piso, estos están centralizados geográficamente para mantener una alta cobertura en cada planta.

Los APs se encuentran distribuidos de la siguiente manera: dos en preventas, financiero y delivery management; dos en talento humano, administrativo y legal; dos en tecnológico y seguridad; dos en gerencia y finalmente dos en Data Center, todos estos se detallan en la Tabla 2.3.

Tabla 2.3 Disponibilidad de los AP

Inspección		
Area	Cantidad	Observación
Primer Piso	2	Activo - Interior
Segundo Piso	2	Activo - Interior
Tercer Piso	2	Activo - Interior
Cuarto Piso	2	Activo - Interior
Quinto Piso	2	Activo - Interior

Cantidad de APs por piso en ARTKOS. Elaborado por: Francys Carrillo

2.7 Racks

El rack de Data Center se encuentra en el último piso este posee el enlace a internet ONT que se conecta a dos equipos Routers Cisco ISR 4321 y estos a su vez se conectan al equipo Firewall Palo Alto PA 220, este se comunica con el Switch Catalyst 3560 – 24 TS, el mismo se conecta a otro Switch de las mismas características, finalmente este interconecta los servidores a través de sus puestos FastEthernet, siendo los servidores: SNMP, SFTP, DNS, POP3, DHCP.

2.7.1 Rack de primer piso

Se encuentra un Switch Catalyst 3560 48 TS que brinda servicio a los usuarios de las áreas talento humano, administrativo y legal, además hay una conexión al subsuelo donde se despachan pedidos.

2.7.2 Rack de segundo piso

En este piso se encuentra un Switch Catalyst 3560 de cuarenta y ocho puertos brindando servicio a las áreas de preventas, financiero y delivery management, todas estas a través de cable UTP CAT 6.

2.7.3 Rack de tercer piso

En el piso actual hay un Switch Catalyst 3560 de cuarenta y ocho puertos dando servicio a las áreas de seguridad y tecnológicas, a través de cable UTP CAT 6.

2.7.4 Rack de cuarto piso

En este piso solo se brinda servicio al área de gerencia, teniendo un Switch Catalyst 3560 de veinte y cuatro puertos, conectado con cable UTP CAT 6.

2.8 Capa de red

Para el tráfico de red se utilizan dos Routers Cisco serie ISR-4321, el ISP proporciona la salida a internet, y este se conecta a los dos Routers que posee 2 Entradas Gigabit Ethernet. Ambos se conectan al Firewall Palo Alto PA 220 y al Switch central de 24 puertos, esto se detalla en la tabla 2.4.

Tabla 2.4 Conexión de puertos Routers Cisco ISR 4321

ROUTER	Puerto	Etiqueta	Etiqueta del puerto de interconexion
RA	Gi0/0/1	RA-FWPA	RA-FW-ETH1/1
	Gi0/0/0	RA-ONT	RA-ONT-ETH1
RB	Gi0/0/1	RB-FWPA	RB-FW-ETH1/2
	Gi0/0/0	RB-ONT	RB-ONT-ETH2

Puertos activos en Routers Cisco ISR 4321 en ARTKOS. Elaborado por: Francys Carrillo

2.8.1 Direccionamiento

Para dar acceso a internet y aplicaciones internas de la empresa, se configuraron distintas VLANS para dar seguimiento, administración a las diferentes áreas, teniendo así las IPs detalladas en la tabla 2.5.

Tabla 2.5 Direccionamiento de la organización ARTKOS

VLAN	Nombre	IP	Máscara
10	Telefonía	192.168.1.X	255.255.255.0
15	Servidores	192.168.10.X	255.255.255.0
30	Usuarios	192.168.30.X	255.255.255.0
26	Administradores	192.168.90.X	255.255.255.0
13	Salida Internet	10.244.10.X	255.255.255.252

Direccionamiento de VLANS. Elaborado por: Francys Carrillo

En la tabla 2.5 se muestra la segmentación por VLANs. Sin embargo, estas segmentaciones no están divididas por áreas o departamentos de ARTKOS.

2.9 Capa de aplicación

ARTKOS usa diferentes aplicaciones para sus hosts, para la seguridad en los mismos se usa MCAFEE, además posee otras aplicaciones para su uso frecuente como: Microsoft 365, WinSCP, Outlook y System center. Los mismos usan un firewall de la marca Palo Alto encargado de la seguridad y de gestionar el tráfico, dando permisos a los usuarios, para el acceso a los diferentes servicios, dependiendo el área.

2.10 Encuesta técnica Wireless

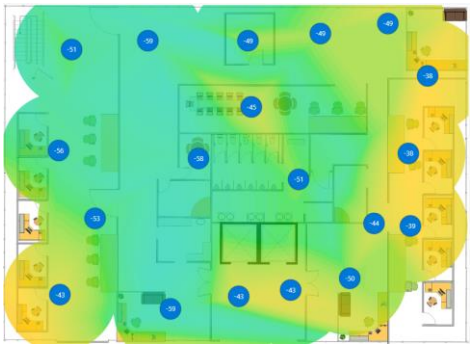
En el estudio inalámbrico TSS (Technical Site Survey) se muestra en rango de cobertura e irradiación de la señal, para esto se utilizó la herramienta informática NetSpot, que muestra un mapa con respecto a los diferentes puntos de acceso, identificando su señal y midiéndola. Siendo verde el rojo con mayor recepción, hasta bajar al azul donde no se tiene recepción. En la tabla 2.6 se observan los colores utilizados por el programa para crear el mapa de la señal.

Tabla 2.6

Rango de Intensidad	Color
-10 dBm a -30 dBm	
-31 dBm a -40 dBm	
- 41 dBm a -70 dBm	
-71 dBm a -90 dBm	

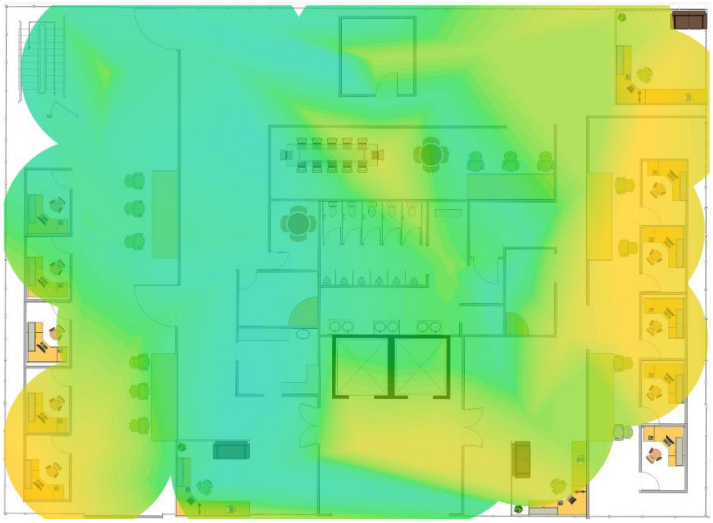
Colorimetría de la atenuación del piso uno hecha en Netspot. Elaborado por: Francys Carrillo

Figura 2.4 Estudio realizado en el piso uno.



APs existentes en el primer piso. Elaborado por Francys Carrillo

Figura 2.5 Mapa de Calor del primer piso.



Mapa de calor existente en el primer piso. Elaborado por: Francys Carrillo.

Como se muestran en las figuras 2.4 y 2.5 existe mucha atenuación en la señal WiFi, por lo que en los sectores verde turquesa no se llega a la señal adecuada, mientras que, en las zonas marcadas con amarillo existe una señal mediamente buena.

CAPÍTULO 3
REDISEÑO DE LA RED

3.1 Planificación de la red

Debido al crecimiento de la organización ésta a experimentado cambios en su infraestructura física y lógica, por lo que, los administradores de red han tenido que hacer ajustes a los equipos, así como al direccionamiento, sin embargo, al ser una red para una PYMES mediana, se tomó el diseño de red de Núcleo Colapsado.

3.1.1 Diseño bajo Cisco SAFE

3.1.1.1 Secure Services

Asegurar el servicio mediante la implementación de medidas de seguridad, y de disponibilidad de la red, para la presente se utilizará: ACLs ya que bloquean el tráfico no deseado, permitiendo tener un mayor control sobre la red. Port Security protege contra accesos no autorizados de conexión, Junto con estos HSRP se configura en caso de fallo del Switch de capa 3 y finalmente se configura EtherChannel para dar Alta Disponibilidad a la red.

3.1.1.2 Thread Defense

Este apartado incluye varias tecnologías para cubrir, como firewalls, IPS, y filtrado de contenido, para la presente se implementará: SNMP, puesto que permite la supervisión y gestión de la red. ACL entran en este apartado debido a que filtra el tráfico de la red. Además de IPS con filtrado por Signatures y un SYSLOG de los eventos ocurridos en el Switch.

3.1.1.3 Segmentación

Se refiere a la práctica de dividir la red en segmentos más pequeños o VLANs para la mitigación de propagación de amenazas. Para cubrir este apartado su utilizarán las ACLy VLANs, ya que contribuyen a la separación bajo responsabilidades de cada colaborador y disminuyen el impacto de un ataque.

3.1.1.4 Compliance

Este apartado se refiere a regulaciones o políticas específicas para la industria. Para la misma se utilizan Port Security, VLANs y ACL, puesto que, establecen políticas de acceso sobre la red.

3.1.1.5 Security Inteligence

Este indica el recopilar, analizar y utilizar información sobre amenazas y vulnerabilidades y su aplicación en la red. Para la misma se utilizará el Servidor SNMP que es propio de la empresa como un servidor SYSLOG, puesto que permite identificar patrones y posibles amenazas.

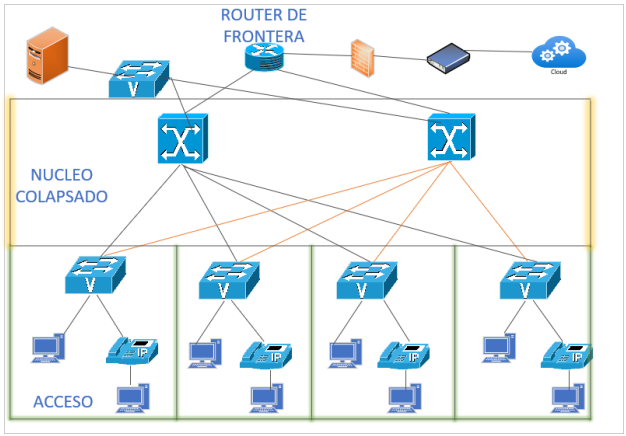
3.1.1.6 Management

Implica la administración de las actividades y recursos con base en la seguridad de la red, gestión de eventos y registros. Para este apartado su utilizará un servidor SYSLOG conectado al Switch de capa 3 para cubrir los acontecimientos dentro de la red. Así mismo un servidor VTP en el Switch ya indicado.

3.2 Diseño físico de la LAN

Para el rediseño se empleó el modelo empresarial de Cisco SAFE, en su sección de CAMPUS, donde se realizaron las modificaciones respecto al enfoque que tenía la red, quitando un Router, reubicando el Firewall y aumentando un Switch L3, como se muestra en la figura 3.1.

Figura 3.1 Topología lógica del rediseño.



Rediseño de la red. Elaborado por: Francys Carrillo.

3.2.1 Capa de acceso a la Red

Para la capa de acceso se mantendrá un switch por cada piso, este tendrá que ser segmentado por VLANS para cada departamento dependiendo el piso. Teniendo así en el primer piso: Talento humano, administrativo y legal. Mientras que en el segundo piso: preventas, financiero y Delivery Management. Consiguientemente en el tercer piso: tecnológicos y seguridad. Finalmente, en el cuarto piso: gerencia.

Ambos switches de núcleo colapsado se conectarán a los de acceso a través de fibra óptica monomodo. Mientras que, los switches de acceso se conectarán a través de fibra óptica Monomodo 652.D. Finalmente hacia los dispositivos finales se conectará a través de cable de red UTP CAT 6ª, los cuales ya se encuentran

3.2.2 Asignación de direcciones

Para el direccionamiento de ARTKOS se consideró la red clase B, puesto que esta es ideal para mediana empresas en crecimiento. Por lo cual se consideró la red 172.22.0.0/20 esta posee 4094 hosts utilizables puesto que dos están reservados para broadcast y red.

Esta red se segmenta para los diferentes departamentos de la empresa. Así mismo, se plantea la dirección IPV6 2023:ACAD:1234::/64.

Tabla 3.2 VLANs

N° PISO	DEPARTAMENTO	VLAN
PISO 1	Talento humano	Administrativo
	Administrativo	Administrativo
	Legal	Administrativo
PISO 2	Preventas	Operaciones
	Financiero	Administrativo
	Delivery Management	Operaciones
PISO 3	Técnológicos	TI
	Seguridad	TI
PISO 4	Gerencia	Gerencia
PISO 5	Data Center	TI
	Servicios otros	Wireless

Segmentación de VLANs por departamento. Elaborado por Francys Carrillo.

En la tabla 3.2 se muestra la segmentación realizada por departamentos y áreas que funcionan en ARTKOS, así mismo se muestran los pisos en los que funciona cada área y como será segmentada.

3.2.3 Direccionamiento

La tabla 3.3 muestra la distribución IP tanto IPv4 e IPv6 de las VLANs para cada segmento antes mencionado.

Tabla 3.3 Diseño de direccionamiento y VLAN

Departamentos/ Áreas	VLAN	IPV4	Netmask	IPV6
Administración	Vlan 90	172.22.10.0	255.255.255.0	2023:ACAD:1234:10:/64
Operaciones	Vlan 91	172.22.20.0	255.255.255.0	2023:ACAD:1234:20:/64
TI	Vlan 92	172.22.30.0	255.255.255.0	2023:ACAD:1234:30:/64
Gerencia	Vlan 93	172.22.40.0	255.255.255.0	2023:ACAD:1234:40:/64
Wireless	Vlan 94	172.22.50.0	255.255.255.0	2023:ACAD:1234:50:/64
Servidores	Vlan 95	172.22.60.0	255.255.255.0	2023:ACAD:1234:60:/64
VoIP	Vlan 96	172.22.70.0	255.255.255.0	2023:ACAD:1234:70:/64

Direccionamiento VLAN en IPv4 e IPv6 para los departamentos y áreas. Elaborado por: Francys Carrillo.

En la tabla 3.4 se indica la asignación de los puertos en el switch del primer piso para cada departamento: Administración, legal y Talento humano. así mismo, se asignaron a los APs para la red WLAN.

Tabla 3.4 Direccionamiento IPv4 Piso 1

Dispositivo	VLAN	Interfaz	Dirección	Máscara	Gateway	VoIP
Rack P1	Trunk all	Fa0/1,Fa0/3	Channel Group 2	255.255.255.0		
	Trunk all					
AP_P1_1	94	Fa0/40	172.22.50.1	255.255.255.0	172.22.50.100	
AP_P1_2	94	Fa0/41	172.22.50.2	255.255.255.0	172.22.50.101	
AP_P1_3	94	Fa0/42	172.22.50.3	255.255.255.0	172.22.50.102	
Dep_TH	90-96	Fa0/5-14	172.22.10.1-9	255.255.255.0	172.22.10.100	172.22.70.1-9
Dep_Admin	90-96	Fa0/15-25	172.22.10.10-22	255.255.255.0	172.22.10.101	172.22.70.10-22
Dep_Legal	90-96	Fa0/26-38	172.22.10.23-35	255.255.255.0	172.22.10.102	172.22.70.23-35

Direccionamiento IPv4 Piso. Elaborado por: Francys Carrillo.

En la tabla 3.5 se indica la asignación de los puertos en el switch del segundo piso para las áreas de: Financiero, Preventas, Delivery Management, así como los APs para la red inalámbrica.

Tabla 3.5 Direccionamiento IPv4 Segundo Piso

Dispositivo	VLAN	Interfaz	Dirección	Máscara	Gateway	VoIP
Rack P2	Trunk all	Fa0/1, Fa0/3	Channel Group 3	255.255.255.0		
	Trunk all					
AP_P4_1	94	Fa0/40	172.22.5.4	255.255.255.0	172.22.50.100	
AP_P4_2	94	Fa0/41	172.22.5.5	255.255.255.1	172.22.50.101	
AP_P4_3	94	Fa0/42	172.22.5.6	255.255.255.2	172.22.50.102	
Dep_PRE	91-96	Fa0/5-15	172.22.20.1-20	255.255.255.3	172.22.20.100	172.22.70.36-43
Dep_Fin	91-96	Fa0/16-30	172.22.20.21-45	255.255.255.4	172.22.20.100	172.22.70.44-51
DEP_DM	91-96	Fa0/31-40	172.22.20.46-50	255.255.255.5	172.22.20.100	172.22.70.52-60

Direccionamiento IPv4 en el Segundo piso. Elaborador por: Francys Carrillo.

En la tabla 3.6 se muestra la asignación de VLANs, puertos y etiquetas, esto para las áreas de: TI, Seguridad.

Tabla 3.6 Direccionamiento IPv4 Tercer Piso

Dispositivo	VLAN	Interfaz	Dirección	Máscara	Gateway	VoIP
Rack P3	Trunk all	Fa0/1, Fa0/3	Channel Group 4	255.255.255.0		
	Trunk all					
AP_P3_1	94	Fa0/41	172.22.5.7	255.255.255.0	172.22.50.100	
AP_P3_2	94	Fa0/42	172.22.5.8	255.255.255.0	172.22.50.100	
AP_P3_3	94	Fa0/43	172.22.5.9	255.255.255.0	172.22.50.100	
Dep_IT	92-96	Fa0/5-25	172.22.3.1-19	255.255.255.0	172.22.30.100	172.22.70.69-89
Dep_SEC	92-96	Fa0/26-40	172.22.3.20-35	255.255.255.0	172.22.30.100	172.22.70.90-105

Direccionamiento IPv4 Tercer Piso. Elaborado Por: Francys Carrillo.

En la tabla 3.7 se muestra la asignación de VLANs, para el cuarto piso, en el área de Gerencia.

Tabla 3.7 Direccionamiento IPv4 Cuarto Piso.

Dispositivo	VLAN	Interfaz	Dirección	Máscara	Gateway	VoIP
Rack P4	Trunk all	Fa0/1, Fa0/3	Channel Group 5	255.255.255.0		
	Trunk all					
AP_P4_1	94	Fa0/40	172.22.5.10	255.255.255.0	172.22.50.100	
AP_P4_2	94	Fa0/41	172.22.5.11	255.255.255.0	172.22.50.101	
AP_P4_3	94	Fa0/42	172.22.5.12	255.255.255.0	172.22.50.102	
Dep_Ger	93	Fa0/5-25	172.22.4.1-20	255.255.255.0	172.22.40.100	172.22.70.106-120

Direccionamiento IPv4 Cuarto piso. Elaborado por: Francys Carrillo.

En la tabla 3.8 se muestra la asignación de VLANs, para el quinto piso donde se encuentra el Data Center.

Tabla 3.8 Direccionamiento IPv4 Quinto Piso.

Dispositivo	VLAN	Interfaz	Dirección	Máscara	Gateway
Rack P5	Trunk all Trunk all	Fa0/1,Fa0/3	Channel Group 6	255.255.255.0	
AP_P5_1	94	Fa0/40	172.22.5.10	255.255.255.0	172.22.50.100
AP_P5_2	94	Fa0/41	172.22.5.11	255.255.255.0	172.22.50.100
Dep_DC	95	Fa0/1-15	172.22.6.1-10	255.255.255.0	172.22.60.100

Direccionamiento IPv4 para el Data Center. Elaborado por Francys Carrillo.

En la tabla 3.9 se encuentra la asignación del direccionamiento en IPv6 para las áreas de: Talento humano, administrativo y legal. Se tomó el segmento de red: 2023:ACAD:1234::/64. Sin embargo, cabe aclarar que esta puede cambiar, puesto que el ISP puede poner el sufijo de red, esto por si la organización lo requiera.

Tabla 3.9 Direccionamiento IPv6 Primer Piso.

Dispositivo	VLAN	Interfaz	Dirección	Gateway
Rack P1	Trunk all Trunk all	Fa0/1,Fa0/3	Channel Group 2	
AP_P1_1	94	Fa0/40	2023:ACAD:1234:50::1/64	2023:ACAD:1234:50::100/64
AP_P1_2	94	Fa0/41	2023:ACAD:1234:50::2/64	2023:ACAD:1234:50::100/64
AP_P1_3	94	Fa0/42	2023:ACAD:1234:50::3/64	2023:ACAD:1234:50::100/64
Dep_TH	90-96	Fa0/5-14	2023:ACAD:1234:10::1-9/64	2023:ACAD:1234:10::100/64
Dep_Admin	90-96	Fa0/15-25	2023:ACAD:1234:10::10 -22/64	2023:ACAD:1234:10::100/64
Dep_Legal	90-96	Fa0/26-38	2023:ACAD:1234:10::23 - 35/64	2023:ACAD:1234:10::100/64

Direccionamiento para las áreas de: Administración, TH y Legal. Elaborado por: Francys Carrillo

En la tabla 3.10 se encuentra la asignación de IPv6 para las áreas de: Preventas, finanzas y delivery management.

Tabla 3.10 Direccionamiento IPv6 Segundo piso.

Dispositivo	VLAN	Interfaz	Dirección	Gateway
Rack P2	Trunk all Trunk all	Fa0/1, Fa0/3	Channel Group 3	
AP_P4_1	94	Fa0/40	2023:ACAD:1234:50::4/64	2023:ACAD:1234:50::100/64
AP_P4_2	94	Fa0/41	2023:ACAD:1234:50::5/64	2023:ACAD:1234:50::100/64
AP_P4_3	94	Fa0/42	2023:ACAD:1234:50::6/64	2023:ACAD:1234:50::100/64
Dep_PRE	91-96	Fa0/5-15	2023:ACAD:1234:20::1-20/64	2023:ACAD:1234:10::100/64
Dep_Fin	91-96	Fa0/16-30	2023:ACAD:1234:20::21-38/64	2023:ACAD:1234:10::100/64
DEP_DM	91-96	Fa0/31-40	2023:ACAD:1234:20::39-42/64	2023:ACAD:1234:10::100/64

Direccionamiento para las áreas de: Preventas, Financiero y Delivery Management. Elaborado por Francys Carrillo.

La tabla 3.11 muestra la asignación de IPv6 para el switch para las áreas de: TI y Seguridad en el tercer piso.

Tabla 3.11 Direccionamiento IPv6 Tercer Piso.

Dispositivo	VLAN	Interfaz	Dirección	Gateway
Rack P3	Trunk all Trunk all	Fa0/1, Fa0/3	Channel Group 4	
AP_P3_1	94	Fa0/41	2023:ACAD:1234:50::7/64	2023:ACAD:1234:50::100/64
AP_P3_2	94	Fa0/42	2023:ACAD:1234:50::8/64	2023:ACAD:1234:50::100/64
AP_P3_3	94	Fa0/43	2023:ACAD:1234:50::9/64	2023:ACAD:1234:50::100/64
Dep_IT	92-96	Fa0/5-25	2023:ACAD:1234:30::1-20/64	2023:ACAD:1234:30::100/64
Dep_SEC	92-96	Fa0/26-40	2023:ACAD:1234:30::21-35/64	2023:ACAD:1234:30::100/64

Direccionamiento para las áreas de TI y Seguridad. Elaborado por: Francys Carrillo.

La tabla 3.12 muestra el direccionamiento IPv6 para el cuarto piso donde se encuentra el área de gerencia.

Tabla 3.12 Direccionamiento IPv6 Cuarto Piso.

Dispositivo	VLAN	Interfaz	Dirección	Gateway
Rack P4	Trunk all Trunk all	Fa0/1, Fa0/3	Channel Group 5	
AP_P4_1	94	Fa0/40	2023:ACAD:1234:50::10/64	2023:ACAD:1234:50::100/64
AP_P4_2	94	Fa0/41	2023:ACAD:1234:50::11/64	2023:ACAD:1234:50::100/64
AP_P4_3	94	Fa0/42	2023:ACAD:1234:50::12/64	2023:ACAD:1234:50::100/64
Dep_Ger	93	Fa0/5-25	2023:ACAD:1234:40::1-15/64	2023:ACAD:1234:40::100/64

Direccionamiento para el área de gerencia. Elaborado por: Francys Carrillo.

Finalmente, la tabla 3.13 muestra el direccionamiento IPv6 para el Data Center, ubicado en el quinto piso.

Tabla 3.13 Direccionamiento IPv6 para el Quinto Piso.

Dispositivo	VLAN	Interfaz	Dirección	Gateway
Rack P5	Trunk all Trunk all	Fa0/1,Fa0/3	Channel Group 6	
AP_P5_1	94	Fa0/40	2023:ACAD:1234:50::13/64	2023:ACAD:1234:50::100/64
AP_P5_2	94	Fa0/41	2023:ACAD:1234:50::14/64	2023:ACAD:1234:50::100/64
Dep_DC	95	Fa0/1-15	2023:ACAD:1234:60::1-10/64	2023:ACAD:1234:60::100/64

Direccionamiento para el Data Center. Elaborado por: Francys Carrillo.

Las tablas de direccionamiento muestran cómo se segmentaron las VLAN, esto para no tener una red plana, con más seguridad y poder administrarla mejor.

3.2.4 Selección de Dispositivos

En el diseño físico se tomarán en cuenta los equipos que cumplan con los requerimientos para la red propuesta y que se ajusten a esta mediana empresa, así mismo, se reutilizarán los equipos que no tengan un EoL corto.

3.2.4.1 Dimensionamiento de tráfico

ARTKOS funciona en un horario de oficina de 8h00 hasta 17h00, teniendo en cuenta el direccionamiento existen 92 hosts, sin embargo, se considera que hay colaboradores que se conectan a la red de la empresa a través de la red Wireless. En la tabla 3.14 se encontró el ancho de banda necesario para ARTKOS, tomando en cuenta el factor de simultaneidad y la carga total. Cabe recalcar los valores típicos de banda ancha para los servicios que circulan por la red.

Tabla 3.14 Dimensionamiento de tráfico ARTKOS.

CBWFQ	Tipo	Reserva	Factor de simultaneidad	MBPS mínimos necesarios
75%	Audio y video	7%	8,05	2,576
	Protocolos de red	3%	3,45	0,1725
	VoIP	10%	11,5	1,472
	Transferencia de archivos	25%	28,75	287,5
	WEB	15%	17,25	86,25
	Correo	15%	17,25	86,25
25%	Reserva	25%	28,75	57,5
	Total	100%	115	521,7205

Dimensionamiento segmentado por tipo de datos. Elaborado por: Francys Carrillo

Como se muestra en la tabla 3.14 se necesitan 524 Mbps para la red. Sin embargo, este cálculo es una aproximación, puesto que el factor de simultaneidad puede cambiar, por lo que para tener una conexión de red más estable se necesita equipos que puedan procesar con una velocidad mayor a la mencionada, así mismo se solicita al ISP una conexión de salida a internet de mayor valor. Todos estos cálculos se realizaron base a la ecuación 3.1.

$$Ancho\ de\ banda = \sum_{i=1}^{n}(Porcentaje_i \times N_i \times B_i) \qquad \textbf{Ec. 3.1}$$

Donde:

$Porcentaje_i$ es el porcentaje de usuarios utilizando simultáneamente un tipo de dato.

N_i es el número total de usuarios que participan en el total de la red.

B_i es el ancho de banda requerido para cada tipo de dato.

3.2.4.2 Dimensionamiento de Tráfico VoIP

Para el cálculo de los Erlangs necesarios se tomó en cuenta el promedio de llamadas por hora y el promedio de duración de las llamadas de la misma. Teniendo así 6 llamadas por hora con una duración de 4 minutos. Teniendo así la ecuación 2.

$$A_1 = n°LH * TL * (\frac{1}{60}) \quad \textbf{Ec. 3.2}$$

Siendo así:

$n°LH$ = El número de llamadas por hora.

TL = Tiempo de llamada.

Finalmente:

$$A_1 = 6 * 4 * (\frac{1}{60}) \quad \textbf{Ec. 3.3}$$

$$A_1 = 0.4\ Erlang$$

Mientras, para el cálculo del volumen de tráfico IP se tiene la ecuación:

$$A = A_1 * NU$$

Donde:

A_1= Tráfico de telefonía IP¨

NU = Número de usuarios

Siendo así:

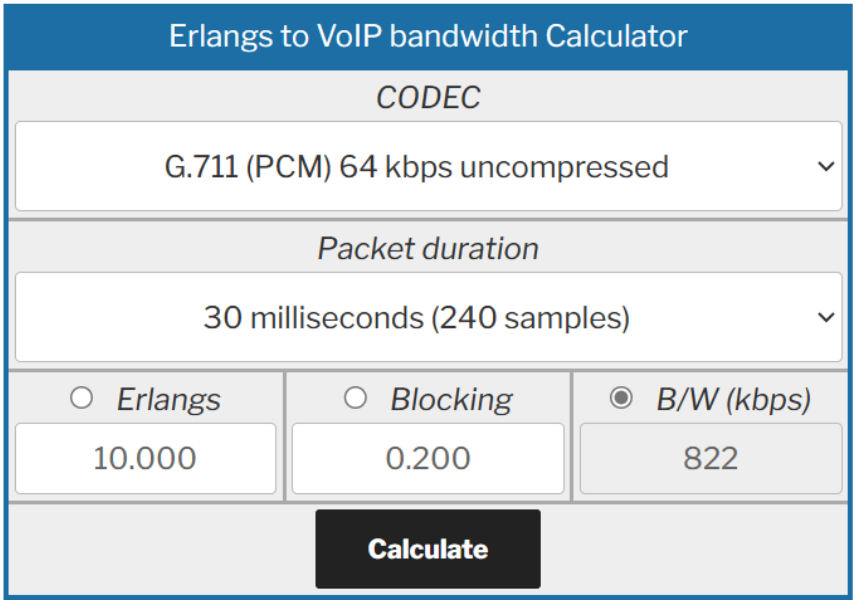
$$A = 0.4 * 25$$

$$A = 10$$

Como se detalló en la tabla 3.14 el número de usuarios aproximado es de 12. Sin embargo, por términos prácticos se debe dejar reservado espacio para más, teniendo así 25 aproximadamente.

El cálculo de 10 Erlangs permite calcular el número de líneas troncales, por lo que se tomó en cuenta el 2% de falla para el bloqueo de llamadas. Obteniendo el cálculo en la figura 3.2.

Figura 3.2 Cálculo de Ancho de banda aproximado.



Calculo con los parámetros encontrados antes. Elaborado por: Francys Carrillo.

En la figura 3.2 se muestra el ancho de banda necesario para las horas pico en llamadas simultaneas, teniendo así 822 Kbps.

3.2.4.3 Dispositivos

Se tomará en consideración los equipos que ya no tengan soporte del proveedor, así como los dispositivos que estén próximos a terminar su soporte. Para esto se utilizaron tablas de decisión, con lo que se elegirán los dispositivos de acceso, y núcleo colapsado, también para los APs, todo esto con el enfoque de las necesidades de la empresa. Todo esto basándose en el anexo 4,5 y 6.

3.2.4.4 Dispositivos de acceso

En la tabla 3.15 se muestra los parámetros para los switches de acceso, teniendo los puntajes de: 1 (regular), 2 (bueno), 3 (excelente).

En la misma el que mejor puntuación tiene es el Cisco SG220.50P, así mismo se muestra en el anexo 5 los parámetros indicados por los fabricantes.

Tabla 3.15 Tabla de decisión para Switches de acceso.

	Dispositivos L2		
Parámetros	HPE OfficeConnect 1950	CISCO SG220 -50P	D-Link DGS-1210
Consumo de energia	3	1	2
Densidad Portuaria	2	3	1
Velocidad	3	3	3
Seguridad	2	3	2
QoS	1	3	2
Alimentación redundante	2	3	2
Precio	2	1	3
Total	15	17	15

Tabla de decisión de los switches de acceso de Huawei, Cisco, Juniper. Elaborado por: Francys Carrillo.

3.2.4.5 Dispositivos de Núcleo Colapsado

Para el switch de núcleo colapsado se utilizará el Cisco 38250 – 48XS, puesto que tiene parámetros óptimos para esta red, igualmente la tabla 3.16 muestra la tabla de decisión para el switch capa 3, cabe recalcar que la compañía mantiene equipos cisco en su mayoría y se tiene tendencia al mismo.

Tabla 3.16 Tabla de decisión para Switch de Núcleo Colapsado.

	Dispositivos L3		
Parámetros	Aruba 2930F	Cisco 3850-48XS	Juniper Networks EX4550
Consumo de energia	3	2	3
Densidad Portuaria	1	3	2
Velocidad de Puerto	3	3	3
Seguridad	2	3	2
QoS	2	3	2
PSR (POWER SUPPLY	2	3	2
Costos	2	2	3
	15	19	17

Tabla de decisión de switches de núcleo colapsado de Aruba, Cisco, Juniper. Elaborado por: Francys Carrillo.

Como se muestra en la tabla 3.16 Cisco 9300 24S posee la calificación más alta con 19, cumple con la segmentación de VLAN, posee módulos para fibra óptica, EtherChannel, para crear redundancia en enlaces y mayor banda ancha.

3.2.4.6 Dispositivos WLAN

Para el apartado de WLAN se tomó en cuenta a los fabricantes Cisco y TP-Link. Las características de estos se encuentran en el Anexo 6. En base a dicho anexo se estableció la tabla de decisión. Tabla 3.17, las características comparadas como: Licencia, seguridad, PoE, y los mencionados en dicha tabla.

Tabla 3.17 Tabla de decisión para la red WLAN.

	Dispositivos	
Caracteristicas	Cisco 3504	EAP660 HD
Licencia	2	3
Interfaces Gigabit	3	3
Clientes simultaneos	3	2
PoE	3	3
Autenticacion	2	3
Precio	2	3
Total	15	17

Tabla de decisión entre Cisco y TP-Link. Elaborado por: Francys Carrillo.

El dispositivo a utilizar será el TP-Link EAP660 HD, ya que posee características similares a modelo de Cisco. Sin embargo, el precio del primero es mucho menor y con buenas prestaciones. Además de poseer el Controlador OMADA.

3.2.4.7 Transceptor

Finalmente se selecciona el transceptor para el núcleo colapsado que será conectado mediante módulos de FO, los cuales si indican sus características en la tabla 3.18. Siendo así de la marca Ubiquiti, un UF-SM-10 G.

Tabla 3.18 Características del transceptor.

Característica del UF-SM-10G	
Marca	Ubiquiti
Tipo de conector	LC/UPC Dual
Velocidad de transferencia	10 GB
Distancia	10 Km

Tabla de características dadas por el proveedor. Elaborado por: Francys Carrillo.

3.2.5 Cableado Vertical

En cuanto al cableado de Backbone se tomó en cuenta el medio de transmisión Fibra óptica, las características para el mismo es una FO Monomodo, esta permite la transmisión a grandes distancias, estas siguen la norma G652 D, teniendo así un menor índice de atenuación, como se muestra en la tabla 3.19.

Tabla 3.19 Perdidas en dB por Kilometro

FO Monomodo		
Atenuación por KM	1310	<= 0,35 dB
	1550	<=0,21 dB
	850	<= 3 dB

Tabla de perdidas en FO de diferentes longitudes de onda. Elaborado por: Francys Carrillo.

Para el despliegue en cuanto a Switches de acceso y núcleo colapsado se utilizará este medio de transmisión, ya que ambos admiten módulos SFP y su velocidad de transmisión es mayor a la del cobre.

3.2.6 Cableado Horizontal

Para este apartado se utilizará cableado UTP CAT 6, este se conectará desde el switch de acceso con un Patch Panel hasta los dispositivos finales a través de la infraestructura para el cableado estructurado para cada área, así mismo estos darán conectividad a los equipos Wireless, AP.

El cableado CAT 6A tendrá un apantallamiento de tipo FTP, esto con el fin de protegerlo de variaciones electromagnéticas, estos pueden recorrer hasta 100 metros y para su conexión se utilizan conectores tipo RJ-45, todos estos viajarán por las bandejas de conectividad que posee la institución. En la figura 3.4 se muestra el diseño del cableado en el piso 2, cabe mencionar que los otros pisos tienen la estructura muy similar. La figura 3.3 muestra la simbología utilizada para el rediseño.

Figura 3.3 Simbología del cableado.

Simbolo	Descripcion
	Conexión a datos
	Acces Point
	Rack de TI
	Bandeja de techo

Simbología para el rediseño del cableado de la red. Elaborado por: Francys Carrillo.

Figura 3.4 Rediseño del cableado.

Rediseño del cableado con la simbología para ARTKOS. Elaborado por: Francys Carrillo

3.2.7 Diseño de Capa de Acceso

3.2.7.1 EtherChannel

Es una tecnología que permite agrupar varios enlaces físicos y convertirlos en uno lógico, aumentando así su ancha de banda también. Además, aplica redundancia en los puertos ya que, si llega caer algún enlace físico, el enlace asociado al puerto EtherChannel sigue en funcionamiento hasta restablecer el enlace caído.

Las tablas 3.2 hasta 3.13 muestran los direccionamientos EtherChannel de lo switches de capa 2, mientras que la tabla 3.20 muestra la tabla de direccionamiento de EtherChannel en el switch de capa 3. (Kurniawan, 2021)

Tabla 3.20 Asignación EtherChannel

Dispositiv	Interfaz	Channel Group
SWL3-1	Fa0/1, Fa0/6	Channel Group 2
	Fa0/2, Fa0/7	Channel Group 3
	Fa0/3, Fa0/8	Channel Group 4
	Fa0/4, Fa0/9	Channel Group 5
	Fa0/5, Fa0/10	Channel Group 6
	Fa0/15, Fa0/16	Channel Group 1
SWL3-2	Fa0/15, Fa0/16	Channel Group 1

Selección de interfaces en una lógica. Elaborado por: Francys Carrillo.

La tabla 3.20 muestra que en el switch de capa tres se agregaron seis Channel Group, esto convirtiendo doce interfaces físicas en seis lógicas, dando redundancia a los enlaces y a su ancho de banda, además en el otro switch de capa 3 también se creó un enlace EtherChannel hacia el Switch L3-1. Todo esto a través de LACP, que es la comunicación común entre distintas marcas para EtherChannel.

3.2.7.2 VTP

VTP (VLAN Trunking Protocol) es un protocolo que permite el intercambio de información de las VLANs. Esta funciona a través de dominios, los cuales permiten que los clientes solo reciban la información de dicho dominio, este protocolo debe configurarse en un dispositivo como Servidor y en los demás como cliente. Para la presente se configuraron a los switches de capa 3 como servidores y a los switches de capa 2 como clientes.

3.2.7.3 VLAN

Las VLAN (Virtual Local Área Network) es una técnica de segmentación de redes, esta divide una red física en segmentos virtuales independientes. Estas pueden comportarse de la manera en la que el administrador las configure de manera independiente cada uno. Esta se muestra en la tabla 2.8.

3.2.7.4 Port Security

Es una funcionalidad de los switches que permite controlar el acceso a los puertos del mismo, este funciona a través de las direcciones MAC de los dispositivos finales. El switch aprende un número máximo de direcciones, estas configuradas previamente, cuando se dicha cifra el switch bloquea el puerto. También puede aprender la MAC que se conectará a la interfaz, bloqueando así las demás. Para la presente se coloca que el switch pueda aprender dos direcciones MAC.

3.2.8 Capa de Internet

En el diseño de capa de internet se muestran los procesos utilizados para optimizar a la red, para la presente se utilizan: SVI, HSRP, DSCP.

3.2.8.1 SVI

SVI (Switched Virtual Interface) es una técnica en la que se configura una IP a una VLAN, esta funciona como Gateway y permite el enrutamiento de tráfico entre las VLANs. EL direccionamiento de las mismas esta especificado en la tabla 2.8, así mismo en las tablas de direccionamiento.

3.2.8.2 HSRP

Es un protocolo de enrutamiento que proporciona redundancia de red, permitiendo que el tráfico se recupere de manera rápida. Este protocolo actúa entre los Switches de Capa 3 conectados en primer salto. Uno actúa de manera activa y los otros actúan de manera pasiva, configurándose con prioridad, es decir, cuando el primer switch falla, pueden activarse alguno de los que lleven dicho protocolo, configurando cuál de ellos previamente. Para le presente el Switch L3-1 esta como activo y el Switch L3-2 está en espera.

3.2.8.3 QoS

QoS (Quality of Service) este término hace referencia a las tecnologías y técnicas que se utilizan para manejar el tráfico de red, dando prioridad y control sobre diferentes características de la misma.

La compañía tiene un horario laboral de 8H00 a 17H:00 por lo que se estima las horas de carga en 8 horas, a través de la red circulan diferentes tipos de datos, por lo que se estima el ancho de banda típico para cada uno, además se estima el crecimiento para 5 años en un 10%.

Tabla 3.21 Ancho de banda por aplicación.

Tipo	Ancho de banda
Audio y video	0,32
Protocolos de red	0,05
VoIP	0,128
Transferencia de archivos	10
WEB	5
Correo	5
Reserva	2

Ancho de banda típico por tráfico de red. Elaborado por: Francys Carrillo.

La tabla 3.21 muestra el ancho de banda por cada tipo de tráfico que se encuentra en la red, además se deja un apartado de reserva por cualquier fluctuación en la misma.

A través de la tabla 3.14 se estimó el ancho de banda necesario para la red, así como el ancho de banda individual típico por cada tipo de dato, esto a través de las ecuaciones 3.4

$$Fs = NH * CT \qquad \text{Ec. 3.4}$$

Donde:

Fs = Factor de simultaneidad

NH = Número de hosts

$CT =$ Carga Total.

Además de la ecuación 3.5 se encontró los MBPS mínimos necesarios para la red.

$$MBPS_{min} = Fs\ x\ AB_T \qquad \text{Ec. 3.5}$$

Donde:

$MBPS_{min}$ = MBPS mínimos

FS = Factor de Simultaneidad

AB_t= Ancho de Banda Típico

Finalmente se tiene la ecuación 3.6 ya con el cálculo del crecimiento del 10% para cinco años.

$$CA_{A*P} = (MBPS_{min} * Y * P) + MBPS_{min}$$

Donde:

CA_{A*P}= Crecimiento Anual del Ancho de Banda

$MBPS_{min}$= MBPS mínimos

Y= Años

P= Porcentaje de crecimiento estimado

A través de todas estas ecuaciones se tiene la tabla 3.22.

Tabla 3.22 Crecimiento estimado para 5 años.

Tipo	Reserva	Factor de simultaneidad	MBPS mínimos necesarios	C.A del 10% para 5 años
Audio y video	7%	8,05	2,576	3,864
Protocolos de red	3%	3,45	0,1725	0,25875
VoIP	10%	11,5	1,472	2,208
Transferencia de archivos	25%	28,75	287,5	431,25
WEB	15%	17,25	86,25	129,375
Correo	15%	17,25	86,25	129,375
Reserva	25%	28,75	57,5	86,25
Total	100%	115	521,7205	782,58075

Crecimiento del Ancho de Banda bajo Tipo de Datos. Elaborado por: Francys Carrillo

Las aplicaciones más utilizadas en Artkos se presentan en la tabla 3.23

Tabla 3.23 Aplicaciones utilizadas en ARTKOS

Servicio	Aplicación	Protocolos
Correo	Outlook	POP3
Web	Página Corporativa - Youtube	HTTP, HTTPS
Transferencia de Archivos	WinSCP	SFT, SFTP
VoIP	Softphone	H323, SKINNY
Audio y Video	Teams	RTP
Protocolos de red	MS Windows Server	ICMP, DHCP, DNS, SSH

Aplicaciones utilizadas en Artkos con sus protocolos de red. Elaborado por: Francys Carrillo.

3.2.8.4 DSCP

DSCP (Differentiated Services Code Point) es un campo de encabezo de los paquetes IP que se emplea para dar priorización y diferenciación de los paquetes de datos de la red. Este permite establecer QoS dentro de la red.

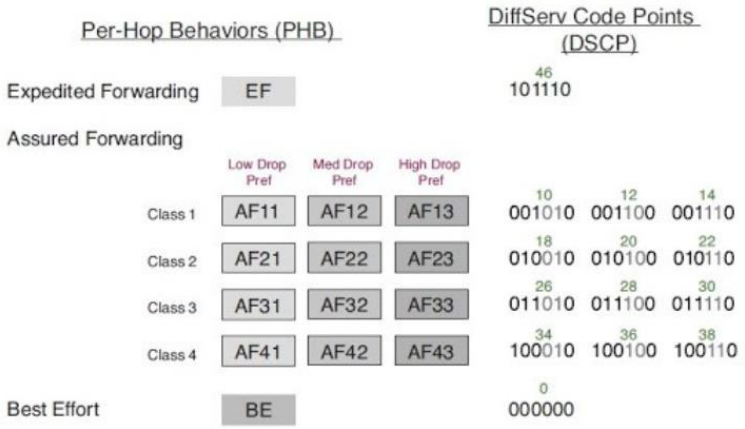
Servicios diferenciados, es un modelo de QoS que gestiona y prioriza el tráfico basándose en clases o niveles de servicios, este se caracteriza por dar encabezados a los paquetes de datos en IPv4 o IPv6, esta marca y clasifica los paquetes según el Código de servicio DSCP (Differentiated Services Code Point), los dispositivos intermediaros utilizan dichos marcadores para utilizar políticas de enrutamiento, asignación de ancho de banda y priorización de tráfico. (Milán, 2021)

Esta marca los paquetes según:

- AF: Renvío de paquetes con clasificación ideal para Vídeo, conferencia y datos. Este se maneja por valores asociados de 31,21,41, entre otros.
- CS: Maneja el tráfico en 7 niveles desde el CS0 hasta el CS7
- EF: Este tipo de manejo indica que el paquete es urgente, el servicio es garantizado de extremo a extremo y la pérdida es mínima.

Para la presente se utilizará AF, puesto que esta es más granular en los enfoques de QoS que permite dar valores pertinentes para priorización y descarte de los paquetes. También se utilizará EF puesto que este es muy favorable para VoIP, mientras que CS no será considerado para la presente puesto que no es tan granular y es una designación más antigua. Los valores de AF se tomarán guiándose de la figura 3.6. Esta indica el valor siguiente de AF, donde se muestra la prioridad de descarte también.

Figura 3.6 Valores de AF en PHB y DSCP



Priorización de paquetes en PHB y DSCP. Tomado de: Cisco Configuración de QoS.

3.2.8.9 Marcaje de QoS

Para la presente se dividió la clase de tráfico usado en la empresa, así mismo se determinaron los valores de prioridad y descarte de los mismos y su clase, los mismos se detallan en la tabla 3.24.

Tabla 3.24 Marcaje QoS

Clase de Tràfico	Capa 3	Valor DSCP	Clase
Correo	AF31	26	3
Web	AF21	18	2
Transferencia de Archivos	AF31	26	3
VoIP	EF	46	5
Audio y Video	AF41	34	4
Protocolos de red	AF11	10	1

Marcaje QoS por valor DSCP tomando AF. Elaborado por: Francys Carrillo.

En la tabla 3.24 se muestra el marcaje DSCP de tipo AF, donde los apartados Correo y Transferencia de archivos se los marca con AF 31 (011010) dando un valor de 26 en decimal, catalogando con prioridad media alta siendo los tres primeros Bits como IP Precedence y los siguientes Bits con mínima probabilidad de descarte.

Para los servicios WEB se marca con AF 21 (010010) teniendo un valor de 18 en decimal. Siendo los primeros 3 Bits de IP Precedence y los siguientes Bits indican prioridad media, con descarte de paquete de datos con bajo porcentaje de probabilidad de descarte.

Mientras que en los servicios VoIP se marca con EF (101110) teniendo un valor de 46 en decimal, con 3 Bits de IP Precedence y los siguientes Bits indican un nivel de prioridad extremadamente alto frente a otros tipos de tráfico.

Para el tráfico Audio y Video se marca con AF 41 (100010) teniendo un valor de 34 en decimal, con los primeros 3 Bits de IP Precedence y los siguientes indican un nivel de prioridad alta, con una probabilidad de descarte de paquetes mínima.

3.2.8.10 MQC

Model Queueing Class Es una metodología de configuración de red que permite la manipulación del tráfico basado en políticas de QoS. Para la presente se definieron clases de tráfico basadas en protocolos utilizados por cada tráfico, luego se asocian a una política de QoS, en dicha política se asigna un ancho de banda para cada clase, además se incluye los valores de DSCP y el ancho de banda para las mismas. Finalmente se agrega la política a una interfaz. (Cisco, 2023)

3.2.8.11 Modelos utilizados en QoS

En la tabla 3.25 se muestra los métodos empleados para el diseño de QoS, según las necesidades de la empresa.

Tabla 3.25 Métodos utilizados para QoS

Modelo	**Diffserv**
Clasificación	Tipo de servicio
	Prioridad del servicio
	Protocolos utilizados en el servicio
Marcaje	DSCP
Encolamiento	CBWFQ
Configuración	MQC

Modelos utilizados para definir la QoS dentro del DiffServ. Elaborado por: Francys Carrillo.

3.2.9 Capa de Transporte

3.2.9.9 ACL

ACL (Access Control List) listas de control de acceso. Permiten o deniegan el tráfico de red basadas en reglas establecidas. Estas se dividen en: extendidas y estándar. Siendo las primeras las que tienen una filtración más amplia en cuestión de criterios. (Laksono, 2020)

Las listas de control de acceso se gestionaron por protocolo utilizado en cada área y se implementó sobre cada interfaz del switch de capa 3, puesto que cada interfaz daba conectividad a los switches de cada piso, teniendo así la tabla 3.26. Además, este control de acceso sobre el tráfico también se basó en la tabla 3.20.

Tabla 3.26 ACL creadas en switch de capa 3.

N° ACL	TIPO DE TRAFICO PERMITIDO
ACL101	TRAFICO de RED, VoIP, CORREO, WEB
ACL102	TRAFICO de RED, VoIP, TRANSFERENCIA DE ARCHIVOS, WEB
ACL103	TODO
ACL104	TODO
ACL105	TRAFICO DE RED, TRANSFERENCIA DE ARCHIVOS, CORREO

Tráfico permitido en cada Access List para cada área. Elaborado por: Francys Carrillo.

Como se observa en la tabla 3.23 se gestionó el acceso a cierto de tráfico, excepto en las áreas de Ti y Gerencia, por ser áreas prioritarias.

3.2.10 Capa de aplicación

3.2.10.1 SSH

SSH es un protocolo de administración remota de red, el mismo establece un nivel de privilegios para sus conexiones, además de establecer usuarios y contraseñas.

3.2.10.2 SYSLOG & IPS

Para el IPS se utilizarán las firmas proporcionadas por Cisco para los protocolos a utilizarse por departamentos, así mismo cuando ocurra algún evento relacionado con dichas firmas se enviará un mensaje al servidor SYSLOG.

3.2.11 WLAN

Para el diseño WLAN se aplican las mismas políticas de servicio, ACL, y demás configurador previamente, puesto que dichas políticas están asentadas en el switch de capa 3, sin embargo, se muestra la tabla 3.27 para indicar el grupo al que pertenece cada AP.

3.2.11.1 WLAN Segura

Para este apartado OMODA tiene la posibilidad de crear un Portal Cautivo, este mismo puede conectarse a RADIUS para la gestión de los usuarios. Cada usuario Radius será vinculado a un miembro de la organización. Como se muestra en la tabla 3.27.

Tabla 3.27 Usuarios Radius

Usuario_Radius	Pass	Usuario
atk_01	@tK_01	David_Cobo
atk_02	@tK_02	Daniel_Chela
atk_03	@tK_03	Maite_Navas
atk_04	@tK_04	Danny_Sarango
atk_05	@tK_05	Edwin_Rodriguez

Usuarios de Artkos vinculados a un Usuario Radius. Elaborador por: Francys Carrillo.

3.2.11.2 WLAN Escalable

Para el diseño en este apartado se escoge el tipo de red controlada, puesto que esta al conectar un AP al controlador este puede fácilmente dar servicio gestionando los grupos de AP mencionado en el controlador, así mismo se crearon los grupos de AP para cada piso del edificio como se ve en la figura 3.28. OMODA es el controlador escogido, el cual permite la gestión centralizada desde el dispositivo OMODA, hasta un servidor OMODA.

Tabla 3.28

Grupo	APs
AP_P1	AP_P1_1
	AP_P1_2
	AP_P1_3
AP_P2	AP_P2_1
	AP_P2_2
	AP_P2_3
AP_P3	AP_P3_1
	AP_P3_2
	AP_P3_3
AP_P4	AP_P4_1
	AP_P4_2
	AP_P4_3
AP_P5	AP_P5_1
	AP_P5_2
AP_DEFAULT	AP_NEW

Grupo que se asignó a cada AP. Elaborado por: Francys Carrillo.

3.2.11.3 WLAN QoS

Para el apartado de QoS se realiza el estudio bajo los parámetros de la tabla 3.24. Sin Embargo, para OMODA se establecen los marcajes como se muestra en la tabla 3.29. Teniendo así Class 1, 2 y 3. Siendo la más prioritaria la 1 y su contraria la 3. Así mismo la capa 3 mantiene AF, en tres apartados: Low Drop, Medium Drop, Hight Drop. Siendo respectivamente: Bajo descarte, Medio descarte y Alto descarte.

Tabla 3.29 QoS para WLAN.

Clase de Tràfico	Capa 3	Class
Correo	AF-Medium Drop	2
Web	AF-Medium Drop	2
Transferencia de A	AF-Low Drop	3
VoIP	EF	3
Audio y Video	AF-Medium Drop	2
Protocolos de red	AF-Medium Drop	2

Calidad de servicio aplicada en OMODA. Elaborado por: Francys Carrillo.

3.2.11.4 WLAN Tolerancia a Fallos

Para tener redundancia en la red WLAN se utilizará el Enlace de respaldo, este permite balancear las cargas que salen por las interfaces de OMADA y utilizar el segundo enlace por si llega a fallar el primero, para este caso, se activan dos interfaces WAN 1 y WAN/LAN1. Por estas interfaces cruzará el tráfico y su balanceo de carga será de 1:1.

3.2.11.5 Distribución de APs

Para la distribución de APs se requieren tres por cada piso, estos enfocados en los espacios de trabajo, siendo uno en cada área de cubículos y el tercero centralizado en el espacio. Como se observa en la figura 3.7.

Figura 3.7 Distribución APs

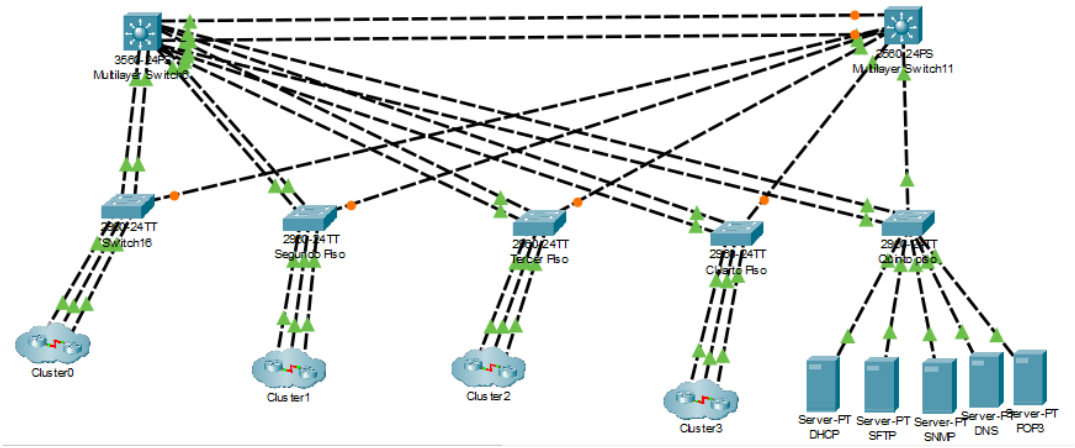
Distribución de APs en el primer piso de ARTKOS. Elaborado por: Francys Carrillo.

CAPÍTULO 4
SIMULACIÓN DE LA RED

La herramienta utilizada para la simulación es Packet Tracer, este nos permite implementar los protocolos adecuados para la red, además presenta el comportamiento de la red diseñada.

Para esta red se diseñó bajo la topología Núcleo Colapsado, este tiene la capa de acceso a los switches de capa 2, mientras que para la distribución y núcleo se implementó el switch de capa 3, se cuente con el segundo equipo switch de capa 3 para tener un respaldo.

Figura 4.1 Simulación del rediseño de la red de campus de Artkos.



Simulación de la red de campus de ARTKOS simulado en Packet Tracer. Elaborado por: Francys Carrillo.

En la figura 4.1 se muestra la topología realizada, esta maneja un switch por piso, además se muestra la granja de servidores, y los enlaces EtherChannel para redundancia de la red.

4.1 Implementación de QoS

En la figura 4.2 se crean las clases para los diferentes tipos de paquetes de datos de la red en los que se adjuntan los protocolos que estos utilizan.

Figura 4.2 Implementación de Clases.

```
class-map match-all AU-VI
match protocol rtp
exit
class-map match-all RED-PROT
match protocol icmp
match protocol dhcp
match protocol DNS
exit
class-map match-all VOZ
match protocol H323
match protocol skinny
exit
class-map match-all TRANS-DATA
match protocol ftp
match protocol tftp
exit
class-map match-all WEB
match protocol https
exit
class-map match-all CORREO
match protocol pop3
exit
```

Implementación de protocolos de red dentro de las clases. Elaborado por: Francys Carrillo.

La figura 4.3 muestra los anchos de banda configurados y las prioridades de los datos con su probabilidad de descarte. Todo esto se ve en el anexo 3.

Figura 4.3 implementación de policy map

```
policy-map marcador

class AU-VI
bandwidth percent 7
set ip dscp af41
exit

class RED-PROT
bandwidth percent 3
set ip dscp af11
exit

class VOZ
bandwidth percent 10
set ip dscp ef
exit

class TRANS-DATA
bandwidth percent 25
set ip dscp af31
exit

class WEB
bandwidth percent 15
set ip dscp af21
exit
class CORREO
bandwidth percent 15
set ip dscp af31
exit

int gi0/1
service-policy output marcador
```

Ajustes de DSCP y porcentaje de uso de ancho de banda en Policy-map. Elaborado por: Francys Carrillo.

4.2 **Simulación EtherChannel.**

La tabla 4.4 muestra que en el switch de capa tres se agregaron seis Channel Group, esto convirtiendo doce interfaces físicas en seis lógicas, dando redundancia a los enlaces y a su ancho de banda, además en el otro switch de capa 3 también se creó un enlace EtherChannel hacia el Switch L3-1. Todo esto a través de LACP, que es la comunicación común entre distintas marcas para EtherChannel.

Figura 4.4 Comprobación EtherChannel.

```
S3-L3-1#sh etherchannel summary
Flags:  D - down        P - in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      f - failed to allocate aggregator
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port


Number of channel-groups in use: 6
Number of aggregators:           6

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------

1      Po1(SU)           LACP   Fa0/15(P) Fa0/16(P)
2      Po2(SU)           LACP   Fa0/1(P) Fa0/6(P)
3      Po3(SU)           LACP   Fa0/2(P) Fa0/7(P)
4      Po4(SU)           LACP   Fa0/3(P) Fa0/8(P)
5      Po5(SU)           LACP   Fa0/4(P) Fa0/9(P)
6      Po6(SU)           LACP   Fa0/5(P) Fa0/10(P)
```

Status de EtherChannel configurado. Elaborado por: Francys Carrillo.

En la figura 4.4 se aprecia los enlaces EtherChannel activos, en capa 2 y participando activamente en el Port-Channel con el protocolo LACP.

4.2.1 **Simulación de las configuraciones VLANs.**

En la figura 4.5 se aprecian las VLANs creadas con el direccionamiento antes mencionado, estas VLANS están interconectadas y sirven para cada área, se muestra su interconexión en el anexo 1 y 2.

Figura 4.5 VLAN en el switch de Capa 3.

```
S3-L3-1#sh vlan br

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/11, Fa0/12, Fa0/13, Fa0/14
                                                Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                                Gig0/2
90   ADMINISTRACION                   active
91   OPERACIONES                      active
92   TI                               active
93   GERENCIA                         active
94   WIRELESS                         active
95   SERVERS                          active
96   VoIP                             active
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
S3-L3-1#
```

Creación de las respectivas VLAN en el switch de capa 3. Elaborado por: Francys Carrillo.

4.2.2 **VTP**

El switch de capa 3 está configurado como servidor, mientras que los switches de capa 2 se mantienen como clientes.

Figura 4.6 VTP en switch de capa 3

```
S3-L3-1#sh vtp status
VTP Version capable             : 1 to 2
VTP version running             : 1
VTP Domain Name                 : artkos.com
VTP Pruning Mode                : Disabled
VTP Traps Generation            : Disabled
Device ID                       : 0001.C916.B950
Configuration last modified by 0.0.0.0 at 3-1-93 00:00:00
Local updater ID is 172.22.10.100 on interface Vl90 (lowest numbered VLAN interface
found)

Feature VLAN :
--------------
VTP Operating Mode              : Server
Maximum VLANs supported locally : 1005
Number of existing VLANs        : 12
Configuration Revision          : 174
MD5 digest                      : 0x7C 0x5D 0x00 0x25 0xFD 0x0B 0x18 0x38
                                  0x05 0x88 0x01 0xE2 0x23 0xE4 0x99 0x00
```

VTP en switch de capa 3 configurado con su dominio. Elaborado por: Francys Carrillo.

En la figura 4.6 se muestra al servidor VTP, mientras que en la figura 4.7 se muestra uno de los switches configurados como clientes.

Figura 4.7 Modo cliente VTP

```
Sw_PRIMER_P#sh vtp status
VTP Version capable             : 1 to 2
VTP version running             : 1
VTP Domain Name                 : artkos.com
VTP Pruning Mode                : Disabled
VTP Traps Generation            : Disabled
Device ID                       : 0000.0C13.0E00
Configuration last modified by 0.0.0.0 at 3-1-93 00:00:00

Feature VLAN :
--------------
VTP Operating Mode              : Client
Maximum VLANs supported locally : 255
Number of existing VLANs        : 12
Configuration Revision          : 174
MD5 digest                      : 0x7C 0x5D 0x00 0x25 0xFD 0x0B 0x18 0x38
                                  0x05 0x88 0x01 0xE2 0x23 0xE4 0x99 0x00
```

Modo cliente en switch de capa dos. Elaborado por: Francys Carrillo.

4.2.3 HSRP

Para la presente se configuro un switch de capa 3 en HSRP, esto con el fin de brindar redundancia, uno como activo, y el otro esperando por si falla el primero. Como se muestra en la figura 4.8

Figura 4.8 HSRP

```
S3-L3-1# sh standby br
                     P indicates configured to preempt.
                     |
Interface   Grp  Pri P State    Active          Standby         Virtual IP
Vl90        90   110 P Active   local           172.22.10.101   172.22.10.254
Vl91        91   110 P Active   local           172.22.20.101   172.22.20.254
Vl92        92   110 P Active   local           172.22.30.101   172.22.30.254
Vl93        93   110 P Standby  172.22.40.101   local           172.22.40.254
Vl94        94   110 P Active   local           172.22.50.101   172.22.50.254
Vl95        95   110 P Active   local           172.22.60.101   172.22.60.254
Vl96        96   110 P Active   local           172.22.70.101   172.22.70.254
```

Configuración de HSRP en el Switch de Capa 3, siendo este el principal.

Este protocolo permite la redundancia de la red al utilizar el switch del siguiente salto ya que este pasa a ser el nuevo Gateway teniendo uno virtual, siendo el caso las VLANS con la terminación .254 que une a los Gateway reales.

4.2.4 Implementación de ACL

Como se observa en la figura 4.9 se gestionó el acceso a cierto de tráfico, excepto en las áreas de Ti y Gerencia, por ser áreas prioritarias. Las demás áreas están gestionadas por el tipo de tráfico que circula por la red.

Figura 4.9 Simulación de las Access-lists en Switch de capa 3

```
S3-L3-1#show ip access-lists
Extended IP access list ALLOW_VLAN90_ADMIN_FA0/1
    10 permit icmp any any
    20 permit udp any any eq bootpc
    30 permit udp any any eq bootps
    40 permit udp any any eq domain
    50 permit tcp any any eq 1720
    60 permit tcp any any eq 2000
    70 permit tcp any any eq pop3
    80 permit tcp any any eq www
Extended IP access list ALLOW_VLAN91_OPER_FA0/2
    10 permit icmp any any
    20 permit udp any any eq bootpc
    30 permit udp any any eq bootps
    40 permit udp any any eq domain
    50 permit tcp any any eq 1720
    60 permit tcp any any eq 2000
    70 permit tcp any any eq ftp
Extended IP access list ALLOW_VLAN92_TI_Fa0/3
    10 permit ip any any
Extended IP access list ALLOW_VLAN93_GEREN_Fa0/4
    10 permit ip any any
Extended IP access list ALLOW_VLAN94_DC_Fa0/5
    10 permit udp any any eq bootpc
    20 permit udp any any eq bootps
    30 permit udp any any eq domain
    40 permit tcp any any eq 1720
    50 permit tcp any any eq 2000
    60 permit tcp any any eq pop3
```

Comando para mostrar las ACLs creadas en el switch de capa 3.

4.2.5 Simulación de Port Security

Para la seguridad de los puertos en los switches de la capa de acceso se simuló que solo se permita al switch aprender dos MAC por cada interfaz, si se intenta introducir una nueva MAC el puerto se bloqueará. Esto con los comandos utilizados en la figura 4.10.

Figura 4.10 Comando para Port- Security

```
int range fa0/5-20
switchport port-security maximum 2
switchport port-security violation shut
exit
```

4.2.6 Simulación SYSLOG & IPS

El IPS funciona a través de firmas, las cuales permiten o deniegan algún tipo de tráfico malicioso según sus bases de datos, para la presente se implementó dicho IPS además de un SYSLOG que se conecta al switch de capa 3 para alertar cualquier anomalía en el tráfico de la red. Como se muestra en la figura 4.12 que advierte de un evento sobre un tipo de tráfico bloqueado.

Figura 4.11 IPS & SYSLOG

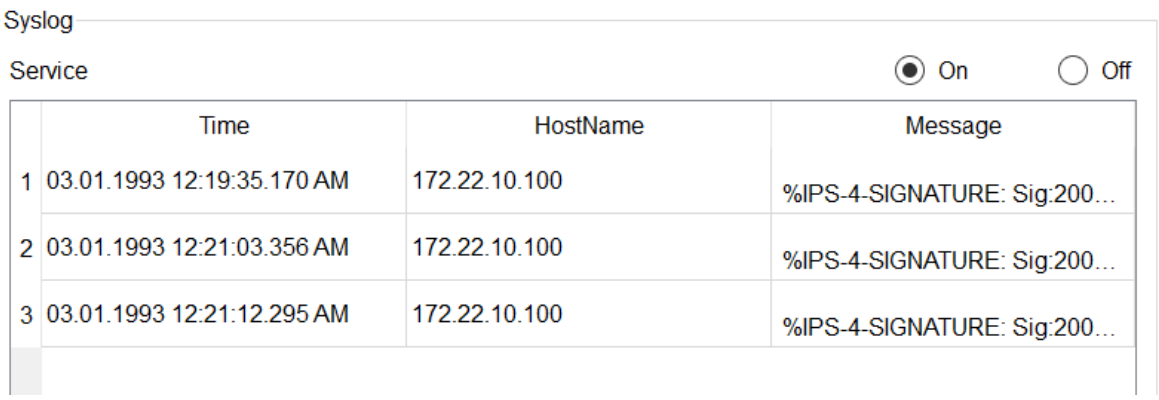
```
ena
mkdir ipsdir
conf t
ip ips config location ipsdir
ip ips name iosips
service timestamps log datetime msec
logging on
logging 172.22.10.30
ip ips notify log
ip ips signature-category
category all
retired true
exit
category ios_ips basic
retired false
exit
exit

int gi0/1
ip ips iosips out
exit

ip ips signature-definition
signature 2004 0
status
retired false
enable true
exit
engine
event-action produce-alert
event-action deny-packet-inline
exit
exit
```

Comandos utilizados para la implementación de IPS & SYSLOG. Elaborado por: Francys Carrillo

Figura 4.12 SYSLOG

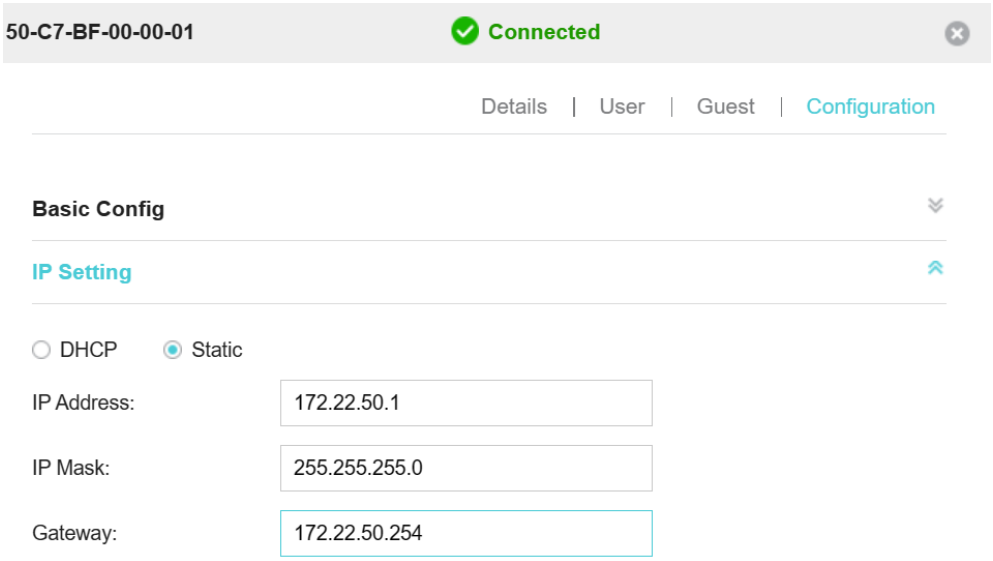


Eventos ocurridos bajo la implementación IPS junto con el SYSLOG. Elaborador por: Francys Carrillo

4.2.7 WLAN

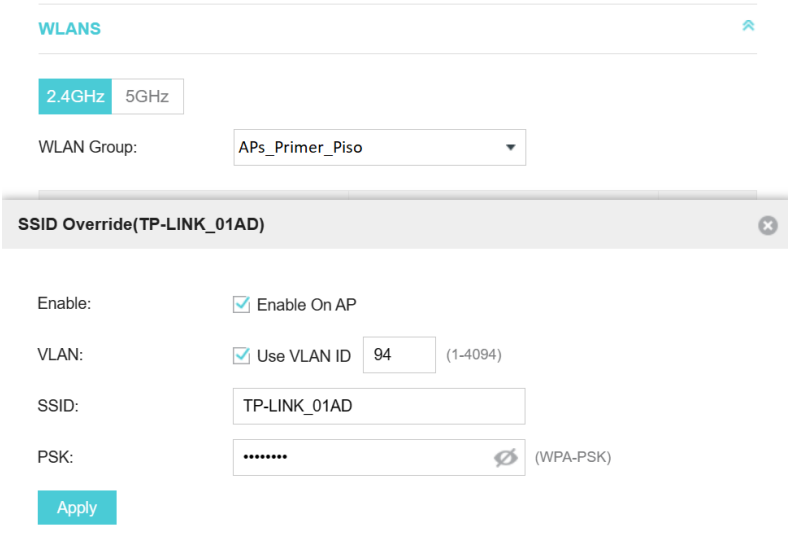
Para el apartado de WLAN se escogió al controlador de AP TP-Link OC200, el cual se configuró con cada AP, todo siguiendo el direccionamiento mencionado en las tablas 3.4 hasta 3.13.

Figura 4.13 Configuración AP Piso 1.



Configuración de AP en controlador TP-Link Omada OC200. Elaborado por: Francys Carrillo.

Figura 4.14 Configuración Grupo AP Piso 1.

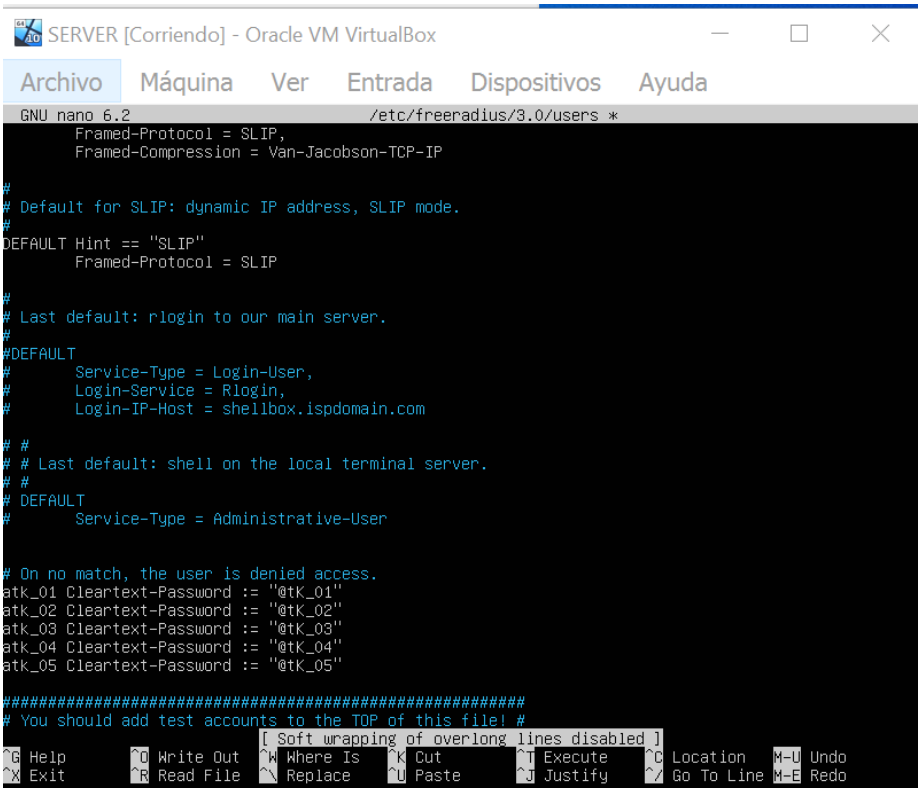


Asignación de grupo y VLAN a la AP. Elaborado por: Francys Carrillo

4.2.7.1 RADIUS & PSK

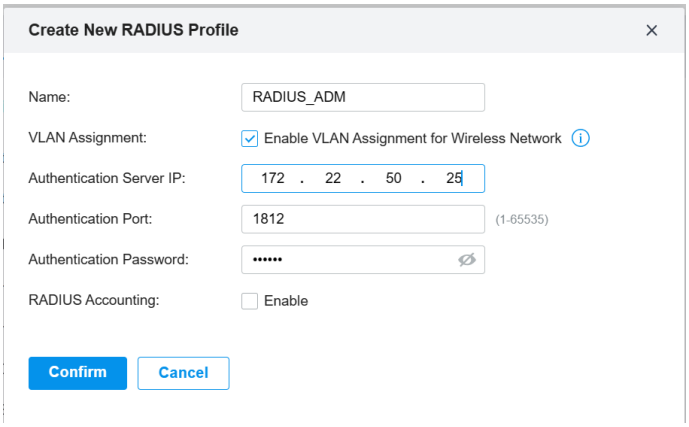
Se muestra la implementación del servidor RADIUS, como su configuración en el Controlador OMADA, todo en la figura 4.15 y 4.16.

Figura 4.15 Usuarios en RADIUS



Usuarios creados en RADIUS para su autenticación. Elaborado por: Francys Carrillo.

Figura 4.16 Configuración RADIUS en OMADA

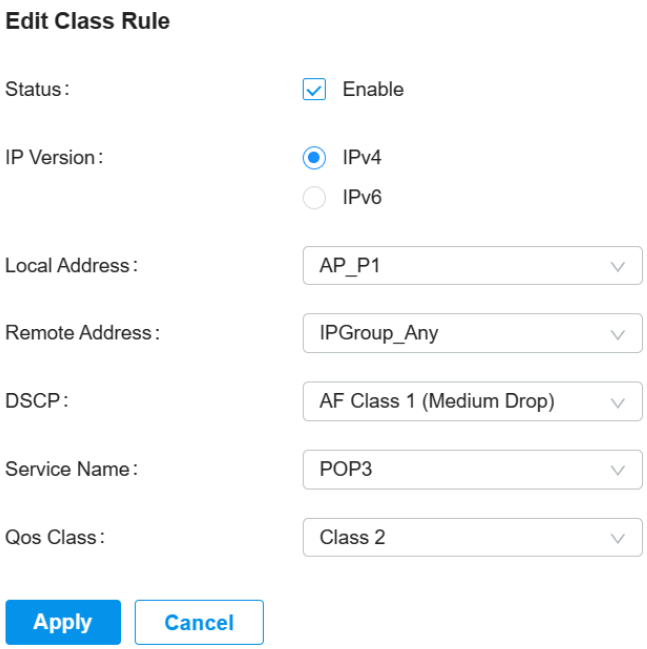


Configuración del servidor RADIUS en OMADA. Elaborado por: Francys Carrillo.

4.2.7.2 WLAN QoS

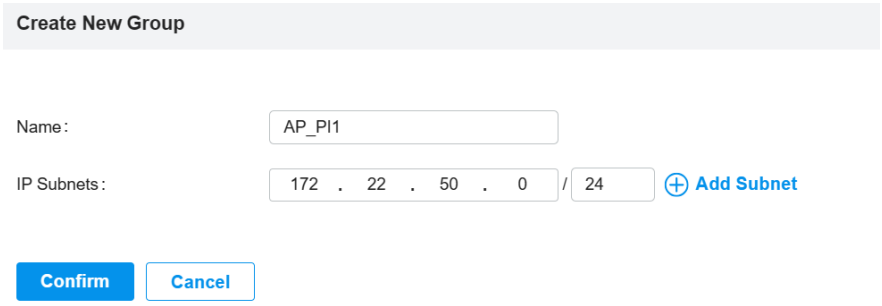
La figura 4.17 muestra la creación de las políticas para POP 3 , la cual se refiere al correo, así mismo para todos los servicios especificados en la tabla 3.29.

Figura 4.17 Políticas de QoS para la red WLAN.



Políticas enlazadas a un grupo de IP. Elaborado por: Francys Carrillo

Figura 4.18 IP-Group para el piso 1.

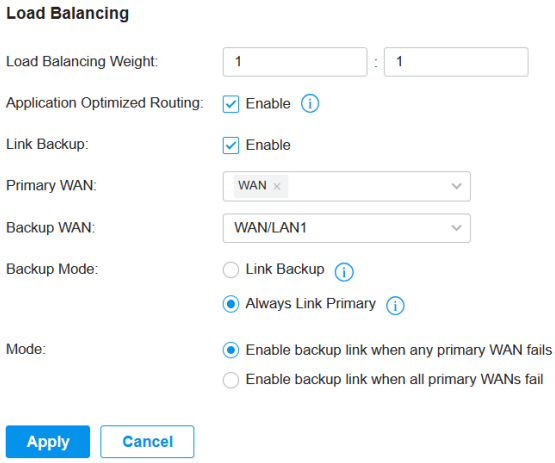


IP-Group para habilitar las políticas de QoS. Elaborado por: Francys Carrillo.

4.2.7.3 Tolerancia a fallos

Se puede observar en la figura 4.19, la cual muestra el balance para las dos interfaces, así mismo se marca a una como la principal y otra la secundaria por si llega a fallar la primera.

Figura 4.19 Balanceo de cargas para WLAN



Redundancia para la red WLAN por Backup Mode. Elaborado por: Francys Carrillo.

CAPÍTULO 5
ANÁLISIS DE COSTOS

En este capítulo, se examinarán en detalle los gastos asociados con la implementación del rediseño de la red de campus. Se abordarán la inversión inicial, los costos de implementación, la configuración y el soporte de los equipos, además del despliegue de la red dentro de la infraestructura civil de ARTKOS. Estos elementos son fundamentales para calcular la Tasa Interna de Retorno (TIR), el Valor Actual Neto (VAN) y el Periodo de Recuperación de la Capital (PRC). Estos indicadores resultan esenciales para evaluar la viabilidad económica y la rentabilidad del proyecto.

4.1 Análisis de precio de activos y pasivos

Este apartado se complementa con la selección de dispositivos, puesto que, se hallaron también los costos basándose en las características. El equipo escogido cumple con los requisitos de la organización, y cumple con el despliegue del rediseño de la red. En este análisis se encontrará el costo total de los equipos a utilizar. La tabla 4.1 muestra los precios de los dispositivos escogidos, todos estos detallados en diversas páginas de compras de TI.

Tabla 5.1 Costos de equipos.

Dispositivos	unidades	Precio	Total
Cisco 3850-48XS	2	6200	12400
Tp- Link EAP660 HD	14	264,99	3709,86
TP-Link Omada OC200.	1	1245	1245
CISCO SG220 -50P	5	2000	10000
SFP	24	162,95	3910,8
Total			31265,66

Costos de los equipos de red para ARTKOS. Elaborado por: Francys Carrillo

4.2 Valores de implementación de Red de Campus de ARTKOS

Para los servicios profesionales tanto como para técnicos, como para especialistas se tomó en cuenta a un ingeniero en TI, este se encarga de los costos de gestión, despliegue de red, configuraciones de los equipos de la red de campus, las pruebas finales de la red y el seguimiento al personal técnico. Todo esto se calculó a través de la tabla de remuneraciones básicas del 2023.

Tabla 5.2 Costo de implementación de la nueva red.

Costos de Implementación				
Dispositivos	**Operadores**	**Horas**	**Precio**	**Total**
Administración de la red	1	150	30	4500
Pruebas de conectividad		50	30	1500
Técnicos de implementación	3	40	40	1600
Capacitación Personal		24	20	60
Monitoreo				
Total				7660

Costos de implementación por sueldos de los especialistas y técnicos. Elaborado por: Francys Carrillo.

En la tabla 4.2 se muestra el coste total de la red, puesto que la organización ya tenía un cableado estructurado CAT6 que es lo que necesita la red, así mismo tienen sus PatchPannel. Además, el valor calculado para los costos de implementación esta aproximado para aproximadamente tres meses. Teniendo así la inversión total de 38925, 86 $.

4.3 Costos Total del proyecto para ARTKOS

El VAN es utilizado para determinar la viabilidad del rediseño, esto después de conocer los ingresos y egresos conocidos a día 09-01-2024, este permite verificar si es rentable o no mediante la ecuación 4.1

$$VAN = -i_0 + \sum_{t=1}^{n} \frac{Ft}{(1+k)^t} \qquad \text{Ec. 5.1}$$

Donde:

$i_0 =$ Inversión inicial

Ft= Flujo de efectivo

$k =$ Tasa de descuento

$n =$ Número de periodos.

Para hallar el flujo de efectivo se restan los ingresos y egresos de ARTKOS, por lo que, se tiene la tabla 4.3 para calcularlos.

Tabla 5.3 Ingresos y Egresos de ARTKOS

Ingresos	**Número**	**Precio**	**Total**
Empresa digital	5	2200	11000
Infraestructura Digital	4	1400	5600
Akros as s Service	5	18000	90000
Cloud	2	2480	4960
Total			111560
EGRESOS			
Salarios	88500		88500
Servicios Eléctricos	4377,77		4377,77
Enlace de Internet	1		4224
Gastos varios	3000		3000
Gastos administrativos	2000		2000
Total			102101,77
Flujo Efectivo			9458,23

Flujo de efectivo encontrado a través de ingresos y egresos. Elaborado por: Francys Carrillo.

Para la tasa de descuento se obtuvo del Banco Central del Ecuador en el apartado de Productivo PYMES, además que se calculó el VAN para seis periodos, es decir seis meses.

Al reemplazar en la ecuación se muestra:

$$VAN = -38925{,}86 + \sum_{t=1}^{n} \frac{9458{,}23}{(1+0{,}1109)^6} \qquad \text{Ec 5.2}$$

Dando un total de VAN=982,95$ por lo que indica que es rentable.

4.4 Tasa Interna de Retorno TIR

El objetivo del TIR es verificar la rentabilidad relativa de un proyecto a través de un porcentaje, esta representa la tasa de rendimiento esperada del proyecto.

En la ecuación 3.8 se muestra el cálculo del TIR a través de los valores antes encontrados.

$$VAN_{tir} = 0 = \sum_{t=1}^{n} \frac{CF_t}{(1+TIR)^t} - i_0 \qquad \text{Ec.}$$

Donde:

$CFt =$ Flujo de efectivo

$i_0 =$ Inversión inicial.

Teniendo así el valor de: 11,93%

Por lo que se muestra que es viable el rediseño de la red de campus, y muestra que la organización no generará pérdidas al implementar el rediseño. Este cálculo también realizó en una herramienta informática la cual se encuentra en el Anexo 8.

4.5 PCR

Periodo de recuperación del Capital, muestra el periodo de recuperación de la implementación del rediseño en base a los flujos de casa.

$$PCR = \frac{i_0}{FM}$$

Donde:

$FM =$ Flujo de la caja

$i_0 = Inversión\ inicial.$

Teniendo:

$$PCR = \frac{38925{,}86}{9458,23}$$

Siendo el tiempo de recuperación de 4,11 periodos, es decir, en cuatro meses, tiempo en el que se volvería al flujo de la caja habitual.

Para concluir los indicadores VAN, TIR, PCR muestran que el proyecto es viable para su implementación, con un tiempo de recuperación corto.

CONCLUSIONES

- Al definir la línea base se encontró una red sin planificación puesto que, si bien habían VLANS, estas no tenían una buena estructura, por el contrario, era una red que se iba adaptando a los problemas emergentes, por lo que, no se tenía una buena administración, además las redes WLAN tenían mucha carencia de señal, sin una optimización de los recursos, justificando así el rediseño de la red.

- El rediseño de la red fue a través del modelo jerárquico Cisco SAFE en su apartado de Campus, donde se tomó en cuenta la topología Núcleo colapsado Spine and Leaf, permitiendo un futuro rediseño con los equipos propuestos, con políticas de QoS, seguridad, escalabilidad y tolerancia a fallos todo esto para un alcance de 5 años. Teniendo así una red más granular.

- Mediante el análisis de QoS basado en Servicios Diferenciados se establecieron prioridades sobre el tráfico, así mismo su modelo de encolamiento, poniendo a los tipos de protocolos sobre otros, poniendo así a Transferencia de archivos y VoIP como más prioritarios.

- Los análisis de costos se realizaron a través del TIR, VAN, PCR. Mediante estos se determinó que el proyecto es viable y rentable, teniendo un periodo de recuperación de 4 meses aproximadamente, y con una inversión aproximada de 38925,86 $ para la implementación del rediseño de su red de campus.

RECOMENDACIONES

- Se recomiendo la realización para trabajos futuros el aplicar el modelo Cisco SAFE para la red de frontera, puesto que, puede incrementar significativamente la seguridad de la red general de ARTKOS, ya que en este apartado se puede rediseñar con elementos como firewalls de próxima generación, permitiendo gestionar de mejor manera el tráfico y añade una capa más de seguridad.

- Se recomienda el estudio del Acceso VPN igualmente con las políticas o recomendaciones de Cisco SAFE, puesto que, el auge de teletrabajo está creciendo estas necesidades deberán ser cubiertas a futuro.

- Explorar el uso de un Sistema de Gestión de Seguridad de la Información, puesto que el mismo permite conocer los riesgos a los que se somete la empresa, las políticas, normativas y directrices para una respuesta oportuna a un ataque, y así mismo documentar las diferentes anomalías en la red.

- Se recomienda un estudio de instalaciones eléctricas en cuanto al tema de aterrizaje para los equipos de Racks, esto con el fin de evitar algún daño sobre los mismos al haber variaciones de tensión.

REFERENCIAS BIBLIOGRÁFICAS.(s.f.).

(s.f.).

Anthony Bruno, S. J. (2010). CCNP Enterprise Design ENSLD 300-420 Official Cert Guide:. *Cisco Press*.

(2023). *Cisco SAFE Reference Guide SAFE Overview Executive Summary.*

Cisco, C. (31 de Mayo de 2023). *www.cisco.com*. Obtenido de https://www.cisco.com/c/es_mx/support/docs/switches/catalyst-3750-series-switches/91862-cat3750-qos-config.html

Hernández, E. A. (2017). Comparación de los modelos OSI y TCP/IP. *Ciencia Huasteca*.

Kurniawan, D. E. (2021). Implementation and Analysis of The EtherChannel Technology Using PAgP and LACP Protocols on Cisco Switch Devices. *IEEE Xplore*.

Laksono, A. T. (2020). Implementasi Keamanan Jaringan Komputer Local Area Network Menggunakan Access Control List pada Perusahaan X. *Jurnal Sistem Komputer dan Informatika*, 32.

Leyva, N. V. (2021). Eficacia y eficiencia de la seguridad de las redes LAN. *Sociedad y Tecnología Revista del Instituto Superior Jubones*.

Lopes, E. (2018). *CCDE: Los Pilares de la Tierra*. Obtenido de The Cisco Learning Network: https://learningnetwork.cisco.com/s/blogs/a0D3i000002SKDOEA4/ccde-los-pilares-de-la-tierra-parte-2

Mamani Bautista, F. (2019). Diseño de una Red corporativa mediante una Red Privada Virtual Dinámica Multipunto (DMVPN) aplicando calidad de servicio (QoS) para optimizar el ancho de banda" caso: Tekhne S.R.L. *Repositorio Institucional de la Universidad Mayor de San Andrés*.

Milán, G. (2021). *Long-Range Dependence, QoS and Self-Similar*. EasyChair Preprint.

Ormachea Mejía, M. J. (2022). Gestión del tráfico de red en la calidad de servicio "QoS" WAN en Tambopata-Perú 2021. *RCS Revista de Ciencias Sociales*.

Patilla, H. J. (2021). Snort Open Source como detección de intrusos para la seguridad de la infraestructura de red. *Revista Cubana de Ciencias Informáticas*.

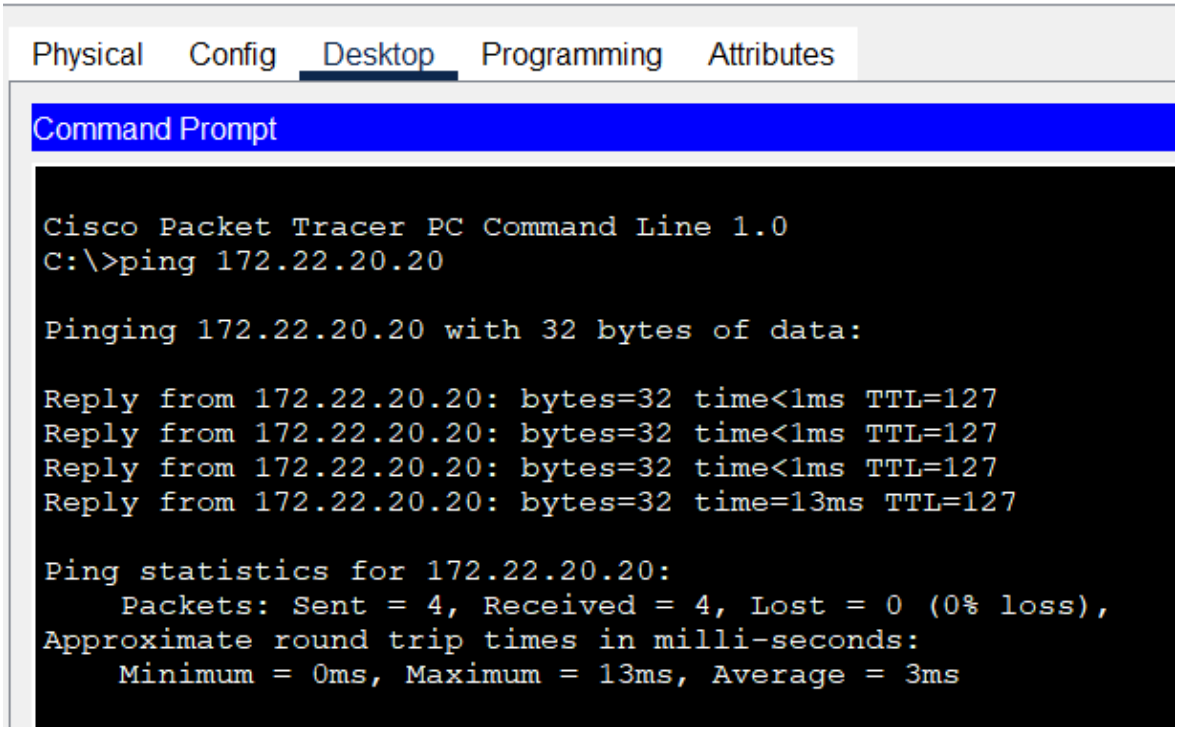
Richard Froom, B. S. (2010). Implementing Cisco IP Switched Networks . *Cisco Press*.

Suarez, H. E. (2020). Diseño de red inalámbrica para la Escuela de Artes y Comunicaciones basada en la metodología Top-Down Network Design. *Anuario de investigación*.

Villamarín, E. J. (2021). Diseño de redes para Instituciones Académicas con criterios QoS. *Iberian Journal of Information Systems and Technologies*, 171.

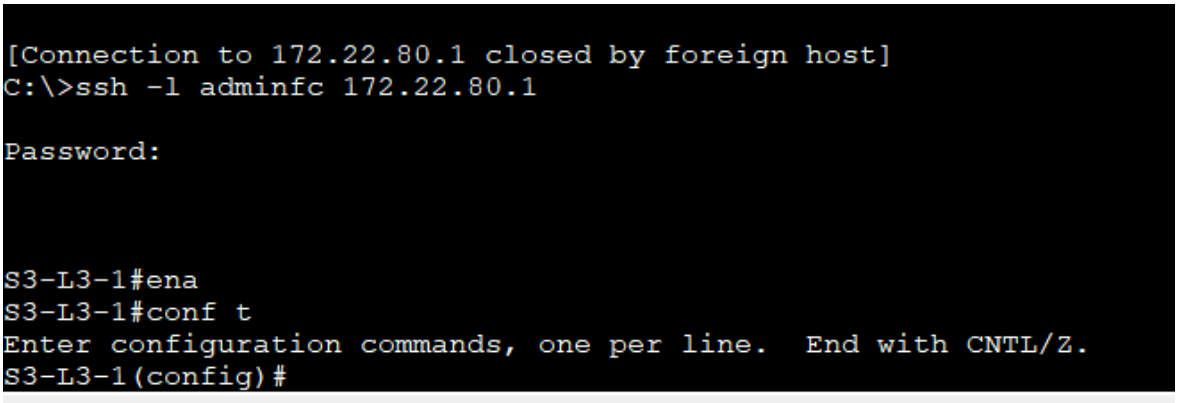
ANEXOS.

Anexo 1



Conexiones a través de Ping entre dos hosts en diferentes VLANs. Elaborado por: Francys Carrillo

Anexo 2



Conexión SSH hacia SWL3. Elaborado por: Francys Carrillo.

Anexo 3

```
S3-L3-1#sh policy-map
  Policy Map marcador
    Class AU-VI
      Bandwidth 7 (%) Max Threshold 64 (packets)
      set ip dscp af41
    Class RED-PROT
      Bandwidth 3 (%) Max Threshold 64 (packets)
      set ip dscp af11
    Class VOZ
      Bandwidth 10 (%) Max Threshold 64 (packets)
      set ip dscp ef
    Class TRANS-DATA
      Bandwidth 25 (%) Max Threshold 64 (packets)
      set ip dscp af31
    Class WEB
      Bandwidth 15 (%) Max Threshold 64 (packets)
      set ip dscp af21
    Class CORREO
      Bandwidth 15 (%) Max Threshold 64 (packets)
      set ip dscp af31
```

Policy Map del switch capa 3. Elaborado por: Francys Carrillo.

ANEXO 4

	Dispisitivos L3		
Parámetros	Aruba 2930F	Cisco 3850-48XS	Juniper Networks EX4550
Consumo de energia	154 watts	200 Watts	183 W
Densidad Portuaria	24	48	32
Velocidad	10 GBPS	10 GBPS	10 GBPS
Seguridad	802.1 x Authentication, ACL, MAC	802.1x, ACL, Port Security, DDOS, ARP	802.1x, ACL, DDoS
QoS	DRR, DSCP	Superior QoS, CoS, DSCP, SRR, CIR	DRR, DSCP
PSR (POWER SUPPLY	si	si	si
Costos	4200	6200	3273

Características por equipo en Capa 3. Elaborado por: Francys Carrillo.

Anexo 5

Parámetros	Aruba CS 6000	CISCO SG220 -50P	D-Link DGS-1210
Consumo de energia	180 Watts	375 watts	238 watts
Densidad Portuaria	24	48	24
Velocidad	10 GB	1 GBPS	1 GBPS
Seguridad	802.1 x Authentication, ACL, MAC, DHCP Snooping	IDS, ACL, IPS, DDOS, ARP, DHCP Snooping	MAC, ARP, DHCP Snooping, Captive Portal
QoS	Interface, WRR, DRR, DSCP	Superior QoS, CoS, DSCP, SRR, WRR	Interface, WRR, DSCP
Alimentación redundante	Si	Si/Cisco Stack Power	Si
Precio	1300	2000	600

Características de equipos en Capa 2. Elaborado por: Francys Carrillo.

Anexo 6

	Dispositivos	
Caracteristicas	Cisco 3504	EAP660 HD
Licencia	Si	No
Interfaces Gigabit	1 GigabitEthernet	1 GigabitEthernet
Clientes simultaneos	3000	1000
PoE	Si	Si
Autenticacion	Radius, TACACS	Portal Cautivo, MAC, VLAN
Precio	1150	264,99

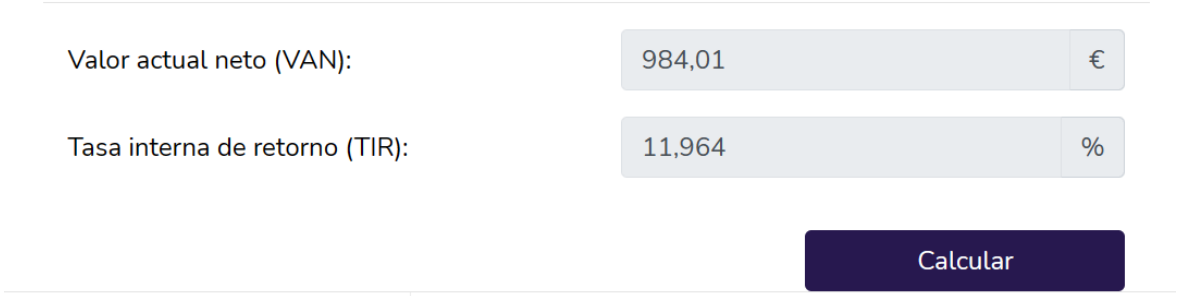
Características de equipos WLAN. Elaborado por: Francys Carrillo.

Anexo 7

Tasas de Interés Activas Referenciales[1]	
Segmentos de Crédito[2]	**% anual**
Productivo Corporativo	10,14
Productivo Empresarial	11,03
Productivo PYMES	11,09
Consumo	16,23
Educativo	8,84
Educativo Social	5,49
Vivienda de Interés Público	4,99
Vivienda de Interés Social	4,98
Inmobiliario	9,94
Microcrédito Minorista	20,00
Microcrédito de Acumulación Simple	20,51
Microcrédito de Acumulación Ampliada	20,09
Inversión Pública	8,11

Tablas de interés activas. Tomado del BCE.

Anexo 8.



Calculo Online: Van y Tir. Elaborado por Francys Carrillo.