

CONTENIDO

I.	Introducción	1
II.	Marco teórico	2
	Modelo OSI.....	2
	Componentes de la red de ESCOM.....	2
III.	Análisis	9
	Descripción general del estado actual de la red en ESCOM	9
	Análisis de la topología actual.....	9
	Conteo de dispositivos de red en ESCOM	10
	Análisis económico de los componentes necesarios.....	11
	Evaluación de los componentes requeridos para la red ESCOM.....	11
	Especificación y simplificación.....	17
	Diseño preliminar 1	19
	Descripción del diseño actual.....	19
	Propuesta de diseño para los laboratorios de sistemas, programación e inteligencia artificial.....	19
	Modelo de dispositivos a utilizar.....	19
	Creación de subredes	20
	VLSM	20
	Configuraciones de red	21
	VLAN	21
	¿Para qué sirven?	21
	Tipos de VLAN.....	21
	Enrutamiento entre VLAN	21
	Enrutamiento Inter-VLAN Router-on-a-Stick	22
	Reubicación de sites con enrutador	22
	Diseño preliminar 2.....	22
	Salones de clase y algunas aulas	22
	Implementación de las configuraciones de red.....	22
	Laboratorios	22
	Comandos de configuración	23
	Edificio de gobierno	24
	Salones.....	24
	Enrutamiento.....	24
	Configuración de rutas entre el enrutador principal y el enrutador del edificio central	25
	Diseño final.....	25
	Pruebas de conectividad.....	25
	Conclusiones.....	27
	Moreno Martínez Diego Alejandro	27
	Chávez Hernández Carol Monserrat	28
	Canseco Aguilar Antony Alexis	30
	Cohete Ronquillo Julio César.....	33
	Referencias	35

Análisis y propuesta de rediseño de la red de la escuela superior de cómputo (ESCOM) del Instituto Politécnico Nacional (IPN).

Canseco Aguilar Antony Alexis
ESCOM – IPN
acansecoa1900@alumno.ipn.mx

Chávez Hernández Carol Monserrat
ESCOM – IPN
cchavezh1900@alumno.ipn.mx

Cohete Ronquillo Julio Cesar
ESCOM – IPN
jcoheter1700@alumno.ipn.mx

Moreno Martínez Diego Alejandro
ESCOM – IPN
dmorenom2002@alumno.ipn.mx

Resumen— El presente documento aborda el análisis y rediseño de la red de la Escuela Superior de Cómputo (ESCOM) mediante la aplicación del modelo OSI y la identificación de sus componentes clave. En la primera sección se presenta el marco teórico, donde se explica el modelo OSI y sus capas, así como los diferentes dispositivos de red como switches, routers, access points y servidores, que son esenciales para la infraestructura de comunicación. Se enfatiza la importancia de un diseño adecuado de la red para garantizar su funcionalidad y eficiencia. Posteriormente, se realiza un análisis del estado actual de la red en ESCOM, destacando que la topología mixta, predominantemente en anillo, presenta inconvenientes como puntos únicos de fallo y dificultades para la expansión. Se incluye un conteo detallado de los dispositivos de red en cada edificio, lo que permite una mejor planificación y gestión. En la sección económica, se presenta un desglose de los costos de los componentes necesarios, resaltando la importancia de un análisis financiero para asegurar la viabilidad del proyecto. El documento también propone un diseño preliminar que contempla la creación de subredes utilizando VLSM, con el objetivo de segmentar la red de acuerdo con la cantidad de hosts requeridos en cada área de la escuela. Finalmente, se plantean configuraciones de red que incorporan VLANs y enrutamiento entre ellas, con el fin de mejorar la gestión del tráfico y asegurar una infraestructura escalable.

Palabras Clave— Red, Escuela Superior de Cómputo (ESCOM), Modelo OSI, Componentes, Switches, Routers, Access Points, Servidores, Diseño, Topología, Fallos, Gestión, Análisis, Subredes, VLSM, Segmentación, LANs, Enrutamiento, Escalable, Infraestructura, Tráfico de datos.

I. INTRODUCCIÓN

La red de la Escuela Superior de Cómputo (ESCOM) es un componente crítico para el funcionamiento de las actividades académicas y administrativas. Sin embargo, la estructura actual de esta red presenta serias deficiencias, principalmente derivadas de un mal diseño de la topología, que ha resultado en fallos frecuentes y en una gestión ineficiente del tráfico de

datos. Este documento tiene como objetivo general rediseñar la red existente utilizando los recursos disponibles, segmentar las subredes por número de dispositivos y áreas de la escuela, implementar una nueva topología y generar una red escalable que responda a las necesidades actuales y futuras de la institución.

El rediseño se fundamenta en el análisis del modelo OSI y en la identificación de los componentes esenciales de la red, tales como switches, routers y servidores. En el marco teórico, se expone cómo cada uno de estos elementos contribuye al funcionamiento eficiente de la red. La sección de análisis detalla el estado actual de la red, revelando que la topología de anillo utilizada presenta inconvenientes significativos, como puntos únicos de fallo, que pueden interrumpir el servicio de forma generalizada. Además, se observa que la dificultad para añadir o quitar nodos complica la expansión de la red, lo que limita su capacidad de crecimiento.

Para abordar estas problemáticas, se propone un diseño preliminar que incluye la creación de subredes segmentadas mediante la técnica de VLSM, permitiendo así una asignación más eficiente de las direcciones IP y una mejor organización del tráfico de datos. La implementación de VLANs será fundamental para la segmentación de la red, lo que facilitará la gestión del tráfico y mejorará la seguridad. Asimismo, se contempla un enrutamiento inter-VLAN que permitirá la comunicación entre las diferentes subredes, garantizando así un funcionamiento fluido y eficaz de la red. Este documento se justifica no solo por la necesidad de mejorar la infraestructura de red de ESCOM, sino también por la importancia de contar con un sistema robusto y escalable que pueda adaptarse a los cambios y demandas futuras. A través de este rediseño, se busca no solo resolver los problemas actuales, sino también establecer una base sólida para el crecimiento continuo de la red en la institución. La adecuada planificación y ejecución de este proyecto son cruciales para asegurar que la red cumpla con los estándares requeridos y proporcione un servicio confiable a todos los usuarios.

Modelo OSI.

El modelo Open Systems Interconnection (OSI) es un modelo conceptual creado por la Organización Internacional para la Estandarización, el cual permite que diversos sistemas de comunicación se conecten usando protocolos estándar. En otras palabras, el OSI proporciona un estándar para que distintos sistemas de equipos puedan comunicarse entre sí. Este modelo sigue siendo muy útil para resolver problemas de red. Ya sea una persona que no puede lograr que su ordenador portátil se conecte a Internet o un sitio web que está caído para miles de usuarios, el modelo OSI puede ayudar a desglosar el problema e identificar la causa [1].

- Capa 1. Capa física: En esta capa, los datos se transmiten en forma de bits y se convierten en señales eléctricas u ópticas para su transmisión gracias a la conmutación que se lleva a cabo. Además, controla el flujo de datos, detecta y corrige errores y convierte los datos en señales físicas adecuadas para su transporte [2].
- Capa 2. Capa de enlace de datos: En esta capa, los datos se organizan en tramas y se añade información de direccionamiento físico para que los dispositivos sepan cómo llegar al destino. Además, realiza verificación y corrección de errores, asegurando que los datos se reciban correctamente [2].
- Capa 3. Capa de red: En esta capa, la transferencia de datos se ejecuta en paquetes y se asignan direcciones para su enrutamiento. Además, resuelve problemas de transmisión a través de enlaces con estructuras no estándar y facilita el direccionamiento en redes grandes. También controla la congestión en la red y garantiza la entrega de datos [2].
- Capa 4. Capa de transporte: Aquí se encuentran protocolos de red como los protocolos FTP, UDP, SMTP o el protocolo TCP/IP (Transmisión Control Protocol/Internet Protocol o Protocolo de Control de Transmisión/Protocolo de Internet); este último garantiza la entrega secuencial y confiable de datos [2].
- Capa 5: Capa de sesión: Esta capa es fundamental para la interacción prolongada entre aplicaciones y asegura que las conexiones se establezcan y cierren de manera adecuada [2].
- Capa 6. Capa de presentación: Además, se encarga de la codificación, decodificación, compresión y descompresión de datos [2].
- Capa 7. Capa de aplicación: Además, se encarga de la codificación, decodificación, compresión y descompresión de datos [2].

Componentes de la red de ESCOM.

Site: También conocido como “Telecom room”, “Centro de datos”, “Sala de telecomunicaciones” o “Cuarto frío”, el site es definido como una instalación aislada, restringida, vigilada, con temperatura y humedad controlada para evitar sobrecalentamiento de equipos; está diseñada especialmente para concentrar dispositivos informáticos y de telecomunicaciones, con el objetivo de mantener seguros el hardware crítico y la información generada por una empresa o institución pública [3].

Conmutador: Los conmutadores de red o switch son equipos encargados de conectar diversos dispositivos, como impresoras, computadoras, etc. Los dispositivos por conectar deben poseer una tarjeta LAN Ethernet o Wifi, ya que la conexión puede ser inalámbrica. Su función es similar a un puente de red, enviando datos entre un segmento a otro de la red y cortando la conexión una vez terminada la transferencia [4].

Un conmutador de red es un dispositivo físico que funciona en la capa de enlace de datos (Data Link) del modelo de interconexión de sistemas abiertos (OSI) o la Capa 2. Recibe los paquetes enviados por los dispositivos conectados a sus puertos físicos y los reenvía a los dispositivos a los que están destinados los paquetes. Los conmutadores también pueden operar en la capa de red (Capa 3), donde se produce el enrutamiento [5].

Router: Los routers guían y dirigen los datos de red mediante paquetes que contienen varios tipos de datos, como archivos, comunicaciones y transmisiones simples como interacciones web. Este dispositivo recibe y envía datos en redes informáticas. Los routers a veces se confunden con los concentradores de red, los módems o los switches de red. No obstante, los routers pueden combinar las funciones de estos componentes y conectarse con estos componentes para mejorar el acceso a Internet o ayudar a crear redes empresariales [6].

Access Point: Un Access Point o “Punto de Acceso” es un dispositivo esencial en redes inalámbricas que permite ampliar el alcance y mejorar la conectividad. Actúa como un punto central que proporciona la conexión a Internet a través de ondas inalámbricas, brindando acceso a dispositivos como computadoras, teléfonos inteligentes y otros dispositivos compatibles con Wi-Fi [7].

Puede obtener acceso a internet a través de una interfaz ethernet (lo más común) que puede provenir de un router principal o bien a través de una conexión inalámbrica existente y su función es retransmitirla para proveer a áreas de forma inalámbrica.

Servidores

Un servidor o server, en el lenguaje informático, es un ordenador y sus programas, que están al servicio de otros ordenadores. El servidor atiende y responde a las peticiones que le hacen los otros ordenadores. Los otros ordenadores, que le hacen peticiones, serán los "clientes" del servidor. Precisamente se llaman servidores porque sirven cosas y están al servicio de otros ordenadores. [8]

Un servidor de red, o simplemente servidor, es un ordenador o equipo informático que ofrece acceso a recursos y servicios compartidos a otros equipos conectados en red denominados clientes. Los recursos compartidos pueden incluir acceso a hardware, como discos duros o impresoras, acceso a servicios, como servicios de email o acceso a internet, y acceso a software. Los clientes pueden ser estaciones de trabajo, equipos personales u otros servidores. [8]

En general, el cliente es un ordenador utilizado por una persona para desempeñar sus tareas, es decir, para trabajar de forma local, mientras que el servidor es el ordenador que ofrece acceso a los recursos compartidos entre todos los integrantes de una red. La diferencia entre un servidor y un cliente es su configuración y no el hardware, pero la realidad es que los ordenadores que van a desempeñar las funciones de servidor suelen estar equipados con componentes más potentes que una estación de trabajo. [8]

Tipos de servidores:

- **Servidor de Datos FTPS**

Entre los servidores de red más antiguos podemos encontrar el Servidor de FTP o File Transfer Protocol por sus siglas en inglés, es uno de los protocolos más antiguos nacidos a principios de los años setentas y que aún hoy sigue siendo utilizado, tal vez ya no por el usuario medio, sin embargo a pesar de su longevidad y que en general es catalogado como obsoleto, en la realidad es un protocolo que sigue vivo gracias a su confiabilidad y flexibilidad por lo que sigue siendo utilizado en muchos ámbitos.

El protocolo sigue siendo útil especialmente cuando otras alternativas más modernas no son una opción o no están disponibles ya sea por compatibilidad, recursos o complejidad, es sumamente sencillo de configurar tanto del lado del servidor como del cliente. [9]

- **Servidor HTTP**

El tipo más común de servidor de red es el servidor web cuya función es publicar información, imágenes, vídeos y casi cualquier tipo de archivo bajo un protocolo llamado hipertexto que permite que programa clientes denominados navegadores puedan entender e interpretar para presentar al usuario un el contenido de una forma atractiva, haciendo el uso de Internet de

forma más sencilla para usuarios de todos los niveles, por eso con el correr de los años se el servidor web sea transformado en uno de los pilares de internet y gran responsable de su popularidad. [9]

- **Servidor de Email**

Otro aún más antiguo que la propia web es el servicio de correo electrónico, en un comienzo el correo electrónico era un sistema de mensajería interna de un servidor que servía para comunicarse de forma asíncrona a los diferentes usuarios de un mismo servidor por lo que no puede hablarse en un principio del correo electrónico como un servicio de red.

Un servidor de correos en realidad está formado por varios servicios como son IMAP y POP que son protocolos que permiten al usuario recibir el correo en su casilla como por el servicio SMTP que es el protocolo que permite al usuario enviar correo al servidor y a los servidores intercambiar el correo entre sí, entre estos tres forman lo que se conoce como Servidor de Correos y que a su vez dependen el servidor DNS y el Sistema de Nombres de Dominios para poder localizar los destinatarios y poder hacerles llegar el correo. [9]

- **Servidor de Almacenamiento**

Un servidor NAS por las siglas en inglés de Network Attached Storage es un servidor de red por naturaleza, aparte su propio nombre lo indica, un NAS es un servidor o dispositivo de almacenamiento de datos en red que es utilizado para compartir cualquier tipo de fichero, permite compartir enormes cantidades de datos de forma segura y acceder a él muy fácilmente desde cualquier otro dispositivo local en la misma red o remoto a través de internet.

Cuando se habla de NAS no se habla de un protocolo ni un servicio específico, en realidad se está hablando de una función (almacenamiento de red). Para poder llevar a cabo esta tarea los NAS utilizan una gran variedad de servicios como pueden ser NFS, SMB (Samba), FTP, TFTP, SFTP, SSH WebDav, HTTP entre muchos otros. [9]

Firewall

Un firewall es un sistema de seguridad que supervisa y controla el tráfico de red, permitiendo o bloqueando el acceso según una serie de reglas de seguridad predeterminadas. Actúa como una barrera entre redes internas seguras (como la red de una empresa o el hogar) y redes externas no confiables (como Internet). Su objetivo es proteger la red interna contra accesos no autorizados y ataques, al tiempo que permite el tráfico legítimo. [10]

Tipos de firewall

Filtro de paquetes

Este es el tipo de firewall más antiguo, pero tiene la ventaja de no afectar al rendimiento general del sistema. Puedes pensar en un firewall de filtrado de paquetes como un punto de control que se emplea en un router o switch de tráfico. El filtro de paquetes evaluará, valga la redundancia, los paquetes de datos que llegan a través de tu router. Normalmente, este filtro puede evaluar la dirección IP de origen, la dirección IP de destino, el tipo de paquete, el puerto de origen y el puerto de destino. No inspecciona el contenido real del paquete, solo la información general a nivel superficial. En función de la configuración del firewall, puedes filtrar para permitir o no los paquetes procedentes de direcciones IP específicas o de puertos concretos. Este tipo de firewall es relativamente simple, por lo que es fácil de evadir si eres un atacante decidido. Es mejor utilizar este tipo de firewall junto con otra arquitectura de firewall más fuerte. [10]

Puerta de enlace a nivel-circuito.

Al igual que el filtro anterior, una puerta de enlace a nivel-circuito tiene un sistema de aprobación o rechazo del tráfico. Funcionan evaluando el protocolo de control de transmisión (TCP por sus siglas en inglés). Esta evaluación determina si el paquete proviene de una sesión legítima. En una red con un firewall de puerta de enlace a nivel-circuito configurado, todos los paquetes que salen de la red parecen proceder de esa puerta de enlace, lo que impide las conexiones directas entre una red de confianza y una no confiable. Los hackers aún pueden burlar este tipo de firewall si se aprovechan de una conexión establecida y envían paquetes con malware u otro contenido malicioso adjunto. [10]

Actuando como servidor proxy

Se cree que este es el tipo de firewall más seguro porque no permite el contacto directo de la red. El servidor de seguridad proxy tiene la capacidad de examinar todo el paquete de red en lugar de detalles a nivel superficial como la dirección IP y el número de puerto. Al verificar la información del paquete, este firewall puede asegurarse que no tenga ningún contenido malicioso. [10]

Un encargado de seguridad puede usar un firewall proxy para administrar y tratar mejor los problemas de seguridad, como evaluar diferentes amenazas y otros ataques en la red. Puedes configurar un servidor proxy para bloquear el acceso a diferentes sitios web y filtrar cierto tráfico de puertos para proteger tu red interna. Un inconveniente de un firewall proxy es que realiza una conexión adicional para cada paquete que

entra y sale, lo que puede causar un retraso en el rendimiento del sistema y puede ser un punto débil durante un ataque externo. [10]

Gateway

Un gateway actúa como un enlace entre dos redes, permitiendo que los dispositivos de una red se comuniquen con los de otra. La presencia de gateways es fundamental para acceder a Internet, facilitando la comunicación y transferencia de datos entre diferentes redes. Estas pasarelas pueden ser implementadas completamente a través de software, hardware o una combinación de ambos. Dado que las pasarelas de red suelen situarse en el extremo de una red, su funcionalidad se extiende para integrar capacidades como cortafuegos y servidores proxy. [11]

Tipos de Gateway

En base a las funcionalidades que habilita, puede haber una gran variedad de gateways, entre los que destacan los siguientes:

- **Gateway de red:** Es el más común y sirve de interfaz entre dos redes que usan protocolos diferentes. Cuando solo se menciona Gateway, nos solemos estar refiriendo a este tipo. [11]
- **Gateway de almacenamiento en cloud:** Este tipo de gateway funciona como un intermediario entre las solicitudes de almacenamiento API SOAP o REST y los servicios de almacenamiento en la nube. Su función esencial radica en facilitar la integración del almacenamiento privado en la nube en las aplicaciones existentes sin requerir la migración de estas aplicaciones a una nube pública. Esto simplifica la transferencia de datos y la comunicación, asegurando una mejor interoperabilidad. [11]
- **Gateway IoT:** Conecta dispositivos IoT locales a la red, permitiendo la recopilación, procesamiento y transmisión de datos entre los dispositivos y la nube o sistemas centrales. [11]
- **Gateway de seguridad:** Protege una red interna de amenazas externas, como ataques cibernéticos, filtrando el tráfico no autorizado y aplicando políticas de seguridad. [11]
- **Gateway de voz:** Facilita la comunicación de voz sobre protocolos de Internet (VoIP), convirtiendo señales de voz analógicas en datos digitales para su transmisión a través de redes IP. [11]
- **Gateway de mensajería:** Sirve como intermediario entre diferentes protocolos de mensajería, como SMS,

correo electrónico y mensajes instantáneos, para facilitar la comunicación entre ellos. [11]

- **Gateway de servicios web:** Permite la interoperabilidad entre aplicaciones y servicios web al traducir solicitudes y respuestas entre diferentes protocolos y formatos de datos. [11]
- **Gateway de API:** Facilita el acceso y la integración de servicios y datos de aplicaciones a través de interfaces de programación de aplicaciones (API), permitiendo la comunicación entre sistemas heterogéneos. [11]

Balanceador de carga

Un balanceador de carga de red distribuye el tráfico de usuarios entre instancias de máquinas virtuales (VM) en la misma región. Los balanceadores de carga de red pueden recibir tráfico de cualquier cliente en Internet, máquinas virtuales de Google Cloud con IP externas y máquinas virtuales que tienen acceso a Internet a través de Cloud NAT o NAT basado en instancias.

Hay dos tipos principales de balanceadores de carga: externos e internos. En Google Cloud, los balanceadores de carga externos distribuyen el tráfico procedente de Internet en tu red de nube privada virtual (VPC). Los balanceadores de carga internos distribuyen el tráfico a instancias dentro de Google Cloud. [12]

Cableado Estructurado

El cableado estructurado es una infraestructura común de telecomunicaciones construida para conectar distintos dispositivos -transportar señales desde dispositivos emisores a otros receptores- en redes locales. O sea, es el conjunto de cables, conectores, canalizaciones y dispositivos que componen la infraestructura de telecomunicaciones interior de un edificio o recinto. Consiste en cables de par trenzado protegidos (Shielded Twisted Pair, STP) o no protegidos (Unshielded Twisted Pair, UTP) en el interior de un edificio con el propósito de implantar una red de área local (Local Area Network o LAN). En otras palabras, consiste en un sistema de conectividad a través cables de pares trenzados de cobre, y/o para redes de tipo IEEE 802.3; no obstante, también puede tratarse de fibras ópticas o cables coaxiales y sus respectivos elementos de conectorización y organización. [13]

Tipos de cableado

Estos sistemas han ido evolucionando para ofrecer mayores velocidades y arquitecturas de red más complejas que permitan una gestión eficiente para los edificios inteligentes. Así las cosas, podríamos hablar de las siguientes categorías:

Cat 1-5

- Cat 1: Usado para comunicaciones telefónicas POTS, ISDN y cableado de timbrado.
- Cat 2: Frecuentemente utilizado para redes token ring (4 Mbit/s).
- Cat 3: Actualmente definido en TIA/EIA-568-B. Fue (y sigue siendo) usado para redes Ethernet (10 Mbit/s). Diseñado para transmisión a frecuencias de hasta 16 MHz.
- Cat 4: Utilizado en redes token ring (16 Mbit/s). Diseñado para transmisión a frecuencias de hasta 20 MHz.
- Cat 5: Muy frecuente en redes Ethernet, fast Ethernet (100 Mbit/s). Diseñado para transmisión a frecuencias de hasta 100 MHz.
- Cat 5e: Se encuentra en redes fast Ethernet (100 Mbit/s) y Gigabit Ethernet (1000 Mbit/s). Diseñado habitualmente para transmisión a frecuencias de 100MHz, pero puede superarlos.

Estas categorías, pese a seguir existiendo, no se recomiendan ya que no son capaces de posibilitar las velocidades y anchos de banda que requieren las tecnologías actuales. Las que van de la 6 a la 8 son las más solicitadas puesto que responden a los requisitos de conectividad actuales. [13]

Cat 6-8

- Cat 6: Actualmente definido en TIA/EIA-568-B. Usado en redes gigabit ethernet (1000 Mbit/s). Diseñado para transmisión a frecuencias de hasta 250 MHz.
- Cat 6a: Definido en TIA/EIA-568-B. Usado en redes 10 gigabit ethernet (10000 Mbit/s). Diseñado para transmisión a frecuencias de hasta 500 MHz. Es totalmente compatible con todas las categorías anteriores, incluidas las categorías 6 y 5e.

Elementos principales de un sistema de cableado estructurado

Un sistema de cableado estructurado consta de una serie de componentes y subcomponentes:

Cableado horizontal

Es un sistema de distribución que corre horizontalmente entre el techo y el suelo. Contiene el mayor número de cables individuales de toda la instalación y se compone de dos elementos básicos: rutas y espacios horizontales que se encargan de, además de distribuir y soportar el cableado horizontal, conectar el hardware entre la salida del área de trabajo y el cuarto de telecomunicaciones. Su misión es llevar la información desde el distribuidor hasta los usuarios. Su composición interior es principalmente de cobre, por lo tanto, es importante que no se tuerza. Su ubicación debe realizarse detrás de los muros para no tener contacto con él. [13]

Cableado vertical o backbone

Conocido también como cableado troncal, brinda las interconexiones entre los servicios del edificio, los cuartos de equipo y cuartos de telecomunicaciones. Realiza la conexión vertical entre los diferentes pisos, estableciendo los medios de transmisión, puntos principales e intermedios de conexión cruzada y terminaciones mecánicas necesarias. O sea, se encarga de establecer la interconexión entre los diferentes cuartos o espacios. Está conformado por cables verticales, conexiones cruzadas, terminaciones mecánicas y cordones de parcheo. [13]

Cuarto de comunicaciones

Es el área destinada en exclusiva para albergar los elementos que conforman la infraestructura de telecomunicaciones. Es decir, la sala en la que se alojan y centralizan todos los elementos que componen el sistema de telecomunicaciones: los cables, accesorios de conexión, dispositivos de protección... y demás equipos necesarios para conectar el edificio a los servicios externos. Necesita de unas características especiales para cumplir correctamente su función. [13]

Cuarto de entrada de servicios de cableado

Consiste en cables, accesorios de conexión, dispositivos de protección, y demás equipo necesario para conectar el edificio a servicios externos. Puede contener el punto de demarcación. Ofrecen protección eléctrica establecida por códigos eléctricos aplicables. En concreto, deben ser diseñadas de acuerdo a la norma TIA/EIA-569-A. Los requerimientos de instalación son:

- Precauciones en el manejo del cable
- Evitar tensiones en el cable
- Los cables no deben enrutarse en grupos muy apretados

- Utilizar rutas de cable y accesorios apropiados 100 ohms UTP y ScTP
- No giros con un ángulo mayor a 90 grados

Sistema de puesta a tierra

El sistema de puesta a tierra y puenteo establecido en estándar ANSI/TIA/EIA-607 es un componente importante de cualquier sistema de cableado estructurado moderno. La sala deberá disponer de una toma de tierra, conectada a la tierra general de la instalación eléctrica, para efectuar las conexiones de todo el equipamiento. Este conducto no siempre se encuentra indicado en planos y puede ser único para ramales o circuitos que pasen por las mismas cajas de pase, conductos o bandejas. Los cables de tierra de seguridad serán puestos a tierra en el subsuelo. [13]

Atenuación

La atenuación es la pérdida de señal debido a la distancia de un punto a otro. Las señales de transmisión a través de largas distancias están sujetas a distorsión que es una pérdida de fuerza o amplitud de la señal. La atenuación es la razón principal de que el largo de las redes tenga varias restricciones. Si la señal se hace muy débil, el equipo receptor no interpreta bien o no reconocerá esta información. [13]

Esto causa errores, bajo desempeño al tener que retransmitir la señal. Se usan repetidores o amplificadores para extender las distancias de la red más allá de las limitaciones del cable. La atenuación se mide con aparatos que inyectan una señal de prueba en un extremo del cable y la miden en el otro extremo. [13]

Capacitancia del cable

La capacitancia es la unidad de medida de la energía almacenada en un capacitor y el cable al tener dos o más electrodos separados por un material dieléctrico se comporta básicamente como un capacitor. Esta unidad puede distorsionar la señal en el cable: cuanto más largo sea el cable, y más delgado el espesor del aislante, mayor es la capacitancia, lo que da lugar a la distorsión. Los probadores de cable pueden medir la capacidad de este par para determinar si el cable ha sido roscado o estirado. La capacidad del cable de par trenzado en las redes está entre 17 y 20 pF. [13]

Impedancia y distorsión por retardado

Las líneas de transmisión tendrán en alguna porción ruido de fondo, generado por fuentes externas, el transmisor o las líneas adyacentes. Este ruido se combina con la señal transmitida. La distorsión resultante puede ser menor, pero la atenuación puede provocar que la señal digital descienda al nivel de la señal de

ruido. El nivel de la señal digital es mayor que el nivel de la señal de ruido, pero se acerca al nivel de la señal de ruido a medida que se acerca al receptor. Una señal formada por varias frecuencias es propensa a la distorsión por retardo causada por la impedancia, la cual es la resistencia al cambio de las diferentes frecuencias. Esta puede provocar que los diferentes componentes de frecuencia que contienen las señales lleguen fuera de tiempo al receptor. Si la frecuencia se incrementa, el efecto empeora y el receptor estará imposibilitado de interpretar las señales correctamente. Este problema puede resolverse disminuyendo el largo del cable. [13]

Repetidor

Un repetidor WiFi, también llamado amplificador o adaptador WiFi, es uno de los dispositivos que puedes encontrar para ampliar la cobertura de tu red doméstica. Sí, las conexiones con cable son lo mejor desde el punto de vista de la velocidad, pero no siempre es posible por cuestiones de distancia y cantidad de dispositivos a conectar. E incluso el alcance de tu router tiene también sus límites. En cuanto a su funcionamiento, este viene a ser bastante simple. Los repetidores WiFi contienen dos enrutadores inalámbricos. Con uno se recoge la señal WiFi existente de tu hogar, la cuál se transfiere al segundo para transmitirla de nuevo potenciada para que tenga más alcance y llegue a las esquinas donde la cobertura del router no llega. [14]

Las características de los repetidores vienen definidas por los siguientes requisitos mínimos que se establecen en el vigente año (2021):

Facilidad de conexión: Poner en marcha un repetidor Wi-Fi es algo muy sencillo. Básicamente necesitarás conectarlo a la corriente y conocer tanto el nombre de la red como la contraseña. Pero todavía puede ser más fácil, mediante configuración protegida - denominada abreviadamente WPS - que conectará este repetidor con tu Wi-Fi simplemente pulsando un botón en ambos dispositivos. [14]

Diseño: El diseño más frecuente de los repetidores de corriente es el de un pequeño bloque de plástico que se conecta directamente a un enchufe. Suelen tener un par de luces LED para que sepamos a simple vista que están encendidos y la fuerza de la señal, así como antenas. Otros repetidores Wi-Fi, generalmente más complejos, disponen de más puertos, opciones y más caros, tienen una estética similar a los de los routers. [14]

Estándares de seguridad: El modelo de repetidor Wi-Fi que compres debería integrar WPA2-PSK (AES), el último estándar y más seguro que existe hasta la fecha. Estos estándares hacen referencia al método de encriptación empleado, algo que evitará que una persona ajena a tu red acceda a ella. Si quieres evitar

intrusos, elegir el mejor sistema de cifrado es una de las medidas para evitarlo. [14]

Cables UTP: Es el cable de pares trenzados mas utilizado, no posee ningún tipo de protección adicional a la recubierta de PVC y tiene una impedancia de 100 Ohm. El conector más utilizado en este tipo de cable es el RJ45, parecido al utilizado en teléfonos RJ11 (pero un poco mas grande), aunque también puede usarse otros (RJ11, DB25,DB11, entre otros), dependiendo del adaptador de red. [15]

Es sin duda el que hasta ahora ha sido mejor aceptado, por su costo accesibilidad y fácil instalación. Sin embargo a altas velocidades puede resultar vulnerable a las interferencias electromagnéticas del medio ambiente. [15]

Cables STP :El nivel de protección del STP ante perturbaciones externas es mayor al ofrecido por UTP. Sin embargo es más costoso y requiere más instalación. La pantalla del STP para que sea más eficaz requiere una configuración de interconexión con tierra (dotada de continuidad hasta el terminal), con el STP se suele utilizar conectores RJ49. [15]

Es utilizado generalmente en las instalaciones de procesos de datos por su capacidad y sus buenas características contra las radiaciones electromagnéticas, pero el inconveniente es que es un cable robusto, caro y difícil de instalar. [15]

Cables FTP: En este tipo de cable como en el UTP, sus pares no están apantallados, pero sí dispone de una apantalla global para mejorar su nivel de protección ante interferencias externas. Su impedancia típica es de 120 Ohm y sus propiedades de transmisión son mas parecidas a las del UTP. Además puede utilizar los mismos conectores RJ45. Tiene un precio intermedio entre el UTP y STP. [15]

Estaciones de Trabajo (PCs) ó Dispositivos Terminales: Son computadoras utilizadas por los usuarios finales en una red para ejecutar aplicaciones, acceder a recursos compartidos y comunicarse con otros dispositivos.

Patch Panel

Un patch panel , también conocido como panel de conexión o bahía de rutas, es una pieza de montaje de hardware con varios puertos para conectar y gestionar los cables LAN o los cables de fibra/cobre entrantes y salientes. Los paneles de conexión pueden ser bastante pequeños, con sólo unos pocos puertos, o muy grandes, con varios centenares de puertos. También pueden configurarse para cables de fibra óptica, cables RJ45 y muchos otros. [16]

Rack: Un rack es una estructura metálica diseñada para alojar y organizar equipos electrónicos, informáticos o de telecomunicaciones de manera ordenada y segura. Estos racks

se utilizan principalmente en entornos como centros de datos, salas de servidores y gabinetes de redes para optimizar el espacio y permitir un acceso más fácil al hardware.

Modem: Un módem es un dispositivo que envía información entre el mundo exterior o red de área extensa (WAN) y tu casa. Convierte una conexión entrante (cable coaxial, línea telefónica, línea de fibra óptica o cualquier otra) en una de Ethernet, lo que le permite al router de Wi-Fi conectarse a Internet. Los proveedores de servicios de Internet (ISP) suelen proporcionarlos. Tendrás que conectar el router o el punto de acceso principal de Google Wifi a tu módem con un cable Ethernet. [17]

DHCP: El protocolo DHCP (Protocolo de configuración dinámica de host) o también conocido como «Dynamic Host Configuration Protocol», es un protocolo de red que utiliza una arquitectura cliente-servidor. Por tanto, tendremos uno o varios servidores DHCP y también uno o varios clientes, que se deberán comunicar entre ellos correctamente para que el servidor DHCP brinde información a los diferentes clientes conectados. [18]

Este protocolo se encarga de asignar de manera dinámica y automática una dirección IP, ya sea una dirección IP privada desde el router hacia los equipos de la red local, o también una IP pública por parte de un operador que utilice este tipo de protocolo para el establecimiento de la conexión. [18]

DNS: El sistema de nombres de dominio (DNS) es el directorio telefónico de Internet. Las personas acceden a la información en línea a través de nombres de dominio como nytimes.com o espn.com. Los navegadores web interactúan mediante direcciones de Protocolo de Internet (IP). El DNS traduce los nombres de dominio a direcciones IP para que los navegadores puedan cargar los recursos de Internet. Cada dispositivo conectado a Internet tiene una dirección IP única que otros equipos pueden usar para encontrarlo. [1]

III. ANÁLISIS





Descripción general del estado actual de la red en ESCOM

En la ESCOM el dispositivo de red que más abunda es el Switch, hay solo dos enrutadores, podríamos llamar a uno de ellos como el enrutador principal, que es el que conecta mediante fibra óptica con otra red proveniente de Zacatenco, el otro enrutador se utiliza como complemento de la red debido a la cantidad de host totales, hay sites ubicados en lugares estratégicos (generalmente dentro de laboratorios de cómputo) o en cuartos diseñados para ello, y finalmente, hay puntos de acceso colocados entre edificios de modo que las áreas con mayor cobertura de red inalámbrica son los salones de clase, en todos los salones de clase, así como laboratorios, cubículos para profesores y salas en general cuentan con al menos dos conectores ethernet de pared. En la Figura 1 se muestra identificado por un ícono estratégico (véase la Tabla 1) la ubicación de estos dispositivos de red, en cada site hay por lo menos un switch, mientras que en cada laboratorio de cómputo cuenta con un rack, que contiene al menos dos switches, ellos proveen de red al mismo laboratorio de cómputo, en la figura antes mencionada, se omiten salones en general, así como oficinas administrativas y cubículos de profesores, pero estas aulas se consideran para el conteo de dispositivos finales.

Análisis de la topología actual

La topología actual es mixta, la red entera es una topología de anillo, pues los sites que contienen conmutadores están todos conectados entre sí mientras que los laboratorios, oficinas y salas en general utiliza una topología de estrella, donde el nodo central es el site más cercano, esto tiene algunos inconvenientes como lo son los siguientes:

- **Punto único de fallo:** Si un solo dispositivo o enlace en el anillo falla, puede interrumpir toda la red (este es uno de los problemas que enfrenta la red actualmente).
- **Dificultad para añadir o quitar nodos:** expandir la red podría ser muy complicado e involucraría una interrupción en el servicio.
- **Ancho de banda compartido:** el rendimiento puede ser ineficiente debido a que se distribuye a los dispositivos del anillo.

Dispositivo	Icono en la Fig. 1
Router	
Site	
Access Point	
Laboratorio de cómputo	

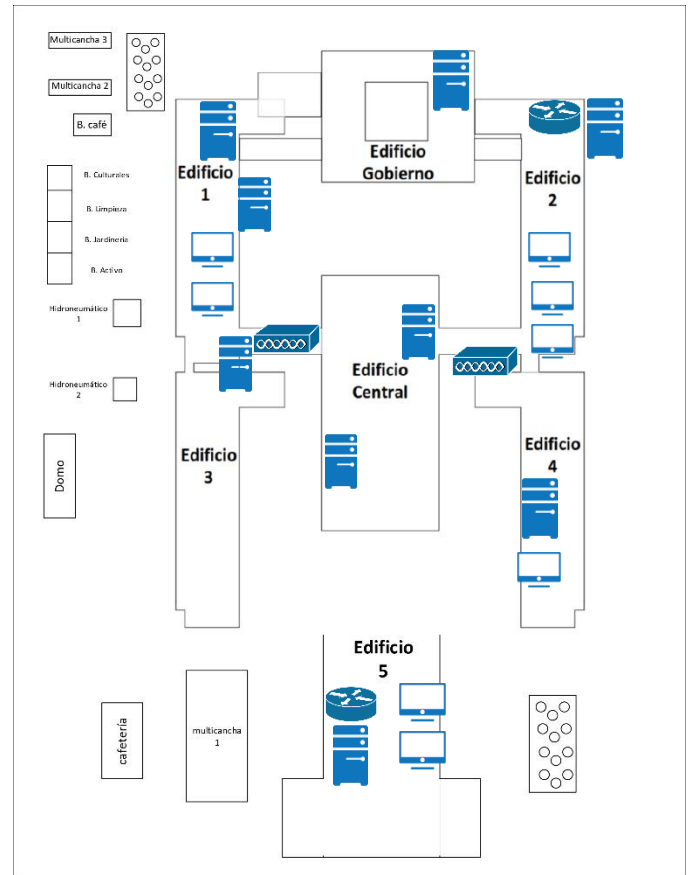


Tabla 1: identificación de dispositivos para el mapa de ESCOM

Figura 1: Mapa de vista superior de la ESCOM hecho con gráficos vectoriales

Recientemente a la topología se ha añadido un nodo importante, que es el que se encuentra en el edificio cinco, ya que surte de red a los laboratorios de la reciente carrera de Ingeniería en inteligencia artificial.

Por parte de laboratorios y aulas en general, la topología de estrella es un muy buen diseño debido a las facilidades que esta tiene, como se su configuración sencilla, sencillez para añadir o eliminar dispositivos del nodo central y detección de fallos relativamente rápido. Por lo que después de estas descripciones generales podemos concluir que en general la topología entera de la red de la ESCOM es un anillo, donde en algunos nodos contienen una topología de estrella.

Conteo de dispositivos de red en ESCOM

Los edificios de la ESCOM están identificados por un número o algún nombre que identifique el uso del edificio, en cada edificio hay un conjunto de aulas y/o laboratorios igualmente identificados por algún nombre y número. Las finalidades de tener un registro de cantidad y ubicación física de los dispositivos de red actuales son las siguientes:

- **Inventario y Documentación:** Tener un registro preciso de todos los dispositivos ayuda a mantener un inventario actualizado, ayuda a la gestión y planificación de la red.
- **Seguridad:** Implementar medidas de seguridad adecuadas, como el control de acceso físico y la protección contra robos o manipulaciones no autorizadas.

- **Planificación de extensiones:** Con un mapa claro de la red actual, es más fácil planificar futuras expansiones o actualizaciones, asegurando que los nuevos dispositivos se integren de manera eficiente.

En la Tabla 2 se tiene dicho recuento de los dispositivos de red por edificio. Esto se ha hecho para ayudar a planificar futuras expansiones de la red. Con un mapa claro de la red actual, es más fácil identificar dónde se pueden añadir nuevos dispositivos sin causar interferencias o problemas de rendimiento. Además, en algunas instituciones, es necesario cumplir con ciertas normativas que requieren un registro detallado de la infraestructura de red. Conocer la ubicación física de los componentes puede ayudar a cumplir con estos requisitos.

Dispositivo	Edificio 1									
	Sala de Intendencia	UDI	Gavetas	Celex	Laboratorio de programación			Laboratorio libre		
					1	2	3			
Switch	0	2	2	0	2	2	2	2		
Site	0	1	1	0	1	1	1	1		
Computadora	1	1	0	4	30	30	30	30		
Dispositivo	Edificio 2									
	Servicio psicológico	Salón de site principal			Laboratorio de sistemas			Puente que conecta con edificio central		
					1	2	3			
Switch	0	2			2	2	2	0		
Site	0	1			1	1	1	0		
Computadora	1	0			30	30	30	0		
Router	0	1			0	0	0	0		
Access Point	0	0			0	0	0	1		
Dispositivo	Edificio central									
	Laboratorio de física	Laboratorio de sistemas digitales		Sindicatos	Sala 14	Sala de profesores	Laboratorio de electrónica 1			
		1	2							
Switch	2	1	1	0	0	0	2			
Site	1	0	0	0	0	0	1			
Computadora	4	6	6	8	1	30	0			
Dispositivo	Edificio 3									
	Club de robótica	Área de desarrollo				Puente que conecta con el edificio central				
Switch	2	0				0				
Site	1	0				0				
Computadora	4	8				0				
Access Point	0	0				1				
Dispositivo	Edificio 4									
	Departamento de ISC	Laboratorio de posgrado	Departamento de ciencias sociales		Departamento de ciencias básicas	Sala de posgrado				
Switch	2	1	0		0	2				
Site	1	0	0		0	1				
Computadora	10	15	10		10	15				
Dispositivo	Edificio 5									
	Laboratorio de IA				Cuarto site IA					
	1	2	3						4	
Switch	0	0	0		0	4				
Site	0	0	0		0	1				
Computadora	30	30	30		30	0				
Router	0	0	0		0	1				
Dispositivo	Edificio de Gobierno									
	Auditorio	Dirección	Subdirección	Gestión escolar	Servicio médico	Biblioteca	Subdirección administrativa	Becas	Servicio dental	Recursos materiales
Switch	2	3	0	0	0	0	0	0	0	0
Site	1	1	0	0	0	0	0	0	0	0
Computadora	1	6	6	15	1	8	4	15	1	6
Router	0	0	0	0	0	0	0	0	0	0

Tabla 2 Dispositivos de red en ESCOM por edificio

Análisis económico de los componentes necesarios

El análisis económico de los componentes necesarios en la red es fundamental ya que permite demostrar viabilidad económica del proyecto, ayuda a seleccionar equipos y tecnologías más adecuados, evitando gastos innecesarios. Además, facilita la toma de decisiones estratégicas sobre el diseño y la implementación de la red [19].

A través del análisis anterior, se busca asegurar que los recursos sean utilizados de manera eficiente y que el proyecto sea financieramente sostenible. En la Tabla 3, se presenta un claro

Dispositivo	Modelo	Cantidad por edificio								Precio unitario	Precio total
		Edificio 01	Edificio 02	Edificio Central	Edificio 03	Edificio 04	Edificio 05	Edificio de Gobierno	Total		
Switches	Switch Cisco 2960 Series Catalyst 24 puertos	12	8	6	2	5	4	5	42	\$2,900.00	\$121,800.00
Routers	Router Cisco 2900 Series 2911 Nuevo con licencias básicas	0	1	0	0	0	1	0	2	\$2,500.00	\$5,000.00
Access Point	Acces Point Huawei Aircengine 5761r-11e	0	1	0	1	0	0	0	2	\$16,000.00	\$32,000.00
Racks	Rack Intellinet 26u 19in Estándar	1	1	1	1	1	1	1	7	\$2,409.00	\$16,863.00
Cable UTP	Cable Ethernet 30m Reforzado Cat6 RJ-45	690 m	469 m	305 m	75 m	325 m	625 m	340 m	2,820 m	\$159.99 x 30 m	\$15,039.06

Tabla 3 Análisis económico de componentes

Evaluación de los componentes requeridos para la red ESCOM.

El análisis económico de los componentes necesarios en la red es fundamental ya que permite demostrar viabilidad económica del proyecto, ayuda a seleccionar equipos y tecnologías más adecuados, evitando gastos innecesarios. Además, facilita la toma de decisiones estratégicas sobre el diseño y la implementación de la red [19].

Switches: Se seleccionó un modelo que ofrece una combinación de puertos, facilidad de uso y características de gestión. Los switches de TP-Link son conocidos por su fiabilidad y bajo costo, mientras que los de Cisco son ideales para entornos empresariales. El switch Cisco Catalyst 2960 Series de 24 puertos que se puede observar en la **Error! Reference source not found.**, se centra en la relación entre su costo inicial y el valor que aporta en términos de funcionalidad y confiabilidad. Este dispositivo, diseñado para redes de tamaño mediano o empresas que requieren una conectividad confiable, suele tener un costo de entre \$500 y \$1000 USD, dependiendo de la configuración específica y la región. Este precio incluye el soporte de Cisco y la posibilidad de actualización de software, lo cual es una ventaja, ya que estos switches suelen tener una vida útil larga. El switch 2960 Catalyst ofrece soporte para funciones de seguridad avanzadas, como la autenticación 802.1X y el monitoreo de red, que son relevantes en entornos empresariales

ejemplo de esto, donde se muestra un desglose detallado de los dispositivos requeridos, tales como switches, routers, access points, racks y cable UTP, distribuidos entre varios edificios.

La Tabla 3 organiza la información por modelo, cantidad, precio unitario y costo total. Al comparar precios de los equipos y determinar su distribución, el análisis económico asegura que el presupuesto del proyecto pueda ser sostenible a largo plazo y que la red sea funcional. Las referencias de precios han sido tomadas de [20], [21], [22], [23] y [24].



Figura 2: Switch Cisco 24 Puertos Ws-c2960-24lt-l De 8 Puertos Poe New. [20]

donde la seguridad es prioritaria. Además, cuenta con capacidades de administración avanzada, que incluyen VLAN y QoS, características que contribuyen a una gestión eficiente del tráfico y a la optimización del ancho de banda. Este tipo de funciones suele encontrarse en dispositivos de alta gama y justifica el costo, sobre todo cuando se compara con alternativas de menor precio y capacidades reducidas. Si bien el precio inicial puede parecer elevado en comparación con switches no gestionables o de gama baja, el Catalyst 2960 tiende a ofrecer un retorno de inversión considerable en términos de durabilidad, soporte y escalabilidad. También reduce los costos de mantenimiento a largo plazo y minimiza el tiempo de inactividad gracias a su confiabilidad, lo que se traduce en ahorros adicionales. Para una organización que proyecta una estructura de red sólida y a futuro, el gasto en un Cisco Catalyst 2960 es una inversión que ofrece estabilidad, robustez en el tráfico de red y, sobre todo, flexibilidad para el crecimiento de la red.

Routers: Se eligió un router que ofrece una buena cobertura, rendimiento y características avanzadas como control parental y soporte para múltiples dispositivos, ideal para diferentes tipos de usuarios. El router Cisco 2900 Series, modelo 2911, con licencias básicas, que se puede observar en la **Error! Reference source not found.**, se centra en su balance entre costo inicial y capacidad de desempeño en redes empresariales. Este router tiene un costo aproximado de \$1500 a \$2500 USD, dependiendo de la región y de las condiciones de compra, lo cual puede parecer elevado en comparación con modelos de gama más baja. Sin embargo, el Cisco 2911 está diseñado para manejar redes de empresas medianas y grandes, brindando funciones avanzadas de enrutamiento y servicios de seguridad, características que, en conjunto, ofrecen una estabilidad y escalabilidad superiores.

Este modelo incorpora puertos y opciones de expansión que permiten su uso en redes complejas, ofreciendo soporte para VPN, calidad de servicio (QoS) avanzada y redundancia. Estas capacidades son fundamentales para empresas que manejan un volumen de tráfico elevado o que dependen de la conectividad constante para sus operaciones diarias, lo que justifica el costo al asegurar un desempeño óptimo y una reducción en potenciales tiempos de inactividad. Adicionalmente, su eficiencia energética y diseño modular permiten disminuir costos operativos a lo largo del tiempo y facilitar futuras actualizaciones sin reemplazar el equipo completo.

El Cisco 2911 cuenta también con soporte de Cisco y la posibilidad de adquirir licencias adicionales para añadir funciones avanzadas, lo cual le da flexibilidad y capacidad de adaptarse al crecimiento de la red en el tiempo. Si bien la inversión inicial es considerable, el retorno de inversión se manifiesta a través de un menor costo de mantenimiento, confiabilidad de la infraestructura y reducción de gastos asociados con el soporte y las interrupciones de red. En una red empresarial que requiere alta disponibilidad y capacidad de expansión, el Cisco 2911 con licencias básicas es una inversión sólida que favorece tanto la eficiencia operativa como la seguridad a largo plazo.



Figura 3: Router Cisco 2900 Series 2911 Nuevo. [21]

Access Points: El modelo seleccionado es popular en entornos empresariales y ofrece gestión centralizada, lo que es esencial para mantener redes grandes y complejas.

El Access Point Huawei AirEngine 5761R-11E se basa en su costo inicial en relación con las funcionalidades avanzadas que ofrece para entornos empresariales. Este dispositivo que se puede observar en la Figura 4, con un precio que oscila entre \$400 y \$800 USD, está diseñado para soportar redes de alta densidad y cubrir áreas extensas, características ideales para oficinas, instituciones educativas y espacios de trabajo de alta demanda. Su costo se justifica principalmente por su capacidad para manejar un gran número de dispositivos conectados simultáneamente, lo cual es esencial en entornos donde la conectividad estable y rápida es prioritaria.

El AirEngine 5761R-11E utiliza la tecnología Wi-Fi 6, lo que significa un aumento considerable en la velocidad y eficiencia en comparación con versiones anteriores, además de una reducción de interferencias y mejoras en el rendimiento de la red. Estas ventajas técnicas permiten a las empresas adaptarse a la creciente demanda de ancho de banda sin necesidad de múltiples puntos de acceso, optimizando costos y reduciendo la complejidad en la gestión de la red. Asimismo, el dispositivo ofrece soporte para administración centralizada, lo que facilita la configuración y supervisión en redes complejas, disminuyendo los costos de operación y mantenimiento.

Aunque su precio es superior al de otros puntos de acceso de gamas más bajas, la durabilidad, la escalabilidad y el soporte de Huawei proporcionan un retorno de inversión que se manifiesta en la reducción de actualizaciones a corto plazo y en un menor número de incidentes de conectividad. Para empresas que requieren conexiones rápidas, estables y con baja latencia, el Huawei AirEngine 5761R-11E representa una inversión eficiente que asegura una infraestructura de red de alto rendimiento y preparada para el crecimiento de la demanda tecnológica.



Figura 4: Acces Point Huawei Airengine 5761r-11e. [23]

Racks: Se optó por un rack de entre distintas marcas que es adecuado para diferentes necesidades de instalación y accesibilidad.

El rack Intellinet 26U de 19 pulgadas, en formato estándar, se enfoca en su costo en comparación con los beneficios que ofrece para la organización y protección de equipos de red en entornos empresariales. Este rack de la Figura 5, tiene un costo promedio de entre \$500 y \$900 USD, lo cual lo convierte en una opción accesible para empresas que requieren una solución segura y eficiente para el montaje de switches, routers, servidores y otros componentes esenciales de la red. Su diseño estándar de 19 pulgadas permite una gran compatibilidad con dispositivos de diferentes fabricantes, lo que facilita su integración en infraestructuras de red existentes.

El rack Intellinet 26U está construido para ofrecer durabilidad y protección a los equipos, lo que se traduce en una inversión a largo plazo. Su estructura permite una gestión eficiente del cableado y la ventilación, lo cual reduce los riesgos de sobrecalentamiento y fallos en los equipos por falta de mantenimiento. Además, el rack proporciona seguridad física mediante sus puertas y cerraduras, protegiendo los equipos de accesos no autorizados y minimizando el riesgo de daños accidentales.

Aunque existen racks de menor precio, el modelo Intellinet 26U destaca por su capacidad para albergar equipos de gran tamaño y peso, junto con una organización que facilita el mantenimiento y la expansión de la red. En entornos donde la confiabilidad y la protección de los equipos de red son cruciales, este rack representa una inversión rentable que asegura tanto la eficiencia operativa como la seguridad del sistema de infraestructura de red en general.



Figura 5: Rack Intellinet 26u Dos Postes 19in Estándar Desarmado7 /vc. [22]

Charola para rack.

El set de cuatro charolas de 1U para rack de servidor D19 de la Figura 6, con capacidad de carga máxima de 25 kg, destaca por su costo en relación con la funcionalidad y versatilidad que aporta en la organización de componentes de red y servidores en entornos empresariales. Este conjunto de charolas tiene un precio promedio que oscila entre \$100 y \$200 USD, lo que representa una inversión moderada para optimizar el uso del espacio en racks estándar de 19 pulgadas. Estas charolas están diseñadas para soportar equipos de peso considerable, hasta 25 kg cada una, lo cual facilita la instalación de dispositivos adicionales sin sobrecargar la estructura del rack.

El set incluye, además, algunos accesorios o “regalos” como tornillos y herramientas básicas de montaje, lo que añade valor al producto y simplifica su instalación. Al proporcionar un espacio adicional para equipos que no cuentan con opciones de montaje directo en rack, estas charolas permiten una organización más eficiente y ayudan a mantener la ventilación adecuada al distribuir uniformemente el peso y la ubicación de los dispositivos.

En comparación con alternativas de charolas más económicas, este set destaca por su capacidad de carga y durabilidad, características que ofrecen seguridad y estabilidad para equipos costosos y críticos en la infraestructura de red. La inversión en este set de charolas se justifica por el aumento en la facilidad de mantenimiento y la reducción de riesgos de daños en los equipos, lo que a largo plazo contribuye a una red más organizada, segura y de bajo costo operativo.



Figura 6: Charola 1 U Para Rack Servidor D19 Max 25kg. [25]

Organizador frontal de cables.

El organizador frontal de cables Intellinet modelo 16995 para racks de 19 pulgadas resalta su impacto en la eficiencia de la administración de cables y la organización general del sistema de red. Este organizador de la Figura 7 tiene un precio aproximado de entre \$15 y \$30 USD, lo que lo convierte en una inversión accesible para mejorar la estructura de red, especialmente en instalaciones donde el orden del cableado es fundamental para el mantenimiento y la operatividad diaria. Al mantener los cables alineados y asegurados, reduce el riesgo de enredos y posibles daños, facilitando además el acceso a los dispositivos para tareas de reparación o actualización.

El organizador Intellinet 16995 ayuda a prolongar la vida útil de los cables al evitar dobleces y tensiones innecesarias, lo que minimiza la necesidad de reemplazos y reduce el costo de mantenimiento a largo plazo. Asimismo, este organizador mejora la ventilación dentro del rack al evitar que los cables obstruyan el flujo de aire, ayudando a mantener una temperatura adecuada y reduciendo el riesgo de sobrecalentamiento en los equipos.

Comparado con otras soluciones de administración de cables, el Intellinet 16995 es una opción económica y de buena calidad, proporcionando un retorno de inversión significativo en términos de facilidad de mantenimiento y protección del cableado. Para organizaciones que buscan mantener sus racks bien organizados y optimizados, este organizador es una inversión valiosa que favorece tanto la estética como la funcionalidad del sistema de red.



Figura 7: Organizador Frontal De Cables Intellinet 16995. [26]

Pach Panel.

El pach panel Cat6 de 24 puertos 1U modelo 520959 de Intellinet para racks de 19 pulgadas se enfoca en su valor en relación con la eficiencia y organización que aporta a la infraestructura de red. Este panel tiene un costo aproximado entre \$50 y \$100 USD, y su diseño permite gestionar conexiones de cables Cat6 de manera ordenada, lo cual es esencial para optimizar el rendimiento y la administración en redes empresariales. Con sus 24 puertos, proporciona suficiente capacidad para redes de tamaño mediano y garantiza la integridad de las conexiones mediante una estructura robusta y segura.

Al usar un pach panel como el de la Figura 8, las conexiones de los dispositivos pueden centralizarse, lo que facilita tanto la instalación como el mantenimiento y reduce el riesgo de desconexiones accidentales. Además, este panel cumple con la norma Cat6, lo que asegura que es capaz de soportar velocidades de transmisión de hasta 1 Gbps y, en ciertos casos, hasta 10 Gbps en distancias cortas, ideal para redes de alta velocidad que requieren transmisión estable y sin pérdidas de datos.

Comparado con otros pach panel de menor calidad o sin soporte Cat6, este modelo ofrece una relación costo-beneficio sólida, ya que, además de su durabilidad, es compatible con configuraciones de redes avanzadas y brinda flexibilidad para futuras expansiones. En resumen, el pach panel Intellinet 520959 representa una inversión moderada que favorece una infraestructura de red organizada, escalable y de alta calidad, reduciendo costos de mantenimiento y mejorando el acceso y la gestión de las conexiones.



Figura 8: Patch Panel Cat6 24puertos 1u Rack 19 520959 Intellinet. [27]

CPU.

La CPU Dell Minitorre con procesador Intel Core i7 de tercera generación, 16 GB de RAM y un SSD de 1 TB, se centra en el equilibrio entre su costo y el rendimiento que ofrece para entornos que no requieren tecnología de última generación. Este equipo que se puede observar en la Figura 9, con un precio estimado entre \$200 y \$400 USD, puede considerarse una opción económica para empresas o usuarios que necesitan ejecutar aplicaciones de oficina, navegar por internet, y realizar tareas moderadas sin necesidad de una inversión en hardware de gama alta.

El procesador i7 de tercera generación, aunque ya no es el más reciente, sigue ofreciendo una capacidad de procesamiento suficiente para aplicaciones de productividad como hojas de cálculo, navegación web, y multitarea básica. Con 16 GB de RAM, este equipo asegura un rendimiento fluido incluso al manejar varias aplicaciones a la vez, mientras que el SSD de 1 TB proporciona un almacenamiento rápido, lo que mejora significativamente los tiempos de arranque del sistema y la apertura de programas en comparación con los discos duros tradicionales.

Si bien no está diseñado para cargas de trabajo intensivas como edición de video de alta resolución o aplicaciones científicas, esta configuración es ideal para usuarios que buscan un equipo de escritorio confiable a un costo accesible. Además, la incorporación del SSD garantiza una extensión de la vida útil de la computadora, haciéndola competitiva con opciones más modernas a un precio menor. En resumen, la CPU Dell Minitorre con estas especificaciones representa una inversión inteligente para entornos que requieren productividad sin alta demanda gráfica o de procesamiento, maximizando el rendimiento a un bajo costo.



Figura 9: Cpu Dell Minitorre I7 3ra Gen. 16gb Ram 1tb Ssd. [28]

Cinta de velcro Nioval 4578.

La cinta de contacto de Velcro Nioval de 10 metros y color negro de la Figura 10 se enfoca en su relación costo-beneficio como herramienta para la organización y gestión de cables en entornos domésticos o empresariales. Con un precio aproximado de entre \$10 y \$20 USD, esta cinta de Velcro representa una opción accesible para mantener ordenado el cableado de redes, equipos de oficina y dispositivos electrónicos, reduciendo los riesgos de enredos, daños y accidentes.

La longitud de 10 metros permite un uso amplio, con la flexibilidad de cortar la cinta en segmentos personalizados según la necesidad específica, optimizando su uso y reduciendo el desperdicio de material. Su diseño de fácil ajuste y reutilización permite que se adapte a diferentes grosores de cables y dispositivos, proporcionando una solución práctica que evita el uso de cintas plásticas o bridas desechables, las cuales son menos sostenibles y convenientes para ajustes frecuentes.

Al compararla con otros métodos de organización de cables, la cinta de Velcro Nioval es económica y altamente duradera, ya que su sistema de sujeción permite múltiples usos sin perder efectividad. En entornos de red o instalaciones con equipos delicados, esta cinta también ayuda a reducir el riesgo de desconexiones accidentales y mejora la accesibilidad a los dispositivos para tareas de mantenimiento. En resumen, la cinta de Velcro Nioval de 10 metros es una inversión pequeña con un gran impacto en la organización, seguridad y flexibilidad de cualquier espacio de trabajo o sistema de cableado, maximizando la eficiencia y reduciendo costos a largo plazo.



Figura 10: Cinta De Contacto De Velcro 10m, Negra Nival 4578. [29]

Cable UTP: Se eligieron cables de diferentes categorías para cubrir una variedad de necesidades de velocidad y presupuesto, finalmente se eligió uno asegurando que haya opciones para implementarlo de manera eficiente en la red.

El cable Ethernet plano SHZHDIKUN de 30 metros, categoría 6, con conectores RJ-45, se basa en su costo y beneficios para aplicaciones de alta velocidad en redes de larga distancia. Este cable de la Figura 11 tiene un precio aproximado de entre \$15 y \$25 USD, lo que lo convierte en una opción asequible para usuarios que requieren conexiones rápidas y estables en entornos domésticos o empresariales de tamaño pequeño a mediano. Su diseño plano facilita su instalación en espacios reducidos, bajo alfombras o pegado a la pared, sin sacrificar calidad de conexión.

La categoría 6 de este cable permite transmitir datos a velocidades de hasta 1 Gbps con anchos de banda de hasta 250 MHz, adecuado para streaming de video, juegos en línea y trabajo en redes empresariales con un tráfico moderado de datos. Además, al ser un cable reforzado, tiene una durabilidad superior que protege contra daños físicos, disminuyendo la probabilidad de fallos y aumentando su vida útil, lo que reduce costos de reemplazo a largo plazo.

Frente a cables redondos o de categorías inferiores, el SHZHDIKUN plano de 30 metros es una inversión razonable que proporciona estabilidad en la conexión y es ideal para instalaciones en las que la apariencia y el orden son prioritarios. El cable Ethernet Cat6 es una solución económica y eficiente para redes que necesitan un cableado estructurado duradero y de alta velocidad, maximizando la eficiencia de la red sin un gasto elevado.



Figura 11: SHZHDIKUN Plano Cable Ethernet Red Lan RJ-45. [24]

Impresiones de los componentes

La elección de componentes en una red es crucial para optimizar el costo y maximizar la funcionalidad y estabilidad de la infraestructura, lo que garantiza la viabilidad económica del proyecto y facilita la toma de decisiones estratégicas sobre su diseño e implementación. Los switches juegan un papel esencial al gestionar el tráfico de red, y en este caso, se ha elegido el Cisco Catalyst 2960 Series de 24 puertos por su confiabilidad y capacidad de administración avanzada, que incluye soporte para VLAN, QoS y autenticación 802.1X. Estas características de seguridad y eficiencia lo convierten en una inversión rentable, especialmente en entornos empresariales donde es crucial minimizar el tiempo de inactividad.

Para enrutamiento, el router Cisco 2911 Series equilibra su costo inicial con un rendimiento robusto que soporta redes de alta demanda y ofrece características avanzadas, como VPN y redundancia. Esto asegura una conectividad estable y escalable, aspectos fundamentales para empresas con tráfico intenso, mejorando así el retorno de inversión al reducir posibles interrupciones y costos de mantenimiento.

Los Access Points Huawei AirEngine 5761R-11E seleccionados destacan por sus capacidades avanzadas y la implementación de Wi-Fi 6, que aumenta la velocidad y disminuye la interferencia, ideal para entornos de alta densidad de usuarios. Su costo se justifica al reducir la necesidad de puntos de acceso adicionales, favoreciendo una gestión centralizada y una conectividad rápida y estable.

El rack Intellinet 26U de 19 pulgadas permite una organización eficiente de los equipos de red, lo que simplifica el mantenimiento y asegura la protección física de los dispositivos, contribuyendo a una infraestructura estable y de

bajo costo operativo. Las charolas de 1U maximizan el uso del espacio en el rack y ofrecen soporte seguro para equipos pesados, mientras que el organizador de cables Intellinet facilita el manejo ordenado del cableado, mejorando la ventilación y reduciendo los riesgos de daños.

Un patch panel Cat6 de 24 puertos asegura una conectividad centralizada y estructurada, permitiendo conexiones de alta velocidad y reduciendo el tiempo de instalación y mantenimiento. Este componente resulta esencial en redes empresariales, optimizando la administración y asegurando una infraestructura escalable y organizada.

La CPU Dell Minitorre con procesador i7, 16 GB de RAM y SSD de 1 TB equilibra costo y rendimiento para tareas de productividad sin alta demanda gráfica, resultando ideal para estaciones de trabajo básicas en un entorno de red empresarial, prolongando la vida útil y asegurando un rendimiento fluido a un bajo costo.

La cinta de Velcro Nioval para organización de cables representa una opción práctica y económica para mantener el orden en el cableado, reduciendo enredos y mejorando la estética de la infraestructura. Cada componente ha sido seleccionado para maximizar la eficiencia, confiabilidad y facilidad de mantenimiento, logrando una red económica y preparada para el crecimiento futuro.

Especificación y simplificación.

La Tabla 4 organiza y resume los componentes de red y equipos necesarios para varios edificios. La primera columna identifica los tipos de componentes (switches, routers, access points, racks, charolas para racks, organizadores frontales, patch panels, CPU, cinta velcro y cable UTP), mientras que la segunda columna especifica el modelo de cada componente.

Las siguientes columnas indican las cantidades de cada componente en los edificios 01, 02, Central, 03, 04, 05 y en el edificio de Gobierno. Cada edificio tiene un conjunto diferente de equipos dependiendo de sus necesidades específicas. Por ejemplo, los switches Cisco 2960 de 24 puertos están distribuidos en cada edificio, con una suma total de 42 switches. Los routers Cisco 2900 Series 2911 están presentes solo en dos edificios.

Los racks están presentes en cada edificio, con un total de 7 racks para todos los edificios. Cada edificio también cuenta con sets de charolas para racks, totalizando 11 sets. Además, los organizadores frontales de cables están distribuidos en cada edificio con un total de 7 organizadores. Los patch panels se asignan a cada rack con un total de 42 en todos los edificios.

Otros componentes incluyen CPUs, cintas de velcro y rollos de cable UTP, que también están repartidos entre los edificios, con

un total de 527 CPUs, 133 cintas de velcro y 90 rollos de cable UTP.

Esta tabla es útil para visualizar la distribución y cantidad de componentes de red en varios edificios, lo que permite planificar y gestionar mejor la infraestructura tecnológica. Además, nos proporciona un resumen claro para llevar a cabo el análisis económico de los componentes.

La Tabla 5 presenta un desglose detallado de los componentes de red y equipos necesarios para la red ESCOM, junto con sus costos. Las columnas incluyen el tipo de componente, el modelo, la cantidad a adquirir, el costo unitario, y el costo total.

Cada componente tiene un modelo específico y se indica cuántas unidades se requieren, así como el costo de cada uno, ya sea por unidad (c/u) o por set. Los componentes listados incluyen switches, routers, access points, racks, charolas para racks, organizadores frontales, patch panels, CPUs, cintas de velcro y cables UTP. Los costos unitarios varían ampliamente; por ejemplo, los access points tienen un costo elevado de \$16,000 c/u, mientras que las cintas de velcro cuestan \$89 c/u. El costo total para cada componente se calcula multiplicando la cantidad requerida por su costo unitario.

Al final de la tabla, se muestra la sumatoria total de los costos de todos los componentes, que asciende a \$1,997,600.50, representando la inversión total necesaria para la adquisición de los componentes de red para la infraestructura de ESCOM.

Al comparar precios de los equipos y determinar su distribución, el análisis económico asegura que el presupuesto del proyecto pueda ser sostenible a largo plazo y que la red sea funcional. Las referencias de precios han sido tomadas de [20], [21], [22], [23], [24], [25], [26], [27], [28] y [29].

Componente	Modelo	Cantidad por edificio							
		Edificio 01	Edificio 02	Edificio Central	Edificio 03	Edificio 04	Edificio 05	Edificio de Gobierno	Suma Total de componentes
Switches	Switch Cisco 2960 Series Catalyst 24 puertos	12 Switches	8 Switches	6 Switches	2 Switches	5 Switches	4 Switches	5 Switches	42 Switches
Routers	Router Cisco 2900 Series 2911 Nuevo con licencias básicas	-	1 Router	-	-	-	1 Router	-	2 Routers
Access Point	Acces Point Huawei Airengine 5761r-11e	-	1 Access Point	-	1 Access Point	-	-	-	2 Access Points
Racks	Rack Intellinet 26u 19in Estándar	1 Rack	1 Rack	1 Rack	1 Rack	1 Rack	1 Rack	1 Rack	7 Racks
Charola para racks	Set4 Charola 1 U Para Rack Servidor D19 Max 25kg	3 Set de charolas	3 Set de charolas	1 Set de charolas	1 Set de charolas	1 Set de charolas	1 Set de charolas	1 Set de charolas	11 Set de charolas
Organizador frontal	Organizador Frontal De Cables Intellinet 16995	1 Organizador	1 Organizador	1 Organizador	1 Organizador	1 Organizador	1 Organizador	1 Organizador	7 Organizadores
Pach Panel	Pach Panel Cat6 24puertos 1u Rack 19 520959 Intellinet	12 Pach panel	8 Pach panel	6 Pach panel	2 Pach panel	5 Pach panel	4 Pach panel	5 Pach panel	42 Pach panel
CPU	Cpu Dell Minitorre I7 3ra Gen. 16gb Ram 1tb Ssd	126 CPU's	91 CPU's	55 CPU's	12 CPU's	60 CPU's	120 CPU's	63 CPU's	527 CPU's
Cinta velcro	Cinta De Contacto De Velcro 10m, Negra Nioval 4578	32 Cintas velcro	23 Cintas velcro	14 Cintas velcro	3 Cintas velcro	15 Cintas velcro	30 Cintas velcro	16 Cintas velcro	133 Cintas velcro
Cable UTP	Cable Ethernet 30m Reforzado Cat6 RJ-45	21 Rollos de cable	16 Rollos de cable	10 Rollos de cable	2 Rollos de cable	10 Rollos de cable	20 Rollos de cable	11 Rollos de cable	90 Rollos de cable

Tabla 4: Análisis de componentes. Fuente: Propia

Componente	Modelo	Cantidad por adquirir	Costo unitario	Costo total
Switches	Switch Cisco 2960 Series Catalyst 24 puertos	42 Switches	\$2,500.00 c/u	\$105,000.00
Routers	Router Cisco 2900 Series 2911 Nuevo con licencias básicas	2 Routers	\$2,500.00 c/u	\$5,000.00
Access Point	Acces Point Huawei Airengine 5761r-11e	2 Access Points	\$16,000.00 c/u	\$32,000.00
Racks	Rack Intellinet 26u 19in Estándar	7 Racks	\$2,499.00 c/u	\$17,493.00
Charola para racks	Set4 Charola 1 U Para Rack Servidor D19 Max 25kg	11 Set de charolas	\$1,019.00 c/set	\$11,209.00
Organizador frontal	Organizador Frontal De Cables Intellinet 16995	7 Organizadores	\$367.00 c/u	\$2,569.00
Pach Panel	Pach Panel Cat6 24puertos 1u Rack 19 520959 Intellinet	42 Pach panel	\$1,155.20 c/u	\$48,518.40
CPU	Cpu Dell Minitorre I7 3ra Gen. 16gb Ram 1tb Ssd	527 CPU's	\$3,325.00 c/u	\$1,752,275.00
Cinta velcro	Cinta De Contacto De Velcro 10m, Negra Nioval 4578	133 Cintas velcro	\$89.00 c/u	\$11,837.00
Cable UTP	Cable Ethernet 30m Reforzado Cat6 RJ-45	90 Rollos de cable	\$129.99 c/u	\$11,699.10
Sumatorio total del costo de los componentes requeridos para la red ESCOM.				\$1,997,600.50

Tabla 5: Análisis económico de componentes. Fuente: Propia

Diseño preliminar 1

Descripción del diseño actual

Actualmente la red de la ESCOM cuenta con tres segmentos de red principales, los cuales son 148.204.5X.0 donde X es un número para distinguir entre distintos segmentos de red, está red cuenta con una máscara de 16 bits, es decir cada segmento de red puede proporcionar hasta $2^{16} - 2$ (debido a los 16 bits restantes de la parte de red de la máscara 255.255.0.0) direcciones posibles, las cuales se reparten entre todos los edificios de la ESCOM, principalmente los segmentos 56 y 57 se reparten en los edificios 1, 2, 3, 4, gobierno y el edificio central, posteriormente en el edificio más reciente de la ESCOM, se añadió un nuevo segmento de red, siendo este el segmento 58.

También es importante mencionar, que aulas como laboratorios, obtienen su dirección IP con el protocolo de configuración dinámico de host (DHCP).

Finalmente, a considerar del diseño actual, la topología es completamente anillo, si consideramos a cada aula de cómputo como un nodo en la red, esta topología se rediseñará con la finalidad de conseguir más nodos independientes.

Propuesta de diseño para los laboratorios de sistemas, programación e inteligencia artificial.

Con el propósito de ahorrar en costes, y aprovechar al máximo los recursos disponibles para este rediseño, se ha propuesto la siguiente topología mostrada en la Figura 12 únicamente para los laboratorios de cómputo. También se ha decidido utilizar dispositivos nuevos además de configuraciones nuevas, como lo son las redes virtuales, cada laboratorio pertenecerá a una red virtual configurada en los switches, y la interfaz del router encargado de administrar esa red, se configurará en modo sub-interfaz para administrar las tres subredes de todos los laboratorios.

El site ubicado en la parte del edificio cinco (edificio de inteligencia artificial) será reubicado al edificio central con la finalidad de que contenga los dispositivos de red para los laboratorios, pues es un punto intermedio en cuanto a distancia de todos los laboratorios de la escuela superior de cómputo.

Modelo de dispositivos a utilizar

Para el rediseño se han sido considerados los dispositivos mostrados en la Figura 13, Figura 14 y Figura 15

- Router Cisco 2900: Ha sido elegido por su mayor cantidad de interfaces Gigabit Ethernet y la posibilidad de hasta cuatro tarjetas de expansión, pues servirá también como router principal.

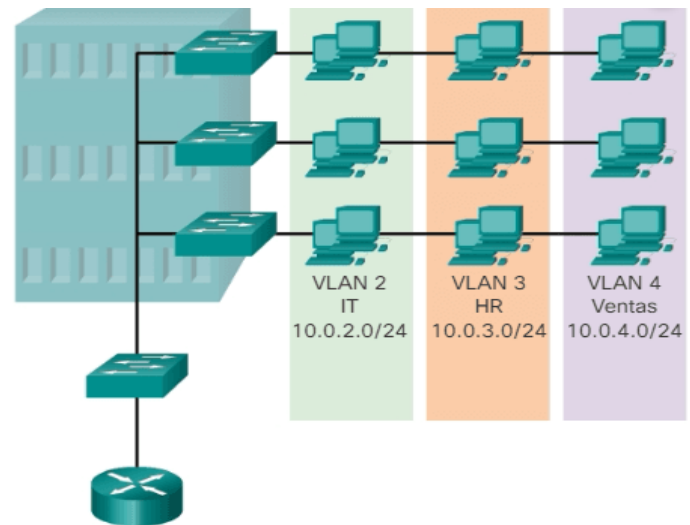


Figura 12 Propuesta de diseño lógico en los laboratorios [33]



Figura 13 Router cisco 2900



Figura 14 Switch Cisco 2960



Figura 15 Switch Cisco SG350-10

- Switch Cisco 2960: cuenta con puertos suficientes para empezar la LAN de un laboratorio o de cualquier parte de la ESCOM además de soportar las configuraciones de redes virtuales.
- Switch Cisco SG350-10: Cuenta con los puertos suficientes para terminar la conexión de distintos hosts en los laboratorios, además de tener la función de ahorrar costes.

Creación de subredes

La red a utilizar será la red 148.204.0.0 / 16 una dirección de clase B la cual dividiremos **por número de host** utilizando VLSM.

VLSM

Significa máscara de subred de longitud variable, se produce cuando el diseño de subred utiliza varias máscaras en la misma red. Significa que se utiliza más de una máscara para varias subredes de una red o una sola clase A, B, C.

Subred	Hosts requeridos	Nº de Host	Dirección de red	Máscara	Primer Host	Último Host	Broadcast
Laboratorios	300	510	148.204.0.0	255.255.254.0	148.204.0.1	148.204.1.254	148.204.1.255
Salones	125	126	148.204.2.0	255.255.255.128	148.204.2.1	148.204.2.126	148.204.2.127
Edificio central	60	62	148.204.2.128	255.255.255.192	148.204.2.129	148.204.2.190	148.204.2.191
Edificio de gobierno	60	62	148.204.2.192	255.255.255.192	148.204.2.193	148.204.2.254	148.204.2.255
Edificio 4	60	62	148.204.3.0	255.255.255.192	148.204.3.1	148.204.3.62	148.204.3.63
Laboratorio libre y alrededores	40	62	148.204.3.64	255.255.255.192	148.204.3.65	148.204.3.126	148.204.2.127
Edificio 3	12	14	148.204.3.128	255.255.255.240	148.204.3.129	148.204.3.142	148.204.3.143

Tabla 6 Distribución de subredes para el rediseño

En la Tabla 6 se observan las subredes que han sido creadas a partir de la cantidad de host requerida para esta tarea, en este primer diseño, únicamente se creará la topología y se han detallado algunas configuraciones especiales, pues a nivel lógico es una red virtual, a su vez el inicio de la red destinada a los laboratorios se volverá a sub netear de modo que cada laboratorio (sistemas, programación y IA) tenga su propia red, esto puede verse en la Tabla 7.

Subred	Hosts requeridos	Nº de Host	Dirección de red	Máscara	Primer Host	Último Host	Broadcast
Laboratorios de sistemas	90	126	148.204.0.0	255.255.255.128	148.204.0.1	148.204.0.126	148.204.0.127
Laboratorios de programación	90	126	148.204.0.128	255.255.255.128	148.204.0.129	148.204.0.254	148.204.0.255
Laboratorios de inteligencia artificial	120	126	148.204.1.0	255.255.255.128	148.204.1.1	148.204.1.126	148.204.1.127

Tabla 7 Subredes para los laboratorios

VLSM es equivalente a dividir subredes en subredes, lo que significa que VLSM permite a los ingenieros de red dividir el espacio de direcciones IP en jerarquías de subredes de diferentes tamaños. Por lo tanto, VLSM permite a los ingenieros de redes crear subredes con diferentes recuentos de hosts con solo una pequeña cantidad de direcciones que se desperdician. VLSM se utiliza para aumentar la disponibilidad de subredes porque las subredes pueden ser de tamaño variable. También se define como un proceso de división en subredes para una subred [30].

Se ha decidido utilizar VLSM para dividir la red de la escuela por cantidad exacta de hosts, los cuales podremos tomar por edificio de la Tabla 2 la dirección IP 148.204.0.0 / 16 ha sido utilizada para realizar las subredes solicitadas.

VLAN

Las VLAN (Virtual LAN), o también conocidas como redes de área local virtuales, es una tecnología de redes que nos permite crear redes lógicas independientes dentro de la misma red física. El objetivo de usar VLAN en un entorno doméstico o profesional es para segmentar adecuadamente la red y usar cada subred de una forma diferente, además, al segmentar por subredes usando VLANs se puede permitir o denegar el tráfico entre las diferentes VLAN gracias a un dispositivo L3 como un router o un switch multicapa L3 [31].

¿Para qué sirven?

Cuando configuramos una red de área local, ya sea en un entorno doméstico donde queramos segmentar los diferentes dispositivos a conectar, o en un entorno profesional, hacemos uso de VLANs para tener diferentes subredes. Podemos crear diferentes VLANs para diferentes usos y realizar una administración mucho más sencilla de la red, además, seremos capaces de «contener» los mensajes de broadcast en dominios de difusión más pequeños, es decir, tendremos subredes pequeñas para proporcionar direccionamiento a las decenas de equipos que tengamos, y no solamente una subred donde haya cientos de dispositivos conectados [31].

Tipos de VLAN

Actualmente existen varios tipos de VLANs que podemos utilizar en los diferentes equipos, es decir, en los switches y puntos de acceso WiFi. Las diferentes VLANs que existen son las basadas en el estándar 802.1Q VLAN Tagging basado en etiquetas, las VLAN basadas en puerto, las VLAN basadas en MAC, las VLAN basadas en aplicaciones, aunque esta última no suele utilizarse habitualmente.

- **VLAN nativa:** La VLAN nativa, también denominada VLAN 1, tiene un papel fundamental en la segmentación de redes. Es la VLAN por defecto en un switch, y su función principal es manejar el tráfico que no lleva información con etiqueta de VLAN.
- **802.1Q VLAN Tagging:** Es el tipo de VLAN más utilizada, hace uso del estándar 802.1Q para etiquetas o quitar la etiqueta a las VLANs. Este estándar consiste en introducir una cabecera 802.1Q dentro de la trama Ethernet que todos conocemos, con el objetivo de diferenciar las diferentes VLANs que tengamos configuradas. Este estándar no encapsula la trama original de Ethernet, sino que añade 4 bytes al encabezado Ethernet original, además, el cambio de «EtherType» se cambia al valor 0x8100 para señalar que se ha cambiado el formato de la trama [31].

- **VLAN tagged:** en las tramas Ethernet se incorpora el «tag» del VLAN ID que hayamos configurado, este tipo de VLANs son entendidas por todos los switches, por los puntos de acceso WiFi profesionales y por los routers. Se pueden configurar en modo «tagged» una o más VLANs en un determinado puerto. En los enlaces troncales (desde un router a un switch, de switch a switch y de switch a AP) se suelen configurar siempre como «tagged» para «enviarles» todas las VLANs [31].
- **VLAN untagged:** en las tramas Ethernet se retira el tag que hayamos configurado, este tipo de VLANs son entendidas por todos los dispositivos, pero principalmente se utilizan de cara a los equipos finales como ordenadores, portátiles, impresoras, cámaras IP y otro tipo de dispositivo. En un puerto en concreto solamente podremos configurar una VLAN como «untagged», no podemos poner dos VLANs como «untagged» porque el equipo final no «entendería» nada [31].

Este estándar es el que será utilizado, de modo que se tienen diferentes formas de ser configurados.

- **Acceso:** El puerto en cuestión del switch, accede a una VLAN en específico.
- **Troncal:** Le da acceso a una o varias VLAN de un switch a otro, a través del puerto que es configurado de este modo.
- **Dinámico:** Dependiendo del tipo de paquete que reciba el switch, se pondrá como access o como trunk. No se recomienda configurar los puertos de un switch en modo dinámico por seguridad para evitar posibles ataques [31].

Enrutamiento entre VLAN

Las VLAN se utilizan para segmentar las redes de switch de Capa 2 por diversas razones. Independientemente del motivo, los hosts de una VLAN no pueden comunicarse con los hosts de otra VLAN a menos que haya un router o un switch de capa 3 para proporcionar servicios de enrutamiento.

El *Enrutamiento Entre VLAN (Inter-VLAN Routing)* es el proceso de reenviar el tráfico de red de una VLAN a otra VLAN [32].

Enrutamiento Inter-VLAN Router-on-a-Stick

Solo requiere una interfaz Ethernet física para enrutar el tráfico entre varias VLAN de una red. Una interfaz Ethernet del router Cisco IOS se configura como un troncal 802.1Q y se conecta a un puerto troncal en un switch de capa 2. Específicamente, la interfaz del router se configura mediante subinterfases para identificar VLAN enrutables. Las subinterfases configuradas son interfaces virtuales basadas en software. Cada uno está asociado a una única interfaz Ethernet física. Estas subinterfases se configuran en el software del router. Cada una se configura de forma independiente con sus propias direcciones IP y una asignación de VLAN. Las subinterfases se configuran para subredes diferentes que corresponden a su asignación de VLAN. Esto facilita el enrutamiento lógico. Cuando el tráfico etiquetado de VLAN entra en la interfaz del router, se reenvía a la subinterfaz de VLAN. Después de tomar una decisión de enrutamiento basada en la dirección de red IP de destino, el router determina la interfaz de salida del tráfico. Si la interfaz de salida está configurada como una subinterfaz 802.1q, las tramas de datos se etiquetan con la nueva VLAN y se envían de vuelta a la interfaz física [32].

Reubicación de sites con enrutador

Para este diseño preliminar, el site principal estará en su ubicación anterior, es decir en el edificio 2, planta baja, mientras que otro site será reubicado al edificio central de modo que pueda conectarse de forma alámbrica a todos los laboratorios de la ESCOM.

Posteriormente el router más reciente, ubicado en el edificio cinco, al lado de los laboratorios de inteligencia artificial, se ha decidió mover hacia el edificio cuatro, para mantener una cercanía con el router del site principal.

Diseño preliminar 2

Salones de clase y algunas aulas

Para la implementación de la topología para los salones, habiendo tomado el segmento de red correspondiente de la Tabla 6, dicha red se ha vuelto a subnetear según el número de salones en cada edificio, pues se han conectado según el dispositivo router que tengan más cercado, por ejemplo, para los salones y salas de los edificios 1 y 3 se ha utilizado una interfaz del router en el site del edificio central.

Para los salones de los edificios 2 y 4 se ha utilizado una interfaz del router en el site principal (misma ubicación que la actual).

Finalmente, para el edificio cinco se ha utilizado la interfaz del último router, ubicado en el edificio 4 en planta baja.

Las nuevas subredes para los salones pueden verse en la Tabla 8, esta misma contiene la cantidad aproximada de host por cada edificio, que es un host por salón más unos cuantos para salas o clubes.

Subred	Host	Dirección de red	Máscara	Primer host	Último host	Broadcast
Edificio 5	25	148.204.2.0	255.255.255.224	148.204.2.1	148.204.2.30	148.204.2.31
Edificio 2	17	148.204.2.32	255.255.255.224	148.204.2.33	148.204.2.62	148.204.2.63
Edificio 3	17	148.204.2.64	255.255.255.224	148.204.2.65	148.204.2.94	148.204.2.95
Edificio 4	14	148.204.2.96	255.255.255.240	148.204.2.97	148.204.2.110	148.204.2.111
Edificio 1	10	148.204.2.112	255.255.255.240	148.204.2.113	148.204.2.126	148.204.2.127

Tabla 8 Subredes para los salones

Como se ha mencionado, en algunas subredes ha sido necesario implementarlas con redes virtuales nuevamente.

Implementación de las configuraciones de red

Laboratorios

En la Figura 12 se ha mostrado la topología utilizada, ahora en esta sección se mostrará la configuración, cada laboratorio necesita 30 computadoras, por lo que se han utilizado switches de 24 y 10 puertos para lograr este número de conexiones, por lo que en cada laboratorio se encuentran al menos estos dos dispositivos, los cuales conectados entre si, pueden ser vistos como un único conmutador de 34 puertos, en la Tabla 9 se muestra la distribución de estas en los laboratorios, con esta información y con la idea de que podemos ver a cada laboratorio como un único conmutador, en la Figura 16 se puede observar un esquema de la configuración que ha de tener cada puerto en el conmutador.

Laboratorios	Vlan	Nombre Vlan
Sistemas	10	LAB SISTEMAS
Programación	20	LAB PROG
Inteligencia artificial	30	LAB_IA

Tabla 9 Distribución de VLAN

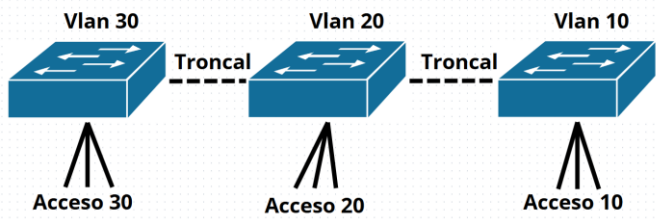


Figura 16 Representación de la configuración de los puertos en los conmutadores

Comandos de configuración

Todos los switches de 24 puertos en todos los laboratorios comparten una configuración en común, en la Tabla 10 se muestra dicha configuración, puede intuirse que el parámetro id, se trata de la vlan en cuestión, según el laboratorio que se esté configurando.

Comandos de configuración en los conmutadores de 24 puertos	
Comando	Significado
en	enable: entra al modo privilegiado
conf t	Configure terminal: Entra en el modo de configuración
Vl 10	Vlan 10: Crea la VLAN con id 10
Na LAB_SISTEMAS	Name LAB_SISTEMAS: se nombra a la VLAN 10 con el nombre dado
Vl 20	Vlan 20: Crea la VLAN con id 20
Na LAB_PROG	Name LAB_PROG: se nombra a la VLAN 10 con el nombre dado
Vl 30	Vlan 30: Crea la VLAN con id 30
Na LAB_IA	Name LAB_IA: se nombre a la VLAN 30 con el nombre dado
ex	Exit: Sale del modo de configuración de VLAN
Int r fa0/1-24	Interface range fa0/1-24: Selecciona el rango de interfaces indicado
Sw m a	Switchport mode Access: Coloca en modo de acceso a los puertos seleccionados
Sw a v [vlan-id]	Switchport access vlan [id]: El Puerto seleccionado, servirá para acceder a la VLAN con el id dado
Int r gi0/1-2	Interface range gi0/1-2: Selecciona el rango de interfaces indicado
Sw m t	Switchport mode trunk: Coloca los puertos seleccionados como acceso troncal para tráfico proveniente de VLANs

Tabla 10 Configuración común de los conmutadores de 24 puertos de los laboratorios

Ya se ha mencionado en la teoría el enrutamiento inter vlan router-on-a-stick, ahora es tiempo de ponerlo en práctica, en la Figura 17 se muestra las configuraciones para interfaces de modo que estos laboratorios tengan comunicación con otras redes externas, la configuración del enrutador que se ha elaborado se encuentra en la Tabla 11.

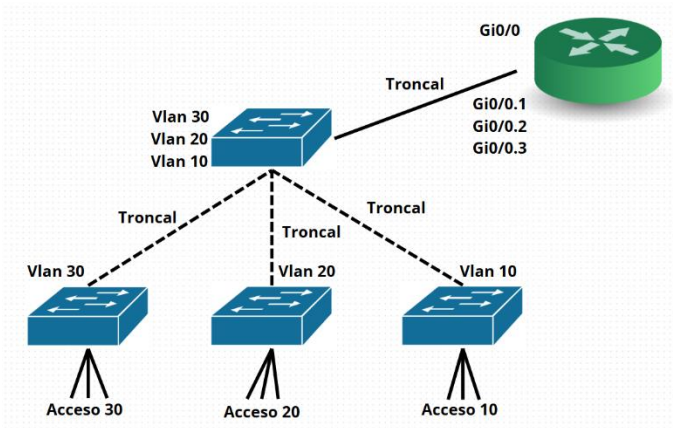


Figura 17

Configuración del enrutador para laboratorios (edificio central)	
En	enable: entra al modo privilegiado
Conf t	Configure terminal: Entra en el modo de configuración
Int gi0/0	Interface Gi0/0: selecciona la interfaz GigabitEthernet 0/0
No sh	No shutdown: enciende la interfaz
Int gi0/0.[n]	Interface GigabitEthernet0/0.[n]: entra en el modo de configuración de sub-interfaz
Encapsulation dot1Q [vlan-id]	Configura la subinterfaz para responder al tráfico encapsulado 802.1Q del vlan-id especificado.
Ip add [ip] [mask]	Ip address [ip] [mask]: se asigna dirección IP con máscara de red en la interfaz seleccionada
No sh	Enciende la sub-interfaz

Tabla 11 Configuración del enrutador del edificio central para los laboratorios

Edificio de gobierno

Para el rediseño de las aulas del edificio de gobierno (Becas, materiales, dirección y subdirección) se ha optado por tomar una interfaz disponible del router principal (planta baja del edificio 2) y asignarle la subred a dicha interfaz, que va hacia una serie de conmutadores, conectados entre sí, siguiendo una topología de estrella, si bien es parecido al diseño actual, el edificio entero cuenta con su propia subred, en la Figura 18 puede verse en la parte superior izquierda el enrutador en cuestión, además de la dirección IP según la división de subredes.

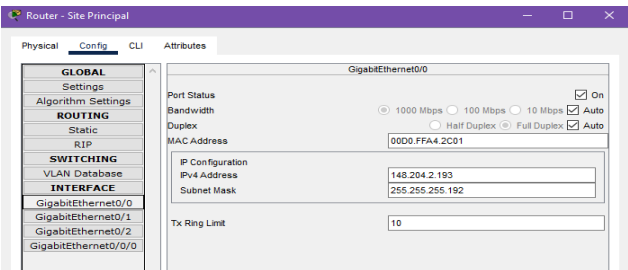


Figura 18 Puerta de enlace edificio de gobierno

Por lo que la configuración se resume a los comandos de asignación de dirección IP `ip add [ip] [mask]`

Salones

Como se ha mencionado en el diseño, se han vuelto a subdividir las redes destinadas a los salones de clase, y el objetivo es conectar cada salón a la interfaz de algún enrutador que tengan más cerca, en el caso de los salones de los edificios 1 y 3, el enrutador del edificio central es el más cercano a ellos, en la Tabla 8 se muestran las redes destinadas y en la Figura 19 una tabla de información de interfaces de dicho router, con el objetivo de utilizar los recursos con los que actualmente se cuentan, se han vuelto a utilizar redes virtuales, está vez en la interfaz GigabitEthernet 0/2, siendo está dividida dos veces.

Device Name: Router Edificio Central					
Device Model: 2911					
Hostname: Router					
Port	Link	VLAN	IP Address	IPv6 Address	MAC Address
GigabitEthernet0/0	Up	--	<not set>	<not set>	0040.0BA3.7101
GigabitEthernet0/0.1	Up	--	148.204.0.1/25	<not set>	0040.0BA3.7101
GigabitEthernet0/0.2	Up	--	148.204.0.129/25	<not set>	0040.0BA3.7101
GigabitEthernet0/0.3	Up	--	148.204.1.1/25	<not set>	0040.0BA3.7101
GigabitEthernet0/1	Up	--	10.10.1.2/29	<not set>	0040.0BA3.7102
GigabitEthernet0/2	Up	--	<not set>	<not set>	0040.0BA3.7103
GigabitEthernet0/2.1	Up	--	148.204.2.65/27	<not set>	0040.0BA3.7103
GigabitEthernet0/2.2	Up	--	148.204.2.113/28	<not set>	0040.0BA3.7103
Vlan1	Down	1	<not set>	<not set>	0080.F97D.75C0

Figura 19 Enrutador del edificio central configurado

Salones	Vlan	Nombre Vlan
Edificio 1	40	E1 SALONES
Edificio 3	50	E3 SALONES
Edificio 2	60	E2 SALONES
Edificio 4	70	E4 SALONES
Edificio 5	80	E5 SALONES

Tabla 12 Distribución de VLAN para salones

En la Tabla 12 se muestra la disposición de redes virtuales para los salones de todos los edificios.

En el caso de los edificios 1 y 3, por la Tabla 8 sabemos que el edificio 1 cuenta con aproximadamente 10 hosts o 10 salones, mientras que el edificio 3, con 17, por lo que se ha conectado un switch de 24 puertos con uno de 10 puertos a través de un cable cruzado, puede verse en la Figura 20

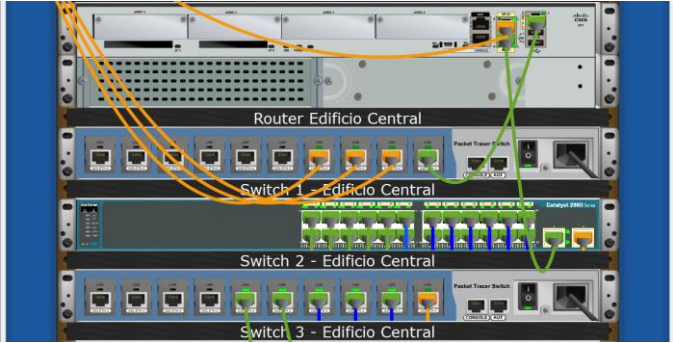


Figura 20

Donde dichos switches se han configurado con las redes virtuales 40 y 50 con los comandos `vlan` y `name`, los puertos 1 al 10 del switch 2, se han configurado de acceso a la vlan 40 con el comando `switch port Access vlan 40` y el resto a la vlan 50 (color azul) las interfaces GigabitEthernet se han configurado como accesos troncales con el comando `switchport mode trunk`, y finalmente se han conectado servidores DHCP para cada vlan.

La misma idea se ha seguido para los salones del edificio 2 y 4 y en el diseño final para el edificio 5.

Enrutamiento

Finalmente, para la comunicación entre todas las subredes, se ha optado por utilizar rutas estáticas, pues aún al ser una LAN mediana, no se ve necesario el uso de enrutamiento dinámico que podría afectar el uso de procesamiento de los enrutadores, puesto que además la red no escala en poco tiempo, más sin embargo no se descarta estas opciones de escalamiento.

Hemos necesitado conectar tres router entre si, para ello utilizamos una dirección de red privada, como la 10.10.1.0 y la 20.20.1.0 con una máscara 255.255.255.248.

Configuración de rutas entre el enrutador principal y el enrutador del edificio central

En la Tabla 13 se muestra la configuración de rutas estáticas de cada enrutador hasta este diseño preliminar.

Router edificio central	Router site principal
Router(config)#ip route 148.204.2.192 255.255.255.192 10.10.1.1 Router(config)#ip route 148.204.2.32 255.255.255.224 10.10.1.1 Router(config)#do wr Building configuration... [OK] Router(config)#	Router(config)#ip route 148.204.0.0 255.255.255.128 10.10.1.2 Router(config)#ip route 148.204.0.128 255.255.255.128 10.10.1.2 Router(config)#ip route 148.204.1.0 255.255.255.128 10.10.1.2 Router(config)#ip route 148.204.2.64 255.255.255.224 10.10.1.2 Router(config)#ip route 148.204.2.112 255.255.255.240 10.10.1.2 Router(config)#do wr Building configuration... [OK] Router(config)#

Tabla 13 Configuración de enrutamiento hasta el diseño preliminar 2

Diseño final

En el diseño final se ha añadido el último enrutador con el que cuenta la escuela, además de configurar todas las subredes y enrutamiento estático, en la Tabla 14 podemos ver todas las subredes configuradas en todos los enrutadores con la salida del comando `show ip route`.





Tabla 14 - subredes en los enrutadores

Como se puede observar, los enrutadores han sido configurados conforme a las descripciones de diseño descritas en este documento, siendo necesario únicamente utilizar direccionamiento IP estático en algunas computadoras del edificio central.

Pruebas de conectividad

Se han realizado pruebas desde un punto de toda la ESCOM, todas estas pruebas se han realizado desde el laboratorio de sistemas digitales 1, con segmento de red 148.204.2.128 hacia cada subred vista anteriormente en el documento. La dirección de la máquina en cuestión se ve en la Figura 21. Y en la Tabla 15 las pruebas.

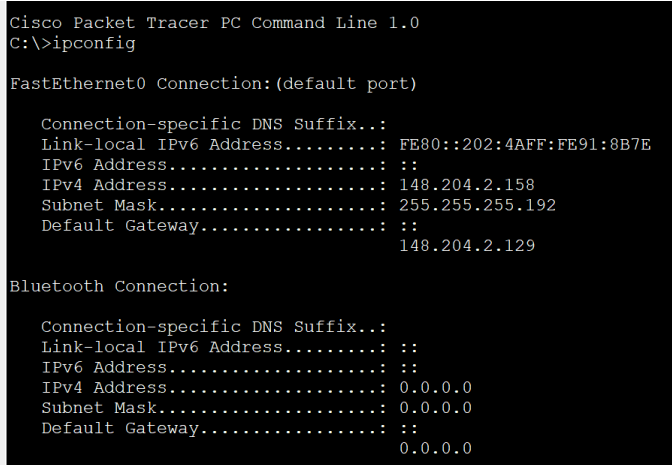


Figura 21

148.204.0.0	148.204.0.128	148.204.1.0
<pre> C:\>ping 148.204.0.2 Pinging 148.204.0.2 with 32 bytes of data: Request timed out. Reply from 148.204.0.2: bytes=32 time=69ms TTL=127 Reply from 148.204.0.2: bytes=32 time=1ms TTL=127 Reply from 148.204.0.2: bytes=32 time<1ms TTL=127 Ping statistics for 148.204.0.2: Packets: Sent = 4, Received = 3, Lost = 1 (25% loss), Approximate round trip times in milli-seconds: Minimum = 0ms, Maximum = 69ms, Average = 23ms </pre>	<pre> C:\>ping 148.204.0.130 Pinging 148.204.0.130 with 32 bytes of data: Reply from 148.204.0.130: bytes=32 time<1ms TTL=127 Reply from 148.204.0.130: bytes=32 time<1ms TTL=127 Reply from 148.204.0.130: bytes=32 time<1ms TTL=127 Reply from 148.204.0.130: bytes=32 time=1ms TTL=127 Ping statistics for 148.204.0.130: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 0ms, Maximum = 1ms, Average = 0ms C:\> </pre>	<pre> C:\>ping 148.204.1.3 Pinging 148.204.1.3 with 32 bytes of data: Request timed out. Reply from 148.204.1.3: bytes=32 time<1ms TTL=127 Reply from 148.204.1.3: bytes=32 time<1ms TTL=127 Reply from 148.204.1.3: bytes=32 time<1ms TTL=127 Ping statistics for 148.204.1.3: Packets: Sent = 4, Received = 3, Lost = 1 (25% loss), Approximate round trip times in milli-seconds: Minimum = 0ms, Maximum = 0ms, Average = 0ms </pre>
148.204.2.192	148.204.2.112	148.204.3.64
<pre> C:\>ping 148.204.2.194 Pinging 148.204.2.194 with 32 bytes of data: Request timed out. Reply from 148.204.2.194: bytes=32 time<1ms TTL=126 Reply from 148.204.2.194: bytes=32 time<1ms TTL=126 Reply from 148.204.2.194: bytes=32 time<1ms TTL=126 Ping statistics for 148.204.2.194: Packets: Sent = 4, Received = 3, Lost = 1 (25% loss), Approximate round trip times in milli-seconds: Minimum = 0ms, Maximum = 0ms, Average = 0ms </pre>	<pre> C:\>ping 148.204.2.114 Pinging 148.204.2.114 with 32 bytes of data: Reply from 148.204.2.114: bytes=32 time=10ms TTL=127 Reply from 148.204.2.114: bytes=32 time<1ms TTL=127 Reply from 148.204.2.114: bytes=32 time<1ms TTL=127 Reply from 148.204.2.114: bytes=32 time=42ms TTL=127 Ping statistics for 148.204.2.114: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 0ms, Maximum = 42ms, Average = 13ms C:\> </pre>	<pre> C:\>ping 148.204.3.66 Pinging 148.204.3.66 with 32 bytes of data: Reply from 148.204.3.66: bytes=32 time=10ms TTL=127 Reply from 148.204.3.66: bytes=32 time=14ms TTL=127 Reply from 148.204.3.66: bytes=32 time=4ms TTL=127 Reply from 148.204.3.66: bytes=32 time=81ms TTL=127 Ping statistics for 148.204.3.66: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 4ms, Maximum = 81ms, Average = 27ms </pre>
148.204.2.32	148.204.2.64	148.204.2.96
<pre> C:\>ping 148.204.2.34 Pinging 148.204.2.34 with 32 bytes of data: Reply from 148.204.2.34: bytes=32 time=12ms TTL=126 Reply from 148.204.2.34: bytes=32 time=26ms TTL=126 Reply from 148.204.2.34: bytes=32 time<1ms TTL=126 Reply from 148.204.2.34: bytes=32 time<1ms TTL=126 Ping statistics for 148.204.2.34: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 0ms, Maximum = 26ms, Average = 9ms C:\> </pre>	<pre> C:\>ping 148.204.2.66 Pinging 148.204.2.66 with 32 bytes of data: Reply from 148.204.2.66: bytes=32 time=37ms TTL=127 Reply from 148.204.2.66: bytes=32 time<1ms TTL=127 Reply from 148.204.2.66: bytes=32 time<1ms TTL=127 Reply from 148.204.2.66: bytes=32 time<1ms TTL=127 Ping statistics for 148.204.2.66: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 0ms, Maximum = 37ms, Average = 9ms C:\> </pre>	<pre> C:\>ping 148.204.2.98 Pinging 148.204.2.98 with 32 bytes of data: Reply from 148.204.2.98: bytes=32 time=10ms TTL=126 Reply from 148.204.2.98: bytes=32 time=10ms TTL=126 Reply from 148.204.2.98: bytes=32 time=2ms TTL=126 Reply from 148.204.2.98: bytes=32 time=26ms TTL=126 Ping statistics for 148.204.2.98: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 2ms, Maximum = 26ms, Average = 12ms C:\> </pre>
148.204.3.0	148.204.2.0	
<pre> C:\>ping 148.204.3.4 Pinging 148.204.3.4 with 32 bytes of data: Request timed out. Reply from 148.204.3.4: bytes=32 time=12ms TTL=125 Reply from 148.204.3.4: bytes=32 time=36ms TTL=125 Reply from 148.204.3.4: bytes=32 time<1ms TTL=125 Ping statistics for 148.204.3.4: Packets: Sent = 4, Received = 3, Lost = 1 (25% loss), Approximate round trip times in milli-seconds: Minimum = 0ms, Maximum = 36ms, Average = 16ms C:\> </pre>	<pre> C:\>ping 148.204.2.2 Pinging 148.204.2.2 with 32 bytes of data: Request timed out. Reply from 148.204.2.2: bytes=32 time=7ms TTL=126 Reply from 148.204.2.2: bytes=32 time=34ms TTL=126 Reply from 148.204.2.2: bytes=32 time=9ms TTL=126 Ping statistics for 148.204.2.2: Packets: Sent = 4, Received = 3, Lost = 1 (25% loss), Approximate round trip times in milli-seconds: Minimum = 7ms, Maximum = 34ms, Average = 16ms C:\> </pre>	

Tabla 15 Pruebas de conectividad

CONCLUSIONES

Moreno Martínez Diego Alejandro

Es importante analizar el rendimiento de una red LAN que diariamente necesita estar disponible prácticamente el cien por ciento del tiempo, y abastecer de red a muchísimos usuarios al mismo tiempo, el análisis de la red actual en la Escuela Superior de Cómputo ha sido analizada a detalle, concluyendo que para redes locales de dicho calibre necesitan una buena elección de topología lógica, pues muchas veces la red es incapaz de tener una ruta en caso de fallas en algún nodo, a su vez se ha aprendido que es necesario evaluar costes, pues es de los factores más importantes a la hora de un rediseño. El diseño de la nueva red es una de las fases más críticas del proyecto. Se ha aprendido a seleccionar la topología de red adecuada basada en los requisitos y el tamaño de la red. También se ha mencionado la segmentación de la red para mejorar la gestión y la seguridad, pues en el diseño se ha planeado dividir la red por categorías de la Escuela Superior de Cómputo. La implementación de rutas redundantes y alta disponibilidad ha sido fundamental para asegurar la continuidad del servicio. Esta fase ha proporcionado una comprensión profunda de cómo diseñar redes eficientes y escalables. De llegar a realizarse la fase de implementación, recibir retroalimentación de los usuarios finales es esencial para identificar áreas de mejora. Se aprenderá a implementar un proceso de mejora continua para adaptar y optimizar la red según sea necesario. La capacidad de escuchar y responder a las necesidades de los usuarios.

Al diseñar, configurar y evaluar una red simplificada, hemos logrado consolidar nuestros conocimientos teóricos y adquirir habilidades prácticas fundamentales en el campo de las redes de computadoras. Uno de los aspectos más relevantes de esta práctica ha sido el primer acercamiento a las VLAN. Hemos comprendido cómo esta tecnología permite segmentar una red en múltiples redes virtuales, mejorando la seguridad, el rendimiento y la administración. Al configurar VLANs basadas en departamentos, hemos simulado un escenario real en el que diferentes áreas de una organización pueden tener requisitos de red específicos.

Asimismo, la práctica nos ha permitido familiarizarnos con los dispositivos de red más comunes, como switches y routers. Hemos aprendido a configurar interfaces, crear tablas de enrutamiento y aplicar listas de acceso para controlar el tráfico de red. Estos conocimientos son esenciales para cualquier profesional que desee diseñar y gestionar infraestructuras de red. Además de los aspectos técnicos, esta práctica ha fomentado el trabajo en equipo y la resolución de problemas. Al colaborar con nuestros compañeros, hemos podido compartir conocimientos y encontrar soluciones creativas a los desafíos que se presentaron durante la implementación de la red.

Esta práctica ha sido un primer paso en nuestro recorrido por el apasionante mundo de las redes de computadoras. Hemos adquirido las bases necesarias para comprender el funcionamiento de las redes LAN y hemos desarrollado habilidades prácticas que nos serán de gran utilidad en nuestra vida profesional. A partir de esta experiencia, estamos motivados a profundizar nuestros conocimientos en áreas como protocolos de red, seguridad informática y virtualización de redes.

He aprendido en el diseño preliminar dos que muchísimas veces se necesita trabajar con los recursos limitados o con los que se cuenta desde un inicio, aprovechar cada interfaz de un enrutador, cada interfaz de un conmutador con las configuraciones correctas es posible conectar muchas LAN's y lo necesario que se vuelve el dividir una LAN cada vez más y más, puesto que al final de este proyecto, si se llegase a implementar, va a ser muchísimo más sencillo ver que cada red cuenta con un número destinado de hosts, y para escalar hay dos alternativas, o bien añadir una nueva subred o utilizar direcciones de las sobrantes tras haber subnetado alguna de ellas. En muchas instituciones educativas, los presupuestos son limitados. Utilizar los dispositivos existentes ayuda a controlar costos y a aprovechar al máximo los fondos disponibles para otras áreas cruciales, además hemos evitado gastos innecesarios, evaluar y optimizar el uso de los dispositivos actuales antes de considerar nuevas adquisiciones.

Para la infraestructura de red de la Escuela Superior de Cómputo (ESCOM), las redes VLAN demostraron ser una herramienta fundamental para optimizar el tráfico de datos y mejorar el rendimiento general de la red. Al segmentar la red física en redes lógicas, fue posible minimizar el tráfico innecesario entre dispositivos y garantizar que los datos lleguen únicamente a los segmentos que realmente los necesitan. Esto se traduce en una mejora significativa en la eficiencia del uso del ancho de banda y en una reducción de las colisiones de paquetes dentro de la red.

En el contexto académico, donde diversas áreas como administración, laboratorios, aulas y servicios generales comparten una única infraestructura de red, las VLAN permiten asignar segmentos específicos para cada departamento. Por ejemplo, una VLAN para los laboratorios puede estar configurada para priorizar datos de alta carga, mientras que otra para servicios administrativos puede enfocarse en la seguridad de datos sensibles. Esto no solo mejora el rendimiento, sino que también facilita la administración de la red al hacer más predecible y controlable el flujo de tráfico.

Uno de los principales beneficios observados fue la capacidad de aislar el tráfico de diferentes departamentos. Por ejemplo, los laboratorios de cómputo generaron un gran volumen de tráfico debido a actividades de simulación, descarga de datos y programación en tiempo real. Al asignarles una VLAN específica, el tráfico de broadcast no afectó a otros segmentos, como el área administrativa, que manejaba información sensible y requería estabilidad en la conexión. Este tipo de segmentación también es útil en escenarios en los que se manejan aplicaciones críticas, como sistemas de videoconferencias o bases de datos institucionales, asegurando que su rendimiento no se degrade debido a la congestión en otras áreas.

Las VLAN son una herramienta invaluable para simplificar la administración y el mantenimiento de redes complejas. Al proporcionar flexibilidad, facilidad de diagnóstico y la capacidad de adaptarse a cambios dinámicos, las VLAN aseguran que la red pueda satisfacer las necesidades actuales y futuras de una institución como ESCOM.

Reducción de Costos Operativos

La consolidación de funciones de red en un número menor de dispositivos físicos y la simplificación de la gestión de la red pueden reducir significativamente los costos operativos. Menos dispositivos físicos significan menos puntos de fallo potenciales, menos necesidad de mantenimiento y una reducción en los costos de energía y espacio.

En conclusión, el diseño de una red es un proceso fundamental que asegura la eficiencia, seguridad y capacidad de adaptación de la infraestructura de una institución. La escalabilidad debe ser una consideración clave para acomodar el crecimiento y los cambios futuros sin incurrir en costos significativos o interrupciones operativas. Además, el uso de redes virtuales ofrece numerosas ventajas que pueden mejorar la flexibilidad, eficiencia y seguridad de la red, permitiendo a las universidades mantener una infraestructura de red robusta y preparada para el futuro. Este enfoque no solo optimiza el uso de los recursos actuales, sino que también posiciona a la institución para integrar nuevas tecnologías y servicios de manera efectiva y eficiente.

Rendimiento de las Redes Virtuales

Las redes virtuales ofrecen numerosos beneficios, entre ellos una mejora significativa en el rendimiento, flexibilidad y eficiencia de la infraestructura de red. Tecnologías como la Virtualización de Funciones de Red (NFV) y las Redes Definidas por Software (SDN) permiten la creación de redes virtuales que pueden ser gestionadas y configuradas con mayor facilidad y adaptabilidad que las redes físicas tradicionales.

1. Optimización del Rendimiento

Las redes virtuales permiten una optimización dinámica del rendimiento de la red, ajustando los recursos según la demanda. Esto significa que se pueden asignar más recursos a áreas de la red que experimentan altos niveles de tráfico, asegurando una experiencia de usuario fluida y sin interrupciones. La capacidad de monitorear y ajustar el rendimiento en tiempo real es una ventaja crucial para mantener altos niveles de rendimiento en una universidad.

Chávez Hernández Carol Monserrat

El rediseño de la red de ESCOM ha implicado evaluaciones de la topología existente hasta el diseño de tecnologías más acorde a las necesidades de la institución. Este proyecto nos ha hecho aplicar los conocimientos sobre gestión de proyectos, pues el análisis de costes es de lo que más debería destacar en cualquier proyecto, en particular en el área de redes de computadores destaca por el hecho de la necesidad de hardware nuevo. Uno de los primeros pasos en el rediseño de la red es la evaluación de la topología existente. Este proceso incluye la identificación de todos los dispositivos de hardware y software en uso, así como la evaluación del rendimiento y la capacidad de la red actual. Que como se ha mencionado, está por su diseño lógico ha provocado muchísimas denegaciones de servicio ante varios inconvenientes como lo son climáticos o de saturaciones por parte de los usuarios, se ha desarrollado un inventario detallado

y se ha documentado cualquier problema o limitación existente. Esta fase es crucial para entender el punto de partida y establecer una base sólida para el rediseño, además definir los objetivos del proyecto y los requisitos de los usuarios es esencial para el éxito del rediseño. Nosotros como alumnos de la institución es de vital importancia la disponibilidad, como mejorar el rendimiento de la red, aumentar la seguridad. Además, ha sido establecido un presupuesto realista que incluya costos de hardware, software, implementación y mantenimiento. Por ahora desconozco los mecanismos de seguridad con los que cuenta la red actual de la Escuela Superior de Cómputo, pero en el rediseño de esta, es importante contar con configuraciones básicas de seguridad para la administración de dispositivos de red de manera remota, como lo podría ser la autenticación básica por usuario y contraseña.

La práctica realizada sobre la estructura de una red LAN para la Escuela Superior de Cómputo nos brindó una comprensión inicial sobre los conceptos fundamentales de redes locales y su configuración en entornos académicos. A través de esta práctica, pudimos observar cómo una LAN permite interconectar diversos dispositivos para lograr una comunicación eficiente y organizada dentro de un espacio físico determinado, en este caso, la escuela.

Uno de los aspectos más relevantes fue el acercamiento a las redes VLAN (Redes de Área Local Virtual), que introducen un nivel adicional de segmentación y seguridad en la LAN. Este primer contacto con VLANs nos permitió entender cómo esta tecnología facilita la administración de grandes redes al dividir una red física en subredes lógicas, lo que resulta en una reducción en la congestión del tráfico de red y un incremento en la seguridad. La implementación de VLANs posibilita la agrupación de dispositivos según criterios lógicos (como departamentos o funciones) en lugar de su ubicación física, aportando flexibilidad a la red y mejorando la eficiencia operativa. Asimismo, aprendimos que una correcta segmentación con VLANs es fundamental para optimizar la transmisión de datos y mejorar el rendimiento general de la red. El ejercicio práctico realizado incluyó la configuración básica de VLANs en los dispositivos, lo cual nos introdujo a los comandos y procedimientos que son necesarios para llevar a cabo esta tarea en un entorno real, así como los beneficios que representa en términos de administración de tráfico y organización de la red.

El diseño de una red es un componente crucial en la infraestructura tecnológica de cualquier organización, especialmente en instituciones educativas como universidades. Un diseño de red bien pensado garantiza no solo la eficiencia y la seguridad de la red, sino también su capacidad para adaptarse y crecer con las necesidades cambiantes de la institución. Este documento explorará la importancia del diseño de la red, la necesidad de hacerla escalable a futuro y las ventajas de utilizar redes virtuales.

Durante la práctica, se destacó que las redes VLAN son esenciales para fortalecer la seguridad dentro de una red como la de ESCOM. En un entorno donde múltiples usuarios acceden a recursos compartidos, es crucial mantener la confidencialidad de los datos y prevenir accesos no autorizados. La segmentación mediante VLAN permite que cada grupo de usuarios tenga acceso únicamente a los recursos necesarios para sus actividades, reduciendo la exposición de datos sensibles.

Además, la práctica permitió observar cómo el uso de VLAN puede ser una solución escalable. En un entorno como ESCOM, donde el número de usuarios y dispositivos puede crecer constantemente, las VLAN ofrecen flexibilidad para expandir la red sin necesidad de modificaciones físicas.

La práctica evidenció que las VLAN no solo son una herramienta técnica, sino una estrategia de diseño que mejora la operatividad, seguridad y flexibilidad de las redes académicas, asegurando que puedan adaptarse a las necesidades cambiantes de la institución sin mencionar que esaltó la importancia de las VLAN en redes escalables. ESCOM, como cualquier institución educativa, está en constante expansión, incorporando nuevos laboratorios, aulas y oficinas administrativas. Con las VLAN, fue posible simular cómo añadir dispositivos y áreas adicionales sin necesidad de realizar cambios físicos en la infraestructura de red. Este enfoque reduce costos operativos y asegura que la red pueda adaptarse rápidamente a nuevas demandas. Así, en lugar de instalar hardware adicional, bastó con configurar nuevas VLAN en los switches existentes, demostrando la flexibilidad de esta tecnología.

En términos de rendimiento, el uso de VLAN permitió priorizar ciertos tipos de tráfico mediante configuraciones avanzadas, como la implementación de QoS (Calidad de Servicio). Por ejemplo, en un escenario donde las clases virtuales y las transmisiones en vivo requieren baja latencia, las VLAN facilitaron la priorización de este tipo de tráfico sobre actividades menos críticas, como la navegación general en internet. En última instancia, estas configuraciones mejoran la experiencia del usuario final y optimizan el uso de los recursos disponibles.

Un beneficio clave observado fue la facilidad para diagnosticar y resolver problemas de red. En un entorno sin VLAN, identificar la fuente de un problema puede ser un desafío, ya que el tráfico de toda la red se mezcla en un único dominio de broadcast. Sin embargo, con las VLAN, los problemas se aíslan a segmentos específicos, lo que facilita su localización y resolución. Por ejemplo, si un laboratorio

experimenta una interrupción en la conexión, los administradores pueden centrarse únicamente en la VLAN correspondiente, ahorrando tiempo y recursos.

Importancia del Diseño de una Red

El diseño de una red es esencial para asegurar que todos los dispositivos y sistemas de una institución puedan comunicarse de manera eficiente y segura. Un diseño bien planificado permite una gestión efectiva del tráfico de datos, minimiza los tiempos de inactividad y asegura que los recursos se utilicen de manera óptima. Sin un diseño adecuado, las redes pueden ser propensas a fallos, lentitud y vulnerabilidades de seguridad.

Para una universidad, donde cientos de estudiantes y personal dependen diariamente de la red para acceder a información, colaborar en proyectos y utilizar servicios en línea, la robustez y fiabilidad de la red son de máxima prioridad. Un diseño de red eficiente también facilita el mantenimiento y la solución de problemas, permitiendo una respuesta rápida a cualquier incidencia que pueda surgir. Diseñar una red con la escalabilidad en mente es vital para asegurar que la infraestructura pueda adaptarse a las necesidades futuras sin requerir rediseños costosos y disruptivos. La escalabilidad permite que la red crezca de manera ordenada, acomodando más usuarios, dispositivos y servicios a medida que la institución crece. Esto es especialmente importante en una universidad, donde los incrementos en la matrícula, la expansión de los programas y la integración de nuevas tecnologías pueden poner presión adicional sobre la red existente.

Una red escalable también facilita la adopción de nuevas tecnologías y aplicaciones, asegurando que la institución pueda mantenerse al día con las innovaciones sin enfrentarse a obstáculos técnicos significativos. Por ejemplo, la implementación de tecnologías de aprendizaje en línea, aplicaciones de realidad aumentada o sistemas avanzados de gestión de estudiantes pueden requerir recursos de red adicionales y configuraciones específicas que una red escalable puede acomodar fácilmente.

He identificado algunas ventajas de las redes virtuales, ofrecen una serie de beneficios que pueden mejorar significativamente la eficiencia y flexibilidad de la infraestructura de red. Las tecnologías como la Virtualización de Funciones de Red (NFV) y las Redes Definidas por Software (SDN) permiten la creación de redes virtuales que pueden gestionarse y configurarse con mayor facilidad y flexibilidad que las redes físicas tradicionales. La virtualización permite maximizar el uso de los recursos de hardware al permitir que múltiples funciones de red se ejecuten en el mismo hardware físico. Esto no solo reduce los costos de hardware, sino que también simplifica la gestión y el mantenimiento de la red. En lugar de tener múltiples dispositivos físicos que requieren espacio y energía, las funciones de red pueden consolidarse en un número menor de dispositivos, optimizando el uso de recursos.

Flexibilidad y Agilidad

Con las redes virtuales, la configuración y la reconfiguración de la red se pueden realizar de manera rápida y eficiente mediante software, sin necesidad de realizar cambios físicos en el hardware. Esto permite una mayor agilidad para adaptarse a las necesidades cambiantes de la universidad, como la creación de nuevas aulas virtuales, la implementación de nuevos servicios en línea o la adaptación a cambios en la carga de trabajo.

Escalabilidad Simplificada

Las redes virtuales facilitan la escalabilidad, ya que los recursos se pueden ajustar fácilmente según la demanda. Por ejemplo, si se espera un aumento en el uso de la red durante un semestre particular, los administradores de red pueden ajustar los recursos virtuales para manejar la carga adicional sin necesidad de adquirir y configurar nuevo hardware físico. Las redes virtuales pueden segmentarse fácilmente para crear entornos aislados para diferentes aplicaciones o departamentos, mejorando la seguridad. Esta segmentación permite que las universidades apliquen políticas de seguridad específicas y monitoricen el tráfico de manera más efectiva, reduciendo el riesgo de brechas de seguridad y ataques cibernéticos.

Canseco Aguilar Antony Alexis

Las topologías de red siguen siendo una herramienta esencial para la resolución de problemas de red, permitiendo desglosar y abordar problemas en las distintas capas que componen la estructura de un sistema de comunicación. Este enfoque ha sido fundamental para la comprensión y mejora de la red de ESCOM, donde la infraestructura actual se caracteriza por una topología mixta que combina elementos de diferentes configuraciones, como estrella, anillo y bus. Esta mezcla puede generar tanto ventajas, como la flexibilidad y la redundancia, como desafíos en su gestión, especialmente en términos de mantenimiento y escalabilidad.

La práctica de analizar y planificar la red de ESCOM ha proporcionado una valiosa experiencia de aprendizaje, enseñando a gestionar una red compleja y desarrollando habilidades para identificar y mitigar posibles puntos de fallo. Este proceso no solo implica la identificación de los componentes existentes, sino también la evaluación de su rendimiento y la proyección de futuras necesidades. Por

ejemplo, al realizar pruebas de velocidad y latencia, se pueden identificar cuellos de botella que afectan el rendimiento general de la red. Además, el esfuerzo significativo en el inventario y planificación de los dispositivos de la red facilita la futura expansión y mejora de la infraestructura. Contar con un inventario detallado de los equipos, su ubicación y su estado permite una gestión más eficiente, asegurando la optimización de recursos y la preparación para el crecimiento de la red.

Los posibles alcances de esta práctica son vastos. La comprensión profunda de las estructuras de red y la capacidad para planificar y gestionar su expansión y mantenimiento son habilidades cruciales que se pueden aplicar en diversas situaciones del mundo real. Estas habilidades son especialmente relevantes en el contexto actual, donde la digitalización y la conectividad son cada vez más importantes. La mejora continua de redes escolares no solo beneficia a los estudiantes y docentes, sino que también puede impactar positivamente en la comunidad local, al facilitar el acceso a recursos digitales y fomentar la inclusión.

Además, la optimización de infraestructura corporativa es un aspecto crítico, ya que las empresas dependen de redes robustas para operar eficientemente. La planificación de nuevas instalaciones de red en diferentes sectores, como salud, educación y comercio, también se convierte en una prioridad, dado que cada uno de estos sectores tiene requerimientos específicos que deben ser atendidos para garantizar un servicio ininterrumpido y de calidad.

Al dominar estas competencias, se estará mejor preparado para enfrentar desafíos en la evolución de las redes de comunicación, lo que incluye la adaptación a nuevas tecnologías como el Internet de las Cosas (IoT), que está transformando la forma en que interactuamos con dispositivos y sistemas. Asimismo, la implementación de soluciones de ciberseguridad se vuelve esencial, ya que las amenazas digitales son cada vez más sofisticadas y pueden comprometer la integridad de la red.

Así, no solo se asegura la sostenibilidad financiera del proyecto, sino también que la red sea funcional y adaptativa a las necesidades futuras. La capacidad de anticipar y responder a cambios en la demanda y la tecnología se convierte en un factor clave para el éxito a largo plazo de cualquier infraestructura de red. Esto garantiza que la red se mantenga relevante y eficiente en un entorno en constante cambio, permitiendo a la ESCOM no solo cumplir con sus objetivos académicos, sino también posicionarse como un referente en el uso de tecnología educativa en la región.

Canseco Aguilar Antony Alexis. Parte 2.

En el presente trabajo se ha llevado a cabo un análisis exhaustivo de la infraestructura de red de la ESCOM, destacando la importancia de una adecuada planificación y diseño para optimizar el rendimiento y la eficiencia de los recursos disponibles. Se ha evidenciado que la topología actual, basada en un anillo con segmentos de estrella, presenta limitaciones significativas, como el riesgo de puntos únicos de fallo, la dificultad para añadir o eliminar nodos y problemas de ancho de banda compartido. Estas limitaciones pueden afectar la disponibilidad y la calidad del servicio, lo que resulta crítico en un entorno educativo donde la conectividad es fundamental para el aprendizaje y la investigación.

A través de la implementación de un rediseño que incorpora subredes utilizando VLSM y la segmentación mediante VLANs, se ha propuesto un enfoque que no solo mejora la gestión del tráfico, sino que también asegura una mayor flexibilidad y escalabilidad en la red. La creación de subredes específicas para cada laboratorio y aula permitirá una mejor asignación de recursos y una administración más eficiente del tráfico, minimizando la congestión y mejorando la experiencia del usuario.

Además, se ha realizado un análisis económico detallado de los componentes necesarios, lo cual ha permitido establecer un presupuesto sostenible que garantice la viabilidad del proyecto a largo plazo. Se ha seleccionado una combinación de dispositivos de red, incluyendo switches, routers y puntos de acceso, que cumplen con los requisitos técnicos y económicos establecidos. La elección de dispositivos de marcas reconocidas, como Cisco y Huawei, asegura no solo un rendimiento óptimo, sino también el soporte y la capacidad de actualización que se requieren en un entorno en constante evolución.

La justificación de cada componente se ha fundamentado en su capacidad para proporcionar un rendimiento óptimo y una alta disponibilidad, lo que se traduce en una infraestructura de red robusta y confiable. La inclusión de dispositivos que permitan la gestión centralizada y la implementación de tecnologías como Wi-Fi 6 contribuirá a mejorar la conectividad en áreas de alta densidad de usuarios, lo cual es esencial en un campus educativo.

Finalmente, se ha resaltado la importancia de la documentación y el inventario de los dispositivos de red, lo que facilitará futuras expansiones y garantizará la seguridad de la infraestructura. Un registro preciso de los dispositivos permitirá implementar medidas de seguridad adecuadas y cumplir con normativas que exigen un control riguroso de la infraestructura tecnológica. Con las recomendaciones y configuraciones propuestas, se espera que la red de la ESCOM no solo satisfaga las necesidades actuales, sino que

también esté preparada para adaptarse a los desafíos futuros en el ámbito educativo y tecnológico, asegurando que tanto estudiantes como docentes cuenten con las herramientas necesarias para un aprendizaje eficiente y efectivo.

Canseco Aguilar Antony Alexis. Parte 3.

Se ha demostrado que el modelo Open Systems Interconnection (OSI) es una herramienta fundamental para la comprensión y resolución de problemas en redes de comunicación. A través de sus siete capas, se ha facilitado la identificación y el análisis de las funciones necesarias para la transmisión efectiva de datos. Cada capa del modelo, desde la capa física hasta la capa de aplicación, desempeña un papel crucial en el proceso de comunicación, asegurando que los datos se envíen y reciban de manera adecuada y eficiente.

La capa física, por ejemplo, se encarga de la transmisión de bits a través de medios físicos, mientras que la capa de enlace de datos garantiza la integridad de los datos mediante la detección y corrección de errores. La capa de red, por su parte, se ocupa del enrutamiento y la asignación de direcciones, lo que permite que los datos encuentren su camino a través de redes complejas. Esta estructura jerárquica del modelo OSI no solo ayuda a los profesionales de la tecnología de la información a abordar problemas complejos de manera sistemática, sino que también proporciona una base sólida para el desarrollo de nuevas tecnologías y protocolos de comunicación.

Además, se ha resaltado la importancia de los componentes de la red, como conmutadores, routers y servidores, en la implementación y mantenimiento de infraestructuras de red. Los conmutadores, que operan en la capa de enlace de datos, son esenciales para la conexión de dispositivos dentro de una misma red, mientras que los routers, que funcionan en la capa de red, permiten la interconexión entre diferentes redes. Los servidores, por otro lado, proporcionan recursos compartidos y servicios a los clientes, facilitando así la comunicación y el acceso a la información. Se ha concluido que la correcta integración de estos elementos, junto con el uso de protocolos estandarizados, es esencial para el funcionamiento óptimo de las redes modernas.

Los laboratorios realizados durante esta práctica han permitido una comprensión más profunda del modelo OSI en acción. A través de ejercicios prácticos, se han simulado situaciones reales de red, donde se han podido aplicar los conceptos teóricos aprendidos. Por ejemplo, en el laboratorio de la capa de enlace de datos, se experimentó con la configuración de conmutadores y se observó cómo estos gestionan el tráfico de datos. En el laboratorio de la capa de red, se realizaron ejercicios de enrutamiento que facilitaron la comprensión de cómo los paquetes de datos se dirigen a través de diferentes redes y cómo se manejan las direcciones IP.

El laboratorio de la capa de transporte permitió la implementación de protocolos como TCP y UDP, lo que ayudó a visualizar las diferencias en la entrega de datos y la confiabilidad de cada uno. Estas experiencias prácticas no solo reforzaron el conocimiento teórico, sino que también desarrollaron habilidades prácticas en la configuración y solución de problemas en redes. Sin embargo, al conectar múltiples computadoras, llevó a la aparición del síndrome del túnel carpiano.

Por último, se ha enfatizado que el modelo OSI sigue siendo relevante en la actualidad, proporcionando un marco de referencia que guía a los profesionales en la resolución de desafíos técnicos y en la optimización de las comunicaciones en entornos cada vez más complejos. A medida que la tecnología avanza y las redes se vuelven más sofisticadas, la comprensión del modelo OSI se vuelve aún más crítica.

Canseco Aguilar Antony Alexis. Parte 4.

En el análisis realizado sobre la infraestructura de red de la Escuela Superior de Cómputo (ESCOM), se ha llegado a diversas conclusiones que reflejan la experiencia de aprendizaje adquirida a lo largo de la práctica. Se ha evidenciado que el diseño y la planificación de redes son fundamentales para optimizar el rendimiento y la eficiencia de los recursos disponibles. La topología mixta actual, que combina elementos de estrella, anillo y bus, presenta limitaciones significativas que afectan la conectividad y la calidad del servicio. Esta situación ha llevado a la necesidad de un rediseño que contemple una estructura más adecuada y escalable.

La experiencia de gestionar una red compleja ha permitido desarrollar habilidades prácticas en la identificación de problemas y en la propuesta de soluciones efectivas. Se ha aprendido que el modelo Open Systems Interconnection (OSI) es una herramienta valiosa para desglosar y abordar problemas en las distintas capas de la red. Cada capa desempeña un papel crucial en la comunicación, y su comprensión ha facilitado la identificación de cuellos de botella y puntos de fallo. Esta metodología ha sido aplicada en el análisis del rendimiento de la red de ESCOM, donde se han realizado pruebas de velocidad y latencia para evaluar la eficacia de la infraestructura actual.

Los posibles alcances de esta práctica son amplios y relevantes en el contexto actual de digitalización y conectividad. La capacidad de planificar y gestionar redes no solo beneficia a la institución, sino que también impacta positivamente en la comunidad local, facilitando el acceso a recursos digitales y fomentando la inclusión. La optimización de la infraestructura de red en entornos educativos es esencial, ya que permite a estudiantes y docentes contar con herramientas adecuadas para el aprendizaje y la investigación.

Además, se ha identificado que la experiencia adquirida en esta práctica puede ser aplicada en diversos sectores, como la salud, la educación y el comercio, donde cada uno presenta requerimientos específicos que deben ser atendidos para garantizar un servicio de calidad. La planificación de nuevas instalaciones de red y la implementación de tecnologías emergentes, como el Internet de las Cosas (IoT), son aspectos que se han proyectado como posibles aplicaciones de los conocimientos adquiridos.

La implementación de soluciones de ciberseguridad también ha sido reconocida como un aspecto crítico en la gestión de redes. La creciente sofisticación de las amenazas digitales exige que se adopten medidas adecuadas para proteger la integridad de la infraestructura. Así, se ha concluido que la capacidad de anticipar y adaptarse a cambios en la demanda y la tecnología es fundamental para el éxito a largo plazo de cualquier red.

Por último, se ha resaltado la importancia de la documentación y el inventario de los dispositivos de red, lo que facilitará futuras expansiones y garantizará la seguridad de la infraestructura. Con las recomendaciones y configuraciones propuestas, se espera que la red de ESCOM no solo satisfaga las necesidades actuales, sino que también esté preparada para enfrentar los desafíos futuros en el ámbito educativo y tecnológico. La experiencia adquirida en esta práctica ha sido enriquecedora y ha proporcionado una base sólida para el desarrollo profesional en el campo de las redes de comunicación.

Cohete Ronquillo Julio César

Uno de los aspectos más destacados de esta práctica ha sido la identificación de las diferentes tecnologías y protocolos empleados en la red. Hemos podido observar cómo se utilizan switches, routers y servidores para interconectar los dispositivos y permitir la comunicación entre ellos. Además, hemos analizado la importancia de las VLAN para segmentar la red y mejorar el rendimiento, así como la función de los protocolos de enrutamiento en la selección de la mejor ruta para los paquetes de datos.

La documentación detallada de la red existente nos ha permitido identificar posibles áreas de mejora y oportunidades de optimización. Hemos detectado algunos cuellos de botella en el tráfico de red y hemos sugerido posibles soluciones, como la actualización de equipos obsoletos o la implementación de nuevas tecnologías. Asimismo, hemos evaluado la seguridad de la red y hemos propuesto medidas para fortalecerla, como la implementación de políticas de seguridad más robustas y la utilización de herramientas de detección de intrusos.

Durante este reporte se ha demostrado la importancia de contar con una red de computadoras bien diseñada y configurada para garantizar el funcionamiento eficiente de los servicios informáticos en una institución educativa. Hemos adquirido habilidades prácticas para analizar, documentar y optimizar redes existentes, lo cual nos será de gran utilidad en nuestro futuro profesional. Además, hemos desarrollado un pensamiento crítico que nos permite identificar problemas y proponer soluciones innovadoras.

Las VLAN simplifican la administración y el mantenimiento de redes complejas como la de ESCOM. Al dividir la red en segmentos lógicos, los administradores pueden realizar tareas de monitoreo, configuración y resolución de problemas de manera más eficiente. En el caso de esta práctica, configurar y gestionar una infraestructura de red que incluye múltiples departamentos y funciones fue más sencillo gracias al uso de VLAN.

La segmentación lógica también permite que los cambios en la red sean menos disruptivos. Por ejemplo, si un laboratorio requiere un cambio en su configuración de red, este puede realizarse sin afectar el funcionamiento de las aulas o los servicios administrativos. En la práctica, observamos cómo el uso de VLAN facilita el aislamiento de problemas, ya que cualquier fallo en un segmento no afecta al resto de la red.

Un aspecto destacado durante la simulación fue cómo las VLAN pueden aislar segmentos de red con diferentes niveles de sensibilidad. Por ejemplo, los servidores que almacenan calificaciones y datos personales del personal administrativo fueron asignados a una VLAN separada, lo que impidió el acceso directo desde otros segmentos, como los laboratorios o las áreas de estudiantes. Este enfoque reduce significativamente el riesgo de accesos no autorizados, ya sea por accidente o por intentos maliciosos.

Además, esta configuración limita el impacto de posibles amenazas internas, ya que cualquier problema en una VLAN no afecta al resto de la red. La seguridad también se fortaleció mediante la implementación de políticas específicas, como listas de control de acceso (ACLs). Estas permitieron definir reglas precisas para el tráfico entre VLANs, bloqueando paquetes no autorizados o restringiendo el acceso a ciertos servicios. Por ejemplo, los laboratorios pudieron ser configurados para acceder únicamente a recursos compartidos específicos, mientras que el tráfico hacia servidores administrativos fue estrictamente controlado. Esta segmentación es clave para cumplir con normativas de privacidad y seguridad, especialmente en instituciones que manejan datos sensibles.

Otra ventaja observada fue la capacidad de las VLAN para proteger la red frente a ataques comunes, como el sniffing o el spoofing. En redes donde todos los dispositivos están en el mismo dominio de broadcast, es más fácil para un atacante interceptar o manipular datos. Sin embargo, con las VLAN, cada segmento opera como una red separada, lo que dificulta significativamente este tipo de actividades maliciosas. Esto fue particularmente útil en la práctica, ya que permitió simular cómo una red académica puede protegerse de amenazas externas e internas.

REFERENCIAS

- [1] Cloudflare, «Cloudflare,» 2023. [En línea]. Available: <https://www.cloudflare.com/es-es/learning/ddos/glossary/open-systems-interconnection-model-osi/>.
- [2] Santos Chávez J., «Delta Protect,» 5 Octubre 2023. [En línea]. Available: <http://www.deltaprotect.com/blog/modelo-osi>.
- [3] Informática Moderna, «Informática moderna,» [En línea]. Available: <https://www.informaticamoderna.com/Site.htm>.
- [4] Hapo, «BigHardware,» 25 Marzo 2021. [En línea]. Available: <https://bighardware.es/conmutadores-de-red-o-switch/>.
- [5] Keith Shaw, «Computerworld,» 2022 Octubre 7. [En línea]. Available: <https://www.computerworld.es/article/2113372/que-es-un-switch-o-conmutador-de-red-y-como-funciona.html>.
- [6] Cisco, «¿Qué es un Router? Definición y usos,» 2021 Octubre 2021. [En línea]. Available: https://www.cisco.com/c/es_mx/solutions/small-business/resource-center/networking/what-is-a-router.html.
- [7] Oscar Moreno, «AO Data Cloud,» 7 Noviembre 2023. [En línea]. Available: <https://aodatacloud.es/blog/que-es-un-access-point/>.
- [8] Curiosoando, «¿Qué es un servidor de red? - Curiosoando,» Curiosoando, 17 febrero 2022. [En línea]. Available: <https://curiosoando.com/que-es-un-servidor-de-red>. [Último acceso: 30 octubre 2024].
- [9] A. De León, «Servidores de Red: ¿Qué son y para qué sirven? Ventajas y Desventajas,» Infranetworking, 24 agosto 2021. [En línea]. Available: https://blog.infranetworking.com/servidores-de-red/#Tipos_de_Servidores_de_Red. [Último acceso: 30 octubre 2024].
- [10] HP, «¿Qué es un firewall de red y cómo funciona? Laptop-Computer,» HP® Deutschland, 31 agosto 2021. [En línea]. Available: <https://www.hp.com/mx-es/shop/tech-takes/que-es-un-firewall-de-red-y-como-funciona>. [Último acceso: 30 octubre 2024].
- [11] Telefónica Tech, «GATEWAY ¿Qué es y para qué sirve? - Telefónica,» Telefónica Tech, 11 abril 2024. [En línea]. Available: <https://conectividadiot.telefonicatech.com/gateway/>. [Último acceso: 31 octubre 2024].
- [12] Google, «Balanceo de carga de red. Google Cloud,» Google, 1 julio 2023. [En línea]. Available: <https://cloud.google.com/use-cases/load-balancing?hl=es>. [Último acceso: 30 octubre 2024].
- [13] C. Albarrán, «Cableado estructurado, qué es, tipos y utilidades,» Redes&Telecom, 6 noviembre 2023. [En línea]. Available: <https://www.redestelecom.es/infraestructuras/cableado-estructurado-que-es-tipos-y-utilidades/>. [Último acceso: 30 octubre 2024].
- [14] Y. Fernández, «Repetidor WiFi, qué es y cómo funciona,» Xataka - Tecnología y gadgets, móviles, informática, electrónica, 26 marzo 2021. [En línea]. Available: <https://www.xataka.com/basics/repetidor-wifi-que-como-funciona>. [Último acceso: 31 octubre 2024].
- [15] Blog de TelecOable, «Diferencias entre los cables de par trenzado UTP, STP y FTP,» TelecOable, 17 11 2024. [En línea]. Available: <https://www.telecable.com/blog/diferencias-entre-cable-utp-stp-y-ftp/1374>. [Último acceso: 15 11 2024].
- [16] J.Doe, «¿Qué es un patch panel y por qué lo necesitamos?,» Comunidad FS, 06 07 2021. [En línea]. Available: <https://community.fs.com/es/article/what-is-a-patch-panel-and-why-use-it.html>. [Último acceso: 15 11 2024].
- [17] Google, «¿Qué es un módem? - Ayuda de Google Nest,» Google Help, 14 05 2022. [En línea]. Available: <https://support.google.com/googlenest/answer/6274112?hl=es-419>. [Último acceso: 15 11 2024].

- [18] S. D. Luz, «Qué es el DHCP, funcionamiento y ejemplos de configuración,» RedesZone, 09 10 2024. [En línea]. Available: <https://www.redeszone.net/tutoriales/internet/que-es-protocolo-dhcp/>. [Último acceso: 15 11 2024].
- [19] L. S. y. H. G. V. D. TAK, ANALISIS ECONOMICO, Madrid: TECNOS, S. A., 1977.
- [20] Mercado Libre, «Switch Cisco 24 Puertos Ws-c2960-24lt-l De 8 Puertos Poe New,» [En línea]. Available: https://articulo.mercadolibre.com.mx/MLM-564056087-switch-cisco-24-puertos-ws-c2960-24lt-l-de-8-puertos-poe-new-_JM. [Último acceso: 05 10 2024].
- [21] Mercado Libre, «Router Cisco 2900 Series 2911 Nuevo,» Mercado Libre, [En línea]. Available: https://articulo.mercadolibre.com.mx/MLM-1431624697-router-cisco-2900-series-2911-nuevo-_JM. [Último acceso: 05 10 2024].
- [22] Mercado Libre, «Rack Intellinet 26u Dos Postes 19in Estándar Desarmado7 /vc,» Mercado Libre, [En línea]. Available: <https://www.mercadolibre.com.mx/rack-intellinet-26u-dos-postes-19in-estandar-desarmado7-vc/p/MLM24688798>. [Último acceso: 05 10 2024].
- [23] Mercado Libre, «Acces Point Huawei Airengine 5761r-11e,» Mercado Libre, [En línea]. Available: https://articulo.mercadolibre.com.mx/MLM-1916013979-acces-point-huawei-airengine-5761r-11e-_JM. [Último acceso: 05 10 2024].
- [24] Mercado Libre, «SHZHDIKUN Plano Cable Ethernet Red Lan 30m Reforzado Cat6 Internet Consola Color Negro RJ-45,» Mercado Libre, [En línea]. Available: <https://www.mercadolibre.com.mx/shzhdikun-plano-cable-ethernet-red-lan-30m-reforzado-cat6-internet-consola-color-negro-rj-45/p/MLM32269209>. [Último acceso: 05 10 2024].
- [25] DeRemate.Com de México, S. de R.L. de C.V., «Set4 Charola 1 U Para Rack Servidor D19 Max 25kg C Regalos,» Mercado Libre, 19 Noviembre 2022. [En línea]. Available: https://articulo.mercadolibre.com.mx/MLM-1415772073-set4-charola-1-u-para-rack-servidor-d19-max-25kg-c-regalos-_JM#polycard_client=recommendations_pdp-pads-up&reco_backend=recos-merge-experimental-pdp-up-c_marketplace&reco_model=ranker_entity_v2-retrieval. [Último acceso: 30 Octubre 2024].
- [26] DeRemate.Com de México, S. de R.L. de C.V., «Organizador Frontal De Cables Intellinet 16995 En Rack De 19,» Mercado Libre, [En línea]. Available: https://articulo.mercadolibre.com.mx/MLM-589114302-organizador-frontal-de-cables-intellinet-16995-en-rack-de-19-_JM#position%3D24%26search_layout%3Dstack%26type%3Ditem%26tracking_id%3D9f6baf9-9d6b-4527-bcfb-4a2ccb6ab7c1. [Último acceso: 30 Octubre 2024].
- [27] DeRemate.Com de México, S. de R.L. de C.V., «Panel De Parcheo Cat6 24puertos 1u Rack 19 520959 Intellinet,» Mercado libre, [En línea]. Available: https://articulo.mercadolibre.com.mx/MLM-825958536-panel-de-parcheo-cat6-24puertos-1u-rack-19-520959-intellinet-_JM#position%3D15%26search_layout%3Dstack%26type%3Ditem%26tracking_id%3D54c14547-489c-46a5-9f81-4d6454914877. [Último acceso: 30 Octubre 2024].
- [28] DeRemate.Com de México, S. de R.L. de C.V., «Cpu Dell Minitorre I7 3ra Gen. 16gb Ram 1tb Ssd,» Mercado libre, 25 Septiembre 2024. [En línea]. Available: https://articulo.mercadolibre.com.mx/MLM-3362031604-cpu-dell-minitorre-i7-3ra-gen-16gb-ram-1tb-ssd-_JM#position%3D8%26search_layout%3Dstack%26type%3Ditem%26tracking_id%3D1b065c7f-e511-48b1-a18e-2367977d7031. [Último acceso: 30 Octubre 2024].
- [29] DeRemate.Com de México, S. de R.L. de C.V., «Cinta De Contacto De Velcro 10m, Negra Nioval 4578 Color Negro,» Mercado Libre, 04 Agosto 2024. [En línea]. Available: https://www.mercadolibre.com.mx/cinta-de-contacto-de-velcro-10m-negra-nioval-4578-color-negro/p/MLM31014840#wid%3DMLM2016286673%26sid%3Dsearch%26searchVariation%3DMLM31014840%26position%3D3%26search_layout%3Dgrid%26type%3Dproduct%26tracking_id%3D9e4a0ffb-. [Último acceso: 30 Octubre 2024].
- [30] Kyra, «What is VLSM (Variable Length Subnet Mask)?,» 29 Marzo 2021. [En línea]. Available: <https://www.bitwarsoft.com/es/what-is-vlsm-variable-length-subnet-mask.html>.

- [31] Sergio de Luz, «VLANs: Qué son, tipos y para qué sirven,» 17 Octubre 2024. [En línea]. Available: <https://www.redeszone.net/tutoriales/redes-cable/vlan-tipos-configuracion/>.
- [32] A Walton, «Funcionamiento de Enrutamiento Entre VLAN,» 10 Junio 2020. [En línea]. Available: <https://ccnadesdecero.es/funcionamiento-enrutamiento-entre-vlan/>.
- [33] A Walton, «Segmentación de VLAN: Introducción,» 15 Febrero 2018. [En línea]. Available: <https://ccnadesdecero.es/segmentacion-de-vlan-definicion-y-tipos/>.