

UNIVERSIDAD DE EL SALVADOR  
FACULTAD MULTIDISCIPLINARIA ORIENTAL  
DEPARTAMENTO DE INGENIERÍA Y ARQUITECTURA  
SECCIÓN DE INGENIERÍA EN SISTEMAS INFORMÁTICOS.



**INFORME FINAL DEL CURSO DE ESPECIALIZACIÓN  
DIPLOMADO DE PRE-ESPECIALIZACIÓN DISEÑO Y ADMINISTRACIÓN  
DE INFRAESTRUCTURA DE REDES EMPRESARIALES DE  
ALTA DISPONIBILIDAD.**

**TÍTULO DEL INFORME FINAL**  
“ANÁLISIS Y PRESENTACIÓN DE PROPUESTA DE MEJORA  
DE INFRAESTRUCTURA DE RED DE LA UNIVERSIDAD DE EL SALVADOR  
DE LA FACULTAD MULTIDISCIPLINARIA ORIENTAL”

**PARA OPTAR AL TÍTULO DE  
INGENIERO DE SISTEMAS INFORMÁTICOS.**

**NOMBRE DE AUTOR:**

JOSÉ NOÉ SARAVIA CHAVARRIA      SC13037  
LEONEL OSMÍN ORTEZ GUTIERREZ      GO16004

**CATEDRÁTICO ASESOR:**

ING. DIEGO ARMANDO HERRERA FLORES

OCTUBRE DE 2025  
SAN MIGUEL, EL SALVADOR, CENTRO AMÉRICA-

**UNIVERSIDAD DE EL SALVADOR  
AUTORIDADES:**



MSC. JUAN ROSA QUINTANILLA

**RECTOR.**

DRA. EVELYN BEATRIZ FARFÁN

**VICERRECTORA ACADÉMICA.**

MSC. ROGER ARMANDO ARIAS ALVARADO

**VICERRECTOR ADMINISTRATIVO.**

LIC. PEDRO ROSALÍO ESCOBAR CASTANEDA

**SECRETARIO GENERAL.**

LIC. CARLOS AMILCAR SERRANO RIVERA

**FISCAL GENERAL.**

**UNIVERSIDAD DE EL SALVADOR  
FACULTAD MULTIDISCIPLINARIA ORIENTAL  
AUTORIDADES**



MSC. CARLOS IVÁN HERNÁNDEZ FRANCO

**DECANO.**

DRA. NORMA AZUCENA FLORES RETANA

**VICEDECANA.**

LIC. CARLOS DE JESÚS SÁNCHEZ

**SECRETARIO.**

ING. JOSÉ LUIS CASTRO CORDERO

**JEFE DEL DEPARTAMENTO DE INGENIERÍA Y ARQUITECTURA.**

INGA. MILAGRO ALICIA GONZÁLES DE REYES

**COORDINADOR DE PROCESOS DE GRADO DE INGENIERÍA DE SISTEMAS  
INFORMÁTICOS**

## ÍNDICE

<b>1. Título del Proyecto.....</b>	<b>5</b>
<b>2. RESUMEN.....</b>	<b>5</b>
<b>3. Palabras Clave (Keywords):.....</b>	<b>6</b>
<b>4. Introducción.....</b>	<b>7</b>
<b>Objetivos del proyecto.....</b>	<b>8</b>
Objetivo General.....	8
Objetivos Específicos.....	8
<b>5. Marco Teórico y conceptual.....</b>	<b>9</b>
5.1. Marco Teórico.....	9
5.1.1. Concepto de redes informáticas.....	9
5.1.2. Tipos de Redes Informáticas.....	11
5.1.3. Tipos de redes por zonas geográficas.....	12
5.1.4. Tipos de red por medio de transmisión.....	13
Modelos de referencia.....	14
5.1.5. Arquitecturas de red.....	15
5.1.6. Protocolos de comunicación.....	15
VLANs y segmentación lógica.....	18
Tecnologías inalámbricas.....	18
5.1.7. Seguridad en redes.....	18
Seguridad en redes.....	19
Escalabilidad y disponibilidad.....	19
5.2. Marco Conceptual.....	20
<b>6. Análisis de la Infraestructura Actual.....</b>	<b>24</b>
Inventario de equipos de red en el data center.....	30
6.1. Segmentación lógica de red.....	33
6.2. Equipamiento de red.....	34
6.3. Infraestructura Inalámbrica.....	38
<b>7. Propuesta de Mejora y Diseño de Red.....</b>	<b>39</b>
Diagrama de enlaces Troncales.....	42
Beneficios de la Propuesta.....	44
<b>8. Justificación Técnica y Económica.....</b>	<b>46</b>
8.1. Justificación Técnica.....	46
8.2. Justificación Económica.....	47
<b>9. Metodología de Trabajo.....</b>	<b>50</b>
<b>10. Conclusiones y Recomendaciones.....</b>	<b>52</b>
Conclusión.....	52
Recomendaciones.....	53
<b>Referencias.....</b>	<b>54</b>
<b>Anexos.....</b>	<b>55</b>
Carta solicitud.....	56

### Índice de Tablas

Tabla 1. Inventario de equipos de red en el data center.....	31
Tabla 2. Presupuesto actual de los equipos de red.....	32
Tabla 3. Segmentación lógica de la red.....	33
Tabla 4. Equipamiento de red.....	34
Tabla 5. Infraestructura inalámbrica organizada por zonas.....	38
Tabla 6 de propuesta económica.....	48
Tabla 7 de subneteo propuesta.....	60
Tabla 8. tabla de vlan propuesta.....	62

### Índice de Figuras

ilustración 1. distribución actual.....	28
Ilustración 2. distribución propuesta.....	40
Ilustración 3. diagrama de enlaces.....	43
Ilustración 4. distribución de Switches propuesta.....	55
Ilustración 5.configuración de core.....	64
Ilustración 6.configuración de core.....	64
Ilustración 7.configuración de core.....	65
Ilustración 8.configuración de VLAN.....	65
Ilustración 9.configuración de VLAN.....	66
Ilustración 10.configuración de VLAN.....	66
Ilustración 11.configuración de VLAN.....	67
Ilustración 12.configuración de VLAN.....	67
Ilustración 13.configuración de VLAN.....	68
Ilustración 14.configuración de servidor DHCP.....	68
Ilustración 15.configuración servidor DHCP.....	69
Ilustración 16.configuración de servidor DHCP.....	69
Ilustración 17.configuración de VLAN.....	70
Ilustración 18.conecciones data center.....	71
Ilustración 19.conecciones data center.....	72
Ilustración 20.conecciones data center.....	72
Ilustración 22.punto de distribución de red wifi.....	73

**1. Título del Proyecto**

“ANÁLISIS Y PRESENTACIÓN DE PROPUESTA DE MEJORA DE INFRAESTRUCTURA DE RED DE LA UNIVERSIDAD DE EL SALVADOR DE LA FACULTAD MULTIDISCIPLINARIA ORIENTAL”

## **2.RESUMEN**

El presente proyecto tiene como objetivo analizar la infraestructura de red actual de la Universidad de El Salvador, Facultad Multidisciplinaria Oriental, y desarrollar una propuesta de mejora orientada a optimizar el rendimiento, la seguridad y la disponibilidad de los servicios tecnológicos institucionales.

La metodología aplicada incluyó la recopilación de información técnica mediante inspección directa, inventario de equipos, análisis topológico, segmentación de VLANs y evaluación de políticas de seguridad. Se documentó la coexistencia de equipos de diferentes marcas y generaciones, lo que genera problemas de compatibilidad, administración y estandarización. Asimismo, se identificaron deficiencias estructurales como la ausencia de una capa core definida, enlaces poco escalables y una dependencia excesiva de nodos únicos de distribución.

Los resultados del diagnóstico permitieron diseñar una propuesta de red jerárquica moderna basada en capas de acceso, distribución y core, incorporando equipos de última generación, controladores inalámbricos, firewalls, sistemas Anti-DDoS y una política de actualización gradual. La inversión estimada supera los \$230,000, incluyendo mantenimiento y licencias.

Se concluye que la implementación de la propuesta fortalecerá significativamente la estabilidad, escalabilidad y seguridad de la red, garantizando un entorno tecnológico confiable que respalde las actividades académicas, administrativas e investigativas de la Facultad a mediano y largo plazo.

### **3.Palabras Claves:**

- Red
- VLANS
- core
- firewalls
- Seguridad informática .

## **Abstract**

This project aims to analyze the current network infrastructure of the University of El Salvador, Eastern Multidisciplinary Faculty, and develop an improvement proposal focused on optimizing performance, security, and service availability.

The applied methodology included the collection of technical information through on-site inspection, equipment inventory, topological analysis, VLAN segmentation, and security policy evaluation. The coexistence of devices from different brands and generations was documented, causing compatibility, management, and standardization issues. Structural deficiencies were also identified, such as the lack of a defined core layer, limited scalability, and excessive dependence on single distribution nodes.

The results of the diagnosis led to the design of a modern hierarchical network proposal based on access, distribution, and core layers, incorporating next-generation switches, routers, firewalls, Anti-DDoS systems, and a gradual modernization plan. The estimated investment exceeds \$230,000, including maintenance and licenses.

It is concluded that implementing the proposed design will significantly strengthen the network's stability, scalability, and security, ensuring a reliable technological environment that supports the Faculty's academic, administrative, and research activities in the medium and long term.

Keywords:

- Network
- VLANS
- core
- firewalls
- computer security

#### **4. Introducción**

El presente proyecto tiene como propósito presentar una propuesta de mejora de la red de la Universidad de El Salvador, Facultad Multidisciplinaria Oriental, con el fin de optimizar su rendimiento, ampliar la cobertura, reforzar la seguridad y asegurar un flujo estable de datos entre las distintas áreas. La propuesta considera la implementación de tecnologías actualizadas, el diseño de una arquitectura escalable y la adopción de buenas prácticas en administración de redes, permitiendo así que la institución esté preparada para enfrentar las necesidades actuales y futuras de su comunidad académica.

No obstante, la Universidad de El Salvador, Facultad Multidisciplinaria Oriental, enfrenta diversos desafíos que dificultan el óptimo funcionamiento de su red. Entre ellos destacan las limitaciones presupuestarias que retrasan la adquisición de equipos de última generación, la falta de infraestructura tecnológica suficiente para cubrir las necesidades actuales, las frecuentes desconexiones y problemas de conectividad en diferentes áreas del campus, así como el constante crecimiento de las instalaciones, lo cual genera una demanda cada vez mayor de recursos de red. Estos factores evidencian la urgencia de implementar un proyecto integral que permita superar estas barreras y garantizar un servicio eficiente y confiable para toda la comunidad universitaria.

A lo largo de los últimos años, la Universidad de El Salvador, Facultad Multidisciplinaria Oriental, ha realizado esfuerzos significativos para mejorar su infraestructura tecnológica. Desde la habilitación de laboratorios de redes en 2013, hasta la construcción de micro centros de datos en fechas recientes, la institución ha avanzado progresivamente en la modernización de sus servicios digitales. Sin embargo, estos logros aún requieren ser complementados con proyectos de actualización y expansión que respondan al crecimiento constante de la población estudiantil y a las exigencias académicas actuales.

## **Objetivos del proyecto**

### **Objetivo General**

Efectuar un inspección y un análisis exhaustivo de la infraestructura actual de la red de la Universidad de El Salvador, Facultad Multidisciplinaria Oriental, con el propósito de mejorar problemas, desarrollando una propuesta de mejora que satisfaga las necesidades estudiantiles, orientados al control de acceso de los usuarios de la comunidad estudiantil, docentes, administrativos y visitantes, garantizando la autenticación, la protección de los recursos institucionales y la continuidad operativa en apoyo a las funciones académicas, investigativas y administrativas de la Facultad.

### **Objetivos Específicos**

- Evaluar la red actual de la Facultad Multidisciplinaria Oriental, identificando su estado, equipos, direcciones IP y necesidades de mejora.
- Documentar la infraestructura de red incluyendo diagramas, IPs, modelos y configuraciones.
- Diseñar estrategias de gestión y actualización, incorporando configuraciones avanzadas y nuevos equipos para encontrar puntos de mejora en el rendimiento y la sostenibilidad.
- Proponer optimización en segmentación de la red mediante VLANs y políticas de tráfico que mejoren el rendimiento y la seguridad.
- Implementar servicios DHCP centralizados para optimizar la asignación de direcciones IP.

## 5. Marco Teórico y conceptual

### 5.1. Marco Teórico

El desarrollo de infraestructuras de red en la Universidad de El Salvador, Facultad Multidisciplinaria Oriental se fundamenta en la necesidad de contar con sistemas de comunicación estables, escalables y seguros que soporten servicios académicos, administrativos y de investigación. A continuación, se presentan los principales fundamentos teóricos aplicables al proyecto:

#### 5.1.1. Concepto de redes informáticas

La conexión en red, o interconexión informática, es el proceso de conectar dos o más dispositivos informáticos, como ordenadores de sobremesa, dispositivos móviles, enrutadores o aplicaciones, para permitir la transmisión y el intercambio de información y recursos. La correcta gestión en esta red es esencial, ya que garantiza la eficiencia y seguridad, permitiendo así una transmisión o un intercambio de información exitosa.

Los dispositivos conectados en red se basan en protocolos de comunicación (reglas que describen cómo transmitir o intercambiar datos en una red) para compartir información a través de conexiones físicas o inalámbricas, asegurando así que diferentes sistemas puedan interactuar, incluso utilizando hardware o software distintos.

¿Qué son las redes informáticas?

Definición de red, una red de computadoras es un conjunto de computadoras autónomas interconectadas. La palabra interconectada hace referencia a que existe algún mecanismo que le permite intercambiar datos. Una computadora es autónoma si tiene CPU y memoria propia, denominando cada computadora en la red como el host. [2]

Una red se compone de dos o más ordenadores conectados entre sí a través de cables de modo que puedan compartir recursos. [3] El diseño de una red es eficaz siempre y cuando estén contemplados los aspectos de rendimiento, aspectos de seguridad, la confiabilidad y el crecimiento en la demanda de usuarios, elementos fundamentales que van encaminados a entornos educativos, donde se encuentra una gran demanda tecnológica.

Antes de adentrarnos en temas de redes de computadoras resulta impredecible conocer y comprender los componentes fundamentales, los elementos y mecanismos que posibiliten la comunicación eficiente entre los distintos dispositivos que las integran.

La dirección IP constituye un identificador único asignado a cada dispositivo dentro de una red basada en el protocolo de Internet (IP). Esta dirección permite localizar al host y establecer la comunicación, dado que en la cabecera de los paquetes se especifica tanto la dirección de origen como la del destino, garantizando la correcta entrega de información. [2] Su función es una de las más importantes, ya que estas actúan como el carné de identidad

de cada dispositivo dentro de la red, gracias a su función se puede localizar y establecer comunicación entre diferentes equipos, asegurando que la información que transmite llegue a su destino sin presentar confusión.

Los nodos representan los puntos de conexión en la red y pueden corresponder a equipos de cómputo, impresoras, conmutadores, módems u otros dispositivos capaces de recibir, procesar, almacenar y transmitir datos. Para integrarse de manera efectiva a la red, cada nodo requiere un identificador como una dirección IP o MAC.[4] Dentro de la red cuando se habla de nodos se refiere a todos los dispositivos que forman parte de una red y que tienen capacidad de comunicarse, compartir información y conectarse entre sí. para que estos nodos puedan funcionar de manera ordenada dentro de la red, es necesario que cuente con un identificador único, en este caso el identificador puede ser una dirección IP, esta actúa como una dirección para poder ubicar el dispositivo o una dirección MAC que es como la huella digital propia de cada tarjeta de red. evitando así la confusión entre equipos y asegurando que la información llegue al destino que corresponde sin tener ningún tipo de interferencia.

El router es un enrutador encargado de interconectar redes distintas y de dirigir los paquetes de datos hacia su destino mediante la aplicación de algoritmos de enrutamiento. Su función resulta esencial para garantizar la conectividad entre diferentes dominios de red.[10] El enrutamiento es el proceso mediante el cual los paquetes de datos encuentran un mejor camino para llegar desde un dispositivo de origen hasta el destino dentro de una red o entre redes distintas. Cuentan con dos enfoques principales, uno es el enrutamiento estático, donde el administrador o encargado configura sus rutas manualmente y estas permanecen fijas, y el enrutamiento dinámico donde los routers se comunican entre sí, esto con el fin de actualizarse constantemente y así poder adaptarse en cambios de la red, como caídas de enlaces o variaciones de tráfico.

Conmutadores o también conocidos como Switches estos permiten interconexión eficiente entre múltiples nodos de la red LAN. Puertos, son los puntos lógicos que permiten a las aplicaciones y servicios de red comunicarse entre sí.[7] En un entorno universitario como la Universidad de El Salvador, Facultad Multidisciplinaria Oriental, los switch son indispensables para la organización de la conectividad de laboratorios, aulas, oficinas y servicios administrativos, logrando así una transmisión más rápida, segura y eficiente, ya que es de gran importancia por la magnitud de usuarios que depende de la red a diario.

Gateway o también conocidos como pasarelas facilitan la comunicación entre redes heterogéneas, actuando como traductores de protocolos y formas de transmisión [7], [8].

Servidor es una computadora que provee servicios a otras computadoras denominadas clientes, también se puede denominar con la palabra servidor a una aplicación informática o programa que realice algunas tareas en beneficio de otras aplicaciones. A ese modelo de comunicación entre unos y otros se le conoce en informática como una arquitectura cliente-servidor. [8]

Sus características principales: no requiere de ningún usuario, está constantemente encendido, requiere de gran capacidad de procesamiento, cuenta con potentes medidas de seguridad, los servidores son encargados de

atender solicitudes de los clientes dentro de la red y de administrar sus recursos disponibles. Aun así los servidores pueden tener funciones muy distintas tales como:

Servidores de Archivo: Almacenan archivos de información o ficheros y alimentan con ellos la red.

Servidores de directorios activos/dominio. Administran la información relacionada con su red, sus usuarios, equipos y grupos internos.

Servidores de impresión. Gestionan el conjunto de impresoras disponibles para una red otorgando acceso a ellas y administrando la cola de impresión.

Servidores de correos. Gestionan el flujo de correo electrónico que entre, desde y hacia los clientes de una red, enviando y recibiendo mensajes y almacenando su historial.

Servidores Proxy. Cumplen un rol de respaldo, almacenando durante un tiempo y en memoria caché una copia de las páginas web disponibles para la red, para acelerar el acceso a ellas o permitir la recuperación de los datos si la original se cae.

Servidores DNS. Almacena la información necesaria para asociar un nombre de dominio con una serie de direcciones IP de los equipos vinculados a ella (sus servidores web).

Servidores DHCP. Se encarga de asignar las direcciones IP dinámicas a los clientes que se conectan a una red.

Servidores FTP. Almacenan la información puntual de los usuarios y permiten el acceso privado entre equipos.

Servidores de juego. Se dedican específicamente a almacenar información para que los clientes puedan acceder al mismo tiempo al programa recreativo.

Los servidores se puede clasificar en dos categorías principales

Los servidores dedicados son aquellos que disponen de todos sus recursos de hardware y procesamiento para atender las solicitudes del cliente y los servidores compartidos son aquellos que reciben solicitudes de cliente a través de una red, al mismo tiempo que atienden procesos de manera local, es decir provenientes de afuera de la red.

### 5.1.2. Tipos de Redes Informáticas

Normalmente, las redes informáticas se definen por zonas geográficas. Una red de área local (LAN) conecta ordenadores en un espacio físico definido, mientras que una red de área amplia (WAN) puede conectar ordenadores a través de continentes. Sin embargo, las redes también se definen por los protocolos que utilizan para comunicarse, la

disposición física de sus componentes , como gestionan el tráfico de red y la finalidad que persiguen en sus respectivos entornos. Las redes LAN más recientes pueden operar a una velocidad de hasta 10 Gbps. En comparación con las redes inalámbricas, las redes LAN inalámbricas son mucho mejores en cuanto al rendimiento, ya que es más fácil enviar señales a través de un cable o fibra óptica. [4] [10]. La Universidad de El Salvador, Facultad Multidisciplinaria Oriental cuenta con su conexión de tipo LAN segmentada por VLANs, con un servicio de wifi 6, que la convierte en una infraestructura híbrida, robusta y segura apta para soportar la demanda académica, administrativa y de investigación.

### 5.1.3. Tipos de redes por zonas geográficas

Los tipos de red de esta categoría se distinguen por la zona geográfica que cubre la red.

#### Red de área local (LAN)

Una LAN conecta ordenadores a una distancia relativamente corta, como los de un edificio de oficinas, una escuela o un hospital. Las LAN suelen ser de propiedad y gestión privada.[4]

La mayoría de las redes LAN se conectan a Internet en un punto central, las redes LAN domésticas suelen usar un único enrutador, mientras que en espacios más grandes pueden utilizar además conmutadores de red para una entrega de paquete más eficiente.

#### Red de área amplia (WAN)

Como su nombre indica, una WAN conecta ordenadores a través de grandes áreas geográficas, como regiones y continentes. Las WAN suelen tener modelos de propiedad colectiva o distribuida a efectos de gestión de la red. Las redes en la nube son un ejemplo, ya que están alojadas y son suministradas por infraestructuras en la nube públicas y privadas de todo el mundo.[3],[4]

Una red de área amplia definida por software (SD-WAN) es una arquitectura WAN virtualizada que utiliza principios SDN para centralizar la gestión de redes WAN desconectadas y optimizar el rendimiento de la red.[10]

#### Red de área metropolitana (MAN)

Las MAN son más grandes que las LAN, pero más pequeñas que las WAN. Las ciudades y las administraciones públicas suelen ser las propietarias y gestoras de las MAN.[4]

### Red de área personal (PAN)

Una PAN sirve a una sola persona. Si un usuario tiene varios dispositivos del mismo fabricante (un iPhone y un MacBook, por ejemplo), es probable que haya configurado una PAN que comparta y sincronice contenidos (mensajes de texto, correos electrónicos, fotos, etc.) entre dispositivos. [4]

#### 5.1.4. Tipos de red por medio de transmisión

Los nodos de la red pueden enviar y recibir mensajes mediante enlaces (conexiones) alámbricos o inalámbricos.

##### Redes cableadas

Los dispositivos de red cableados se conectan mediante hilos y cables físicos, incluidos hilos de cobre y cables Ethernet, de par trenzado, coaxiales o de fibra óptica. Los requisitos de tamaño y velocidad de la red suelen dictar la elección del cable, la disposición de los elementos de red y la distancia física entre dispositivos.[4]

##### Redes inalámbricas

Las redes inalámbricas sustituyen los cables por la transmisión por infrarrojos, radio u ondas electromagnéticas a través de dispositivos inalámbricos con antenas y sensores incorporados.[4]

##### Redes de Difusión

En estas varias partes interesadas en este caso dispositivos pueden recibir transmisiones unidireccionales de un único dispositivo emisor.[4]

#### Tipos de red por tipo de comunicación.

Las redes informáticas pueden transmitir datos mediante el uso de una serie de dinámicas de transmisión.

##### Redes Compartidas

Las redes compartidas se caracterizan porque varios dispositivos utilizan un mismo medio físico de transmisión para enviar y recibir datos. Este tipo de arquitecturas fue común en los inicios de las redes locales especialmente en topología de bus con cable coaxial, donde todos los nodos compiten por el canal de comunicación.[2] Para evitar que dos dispositivos transmitieran al mismo tiempo, se aplican los protocolos de control de acceso como CSMA/CD en las primeras versiones de Ethernet. [10]

## Modelos de referencia

El modelo OSI (Interconexiones de Sistemas Abiertos) es el marco conceptual que describe cómo los datos viajan a través de la red informática. El modelo propone una división de problemas para interconectar computadoras a través de redes en 7 capas.

Las capas son: Capa física , capa de enlace, capa de red, capa de transporte, capa de sesión, capa de presentación, capa de aplicación

La capa física controla la transmisión de datos de una forma adecuada, los protocolos de capa 1 incluyen especificaciones eléctricas y mecánicas.

Hay dos tipos de conexiones físicas.

### Redes Multipuntos

Una conexión de multipuntos es una configuración de red en la que solo un nodo puede comunicarse con múltiples nodos simultáneos. Varios dispositivos comparten la capacidad del canal y los enlaces de red. [4]

### Redes Punto a Punto

Los dispositivos de red establecen un enlace directo de nodo a nodo para transmitir datos, permiten la conexión en línea directa entre terminales y computadoras. [3] Cada equipo cuenta con autonomía y puede actuar como un servidor, de igual forma puede acceder a los recursos de otros equipos de red, actuando como cliente.

Los medios de transmisión se comparan en función de un conjunto de características: costo, velocidad de transmisión, ancho de banda, relación señal/ruido, distancia de operación y dificultad de instalación y uso.

Los medios de transmisión se dividen en guiados o no guiados, los guiados se encuentran por trenzados (blindado o no blindado), coaxial y fibra óptica, y los no guiados se encuentran las ondas de radio, microondas, enlace satelitales y ondas infrarrojas.

El cable trenzado es un par de conductores cada uno aísla trenzados entre sí cada cable puede ser unifilar o multifilar.

El modelo **OSI** (Open Systems Interconnection) y el modelo **TCP/IP** son la base conceptual para el diseño de redes. Estos modelos describen las funciones necesarias para la comunicación entre dispositivos, organizándose en capas que facilitan la interoperabilidad y estandarización.

Estos modelos describen las funciones necesarias para la comunicación entre dispositivos, organizándose en capas jerárquicas. El modelo OSI se compone de siete capas y el modelo TCP/IP simplifica estas funciones en cuatro capas principales facilitando su implementación en entornos reales [2], [10].

### 5.1.5. Arquitecturas de red

La arquitectura de redes informáticas establece el marco teórico de una red informática, incluidos los principios de diseño y los protocolos de comunicación.

#### Principales tipos de arquitecturas de red

##### Arquitecturas peer-to-peer (P2P)

En una arquitectura P2P, dos o más ordenadores están conectados como "pares", lo que significa que tienen el mismo poder y privilegios en la red. Una red P2P no necesita un servidor central para coordinarse. En su lugar, cada ordenador de la red actúa como cliente (un ordenador que necesita acceder a un servicio) y como servidor (un ordenador que proporciona servicios a los clientes). Cada ordenador de la red pone algunos de sus recursos a disposición de otros dispositivos de la red, compartiendo almacenamiento, memoria, ancho de banda y capacidad de procesamiento a través de la red.

##### Arquitecturas cliente-servidor

En una red cliente-servidor, un servidor central (o grupo de servidores) gestiona los recursos y presta servicios a los dispositivos cliente de la red; en esta arquitectura, los clientes no comparten sus recursos y sólo interactúan a través del servidor. Las arquitecturas cliente-servidor suelen denominarse arquitecturas por niveles debido a sus múltiples capas.

##### Arquitecturas híbridas

Las arquitecturas híbridas incorporan elementos de los modelos P2P y cliente-servidor.

### 5.1.6. Protocolos de comunicación

Ya se trate del conjunto de protocolos de Internet (IP), Ethernet, LAN inalámbrica (WLAN) o estándares de comunicación celular, todas las redes informáticas siguen protocolos de comunicación: conjuntos de reglas que cada nodo de la red debe seguir para compartir y recibir datos. Los protocolos también se basan en pasarelas que permiten la comunicación entre dispositivos incompatibles (por ejemplo, un ordenador Windows que intenta acceder a servidores Linux).

Muchas redes modernas funcionan con modelos TCP/IP, que incluyen cuatro capas de red.

#### Capa de acceso a la red.

También llamada capa de enlace de datos o capa física, la capa de acceso a la red de una red TCP/IP incluye la infraestructura de red (componentes de hardware y software) necesaria para interactuar con el medio de red. Se encarga de la transmisión física de datos (utilizando Ethernet y protocolos como el de resolución de direcciones [ARP]) entre dispositivos de la misma red.

#### Capa de Internet.

La capa de Internet es responsable del direccionamiento lógico, el enrutamiento y el reenvío de paquetes. Se basa principalmente en el protocolo IP y el Protocolo de mensajes de control de Internet (ICMP), que gestiona el direccionamiento y enrutamiento de paquetes a través de distintas redes.

#### Capa de transporte.

La capa de transporte TCP/IP permite la transferencia de datos entre las capas superior e inferior de la red. Utilizando los protocolos TCP y UDP, también proporciona mecanismos de comprobación de errores y control de flujo.

TCP es un protocolo basado en conexiones que suele ser más lento pero más fiable que UDP. UDP es un protocolo sin conexión que es más rápido que TCP pero no proporciona una transferencia garantizada. Los protocolos UDP facilitan la transmisión de paquetes para aplicaciones sensibles al tiempo (como plataformas de streaming de vídeo y juegos) y búsquedas DNS.

#### Capa de aplicación.

Capa de aplicación: La capa de aplicación de TCP/IP utiliza los protocolos HTTP, FTP, Post Office Protocol 3 (POP3), SMTP, sistema de nombres de dominio (DNS) y SSH para proporcionar servicios de red directamente a las aplicaciones. También gestiona todos los protocolos que dan soporte a las aplicaciones de usuario.

Aunque TCP/IP se aplica de forma más directa a las redes, el modelo de interconexión de sistemas abiertos (OSI) (a veces denominado modelo de referencia OSI) también ha tenido un impacto sustancial en las redes informáticas y en la informática en general.

OSI es un modelo conceptual que divide la comunicación de red en siete capas abstractas (en lugar de cuatro), lo que constituye una base teórica que ayuda a ingenieros y desarrolladores a comprender los entresijos de la comunicación de red. El principal valor del modelo OSI reside en su utilidad educativa y su papel como marco conceptual para diseñar nuevos protocolos y asegurarse de que puedan interoperar con los sistemas y tecnologías existentes.

Sin embargo, el enfoque práctico del modelo TCP/IP y su aplicabilidad en el mundo real lo han convertido en la columna vertebral de las redes modernas. Su diseño sólido y escalable y su enfoque de capas horizontales han impulsado el crecimiento explosivo de Internet, dando cabida a miles de millones de dispositivos y cantidades masivas de tráfico de datos.

### **Arquitectura de red en capas.**

El método Controlled Requirements Expression (CORE) es un conjunto de notaciones textuales gráficas, con guías específicas para la captura y validación de requerimientos del sistema, en las etapas iniciales del diseño del sistema. CORE ha sido, por tradición, pensando como puramente una técnica de captura y análisis de requerimientos (RCA), aunque soporta algunos aspectos de diseño tales como estructura de datos. CORE está basada en el principio de primero definir el problema a ser analizado (definición del problema), y luego dividirlo en unidades o puntos de vista a considerar.

El método CORE consiste en siete etapas, cada una de las etapas producen salidas que alimentan a las etapas subsecuentes como entrada o que forman parte de la especificación de requerimiento final. CORE pretende examinar el sistema y su ambiente en un número de niveles, con detalles más finos progresivamente en cada nivel.

Sus siete etapas están demostradas a continuación:

Definición del problema, siendo su propósito identificar las limitaciones del mismo. Este contiene detalles de los objetivos de las empresas de los usuarios de los usuarios del sistema, la base para la necesidad de un nuevo sistema, limitaciones del costo y tiempo, y quien va a ser el responsable de la revisión y aceptación de los resultados finales.

La estructuración del punto de vista, su principal objetivo es descomponer el ambiente del sistema en los elementos para que el sistema propuesto pueda ser analizado desde el punto de vista de todas las entidades que se comunican con él, la más importante de las cuáles son los usuarios. Durante esta etapa, todas las entidades que son fuentes potenciales de información deben ser identificadas

Colección Tabular esta etapa es cuando la información sobre los flujos de datos entre los puntos de vista y el procesamiento de estos son reunidos. Ayudando así a establecer la totalidad y consistencia.

Estructura de datos en esta etapa se da una vista más cercana del contenido, a la estructura y a la derivación de datos, al producir diagramas de estructuras de datos.

La modelación individual de punto de vista, se divide en dos partes, la primera es convertir las TCF'S en una notación diferente para producir los diagramas individuales de modelo de punto de vista. La segunda parte se refiere a agregar información nueva perteneciente a flujo de datos internos, control de acciones y tiempo de acciones.

La sexta etapa facilita el análisis de una secuencia de eventos de más de un punto de vista.

La séptima etapa se consideran restricciones adicionales tales como desempeño y seguridad, análisis de restricción.

Una red moderna se organiza bajo un esquema jerárquico que incluye:

- **Capa Core:** provee el backbone principal con alta capacidad de conmutación.
- **Capa de Distribución:** gestiona el enrutamiento y segmentación de la red.
- **Capa de Acceso:** conecta a los usuarios finales y dispositivos.

Este modelo facilita la escalabilidad, seguridad y administración.

### **VLANs y segmentación lógica**

Las **VLANs (Virtual Local Area Networks)** permiten dividir una infraestructura física en múltiples redes lógicas, incrementando la seguridad y eficiencia del tráfico. La segmentación es fundamental en instituciones educativas con múltiples departamentos y servicios.

### **Tecnologías inalámbricas**

El estándar **IEEE 802.11ax (WiFi6)** representa la última generación en conectividad inalámbrica. Ofrece mayor capacidad, menor latencia y la posibilidad de atender simultáneamente a un gran número de usuarios, condición esencial en universidades donde se conectan miles de dispositivos.

#### 5.1.7. Seguridad en redes

Las organizaciones deben planear la seguridad de sus datos, revisando las prácticas, desarrollando planes de mejoras,

es decir administrando su sistema. Para implementar un esquema de seguridad se debe tener una administración definida del sistema

Los riesgos de la información están presentes en un sistema cuando dos elementos, Amenaza y vulnerabilidad se unen, la vulnerabilidad es una debilidad en los procesos de la información, una amenaza es una situación que puede afectar la organización

Los ataques de seguridad generalmente son realizados por los más conocidos piratas informáticos, algunos los conocen como “Hackers”. Es por ello por lo que los administradores de red deben conocer los principales ataques de internet, para tomar decisión acerca de los equipos de seguridad, y conocer los posibles riesgos

### **Seguridad en redes**

Las amenazas cibernéticas hacen imprescindible contar con dispositivos y políticas de seguridad como **firewalls de próxima generación, sistemas Anti DDoS, autenticación de usuarios, segmentación de tráfico y monitoreo continuo**. La seguridad asegura la confidencialidad, integridad y disponibilidad de la información.

#### 5.1.8. Escalabilidad y rendimiento

### **Escalabilidad y disponibilidad**

La infraestructura de red debe estar preparada para crecer con las necesidades institucionales. La **escalabilidad** implica poder ampliar la red sin perder rendimiento, mientras que la **alta disponibilidad** se logra con redundancia en equipos y enlaces críticos.

## 5.2. Marco Conceptual

A continuación, se definen los conceptos clave que guiarán el desarrollo del proyecto:

- **Infraestructura de red:** Conjunto de dispositivos, protocolos y medios físicos/lógicos que permiten la comunicación de datos en una organización.
- **Escalabilidad:** Capacidad de la red para adaptarse al crecimiento de usuarios, servicios y dispositivos sin afectar su rendimiento.
- **Topología de red:** Estructura física o lógica que describe la forma en que los dispositivos están interconectados.
- **Tecnologías de la información (TI):** Conjunto de recursos tecnológicos que permiten la gestión, procesamiento y transmisión de información.

Red de computadoras

Las redes de computadores son una parte integral de nuestra vida cotidiana en la era digital. Facilitan la comunicación, el intercambio de información y la colaboración en todo el mundo.

Infraestructura de red

La infraestructura de red es la base tecnológica compuesta por hardware, software, protocolos, topologías y servicios que permiten el flujo de datos, la interconexión de dispositivos y la prestación de servicios digitales de manera segura, escalable y eficiente.

Topología de red

La topología de red es la estructura de las conexiones entre computadoras y otros componentes de la red. Existen numerosas topologías de red física entre las que una organización puede elegir según el tamaño de la red, su idoneidad y sus objetivos comerciales. Cada tipo de topología de red comprende diversas configuraciones de nodos y enlaces, y presenta sus propias ventajas y desventajas.

Switch

El switch o conmutador de red es un dispositivo multipuerto que opera en el enlace de datos, pasando datos de un segmento a otro de acuerdo con la dirección MAC de destino de las tramas en la red y eliminando la conexión una vez finalizada. Estos se utilizan cuando se desea conectar múltiples tramos de una red, fusionándose en una sola red.[7]

El conmutador mantiene información limitada sobre los nodos de enrutamiento en la red interna y proporciona enlaces a sistemas como concentradores o enrutadores, lo que le permite mejorar la capacidad de la red. También mejoran la protección de la red, ya que el control de la red facilita la investigación de los circuitos digitales

### Router

El trabajo del router o enrutador, es establecer la mejor ruta para permitir que los paquetes se transmitan a sus destinos. Esto lo logra al monitorear el mar de dispositivos de red interconectados con diferentes topologías de red. [7]

Además el router almacena datos en las redes a las que están conectados y también se utiliza para convertir tramas de LAN a WAN junto con la unidad de control de red/unidad de servicio de datos.[7]

### Punto de Acceso (Access Point)

Los puntos de acceso o access points, suelen ser máquinas independientes conectadas en red con una antena, un transmisor y un adaptador integrados. Puede actuar como un puente que conecta una red inalámbrica estándar a dispositivos inalámbricos o como un enrutador que transmite datos a otro punto de acceso.[7]

### Servidor

Un servidor (del inglés server) es una computadora o un conjunto de computadoras que, en una red informática, reciben, procesan y responden a las solicitudes hechas por los terminales de usuario, llamadas “clientes”. A este modelo de comunicación entre unos y otros se lo conoce en computación como una arquitectura cliente-servidor.[7]

### Firewall

Un firewall es un sistema de seguridad que supervisa y controla el tráfico de la red en base a un conjunto de reglas de seguridad. Los firewalls suelen situarse entre una red de confianza y una red no fiable; con frecuencia, la red no fiable es Internet. Por ejemplo, las redes de oficinas suelen utilizar un firewall para proteger su red de las amenazas en línea.[7]

### Ancho de banda.

El ancho de banda es la capacidad de una conexión de red para transmitir datos en un período de tiempo determinado. Aprende más sobre este concepto.

### Latencia

La latencia se refiere al retraso que ocurre entre el momento en que un usuario realiza una acción en una red o aplicación web y el momento en que llega a su destino, que se mide en milisegundos. Esto puede deberse a una variedad de factores y componentes dentro de la red en sí. Agregar elementos a una red puede, por lo tanto, aumentar la latencia.[7]

### Escalabilidad

La escalabilidad en redes informáticas se refiere a la capacidad de una red para crecer y adaptarse a las necesidades cambiantes sin perder rendimiento. Es esencial que una red pueda manejar un aumento en la cantidad de usuarios o dispositivos sin problemas.

### Seguridad informática

La seguridad de la tecnología de la información (seguridad informática) constituye un amplio conjunto de medidas multidisciplinarias de protección para evitar que una red informática y sus datos sufran algún tipo de vulneración, filtración, publicación de información privada o ataque.

### 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. En RedesZone os vamos a explicar en detalle qué son las VLANs, para qué sirven y qué tipos existen.

### QoS (Calidad de Servicio)

La calidad de servicio (quality of service o QoS) se refiere a cualquier tecnología que gestiona el tráfico de datos para reducir la pérdida de paquetes, la latencia y el jitter, o fluctuación, en una red. QoS controla y administra los recursos de la red estableciendo prioridades para tipos específicos de datos en la red.

#### CORE

El CORE de la red es la columna vertebral de la infraestructura de la comunicación, responsable de la transmisión rápida, confiable y segura de datos entre los distintos segmentos de la red, garantizando el soporte a los servicios críticos de la organización.

#### Gateway (Puerta de enlace)

Un Gateway es la puerta de entrada y salida de una red, encargada de interconectar sistemas con diferentes tecnologías y asegurar que la comunicación sea posible, además de contribuir al control y la seguridad del tráfico.

#### WIFI

El Wi-Fi es una tecnología de red inalámbrica que permite conectar computadoras, teléfonos, tablets, impresoras y otros dispositivos a una red local o a Internet sin necesidad de cables, usando ondas de radio. Depende de factores como el ancho de banda disponible, la latencia y la topología en la que está integrada.

## **6. Análisis de la Infraestructura Actual**

Para poder conocer la infraestructura actual de la Universidad de El Salvador, Facultad Multidisciplinaria Oriental debemos apreciar su evolución a lo largo de los años para lo cual se a preparado una cronología completa la cual se muestra a continuación:

### **Cronología de Proyectos de Red en la Universidad de El Salvador, Facultad Multidisciplinaria Oriental**

Década de 1990 – 2000 Inicio de la modernización tecnológica en la Universidad de El Salvador, Facultad Multidisciplinaria Oriental, con laboratorios de informática básicos y primeras conexiones a internet, en un contexto de expansión académica tras la firma de los Acuerdos de Paz.

2011 – 2012 Estudiantes y docentes de Ingeniería en Sistemas impulsan proyectos de redes en la facultad. Aparecen tesis y trabajos que describen el estado de la red informática de la Universidad de El Salvador, Facultad Multidisciplinaria Oriental, incluyendo limitaciones de infraestructura y conectividad.

22 de marzo de 2013 Se inaugura oficialmente un Laboratorio de Redes en la Universidad de El Salvador, Facultad Multidisciplinaria Oriental, impulsado por estudiantes y docentes de Ingeniería en Sistemas. Este espacio marcó un avance importante en la enseñanza práctica de tecnologías de red en la sede.

2015 – 2018 Diversos estudios técnicos evalúan la red de la Universidad de El Salvador, Facultad Multidisciplinaria Oriental, para soportar modalidades de enseñanza a distancia y la integración de servicios académicos en línea.

Comienza la integración de la Universidad de El Salvador al servicio internacional de eduroam, lo que incluye el campus de San Miguel y sus edificios, mejorando la conectividad inalámbrica para estudiantes e investigadores.

2022 en adelante

La Universidad de El Salvador Digital reporta la construcción de infraestructura tecnológica y micro centros de datos en las facultades multidisciplinarias, incluyendo la de Oriente, con el fin de modernizar la red, mejorar la gestión de datos y ampliar los servicios digitales.

### **Hardware Utilizado.**

Actualmente, en la Universidad de El Salvador, Facultad Multidisciplinaria Oriental, gracias a la investigación de campo se ha identificado, que se utilizan equipos de diferentes marcas, entre las cuales podemos mencionar: **Huawei, Cisco, Dahua, TP-Link y D-Link**. Esto se debe a que, con el paso de los años, se ha optado por conservar tecnología que aún se encontraba en buen estado o, en otros casos, por la falta de presupuesto para realizar un reemplazo completo de todos los equipos necesarios para una actualización. Como consecuencia, a lo largo del campus universitario se pueden encontrar switches y otros dispositivos de distintas marcas, siendo los más recientes los de la marca Huawei.

En cuanto a los fabricantes, **Huawei** se caracteriza por ofrecer soluciones de red modernas y escalables, muy utilizadas actualmente en entornos académicos y corporativos, además de contar con equipos de última generación en cuanto a gestión y seguridad, en el caso de la facultad se utilizan actualmente los siguientes equipos, switches de alto rendimiento como los modelos **S5735, S5736, S6730 y S1720**, así como routers **SMGEdgeNE8KM1A** y firewalls **USG6610E** en el Data Center. También se cuenta con soluciones especializadas como **equipos AntiDDoS** y controladoras **AirEngine9700-M1**, lo que permite desplegar una red inalámbrica de última generación con **WiFi 6** en diferentes edificios de la Facultad.[4], [5]

**Cisco**, por su parte, es considerado uno de los líderes mundiales en el sector de redes, reconocido por la estabilidad, confiabilidad y soporte técnico de sus equipos, aunque su costo suele ser más elevado aunque algunos de sus equipos presentan mayor antigüedad, sigue siendo un pilar importante de la red institucional [2],[10]. Se emplean switches **Catalyst 3850, WS-C2960X-48TS-L, SG350-10 y SF200-24**, además de una controladora **C9800-L-F-K9** en el Data Center. Su robustez y confiabilidad han permitido que continúen operativos en áreas académicas, residencias y laboratorios de redes.

En cuanto a **Dahua** es una marca principalmente asociada a soluciones de videovigilancia y seguridad, pero en algunos casos sus dispositivos de red también son empleados como parte de la infraestructura tecnológica, la facultad cuenta con switches como el **DH-S5600-48GT4XF**, utilizados en áreas administrativas y de servicios al público, lo que amplía la diversidad de fabricantes en el entorno [7].

**TP-Link y D-Link**, en cambio, son marcas que se destacan por ser más accesibles económicamente, utilizadas frecuentemente en instituciones educativas y oficinas pequeñas, aunque su rendimiento y opciones de

gestión avanzada pueden ser limitados en comparación con Cisco o Huawei [8], de TP-Link se encuentran switches como el **JetStream TL-SG3452P**, instalados en facultades como **Sociología** y en sistemas de vigilancia. Suelen ser equipos más accesibles y funcionales en entornos de menor demanda, mientras que D-Link tiene una presencia más reducida, con modelos como el **DE-1210**, ubicados en oficinas y residencias, principalmente para brindar conectividad básica.

La diversidad de los fabricantes en la infraestructura de la red de la Facultad, si bien ha permitido asegurar la operatividad de distintas etapas de desarrollo, plantea desafíos técnicos relevantes. La heterogeneidad obliga al personal de IT a gestionar diferentes interfaces de administración, metodologías de configuración y, en algunos casos funciones propietarias, lo que dificulta la estandarización de procesos y el mantenimiento integral de la red. [2],[10] Aunque la compatibilidad básica entre dispositivos está garantizada por la adopción de estándares internacionales como IEEE 802.1Q, la coexistencia de equipos de distinta generación puede generar limitaciones en la gestión avanzada de VLANs, la aplicación de políticas de seguridad y la integración de servicios como telefonía IP o videovigilancia. [6],[11],[13]

En términos de cobertura, la Facultad ha realizado esfuerzos por **modernizar el acceso inalámbrico**, desplegando puntos de acceso **WiFi 6** en áreas estratégicas como Biblioteca, Medicina, Agronomía, Ingeniería y espacios comunes. Esto representa un avance significativo en comparación con la infraestructura cableada, que aún mantiene dispositivos de generaciones anteriores [12].

En conclusión, la infraestructura de red actual de la Facultad presenta una **combinación de equipos modernos y antiguos**. Si bien esto ha permitido garantizar la continuidad de los servicios tecnológicos, también supone retos en cuanto a **administración, compatibilidad, seguridad y escalabilidad** [14],[15]. La situación actual hace evidente la necesidad de una estrategia de estandarización y actualización gradual que permita consolidar una red más homogénea, eficiente y preparada para responder a las necesidades académicas y administrativas de la facultad.

### **Infraestructura general**

- La red está organizada bajo una **arquitectura jerárquica con core, distribución y acceso**.

### **Análisis de La Red Actual**

La infraestructura de red institucional de la Facultad Multidisciplinaria Oriental se compone de una arquitectura híbrida que integra equipos de distintas marcas, entre ellas Huawei, Cisco, Dahua, D-Link y TP-Link, los cuales se encuentran distribuidos en el Data Center, edificios académicos y áreas administrativas. Actualmente, la red implementa un esquema de segmentación por VLANs para la gestión de las distintas áreas funcionales, utilizando direccionamientos IP privados dentro de los rangos 172.16.0.0/20 y 192.168.x.0/24, además de subredes dedicadas para la red inalámbrica WiFi 6. La infraestructura incluye controladoras CAPWAP, firewalls redundantes Huawei USG6610E, y routers Huawei NE8KM1A, lo que permite un control centralizado del tráfico y la aplicación de políticas de seguridad. No obstante, se evidencia una heterogeneidad en los dispositivos de acceso y distribución, derivada de la coexistencia de múltiples fabricantes y modelos, lo que complica las labores de administración, monitoreo y mantenimiento. Asimismo, la ausencia de una arquitectura jerárquica plenamente estandarizada y de un backbone de alta capacidad entre los nodos de distribución limita la escalabilidad y el desempeño de la red. Estas condiciones justifican la necesidad de plantear una propuesta de mejora orientada a la optimización del diseño lógico y físico de la red, con el fin de fortalecer su eficiencia, redundancia, seguridad y capacidad de expansión.

A continuación se coloca el diagrama de red actual utilizado por la Universidad de El Salvador, Facultad Multidisciplinaria Oriental.

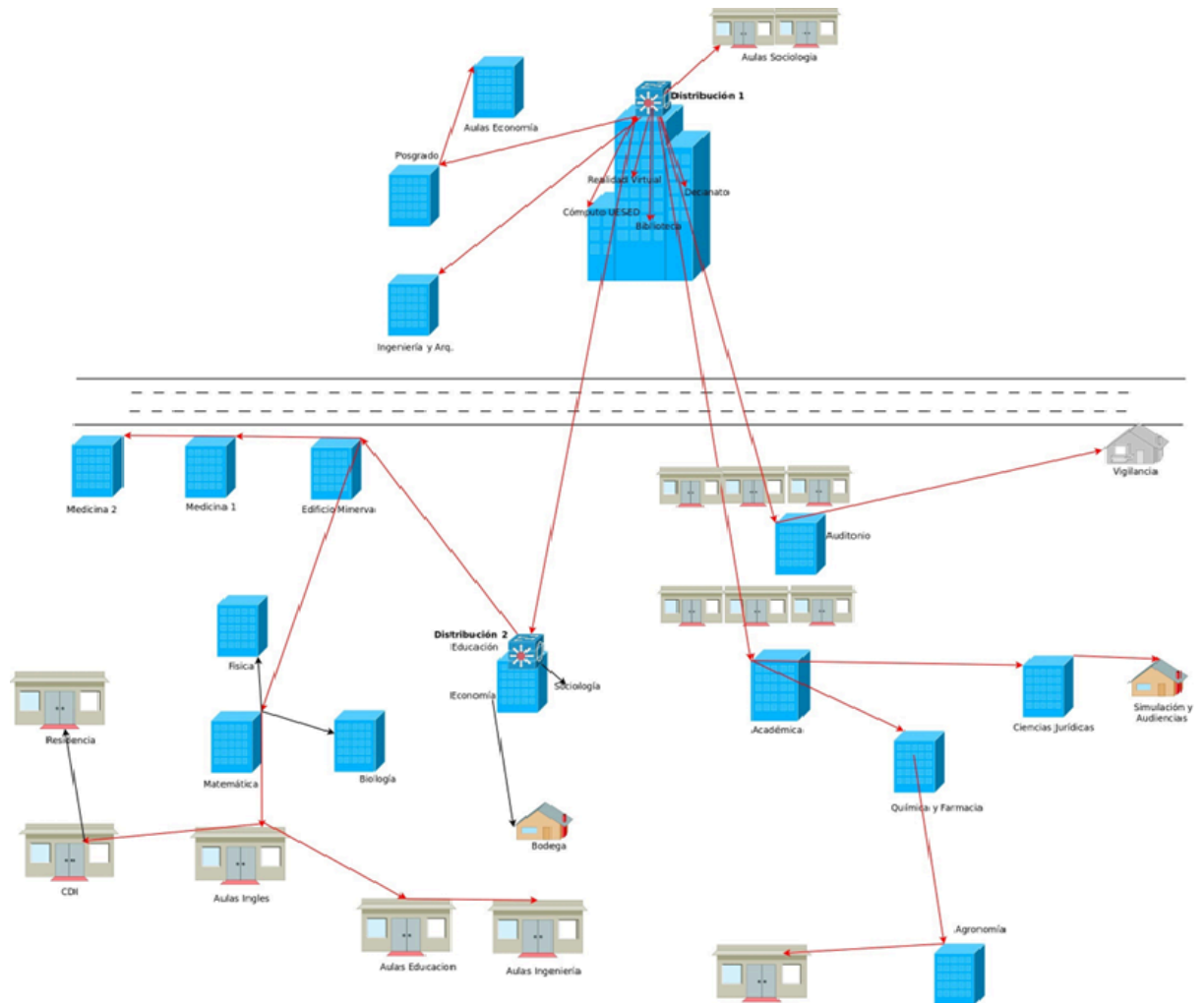


ilustración 1. distribución actual

En la topología anterior se muestran los diferentes departamentos y edificios a los cuales se distribuye la red en el cual podemos destacar los siguientes aspectos

La red se encuentra conectada a dos nodos o dos puntos principales de distribución en el diagrama están definidas como Distribución 1 y Distribución 2

**Distribución 1:** Nodo central, conectado a Realidad Virtual, Biblioteca, Cómputo UESED, Decanato, Posgrado, Aulas de Economía, Sociología, Vigilancia, Auditorio, Académica, Ciencias Jurídicas, Química y Farmacia, Agronomía, Simulación y Audiencias, Aulas Agronomía .

**Distribución 2 (Educación):** Nodo secundario que concentra Medicina, Edificio Minerva, Física, Matemática, Biología, Aulas de Educación, Inglés, Ingeniería, Residencia, CDI, Bodega, Psicología, etc.

**En el diagrama anterior podemos observar algunas características.**

- La red está organizada en **dos grandes centros de distribución** que se interconectan con diferentes edificios.
- Cada edificio representa un segmento de red, con enlaces de fibra óptica o cables UTP en pequeños tramos.
- Se nota un **modelo jerárquico** en estrella extendida, donde los switches de distribución se centralizan y luego se extienden a cada facultad o dependencia.
- Se incluyen áreas críticas como **Vigilancia y Residencia**, lo cual muestra que la red soporta no solo actividades académicas sino también administrativas y de seguridad.

#### **Análisis De La Topología de Red Utilizada**

- En el **centro principal** está el nodo **Distribución 1**, que funciona como **core** de la red.
- Un segundo nodo (**Distribución 2 – Educación**) actúa como un **switch de distribución secundario**, enlazado a diferentes facultades y edificios.
- Desde cada distribución salen conexiones hacia los diferentes edificios (facultades, aulas, residencias, auditorios, etc.), lo que forma **estrellas locales**.

#### **Fortalezas del diseño**

- **Aislamiento de fallas:** una caída en acceso suele afectar solo a ese edificio.
- **Simplicidad operativa:** Los enlaces de las redes son claros, Distribución -> Edificio, de esta manera es más fácil de documentar fácil de documentar y monitorear.
- **Potencial de redundancia:** los enlaces laterales pueden servir para *backup* si se diseñan con protocolos correctos

### **Problemáticas Detectadas**

#### **Dependencia en gran medida del punto de distribución 1:**

La mayor parte de los edificios y departamentos se conectan a un solo punto de distribución, lo que genera riesgo de saturación y caída total de servicios si este falla.

#### **Ausencia de una capa Core definida:**

El diseño actual mezcla funciones de distribución y Core en los mismos equipos, lo que reduce la capacidad de procesamiento y la tolerancia a fallos.

#### **Topología poco escalable:**

La red actual tiene enlaces directos desordenados y difícil expansión sin afectar la estabilidad.

#### **Enlaces directos no optimizados:**

Existen múltiples conexiones directas entre edificios sin pasar por una capa de distribución adecuada, lo que genera cuellos de botella y dificulta el control del tráfico.

#### **Falta de resiliencia en caso de fallos:**

Si un enlace principal o un switch de distribución falla, varios edificios pierden conexión total.

#### **Gestión compleja de la red:**

La mezcla de funciones y enlaces irregulares dificulta la administración, la segmentación de VLANs y la aplicación de políticas de seguridad.

#### **Inventario de equipos de red en el data center**

El inventario del Data Center consiste en un registro técnico detallado con la información que se necesita, para tener registrada los dispositivos que conforman la infraestructura de red y seguridad de la facultad. Este inventario incluye Switches de acceso y distribución, routers, firewall, controladoras inalámbricas, dispositivos de protección AntiDDoS y equipos de sistemas y servidores. Cada dispositivo se encuentra identificado con su ubicación, dirección IP, marca, modelo y número de serie (NS), lo que permite un control detallado y una gestión eficiente de todos los recursos. Este documento garantiza la trazabilidad de los equipos, facilita las tareas de mantenimiento preventivo y correctivo y sirve como base para futuras aplicaciones o actualizaciones de la infraestructura.

Tabla 1. Inventario de equipos de red en el data center

N°	Equipo	Ubicación	Marca	Dirección IP	Modelo	SN	Rol en la red
1	NCE	Data Center	Huawei	172.17.24.X:18008	AirEngine9700-M1_6F0DD791	1021C6034988	Controlador al centro WLAN
2	WAC	Data Center	Huawei	172.17.60.X MGMT 10.60.100.XC APWAP	Wireless LAN AirEngiene9700-M1	1021C6034988	Controlador WLAN secundaria
3	FIREWALL01_ETH H_PORT	Data Center	Huawei	172.17.60.X84 43	MGDEdgeFW USG6610E-0	1021C0011920	Firewall perimetral principal
4	FIREWALL 02_ETH_PORT	Data Center	Huawei	172.17.60.X	MGDEdgeFW USG6610E-0	1021C0011919	Firewall redundante
5	ROUTER01_ETH _PORT	Data Center	Huawei	172.17.60.X/lo op: 172.17.62.X	SMGEdgeNE8K M1A	210253HF W10MC100 068	Router WAN
6	ROUTER02_ETH _PORT	Data Center	Huawei	172.17.60.X/lo op: 172.17.62.X	SMGEdgeNE8K M1A	2102353HF W10MC100 070	Router WAN redundante
7	ANTIDDOS 01	Data Center	Huawei	172.17.60.X	1905_CLEANIN G	1021C0011654	Protección DDos
8	ANTIDDOS 02	Data Center	Huawei	172.17.60.X	1906_CLEANIN G	1021C00116551	Protección DDos redundante
9	SW_ACCESS_DC	Data Center	Huawei	172.19.29.X	S5736-S24U,4X C	3G21C0046597	Switch acceso DC
10	Controladora 1	Data Center	Cisco	172.16.0.X	CONTROLADO RA		Controladora inalámbrica
11	Controladora 2	Data Center	Cisco	172.16.16.X	C9800- L-F-K9	FCL240200 U2	Controladora WLAN
12	Data Center	Data Center	Cisco	172.16.0.X			Switch/Data Center
13	Core Distribución 1	Data Center	Huawei	192.168.10.X	S630-H48X6C	10201002304	Core principal
14	Sistemas Servidores	Data Center	Cisco	192.168.10.X	CATALYST 3850		Switch servidores
15	Sistemas	Data Center	Huawei	192.168.10.X	S5735-L48T4X- A	2198010936 4ELC00842 2	Switch acceso

### Presupuesto Actual de los equipos

En la siguiente tabla se detalla la información del presupuesto inicial de los equipos de red adquiridos en el año 2022, incluyendo soluciones de seguridad (AntiDDoS y Firewall), conectividad inalámbrica (puntos de accesos indoor y outdoor, controlador inalámbrico), equipos de enrutamiento (NetEngine 8000) y conmutador (CloudEngine S5736).

Cada registro muestra el modelo, número de serie, fecha de adquisición y el precio unitario en dólares estadounidenses. Este desglose permite identificar de forma precisa los activos de infraestructura tecnológica, facilitando tanto la gestión de inventario como el análisis financiero del proyecto.

Tabla 2. Presupuesto actual de los equipos de red

Descripción	Marca	Modelo	Serie	Fecha	Precio (USD)
ANTIDDOS	HUAWEI	ANTIDDOS 1905_CLEANING	1021C0011651	25/07/2022	\$36,504.97
ANTIDDOS	HUAWEI	ANTIDDOS 1905_CLEANING	1021C 0011654	25/07/2022	\$36,504.97
AP INDOOR	HUAWEI	AIRENGINE 5761-21	2102353VUT6R MC001202	25/07/2022	\$1,443.35
AP OUTDOOR	HUAWEI	AIRENGINE 6760R-51E	210235 3KCM6RMC00 0681	25/07/2022	\$2,717.17
AP OUTDOOR	HUAWEI	AIRENGINE 6760R-51E	2102353KCM6 RMC000786	25/07/2022	\$2,717.17
FIREWALL	HUAWEI	USG6610E	1021C0011919	25/07/2022	\$26,710.90
FIREWALL	HUAWEI	USG6610E	1021C0011920	25/07/2022	\$26,710.90
ROUTERS	HUAWEI	NETENGINE 8000 M1A	2102353HFW10 MC100068	25/07/2022	\$9,287.79
ROUTERS	HUAWEI	NETENGINE 8000 M1A	2102353HFW10 MC100070	25/07/2022	\$9,287.79
SWITCH ACCESO	HUAWEI	CLOUD ENGINE S5736 - S24UM4XC	3G21C0046822	25/07/2022	\$5,092.76
WIRELESS CONTROLLER	HUAWEI	AIRENGINE9700- M1	1021C6034988	25/07/2022	\$19,558.53
TOTAL EQUIPOS					\$176,536.30

FLETE Y SEGURO (7%)	\$12,357.54
IMPUESTOS (23%)	\$43,424.13
TOTAL GENERAL ESTIMADO	\$232,317.97

Además del costo de adquisición de los equipos, se debe considerar un gasto anual aproximadamente del 20% del valor total de la infraestructura en concepto de mantenimiento, soporte técnico y licencias. Esto garantiza la continuidad operativa, la actualización del software y la atención de fallas críticas.

### 6.1. Segmentación lógica de red

La red en la Universidad de El Salvador, Facultad Multidisciplinaria Oriental, está organizada por medio de VLANs que permite la separación de tráfico por áreas académicas, administrativas y de servicio. Esta segmentación facilita el aislamiento de procesos críticos, como los servidores, la telefonía IP, y la video vigilancia, reduciendo riesgos de saturación y vulnerabilidad.

Tabla 3. Segmentación lógica de la red

N°	Área/Servicio	VLAN ID	Dirección IP/Máscara	Observaciones
1	WIFI	1101	172.16.0.1/20	Red inalámbrica principal
2	ADMINISTRATIVOS	1102	192.168.30.1/24	Acceso oficinas administrativas
3	UESED	1103	192.168.8.1/24	Unidad UESED
4	CÓMPUTO	1104	192.168.60.1/24	Laboratorios de cómputo
5	AGRONOMÍA	1105	192.168.9.1/24	Facultad de Agronomía
6	ADMINISTRACIÓN	1106	192.168.10.1/24	Facultad de Administración
7	SERVIDORES	1107	192.168.7.1/24	Segmento crítico de servicio
8	BIBLIOTECA	1108	192.168.11.1/24	Biblioteca Central7
9	ACADÉMICA	1109	192.168.12.1/24	Área académica
10	POSTGRADO	1110	192.168.13.1/24	Estudios de Postgrado

11	SALA-INTERNET	1111	192.168.14.1/24	Sala de internet
12	ECONOMÍA	1112	192.168.15.1/24	Facultad de Economía
13	CCNN	1113	192.168.16.1/24	Ciencias Naturales
14	MEDICINA	1114	192.168.17.1/24	Facultad de Medicina
15	CCJJ	1115	192.168.18.1/24	Ciencias Jurídicas
16	QUÍMICA	1116	192.168.19.1/24	Facultad de Química
17	HUMANIDADES	1117	192.168.20.1/24	Facultad de Humanidades
18	INGENIERÍA	1118	192.168.21.1/24	Facultad de Ingeniería y Arquitectura
19	CÁMARAS	1119	192.168.22.1/24	Videovigilancia
20	TELEFONÍA IP	1120	192.168.23.1/24	Telefonía VoIP
21	AUDIOVISUALES	1121	192.168.24.1/24	Servicios Audiovisuales
22	WIFI2	1122	172.16.1.1/20	Red Wifi secundaria
23	WIFI 6	1123	IP PLAN	Red inalámbrica WIFI 6

## 6.2. Equipamiento de red

La infraestructura de red combina equipos de distintas marcas y modelos, instalados en el Data Center y en cada una de las áreas de la Universidad. El núcleo de la red está conformado principalmente por Switch Huawei de la serie S6730 y S5730, siendo el S6730 el corazón de la red, ya que este maneja la virtualización y maneja el tráfico más pesado. El S5730 conecta a usuarios y equipos finales, con soporte PoE y gestión flexible. Además de utilizar los routers NE8KM1A y firewalls USG6610E. A nivel de acceso se encuentran equipos de marca diversas como Cisco, Dahua, TP-Link y D-Link.

Tabla 4. Equipamiento de red

N°	Equipo	Ubicación	Marca	Dirección IP	Modelo	SN	Rol en la red
----	--------	-----------	-------	--------------	--------	----	---------------

1	NCE	Data Center	Huawei	172.17.24.X:18008	AirEngine9700-M1_6F0DD791	1021C6034988	Controlador al centro WLAN
2	WAC	Data Center	Huawei	172.17.60.X MGMT 10.60.100.XC APWAP	Wireless LAN AirEngiene9700-M1	1021C6034988	Controlador WLAN secundaria
3	FIREWALL01_ETH_PORT	Data Center	Huawei	172.17.60.X8443	MGDEdgeFW USG6610E-0	1021C0011920	Firewall perimetral principal
4	FIREWALL02_ETH_PORT	Data Center	Huawei	172.17.60.X	MG DEdgeFW USG6610E-0	1021C0011919	Firewall redundante
5	ROUTER01_ETH_PORT	Data Center	Huawei	172.17.60.X/loop: 172.17.62.X	SMGEdgeNE8KM1A	210253HFW10MC100068	Router WAN
6	ROUTER02_ETH_PORT	Data Center	Huawei	172.17.60.X/loop: 172.17.62.X	SM GEdgeNE8KM1A	2102353HFW10MC100070	Router WAN redundante
7	ANTIDDOS 01	Data Center	Huawei	172.17.60.X	1905_CLEANING	1021C0011654	Protección DDos
8	ANTIDDOS 02	Data Center	Huawei	172.17.60.X	1906_CLEANING	1021C00116551	Protección DDos redundante
9	SW_ACCESS_DC	Data Center	Huawei	172.19.29.X	S5736-S24U, 4XC	3G21C0046597	Switch acceso DC
10	Controladora 1	Data Center	Cisco	172.16.0.X	CONTROLADORA		Controladora inalámbrica
11	Controladora 2	Data Center	Cisco	172.16.16.X	C9800-L-F-K9	FCL240200U2	Controladora WLAN
12	Data Center	Data Center	Cisco	172.16.0.X			Switch/Data Center
13	Core Distribución 1	Data Center	Huawei	192.168.10.X	S630-H48X6C	102010022304	Core principal
14	Core Distribución 2	Educación	Huawei	192.168.10.X	S1720-52GWR-4X	21980106112SK5600071	Core secundaria
15	Sistemas Servidores	Data Center	Cisco	192.168.10.X	CATALYST 3850		Switch servidores
16	Sistemas	Data Center	Huawei	192.168.10.X	S5735-L48T4X-A	21980109364ELC008422	Switch acceso

17	Decanato	Decanato	Huawei	192.168.10.X	S5735-L48T4 X-A	21980109364E LC008270	Switch acceso computo
18	Cómputo USED	Cómputo UESED	Huawei	192.168.10.X	S1720-52GW R-4X	21980106112S K5600056	Switch acceso
19	Servicios Al Público	Servicios al público	Dahua	192.168.10.X	DH-S5600-4 8GT4XF	219801A2A59 242Q0004C	Switch acceso
20	Educación	Educación	Huawei	192.168.10.X	S1720-52GW R-4X	21980106112S K5600010	Switch acceso
21	Académica	Académica	Huawei	192.168.10.X	S1720-52GW R-X	21980106112S K5600081	Switch acceso
22	Aulas Economía	Aulas Economía	Cisco	192.168.10.X	SF200-24		Switch acceso
23	Economía	Economía	Huawei	192.168.10.X	S6730-H48X 6C		Switch acceso
24	Matemática	Matemática	Huawei	192.168.10.X	S6730-H48X 6C	21980106112S K5600072	Switch acceso
25	Agronomía	Agronomía	Huawei	192.168.10.X	S6730-H48X 6C	21980106112S K5600042	Switch acceso
26	Biología	Biología	Cisco	192.168.10.X	WS-C2960X- 48TS-L		Switch acceso
2	Postgrado	Postgrado	Huawei	192.168.10.X	S5735-L48T4 X-A	21980109364E LC008861	Switch acceso
28	Medicina	Medicina	Huawei	192.168.10.X	S1720-52GW R-4X	21980106112S K5600042	Switch acceso
29	Bodega	Bodega	Cisco	192.168.10.X	SG350-10		Switch acceso
30	CDI	CDI	Cisco	192.168.10.X	SF200-24	DNI204002CC	Switch acceso
31	Ciencias Jurídicas	Ciencias Jurídicas	Huawei	192.168.10.X	S1720-52GW R-4X	21980106112S K5600072	Switch acceso
32	Residencia 2	Residencia 2	Cisco	192.168.10.X	SF200-24	DNI2040026P	Switch acceso
33	Financiera	Financiera	Dahua	192.168.10.X		219801A2A59 242Q0000D	Switch acceso
34	Química	Química	Huawei	192.168.10.X	S1720-52GW R-4X	21980106112S K5600025	Switch acceso
35	Computo Redes 1	Computo redes 1	Cisco	192.168.10.X	SF200-24	DNI22110F39	Switch acceso

36	Ingeniería	Ingeniería y Arquitectura	Huawei	192.168.10.X	S17 20-52GWR-4 X	21980 106112SK560 0004	Switch acceso
37	Cómputo Redes 2	Computo redes 2	Cisco	192.168.10.X	SF200-24	DNI22110F5E	Switch acceso
38	Cómputo Redes 3	Computo redes 3	Cisco	192.168.10.X	SF200-24	PSZ21471ML U	Switch acceso
39	Residencia	Residencia	Dlink	192.168.10.X	SG350-10	PSZ21471MM 0	Switch acceso
40	UESED	Oficina UESED	Cisco	192.168.10.X	DE-1210	F3XZ4FC0013 81	Switch acceso
41	Financiera 2	Financiera 2	Cisco	192.168.10.X	SF200-24	DNI223405H G	Switch acceso
42	Edificio Minerva	Edificio de Minerva	Huawei	192.168.10.X	S1720-52GW R-4X	21980106112S K5600074	Switch acceso
43	Sala De Internet	Sala de internet	Cisco	192.168.10.X	SF200-24	DNI204302B G	Switch acceso
44	Vigilancia Estacionamiento	Vigilancia estacionamiento	Cisco	192.168.10.X	SF200-24	DNI223405H N	Switch acceso
45	Aulas Ingles	Aulas Ingles	Huawei	192.168.10.X	S5735-L24T AX-A	2S2180007582	Switch acceso
46	Aulas Educación	Aulas Educación	Huawei	192.168.10.X	S57 35-L24TAX- A	2S2180007714	Switch acceso
47	Aulas De Ingeniería	Aulas Ingeniería	Huawei	192.168.10.X	S57 35-L24TAX- A	2S2180007811	Switch acceso
48	Aulas De Agronomía	Aulas Agronomía	Huawei	192.168.10.X	S57 35-L24TAX- A1	2S2180007728	Switch acceso
49	Simulación Y Audiencias	Simulación y audiencias	Huawei	192.168.10.X	S57 35-L48T4X- A	21980109364E LC00886	Switch acceso
50	Sociología	Sociología	Tp-Link	192.168.10.X	TL-SG3452P	Y2270220004 12	Switch acceso
51	Edificio Minerva Pantallas 1	Edificio Minerva	Huawei	192.168.10.X	S5731-S24P4 X		Switch acceso

52	Edificio Minerva Pantallas 2	Edificio Minerva	Huawei	192.168.10.X	S57 31-S24P4X		Switch acceso
53	Ciencias Jurídicas Pantallas	Aulas Ciencias Jurídicas	Huawei	192.168.10.X	S57 31-S24P4X	DM22B00206 28	Switch acceso
54	Aula Sociología Pantallas	Aulas Sociología	Huawei	192.168.10.X	S57 31-S24P4X	102285825322	Switch acceso
55	Vigilancia Entrada	Caseta vigilancia entrada	Tp-Link	192.168.10.X	TL-SG3452P	Y2270A50000 27	Switch Cámaras

### 6.3. Infraestructura Inalámbrica

La facultad cuenta con una red inalámbrica moderna basada en tecnología WiFi 6, desplegada en aulas, bibliotecas, laboratorios y áreas comunes. Los puntos de acceso (APs) se gestionan mediante controladoras CAPWAP, con soporte de autenticación y portal cautivo. La cobertura abarca espacios interiores y exteriores, garantizando conectividad en la mayoría de edificios.

La red inalámbrica está basada en WiFi 6 (Huawei AirEngine), el control y aprovisionamiento de los APs se hace mediante CAPWAP, que permite gestionar los puntos de acceso de forma centralizada desde la controladora inalámbrica. Su mayor ventaja es que se han instalado múltiples APs en aulas y auditorios para soportar un gran número de conexiones simultáneas, garantizando así la cobertura tanto en interiores como en exteriores, asegurando conectividad en aulas jardines y entradas principales, cuenta con puertos libres para poder darle crecimiento a la red si así lo requiere.

Tabla 5. Infraestructura inalámbrica organizada por zonas

N.º	NAME	MANAGE IP ADDRESS	MARCA	MODELO	ESN
1	Aulas de Ingeniería	172.19.29.X	HUAWEI	S5736-S24UM4XC	3G21C0046776
2	Auditorium 1 Patch panel 1	172.19.29.X	HUAWEI	S5736-S24UM4XC	3G21C0046580
3	Bodega Medicina 2	172.19.29.X	HUAWEI	S5736-S24UM4XC	3G21C0046506
4	Jefatura de Medicina 1	172.19.29.X	HUAWEI	S5736-S24UM4XC	3G21C0046822
5	Bodega Medicina 1	172.19.29.X	HUAWEI	S5736-S24UM4XC	3G21C0046499
6	Biología	172.19.29.X	HUAWEI	S5736-S24UM4XC	3G21C0046639
7	Aula 30 de Economía	172.19.29.X	HUAWEI	S5736-S24UM4XC	3G21C0046782
8	Jefatura de Medicina 2	172.19.29.X	HUAWEI	S5736-S24UM4XC	3G21C0046849

9	Sala de Estudios Biblioteca	172.19.29.X	HUAWEI	S5736-S24UM4XC	3G21C0046630
10	Minerva	172.19.29.X	HUAWEI	S5736-S24UM4XC	3G21C0046543
11	Física	172.19.29.X	HUAWEI	S5736-S24UM4XC	3G21C0046622
12	Ciencias jurídicas	172.19.29.X	HUAWEI	S5736-S24UM4XC	3G21C0046603
13	Edificio Riñón 02	172.19.29.X	HUAWEI	S5736-S24UM4XC	3G21C0046537
14	Edificio Riñón 01	172.19.29.X	HUAWEI	S5736-S24UM4XC	3G21C0046507
15	Aulas de Inglés	172.19.29.X	HUAWEI	S5736-S24UM4XC	3G21C0046594
16	Lab. De química	172.19.29.X	HUAWEI	S5736-S24UM4XC	3G21C0046851
17	Auditórium 1 Patch panel 2	172.19.29.X	HUAWEI	S5736-S24UM4XC	3G21C0046633
18	Aulas Agronomía	172.19.29.X	HUAWEI	S5736-S24UM4XC	3G21C0046598
19	Aulas de Educación	172.19.29.X	HUAWEI	S5736-S24UM4XC	3G21C0046620
20	Unidad Financiera	172.19.29.X	HUAWEI	S5736-S24UM4XC	3G21C0046511
21	Posgrado	172.19.29.X	HUAWEI	S5736-S24UM4XC	3G21C0046860
22	SW_ACCESS_DC	172.19.29.X	HUAWEI	S5736-S24UM4XC	3G21C0046597
23	Centro de Computo Lab. De Red	172.19.29.X	HUAWEI	S5736-S24UM4XC	3G21C0046595
24	Vice Decanato	172.19.29.X	HUAWEI	S5736-S24UM4XC	3G21C0046616
25	Oficinas de administración acad	172.19.29.X	HUAWEI	S5736-S24UM4XC	3G21C0046793

## 7. Propuesta de Mejora y Diseño de Red

La propuesta de mejora de red busca modernizar pero sin excluir tecnología actual que aún puede ser de utilidad para la Universidad mediante la incorporación de dos equipos Core que brindan redundancia y mayor capacidad de procesamiento, garantizando la continuidad del servicio en caso de fallos. Asimismo, se establece una nueva estructura de tres puntos de distribución, lo que permite una mejor organización del tráfico, balanceo de carga y escalabilidad de la red. Con estos cambios, se optimizan los enlaces de interconexión entre edificios y departamentos, reduciendo la dependencia de un único nodo central y aumentando la resiliencia general de la topología. Esta reorganización no sólo mejora la eficiencia en la transmisión de datos, sino que también sienta las bases para soportar futuras expansiones y aplicaciones críticas dentro de la institución.

### 7.1. Diseño Propuesto de Red.

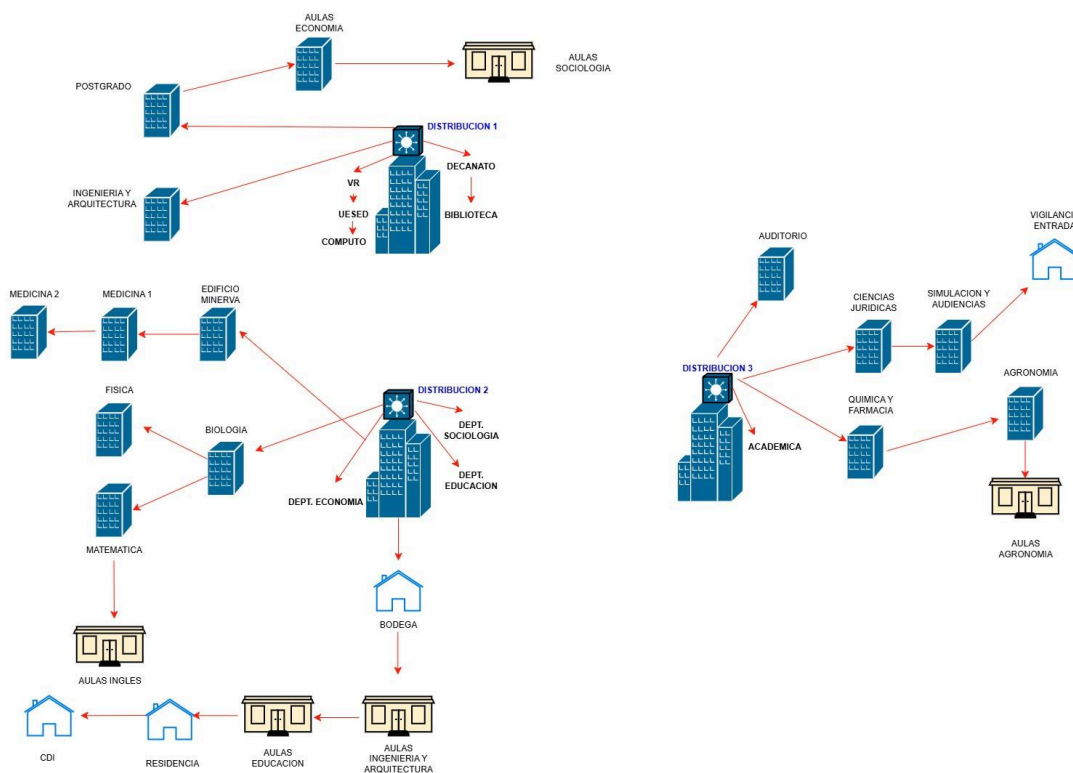


Ilustración 2. distribución propuesta

Este diagrama expone la propuesta de red mejorada para la Universidad, en la cual se establece una topología jerárquica con la incorporación de un Core conformado por dos equipos de alto rendimiento, cuya función principal es centralizar y gestionar el enrutamiento y la interconexión de toda la infraestructura, garantizando redundancia y alta disponibilidad de los servicios. A partir de este Core se despliegan tres nodos de distribución, diseñados para segmentar de manera eficiente el tráfico y descentralizar la carga de los switches de acceso, lo que incrementa la

escalabilidad y la capacidad de administración de la red. Asimismo, los enlaces troncales entre Core, distribución y acceso han sido reorganizados con el fin de optimizar la latencia, mejorar la resiliencia y asegurar una transmisión de datos más estable y continua entre las distintas facultades, departamentos y áreas administrativas. Esta arquitectura propone una solución robusta, preparada para soportar el crecimiento institucional y la integración de servicios críticos a futuro.

El diseño propuesto se organiza bajo una **arquitectura jerárquica de tres capas**:

#### 1. **Capa Core (Núcleo)**

- Switches de alta capacidad (Huawei S6730) ubicados en el Data Center.
- Enlaces redundantes hacia los switches de distribución.

#### 2. **Capa de Distribución**

- Switches de nivel intermedio en cada edificio (Huawei S5735/S5736 o Cisco Catalyst 9300), gestionados de forma centralizada.
- Implementación de enlaces troncales de 10 Gbps al core.

#### 3. **Capa de Acceso**

- Switches de menor capacidad en laboratorios, oficinas y aulas (Huawei S1720, Cisco 2960/9200 o equivalentes).
- Integración con puntos de acceso WiFi 6, garantizando acceso seguro tanto a estudiantes como a personal administrativo.

#### 4. **Red Inalámbrica**

- Controladoras WLAN redundantes (Huawei AirEngine o Cisco C9800).

- Despliegue uniforme de APs WiFi 6 con gestión centralizada y autenticación por portal cautivo o 802.1X.

## 5. Seguridad y Monitoreo

- Firewalls redundantes de nueva generación (NGFW).
- Integración de soluciones AntiDDoS existentes.
- Sistema de monitoreo proactivo con alarmas de fallos y análisis de tráfico.

### Diagrama de enlaces Troncales.

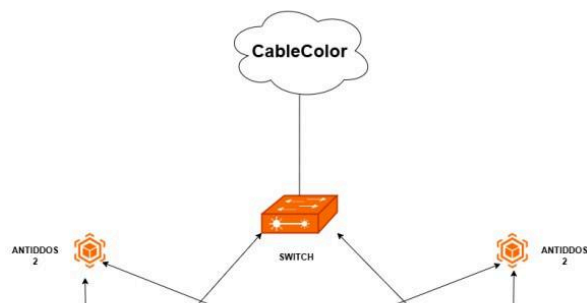




Ilustración 3. diagrama de enlaces

La arquitectura de red se diseñó siguiendo un enfoque jerárquico, priorizando la redundancia y la seguridad en cada una de sus capas. A continuación, se describen los principales componentes:

1. Conexión al Proveedor de Servicios de Internet (ISP):  
La red recibe conectividad desde el proveedor CableColor, el cual entrega el enlace principal a un switch de borde.
  
2. Capa de Protección Perimetral (Antiddos):  
Desde el switch de borde se interconectan dos equipos Antiddos que tienen como función mitigar ataques distribuidos de denegación de servicio (DDoS). La existencia de dos dispositivos asegura tolerancia a fallos y continuidad del servicio.
  
3. Capa Core:  
El núcleo de la red está conformado por dos equipos Core que operan en redundancia, garantizando alta disponibilidad y balanceo de carga. Estos equipos son responsables de la conmutación y el enrutamiento de

alto rendimiento dentro de la red.

4. Capa de Seguridad (Firewalls):

Posterior al Core, el tráfico atraviesa dos Firewalls implementados en paralelo. Estos dispositivos permiten aplicar políticas de seguridad, segmentación de tráfico y filtrado de accesos, protegiendo así la infraestructura interna.

5. Capa de Distribución:

La capa de distribución está compuesta por tres switches de distribución, los cuales reciben la conectividad desde los firewalls.

- Distribución 1 y Distribución 3 proporcionan acceso a diferentes zonas de usuarios finales.
- Distribución 2 cumple un rol central, ya que mantiene enlaces hacia los otros dos equipos de distribución, fortaleciendo la redundancia y la resiliencia de la red.

6. Control de Acceso Inalámbrico:

Desde el switch de Distribución 1 se conecta un Wireless Access Controller (WAC), encargado de la administración centralizada de los puntos de acceso inalámbricos. Esto permite una gestión eficiente de la conectividad WiFi y de los usuarios móviles dentro de la red.

### **Beneficios de la Propuesta**

**Redundancia y alta disponibilidad:** la incorporación de dos equipos Core asegura continuidad de los servicios incluso si uno de ellos falla.

**Mayor escalabilidad:** con tres nodos de distribución, la red puede crecer de forma ordenada al integrar nuevas facultades, departamentos o laboratorios sin sobrecargar los enlaces existentes.

**Mejor segmentación del tráfico:** la división en tres distribuciones permite organizar y balancear la carga de usuarios, evitando cuellos de botella en un solo punto.

**Optimización de la latencia:** los nuevos enlaces troncales reducen los saltos de red innecesarios, lo que mejora los tiempos de respuesta y la velocidad de acceso a los recursos.

**Mayor resiliencia de la infraestructura:** al existir múltiples rutas y distribución de carga, se disminuye el riesgo de interrupción total ante fallos en un enlace o dispositivo.

**Mejor administración y control:** al estar la red estructurada en Core, distribución y acceso, se facilita la gestión, la aplicación de políticas de seguridad y la resolución de incidencias.

**Preparación para servicios críticos:** la topología propuesta ofrece la robustez necesaria para soportar aplicaciones que demandan alta disponibilidad como telefonía IP, videoconferencias, sistemas académicos y plataformas virtuales.

**Base para futuras mejoras:** la nueva arquitectura permite integrar tecnologías modernas (VLANs más complejas, QoS, balanceo de carga, monitoreo avanzado) sin necesidad de rediseñar completamente la red.

## **8. Justificación Técnica y Económica.**

### 8.1. Justificación Técnica

La red actual de la Facultad Multidisciplinaria Oriental constituye la base de los procesos académicos y administrativos de la institución. No obstante, presenta limitaciones de rendimiento, seguridad y administración, las cuales afectan la continuidad de los servicios digitales, las clases virtuales, la conectividad inalámbrica y la gestión de datos administrativos.

La optimización de la red se justifica técnicamente en los siguientes aspectos:

#### 1. Aprovechamiento de infraestructura existente

En lugar de reemplazar de manera completa la red, se busca optimizar lo instalado. Muchos de los equipos actuales, como switches de acceso, cableado estructurado y racks, pueden ser reutilizados mediante actualizaciones de firmware, reconfiguraciones o migraciones progresivas. Esta estrategia asegura que la institución maximice la inversión ya realizada y al mismo tiempo incorpore mejoras necesarias.

#### 2. Segmentación lógica mediante VLANs

Actualmente, la red carece de una segmentación adecuada que permita diferenciar el tráfico académico, administrativo y de invitados. Esta situación genera congestión y problemas de seguridad. La implementación de VLANs optimizará el flujo de datos, reducirá el broadcast innecesario y permitirá aplicar políticas de calidad de servicio (QoS). Esto mejora el rendimiento de los servicios críticos como videoconferencias, plataformas de gestión académica y sistemas de matrícula en línea.

#### 3. Fortalecimiento de la seguridad

La seguridad de la red es una prioridad institucional. En la situación actual, el uso de contraseñas simples, la ausencia de firewalls de nueva generación y la carencia de un sistema de detección de intrusos representan riesgos significativos. La optimización incluye:

Actualización de políticas de contraseñas y autenticación centralizada (802.1X).

Implementación de firewalls con funciones de filtrado avanzado y control de tráfico.

IDS/IPS para detectar y mitigar amenazas en tiempo real.

Estas medidas elevan el nivel de seguridad sin necesidad de reemplazar toda la infraestructura.

#### 4. Optimización de la red inalámbrica

La red WiFi actual presenta problemas de cobertura desigual y saturación de canales. La optimización contempla la reubicación estratégica de los puntos de acceso existentes, la incorporación de algunos equipos bajo estándar WiFi6 y la configuración de redes de invitados aisladas. Esto permite ampliar la cobertura y asegurar un servicio más estable a estudiantes y personal docente.

#### 5. Administración centralizada

Actualmente, la gestión de la red es manual y dispersa. Se justifica la implementación de una plataforma de monitoreo y administración centralizada (NMS) que permita supervisar el estado de los equipos, generar alertas preventivas y automatizar tareas. Esto reducirá tiempos de respuesta, facilitará la detección de fallos y disminuirá la carga de trabajo del personal técnico.

En resumen, la optimización técnica se centra en reutilizar lo que funciona, actualizar lo obsoleto y reconfigurar lo mal implementado, garantizando una red más eficiente, segura y escalable, sin incurrir en gastos excesivos.

### 8.2. Justificación Económica

El aspecto económico constituye un factor decisivo para optar por la optimización en lugar de una sustitución completa de la infraestructura.

#### 1. Maximización de recursos existentes

Reemplazar toda la red implicaría una inversión de entre \$120,000 y \$160,000. Sin embargo, la estrategia de optimización reduce el gasto a un rango estimado de \$40,000 a \$60,000, ya que se reutilizan switches, racks, cableado y puntos de acceso que aún conservan vida útil. Esto representa un ahorro de hasta un 65% respecto a una renovación completa.

#### 2. Costos de implementación escalonada

La optimización puede implementarse por fases, lo cual permite distribuir la inversión en el tiempo. Se priorizan las áreas críticas (seguridad, administración y cobertura inalámbrica), dejando para etapas posteriores las expansiones menores. De esta manera, la Facultad puede planificar su presupuesto anual sin necesidad de un desembolso inmediato elevado.

### 3. Reducción de gastos de mantenimiento

Una red desorganizada y sin monitoreo centralizado genera costos recurrentes en reparaciones, pérdida de horas laborales y contratación de soporte externo. Con la optimización se espera una reducción del 30% en costos de mantenimiento anual, gracias a la estandarización de equipos, la capacitación del personal y la detección temprana de fallos.

### 4. Beneficios indirectos

Productividad académica: clases virtuales sin interrupciones, acceso estable a plataformas digitales y conectividad fluida en laboratorios.

Eficiencia administrativa: sistemas de matrícula, biblioteca digital y gestión de expedientes operando con mayor rapidez.

Proyección institucional: la Facultad gana prestigio al contar con una infraestructura confiable que respalda procesos de investigación y vinculación social.

### 5. Retorno de inversión (ROI)

Si bien la optimización exige una inversión inicial, esta se recupera en un plazo estimado de 3 a 4 años, considerando los ahorros en mantenimiento, menor tiempo de inactividad y mayor rendimiento de los recursos humanos. En este sentido, el ROI es favorable y justifica plenamente la inversión.

Tabla 6 de propuesta económica

Componente	Cantidad	Modelo sugerido	Costo Unitario	Sub Total
Switch Core de alto rendimiento	2	Huawei S6730-H48X6C / Cisco Catalyst 9500	\$20,000 aprox.	\$40,000
Switch de Distribución	1	Huawei S5735-L48T4X-A / Cisco Catalyst 9300	/\$5,000 aprox.	\$5,000

Transceptores SFP+ (10G)	10	Módulos ópticos para uplinks	\$300 aprox.	\$3,000
Fibra óptica OM4 1000 m (conectorizada)	(aprox.)	Backbone entre Core y Distribución	\$2.50 / m	\$2,500
Licencias y soporte (15%)		Software, garantías, actualizaciones		\$8,000
Instalación y Configuración		Mano de obra, puesta en marcha		\$5,500
Total Estimado				\$74,000

## 9. Metodología de Trabajo

La metodología adoptada para el diseño y justificación de la propuesta de mejora de la red en la Universidad de El Salvador, Facultad Multidisciplinaria Oriental, se basó en un enfoque mixto, descriptivo y proyectivo, combinando técnicas de investigación documental, análisis de campo y diseño técnico. Su propósito fue obtener una visión integral del estado actual de la red, identificar sus limitaciones y plantear una solución técnica y económicamente viable.

### 1. Enfoque de la investigación

El proyecto se fundamenta en un enfoque descriptivo porque analiza y caracteriza la situación actual de la infraestructura tecnológica, y en un enfoque proyectivo porque plantea una propuesta de mejora a implementar en el corto y mediano plazo. Este doble enfoque permitió no solo identificar los problemas existentes, sino también formular soluciones concretas y adaptadas a las necesidades de la Facultad.

### 2. Etapas metodológicas

La metodología se estructuró en varias etapas que garantizaron un análisis riguroso y la formulación de una propuesta coherente:

#### a) Diagnóstico de la situación actual

Levantamiento de información: se recopilaron datos mediante observación directa en los laboratorios, aulas, oficinas administrativas y áreas comunes.

Inventario de infraestructura: se elaboró un listado de equipos de red, identificando marcas, modelos, antigüedad, configuraciones y estado funcional.

#### b) Diseño de la propuesta técnica

Se definió un modelo jerárquico de tres capas (Core, Distribución y Acceso) para garantizar escalabilidad, redundancia y facilidad de administración.

Se seleccionaron tecnologías y equipos de acuerdo con estándares internacionales y necesidades específicas de la Facultad.

Se planificó la segmentación de la red mediante VLANs, con políticas de acceso diferenciadas para estudiantes, docentes, administrativos y visitantes.

Se incorporaron mecanismos de seguridad avanzada: firewalls de nueva generación, IDS/IPS, autenticación 802.1X y encriptación de datos.

### 3. Técnicas e instrumentos

Durante el desarrollo de la investigación se aplicaron los siguientes instrumentos:

- Entrevistas semiestructuradas al personal técnico de TI para identificar problemas recurrentes.
- Observación directa de equipos e instalaciones.
- Herramientas de simulación de red (Cisco Packet Tracer) para validar la propuesta técnica.
- Matrices de costo-beneficio para el análisis económico.

### 4. Alcance y limitaciones

La metodología aplicada permite diseñar una solución técnicamente sólida y económicamente viable. Sin embargo, se reconoce que el estudio se centró en la infraestructura física y lógica de la red, sin profundizar en la capa de aplicaciones o servicios específicos de software. Asimismo, la estimación económica se basó en promedios de mercado, por lo que podría variar según los proveedores seleccionados.

### 5. Justificación metodológica

La combinación de métodos cualitativos (entrevistas, observación) y cuantitativos (encuestas, simulación, estimación de costos) asegura una visión integral del problema y de la solución propuesta. De esta forma, la metodología aplicada garantiza que la propuesta no solo responde a un análisis técnico, sino también a las necesidades reales de los usuarios de la Facultad.

## 10. Conclusiones y Recomendaciones

### Conclusión

La coexistencia de múltiples fabricantes de equipos, la falta de estandarización en la configuración de la red, la insuficiente cobertura inalámbrica y la ausencia de mecanismos de seguridad avanzados constituyen un escenario que dificulta la continuidad de las actividades universitarias.

La propuesta de mejora basada en un modelo jerárquico de tres capas (Core, Distribución y Acceso) representa una solución integral y sostenible. Este enfoque permitirá consolidar la red, mejorar la seguridad, garantizar redundancia y asegurar que la infraestructura tecnológica esté preparada para las demandas actuales y futuras de la comunidad universitaria. La implementación de VLANs, firewalls de próxima generación, autenticación centralizada y un sistema de monitoreo de red refuerza la confiabilidad y la capacidad de gestión de la infraestructura.

Los ahorros derivados de la reducción de fallos, menor consumo energético, centralización de la administración y mitigación de riesgos de seguridad permiten afirmar que el retorno de inversión será positivo. Asimismo, los beneficios indirectos en términos de productividad académica, eficiencia administrativa, prestigio institucional y proyección comunitaria fortalecen el valor de la propuesta.

En síntesis, la modernización de la red no sólo resolverá las deficiencias actuales, sino que proyectará a la Facultad hacia una infraestructura tecnológica moderna, segura y escalable, alineada con las exigencias de la educación superior en el siglo XXI.

## Recomendaciones

- Implementación en fases: Desarrollar la modernización en etapas (Core, Distribución, Acceso, WiFi, Seguridad), lo que permitirá una inversión progresiva y reducirá riesgos de interrupción de los servicios.
- Estandarización tecnológica: Seleccionar uno o dos fabricantes principales para garantizar compatibilidad, facilitar la administración y reducir costos de mantenimiento.
- Seguridad prioritaria: Invertir en firewalls de próxima generación, segmentación por VLAN y sistemas IDS/IPS, priorizando la protección de datos académicos y administrativos.
- Ampliación de cobertura inalámbrica: Instalar puntos de acceso WiFi6 en todos los edificios y áreas comunes, con especial atención a laboratorios, bibliotecas y auditorios.
- Gestión centralizada de red: Adoptar un NMS (Network Management System) que permite monitoreo en tiempo real, generación de alertas y administración proactiva de fallos.
- Capacitación continua: Invertir en la formación del personal técnico para garantizar un manejo eficiente de los nuevos equipos y herramientas de gestión.
- Política de sostenibilidad: Integrar prácticas de ahorro energético y gestión responsable de residuos electrónicos en la modernización de la infraestructura.
- Evaluación periódica: Establecer revisiones técnicas cada dos años para verificar el rendimiento de la red, identificar necesidades emergentes y planificar futuras ampliación

## Referencias

### ANÁLISIS, DIAGNÓSTICO, DOCUMENTACIÓN Y FORMULACIÓN DE UNA PROPUESTA DE MEJORA AL PLAN DE GESTIÓN DE LA RED DE DATOS DE LA UIS

[content](#)

[mgomezya.pdf](#)

- [1]. Formato IEEE ( <https://www.scribbr.com/ieee/ieee-paper-format/> )
- [2] A. Caffa, \*Conceptos de redes de computadoras\*. Montevideo, Uruguay: Udelar.CSEP, 2005. [En Línea]. <https://infolibros.org/pdfview/conceptos-de-redes-de-computadoras-ing-angel-caffa-377/>
- [3] J. Rivera Darín, *Fundamentos de Redes Informáticas*, 2a ed. -: IT Campus Academy, 2016.
- [4] “¿Qué son las redes informáticas?” \*IBM\*. <https://www.ibm.com/es-es/topics/networking>
- [5] “Topología de red: tipos e importancia.” \*ManageEngine OpManager\*. <https://www.manageengine.com/latam/network-monitoring/tech-topics/topologia-de-red.html>
- [6] “Estructura de redes de computadoras.” \*Universidad Isabel I (UI1) \*. <https://www.ui1.es/blog-ui1/estructura-de-redes-de-computadores>
- [7] “8 Tipos de dispositivos de red y sus características.” \*Conzultek (blog) \*. <http://blog.conzultek.com/dispositivos-de-red-caracteristicas>
- [8] “Servidor”. \*Concepto\*. <https://concepto.de/servidor>
- [9] “¿Qué es la latencia?¿Cómo reducir la latencia?”. \*Fortinet CyberGlossary\*. <https://www.fortinet.com/lat/resources/cyberglossary/latency>
- [10] A. S. Tanenbaum y D. J. Wetherall, \*Redes de Computadoras\*, 5a ed. México: Pearson, 2011
- [11] “La importancia de la escalabilidad en el diseño de redes informáticas ”. [Shern.net](https://shern.net). [En Línea] Disponible en: <https://shern.net/la-importancia-de-la-escalabilidad-en-el-diseno-de-redes-informaticas/>
- [12] “¿Qué es la seguridad informática?” Hewlett Packard Enterprise (HPE). [En Línea]. Disponible en: <https://www.hpe.com/lamerica/es/what-is/it-security.htm>
- [13] “VLAN: tipsy configuración.” [RedesZone](https://www.redeszone.net/tutoriales/redes-cable/vlan-tipos-configuracion/). [En Línea] Disponible en: <https://www.redeszone.net/tutoriales/redes-cable/vlan-tipos-configuracion/>
- [14] “¿Qué es un firewall?” [Cloudflare](https://www.cloudflare.com/es-es/learning/security/what-is-a-firewall/). [En Línea] Disponible en: <https://www.cloudflare.com/es-es/learning/security/what-is-a-firewall/>
- [15] “Ancho de banda: que es, para qué sirve y cómo se mide.” [Olin](https://olin.es/es/blog/ancho-de-banda-que-es-para-que-sirve-y-como-se-mide/). [En Línea]. Disponible en: <https://olin.es/es/blog/ancho-de-banda-que-es-para-que-sirve-y-como-se-mide/>



**Carta solicitud**

**San Miguel, 8 de agosto del 2025**

**Ingeniera Ligia Astrid Ilernández Bonilla**

Jefa de la Unidad de Sistemas Informáticos

Universidad de El Salvador FMO



Presente.

Estimada ingeniera Astrid:

Reciba un cordial saludo de parte del grupo de estudiantes del curso de Pre-Especialización denominado "Diseño Y Administración De Infraestructura De Redes Empresariales AIta Disponibilidad"

Por medio de la presente, solicitamos respetuosamente su autorización para realizar un levantamiento técnico de la infraestructura tecnológica de red de la Facultad, como parte de nuestras actividades académicas y con el objetivo de realizar nuestro proyecto final de la Pre-Especialización.

Este trabajo consistirá en recolectar información detallada sobre los equipos instalados en el data center incluyendo como mínimo los siguientes aspectos por dispositivo:

- Marca, modelo y número de serie.
- Tipo de equipos (switch, router, firewall, servidor, entre otros).
- Sistema operativo o firmware instalado.
- Interfaces físicas activas. Direcciones IP asignadas y subredes configuradas'

- Servicios brindados (por ejemplo, DHCP, DNS, NAT, etc.).
- Conectividad con otros dispositivos de red.

Asimismo, solicitamos su permiso para realizar un inventario de los equipos tecnológicos presentes en las siguientes áreas de la Facultad:

- Departamentos administrativos
- Aulas de clase.
- Laboratorios.
- Biblioteca.
- Oficina de coordinación y dirección

Este trabajo podrá complementarse con esquemas, planos o fotografías con anotaciones técnicas, que permitan representar de forma clara la ubicación y conectividad de los dispositivos.

Agradecemos de antemano su atención y quedarnos atentos a cualquier indicación adicional que estime conveniente.

Sin más por el momento, nos despedimos con el mayor de los respetos.

Atentamente,

Nombre: Yictoria Gabriela Velásquez Orellana

Carné: YV19020

Nombre: Angela Emeli Gómez López

Carné: GL16004

Nombre: Leonel Osmín Gutiérrez Ortez

Carné: GO16004

Nombre: Débora María Martínez Méndez

Carné: MMI5187

Nombre: Jose Noe Saravia Chavarria

Carné: SC13037

Nombre: José Manuel Silva Paiz

Carné: SP19002

Nombre: Elian Francisco TERNINIO PARADA


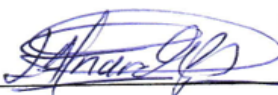
Carné: TP2ü007

Nombre: Bryan Alexander Mata Cáceres

Carné: MC19038

Estudiantes del Diplomado de Pre-especialización denominado: \*Diseño Y Administración De Infraestructura De Redes'

Ingeniería en Sistemas Informáticos  
Universidad de El Salvador - FMO



---

**Ingeniera Ligia Astrid Hernández Bonilla**

Tabla 7 de subneteo propuesta

<b>NOMBRE VLAN</b>	<b>RED</b>	<b>RANGO HOSTS</b>	<b>BROADCAST</b>
ADMINISTRACIÓN (DECANATO)	192.168.0.0/24	192.168.0.1 -- 192.168.0.254	192.168.0.255
BIBLIOTECA	192.168.1.0/24	192.168.1.1 -- 192.168.1.254	192.168.1.255
VR	192.168.2.0/24	192.168.2.1 -- 192.168.2.254	192.168.2.255
UESED	192.168.3.0/24	192.168.3.1 -- 192.168.3.254	192.168.3.255
CÓMPUTO	192.168.4.0/24	192.168.4.1 -- 192.168.4.254	192.168.4.255
ING. Y ARQU.	192.168.5.0/24	192.168.5.1 -- 192.168.5.254	192.168.5.255
POSTGRADO	192.168.6.0/24	192.168.6.1 -- 192.168.6.254	192.168.6.255
SERVIDORES	192.168.7.0/24	192.168.7.1 -- 192.168.7.254	192.168.7.255
ADMINISTRATIVOS	192.168.8.0/24	192.168.8.1 -- 192.168.8.254	192.168.8.255
SOCIOLOGÍA	192.168.9.0/24	192.168.9.1 -- 192.168.9.254	192.168.9.255
EDUCACIÓN	192.168.10.0/24	192.168.10.1 -- 192.168.10.254	192.168.10.255
ECONOMÍA	192.168.11.0/24	192.168.11.1 -- 192.168.11.254	192.168.11.255
BIOLOGÍA	192.168.12.0/24	192.168.12.1 -- 192.168.12.254	192.168.12.255

FÍSICA	192.168.13.0/24	192.168.13.1 -- 192.168.13.254	192.168.13.255
MATEMÁTICA	192.168.14.0/24	192.168.14.1 -- 192.168.14.254	192.168.14.255
BODEGA	192.168.16.0/24	192.168.16.1 -- 192.168.16.254	192.168.16.255
AUDITORIO	192.168.21.0/24	192.168.21.1 -- 192.168.21.254	192.168.21.255
CIENCIAS JURÍDICAS	192.168.22.0/24	192.168.22.1 -- 192.168.22.254	192.168.22.255
CÁMARAS	192.168.24.0/24	192.168.24.1 -- 192.168.24.254	192.168.24.255
QUÍMICA Y FARMACIA	192.168.25.0/24	192.168.25.1 -- 192.168.25.254	192.168.25.255
AGRONOMÍA	192.168.26.0/24	192.168.26.1 -- 192.168.26.254	192.168.26.255
ACADÉMICA	192.168.28.0/24	192.168.28.1 -- 192.168.28.254	192.168.28.255
MEDICINA	192.168.29.0/24	192.168.29.1 -- 192.168.29.254	192.168.29.255
TELEFONÍA IP	192.168.30.0/24	192.168.30.1 -- 192.168.30.254	192.168.30.255
AUDIOVISUALES	192.168.31.0/24	192.168.31.1 -- 192.168.31.254	192.168.31.255

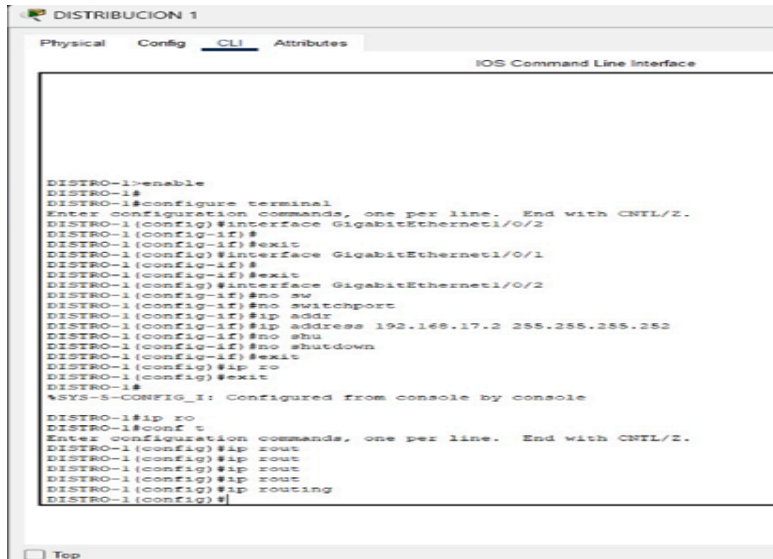
Tabla 8. tabla de vlan propuesta

<b>NOMBRE VLAN</b>	<b>VLAN-ID</b>
ADMINISTRACIÓN (DECANATO)	10
BIBLIOTECA	2
VR	3
UESED	4
CÓMPUTO	5
ING. Y ARQU.	6
POSTGRADO	7
SERVIDORES	8
ADMINISTRATIVOS	9
SOCIOLOGÍA	16
EDUCACIÓN	11
ECONOMÍA	12
BIOLOGÍA	13

FÍSICA	14
MATEMÁTICA	15
BODEGA	17
AUDITORIO	22
CIENCIAS JURÍDICAS	23
CÁMARAS	25
QUÍMICA Y FARMACIA	26
AGRONOMÍA	27
ACADÉMICA	29
MEDICINA	30
TELEFONÍA IP	31
AUDIOVISUALES	32

Configurando SVI, interfaz lógica para que se comuniquen las VLANS

DISTRIBUCION 1 -> CORE 1 -> 1/0/2 -> RED = 192.168.17.0/30  
192.168.17.2 /30 -> CORE1 por Gigabit 1/0/2



```

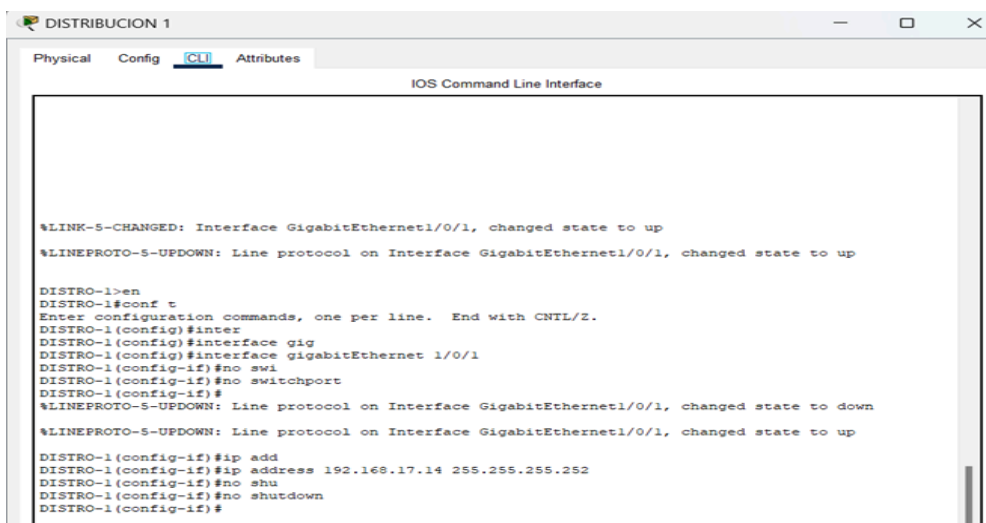
DISTRIBUCION 1
Physical Config CLI Attributes
IOS Command Line Interface

DISTRRO-1>enable
DISTRRO-1#
DISTRRO-1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
DISTRRO-1(config)#interface GigabitEthernet1/0/2
DISTRRO-1(config-if)#
DISTRRO-1(config-if)#exit
DISTRRO-1(config)#interface GigabitEthernet1/0/1
DISTRRO-1(config-if)#
DISTRRO-1(config-if)#exit
DISTRRO-1(config)#interface GigabitEthernet1/0/2
DISTRRO-1(config-if)#no sw
DISTRRO-1(config-if)#no switchport
DISTRRO-1(config-if)#ip addr
DISTRRO-1(config-if)#ip address 192.168.17.2 255.255.255.252
DISTRRO-1(config-if)#no shu
DISTRRO-1(config-if)#no shutdown
DISTRRO-1(config-if)#exit
DISTRRO-1(config)#ip ro
DISTRRO-1#
%SYS-5-CONFIG_I: Configured from console by console

DISTRRO-1#ip ro
DISTRRO-1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
DISTRRO-1(config)#ip rout
DISTRRO-1(config)#ip rout
DISTRRO-1(config)#ip rout
DISTRRO-1(config)#ip routing
DISTRRO-1(config)#
  
```

Ilustración 5.configuración de core

CORE 1 -> DISTRIBUCION 1 -> 1/0/2 -> RED = 192.168.17.0/30  
192.168.17.1 /30 -> DISTRIBUCION1 por Gigabit 1/0/2



```

DISTRIBUCION 1
Physical Config CLI Attributes
IOS Command Line Interface

%LINK-5-CHANGED: Interface GigabitEthernet1/0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/1, changed state to up

DISTRRO-1>en
DISTRRO-1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
DISTRRO-1(config)#inter
DISTRRO-1(config)#interface gig
DISTRRO-1(config)#interface gigabitEthernet 1/0/1
DISTRRO-1(config-if)#no swi
DISTRRO-1(config-if)#no switchport
DISTRRO-1(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/1, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/1, changed state to up

DISTRRO-1(config-if)#ip add
DISTRRO-1(config-if)#ip address 192.168.17.14 255.255.255.252
DISTRRO-1(config-if)#no shu
DISTRRO-1(config-if)#
  
```

Ilustración 6.configuración de core

CORE 2 -> DISTRIBUCION 1 -> 1/0/2 -> RED = 192.168.17.12/30  
 192.168.17.13 /30 -> DISTRIBUCION 1 por Gigabit 1/0/2

```
Switch>en
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#inter
Switch(config)#interface gig
Switch(config)#interface gigabitEthernet 1/0/2
Switch(config-if)#no swi
Switch(config-if)#no switchport
Switch(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/2, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/2, changed state to up

Switch(config-if)#ip add
Switch(config-if)#ip address 192.168.17.12 255.255.255.252
Bad mask /30 for address 192.168.17.12
Switch(config-if)#exit
Switch(config)#interface gigabitEthernet 1/0/2
Switch(config-if)#ip address 192.168.17.13 255.255.255.252
Switch(config-if)#no shu
Switch(config-if)#no shutdown
Switch(config-if)#
```

Ilustración 7. configuración de core

## AGREGANDO LAS VLANS AL ÁREA 0 EN OSPF EN DISTRIBUCIÓN 1

```
Physical Config CLI Attributes
IOS Command Line Interface
Press RETURN to get started.

DISTRO-1#en
DISTRO-1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
DISTRO-1(config)#ip routing
DISTRO-1(config)#router ospf 1
DISTRO-1(config-router)#router-id 3.3.3.3
DISTRO-1(config-router)#net
DISTRO-1(config-router)#network 192.168.7.0 0.0.255.255 area 0
DISTRO-1(config-router)#network 192.168.7.0 0.0.255.255 area 0
DISTRO-1(config-router)#exit
DISTRO-1(config)#router ospf 1
DISTRO-1(config-router)#router-id 3.3.3.3
DISTRO-1(config-router)#net
DISTRO-1(config-router)#network 192.168.31.0 0.0.255.255 area 0
DISTRO-1(config-router)#network 192.168.31.0 0.0.255.255 area 0
DISTRO-1(config-router)#network 192.168.30.0 0.0.255.255 area 0
DISTRO-1(config-router)#exit
DISTRO-1(config)#

06:14:55: %OSPF-5-ADJCHG: Process 1, Nbr 1.1.1.1 on GigabitEthernet1/0/2 from LOADING to FULL,
Loading Done
06:14:57: %OSPF-5-ADJCHG: Process 1, Nbr 2.2.2.2 on GigabitEthernet1/0/1 from LOADING to FULL,
Loading Done

DISTRO-1(config-router)#net
DISTRO-1(config-router)#network 192.168.1.0 0.0.255.255 area 0
DISTRO-1(config-router)#network 192.168.1.0 0.0.255.255 area 0
DISTRO-1(config-router)#network 192.168.2.0 0.0.255.255 area 0
DISTRO-1(config-router)#network 192.168.3.0 0.0.255.255 area 0
DISTRO-1(config-router)#network 192.168.4.0 0.0.255.255 area 0
DISTRO-1(config-router)#network 192.168.5.0 0.0.255.255 area 0
DISTRO-1(config-router)#network 192.168.6.0 0.0.255.255 area 0
DISTRO-1(config-router)#
```

Ilustración 8. configuración de VLAN

## AGREGANDO LAS VLANS AL ÁREA 0 EN OSPF EN DISTRIBUCIÓN 2

```

DISTRIBUCION 2
Physical Config CLI Attributes
IOS Command Line Interface
Press RETURN to get started.

DISTRIBUCION 2>en
DISTRIBUCION 2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
DISTRIBUCION 2(config)#ip routing
DISTRIBUCION 2(config)#router ospf 1
DISTRIBUCION 2(config-router)#router-id 4.4.4.4
DISTRIBUCION 2(config-router)#net
DISTRIBUCION 2(config-router)#network 192.168.10.0 0.0.0.3 area 0
DISTRIBUCION 2(config-router)#network 192.168.17.4 0.0.0.3 area 0
DISTRIBUCION 2(config-router)#network 192.168.17.4 0.0.0.3 area 0
06:00:18: %OSPF-5-ADJCHG: Process 1, Nbr 1.1.1.1 on GigabitEthernet1/0/1 from LOADING to FULL,
Loading Done
DISTRIBUCION 2(config-router)#network 192.168.17.16 0.0.0.3 area 0
DISTRIBUCION 2(config-router)#
06:00:17: %OSPF-5-ADJCHG: Process 1, Nbr 2.2.2.2 on GigabitEthernet1/0/2 from LOADING to FULL,
Loading Done
DISTRIBUCION 2(config-router)#network 192.168.9.0 0.0.255.255 area 0
DISTRIBUCION 2(config-router)#network 192.168.11.0 0.0.255.255 area 0
DISTRIBUCION 2(config-router)#network 192.168.12.0 0.0.255.255 area 0
DISTRIBUCION 2(config-router)#network 192.168.13.0 0.0.255.255 area 0
DISTRIBUCION 2(config-router)#network 192.168.14.0 0.0.255.255 area 0
DISTRIBUCION 2(config-router)#network 192.168.16.0 0.0.255.255 area 0
DISTRIBUCION 2(config-router)#
Copy Paste

```

Ilustración 9.configuración de VLAN

## AGREGANDO LA VLAN ESPECÍFICA PARA EL DEPARTAMENTO DE INGENIERIA

```

Ingeniería y Arqu.
Physical Config CLI Attributes
IOS Command Line Interface
Switch(config)#interface gigabitEthernet 1/0/3
Switch(config)#interface gigabitEthernet 1/0/3
% Invalid input detected at '^' marker.
Switch(config)#interface fas
Switch(config)#interface fastEthernet 0/1
Switch(config-if)#swi
Switch(config-if)#switchport mode
Switch(config-if)#switchport mode trun
Switch(config-if)#switchport mode trunk
Switch(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up
Switch(config-if)#switchport mode trunk enca
Switch(config-if)#switchport trun
Switch(config-if)#switchport trunk enca
Switch(config-if)#switchport trunk encapsu
Switch(config-if)#switchport trunk encapsulation dotiq
Switch(config-if)#
% Invalid input detected at '^' marker.
Switch(config-if)#switc
Switch(config-if)#switchport mode
Switch(config-if)#switchport mode tr
Switch(config-if)#switchport mode trunk
Switch(config-if)#switch
Switch(config-if)#switchport tru
Switch(config-if)#switchport trunk enc
Switch(config-if)#switchport trunk
% Incomplete command.
Switch(config-if)#switchport trunk
Switch(config-if)#switchport trunk
Switch(config-if)#switchport trunk
Switch(config-if)#switchport acc
Switch(config-if)#switchport access vlan 6
Switch(config-if)#
Copy Paste

```

Ilustración 10.configuración de VLAN

ASIGNANDO VLAN 13 BIOLOGÍA DE MANERA LOCAL EN EL SWITCH DE ACCESO Y DÁNDOLE SALIDA TRONCAL AL DE DISTRIBUCIÓN PARA QUE SE COMUNIQUE CON OTRA VLAN

```

Biologia
Physical Config CLI Attributes
IOS Command Line Interface

%LINK-5-CHANGED: Interface FastEthernet0/3, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to up
%LINK-5-CHANGED: Interface FastEthernet0/4, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/4, changed state to up

Switch>en
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#vlan 13
Switch(config-vlan)#name BIOLOGIA
Switch(config-vlan)#exit
Switch(config)#inter
Switch(config)#interface fas
Switch(config)#interface fastEthernet 0/4
Switch(config-if)#swi
Switch(config-if)#switchport mode acc
Switch(config-if)#switchport mode access
Switch(config-if)#sw1
Switch(config-if)#switchport acc
Switch(config-if)#switchport access vlan 13
Switch(config-if)#exit
Switch(config)#inter
Switch(config)#interface fas
Switch(config)#interface fastEthernet 0/1
Switch(config-if)#swit
Switch(config-if)#switchport mode
Switch(config-if)#switchport mode trun
Switch(config-if)#switchport mode trunk

Switch(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up

Switch(config-if)#no shu
Switch(config-if)#no shutdown
Switch(config-if)#
Copy Paste
Top

```

Ilustración 11.configuración de VLAN

```

Educacion
Physical Config CLI Attributes
IOS Command Line Interface

%LINK-5-CHANGED: Interface FastEthernet0/2, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to up

Switch>en
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#vlan 11
Switch(config-vlan)#name BIOLOGIA
Switch(config-vlan)#exit
Switch(config)#inter
Switch(config)#interface fas
Switch(config)#interface fastEthernet 0/2
Switch(config-if)#sw1
Switch(config-if)#switchport mode acc
Switch(config-if)#switchport mode access vlan 11
Switch(config-if)#switchport mode access
Switch(config-if)#switchport mode access
Switch(config-if)#switchport acc
Switch(config-if)#switchport access vla
Switch(config-if)#switchport access vlan 11
Switch(config-if)#exit
Switch(config)#interf
Switch(config)#interface fas
Switch(config)#interface fastEthernet 0/1
Switch(config-if)#sw1
Switch(config-if)#switchport mode
Switch(config-if)#switchport mode tr
Switch(config-if)#switchport mode trunk

Switch(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up

Switch(config-if)#no shu
Switch(config-if)#no shutdown
Switch(config-if)#
Copy Paste
Top

```

Ilustración 12.configuración de VLAN

AGREGANDO VLAN 8 AL PUERTO DEL SERVIDOR DHCP Y AL PUERTO DEL SERVIDOR DNS y DÁNDOLE SALIDA POR EL PUERTO QUE VA AL SWITCH DISTRIBUCION 1

```

Switch>en
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#interf
Switch(config)#interface fas
Switch(config)#interface fastEthernet 0/4
Switch(config-if)#swi1
Switch(config-if)#swi
Switch(config-if)#switchport mode ac
Switch(config-if)#switchport mode access
Switch(config-if)#swi
Switch(config-if)#switchport acc
Switch(config-if)#switchport access vlan 8
Switch(config-if)#no shu
Switch(config-if)#no shutdown
Switch(config-if)#exit
Switch(config)#inter
Switch(config)#interface fas
Switch(config)#interface fastEthernet 0/3
Switch(config-if)#swi
Switch(config-if)#switchport mode
Switch(config-if)#switchport mode access
Switch(config-if)#swi
Switch(config-if)#switchport acc
Switch(config-if)#switchport access vlan 8
Switch(config-if)#no shuc
Switch(config-if)#no shutdown
Switch(config-if)#exit
Switch(config)#inter
Switch(config)#interface fas
Switch(config)#interface fastEthernet 0/5
Switch(config-if)#swi
Switch(config-if)#switchport mode
Switch(config-if)#switchport mode tru
Switch(config-if)#switchport mode trunk

Switch(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/5, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/5, changed state to up
  
```

Ilustración 13.configuración de VLAN  
DHCP SUCCESSFUL

The screenshot shows the configuration of a PC (PC4) in a network simulation. The 'IP Configuration' tab is active, showing the following settings for the 'FastEthernet0' interface:

- IP Configuration:**
  - DHCP (DHCP request successful.)
  - Static
  - IPv4 Address: 192.168.10.2
  - Subnet Mask: 255.255.255.0
  - Default Gateway: 192.168.10.1
  - DNS Server: 192.168.7.4
- IPv6 Configuration:**
  - Automatic
  - Static
  - IPv6 Address: [Empty]
  - Link Local Address: FE80::201:C9FF:FED0:E977
  - Default Gateway: [Empty]
  - DNS Server: [Empty]
- 802.1X:**
  - Use 802.1X Security
  - Authentication: MD5
  - Username: [Empty]
  - Password: [Empty]

To the right, a network diagram shows a switch (2960-24TT) connected to two PCs (PC4 and PC7). The switch has two interfaces: Fa0/1 (connected to PC4) and Fa0/24 (connected to PC7). The switch is configured with two VLANs: 2.168.9.0/24 and 68.10.0/24. The PC4 is connected to the 2.168.9.0/24 VLAN, and the PC7 is connected to the 68.10.0/24 VLAN.

Ilustración 14.configuración de servidor DHCP

## SERVER DHCP

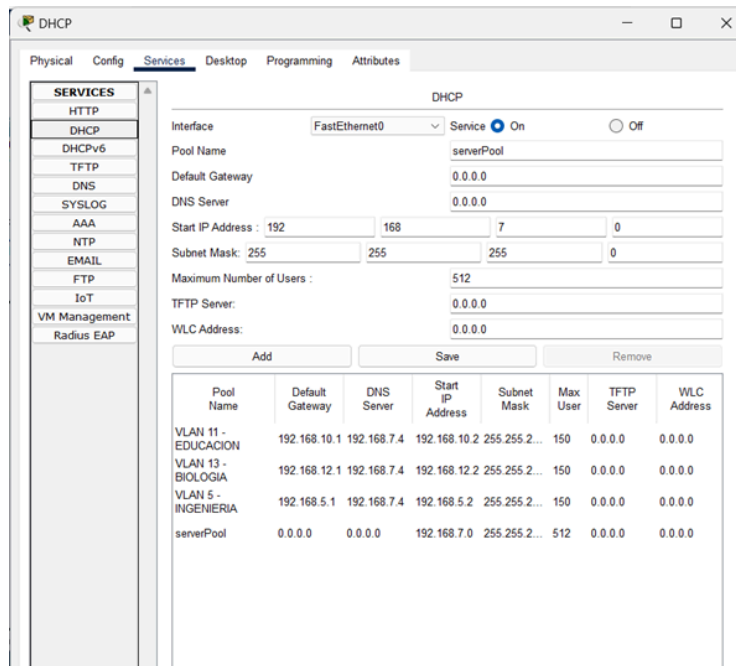


Ilustración 15.configuración servidor DHCP

```

DISTRO-1>enable
DISTRO-1#
DISTRO-1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
DISTRO-1(config)#interface GigabitEthernet1/0/1
DISTRO-1(config-if)#
DISTRO-1(config-if)#exit
DISTRO-1(config)#
DISTRO-1(config)#
DISTRO-1(config)#inte
DISTRO-1(config)#interface vlan 6
DISTRO-1(config-if)#ip hel
DISTRO-1(config-if)#ip help
DISTRO-1(config-if)#ip helper-address 192.168.7.3
DISTRO-1(config-if)#no shu
DISTRO-1(config-if)#no shutdown
DISTRO-1(config-if)#exit
DISTRO-1(config)#

```

Ilustración 16.configuración de servidor DHCP

```
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/6, chang  
  
DISTRO-2>  
DISTRO-2>enable  
DISTRO-2#conf t  
Enter configuration commands, one per line. End with CNTL/Z.  
DISTRO-2(config)#inter  
DISTRO-2(config)#interface vlan 11  
DISTRO-2(config-if)#ip help  
DISTRO-2(config-if)#ip helper-address 192.168.7.3  
DISTRO-2(config-if)#no shu  
DISTRO-2(config-if)#no shutdown  
DISTRO-2(config-if)#
```

Ilustración 17.configuración de VLAN

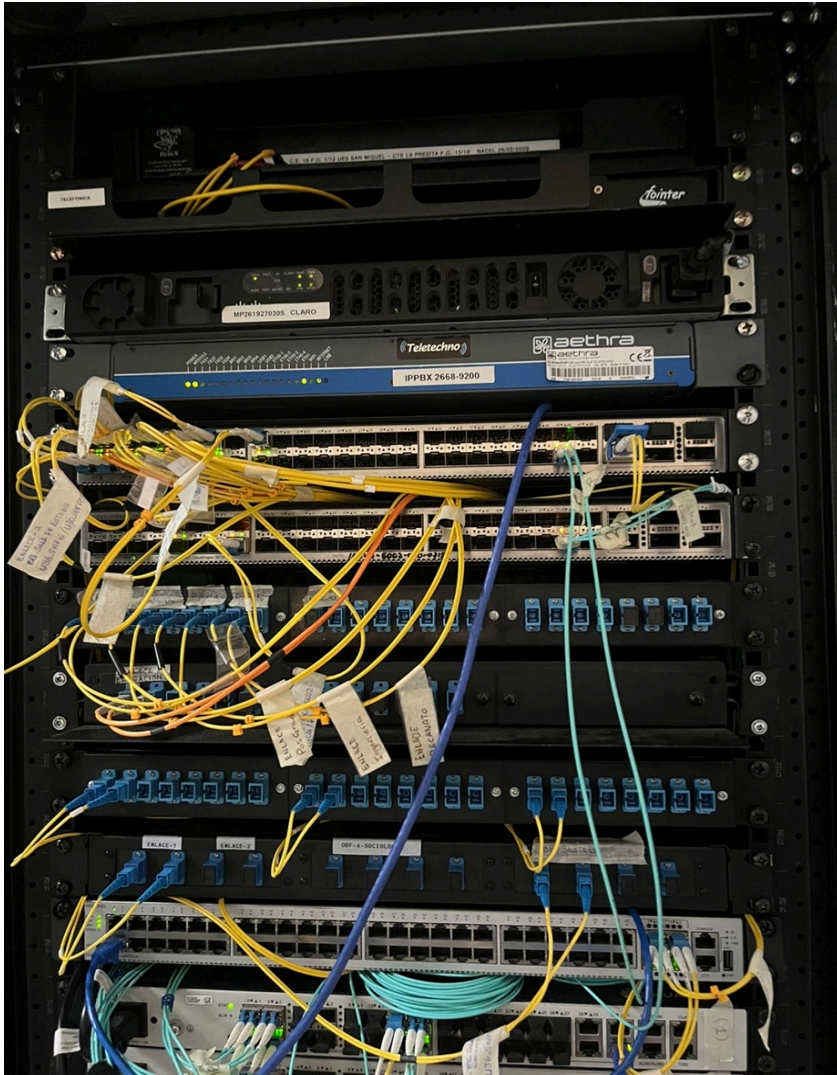


Ilustración 18.conecciones data center



Ilustración 19.conecciones data center

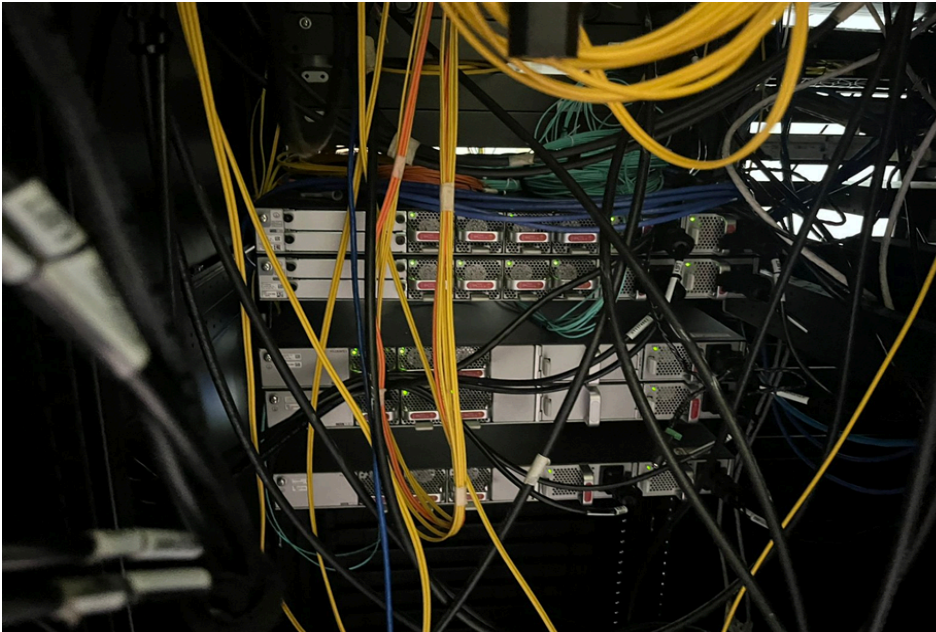


Ilustración 20.conecciones data center



Ilustración 22.punto de distribución de red wifi